
autentikacija
ZAŠTITA
Vanja Korać
Andrej Diligenski
Dragan Prlja
BEZBEDNOST
PODACI
informacije
INTEGRITET
LINUX
DIGITALNA
FORENZIKA
WINDOWS
autentikacija
neporecivost
ZAŠTITA
BEZBEDNOST
informacije

Vanja Korać
Dragan Prlja
Andrej Diligenski

DIGITALNA FORENZIKA

Vanja Korać
Dragan Prlja
Andrej Diligenski

DIGITALNA FORENZIKA

Beograd, 2016.

Vanja Korać
Dragan Prlja
Andrej Diligenski
DIGITALNA FORENZIKA

Izdavači
Centar za nove tehnologije Viminacium
Arheološki Institut Beograd
Institut za uporedno pravo

Za izdavače
dr Miomir Korać, direktor
dr Jovan Ćirić, direktor

Recenzenti
Prof. dr Stevan Lilić
Prof. dr Gojko Grubor
Prof. dr Žarko Mijajlović

Urednik
dr Miomir Korać

Dizajn korica
dipl. inž. arh. Tijana Milanović

Dizajn i tehničko uređenje
Digital Art Company, Beograd

Štampa
Digital Art Company, Beograd

ISBN
978-86-87271-34-0

Tiraž
300

SADRŽAJ

UVOD

Sa pojavom računarskih mreža, njihovom ekspanzijom i integracijom u sistem globalne mreže - interneta, dolazi do njene zloupotrebe u smislu narušavanja njene prvobitno osmišljene funkcije - prenosa informacija i komunikacija. Tehnologija je, sa jedne strane, postala moćan alat, međutim sa druge strane ona može biti i zloupotrebljena sa neverovatnom lakoćom. Uklanjanje fizičkih ograničenja i zloupotrebe interneta mogu biti izazvane najrazličitijim oblicima malicioznih programa, ili direktnim napadom zlonamernog napadača.

Razlozi za pojavu ovih napada su različiti i generalno se mogu podeliti na materijalno i nematerijalno motivisane. Na prvom mestu razlog je sticanje finansijske dobiti. Kao drugi motivi za napade na računarske sisteme ističu se izazov, znatiželja, samopotrvđivanje, krađa podataka, špijunaža i drugi. Pod kompjuterskim kriminalom u najširem smislu podrazumevaju se krivična dela prema krivičnom zakonu nacionalne države, u kojoj su na bilo koji način uključeni računarski sistemi i mreže.[1] Glavni cilj istrage visokotehnolškog kriminala je, kao i u slučaju klasičnog kriminala, izgraditi za pravosudne organe neoboriv, ili čvrst dokaz, i/ili dokaz za oslobadanje osumnjičenog, i/ili pravedno sankcionisanje učinjenog dela.[2] Da bi se obezbedio takav dokaz, u slučaju visokotehnološkog kriminala, neophodno je, uz pomoć niza posrednih dokaza, pronaći informacije u digitalnom obliku koje imaju verodostojnu vrednost, a koje su uskladištene ili prenesene u digitalnom obliku. Takve informacije se nazivaju digitalni dokazi. Digitalni dokazi mogu biti u formi koju generiše sam sistem kao proizvod rada računarskog sistema (sistemski logovi) i dokazi koji su uskladišteni na računarskom sistemu kao na primer baza podataka korisnika.

Bilo da je reč o zvaničnoj ili korporativnoj istrazi, u toku prikupljanja, analize i prezentacije digitalnih dokaza moraju se poštovati određeni principi. Kada je reč o visokotehnološkom kriminalu najčešće se zahteva i svedočenje ili veštačenje eksperta. U Srbiji postoji regulatorno telo koje izdaje licence potrebne za vršenje eksperstkog veštačenja iz oblasti digitalne forenzike. Fizičko lice može obavljati veštačenja ukoliko je upisano u Registar veštaka. Pravno lice može obavljati veštačenja ako ispunjava sledeće uslove: ako je

1 APWG, *Phishing Activity Trends Report, 3rd Quarter (July – September 2012)*, 2013, http://www.apwg.org/download/document /84/apwg_trends_ report_q3_2012.pdf, 20.07.2016.

2 Popek J. G., Goldberg P. R., *Formal requirements for virtualizable third generation architectures*, Communications of the ACM 17 (7), 1974, str. 412–421.

upisano u registar nadležnog organa za delatnost veštačenja u odgovarajućoj oblasti i ako su u njemu zaposlena lica, koja su upisana u Registar veštaka Ministarstva pravde.

Uspešno suzbijanje visokotehnološkog kriminala podrazumeva stalni razvoj digitalne forenzike. Činjeničko stanje u oblasti visokotehnološkog kriminala je sledeće:

1. gotovo da ne postoji nijedna veća organizacija na svetu koja nije pretrpela kompromitovanje svojih sistema od strane napadača;
2. većina *outsourced* (eng. outsourced) programa se pravi sa backdoor-ovima, što može napadaču da omogući upad u sistem;
3. *firewall* sistemi za detekciju napada na sistem (eng. intrusion detection system - IDS) i antivirusi nisu rešili bezbednosne probleme;
4. postoji veliki broj umreženih računara (tzv. *botnet* mreža) namenjenih distribuciji nelegalnih sadržaja ili piraterije;
5. dok pišemo ovu knjigu postoje na stotine ne objavljenih exploita koji se koriste.

Na osnovu svetskih statistika može se reći da je trenutno u svetu od kriminala procentualno najdominantniji visokotehnološki kriminal. S ozbirom na dinamičan porast visokotehnološkog kriminala i njegovih novih pojavnih oblika od digitalne forenzike se očekuje da isprati sve tehnološke promene u informatici kako bi se što efikasnije suočila sa izazovima koje sajber kriminal donosi.

Zato je bavljenje digitalno forenzičkim procesima postalo nezaobilazna disciplina, kada je reč o otkrivanju nedozvoljenih digitalnih aktivnosti i računarskih incidenata, kako sa aspekta zvanične istrage, tako i sa aspekta korporacijske istrage. Digitalno forenzički procesi mogu da se prošire i na istraživanje bezbednosti u okviru organizacija sa ciljem pronalaženja tzv. „zero date" ranjivosti (ranjivosti za koji ne postoji patch razvijen od strane vendora), čime bi bili obuhvaćeni i hardver i programi.

Istraživanje incidentnih/nedozvoljenih aktivnosti podrazumeva *prikupljanje* digitalnih *podataka* (potencijalnih dokaza) sa računarskih sistema i mrežnih uređaja *utvrđivanje autentičnosti i njihovu analizu*. Pre svake istrage podrazumeva se ispitivanje potrebnih preduslova kao što su: postojanje dovoljnog broja obučenih profesionalaca, postojanje forenzičkih radnih stanica i forenzičkih laboratorija za oporavak podataka, saradnja sa javnim tužilaštvom i definisanje metodologije istrage. U zavisnosti od tipa

istrage (zvanična ili korporativna) zavisi i ko će dati forenzički inicijalni na incidnentnu/nedozvoljenu aktivnost.

Koliku važnost ima forenzički odgovor i koliko je on osetljiv, možda je i najslikovitiji opis o potrazi za digitalnim podacima dao Fridman u sledećim rečenicama svoje knjige:

"*Svi podaci ostavljaju trag. Potraga za podacima ostavlja trag. Brisanje podataka ostavlja trag. Odsustvo podataka pod određenim okolnostima može da ostavi najjasniji trag od svih.*".[3]

Prema tome, digitalni podaci generisani ili uneti u računar ostavljaju brojne tragove u operativnim sistemima. Pretraga za podacima podrazumeva priključivanje forenzičkog alata, što znači ostavljanje tragova na digitalne podatke (Lokardov zakon). Izbrisani podaci ostavljaju tragove u nealociranim i slek prostorima diska, a odsustvo podataka ukazuje na antiforenzičku aktivnost i predstavlja jaku osnovu za sumnju u nedozvoljene aktivnosti. Virusi na primer ostavljaju svoj kod u zaraženim programima. Tragovi kompromitovanja mogu biti prisutni u različitim oblicima na primer u izvornim fajlovima programskog jezika, u objektnim fajlovima (eng. Object files), u izvršnim kodovima, u šel skriptama, u izmenema nad postojećim programima ili čak u tekstualnim fajlovima pisanim od strane napadača. Za istragu je vrlo značajno ukoliko bi se ovi delovi informacija mogli iskoristiti za utvrđivanje izvora napada.[4] Prikupljanje podataka može da podrazumeva prikupljanje podataka iz živog sistema (eng. live) da bi se sakupile osetljive tj. nestabilne informacije ili se vrši post-mortem prikupljanje podataka bez izmene ili oštećenja i u tom slučaju se vrši preuzimanje fizičkih dokaza (kao na primer hard diskovi, diskete ili drugi mediji). Nakon preuzimanja fizičkih dokaza vrše se forenzička dupliranja – uzimanje softerskog imidža ili kloniranje diska računarskih dokaza i utvrđuje se autentičnost između originalnog digitalnog dokaza sa forenzičkom kopijom. Paralelno se vrši istraživanje i nadzor mreže za dobijanje dodatnih informacija. Pored toga, za dobijanje dodatnih informacija vrše se i intervjui sa odgovarajućim ljudima koji imaju određene detalje u vezi sa incidentnom odnosno nedozvoljenom aktivnošću.

---

3 C.S.Friedman, *This Alien Shore*, DAW BOOKS, INC, New York 1998, http://rose.digitalmidnight.org/ temp/books/ CS_ Friedman/C.%20S.%20Friedman%20-%20This%20Alien%20Shore.pdf, 23.01.2016.

4 One A., *Smashing the Stack for Fun and Profit*, Phrack, Volume 7, Issue 49, 1996.

Kada se podaci prikupljaju iz "živog" operativnog sistema važno je znati koji su podaci lako promenljivi tj. podaci privremenog karaktera (eng. volatile), a koji podaci su postojanog karaktera (eng. non-volatile). Na prvom mestu "lako izmenjivih" podataka odnosno volatile podaci, sistemski detalji koji istražiteljima pružaju uvid u način i prirodu kompromitovanja sistema i nekada mogu biti podaci od krucijalnog značaja. Od podatka koji neće lako biti izmenjeni u sistemu, na prvom mestu su oni koji daju informacije o statusu, setovanjima, konfiguraciji sistema i istorijske informacije na osnovu kojih se može utvrditi način i priroda kompromitovanja sistema. Treba napomenuti da forenzički odgovor "uživo" ne može dati uvek adekvatne rezultate, ali može dati dobru predstavu o onom šta se desilo. Dodatne analize moguće je uraditi sa mrežnom forenzikom, a kasnije forenzičkom duplikacijom, post-mortem forenzikom (analiza fajlova: slika, audio video fajlova, arhiva i dokumenta).

Cilj naše knjige je da se pruži prikaz stanja oblasti digitalne forenzike, da se baci svetlo na metode i tehnike digitalne forenzike računarskih sistema koji otkrivaju ovakvu vrstu kriminala i preventivno deluju kao vid zaštite računarskih sistema. Analizom će se pokazati stanje sistema, tj. koliko je sistem ranjiv posle njegove instalacije na računaru. Na taj način se detektuju ranjivosti u sistemu, dobijaju se preporuke za prevazilaženje ovih bezbedonosnih problema, čime se preventivno deluje protiv mogućeg forenzičkog relevatnog događaja. Tako da se ovo sveobuhvatno istraživanje može posmatrati i kao jedna proaktivna digitalna forenzika u smislu spremnog dočekivanja, ali i otkrivanja forenzički relevatnog događaja.

Napomena: Zbog specifične stručne terminologije u ovoj multidisciplinarnoj materiji upućujemo čitaoce da pogledaju poglavlje br. 7 „Rečnik pojmova i izraza".

1. SAJBER KRIMINAL

Sa pojavom prvih računara pa do danas prošlo je skoro 60 godina. Iako skromni po mogućnostima, a veliki po gabaritima, na samom početku oni su bili namenjeni da olakšaju i ubrzaju kompleksne proračune iz naučnih i tehničkih oblasti kao i obrađivanje velikih količina podataka kako u poslovnom tako i na administrativnom polju.

Pojava savremenih računara i široka rasprostranjenost velike količine najrazličitijih korisničkih programa uticali su na promene života ljudi širom sveta. Današnji računari koji postaju sve manji, a istovremeno „snažniji", nalaze primenu gotovo u svim naučnim oblastima od planiranja, prikupljanja, proračuna i obrade podataka do analize i projektovanja procesa i vrednovanja istog, na primer u računarskoj grafici, obrazovanju, saobraćaju, komunikaciji, informisanju, umetnosti, zabavi, upravljanju uređajima, bezbednosti, veštačkoj inteligenciji itd. Međutim, mora se razumeti da ona sa sobom donosi i mnogo rizika.

Paralelno sa ovakvim razvojem računara razvile su se i računarske mreže, od kojih je najpoznatija tzv. globalna mreža – internet. Kolika je danas upotreba interneta u svetu možda najbolje odslikava sledeća tabela:

Tabela br. 1: Upotreba interneta u svetu dan 30. novembar 2015.g.

Statistika upotrebe interneta u svetu u odnosu na populaciju **30. novembar 2015.**					
Svetski regioni	**Populacija (2015)**	**Internet korisnici 30. nov. 2015**	**Penetracija (% populacije)**	**Rast 2000-2015**	**Korisnici %** prema tabeli
Afrika	1,158,355.663	330,965,359	28.6 %	7,231.3 %	9.8 %
Azija	4,032,466,882	1,622,084,293	40.2 %	1,319.1 %	48.2 %
Evropa	821,555,904	604,147,280	73.5 %	774,9 %	18.0 %
Srednji istok	236,137,235	123,172,132	52.2 %	3,649.8 %	3.7 %
Severna Amerika	357,178,284	313,867,363	87.9 %	190.4 %	9.3 %
Latinska Amerika / Karibi	617,049,712	344,824,199	55.9 %	1,808.4 %	10.2 %
Okeanija / Australija	37,158,563	27,200,530	73.2 %	256.9 %	0.8 %
SVET UKUPNO	**7,259,902,243**	**3,366,261,156**	**46.4 %**	**832.5 %**	**100.0 %**
Izvor: InternetWorldStats - http://www.internetworldstats.com/stats.htm, statistika je bazirana na osnovu obuhvaćenih **3,366,261,156 internet korisnika.** Copyright © 2015, Miniwatts Marketing Group					

S obzirom da novu tehnologiju koristi *3,366,261,156* mora se razumeti

da ona sa sobom donosi i mnogo rizika. Tehnologija sa jedne strane, može postati moćno oružje u našim rukama, međutim isto tako ono može biti usmereno i protiv nas jer je to oružje postalo globalno dostupno. Nažalost, možemo da konstatujemo da je ovakav tehnološki progres pratilo i razvijanje ideje o korišćenju novih tehnologija u nedozvoljene svrhe. Internet je uvećao lakoću i brzinu kojom se sprovode kriminalne radnje uklanjajući fizička ograničenja i smanjujući fizički napor da bi se neko prevario. Npr. iz banke mogu biti ukradene milijarde dolara u online okruženju za nekoliko minuta, za razliku od perioda pre pojave interneta kada su razbojnici fizički pljačkali banke i bili ograničeni i vremenom i količinom novca koji mogu da iznesu iz banke uz ogromnu količinu utrošene fizičke energije.

Za razliku od prvih računara koji su bili izolovani od uticaja ostalih računara, nakon početka njihove masovnije proizvodnje osmišljene su računarske mreže i to u vrlo kratkom vremenskom periodu, sa ciljem da se podaci, koji se nalaze na različitim računarima mogu deliti (eng. share) i distribuirati pojedinim ili svim korisnicima određene mreže. Danas se primeri ovakvih mreža mogu naći praktično u svakoj organizaciji čiji zaposleni koriste računare u svom poslu, umrežene u jedinstveni sistem radi lakše i brže međusobne komunikacije. Nažalost takav sistem je dvostruko ranjiv – kako spolja tako i iznutra.

Fantastičnim razvojem informaciono-komunikacionih tehnologija (u daljem tekstu IKT) i računarskih mreža, već sedamdesetih godina prošlog veka dolazi do pojave visokotehnološkog kriminala.

Globalna ekspanzija korisnika interneta (31. Decembra 2000. godine je bilo *360,985,492* korisnika, 31.marta 2011 taj broj je *2,095,006,005***,** dok je 30. novembra 2015. godine taj broj bio *3,366,261,156*) čiji se godišnji rast meri geometrijskom progresijom, imala je za posledicu i globalni talas krivičnih dela koja su povezana sa računarskim tehnologijama.[5] Još devedesetih godina zajedno sa rastom korisnika interneta rastao je i globalni talas visokotehgnološkog kriminala. U SAD je 1995. godine uhapšen i osuđen Kevin Mitnik zbog falsifikovanja 20.000 kreditnih kartica. U Londonu je 1997. godine uhapšen Vladimir Levin iz Petrograda koji je od juna do avgusta 1994. godine u 18 upada ukrao 10 miliona dolara iz sistema Siti banke. U SAD je 1998.g. uhapšen i osuđen Robert Moris zbog prvog masovnog napada na internetu kada je u mrežu ubacio samorepliciraući program koji je uništavao podatke na računarima i širio se samostalno po mreži (tzv. "crv", engl. "worm").[6] Ovo je bio

5 Miniwatts Marketing Group, *Internet World Stats*, http://www.internetworldstats.com/stats.htm, 09.07.2016.

6 Acunetix Ltd., *Acunetix Web Vulnerability Scanner*, Manual v. 4.0, Acunetix Ltd, 2006, http://www.acunetix.com/vulnerability-scanner, 10.07.2016.

samo početak, jer je visokotehnološki kriminal postao svakodnevica, a razvoj tehnologija je uslovio i neverovatnu diferencijaciju vrsta nedozvoljenih dela koja se mogu izvršiti njihovim korišćenjem od onih naivnih i bezopasnih, koja se uglavnom vezuju za reklamiranje različitih proizvoda, do veoma opasnih ponašanja koja spadaju među teška (ponekad čak i najteža) krivična dela u mnogim nacionalnim zakonodavstvima.[7] U stvari visokotehnološki kriminal podrazumeva korišćenje interneta, računara, mreža i srodnih tehnologija u izvršenju krivičnog dela uključujući kako tehnološki specifična krivična dela tako i tradicionalna krivična dela uz pomoć IKT. U otkrivanju i sankcionisanju visokotehnološkog kriminala, digitalna forenzika je nezamenljiv alat. Naša knjiga je usmerena pre svega na digitalnu forenziku informacionih sistema baziranih na Windows i Linux platformama.

1.1. VISOKOTEHNOLOŠKI KRIMINAL - SAJBER KRIMINAL - RAČUNARSKI KRIMINAL

Napredak računarskih i komunikacionih tehnologija uslovio je neverovatno brz razvoj elektronskog poslovanja pa su se odmah potom pojavili i oni koji su želeli da zloupotrebe mogućnosti novih tehnologija. Oni koji su i do tada činili krivična dela nastojali su da za svoje aktivnosti iskoriste nove tehnologije, ali se pojavio i veliki broj novih počinilaca koji nisu imali kriminalnu prošlost.[8]

Sinonimi koje najčešće srećemo u literaturi povodom ove nove vrste kriminala su internet kriminal, eKriminal, računarski kriminal, mrežni kriminal, tehnološki kriminal, informacioni kriminal, elektronski kriminal, digitalni kriminal i termin koji se koristi u našem zakonodavstvu visokotehnološki kriminal. Iako ne postoji zvanična i opšteprihvaćena definicija ovog pojma kriminaliteta, termin sajber kriminal je u literaturi dominantno zastupljen u Americi, a naše zakonodavstvo ga definiše kao visokotehnološki kriminal pa ćemo u daljem tekstu ovu vrstu kriminala nazivati visokotehnološki kriminal.

S obzirom da ne postoji opšteprihvaćena definicija koja se vezuje za ovu vrstu kriminala u daljem tekstu biće izložene one definicije koje su najzastupljenije u relevatnim literaturama koja se bave ovom oblašću.

Šta je međutim, tačno: visokotehnološki kriminal ili sajber kriminal, kako glasi američki naziv ove vrste kriminala koji se odomaćio u mnogim svetskim jezicima? Jedinstveni odgovor na ovo pitanje još ne postoji, ali ono

7 *Ibidem.*

8 Dragan Prlja, Vanja Korać, i Andrej Diligenski, *Maloletnici i sajber kriminal*, u: Maloletnici kao učinioci i žrtve krivičnih dela i prekršaja, Beograd, Institut za kriminološka i sociološka istraživanja, 2015, str. 351.

što je zajedničko za mnoge definicije koje određuju ovaj pojam, može se uočiti zajednički element – *korišćenje računara ili računarske mreže i interneta*. U svetu istraživanja visokotehnološkog kriminala ovakvo usko tumačenje ovog termina koristi veliki broj internet enciklopedija i rečnika, pa sajber kriminal definišu kao „kriminalnu aktivnost počinjenu korišćenjem računara i interneta".[9]

Neki autori ističu da se u praksi može dogoditi da počinilac koristi, pored računara, mnogo drugih sredstava za izvršenje krivičnog dela, pa je očigledno da ovako uska definicija nikako ne zadovoljava sve potrebe percipiranja ove vrste kriminaliteta, koje je od velike važnosti za njihovo dalje suzbijanje. Identifikovati šta predstavlja krivično delo visokotehnološkog kriminala i kako se ono razlikuje od drugih vrsta nepoželjnog ponašanja koje nije uvek društveno opasno, osnovni je problem koji nijedna definicija još uvek nije uspela da prevaziđe. I pored velikih napora da se ovaj problem što jednostavnije, a opet što preciznije odredi, završava se identifikacijom sajber kriminala kao vršenje krivičnih dela upotrebom računara ili računarskih mreža.[10] Iako naizgled suviše jednostavna, ova definicija veoma dobro pokriva široko polje mogućeg kriminalnog delovanja. Ono što se uzima kao zamerka koncepcijske prirode odnosi se na činjenicu da nisu samo računari moguća sredstva zloupotrebe novih tehnologija. Ukoliko se ona uopšti i ispravi tako da pod sajber kriminalom obuhvati i one nedozvoljene aktivnosti preduzete nekim drugim digitalnim uređajima i internetom, ta bi definicija zbog svoje širine bila sveobuhvatnija. Na ovaj način obuhvaćeno je sve od nelegalnog preuzimanja raznih vrsta muzičkih i video fajlova pa do velikih finansijskih zloupotreba sa online bankovnih računa. Ostala dela se moraju inkriminisati u okviru postojećih krivičnih dela, kao njihovi specifični oblici. Pri tome se mora voditi računa o činjenici da savremene tehnologije napreduju daleko brže od mogućnosti zakonodavca da vrši izmene krivičnog prava, kao i o činjenici da u mnogim od ovih oblasti ne postoje utvrđeni međunarodni standardi, niti nedvosmislena praksa.[11]

Izdvojićemo jednu najpotpuniju, mada mažda ne i najpreciznu definiciju o kompleksnom pojmu sajber kriminala predstavljenu na Desetom

9 Http://www. techterms. com/ definition/ cybercrime, http://www. crime - research. org/ analytics/ 702, http://www.thefreedictionary.com /cybercrime, http://www. webopedia.com/ TERM/C/ cyber_crime. html, http://www.pcmag.com/ encyclopedia_ term/0,2542,t=cybercrime&i=40628,00.asp, 21.11.2015.

10 Vangie Beal, *Cyber Crime*, Webopedia, http://www.webopedia.com/TERM/C/cyber_crime. html, 21.11.2015.

11 Dragan Prlja, Mario Reljanović, *Pravna informatika*, Pravni fakultet Univerziteta Union u Beogradu, 2014, str. 97.

kongresu Ujedinjenih Nacija posvećenog Prevenciji od kriminala i tretmanu počinioca u aprilu 2000. godine.[12]

"*Sajber kriminal je kriminal koji se odnosi na bilo koji oblik kriminala koji se može izvršavati sa računarskih sistemima i mreža, u računarskim sistemima i mrežama ili protiv računarskih sistema i mreža*".

To zapravo podrazumeva neku kriminalnu radnju koja angažuje računarski sistem ili mrežu kao sredstvo ili kao cilj izvršenja krivičnih dela ili koja se realizuje u elektronskom okruženju. Karakteristika sajber kriminala je ta što je ona učinjena sa namerom a ne slučajnošću.

U Konvenciji o sajber kriminalu (Convention on Cybecrime) Saveta Evrope računarski sistem je definisan kao svaki uređaj ili grupa međusobno povezanih uređaja kojima se vrši automatizivana obrada podataka. To dalje implicira da bez istih i bez računarskih mreža nema ovog oblika kriminala. [13]

Ovako predstavljen sajber kriminal pokriva veliki broj različitih kriminalnih aktivnosti uključujući napade na računarske podatke i računarske sisteme, napade vezane za računare, sadržaje ili intelektualnu svojinu pa se u literaturi najčešće navodi kao jedan opšti odnostno eng. umbrella termin – kišobran termin.

Gojko Grubor profesor na katedri za Bezbednost i zaštitu informacionih sistema i profesor Milan Milosavljević rukovodilac doktorskog programa Napredni sistemi zaštite, u najširem smislu pod računarskim kriminalom podrazumevaju krivična dela prema krivičnom zakonu nacionalne države, koja su na bilo koji način uključeni računarski sistemi i mreže. U računarskom i kibernetičkom (sajber) kriminalu, računari se koriste kao predmet napada i krađe, izmene ili uništavanja podataka, kao alat za izvršavanje tradicionalnih oblika kriminala i za skladištenje kompromitujućeg materijala. Glavni cilj istrage računarskog kriminala je da se kao i slučaju klasičnog kriminala, izgradi za pravosudne organe neoboriv ili čvrst dokaz krivice, i/ili dokaz za oslobađanje osumnjičenog, i/ili pravedno sankcionisanje učinjenog dela. Ključnu metodologiju istrage i dokazivanja računarskog kriminala obezbeđuje metodologija istrage klasičnog kriminala, sa specifičnostima istrage osetljivih,

12 Tumačenje i razmere ovog kriminala i njegove opasnosti opisane su u dokumentu *Kriminal vezan za kompjuterske mreže* (eng. *Crime related to computer networks*), UNODC (United Nations Office on Drugs and Crime), http://www.uncjin.org/Documents/congr10/10e.pdf, 11.07.2016.

13 Council of Europe treaties, Details of Treaty No.185, *Convention on Cybercrime*, http://conventions.coe.int/treaty/en/treaties/html/185.htm, 01.03.2016.

lako promenljivih i po svojoj prirodi posrednih digitalnih dokaza.[14] [15]

Dr Linda Volonino profesor Informacionih sistema Canisius i predsednik FBI Infragard ISSA (Infomation system security association – udruženja za bezbednost informacionih sistema) definiše termin sajber kriminal, prema načinu izvršenja krivičnih dela koje uključuju računare, u dve kategorije: [16] [17]

-*računar kao cilj* - računar ili podaci su meta ove vrste kriminala uključujući i napade na mrežama koje mogu da prouzrokuju obaranje mreže, kao na primer napadi crva, neovlašćen pristup računaru ili zloupotreba informacionih sistema, računara, programa ili podataka. Najčešći primeri su virusi, crvi, trojanski konji, industrijske špijunaže, softverska piraterija, i hakovanja (zlonamerni upadi na računare);

-*računar kao sredstvo* - u ovom slučaju računar se koristi da bi se izvršila neka nedozvoljena aktivnost. Mnoga krivična dela počinjena sa računarom su tradicionalna kao što su krađe, prevare, falsifikovanja, uhođenja ili distribucija dečije pornografije. Razlika je u tome da su ovi tradicionalni zločini počinjeni korišćenjem informaciono komunikacione tehnologije. Novije vrste krivičnih dela koje spadaju u ovu kategoriju spadaju: ugrožavanje e-maila, krađa identiteta, spam, fišing (eng. phishing), farming (eng. pharming) kao i sve aktivnosti planiranja, rukovođenja, izvršenja i prikrivanja nedozvoljenih aktivnosti.

To znači da računar može biti sredstvo ili cilj izvršenja ovih krivičnih dela, što podrazumeva da je na neki način ostvarena u krivičnopravnom smislu kažnjiva posledica, s tim što posledica može biti ispoljena na objektima IKT (računari, mreže i ostali digitalni uređaji). Međutim, računar može biti i posrednik u izvršavanju krivičnog dela sajber kriminala, na primer, u slučaju preuzimanja tuđeg računara i izvršenja krivičnog dela sa tog računara.

U vezi sa ovakvom kategorizacijom ove vrste kriminala postoji i definicija koja određuje sajber kriminal kao oblik kriminalnog ponašanja, kod koga se korišćenje računarske tehnologije i informatičkih sistema ispoljava kao način izvršenja krivičnog dela ili se računar upotrebljava kao sredstvo ili cilj izvršenja,

---

14 Milan Milosavljević, Gojko Grubor, *Istraga kompjuterskog kriminala - metodološko tehnološke osnove*, Beograd, Singidunum 2009. str. 4.

15 APWG, *Phishing Activity Trends Report, 3rd Quarter (July – September 2012)*, 2013. http://www.apwg.org/download/document /84/apwg_trends_ report_q3_2012.pdf, 20.06.2016.

16 Linda Volonino, *Computer forensics principles and practices*, Pearson Education, Inc Upper Saddle River, New Jersey, 2007, str. 6.

17 Caloyannides M. A., Privacy Protection and Computer Forensics Second Edition, Artech ouse Inc., 2004.

čime se ostvaruje neka u krivično-pravnom smislu relevantna posledica.[18]

Odeljenje za pravosuđe SAD (DOJ The department of Justice) sajber kriminal definiše u širem smislu kao svako kršenje krivičnog zakona koje uključuju dobro poznavanje i korišćenje računarske tehnologije kako bi se izvršilo krivično delo. Takođe potrebno je dobro poznavanje računarskih tehnologija kako bi se uspešno sprovela istraga i dalje procesuiranje takvih krivičnih dela.

Računarski kriminal se može definisati i na način kao što to čini prof. Milan Škulić: "Kompjuterski kriminalitet predstavlja oblik kriminalnog ponašanja, kod koga se korišćenje kompjuterske tehnologije i informatičkih sistema ispoljava kao način izvršenja krivičnog dela, ili se kompjuter upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka u krivično pravnom smislu relevantna posledica."[19]

Prof. Đorđe Ignjatović definiše kompjuterski kriminalitet na sledeći način: "Kompjuterski kriminalitet predstavlja poseban vid inkriminisanih ponašanja kod kojih se računarski sistem (shvaćen kao jedinstvo hardvera i softvera) pojavljuje ili kao sredstvo izvršenja ili kao objekat krivičnog dela, ukoliko se deo na drugi način, ili prema drugom objektu, uopšte ne bi moglo izvršiti ili bi ono imalo bitno drugačije karakteristike".[20]

Definicija iz Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala Republike Srbije glasi: "Visokotehnološki kriminal predstavlja vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja dela javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom i elektronskom obliku".[21]

Razlog ne postojanja univerzalne definicije je i taj što se broj krivičnih dela koja se mogu podvesti čak i pod najrestriktivnije i najuže definicije računarskog kriminala, neprekidno povećava. Klasifikacija takvih ponašanja je teška zato što se ne mogu utvrditi kriterijumi koji će određena dela svrstati isključivo u jednu kategoriju, dok sa druge strane, pojave novih načina zloupotrebe nužno iziskuju i proširenje pomenute liste kriterijuma.[22]

Na osnovu svih navedenih definicija o sajber kriminalu može se uočiti da se u stvari sajber kriminal kao termin odnosi na sve nedozvoljene radnje u

---

18 Dragan Prlja, Mario Reljanović, *Pravna informatika*, Pravni fakultet Univerziteta Union u Beogradu, 2014, Beograd, str. 94.

19 Škulić Milan, Aleksić Živojin , *Kriminalistika*, Beograd, Dosije, 2002, str.396.

20 Đorđe Ignjatović, *Pojmovno određenje kompjuterskog kriminaliteta,* Anali Pravnog fakulteta u Beogradu, br. 1/1991, str. 142.

21 Zakon o organizaciji i nadrežnosti državnih organa za borbu protiv visokotehnološkog kriminaliteta, Sl. Glasnik RS, br. 61/2005.

22 Ashcroft J., *Electronic Crime Scene Investigation - A Guide for First Responders*, U.S. Department of Justice, 2001, https://www.ncjrs.gov/ pdffiles1/ nij/187736.pdf, 26.06.2016.

čijem izvršenju su korišćene informaciono-komunikacione tehnologije.

1.2. TIPOVI VISOKOTEHNOLOŠKOG KRIMINALA

Kada se spomenu tipovi sajber kriminala (visokotehnološkog kriminala), onda se govori o aktivnostima na osnovu kojih je izvršen napad zajedno sa različitim oblicima tehničkih i informacionih pomagala. To mogu biti različiti hardverski uređaji ili softverska rešenja, koja napad mogu da olakšaju nanoseći štetu fizičkim ili pravnim licima.

Profesor Ronald Standler sajber kriminal prema obliku, odnosno vrsti krivičnog dela deli u tri kategorije: 1. neautorizovano korišćenje računara, 2. stvaranje i distribucija štetnih računarskih programa, 3. uznemiravanje i uhođenje u sajber prostoru. [23]

Profesor Predrag Dimitrijević kada govori o ovom obliku kriminala podrazumeva jednu uopštenu formu kroz koju se ispoljavaju različiti vidovi nedozvoljenog postupanja. Ovaj vid kriminala je usmeren protiv bezbednosti informacionih sistema u celini ili u njenom pojedinačnom delu (mrežni ili računarski sistemi i drugi elektronski uređaji).[24] Ispoljava se na različite načine, različitim sredstvima i motivisan je koristoljubljem i/ili nanošenjem štete drugome.

Tipovi sajber kriminala, navedeni u materijalu za "radionicu" o kriminalu na mreži sa Desetog kongresa UN su navedeni kroz definicije u užem i širem smislu:[25]

1. Sajber kriminal u užem smislu predstavlja svako ilegalno ponašanje obavljeno elektronskim putem usmereno ka bezbednosti računarskih sistema i podacima koje oni obrađuju;
2. Sajber kriminal u širem smislu (kriminal vezan za računarsku tehnologiju) je svako ilegalno ponašanje obavljeno pomoću ili u vezi sa računarskim sistemom ili računarskom mrežom, uključujući i takve aktivnosti kao što su ilegalno posedovanje i/ili nuđenje i distribucija informacija pomoću računarskog sistema ili računarske mreže.[26] Naravno, najveći problem prilikom definisanja ovog termina predstavlja razlika u zakonskoj regulativi u većini zemalja.

---

23 Ronald B. Standler, *Computer Crime*, http://www.rbs2.com/ccrime.htm, 22.04.2016.

24 Predrag Dimitrijević, *Kompjuterski kriminal*, http://www.prafak.ni.ac.rs/ files/nast_mat/ Kompjuterski_kriminal.pdf, 25.11.2011.

25 Bradford P. G., Hu N., *A Layered Approach to Insider Threat Detection and Proactive Forensics*, 21st Annual Computer Security Applications Conference, Applied Computer Security Associates (ACSA), 2005. http://www.acsac.org/ 2005/techblitz/hu.pdf, 20.06.2016.

26 *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, Vienna, 10-17 April 2000, http://www.uncjin.org/Documents/congr10/10e.pdf, 22.01.2016.

U istom dokumentu navode se i konkretni oblici kompjuterskog kriminaliteta, u skladu sa Preporukom Saveta Evrope i listom OECD-a iz 1989., odnosno 1985. godine.[27] [28] To su:

1. neovlašćen pristup (upad) računarskom sistemu ili mreži (onesposobljavanje zaštitnih mera na sistemu ili mreži);
2. oštećenje računarskih podataka ili programa;
3. računarska sabotaža;
4. neovlašćeno presretanje komunikacija u kompjuterskim sistemima i mrežama;
5. računarska špijunaža.

Ono što treba napomenuti je da u praksi uglavnom dolazi do ukrštanja ovih oblika kriminala. Na primer prilikom neovlašćenog upada u računarski sistem ili mrežu uglavnom on može obuhvatiti i računarsku špijunažu ili postavljanje malicioznih programa sa svrhom presretanja komunikacija ili uništavanja podataka.

Kada je reč o sajber kriminalu u širem smislu najčešće se pojavljuju sledeći pojavni oblici:

1. računarski falsifikati;
2. računarske krađe;
3. tehničke manipulacije uređajima ili elektronskim komponentama uređaja;
4. zloupotrebe sistema plaćanja (manipulacije i krađe elektronskih kreditnih kartica ili korišćenje lažnih šifri u nezakonitim finansijskim aktivnostima).

Evropska konvencija o sajber kriminalu grupiše ova dela u 4 kategorije:[29]

1. dela protiv poverljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema – tu spadaju nezakoniti pristup, presretanje, uplitanje u podatke ili sisteme, korišćenje uređaja (proizvodnja, prodaja, uvoz, distribucija), programa, šifri;
2. dela vezana za računare – tu spadaju krađe i falsifikovanje kao oblici napada;
3. dela vezana za sadržaje – tu spada dečija pornografija obuhvatajući posedovanje, distribuciju, transmisiju, čuvanje ili činjenje dostupnim

27 Brown C., *Computer Evidence - Collection and Preservation*, Thomson Delmar Learning, Charles River Media, Inc, Hingham, Massachusetts, 2006, str. 213-218.

28 Bunting S., Wei W., *EnCase Computer Forensics: The Official EnCE: EnCase Certified Examiner Study Guide*, Indianapolis, IN: Wiley Publishing, 2006.

29 Burdach M., *Detecting Rootkits And Kernel-level Compromises In Linux*, Symantec, Novembar 2004. http://www.symantec.com/ connect /articles /detecting-rootkits-and-kernel-level-compromises-Linux, 22.06.2016.

i raspoloživim ove vrste materijala, njihova proizvodnja radi distribucije i obrade u računarskom sistemu ili na nosiocu podataka;
4. dela vezana za kršenje autorskih i srodnih prava obuhvataju reprodukovanje i distribuciju neautorizovanih primeraka pomoću računarskih sistema (ili pomoću mreže).

Profesor na Ročesterovom Tehnološkom institutu Samuel McQuade u Enciklopediji Sajber kriminala čiji je urednik, prikazuje i prepoznaje sledeće oblike nedozvoljenog ponašanja koje FBI i Nacionalni centar za kriminal belih kragni SAD (*National White Collar Crime Center*) otkrivaju i prate: upadi u računarske mreže; industrijska špijunaža; softverska piraterija; dečija pornografija; zatrpavanje elektronskom poštom; „njuškanje" lozinki (eng. sniffing); farming (imitiranje drugog računara radi neovlašćenog upada) i prevare sa kreditnim karticama.[30]

Zavisno od tipa učinjenih dela sajber kriminal može imati političku ili ekonomsku pozadinu.

U politički motivisan sajber kriminal spadaju sledeća dela:[31]
1. sajber špijunaža;
2. upad u računare i mreže (hakovanje);
3. sajber sabotaža;
4. sajber terorizam;
5. sajber ratovanje.

U ekonomski motivisan sajber kriminal spadaju sledeća dela:[32]
1. sajber prevare;
2. neovlašćeno upadanje u računare i mreže (hakovanje);
3. krađa internet usluga i vremena;
4. piraterija programa, mikročipova i baza podataka;
5. sajber industrijska špijunaža;
6. prevarne internet aukcije (neisporučivanje proizvoda, lažna prezentacija proizvoda, lažna procena, nadgrađivanje cene proizvoda, udruživanje radi postizanja veće cene, trgovina robom sa crnog tržišta, višestruke ličnosti);
7. proizvodnja i distribucija nedozvoljenih i štetnih sadržaja (dečija

30 Burdach M., *Forensic Analysis of a Live Linux System, Pt. 2*, Symantec, April 2004, http:// www.symantec.com/ connect/ articles/ forensic -analysis-live-Linux-system-pt-2, 22.06.2016.
31 Bergadano F., Gunetti D., Picardi C., *User Authentication through Keystroke Dynamics*, ACM Transactions on Information and System Security, Vol. 5, No. 4, pp. 367-397, November 2002.
32 *Ibidem.*

pornografija, pedofilija, verske sekte, širenje rasističkih, nacističkih i sličnih ideja i stavova, zloupotreba žena i dece, pružanje nedozvoljenih usluga (kockanje prostitucija);

8. manipulacija zabranjenim proizvodima, supstancama i robama (drogom, ljudskim organima, oružjem);
9. povrede sajber privatnosti (nadgledanje e-pošte, spam, fišing prisluškivanje, njuškanje lozinki tj. sniffing, praćenje e-konferencija, prikačinjanje i analiza kolačića tj. "cookies");
10. distribucija zlonamernih programa (virusi, crvi, trojanci, fišing, farming).

Štete prouzrokovane visokotehnološkim kriminalom, mogu se podeliti na:

- *materijalne* – za posledicu imaju objektivno učinjenu finansijsku štetu bilo da je učinilac izvršio delo sa ili bez namere sticanja imovinske koristi;
- *nematerijalne* – odnose se na neovlašćeno otkrivanje nečijih poverljivih informacija, ili neko drugo "indiskretno zlonamerno ponašanje";
- *kombinovane* – kod kojih kao posledica izvršenja krivičnog dela dolazi do materijalne i nematerijalne štete (npr. zloupotrebom mreže ili računara; ili ukoliko je izvršena krađa autorskog dela i javno objavljivanje istog pod tuđim imenom).

Prema prikazanim različitim kategorijama ove vrste kriminala mogu se uočiti različiti interesi koje motivišu ljude da počine zakonom zabranjene radnje. U praksi naravno postoje i slučajevi kada je u pitanju radoznalost, samodokazivanje ili hvalisavost pred drugim licima. Zato se nikada ne može sa sigurnošću govoriti o jedinstvenom profilu učinilaca računarskog kriminala, jer se oni svrstavaju u različite kategorije prema pojavnim oblicima dela koja čine, ali i prema motivima, koji ih pokreću u vršenju kriminalnih aktivnosti.

Učinioci dela visokotehnološkog kriminala mogli bi se podeliti na dve grupe:

1. zlonamerne učinioce, koji mogu da deluju radi ostvarenja imovinske koristi, ili samo u cilju nanošenja štete ili osvete;
2. učinioce koji nisu motivisani ni ostvarenjem koristi, niti prouzrokovanjem štetnih posledica, već jednostavno traže zadovoljstvo u neovlašćenom prodiranju u neki dobro obezbeđen informacioni sistem iz zabave.

Zlonamerni učinioci računarskih delikata najčešće su motivisani koristoljubljem, a smatra se da podaci iz prakse ukazuju na određeni skup osobina koje čine njihov kriminalni profil. Oko 80% delikvenata čini delo prvi

put, a 70% je zaposleno više od pet godina u oštećenoj kompaniji. Njihovo starosno doba je u proseku između 19 i 30 godina, pretežno su muškog pola, veoma su inteligentni, imaju uglavnom više godina radnog iskustva i važe kao savesni radnici koji prilikom obavljanja radnih zadataka ne prouzrokuju nikakve probleme. U većini slučajeva su tehnički kvalifikovaniji nego što to zahteva radno mesto na koje su raspoređeni. Ovi učinioci sebe po pravilu ne smatraju kradljivcima ili uopšte kriminalcima, već samo pozajmljivačima.

Kada je reč o drugoj grupi tu se radi o tzv. hakerima, koji koriste svoje računarsko znanje da upadaju u tuđe računarske sisteme. Oni zadovoljstvo mogu pronaći u samom činu upada u višestruko obezbeđene informacione sisteme. Što su računarski sistemi i mreže bolje čuvani, to je za njih veći izazov. Iako neki od njih nisu zlonamerno motivisani, oni mogu svesno ili nesvesno da prouzrokuju ogromne štete.

Sa druge strane, kada je reč o statistici oštećenih, prema izveštaju Internet Crime Complaint Center (IC3) iz 2009. godine u SAD više od polovine oštećenih zbog internet zloupotreba su stariji od 40 godina. Izveštaj je pokazao da su 76% sajber kriminalaca muškarci.[33]

Prema statistikama najveći procenat narušavanja bezbednosti (preko 70%) nastaje interno u okviru organizacije. Zato je važno da se u okviru organizacije prepreme dokumenta koja moraju biti potpisana od strane zaposlenih, da bi se u okviru organzicije mogla uraditi forenzička istraga na bilo kom računarskom sistemu koji se koristi. Kada se u organizaciji desi određena nedozvoljena aktivnost forenzička istraga može biti potpomognuta dodatnim istražnim merama. Zlonamerni napadač u tom slučaju nema saznanja o tome da su forenzičari na tragu i u skladu sa tim može se postaviti keylogger hardverskog ili softverski tipa. Hardverski tip može biti u vidu adaptera na kablu tastature. Ukoliko organzicija poseduje proceduru navedenu u dokumentu koji je zaposleni potpisao prilikom svog zaposlenja u kojoj je navedeno da poslodavac može sprovoditi takvu vrstu nadzora, to znači da dokaz koji je snimljen na keyloggeru može biti upotrebljen kao digitalni dokaz u slučaju nedozvoljene aktivnosti.

Pored posledica finansijske prirode koje mogu da nastanu kada učinilac vrši delo u cilju sticanja nedozvoljene imovinske koristi, postoje i posledice nematerijalne prirode. One se ogledaju u neovlašćenom otkrivanju tuđih tajni, narušavanju ugleda, povredi moralnog prava ili drugom sličnom postupanju. Tu su i kombinovane posledice, koje postoje kada se otkrivanjem

33 Korać V., *Prevencija širenja virusa kroz autorun funkciju operativnog sistema,* Arheologija i prirodne nauke br.4/2008, Beograd, str. 103-107.

određene tajne ili povredom autorskog prava, putem zloupotrebe kompjutera ili informatičke mreže nanese određeni vid nematerijalne štete, a istovremeno se prouzrokuje i konkretna finansijska šteta.[34]

Svrha detaljnije klasifikacije podrazumeva razdvajanje sajber kriminala od ostalih oblika kriminala. Direktor Kriminološkog instituta Australije Adam Graycar, pokušao je da prevaziđe upravo ovaj problem navođenjem devet kategorija sajber kriminala.

Te kategorije sortirane su na sledeći način: dela protiv telekomunikacionih službi, komunikacija u cilju zločinačkog udruživanja, telekomunikaciona piraterija, rasturanje neprikladnog sadržaja, pranje novca i evazija poreza, elektronski vandalizam terorizam i iznuda, prevare u vezi sa prodajom investicija, nezakonito presretanje telekomunikacija, prevare vezane za elektronsko poslovanje.[35] Međutim, iako je Graycar svojim širokim definicijama zaista gotovo uspeo da pokrije sve oblike neželjenog i nezakonitog ponašanja, u nekim slučajevima one nisu upotrebljive. Kao na primer, analiza rasturanja materijala neprikladnog sadržaja – jer bi u ovu grupu spadale kako reklamne poruke čije slanje u principu nije kažnjivo, tako i slanje rasističkih poruka, pornografskog materijala (uključujući i dečiju pornografiju), uputstva za pravljenje eksplozivnih naprava itd.

Pavel Dugal, predsednik međunarodne organizacije „Cyberlaws", koja se bavi istraživanjem sajber kriminala, sa druge strane izneo je jednu jednostavniju kategorizaciju ovakvih krivičnih dela, ali ona nije dovoljno detaljna.

Prema Dugalu sva krivična dela iz ove grupe mogu svrstati na:

1. dela protiv ličnosti,
2. dela protiv imovine,
3. dela protiv države.[36]

U pojavne oblike krivičnih dela iz grupe *dela protiv ličnosti* Alice Hutchings, istraživač i analitičar programa za Globalni ekonomski i elektronski kriminal Australijskog instituta za kriminologiju svrstava:[37]

- *sajber manipulaciju* (eng. cyber grooming), kao vrstu psihološke manipulacije koja se obavlja na internetu preko sinhronih i asinhronih

34 Korać V., *Zaštita usb prenosnog drajva i operativnog sistema od zlonamernog koda tipa autorun.inf*, Zbornik Radova - Forum BISEC 2010, II konferencija o bezbednosti, Univezitet Metropolitan, Fakultet informacionih tehnologija, 2010, str. 77-82.

35 Australian Institute of Criminology, *9 types of cyber crime*, http://www. crime. hku.hk/ cybercrime.htm, 22.11.2015.

36 Maya Babu, Mysore Grahakara Parishat, *What Is Cybercrime?*, Computer Crime Research Center, http://www.crime-research.org/analytics/702, 27.10.2015.

37 Australian Institute of Criminology, cyber crime 2.0, http://www.aic.gov.au/ events/aic%20 upcoming%20events/2011/~/media/conferences/2011-studentforum/alice_hutchings.pdf, 22.11.2015.

komunikacionih platformi (javne chat pričaonice, internet sajtovi za upoznavanje, instant messengeri i VOIP servisi tipa ICQ i Skype) i u novije vreme putem socijalnih mreža (facebook, twitter, myspace). Žrtve manipulacijom su uglavnom deca i maloletna lica od 11-17 godina, kao krajnji cilj ove manipulacije je sastanak koji se obično pretvara u seksualno zlostavljanje, fizičko nasilje, dečiju prostituciju i pornografiju;[38] [39]

- *sajber uznemiravanje, uhođenje* (eng. cyber stalking). Primeri za to su bombardovanje sms porukama, uznemiravanje e-mail porukama, uznemiravanje telefonskim pozivima, neželjena pažnja – pokloni, slanje različitih poruka putem instant messenger-a čata i voip tehnologije putem društvenih mreža, pa čak i postavljanja web strana i blogova u cilju izazivanja straha kod žrtve. Žrtve ove vrste kriminala su uglavnom poznate ličnosti.[40] [41] U Americi postoje organizacije koje se bave suzbijanjem ovog problema kao na primer WHOA (Working to Halt Online Abuse);[42]
- *sajber nasilje – maltretiranje* (eng. cyber bullying). Dok se tradicionalno maltretiranje može izraziti kroz fizičke ili psihičke napade, sajber maltretiranje se odvija na mentalnom planu kao vrsta psihološkog šikaniranja koja se manifestuje kroz slanje uznemirujućih, ponižavajućih, uvredljivih i neprikladnih poruka ili sadržaja. Napadi ovog tipa mogu biti toliko intenzivni i ponavljajući da žrtva može da doživi mentalni slom, a posledice mogu da dovedu i do samoubistva.[43] [44]

Realizacija ove vrste kriminala vezane za dela protiv ličnosti uglavnom prolazi kroz četiri faze prema sledećem scenariju:

---

38 Kamil Kopecký, *Cyber grooming danger of cyberspace*, Olomouc, 2010, http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=15%3Acybergrooming-danger-of-internet, 22.11.2015.

39 Carrier B., *Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers*, International Journal of Digital Evidence, Winter 2003.

40 Kamil Kopecký, *Stalking a kyberstalking nebezpečné pronásledování*, Olomouc, 2010, http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=9%3Astudie-o-stalkingu-a-kyberstalkingu, 22.11.2015.

41 Carrier B., *File System Forensic Analysis*, Addison Wesley Professional, 2005.

42 Working to Halt Online Abuse, WHOA, http://www.haltabuse.org/about/about.shtml, 28.11.2015.

43 Veronika Krejčí, *Kybersikana kiberneticka sikana*, Olomouc, 2010, http://www.e-nebezpeci.cz/ index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=14%3Akybersikana-studie, 22.11.2015.

44 Carrier B., *Open Source Digital Forensics Tools - The Legal Argument*, @tstake, 2002, http://www.digital-evidence.org/papers/opensrc_legal.pdf, 10.07.2016.

Prvo se identifikuje i locira žrtva, sledeći korak je uspostavljanje kontakta sa žrtvom što za cilj ima prikupljanje svih relevantnih informacija potrebnih napadaču da bi sproveo uznemiravanje odnosno krivičnu radnju.

U dela protiv imovine spadaju:

- *neovlašćen pristup* – ova dela se obično realizuju uz pomoć fišinga, farminga, malware-a, wifi ranjivostima, socijalnim inženjeringom;
- *internet prevare* – vezuju se za zahtevom za transfer novca, spam, clickjacking prevare kroz sajtove za upoznavanje;[45]
- *krađa identiteta* - predstavlja još jedan oblik visokotehnološkog kriminala koji se manifestuje kroz krađu identiteta druge osobe, a zlonamerna osoba pretenduje da se predstavi kao neko drugi u cilju pristupanja resursima od materijalne koristi (npr. kredita) i drugih privilegija u ime te druge osobe. Žrtva krađe identiteta (znači lice čiji identitet zlonamerni napadač preuzima) može trpeti štetne posledice ako se smatra odgovornim za postupke počinioca. Organizacije i pojedinci koji su prevareni na ovakav način od strane lopova takođe mogu imati štetne posledice i gubitke u istoj meri kao i osobe čiji je identitet kompromitovan;
- *zlonamerni programi* - predstavljaju zlonamerne programe (npr. programski kod, skripta, aktivni sadržaj) koji za cilj imaju određenu zlonamernu aktivnost (da ometaju ispravan rad informaciono komunikacionih sistema, programa ili da ga onemoguće, da prikupljaju takve informacije ili da ih iskorištavaju, čime se dovodi do kršenja propisa o zaštiti privatnosti).[46] Prema Johny Aycocku profesoru informatike sa

45 Radi se o psihološkim trikovima da bi se namamile potencijalne žrtve kroz sajtove za upoznavanje. Koristeći lažne profile na tim sajtovima za upoznavanje pretvarajući se da savršeno odgovaraju potencijalnoj žrtvi korišćenjem takođe lažne fotografije koja je ukradena sa neke od društvenih mreža. Ljudi na tim fotografijama su takođe žrtve. Akcenat je stavljen na što većem zbližavanju sa potencijalnom žrtvom kroz korišćenje poezije, poklona i drugih „romantičnih trikova", tako da se žrtvi učini da može da im veruje. Nakon uspostavljanja poverenja krajnji cilj je traženje od žrtve da pošalje novac , ček ili neki drugi oblik načina plaćanja, kako bi se napadaču pomoglo zbog navodnih finansijksih poteškoća kako su predstavili svojoj žrtvi. Kao način borbe protiv ovakve vrste kriminala jesti i obrazovanje što većeg broja ljudi po pitanju ovog načina prevare. Sajt http://www.romancescam.com/ je jedan od sajtova koji doprinose borbi protiv ovakve vrste prevare.

46 Windows Mikrosoft, Da li vam je potrebna pomoć za Windows 10?, http://windows.microsoft.com/sr-Latn-CS/windows-vista/What-is-active-content-and-why-does-Internet-Explorer-restrict-it, 01.03.2016.

univerziteta Calgary, ovde spadaju:[47] logičke bombe (eng. logic bomb), trojanski konji (eng. trojan horse), zadnja vrata (eng. backdoor), virusi[48] (eng. virus), crvi (eng. worm), zečevi (eng. rabbit), spajveri (eng. spyware), adveri (eng. adware), hibridi, kapalice (eng. droppers), zamke i zombiji[49] (eng. zombies)[50] i ransomware zlonamerni programi. [51]

U *dela protiv države* - spadaju ona dela koja su usmerena protiv vlade i vojske. Najzastupljenija vrsta u ovoj kategoriji je sajber terorizam. Sajber terorizam se može definisati kao što to čini profesor Clay Wilson direktor programa Politika Sajber bezbednosti (eng. Cyber Security Policy Program) "*kao politički motivisano korišćenje računara kao oružja ili kao cilja, pod-nacionalnih grupa ili tajnih agenata sa namerom da izazovu nasilje, da utiče na javnost ili na vladu da promeni svoju politiku*".[52] [53] Cilj ovog kriminala je da se napadne kritična infrastruktura u pokušaju da se nanese velika šteta u smislu gubitka života ili materijalne štete. Takvi napadi imaju za cilj da onesposobe informacione sisteme (npr. vladine ili vojne web sajtove ili servise) koji su sastavni deo javne bezbednosti,

47 John Aycock, *Computer Viruses, and Malware*, Springer , Canada, 2006, str. 11-18.

48 Frederick B. Cohen je 1983 skovao termin „računarski virus" i odredio je možda i najbolju definiciju virusa u kojoj se kaže da virus predstavlja program koji može inficirati druge programe, modifikujući ih tako da uključuju kopiju njega samoga, koja takođe može biti modifikovana, tako da se virus može širiti u računarskom sistemu ili u mreži koristeći ovlašćenja svakog korisnika sa namerom da se inficiraju njegovi programi. Svaki program koji postane inficiran može delovati kao virus i na taj način se infekcija širi. Virusi najčešće oštećuju ili modifikuju fajlove na ciljanom računaru tako da mogu da dovedu sistem u stanje u kome ne može više da se normalno koristi. Ne koriste mrežne resurse za svoje širenje, ali mogu da se šire kroz mrežu kao deo nekog crva. Uglavnom se širi kao posledica delovanja ljudskog faktora. To znači da virus može postojati na računaru ali to ne znači da će sam računar biti zaražen. Računarski virusi mogu biti detektovani i uklonjeni antivirusnim ili antimalware programima. Fred Cohen, A Computer Virus, http://all.net/books/virus/part2.html, 26.11.2015.

49 Nelson B., Phillips A., Enfinger F., Steuart C., *Guide to Computer Forensics and Investigations, third edition,* Thomson Course Technology, Boston, 2008.

50 Carroll O. L., Brannon S. K., Song T., Vista and BitLocker and Forensics! Oh My!, Computer Forensics, Volume 56 Number 1, January 2008.

51 Predstavlja vrstu zlonamernog programa koji vrši enkripciju korisničkih podataka. Određenom porukom korisnik se ucenjuje i zahteva se da plati digitalnim novcem (Bitcoin-om) njihov otkup tj. da bi se korisniku – žrtvi poslao enkripcioni ključ neophodan za dešifrovanje podataka.

52 Clay Wilson, *Computer attack and cyber terrorism: Vulnerabilities and policy issues for Congress,* Us Congressional Research Report RL32114, http://www.fas.org/irp/crs/RL32114.pdf, 17.10.2015.

53 Carrier B., *Open Source Digital Forensics Tools - The Legal Argument,* @tstake, 2002, http://www.digital-evidence.org/papers/opensrc_legal.pdf, 10.07.2016.

kontrole saobraćaja medicinske i hitne službe i javne radove.[54] Uglavnom se radi o grupama ili pojedincima koji prete međunarodnim vladama i terorišu građane u zemlji.

Sve ove iznete informacije o tipovima napada i zlonamernim programima koji se koriste za njihovu realizaciju digitalni forenzičar mora da prepoznaje i da bude informisan o njihovim novijim verzijama. Nove tehnologije koje su inicirale prelazak na mobilnu komunikaciju, pojavu virtuelnih valuta[55] i pojavu TOR mreže[56], oblikovale su okruženje da zlonamerni programi ransomware tipa koji vrše enkripcije podataka, postanu trenutno jedna od najvećih pretnji na internetu donoseći veliku opasnost kada je u pitanju bezbednost podataka na računarskim sistemima kako u organizacijama tako u kućnom okruženju. Dodatno zabrinjavajuće jeste pojava ovog zlonamernog programa u formi servisa (Ransomware as a service[57] [58] [59] - RaaS). Pomoću ovog programa je moguće organizovati odnosno naručiti napad kao uslugu logovanjem na određeni sajt, kreiranjem zlonamernog programa i njegovo distribuiranje ciljanim korisnicima-žrtvama. Dodatno omogućeno je upravljenje ovim zlonamernim programom uz pomoć iznajmljenog kontrolnog centra.

Zlonamerni programi o kojima je bilo reči, dakle osim što predstavljaju alate zlonamernih pojedinaca mogu se naći i u formi servisa organizovanih od strane sajber kriminalaca, što zapravo predstavlja oblik biznisa kome je svrha sprovođenje nedozvoljenih aktivnosti i/ili anti-forenzička delovanja vezanih za uklanjanje potencijalnih dokaza o nedozvoljenoj aktivnosti. To za posledicu može da ima nanošenje velike štete kako kompaniji tako i pojedincu, ali i državi.

Kada je reč o visokotehnološkom kriminalu u Srbiji, on obuhvata

---

54 Carrier B., Spafford H. E., *Getting Physical with the Digital Investigation Process*, International Journal of Digital Evidence Fall 2003, Volume 2, Issue 2, 2003.

55 Virtuelna valuta na primer BitCoin. Koristeći virtuelnu valutu kao metod plaćanja otkupnine zlonamerni napadači nisu izloženi tradicionalnom bankarstvu i mogućnostima ostavljanja tragova prilikom transfera novca.

56 Upotrebom TOR mreže zlonamerni napadači mogu lakše sakriti lokacije svojih kontrolnih servera koji čuvaju privatne ključeve korisnika kome su enkriptovani podaci. TOR omogućava održavanje infrastrukture za izvršavanje sajber kriminala u dužem vremenskom periodu, obezbeđujući i iznajmljivanje ovakve infrastrukture drugim zlonamernim napadačima čime se pruža mogućnost i za međusobna udruživanja sa ciljem sprovođenja nedozvoljenih aktivnosti.

57 Http://www.techrepublic.com/article/ransomware-as-a-service-is-exploding-be-ready-to-pay/, 20.07.2016.

58 Http://www.securityweek.com/ransomware-service-lets-anyone-be-cybercriminal, 20.07.2016.

59 Https://www.flashpoint-intel.com/home/assets/Media/Flashpoint_Ransomware_April2016.pdf, 20.07.2016.

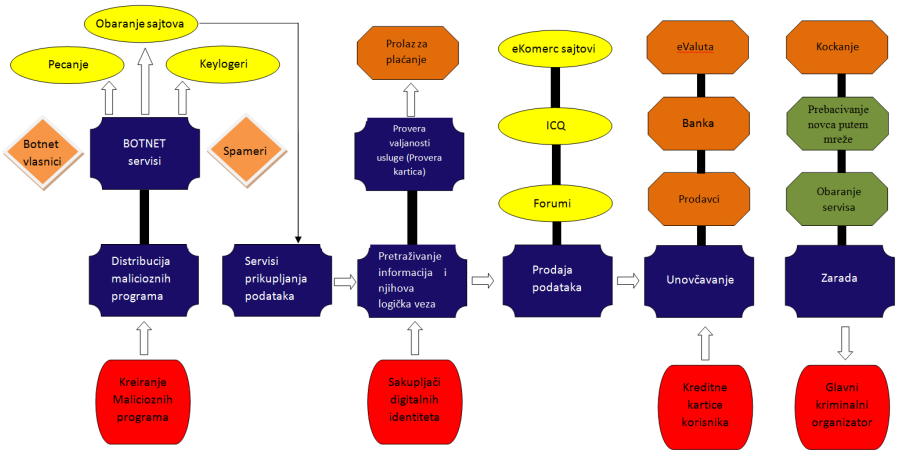
široku lepezu pojavnih oblika. Najčešći slučajevi su neovlašćen pristup računarima, računarskoj mreži ili bazama podataka, pravljenje i unošenje (širenje) računarskih virusa (kako bi se prikupili podaci o platnim karticama), krivična dela protiv ugrožavanja sigurnosti, povreda autorskih prava tzv. piraterija, zloupotrebe u vezi sa platnim karticama (zloupotreba ukradenih šifri), kompanijska odnosno industrijska špijunaža, napadi sa ciljem onemogućavanja serverskih servisa, zabranjeni pornografski materijali (npr. pedofilski materijali), iznuđivanje ili kompromitovanje, pljačke banaka, ali i svih ostalih krivičnih dela u kojima se koriste računari.

Sama količina informacija koja se nudi na internetu o kompromitovanju platnim karticama je prilična. Postoje određeni profesionalni sajtovi koji se bavi prodajom potrebne opreme za ovaj vid kriminala. Koncept je sledeći: traži se preporuka najmanje dva člana, da bi se postao član unutar tog foruma; Po prijemu na forum postaje se običan korisnik; Da bi se došlo do pravih informacija mora se biti VIP korisnik da biste našli ono što je tu najbolje. Da bi se postao VIP korisnik prate se aktivnosti i nakon određenog vremena dopušta se pristup ozbiljnim ilegalnim stvarima (skimeri, dumpovi, 100% ispravni kradeni računi). Isto tako nije redak slučaj, kada je reč i distribuciji i pristupu zabranjenim pornografskim materijalima, da se pristup specifičnim forumima ostvaruje kroz ostavljanje svojih ličnih podataka koji se proveravaju. Zatim se od korisnika traži takođe da ostavi materijale koje im nisu bili poznati ili neke svoje "lično" napravljene (uglavnom kompromitujuće) slike ili video materijale kako bi bili sigurni u iskrenost korisnika i sve to da bi korisnici postali VIP članovi, koji imaju pristup velikom broju zabranjenog pornografskog sadržaja.

Praksa je pokazala, da jedan od najboljih vidova borbe protiv ovog tipa kriminala, predstavlja infiltraciju u takve grupe i forume da bi se došlo do organizatora. Čuveni forum kriminalaca Dark Market razotkriven je upravo na takav način (uspešnom infiltracijom), prouzrokujući štetu od 700 miliona dolara zbog aktivnosti te grupe organizujući kupovinu i prodaju ukradenih kreditnih kartica.[60]

Na slici 1. dat je ilustrativan prikaz načina na koje se realizuje ovakva vrsta kriminala i na koji način kriminalci ostvaruju zaradu.

60 The Guardian, *Welcome to DarkMarket – global one-stop shop for cybercrime and banking fraud*, http://www.guardian.co.uk/technology/2010/jan/14/darkmarket-online-fraud-trial-wembley, 05.01.2016.



Slika 1. Način realizacije visokotehnološkog kriminala

Kriminalci koji se bave ovim visokotehnološkim kriminalom pretežno deluju iz zemlje gde pravna regulativa iz ove oblasti nije dobro definisana. Uglavnom biraju zemlje poreskog raja i u njima formiraju offshore firme. Postoje određene ostrvske zemlje gde postoji više servera nego stanovnika. Stoga odatle sajber kriminalci deluju kako bi sakrili svoje tragove i dokaze.

Kao što se moglo primetiti iz svega prethodno izloženog u pitanju je ogroman broj različitih klasifikacija ove vrste kriminala što nam govori o tome kolika je raznovrsnost ovih dela i koliko su kompleksni njihovi pojavni oblici. Stvar se prilično usložnjava i zbog različitih kriterijuma koji se koriste po pitanju njihove klasifikacije što samo potvrđuje o kakvom se problemu radi. Ovom vrstom kriminala se bave pripadnici svih starosnih grupa - od maloletnih lica, studenata, pa sve do penzionera. Od samog znanja i veština učinioca, tipovi krivičnih dela mogu da variraju od ilegalnog kopiranja filmova, muzike, računarskih programa i njihove distribucije na ulici ili na veliko, kao i distribucije zabranjenih pornografskih materijala, pa sve do upadanja u državne informacione sisteme i informacione sisteme velikih korporacija.

Visokotehnolški kriminal je stvorio potrebu za angažovanjem posebno tehnički obučenih stručnjaka, ali i za reorganizacijom državnih organa (Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog

kriminala).[61] Glavni nosioci sistema za efikasno suzbijanje visokotehnološkog kriminala su nadležni državni organi koji predstavljaju policija, tužilaštvo, sudstvo, kao i njihove specijalizovane službe, ali i organi državne odbrane, ukoliko se učinjenim delom nanosi šteta ne samo pojedincu nego i celokupnoj državi. U Srbiji se ovom problemu poslednjih godina pristupilo veoma ozbiljno i postoje ohrabrujuća iskustva u radu specijalizovanih organa kao što su: posebne jedinice policije, bezbednosne agencije¸ Specijalno tužilaštvo i Specijalno odeljenje Viših sudova. Krivična dela iz oblasti visokotehnološkog kriminala su u isključivoj nadležnosti tih organa što ujedno predstavlja i institucionalni oblik za borbu protiv visokotehnološkog kriminala.[62]

Prethodno navedene informacije o visokotehnološkom kriminalu su veoma važne i moraju se shvatiti krajnje ozbiljno ukoliko postoji bilo kakva indicija o njihovom postojanju. Da bi država mogla efikasno da suzbija ovaj vid kriminala, neophodno je postojanje razvijenog pravnog sistema kao i zakonskih propisa koji se moraju poštovati i dosledno primenjivati. Ono što posebno zabrinjava je i činjenica da se sudije, tužioci i advokati zbog niskog nivoa, čak i elementarnog, znanja informatike, susreću sa mnogobrojnim problemima u postupku procesuiranja osumnjičenih odnosno okrivljenjih za izvršenje ovih tipova krivičnih dela. Ovo je i jedan od razloga što se umnogome otežavaju i produžuju postupci, zbog same prirode digitalnih dokaza, koji iziskuju brzinu i sposobnost, da bi se za veoma kratko vreme spasli digitalni dokazi i identifikovali izvršioci. Takođe, treba istaći da je proces suzbijanja ovog tipa kriminala nerazdvojivo povezan sa prevencijom i edukacijom u ovoj oblasti, a na tim poljima se do sada nije mnogo uradilo i da treba očekivati da se one realizuju kroz organizovani, sistematizovani i kontinuirani rad.

Na osnovu navedenog može se zaključiti da postoji velika potreba za dodatnom edukacijom iz informatičkih oblasti koja bi bila prilagođena pravnicima koji se bave tom oblašću. Takođe, na taj način će se graditi svest državnih organa u istražnom i krivičnom postupku o potrebi izuzetno brzog i efikasnog postupanja radi blagovremenog pribavljanja relevantnih digitalnih dokaza. Potrebno je postojanje brže i efikasnije saradnje istražnih i pravosudnih organa sa stručnjacima koji se bave upravo digitalnom forenzikom.

---

61 IPC Informativno Poslovni Centar, http://www.ipc.rs/Arhiva/Download/1010-241.pdf, 03.01.2016.

62 Banjeglav T., Dimitrijević N., *Istraga aktivnog kompjuterskog incidenta*, Ziteh - Udruženje sudskih veštaka za informacione tehnologije It veštak, 2004, http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-02.pdf, 27.06.2016.

1.3. ZAKONSKA REGULATIVA SAJBER KRIMINALA

Kao odgovor na rast visokotehnološkog kriminala, pojavljuje se i prvi zakoni koji se bavi rešavanjem problema vezanih za računarske prevare i nedozvoljenog upade u računare i računarske sisteme. Džava Florida je donela 1978. godine - „The Florida Computer Crimes Act". Ubrzo nakon toga usvojen je i američki federalni zakon o računarskim prevarama i zloupotrebama 1984. godine (eng. The Computer Fraud and Abuse Act - CFAA), sa svojim izmenama i dopunama u 1986, 1988, 1989 i 1990. godine. [63] Dok zakoni još nisu jasno definisali sajber kriminal odnosno visokotehnološki kriminal, tužioci su morali da se oslanjaju na tradicionalna krivična dela (prevara, zloupotreba službenog položaja, itd.), koja su definisana u krivičnim zakonima.

Computer analyze and response team kreiran je 1984. godine kao odgovor novom računarskom kriminalu, što se može smatrati prvim početkom digitalno forenzičke istrage.

U početku CFAA je trebalo da štiti samo računare, vlade i finansijske institucije od spoljnih upada i krađa. Godine 1986., CFAA iako dopunjen oštrijim kaznama štitio je i dalje samo računare koje koristi vlada ili finansijske institucije. Konačno 1994, napravljena je značajna revizija CFFA u kome se prvi put pojavljuje građansko-pravna komponenta i mogućnost vođenja građanskog parničnog postupka.

U Australiji je 1989. godine izmenjen i dopunjen „The Australian Crimes Act" u vezi sa prekršajima koji se odnose na računare (član 76.). U Velikoj Britaniji 1990 usvojen je Zakon o računarskim zloupotrebama (eng. Computer abuse act), kojim se upad na računar smatra kriminalnom radnjom.[64] Takođe je u Holandiji 1993. godine usvojen Zakon o računarskom kriminalu. Mnoge međunarodne organizacije su takođe donele preporuke u vezi sa izmenama zakonodavstava u vezi sa sprečavanjem računarskog kriminala. Na primer, Ujedinjene nacije su se bavile ovim problemom na VIII kongresu UN o sprečavanju zločina i postupanju sa delinkventima, koji je održan u Havani 1990. godine. Doneta je rezolucija, koja od svih članica UN-a traži da pojačaju napore u pravcu suzbijanja manipulacija sa elektronskim računarima koje zaslužuju primenu kaznene sankcije te da razmotre primenu različitih mera

63 The Computer Fraud and Abuse Act (as amended 1994 and 1996), Section 1030. Fraud and related activity in connection with computers, http://www.panix.com/~eck/computer-fraud-act.html, 22.01.2016.

64 Eoghan Casey, Digital Evidence and Computer Crime - Forensic Science, Computers, and the Internet, Second Edition, Academic Press 2004, str. 19.

u tom pravcu. Tu spada modernizacija krivičnog prava i postupka, razvijanje javne svesti o opasnosti od novog kriminala i potreba njegovog suzbijanja. To je potrebno uraditi putem obrazovanja i stručnog usavršavanja službenika državnih organa koji se sa njim susreću, razradom pravila profesionalne etike o postupanju sa kompjuterizovanim informacionim sistemima, kao i unapređenjem svih oblika zaštite računarskih delatnosti.[65]

Paralelno sa donošenjem raznih zakona vezanih za sajber kriminal, krajem 80-tih i u ranim devedesetim godinama pojavljuju se agencije u SAD koje su se bavile ovom problematikom i radile na razvoju treninga i izgradnji kapaciteta da bi rešavale problem vezan za sajber kriminal. Centri kao što su „SEARCH, Federal Law Enforcement Center (FLETC) i National White Collar Crime Center (NW3C)", pokrenuli su inicijativu za sprovođenje programa treninga za agencije reda i zakona.[66] NW3C u saradnji sa FBI osnivaju "Internet Crime Complaint Center" (IC3).[67] IC3 prihvata i prosleđuje žalbe koje se odnose na visikotehnološki kriminal odgovarajućim agencijama na ispitivanje. Takođe IC3 vodi statistiku o količini, tipu ovih žalbi.[68]

U Americi postoje zakoni kojima se sankcioniše slanje neželjene pošte. Zakon o kontroli napada slanjem neželjenog marketinga i pornografije ili CAN-SPAM stupio je na snagu 1. januara 2004. godine. [69] Prema tom zakonu za krivično delo se smatra svako slanje komercijalnog e-maila sa lažnim ili obmanjujućim zaglavljima poruke ili obmanjujućim naslovom poruke.

Kada je reč o Evropi, krupan korak u unapređivanju zakonodavstva u oblasti borbe sa visokotehnološkim kriminalom napravljen je 2001.g. usvajanjem *Konvencije Saveta Evrope o viokotehnološkom kriminalu*. Konvenciju su do sada potpisale 53 zemlje, a ratifikovale 42. Srbija se nalazi među državama koje su Konvenciju potpisale (2005) i ratifikovale (2009).[70] Od država koje nisu članice Saveta Evrope potpisale su je Kanada, Japan, Južna Afrika i SAD, ali su je ratifikovale samo SAD.

Ciljevi Konvencije su, pre svega, harmonizacija između nacionalnih

---

65 Vladica Babić, *Kompjuterski kriminal*, RABIC, Sarajevo, 2009, str. 71.

66 Ansonand S., Bunting S., Mastering Windows Network Forensics and Investigation, Sybex, 2007.

67 Internet crime Complaint Center. IC3, http://www.ic3.gov/, 23.03.2016.

68 Keith J. J., Forensic Analysis of Microsoft Windows Recycle Bin Records, Foundstone.com, April 2003.

69 The CAN-SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003) (codified at 15 U.S.C. §§ 7701-7713 and 18 U.S.C. § 1037) took effect on January 1, 2004, htpp://www.spamlaws.com/federal/can-spam.shtml, 28.05.2016.

70 Sl. glasnik RS, broj 19/09; Srbija je istovremeno ratifikovala i Dodatni protokol uz Konvenciju.

zakonodavstava kada je reč o materijalnopravnim odredbama u oblasti visokotehnološkog kriminala; uvođenje adekvatnih instrumenata u nacionalna zakonodavstva kada je reč o procesnim odredbama, kako bi se stvorila osnova za istraživanje i procesuiranje ovih krivičnih dela; ustanovljavanje brzih i efikasnih institucija i procedura međunarodne saradnje.[71] Prema Konvenciji, nadležni državni organi imaju ovlašćenja da pregledaju i zaplene svaki računar ili nosač podataka na kome se nalaze ili sumnja da se mogu nalaziti inkriminišući materijali, kao i da od provajdera elektronskih komunikacija prikupljaju podatke koji se odnose pre svega na upotrebu interneta i kreditnih kartica, preko kojih se može doći do podataka o potencijalnom počiniocu krivičnog dela visokotehnološkog kriminala.

Jedna od verovatno najdalekosežnijih odredbi tiče se tzv. *presretanja podataka*, odnosno vrste prisluškivanja elektronskih komunikacija (član 21. Konvencije). Do te mere će doći onda kada je za dokazivanje o postojanju krivičnog dela potrebno imati dokaze sakupljene u realnom vremenu, odnosno u trenutku kada se komunikacija vrši.[72] Ta oblast intervencije državnih organa je i najosetljivija, jer se praktično povređuje pravo na privatnost i pravo na prepisku, a sama Konvencija ne sadrži odgovarajuća ograničenja i garancije da takva prava neće biti zloupotrebljena (osim generalnog ograničenja da se pri izvršenju svih mera moraju poštovati međunarodni standardi ljudskih prava postignuti kroz pomenute međunarodne dokumente). Član 21, koji reguliše presretanje podataka, navodi da će se ova mera preduzeti za „ozbiljna dela", ali se iz same Konvencije ne može uvideti na koja se dela tačno mislilo, i koje bi karakteristike mogle neko delo odrediti kao ozbiljno. Ovako formulisan, član 21. zapravo ostavlja državama potpisnicama da same odrede kada će se primenjivati ovakve mere. Kada se posmatraju istrage koje mogu dovesti do jednog ili više izvršilaca krivičnih dela, kao što su dela organizovanog kriminala, terorizam, zlostavljanje dece, ovakva procedura može biti opravdana i moguća. Problem je što Konvencija ne poseduje mehanizme zaštite, kako se ona ne bi sprovodila za elektronske komunikacije preko računara i računarskih mreža osoba koje nisu počinioci, niti su pod istragom za vršenje dela visokotehnološkog kriminala. Ipak, ne treba previše kritikovati ovo rešenje budući da se radi o međunarodnom instrumentu koji treba da zaživi kroz legislativu i praksu svake pojedinačne zemlje. Odredba iz člana 21 Konvencije koja se tiče procesnog prava, isključivo je usmerena na

71 *Convention on Cybercrime – Explanatory Report*, http://conventions.coe.int/ Treaty/en/ Reports/ Html/185.htm, 01.04.2016.

72 Nasuprot tome je mera zaplene postojećih dokaza koji su ranije snimljeni na računaru ili drugom medijumu za čuvanje i prenos podataka, koju Konvencija takođe predviđa.

prikupljanje podataka (u smislu dokaza) u krivičnim istragama ili krivičnom postupku. Konvencija ne predviđa automatsko prikupljanje i snimanje podataka od strane provajdera, koje bi oni mogli po potrebi ustupiti policiji ili drugim nadležnim organima. Regulisano je ciljano sakupljanje od strane provajdera, nakon što dobiju nalog za tako nešto od organa koji sprovodi istražni ili krivični postupak.

Član 22. Konvencije bavi se *nadležnošću države potpisnice* kada dođe do činjenja nekog od krivičnih dela iz Konvencije. Država će imati nadležnost za procesuiranje ukoliko je krivično delo počinjeno na njenoj teritoriji, na brodu ili avionu koji nosi njenu zastavu. Osim toga nadležnost se ustanovljava i ako je krivično delo počinio državljanin te države, pod uslovom da je krivično delo počinjeno u drugoj državi koja poznaje istu takvu inkriminaciju ili van državnih teritorija (npr. na slobodnom moru). Može se reći da kombinacija teritorijalno-personalne jurisdikcije nije najsrećnije rešenje, iako je reč o klasičnom instrumentu kada je reč o međunarodnom pravu. Ipak, visokotehnološki kriminal izmiče klasičnim obrascima krivičnih dela, pa i krivične nadležnosti, tako da ovakva formulacija ostavlja niz otvorenih pitanja. Situaciju dalje komplikuje stav 2. istog člana, koji omogućava državama da ne primenjuju pravila o nadležnosti u određenim slučajevima ili pod određenim okolnostima. Kao da su i tvorci Konvencije bili svesni sprovođenja u praksi rešenja iz st. 3. i 4., pa su pokušali da stvari postave na malo čvršćim osnovama. Tako je regulisano da ako država ne izvrši ekstradiciju svog državljanina, mora suditi izvršiocu za počinjena dela na teritoriji druge države potpisnice; takođe, odredbe o nadležnosti države sadržane u Konvenciji neće derogirati odredbe domaćeg prava, prema kojem država može i na neki drugi način uspostaviti svoju krivičnu nadležnost.

Treći deo Konvencije se bavi *međunarodnom saradnjom država* na suzbijanju visokotehnološkog kriminala i prevazilaženju prepreka pri sprovođenju nacionalnog zakonodavstva za krivična dela koja po pravilu prelaze državne granice. Krivična dela visokotehnološkog kriminala često podrazumevaju učešće pojedinaca iz nekoliko zemalja širom sveta. Glavne odredbe ovog dela Konvencije posvećene su saradnji država na organizovanoj ili spontanoj razmeni podataka, koji se tiču eventualnog izvršenja nekog od krivičnih dela vezanih za upotrebu elektronskih komunikacija kao i mogućnosti ekstradicije počinilaca takvih dela iz jedne države potpisnice u drugu. Svaka država potpisnica mora poveriti određenom telu posao saradnje sa drugim državama u oblasti visokotehnološkog kriminala. U slučaju hitnosti, saradnja može biti uspostavljena i direktno između pravosudnih organa dve

države, kao i preko Interpola i drugih relevantnih kanala saradnje.

Prema članu 31. Konvencije svaka država potpisnica može tražiti od druge da sprovede određene istražne radnje na svojoj teritoriji ako je to neophodno za vršenje istrage u vezi sa nekim od dela predviđenih Konvencijom. Ukupno gledano, Konvencija predviđa različite vidove saradnje država, prilagođene tehnologiji vršenja istraga i procesuiranja ove vrste krivičnih dela. Takođe, državama je ostavljeno dosta prostora da u praksi ili dodatnim bilateralnim sporazumima dalje preciziraju one vrste saradnje za koje imaju poseban interes.[73]

Prema Mirjani Drakulić i Ratomiru Drakuliću možda najznačajnija aktivnost kojom se pokušava operacionalizovati saradnja u borbi protv visokotehnološkog kriminala u Evropi je formiranje EU Foruma, koji obuhvata razne agencije, provajdere internet usluga, operatore telekomunikacija, organizacije za ljudska prava, predstavnike korisnika, tela za zaštitu podataka i sve druge zainteresovane koji žele da se uspostavi saradnja u borbi protiv visokotehnološkog kriminala na evropskom nivou.[74] [75]

Zakonodavni okvir u zakonodavstvu Republike Srbije koji se odnosi na obezbeđivanje i pružanje krivično-pravne zaštite obuhvata, kao najvažnije, Krivični zakonik, Zakonik o krivičnom postupku, Zakon o organizaciji nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, Zakon o informacionoj bezbednosti i ratifikovanu Konvenciju Saveta Evrope o sajber kriminalu.

Kompjuterska krivična dela uvedena su u pravo Republike Srbije *Krivičnim zakonikom* iz 2005. godine. Regulisana su u Glavi 27 kao „krivična dela protiv računarskih podataka" (čl. 298–304a).[76] Osim toga Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala ustanovljeni su posebna policijska jedinica, posebno odeljenje pri Okružnom tužilaštvu u Beogradu i posebno odeljenje pri Okružnom sudu u Beogradu, čija je nadležnost isključivo vezana za borbu protiv

73 Dragan Prlja, Mario Reljanović, *Pravna informatika*, Pravni fakultet Univerziteta Union u Beogradu, 2014, str. 109-111.

74 Mirjana Drakulić, Ratomir Drakulić, *Cyber kriminal*, Fakultet Organizacionih nauka, Beograd, http://www.ponude.biz/ seminarski/0/49.pdf, 22.05.2015.

75 Grubor G., Galetin A., *Digitalna forenzička istraga u korporacijskoj zaštiti informacija*, Singidunum Revija, 2010.

76 *Krivični zakonik*, Sl. glasnik RS, br. 85/2005, 88/2005, 111/2009, 121/2012, 104/2013, i 108/2014.

visokotehnološkog kriminala.[77] [78] *Visokotehnološki kriminal* u smislu ovog zakona predstavlja vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku.

Cilj donošenja *Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala* bio je da se otkriju i krivično gone počinioci krivičnih dela protiv bezbednosti računarskih podataka, određenih krivičnim zakonom. Cilj *Krivičnog zakonika* je takođe da se otkriju počinioci krivičnih dela protiv intelektualne svojine, imovine i pravnog saobraćaja, kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže, računarski podaci kao i njihovi proizvodi u materijalnom ili elektronskom obliku.

U posebnom odeljku, Krivični zakonik definiše izraze koji se koriste u zakoniku, a u okviru toga daje *zakonske definicije* koje se odnose na kompjuterska krivična dela. *„Računarski podatak"* je predstavljena informacija, znanje, činjenica, koncept ili naredba koja se unosi, obrađuje ili pamti ili je uneta, obrađena ili zapamćena u računaru ili računarskoj mreži. *„Računarska mreža"* je skup međusobno povezanih računara koji komuniciraju razmenjujući podatke. *„Računarski program"* je uređeni skup naredbi koji služi za upravljanje radom računara, kao i za rešavanje određenog zadatka pomoću računara. *„Računarski virus"* je računarski program ili neki drugi skup naredbi unet u računar ili računarsku mrežu, koji je napravljen da sam sebe umnožava i deluje na druge programe ili podatke u računaru ili računarskoj mreži dodavanjem tog programa ili skupa naredbi jednom ili više računarskih programa ili podataka. *„Ispravom"* se smatra svaki predmet koji je podoban ili određen da služi kao dokaz kakve činjenice, koja ima značaj za pravne odnose, kao i računarski podatak, dok je *„pokretna stvar"* svaka proizvedena ili sakupljena energija za davanje svetlosti, toplote ili kretanja, telefonski impuls, kao i računarski podatak i računarski program.

Krivični zakonik predviđa sledeća *krivična dela protiv bezbednosti računarskih podataka:*

Oštećenje računarskih podataka i programa (član 298): „Ko neovlašćeno izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljivim

77 Reformom pravosuđa od 1. januara 2010. prestalo je da funkcioniše posebno sudijsko odeljenje i suđenje za ova dela je vraćeno u opštu nadležnost. Ukinuto je posebno odeljenje pri Okružnom tužilaštvu u Beogradu. Sada se gonjenjem dela VTK bave dva zamenika višeg javnog tužioca u Beogradu, koji su specijalizovani za tu oblast.

78 Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, Sl. glasnik RS, br. 61/05.

računarski podatak ili program, kazniće se novčanom kaznom ili zatvorom do jedne godine. Ako je prouzrokovana šteta u iznosu koji prelazi četiristo pedeset hiljada dinara, učinilac će se kazniti zatvorom od tri meseca do tri godine. Ako je prouzrokovana šteta u iznosu koji prelazi milion i petsto hiljada dinara, učinilac će se kazniti zatvorom od tri meseca do pet godina. Uređaji i sredstva kojima je učinjeno ovo krivično delo, ako su u svojini učinioca, oduzeće se".

Računarska sabotaža (član 299): „Ko unese, uništi, izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program ili uništi ili ošteti računar ili drugi uređaj za elektronsku obradu i prenos podataka sa namerom da onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte, kazniće se zatvorom od šest meseci do pet godina".

Pravljenje i unošenje računarskih virusa (član 300): „Ko napravi računarski virus u nameri njegovog unošenja u tuđ računar ili računarsku mrežu, kazniće se novčanom kaznom ili zatvorom do šest meseci. Ko unese računarski virus u tuđ računar ili računarsku mrežu i time prouzrokuje štetu, kazniće se novčanom kaznom ili zatvorom do dve godine. Uređaj i sredstva kojima je učinjeno ovo krivično delo oduzeće se".

Računarska prevara (član 301): „Ko unese netačan podatak, propusti unošenje tačnog podatka ili na drugi način prikrije ili lažno prikaže podatak i time utiče na rezultat elektronske obrade i prenosa podataka u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist i time drugom prouzrokuje imovinsku štetu, kazniće se novčanom kaznom ili zatvorom do tri godine. Ako pribavljena imovinska korist prelazi iznos od četiristo pedeset hiljada dinara, učinilac će se kazniti zatvorom od jedne do osam godina. Ako pribavljena imovinska korist prelazi iznos od milion i petsto hiljada dinara, učinilac će se kazniti zatvorom od dve do deset godina. Ko ovo delo učini samo u nameri da drugog ošteti, kazniće se novčanom kaznom ili zatvorom do šest meseci".

Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka (član 302): „Ko se, kršeći mere zaštite, neovlašćeno uključi u računar ili računarsku mrežu, ili neovlašćeno pristupi elektronskoj obradi podataka, kazniće se novčanom kaznom ili zatvorom do šest meseci. Ko upotrebi ovako dobijen podatak, kazniće se novčanom kaznom ili zatvorom do dve godine. Ako je došlo do zastoja ili ozbiljnog poremećaja funkcionisanja elektronske obrade i prenosa podataka ili mreže ili su nastupile druge teške posledice, učinilac će se kazniti zatvorom do tri godine".

Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (član 303): „Ko neovlašćeno sprečava ili ometa pristup javnoj računarskoj mreži, kazniće se novčanom kaznom ili zatvorom do jedne godine. Ako delo učini službeno lice u vršenju službe, kazniće se zatvorom do tri godine".

Neovlašćeno korišćenje računara ili računarske mreže (član 304): „Ko neovlašćeno koristi računarske usluge ili računarsku mrežu u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist, kazniće se novčanom kaznom ili zatvorom do tri meseca. Gonjenje za ovo krivično delo preduzima se po privatnoj tužbi".

Pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka (član 304a). Ovo delo podrazumeva da je izvršeno neko od prethodno navedenih dela. Počinilac je svako ko poseduje, pravi, nabavlja, prodaje ili daje drugom na upotrebu računare, računarske sisteme, računarske podatke i programe radi izvršenja krivičnih dela.[79]

Uništenje i oštećenje tuđe stvari (član 212): „Ko uništi, ošteti ili učini neupotrebljivom tuđu stvar, kazniće se novčanom kaznom ili zatvorom do šest meseci. Ako je delom iz stava 1. ovog člana prouzrokovana šteta u iznosu koji prelazi četristopedeset hiljada dinara, učinilac će se kazniti novčanom kaznom ili zatvorom do dve godine. Ako je delom iz stava 1. ovog člana prouzrokovana šteta u iznosu koji prelazi milion i petsto hiljada dinara ili je delo učinjeno prema kulturnom dobru, zaštićenoj okolini nepokretnog kulturnog dobra, odnosno prema dobru koje uživa prethodnu zaštitu učinilac će se kazniti zatvorom od šest meseci do pet godina. Za delo iz st. 1. do 3. ovog člana, ako je oštećena stvar u privatnoj imovini, gonjenje se preduzima po privatnoj tužbi".

Ilegalno prenošenje novca ili njegovo preuzimanje, ilegalni download zaštićenih materijala kao npr. muzičkih fajlova, videa ili programa ili drugi fajlova, koji su zakonom zabranjeni (upotreba računara za čuvanje slanje i primanje dečije pornografije, kockanje) ili kršenje bilo kog zakona određene države tumačiće se kao nedozvoljena aktivnost. Članom 185 b. Krivičnog zakonika definisano je kao krivično delo *iskorišćavanje računarske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnih dela protiv polne slobode prema maloletnom licu*.

Deo zakonskog okvira u Republici Srbiji u borbi protiv visokotehnološkog kriminala je i *Zakonik o krivičnom postupku (ZKP)*.[80] U njemu su opisani

79 Dragan Prlja, Mario Reljanović, *Pravna informatika*, Pravni fakultet Univerziteta Union u Beogradu, 2014, str. 106-108.

80 *Zakonik o krivičnom postupku*, Sl. glasnik RS, br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 i 55/2014.

procesni mehanizmi kroz koje nadležni državni organi svake zemlje pružaju mogućnosti, daju ovlašćenja i obaveze prikupljanja dokaza u svakom konkretnom krivičnom predmetu, kao i obezbeđivanje integriteta tih dokaza tj. mogućnosti njihovog kasnijeg oporavljanja i izvođenja na sudu. ZKP poznaje neke opšte dokazne radnje odnosno mehanizme kao što su privremeno oduzimanje predmeta, saslušanje itd. Osim toga ZKP poznaje posebnu definiciju elektronskih dokaza koji se pojavljuju u vezi sa izvršenjem krivičnog dela kao podatke i informacije koji su značajni za istragu, a smešteni su ili su preneti putem računara. Ti podaci imaju veliki značaj, a od presudne je važnosti način njihovog prikupljanja s obzirom da su ti podaci izuzetno osetljivi, vrlo se lako mogu izmeniti, obrisati ili na neki drugi način uništiti, što zahteva posebnu pažnju i adekvatan pristup u postupku prikupljanja i obezbeđivanja ovakvih dokaza.

Zakon o informacionoj bezbednosti, koji je donet 26. januara 2016. godine, a stupio je na snagu 5. februara 2016. godine. uređuje mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima.[81] Ovim zakonom se takođe reguliše odgovornosti pravnih lica prilikom upravljanja i korišćenja informaciono-komunikacionih sistema, određuju se nadležni organi za sprovođenje mera zaštite, koordinaciju između činilaca zaštite i praćenje pravilne primene propisanih mera zaštite.

Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala primenjuje se radi otkrivanja, krivičnog gonjenja i suđenja za:

„(1) krivična dela protiv bezbednosti računarskih podataka određena Krivičnim zakonikom;

(2) krivična dela protiv intelektualne svojine, imovine, privrede i pravnog saobraćaja, kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže i računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku, ako broj primeraka autorskih dela prelazi 2000 ili nastala materijalna šteta prelazi iznos od 1.000.000 dinara;

(3) krivična dela protiv sloboda i prava čoveka i građanina, polne slobode, javnog reda i mira i ustavnog uređenja i bezbednosti Republike Srbije, koja se zbog načina izvršenja ili upotrebljenih sredstava mogu smatrati krivičnim delima visokotehnološkog kriminala, u skladu sa članom 2. stav 1. ovog zakona".

81 *Zakon o informacionoj bezbednosti,* Sl. glasnik RS, br. 6/16, 28.01.2016, http://www.parlament. gov.rs, 20.02.2016.

U cilju odgovora na izazove informacione bezbednosti MUP Srbije je u okviru Službe za borbu protiv organizovanog kriminala osnovao Odeljenje za borbu protiv visokotehnološkog kriminala. U okviru izmena Pravilnika o organizaciji i sistematizaciji radnih mesta u MUP-u 2015. godine je formirano Odeljenje za informacionu bezbednost, kojim su objedinjene organizacione celine iz Uprave za IT i Uprave za vezu koje su se bavile različitim aspektima zaštite informacija i Centar za reagovanje na napade na informacioni sistem MUP-a (CERT MUP).[82]

Od velikog značaja za borbu protiv visokotehnološkog kriminala u Republici Srbiji imaće i izrada *Nacionalne strategije za razvoj informacione bezbednosti* na kojoj je rad započet u maju 2016.g.[83]

1.4. VISOKOTEHNOLOŠKI KRIMINAL - PRIMERI IZ PRAKSE

Internet ima i svoju drugu, ružnu stranu medalje. Za organizatore i izvođače upada u računarske sisteme i prevare koje se odnose na visokotehnološki kriminal, internet predstavlja platformu bez nadzora za podršku pri razmenjivanju informacija. Internet pruža informacije o novootkrivenim ranjivostima računarskih sistema, novootkrivenim exploitima (i njihovom razvoju), listama ranjivih lokacija (mreža i sistema), ukradenim finansijskim podacima kao i platformu za razmenu zabranjenih sadržaja.[84] Neke od najpopularnijih baza exploita koje koriste zlonamerni napadači su: The Exploit Database,[85] SecurityFocus[86] i OSVDB.[87]

Da bi se stekao bolji uvid u razmere specifičnosti i težinu ovog vida kriminala navešćemo neke od najinteresantnijih primera visokotehnološkog kriminala, koji su obeležile poslednje 2 decenije. Između juna i avgusta 1994. godine Vladimir Levin iz Petrograda nakon osamnaest upada u sistema Citybank izvukao je preko 10 miliona dolara. Sledeće godine je uhapšen u

82 Slobodan Nedeljković, *Razvoj e-uprava servisa, implikacije za bezbednost, odgovor MUP*, http://www.parlament.gov.rs/Odr%C5%BEano_javno_slu%C5%A1anje_o_sajber_bezbednosti_u_Republici_Srbiji.26780.941.html, 0706.2016.

83 Slobodan Nedeljković, *Koncept sajber bezbednosti MUP-a*, ICT Security, Beograd, 19-20. maj 2016.g.

84 McQuade III S. C., *Encyclopedia of Cybercrime*, Greenwood Publishing Westport, Connecticut, 2009.

85 Exploit Database, http://www.exploit-db.com/, 25.05.2016.

86 SecurityFocus, http://www.securityfocus.com/, 25.05.2016.

87 OSVDB, Response to Kenna Security's Explanation of the DBIR Vulnerability Mess, http://osvdb.org/, 25.05.2016.

Londonu 1997. je izručen američkim vlastima i osuđen na 36 meseci zatvora i novčanu kaznu od 250.000 dolara.

Kevin Mitnik u SAD je uhapšen i osuđen 1995. godine nakon krađe programa i upada u velike računarske sisteme i krađe programa. Interesantno je da je on to uspeo da uradi sa vrlo malo hakerskog znanja. Zapravo, najviše se služio metodama socijalnog inženjeringa.

Prvi masovni napad na internetu desio se 1998. godine kada je u mrežu ubačen samoreplicirajući program koji uništava podatke na računarima i širi se samostalno po mreži (tzv. „crv", eng. worm) koji je napravio veliku štetu i praktično uništio gotovo trećinu internet sadržaja u SAD. Iste godine uhapšen je Robert Tappan Morris koji je napisao kod za crv Morris. On je tvrdio da je to uradio iz radoznalosti da vidi koliko je internet veliki. Osuđen je na 3 godine uslovne kazne, 400 sati dobrovoljnog rada i 10.500 dolara novčane kazne.

Između avgusta 1999 i oktobra 1999. Jonathan Joseph James sa svega 16 godina izvršio je upade na high-profile organizacija. Jedna takva meta je bila i Agencija Ministarstva odbrane gde je postavio svoj backdoor, koji je omogućio da se vide osetljivi podaci kao što su elektronska pošta, korisnička imena i šifre zaposlenih. Takođe je upao i u NASA računare i ukrao program vredan 1.7 miliona dolara. Kao posledica toga NASA je bila prinuđena da privremeno isključi svoje računarske sisteme, čime je prouzrokovana velika finansijska šteta.

U narednim godinama gotovo da nije bilo internet prezentacije važnije vladine institucije u SAD, multinacionalne korporacije, međunarodne organizacije i sl. koja nije „hakovana" (eng. hacked) ili čiji sadržaj nije izbrisan, zamenjen nekim drugim sadržajem ili sklonjen na izvesno vreme sa interneta.

Do sada najdestruktivniji crv tzv. Slammer (poznati i kao Sapphire, Helkern or SQLExp), pušten je 2003. godine i on je u roku od deset minuta zarazio 90% računarskih sistema na planeti koji nisu imali (adekvatnu) zaštitu. Londonski Market intelligance (Mi2g) procenio je štetu koji je ovaj crv izazvao na oko 1.2 milijarde dolara.[88]

Prema rečima Davida Perry-a, direktora sektora za obrazovanje kompanije Trend Micro koja se bavi bezbednosti računara, napadi na računarske mreže postaju sve sofisticiraniji, teži za uočavanje, odbranu i okrenuti profitabilnoj dimenziji ove aktivnosti.[89]

Kako vreme prolazi svedoci smo sve ozbiljnijih finansijski prevara, naročito

88 Wikia Inc., http://malware.wikia.com/wiki/Slammer, 12.9.2015

89 Michael Coren, Cyber-crime bigger threat then cyber-terror, CNN International, 2005.

nakon pojave elektronskog bankarstva polovinom devedesetih godina prošlog veka i početkom masovnog korišćenja platnih kartica putem interneta. Na taj način su stvorene pretpostavke za rađanje modernog visokotehnološkog kriminala.[90] Organizovani kriminal odnosno terorističke grupe, pornografske i pedofilske mreže, grupe za ilegalnu trgovinu oružija, narkotika, ljudi, uznapredovale su u korišćenju modernih tehnologija. Šteta pričinjena od strane sajber kriminalaca u 2006. godini, iznosila je oko 200 milijardi evra na globalnom nivou. Na primer ChoicePoint, Inc korporacija je u 2006. godini morala da plati preko 15 miliona dolara kazne na osnovu tužbi građana i miliona potrošača zbog kompromitovanja finansijskih podataka.[91]

2007 zlonamerni program Zeus ili Zbot se prvi put pojavio, a do danas se modifikovao u nekoliko varijanti. Ovaj zlonamerni program služi za krađu bankarskih informacija preko internet pretraživača. Jedna od varijatni jeste da se on pojavljuje kao plugin za IE u vidu ActiveX komponente. U slučaju zaraze, prema rečima stručnjaka za bezbednost Piperevskog, jako je teško zaštiti korisnički računar, jer je zlonamerni program postao deo internet pretraživača. [92] Sve što korisnik unese kao input kroz internet pretraživač, zlonamerni program može da prikupi kao deo response/request interakcije, sa ciljem izvršenja određenih izmena u okviru tog servisa. Kada korisnik unese potrebne informacije za određenu transakciju željenog tranzita, ona se izvrši, međutim zlonamerni program u pozadini će izmeniti informacije o tranzitu, tako da bi transfer novca bio prerutiran na drugi račun, a ne željeni račun. To korisnik ne može da primeti, jer zlonamerni program lažira prikaz realnog transfera, sve dok ne proveri izvod sa računa.

Kriminalna organizacija „vor v zakone" sa bivšim sedištem u Ukrajini koja se 2007 raspala, raskrinkana je i trenutno funkcioniše po strukturi Al Kaide (rasprostranjene ćelije po zemljama u Evropi). Prepoznaju se po određenim tetovažama koje označavaju kako njihove aktivnosti tako i njihov rang u hijerarhiji. 2009 u gradu u Rumuniji (Craiov) organizacija je bila sponsor najboljim studentima da bi razvijali što više hakerskih alata tako da bi organizacija bila jedan korak ispred vendora koji proizvode

90 Koliko je „moderni" visokotehnološki kriminal opasan, može se videti iz napada koji se desio u februaru 2007. godine, kada je simultano napadnuto sa ciljem potpunog onesposobljavanja šest od trinaest tzv. „root servera" na internetu. Da su napadači uspeli u svojoj nameri, internet bi u potpunosti prestao da funkcioniše. Na sreću, samo su dva servera pretrpela značajnije posledice. Aaron Mannes, Threats to Internet, Computer Crime Research Center, http://www.crime-research.org/articles/threat-ti-Internet, 12.09.2015.

91 Matijašević J., Ignjatijević S., *Kompjuterski kriminalitet u pravnoj teoriji, pojam, karakteristike, posledice*, Infoteh-Jahorina Vol. 9, Ref. E-VI-8, pp. 852-856, March 2010.

92 Http://piperevski.com/, 20.07.2016.

alate za zaštitu od zlonamernih napada. Uz pomoć tih alata su pokupili veliki količinu brojeva kreditnih kartica sa kojim bi izrađivali falsifikovane kreditne kartice. Na osnovu falsifikata kartica kupovali bi zlato koje bi pretopljeno bilo prodato za gotov novac. Taj novac bi se dalje distributirao najvišim klasama u hijerahiji koje su zadužene za pranje novca (to mogu biti ministri, rukovodioci, banke koji su uključeni za određene procente i drugi ljudi na rukovodećim položajima).

U julu 2015, godine slučaj AshleyMadison.com – kanadski sajt za upoznavanje je bio kompromitovan od strane zlonamerni napadača (koji sebe nazivaju The Impact Team) da bi prikupili podatke iz cele baze korisnika tog sajta.[93] Svim korisnicima, koji su imali profile sa slikama, video materijalima i čet komunikacijom, bili su ukradeni podaci i objavljeni na Underground portalu. Podaci su javno postavljeni i na Dark web sajtu kome se može pristupiti samo preko TOR mreže preko portala Hidden Wiki. Posledica ovakve zlonamerne aktivnosti bila je određeni broj samoubistava članova sajta za upoznavanja zbog kompromitovanja privatnosti, jer su neki članovi imali javni život, porodice itd.

Takođe u 2015. godini desio se avionski incident, koji je prouzrokovan hakerskim napadom na mobilni telefon. Forenzički posmatrano mobilni telefon ima svoj operativni sistem u kome se nalaze drajveri koji regulišu hardverske komponente, između ostalog i drajveri za kontrolu baterija. Kernel operativnog sistema ima kontrolu upravljanja nad tim drajverima nezavisno od korisnika. Većina korisnika rootira (Android) tj. jailbreakuje (IOS) telefone. Na taj način se dozvoljava instaliranim programima da kontrolišu te drajvere, a ne operativni sistem. To znači da ako drajver sa kojim se reguliše baterija (njena temperature, voltaža) bude zloupotrebljen može za posledicu imati eksploziju mobilnog telefona. Za izazivanje eksplozije baterije nije uslov da telefon mora biti na internetu, već on može biti i u airplane modu, jer prisutni zlonamerni program na samom mobilnom telefonu može da zada zlonamernu instrukciju na primer kada se telefon nađe na određenoj visini. U tom slučaju ukoliko je mobilni telefon u avionu, prilikom poletanja određena visina postaje okidač tj. trigger (npr. na 300 metara) za zlonamernu instrukciju. Od decembra 2015. godine Austrian Airlines, Turkish Airlines obavezno isključivanje telefona u avionu. Eksplozija koja potencijalno može da se izazove nije velika ali može ugroziti integritet strukrure aviona. S obzirom na to da su Li-On baterije

93 Https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/, 20.07.2016.

zapaljive i da su se dešavali avionski incidenti koji su povezani direktno sa baterijom mobilnog uređaja u 2016. godine doneta je odluka od strane ICAO (International Civil Aviation Organization) da se kao kargo na civilnim letovima zabranjuje prenošenje LI-ON baterija.

Koliko štete ova vrsta kriminala može da prouzrokuje i koje metode odnosno tehnike koriste kriminalci, možemo sagledati kroz neke primere a koji se dešavaju kod nas i u okruženju.

Primer 1 Libanska klopka

Prevare koje se odnose na bankomate ostvaruju se upotrebom lažnih maski ili libanskih klopki koje se montiraju na otvor na bankomatu u koji ulazi kartica sa specijalnim štipaljkama u istoj boji kao i automat. Kada korisnik ubaci svoju karticu da podigne novac, ona ne ulazi u automat već upada u tu štipaljku. Pošto automat ne registruje karticu, korisnik ne uspeva da podigne novac ali ni da izvadi karticu. U tom momentu korisniku prilazi jedan građanin (kriminalac) koji počinje razgovor povodom problema na bankomatu, koji je navodno i pomenutom građaninu napravio problem sa karticom, ali da zna kako da se problem reši samo mu je potreban pin od kartice. Lakoverni građani obično daju pin. Međutim i pored toga što je navodno ukucan pin kartica ostaje i dalje u bankomatu bez izdatog novca. Zatim kriminalac daje predlog da se ode do centrale banke i da se tamo zatraži novac. I na kraju kad žrtva ode van vidokruga bankomata kriminalac skida štipaljku ubacuje karticu kuca pin i uzima novac.[94]

Primer 2 Kopiranje podataka sa kreditnih kartica

Ova prevara se uglavnom sprovodi u buticima, prodavnicama, restoranima i prevarant mora imati saučesnika iznutra. Zadatak saučesnika npr. konobara je da karticu koju uzme od gosta, odnosno mušterije prilikom naplate provuče kroz specifičan mali uređaj (skimmer) i iskopira podatke sa kartice. Tada se ti podaci prenose na magnetnu traku, koja se zalepi na belu plastiku, koja se onda koristi kao prava kartica.

Primer 3 Bugarski recept

Do ove prevara dolazi kada korisnik banke stoji ispred bankomata. Izvršioci krivičnog dela obično se pozicioniraju da budu iza korisnika da bi videli pin broj koji se ukucava. Npr. korisnik banke prilazi bankomatu i dok on odabira parametre iz menija bankomata oni mu neprimetno podmeću neku novčanicu ili papir da izgleda kao da mu je nešto ispalo. Paralelno prate šta on kuca i fokusiraju se da zapamte pin tj. četvorocifreni broj. Čim ukuca pin obraćaju mu se da mu kažu da mu je nešto ispalo. U momentu kada se korisnik savije da podigne tu „podmetnutu novčanicu" izvršioci krivičnog dela za to vreme izvlače karticu i beže. U tom momentu oni imaju podatke o pin kodu i vrše zloupotrebu dok se kartica ne blokira.

94 Banjeglav T., Dimitrijević N., *Istraga aktivnog kompjuterskog incidenta*, Ziteh - Udruženje sudskih veštaka za informacione tehnologije It veštak, 2004, http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-02.pdf, 20.06.2016.

Primer 4 Ugovor sa kućnim savetom o postavljanju bankomata

U jednoj od naših susednih država kriminalci su napravili ugovor sa kućnim savetom o postavljanju jednog bankomata predstavljajući se kao radnici banke. Kao uslugu za postavljenje bankomata rekli su da će da im renoviraju zgradu (da okreče ulaz, izvrše servisiranje i održavanje lifta). Bankomat je bio postavljen, ali nikada ni jednu novčanicu nije izbacio iz bankomata. To je naime bio lažni bankomat čiji je cilj bio da se iskopira što veći broj dump-ova (podataka sa kartice) sa kartica od građana, koji su pokušali da koriste postavljeni bankomat.

Primer 5 Farming ranjivost DNS servera

Do sada nije bilo primera u Srbiji koji predstavlja redirekciju sa nekog sajta. Ukoliko se pristupi nekom internet portalu koji se bavi elektronskom trgovinom, kriminalci mogu da iskoriste ranjivost DNS servera tako što će da preusmere saobraćaj. To znači kad korisnik pokuša da pristupi željenom serveru, vrši se redirekcija na neki server koji oni drže pod kontrolom. Obično se korisnicima nude se povoljne akcije tipa (ovonedeljna akcija tv 42 za samo 100 evra). Prevaranti daju primamljivu ponudu, a naivni korisnici obavljaju pravu kupovinu robe ili usluga, normalno unoseći sve one parametre sa svoje kartice. U ovom slučaju neće doći do zloupotrebe pin koda, ali će biti zloupotrebe podataka sa kartice, broja kartica i cvv2 broja, da bi kriminalci mogli dalje da je koriste. Uglavnom se koriste kombinovane tehnike fišinga farminga i tehnike socijalnog inženjeringa.

Primer 6 Fišing

Kriminalci su napravili lažnu web stranicu jedne banke. Zatim su koristili spam metode ili mail bombere šaljući elektronske poruke na milione adresa. Otuda i naziv fišing odnosno pecanje, a ko se upeca-upeca se. U tim e-mailovima postavlja se hyperlink ka toj određenoj stranici i kad se klikne na link, link vodi do mesta, gde se traže podaci korisnika i pin broj. U e-mail-u mogu biti navedeni različiti razlozi zbog čega korisnike banka kontaktira. Razlozi mogu biti od poboljšanja sigurnosti, pa do pretnji da će se u određenoj proceduri zbog nekorišćenja platne kartice, ukoliko se ne sarađuje, ugasiti račun. Ono što treba da se zna to je, da koja god banka da je u pitanju nikada neće e-mailom od korisnika tražiti pin kod kartice.

Primer 7 Socijalni inženjering korišćenjem telefoniranja

Kada korisnika neko pozove i predstavi se kao referent Banke i kaže: „poštovani korisniče primetili smo da je došlo do tri uzastopna neuspešna pokušaja prilikom pristupa vašem bankovnom računu, a kako vaš račun nije bio siguran i da bi vaši privatni podaci bili zaštićeni banka je zaključala vaš račun. Obavezni smo osigurati vaše transakcije putem interneta i molimo vas da pozovete određeni broj telefona". Pozivom tog broja telefona otpočinje tačno razrađeni scenario. Javlja se sekretarica, koja daje obaveštenje o mogućnosti izbora tipa usluge, koju korisnici mogu da odaberu pritiskom određenog tastera, a kao glavni cilj je da korisnici izdiktiraju svoje podatke o platnoj kartici.

Primer 8 Socijalni inženjering korišćenjem fišinga za zloupotrebu sms servisa na mobilnim telefonima

U Beogradu se dosta koristi sms servis prilikom plaćanja parkinga mobilnim telefonom. Za zloupotrebu ovog servisa napravljen je lap top sa uključenim bluetooth uređajem u sebi i specijalno podešenim programom, koji služi za sniffing tj. njuškanje. Na taj način vrši se uspostavljanje veze, preuzima se kontrola, vrši se širenje virusa, koji daje mobilnom telefonu naredbe za plaćanje u zavisnosti kako se to definiše. Većina korisnika ostavlja neke svoje podatke o platnim karticama, o pin kodovima upravo u telefonskom imeniku svog mobilnog telefona ili na nekom drugom mestu u telefonu. Osim pomenutog lap topa, na tržištu je moguće naći i bluetooth-ovu sniper pušku koja skenira i napada bluetooth uređaje na udaljenosti koje mogu biti veće i preko 1 km. Prva verzija ove puške prikazana je još 2004. godine na sajmu u Las Vegasu.

Primer 9 Socijalni inženjering korišćenjem uz pomoć fejsbuk profila

Kriminalci su otvorili profil na fejsbuku koji se zove Dream team agencija. Agencija je nudila mogućnost osvajanja 100 evra radi promocije otvaranja agencije i važila je za 3 osobe. Od potencijalnog dobitnika se očekivalo da pozove još jednog prijatelja u ovu grupu i da ako bude imao sreće, slučajnim izbornim sistemom može dobiti 100 evra. Sledeći korak je bio da učesnici u nagradnoj igri dobiju mail u kome se kaže da su slučajnim izborom sistema dobili nagradu od 100 evra. Naravno tom prilikom bili su zamoljeni da popune formular sa svojim podacima, kako bi im nagrada bila uplaćena. Podaci koji su traženi od korisnika su: broj kartice, cvv2 broj, datum i vreme

isteka kartice. Tom prilikom moraju se sve cifre napisati sa naznakom da se ti podaci dostave na ovaj profil. Time se serviraju sve potrebne informacije. Prevaranti su potom dodali u ovoj ponudi i poklanjanje kuće sa bazenom.

Primer 10 Socijalni inženjering korišćenjem trojanca u online bankarstvu

Korišćenje malicioznih programa bio je slučaj u Srbiji. Momak iz okoline Beograda je napisao Irc trojanca u Visual Basicu. Bio je oduševljen kako njegov virus funkcioniše u zemljama evropske unije jer je mislio da EU ima bolje sisteme zaštite. Primenom tehnike socijalnog inženjeringa, došao je do podataka o računu nemačkog državljanina. Svojim programom preuzeo je daljinsku kontrolu nad njegovim računarom. Praćenjem web kretanja ovog korisnika uvideo je da isti koristi online bankarstvo. Sa ovim programom pokupio je sve pristupne podatke o korisnikovoj banci. Uvideo je i opciju, da je moguće da se transfer novca vrši van zemalja EU. Za tu svrhu je otvorio poseban račun u našoj zemlji da bi tu nameru mogao da sprovede. Paralelno je kreirao jednu lažnu stranicu njegove banke koju je upload-ovao (pohranio) na njegov računar. U međuvremenu je korisniku banke poslao mail sa tekstom: „Poštovani Gospodine naša banka je uočila da ste Vi u protekloj godini izuzetno dobro trgovali sa hartijama od vrednosti. Sa tim u vezi mi smo odlučili da Vas nagradimo sa 1300 evra. Molimo vas da sledite dalja uputstva". Razlog za ova uputstva je bio taj da bi se dobio TAN kod (jedinstveni jednoznačni kod koji se koristi samo jednom) koji mu je bio potreban da izvrši transakciju. Međutim optuženi se nije najbolje snašao sa TAN kodom što je doprinelo otkrivanju njegovog identiteta.

Primer 11 Otmica IT-stručnjaka

Opasni kriminalci koji se bave pljačkama iznudama i otmicama, takođe su uvideli koristi od sajber kriminala tako što su počeli da vrše otmicu nekog stručnjaka, koji se sam bavio ilegalnim poslom i koji zna kako da donese pare iz daljine. Tako su jednog programera uhvatili i odveli u Budimpeštu, uzeli mu pasoš. Cilj je da stručnjak ubuduće radi za kriminalnu grupu, a ne za sebe. Stručnjak je pristupio australijskoj banci (koja nije tada koristila TAN brojeve) i pristupio je računu određene žrtve i izvršio transfer 5036 autralijskih dolara na račun naše domaće banke. Podatke je nabavio sa posebnog foruma, sa kog je posle izbačen kada se pročulo da je uhapšen. Ovo krivično delo izvršila su uglavnom lica starosnog doba 20-30 godina. Radilo se o organizovanom obliku kriminala na internetu.

Primer 12 Internet prevara

Reč je o falsifikovanju poštanskih markica u SAD. Ikar Dakota Feris je priznao da je u periodu od 2004 do 2009 godine bio umešan u izradi i štampanju falsifikovanih SAD poštanskih markica, koje su se legitimno prodavale preko sajta stamps.com. Takođe je priznao da je nudio falsifikovane poštanske markice putem interneta predstavljajući ih kao popust za poštarine. Ukupan profit koji je napravio je iznosio 345.000 dolara.[95]

Primer 13 Kršenje autorskih prava

Okružni sud u Beogradu oglasio je krivim G.M. iz Beograda i osudio na zatvorsku kaznu od 6 meseci uslovno, zbog toga što je od 2006 do 2008 u svom stanu u Beogradu neovlašćeno umnožavao primerke autorskih dela i oglašavao njihovu prodaju preko interneta. Nudio je 13.433 naslova autorskih dela i nakon elektronske porudžbine slao CD i DVD diskove poštom i na taj način ostvario imovinsku korist od 400.000 din.[96]

Primer 14 Internet prevara

Okružni sud u Beogradu oglasio je krivim J.Š. I njegovu devojku T.D. iz Novog sada zbog prevare počinjene preko interneta i osudio na zatvorsku kaznu od 6 meseci uslovno, zato što su od januara 2007 do jula 2007.g. doveli u zabludu 29 britanskih državljana da će im obezbediti smeštaj tokom Exit-a u hotelu u Novom Sadu. Prevaranti su oštećene slali taksijem u hotel sa kojim nisu imali nikakav poslovni aranžman.[97]

Primer 15 Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka (čl. 302 str.1 Krivičnog zakonika)

Posebno tužilaštvo podnelo je istražnom odeljenju Okružnog suda u Beogradu predlog za preduzimanje određenih istražnih radnji Kt.vtk.br. 56/07 protiv V.M. (31) iz Beograda zbog osnovane sumnje da je, dana 08.02.2007. godine, u vremenskom intervalu od 22:39:50 do 22:49:08 časova, u Kragujevcu, u hotelu „Stari Grad", koji posluje u sastavu preduzeća „Tourist gamesstari grad", neovlašćeno pristupio računarskoj mreži ošt. preduzeća „Yunicom" sa sedištem u Beogradu. Putem interne računarske mreže hotela u kojem je

95 The Department of Justice, http://www.justice.gov/criminal/cybercrime/ferrisPlea.pdf, 23.05.2016.

96 Dragan Prlja, *Sajber kriminal*, Pravni fakultet Univerzitet Union, http://www.prlja.info/sajberkriminal.pdf, 30.04.2012.

97 *Ibidem*.

boravio okrivljeni je konektovao svoj računar na globalnu računarsku mrežu - internet i pristupao sa IP adrese: 87.116...., koja je u to vreme od strane internet provajdera „SBB“ bila dodeljena preduzeću „Tourist gamesstari grad“. Na taj način prekršio mere zaštite uspostavljene od strane ošt. preduzeća „Yunicom“ , unoseći u svoj računar web - adresu broj: 217.24..... dodeljenu ošt. preduzeću „Yunicom“ za pristupanje web - mail serveru „World Client for MDaemon“, preko kojeg su zaposleni iz ošt. „Yunicom-a“ ostvarivali poštanski saobraćaj. Nakon čega je kao bivši radnik „Yunicom-a“, znajući adrese elektronske pošte i lozinke zaposlenih lica, iste unosio na svom računar i neovlašćeno pregledao sadržaj elektronske pošte.[98]

Iz navedenih primera mogu se uočiti određene specifičnosti:

1. nedozvoljene aktivnosti se uglavnom rade za novac, profit ili korist;
2. nedozvoljene aktivnosti (pogotovu napadi na računarske sisteme) postaju sve sofitsticiranije, odnosno teže su za detekciju, analizu, brzo se šire, a alati koji se koriste za tu namenu nisu javno dostupni;
3. krajnji korisnici postaju izloženiji sve većim rizicima (napadi su promenili fokus sa servera na klijentske računare);
4. napadi su uglavnom pokreću iz inostranstva;
5. postoje velike razlike između sofictičiranih alata za napad i onih koji se koriste za njihovu detekciju i analizu.

Prema APWG (Anti-Phishing Working Group) izveštaju u trećem kvartalu 2012 godine detektovano je preko 6 miliona malicioznih programa. [99] [100] Od toga bili su 78.04% trojanci, 6.56% virusi, 6.53% crvi, 5.33% maliciozni programi za internet prevare eng. Rogueware, i ostali 3.33%. Procenat napada na finansijske usluge i usluge plaćanja iznosio je čak 66.5% od svih napada. Primetan je porast napada na aukcijske sajtove na 4.5%. Prema broju hostovanja fišing sajtova u trećem kvartalu 2012 Amerika je vodeća sa 73.04% , iz razloga što se najveći procenat svetskih web sajtova i domenskih imena hostuje u Americi (a fišing se realizuje preko hakovanih ili kompromitovanih web sajtova). Države sa najvećim procentom zaraženih računara su Kina 53.17%, Južna Koreja 52.77%, Turska 42.51%, Slovačka 40.59%, Tajvan 40.20%. Norveška sa 20.16% i Irska sa 18.40% spadaju u

98 *Ibidem.*

99 APWG, Phishing Activity Trends Report, 3rd Quarter 2012 http://www.apwg.org/ download/ document/84/apwg_trends_report_q3_2012.pdf, 27.05.2016.

100 Unifying the global response to cybercrime, http://www.antiphishing.org, 26.05.2016.

zemlje sa najmanjim brojem zaraženih računara.[101]

U sledećoj tabeli dati su statistički podaci koji pokazuju različite tipove napada na računarske sisteme i njihov ukupan procenat (prijavljenih slučajeva) u 2012 godini:

Tabela br. 2. Statistički prikaz prijavljenih napada[102]

TIP NAPADA	PRIJAVLJENI SLUČAJEVI
Krađa podataka	33%
Zloupotreba email-a	22%
Nedozvoljen pristup	19%
Izmena podataka	15%
Napadi virusima	5%
DoS napadi	3%
Ostalo	3%

Kada je u pitanju visokotehnološki kriminal digitalna forenzika je jedan od najznačajnih faktora u procesu otkrivanja istine o nedozvoljenim aktivnostima. Međutim, digitalna forenzika, odnosno forenzika računarskih sistema može da deluje i preventivno. Upravo njeni rezultati su ti koji pokazuju kako se neka nedozvoljena aktivnost desila, na primer gde su bili propusti i na koji način su se oni desili. Samim tim moguće je predupredi ti iste ili slične nedozvoljene aktivnosti. Dakle, učenjem od računarske forenzike kao podskupa digitalne forenzike i implementacijom tih saznanja u mehanizme zaštite IKT-a, ona postaje bitan elemenat proaktivne zaštite.

101 Kent K., Chevalier S., Grance T., Dang H., *Guide to Integrating Forensic Techniques into Inci dent Response*, NIST Special Publication 800-86, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930, August 2006.

102 Carvey H., *Windows Forensics and Incident Recovery*, Addison Wesley, 2004.

2. DIGITALNA FORENZIKA I POSTUPAK ISTRAGE

Kao odgovor na visokotehnološki kriminal javila se potreba za razvojem nove naučne discipline koja će se njime baviti, kao i potreba regulisanja pravnih osnova vezanih za uspešno procesuiranje krivičnih dela iz ove oblasti.

Digitalna forenzička istraga predstavlja proces koji korišćenjem naučnih metoda i tehnologije, razvija i testira teorije kroz hipoteze, analizirajući digitalne uređaje, koji predstavljaju relevantan dokaz u sudskom postupku.[103] Cilj takve istrage je da se utvrdi istina o nedozvoljenoj aktivnosti i svim okolnosti u vezi sa počiniocem i načinom izvršenja krivičnog ili prekršajnog dela. Digitalni dokaz u tom slučaju predstavlja digitalni objekat koji sadrži pouzdane informacije koje podržavaju hipotezu ili je opovrgavaju.[104]

Kada je reč o elementima računarskog i internet kriminala, njih predstavljaju nedozvoljene aktivnosti počinilaca zajedno sa okolnostima pod kojima je to delo počinjeno. Kako bi se učinjena dela dokazala i njihovi počinioci procesuirali i sankcionisali, potrebno je primeniti procedure digitalne forenzike kao naučne discipline sa izuzetno značajnom praktičnom primenom.

Digitalna forenzika kao relativno nova naučna disciplina uspostavljena 1999. godine. Ona obezbeđuje pouzdane alate za istragu (tj. otkrivanje) računarskog kriminala, čuvanje (upravljanje) digitalnih podataka, dokazivanje (analizu) i ekspertsko svedočenje/veštačenje (prezentaciju) digitalnih dokaza pred sudom. U slučaju kada je došlo do zloupotrebe IKT sistema odnosno računarskog kriminala ili kada postoji potreba za upravljanjem računarskim incidentom, odgovore će nam dati digitalna forenzika.[105]

Tradicionalna forenzika (forenzička obrada različitih vrsta nedozvoljenih postupanja) nije imala adekvatan odgovor na sve prisutniju vrstu kriminala vezanu za računarske sisteme, odnosno kriminala koji se odvija na globalnoj mreži internetu. Upravo je digitalna forenzika ta naučna disciplina koja može ponuditi relevantan dokaz odnosno digitalni dokaz. Razvoj IKT postavlja velike izazove pred digitalne forenzičare, koji moraju

103 Vanja Korać, Dragan Prlja, i Gordana Gasmi, *High Tecnology Criminal and Digital Forensics*, in: Preventing and Combating Cybercrime, Cluj-Napoca, Accent, 2016, str. 85.

104 Allen B., *Collecting Digital Evidence from Intrusion Detection System*, CGS 5132 - Computer Forensics II, 2002, http://www.authorstream.com/ Presentation/ Kliment-24060-allen-Collecting-Digital-Evidence-Intrusion-Detection-Systems-designed-forensic-use-as-Entertainment-ppt-powerpoint/, 19.06.2016.

105 Aaron P., Cowen D., Davis. C., *Hacking Exposed Computer Forensics*, Second Edition, The Mcgraw-Hill Companies, 2010.

imati permanentnu i svakodnevnu edukaciju, kako bi bili za korak ispred počinioca koji sprovode nedozvoljene aktivnosti u digitalnom okruženju. Za digitalnog forenzičara od presudne važnosti je praćenje i razvoj informacionih tehnologija. Ponekad su razlike u operativnom sistemu ili verziji nekog programa od suštinskog značaja. Zato je bitno postojanje profilisanosti digitalno-forenzičkih eksperata prema stručnoj oblasti (operativni sistemi, baze podataka, mrežni sistemi itd.). Brzina tehnološkog razvoja uticala je i na razvijanje ove mlade naučne discipline, koja zajedno sa paralelnim razvojem drugih nauka, primenjuje nove metode koje utiču na brzinu i jednostavnost prikupljanja čvrstih dokaza. Upravo takva složenost problema na koju forenzičari nailaze, uslovili su i specijalizovanje stručnjaka za različite oblasti.

U taksonomiji digitalne forenzike, a u odnosu na predmet forenzičke istrage, digitalnu forenziku možemo podeliti na: *forenziku računarskih sistema, forenziku mobilnih uređaja, forenziku baza podataka i forenziku računarske mreže uključujući i internet ili kibernetičku forenziku.*[106]

Digitalna forenzika može se primeniti od javnog sektora (policijskog, sudskog i vojnog), do civilnog sektora (bankarskog sektora, sektora osiguranja i kompanija različitih profila). Svi ovi sektori moraju biti izuzetno oprezni sa podacima kojima raspolažu, jer u protivnom može biti prouzrokovana nemerljiva šteta zbog industrijske špijunaže, zloupotrebe IKT sistema, ali i nekih drugih oblika nedozvoljenih postupaka. Procena je da šteta od različitih delovanja visokotehnološkog kriminala, ne uzimajući u obzir njegove potencijalne veze sa organizovanim kriminalom, na godišnjem nivou iznosi oko 200 milijardi dolara.107

Najveći deo računarske forenzike odnosi se na forenziku računarskih sistema. *Digitalna forenzika računarskog sistema* obuhvata naučno ispitivanje i analizu podataka sa hard diskova, fajl sistema i prostora za skladištenje podataka unutar računarskog sistema, da bi se ti podaci mogli koristiti kao neoborivi i čvrsti dokazi pred sudom.[108] [109]

Prema dr. Vulfu računarska forenzika predstavlja metodičan niz tehnika i procedura za prikupljanje dokaza iz računarske opreme i drugih uređaja za skladištenje podataka i digitalnih medija, koji mogu biti predstavljeni sudu u adekvatnoj formi.

106 Albert J. Marcella, Robert S. Greenfield, *Cyber Forensics*, CRC Press LLC, 2002, str. 317.

107 Dragan Prlja, *Sajberkriminal*, http//www.prlja.info/sk2008.pdf, 25.02.2012.

108 Ahmad D., Dubrawsky I., Flynn H., Grand J., Graham R., Johnson N. L., Kaminsky D., Lynch F. W., Manzuik S. W., Permeh R., Pfeil K., Russell R., *Hack Proofing Your Network*, Second Edition, Syngress Publishing, Inc, Rockland, MA, 2002.

109 Alghafli K. A., Jones A., Martin T. A., *Forensic Analysis of the Windows 7 Registry*, Khalifa University of Science, Technology and Research, 2010.

Stiv Hejli sa instituta Cybersecurity posmatra računarsku forenziku kroz postupke dobijanja, očuvanja, identifikacije, tumačenja i dokumentovanja računarskih dokaza prema propisanim pravilima, kroz pravne procese i postupak očuvanja integriteta dokaza, činjenična izveštavanja o pronađenim informacijama kao i pružanje stručnog mišljenja pred sudom u vezi sa pronađenim dokazima.

Na osnovu navedenih definicija može se zaključiti da računarska forenzika podrazumeva upotrebu unapred definisanih procedura i tehnika za detaljno ispitivanje računarskog sistema, a sa ciljem dobijanja relevantnih digitalnih dokaza.

U literaturi neretko može da se pronađe poistovećivanje digitalne forenzike računarskog sistema sa procesom povratka podataka. Ovo je samo delimično tačno. Digitalna forenzika oporavlja podatke koje je korisnik (maliciozni) namerno sakrio ili izbrisao, za razliku od slučajno izgubljenih ili izbrisanih podataka. Krajnji cilj digitalne forenzike je da se obezbedi validnost oporavljenih podataka kao dokaza pred sudom.

Forenzičari računarskih sistema sledeći strogo definisana pravila prikupljaju medijume (hard diskove i sve druge sekundarne medije za skladištenje podataka) za koje sumnjaju da se na njima nalaze digitalni dokazi. Osiguravaju ih od bilo kakvih promena, i od velike količine digitalnih podataka moraju pronaći relevantne i održive dokaze. Oni vrše analize, kako bi rekonstruisali aktivnosti, koje su vršene sa računarima i pripremaju razumljiv izveštaj, koji će moći poslužiti za vođenje sudskog procesa ili interne istrage u kompaniji. Procedura upravljanja i oporavka podataka posle destruktivnog vanrednog događaja podrazumeva korišćenje digitalno-forenzičkih tehnika i alata za oporavak izgubljenjih podataka sa hard diskova. Računarska forenzika igra veliku ulogu u praćenju potencijalnih počinilaca nedozvoljenih aktivnosti, putem identifikacije nedozvoljenih aktivnosti, prikupljanja dokaza, izgradnje "lanca nadležnosti nad digitalnim dokazima", analize dokaza, prezentovanja pronađenih dokaza, svedočenja u cilju vođenja sudskog postupka protiv okrivljenog. Digitalni dokazi mogu biti oslobađajući, optužujući ili mogu da ukazuju na osnovanu sumnju.

2.1. ULOGA RAČUNARA U KRIMINALNIM AKTIVNOSTIMA

U periodu od 1994. godine do 1998. godine Ministarstvo pravde Sjedinjenih Američkih Država (eng. *US Department of Justice* - USDOJ) kreiralo je skup kategorija i objavilo vodiče, koji se odnose na pretragu i zaplenu računara. U vodičima su definisane kategorije u kojima se pravi razlika između informacija i hardvera, kada su u pitanju dokazi. *Hardver* se posmatra kao *elektronski dokaz*, a *informacija* kao *digitalni dokaz*. Ova distinkcija je veoma važna sa aspekta dokaznog stanovišta kao i razvoja različitih procedura. U ovom kontekstu informacije se posmatraju u formi programa i podataka koji su smešteni u računaru, dok se pod hardverom podrazumevaju sve fizičke komponente računarskog sistema. S obzirom da kategorije nisu međusobno isključive, neka kriminalna aktivnost može da pripada u više kategorija. Te kategorije Casey je sintetizovao na sledeći način:

1. Hardver kao dokaz (*Hardware as Evidence*);
2. Hardver kao instrument kriminalne aktivnosti (*Hardware as an Instrumentality*);
3. Hardver kao zabranjeni materijal ili plod kriminalne aktivnosti (*Hardware as Contraband or Fruits of Crime)*;
4. Informacija kao dokaz (*Information as Evidence*);
5. Informacija kao instrument kriminalne aktivnosti (*Information as an Instrumentality*);
6. Informacija kao plod kriminalne aktivnosti (*Information as Contraband or Fruits of Crime*).[110] [111]

Ministarstvo pravde Sjedinjenih Američkih Država je 2002. godine ažuriralo postojeće vodiče u skladu sa današnjom tehnologijom i zakonom i objavilo uputstvo za "Pretragu i zaplenu računara i pribavljanje elektronskih dokaza u krivičnim istragama".[112] Veliku zaslugu u kreiranju dokumenta ima profesor Pravnog fakulteta univerziteta Džordž Vašington Orin S. Kerr, koji je zajedno sa svojim kolegama bio angažnovan na izradi ovog uputstva. Razlika između vodiča i uputstva je ta što se informacijama i hardveru pridaje ista

110 Computer Crime and Intellectual Property Section (CCIPS), *Searching and seizing computers*, http://www.irational.org/APD/CCIPS/toc1.htm#IV, 15.12.2015.

111 Casey E., *Digital Evidence and Computer Crime - Forensic Science*, Computers and the Internet, third Edition, Elsevier Academic Press, 2011, str. 42-48.

112 Eng. "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations"The Department of Justice, http://www.justice.gov/criminal/cybercrime/searching.html, 15.12.2015.

važnost, dok se kod uputstva pridaje veći značaj informacionom delu. Ukoliko hardver sam po sebi ne predstavlja dokaz, instrument ili plod kriminalne aktivnosti onda se on posmatra kao skladište za podatke.[113] Uputstvo ukazuje na to da čak i ako je sama informacija bila meta kriminalne aktivnosti može biti neophodno da se zapleni hardver iz različitih razloga. S obzirom da svaka od navedenih kategorija podrazumeva jedinstvene zakonske procedure koje se moraju poštovati, ovo uputstvo treba da bude konsultovano od strane istražitelja, tužioca i advokata odbrane.

Dakle kada je reč o konfiskovanju i pretraživanju računara pre samog preuzimanja računarskog sistema mora postojati pravni dokument, da se takva aktivnost može sprovesti. Pretraživanje sa ciljem pronalaženja digitalnih dokaza ne radi se za svaku nedozvoljenu aktivnost na isti način (procedure su iste, ali se tehnike razlikuju od slučaja do slučaja) već može biti izvedeno na različite načine. Na primer, kod zlonamerne aktivnosti tipa email fišing napada, uglavnom se štampaju email zaglavlja i tela samih poruka. Znači nakon pretraživanja računarskog sistema i pronalaženja fajlova koji sadrže email poruke vrši se njihovo štampanje. Ne postoji potreba da se radi bitstream kopija hard diska. Ukoliko je reč o računarskom kriminalu za čije je izvođenje podrazumevalo upotrebu malicioznih programa kopiraju se kompletne strukture instalacionih fajlova u momentu kada je računar u operativnom radu i nema potrebe da se radi bitstream kopija hard diska. Ukoliko digitalnom forenzičaru nije poznato šta se konkretno traži u fajl sistemu, a stigao je zahtev iz suda da se daju odgovori na pitanja (koja se odnose na digitalne dokaze iz prenosnog računara osuđenika), sa kim je komunicirano, kad je komunicirano, šta je otvarano na internetu, kakve dokumente je imao na svom računaru. U tom slučaju se mora uraditi bitstream kopija kompletnog hard diska da bi se tražene informacije pronašle. U slučaju privermenog oduzumanja opreme iz organizacije i njenog prenošenja u forenzičku laboratoriju, forenzičar je obavezi da izvrši uslikavanja opreme pre odnošenja i nakon vraćanja iz forenzičke laboratorije. Oprema se uslikava sa profesionalnim digitalnim aparatom da bi se utvrdilo stanje pre i posle forenzičkih aktivnosti, kao potvrda da li je nešto menjalo ili je oprema ostala u istom stanju. Na primer, kod transporta prenosnih računara obavezno je uslikavanja stanja šrafova, da bi se sprečilo neko namerno zameni hard disk. S tim u vezi vrši postavljanje specijalnih plombi prozvedeni od proizvođača forenzičke opreme.

Henry Lee, profesor Forenzičke nauke na univerzitetu New Have i direktor "Forensic Research and Training Center" ističe da paralelno sa istražnim fazama,

113 Ansonand S., Bunting S., Mastering Windows Network Forensics and Investigation, Sybex, 2007.

digitalni dokazi prolaze kroz svoje faze.[114] Prva faza je faza *prepoznavanja* (eng. recognition) odnosno izjednačavanje mesta pronalaženja dokaza sa mestom izvršenog zločina. Navedeno prepoznavanje vrši se tokom izvođenja istražnih radnji prikupljanja dokaza (faza istraživanja i pretraživanja). Druga faza je *identifikacija* (eng. identification) u kojoj se pregledaju i upoređuju klasne karakteristike dokaza sa poznatim uzorcima da bi se utvrdila klasa konkretnog dokaza. Poslednja faza je *individualizacija* (eng. individualization), gde se pregledaju individualne karakteristike predmetnog dokaza. Tom prilikom se određuje da li je predmetni dokaz jedinstven u odnosu na druge dokaze u okviru klase ili predmetni dokaz potiče iz predmetnog izvora izvršenja krivičnog dela kao i ostali dokazi. Kada su računari u pitanju, teško je izvršiti individualizaciju digitalnog dokaza u istoj meri kao što se to može uraditi sa fizičkim dokazom, zato što su digitalni objekti generisani instrukcijama kod kojih se može javiti i element slučajnosti.

Računar postaje deo istrage kada se na njemu ili sa njim izvrši neka nedozvoljena radnja. *Lokardov zakon*, čiji je tvorac Edmond Lokard, govori o tome da prilikom svakog kontakta dva objekta, postoji neka razmena materije, tj. svaki kontakt ostavlja trag.[115] U slučaju digitalnih dokaza tu materiju možemo da posmatramo kao npr. fajlove koji se generišu ili razmenjuju putem računara, koji međusobno komuniciraju i time vrše razmenu podataka, informacija tj. fajlova, a u osnovi su bitovi. To znači da je moguće dovesti određene dokaze u vezu sa izvršiocem. Prema tome sve što uđe na scenu nedozvoljenih aktivnosti i izađe ostavlja trag. Instalacije i deinstalacije programa na operativnom sistemu ostavljaju tragove u operativnom sistemu. Kod analize mrežnih uređaja postoji log fajlovi (na primer kod DHCP servera) koji čuvaju informacije o IP adresama, o pripadajućim MAC adresama i vremenima kada su adrese dodeljivane. U forenzičkoj praksi čest je slučaj da se prilikom forenzičke istrage u okviru organizacije desi da se prema logovima ustanovi prisustvo računara sa MAC adresom koja ne pripada organizaciji. U tom slučaju proverava se proizvođač te MAC adrese. Kada se ustanovi da računar sa otkrivenom MAC adresom nije vlasništvo organizacije, vrše se mere pojačanog nadzora, da se utvrdi ko od korisnika u organizaciji ima privatni računar određenog vendora i na taj način se pronalazi zlonamerni napadač koji je izvršio nedozvoljenu aktivnost.

114 Carvey H., Altheide C., *Tracking USB storage: Analysis of Windows artifacts generated by USB storage devices*, Digital Investigation 2, pp. 94-100, Elsevier Academic Press, Burlington, MA 2005, http://www.sciencedirect.com/,10.07.2016. science/ article/ pii/ S1742287605000320/ pdfft?md5= b4d986c553c49a983e66ae2b68a0c4a6&pid=1-s2.0-S1742287605000320-main.pdf, 19.06.2016.

115 Bem D., Huebner E., *Computer Forensic Analysis in a Virtual Environment*, International Journal of Digital Evidence Fall 2007, Volume 6, Issue 2, 2007.

2.1.1. Hardver kao instrument kriminalne aktivnosti

U slučaju da je hardver odigrao značajnu ulogu u kriminalnoj aktivnosti, onda se on smatra instrumentom kriminalne aktivnosti. Ova diferencijacija je veoma bitna zbog slučajeva kada je hardver korišćen kao oružje u kriminalnoj aktivnosti, što može dovesti i do dodatnih optužbi ili uvećanja kazne. Dobar primer hardvera kao instrumenta kriminalne aktivnosti, može da bude hardver koji je napravljen isključivo za svrhu kriminalne aktivnosti kao što je snifer (eng. sniffer) uređaj koji je posebno dizajniran da prisluškuje mrežu. Ovaj tip uređaja se koristi za prikupljanje velikog broja osetljivih informacija, koje se mogu zloupotrebiti kao što su šifre, privatni podaci, brojevi bankovnih računa ili kartica, hardverske adrese računara, IP-adrese računara i druge informacije, koje mogu napadaču pomoći da kompromituje bezbednost računarskog sistema. Forenzička provera da li postoji neko ko sniffuje saobraćaj između lokalne i kranje destinacije može da se ostvari kroz traceroute uz pomoć vrednosti TTL parametra. TTL prilikom pingovanja Microsoft OS ima vrednost 255 umanjen za broj hopova između lokala i destinacije. Ukoliko se pinguje Linux OS on ima vrednost 64 umanjen za broj hopova između lokala i destinacije. Ukoliko postoji više hopova od predviđenog moguće je da postoji neko ko vriši sniffing.

Svrha zaplene instrumenta kriminalne aktivnosti je da se spreče buduće kriminalne aktivnosti. Ukoliko se ne može dati argument da je hardver imao "značajnu" ulogu instrumenta u kriminalnoj aktivnosti onda se ne bi trebala vršiti njegova zaplena. Odluku o zapleni hardvera donose sudovi.

Slučajevi iz prakse:

1. U New York-u Severni okružni sud u vezi sa slučajem dečije pornografije, odlučio je da je računar bio instrument izvršenja krivičnog dela. Razlog je taj što je računar imao mogućnost slanja i primanja slika. (United States of America v. Michael LAMB, 1996.).[116]
2. U Virdžiniji Istočni okružni sud odlučio je da je računar bio instrument krivične aktivnosti zato što je posedovao fajl koji je detaljno opisivao uzgajanje biljke marihuane. (United States v. Real Property 783 F.Supp. 253, 1991.).[117]

116 Http://securitylaw.info/pdf/945_F_Supp_441.pdf, 16.12.2015.

117 Http:/ /www. leagle.com/ xmlResult.aspx?xmldoc= 19911036783FSupp253 _11003. xml&docbase= CSLWAR2 - 1986 - 2006, 16.12.2015.

2.1.2. Hardver kao zabranjeni materijal ili plod kriminalne aktivnosti

Nelegalni materijal (zabranjeni materijal) je imovina koju građani ne smeju posedovati u svom vlasništvu. Na primer, nelegalno je imati u svom posedu uređaj koji služi za presretanje elektronskih komunikacija.[118] Razlog je što ovi uređaji mogu da omoguće pojedincima da dođu do poverljivih informacija presretanjem mrežnog saobraćaja, kršeći privatnost drugih građana, čime se otvara mogućnost činjenja širokog spektra drugih kriminalnih aktivnosti. Primer nelegalnog posedovanja materijala bi bio i oprema za kloniranje mobilnih telefona kao plod kriminalne aktivnosti. Prema tome plod kriminalne aktivnosti i njegovo posedovanje predstavljaju vlasništvo, koje je dobijeno kriminalnom aktivnošću (ukraden hardver kao npr. lap top) ili kupljen hardver ukradenom kreditnom karticom.

2.1.3. Hardver kao dokaz kriminalne aktivnosti

Ovo je posebna kategorija kriminalnih aktivnosti hardver kao dokaz, jer ne pripada ni grupi hardvera kao instrumenta kriminalne aktivnosti, ni grupi hardvera kao zabranjenog materijala ili ploda kriminalne aktivnosti. Na primer, ako se skener ili štampač koristi za falsifikovanje dokumenata, novca ili poštanskih marki. Ukoliko se poseduju jedinstvene karakteristike skeniranog ili odštampanog dokumenta (npr. novca, slike, poštanske marke), koje povezuju hardver sa tim dokumentima, taj uređaj (hardver) može da se zapleni kao dokaz.

2.1.4. Informacija kao instrument kriminalne aktivnosti

Informacija može da bude instrument, kojim je izvršena kriminalna aktivnost ili ukoliko je ona dizajnirana sa ciljem da se koristi kao sredstvo za izvršenje kriminalne aktivnosti. Svi programi koji se koriste za izvršenje kriminalnih aktivnosti predstavljaju instrumente kriminalne aktivnosti. Različiti tipovi programa mogu biti iskorišćeni za različite kriminalne aktivnosti kao njihovi instrumenti. Tako da neki programi mogu da omoguće neovlašćeni pristup računarskom sistemu, neki mogu da snimaju korisničke šifre prilikom logovanja na računarski sistem, neki od njih mogu da se koriste za razbijanje zaštita (šifara) itd. Ovi programi poznatiji su po imenu *eksploiti* (eng. exploits) i upotrebljavaju se sa ciljem da se zloupotrebi ranjivost (eng. vulnerability)

118 Primer se odnosi na Sjedinjene Američke države 18 USCS 2512, 16.12.2015.

nekog operativnog sistema (servisa, programa ili programskog koda), zarad sprovođenja neke kriminalne aktivnosti.[119] Samo u slučaju da se prikaže da je informacija imala značajnu ulogu u kriminalnoj aktivnosti može se zapleniti kao instrument kriminalne aktivnosti. U suprotnom se ne konfiskuje.

2.1.5. Informacija kao zabranjeni materijal ili plod kriminalne aktivnosti

Kao što je napomenuto za hardver, zabranjen materijal može da bude i informacija koju građani ne smeju posedovati. Najčešća forma informacije koja nije dozvoljena za posedovanje je program za šifrovanje. U određenim zemljama nije dozvoljeno posedovati program koji omogućava jake algoritme za šifrovanje (odnosno ograničena je dužina ključa koji se koristi za šifrovanje ili tip algoritma). Razlog je taj što bi to kriminalcima omogućilo zaštićenu komunikaciju i omogućilo im veliku privatnost. To za posledicu može sledeći scenario: pronađeni inkriminišući dokazi koji su neophodni za uspešnu tužbu su šifrovani, a ukoliko ne mogu da se dešifruju ti podaci, kao posledica dolazi do odbacivanja tužbe usled nedostataka dokaza. Drugi oblik informacije kao plod kriminalnih aktivnosti su slike dečje pornografije, nelegalne kopije računarskih programa, ukradene poslovne tajne, šifre ili bilo koje druge informacije dobijene iz kriminalnih aktivnosti.

2.1.6. Informacija kao dokaz

Ova kategorija je najbitnija od svih pomenutih. Mnoge naše dnevne aktivnosti ostavljaju digitalne tragove. Svi pružaoci usluga (npr. internet servis provajderi, banke, kreditne institucije) vode i prikupljaju informacije o svojim klijentima. Ovi podaci mogu otkriti veoma važne informacije kao što su: vreme aktivnosti pojedinca i njegovo kretanje (npr. vreme kupovine u marketu, iznajmljivanje automobila, kupovina goriva, elektronska naplata putarine, online bankarstvo, telefonski pozivi, slanje elektronske pošte itd.). Sve te informacije mogu se naći u log fajlovima pomenutih pružaoca usluga. Zapisi o komunikaciji telefonom mogu da se nabave od mobilnih operatera (početak i kraj razgovora,

119 Ranjivost se definiše kao postojanje slabosti usled projektovane ili implementirane greške, koja može dovesti do neočekivanog i/ili neželjenog događaja odnosno do ugrožavanja bezbednosti sistema, Wikipedia, Vulnerability (computing), http://en.wikipedia.org/wiki/Vulnerability_%28computing%29, 21.04.2016.

vreme, broj telefona koji je pozvan ili broj primljenog poziva, jedinstveni identifikatori i jedinstveni idenfitkatori uređaja kao na primer IMEI broj itd). Zapisi o posećenoj web stranici mogu se naći na serveru, kao i podaci o adresama računara koji su pristupali pomenutoj web stranici na serveru. Od internet servis provajdera mogu se dobiti podaci o vremenu i lokaciji sa koje je osumnjičeni pristupao web stranici. Važno je istaći da su ove informacije u slučaju kriminalnih aktivnosti izuzetno dragocene, jer mogu dokazati njihovu vezu sa potencijalnim učiniocem kriminalnih aktivnosti. Na taj način može se dokazati nečija krivica ili nevinost. Sam dokaz može biti optužujući ili oslobađajući.

U Americi u skladu sa aktom Computer Assistance Law Enforcement (CALEA) iz 2000. godine, telekomunikacione kompanije moraju držati detaljne liste poziva svojih klijenata na neodređeno vreme.[120] U Evropskoj uniji su države članice na osnovu direktive iz 2006. godine (Directive 2006/24/EC) bile u obavezi da čuvaju specifične telekomunikacione podatke definisane direktivom, od 6 meseci do 2 godine.[121]

Navedenu direktivu Evropski sud je proglasio nevažećom zato što je nespojiva sa članom 8 Povelje o osnovnim pravima Evropske unije i krši pravo EU.[122] U obrazloženju presude sudije su objasnile, da ova direktiva „predstavlja zadiranje u ogromnoj meri u osnovna ljudska prava na poštovanje privatnog života i zaštitu podataka o ličnosti, kao i da direktivom ovo zadiranje nije svedeno na apsolutno neophodno".[123] [124]

Pored toga sud je ustanovio da podaci o saobraćaju kao takvi omogućavaju „veoma tačne i precizne zaključke" o privatnom životu građana kao npr. o njihovim navikama iz svakodnevnog života, trajnom i privremenom boravištu, dnevnom ili povremenom menjanju mesta,

120 The Department of Justice, http://www.justice.gov/criminal/cybercrime/usamay2001_4.htm, 22.01.2016.

121 Wikipedia, Data Retention Directive, http://en.wikipedia.org/wiki/Directive_2006/24/EC, 17.12.2015.

122 EuGH, U. v. 08.04.2014, C-293/12 u. C-594/12, Rn. 68, DVBl. 2014, 712 = NVwZ 2014, 713. http://curia.europa.eu/juris/liste.jsf?language=de&num=C-293/12#, 01.07.2016.

123 Peter Mühlbauer, EuGH erklärt Vorratsdatenspeicherungsrichtlinie für ungültig, heise.de, http://www.heise.de/tp/artikel/41/41454/1.html, 22.05.2016.

124 Urteil des Gerichtshofs (Große Kammer) 8. April 2014(*) „Elektronische Kommunikation – Richtlinie 2006/24/EG – Öffentlich zugängliche elektronische Kommunikationsdienste oder öffentliche Kommunikationsnetze – Vorratsspeicherung von Daten, die bei der Bereitstellung solcher Dienste erzeugt oder verarbeitet werden – Gültigkeit – Art. 7, 8 und 11 der Charta der Grundrechte der Europäischen Union" In den verbundenen Rechtssachen C-293/12 und C-594/12, http://curia.europa.eu/ juris/document/ document.jsf; jsessionid =9ea7d0f130d50 ea58a0fad7442ea81f4aa 12b928d88b. e34KaxiLc3eQc40 LaxqMbN4OchuOe0? text =&docid=l 50642&pageIndex=0&doclang=DE&mode =lst&dir=&occ= first&part=1&cid= 32184, 22.05.2016, Rz 52, 56, 62, 64 i 65, 21.06.2016.

obavljanju aktivnosti, društvenim odnosima i socijalnom okruženju. Zbog svega toga snimanje podataka na sveobuhvatan i nesrazmeran način može kod građana „proizvesti osećaj neprekidnog praćenja njihovog privatnog života". Sud je dalje utvrdio, da „predviđeni podaci koji se snimaju na osnovu direktive, nisu pogodni i odovarajući, jer se sa snimanjem podataka zadire u suštinu osnovnih ljudskih prava na poštovanje privatnog života i zaštitu podataka o ličnosti".[125] Prema viđenju Evropskog suda „snimanje podataka sa zadržavanjem tj. skladištenjem je naročito zbog toga nesrazmerno, jer ne pravi nikakvu razliku, ograničenje ili izuzetak sa ciljem prevencije od teških krivičnih dela, već se generalno odnosi na sve građane, sva telekomunikaciona sredstva i sve podatke o saobraćaju". Osim toga je i pristup prikupljenim podacima na ovaj način neograničen i ne postoji kontrola od sudova ili nezavisnih upravnih organa. Sudije su u presudi takođe istakle, da u direktivi nedostaje i jasno regulisanje uništavanja podataka, nakon isteka roka čuvanja podataka. Na taj način je povećana mogućnost zloupotrebe podataka.[126]

U kojoj meri uopšte je ovakav način snimanja podataka bio efikasan u praksi i mogao da doprinese ostvarenju njegovog cilja (borbi protiv teških krivičnih dela) govori i podatak veštačenja od strane nemačkog Bundestaga. Zadržavanje i snimanje podataka je doprinelo razjašnjenju krivičnih dela u 0,006% slučajeva.[127]

2010. godine od strane Interpola je prosleđena direktiva, kako svim Internet servis provajderima (ISP) u Evropi, tako i svim ISP zemaljama koje žele da budu članice Evropske unije, da se sve IP komunikacije loguju na takav način da se javne IP adrese uspostavljenih TCP state sesija loguju u jedinstvenu bazu podataka. To znači da, kada korisnik prilikom dobijanja javne IP adrese od strane ISP otvori neki veb sajt uspostavlja TCP state sesiju. Nakon kreiranja sesije omogućena je razmena podatka između na primer sajta yahoo.com i računarskog sistema korisnika. Ti podaci koji se razmenjuju između korisnika i servera kome on pristupa ISP ne loguje, već samo loguje uspostavljenu TCP state sesiju. U bazi se dakle nalaze zapisi o svim uspostavljenim TCP sesijama sa pripadajućim IP

125 Urteil in den verbundenen Rechtssachen C-293/12 und C-594/12 Digital Rights Ireland und Seitlinger, Gerichtshof der Europäischen Union Pressemitteilung Nr. 54/14, Luxemburg, den 8. April 2014, http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054de.pdf, 22.05.2016.

126 *Ibidem.*

127 Roland Derksen, Zur Vereinbarkeit der Richtlinie über die Vorratsspeicherung von Daten mit der Europäische Grundrechtecharta, Die Wissenschaftlichen Dienste des deutschen Bundestags, http://www. vorratsdatenspeicherung.de/ images/rechtsgutachten_grundrechtecharta.pdf, 22.05.2016.

adresama. Internet servis provajderi su u obavezi da čuvaju minimum 6 meseci te logove o TCP sesijama prema direktivi Interpola. Na taj način forenzički istraživači lakše mogu pronaći na primer koji je komandno kontrolni centar određene bot net mreže. Da bi se to otkrilo moraju se rekonstruisati sve TCP state sesije i pronaći koja je stvarna IP adresa komandno kontrolnog centra da bi zlonamerni napadač koji rukovodi botnet mrežom bio uhvaćen.

U Srbiji je 2010. godine usvojen Zakon o elektronskim komunikacijama, prema kojem pružaoc komunikacionih usluga (operator) mora da čuva podatke o elektronskim komunikacijama 12 meseci.[128] Ova vrsta nadzora ima svoje dve strane, dobre i loše. Dobra strana je što te informacije mogu da pruže dokaze u vezi sa kriminalnim aktivnostima, a loša je što iste mogu da se zloupotrebe i što se time ugrožava privatnost građana (kao što je ustanovio Evropski sud). U velikom broju zemalja se i dalje vode velike polemike vezane za ovu vrstu čuvanja informacija po pitanju vremena i vrste podataka zbog ugrožavanja privatnosti (u ovom slučaju pravo na privatni život i privatnu komunikaciju), koja je zagarantovana ustavom, zakonima i članom 12. Univerzalne deklaracije o ljudskim pravima. U svakom slučaju potrebno je postići balans između dovoljne sigurnosti sa jedne strane i privatnosti sa druge strane.

2.2. DIGITALNA FORENZIČKA ISTRAGA

Digitalna forenzička istraga podrazumeva prikupljanje činjenica i njihovu proveru. Zatim se formira hipoteza i vrše testiranja kroz traženje dokaza, koji mogu da je potvrde ili opovrgnu. To može da utiče na menjanje zaključaka, ukoliko se pronađu novi dokazi (što bi izazvalo i novi ciklus obrade dokaza).[129] *Centralno mesto u digitalnoj istrazi* predstavlja neki *digitalni uređaj* koji predstavlja predmet ili sredstvo nezakonitog postupanja. Digitalni uređaj može biti zloupotrebljen sa ciljem osumnjičenog da putem interneta izvrši određene pripremne radnje izvršenja krivičnog dela ili neke druge digitalne aktivnosti u virtuelnom okruženju, koje su u suprotnosti sa pozitivnim propisima (važeći propisi određene nacionalne države) ili opštim aktima pravnog lica (npr. neovlašćen pristup računaru, posedovanje i distribucija nedozvoljenog materijala, različiti tipovi zloupotrebe mailova kao što su ucene, pretnje itd.). Identifikacijom

128 Zakon o elektronskim komunikacijama ("Sl. glasnik RS", br. 44/2010, 60/2013 - odluka US i 62/2014), http://www.paragraf.rs/propisi/zakon_o_elektronskim_komunikacijama.html, 17.12.2015.

129 Vanja Korać, Dragan Prlja, i Gordana Gasmi, *High Tecnology Criminal and Digital Forensics*, in: Preventing and Combating Cybercrime, Cluj-Napoca, Accent, 2016, str. 87.

izvršenja nedozvoljene aktivnosti od strane nadležnih organa, isti iniciraju istragu u pretkrivičnom postupku. Digitalna forenzička istraga se generalno može podeliti u dve različite kategorije: *zvanična istraga i korporativna istraga*.

Kada je reč o zvaničnoj istrazi ona obuhvata istragu o sredstvima odnosno alatima sa kojima je učinjena nedozvoljena aktivnost. Utvrđuje se motiv nedozvoljene aktivnosti i definiše se tip nedozvoljene aktivnosti i procesuira se. Zvanične istrage vode zvanični istražni organi, koji čine tim sa tačno označenim rukovodiocem istrage i zahtevaju sudske naloge. Zvaničnu istragu reguliše *Zakonikom o krivičnom postupku* u članu 2., kojim se definišu osnovni pojmovi kao što je osumnjičeni, okrivljeni, optuženi. [130]

"Osumnjičeni" je lice prema kome je zbog postojanja osnova sumnje da je učinilo krivično delo i prema kome je nadležni državni organ u predistražnom postupku preduzeo radnju propisanu ovim zakonikom i lice protiv koga se vodi istraga.

"Okrivljeni" je lice protiv koga je podignuta optužnica koja još nije potvrđena, ili protiv koga je podnet optužni predlog, privatna tužba ili predlog za izricanje mere bezbednosti obaveznog psihijatrijskog lečenja, a glavni pretres ili ročište za izricanje krivične sankcije još nije određeno, odnosno izraz koji služi kao opšti naziv za osumnjičenog, okrivljenog, optuženog i osuđenog.

"Optuženi" je lice protiv koga je optužnica potvrđena i lice za koje je povodom optužnog predloga, privatne tužbe ili predloga za izricanje mere bezbednosti obaveznog psihijatrijskog lečenja određen glavni pretres ili ročište za izricanje krivične sankcije u skraćenom krivičnom postupku.

Krivično gonjenje je definisano članom 5. Zakonika o krivičnom postupku, a krivično gonjenje se smatra započetim:

1) prvom radnjom javnog tužioca ili ovlašćenih službenih lica policije na osnovu zahteva javnog tužioca, preduzetom u skladu sa ovim zakonikom radi provere osnova sumnje da je učinjeno krivično delo ili da je određeno lice učinilo krivično delo.

Članom 7. Zakonik o krivičnom postupku definisan je *način pokretanja krivičnog postupka*, a krivični postupak se smatra pokrenutim:

(1) donošenjem naredbe o sprovođenju istrage (član 296.);

(2) potvrđivanjem optužnice kojoj nije prethodila istraga (član 341. stav 1.);

130 *Zakonik o krivičnom postupku RS*, Sl. glasnik RS, br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 i 55/2014.

(3) donošenjem rešenja o određivanju pritvora pre podnošenja optužnog predloga u skraćenom postupku (član 498. stav 2.);

(4) određivanjem glavnog pretresa ili ročišta za izricanje krivične sankcije u skraćenom postupku (član 504. stav 1, član 514. stav 1. i član 515. stav 1.);

(5) određivanjem glavnog pretresa u postupku za izricanje mere bezbednosti obaveznog psihijatrijskog lečenja (član 523.).

Zakon stavlja u nadležnost javnom tužiocu da goni počinioca krivičnih dela pa je to regulisano članom 43. Osnovno pravo i osnovna dužnost javnog tužioca je gonjenje učinilaca krivičnih dela.

Za *krivična dela* koja se gone *po službenoj dužnosti,* javni tužilac je nadležan da:

(1) rukovodi predistražnim postupkom;

(2) odlučuje o nepreduzimanju ili odlaganju krivičnog gonjenja;

(3) sprovodi istragu;

(4) zaključi sporazum o priznanju krivičnog dela i sporazum o svedočenju;

(5) podiže i zastupa optužbu pred nadležnim sudom;

(6) odustane od optužbe.

(7) izjavljuje žalbe protiv nepravnosnažnih sudskih odluka i da podnosi vanredne pravne lekove protiv pravosnažnih sudskih odluka;

8) preduzima druge radnje kada je to određeno ovim zakonikom.

Kod korporativne forenzičke istrage odgovor na incident izvodi jedna osoba i ove istrage uglavnom spadaju u istrage niskog nivoa. Ove istrage ne spadaju u nedozvoljene aktivnosti već u *incidentne radnje*. Mogu se smatrati i kao predistražni postupak zvanične istrage visokotehnološkog kriminala. Istraga u organizaciji se sprovodi u kontrolisanom okruženju. U praksi se realizuje kroz pokretanje istrage, utvrđivanje karaktera računarskog incidenta i analiziranje prikupljenih podataka. Prikupljanje i prosleđivanje digitalnih dokaza zvaničnim organima istrage odnosno organima u organizaciji vrši se jedino po odobrenju vlasnika kompromitovanog sistema i nakon odluke organizacije. Zvanična i korporativna istraga slede ista forenzička pravila.

Pre istrage nedozvoljene aktivnosti neophodne su određene pripreme. Potrebno je definisati politike i procedure u okviru organizacije, odrediti istražni tim, definisati procedure za forenzički inicijalni odgovor za očuvanje integriteta digitalnog dokaza, spremiti određene alate, i poznavati zakone matične zemlje koji se odnosi na visokotehnološki kriminal. Na primer kada zlonamerni napadač iskoristi fasfifikovanu karticu da podigne novac sa bankomata to spada u krivično delo računarskog kriminala - neovlašćeni upad u računarski sistem. Zato je

izuzetno važno poznavanje krivičnog zakonodavstva u delu koji se odnosi na računarski kriminal kako bi se ispravno identifikovale nedozvoljene aktivnosti.

Bitno je istaći da nije svaka incidentna aktivnost i zakonom zabranjena aktivnost. Postoje različiti pojavni oblici incidentnih radnji, a neke od njih predstavljaju i aktivnosti zabranjene pravnim propisima, što za sobom povlači i zvaničnu istragu. Na osnovu pojavnih *oblika incidentnih radnji* moguće je izvršiti njihovu klasifikaciju prema stepenu značajnosti (ozbiljnosti) na sledeći način: nizak nivo, srednji nivo i visoki nivo značajnosti. Način klasifikacije je izložen u EC-Council i Cengage learning literaturi za serfifikaciju za računarskog forenzičara (eng. *Computer hacking forensics investigator certification CHFI*).[131] Detaljnija klasifikacija sa više kategorija definisana je u *Federal Incident Reporting Guidelines* od strane US-Cert-a.[132] Kod nas se klasifikacija težine krivičnih dela definiše opisom bića krivičnog dela u Krivičnom zakoniku Srbije.

FBI za kvalitativnu procenu rizika i zaštitu federalnog informacionog sistema, predlaže i koristi bezbednosnu kategorizaciju: *nizak-N, srednji-S, visok-V*.

Ako neka informacija ima sledeću procenu rizika: poverljivost - *N*, integritet - *S* i raspoloživost - *V*, onda ovu informaciju svrstavamo u *kategoriju visoko rizičnih*, što znači da će i preduzete mere zaštite biti najveće. Ovaj metod je prihvatljiv, jer istovremeno anulira veliki broj neodređenosti koje kvalitativna procena rizika uključuje.

Kada je reč o nedozvoljenim *aktivnostima visokog nivoa značajnosti*, njih treba rešavati odmah nakon njihovog nastanka. Zahtevaju odgovor u roku od 15 minuta, a rešavanje do 2 sata. U ovu kategoriju spadaju DoS napadi, upad u računarski sistem ili mrežu, računarski virus ili crvi velikog inteziteta, trojanski konji ili zadnja vrata (eng. backdoor), neovlašćenja izmena hardverskih komponenti na računaru, neovlašćeno instaliranje firmware-a na računarskom sistemu ili neovlašćeno instaliranje programa na serveru.

Incidenti niskog nivoa značajnosti nose najmanje opasnosti, ali se moraju rešavati u toku radnog dana nakon njegove detekcije. Zahtevaju odgovor u roku od 90 minuta a rešavanje može biti i do 6 sati. Na primer u ovu kategoriju može spadati gubitak lične šifre, neuspešna skeniranja i pokušaji skeniranja mreže i personalnih računara i servera, prisustvo računarskog virusa ili crva i pozajmljivanje računarskih naloga u okviru organizacije. Neovlašćeno skeniranje mreže za proveru prisutnosti IP adresa

131 Grubor G., Funkcionalni model istrage kompjuterskog događaja, Udruženje IT Veštak, 2004.
132 Http://www.us-cert.gov/government-users/reporting-requirements.html, 21.04.2016.

smatra se zlonamernim činom. Prikupljeni paketi koji ukazuju na aktivnost skeniranja mreže može biti upotrebljen kao digitalni dokaz neovlašćenog skeniranja mreže.

Incidenti srednjeg nivoa značajnosti su znatno ozbiljniji i uglavnom su inkriminisani propisanim odredbama zakona određene države na osnovu visine pričinjene štete. Zahtevaju odgovor u roku od 30 minuta, a rešavanje do 4 sata.

Kod nas *težina krivičnog dela* definisana je u Krivičnom zakoniku. Incidenti visokog nivoa značajnosti su najozbiljniji incidenti i takođe su inkriminisani propisanim odredbama zakona određene države na osnovu visine pričinjene štete. Kod nas za svako krivično delo, definisana je težina dela na osnovu štete koja je pričinjena, a takvih krivičnih dela ima dvadesetak. Neki od primera bi bili neovlašćeno skladištenje i obrada podataka, ilegalan pristup kancelarijama, uništavanje imovine pričinjena računarskim incidentom, krađa ličnih podataka, širenje računarskog virusa ili crva većeg inteziteta, neovlašćeno dobijanje privilegovanog pristupa računaru ili serveru.

Period odgovora, prema navedenim kategorijama, na incidentnu radnju odnosno nedozvoljenu aktivnost i njihovo rešavanje varira u zavisnosti od velikog broja faktora kao na primer specifičnosti delatnosti organizacije, osetljivosti samih podataka, mogućnosti ponavljanja napada i mnogih drugih faktora.[133] Praksa je pokazala da se sve češće javlja potreba primena forenzičke istrage u korporativnom okruženju u vezi sa računarskim incidentima. Ove interne istrage u organizaciji imaju za cilj utvrđivanje tipa incidentne radnje kao i trajno eliminisanje uzroka incidenta.

U današnje vreme većina kompanija za svoj marketing i promociju koristi internet, čime njihova izloženost postaje sve veća, a samim tim raste mogućnost potencijalnih napada i špijunaže (kao jedan od pojavnih oblika visokotehnološkog kriminala). Ukoliko dođe do određene incidentne situacije u okviru kompanije (koja nije bila pretnja po bezbednost države), takve istrage pre svega vode timovi koje angažuje kompanija. U tom slučaju pokreće se *kompanijska istraga* koja nema represivan karakter prema pojedincu-izvršiocu (u smislu njegovog lišavanje slobode), već može pribaviti dokaze za eventualno dalje postupanje nadležnih državnih organa. Istraga unutar kompanije može dovesti do pokretanja disciplinskog postupka u slučaju da se dokaže postojanje nedozvoljenog postupanja od strane zaposlenog. Kada se steknu uslovi za sprovođenje zvanične istrage po dobijanju odobrenja, istraga počinje da se sprovodi fazno, ulaskom u trag izvršiocu ili osumnjičenom,

133 US-CERT, Federal Incident Reporting Guidelines, http://www.us-cert.gov/government-users/reporting-requirements.html , 21.04.2016.

otkrivanjem njegovog identiteta, i po potrebi lišavanjem slobode, kako bi se onemogućilo uništavanje dokaza ili ponavljanje istog dela odnosno uticaja na potencijalne svedoke.

Treba napomenuti da su principi i standardne operativne procedure digitalne forenzičke istrage gotovo iste kako u zvaničnoj tako i u korporativnoj istrazi. Forenzički istražitelji istragu moraju voditi na takav način „kao da će slučaj koji se istražuje završiti na sudu". To znači da je moguće da u nekoj od istražnih faza, za koju se utvrdi da forenzički istražitelji u organizaciji nemaju nadležnost, istragu preuzmu zvanični organi. Sam intenzitet istrage može varirati, ali pristup izvorima dokaza kao i procedure očuvanja dokaza u lancu istrage, moraju biti isti u zvaničnoj i korporacijskoj istrazi.134 Dakle važe ista pravila, izvršiti identifikovanje digitalnih dokaza, prikupiti što veći broj digitalnih dokaza, izvršiti kvalitetno skladištenje i čuvanje digitalnih dokaza, i kreirati digitalnu kopiju jer se pri digitalnoj istrazi uglavnom ne radi istraga na računaru gde se desila nedozvoljena aktivnost, već se radi forenzička kopija digitalnog dokaza identična onoj koja se nalazi na računaru gde se nedozvoljena aktivnost desila. Rad na forenzičkoj kopiji treba da pruži odgovor na pitanja odakle je napad došao (gde je mesto nedozvoljene aktivnosti), ko je izvršio napad, kada se desila zlonamerna aktivnost i šta je prouzrokovano od štete. Sve te podatke je potrebno dokumentovati. Bez dokumentacije sav proces računarske forenzike nije verodostojan. Prema tome mora postojati i dokaz na koji je način digitalna forenzika računarskih sistema izvedena tj. na koji je način prikupljen digitalni dokaz, da li je integritet digitalnog dokaza narušen u proceduri prikupljanja i mora se potvrditi integritet digitalnog dokaza, a to se radi upotrebom heširanja. Uz pomoć heširanja radi se analiza strukture sadržaja digitalnog dokaza, a dobija se kao izlaz heš vrednost određenog broj karaktera u zavisnosti od korišćenog algoritma za heširanje.

Krajnja tačka interne istrage u okviru organizacije jeste priprema forenzičkog izveštaja od strane digitanog forenzičara koji zaključuje istragu, omogućujući pravnom sektoru u okviru organizacije da donese jasnu odluku da li će se na osnovu predočenih dokaza interna istraga proširiti u zvaničnu. Na primer, preuzet je računarski sistem jednog od zaposlenog u okviru organizacije na kome se desio bezbednosni incident u formi kompromitovanja email naloga i u toku analize su se pronašle slike dečije pornografije. Ukoliko postoje određene indikacije o dodatnom računarskom kriminalu to se mora evidentirati i u tom slučaju se otvara još jedan slučaj (po odobrenju nadležnih,

134 Grubor G., Gotić A., *Korporativna aktivna digitalna forenzička istraga primenom Backtrack – a*, 10. Međunarodni naučni skup Sinergija 2012. Univerzitet Sinergija, 2012.

to ne radi forenzički istražitelj on procesira, on ne odlučuje).

Potreba za specijalizacijom personala i procesa u digitalno forenzičkoj oblasti je postala nužnost zbog munjevitog razvoja tehnologije i sajber kriminala. Prikupljanje digitalnih dokaza vrše tehničari digitalnog mesta zločina, ljudi koji pregledaju dokaze i istraživači koji analiziraju sve raspoložive dokaze kako bi se izgradio slučaj. Ove specijalizacije ne odnose se samo na policiju već su uspostavljaju i na korporativnom nivou. U slučaju da je jedna osoba angažovana i odgovorna za prikupljanje, procesiranje i analiziranje digitalnih dokaza, bitno je da se ovi postupci izvode posebno. Svaka od oblasti specijalizacije podrazumeva određene veštine kao i primenu različitih procedura.

Radna grupa za digitalne dokaze (SWGDE)[135] 2002. godine je objavila vodiče za trening "Najbolje prakse računarske forenzike".[136] Američko udruženje direktora laboratorije za zločine - ASCLD (eng. American Society of Crime Laboratory Directors) je predložilo zahteve za ljude koji pregledaju digitalne dokaze u forenzičkim laboratorijama (ASCLD 2003). Tako je 2005. godine objavljen međunarodni standard kvaliteta *ISO 17025:2005 standard* (Opšti zahtevi za kompetentnost laboratorija za ispitivanje i eteloniranje laboratorija - General requirements for the competence of testing and calibration laboratories), u kome se spominje pregled digitalnih dokaza u kontekstu akreditovane discipline pod internacionalnim standardom (ISO 17025; ENFSI 2003). U ovom standardu opisano je šta treba jedna forenzička laboratorija da pripremi za akreditaciju da bi dokazala kvalitet svog servisa koji nudi.

U Evropi postoji računarska forenzička laboratorija OLAF (European Anti-Fraud Office) koja je osnovana je 1999. godine u kojoj radi 3500 zaposlenih istražitelja. [137] U slučaju pravljenja računarske forenzičke laboratorije njime je potrebno obratiti se da bi se dobila preporuka za akreditovanje forenzičke laboratorije.

Kada je reč o aplikativnom delu forenzike u oblasti informatičke tehnologije pouzdan standard jeste OWASP top 10 standard u sferi bezbednosti veb i desktop aplikacija.[138] Omogućuje forenzičarima adekvatno smeštanje identifikovanog napada u određene kategorije. Nakon identifikacije radi se evaluacija rizika tog napada na osnovu OWASP risk rating metodologije uz

135 Scientific Working Group for Digital Evidence, *Best practices for Computer Forensics*.

136 Frank Adelstein, *Live forensics: Diagnosing your system without killing it first*, Communications of the ACM, 49(2), 2006, str. 63–66.

137 Http://ec.europa.eu/anti_fraud/index_en.htm, 20.07.2016.

138 Https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project, 20.07.2016.

pomoć identifikacije određenih faktora koji se odnosi na konkretni napad na veb ili mobilne aplikacije. Krajnji cilj je dobijanje težinskog faktora zlonamernog napada (low, medium, high) na osnovu više faktora (veštine, motiva, obim štete i dr.).

Razvoj tehničkih standarda iz ove oblasti je izazvao potrebu utvrđivanja standarda u samoj praksi namenjenih pojedincima. To obuhvata *sertifikaciju personala*, koji pregladaju digitalne dokaze imaju sve potrebne veštine da obavljaju svoj posao kompetentno i da prate ispravne procedure. Razvijani su treninzi i programi sertifikacije prema pomenutim standardima. Postoji više nivoa sertifikacija:[139]

1. Ispit opšteg znanja (koji svi moraju da prođu, uključujući i osoblje koje prvo odgovara na incident, a koje rukuje digitalnim dokazima);
2. Viši sertifikati za pojedince koji se bave mnogo kompleksnijim slučajevima u laboratorijskim uslovima.

U slučajevima bezbednosnih incidenata, pravilno prikupljanje relevantnih podataka može značajno povećati verovatnoću dolaska do informacija o tome ko je izvršilac napada, odakle je napad izvršen, na koji način je napad izvršen. Potrebno je istaći i značaj *informacije o cilju napada* ali i utvrditi eventualno *postojanje uzročno-posledične veze* (direktne ili indirektne) sa ostalim kumulativno počinjenim krivičnim delima kao što su na primer trgovina narkoticima, ljudima, oružjem, nedozvoljeno sticanje imovinske koristi putem prevare, iznude, zloupotrebe službenog položaja i dr.

Digitalna forenzička istraga podrazumeva *upotrebu različitih forenzičkih alata i tehnika*, odnosno njihovu primenu u toku trajanja istrage. Primenjuje se u različitim slučajevima npr: kada treba da se postavi hipoteza o nedozvoljenoj radnji, zatim prilikom eliminisanja očiglednosti (npr. delo je nesumnjivo izvršeno sa određenog računara, ali to ne znači da je delo izvršio vlasnik tog računara, već je moglo biti reči o upadu trećeg lica na taj računar). Osim toga nalazi primenu pri rekonstrukciji nedozvoljene radnje ili otkrivanju tragova osumnjičenog na računaru.

Ukoliko se desi nedozvoljena aktivnost ili računarski incident na opremi koja nije u ličnom vlasništvu ili vlasništvu organizacije (outsource infrastruktura) kao na primer iznajmljena cloud infrastruktura, postoje politike i procedure koji razrešavaju takav specifičan tip problema. Te politike i procedure se definišu pre potpisivanja ugovora sa provajderom cloud usluga

139 Allen B., *Collecting Digital Evidence from Intrusion Detection System*, CGS 5132 - Computer Forensics II, 2002, http://www.authorstream.com/ Presentation/ Kliment-24060-allen-Collecting-Digital-Evidence-Intrusion-Detection-Systems-designed-forensic-use-as-Entertainment-ppt-powerpoint/, 23.06.2016.

(definisanje zona odgovornosti). Postoje dva nivoa odgovornosti prvi nivo je odgovornost cloud provajdera drugi nivo je korisnički nivo odgovornosti. Za forenzičku istragu je vrlo važno definisati gde je ta odgovornost kada je u pitanju nastala nedozvoljena aktivnost. Na primer, cloud sistemi mogu da rentiraju svoj storidž (prostor na disku) i procesorsku snagu, a operativni sistem sa programima je ono što korisnik tj. organizacija poseduje. Zona odgovornosti se može u tom slučaju podeliti zonu iznad (odgovornost korisnika tj. organizacije) i zonu ispod hardvera (odgovornost cloud provajdera).

U literaturi se *modeli*, koje možemo pronaći uglavnom razlikuju na osnovu ugla posmatranja krivičnog dela, a od toga zavisi i njihova primenjivost. Postoje *modeli istrage fizičkog mesta krivičnog dela*, *modeli istrage digitalnog mesta krivičnog dela* (koji se zasnivaju na postojećoj teoriji fizičke istrage) i *integrisani modeli gde je računar sam po sebi digitalno mesto krivičnog dela*. Istraga fizičkog mesta krivičnog dela koristi zakone prirode da bi našla fizičke dokaze, a istraga digitalnog mesta krivičnog dela se koristi da bi se pronašli digitalni dokazi.[140]

Kada je u pitanju *istraga fizičkog mesta krivičnog dela* dominantna već spomenuta teorija Lokardov zakon razmene.[141] Kada dva objekta dođu u interakciju (kontakt) doći će do razmene materije između njih. Na primer dlake sa izvršioca krivičnog dela vrlo često se zadrže na fizičkoj mestu izvršenja krivičnog dela.

Kada je u pitanju *digitalno mesto krivičnog dela* mogu postojati privremeni fajlovi, sadržaj RAM memorije, koji su snimljeni ili izbrisani na disku. Ovi delovi zbog uticaja programa odnosno operativnog sistema koji je osumnjičeni koristio ili izvršavao, mogu biti promenjeni ili iskorišteni. Prema tome podatak koji uđe u digitalno mesto ostavlja tragove digitalnog dokaza iza sebe na različitim mestima: memoriji, hard disku, prenosivoj memoriji.

Što se tiče ključnih reči u literaturi ima mnogo različitih mišljenja kada je reč o najvažnijim forenzičkim pojmovima kada su u pitanju digitalno forenzički procesi. Najvažniji *forenzički pojmovi za proces istrage* su:

-*fizički dokazi* - predstavljaju fizičke objekte na osnovu kojih se može utvrditi izvršenje krivičnog dela. Mogu da dokažu vezu između počinioca krivičnog dela i žrtve ili mogu da dokažu vezu između izvršioca zločina sa samim zločinom. Primeri fizičkih dokaza su: računar, DVD, hard disk, mobilni telefon;

140 Council of Europe, Recommendation No. R (95) 13, http://www.justice.gov/ criminal/ cybercrime/ crycoe.htm, 22.06.2016.

141 Bem D., Huebner E., *Computer Forensic Analysis in a Virtual Environment*, International Journal of Digital Evidence Fall 2007, Volume 6, Issue 2, 2007.

-*digitalni dokaz* - predstavlja digitalni podatak koji može potvrditi računarski kriminal i koji može da dokaže vezu između počinioca krivičnog dela sa samim krivičnim delom. Primeri digitalnih dokaza su: podaci na hard disku (na primer log fajl), podaci u memoriji mobilnog telefona;

-*fizičko mesto krivičnog dela* - predstavlja fizičko okruženje u kome se nalaze fizički dokazi zločina. Okruženje gde se dogodila prva nedozvoljena aktivnost naziva se primarno fizičko mesto krivičnog dela, a sva ostala fizička mesta nazivaju se sekundarnim fizičkim mestima krivičnih dela;[142]

-*digitalno mesto krivičnog dela* - predstavlja digitalno (virtuelno) okruženje, koje čine sistemski programi, programi i hardver u kome se nalaze digitalni dokazi nedozvoljene aktivnosti. Okruženje gde se dogodila prva nedozvoljena aktivnost naziva se primarno digitalno mesto krivičnog dela, a sva sledeća digitalna mesta nazivaju se sekundarna digitalna mesta krivičnih dela.

Kada se sumiraju informacije koje iznete u okviru ovog poglavlja mogu se izdvojiti najvažniji elementi koji su neophodni da se obezbede kako bi istraga bila uspešna:

- utvrđivanje da li se radi o nedozvoljenoj aktivnosti ili ne (računarski incident);

- pribavljanje naloga za ulazak na računarski sistem kada je reč o zvaničnoj istrazi, a ukoliko je reč o internoj istrazi u okviru organizacije nije potreban nalog ukoliko postoji procedura koju je zaposleni potpisao, a koja daje ovlašćenje odgovornom licima iz organizacije koji rade forenzičku istragu da mogu da sprovedu istragu na korisničkom računaru;

- uraditi forenzički odgovor na nedozvoljenu aktivnost i izvršiti prikupljanje digitalnih dokaza na forenzički ispravan način;

- transport digitalnih dokaza je takođe izuzetno važan deo forenzičke istrage jer može da utiče na integritet prikupljenih dokaza. Postoje Antistatic torbice za hard diskove usb stick, futrole sa bakarnom folijom za wireless uređaje (onemogućavanje wireless signala) prilikom transporta do forenzičke laboratorije. Treba reći da su SSD diskovi naročito osetljivi na elektromagnetna zračenja i da podaci mogu biti uništeni ukoliko se ne ispoštuje procedura bezbednog transporta.

142 Carvey H., Altheide C., *Tracking USB storage: Analysis of Windows artifacts generated by USB storage devices*, Digital Investigation 2, pp. 94-100, Elsevier Academic Press, Burlington, MA 2005, http://www.sciencedirect.com/science/article/pii/S1742287605000320/pdfft?md5=b4d986c553c49a983e66ae2b68a0c4a6&pid=1-s2.0-S1742287605000320-main.pdf, 22.06.2016.

2.2.1. Istražne metodologije - modeli

Brzim tehnološkom razvojem i razvojem programa, kriminalne radnje postaju sve sofisticiaranije kada je u pitanju način izvršenja. Primena zakona je u stalnoj trci sa kriminalcima kada je reč o visokotehnološkom kriminalu. Jedan deo trke se odnosi na razvoj alata za prikupljanje i pretragu digitalnih dokaza u odnosu na one kojima se vrši prikrivanje kriminalnih radnji, a drugi deo trke se odnosi na razvoj metodologije u digitalnoj forenzici. *Metodologijom* se obuhvataju forenzičke analize svih tipova digitalnih istraga kriminalnih radnji. Primenjuje se na sve aktuelne digitalne zločine kao i na zločine u budućnosti.[143]

Svrha definisanja modela digitalne istrage je da informiše, oblikuje i standardizuje proces digitalne istrage.[144] Neki od modela prilaze digitalnoj istrazi sa naučno-tehničkog aspekta, a neki sa ne tehničkog aspekta. Neki od modela su detaljniji u odnosu na druge po pitanju korespodencije fizičke i digitalne istrage, a opet kada je reč o istražnom procesu neki modeli imaju veći okvir u metodološkom smislu. Cilj prikaza istražnih metoda, predstavlja presek trenutnog stanja istražnih metoda. Ovo je od pomoći istražiteljima jer na osnovu preseka stanja, mogu u skladu sa specifičnostima istrage, primeniti odgovarajući model.

Različite *istražne metodologije* mogu biti primenjene na digitalnu forenzičku analizu u zvaničnom tipu istrage i u korporacijiskom tipu istrage. Zajedničko za sve modele jesu četiri osnovne istražne faze: *identifikacija/ rukovanje* (skupljanje, prenos, integritet u lancu istrage), *forenzička akvizicija* (otkrivanje, fiksiranje i izvlačenje), *forenzička analiza* (analiza DP i izgradnja čvrstog DD) *i prezentacija* (stručno svedočenje/veštačenje na sudu).

2.2.1.1. The DFRWS model

DFRWS model je razvijen između 2001. i 2003. godine[145] u digitalnoj forenzičkoj istraživačkoj radionici (eng. Digital Forensics Research Workshop) od strane grupe istraživača i stručnjaka iz digitalno forenzičkih

143 Carvey H., *Windows Forensics and Incident Recovery*, Addison Wesley, 2004.
144 Daniel A. Ray, Phillip G. Bradford, *Models of Models: Digital Forensics and Domain-Specific Languages*, http://www.ioc.ornl.gov/csiirw/07/abstracts/Bradford-Abstract.pdf, 18.12.2015.
145 Http://www.dfrws.org/2001/dfrws-rm-final.pdf, 18.12.2015.

oblasti.[146] Ovim modelom su obuhvaćene digitalno istražne radnje definisane klasama. Klase služe za kategorizaciju istražnih radnji po grupama. Ovim modelom su predviđene liste radnji koje se mogu izvršavati, a neke od njih su obavezne. Specifičnost ovog okvira je ta što za svaku pojedinačnu istragu u velikoj meri model mora biti redefinisan. Okvir je predstavljen tabelom čije kolone predstavljaju klase radnji koje treba preduzeti u digitalnoj istrazi, a svaki red sadrži elemente te klase. Prema ovom modelu postoji ukupno sedam faza u procesu istrage digitalnih dokaza: identifikacija, čuvanje, sakupljanje, pretraživanje, analiza, prezentacija i odluka.

Definisane klase ovih radnji i njenih elementa predstavljeni su u tabeli br. 3.[147]

Tabela br. 3. DFRWS model digitalne istrage

1	2	3	4	5	6	7
Identifikacija	Zaštita (čuvanje)	Prikupljanje	Ispitivanje	Analiza	Izvođenje (prezentacija)	Odluka
Događaj/ otkrivanje zločina	Menadžment slučaja	Čuvanje	Čuvanje	Čuvanje	Dokumentacija	
Razjašnjenje potpisa	Tehnologija predstavljanja	Odobreni metodi	Sledljivost	Sledljivost	Veštačenje	
Otkrivanje profila	Sistem kontrole	Odobreni softver	Tehnike potvrđivanja	Statistika	Objašnjenje	
Otkivanje nepravilnosti	Vermenska sinhronizacija	Odobreni hardver	Tehnike filtriranje	Protokoli	Model uticaja	
Žalbe		Sudska nadležnost	Uklapanje modela	Pretraga podataka	Preporučene kontramere	
Kontrola sistema		Bez gubitka kompresije (podataka)	Skriveno otkrivanje podataka	Vermenska lista (hronika)	Statistička interpretacija	
Analiza interne revizije		Uzimanje uzoraka	Skriveno izvlačenje podataka	Veza		
		Smanjenje podataka		Prostor		
		Tehnike povratka (podataka)				

146 Carvey H., *Windows Forensic Analysis DVD Toolkit 2E*, Elsevier, Inc. 2009.

147 Eng.
Electronic Crime Scene Investigation Guide, http://www.dfrws.org/2001/dfrws-rm-final.pdf, strana 17, 18.12.2015.

2.2.1.2. America's department of justice - DOJ model

DOJ model je predložilo američko pravosuđe 2001. godine u "Vodiču za istragu digitalnog mesta krivičnog dela" i veoma je sličan Kruse i Heiser modelu, koji je *nezavistan od tehnologije*.[148] [149] Razlika je u tome što je istaktnuta posebna faza - *izveštaj*. Ovaj model orijentisan je više ka fizičkom mestu krivičnog dela, a manje ka forenzičkoj analizi i ispitivanju digitalnog sistema.

Model se sastoji od sledećih faza:

- *priprema* – u ovoj fazi vrši se pripremanje opreme i alata koji će biti neophodni u istrazi;
- *prikupljanje dokaza* – ovoj fazi vrši se pretraga i prikupljanje elektronskih dokaza koje se realizuje kroz sledeće podaktivnosti: 1. *obezbeđenje mesta krivičnog dela*, radi bezbednosti lica i integriteta podataka, kao i identifikacije potencijalnih dokaza. Treba napomenuti da profesionalana radoznalost ljudi koji nisu deo istražnog tima (policajci i drugi profesionalci), može ugroziti dokazni materijal. 2. *dokumentacija mesta krivičnog dela*, koja podrazumeva dokumentovanje fizičkog opisa mesta krivičnog dela (npr. fotografisanje računara). 3. *sakupljanje dokaza*, koja podrazumeva konfiskovanje računarskog sistema ili pravljenje kopije podataka na forenzičkom sistemu;
- *ispitivanje* – obezbeđuje se prepoznavanje dokaza objašnjavajući njegovo poreklo i značaj, kao i pregled skrivenih i nejasnih informacija uz pravljenje odgovarajuće dokumentacije u vezi sa ispitivanim dokazima;
- *analiza* - cilj ove faze je da se na osnovu rezultata faze ispitivanja ukaže na značaj i dokaznu vrednost koju mogu posedovati pronađeni dokazi;
- *izveštaj* - ovaj korak podrazumeva pisanje izveštaja sa akcentom na proces analize dokaza i oporavka važnih podataka tokom cele istrage. Svaki slučaj računarskog kriminala obavezno prati izveštaj.

148 John Ashcroft, Attorney General, *Electronic Crime Scene Investigation, A Guide for First Responders*, U.S. Department of Justice,Office of Justice Programs, National Institute of Justice, https://www.ncjrs.gov/pdffiles1/nij/187736.pdf, 22.04.2016.

149 Ciardhuáin O. S., *An Extended Model of Cybercrime Investigations*, International Journal of Digital Evidence. Summer 2004, Volume 3, Issue1, 2004, https://utica.edu/ academic/institutes/ ecii/publications /articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf, 10.07.2016.

2.2.1.3. Model "Odgovor na incident"

Prosise i Mandia su 2001. godine predstavili digitalno istražni model "Odgovor na incident".[150] [151] Ova metodologija je *adekvatna za korporacijski model istrage* i fokusirana je na incidenti odgovor kada su u pitanju kritični sistemi koji mogu biti kompromitovani.

Model se sastoji od sledećih jedanaest faza:

- *priprema za incident* - podrazumeva sve one radnje, koje će pomoći da se forenzički relevantan događaj spremno dočeka. Omogućava jednostavniju koordinaciju između kadrova zaduženih za odgovor na incidentnu radnju. U pripremnoj fazi vrši se: identifikovanje i klasifikovanje kritične informacione imovine, implementacija računarskih i mrežnih protivmera koje podstiču efikasniji odgovor na incident, posedovanje programskih i hardverskih alata za odgovor na incident (npr. alata za pronalaženje i eliminisanje virusa i pretnji), uspostavljenje efikasnije interne politike, koja podstiče odgovor na incidentnu radnju uz odgovarajuća interna dokumenata i kontrolne liste (koje imaju za cilj brži oporavak sistema i mreže od incidente radnje).[152] *Ulaganje u razvoj kapaciteta za incidentne odgovore u okviru organizacije* zavisi od procenjenog rizika, organizovanja obuke IT-kadrova kao i nabavke neophodne infrastrukture. Zato je važno da je u organizaciji identifikovan svaki rizik digitalne imovine koji postoji u organizaciji na primer baze podataka korisnika, baze transakcija, baze PAN brojeva kreditnih kartica kada su u pitanju bankarske organizacije;
- *detektovanje incidentne radnje* - identifikacija sumnjive radnje;
- *inicijalni odgovor na incident* - u ovoj fazi se vrši potvrđivanje da se desila incidentna radnja i skupljaju se nestabilni dokazi tj. lako promenljivi dokazi (podaci koji mogu lako da se izgube npr. podaci RAM memorije);

---

150 Computer Crime and Intellectual Property Section Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, United States Department of Justice, 2002, http://www.justice.gov/ criminal/cybercrime/searching.html, 24.06.2016.

151 *Convention on cybercrime*, Council of Europe, Budapest novembar 2001, http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc, 10.07.2016.

152 Kao na primer: kreiranje spiska za proveru eng. notification checklist, kreiranje načina označavanje (eng. tag) i obeležavanje (eng. label) digitalnih dokaza, kreiranje početne kontrolne liste odrziva na incidentnu radnju prilagođenu okruženju, obuka zaposlenih koji će učestvati u odgovorima na incidentne radnje/nedozvoljene aktivnosti.

- *izrada strategije za odgovor na incident* - određivanje odgovora na incidentnu radnju u skladu sa poznatim činjenicama;
- *duplikacija* - pravljenje bekapa, odnosno mirror postojećeg sistema;
- *istraga* - istraživanje sistema da bi se identifikovalo ko je, zbog čega i na koji način realizovalo incidentnu situaciju;
- *realizacija sigurnosnih mera* - ova faza podrazumeva izolovanje sumnjivog sistema;
- *posmatranje mreže* - ova faza podrazumeva posmatranje mreže radi potencijalne detekcije novih odnosno ponovljenih napada;
- *oporavak* - vraćanje sistema u njegovo originalno stanje sa pridodatim merama zaštite;
- *izveštavanje* - podrazumeva izradu dokumentacije u vezi sa odgovorom na incidentnu radnju;
- *revizija* - razmatranje odgovora i prema potrebi adekvatno prilagođavanje.

2.2.1.4. Eoghan Casey model

Casey model je predstavljen 2000. Godine. U početku je bio zamišljen kao model koji se primenjuje isključivo na nezavisne računare (eng. standalone computers), da bi se vrlo brzo počeo primenjivati i u mreženom okruženju.[153] Istražnom procesu prilazi se sa pravnog stanovišta i ima nešto veći okvir. Veoma je primenjiv kako na *korporativnu istragu tako i na zvaničnu istragu*. Predstavljene kategorije su opšteg karaktera. Model omogućava ispitivačima i istražiteljima principe na osnovu kojih može da se formira argumentovana hipoteza koja je zasnovana na činjenicama uzimajući u obzir pravni kriterijum prihvatljivosti.[154] Ovaj *model* je široko primenljiv i *nezavistan je od tehnologije*. Faza analize u ovom modelu se zasniva na naučnim metodama.

Principi su sledeći:[155]

- *prihvatljivost* - koriste se metode i koraci koje su stekle konsenzus u

153 Citrix, *Citrix Xenserver,* http://www.citrix.com/English/ps2/ products/ product.asp? contentID =683148, 19.06.2016.

154 Communication from the Commission to the Council, The European Parliament, The Economic and Social Committee and Committee of the regions, *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, 2012, http://europa.eu.int, 22.06.2016.

155 Clarke N., *Computer Forensics A Pocket Guide*, IT Governance Publishing, United Kingdom, 2010.

relevatnim krugovima;
- *pouzdanost* - korišćeni metodi su lako proverljivi i dokazivi kako bi otkrića bila potkrepljena;
- *ponovljivost* - postupak je nezavistan prostorno i vremenski i može se ponoviti;
- *integritet* - postojanje mogućnosti provere nepromenjenosti stanja dokaza;
- *uzročno-posledični sled* - logičan sled događaja koji povezuje dokaze sa osumnjičenim;
- *dokumentacija* - ceo istražni postupak je pokriven dokumentacijom uključujući i ekspertska svedočenja.

Koraci Casey modela su sledeći:[156]

- *sumnje ili incidentna upozorenja* - svaki proces ima neki svoj početni korak. Početni korak može da bude npr. signaliziran od strane alarma nekog sistema za zaštitu (sistem za detektovanje napada eng. *intrusion detection* ili sistem za detektovanje zlonamernih aktivnosti eng. *proactive threat protection*), senzora zaštite na mreži, administratora sistema nakon pregleda log fajlova. Takođe može biti iniciran na tradicionalan način, u slučaju da neko prijavi kriminalnu aktivnost, što za posledicu ima izlazak istražnog tima na fizičko mesto krivičnog dela. U slučaju da se na tom mestu nalaze i elektronski uređaji (računari, telefoni, mrežna oprema i ostali digitalni izvori) deo istrage će se odvijati i u digitalno forenzičkom pravcu. U ovoj fazi se vrši prikupljanje inicijalnih činjenica pre pokretanja potpune istrage, da bi se razmotrio izvor i pouzdanost informacije. Na primer, pojedinac se žali na uznemiravanje zbog pretećih poruka na ekranu, a uzrok može biti virus, neuspešni upad u sistem, a može biti i lažan alarm. Zbog navedenog prvi korak je izuzetno osetljiv (jer se donose zaključci o tome da li se desila nedozvoljena aktivnost ili ne), jer svaka intervencija na mestu zločina može uticati na promenu dokaza, što može ugroziti ceo proces. Neophodno je da se uđe na mesto zločina, u ovom slučaju digitalno mesto.[157] Tom prilikom se prikupljaju inicijalne činjenice

156 *Ibidem.*

157 Mesto kriminala kod klasičnog kriminala kada je ubistvo u pitanju može biti ono što je trenutno prisutno i vidljivo kao na primer hotelska soba, parking, stan itd. Sa druge strane kod sajber kriminala mesto kriminala može biti ceo svet. Zato je važno da se kroz forenzički inicijalni odgovor reaguje veoma brzo da se ne bi određeni dokazi uništili ili nestali.

koje mogu sadržati relevatne informacije, ali se to mora obaviti na izuzetno pažljiv način. Iskustvo samog istraživača ili eksperta u ovoj fazi je veoma bitno, jer se na osnovu malog broja dokaza može doći do zaključaka da li se kriminalni akt dogodio ili nije. Ulazak u istragu prerano, odnosno bez odgovarajućeg ovlašćenja ili protokola može dovesti do kompromitovanja celog slučaja;

- *procena značajnosti* - istražni resursi (osoblje koje je uključeno u istražne aktivnosti) su ograničeni, zbog angažovanja u više slučajeva istovremeno, koji mogu biti ekvivalentni po značaju. Resursi se primenjuju se samo tamo gde su najpotrebniji. U zavisnosti od istražnog okruženja značaj ispitivanja sumnjivih kriminalnih aktivnosti varira. Kada je u pitanju *zvanična istraga* sve sumnjive kriminalne aktivnosti se moraju ispitati od strane nadležnih državnih organa. U *privatnom i poslovnom okruženju* sumnjive aktivnosti će biti predmet istrage, ali politika i kontinuitet poslovanja su češće u prvom planu po značaju u odnosu na pravni aspekt. Faktori koji utiču na značajnost su: pretnje fizičkim povredama, mogućnost značajnih gubitaka, rizik kompromitovanja ili ometanja sistema većih razmera. Ukoliko se problem može brzo zaustaviti ili ukoliko štete nema ili je minimalna, istraga se ne mora sprovoditi. U ovom koraku donosi se odluka o nastavku primene istražnih resursa (na osnovu važnosti dokaza pregledanih do ovog koraka) ili o obustavljanju daljih akcija, ukoliko podaci i informacije ukazuju da nedozvoljena aktivnost nije učinjena, uz detaljno obrazloženje;
- *protokoli incidenta i mesta zločina* - ukoliko je potpuna istraga odobrena, glavni cilj ovog koraka je sačuvati mesto zločina u "netaknutom" stanju. To se postiže dokumentovanjem stanja i očuvanjem integriteta predmeta sa mesta zločina na osnovu protokola. Procedure i prakse, moraju da se primenjuju da bi se smanjio procenat greške, previda i povreda, onih koji su odgovorni za osiguravanje mesta zločina (digitalni istražitelji ili lica koja su prva odgovorila na incidentnu radnju). Rezultat ove faze je obezbeđeno mesto zločina, gde je sav sadržaj dokumentovan i snimljen sa pratećim fotografijama i sa osnovnim dijagramima da bi se mapirale važne oblasti i predmeti. Ovakvo obezbeđeno mesto zločina je dobar temelj za sve naredne aktivnosti. Predmeti otkriveni u ovoj fazi ostaju nepromenjeni tokom cele istrage. U ovom koraku se ne prikupljaju dokazi i ne radi se analiza već se samo identifikuju

dokazi koji su relevantni za slučaj;

- *identifikacija ili konfiskacija* - nakon što je mesto zločina osigurano, potencijalni dokazi zločina ili incidenta moraju biti konfiskovani. Od izuzetne je važnosti da procedure budu jasne, a da bi se one uspešno sprovodile neophodno je razumevanje pravnih kriterijuma. Cilj ove faze je da se napravi dobar odabir objekata;
- *trijaža*, koje treba konfiskovati (fizičke i digitalne) uz detaljno dokumentovanje i obrazloženje svake sprovedene aktivnosti. Dokumentacija je prisutna u svim fazama istražnog postupka ali je pri konfiskovanju digitalnih dokaza najvažnija zbog uspostavljanja lanca nadležnosti i autentičnosti samih zaplenjenih dokaza. Na primer, fotografisanje i snimanje serijskih brojeva, predmeta, dokumentovanje ko je rukovao dokazima, pomaže da se prati kretanje dokaza nakon prikupljanja. U tu svrhu postoje unapred predviđeni obrasci i definisane procedure. U tradicionalnom kontekstu konfiskovanje podrazumeva "uzimanje predmeta", a u digitalnom kontekstu se vrši konfiskovanje predmeta takođe, ali sa tom razlikom što ti predmeti nose i *"određena stanja"* koja mogu da se izgube nakon zaplene ili nestabilnosti elektronskih uređaja (npr. slaba baterija, prekid struje). Ta stanja su zapisana u RAM memoriji (eng. Random Access Memory) računara koja sadrže podatke o procesima, informacije o stanju mreže, konekcije sa udaljenim računarom kao i mnoge druge. Kada dođe do isključenja sistema trenutni sadržaj RAM memorije je izgubljen i može se povratiti samo deo informacija. Ova specifičnost je veoma bitna jer daje šansu istražiteljima da se prikupe informacije iz zatečenog stanja pre nego što isključe napajanje i izvrše zaplenu. Iako se u ovoj fazi podrazumeva konfiskacija treba uzeti u obzir i metode i tehnike koje omogućuju prikupljanje osetljivih sistemskih i mrežnih informacija. Takođe treba skrenuti pažnju da *digitalni dokazi* mogu postojati u velikom broju *različitih formi*: logovi aplikacija, biometrijski podaci, aplikacijski metadata podaci, logovi internet servis provajdera, firewall logovi, proxy logovi, logovi mrežnog saobraćaja, logovi sistema za detektovanje upada u sistem, sadržaji podataka iz baze podataka i logovi transakcija, logovi audit programa i mnogi drugi logovi.

Da bi se proces zaplene što efikasnije sproveo publikovani su i *vodiči* u kojima su dati praktični saveti i principi koji su od koristi onima

koji se bave digitalnim dokazima.[158] [159] [160] Ovi dokumenti su veoma korisni u smislu razvijanja standardnih operativnih procedura koje mogu da omoguće izvođenje jednostavnijeg tipa istrage sa manjim brojem računara (do 5). Ove procedure služe da bi se smanjio rizik od greške, obezbedilo korišćenje najbolje moguće metode i uticalo na povećanje verovatnoće da dva forenzička istražitelja dođu do istih zaključaka nakon pregledanja dokaza. Što je bolje utrenirano i obučeno osoblje, koje prvo odgovara na incident, veće su šanse da se pronađe veliki broj dokaza i da se konfiskuju predmeti koji sadrže veliki broj relevantnih informacija;

- *očuvanje* - ova faza je odgovorna za preduzimanje potrebnih mera kako bi se očuvali integriteti fizičkih i digitalnih dokaza odnosno njihova nepromenjivost. Za uspeh ove faze bitnu ulogu imaju alati i metodi koji se koriste, kao i sama stručnost istražitelja, jer se u krivčnom postupku uglavnom pokušava to osporiti od suprotne strane. Veliki broj stručnjaka koji se bavi digitalnom forenzikom tvrde da od ove faze počinje prava digitalna istraga. U ovoj fazi se prave veći broj dupliranih kopija digitalnih dokaza iz svih izvora, dok se originalni materijal stavlja u katolog i smešta u kontrolisano okruženje u neizmenjenom stanju. Kopija dobijena odgovarajućim forenzičkim alatima je identična kopija originalnog materijala koja služi za pregledanje, ispitivanje i analize u daljim fazama digitalno forenzičke istrage;
- *oporavak podataka* - pre same analize podataka neophodno je izvršiti

158 Jedan od njih je *"Electronic Crime Scene Investigation: A Guide for First Responders"*, publikovan od strane US Department of Justice 2001. godine u USA1. U ovom vodiču opisani su različiti izvori digitalnih dokaza. Na slikovit način kroz ilustracije opisuje se kako se kojim digitalnim dokazom rukuje kako bi pomogle osoblju koje prvo odgovara na incident, John Ashcroft, Attorney General, *Electronic Crime Scene Investigation, A Guide for First Responders*, U.S. Department of Justice,Office of Justice Programs, National Institute of Justice, https://www.ncjrs.gov/pdffiles1/nij/187736.pdf, 23.05.2016.

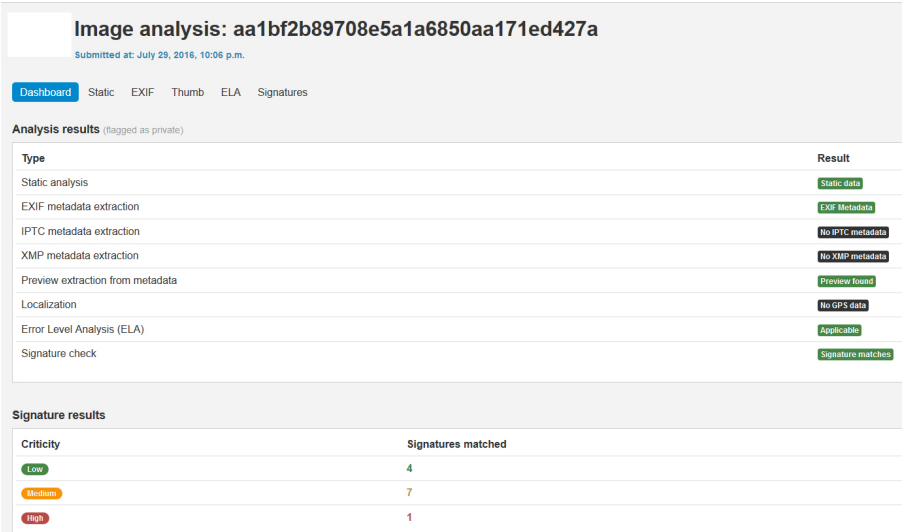
159 *„Forensic Examination of Digital Evidence: A Guide for Law Enforcement",* publikovan 2004. godine u USA. U ovom vodiču se opisuju opšti forenzički principi i procedure koji se primenjuju u radu sa digitalnim dokazima. Aktivnosti koje se preduzimaju sa ciljem prikupljanja i zaštite digitalnih dokaza ne smeju da utiču na integritet digitalnih dokaza. Ove aktivnosti sme da izvodi samo stručno lice uz dokumentovanje svih aktivnosti (zaplena, pregled, prenos, skladištenje i zaštita). Vidi više: *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, National Institute of Justice, http://www.nij.gov/pubs-sum/199408.htm , 21.05.2016.

160 *„The Good Practices Guide for Computer Based Electronic Evidence"*, publikovan 2003. godine od strane " Association Chief Police Officers - ACPO" u Velikoj Britaniji. Ovaj vodič pruža polaznu tačku za inicijalne korake u rukovanju digitalnim dokazima. Vidi više: http://www.7safe.com/ electronic_evidence /ACPO_guidelines_computer_evidence.pdf, 22.05.2016.

povraćaj podataka koji mogu biti izbrisani, sakriveni, prikriveni (zamaskirani) ili iz nekih drugih razloga nedostupni za pregled (npr. zbog postojanja nekog specifičnog operativnog ili fajl sistema). Takođe u ovoj fazi će možda biti neophodno da se vrši rekonstrukcija delova podataka sa ciljem oporavka nekog objekta. U ovoj fazi treba isključivo raditi na forenzičkim kopijama originalnih digitalnih dokaza dobijenih iz faze čuvanja.[161] Akcenat u ovoj fazi je proces oporavka i identifikacije svih nedostupnih podataka. Cilj ove faze je da se učini dostupnim što veća količina podataka za narednu fazu. Osim toga ova faza omogućuje, ukoliko je konkretan dokaz pronađen ili snimljen, najkompletniji uvid u vremenski okvir podataka, motive i namere prikrivanja nedozvoljene aktivnosti putem brisanja, skrivanja ili maskiranja podataka uz upotrebu različitih tehnika od strane počinioca. *Tehnike skrivanja podataka* od strane malicioznih korisnika odnose se na manipulaciju sa fajlovima, manipulaciju sa diskom, šifrovanje i tehnike prikrivanja podataka (eng. steganography). Kada je reč o steganografiji forenzičari se najčešće susreću sa tehnikama prikrivanja podatke u obliku normalnih fajlova tipa word, pdf, mp3, .jpg, .mkv. Na primer, forenzičkom istragom utvrđeno je da je jedan mp3 fajl veličine 2 GB, a postoje samo 2 pesme što izaziva sumnju da je upotrebljena steganografija. Forenzičkom analizom ustanovljeno je da fajla sadrži i 2 pesme, ali u telu tog fajla se nalazio i kontejner koji sadržao skrivene podatke u sklopu mp3 fajla. Postoje profesionalni alati koji omogućuju otkrivanje ovakvih slučajeva steganografije (ENCASE, AccessData FTK). Trend kod anti-forenzičkih procesa jeste razvijanje sopstvenih algoritama steganografije koje se teško uočavaju.

Za analizu steganografije koriste se alati Stegsecret162, Spyhunter[163] i servis automatske analize slike koji postoji na web sajtu http://www.imageforensic.org/ koji može da generiše statičke rezultate. U forenzičkoj istrazi radi se detaljna inspekcija slika koja se pronađu u ispitivanom operativnom sistemu, analizirajući određene karakteristike slike kao što su pikseli, bit depth (broj boja), fajl format, rezolucija, veličina slike, stepen kompresije, tip (vektorski ili rasterski) i meta podaci. Među najvažnijim podacima o slici su meta podaci.

161 Osim u izuzetnim slučajevima kada su u pitanju ugrađeni sistemi (eng. embedded systems).
162 Http://stegsecret.sourceforge.net/, 20.07.2016.
163 Http://www.spy-hunter.com/stego.html, 20.07.2016.



Slika 2. Prikaz analize slike sa sajta Imageforensic.org

Na osnovu meta podataka moguće je saznati koja je aplikacija kreirala sliku, GPSs lokaciju gde je slika nastala, ime računara na kome je slika generisana itd.

U statičkim rezultatima mogu se pronaći statičke informacije kao što su dimenzije, datum analize slike, zatim tip fajla koji se identifikuje na osnovu hedera samog fajla. Kada je reč o metadata podacima oni se nalaze pod opcijom EXIF, a parametri koji su bili u momentu kreiranja same slike nalaze se pod sekcijom PHOTO. Sekcija ELA predstavlja spektralnu analizu slike odnosno identifikaciju elemenata slike koji potencijalno mogu da predstavljaju delove nedozvoljene aktivnosti (mogu se uočiti izmene na slici). Pod sekcijom Signatures moguće je identifikovati program sa kojim je kreirana ova slika, uređaj sa kojim je napravljena slika, vreme nastanka slike, korisnički komentari uneti u sliku, serijski broj aparata i GPS kordinate.

Kada je reč o *manipulaciji sa fajlovima* uglavnom se menjaju imena i ekstenzije i daju im se osobine skrivenog fajla (eng. hidden properties). *Manipulisanje diskom* podrazumeva skrivanje particija (PartitionMagic,[164] Partition Commander,[165] LILO) i skrivanje podataka u loše sektore. *Kod*

164 Http://www.symantec.com/press/powerquest/pq092302.html, 22.05.2016.
165 Https://www.vcom.com/partition-commander, 22.05.2016.

enkriptovanja koriste se bit šifting (Hex Workshop)[166] i steganografija (S-tools,[167] Anubis,[168] MP3STEGO,[169] OpenPuff)[170] i upotreba EFS (Encrypting File System)[171] fajl sistema. Prisustvo ovih alata (bez znanja administratora ili korisnika) na kompromitovanom računaru ukazuje forenzičaru da je maliciozni korisnik nameravao da izvrši skrivanje potencijalnih dokaza ili tragova;

- *pronalaženje značajnih podataka* - u ovoj fazi istražitelji imaju na raspolaganju sve potencijalne digitalne dokaze. Vrši se prikupljanje podataka i metadata podataka (podaci o podacima) iz očuvanog i oporavljenog izvora prema kategorijama dokaza, a ne prema sadržaju ili kontekstu. Ovi podaci u slučaju digitalnog dokaza mogu pružiti informacije o tome koji je korisnički profil kreirao određeni fajl. Na primer, ukoliko se otvori pdf dokument i vidi se ko je autor fajla može se identifikovati određeno lice, dodatno kroz pdf metadata može se identifikovati i koja je aplikacija kreirala taj pdf fajl. To može biti veoma značajno jer ukoliko se utvrdi da je to u pitanju aplikacija Microsoft Word 2010, to znači da potencijalni zlonamerni napadač koristi i Outlook 2010 što može biti od pomoći pri analizi računara na mreži koji imaju outlook 2010, pa zatim kroz analizu Aktivnog direktorijuma pokušati da se otkrije ko sve ima Outlook 2010 u organizaciji. Na taj način može da se pronađe zlonamerni napadač. Dodatno metadata podaci mogu sadržati i GPS lokacije, na primer forenzičar je pronašao sliku koja predstavlja digitalni dokaz i ukoliko je ona napravljena sa mobilnim uređajem koji ima GPS funkcionalnost metadata informacije sadržaće i lokaciju gde je slika napravljena. Za analizu metadata podataka postoje korisni alati za njihovu automatsku ekstrakciju iz zadatih podataka pružajući uvid u sadržaj tih fajlova.

Istražitelj na osnovu poznavanja tehnologija i alata, utreniranosti i iskustva, pretražuje određene kategorije koje imaju određene klasne karakteristike za koje se zna ili postoji verovatnoća da su u vezi sa relevatnim činjenicama iz slučaja. Ovo je faza gde konkretne činjenice dobijaju oblik

---

166 The Hex Workshop Hex Editor, BreakPoint Software, hhttp://www.hexworkshop.com/, 22.05.2016.

167 Http://www.spychecker.com/program/stools.html, 22.05.2016.

168 Http://sourceforge.net/projects/anubisstegano/, 22.05.2016.

169 Digital watermarking & steganography, MP3stego, The information hiding homepage, http://www. petitcolas.net/fabien/steganography/mp3stego/, 22.05.2016.

170 Advanced Embedded Solutions, http://embeddedsw.net/OpenPuff_Steganography_Home.html, 22.05.2016.

171 University Information Security Services, University Information Security, *Information Security Policies and Guidance*, http://www.oit.umn.edu/security/topics/windows-efs/index.htm, 22.05.2016. EFS može koristiti ugrađenu 128-bitnu enkripciju što se često sreće u praksi.

koji *potvrđuje ili opovrgava hipotezu* izgrađenu od strane istražnog tima. Na primer, ukoliko se radi o optužbi koja ima veze sa dečijom pornografijom, zahtevaće se vizuelni digitalni dokazi u nekom od strandardnih grafičkih formata kao na primer JPG, GIF, BMP, TIFF. U tom slučaju istražitelj će se fokusirati na pretragu fajlova koji sadrže određene karakteristike ovih grafičkih formata. Ukoliko se radi o incidentnoj radnji "upadanju u sistem" istražitelji će se fokusirati na pretraživanje fajlova ili objekata koji su u vezi sa rutkit alatima (eng. rootkit), exploitima (grupe izvršnih fajlova ili skripti) koji pomažu napadaču da uspešno kompromituje sistem.[172] Rezultat je uglavnom velika količina digitalnih informacija koji u sebi sadrže potencijalne dokaze;

- *redukcija* - ova faza je specifična po tome što se u njoj ciljaju specifični objekti koji su prikupljeni i povezani sa istragom ili se donosi odluka da se neki od njih eliminišu. U ovom koraku se *izdvajaju nebitni podaci od bitnih* na osnovu eksternih atributa podataka (hash ili checksum vrednosti) ili tipova podataka, ne uzimajući u obzir sadržaj ili kontekst. Kriterijum na osnovu kog se vrši eliminisanje određenih podataka izuzetno je važan i može biti preispitan od strane suda. Kao rezultat ove faze dobija se skup digitalnih informacija, koje imaju najveći potencijal da sadrže podatke sa dokaznom vrednošću;
- *organizovanje i pretraga* - u ovoj fazi se vrši priprema podataka za temeljnu analizu koja sledi u narednoj fazi. Savet je da se dobijena grupa materijala iz prethodne faze ogranizuje putem grupisanja i označavanja da bi se ubrzala faza analize. Određeni fajlovi se mogu grupisati u grupe koristeći foldere ili eksterne medije za skladištenje podataka. Cilj ove faze je da se olakša istražiteljima da pronađu i identifikuju podatke tokom analize, koji će kasnije koristiti pri kreiranju finalnih izveštaja i svedočenja pred sudom. Ova faza podrazumeva korišćenje različitih tehnologija pretraga kao pomoć istražiteljima za brzo lociranje potencijalnih dokaza. Na primer, podaci se mogu indeksirati radi efikasnijeg pregleda materijala što će pomoći istražiteljima pri identifikovanju materijala prema značajnosti (relevantni, nebitni).[173] Rezultat ove faze su

172 Rootkit Hunter, http://www.rootkit.nl/projects/rootkit_hunter.html, 26.11.2015. http://download.nai. com/ products/mcafee-avert/whitepapers/akapoor_rootkits1.pdf, 26.11.2015

173 Indeksiranje je tehnika koja se koristi za brzo pretraživanje podataka. Indeksiranje prolazi kroz kompletno telo podatka i kreira mapu lokacija svih informacija. Ova mapa odnosno indeks ima funkciju kao na primer indeks u knjizi ili listni katalog u biblioteci. Proces indeksacije može biti dugotrajan ali kada se jednom uradi pretraživanje je izuzetno brzo.

dobro organizovani atributi podataka koji moraju da omoguće ponovljivost i preciznost aktivnosti u narednoj fazi - analizi;

- *analiza* - ova faza podrazumeva detaljnju pretragu padataka, koji su identifitikovani u prethodnim fazama. Vrši se detaljan pregled unutrašnjih atributa podataka kao što je tekst i njegovo značenje, specifični formati audio i video zapisa. Na osnovu individualnih i klasnih karakteristika pronađenih digitalnih dokaza prave se veze između podataka, određuje se njihovo poreklo, da bi se locirali učinioci nedozvoljene radnje;
- *procena konteksta i sadržaja* - sadržaje, čitljivih ili vidljivih digitalnih podataka moguće je pregledati i na osnovu njih utvrditi faktore kao što su način (sredstva), motiv i prilika;
- *eksperimentisanje* - proba novih i neisprobanih tehnika i metoda, koji su zasnovani na naučnoj osnovi uz rigorozno dokumentovanje za potrebe testiranja. Rezultat eksperimenta može biti ili odbijen ili opšte prihvaćen;
- *fuzija i povezanost* - tokom istrage podaci (informacije) se prikupljaju iz mnogih izvora (digitalni i nedigitalnih). Sami za sebe podaci (informacije) ne mogu da prenesu sliku stanja o istraživanom događaju, već moraju da se fuzionišu da bi se sklopila cela priča. Primer fuzije može predstavljati vremenski okvir nekog događaja ili radnje, koji se odnosi na određeni slučaj odnosno incident. Svaka nedozvoljena aktivnost ili incident poseduje hronološku komponentu, gde događaji ili radnje traju tačno određeni vremenski period. Ovim se dobijaju odgovori na to gde, kada i kako se desio forenzički relevantan događaj. Vremenski delovi svih predočenih aktivnosti biće fuzionisani sa različitih izvora (digitalnih i nedigitalnih). Npr. digitalni podaci, zapisi telefonskih kompanija, poruke elektronske pošte, izjave svedoka i izjave osumnjičenih se fuzionišu. Korelacija se odnosi na uzročno posledičnu vezu između događaja uz hronološko praćenje;
- *provera valjanosti* - rezultat faze analize predstavlja podnošenje obrazloženih dokaza sudu ili organima krivičnog gonjenja (policiji i tužilaštvu);
- *izveštavanja* - da bi se obezbedila transparentnost u istražnom postupku, konačni izveštaj treba da sadrži važne detalje o svakom istražnom koraku, uključujući: protokole, metode prilikom konfiskacije, dokumentaciju, čuvanje, oporavak, rekonstrukciju,

organizovanje i pretragu ključnih dokaza. U izveštaju potrebno je pokloniti najviše pažnje analizi na osnovu koje su se izveli zaključci ili na opisima dokaza koji podkrepljuju te zaključke. Ne smeju se donositi zaključci bez detaljno opisanih potkrepljujućih dokaza i analiza. Izveštaj mora biti objektivno napisan uključujući i iznošenje alternativne teorije koje su kontradiktorne ili nepotkrepljene dokazima;

- *argumentovano uveravanje i svedočenje* - cilj ove faze je da analitičari i/ili eksperti obuhvate sve tehničko-tehnološke i inženjerske detalje, kao i korišćene metode u istrazi i prenesu ih u jasnom obliku razumljivo sudu.

2.2.1.5. Carrier i Spafford model

Carrier i Spafford model je predstavljen 2003. godine.[174] Ovaj model posmatra *računar kao mesto zločina* i naziva ga digitalno mesto krivičnog dela na kome se primenjuju tehnike istrage fizičkog mesta krivičnog dela. Ovaj model može biti primenjen kako na *zvaničnu istragu tako i na korporacijsku istragu*. Mesto zločina predstavlja okruženje (fizičko ili virtuelno) dok incident predstavljaju nedozvoljene aktivnosti koje za posledicu imaju reakciju forenzičkog tima. Model sastoji se iz 17 podfaza organizovanih u pet faza:

1. pripremna faza podrazumeva obezbeđivanje neophodne infrastrukture i operacija koje su u stanju da u potpunosti podrže proces istrage, jer dokazi i fizički i digitalni mogu biti izgubljeni ukoliko nisu na adekvatan način prikupljeni i čuvani. Ova faza podrazumeva i dve podfaze: *faza operativne spremnosti* (FOS) i *faza infrastrukturne spremnosti* (FIS):

- *FOS* podrazumeva postojanje neophodne obuke i opreme za lica uključena u forenzičko istraživanje. Na primer, obuke interventnog tima za odgovor na incident, obuke forenzičkih laboratorijskih analitičara i lica koja primaju inicijalne izveštaje o incidentnoj radnji. Sva oprema (koja će biti upotrebljena na mestu krivičnog dela i ona iz forenzičkih laboratorija) koja će biti korišćena u digitalnoj forenzičkoj istrazi mora da bude ispravna, održavana i tehnološki najsavremenija;
- *FIS* osigurava postojanje potrebnih podataka kako bi se izvršila potpuna istraga. Odnosi se na one koji održavaju okruženje, koje

174 Council of Europe, Recommendation No. R (95) 13, http://www.justice.gov/ criminal/ cybercrime/crycoe.htm, 11.07.2016.

može biti meta kriminalnih aktivnosti odnosno mesto krivičnog dela. Od fizičkih primera ovde mogu da spadaju instaliranje i raspoređivanja video kamera ili čitača kartica za snimanje potencijalnih fizičkih mesta krivičnih dela. Digitalni primeri ove faze podrazumevaju slanje log fajlova sa servera na određeni zaštićeni "log server", sinhronizovanje satova na serverima sa NTP serverom, heširanjem kritičnih izvršnih fajlova sa SHA1 ili sa SHA256 kao vid osnovnog tipa zaštite.

2. razvojna faza - je odgovorna za uspostavljanje mehanizama za detektovanje i potvrđivanje incidenta. Zadaci koji se u ovoj fazi obavljaju razlikuju se od tipa istrage odnosno da li je angažovan zvanični istražni tim ili korporacijski istražni tim. Ova faza podrazumeva dve podfaze:

- *podfaza detekcija i obaveštavanje* - podrazumeva detektovanje incidentne radnje i obaveštavanje nadležnih odnosno ovlašćenih lica. Podrazumeva različite načine obaveštavanja kao npr. upućivanje poziva na 92, alarm mrežnog sistema za detekciju napada, a može biti i obaveštavanje od strane ljudi koji istražuju ilegalne aktivnosti na mreži;
- *podfaza potvrda i autorizacija* - cilj ove faze je dobijanje ovlašćenja da se u potpunosti istraži incident i mesto krivičnog dela. U zavisnosti od tipa istrage ova faza ima svoj različit razvoj. Kada je u pitanju zvanična istraga ova podfaza podrazumeva *dobijanje naloga za pretres* potkrepljenog dovoljnim dokazima. Kada je u pitanju korporacijska incidentna radnja, nisu potrebni nalozi za pretres ukoliko nije došlo do kršenja prava privatnosti ili ukoliko slučaj ne prevazilazi kapacitete korporacijskog istražnog tima (npr. međunarodni incident, zahtev za prisluškivanje telefonskog aparata). U slučaju neovlašćenog upada u server, angažuje se *interventni tim* kao odgovor na incidentu radnju i preduzima potrebne aktivnosti kako bi proverili da li je sistem kompromitovan (nadgledanje mreže u potrazi za sumnjivim aktivnostima, pretraživanje sistema, radi pronalaženje rootkit programa ili drugih exploit alata). Bitno je naglasiti da ukoliko se analiza sprovodi "uživo", prema sistemu se treba odnositi kao prema mestu krivičnog dela uz minimalan uticaj na sistem. Ukoliko se potvrdi da se desila incidentna radnja, neophodno je odobrenje nadležnih za preduzimanje daljih aktivnosti.[175]

175 Ukoliko se radi o serverima gde je vreme aktivnog rada kritično za kompaniju odobrenje mora da se dobije od strane izvršnog nivoa kompanije.

3. Faza istrage fizičkog mesta krivičnog dela - u ovoj fazi se vrše prikupljanje i analiza fizičkih dokaza, kao i rekonstrukcija događaja koji su doveli do incidentne radnje.[176] Najvažniji cilj digitalno forenzičke istrage je identifikovanje učinioca nedozvoljene aktivnosti ili incidentne radnje, a za to je neophodno postojanje fizičkih dokaza. Kada je u pitanju *zvanična istraga*, istražitelj fizičkog mesta krivičnog dela odgovoran je za izvršenje većeg broja zadataka koji će biti navedeni. Kada je reč o *korporacijskoj istrazi*, te zadatke će vršiti interventni tim za odgovor na računarski incident ili tim za fizičku bezbednost.

Ova faza sastoji se od 6 podfaza:

- *podfaza očuvanje* - ova faza je ista za svaki tip nedozvoljene aktivnosti. Podrazumeva, osiguranje izlaza, pomoć povređenima, zadržavanje osumnjičenih kao i identifikovanje svedoka. Kada je reč o digitalnom incidentu, fizičko mesto zločina trebalo bi da se osigura koristeći iste procedure kao kod fizičkog incidenta. Ako je reč o istrazi vezanoj za upad u server, ova faza podrazumeva identifikaciju osobe iz računarskog centra i sprečavanje drugih lica da uđu u centar, pošto je moguće da je neko od zaposlenih odgovoran za incidentnu radnju. U ovoj podfazi se ne čuvaju konkretni dokazi, već se vrši očuvanje fizičkog mesta krivičnog dela od bilo kakvih izmena, da bi se mogli prikupiti i identifikovati dokazi;
- *podfaza pregled* - podrazumeva opservaciju fizičkog mesta krivičnog dela od strane istražnog organa osobe koja prva odgovara na incident. U ovoj fazi vrši se identifikovanje delova fizičkih dokaza i osetljivih delova fizičkih dokaza (koji moraju brzo da se sakupe i dokumentuju da bi se izbeglo oštećenje), uz razvijanje hipoteze o nedozvoljenoj aktivnosti. Kada je reč o digitalnom incidentu primeri bi bili sledeći: identifikacija fizičkih dokaza (broj računara, lokacija računara, mrežne konekcije računara, mobilni telefoni, optički mediji kao što su CD-Rom, DVD-Rom, Blue ray), eksterni prenosni uređaji, moguće šifre iz beleški. Akviziciju dokaza (prikupljanje) neophodno je da izvrši digitalni forenzičar specijalista za računare. Uključen računar se smatra osetljivim dokazom, jer se digitalni dokazi koji na njemu postoje mogu lako uništiti sa udaljenog sistema. Zato su obavezne standardne procedure kao npr. isključivanje računara sa mreže, pre nego što se započne potpuna forenzička istraga;

176 Faza istrage fizičkog mesta krivičnog dela odvija se paraleleno sa fazom istrage digitalnog mesta krivičnog dela, a dobijeni rezultati iz istrage digitalnog mesta krivičnog dela koriste se u istrazi fizičkog mesta krivičnog dela.

- *podfaza dokumentovanje* - podrazumeva fotografisanje, skiciranje i video snimanje mesta krivičnog dela i fizičkih dokaza. Glavni cilj ove faze je da se prikupi i zabeleži što više mogućih informacija i detalja na fizičkom mestu zločina da bi se sačuvali raspored i važni detalji. Kada je reč o digitalnom incidentu vrši se fotografisanje i dokumentovanje računarskih konekcija kao i samo stanje računara. Od značaja može biti i dokumentovanje broja i veličine hard diskova i RAM memorije, dokumentovanje MAC adresa mrežnih adaptera sa računara, na osnovu kojih je moguće identifikovati sistemske i mrežne aktivnosti iz DHCP logova. Takođe se preporučuje da se dokumentuju i serijski brojevi računara ili neki drugi tragovi na računarima. S obzirom da forenzičke laboratorije ne mogu da dobiju originalni fizički hardver na analizu, veoma je važno da se u ovoj fazi dokumentuje što više detalja. Ti detalji, koji su u vezi sa fizičkim dokazima, mogu biti od velike koristi za analizu i kasniju rekonstrukciju;
- *podfaza akvizicija* - podrazumeva temeljnu pretragu i prikupljanje dodatnih fizičkih dokaza sa fizičkog mesta krivičnog dela. Pretraga može biti orijentisana prema nedostajućim delovima fizičkih dokaza kao na primer oružje, a može da bude metodična sa striktnim šablonima pretrage jer svaki tip dokaza podrazumeva specifične standardne procedure o načinu akvizicije. Kada je reč o digitalnom incidentu ova faza podrazumeva pretragu za dodatnim medijima i digitalnim uređajima na mestu zločina. Može uključivati i kontaktiranje mrežnog ili sistem administratora sa ciljem obezbeđivanja i dobijanja informacija iz log fajlova o pristupu sistemu, updatu sistema, firewall-u, antivirusa, sistema za detektovanje upada na sistem - IDS. Svi fizički prikupljeni dokazi sa mesta krivičnog dela, se šalju u forenzičke laboratorije radi analize, a njeni rezultati će se koristiti u narednoj podfazi. Ukoliko se računarski sistem smatra za fizički dokaz on će se konfiskovati kao dokazni materijal. Prilikom izvođenja procesa akvizicije mora se posedovati hardverski write blocker da bi se zaštitio originalni dokaz od izmena. Akvizicija može da se radi kao statična ili „uživo". Statična akvizicija se podrazumeva kada na primer hard disk (memorijska karica ili USB disk) nije u radnom režimu i u tom slučaju se vrši kreiranje forenzčke bit-stream kopije. Akvzicija uživo podrazumeva akviziciju podataka sa sistema koji je u radnom režimu. Za tu svrhu može se koristi USB port, serijski port. Procedura akvizicije mora biti dokumentovana u smislu na koji način se prikupljaju osetljivi podaci sa

sistema koji je aktivan i na koji način se isključuje računar;

- *podfaza rekonstrukcija* - podrazumeva razvijanje teorije o nedozvoljenoj aktivnosti na osnovu organizovanja rezultata analize prikupljenih iz fizičkih i digitalnih dokaza i fotografija i video snimaka sa mesta krivičnog dela. Uključuje korišćenje naučnih metoda u radu sa dokazima da bi se proverila razvijena teorija o nedozvoljenoj aktivnosti. U slučaju digitalne nedozvoljene aktivnosti rezultati istrage digitalnog mesta krivičnog dela su u korelaciji sa fizičkim dokazima da bi se osumnjičeni povezao sa digitalnim događajima. Na primer, aktivnosti u ovoj podfazi mogu da povežu aktivnosti kompromitovanog servera sa aktivnostima na radnoj stanici (npr. kućnim računarom) osumnjičenog preko logova na jednom i na drugom sistemu ili preko logova sa mrežnih uređaja od strane internet servis provajdera. Efikasnost ove faze zavisi upravo od angažovanja dobrih eksperata digitalne forenzike koji mogu da povežu događaje iz više izvora digitalnih dokaza;
- *faza prezentacije* - podrazumeva prezentovanje fizičkog mesta krivičnog dela i digitalnih dokaza o učinjenoj nedozvoljenoj aktivnosti sudu ili rukovodstvu korporacije.

4. Faza istrage digitalnog mesta krivičnog dela - ova faza počinje, kada su digitalni uređaji prikupljeni kao fizički uređaji sa fizičkog mesta krivičnog dela ili kada se počne sa analizom sačuvanog mrežnog saobraćaja radi obezbeđivanja dokaza. Računarski sistem se posmatra kao mesto zločina i pretražuje se radi prikupljanja dokaza. Svrha ove faze je da se identifikuju elektronski događaji koji su se desili na sistemu, da bi se prezentovali istražitelju fizičkog mesta krivičnog dela. Postoji interakcija istrage fizičkog mesta krivičnog dela sa istragom digitalnog mesta krivičnog dela. To znači da se rezultati ove faze prenose u istragu fizičkog mesta krivičnog dela. Svaki digitalni uređaj se posmatra kao posebno fizičko mesto krivičnog dela i rezultati dobijeni iz analize svakog digitalnog uređaja prosleđuju se podfazi istrage fizičkog mesta krivičnog dela. Takođe vrši se rekonstrukcija da bi se identifikovale veze između digitalnih uređaja. Fizička mesta krivičnih dela kao i digitalna mesta mogu da budu organizovani u primarna i sekundarna mesta, što omogućava analizu različitih tipova uređaja na različitim mestima.[177] Na primer, server na koji je izvršen upad bio bi primarno mesto zločina, a log server koji je kompromitovan zbog izmene log fajlova koji su u vezi sa upadom, posmatrao bi se kao sekundarno digitalno mesto zločina.

177 Carvey H., Altheide C., *Tracking USB storage: Analysis of Windows artifacts generated by USB storage devices*, Digital Investigation 2, pp. 94-100, Elsevier Academic Press, Burlington, MA 2005, http://www.sciencedirect.com/science/article/pii/S1742287605000320/pdfft?md5=b4d986c553c49a983e66ae2b68a0c4a6&pid=1-s2.0-S1742287605000320-main.pdf, 10.07.2016.

Podfaze istrage digitalnog mesta krivičnog dela uglavnom obavljaju forenzički specijalisti obučeni za rad sa forenzičkim alatima i tehnikama za digitalnu analizu. Ove podfaze su:

- *podfaza očuvanje* - očuvanje digitalnog mesta krivičnog dela podrazumeva obezbeđivanje izlaza i ulaza digitalnog mesta krivičnog dela uz očuvanje osetljivih digitalnih dokaza (dokazi koji se lako mogu izmeniti ili nestati). Podrazumeva korake kao što su izolovanje sistema od mreže, prikupljanje osetljivih podataka (dokazi koji se lako mogu izmeniti ili nestati), koji se mogu izgubiti prilikom isključivanja sistema, identifikovanje sumnjivih procesa na sistemu. Takođe je neophodno i evidentiranje svih ulogovanih sumnjivih korisnika na sistemu. Potrebno je obratiti posebnu pažnju na log datoteke, koje predstavljaju svedoke događaja i njih posebno obezbediti (ukoliko postoji pretnja njihovog brisanja pre kreiranja forenzičkih kopija). Neki od modela ovu podfazu očuvanja podrazumevaju kao čuvanje digitalnih dokaza dok ovaj model podrazumeva očuvanje kompletnog digitalnog okruženja. U ovoj fazi pravi se kompletna forenzička kopija fizičkog sistema (mirror) na forenzičkom računaru čime se realizuje očuvanje kompletnog digitalnog mesta krivičnog dela. To predstavlja veliku prednost nad fizičkim svetom zbog lakog kopiranja digitalnog okruženja. Ove forenzičke kopije sadrže celokupno digitalno mesto krivičnog dela za razliku od običnog bekapa, koji čuva samo dodeljene podatake (eng. allocated) u digitalnom mestu krivičnog dela. U zavisnosti od tipa istrage originalni hard disk može da bude čuvan kao fizički dokaz sve do okončanja postupka, a može posle postupka replikacije biti vraćen u produkciju ako su u pitanju kritični sitemi. Isto tako kada se izvrši snimanje mrežnog saobraćaja postiže se efekat čuvanja neizmenjenog stanja mreže;
- *podfaza pregled* - u ovoj fazi se pronalaze delovi digitalnih dokaza koji odgovaraju tačno određenoj vrsti nedozvoljene aktivnosti. Preporuka je da se ova faza realizuje u forenzičkoj laboratoriji, jer se u njoj može postići kontrolisano okruženje. Ukoliko to situacija nalaže, ova faza može da se izvršava i na kompromitovanom sistemu "uživo", ali bi bilo neophodno napraviti forenzičku kopiju sistema, da bi se digitalni dokazi mogli ponovo prikupiti i u kontrolisanim uslovima. Ponekad se ova faza izvodi i direktno na terenu da bi se utvrdilo, da li je potrebno da se sistem donosi na punu forenzičku analizu. U tom slučaju sistem se podiže u sigurnom okruženju pomoću butabilnog DVD/CD/floppy diska/

diskete, da bi digitalni dokazi ostali nepromenjeni. Na primer, ukoliko se radi o dečijoj pornografiji istražni organi će prikupiti sve grafičke slike sa sistema i identifikovaće one koje bi predstavljale potencijalne dokaze. Ako dođe do neovlašćenog upada na server, istražni organi će tražiti očigledne znakove rootkit instalacija, exploite, logove aplikacija i izvršiti pretragu za novim konfiguracionim datotekama. U nekim drugim slučajevima mogu se vršiti analize keša internet pretraživača i njegove istorije. U zavisnosti od veštine osumnjičenog u nedozvoljene aktivnosti, istražitelji će izvršiti procenu potrebnih tehnika koje će se primeniti u istrazi. Moguće je i dodatno konsultovanje ili angažovanje eksperata iz kriptografskih oblasti, eksperta za oporavak podataka (ako su određeni podaci obrisani ili nestali), eksperta iz digitalne forenzičke analize;

- *podfaza dokumentovanje* - podrazumeva pravilno dokumentovanje pronađenih digitalnih dokaza. Forenzička kopija sistema dobijena u toku podfaze "očuvanje" ima istu ulogu kao i fotografija ili video snimak fizičkog mesta krivičnog dela. Svaki deo digitalnog dokaza koji je pronađen u toku analize forenzičke kopije (mirror) originalnog sistema mora biti jasno i precizno dokumentovan. Digitalni dokazi u računarskom sistemu mogu postojati na različitim nivoima apstrakcije pa moraju biti dokumentovani u skladu sa tim.[178] Na primer, fajl može biti dokumentovan, koristeći njegovu punu putanju i puno ime. Takođe može biti određen klasterima na fajl sistemu koje fajl koristi ili sektorima na disku koje fajl koristi. Mrežni podaci mogu biti dokumentovani izvornom i ciljnom adresom na različitim mrežnim nivoima. Da bi se na sudu dokazao integritet digitalnih dokaza obavezna je primena kriptografske hash funkcije npr. SHA-1, SHA-256, nad dokazima da bi se dobila heš vrednost koja dokazuje integritet. [179] Postoje tri pravila o forenzičkom hešu.[180] 1. Ne može se predvideti heš vrednost fajla ili drajva, jer ne postoje dva heša koja se odnose na isti fajl odnosno drajv. 2. Ukoliko se bilo šta promeni u fajlu ili drajvu heš vrednost se mora promeniti. 3. Da bi dokazi mogli da se koriste na sudu u ovoj fazi vrši se kreiranje lanca neprekidnog očuvanja i nadzora dokaza (eng. chain of custody);
- *podfaza akvizicija* - predstavlja vremenski najzahtevniju fazu, podrazumeva detaljnu digitalno forenzičku analizu sistema radi

178 Cross M., *Scene of the Cybercrime*, Second Edition, syngress, 2008.

179 SHA-1 predstavalja unapređenu verziju heš algoritma razvijenu od strane *National Institute of Standards and Technology (NIST)*

180 Danchev D., *Building and implementing a successful information security policy*, 2003, http://www.Windowsecurity.com/pages/security-policy.pdf, 11.07.2016.

pretrage i prikupljanja digitalnih dokaza. Koristi rezultate iz faze "pretraga" da bi tipski fokusirala analizu. Na primer, pretraga se može vršiti prema ključnoj reči, ukoliko su one identifikovane iz drugih dokaza. Nealocirani prostor na fajl sistemu je predmet analize, jer može sadržati obrisane fajlove. Prikupljeni mrežni saobraćaj programom za snimanje mrežnog saobraćaja takođe može biti predmet analize. U zavisnosti od okolnosti pretraga može biti usmerena na pregledanje sadržaja svakog klastera (što se smatra fizičkom pretragom) ili svakog fajla (što se smatra logičkom pretragom);

- *podfaza rekonstrukcije* - ova faza koristi naučne metode da bi se testirali dokazi i na osnovu toga odbacili neodgovarajući digitalni dokazi. U ovoj fazi se konstatuje na koji je način digitalni dokaz dospeo na mesto izvršenja nedozvoljene aktivnosti i šta predstavlja njegovo prisustvo. Ukoliko određeni digitalni dokaz nedostaje, faza "pretrage" nastaviće da identifikuje dodatne dokaze. Na primer, ukoliko je reč o upadu na server ova faza može dovesti u vezu iskorišćavanje ranjivosti određenih servisa sa rootkit instalacijom uz korišćenje mrežnog sniffera;

- *podfaza prezentacija* - ova faza podrazumeva prezentovanje pronađenih digitalnih dokaza fizičkom istražnom timu (ukoliko postoje posebni istraživački timovi fizičkih i digitalnih mesta krivičnih dela), jer rezultate iz digitalne istrage ovaj tim koristi (integrišući rezultate istrage iz svakog digitalnog mesta krivičnog dela) u fazi "rekonstrukcije". U većini slučajeva fizički i digitalni tim za istragu su isti, pa se informacije lakše razmenjuju između članova tima.

5. *kontrolna faza* - predstavlja fazu pregleda stanja istrage sa ciljem identifikovanja oblasti koje bi mogle da se poboljšaju. Potrebno je da se izvrši procena uspešnosti obavljene fizičke i digitalne istrage zajedno kao i svaka ponaosob, kao i da li postoji dovoljno fizičkih i digitalnih dokaza da bi se slučaj rešio. Ukoliko rezultat nije pružio očekivane rezultate može biti primenjena neka nova procedura ili nova obuka.

Glavni cilj svih ovih navedenih modela jeste da se prikupi dovoljno dokaza, koji će biti adekvatni i prihvatljivi za sud. Ne postoji univerzalni okvir digitalne istrage, pa se može uočiti da se izneti modeli uglavnom oslanjanju jedni na drugi sa izmenama ili dopunama prethodnih modela. Neki od njih imaju veoma slične pristupe. Razlike se mogu uočiti prema fokusu samog modela u smislu da li je skoncentrisan na određenu fazu digitalne istrage.[181]

181 Michael Kohn, JHP Eloff, and MS Olivier, *Framework for a Digital Forensic Investigation*, http://mo.co.za/open/dfframe.pdf, 03.01.2016.

Prilikom digitalne istrage uvek treba odabrati upotrebljiv i fleksibilan model (nezavisan u odnosu na trenutnu tehnologiju) koji se može primeniti na sve aktuelne visokotehnološke kriminalne aktivnosti i one koje mogu da se dese u bliskoj budućnosti.[182] Model koji se odabre mora biti zasnovan na postojećoj teoriji fizičke istrage, što u praktičnom smislu podrazumeva sprovođenje istih koraka koje sledi stvarna istraga. On mora biti i dovoljno apstraktan i primenjiv kako na zvanični tip istrage tako i na korporacijiski tip i da obuhvata računarske incidente. U takve modele spadaju model Casey i model Carrier i Spafford.[183]

2.3. DIGITALNI DOKAZI

Cilj postupka pred sudom je da se utvrde sve činjenice i okolnosti koje mogu biti od uticaja na rešavanje konkretne stvari. U krivičnom postupku sprovode se različite dokazne radnje: pretresanje stana, privremeno oduzimanje predmeta, saslušanje okrivljenog, saslušanje svedoka, uviđaj i rekonstrukcija, veštačenje, uvid u fotografije, zvučni i video snimci, tajni zvučni i optički nadzor osumnjičenog, pružanje simulovanih poslovnih usluga i sklapanje simulovanih pravnih poslova, angažovanje prikrivenog islednika, automatsko računarsko pretraživanje ličnih i drugih podataka, saslušanje svedoka saradnika itd. Ovako prikupljene dokaze sud ili drugi organ slobodno ocenjuje, odnosno utvrđuje postojanje ili nepostojanje činjenica značajnih za određeni postupak. Zajedničko kod svih dokaznih postupaka je da se utvrdi stvarno stanje stvari koje odgovara konkretnom slučaju.[184]

Dokaz je ono što razdvaja hipotezu od neosnovane tvrdnje.[185] Dokazom se može potvrditi ili oboriti hipoteza. Stoga je od izuzetne važnosti pitanje njegovog integriteta, odnosno koji se dokaz može prihvatiti na sudu. Na zasedanju Međunarodne asocijacije računarskih naučnika IACIS u Portlandu (država Oregon) 1991. godine je konstatovano i odlučeno da su „digitalni dokazi" ravnopravni sa dokazima prikupljenim na tradicionalan

182 Cole E., *Hackers Beware*, New Riders Publishing, 2002.
183 Vanja Korać, *Digitalna forenzika kao arheologija podataka u visokotehnološkom kriminalu*, Beograd, Centar za nove tehnologije Viminacium, 2013, str. 76.
184 Dragan Prlja, Miodrag Savović, *E-mail kao dokazno sredstvo u uporednom pravu*, Strani pravni život, br. 2/2009, str. 71-74.
185 Manzuik S., Gold A., Gatford C., *Network Security Assessment: From Vulnerability to Patch*, Syngress Publishing, Inc., 2007.

način, odnosno fizičkim predmetima.[186] [187]

Priznavanjem digitalnih dokaza kao ravnopravnih i prihvatljivih za sud, nastala je *računarska forenzika* kao deo forenzičke nauke, u čijem je fokusu obrada legalno pribavljenih dokaza pronađenih u računaru i na digitalnim medijima za čuvanje podataka.[188]

Pod *pojmom digitalnih dokaza* prema definiciji IOCE u oblasti forenzičkih nauka, digitalni dokaz je svaka informacija u digitalnom obliku koja ima dokaznu vrednost i koja je uskladištena ili prenesena u takvom obliku. Prema tome digitalni dokaz obuhvata računarski uskladištene i generisane dokazne informacije, digitalne audio i video signale, digitalnu fotografiju, zapis sa digitalnog mobilnog telefona, informacije na digitalnim faks mašinama i informacije sa drugih digitalnih uređaja. Digitalni dokaz je svaka informacija uskladištena, generisana ili prenesena u binarnoj (digitalnoj) formi, uključujući i njihovu odštampanu formu, koja obuhvata digitalne podatke: računara, digitalnog foto/audio/video/mobilnog telefona/faksa i drugih digitalnih uređaja, a koja ima dokaznu vrednost na koju se sud može osloniti.[189] [190]

Prema SWGDE/IOCE[191] [192] standardu dokazi su klasifikovani u tri osnovne kategorije:[193]

- *digitalni dokaz* - informacija od značaja za krivični postupak koja se nalazi ili prenosi u digitalnom obliku;
- *fizički predmeti kao dokaz* - fizički medijum koji skladišti ili prenosi digitalnu informaciju;
- *digitalni podaci* - informacije od značaja za krivični postupak koje su povezane sa fizičkim predmetom.[194]

---

186 IACIS – International Association of Computer Specialist

187 Aycock J., *Computer Viruses and Malware* , Springer , Canada, 2006.

188 Vanja Korać, Dragan Prlja, i Gordana Gasmi, *High Tecnology Criminal and Digital Forensics*, in: Preventing and Combating Cybercrime, Cluj-Napoca, Accent, 2016, str. 93.

189 Beebe N. L., Clark J. G., *A hierarchical, objective-based framework for the digital investigations process*, In Proceedings of the 2005 Digital Forensics Research Workshop, 2005, str. 146-166.

190 Kornblum J. D., *Exploiting the Rootkit Paradox with Windows Memory Analysis*, International Journal of Digital Evidence Fall 2006, Volume 5, Issue 1, 2006.

191 Scientific Working Group on Digital Evidence (SWGDE), http://www.swgde.org/, 03.01.2016.

192 International Organization on Digital Evidence (IOCE), http://www.ioce.org/core.php?ID=1, 03.01.2016.

193 Baker S., Green P., Meyer T., Cochrane G., *Checking Microsoft Windows Systems for Signs of Compromise version 1.3.4*, 2005, http://www.oucs.ox.ac.uk/network/ security/documents/win_intrusion.pdf, 22.06.2016.

194 Michael Cross, S*cene of the Cybercrime*, Second Edition, Syngress, 2008, str. 628.

Neophodno je razgraničiti značenje pojedinih *pojmova* koji se često koriste kao sinonimi, što pri svakodnevnom korišćenju računara ne predstavlja problem, ali prilikom forenzičke analize njihovo razlikovanje je veoma značajno.

Originalni digitalni dokaz (eng. evidence media) je fizički predmet i/ili podatak sadržan u tom predmetu u vreme akvizicije ili zaplene predmeta koje treba istražiti. Na primer, to mogu biti podaci snimljeni na računaru, koji je fizički privremeno oduzet dok istraga traje sa ciljem dostavljanja tog dokaza sudu, nakon pokretanja sudskog postupka.

Duplikat digitalnog dokaza (eng. target media) je verna digitalna reprodukcija svih objekata podataka sadržanih u originalnom fizičkom predmetu (HDu, CD ROMu, FD, memoriji itd.).

Kopija digitalnog dokaza je verna reprodukcija informacija koje su sadržane na originalnom fizičkom predmetu, nezavisno od originalnog fizičkog predmeta.[195]

Mesta na kojima digitalni forenzičari u praksi pronalaze potencijalne dokaze su sledeća: log fajlovi, konfiguracioni fajlovi, bekap fajlovi, artefakti fajl sistema, printer spool fajlovi, internet kolačići, swap/page fajlovi, sistemski fajlovi, fajlovi sa istorijom, privremeni fajlovi, internet bookmarks, internet omiljene lokacije, hibernacijski fajlovi, korisnički kreirani fajlovi, fajlovi zaštićeni šifrom;[196] fajlovi zaštićeni enkripcijom, skriveni fajlovi, kompresovani fajlovi, tabelarni fajlovi, fajlovi baza podataka, kalendar, multimedijski fajlovi (audio, video, grafički fajlovi), adresar, fajlovi elektronske pošte.

Elektronski uređaji na kojima je moguće pronaći digitalne dokaze: interni storidž (HDD, SSD), memorijske kartice, biometrijski skeneri, usb fleš drajv, smart kartice, digitalne kamere, mobilni uređaji, eksterni drajvovi, štampači, digitalne sekretarice, modemi, ruteri swicthevi habovi, serveri,

---

195 Forensic Science Communications (FBI), Scientific Working Group on Digital Evidence (SWGDE)International Organization on Digital Evidence (IOCE), http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/, 01.11.2015.

196 Za uklanjenje šifri ili enkripcije sa fajlova koriste se za to specijalizovani alati. Za uklanjanje šifri sa fajla koristi se Winhex editora. Jedan od specijalizovani alata koji može oporaviti šifru ili je zaobići je *Passware Kit Forensic*. Za zaobilaženje šifara za logovanje koristi se program *ntpasswd ili ERD commander*. LC4 može pogoditi šifre starijih NT sistema. Forenzički jedan od najmoćnih alata su *PRTK i DNA* kompanijie AccessData. Postupak oporavka zaštićenih fajlova je veoma kompleksan i spada deo posebne forenzičke oblasti koja nije predmet ove knjige. Videti: Passware Kit Forensic, http://www.lostpassword.com/kit-forensic.htm, 22.04.2016., i http://www.password-crackers.com/en/category_117/, 22.04.2016.

mrežne kartice, gps uređaji, skeneri, dongle, pejdžer, kopir uređaji, skimeri kreditnih kartica, konzole za igranje, digitalni satovi, fax uređaji. [197]

Kada je reč o internim storidžima na kojima je moguće pronaći digitalne dokaze tu se pre svega misli na hard diskove (HDD) i SSD diskove. SSD predstavlja čip disk memoriju koja koristi mikro čipove na koju se smeštaju podaci. Zbog svoje osetljivosti, digitalni podaci se lako se mogu izgubiti. HDD predstavlja mehanički hard disk koji na svojim cilindrima smešta velike količine podataka. Za razliku od SSD-a, hard diskovi su mnogo otporniji na oštećenja. Na primer i pored strujnog udara ili požara moguće se povratiti podatke koji su se nalazili na hard disku jer je u pitanju cilindar. Njegovo uništetnje je moguće samo ukoliko se razbije na vrlo sitne delove. Postoje dva tipa mikročip memorije: NAND based flash memorija i Volatile Ram. NAND flash memorija se najčešće nalazi na SSD disku, a Volatile RAM predstavlja micro ssd koji se koristi za keširanje kod operativnih sistema (ili storidž sistema ili za swaping) sa ciljem dobijanja brzine pristupa/iščitavanja podataka. Prilikom forenzičke istrage neophodno je da forenzičar ima sa sobom adaptere za sve tipove konekcija (IDE-EIDE/ATA/SCSI/FibreChannel/USB) kada su hard diskovi u pitanju. U slučaju da je hard disk spojen preko optičkog kabla, mora se posedovati potrebna oprema koja podržava konektovanje preko optike, u suprotnom se ne može izraditi forenzička kopija hard diska.

Zato, je neophodno permanentno praćenje noviteta na polju računarskih sistema što ujedno predstavlja i preduslov valjane akvizicije dokaza sa njih. Sa jedne strane je primetan porast broja načina zaštite podataka, dok sa druge strane to otežava i usporava rad forenzičara i zahteva nova napredna znanja. *Digitalni dokaz* kao element istrage je mnogo ranjiviji od fizičkog, pa je veštom napadaču lakše da ga ukloni, a nepažljivo i nestručno vođenje istrage takođe može dovesti do gubitka ključnih podataka. Zato je praksa pokazala da digitalni forenzičar timski radi sa specijalistom zaštite da bi se obezbedila prihvatljiva zaštita računarskih sistema i bezbedan rad računarske mreže u poslovnim sistemima.[198]

O bilo kom tipu visokotehnološkog kriminala da je reč moraju se pronaći odgovori na pitanja koje digitalni forenzičar treba da postavi: ko je izvršio nedozvoljenu radnju?, kada se ona desila i kako?, zašto je delo učinjeno?, gde je mesto incidenta?, šta je bio cilj?, a na tužilaštvu je dalje da uz sve to dokaže i uzročno-posledičnu vezu između dela i učinioca kao i

197 Mane Piperevski, *Workshop ICT Forensics Investigation – module 1*, Piperevski & Associates, Beograd 2016.

198 Altheide C., Carvey H., *Digital Forensics with Open Source tools*, Elsevier, Waltham USA, 2011.

nameru da se to delo izvrši (krivicu). Odgovore na ova pitanja će pružiti *tri tipa dokaza*: vremenski dokazi (će pomoći u otkrivanju sekvenci ili obrasce u vremenskim dešavanjima i daju odgovor na pitanje „kada"), relacioni dokazi (podrazumevaju elemente nedozvoljenih aktivnosti, njihov odnos i pozicije, daju odgovor na pitanja „ko, šta i gde") i funkcionalni dokazi (pružaju uvid u to šta je moguće, a šta nije dajući odgovor na pitanje „kako").

Da bi se *prikupile sve relevantne informacije i dokazi*, bilo da su oni digitalni ili fizički, neophodno je izvršiti analizu ne samo ciljnog računara, već i onih sa kojih je pokrenuta neka nezakonita aktivnost. Takođe analiziraju se i oni računari koji su indirektno učestvovali u nedozvoljenom delu. Kada se sve te informacije i dokazi sakupe oni se dostavljaju nadležnim organima u slučaju da je došlo do ugrožavanja državne i javne bezbednosti ili korporativnim organima ukoliko se incidentna radnja desila u njenim okvirima.

Digitalni dokazi su apstraktni i kao takvi mogu se lako izmanipulisati u smislu izmene ili njihovog uklanjanja. U ovoj knjizi u fokusu su upravo informacije od značaja za digitalnu forenzičku istragu koje se nalaze na hard diskovima u okviru računara bilo da su pod Linux ili Windows operativnim sistemom.

Na osnovu pomenutog *Lokardovog principa razmene* mogu biti proizvedeni digitalni dokazi koje možemo da svrstati u sledeće dve kategorije:[199]

1. Dokazi sa atributima koji odgovaraju grupi klasnih karakteristika - karakteristike klase ispoljavaju zajedničke osobine kada se posmatraju slični predmeti odnosno stvari. Mogu biti povezani samo sa grupom izvora a ne samo sa jednim izvorom.[200]
2. Dokazi sa atributima koji pripadaju grupi individualnih karakteristika - pojedinačne karakteristike su jedinstvene i mogu povezati izvršioca sa većom sigurnošću.

Preko ovih atributa i tumačenjem njihovih karakteristika na osnovu informacija koje u sebi sadrže, digitalni dokazi se mogu razvrstavati prema pomenutim grupama. Digitalni podaci mogu biti prisutni u mnogim nivoima apstrakcije tako da je od značaja na koji način će se vršiti klasifikacija. Na primer, neki slučajevi zahtevaju pregledanje image-a diska sa hex editorom, a u nekim slučajevima je više odgovarajuće procesiranje samog fajl sistema kroz prikazivanje fajlova i foldera.

Na osnovu klasne karakteristike dokaza istražitelji mogu na primer da otkriju da li je korišćen određeni web server (npr. Apache) ili ftp server (npr.

199 Ansonand S., Bunting S., Mastering Windows Network Forensics and Investigation, Sybex, 2007.

200 Carvey H., *Pearl scripting Live Response*, Forensic Analysis, and Monitoring, Syngress Publishing, Inc 2007.

Vsftpd). Osim toga mogu otkriti prizvođača mrežne kartice koju je koristio napadač ili mail server (npr. Sendmail) ili koja se šema enkapsulacije koristila pri slanju maila (npr. MIME eng. Multipurpose Internet Mail Extensions preko koje možemo saznati da li postoje attachmenti, koji tip podataka se nalazi, koji format originalnog fajla je u pitanju itd.). Klasne karakteristike digitalnih objekata mogu da ukažu na strukturu podataka, opšte vrednosti kao što su vreme ili veličina.

Individualne karakteristike podrazumevaju jedinstvene identifikatore formata datoteka i njenog rasporeda, te mogu biti klasifikovane na osnovu tipa u inodu (ili druge meta data strukture) ili ekstenzije datoteke.

Značaj *Lokardovog principa razmene,* klasnih karakteristika i individualnih karakteristika u digitalnom okruženju, može se prikazati na primeru upada na računar. Kada napadač dobije neovlašćeni pristup Linux sistemu sa njegovog računara koristeći ukradeni dial-up nalog i ako uploaduje različite programske alate na Linux računar preko FTP servera (eng. File transfer protocol). Programski alati se nalaze i na Linux i na Windows računaru. Određene karakteristike ovih alata će biti iste na oba sistema uključujući vremenske pečate i SHA-1 ili SHA-256 hash vrednosti. Forenzičar mora poznavati karakteristike operativnog sistema sa kojim vrši heširanje prikupljenog imidža, jer se može desiti da kernel do (i uključujući) verzije 2.4 ne može pristupiti poslednjem sektoru particije na hard disku ukoliko on ima neparan broj sektora.[201] To za posledicu može da ima dobijanje različite heš vrednosti od one dobijene sa kernelom 2.6 baš kao što je Jesse D. Kornblum objavio u svom radu „The Linux Kernel and the Forensic Acquisition of Hard Disks with an Odd Number of Sectors".

Windows aplikacije koje se koriste za povezivanje na Linux (Putty, Secure CRT, Telnet, Tunnelier) mogu posedovati zapis o ciljnoj IP-adresi računara ili njegovom imenu. Na računaru napadača moguće je pronaći i listing direktorijuma sa Linux računara, (odnosno računara koji je napadnut) dok ih je program npr. Putty prikazivao na ekranu u nekom sesijskom fajlu. Ukradeni nalog i šifre su smešteni u operativnom sistemu napadačevog računara tj. najverovatnije u nekom programu tipa sniffer. Isto tako ftp serveri u svojim logovima skladište podatke o razmeni fajlova, tako da se može utvrditi koje alate je prebacivao napadač na ciljani računar čime se potvrđuje veza između napadača i napadnutog računara.

Kada digitalni forenzičar preuzme *ispitivanje digitalnog dokaza*, prave se dve forenzičke kopije za dalju analizu. Dve forenzičke kopije se kreiraju istovremeno i na njih se primenjuje heširanje sa SHA-1 ili SHA-256

201 National Policing Improvement Agency, *Core Skills in Data Recovery & AnalysisCourse Reference* Book V2.01, Bradford, UK, 2007.

algoritmom da bi se sačuvao integritet (nepromenjivost) digitalnog dokaza. Jedna kopija se izdvaja i povezuje na forenzički računar da bi se nad njom vršila analiza i ispitivanje. Druga kopija služe kao rezervne kopije (backup) za bilo koji nepredviđeni slučaj, a može poslužiti i u analizi pod virtuelnim okruženjem. Rad na originalnim dokazima može se izvoditi *ako i samo ako situacija nalaže i sud odobri* i samo u tom slučaju takav digitalni dokaz može biti validan na sudu, u suprotnom rad na originalnom dokazu smatra se kao kršenje forenzičke procedure i takav dokaz nije prihvatljiv na sudu.

Potrebno je ukazati i na određena *pravila* koja su se kroz praksu pokazala kao vrlo korisna: digitalni forenzičar mora da svede mogućnost ispitivanja originalnog dokaza na najmanju moguću meru, mora poštovati pravila koja se odnose na dokaze, treba da radi u okviru svojih stručnih znanja i ovlašćenja i da dokumentuje bilo kakvu promenu na dokazu.

2.4. PRIKUPLJANJE PODATAKA

U korporativnom okruženju, u slučaju da je organizacija sama sprovela proceduru forenzičkog prvog odgovora (eng. First incident response) koja se odnosi na prikupljanje digitalnih podataka, prvo treba istražiti da li je procedura forenzičkog prvog odgovora izvedena u skladu sa best practice procedurom za first incident response, kako ne bi bio ugrožen integritet digitalnih dokaza. Na osnovu prikupljenih podataka digitalni forenzičar kao stručno lice sa sertifikatom će sprovesti postupak analize digitalnih dokaza kako bi dao odgovor na određena ključna pitanja koja se odnose na nastalu nedozvoljenu aktivnost. To je zapravo slučaj kada licencirani ekspertski veštak iz oblasti digitalne forenzike stupa u kontakt sa digitalnim dokazima koji su već prethodno prikupljeni u organizaciji (na primer digitalni dokazi prikupljeni su od strane sistem administratora) gde je nedozvoljena aktivnost nastala. Ukoliko se nisu ispoštovale best practice procedure za prikupljanje digitalnih dokaza neće se znati da li je to zaista digitalni dokaz ili „izmenjeni" digitalni dokaz. Zato je jako važno da prikupljanje podataka izvede stručna i ovlašćena osoba ili tim koji će to procesirati na forenzički ispravan način.

Nije retko da digitalni dokazi mogu da budu uništeni potpuno nenamerno. Kao primer biće naveden slučaj gde je izvršena zloupotreba kreditnih kartica u kome je zlonamerni napadač iskopirao sadržaj kreditnih kartica i kreirao falsifikat. Kreditna kartica koja nema čip na sebi sadrži magnetnu traku i na njoj su smešteni podaci (ime prezime, broj računa kontrolni broj) neophodni da bi se ostvarila tansakcija zajedno sa PIN

brojem. U praksi kada se procesira nedozvoljena aktivnost koja se odnosi na falsifikovanje kreditnih kartica postupak može trajati i po nekoliko godina, skladištenje digitalnog dokaza je u tom slučaju od velikog značaja. Kako u ovom slučaju digitalni dokazi predstavljaju same falsifikate kartica oni moraju biti uskladišteni i čuvani na određeni način (izolovane i udaljene od uređaja sa elektromagnetnim zračenjem). Lošim čuvanjem mogu se izgubiti informacije. Na primer kada se dve kartice poklope jedna preko druge, na takav način da su licem prema licu okrenute magnetne trake jedna prema drugoj, podaci se na njima mogu izgubiti nakon 6 meseci, odnosno doći će do narušavanja integriteta digitalnog dokaza i neće se moći očitati podaci sa kartice što se smatra uništenim dokazom.

Prikupljanje samih podataka moguće je realizovati forenzičkim odgovorom uživo tj. aktivnom ili post-mortem forenzikom, koja podrazumeva privremeno oduzimanje računarskog sistema, imidžovanje (uzimanje forenzičke slike bit po bit) elektronskih, optičkih i fleš diskova, akviziciju i analizu digitalnih podataka na radnom imidžu.

Digitalna forenzika "uživo" (eng. Live forensic) - podrazumeva prikupljanje podataka i analizu koja se sprovodi nad originalnim dokazima. S obzirom da je to momenat gde se spaja forenzika sa bezbednosnim elementima i zaštitom koja je jedan od tih elemenata, forenzički odgovor "uživo" biće predmet posebnog razmatranja.

U post-mortem forenzičkom prikupljanju postoji nekoliko načina izrade kopija i duplikata digitalnog dokaza uz pomoć specijalnih alata za te namene:

- kopija (eng. copy) - uključuje samo informacije o datotekama iz fajl sistema, ne i iz slack ili neiskorišćenom prostora i o vremenskim oznakama. Prema tome klasično kopiranje ne zadovoljava zahteve digitalno forenzičke istrage;
- *rezervna ili mirror kopija* (eng. *backup*) - datoteke kopirane za buduću restauraciju sistemskih ili programskih podataka, služe kao sigurnosna kopija (npr. ISO image). Ovaj način očuvanja dokaza zasniva se na metodi kopiranja svih podataka na disk, što predstavlja mirror kopiju (eng. *mirror image*). Ova kopija može, a ne mora predstavljati identičnu kopiju originala, zato što se ona najčešće koristi samo kao sigurnosna kopija (eng. *backup*). U složenijim situacijama *mirror image* se ne tretira kao forenzička kopija, jer ne zadovoljava sve zahteve digitalno forenzičke istrage;
- *forenzička kopija bitsream image* (bit-po-bit, sektor-po-sektor kopija, disk-to-file, disk-to-image*)* - ova kopija predstavlja egzaktnu

repliku svih sektora tj. forenzički duplikat originalnog hard diska. Rad na njemu se smatra kao rad na originalnom računaru. Metodom dr reprodukuju se podaci, kopirajući svaki bit, jedinice i nule, od početka do kraja (bez brisanja ili bilo kakve izmene podataka) medija u jedan logički fajl tj. *imidž*. Takođe se kopiraju i slobodni i nealocirani prostori na disku, jer se na njima često nalaze izbrisani podaci. Prave se obavezne dve forenzičke kopije – jedna radna i jedna referentna za dokazivanje integriteta ispitivanog hard diska pred sudom. Dve forenzičke kopije kreiraju se u istom trenutku odjednom, a ne jedna za drugom (svakim paljenjem hard diska povećava se rizik od gubitka integriteta digitalnog dokaza) i to sa hardverskim blokatorom upisa koji ima mogućnost samo jednosmernog prenosa podataka tj. isčitavanja.

Bitstream disk-to-image je i *najčešće korišćena metoda u praksi*. Alati kojima se prave forenzičke kopije su: *EnCase*,[202] *AccessData FTK*,[203] *SMART*,[204] *Sleuth Kit*,[205] i *Look*.[206] Postoje različiti formati forenzičkih bitstream kopija. To može biti raw format ukoliko je urađena kao jedan imidž fajl i takav format je kompatibilan sa svim forenzičkim alatima. Sa druge strane komercijalni vendori kreiraju svoje formate forenzičkog imidža na primer AccessData FTK ima svoj format (.AFF), Encase ima svoj format (.E01) dok se format AFF može upotrebiti i na komercijalnim alatima.

- *forenzička kopija bistream disk-to-disk* - replicira sadržaj medija (diska) direktno na drugi medijum (disk). Izvodi se kada nije moguće uraditi bitstream image kopiju. Prilikom izvođenja ovog postupka treba voditi računa o geometriji i CHS (Cylindar-Head-Sector) konfiguraciji diska na koga se kloniraju originalni podaci. Ovaj način zahteva postojanje medija sličnog originalu, forenzički čistog, sa većim kapacitetom nego originalni medijum.[207] Alati kojima se izvodi bitstream disk-to-disk su: *AccessData FTK*, *EnCase*,

202 Http://www.guidancesoftware.com/encase-forensic.htm, 02.03.2016.
203 Http://www.accessdata.com/, 02.03.2016.
204 SMART for Linux software, http://www.asrdata.com/forensic-software/smart-for-linux/, 02.03. 2016.
205 Open Source Digital Forensics, http://www.sleuthkit.org/, 02.03.2016.
206 ILook Investigator, http://ilook-investigator.software.informer.com/, 02.03.2016.
207 National Institute of Justice, *Electronic Crime Scene Investigation*. A Guide for First Responder, 2001, https://www.ncjrs.gov/pdffiles1/nij/187736.pdf, 11.07.2016.

SafeBack,[208] i *OSFClone*.[209] Treba reći da alat Norton po difoltu pravi imidž koji nije forenzički, kopiraju se podaci sa jednog na drugi hard disk ili sa jednog harda disk u imidž fajl, ali ne pravi egzaktnu repliku svih klastera tako da se takav output ne može koristiti kao forenzička kopija originalnog dokaza.[210] Kreiranje bitstream kopija (disk-to-image ili disk-to-disk) su vremenski zahtevne operacije za izvođenje. Zato se u forenzičkoj praksi nakon kreiranja bitstream kopije kreira i bekap nad kojim se vrši pretraga i analiza koja je nije vremenski zahtevna. Ukoliko se na bekapu pronađu tražene informacije, nad bistream kopijom se izvršavaju forenzičke procedure da bi raspakovao tačno određeni deo u okviru bitstream kopije i sve se dokumentuje. Na taj način se dobija ušteda vremena potrebnog za forenzičku analizu.

Kada se radi bitstream kopija neophodno je imati uređaj istog kapaciteta kao originalni. Na primer ako je originalni hard disk veličine 2TB a poseduje 400 GB podataka bit strim kopija biće 2 TB a ne 400 GB jer se replicira svaki memorijski sektor sa originalnog digitalnog dokaza. Dve bit strim kopije predstavljaju digitalne dokaze. Jedna digitalna forenzička kopija se u antistatic vrećici deponuje u sef posebne namene, dok će druga kopija biti namenjena forenzičkoj istrazi. U novije vreme vrši se moderniji pristup kada je reč o skladištenju podataka sa originalnog dokaza. Ne koriste se hardverski ekvivalenti za kreiranje bitstream kopije sa originalnog hard diska već se bitstream kopija direktno prenosi i čuva na internom cloud sistemu. U pitanju je serverski sistem koji sa forenzičkog bridža, koji sadrži write blokator funkcionalnost, na koji je konektovan originalni digitalni dokaz (hard disk) prikuplja podatke kroz lan mrežu i zapisuje na interni storidž tj. cloud. Kao rezultat ove aktivnosti na forenzičkom internom cloud-u snimiće se imidž fajl koji predstavlja egzaktnu repliku originalnog digitalnog dokaza. Sa aspekta očuvanja integriteta digitalnog dokaza prilikom kreiranja kopije digitalnog dokaza vrši se heširanje dobijenog imidža i heširanje originalnog digitalnog dokaza i te dve vrednosti heša moraju biti identične. Na taj način se potvrđuje forenzička ispravnost kopije digitalnog dokaza. Ukoliko je potrebna još jedna bitstream kopija originalnog dokaza (u slučaju da je radna kopija kompromitovana) kreiraju se nove kopije i izvodi sa deponovane kopije ali ne sa originala. Prilikom izrade treće kopije ponovo se mora odraditi heširanje da bi se potvrdio integritet. MD5 heš algoritam više nije u standardu i koriste se SHA-1, SHA-256.

208 Http://www.forensics-intl.com/safeback.html, 02.03.2016.

209 Http://www.osforensics.com/tools/create-disk-images.html, 02.03.2016.

210 Https://support.symantec.com/en_US/article.TECH106937.html, 08.08.2016

U slučajevima nedozvoljenih aktivnosti npr. bezbednosnih incidenata, pravilno prikupljanje relevantnih podataka može povećati verovatnoću dolaska do informacija o tome ko je izvršilac, gde je izvršena nedozvoljena aktivnost i na koji način je ona izvršena.

Pre izvršenja forenzičke duplikacije digitalnih dokaza veoma je važno da se digitalni forenzičar upozna sa *podacima iz BIOS-a* računarskog sistema, koji je predmet istrage da bi odredio osnovnu geometriju hard diska (evidentiranje parametra vezanih za maksimalni kapacitet, broj cilindara, glavu i sektor ispitivanog hard diska) na kompromitovanom računaru i utvrdio but sekvencu (eng. boot sequince) na njemu.

Kada je u pitanju forenzička duplikacija u literaturi su dominantni pristupi koji se uglavnom realizuju sa *forenzičkim alatima* AccessData FTK, [211] Encase,[212] Diskpro Clone-N-Recover,[213] SafeBack,[214] ASR Data SMART for Linux,[215] DD za Linux[216] i DD za Windows.[217] U principu *DD komanda* je ugrađena u gotovo sve savremene forenzičke alate.

Prvi pristup počinje nakon preuzimanja originalnog hard diska iz ispitivanog računara i njegovog povezivanja na forenzičku radnu stanicu. Potom se pravi *slika* (eng. *image*) *originalnog hard diska* koristeći pomenute forenzičke alate. Izuzetno je važno da se dokumentuju svi detalji vezani za hard disk kao što su serijski broj, pozicije džampera (eng. jumpers) na hard disku, vidljiva oštećenja i neke druge specifične karakteristike.

Drugi pristup jeste pravljenje *slike hard diska* (ili eksternog hard diska ili uređaja za skladištenje podataka), koja će biti preneta na forenzičku radnu stanicu putem zatvorene mreže ostvarene isključivo između ispitivanog uređaja i forenzičke radne stanice. Ove specijalne forenzičke mreže koriste se u slučaju masovnih istraga na više distribuisanih lokacija u kojima učestvuje više digitalnih forenzičkih istražitelja, za uzimanje imidža osumnjičenih računara na terenu i njihovo slanje u forenzičku laboratoriju. Ova veza može da se realizuje na osnovu point-to-point interfejsa između ispitivanog sistema

---

211 Forensic Toolkit (FTK), AccessData, http://accessdata.com/products/computer-forensics/ftk, 27.04.2016.

212 Guidance Software, http://www.guidancesoftware.com/forensic.htm, 27.04.2016.

213 E-mart.com, http://www.e-mart.com/www/index.html, 27.04.2016.

214 Http://www.forensics-intl.com/safeback.html, 27.04.2016.

215 SAW (SMART Acquisition Workshop), ASR Data, http://www.asrdata.com/forensic-software/saw/, 27.04.2016.

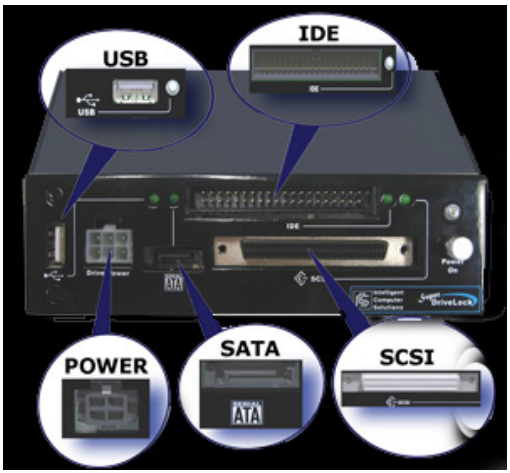
216 Linux / Unix Command: dd, http://linux.about.com/od/commands/l/blcmdl1_dd.htm, 27.04.2016.

217 Dd for windows, dd - convert and copy a file, chrysocome.net, http://www.chrysocome.net/dd, , 27.04.2016.

i forenzičke radne stanice putem mrežnog sviča ili ukrštenim mrežnim kablom (cross-connect cable).

Koji god da se pristup primeni potrebno je koristiti hardverske *blokatore upisa* (eng. write blockers) *na hard disk*. Treba koristiti blokatore prihvatljive od strane NIST organizacije.[218]

Svaki preduzeti proces treba dokumentovati i uraditi kao što je već pomenuto čeksum SHA1 i SHA-256 nad originalnim digitalnim dokazom i nad dobijenom slikom. Tako se pouzdano pred sudom može dokazati integritet i autentičnost dobijenog digitalnog dokaza.[219] Prema tome, iz forenzičkog ugla primarni cilj jeste prikupljanje podataka iz računarskog sistema, ali krajnji cilj jeste obezbeđivanje dokaza koji će biti priznati na sudu. Ukoliko se vrši istraga na računarskom sistemu u smislu kreiranja bit-stream kopije bez upotrebe hardverskog write-blockera i ne izvede se heširanje bit-stream kopije, to automatski znači kršenje zvanične procedure, što za posledicu može proizvesti da dokaz ne bude prihvatljiv za sud. Hard disk jeste preuzet, kreirana je forenzička kopija originalnog dokaza, ali procedura nije ispoštovana i integritet digitalnog dokaza je bio ugrožen. To za posledicu može imati promenu bita i na osnovu toga heš vrednost forenzičke kopije i originalnog dokaza se može razlikovati i takav dokaza neće biti prihvatljiv za sud.



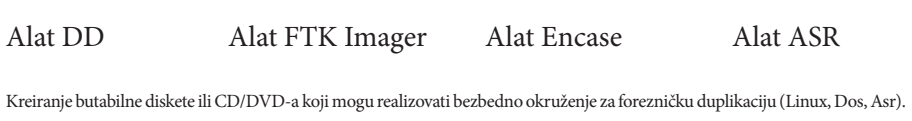
Slika 3. Hardverski blokator upisa Agape SuperDrive Lock[220]

218 The National Institute of Standards and Technology (NIST), http://www.nist.gov/index.html, 27.04.2016.

219 Primer za softverske blokatore je SAFE Block, a za svaki operativni sistem postoji posebno namenjena verzija. Videti: http://www.forensicsoft.com/, 27.04.2016.

220 Http://www.agapeinc.in/visitforensicsite.php, 03.03.2016.

Na sledećoj je prikazna ilustracija postupka forenzičke duplikacije:



Kreiranje butabilne diskete ili CD/DVD-a koji mogu realizovati bezbedno okruženje za forezničku duplikaciju (Linux, Dos, Asr). Kreiranje forenzičke slike originalnog diska dd, Encase, FTK, ASR, Safeback ili nekim drugim alatima. Kao rezultat dobija se fajl sa ekstenzijama pripadajućih alata koji su ga kreirali na primer .dd, .E00, .s00, .SFB. Nakon kreiranja forenzičke slike, vrši se njeno vraćanje (eng. restore) na drugi hard disk u bezbednom okruženju da bi se izvršila forenzička analiza sadržaja forenzičkim alatima.

Slika 4. Postupak forenzičke duplikacije

Takođe treba naglasiti da forenzička duplikacija računarskih sistema može biti neadekvatna u određenim okolnostima u smislu previše potrebnog vremena i adekvatnosti u operativnom smislu kada je reč o prikupljanju podataka. Na primer, dupliranje velikih terabajtnih diskova ili RAID diskova ili prostora za skladištenje u *cloud computing* sistemima, gde se čuvaju velike količine digitalnih podataka (tzv. *Big Data*). U ovakvim slučajevima uzimaju se selektivno imidži onih particija koje sadrže podatke navedene u osnovanoj sumnji za pokretanje istrage.

Dokazi su u većini slučajeva u apstraktnom obliku. Apstraktni dokazi su uglavnom u binarnoj formi predstavljeni 0 i 1. Skup binarnih brojeva sačinjava niz kojim mogu da se opišu folderi, fajlovi koji mogu biti dokumenta, slike, aplikacije. Ovi digitalni dokazi su izuzetno *nestabilni* (lako promenljivi, „isparljivi podaci" eng. volatile), jer mogu da se lako uklone, izmene ili nestanu, što u dokaznom postupku može predstavljati veliki problem. Prema definiciji US-CERT (The United States Computer Emergency Readiness Team) volatile podaci predstavljaju one podatke koji se čuvaju u memoriji, ili postoje u tranzitu a koji će biti izgubljeni kada računar ostane bez napajanja ili se isključi. [221] Međutim, ti podaci mogu i da se sačuvaju ukoliko digitalni forenzičar pravovremeno odreaguje.

Posebno kada se *podaci prikupljaju iz "živog" operativnog sistema* važno je znati koji su to podaci promenljivi tj. podaci privremenog karaktera (eng. volatile), a koji podaci su postojanog karaktera (eng. non-volatile). Na prvom mestu "lako izmenjivih" podataka odnosno volatile podaci, su sistemski

221 The US-CERT (United States Computer Emergency Readiness Team), http://www.us-cert.gov/, 02.06.2016.

detalji koji istražiteteljima pružaju uvid u način i prirodu kompromitovanja sistema i nekada mogu biti podaci od krucijalnog značaja. Na primer, to su detalji koji pružaju informaciju o tome ko je logovan na sistem, aktivne mrežne konekcije i pokrenuti procesi na sistemu.[222] Na drugom mestu su podaci koji su po prirodi privremenog karaktera, ali su korisni istražitelju, jer može dopuniti informacije o sistemskim detaljima. Na primer, podaci iz privremene memorije (eng. clipboard) i podaci iz planiranih zadataka za pokretanje na sistemu (eng. scheduled tasks).

Od *podatka koji neće lako biti izmenjeni* na sistemu na prvom mestu su oni koji daju informacije o statusu, setovanjima i konfiguraciji sistema, na osnovu kojih se može utvrditi način kompromitovanja sistema. Na primer, tu su setovanja registra (eng. registry) i auditinga (praćenje tragova aktivnosti na sistemu). Na drugom mestu neizmenjivih podataka su oni podaci koji pružaju istorijske informacije i dodatni kontekst za razumevanje načina i prirode kompromitovanja sistema. Na primer to mogu biti podaci iz logova događaja (eng. event log) i iz istorije internet pretraživača (eng. Web browser history).

Veoma je važno da se *inicijalni tookit* (skup alata) dobro pripremi. To podrazumeva korišćenje pozdanog toolkit-a za inicijalni odgovor koji sadrži pouzdano kreirane binarne izvršne datoteke, pokretanje komandi sa pouzdanog mediuma koji mogu da se pokreću iz komandnog okruženja. Pri kreiranju inicijalnog toolkita treba obratiti pažnju da li se neke binarne datoteke oslanjanju (eng. dependencies) na biblioteke ili zavise od nekih drugih fajlova. U nastavku biće navedeni osnovni alati koji su neophodni pri inicijalnom odgovoru.

Na osnovu iznete klasifikacije izmenjivih i neizmenjivih podataka biće prikazani specifični *tipovi izmenjivih podataka* koji su veoma značajni za forenzičku analizu. To su: sistemsko vreme, ulogovani korisnici, otvoreni fajlovi, informacije o mreži, mrežne konekcije, informacije o procesima, status mreže, sadržaj privremene memorije za skladištenje (eng. clipboard), mapiranje procesa na portove, procesi u memoriji, spisak servisa, istorija pokrenutih komandi, mapirani drajvovi, deljeni resursi na mreži (eng. shares).

Za svaki od ovih tipova izmenjivih podataka postoje određeni alati

222 Harms K., *Forensic Analysis of System Restore Points in Microsoft Windows XP*, Mandiant Corporation, 2006, http://citeseerx.ist.psu.edu/ viewdoc/ download?doi=10.1.1.84.4474&rep=rep1&type=pdf, 22.06.2016.

koji mogu poslužiti da bi se ovi podaci dobili iz sistema.[223] [224] Prilikom prikupljanja podataka redosled prikupljanja treba prilagoditi prema karakteru postojanosti podataka. To znači da podaci koji su skloniji brzim promenama trebaju biti sačuvani na prvom mestu. Očekivani vek trajanja podataka u zavisnosti od postojanosti podataka dat je u sledećoj tabeli:

Tabela 4: Očekivani vek trajanja podataka[225]

Tip podataka	Vek trajanja
Registri, periferna memorija, keš	Nanosekunde
RAM memorija	10 nanosekundi
Mrežno stanje	Milisekunde
Startovani procesi	Sekunde
Disk	Minuti
Flopi drajv i drugi mediji za bekap	Godine
Cd-rom, Dvd-rom, odštampani papiri	Desetine godina

Treba skrenuti pažnju da čak iako postoji plan i inicijalni toolkit za odgovor, odgovor „uživo" može da bude prilično dugotrajan. Takođe inicijalni odgovor može da bude pun izazova za onog ko ga izvodi zbog postojanja različitih nepravilnosti koje moraju biti prepoznati na vreme.

Izuzetno je važno da digitalni dokazi, koji se iznose *pred sud* budu u *originalnom zapisu*. Zabranjeno je eksperimentisanje, menjanje ili testiranje nad dokazima dok traje istraga. Upravo zato služe kopije digitalnih dokaza nad kojima se mogu sprovoditi istražni postupci od strane digitalnog forenzičara i koji se ne iznose pred sudske organe.

Najčešće greške koje mogu da se jave prilikom prikupljanja podataka su sledeće:

-izmena vremenskih pečata (eng. timestamps);

-zaustavljanje zlonamernih procesa na računarskom sistemu;

-instaliranje zakrpa na sistemu (eng. patching) pre izvršene istrage nad sistemom;

-ne evidentiranje izvršenih komandi na sistemu;

223 Harris R., *Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem*, Journal Digital Investigation: The International Journal of Digital Forensics & Incident Response, vol. 3, 2006, str. 44-49.

224 Harrison W., Heuston G., Morrissey M., Aucsmith D. Mocas S., Russelle S., *A Lessons Learned Repository for Computer Forensics*, International Journal of Digital Evidence, Vol. 1 No. 3, 2002, http://www.ijde.org /docs/ 02_fall_art2.html, 23.06.2016.

225 Home page The United States Department of Justice, *Reporting Computer related crime,* http://www.justice.gov/criminal/cybercrime/intl.html, 25.06.2016.

-korišćenje nepouzdanih komandi i binarnih fajlova;

-upisivanje preko potencijalnih dokaza u vidu instaliranja programa na originalnim dokaznim medijima (na primer hard disk), pokretanje ili izvršenje programa koji čuvaju svoje izlaze (eng. output) na originalnom dokazu.

U praksi se dešava da nije moguće uraditi forenzičku kopiju, jer je u upotrebi stari IKT sistem na primer storidž sistem sa hot swap diskovima kod koga nije moguće izvršiti replikaciju raida (izvađeni hard diskovi se nemaju gde postaviti da bi se simulirao identičan raid i izvukli podaci). U tom slučaju vrši se direktan pristup live sistemu i live forenzička istraga nad originalnim dokazima, *ali samo ukoliko je to prethodno dozovljeno od strane suda*. U tom slučaju od suštinske je važnosti da se o svakoj sprovedenoj aktivnosti mora imati dokumentovan trag i to se radi samo jedanput. U praksi se dešava da organizacije imaju bekapovane informacije na trakama i da ih čuvaju više od decenije. Međutim, kako se vremenom osavremenjivala oprema koja je služila za kreiranje i očitavanja bekapa, ukoliko postojeći podaci nisu migrirani na trake ili u oblik koji je čitiljiv uređajima koji su trenutno aktivni, ti bekapi praktično postaju beskorisni, jer ne mogu da se očitavaju na novijim uređajima za bekap. I to je problem sa kojima se danas organizacije suočavaju.

Ovde treba spomenuti termin *"lanac očuvanja nadležnosti" COC* (eng. chain of custody). U literaturi se može još naći i termini poput „*kontinuitet dokaznog materijala*" ili "lanac nadzora", koji predstavlja izuzetno važan proces kojim se prati kretanje dokaza kroz prikupljanje, čuvanje i analizu njegovog životnog ciklusa do momenta kada su prezentovani u sudskom postupku. COC se odnosi na to gde je bio digitalni dokaz, ko je posedovao digitalni dokaz, ko je radio na digitalnom dokazu, zašto i šta je sa digitalnim dokazom rađeno.[226] Ovim procesom se evidentira svaka osoba koja u nekom određenom momentu obrađuje dokaze, uključuje se datum i vreme kada su prikupljeni, preneseni dokazi kao i razlog prenošenja, broj slučaja i broj dokaznog predmeta. Svaki put, ukoliko se dokaz premešta od jedne osobe do druge ili sa jednog medija na drugi to mora biti evidentirano. Može se desiti da više digitalnih forenzičara imaju pristup originalnom dokazu i ukoliko se ne zna ko je bio sve u dodiru sa dokazom i šta je rađeno, neće se znati ko je odgovoran u slučaju kompromitovanja originalnog dokaza. Prekid COC može dovesti u sumnju da je dokaz izmenjen, zamenjen ili falsifikovan odnosno zloupotrebljen. Ono što se može uočiti kao problem jeste nemogućnost konstantnog prisustva jedne osobe koja prati dokazni materijal od njegovog

226 Prlja D., Reljanović M., *Pravna informatika*, Pravni fakultet Univerziteta Union, Beograd, 2014.

prikupljanja sa lica mesta do njegovog prezentovanja na sudu. Praksa je pokazala da se to može prevazići *kreiranjem potvrda iz forenzičkih laboratorija* po prijemu dokaznog materijala na ispitivanje. Forenzičke laboratorije izdaju odgovarajuću potvrdu u momentu isporuke rezultata čime se obezbeđuje *integritet dokaza*. U slučaju kada se u proces uključuje i forenzička laboratorija, neophodno je i svedočenje forenzičara ili laboranta o načinu na koji je dokazni materijal skladišten i zaštićen u laboratoriji za vreme ispitivanja. Bolje rešenje može biti ako se svaki pristup ispitivanom imidžu *verifikuje uzimanjem heš vrednosti*, koja mora biti istovetna kao originalna heš vrednost imidža. Ne podudaranje heš vrednosti sa originalnom u bilo kojem koraku istrage, znači prekid COC, što može dovesti u sumnju da je dokaz izmenjen, zamenjen ili falsifikovan, odnosno zloupotrebljen.

Pored digitalnih postoje i *fizički dokazi*, koji mogu biti prikupljeni na incidentnom mestu i koji mogu imati dokaznu vrednost u smislu da se na tom mestu nalazilo osumnjičeno lice. Ovi dokazi pružaju potvrdu o povezanosti određenog uređaja i osumnjičenog koji je sprovodio nedozvoljenu radnju.

Za opis incidenta pojedinačni dokazi se moraju kombinovati kako bi se izgradio čvrsti i neoboriv dokazni materijal pred sudom. Od izuzetne je važnosti da se svi originalni dokazi, deponuju u sefove, ili da se čuvaju u skladištima za posebne namene. U zavisnosti od osetljivosti incidenta potrebno je da se uvede zabrana fizičkom pristupu mestu incidenta, svima osim digitalnim forenzičarima i ovlašćenim istražiteljima. Ove mere se preduzimaju da se ne bi ugrozio proces istrage (sa ciljem da se izbegne slučajno ili namerno kompromitovanje ili uništavanje prikupljenih dokaza). U suprotnom može doći do uništenja dokaza, a samim tim bi i uspeh kompletnog istražnog postupka bio ozbiljno doveden u pitanje. Osnovno pravilo je da svi dokazi moraju biti adekvatno dokumentovani, a lica koja njima pristupaju moraju imati utvrđenu odgovornost kada nad njima vrše ispitivanja.

Lica koja imaju mogućnost *sprovođenja ispitivanja i izvođenja digitalnih dokaza* možemo podeliti u tri kategorije:

1. *Istražitelji* - koriste veliki broj forenzičkih alata i tehnika, a uglavnom su zaposleni u nadležnim inspekcijskim i kontrolnim organima;
2. *Profesionalci informaciono komunikacionih tehnologija* - koriste mali broj forenzičkih alata i tehnika i to uglavnom iz njima stručne oblasti. Zaposleni su u organizacijama: klasični informatičari u IT odeljenjima, kao što su administratori sistema i mreža, inženjeri mrežne infrastrukture, specijalisti zaštite, administratori zaštite računarskih sistema, administratori zaštite računarskih mreža, procenitelji rizika

itd. Oni koriste elementarne forenzičke alate komandne linije (DOS komande ili Linux komande). U Win XP OS ima najmanje 100 DOS komandi, koje se mogu aktivirati i koristiti kao odličan forenzički alat. To je i prva kategorija forenzičkih alata. Inače forenzički alat je sve što forenzičaru može poslužiti za otkrivanje digitalnog dokaza (uporedivo je sa oružjem u ratu);

3. *Timovi* - koriste veliki broj alata i tehnika, imaju sposobnost da odgovore na širok spektar računarskih incidenata. Od specijalista zaštite i informatičara i drugih lica iz organizacije (pravnika, HR specijalista, fizičkog obezbeđenja) formiraju se timovi za upravljanje rizicima i upravljanje računarskim incidentom. Ovi timovi se angažuju po potrebi. Svaki član tima obavlja redovne zadatke, a uključuje svoje kompetencije kad se zahteva npr. neophodna godišnja detaljna analiza rizika (prema ISO/IEC 27001 ISMS standardu) u slučaju incidenta, kada je naneta šteta organizaciji. U oba tima mogu biti angažovani i profesionaci i pojedinci kao spoljni saradnici ili konsultanti.

2.5. ANALIZA PRIKUPLJENIH PODATAKA

Svaki tip fajla je digitalni dokaz. Fajl sistem je digitalni dokaz koji se nalazi u digitalnoj formi koja je smeštena na hard disku, prikupljeni mrežni paketi takođe predstavljaju digitalni dokaz. Forenzički gledano bitovi takođe mogu biti digitalni dokaz ali pod određenim uslovom. Na primer ako je originalni hard disk veličine 2TB, a poseduje 400 GB podataka postavlja se pitanje da li preostalih 1.6 TB podataka koji predstavljaju slek odnosno „prazan prostor“ mogu biti digitalni dokaz. Taj „prazan prostor“ zapravo nije prazan, jer se na njemu nalaze određeni podaci (bajtovi) koji nose informacije od obrisanih fajlova. Ovi obrisani fajlovi se mogu tačno rekonstruisati ukoliko se mogu identifikovati hederi fajlova i ukoliko je moguće uraditi carving svih bajtova sadržaja određenog fajla, tako da on ne bude oštećen. U tom slučaju to može biti prihvatljiv digitalni dokaz za sud. Ukoliko su prikupljeni slučajni bajtovi koji sadrže listu šifara, korisničkih naloga ili određeni tekstualni fajl koji nije u celini rekonstruisan, to se može smatrati kao fragment digitalnog dokaza, ali to neće biti prihvatljivo za sud, ukoliko se ne utvrdi autentičnost te informacije. Na primer, ukoliko je carving-om izvučen segment serijskih brojeva kreditnih kartica, to ukazuje da je vlasnik hard diska imao te brojeve u svom posedu, ali da ih je obrisao. Nakon forenzičke analize utvrđeno je da su deo tih brojeva bili upisani u delimično rekonstruisan fajl *ukradeni_brojevi_kreditnih kartica*.txt. U slučaju da forenzičar ima sa čim da uporedi fragmet toga

fajla, na primer pronađen je isti fajl *ukradeni_brojevi_kreditnih kartica.txt* na serveru koji sadrži listu serijskih brojeva kreditnih kartica koji se poklapaju sa brojevima iz rekonstruisanog fragmenta, taj digitalni dokaz može se uzeti kao prihvatljiv dokaz za sud. Carving metodom odnosno izvačenjem informacija iz praznog prostora mogu se povratiti slike, video zapisi, tekstualna dokumenta i druge vrste dokumenata.

Forenzička analiza podataka u opštem smislu može da se posmatra kao fizička i logička analiza. Fizička analiza izvodi se isključivo nad forenzičkom slikom. Ona podrazumeva pretraživanje *stringova* (eng. string), pretraživanje i raspakivanje (eng. extract) fajlova prema tipu fajlova i prema formatima, izdvajanje *slek prostora* ili praznog ili nealociranog prostora. Dokazni tragovi u vidu fragmenta informacija se mogu naći u slobodnom ili slek prostoru. *Prazan prostor* predstavlja deo fajl sistema ali koji nije dodeljen podacima. *Nealociran prostor* predstavalja prostor na hard disku koji nije dodeljen fajl sistemu. Postupak prikupljanja informacija sa hard diska iz slek prostora odnosno „praznog prostora" koje su postojale na fajl sistemu, ali su obrisane naziva se carvingom. Kada se radi carving odnosno izvlačenje informacije iz obrisanih sektora ili praznog prostora prvo što se identifikuje su hederi fajlovi. Na osnovu hedera fajlova forenzičaru je cilj da rekonstruiše fajlove. Svaki tip fajla ima svoj unikatan header. Alati sa kojima se radi carving imaju svoju bazu headera na osnovu koje identifikuju fajlove. Nakon carvinga se analizira fajl host.data. Treba obratiti pažnju na timestamp-ove koji mogu biti različiti i u tom slučaju se vrši kreiranje time frame tabele, da bi se ustanovilo tačno vreme kreiranja određenih fajlova. U hosts.data mogu se identifikovati svi startovani i aktivni procesi ispitivanog operativnog sistema.

Logička analiza obuhvata analizu svakog fajla na svim particijama. Na primer, mountovanje svake ispitivane particije u read only modu pod Linuxom, exportovanje particije putem SAMBE do forenzičke radne stanice kao i ispitivanje svake datoteke odgovarajućim programom za pregled datoteka (eng. file viewer). Tipične liste koje se kreiraju prilikom analize podataka odnose se na posećene web sajtove, email adrese kao i određene ključne reči.

Forenzička analiza podataka sa računarskih sistema podrazumeva pripremu podataka i samu analizu podataka. *Priprema podataka* podrazumeva izradu radnih kopija svih digitalnih dokaza koji mogu da se nalaze na različitim medijima. Zatim se kreira lista postojećih fajlova na sistemu. Potom se radi oporavak obrisanih fajlova i nedodeljenog prostora. U okviru pripreme podataka potrebno je proveriti potpis svakog fajla na sistemu i izvršiti identifikaciju onih fajlova kod kojih je promenjena ekstenzija (eng.

signature analysis) i identifikovati sve poznate sistemske datoteke.

Sama *analiza podataka* može da obuhvati veliki broj forenzičkih ispitivanja. Tu spada i izvlačenje elektronskih poruka i atačmenta (eng. attachments), pregledanje istorije web pretraživača, pretraga prema kriterijumu relevantnih stringova (eng. strings), pregledanje instaliranih aplikacija, analiza instaliranih programa, identifikovanje i dešifrovanje zaštićenih fajlova, detaljan pregled fajl po fajl i analiza datuma i vremena sistema i relevantnih foldera i fajlova (eng. date/time stamp).

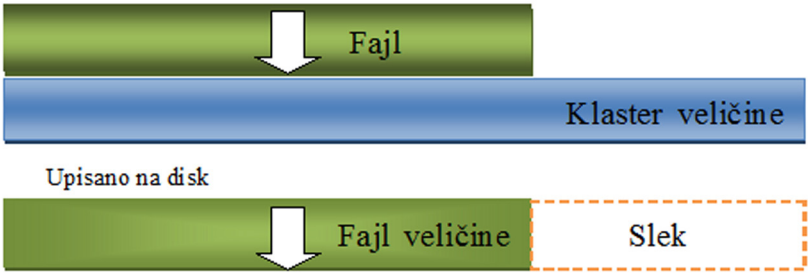
Izazov u ovoj fazi predstavlja mogućnost realizovanja brze forenzičke analize, koja može da se ostvari kroz korišćenje najnovije tehnologije i primene specijalno obučenog kadra za otkrivanje nedozvoljenih aktivnosti. Izazov mogu biti i veliki troškovi (koje bi trebalo predvideti u fazi pripreme za otkrivanje nedozvoljenih aktivnosti) koji se odnose na generisanje podataka za digitalnu forenzičku istragu ili za internu istragu u organizaciji.

Ukoliko je dobijeno dovoljno informacija koje potrvrđuju da se nedozvoljena aktivnost dogodila sledi *odluka o izvođenju forenzičke duplikacije*. Mesta koja mogu da sadrže dragocene informacije je potrebno analizirati nakon urađene duplikacije u post-mortem analizi, a to su:

- slek prostor na disku (eng. slack space);
- slobodan ili nedodeljen prostor na disku (eng. free or unallocated space);
- loši sektori na hard disku (eng. bad sectors).

Na navedenim mestima se mogu naći veoma značajni podaci kada je u pitanju forenzička istraga.

Da bi se razumelo šta je to *slek prostor na disku* najpre treba razumeti kako se disk organizuje na najnižem nivou. *Diskovi* su podeljeni u niz *staza* (eng. track). Ove staze su fabrički podeljene dalje na niz *sektora*. U jednom sektoru se upisuje *512B* (bajta) podataka. Skup sektora, zavisno od veličine hard diska, formira *klaster*. Neiskorišćeni deo prostora na hard disku u okviru klastera podrazumeva oblast od kraja datoteke (koja popunjava deo klastera) do kraja klastera kao na slici:



Slika 5. Prikaz fajla, klastera i slek prostora

Ono što treba da se primeti je da jedan fajl na operativnom sistemu Windows ima dve veličine: logičku i fizičku veličinu (kada se uradi properties nekog fajla možemo primetiti dve veličine: size i size on the disk, koje se u nekim slučajevima ne poklapaju). Razlog leži upravo u pomenutom načinu na koji fajl sistem skladišti podatke na hard disku. Bez ulaska u previše detalja o načinu rada fajl sistema odgovor na nepoklapanje fizičke i logičke veličine leži u razumevanju *fajl sleka* koji se sastoji iz dva dela: *drajv slek* i *RAM slek*. Poznavanje ovih karakteristika fajl sistema kada je u pitanju digitalna forenzika igraju važnu ulogu po pitanju forenzičke analize operativnog sistema.

Na osnovnom nivou, *sektor* (eng. sector) čini najmanju oblast hard diska na koju se mogu upisivati podaci. Ovi sektori su grupisani u *klastere* (eng. clusters). Na Windows sistemima sektori su fiksne veličine 512 bajtova (eng. bytes), dok veličina klastera zavisi od veličine samog hard diska. Manji diskovi će imati manju veličinu klastera i obrnuto.

Kad se fajlovi skladište, fajl sistem koristi fiksne veličine blokova koji se nazivaju klasteri. *Klasteri* predstvaljaju grupe sektora koji se koriste za raspodelu prostora na disku u cilju skladištenja podataka u majkrosoftovim operativnim sistemima. Znači da se svakom novom fajlu dodeljuje određen broj klastera po sledećem principu:

*Veličina fajla <= broj klastera * veličina jednog klastera.*[227]

Kada se kreira fajl, fajl sistem dodeljuje prvi raspoloživ klaster u zavisnosti od logičke veličine podataka. Očigledno je da svaki sačuvani fajl na disku ne može biti tačna veličina jednog ili više klastera tako da će ostati prostora u poslednjem klasteru. Taj prostor se naziva *fajl slek* i kreira se u vreme kada se fajl snima na disk. Na primer, ukoliko je klaster veličine 32K,

227 Chetan Gupta , File slack vs ram slack vs drive slack, http://niiconsulting.com/checkmate/2006/06/21/file-slack-vs-ram-slack-vs-drive-slack/, 12.03.2016.

a fajl koji se upisuje je veličine 10K, dodeljen prostor za fajl će biti 32K a preostalih 22K se naziva *slek prostorom*.

Već je pomenuto da *fajl slek* ima dva dela: RAM slek i drajv slek. *RAM slek* se odnosi na preostali prostor u poslednjem sektoru samog fajla (odnosno od kraja logičkog fajla do kraja sektora).[228] Fajlovi se upisuju u delovima od 512 bajtova. Veoma retko će veličina datoteke biti tačan umnožak od 512. To znači da kada fajl sistem završi upisivanje poslednjeg sektora nekog fajla pojaviće se prostor na kraju tog sektora. Do Windows 95 version B taj prostor se popunjavao slučajnim podacima iz RAM memorije, što je predstavljalo veliku bezbednosnu rupu, jer podaci iz RAMa mogu da sadrže šifre i druge osetljive podatke.[229] Od tada windows operativni sistemi ne upisuju podatke iz memorije u fajl sistem, već umesto toga upisuju u preostali prostor poslednjeg sektora fajla heksadecimalnu vrednost x00.

Termin *Drajv slek* se ne upotrebljava često.[230] Najčešće povezuje sa terminom fajl slek i odnosi se na preostale neupisane sektore u poslednjem klasteru fajla (obuhvata prostor preostalih sektora do kraja klastera). Fajl sistem ne popunjava ovaj prostor kao što se to nekad radilo sa RAM slekom i on ne čini ništa sa ovim prostorom. Ovi sektori mogu da sadrže različite tipove podataka i mogu sadržati ostatke prethodno obrisanih fajlova ili čak podatke koji su postojali pre poslednjeg formatiranja.

Uz pomoć odgovarajućih alata i sa iskustvom digitalnog forenzičara, podaci koji se nalaze u fajl sleku i nealociranom prostoru mogu biti oporavljeni. Fajl slek može biti predmet analize sa ciljem identifikovanja prethodnih radnji osumjičenog računara i može sadražati delove (eng. fragments) elektronskih poruka, dokumenata za obradu teksta i mnogo drugih osetljivih podataka, koji mogu pomoći pri otkrivanju učinioca nedozvoljene aktivnosti. Slek fajlovi mogu da postoje i na flopi disketama, zip diskovima i ostalim uređajima za skladištenje podatka na računaru. Sa forenzičke tačke gledišta fajl slek je veoma važan kao izvor potencijalnih računarskih dokaza u istrazi računrskog incidenta.

Na primer jedan od *linuxovih alata* koji se koristi za prikupljanje i oporavak podataka iz nealociranog prostora sa fajl sistema jeste alat iz TCT

228 Centar for computer forensic, *What is file slack*, http://www.computer-forensics.net/what-is-file-slack?/, 12.03.2016.

229 Solutions Centar, *The Importance of File slack to Digital Forensics and eDiscovery*, http://www.trigonit.com/tech-blog/bid/32299/The-Importance-of-File-Slack-to-Digital-Forensics-and-eDiscovery, 12.03.2016.

230 Razlog je taj što u RAM slek prostor (kao deo fajl sleka) Windows operativni sistem ne smešta podatke iz RAM memorije, pa se onda za preostali deo slek prostora umesto termina drajv sleka koristi termin fajl slek.

kolekcije koji se zove "*unrm*".[231] Drugi alat koji se takođe odnosi na podatke iz nealociranog prostora zove se *Lazarus* (iz TCT kolekcije). Ovaj alat analizira sirove podatke prikupljene unrm alatkom i klasifikuje podatke prema tipu.

Primer 1 Zauzeće fajla na NTFS disku

Na NTFS disku sa sektorima veličine 512 bajtova i 8 sektora po klasteru, čine veličinu klastera 4096 bajtova (512*8). Ukoliko je fajl veličine 5200 bajtova, to znači da će slek prostor biti 3072 bajta i 20 bajta RAM sleka.

Fajl veličine 5100 bajtova zauzima 9 sektora. S obzirom da NTFS fajl sistem radi sa klasterima ne sa sektorima fajlu će biti dodeljena 2 klastera. Prvi klaster (8 sektora) biće kompletno popunjen fajlom, ali drugi klaster će da sadrži samo 1004 bajta fajla (4096+1004=5100).

To znači da će prvi sektor (512 bajtova) od drugog klastera biti kompletno popunjen fajlom, ali će drugi sektor drugog klastera sadržati samo 492 bajta. Prostor na kraju drugog sektora drugog klastera je poznat kao RAM slek (kao dump iz RAM-a nekadašnjih operativnih sistema) i u ovom slučaju iznosi 20 bajtova (492+20=512).

Nakon ovog sektora postoji još 6 sektora do kraja drugog klastera (jer fajlu je dodeljeno dva klastera odnosno 16 sektora ukupno). Ovih 6 sektora predstavljaju fajl slek što iznosti 3072 bajta slek fajla.

Primer 2 Zauzeće fajla na NTFS disku

Kreiraćemo jedan txt fajl sa notepadom i unutra napisaćemo doktorat. Snimićemo i izaći iz editora. Desnim klikom na taj fajl proverićemo properties tog fajla. Možemo primetiti da postoje dva njegova svojstva (eng. Attributes) „Size" i „Size on disk".

Size: 8 bytes (8 bytes)

Size on disk: 4.00 KB (4096 bytes)

Postavlja se pitanje odakle se stvara ova razlika. Ukoliko je fajl velik samo 8 bajtova zašto su preostali bajtovi dodeljeni datoteci i da li oni služe nekoj svrsi. Prosečnom korisniku nije od koristi, ali digitalnom forenzičaru je i te kako od koristi. Odgovor leži u razumevanju slek prostora. S obzirom da se u literaturi povezuju sa slekom (kako se kolokvijalno naziva) različiti termini poput fajl slek, RAM slek i drajv slek to može biti dosta zbunjujuće. Iako ovi termini izgledaju slično razumevanje i poznavanje razlika između njih jako je bitna kada je u pitanju forenzička analiza računarskog sistema.

231 The Coroner's Toolkit (TCT) predstavlja kolekciju forenzičkih alata čiji su autori Wietse Venema i Dan Farmer. Vidi: http://www.porcupine.org/forensics/tct.html , 05.04.2016.

Slobodan prostor

Podrazumeva prostor na hard disku koji trenutno nije dodeljen datoteci a može biti i prostor koji nikada nije dodeljen datoteci i obično se nalazi na kraju diska.

Primer jednog klastera koji može sadržati bitne informacije u jednom delu slek prostora.

Veličina klastera - 4096 bajta

Veličina sektora - 512 bajta

Trenutni sadržaj klastera predstavlja fajl doktorat.txt - 800 bajta

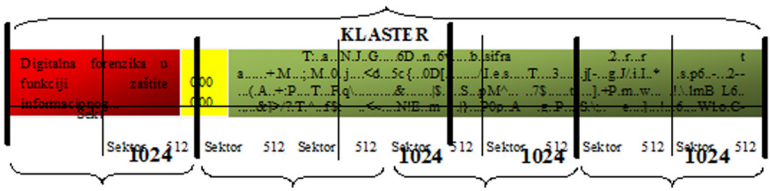
- Predstavlja upisan sadržaj fajla doktorat.txt

- Zaključno sa verzijom Windows 95 i Win NT 3.5 ovde bi se našli podaci iz RAM memorije i to je ono što se u literaturi može naći kao termin RAM slek.

- Predstavlja drajv slek odnostno fajl slek ukoliko ne računamo RAM slek i tu se nalaze sirovi podaci (eng. Raw data) koji se nalaze od ranije u ovim sektorima.

Loši sektori

Loši sektori (eng. Bad sectors) predstavljaju oštećeni deo diska na kome se ne mogu izvršiti operacije čitanja i pisanja. Procesom formatiranja diska omogućava se operativnom sistemu da identifikuje neupotrebljiv sektor i obeleži ga kao loš. Postoje specijalni programi koji se koriste za oporavak podataka u lošim sektorima što digitalnom forenzičaru može biti od velike važnosti.



Slika 6. Prikaz sadržaja klastera nakon snimanja fajla

Sa stanovišta digitalne istrage bitno je znati da klasteri mogu biti označeni kao loši sa ciljem skrivanja podataka. U NTFS loši klasteri su označeni u metadata fajlu koji se zove $BadClus koji je u MFT-u 8 zapisu.[232] *$BadClus* jeste rasčlanjeni fajl čija je veličina podešena prema veličini celog fajl sistema.[233] Kada se detektuje loš klaser on će biti dodeljen ovom fajlu. Veličina podataka koji mogu biti skriveni sa ovom tehnikom je neograničena,

232 Postupak opisan u radu Cheong Kai Wee, *Analysis of hidden data in the NTFS file system*, http://www.forensicfocus. com/hidden-data-analysis-ntfs, 24.05.2016.

233 Kopecký K., *Cyber grooming danger of cyberspace*, study, Olomouc, 2010.

prostim dodeljivanjem klastera.[234]

Na osnovu iznetog treba uzeti u obzir da se prilikom carving aktivnosti iz hard diska veličine na primer 500 GB može izvući preko 1 TB podataka, a to je upravo zbog klastera koji sadrži i po nekoliko bajtova koji nisu upotrebljeni za upis fajla ali takođe sadrže podatke (slek prostor). Prilikom analize forenzičke kopije od suštinske važnosti je brzina analize prikupljenih podataka koja može da se ostvari uz veliku procesorsku snagu i velikim skladišnim prostorom, da bi digitalni dokaz bio brzo pronađen. U svetski forenzičkim laboratorijama koriste se superkompjuteri koji forenzičke aktivnosti kao što su kreiranje bitstream kopije, proces carving-a, analiza podataka i kreiranje izveštaja obavljaju u jako kratkom vremenskom periodu (do 20 min).

2.6. PRIHVATLJIVOST DIGITALNOG DOKAZA

Digitalni dokaz ne predstavlja samo jedan fajl i kao takav on ima svoje karakteristike i u skladu sa njima moraju postojati određene smernice prema kojima moramo usaglasiti forenzičke procedure prikupljanja. Da bi *digitalni dokaz bio prihvaćen od strane suda* treba da bude:

Prihvatljiv - u skladu sa određenim pravnim pravilima, pre nego što bude dostavljen sudu. Ukoliko se koristi kopija, potrebno je koristiti najbolju kopiju. Ukoliko se koristi original tada kopija nije od značaja. S obzirom da se danas može napraviti kopija digitalnog dokaza istovetnog originalu, upotreba kopije je pravno prihvatljiva iako postoji original. U praksi se koristi i primenjuje prezentovanje kopije da bi se eliminisale sve sumnje vezane za izmenu tj. zloupotrebu sa originalnim dokazom;

Autentičan - Dokazni materijal mora nedvosmisleno upućivati na krivično delo i učinioca. Ukoliko se ne može dokazati autentičnost digitalnog dokaza na sudu, bez obzira što je dokaz prikupljen i analiziran na propisan način, sudija može proglasiti dokaz nevažećim ili nerelevantnim za donošenje sudske odluke. Na primer: Da li je log fajl koji forenzičar prikupio zaista originalni ili je to neki izmenjeni „custom“ log fajl;

Kompletan - u smislu da dokaz treba da prikaže ceo slučaj sa svim

234 Klevinsky T. J., Laliberte S., Gupta A., Hack I.T.: Security Through Penetration Testing, Addison Wesley, 2002.

aspektima bitnim za donošenje sudske odluke. Dokaz mora biti objektivan i prikazati sve bitne okolnosti za sudsko odlučivanje, kako one koje se stavljaju na teret okrivljenog, tako i okolnosti koje mogu biti oslobađajuće;

Pouzdan - ne sme postojati nikakva sumnja u vezi sa načinom na koji su dokazi prikupljeni i kako je sa njima rukovano. U suprotnom, to bi bacilo sumnju na autentičnost i istinitost dokaza;

Verodostojan i razumljiv - za sud i stranke u postupku. Nema svrhe pred sud iznositi na primer „memory dump" (slika stanja memorije u računaru), s obzirom da sud nema obavezu da poseduje takva stručna znanja pa samim tim neće razumeti šta to znači.[235] [236]

Da bi *sud priznao digitalni dokaz* postoje određeni uslovi i procedure koje je neophodno ispuniti: analiza, čuvanje kao i ponovljivost kompletne procedure istrage, ukoliko to sud zahteva od digitalnog forenzičara.

Kada je reč o *čuvanju dokaza*, zahteva se poštovanje procedura da bi dokaz posedovao sve potrebne atribute. Ovi atributi opisuju elemente standardne operativne procedure digitalne forenzičke istrage. Prvi element je *naziv procedure*, zatim sledi *namena*, tj. opis namene digitalnog dokaza, *kada će se koristiti i ko će ga koristiti* (ovo je vrlo značajno zbog preuzimanja odgovornosti da se neće uticati na dokaz). Svaki digitalni dokaz mora pratiti opisana procedura u koracima i merama opreza pod kojima se digitalni dokaz koristio u istrazi. Osim atributa koji opisuju pomenute elemente, oni mogu opisivati i korake kod kojih se zahteva tačnost u istrazi tzv. kalibrisanje i opis korišćenih matematičkih operacija tzv. kalkulisanje. Neophodno je opisati ograničenja sigurnost i reference same opreme i alata sa kojom se vrši ispitivanje.

Jedan od najčešćih principa koji su za sud prihvatljivi, a odnose se na digitalne dokaze je *„Daubert princip*" . Podrazumeva primenu naučnog metoda od strane eksperta kako bi se izvršila proverljivost prezentovanih naučnih dokaza na sudu. Ovaj princip podjednako važi za sve naučne, tehničke i inženjerske dokaze, koji će biti predstavljeni sudu.

Izuzetno je bitno da digitalni dokazi sa osumnjičene mašine budu dobijeni ili prikupljeni *forenzičkim alatima koji su prihvatljivi pred sudom*. Isto

235 Douglas Schweitzer, *Incident Response - Computer Forensics Toolkit*, Wiley Publishing, Inc, Indianapolis, 2003, str. 140.

236 Beek C., *Virtual Forensics*, TenICT proffesionals, 2010, http://securitybananas.com/ wp-content/ uploads/ 2010/04/Virtual-Forensics _Black HatEurope2010_CB.pdf, 11.07.2016.

tako digitalne dokaze sud može verifikovati iako je digitalni dokaz u obliku određenog fajla. U svim sudskim postupcima u kojima se koriste digitalni dokazi isti moraju biti dobijeni ili izvučeni sa osumnjičene mašine zahvaljujući forenzičkim alatima prema tačno definisanim procedurama.

U SAD 2004. godine odlučeno je da su merodavni forenzički alati *AccessData FTK Imager* i *EnCase*. Ovo su forenzički alati testirani na bagove u NIST-ovoj laboratoriji za nepoznate softvere i prvi priznati u svetu od pravosudnih sistema na Zapadu.[237] Koriste se u brojnim zemljama i drugi alati kao što su *Ilook-IX*[238] (FBI,[239] SAD), *X-Way Forensic*[240] (NPIA,[241] Engleska), *Paraben*[242] (BKA,[243] Nemačka), kao brojni alati na Linux platformama otvorenog koda.

Naše službe koje se bave digitalnom forenzikom koriste *EnCase* (prvi je naučno verifikovan sa preciznim brojem grešaka koje unosi u ispitivani digitalni materijal, a koje ne menjaju intergitet ispitivanog materijala), *FTK Imager*-om, *HELIX* kompilacijom alata (verzijom u kojoj se nalazi licenciran EnCase 4).

Treba napomenuti da se priča o alatima mora prihvatiti fleksibilno. Forenzičar koji koristi bilo koji alat treba da zna da objasni, da li je bilo neke promene na ispitivanim podacima. Taj rezultat mora biti priznat na sudu, pod uslovom da druga strana na bilo koji način (ne uvek forenzički) ne ospori i ne obori dokaze i hipotezu. Kod nas sudija ne ulazi u prirodu alata (kao dokaznog sredstva), ali to može osporiti advokat suprotne strane. Zato u međunarodnoj sudskoj praksi, koja je vezana za visokotehnološki kriminal, mogu da variraju tipovi alata koji se primenjuju pri izvođenju dokaza. Da bi forenzički alati bili prihvatljivi pred sudom uslov je da imaju poznati stepen greške i moraju biti prihvaćeni od strane relevantnih naučnih krugova, ili objavljeni u relevantnim naučnim časopisima.

2.7. IZVEŠTAVANJE

Forenzika je egzaktna nauka koja se bazira isključivo na dokazima i koja ne priznaje pretpostavke. Svaki navod kreiran od strane forenzičara mora

237 The National Institute of Standards and Technology (NIST), http://www.nist.gov/index.html, 30.04.2016.

238 Perlustro, http://www.perlustro.com/, 30.04.2016.

239 Federal Bureau of Investigation, http://www.fbi.gov/, 30.04.2016.

240 X-Ways Forensics: *Integrated Computer Forensics Software*, http://www.x-ways.net/forensics/, 30.04.2016.

241 National Policing Improvement Agency, http://www.npia.police.uk/, 30.04.2016.

242 Paraben Corporation, http://www.paraben.com/, 30.04.2016.

243 BKA odnosno , Federal Criminal Police Office, http://www.bka.de/, 30.04.2016.

biti potkrepljen digitalnim dokazom. U slučaju da je istraga sprovedena u potpunosti obavezno je dostavljanje *"Izveštaja o istrazi"*. Kada je reč o istrazi u okviru organizacije izveštaj se dostavlja vlasniku sistema koji dalje donosi odluku o istrazi. Kada je u pitanju zvanična istraga izveštaj se dostavlja nadležnim državnim organima za dalji pravosudni postupak.

Kreiranje izveštaja je jedan od jako bitnih elemenata forenzičke analize i predstavlja veliki izazov za digitalnog forenzičara. Izveštaj mora da sadrži precizan opis nedozvoljene aktivnosti razumljiv sudu, odnosno donosiocu odluka. Izveštaj mora biti blagovremeno kreiran i pravno relevantan, odnosno nesporan. Bitno je istaći da svi koraci u digitalnoj istrazi kao i zaključci moraju da budu dokumentovani. Kada se definiše željeni format izveštaja bitno je da ga digitalni forenzičar striktno poštuje. To podrazumeva kreiranje formi, skica i šablona kojim se, adekvatno organizuje i podstiče proces odgovora na nedozvoljenu aktivnost i evidentiraju svi relevantni podaci. Takav kreirani dokument „Izveštaj o istrazi" treba da *sadrži sledeće celine*:[244]

Apstrakt istrage: opis događaja, kratka metodologija istrage, kratak opis skupljanja dokaza i metoda čuvanja istih, zaključak sa kratkim uopštenim rezonima;

Metodološke detalje: istraga, skupljanje i čuvanje dokaza;

Nalaz 1- opis, diskusija, dokazi koji potvrđuju nalaz;

Nalaz N - opis, diskusija, dokazi koji potvrđuju nalaz;

Kratak sadržaj i zaključke;

Dodatak: lista ispitanih (intervijuisanih), lista dokaza, programi i alati korišćeni u istrazi, IT eksperti konsultanti, drugi važni listinzi i informacije.

Dakle, prilikom kreiranja izveštaja za davanje mišljenja sudu, od suštinske važnosti je da svaki segment bude dokumentovan. Koji slučaj je u pitanju, ko je dao ovlašćenje digitalnom forenzičaru, sa kim je rađena forenzička istraga, kad je rađena digitalna forenzika, gde se radila digitalna forenzika, koliko je vremenski trajala digitalna forenzika, dokaz da je rađena digitalna forenzika (u formi screenshota, fotografija najznačajnijih elementa na kojima se radilo). Na primer ukoliko se mora izvaditi memorija, kartica, hard disk iz računarskog sistema svaki korak se mora fotografisati (pre i nakon vađenja šrafova) da bi se znalo kako je to izgledalo pre i nakon preizimanja i pre i nakon vraćanja originalnog dokaza.

Veoma je važno da se dokumentovanje vrši blagovremeno i da to obavlja iskusno osoblje da ne bi došlo do određenih propusta i grešaka, koje mogu da kompromituju kompletnu digitalnu istragu. Izveštaj treba da se razloži

244 APWG, *Phishing Activity Trends Report, 3rd Quarter (July – September 2012)*, 2013, http://www.apwg.org/download/document /84/apwg_trends_ report_q3_2012.pdf, 24.06.2016.

na tehnički i netehnički deo.[245] Kada je reč o tehničkom delu treba opisati detaljno sprovedene aktivnosti, koji su alati bili korišćeni, koja je tehnologija bila upotrebljena prilikom identifikovanja zlonamernog računarskog sistema na primer koji string u hederu fajla ukazuje da je OS bio Windows, koji string u email hederu identifikuje da je SMTP server lociran u određenoj zemlji. Organizovati dokumentaciju za sve ono što je uslikano od strane digitalnog forenzičara prilikom prikupljanja i analize dokaza. Takođe svu dokumentaciju i vođene dnevnike treba numerisati.

Netehnički deo treba da obrazloži sudu razumljivim jezikom u formi odgovora na pitanje da li je u forenzičkoj istrazi identifikovan digitalni dokaz koji ukazuje da je osumnjičeni izvršilac određene zlonamerne aktivnosti ili je u određenoj vezi sa njom, ili takvog dokaza nema. Dokumentacija treba da sadrži broj predmeta u sudu, arhivski broj, kratku istoriju predmeta i aktivnosti (ukoliko postoje određeni dokumenti koji su u vezi sa slučajem) i treba navesti detaljno sve informacije. Jako je važno da se izveštaj indeksira zbog lakšeg i bržeg pronalaženja informacija. Ne treba davati lično konačno mišljenje o slučaju u izveštaju. Od forenzičara se očekuje samo da obrazloži napisan izveštaj. Suprotna strana (advokat) može dokazivati nekompetentnost ili nepoznavanje određene tehnologije od strane licenciranog IT veštaka.

U praksi se upotrebljavaju određeni formulari od kojih će najznačajniji biti detaljnije razmotreni:

- Formular za izvođenje procedure forenzičkog inicijalnog odgovora
- Formular za skladištenje digirtalnih dokaza
- Dokument o očuvanju lanca nadležnosti
- Formular o očuvanju lanca nadležnosti
- Radni list računarskih dokaza
- Radni list hard diska
- Radni list prenosivih uređaja.[246]

Svaka promena u digitalno forenzičkom slučaju mora se evidentirati u dnevniku slučaja koji forenzičar mora da vodi. Na osnovu toga biće uočljivi novi momenti koji se tiču vođenog slučaja kao i ime forenzičara koji je promenu uneo.

Primer dokumenta o očuvanju lanca nadležnosti prikazan je na sledećoj slici.[247]

---

245 Mane Piperevski, *Workshop ICT Forensics Investigation – module 6*, Piperevski & Associates, Beograd 2016.

246 Mane *Piperevski, Workshop ICT Forensics Investigation – module 1*, Piperevski & Associates, Beograd 2016.

247 Https://www.asdfed.com/public_downloads, 04.08.2016.

Chain of Custody Document	Sequence Number:	
Receiving Organization:	Location:	
Name of Person From Whom Received:	Address:	
Location from Where Obtained:	Reason:	Date/Time Obtained:

Item Number	Quantity	Description

Item Number	Date	Released By:	Received By:	Reason for Change:
		Signature	Signature	
		Name & Title	Name & Title	
		Signature	Signature	
		Name & Title	Name & Title	

Slika 7. Dokument o očuvanju lanca nadležnosti
(Izvor: The American Society of Digital Forensics & eDiscovery, Inc For Digital Evidence Experts https://www.asdfed.com/public_downloads)

Najvažniji podaci u ovom dokumentu su sledeći:

Sequence number – broj naloga;

Item number – predstavlja jedinstven broj pod kojim je zaveden digitalni dokaz koji može biti računar, SD kartica, USB flash, a može biti i odštampan digitalni dokaz kao na primer heder email-a;

Quantity – količina digitalnih dokaza;

Description – opis digitalnog dokaza;

Date/time – datum i vreme;

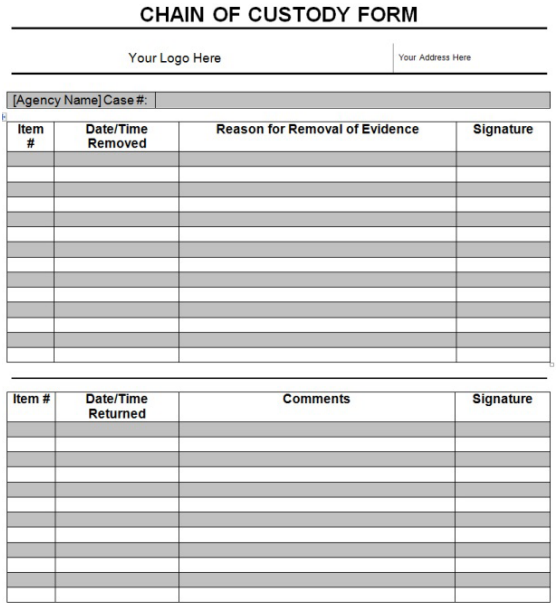
Released by – ko je izdao digitalni dokaz;

Received by – ko je primio digitalni dokaz;

Reasaon – koji je razlog transfera digitalnog dokaza iz jedne organizacije u drugu,

Chain of custody dokument – šta je to što se predaje izmedju organizacija ili ljudi i sadrži detaljnije elemente.

Formular o očuvanju lanca nadležnosti koji služi za evidenciju nastalih promena koji su u vezi sa digitalnim dokazom prikazan je na sledećoj slici:



CHAIN OF CUSTODY FORM

Your Logo Here | Your Address Here

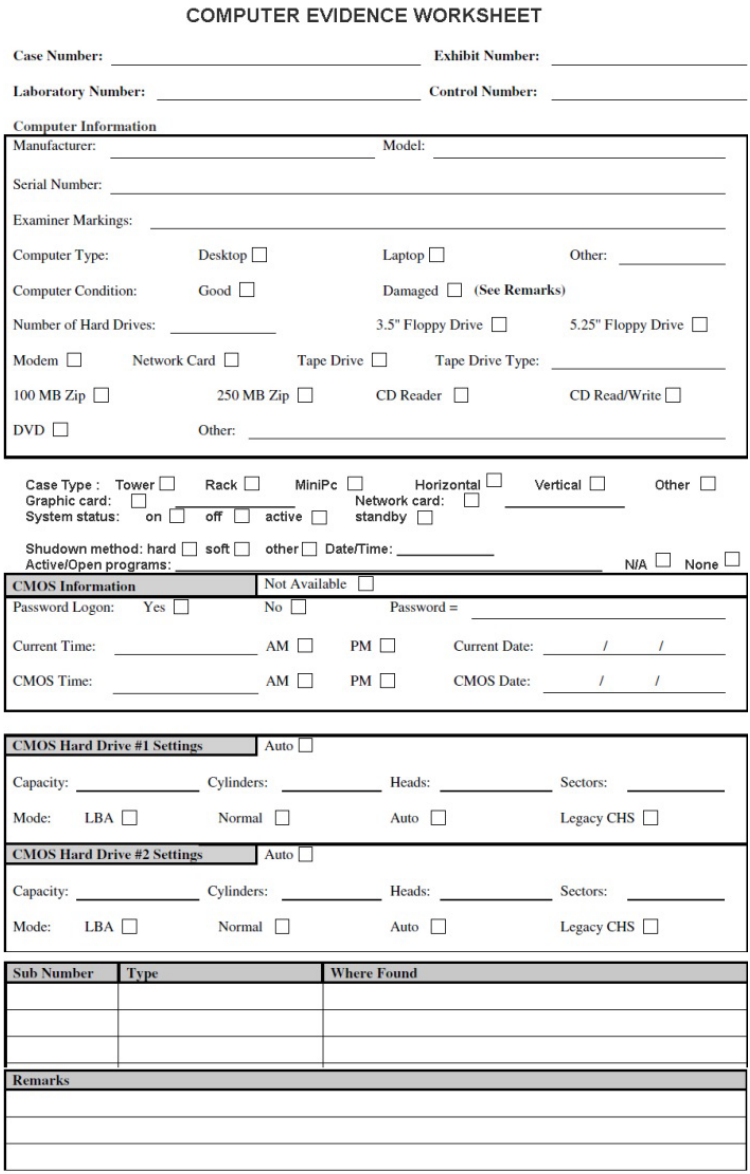
[Agency Name] Case #:

Item #	Date/Time Removed	Reason for Removal of Evidence	Signature

Item #	Date/Time Returned	Comments	Signature

Slika 8. Formular o očuvanju lanca nadležnosti
(Izvor : http://www.joshmoulin.com/digital-forensics-incident-response-forms-policies-and-procedures/)

Radni list računarskih dokaza prikazan je na sledećoj slici :



COMPUTER EVIDENCE WORKSHEET

Case Number: _____ Exhibit Number: _____

Laboratory Number: _____ Control Number: _____

Computer Information

Manufacturer: _____ Model: _____

Serial Number: _____

Examiner Markings: _____

Computer Type: Desktop ☐ Laptop ☐ Other: _____

Computer Condition: Good ☐ Damaged ☐ (See Remarks)

Number of Hard Drives: _____ 3.5" Floppy Drive ☐ 5.25" Floppy Drive ☐

Modem ☐ Network Card ☐ Tape Drive ☐ Tape Drive Type: _____

100 MB Zip ☐ 250 MB Zip ☐ CD Reader ☐ CD Read/Write ☐

DVD ☐ Other: _____

Case Type : Tower ☐ Rack ☐ MiniPc ☐ Horizontal ☐ Vertical ☐ Other ☐

Graphic card: ☐ _____ Network card: ☐ _____

System status: on ☐ off ☐ active ☐ standby ☐

Shudown method: hard ☐ soft ☐ other ☐ Date/Time: _____

Active/Open programs: _____ N/A ☐ None ☐

CMOS Information | Not Available ☐

Password Logon: Yes ☐ No ☐ Password = _____

Current Time: _____ AM ☐ PM ☐ Current Date: / /

CMOS Time: _____ AM ☐ PM ☐ CMOS Date: / /

CMOS Hard Drive #1 Settings | Auto ☐

Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____

Mode: LBA ☐ Normal ☐ Auto ☐ Legacy CHS ☐

CMOS Hard Drive #2 Settings | Auto ☐

Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____

Mode: LBA ☐ Normal ☐ Auto ☐ Legacy CHS ☐

Sub Number	Type	Where Found

Remarks

Slika 9. Radni list računarskih dokaza
(Izvor https://www.ncjrs.gov)

Najvažniji podaci u ovom dokumentu su sledeći:

- Case number - broj slučaja;

-Laboratory number - laboratorijski broj (ukoliko postoji forenzička laboratorija to je njen ID broj ili se upisuje naziv organizacije gde radi forenzičar jer se tamo nalazi forenzička laboratorija);

-Exhibit number - broj pod kojim je digitalni dokaz zaveden;

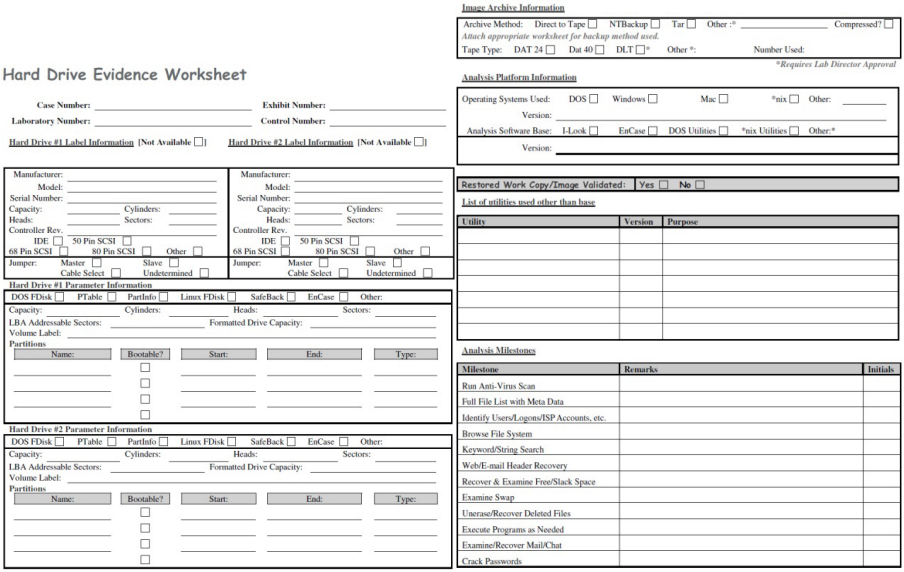
-Control number - kontrolni broj – dodatni broj za kontrolu.

Sa ova četiri ID broja se mogu pratiti kroz dokumentaciju određenog slučaja. Najvažniji podaci u ovom dokumentu su sledeći :

- Computer information - informacije o računaru sadrže sve one podatke koje mogu detaljno identifikovati jedan računar. Tu se nalaze informacije o proizvođaču, modelu, serijskom broju, dopunskoj oznaci, tipu računara (desktop, prenosni, server), stanju računara (da li je oštećen), broju hard diskova, case type (tower, rack, mini, horizontal);
- System status – zatečeno stanje računarskog sistema (on, off, active, standby);
- Shutdown method – način isključenja računarskog sistema (hard, soft, other). Od metoda isključenja zavisi opstanak određenih podataka. Vađenjem kabla iz napajanja određeni podaci se zadržavaju na hard disku u tekućem swap prostoru, dok se pri soft shutdownu određeni podaci ne zadržavaju u swap fajlu. Sa druge strane, vađenjem kabla obrada podataka prestaje momentalno, gube se informacije iz RAM memorije i moguće je oštećenje fajlova, dok se softverskom shutdownom procedurom štite fajlovi od oštećenja, ali se upisiju zapisi u logu aktivnosti čime se menja stanje dokaza. Najbolje je da se računar prenese upaljen tako što je prespojen na uređaj za neprekidno napajanje, da bi se uradila live forenzička kopija računarskog sistema.
- Data and time – datum i vreme;
- Active open programs – ukoliko je računar u operativnom radu zapisao imena programa koji su otvoreni;
- Remarks – drugi računarski elementi;
- CMOS information – predstavljaju informacije iz BIOSa (vreme BIOSa i trenutno vreme, da li postoji šifra, informacije o hard diskovima).

Radni list hard diska služi za identifikaciju svih elementa hard diska koji predstavlja digitalni dokaz u ispitivanom slučaju. Pre kreiranja digitalne kopije hard diska forenzičar treba da obrati pažnju na „jumpere“ koji su podešeni na hard disku i na sam raspored kablova. Podešenost „jumpera“ može ukazati na to da li je i koji je ispitivani hard disk bio bootabilan. Primer radnog lista hard

diska prikazan je na sledećoj slici:



Hard Drive Evidence Worksheet

Case Number: _____ Exhibit Number: _____

Laboratory Number: _____ Control Number: _____

Hard Drive #1 Label Information [Not Available ☐] Hard Drive #2 Label Information [Not Available ☐]

Manufacturer: / Model: / Serial Number: / Capacity: _____ Cylinders: _____ / Heads: _____ Sectors: _____ / Controller Rev. _____

IDE ☐ 50 Pin SCSI ☐ 68 Pin SCSI ☐ 80 Pin SCSI ☐ Other ☐

Jumper: Master ☐ Slave ☐ Cable Select ☐ Undetermined ☐

Hard Drive #1 Parameter Information

DOS FDisk ☐ PTable ☐ PartInfo ☐ Linux FDisk ☐ SafeBack ☐ EnCase ☐ Other:

Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____

LBA Addressable Sectors: _____ Formatted Drive Capacity: _____

Volume Label: _____

Partitions

Name:	Bootable?	Start:	End:	Type:
	☐			
	☐			
	☐			
	☐			

Hard Drive #2 Parameter Information

DOS FDisk ☐ PTable ☐ PartInfo ☐ Linux FDisk ☐ SafeBack ☐ EnCase ☐ Other:

Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____

LBA Addressable Sectors: _____ Formatted Drive Capacity: _____

Volume Label: _____

Partitions

Name:	Bootable?	Start:	End:	Type:
	☐			
	☐			
	☐			
	☐			

Image Archive Information

Archive Method: Direct to Tape ☐ NTBackup ☐ Tar ☐ Other :* _____ Compressed? ☐

Attach appropriate worksheet for backup method used.

Tape Type: DAT 24 ☐ Dat 40 ☐ DLT ☐* Other *: Number Used:

**Requires Lab Director Approval*

Analysis Platform Information

Operating Systems Used: DOS ☐ Windows ☐ Mac ☐ *nix ☐ Other: _____

Version: _____

Analysis Software Base: I-Look ☐ EnCase ☐ DOS Utilities ☐ *nix Utilities ☐ Other:*

Version: _____

Restored Work Copy/Image Validated: Yes ☐ No ☐

List of utilities used other than base

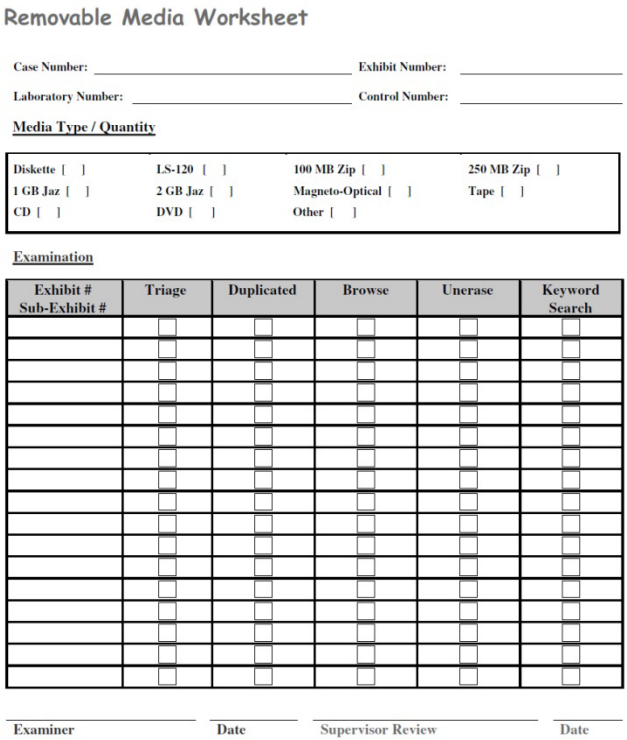
Utility	Version	Purpose

Analysis Milestones

Milestone	Remarks	Initials
Run Anti-Virus Scan		
Full File List with Meta Data		
Identify Users/Logons/ISP Accounts, etc.		
Browse File System		
Keyword/String Search		
Web/E-mail Header Recovery		
Recover & Examine Free/Slack Space		
Examine Swap		
Unerase/Recover Deleted Files		
Execute Programs as Needed		
Examine/Recover Mail/Chat		
Crack Passwords		

Slika 10. Radni list hard diska
(Izvor https://www.ncjrs.gov)

Radni list prenosivih uređaja sadrži idenfikacione brojeve i detaljne karakteristike samih prenosivih uređaja i njihovu količinu. Dodatno unose se opisi nakon njihovog ispitivanja. Izgled dokumenta prikazan je na sledećoj slici:



Removable Media Worksheet

Case Number: _____ Exhibit Number: _____

Laboratory Number: _____ Control Number: _____

Media Type / Quantity

Diskette [ ]	LS-120 [ ]	100 MB Zip [ ]	250 MB Zip [ ]
1 GB Jaz [ ]	2 GB Jaz [ ]	Magneto-Optical [ ]	Tape [ ]
CD [ ]	DVD [ ]	Other [ ]	

Examination

Exhibit # Sub-Exhibit #	Triage	Duplicated	Browse	Unerase	Keyword Search
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐

Examiner _____ Date _____ Supervisor Review _____ Date _____

Slika 11. Radni list prenosivih uređaja
(Izvor https://www.ncjrs.gov)

Iz navedenog proizlazi da izveštaj mora sadržati opis korišćene metodologije, opis uspostavljenih i pridržavanih protokola, detaljno (step-by-step) opisane forenzičke aktivnosti, detaljno opisane korišćene metode i alate, detaljno opisan postupak forenzičke analize i donete zaključke uključujući i ograničenja. U izveštaju je potrebno naglasiti da je prikupljanje i čuvanje dokaza u toku istrage bilo izvedeno u skladu sa zakonom o istražnom postupku i da su obavljeni informativni razgovori i saslušanja izvršena u skladu sa propisima. Na izloženi način biće formiran detaljan izveštaj u okviru interne istrage u organizaciji koji će biti spreman i za ekspertsko veštačenje za sud ukoliko bude potrebno.

Prilikom svedočenja u sudu, od forenzičkog eksperta se očekuje detaljno obrazloženje na razumljivom jeziku (imajući u vidu da sudije ne moraju biti informatički edukovani) na koji način je učinjena nedozvoljena aktivnost i potvrđivanje nalaza i mišljenja napisanog u izveštaju. Na sudu

forenzički ekspert ne sme da ulazi u diskusiju već da se drži činjenica koje se tiču isključivo istrage. Advokati uvek imaju težnju da ruše integritet forenzičkog eksperta uvlačenjem u raspravu i izvlačenjem ličnog mišljenja. To se ne sme dogoditi, jer bi sud forenzičkog experta označio kao pristrasnog.

2.8. DIGITALNA FORENZIKA U VIRTUELNOM OKRUŽENJU

Kada je u pitanju digitalna forenzika u virtuelnom okruženju vrlo je važno poznavanje samog virtuelnog okruženja i njegove specifičnosti kao i mogućnosti koje okruženje može ponuditi. U tom smislu je od značaja poznavanje prednosti i nedostataka, koje mogu da se jave prilikom eksploatacije virtuelnog okruženja. Treba istaći da postoje izvesne razlike u istražnom pristupu digitalnog forenzičara, kada su u pitanju fizičke odnosno virtuelne mašine. *Ideja virtuelizacije* je isprojektovana sa ciljem jednostavnijeg upravljenja velikim brojem virtuelnih mašina čime se pre svega štedi prostor, vreme, novac i potrošnja energije. Kao koncept se prvobitno pojavila još 1960. godine sa pojavom mainframe računara. Sa nastankom personalnih računara 1990. godine došlo je do njene veće upotrebe. Popek i Goldberg su u svom radu "Formal requirements for virtualizable third generation architectures" izneli preduslove za arhitekturu koji može da podržava virtuelnu mašinu opisujući je kao „efikasan, izolovan duplikat prave mašine".[248] Samu virtuelizaciju su opisali kroz ideju VMM (eng. Virtual machine monitor).[249]

Ono što je specifično za virtuelne mašine je to što one koriste u potpunosti hardver fizičkog servera. VM aplikacija (eng. guest) tzv. gost pokreće sopstveni operativni sistem na stvarnoj (eng. host) mašini. Jednostavnije rečeno VM predstavlja virtuelni računar pokrenut u okviru fizičkog računara. Na primer, jedan fizički server može predstavljati virtuelno okruženje sa preko 20 virtuelnih mašina. Komunikacija između fizičkog servera i virtuelnih mašina se realizuje preko hypervisor-a (program koji obezbeđuje virtuelizaciju) ili *virtual machine manager-a* putem hiper poziva. Hypervisor program upravlja sistemskim procesorom, memorijom i drugim resursima,

248 Ligh M. H., Adair S., Hartstein B., Richard M., *Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code*, Wiley Publishing, Inc., Indianapolis, Indiana, 2011.

249 Virtual machine monitor predstavlja deo programa koji ima 3 karakteristike. Prva je da VMM pruža okruženje za programe koje je identično okruženju na fizičkoj mašini. Drugo, programi koji se pokreću u ovom virtuelnom okruženju imaju veoma mali pad performansi kada je u pitanju brzina u odnosu na fizičku mašinu i treće je da VMM u potpunosti kontroliše sistemske resurse.

koje dodeljuje drugim gost sistemima na zahtev.[250] Hypervisor program može da obezbeđuje virtuelizaciju direktno na hardveru (native VM ili Bare-Metal Hypervisor) ili na operativnom sistemu (host VM ili Hosted Hypervisor).[251] Predstavnici virtuelizacije koja se realizuje direktno na hardveru su: VMware ESX,[252] Citrix XenServer,[253] i Microsoft Hyper-V.[254] Predstavnici virtuelizacije koja se realizuje na OS su: Parallels Desktop,[255] Microsoft Virtual Server,[256] VMware Server,[257] i VMware Workstation.[258]

Virtuelna mašina može raditi izolovano ili može deliti resurse sa drugim virtuelnim mašinama u okviru iste ili druge serverske platforme. Na osnovu ovog specifičnog dizajna i optimizovanih procesorskih operacija u okviru realizovanog virtuelnog okruženja, nema razlike u radu na virtuelnim mašinama u odnosu na fizičke mašine. Postoje različiti tipovi virutelnog okruženja, a najpoznatiji su *Microsoft Hyper-V,*[259] *VMWare Vsphere ESXi,*[260] *QEMU,*[261] *Citrix XenServer.*[262]

---

250 Lillard T. V., Digital forensics for network, Internet, and cloud computing - A forensic evidence guide for moving targets and data, Elsevier Inc, USA, 2010.

251 Barrett D., Kipper G., Virtualization and Forensics – A digital forensic Investigator's guide to Virtual Environments, Elsevier Inc., USA, 2010.

252 VMware, http://www.vmware.com/products/esxi-and-esx/overview, 27.05.2016.

253 Citrix XenServer, http://www.citrix.com/products/xenserver/overview.html, 27.05.2016.

254 Microsoft, Experience greater flexibility and agility, http://www.microsoft.com/en-us/server-cloud/hyper-v-server/default.aspx, 27.05.2016.

255 Parallels, http://www.parallels.com/, 27.05.2016.

256 Microsoft, Microsoft Hyper-V Server 2008 R2, http://www.microsoft.com/windowsserversystem/ virtualserver/, 27.05.2016.

257 VMware, http://www.vmware.com/products/vcenter-server/, 27.05.2016.

258 Vmware Workstation, http://www.vmware.com/products/workstation/, 27.05.2016.

259 Dart K. A., *Deleted Files Can Be Recovered*, February 24, 2008, http://www.akdart.com/priv9.html, 10.07.2016.

260 Davidovac Z., Korać V., *Vulnerability management and patching it systems*, Arheologija i prirodne nauke, br. 6, 2011, str. 129-144.

261 Davis N., *Live Memory Acquisition for Windows Operating System : Tools and Techniques for analyses*, Eastern Michigan University, 2008, http://www.emich.edu/ia/pdf/research/Live%20Memory% 20Acquisition%20for%20Windows%20Operating%20Systems,%20Naja%20Davis.pdf, 27.06.2016.

262 Digital Forensics Research Workshop, *A road map for digital forensics research*, Technical report, Digital Forensics Research Workshop, 2001.

2.8.1. Virtuelno okruženje kao mesto krivičnog dela

Kao i svako drugo okruženje i virtuelno okruženje može biti kompromitovano na različite načine, što za posledicu može da ima kompromitovanje kako samih virtuelnih mašina tako i operativnog sistema i fajlova koji se u tom okruženju nalaze.

Dobra informisanost i poznavanje načina rada u virtuelnom okruženju su veoma bitni digitalnom forenzičaru, za koga je mesto krivičnog dela upravo virtuelno okruženje koje čine virtuelne mašine. Pristup istrazi se bazira na lociranju i pristupu fizičkom serveru koji pokreće virtuelne mašine. Od velike je važnosti da digitalni forenzičar ima pristup "uživo" (eng. live) digitalnoj mašini, koja se posmatra kao mesto krivičnog dela.[263] Na taj način mogu se prikupiti dragoceni podaci i informacije kao potencijalni digitalni dokazi, u toku rada fizičkog servera. Mogućnost manipulacije dokaza u ovom okruženju od strane osumnjičenog je velika, pa se posao prikupljanja digitalnih dokaza prilično usložnjava.

Isti principi koji se odnose na digitalnu forenziku računara i koji važe u toku prikupljanja, analize i prezentacije digitalnih, važe i za virtuelne mašine u virtuelnom okruženju sa određenim razlikama. Bitno je istaći da je potrebno koristiti samo testirane i proverene forenzičke alate (kao na primer *Access data FTK, Encase, X-Way Forensic*), koji podržavaju rad u virtuelnom okruženju i poseduju kompatibilnost sa novijim operativnim sistemima.

Ukoliko se istraga u vezi sa nedozvoljenim aktivnostima u virtuelnom okruženju obavlja prema nekim od predloženih metodologija, uz korišćenje odgovarajućih forenzičkih alata, sa ciljem pronalaženja relevantnih digitalnih dokaza, istražni postupak će se uspešno okončati. U suprotnom istraga može da ode u neželjenom pravcu. U zavisnosti o kom tipu incidentne radnje je reč digitalna istraga u virtuelnom okruženju može biti javna (zvanična) ili korporacijska. Istraga počinje fizičkim pristupom fizičkom mestu krivičnog dela, gde se vrši prikupljanje fizičkih dokaza, zatim se pristupa digitalnom mestu krivičnog dela (virtuelnom okruženju koga čine virtuelne mašine) i traje dok digitalni forenzičar ne završi istragu nad digitalnim podacima, koji će biti spremni za izveštaj odnosno prezentovanje rekonstruisanog zločina ili incidenta.

Treba istaći činjenicu da je virtuelno okruženje, okruženje koje nudi čitav niz pogodnosti putem svojih veoma korisnih operacija, ali da upravo

263 Vanja Korać, *Digitalna forenzika kao arheologija podataka u visokotehnološkom kriminalu*, Beograd, Centar za nove tehnologije Viminacium, 2013, str. 117.

one mogu biti i zloupotrebljene. Na primer, operacije koje mogu biti zloupotrebljene su migracija virtuelnih mašina, manipulacije sa image-om (slikama stanja) virtuelnih mašina, live migration (manipulacije vezane za migriranje virtuelnih mašina "uživo"). Neke od ovih zloupotreba mogu da za posledicu imaju kontrolu odnosno zloupotrebu virtuelnih mašina od strane zlonamarnog lica.

Zlonamerne aktivnosti se mogu pronaći, jer se sve aktivnosti beleže na serveru odnosno hostu. Veoma je važno da digitalni forenzičar pristupa samoj istrazi kao i prikupljanju dokaza striktno prema definisanim procedurama sa početka istrage, jer u suprotnom može doći do gubitaka ili nestanka važnih digitalnih informacija. Virtualna forenzika mora da ima veći broj prikupljenih dokaza u odnosu na klasičnu digitalnu forenziku, jer digitalni forenzičar mora da prikupi informacije i o paketima podataka kao i komunikaciji između zlonamernog korisnika i korisnika nad kojim je izvršena nedozvoljena aktivnost. U virtuelnoj forenzici se aktivnosti dešavaju u virtuelnim prostorima, koji su smešteni na fizičke (serverske) mašine. Pritom su mašine povezane sa internetom tako da virtualno mogu biti bilo gde (jedan takav primer je cloud computing). Da bi se digitalna mesta krivičnog dela istražila, digitalni forenzičar mora da uđe u digitalno virtuelno okruženje, koje je složeno, što može predstavljati veliki problem forenzičaru. Naročito, ukoliko nisu izvšene pripremne radnje praćenja uz snimanja aktivnosti osumnjičenog kao i upoznavanje sa samim operativnim sistemamima koji se nalaze u virtuelnom okruženju. Za razliku od klasične digitalne forenzike, gde se fizičkom računaru pristupalo fizičkim putem, kada je reč o forenzici u virtuelnom okruženju, forenzičar neće moći da ima jednostavan pristup fizičkoj mašini na kojoj je realizovano virtuelno okruženje. To upravo predstavlja i specifičnost digitalne forenzike u virtuelnom okruženju. Jedan od ciljeva koji se postavlja pred digitalnim forenzičarem je i lociranje centralnog mesta sa virtuelnim računarima (a ne, samo lokacija virtuelne mašine), koji u sebi nose veliki broj korisnih informacija, koje mogu biti iskorišćene kao potencijalni digitalni dokaz. Takođe vrlo je važno da digitalni forenzičar poznaje sve koncepte virtuelizacije.

2.8.2. Servisi u virtuelnom okruženju

U nastavku će biti naveden slikovit opis važnih servisa koji realizuju virtuelno okruženje, a njihovo upoznavanje može biti od koristi

digitalnim forenzičarima:[264] [265]

-*servis za upravljanje virtuelnih mašina* (Virtual machine management service, VMMS) - upravlja odnosno određuje koje operacije mogu da se izvršavaju u nekom od mogućih stanja vrituelnih mašina. VMMS upravlja sledećim stanjima virtualnih mašina: pokretanje, aktivno stanje, neaktivno stanje, stanje pravljenja slike stanja (eng. snapshot), stanje primene slike stanja (eng. snapshot), brisanje slike stanja, spajanje diskova. Na osnovu ovih stanja VMMS upravlja operacijama na virtuelnim mašinama (eng. child). Ne upravlja operacijama *pauza, snimanje, isključenje*, već je za to odgovoran proces *Virtual machine worker proces* (VMWP) koji se kreira pri pokretanju virtuelne mašine;

-*radni proces virtuelne mašine* (eng. Virtual machine worker proces) - kreira se na virtuelnoj mašini, pojavljuje se kao izvršni fajl vmwp. exe i učetstvuje u velikom broju interakcija između operativnog sistema na hostu i virtuelnih mašina (child-ova). Ove interakcije podrazumevaju kreiranje virtuelnih mašina njihovo konfigurisanje, upravljanje stanjima pauza (eng. pause) i nastavak rada virtuelnih mašina (eng. resume), čuvanje (eng. saving), obnavljanje virtuelne mašine (eng. restore) i snimanje slike stanja virtuelnih mašina. Takođe upravljanje memorijom, ulazno-izlaznim portovima na matičnoj ploči računara (eng. motherboard) i upravljanje IRQ-ovima. Na primer postojanje ovog fajla (vmwp.exe) predstavlja dokaz da na hostu postoje viruelne mašine.

-*virtuelni uređaji* (eng. virtual device) - predstavljaju programske module (upravljačke programe), koji omogućuju konfigurisanje uređaja i kontrolu particija virtuelnih mašina. Upravljaju se putem virtuelne matične ploče (eng. Virtual motherboard - VMB) koja se dodeljuje svakoj virtuelnoj mašini;

-*drajver VMBus* - pruža optimizovanu komunikaciju između *host-a* i *child-a* i sastavni je deo *Hyper-V servisa*;

-*drajver za virtuelizaciju infrastrukture (eng. Virtual Infrastructure Driver)*-predstavlja komponentu kernela odgovornu za režim virtuelizacije na *host-u*, koji omogućuje upravljanjem virtuelnim procesorom i memorijom;

---

264 Primer je vezan za realizaciju Hiper V okruženja gde je na host-u podignuto okruženje Windows server 2008 R2.

265 Drakulić M., Drakulić R., *Cyber kriminal*, Fakultet organizacionih nauka u Beogradu, http://www.bos.rs/cepit/idrustvo/sk/ cyberkriminal.pdf, 10.07.2016.

-windows Hypervisor Interface biblioteka (eng. The Windows Hypervisor Interface Library) – predstavlja komponentu kernela kao dinamička bibliotka (eng. dynamic link library - DLL). Omogućava drajverima operativnog sistema pristup procesoru. Nalazi se kao sastavni deo operativnog sistema na hostu. DLL fajl omogućava *driver-ima* operativnog sistema da pristupaju procesoru.

Navedeni servisi možda nemaju direktan uticaj na istražni postupak, ali je važno poznavati bitne procese i njihove mogućnosti u hardverskoj komunikaciji između procesora i hypervizora odnosno između *host-a* i *child-a.* Prisustvo pomenutih fajlova u vidu virtuelnih uređaja i drajvera digitalnom forenzičaru može ukazivati o postojanju virtuelnih mašina.

Univerzitet Fairbanks Aljaska se bavi istraživanjima u oblasti ispitivanja osetljivih (nestabilnih eng. volatile) podataka korišćenjem *virtuelne instrospekcije* (eng. Virtual Introspection).[266] Virtuelna introspekcija, kao oblast novog istraživanja i razvoja u digitalnoj forenzici, predstavlja proces posmatranja stanja virtuelne mašine ili putem Virtual Machine monitor (VMM) ili sa neke druge virtuelne mašine koja nije predmet forenzičkog ispitivanja. Oni su razvili set alata za Xen okruženje koji se zove VIX tools ca ciljem da se smanji rizik od izmene dokaza tokom njihovog ispitivanja.[267] Takođe ovaj alat omogućava analizu "uživo" nad Xen virutelnoj mašini.[268] Osnovni pristup ovih alata je da se pauzira osumnjičena virtuelna mašina, zatim se vrši prikupljanje neophnodnih podataka korišćenjem samo read only operacije i potom se pauza prekida. Kao korisna stvar koja može da se realizuje ovim alatom je mapiranje memorije osumnjičene mašine i dodeljivanje mapiranog dela virtuelnoj forenzičkoj mašini.

2.8.3. Mreže u virtuelnom okruženju

Kada je reč o mrežama u virtuelnom okruženju postoje tri vrste virtuelnih mreža:[269]

- *Interna virtuelna mreža (eng. Internal virtual networks)* - ovaj tip mreže se ne oslanja na fizički mrežni adapter, već se koristi virtuelni

266 The University of Alaska Fairbanks, http://www.uaf.edu/, 03.01.2016.

267 Farmer D., Venema W., *Forensic discovery*, Pearson Education Inc, Crawfordsville, 2008.

268 Brian Hay, Kara Nance, *Forensics Examination of Volatile System Data Using Virtual Introspection*, Department of Computer Science University of Alaska Fairbanks, http://assert.uaf.edu/papers/ forensicsVMI_SIGOPS08.pdf, 03.01.2016.

269 Drakulić M., Drakulić R., *Cyber kriminal*, Fakultet organizacionih nauka u Beogradu, http://www. bos.rs/cepit/idrustvo/sk/ cyberkriminal.pdf, 10.07.2016.

mrežni adapter. Interna virtuelna mreža se upotrebljava kao intranet i koristi se za međusobno umrežavanje virtualnih mašina u intranetu. Takođe postoji i opcija njihovog umrežavanja sa *host-om*, što potencijalno otvara mogućnost zloupotrebe child-ova ukoliko dođe do kompromitovanja host računara. Zlonamerni napad bi bio usmeren na programsku oblast sa ciljem zloupotrebe virtuelne mašine ili njenog gašenja;

- *Eksterna virtualna mreža (eng. External virtual networks)* - ovaj tip mreže se oslanja na fizički mrežni adapter i na virtuelni mrežni adapter, čime se ostvaruje međusobna komunikacija fizičkih i virtuelnih mašina, kako u intranetu tako i na internetu. Potencijalno se otvara mogućnost zloupotrebe host-a, kako spolja tako i od strane samih virtuelnih mašina, jer je otvorena komunikacija između hosta i childa. Zlonamerni napad bi bio usmeren na programsku oblast sa ciljem zloupotrebe virtuelne mašine ili njenog gašenja;
- *Privatna virtuelna mreža (eng. Private virtual networks)* - ovaj tip mreže ne oslanja se na fizički mrežni adapter (slično kao kod interne virtuelne mreže) i nije dozvoljena komunikacija sa članovima van privatne virtualne mreže. Takođe ni *host* nema direktnu komunikaciju sa tom mrežom, čime se sprečava zlonamerni napad na ovaj tip mreže. Teoretska mogućnost napada postoji ali ona je ograničena na hardverski deo hosta.

Da bi se saznalo ime host-a, podaci o mrežnim karticama (fizičkim i virtuelnim) i njihovim konfiguracijama (DHCP parametri, MAC adrese), koriste se određeni alati za tu namenu. Sve ove informacije o mrežnim adapterima virtuelnih mašina koje se nalaze direktno na hostu su jako važne digitalnom forenzičaru da bi se upoznala arhitektura virtuelnog okruženja.[270]

2.8.4. Dokaz postojanja hardvera koji podržava virtuelizaciju

Savremeni koncept virtuelizacije (npr. realizacija cloud computing-a), može da se realizuje samo ukoliko se koriste posebno podešeni hardverski kompatibilni procesori, koji imaju podršku za rad sa hypervizorom. Procesori koji se najčešće koriste za realizaciju virtuelnog

270 Vanja Korać, *Digitalna forenzika kao arheologija podataka u visokotehnološkom kriminalu*, Beograd, Centar za nove tehnologije Viminacium, 2013, str. 122.

okruženja su Intel VT[271] i AMD-V.[272] Značajno je digitalni forenzičar ustanovi tačnu lokaciju fizičkog servera na kojoj se nalazi virtuelna mašina koja je predmet istrage. Razlog leži u tome što se upravo na taj način (fizičkim pristupom hostu) može dokazati postojanje ovakvih tipova procesora, koji podržavaju hardversku virtuelizaciju. Time se dokazuje mogućnost postojanja virtuelnih mašina, koje su mogle biti iskorišćene za izvršenje nedozvoljenih aktivnosti, a koje su smeštene na samom hostu odnosno fizičkoj mašini. Na primer, Properties operativnog sistema može pružiti osnovne, a dovoljne informacije o tipu procesora. Takođe digitalni forenzičar za dodatne informacije o virtuelizaciji može pronaći i u BIOS-u (pod opcijama za podešavanje virtuelizacije), koje mogu indirektno uticati na ispitivanje i prikupljanje dokaza. Takođe prisustvo aplikacije kojom se upravljaju virtuelne mašine (menadžer virtuelnih mašina) ukazuje na postojanje virtuelnih mašina, ali i na mesto odakle se pokreću virtuelne mašine o čemu mogu posvedočiti i log fajlovi pripadajućeg okruženja.

Ovi konzolni alati koji mogu upravljati virtuelnim mašinama digitalnom forenzičaru mogu biti od koristi u slučaju potrebe monitoring-a i upoznavanja sa virtuelnim mašinama u živo (eng. live). Tako se mogu otkriti značajne informacije: imena virtuelnih mašina, stanje virtuelnih mašina (da li su aktivne ili nisu), u kom režimu rada se one nalaze, iskorišćenost resursa i podaci o vremenu i vremenskim zonama. Ti podaci mogu biti npr. „last logon" log fajlovi ili „configuration log" fajlovi, a njihove putanje zavise od vrste programa koji realizuju virtuelno okruženje. Pored toga moguće je ako se koriste, otkriti podatke o profilima ili roaming profilnim fajlovima kao npr. NTUSER.dat (specifični sistemski registri korisnički fajl) i drugim aplikativnim podacima. U nekim slučajevima se može desiti da se diretktorijum TEMP ne kopira zajedno sa profilom pa je potrebno primeniti posebnu pažnju prilikom forenzičkog ispitivanja prikupljenog virtuelnog hard diska.

2.8.5. Dokazivanje vremena

Digitalni forenzičar mora posvetiti izuzetnu pažnju na vreme i vremenske zone ispitivane virtuelne mašine, samog hosta (ukoliko je fizički pristup moguć) i okruženja u kome se trenutno to forenzičko

271 Ovde se nalazi lista Intelovih procesora koji imaju podršku za virtuelizacije: http://ark.intel.com/VTList.aspx, 10.02.2016.

272 AMD platforma za virtuelizaciju: http://sites.amd.com/uk/business/it-solutions/virtualization/Pages/amd-v.aspx, 10.02.2016.

istraživanje sprovodi. Potrebno je evidentirati da li se vremena poklapaju i kolika su odstupanja.[273]

2.8.6. Obezbeđivanje mesta krivičnog dela u virtuelnom okruženju

Da bi se sačuvali svi potencijalni digitalni dokazi, kako u klasičnoj digitalnoj forenzici tako i u forenzici virtuelnog okruženja, veoma je bitno pre započinjanja ispitivanja "uživo" (eng. live), da se onesposobe sve mrežne komunikacije osumnjičenog host-a. To se radi izvlačenjem mrežnog kabla iz fizičke mašine-host-a, odnosno ukoliko host ostvaruje bežičnu (eng. wireless) komunikaciju za izlaz na internet ili intranet, isključivanjem bežičnog uređaj na koji je povezan.

2.8.7. Pristup RAM-u

Da bi se realizovalo virtuelno okruženje sa 16 virtuelnih mašina koji radi pod Windows 7 operativnim sistemom, biće nephodno minimum 16 GB RAM-a. Windows 7 kao minimum RAM memorije zahteva 1 GB RAM-a. Za operativni sistem na hostu biće potrebno minimalno od 512 MB do 4 GB RAM memorije u zavisnosti od OS-a koji je odgovoran za realizovanje virtuelizacije. Ukupna količina memorije će u tom slučaju iznositi 20 GB RAM-a (16 GB RAM memorije po childu i 4 GB na hostu). Ove informacije su važne da bi na osnovu njih digitalni forenzičar imao uvid u ukupnu količinu RAM memorije koja se nalazi na fizičkoj mašini i koliko je od toga iskorišćeno od strane virtuelnih mašina.

Izvlačenje informacija iz RAM memorije moguće je iz onog dela RAM memorije na host-u koji je određen za virtuelnu mašinu koja je pod istragom. To se izvodi uz korišćenje forenzike na živo (pod uslovom da računar nije prethodno isključivan jer bi se time izbrisao sadržaj RAM-a) uz primenu forenzičkih alata za pristupanje digitalnim podacima. Neki od tih alata su *Encase, FTK Imager*, *X-Way Forensic*. Kada se radi slika stanja virtuelne mašine (kod VMware) postoji opcija kojom se bira da li slika stanja da uključi i memoriju. Ukoliko je ispitivana virtuelna mašina imala uključenu

273 Dokumentovanje vremena sa virtuelne mašine ili samog hosta može biti snimljeno kamerom ili fotoaparatom, dok vreme okruženja može biti snimljeno na nekoj zvaničnoj tv stanici ili preko radio aparata.

ovu opciju prilikom kreiranja slike stanja, fajlovi „vmem“ će biti prisutni u slici stanja. Alatka napisana od strane Chris Betza koja može da istražuje ove vmem fajlove zove se *Memparser*.[274] [275]

2.8.8. Virtuelni hard disk

Svaka virtuelna mašina upisuje svoje podatke na virtuelnom hard disku. Za digitalnog forezičara su veoma važne njegova lokacija, ekstenzije, veličina i konfiguracija, jer virtuelni hard disk može sadržati potencijalne digitalne dokaze.

Svaki *child* na *host-u*, mora negde da beleži svoje podatke. Virtuelni hard diskovi mogu biti smešteni na SAN (eng. Storage area network) ili NAS (eng. Network Attached Storage) uređajima ili na lokalnim hard diskovima.

SAN predstavlja uređaj za skladištenje podataka i funkcioniše na nivou blokova podataka i namenjen je enterprise rešenjima. Za razliku od NAS uređaja, SAN uređaji dozvoljavaju deljenje skladištenog prostora na poolove koji mogu da se dodeljuju većem broju servera povezanih direktno (eng. direct attached storage) čime se ostvaruje velika brzina prenosa podataka. Konekcija se vrši optičkim kablom (eng. fibre channel). Sastoji se od velikog broja brzih SAS diskova (15K rpm) a mogu se koristiti i SSD diskovi (eng. solid state disk), ukoliko su performanse i ušteda energije prioriteti. Pojavili su se i vendori koji nude kombinovane sisteme tako da podaci mogu biti dostupni i putem blok pristupa preko Fibre channela ili im se može prići na nivou datoteka sa očekivanim povećanjima brzine i do 100GBps.

NAS predstavlja uređaj za skladištenje podataka i funkcioniše na nivou datoteka, konekciju sa računarima ostvaruje preko lokalne mreže najčešće preko TCP/IP preko etherneta. Sastoji se od veće količine diskova podešenih u raid i najčešće se koriste SAS SCSI ili SATA diskovi. Najčešća uloga NAS-a je fajl-server uloga i uloga pružanja podrške za fajl-sisteme i protokole, za windows umrežavanje CIFS, HTTP, linux umrežavanja SAMBA, NFS.

Informacija o veličini hard diska je bitna zbog organizovanja kopiranja image-a virtuelnog hard diska na svoj forenzički medij sa kog će se vršiti dalja ispitivanja. Ukoliko se radi o virtuelnim hard diskovima

274 Sourceforge, Mamparser, http://sourceforge.net/projects/memparser, 22.02.2016.

275 Forensics science communications, *Digital Evidence : Standards and Principles*, Scientific Working Group on Digital Evidence (SWGDE) International Organization on Digital Evidence (IOCE), Volume 2 - Number 2, April 2000, http://www.fbi.gov/about-us/lab/forensic-science-communications/ fsc/ april2000/ swgde.htm/, 23.06.2016.

velikog kapaciteta proces može znatno da produži istragu. Zato je važno da iz konfiguracionih fajlova digitalni forenzičar sazna što više informacija o broju particija i da uradi sliku samo particije za koju se sumnja da sadrži digitalne dokaze. Te informacije se mogu naći u konfiguracionim fajlovima same virtuelne mašine.

Određene ekstenzije mogu da ukažu na stanje same virtuelne mašine da li je kompletna ili se radi o *slici stanja (eng. snapshot) ili promeni stanja*.[276] Ove promene stanja mogu da svedoče o instaliranju određenih programa i korišćenju istih. U odnosu na klasično istraživanje digitalnog mesta krivičnog dela koja se bavi isključivo fizičkim digitalnim okruženjem, informacije koje se odnose na stanje virtuelne mašine mogu se naći samo u virtuelnom okruženju. Takođe postoje i fajlovi koji nose informacije o konfiguraciji virtuelne mašine koja je predmet istrage. Bitno je razlikovati statičke (definisana veličina) i dinamičke virtuelne diskove (dinamički povećavaju kapacite u zavisnosti od potreba). Bitno je istaći da neki programi za virtuelizaciju mogu da upravljaju virtuelnim hard diskovima na različite načine. Ovo je bitno za digitalnog forenzičara jer nakon određenih operacija nad virtuelnim hard diskovima može doći do značajnih izmena u strukturi. Postoje operacije koje mogu da smanje veličinu virtuelne mašine uklanjajući neiskorišćeni deo prostora (na hostu bi se taj prostor upisao nulama). Postoje i operacije koje mogu da konvertuju dinamičke virtuelne diskove u fiksne i obrnuto da fiksne virtuelne diskove prošire. Moguće je izvršiti i spajanje virtuelnih hard diskova kao i spajanje fizičkog hard diska u novi virtuelni hard disk.

S obzirom da polje virtuelizacije postaje sve veće, Microsoft je tehnike virtuelizacije počeo da intergriše u svojim operativnim sistemima (npr. operativni sistem Microsoft Windows 7). U konfiguracionom meniju koji se odnosi na upravljanje diskovima (eng. Disk management) moguće je napraviti ili priključiti (eng. mount) virtuelni hard disk (VHD) u read only modu. Druga korisna opcija je i podizanje računara (eng. boot) sa virtuelnog hard diska (odnosi se samo na Windows vhd fajlove). Ono što se u Windows Visti zvalo Complete PC backup to se u Windows 7 zove System image backup i čuva se u vhd formatu.[277] To je iz perspektive digitalnog forenzičara izuzetno korisno jer takva slika (koja može sadržati veliku količinu korisnih

276 Ekstenzije ovih fajlova razlikuju se u zavisnosti od progama koji realizuje virtuelno okruženje.

277 Forensics science communications, *Digital Evidence : Standards and Principles*, Scientific Working Group on Digital Evidence (SWGDE) International Organization on Digital Evidence (IOCE), Volume 2 - Number 2, April 2000, http://www.fbi.gov/about-us/lab/forensic-science-communications/ fsc/ april2000/ swgde.htm/, 23.06.2016.

informacija) može da se priključi na forenzički računar u read only modu.

2.8.9. Slike stanja virtuelnih mašina

Slike stanja (eng. snapshots) virtuelnih mašina imaju široke mogućnosti primene. Mogu da se koriste za evidentiranje nastalih promena na operativnom sistemu, povraćaj virtuelne mašine u prethodno radno stanje, ukoliko je instaliranje nekog programa (aplikativnog ili sistemskog) uticalo na promenu u radu operativnog sistema. Za digitalnog forenzičara slike stanja jako su važne, jer se na osnovu saznanja trenutka kada su izvršene nedozvoljene aktivnosti, preko pokretanja slika stanja (od poslednje ka prvoj) na forenzičkoj mašini, uz primenu forenzičkih alata, može izvršiti jednostavan pregled virtuelne mašine za forenzički relevantan trenutak. Na osnovu toga moguće je izvući podatke iz RAM memorije ili virtuelnog hard diska o delovanju virtuelne mašine. Od koristi može biti poređenje slika stanja ispitivane virtuelne mašine radi praćenja promena fajlova ili prilikom identifikacije skrivenih fajlova. Alatka sa kojom može da se prate ove promene nad Vmware virtuelnim mašinama napisana je od strane Zairon-a i zove se *Compare Vmware snapshots*.[278] [279]

2.8.10. Forenzičke kopije virtuelnih mašina

U dosadašnjoj praksi u digitalnoj forenzici, fizičke mašine su pravile dve kopije fizičkog hard diska uz pomoć odgovarajućih forenzičkih alata. Nad jednom kopijom koja se numeriše, izračunavala bi se hash vrednost SHA-1 ili SHA-256 algoritma, sa ciljem da se dokaže nepromenjenost tj. integritet hard diska. Ta kopija predstavlja dokazni materijal i čuva se radi dokazivanja pred sudom, kako bi se dokazalo da nije bilo promene u bitovima. Druga kopija služi za izvođenje forenzičke analize na forenzičkom računaru. U novije vreme kada su se pojavile i virtuelne mašine postalo je neophodno da se pravi i treća kopija hard diska sa osumnjičene mašine. Na ovim kopijama se nalaze virtuelni hard diskovi i njihove slike stanja (eng. snapshots)

278 My infected computer, Tool: Compare VMware snapshots, http://zairon.wordpress.com/2007/ 09/19/tool-compare-vmware-snapshots/, 25.01.2016.

279 Forensics science communications, *Digital Evidence : Standards and Principles*, Scientific Working Group on Digital Evidence (SWGDE) International Organization on Digital Evidence (IOCE), Volume 2 - Number 2, April 2000, http://www.fbi.gov/about-us/lab/forensic-science-communications/ fsc/ april2000/ swgde.htm/, 24.06.2016.

zajedno sa svim folderima i fajlovima, koji opisuju virtuelnu mašinu koja je pod istragom. Treća kopija se koristi za ispitivanje na forenzičkoj virtuelnoj mašini u sličnom okruženju. Pravljenje slike operativnog sistema je izuzetno zahtevan proces jer ne sme biti narušen integritet hard diska. Za tu priliku se uglavnom koristi butabilan disk koji sadrži sve potrebne forenzičke alate. Takođe se može iskoristiti eksterni forenzički uređaj da se sa na njega smesti slika hard diska osumnjičene mašine. Analizu fajlova sa slike hard diska treba vršiti na forenzičkom računaru. Kao i kod svake forenzičke analize treba voditi dokumentaciju o prikupljenim dokazima.

2.8.11. Migracija virtuelne mašine

Jedna bitna karakteristika virtuelnog okruženja (kao njen sastavni deo u velikom broju slučajeva) je operacija premeštanja odnosno migracija virtuelnih mašina. Već je spomenuto da ova operacija donosi niz pogodnosti za administratora virtuelnog okruženja (premeštanje virtuelne mašine sa jednog mesta na drugo i okviru istog fizičkog severa ili na neki drugi fizički sever). To sa druge strane može da omogući učiniocu nedozvoljene aktivnosti prikrivanje dokaza o nedozvoljenom postupanju.

Treba istaći činjenicu da kada virtuelna mašina migrira, prenose se samo informacije koje sadrže podatke o konfiguraciji koji se koriste pri umnožavanju virtuelnih mašina. Međutim, ukoliko se radi o izvozu virtuelne mašine tada će biti prenete sve informacije uključujući i slike stanja (ukoliko su postojale). Ove operacije mogu da utiču na digitalnog forenzičara da donese pogrešne zaključke, u slučaju da nisu sprovedene određene pripremne radnje tj. praćenje virtuelnog okruženja.

Zadatak digitalnog forenzičara virtuelnog okruženja je da na osnovu informacija koje može da prikupi, prikupi podatke o: mrežnim adapterima, mrežnoj konfiguraciji samog virtuelnog okruženja, domenu, virtuelnim hard diskovima, slikama stanja sistema (eng. snapshots), perifernim virtuelnim uređajima, RAM memoriji. Potrebno je da kreira redosled događaja nedozvoljene aktivnosti, koji će biti potkrepljen kako digitalnim dokazima tako i fizičkim.

Forenzički postupak treba da se usmeri ka virtuelnom okruženju, jer se neki od klasičnih alata za digitalnu forenziku ne mogu upotrebiti u potpunosti u virtuelnom okruženju. Nemogućnost se ogleda u kompatibilnosti sa novijim operativnim sistemima i u nepraktičnoj primeni samih alata (dinamička i kapacitetska hardverska razvijenost je tolika da bi se celokupna

istraga drastično usporila). To predstavlja još jednu specifičnost virtuelnog okruženja. Stoga se preporučuje da se forenzički postupak virtuelnog okruženja sprovodi što više "uživo" putem pravljenja slike particija ili delova diska, koji mogu da sadrže potencijalne dokaze. Kada je istraga usmerena ka virtuelnom okruženju u kojoj se jedna virtuelna mašina dovodi u vezu sa nedozvoljenom aktivnošću, ostale virtuelne mašine takođe je potrebno ispitati na forenzičkoj radnoj stanici. Sve ovo ukazuje na određene specifičnosti u pristupu prikupljanja podataka u odnosu na klasičnu digitalnu forenziku fizičkih mašina.

2.8.12. Upotreba dokaza dobijenih iz virtuelnog okruženja u digitalno forenzičkoj analizi

Napredovanjem računarske tehnologije i sa dostupnošću moćnih konfiguracija, olakšava se posao digitalnim forenzičarima primenom virtuelizacije. Forenzičar danas na jednom računaru poseduje mogućnost da ima više instaliranih operativnih sistema tj. više virtuelnih sistema. Oni se ponašaju kao zasebni računari i u pogledu softvera i u pogledu hardvera. Proces digitalno forenzičke analize može se obuhvatiti u 3 ključne faze kao što su to prikazali Kruse i Heiser u svom modelu: dobijanje dokaza, utvrđivanje autentičnosti i analiza.[280]

Christopher Brown, osnivač jedne od vodećih kompanija koja se bavi digitalnom forenzikom (CTO of Technology Pathways LLC) ističe da tokom faze prikupljanja (eng. acquire) digitalni forenzičar treba da snimi i zabeleži što je više moguće osetljivih tj. lako izmenjivih (nestabilnih) podataka sa živog sistema (eng. live).[281] Zatim treba da isključi računar da bi se na kraju kreirale forenzičke kopije (eng. bit stream copy) svih uređaja za skladištenje podataka tj. hard diskova.[282] Većina autora ističe da se pravljenje forenzičke kopije odnosno slike (eng. image) osumnjičenog hard diska realizuje sa programima, koji su bazirani na "*dd alatu*" kao i da se dobijena foreznička

280 Chaouchi H., Laurent-Maknavicius M., Wireless and Mobile Network Security, Security Basics, Security in On-the-shelfand Emerging Technologies, ISTE Ltd and John Wiley & Sons, Inc. USA, 2009.

281 The ARC Group, http://www.techpathways.com/DesktopDefault.aspx, 31.02.2016.

282 Ove bit-stream kopije mogu da budu realizovane kao bit-for-bit kopije ili bit-for-bit plus kopije. Oba pristupa su široko prihvaćena, a razlika je u tome što se kod bit copy plus implementiraju i određeni meta podaci koji imaju ulogu tagovanja dokaznih fajlova sa ciljem očuvanja lanca nadležnosti.

kopija čuva u dd formatu ili nekom koji je baziran na dd-u.[283] [284] [285] Ukoliko forenzičar ne koristi neke od komercijalnih forenzičkih alata već se oslanja na open source forenzičke alate, važno je da poseduje sopstvene prekompajlirane alate za forenzičku akviziciju i analizu (soruce kode kompajliran i na taj način dobijen binarni fajl). Upotreba DD linux alatke koja pruža mogućnost kreiranje forenzičke bit-stream disk-to-disk kopije originalnog hard diska dat je u sledećem primeru:

#dd if=/dev/sda of=/dev/sdb

#dd if=/dev/sda of=/dev/sdb conv=noerror,sync (kreira forenzičku kopiju kod koje proces akvizicije neće da prestane u slučaju nailaska na bad sektor)

Kreiranje forenzičke bit-stream disk-to-image kopije originalnog hard diska :

#dd if=/dev/hda of=/home/hdadisk_evidence.img

Dobijena forenzička kopija tj. slika (eng. image) predstavlja identičnu kopiju originalnog diska.[286] Treba napomenuti da se staro pravilo, da slika mora biti identična originalnom disku, u novije vreme ne primenjuje striktno. Postoji priličan broj adekvatnih formata slike originalnog hard diska koji se najčešće koriste, a koji nisu identični originalnom hard disku, jer mogu sadržati dodatne meta podatke (npr. imena istraživača, beleške istraživača ili hash vrednosti). Primer za jedan takav forenzički adekvatan format je popularni napredni forenzički format (eng. *Advanced forensic format - AFF*) razvijen od strane profesora Simsona Garfinkela i kompanije Basis Technology.[287] S obzirom da ovaj format podrazumeva segmentiranje originalne slike sa dodavanjem zaglavlja, digitalni forenzičar tada svoj nalaz zasniva na ispitivanju slike, koja je na neki način izmenjena odnosno nije identična originalu.[288] [289]

Sa druge strane alat dd daje sliku identičnu originalu, koja može biti kreirana na istom ili na hard disku većeg kapaciteta ili može biti pokrenuta na drugom računarskom sistemu. Ovde se može pojaviti jedan *problem* koji se odnosi na ponovno uspostavljanje originalnog okruženja zbog *različitih*

283 Wikipedia, dd (Unix), http://en.wikipedia.org/wiki/Dd_%28Unix%29, 31.02.2016.

284 Ec-Council Press, *Computer Forensics: Investigating Data and Image files*, Course Technology Cengage learning, USA, 2010.

285 Ec-Council Press, Computer *Forensics: Investigating hard disks, file and operating systems*, Course Technology Cengage learning, USA, 2010.

286 Ec-Council Press, *Computer Forensics: Investigation procedures and response*, Course Technology Cengage learning, USA, 2010.

287 Basis Technology, http://www.basistech.com/e-discovery/ , 13.02.2016.

288 Farmer D. J., *A Windows Registry Quick Reference. eptuners.com,* October 2007, http://www. eptuners. com/forensics/A%20Windows%20Registry%20Quick%20Reference.pdf, 27.06.2016.

289 Johnson T. A., *Forensic Computer Crime Investigation*, Taylor & Francis Group, LLC, 2005.

kombinacija hardverskih komponenti računara. Na primer, ukoliko se slika ispitivanog računara pokreće na računaru koji poseduje drugačije hardverske komponente od ispitivanog računara, operativni sistem će pokušati da prepozna razlike i da doda upravljačke programe za nedostajuće hardverske komponente da bi se operativni sistem uspešno startovao. Međutim u nekim slučajevima sistem neće moći uspešno da se startuje ili će postojati servisi i programi koji neće moći da se pokrenu. Pomenuti problem se odnosi i na *primenu u virtuelnom okruženju*, jer virtuelne mašine mogu da simuliraju samo osnovne hardverske komponente. Nisu predviđene da imaju podršku za veliki broj hardverskih uređaja. To znači da forenzička slika dobijena sa „dd alatom" takođe ne može biti pokrenuta bez dodavanja fajlova sa određenim parametrima potrebnih za podizanje te slike u novom okruženju. Postoje različiti alati koji mogu da reše ovaj problem. Od komercijalnih alata to su: *Encase-ov Physical Disk Emulator*[290] i *Technology Pathways-ov Prodiscover*.[291] Od besplatnih alata to su *Live View* i *Technology Pathways*.[292]

U nauci se polemiše oko toga da li *podaci dobijeni iz virtuelnog okruženja* mogu biti relevantni. Razlozi su upravo izmene, koje moraju da se primene na sliku originalnog hard diska (originalno okruženje), da bi se omogućilo podizanje u virtuelnom okruženju. Ako se zna da je slika pretrpela značajne izmene može biti odmah osporena pred sudom, iako IT stručnjak može tvrditi da promene nemaju uticaja na izmenu dokazne snage prezentovanih dokaza. Neki autori smatraju da virtuelno okruženje u ulozi digitalno forenzičkog alata nema perspektivu što se tiče njihove primene u forenzičkoj analizi.[293]

Međutim, ukoliko se virtuelno okruženje u ulozi digitalno forenzičkog alata primenjuje u kombinaciji sa klasičnim digitalno-forenzičkim pristupom, analiza podataka se može značajno skratiti i mogu se dobiti bolji rezultati. Jedan od modela koji predlaže ovakav pristup je *model Ben i Huebner*.[294] Ovaj tip modela podrazumeva dva nivoa digitalno forenzičkog kadra. Prvi nivo predstavlja digitalno forenzičke istražitelje tj. profesionalce (DFIP) potpuno obučene i sa velikim iskustvom, koji striktno poštuju metode pravila i procedure digitalno-forenzičke istrage. Drugi nivo predstavljaju digitalno

290 Comparex, http://www.pc-ware.com/medialibrary/ central_files/de/ hersteller/ software/ guidance_software/ files/ guidance_07_06_19_ encase_forensic_prosuite.pdf, 16.02.2016.

291 The ARC Group, http://www.techpathways.com/prodiscoverdft.htm, 16.02.2016.

292 Http://liveview.sourceforge.net/, 16.02.2016.

293 Fogie S., *VOOM vs The Virus (CIH)*, 2004, http://voomtech.com/downloads/Shadow%20 Eval%20-%20Fogie.pdf, 25.06.2016.

294 Foster M., Wilson J. N., *Process Forensics: A Pilot Study on the Use of Checkpointing Technology in Computer Forensics*, International Journal of Digital Evidence, Volume 3, Issue 1, 2004.

forenzički istražitelji tj. računarski tehničari (DFIRT) sa manje forenzičkog znanja i iskustva, koji se ne moraju striktno pridržavati forenzičkih pravila i procedura jer nemaju direktan uticaj na proces izveštavanja. Njihova uloga je da pretražuju kopije digitalnih dokaza u cilju pronalaženja što više podataka od potencijalnog interesa za istragu i da sve što pronađu prijavljuju i prosleđuju digitalnim istražiteljima tj. profesionalcima. Profesionalci trebaju da uz pomoć odgovarajućih forenzičkih tehnika potvrde nalaze ili da dalje pretražuju podatake ukoliko za tim ima potrebe.

Što se tiče okruženja jedna od *pouzdanih virtuelnih platformi* koja omogućava kreiranje virtuelnih računara i virtuelnih mreža uz korišćenje hardvera jednog sistema jeste *Vmware*. U forenzičkom smislu ova mogućnost ima brojne prednosti. Na primer, moguće je podešavanje gostujućeg sistema prema forenzičkim potrebama, kreiranje slike stanje sistema, rad na njemu i vraćanje sistema u početno predefinisano stanje. Sa takvog virtuelnog sistema moguće je vršiti sva forenzička ispitivanja, uključujući instaliranja i praćenja zlonamernih programa kao i simulacije sigurnosnih incidentnih aktivnosti. Dodatni benefit uključivanja virtuelne platforme u forenzičko istraživanje jeste mogućnost „zamrzavanja" rada na virtuelnoj stanici. Tako da je suspendovanom virtuelnom sistemu lako dostupan sadržaj fizičke memorije koji se nalazi u datoteci sa ekstenzijom *.vmem. Treba napomenuti da je format ove datoteke veoma sličan sa dd image fajlovima, koji se dobijaju forenzičkim prikupljanjem, tako da se one mogu uspešno analizirati.[295] Kada je reč o prenosivim uređajima, Vmware poseduje opciju gde gostujući operativni sistem nema kontakta sa hostom (domaćinom), čime se blokira veza između prenosivog uređaja i operativnog sistema. Savetuje se da se upotreba Write protect zaštite na operativnom sistemu sa kojeg se podiže Vmware virtuelna radna stanica.

Ilustrativan *primer forenzičke primene u virtuelnom okruženju* bi bio sledeći: računarski tehničari pokreću kopiju prikupljene slike u virtuelnom okruženju (kao virtuelnu mašinu), tretirajući sistem kao normalan sistem i "uživo" pretražuju sve detalje relevatne za istragu. Iako metodologija koju koristi računarski tehničar utiče na integritet prikupljene slike originalnog sistema to ne utiče na istragu. Razlog je taj što računarski tehničar radi sa jednom od kopija digitalnih slika osumnjičenog hard diska. To znači da računarski tehničari koji poseduju dobra tehnička, a manje forenzička znanja mogu primenjivati računarske forenzičke tehnike u fazama bez ugrožavanja

295 Brett Shavers, *VMWare as a forensic tool,* Forensic Focus digital forensics portal for computer forensics and eDiscovery professionals, http://www.forensicfocus.com/vmware-forensic-tool, 16.02.2016.

digitalnih dokaza. Potrebno je da se nad jednom kopijom primeni funkcija haširanja sa ciljem očuvanja integriteta i ta kopija treba biti sklonjena na sigurno mesto. Druga kopija treba biti u posedu digitalnih istražitelja tj. profesionalaca. Ova kopija ostaje netaknuta i forenzički validna. Dakle, nakon urađene forenzičke kopije nju je potrebno implementirati na istovetnom operativnom sistemu, na forenzičkoj virtuelnoj mašini pokrenuti ga i videti šta se tačno dešavalo na operativnom sistemu kroz ispitivanje registry baze (gde se mogu otkriti informacije o tome kad je sistem prvi put instaliran, kad je bio upaljen, kad je isključivan, koji su programi bili instalirani, a koji više nisu prisutni, koji su USB uređaji bili priključeni, i razne druge aktivnosti). Na primer, ukoliko je bio upotrebljen alat CCleaner koji briše registre, ti registri se mogu pronaći ukoliko forenzičar poznaje način kako da rekonstruiše SOFTWARE fajl koji sadrži registre u sebi. Kod Microsofta u Windows direktorijumu u system32/config folderu nalazi se software fajl koji sadrže registre. Ukoliko forenzičar uspe da rekonstruiše šta je taj fajl sadržao, moguće je izvući prefetch registry key. Međutim, ti prefetch registry registry key na sudu nisu prihvatljivi, jer se nemaju sa čim uporediti i potvrditi njihovu autentičnost, ali to forenzičaru može pomoći oko saznavanja šta je na operativnom sistemu urađeno (može se otkriti da su bili instalirani određeni zlonamerni alati). Na osnovu dobijenih informacija od strane računarskih tehničara, DFIP mogu potvrditi sve rezultate koristeći odgovarajuće forenzičke alate, pridržavajući se striktno odgovarajuće forenzičke metodologije tehnike i procedura. Ovakvim forenzičkim pristupom (kombinacijom klasičnog i virtuelnog pristupa), koji se ostvaruje kroz saradnju timova različitih nivoa stručnosti uz korišćenje različitih tipova alata, dolazi se do bržih rezultata u fazi digitalno forenzičke analize. Na taj način se štedi vreme i smanjuje opterećenje na digitalno forenzičke istražitelje tj. profesionalce (što je veoma bitno, zbog nedostatka stručnog kadra forenzičkih profesionalaca).

3. DIGITALNA FORENZIKA WINDOWS I LINUX RAČUNARSKIH SISTEMA

Digitalni podaci su po svojoj prirodi tragovi u računaru. Digitalni podaci generisani ili uneti u računar ostavljaju brojne tragove u Windows operativnim sistemima. Pretraga za podacima podrazumeva priključivanje forenzičkog alata, što znači ostavljanje tragova na digitalne podatke (Lokardov zakon). Izbrisani podaci ostavljaju tragove u nealociranim i slek prostorima diska, a odsustvo podataka ukazuje na anti-forenzičku aktivnost i predstavlja osnovanu sumnju u nedozvoljene aktivnosti. Zlonamerni napadači upotrebljavaju metode anti-forenzike kako prikupljeni digitalni dokazi ne bi bili prihvatljivi na sudu. Na primer, time-stampovi na logovima generišu se od strane log menadžment sistema koji dobija vreme od centralnog sistema u domenu (ntpd). Taj time-stamp može lako da se promeni ukoliko se promeni vreme na domen kontroleru jer će se to vreme ispropagirati svim računarima u domenu i nakon toga ukoliko nastane nedozvoljena aktivnost svi logovi koji nose informaciju o izvedenoj nedozvoljenoj aktivnosti imati pogrešan time-stamp. Kada domen kontroler na taj način dobija lažnu vremensku zonu uz promenjene vrednosti timestampa logova smatra se klasičnim antiforenzičkim napadom. Ukoliko digitalni dokaz bude priložen sudu sa pogrešnim time-stampom taj dokaz neće biti prihvatljiv. Zlonamerni napadači takođe koriste alate koji primenjuju tehniku „skrivanja" tzv. obfuskaciju digitalnog dokaza odnosno njegovu promenu kako digitalni dokaz ne bi bio prihvatljiv za sud. Takođe šifre mogu biti u obfuscated formi na primer fajl ili string nije enkriptovan nego je enkodovan sa base64 (konvertovanje binarnog fajla u ASCII format).

Na primer, virusi ostavljaju svoj kod u zaraženim programima. Tragovi kompromitovanja mogu biti u prisutni u različitim oblicima: u izvornim fajlovima programskog jezika, u objektnim fajlovima (eng. Object files), u izvršnim kodovima, u šel skriptama, u izmenma nad postojećim programima ili čak u tekstualnim fajlovima pisanim od strane napadača. Za istragu je vrlo značajno ukoliko bi se ovi delovi informacija mogli iskoristiti za utvrđivanje izvora napada.[296]

Pre svake istrage podrazumeva se ispitivanje potrebnih preduslova kao što su: postojanje dovoljnog broja obučenih profesionalaca, forenzičke radne stanice i forenzičke laboratorije za oporavak podataka, saradnja sa javnim tužilaštvom i definisana metodologija. U zavisnosti od tipa istrage

296 One A., *Smashing the Stack for Fun and Profit*, Phrack, Volume 7, Issue 49, 1996.

(zvančna ili korporativna) zavisi i ko će dati prvi odgovor na incidnentnu ili nedozvoljenu aktivnost.

First incident response (forenzički inicijalni odgovor) predstavlja prvo suočavanje sa sajber kriminalom gde je najvažnije prikupiti što više dokaza na forenzički ispravan način uz poštovanja tačno određenih procedura. Osoba koja nije obučena za forenzički inicijalni odgovor ne sme prikupljati digitalne dokaze zbog mogućnosti pravljenja grešaka, već to treba da obavi forenzički stručnjak. Kada je reč zvaničnoj istrazi forenzički inicijalni odgovor može da izvede ovlašćeno lice, ali davanje mišljenja kroz izveštaj o konkretnoj nedozvoljenoj aktivnosti mora uraditi i napisati ovlašćeno i stručno lice koje poseduje sertifikat.

Forenzički odgovor ima za cilj pronalaženje što većeg broja dokaza, otkrivanje relevantnih podataka, očuvanje podataka prema njihovoj osetljivosti (eng. volatile), sprečavanje spoljašnje izmene podataka uz pripremu lanca očuvanja nadležnosti za pronađene dokaze sa kompletno dokumentovanim aktivnostima.

U slučaju da je potrebno prikupiti informacije iz sistema koji je u produkciji potrebno je imati odgovorno lice koje će doneti odluku o tome da li će produkcioni sistem biti privremeno isključen ili ne. To odgovorno lice (decision-maker) je nephodno definisati u okviru procedura organizacije. Decision-maker je kontakt osoba kada je u pitanju proces prikupljanja digitalnih dokaza sa sistema koji su u produkciji i ima ovlašćenja da da saglasnost za izvršenje forenzičkih aktivnosti.

U skladu sa navedenim ciljem forenzičkog odgovora posebnu pažnju ćemo posvetiti prikupljanju podataka iz "živog" sistema sa određenih mesta na sistemu koji mogu ukazati na one forenzičke relevantne događaje koji utiču na bezbednost sistema. Prikupljanje podataka kao što je pomenuto podrazumeva prikupljanje podataka sa računarskih sistema i prikupljanje podataka sa mreže. Fokus će biti usmeren ka računarskim sistemima baziranih na Windows i Linux platformama. Biće prikazani alati i tehnike za prikupljanje dokaza sa pomenutih računarskih sistema (eng. host based evidence). Izvršavanje forenzičkih aktivnosti bez metodologije donosi rizik pravljenja grešaka.

3.1. FORENZIČKI ODGOVOR NA NEDOZVOLJENU / INCIDENTNU AKTIVNOST "UŽIVO" NA WINDOWS PLATFORMI

Obezbeđivanje integriteta podataka je od krucijalne važnosti za svaki

tip istrage koji se sprovodi od strane pravosudnih organa. Očuvanje digitalnih dokaza prikupljanjem kroz prikupljanje sistema (forenzičkim kopijama) i dalje će biti standard u narednim godinama.[297] Ipak postoje izuzeci od ovog pravila. U praksi se dešavaju takve okolnosti da u toku istrage ispitivanog računara postoji potreba da se vrši ispitivanje sistema „uživo". *Istraga uživo* dozvoljava forenzičarima da prikupe sa sistema lako izmenjive podatke kojih neće biti u postmortem forenzičkoj analizi.[298]

To znači da se na mestu incidentne radnje odnosno nedozvoljene aktivnosti mora doneti odluka da li da se računar ugasi i ukloni sa mreže, pa da se tek onda prikupljaju potencijalni dokazi ili da se radi digitalna forenzika na "živom" sistemu. Ova odluka ne zavisi samo od incidentne radnje odnosno nedozvoljene aktivnosti već i od tipa samih sistema kao što su na primer veliki kritični sistemi banaka ili sistemi elektronskog poslovanja. Uslovi u kojima se javlja potreba za ispitivanjem računara "uživo" postaju sve učestaliji. Ispitivanje računarskog sistema "uživo" treba da bude strukturisano tako da bude ciljano i da se brzo i efikasno sprovede od strane stručnjaka. U suprotnom raste verovatnoća pojavljivanja novih pravnih izazova odnosno odbacivanja dokaza.

Član 16. i Član 84. Zakonika o krivičnom postupku definišu kada se dokazi mogu odbaciti: „Sudske odluke se ne mogu zasnivati na dokazima koji su, neposredno ili posredno, sami po sebi ili prema načinu pribavljanja u suprotnosti sa ustavom, ovim zakonikom, drugim zakonom ili opšteprihvaćenim pravilima međunarodnog prava i potvrđenim međunarodnim ugovorima, osim u postupku koji se vodi zbog pribavljanja takvih dokaza. Sud je dužan da nepristrasno oceni izvedene dokaze i da na osnovu njih sa jednakom pažnjom utvrdi činjenice koje terete ili idu u korist okrivljenom. Izvedene dokaze koji su od značaja za donošenje sudske odluke sud ocenjuje po slobodnom sudijskom uverenju. Presudu ili rešenje koje odgovara presudi, sud može zasnovati samo na činjenicama u čiju je izvesnost uveren. Sumnju u pogledu činjenica od kojih zavisi vođenje krivičnog postupka, postojanje obeležja krivičnog dela ili primena neke druge odredbe krivičnog zakona, sud će u presudi ili rešenju koje odgovara presudi, rešiti u korist okrivljenog".

Član 84. ZKP: „Dokazi koji su pribavljeni protivno članu 16. stav 1. ovog zakonika (nezakoniti dokazi) ne mogu biti korišćeni u krivičnom postupku. Nezakoniti dokazi se izdvajaju iz spisa, stavljaju u

297 Keith J. J., Bejtlich R., Curtis W. R., *Real Digital Forensics Computer Security and Incident Response*, Addison-Wesley, 2006.

298 Prosise C. Mandia K, *Incident response and computer forensics*, second edition, The McGraw-Hill Companies, 2003.

poseban zapečaćeni omot i čuvaju kod sudije za prethodni postupak do pravnosnažnog okončanja krivičnog postupka, a nakon toga se uništavaju i o tome se sastavlja zapisnik. Izuzetno od stava 2. ovog člana, nezakoniti dokazi se čuvaju do pravnosnažnog okončanja sudskog postupka koji se vodi zbog pribavljanja takvih dokaza".

Ukoliko je reč o forenzici na "živom" računarskom sistemu potrebno će biti snimanje stanje RAM memorije i page fajla, otvorenih fajlova, otvorenih portova i otvorene konekcije prema preporuci koja je detaljno objašnjena u dokumentu *RFC 3227: Guidelines for Evidence Collection and Archiving,* da bi se smanjile promene napravljene na samom sistemu.[299]

Cilj odgovora na incident "uživo" je da se potvrdi da li je postojao incident i ako jeste da li se radi o nedozvoljenoj aktivnosti ili incidentnoj radnji.

Odgovor na nedozvoljenu aktivnost "uživo" u praksi podrazumeva pokretanje samo proverenih komandi na kompromitovanom računarskom sistemu. Mora sa voditi računa o jednom vrlo važnom već pomenutom principu - Lokardovom principu razmene. Kada smo u interakciji sa "živim" sistemom, bez obzira da li smo korisnik, administrator ili digitalni forenzičar, promene će nastati na tom sistemu. Promene na "živom" sistemu dešavaju se kao rezultat procesa rada, snimanja ili brisanja fajlova, prilikom kreiranja ili prekida mrežnih konekcija, a mogu se desiti čak samo protokom vremena odnosno radom samog sistema.[300] Na primer, kod Windows Vista operativnog sistema prema difoltnoj konfiguraciji program za defragmentaciju je podešen da se izvršava svake srede u 03:00 časa.[301] Prilikom istrage ovu informaciju treba uzeti u razmatranje jer korisnici uglavnom ne menjaju ovu difoltnu postavku.

Prema tome promene nastaju samim protokom vremena i u slučaju da digitalni forenzičar izvršava programe na sistemu da bi prikupio informacije i podatke, kako one koji su po prirodi lako izmenjivi (eng. volatile) tako i one koji to nisu.

Za forezničara je važno da poznaje uloge esencijalnih Windows fajlova naročito kada su predmet analize zlonamerni programi: [302]

---

299 RFC 3227: Guidelines for Evidence Collection and Archiving, http://www.faqs.org /rfcs/ rfc3227. html, 22.05.2016.

300 Na primer kod Windows XP operativnog sistema prema defaultnim sistemskim postavkama kreiraće se posle 24h System restore point. Ukoliko sistem radi neprekidno 3 dana bez ikakve interakcije biće sprovedena delimična defragmentacija podataka.

301 Kipper G., *Wireless crime and forensic investigation*, Auerbach Publications Taylor & Francis Group, 2007.

302 Mane Piperevski, *Workshop ICT Forensics Investigation – module 2*, Piperevski & Associates, Beograd 2016.

Ntoskrnl.exe – sadrži u sebi izvršne funkcije kernela Microsoft OS

Ntkrnlpa.exe – sadrži u sebi izvršne funkcije kernela Microsoft OS sa podrškom za fizičke adrese

Hal.dll – hardware abstracion layer implementiran u DLL biblioteku koja sadrži veliki broj funkcija implementiranih na različite načine u zavisnosti od hardvrera, a koja je odgovorna za komunikaciju na hardverskom nivou. HAL.dll vrši konverziju korisničkih inputa u assembler.

Win32k.sys – kernel-mode win32 podsistema – win32 ne podrazumeva da je u pitanju 32-bitni operativni sistem već se odnosi na windows strukturu do Windows 10.

Ntdll.dll – interne pomoćne funkcije i sistemski servisi sa izvršnim modom – najčešća meta napada su funkcije koje imaju executive flag ON u memorijskom prostoru kada se OS pokrene (kao na primer sysinfo, dir). Najčešće zlonamerni napadači pronalaze adrese gde se nalaze ove funkcije i izmene kod sa svojim zlonamernim kodom. Na taj način moguće je pokretanje i izvršenje tog zlonamernog koda. Sa forenzičke tačke gledišta virusi i drugi zlonamerni programi često znaju direktno da preinače konstrukcije ntdll.dll fajla i da inficiraju operativni sistem sa zlonamernim programom.

Win32 subsistem - sadrži različite biblioteke neophodne za rad operativnog sistema: gdi32.dll, user32.dll, advapi32.dll, kernel32.dll. Zlonamerni programi takođe mogu se pronaći u kernel32.dll fajlu.

Kada se startuje operativni sistem prvo se učitavaju drajveri kernela, pa se tek nakon toga učitava ostatak sistema. Opasnost leži u činjenici da ukoliko zlonamerni napadač uspe da integriše zlonamerni program u drajvere kernela, on u potpunosti može da kontroliše operativni sistem. Da bi se takva zlonamerna aktivnost identifikovala forenzičkim aktivnostima, prvo se radi analiza MBRa i analiza windows fajlova sa alatkom Tripwire, Afick ili drugim alatima sa kojima je moguće uraditi komparaciju Windows postojećih fajlova na ispitivanom OS (ili sa onima koji se nalaze na forenzičkoj kopiji) sa bazom poznatih heševa windows fajlova[303]. Na taj način moguće je ustanoviti kompromitovanje određenih sistemskih biblioteka. Nakon pronalaženja sledi dodatna analiza kroz reverzni inženjering kako bi se uočilo kojim je kodom infiriciran regularni fajl.

Forenzičari moraju da prepoznaju koji je fajl sistem kom operativnom sistemu svojstven i da poznaju njihove sličnosti i razlike. U slučaju Windows fajl sistema, razlika između FAT32 i NTFS ne ogleda se samo u veličini

303 Za analizu odnosno komparaciju poznatih heševa sa postojećim fajlovima na ispitivanom Linux operativnom sistemu upotrebljavaju se alati se Tripwire Open source, Aide, Ossec, Samhain.

particija (FAT32 limit 2TB), veličini fajla (FAT32 limit 4GB), i bezbednosnih opcije (FAT32 nema Access Control/Permissions/Security opcije), već i u postojanju ADS (eng. alternate data stream) na NTFS-u. Sa stanovišta digitalnog forenzičara ADS predstavlja funkcionalnosti NTFS particije u kojoj se mogu smestiti i sakriti informacije. Sa ovom funkcionalnošću može se omogućiti dodatni kontejner koji nije vidljiv na fajl sistemu, ali se nalazi u fajl sistemu NTFS-a. U taj kontejner se može smestiti velika količina fajlova i može se povezati na postojeći fajl uz pomoć simboličkih linkova. ADS se može zamisliti kao neka vrsta nevidljivih atačmenta prikačenih uz fajl. U ADS se mogu smeštati i fajlovi (tekstuelni ili binarni) i folderi. Zlonamerni napadači često kriju izvršne fajlove u ADS-u, ali postoje i slučajevi gde se u organizacijama ADS koristi za prikrivanja poverljivih dokumenta kao na primer duplo knjigovodstvo, korupcijske knjige. Treba napomenuti, da od Windows7 OS nije moguće izvršenje binarnih fajlova u skrivenom stream-u komandom start (u Windows XP-u je to bilo moguće) ali je moguće izvršenje simboličkog linka koji je povezan sa izvršnim fajlom i to je ono što zlonamerni napadači u praksi iskorišćavaju.

Način na koji zlonamerni napadači vrše skrivanja zlonamernog programa *ime_zlonamernog_prg.exe* u ADS skriveni stream fajla *vidljivi_fajl.txt* :

C:\alt_data_stream>type *ime_zlonamernog_prg.exe* > *vidljivi_fajl. txt:ime _zlonamernog_prg.exe*

Kreiranje simboličkog linka *link_zlnm_prg.exe* na zlonamerni program skrivenog pod ADS fajla *vidljivi_fajl.txt* :

C:\alt_data_stream>mklink *link_zlnm_prg.exe vidljivi_fajl.txt: ime_ zlonamernog _prg.exe*

Symbolic link created for link_zlnm_prg.exe <<===>> vidljivi_fajl. txt:ime_zlonamernog_prg.exe

Izvršenje zlonamernog programa koji svoj izlaz usmerava na ADS skriveni stream *korisnicke_sifre.txt* fajla *vidljivi_fajl_2.doc*

C:\alt_data_stream>start *link_zlnm_prg.exe* /stext *vidljivi_fajl_2. doc: korisnicke_ sifre.txt*

Ima dosta načina na koji digitalni forenzičari mogu videti koji su to fajlovi koji kriju ADS kontejnere i nakon toga se vrši izvlačenje sadržaja tog kontejnera sa sistema. Jedna od osnovnih alatki koja daje uvid u to da li postoje fajlovi koji kriju ADS kontejrner je Windows-ova alatka „dir /R", ali je ona ograničena na folder, međutim postoje i alati koji skeniraju ceo drajv i prikazuju da li postoje ADS skriveni streamovi kao što je LADS[304] (List

304 Https://www.aldeid.com/wiki/LADS

Alternate Data Streams by Frank Heyne) ili Streams.exe[305] od SysInternals-a.

U daljem tekstu biće naveden *primer Lokardovog principa sa Alatom Netcat* koji za cilj ima demonstraciju pomenutog principa i prikupljanje podataka sa ispitivanog računara. Alati koji će biti korišćeni su Netcat,[306] Pmdump,[307] i Strings.[308] Potrebne su dve radne stanice jedna ispitivana i jedna forenzička. Postupak je sledeći:

1. Na ispitivanoj mašini pokreće se alatka Netcat sa sledećim parametrima:

c:\pmdump.exe -list | nc.exe IP_ADRESA_FORENZIČKE_RADNE_STANICE 9898

Umesto pmdump.exe -list komande može biti bilo koja komanda koja se pokreće sa ciljem prikupljanja podataka sa živog sistema. Izlaz komande šalje se preko TCP kanal na port 9898 na forenzičku radnu stanicu gde će se podaci snimati u fajl pmdump.txt umesto na hard disk ispitivanog računara.

2. Na forenzičkom računaru pokreće se alatka Netcat sa sledećim svičevima:

"*c:\nc.exe -v -l -p 9898 > pmdump.txt*"

Ova komanda podrazumeva da program netcat sluša (switch -l) na portu (switch -p) 9898 u verbose modu (switch -v).[309] Nakon pokrenute komande na ispitivanom računaru svi podaci koji se šalju na TCP port 9898 forenzičke radne stanice biće snimljeni u pmdump.txt.

U task menadžeru ispitivanog sistema možemo primetiti nc.exe sa identifikatorom procesa (eng. PID) koji je potrebno zapisati jer je to upravo nov proces koji se pridodao ispitivanom računaru.

Ova komanda podrazumeva pokretanje programa netcat u klijentskom modu i da se konektuje na port 9898 IP-adrese ispitivanog računara. Nakon uspostavljene konekcije sa ispitivanim računarom pojaviće se komandno okruženje (eng. command prompt) sa verzijom operativnog sistema. Komande koje budu pozivane izvršavaće se kroz

305 Https://technet.microsoft.com/en-us/sysinternals/bb897440

306 Http://joncraton.org/media/files/nc111nt.zip, 20.05.2016.

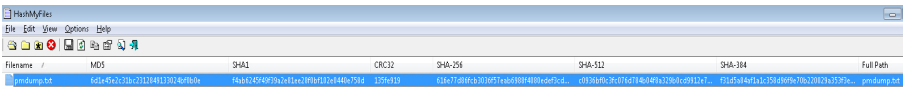
307 Http://ntsecurity.nu/downloads/pmdump.exe, 20.05.2016.

308 Http://Corrupteddatarecovery. com, http://download. corrupteddatarecovery. com/ download-file/ strings.exe, 20.05.2016.

309 Netcat alataka može biti pokrenuta i u nevidljivom modu (switch -d) izvršavajući određeni program koristeći switch, na šta forenzičar treba posebno da obrati pažnju ukoliko je takva komanda pokrenuta na ispitivanom računaru. To može biti i pokazatelj namera zlonamernog korisnika.

uspostavljenu konekciju.

Nakon što se komanda izvrši sesija se prekida pritiskom tastera CTRL-C, neophodno je uraditi SHA-1 ili SHA-256 checksum pmdump.txt fajla sa alatkom md5sum za dokazivanje autentičnosti. Zbog veće pouzdanosti mogu se koristiti alati (Quickhash,[310] Hashmyfiles,[311] MD5 & SHA Checksum Utility[312]) koji pružaju dodatne heš algoritme. Na primer, alatka *Hashmyfiles* generiše MD5, SHA1, CRC32, SHA-256, SHA-384 heš vrednosti. Izlaz ove alatke prikazan je na sledećoj slici:



Slika 12. Izlaz alatke Hashmyfiles sa različitim heš vrednostima

Treba napomenti da forenzičar može koristiti i netcat varijantu koja se zove *Cryptcat*.[313] Ona omogućuje zaštićen prenos podataka preko mreže tj. TCP kanalom pružajući zaštitu poverljivosti i autenitčnosti. S obzirom da je komunikacija šifrovana napadač nije u mogućnosti da vidi podatke koji se prikupljaju prilikom forenzičkog ispitivanja.

Za iščitavanje prikupljenog fajla koji predstavlja listu procesa u memoriji mogu se koristiti ili besplatne alatke kao što su Systernals *Strings.exe,*[314] ili FoundStone-ov *BinText.exe*[315] ili određeni komercijalni programi kao što su *AccessData FTK,*[316] *ENCASE.*[317] U njemu će biti prikazana i IP-adresa forenzičkog računara, što predstavlja i demonstraciju Lokardovog principa.

Programi koji se koriste za prikupljanje informacija (bez obzira što se podaci ne snimaju direktno na hard disk ispitivanog računara) imaju određeni uticaj na "živi" sistem. Na primer, neki programi će morati da isčitavaju više registarskih ključeva iz baze registra i putanje do ključeva biće učitane u memoriju. Na primer, Windows sistemi imaju implementiran *prefečing*

310 Https://sourceforge.net/projects/quickhash/, 20.07.2016.
311 Http://www.nirsoft.net/utils/hash_my_files.html, 05.02.2013.
312 Https://raylin.wordpress.com/downloads/md5-sha-1-checksum-utility/, 20.07.2016.
313 Http://sourceforge.net/projects/cryptcat/files/, 05.02.2016.
314 Mark Russinovich, Strings v2.52, Windows Sysinternals, http://technet.microsoft.com/en-us/sysinternals/ bb897439.aspx, 11.02.2016.
315 Softpedia, http://www.softpedia.com/developer/Foundstone-Inc-16182.html, 05.02.2016.
316 Forensic Toolkit (FTK), AccessData, http://www.accessdata.com/products/digital-forensics/ftk, 05.02.2016.
317 EnCase Forensic, Guidance Software, http://www.guidancesoftware.com/encase-forensic.htm, 05.02.2016.

(eng. prefetching) *za aplikacije*, koji služi za ubrzavanje svakodnevnog rada u Windows okruženju. [318] Ono što je važno pomenuti je da se sve akcije (vezane za određene aplikacije, ne samo podizanje sistema već i korišćenje određenih delova tih programa), koje pokreće korisnik administrator ili digitalni forenzičar na računarskom sistemu beleže u određeni direktorijum "C:\Windows\Prefetch" (kada je u pitanju Windows XP). Kao benefit se dobija brže podizanje sistema, odziv sistema kao i brži odziv aplikacija. Analogijom se može uporediti sa nekom vrstom keša.

Ukoliko digitalni forenzičar pokreće program koji je već pokrenut na sistemu od strane korisnika biće modifikovano vreme, poslednji pristup i sadržaj prefetch fajla. Ukoliko digitalni istražitelj pokreće program, koji ne postoji na sistemu kreiraće se novi prefetch fajl u C:\Windows\Prefetch direktorijumu. Kod Windows XP Limit kreiranja ovih fajlova je 128 nakon čega se direktorijum prazni, ali ostaju 32 najčeće korišćena prefetch faja. Kod Windows Viste limit kreiranje jeste 134 fajla.[319] Na osnovu navedenog proizlazi da je digitalnom forenzičaru potrebno ne samo znanje da se ove promene dešavaju već je potrebno i dokumentovanje tih promena, da bi mogli da objasne uticaj njihovih akcija na ispitivani sistem. Na primer, ukoliko korisnik pokrene aplikaciju *Notepad*, sistem će prifečovati fajl smeštajući ga u prifeč direktorijum i imenovati ga sa ekstenzijom .pf na kraju. Uz ime postojaće i dodatni heksadecimalni karakter koji predstavljaju heš vrednost putanje do fajla, što bi u praksi izgledalo kao "notepad.exe-598342B8". Ukoliko takav fajl postoji za digitalnog forenzičara to je signal da je ta aplikacija pokrenuta na sistemu. Takođe je važno spomenuti i da *prifeč fajlovi sadrže i metadata podatke* kao na primer: datum kreiranja prifeč fajla, koliko je puta startovan program, kada je poslednji put startovan program, volume i putanju odakle je program startovan. Ti podaci forenzičaru mogu ukazati na datum kada je program prvi put startovan (pod pretpostavkom da prethodni prifeč fajl nije obrisan i da na njegovo mesto nije kreiran novi) i na putanju (uređaja ili drajva) sa kog je program startovan. *Programi koji mogu da izvuku metadata podatke iz prefetch fajlova* su bintext (već pomenut), koji ima grafički interfejs, prefetch_info.[320] On se pokreće iz komandnog okruženja i zgodan je za foreziku "uživo". Pored toga tu su i alati: WFA sa

318 Windows XP, Vista, Windows 7 po difoltu imaju uključen prefetch-ing dok je kod Windows 2003 i Windows 2008 ostavljena mogućnost da se uključi, ali je po difoltu ona onemogućena.

319 Kipper G., *Wireless crime and forensic investigation*, Auerbach Publications Taylor & Francis Group, 2007.

320 Http://redwolfcomputerforensics.com/downloads/prefetch_info.zip, 25.04.2016.

grafičkim interfejsom, TzWorkLLC-ov windows prefetch parser.[321] Ovaj alat se pokreće iz komandnog okruženja skripte Harlana Carvey, koja se dobijaja uz knjigu Windows forensic analysis[322] i koji radi sa prefetch fajlovima koje generiše Windows XP i Windows Vista. Alat SuperFetch files dumper je pogodan za analizu superfetch fajlova (sa ekstenzijama .db), koje generišu Windows Vista, Windows 7, Windows 2008. [323] Svi ovi programi mogu forenzičaru pomoći u kreiranju slike o redosledu događaja na ispitivanom računaru.

Prema preporuci NIST-a redosled prikupljanja lako izmenjivih podataka sa računarskih sistema radi se na sledeći način:[324]

1. Mrežne konekcije;
2. Logovani korisnici i sesije;
3. Sadržaji memorije;
4. Pokrenuti procesi;
5. Otvoreni fajlovi;
6. Mrežna podešavanja;
7. Vreme operativnog sistema.

3.1.1. Podaci od značaja privremenog karaktera na Windows-u - datum i vreme

Operativni sistem skladišti informacije o tekućem vremenu (pomeranju vremena) i vremenskoj zoni. Ove informacije su izuzetno korisne prilikom izgradnje hronologije događaja ili korelacije događaja između različitih sistema. Forenzičar treba da bude svestan da može postojati razlika u vremenu između onog koje prikazuje operativni sistem i onog vremena iz BIOS-a, zbog specifičnih setovanja u operativnom sistemu kao što su vremenske zone.[325] Prikupljanje podataka o vremenu i datumu će biti od velike

321 Windows Prefetch Parser, TZWorks Limited Liability Company, http://www.tzworks.net/ prototype _page.php?proto_id=1, 27.05.2016.

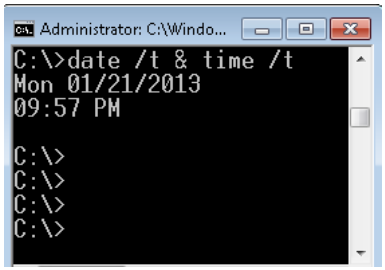
322 Harris R., *Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem*, Journal Digital Investigation: The International Journal of Digital Forensics & Incident Response, vol. 3, 2006, str. 44-49.

323 Http://code.google.com/ p/ rewolf-superfetch-dumper/downloads/ detail?name= rewolf. superfetch. dumper.v1.0.zip&can=2&q=, 25.05.2016.

324 National Institute of Justice, *Electronic Crime Scene Investigation. A Guide for First Responder,* 2001, https://www.ncjrs.gov/pdffiles1/nij/187736.pdf, 11.07.2016.

325 National Institute of Justice, *Electronic Crime Scene Investigation*. A Guide for First Responder, 2001, https://www.ncjrs.gov/pdffiles1/nij/187736.pdf, 11.07.2016.

važnosti, jer će doprineti stavljanju u kontekst podataka prikupljenih u daljem toku istrage i pomoći će u izradi precizne hronologije dešavanja na sistemu. Treba napomenuti i to da je od značaja i vreme neprekidnog rada računarskog sistema tzv. eng. uptime. Ono se može dobiti putem posebnog alata koji je dostupan na majkrosoftovom sajtu.[326] Preporuka je i da se paralelno uslika i realno vreme npr. slikanjem vremena na zidnom satu. Važna informacija za dalji tok istrage je i vremenska zona podešena na ispitivanom računaru.[327]



Slika 13. Prikaz datuma i vremena na sistemu

Sa preciznom analizom datuma i vremena mogu se proizvesti dokazi o tome kada su se određene akcije desile. Kada se radi u različitim vremenskim zonama ili usled promene vremena, bitno je konstatovati da li je vreme prevedeno na univerzalno kodirano vreme tzv. UTC ili se koristi lokalno vreme. Ključ u registarskoj bazi koji sadrži informacije i o vremenskoj zoni i promeni vremena nalazi se:

„HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation“

Iako ova informacija nije direktno korisna, od izuzetnog je značaja pri konvertovanju vremenskih pečata, ukoliko je računar premešten ili ukoliko je vremenska zona pogrešno podešena.

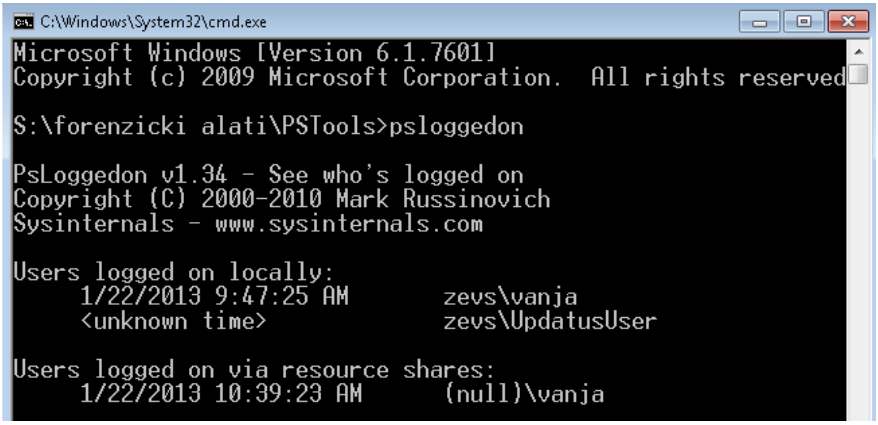
3.1.2.Podaci od značaja privremenog karaktera na Windows-u - logovani korisnici na sistemu i sesije

Prilikom forenzičkog istraživanja ispitivanog računara biće značajan

326 Http://www.microsoft.com/, 27.05.2016.

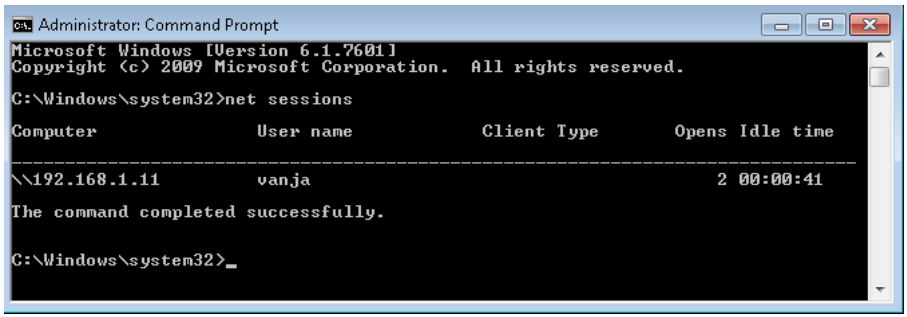
327 Windows sistemi koji koriste NTFS fajl sistem čuvaju podatke o vremenu u UTC formatu, dok sistemi sa FAT fajl sistemom čuvaju podatke o vremenu iz lokalnog sistemskog vremena. File Times, Microsoft, http://msdn.microsoft. com/ en-us/ library/ windows/ desktop/ ms724290%28v =vs.85%29.aspx, 28.05.2016.

za dalji tok istrage *spisak ulogovanih korisnika* na sistem kao i postojeće *sesije*. U nastavku će biti prikazani alati koji digitalnom forenzičaru omogućuju da to utvrdi. Korisnici mogu biti prijavljeni na sistem lokalno, preko konzole ili mogu biti udaljeni korisnici koji koriste "net use" komande i deljene resurse ispitivanog računara. Dobijene informacije o korisnicima i sesijama na sistemu pružaju *uvid u startovanje procesa od strane korisnika/zlonamernog korisnika, vlasništva nad fajlovima kao i poslednji pristup fajlovima*. Ukoliko se ovi podaci posmatraju zajedno sa podacima iz bezbednosnih logova događaja (eng. security event log), u slučaju da je uključen auditing na sistemu, može doprineti još boljem razumevanju ispitivanog slučaja na sistemu. Bez konfigurisanog praćenja tragova aktivnosti na sistemu izuzetno je teško uspešno ispitati sigurnosni incident. Besplatna alatka koja digitalnom forenzičaru može pružiti pomenute informacije o korisnicima je *psloggedon*. Izlaz izvršene komande psloggedon dat je na sledećoj slici:



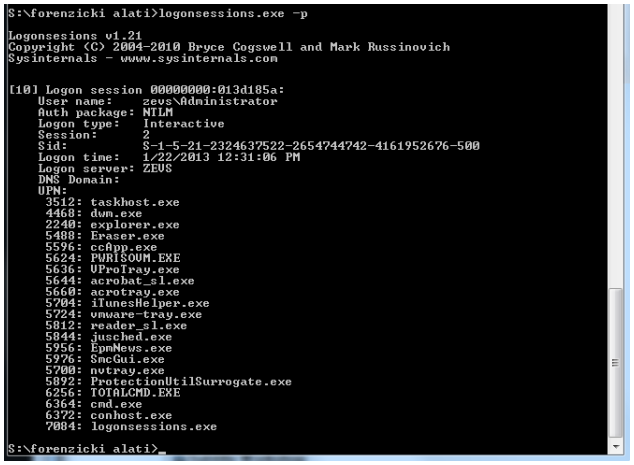
Slika 14. Prikaza ulogovanih korisnika lokalno i udaljeno preko deljenih resusra na Windows 7

Izlaz komande net sessions (koja mora da bude pokrenuta sa nalogom koji ima administratorske privilegije) dat je na sledećoj slici i pokreće se komandom net sessions.



Slika 15. Prikaz imena udaljenog korisnika koristi deljene resurse sa IP-adresom

Besplatan alat *logonsession.exe* daje prikaz postojećih sesija na sistemu, koji forenzičaru može da ukaže na tip logovanja, tip autentifikacije na sistem (NTLM, Kerberos, RADIUS), aktivne procese i druge korisne informacije, dat je na sledećoj slici i pokreće se komadnom logonsessions.exe -p.



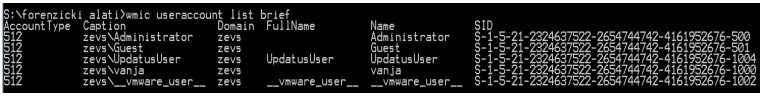
Slika 16. Prikaz postojećih sesija na sistemu sa alatom logonsessions.exe

Besplatna alatka *netusers* prikazuje poslednja vremena logovanja korisnika na sistem. Pošto se ti podaci nalaze u registru bazi i ova alatka može da se koristi na "živom" sistemu i prepoznaje samo logovanja korisnika preko windows autentifikacionog mehanizma.

Slika 17. Prikaz detalja vezanih za poslednje vreme logovanja korisnika sistema

Alatkom *wmi* koja je sastavni deo windows operativnog sistema može se dobiti lista korisničkih naloga na sistemu:

„c\ wmic useraccount list brief"



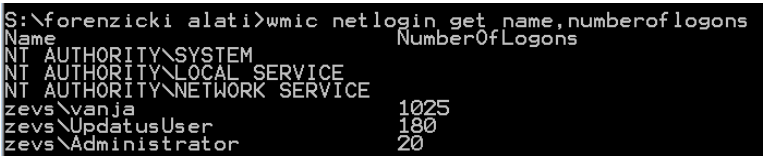
Slika 18. Prikaz postojeći korisničkih naloga na sistemu

Listu sa više detalja moguće je dobiti sa komandom:

„C:\wmic useraccount"

Ova alatka može pružiti informaciju o tome koliko se korisnik logovao puta na sistem:

„c:\wmic netlogin get name,numberoflogons"



Slika 19. Prikaz broja logovanja za korisnike na sistemu

Ukoliko sistem ima veliki broj korisnika moguće je dobiti informaciju o broju logovanja putem pretrage na osnovu imena sa komandom:

"c:\ wmic netlogin where (name like "%vanja%") get numberoflogons"

U windows operativnom sistemu moguće je dobiti informaciju o tome koji se korisnik poslednji logovao na sistem. Te informacije se nalaze u

registru bazi:

"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" kada je reč o Windows XP sistemu, odnosno

"HKLM\Software\Microsoft\Windows\CurrentVersion\Authentication\LogonUI" kada je reč o sistemima Windows Vista 7, 8.

Svi ovi podaci mogu biti korisni forenzičaru jer mogu da doprinesu kontekstu u daljem toku istrage. Dobijeni podaci mogu ukazati na činjenicu da se određeni korisnik logovao više puta od uobičajenog prosečnog broj puta, što može biti i vredan bezbednosni parametar.

3.1.3. Podaci od značaja privremenog karaktera na Windows-u - dump memorijskog procesa i kompletan dump memorije

Prikupljanje podataka iz memorije sistema je važno za forenzičku istragu jer se tu mogu pronaći dragoceni podaci. *Podaci koji se mogu izvući su sledeći*: ulogovani korisnici, sistemsko vreme, otvoreni fajlovi, informacije o aktivnim procesima, memorija procesa, sadržaj *Clipboard*-a, mapirani procesi i portovi, status mreže, mrežne informacije, mrežne konekcije, mapirani drajvovi, deljeni resursi (fajlovi, direktorijumi), informacije o servisu ili drajveru, istorija komandi.

Da bi forenzičar uspeo da izdvoji deo memorije koje se odnosi na određeni ispitivani proces Microsoft je omogućio alatku koja se zove *Userdump.exe.*[328] Treba je koristiti kada forenzičar zna da je napadač pokrenuo maliciozni proces, ali tek treba utvrditi o kom procesu je reč. Ova alatka omogućava forenzičaru da prikupi memorijski prostor koji koristi bilo koji izvršni proces. S obzirom da alatka userdump.exe upisuje rezultate direktno na disk upotreba netcat alata nije izvodljiva. Zbog navedene okolnosti, a da bi forenzički "uticaj" na ispitivani sistem bio što manji, preporuka je da se za ovu namenu mapira jedan mrežni disk i to treba dokumentovati. Razlog leži u činjenici da prikupljena memorija može biti većeg kapaciteta. To se radi sa komandom "net use":

c:\>net use o: \\192.168.1.5\podaci_prikupljanje

Nakon toga pokreće se Userdump komanda:

c:\>userdump.exe -p koja će izlistatati procese, nakon toga pokreće se

328 User Mode Process Dumper Version 8.1, Microsoft, http://www.microsoft.com/en-us/download/ confirmation.aspx?id=4060, 06.06.2016.

c:\>userdump.exe broj_sumnjivog_procesa o:\dump_procesa.dmp

Treba reći da se ID sumnjivog procesa može dobiti i iz pomenute alatke *"pslist.exe"*

Sa određenim switchevima moguće je uraditi i dump više od jednog procesa u okviru jedne komande. Izlaz alatke userdump prikazan je na sledećoj slici:

```
S:\forenzicki alati\userdump\x64>userdump 4384 testni_dump
User Mode Process Dumper (Version 8.1.2929.5)
Copyright (c) Microsoft Corp. All rights reserved.
Dumping process 4384 (U.S.RoboticsUSBPhone.exe) to
S:\forenzicki alati\userdump\x64\testni_dump...
The process was dumped successfully.
```

Slika 20. Prikaz uspešno izvršenog dumpovanja procesa komandom userdump.exe

Da bi se izvršila validacija dumpovanog procesa postoji alatka koja se zove dumpchk.exe dostupna na Debbuging tools for Windows.[329] Treba reći da proces u memoriji umesto u ASCII može biti i u Unicode formatu pa je za pregled dumpa potrebno korstiti alat koji može da radi i ASCII i Unicode. O jednoj takvoj alatki je već bilo reči i zove se *Strings.*[330] Kada je reč o Linuxovom strings alatu treba napomenuti da on po difoltu ne prikazuje Unicode stringove već se to mora posebno omogućiti.

Jako je važno ispitati sumnjivi proces pre gašenja sistema, jer može biti podešen tako da se nakon izvršenja obriše i da bude samo u memoriji. Opisani način je jedni način da se maliciozni proces otkrije, dokaže njegovo prisustvo i spreči dalja šteta. U suprotnom, odnosno da je računar isključen ovaj dokaz o malicioznom programu bio bi izgubljen.

Ukoliko forenzičar ima potrebe da prikupi kompletan sadržaj sistemske memorije koji može sadržati delove malicioznog procesa, a ne samo procesa, to se može uraditi sa alatima posebne namene. Forenzičar mora da bude svestan da prilikom postupka prikupljanja memorije na "živom" sistemu sa programskim alatima, može doći do izmene podataka. Razlog je taj što uvođenje novog programa u memoriju može izmeniti podatke iz memorije koji su po karakteru lako izmenjivi (novi podaci zauzeće prostor koji su postojeći zauzimali).

U daljem tekstu biće predstavljeni alati koji su dominantno prisutni u praksi kada je reč o prikupljanju podataka iz fizičke memorije. Jedan od

329 Download the WDK, WinDbg, and associated tools, Microsoft, http://msdn.microsoft.com/en-us/windows/hardware/gg463009.aspx, 07.06.2016.

330 Mark Russinovich, Strings v2.52, Windows Sysinternals, http://technet.microsoft.com/en-us/sysinternals/ bb897439.aspx, 07.06.2016.

takvih alata koji služi za kreiranje slike iz memorije *UNIX dd* alat koji je kao takav ili uz određene modifikacije sastavni deo mnogih forenzičkih kompleta. DD format je podržan od većine forezničkih programa. Modifikovana dd verzija čiji je autor George M. Garner iz GMG system inc. koja je u sastavu FAU alata može kreirati dump cele memorije (ali samo kroz korisnički mod).[331] Način upotrebe je opisao Keith Jones:[332]

c:\dd.exe rt if=\\.\physicalmemory of=o:\fullmemorydump.dd bs=4096

Međutim FAU dd radi samo na Windows 2000, Windows XP, jer je kod ovih sistema dozvoljen pristup fizičkoj memoriji (odnosno objektu \\.\ PhysicalMemory) iz korisnčkog moda (eng. user mod). [333] Od Windows XP SP2 i kasnije promenjen način adresiranja i pristupa objektu \\.\ PhysicalMemory, koji nije više moguć kroz korisnički mod već samo kroz drajvere kernel moda (eng. kernel-mode driver). S obzirom da se podaci tokom prikupljanja menjaju u RAM-u preporuka je da se heširanje uradi tek nakon što se podaci prikupe na forenzički disk, a ne u toku prikupljanja.[334] [335]

Druga alatka čiji je autor Matt Shannon iz Agile Risk Management-a, koja je slična DD-u zove se *Nigilant32*. Ova alatka omogućava forenzičaru da prikaže hard disk, da prikupi podatke iz RAM memorije i da snima stanja (eng. snapshot) trenutno pokrenutih procesa i otvorenih portova. Ova alatka koristi grafički interfejs, jako malo prostora zauzima na sistemu (1MB kada je učitan u memoriju) i ima mali uticaj na ispititvani sistem. Može se pokretati sa USB-a ili CD-a. Podržava Windows 2000, XP i 2003.

Treća alatka jeste deo *ProDiscover Incident Response* seta alata kompanije Technology Pathway. Dozvoljava forenzičaru da prikupi sadržaj fizičke memorije sa "živog" sistema.[336] Uz pomoć ovog seta alata moguće je utvrditi da li je sistem kompromitovan i omogućava prikupljanje potrebnih dokaza. Istraživanje može obuhvatati kreiranje slike fizičkog diska ili

---

331 George M. Garner Jr. , Forensic Acquisition Utilities, http://www.gmgsystemsinc.com/fau/, 13.04.2016.

332 Haruyama T., Suzuki H., One-byte Modification for Breaking Memory Forensic Analysis, BlackHat Europe, Mart 2012.

333 Kaufman R. J., *Computer Incident Response*, Texas Security Symposium Agenda, San Antonio TX, 2003.

334 Harrison W., Heuston G., Morrissey M., Aucsmith D. Mocas S., Russelle S., *A Lessons Learned Repository for Computer Forensics*, International Journal of Digital Evidence, Vol. 1 No. 3, 2002, http://www.ijde.org /docs/ 02_fall_art2.html, 21.06.2016.

335 Grubor G., *Funkcionalni model istrage kompjuterskog kriminala*, Ziteh 2010.

336 The ARC Group, http://www.techpathways.com/prodiscoverir.htm, 14.04.2016.

memorije. Zahteva se instaliranje serverskog apleta (PDServer program) na ispitivanom računaru da bi se realizovao postupak prikupljanja podataka, što ga čini više prihvatljivim u korporativnom okruženju.

Četvrta alatka *KnTDD* koja je deo KntTools forenzičkog seta alata čiji je autor George Garner rešava problem pristupa objektu \\.\PhysicalMemory preko drajvera kernel-moda.[337] Podržava gotovo sve Windows operativne sisteme od Windows 2000 do Windows 8 RTM uključujući i 64-bitne verzije pomenutih sistema. Uz pomoć ove alatke moguće je konvertovati sliku memorije iz "raw" formata u Microsoft crash dump format i analizirati dobijene rezultate uz pomoć Microsoft debugging tools-a. Kreiranje slike memorije može da se prikuplja na eksternom uređaju ili putem mreže. Forenzičar prilikom prikupljanja mora biti svestan lokardovog principa razmene i shodno tome mora voditi računa da sve što radi na "živom" sistemu detaljno dokumentuje. Ovaj set alata namenjen je pre svega vojsci, pravosuđu, vladinim agencijama i visokoškolskim ustanovama. Za korporacijske potrebe moguće ga je koristiti u zavisnosti od slučaja.

MDD je alatka kreirana od strane kompanije ManTech International Corporation služi za prikupljanje slike memorije sa ispitivanog računara iz komandnog okruženje Windows OS.[338] Može prikupljati slike memorije sa Windows 2000, XP, Vista i Windows Server 2003 SP1 ali je ograničena sa prikupljanjem do 4GB RAM podataka.

Win32DD i wind64dd su alatke čiji je autor Matthieu Suiche, koje služe za prikupljanje sadržaja fizičke memorije.[339] Od dodatnih pogodnosti ima opciju da kreira crash dump (sličan Windows crash dump fajlu) kombatibilan sa Windows debugger alatima. Postoji u 32-bitnoj i 64-verziji.[340] Od operativnih sistema podržava Microsoft Windows XP, 2003, 2008, Vista, 2008 R2, 7.

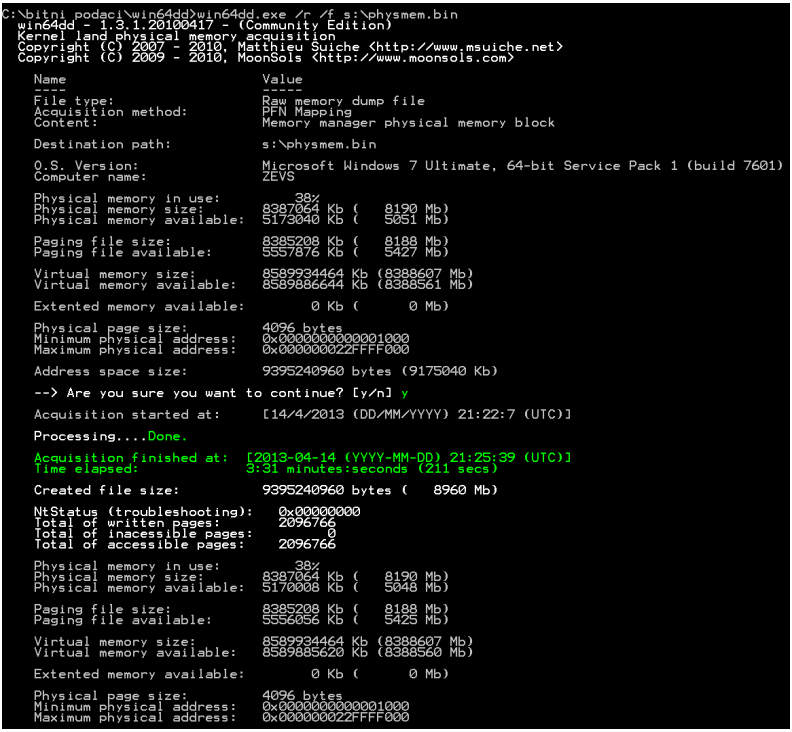
Jedan primer prikupljanja fizičke memorije sa računarskog sistema Windows 7 x64 biće prikazan na sledećoj slici:

337 KnTTools with KnTList, GMG Systems, Inc., http://www.gmgsystemsinc.com/knttools/, 14.04.2016.

338 Http://sourceforge.net/projects/mdd/files/latest/download?source=files, 14.04.2016.

339 Http://www.moonsols.com/windows-memory-toolkit/, 14.04.2016.

340 Korać V., *Infrastruktura sa javnim ključevima u funkciji zaštite informacionog toka i elektronskog poslovanja*, Arheologija i prirodne nauke, specijalna izdanja, Centar za nove tehnologije, 2010.



Slika 21. Prikupljanje sadržaja fizičke memorije alatom win64dd.exe

Winen je samostalna alatka kompanije Guidance Software koja dolazi u sklopu forenzičkog kompleta Encase (od verzije 6.11) i u sklopu kompleta Helix (od verzije 2.0) i služi za prikupljanje sadržaja fizičke memorije.[341] Pokreće se iz komandnog okruženja. Može se pokrenuti sa prenosnog drajva (npr. USB) koji se priključi na računar koji se ispituje. Ima jako mali otisak u memoriji sa minimalnim uticajem na sistem. Prikupljen sadržaj RAM memorije smešta se u fajl .E0XX. Postoji 32-bitnoj i 64-bitnoj varijanti. Podržava sve Windows OS počev od Windows 2000.

FastDump je alatka kompanije HBGary, koja služi za prikupljanje sadržaja fizičke memorije.[342] Ima jako mali otisak sa minimalnim uticajem na memoriju. Sav kod je statički linkovan tako da nema učitavanja DLL-ova. Veličina mu je samo 80KB. Postoje dve verzije ove alatke Fastdump

341 Http://www.guidancesoftware.com/, 14.04.2016.

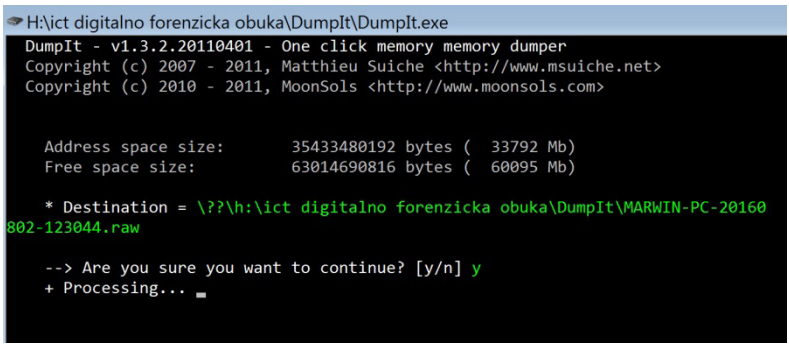
342 Http://www.hbgary.com/free-tools#fastdump, 14.04.2016.

community verzija, koja je besplatna i Pro verzija. Fastdump community podržava samo 32 operativne sisteme sa prikupljanjem podataka iz RAM memorije do 4GB. Ova verzija ne podržava Windows Vistu, Windows 2003 i Windows 2008. Pro verzija podržava sve Windows OS kako 32-bitne tako i 64-bitne sa mogućnošću prikupljanja podataka iz RAM više od 4GB.

Najčešće korišćena besplatna alatka od strane forenzičara, sa kojom je moguće izvršiti kompletno kopiranje sadržaja RAM memorije u lokalni imidž fajl zove se Dumpit. Ima jako mali otisak u memoriji i bezbedan je za korišćenje u „live" forenzici, jer neće prebrisati nešto što je već bilo u memoriji zbog izuzetno malog impacta na memoriji oko 200k. Nema ograničenja po pitanju veličine rama i radi pod svim verzijama Windows OS (podržane i 32bit i 64bit verzije) ali zahteva administratorske privilegije za njegovo pokretanje na operativnom sistemu. Nakon kreiranja imidža taj fajl može se analizirati sa alatom koji se zove scalpel. Postoje i drugi alati sa kojima se radi carving nad prikupljenom volatile memorijom, a moguće je uraditi i forenzičku analizu mrežnog saobraćaja (koji su isto po prirodi volatile podaci) iz RAM memorije. Dumpit mora biti digitalno potpisan. Ukoliko je verified publisher označen kao „unknown" treba biti oprezan, jer možda je izvršen nad njim reverzan inženjering i ubačen zlonamerni program. Nakon dumpita dobija se sadržaj u .raw formatu. Njegovo pokretanje je jednostavno:

C:>dumpit.exe

Nakon kreiranja imidža radne memorije kreira se heš vrednost za obezbeđivanje integriteta digitalnog dokaza radne memorije na primer sa programom quickhash. [343] Učitati raw fajl u tabu FILE i odabrati Hash algoritam SHA-256.



Slika 22. Upotreba Dumpit alata

343 Https://sourceforge.net/projects/quickhash/, 20.07.2016.

Analiza fajla crash dump predstavlja takođe jedan od načina dobijanja informacija o sadržaju memorije. Za razliku od prikupljanja podataka iz memorije pomenutim specijalnim alatkama slika memorije dobijena u formi crash dump fajla predstavlja neizmenjenu kopiju sistemske memorije u momentu kada se desio krah sistema.[344] Nedostatak ovog načina jeste taj što se za dobijanje crash dump fajla mora desiti krah sistema, jer nisu svi sistemi podešeni da generišu ovaj fajl. Druga mana je ta što upisivanje ovog fajla može prepisati druge dokaze (obrisani, ali ne i nestali podaci). Postoji način na koji crash dump fajl može da se dobije, ali on zahteva izmenu odnosno kreiranje registarskog ključa i restartovanje računara opisanog na Microsoft sajtu.[345] [346]

Postoje *3 tipa crash dump fajla*: kompletan, kernel, mali. Kod Windows XP i Windows Viste po difoltu se kreira "mali" crash dump fajl, dok se kod Windows 2003 servera kreira kompletan crash dump. Treba spomenuti da sistemi sa preko 2 GB RAM memorije ne podržavaju kompletan crash dump fajl.[347] Iako je crash dump fajl forenzički ispravan fajl, pomenute mane prilikom njegovog "izazvanog" dobijanja (što nije u forenzičkom maniru) čine ga beskorisnim u istragama pravosudnih oragana. Kada su u pitanju istrage *u korporacijama (ne zvanične istrage)*, uz adekvatno konfigurisanje računarskih sistema pomenuto "izazvano" dobijanje crash dump fajla može biti od velike koristi da se pronađu informacije o kompromitovanju sistema.

Analiza hibernacijskog fajla predstavlja takođe jedan od načina dobijanja informacija o sadržaju memorije. Kada sistem odlazi u hibernacijski režim on sadržaj RAM memorije smešta u kompresovan fajl na hard disku pod nazivom hiberfil.sys pod root direktorijumom. Kada se sistem podiže on proverava da li postoji hibernacijski fajl i ukoliko postoji njegov sadržaj učitava u memoriju. S obzirom da su takvi fajlovi uglavnom starijeg datuma oni se mogu postaviti u kontekst aktivnosti koje su se dešavale u prošlosti. Matthieu Suiche je dekodirao hibernacijski fajl format i prezentovao javnosti (Windows hibernation file for fun "N" profit) svoje otkriće na konferenciji BlackHat USA 2008. godine.[348] Alati

---

344 Kaufman R. J., *Computer Incident Response*, Texas Security Symposium Agenda, San Antonio TX, 2003.

345 Http://support.microsoft.com/kb/927069, 14.04.2016.

346 Http://support.microsoft.com/kb/244139, 14.04.2015.

347 Harris R., *Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem*, Journal Digital Investigation: The International Journal of Digital Forensics & Incident Response, vol. 3, 2006, str. 44-49.

348 Http: //ebookbrowse.com/ bh-us- 08 -suiche-windows -hibernation- file- for- fun- n- profit- 0-3- pdf-d209085775, 22.06.2016.

kao što su *powercfg.exe*[349] i *psshutdown.exe*[350] mogu naterati sistem da ode u hibernaciju i time da se prikupi dump memorije. Isto pravilo važi kao i kod dobijanja crash dump fajla: kada su u pitanju istrage *u korporacijama (ne zvanične istrage)*, uz adekvatno konfigurisanje računarskih sistema pomenuto *"izazvano" dobijanje crash dump fajla* može biti od velike koristi da se pronađu informacije o kompromitovanju sistema, ali sticanje na takav način nije od koristi za istrage pravosudnih organa.

U zavisnosti od upotrebljenog alata nakon dobijene slike ili dumpa memorije sledi *memorijska analiza*. Postoje alati i kompleti alata sa kojima se radi memorijska analiza (npr. *find.exe strings.exe, grep, hex editori, paket alata Volatility*) koja pretražuje sadržaj slike ili dumpa memorije u kome se mogu naći dragoceni dokazi.

Paket alata Volatility koristi se za analizu prikupljenog dumpa fizičke memorije sa operativnog sistema. Uz pomoć određenih python skripti moguće je izvući procese i servise koji su bili pokrenuti, kernel moduli koji su bili učitani u memoriji, listu korisničkih SIDa iz dobijenog memorijskog dumpa.

Slede preporučene forenzičke aktivnosti prilikom analize dumpa radne memorije. Da bi se dobile informacije o operativnom sistemu pokreće se komanda:

#python vol.py –f /home/forenzika/mem_image/dump_mem.raw imageinfo

Da bi se dobila lista procesa koji su bili na OS identifikovani kao pokrenuti:

#python vol.py –f /home/forenzika/mem_image/dump_mem.raw --profile=Win10x64 pslist

Da bi se izvršio dump određenog procesa iz dumpa memorije:

#python vol.py –f /home/forenzika/mem_image/dump_mem.raw --profile=Win10x64 –D procdump/ -p 322(ID procesa)

Da bi se dobila lista kernel modula koji su bili učitani:

#python vol.py –f /home/forenzika/mem_image/dump_mem.raw --profile=Win10x64 modscan

Da bi se dobila lista korisničkih SID-ova iz dumpa memorije:

#python vol.py –f /home/forenzika/mem_image/dump_mem.raw --profile=Win10x64 getsids

---

349 Powercfg Command-Line Options, Microsoft, http://technet.microsoft.com/en-us/library/cc748940%28v=ws.10%29.aspx, 22.06.2016.

350 Mark Russinovich, PsShutdown v2.52, Windows Sysinternals, http://technet.microsoft.com/en-us/sysinternals/bb897541.aspx, 22.06.2016.

Na osnovu toga moguće je dobiti informacije koji je servis sa kojim korisničkim nalogom pokrenut. Na taj način vidi se koji su sistemski servisi, a koji su servisi pokrenuti sa korisničkim nalogom.

Za dobijanje liste svih komandi koje je korisnik unosio kroz komandno okruženje:

#python vol.py –f /home/forenzika/mem_image/dump_mem.raw --profile=Win10x64 cmdscan

Moguće je izvršiti oporavak history fragmenata index.data keš fajla i na taj način postoji mogućnost pronalaženja podataka o pristupljenim linkovima (URL), preusmerenim linkovima (REDR) i obrisanim unosima (LEAK) sa iehistory ili yarascan pluginom.

Dobijanje ID procesa IE kod Windows OS 7

#python vol.py –f /home/forenzika/mem_image/dump_mem.raw --profile=Win7SP0x64 pslist | grep iexplore

#python vol.py –f /home/forenzika/mem_image/dump_mem.raw --profile=Win7SP0x64 iehistory -p 555,1300(iexplorer procesi)

Ili,

#python vol.py –f /home/forenzika/mem_image/dump_mem.raw --profile=Win7SP0x64 yarascan -Y "/(URL |REDR|LEAK)/" -p 555,1300

Sa forenzičke tačke gledišta poznato je da IE history fajlovi generišu i tzv. slack prostor na osnovu toga što se stariji zapisi sa dugačkim URL adresama prepisuju sa novim zapisima ali sa kraćim URL adresama. To znači da delovi zapisa starijeg domena ostaju netaknuti. Primer jednog naprednijeg pretraživanje uz pomoć regularnih izraza moguće je ostvariti na sledeći način :

#python vol.py –f /home/forenzika/mem_image/dump_mem.raw --profile=Win7SP0x64 yarascan -p 555 -Y "/[a-zA-Z0-9\-\.]+\. (com| org| net| mil| edu| biz| name|info)/"

Jednu detaljnu analizu dump alata za prikupljanje podataka iz memorije prikazali su Takahiro Haruyama i Hiroshi Suzuki na BlackHat Europe konferenciji u radu „One-byte Modification for Breaking Memory Forensic Analysis".[351] Pronađene informacije putem pretraživanja samo na osnovu stringova ponekad je teško uklopiti u kontekst, jer ne postoji način da se pruži uvid u to koji je proces koristio određene informacije. Najnovije tehnike koje se primenjuju u analizi raščlanjuju sliku ili dump memorije i identifikuju

351 Kornblum J. D., The Linux Kernel and the Forensic Acquisition of Hard Disks with an Odd Number of Sectors, International Journal of Digital Evidence, Volume 3, Issue 2, 2004.

blokove procesnog okruženja (eng. Process Environment Block) ili PEB.[352] [353] Na osnovu onih informacija koje se nalaze u PEB-u moguće je saznati kome pripada određeni procesni deo memorije.[354] U praksi to znači da ukoliko se na ispitivanom računaru nalazi nezakonit materijal, forenzičar će biti u stanju da otkrije da li je taj materijal preuzet sa znanjem korisnika ili je automatski preuzet od strane malicioznog programa. Sa bezbednosne tačke gledišta prednost ovakvog pristupa, jer se povećava šansa za pronalaženje malicioznih programa, pošto PEB informacije istraživaču mogu pomoći pri diferencijaciji normalnog i malicioznog procesa.

Na primer, moguće je naći određene sekcije log fajlova web servera, koji su ukazivali da je upotrebljen bio exploit sa određene IP-adrese. S obzirom da je log fajl obrisan ovo je dragocen dokaz u istrazi. Ova informacija bi ukazivala i na ranjivost pomenutog web servera što bi podrazumevalo primenu bezbednosnih zakrpa na pomenutom sistemu. Treba napomenuti da se koriste uvek ažurirani alati zbog činjenice da se sa novim verzijama Windowsa ili novim servis pakovima može promeniti struktura procesa u memoriji.

Za forenzičku analizu radne memorije na Windows OS koristi se i alat Caploader koja služi za carving podataka iz radne memorije. [355] Ova alatka je specifična jer je sa njom moguće izvlačenje mrežnih paketa iz radne memorije da bi se dobila informacija o generisanom saobraćaju određenog zlonamernog programa koji je bio aktivan. Prilikom učitavanja dump-a radne memorije program kao što je Caploader identifikuje svaki deo radne memorije koji predstavlja mrežni paket. Kao rezultat ova alatka proizvodi informacije o IP adresama i korišćenim protokolima. Moguće je raspakivanje TCP sesija određenih mrežnih paketa i izvlačenje fajlova, na primer, email poruka koja su prosleđene kroz mrežu biće identifikovane na ispitivananoj sesiji uz pomoć Caploader alata. Ovaj alat nije ograničen samo na radnu memoriju već može da analizira i povrati podatke koji su snimljeni i obrisani na hard disku (npr. zlonamerni napadač je sa alatom Whireshark prikupljao sadržaj na ispitivanoj mreži, a podaci su se snimali u određeni fajl na hard disku).

---

352 Harris R., *Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem*, Journal Digital Investigation: The International Journal of Digital Forensics & Incident Response, vol. 3, 2006, str. 44-49.

353 Harrison W., Heuston G., Morrissey M., Aucsmith D. Mocas S., Russelle S., *A Lessons Learned Repository for Computer Forensics*, International Journal of Digital Evidence, Vol. 1 No. 3, 2002, http://www.ijde.org /docs/ 02_fall_art2.html, 22.06.2016.

354 PEB nam takođe pokazuje gde se nalazi slika izvršnog fajla, DLL putanje i komanda koje je startovala proces.

355 Http://www.netresec.com/, 25.07.2016.

Tabela 5. Alati za analizu memorijske slike ili dumpa

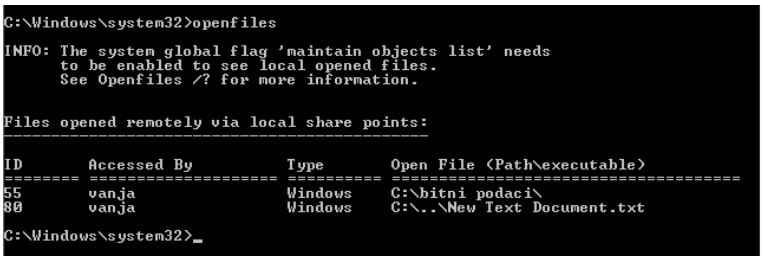
Alat	Operativni sistem	Namena	Zahtev	Dostupnost
Memoryze	Svi x32 i x64	Omogućava raščlanjivanje i analizu memorijskog dump fajla. Podržava Raw image format.	Python	https://www.mandiant.com/resources/download/memoryze
HBGary responder	Svi x32 i x64	Omogućava sveobuhvatnu analizu memorije. U stanju je da obnovi sve osnovne strukture podataka iz prikupljene memorije. Podržava Raw image format. Može se naći u 3 verzije: Pro, Field i Community.		http://www.hbgary.com/hbgary-releases-responder-ce
Lsproc.pl	Windows 2000	Izlistava procese.	Perl	http://sourceforge.net/projects/windowsir/files/Windows2000%20Memory/lsproc/
Lspd.pl	Windows 2000	Izslistava detalje o procesima.	Perl	http://sourceforge.net/projects/windowsir/files/Windows2000%20Memory/lspd%200.8/
Osid.pl	Bilo koji	Identifikuje verziju operativnog sistema iz dumpa ili slike memorije.	Perl	Dolazi uz knjigu Harlana Carvey-a[1]
PoolFinder	Windows 2000, Windows XP	Pronalazi dodeljen prostor kernelu OS u dump-u memorije i pagefile-u.	Perl	Sastavni je deo paketa Pool Tools: http://computer.forensikblog.de/files/poolfinder/poolfinder-current.zip
PoolGrep	Windows 2000, Windows XP	Pronalazi stringove u dodeljenom pool-u.	Perl	Sastavni je deo paketa Pool Tools: http://computer.forensikblog.de/files/poolfinder/poolfinder-current.zip
PoolDump	Windows 2000, Windows XP	Kreira hex dump od svog alociranog prostora za određenu klasu.	Perl	Sastavni je deo paketa Pool Tools: http://computer.forensikblog.de/files/poolfinder/poolfinder-current.zip

PoolView	Windows 2000, Windows XP	Prevodi određene alocirane poolove u razumljiv format.	Perl	Dostupan je za pravosudne organe i sve zainteresovane na zahtev http://computer.forensikblog.de/en/2007/11/pooltools-version-130.html
PTFinder	Windows 2000, Windows XP	Uključuje sve skripte iz paketa PoolTools kao i osid.pl skriptu i ima grafički interfejs.	Perl, Graphviz i ZGRViewer koji služi za pregled grafičkog fajla	http://computer.forensikblog.de/files/ptfinder/ptfinder-current.zip
Volatility Framework	Windows XP, 2003, Vista, 7, 2008 samo u x32	Predstavalja sveobuhvatan komplet alata sa različim funkcijama analize memorije. Može rasčlanjivati crash dump fajlove. Od formata podržava raw, crash dump i hibernacijski. Takođe može vršiti konverziju raw formata (dd tip) u crash memory dump format tako da se za analizu mogu–koristiti i Microsoft debugger alati. Može vršiti izvlačenje informacija o ugašenim procesima i prekinutim konekcijama.	Python	https://www.volatilesystems.com/default/volatility
Caploader	Windows sve verzije	Izvlačenje mrežnih paketa iz radne memorije da bi se dobila informacija o generisanom saobraćaju određenog zlonamernog programa koji je bio aktivan.	Microsoft .NET Framework 4.0	http://www.netresec.com/

3.1.4. Podaci od značaja privremenog karaktera na Windows-u - otvoreni fajlovi na sistemu

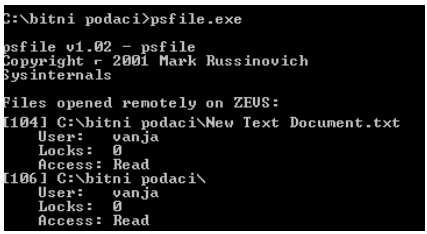
Neke od prethodnih alatki kao na primer psloggedon.exe mogu ukazati digitalnom forenzičaru ko je ulogovan kao udaljeni korisnik i koristi deljene resurse na mreži. Značajna informacija koju je potrebno dobiti je koji su to fajlovi koje koristi udaljeni korisnik. Alati koji mogu pružiti ove detalje su: komanda net file, alatka openfiles.exe i psfile.exe.

Alatka *openfiles* (sastavni deo windows os od verzije XP pro) prikazuje otvorene fajlove na sistemu i korisnika koji im je pristupio.



Slika 23. Prikaz otvorenih fajlova na sistemu od strane korisnika komandom openfiles

Alatka *psfile* prikazuje otvorene fajlove na sistemu i ime udaljenog korisnika koji im je pristupio.

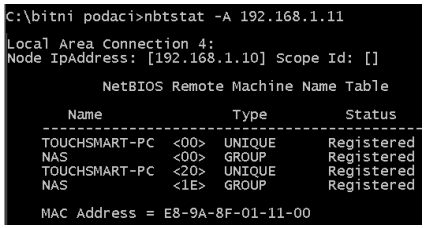


Slika 24. Prikaz otvorenih fajlova od strane korisnika alatkom psfile.exe

3.1.5. Podaci od značaja privremenog karaktera na Windows-u - informacije o mreži

Ukoliko je reč o kompromitovanju računarskog sistema (npr. upad u sistem), treba ispitati je da li je sa tog sistema pokušano ili je uspeo upad na neki drugi računarski sistem. Kod Windows OS, pri pravljenju konekcije prema drugom Windows OS ostaje *zapis u kešu Netbios tabeli imena* (eng. cached NetBIOS Name Table).[356] Digitalnom forenzičaru ovo može biti od velike koristi pri lociranju kompromitovanih računarskih sistema. Alatka je implementirana u Windows os i zove se *nbtstat.exe*. Ukoliko se želi videti keš Netbios tabele na računarskom sistemu upotrebljava se komanda "c:\nbtstat. exe -c", odnosno ukoliko se želi videti Netbios tabela udaljenog računara sa korisnim informacijama o servisima na ispitivanom računaru, koristi se komanda "c:\nbtstat -A ipadresa_udaljenog_racunara".

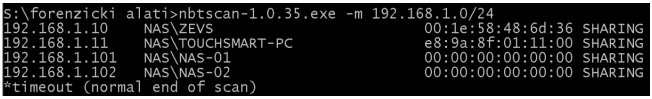
356 Netbios servis je prisutan gotovo kod svih Windows OS čak je u Windows serveru 2008 u defaultnim postavkama omogućen kao servis.



Slika 25. Prikaz NetBios tabela udaljenog računara

Nedostaci prethodnog alata su rad sa jednom IP-adresom, funkcionisanje samo na Windows platformi kao i nečitak format izlaza komande. Ove nedostatke prevazilazi sjajna besplatna alatka *nbtscan.exe*. Ona digitalnom forenzičaru omogućuje skeniranje IP-adresa iz zadatog mrežnog opsega šaljući NetBios upite, a kao izlaz komande dobija se lista sa IP-adresama, Netbios imenima računara, imenima ulogovanih korisnika kao i MAC adresa. Osim Windows platforme može da se koristi i na Linux platformi. Kao benefit digitalni istražitelj brzo i lako može da uoči sumnjiva NetBios imena na mreži što može da olakša i ubrza forenzičko ispitivanje. Ukoliko se blagovremeno uoči takva mašina može se sprečiti i potencijalna šteta koja može nastati, pa se na taj način i povećava zaštita računara na mreži pa i samog informacionog sistema.

Prikaz izlaza nbtscan.exe dat je na sledećoj slici:



Slika 26. Izlaz alatke nbtscan u razumljivom formatu sa IP-adresama i Netbios imenima

U slučaju da je potrebno uraditi forenzičku analizu mrežnog saobraćaja primarni cilj jeste izvršiti kategorizaciju mrežnih paketa odnosno identifikovati pakete prema tipu (TCP, UDP), njihov broj, identifikovati sve IP adrese koje su se pojavile u saobraćaju, rekonstrucija TCP sesija (podrazumeva se tekuća sesijska komunikacija između ispitivanog klijenta i servera) i ekstrakcija fajlova iz mrežnog saobraćaja.[357]

357 Prilikom otvaranja nekog sajta na primer yahoo.com, ostvaruje se tzv. tcp 3 way handshake koji služi za uspostavljanje tcp sesije. Nakon toga informacije mogu da se razmenjuju kroz primanje i slanje podataka ka yahoo serveru. Upravo te informacije u forenzičkoj analizi mogu biti prikupljenje iz mrežnog saobraćaja i rekonstruisane kako bi se ustanovilo da je je određena slika ili fajl poslat ili primljen od strane servera.

3.1.6. Podaci od značaja privremenog karaktera na Windows-u - status mreže i konekcije

Izuzetno je značajno da digitalni forenzičar po prijavi incidentne/ nedozvoljene aktivnosti, pravovremeno reaguje da bi sakupio što više informacija o lako izmenjivim (eng. volatile data) podacima. Neki od njih se upravo odnose na informacije koje računar sadrži o dolaznom i odlaznom mrežnom saobraćaju. To može pomoći forenzičaru da utvrdi da li je malicionzni korisnik (napadač) još uvek prijavljen na sistem. Osim toga moguće je utvrditi i postojanje malicioznog programa (npr. crva ili Bot-a), koji pokušava da zarazi druge računarske sisteme na mreži. U praksi detektovanje konekcije koju pravi zlonamerni korisnik odnosno malicioni program nije jednostavan postupak, ukoliko na samom sistemu ne postoji neki *zaštitni zid* (eng. firewall), koji prati odlazni i dolazni saobraćaj i snima log fajlove mrežnog saobraćaja. Jedan takav besplatan program koji se na sistemu startuje kao servis koji prati TCP i UDP pakete zove se *Port Reporter*.[358] Za jednostavniji preled log fajlova koji je Port reporter generisao postoji besplatan program Port Reporter parsing tool.[359] U nastavku će biti prikazani neki od alata, koji digitalnom forenzičaru mogu biti od velike pomoći u prikupljanju informacija o mrežnim konekcijama.

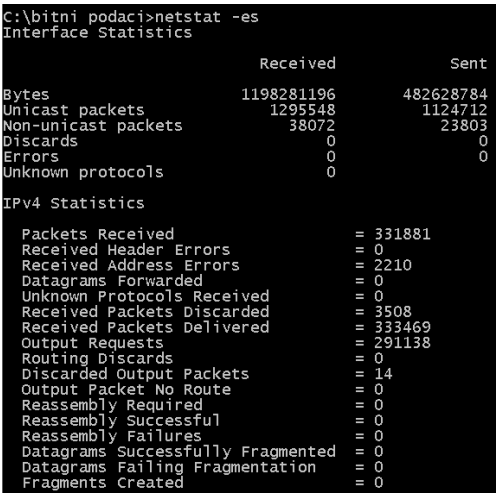
Alatka *Netstat*, koja je deo Windows OS jedna je od najpoznatijih alatki, koja služi za brzo i jednostavno prikupljanje informacija o TCP i UDP konekcijama, njihovim stanjima i statitici mrežnog protoku paketa (IPv4, IPv6, TCP, UDP, ICMPv4, ICMPv6). Najčešće se upotrebljava da se izlistaju sve aktivne konekcije i otvoreni portovi na računaru. S obzirom da se uobičajeno portovi koriste za kreiranje zadnjih vrata na sistemima, forenzičar prepoznajući otvorene portove može otkriti zlonamerne konekcije i blagovremeno zatvoriti te portove. Ova komanda istu namenu ima i na Linux računarskim sistemima.

```
C:\bitni podaci>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       828
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING       2172
  TCP    0.0.0.0:2160           0.0.0.0:0              LISTENING       1992
  TCP    0.0.0.0:2161           0.0.0.0:0              LISTENING       1964
  UDP    127.0.0.1:1900         *:*                                    1724
  UDP    127.0.0.1:48000        *:*                                    2244
  UDP    127.0.0.1:48001        *:*                                    3636
  UDP    127.0.0.1:48002        *:*                                    5700
  UDP    127.0.0.1:53177        *:*                                    2024
  UDP    127.0.0.1:53178        *:*                                    2024
  UDP    127.0.0.1:56254        *:*                                    3824
```

Slika 27. Prikaz aktivnih konekcija alatkom netstat

358 Http://www.microsoft.com/ downloads/ details. aspx? familyid= 69ba779b- bae9- 4243- b9d6-63e62b4bcd2e&displaylang=en, 22.05.2016.

359 Http://www.microsoft.com/kb/884289, 23.05.2016.



Slika 28. Prikaz statistike mrežnih paketa

Prilikom forenzičkog istraživanja takođe treba obratiti pažnju na neuobičajeno otvorene portove. Praksa je pokazala da treba detaljno razmotriti i saobraćaj koji ide preko standardnih portova, koji mogu forenzičara da dovedu u zabludu. Jedan od primera bi bio da zlonamerni korisnik preko porta 80 wget.exe aplikacijom download-je zlonamerne programe i alate za kompromitovanje sistema, što će forenzičaru ili sistemu za prepoznavanje upada (eng. IDS) izgledati kao legitiman saobraćaj u mreži.[360]

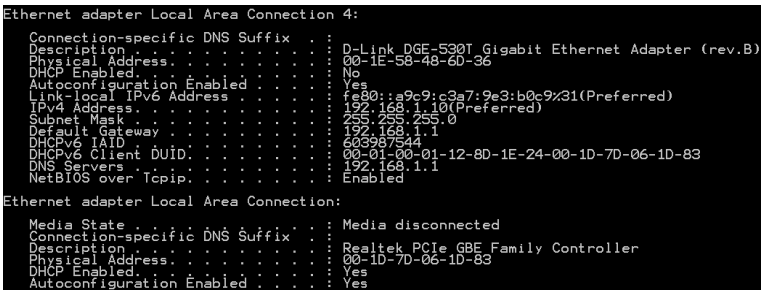
Od izuzetne važnosti za istragu može biti dobijanje *informacija o statusu mrežnog adaptera* (eng. network interface card - NIC, LAN ili WLAN) ispitivanog računarskog sistema.[361] Na primer, danas se većina prenosnih računarskih sistema (eng. lap top) isporučuje sa već ugrađenim bežičnim mrežnim adapterom. To znači da forenzičar na prvi pogled (uvidom u Desktop sistema) ne može da utvrdi da li je ispitivani sistem uspostavio konekciju sa nekom pristupnom tačkom (eng. Access Point - AP) i koju je adresu dobio. Nekada je ta informacija o statusu mrežnog adaptera od velikog značaja za dalji tok istrage. U nastavku će biti izloženi određeni *alati sa kojima će biti moguće utvrditi status mrežnog adaptera.*

Alatka *ipconfig* je sastavni deo Windows OS. Pomoću nje se dobijaju konfiguracione informacije postojećih mrežnih adaptera na sistemu i njihov

360 Harrison W., Heuston G., Morrissey M., Aucsmith D. Mocas S., Russelle S., *A Lessons Learned Repository for Computer Forensics*, International Journal of Digital Evidence, Vol. 1 No. 3, 2002, http://www.ijde.org /docs/ 02_fall_art2.html, 22.06.2016.

361 Bežični lan adapter.

status. Alatka ima veliki broj korisnih svičeva ali najsveobuhvatniji upravo "/all" svič (c:\ipconfig /all).



Slika 29. Prikaz izlaza komande c:\ipconfig /all iz Windows 7 OS

Kao što se može primetiti informacije koje možemo dobiti ovom alatkom su status mrežnog adaptera, njegovo ime, status DHCP-a, IP-adresa, fizička adresa, NetBIOS status i drugi paratmetri. Ovi parametri su izuzetno važni u toku istrage naročito kada se vrše ispitivanja logova mrežnog saobraćaja.

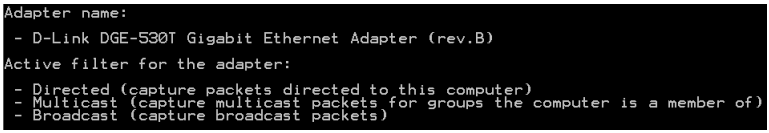
Kada je reč o *statusu mrežnog adaptera* važno je utvrditi u kom modu je postavljen mrežni adapter. Na kompromitovan računaru postoji mogućnost da je mrežni adapter postavljen u tzv. promiscuous modu tj. režim kartice sa kojim je moguće "osluškivati" mrežni saobraćaj nasuprot normalnom režimu rada.[362]

S obzirom da administrator sistema i mreže ili digitalni forenzičar ne mogu na jednostavan način utvrditi u kom režimu je podešena da radi kartica, ukoliko ne postoje neki od očiglednih pokazatelja kao npr. postojanje određenih programa koji mogu raditi u režimu prisluškivanja. Jedini način da se ovo otkrije na živom sistemu je korišćenjem određenih alata ili skripti. Sniffing sa injectiranjem paketa je krivično delo neovlašćenog pristupa zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka i

362 Mrežne kartice mogu da rade u različitim modovima. Za analizu saobraćaja upotrebljava se promiscuous mode ili monitor mode. Promiscuous mode se koristi za „hvatanje" paketa u mreži na koju je kartica povezana, a alati sa kojima se može vršiti analiza su Whireshark, Tcpdump, Kismet, Ettercap, NetworkMiner, Dsniff i dr. Monitor mod se odnosi na WiFi mrežne adaptere i koristi se za hvatanje mrežnih paketa iako mrežni adapter nije povezan na mrežu odnosno na access point (AP). S obzirom na to da nije povezan na mrežu paketi se sniffuju u raw formi a nema mogućnosti da se obrađuje ethernet informacije ali se mogu obrađivati neke druge informacije kao na primer mac adrese, SSID, korišćena mrežna konekcija, primenjena zaštita i drugi parametri. Za tu svrhu koriste se drugi alati kao što su aircrack-ng, ELK stack (Kibana). Problem se javlja kada neko ne koristi ove alate za dobrobit analize mrežnog saobraćaja već u zlonamerne svrhe.

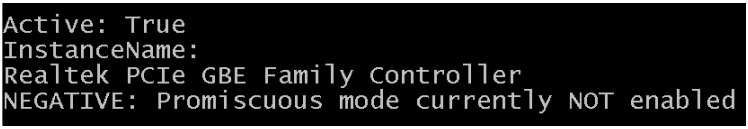
takva aktivnost se detektuje u mrežnim paketima.[363]

Neki od tih alata su *promiscdetect.exe*,[364] *ndis.exe*[365] i *promqry.exe*[366] čiji su izlazi prikazani na sledećim slikama.



Slika 30. Prikaz izlaza alatke promiscdetect.exe na Windows 7 Os

Slika 31. Prikaz izlaza alatke ndis.exe na Windows 7 Os



Slika 32. Prikaz izlaza alatke promqry.exe na Windows 7 Os

Takođe, detektovanje može da se izvši uz pomoć alatke *nmap* (pokrenute sa spoljne Linux mašine) uz pomoć predefinisane skripte koja se zove sniffer-detect.nse odnosno promiscuous.nse u zavisnosti od verzije Nmap-a.[367] Pokreće se sa komandom za zadatu mrežu na primer # nmap --script=promiscuous 192.168.1.0/24.

Ukoliko sistem detektuje neku karticu na mreži koja je u režimu "osluškivanja" izlaz komade će biti prikazan na sledeći način:

---

363 U Srbiji je za ovo krivično delo po čl. 302. Krivičnog zakonika zaprećena novčana kazna ili kazna zatvora do 3 godine.

364 Http://ntsecurity.nu/downloads/promiscdetect.exe, 28.05.2016.

365 Dostupno na disku koji se dobija uz knjigu Windows Forensic Analisys od Harlana Carvey-a. Ovoj alatki je potrebna biblioteka p2x588.dll.

366 Alatka, koju je napisao Tim Rains ima mogućnost testiranja nad udaljenim računarskim sistemom. Dostupna je na Microsoft sajtu: http://www.microsoft.com/en-us/download/details.aspx?id=185, 28.05.2016.

367 Marek Majkowski, File sniffer-detect, Fyodor, http://nmap.org/nsedoc/scripts/sniffer-detect.html, 28.05.2016.

```
Interesting ports on Sumnjiv_racunar (192.168.1.123):
Not shown: 996 closed ports
PORT            STATE         SERVICE
22/tcp          open          ssh
23/tcp          open          telnet
53/tcp          open          dns
80/tcp          open          IIS/http
MAC Address: 00:26:39:41:15:82 (Linksys)
Host script results:
Promiscuous detection: PROMISCUOUS (tests: "111___1_")
```

Ovo je signal digitalnom forenzičaru da računar ima mrežni adapter, koji je u režimu "osluškivanja" i da je u pitanju jedan od Windows OS (počev od Windows 2000). Windows 98 se manifestuje sa oznakom "1111__1_" dok se Linux OS manifestuje sa oznakom "11111111". Važno je napomenuti da skripta daje prikaz samo ukoliko pronađe jedan od mrežnih adaptera u modu za "osluškivanje". Ukoliko se ne pronađe ne prikazuje se izveštaj. Treba reći da je blagovremenom detekcijom takvih računara na mreži moguće sprečiti nanošenje dalje štete (ukoliko je ona već nastala), čime se povećava sigurnost ukoliko se način detektovanja automatizuje. Oslanjanje samo na detektovanje nije pouzdana mera bezbednosti i ne treba biti jedina, jer u određenim slučajevima samo detektovanje može doći prekasno da bi se sprečilo kompromitovanje određenih podataka.

Da bi forenzičari mogli da pokrenu sniffing aktivnost mrežni adapter mora da se postavi u *promiscuous* mod (sluša sve mrežne pakete koji dolaze na lokalni mrežni adapter a nisu njemu namenjeni). Po defaultu mrežni adapter nisu u primiscous modu već oni rade u *non-promiscuous* modu. Ukoliko je neko na mreži konfigurisao karticu da radi u *promiscuous* modu on verovatno ima zlonamerni cilj. Pred forenzičarem je zadatak da pronađe uređaj koji ima karticu konfigurisanu u *promiscuous* modu. Da bi se to otkrilo može se koristiti pored pomenutih i alata PromqryUI 1.0. Svi paketi koji dođu do mrežnog adaptera a nisu namenjeni za destinaciju određenog mrežnog adaptera u non-*promiscuous* modu biće dropovani sa mrežnog interfejsa. U *promiscuous* modu svi paketi koji dođu do mrežnog adaptera mrežni interfejs ih procesira odnosno prikuplja za sniffing aktivnosti. Pronalaženje mrežnog adaptera koji je u *promiscuous modu* u Windows okruženju se detektuje na osnovu praćenja paketa koji se procesiraju na određeni način. U *non-promiscuous modu* se paketi procesiraju na jedan način dropujući ih, a u *promiscuous* modu se procesiraju

na drugačiji način.

Korisničke aktivnosti na internetu evidentiraju se na operativnom sistemu i čuvaju se kao keš u DNS formatu. Informacije koje se čuvaju obuhvataju kako one iz hosts fajla tako i URL-ove koji su razrešeni od strane DNS servera. Keširanje DNS-a omogućava ubrzanje isčitavanja sadržaja internet lokacija koje se posećuju često. Sa aspekta bezbednosti i privatnosti ovaj keš može predstavljati potencijalnu ranjivost ukoliko zlonamerni napadač dobije pristup korisničkom operativnom sistemu jer može preuzeti ove informacije i zloupotrebiti ih. Sa stanovišta forenzičke istrage ovo mesto je značajno, jer se u njemu mogu pronaći dragocene informacije koje se tiču uspostavljanih konekcija na internetu. Takođe ove informacije mogu biti od velike koristi prilikom uspostavljanja određenih korelacija u ispitivanom slučaju.

U Windows 10 (Windows 7, Windows 8) operativnom sistemu za pregledanje keša DNS-a koristi se alatka ipconfig komandnog okruženja sa određenim svičem:

C:\>ipconfig /displaydns

Za brisanje keša DNS-a koristi se ipconfig alatka komandnog okruženja sa određenim svičem, nakon zatvaranja svih internet pretraživača :

C:\>ipconfig /flushdns

Ukoliko je privatnost imperativ moguće je izvršiti trajno ukidanje keširanja DNS-a iz Control panel-a:

-Administrative tools – Services – DNS client – Desnim klikom odabrati *Properties* i izvršiti stopiranje servisa nakon odabiranjaopcije *Stop*, a pod opcijom Startup type odabrati *Disabled*

Nakon trajnog ukidanja DNS keša upotreba interneta će biti nešto sporija.

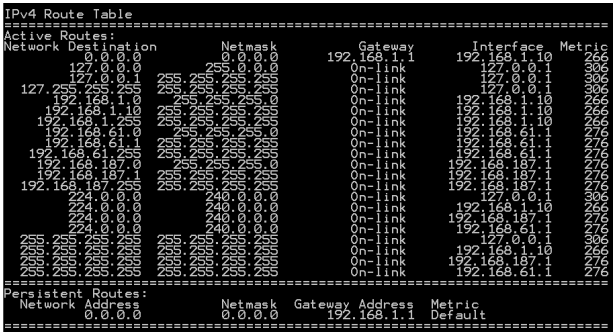
Tokom forenzičke istrage potrebno je da se posebna pažnja obrati na *aktivne mrežne adaptere* ispitivanog računara. To može dati dodatan kontekst u daljem toku istrage i značajan podatak za post-mortem forenzičku analizu.

3.1.7. Podaci od značaja privremenog karaktera na Windows-u - interna tabela rutiranja

U praksi jedna od malicioznih upotreba kompromitovanog servera podrazumeva nameru napadača da izmenom interne tabele rutiranja preusmeri saobraćaj određeni način. Očekivana korist od preusmeravanja saobraćaja je zaobilaženje zaštitinih barijera (eng. firewall). Na primer, ukoliko postoji zaštita prema računaru koji je sledeća meta napada, napadač može uz pomoć kompromitovanog računara (koji ima direktan pristup meti) zaobići

zaštitne barijere. Druga korist koju napadač može da ima od izmena ruting tablela je prisluškivanje paketa na mreži. Da bi administrator ili forenzičar ustanovili da li je ruting tabela menjana tj. da li ima tragova pokušaja napada, treba pokrenuti *netstat komandu* kao na sledećoj slici:

#netstat -nr



Slika 33. Prikaz interne tabele rutiranja komandom netstat -nr

3.1.8. Podaci od značaja privremenog karaktera na Windows-u – startovani procesi i servisi

Za forenzičko istraživanje ispitivanog sistema važno je znati koji su procesi startovani na tom sistemu. Treba istaći da *Task menadžer* (eng. Task Manager) ne pokazuje sve procese kao i procesne detalje koji su od značaja za ispitivanje. Digitalni forenzičar će želeti da zna npr.: apsolutnu putanju izvršnog fajla, iz kog komandnog okruženja je pokrenut proces koji je potrebno ispitati, vreme trajanje procesa, vlasništvo pokrenutog procesa, koji su moduli učitani od strane procesa, sadržaj koji je proces učitao u memoriju. Neke od navedenih podataka Task menadžer može omogućiti, a neke ne. U praksi se dešava sledeći scenario: maliciozni program se instalira pod imenom svchost.exe, a to ime je ime regularnog programa na Windows OS, koji se nalazi u *„c:\windows\system32\"* direktorijumu, koji je zaštićen sa WFP (eng. Windows File Protection).[368] Pregledom u Task menadžeru forenzičaru neće biti jednostavno utvrditi koji je od procesa sumnjiv ukoliko nema putanju

368 WFP je prisutan od Windows 2000 i štiti sistemske fajlove od izmena i slučajnih brisanja čuvajući svoju "dobru" kopiju u kešu, za slučaj da je došlo do namerne ili slučane izmene ili brisanja. Ukoliko se desi da se generiše ID 64001 ostavljajući trag na sistemu. Vidi: http://support.microsoft.com/kb/222193, 27.05.2016.

do izvršnog fajla. Ukoliko forenzičar otkrije putanju i vidi da se svchost.exe pokreće iz nekog drugog foldera umesto iz c:\windows\system32\, to je signal da taj proces treba biti predmet ispitivanja. U praksi se dešavalo da se ime procesa zamaskira imenom da izgleda kao da se radi o sistemskom procesu. Iskusnom forenzičaru ili administratoru će biti sumnjiv proces netsysw. exe s pokrenutim svičevima -L -d -p 80 -e cmd.exe, jer ukazuje da se radi o startovanom netcat programu ili nekom malicioznom programu tipa zadnja vrata (eng. backdoor). Može se reći da od iskustva i veština samih forenzičara i administratora i dobrih alata u pronalaženju malicioznih procesa može zavisiti kako sama bezbednost sistema tako i uspešnost u digitalnoj forenzičkoj istrazi ispitivanog računara.

U daljem tekstu biće opisani *alati* koji će forenzičaru pomoći u dobijanju više detalja *o ispitivanim procesima i servisima*.

Alatka koja se sastavni deo Windows OS i daje prikaz postojećih servisa na sistemu sa njihovim stanjem, statusom, modom, oznakom procesa je prikazana na sledećoj slici:

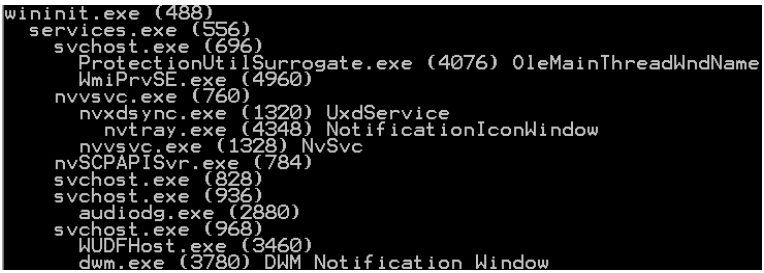
„c:\ >wmic service list brief"

```
S:\forenzicki alati>wmic service list brief
ExitCode  Name                          ProcessId  StartMode  State    Status
0         AdobeFlashPlayerUpdateSvc     0          Manual     Stopped  OK
0         AeLookupSvc                   0          Manual     Stopped  OK
0         AgereModemAudio               1920       Auto       Running  OK
1077      ALG                           0          Manual     Stopped  OK
0         APCPBEAgent                   1948       Auto       Running  OK
0         APCPBEServer                  2004       Auto       Running  OK
1077      AppIDSvc                      0          Manual     Stopped  OK
0         Appinfo                       120        Manual     Running  OK
0         Apple Mobile Device           2024       Auto       Running  OK
```

Slika 34. Prikaz alata wmi koji sa dodatnim argumentima daje detaljnu listu o procesima

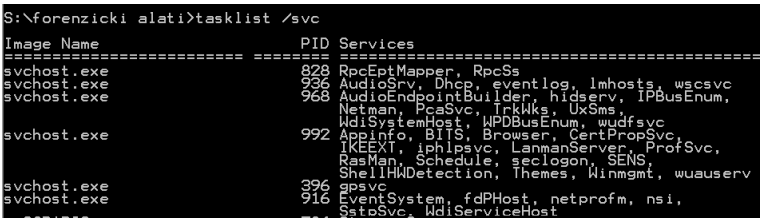
Jako dobra alatka za pregledanje procesa na sistemu jeste *Tlist*. Ona je sastavni deo microsoftovog alata za debagovanje.[369] Postoji u 32-bitnoj i 64-bitnoj verziji, ali se ne može naći u novijim verzijama Windowsa (nije sastavni deo od Windowsa XP, a njegov naslednik je *TASKLIST*). Daje jako dobre detalje kada su u pitanju ID procesi, ime procesa, identifikator sesije, korišćenje memorije i dll-ova za svaki pokrenut proces, može da da punu putanju procesa (slika) i hijerarhijski prikaza procesa tako da se može saznati koji su procesi kreirani od strane nekog drugog procesa, za razliku od TASKLISTA. Na sledećim slikama su prikazani neki izlazi tlist alata sa različitim svičevima:

369 Http:// download. microsoft. com/ download/ 4/A/2/4A25C7D5-EFBE-4182-B6A9-AE6850409A78/ GRMWDK_ EN_7600 _1.ISO, 27.05.2016.



Slika 35. Prikaz izlaza komande Tlist prema hijerhiji nastajućih procesa sa c:\tlist -t

Alatka Tasklist je naslednik komande Tlist i sastavni je deo Windows OS počev od Windows XP verzije. Ima detaljan pregled procesa i forenzičaru može pomoći dajući različite izlazne formate koju ova alatka može da obezbedi (tabelaran prikaz, prikaz sa ";" eng. csv ili kao listing). Izlistava većinu informacija o procesima uključujući imena programa baš kao i prethodno pomenut alat, ali bez cele putanje. Može da omogući pregledan prikaz procesa i servisa sa identifikatorom procesa ukoliko se uključi svič "c:\tasklist /svc" kao na sledećoj slici.



Slika 36. Prikaz izlaza alata tasklist sa uključenim svičom /svc

Alatka *Pslist*, takođe forenzičaru može da pomogne oko dobijanja informacija o procesima i kroz svoje svičeve može da omogući prikaz zauzeća memorije i procesorskog vremena, dužinu trajanja procesa kao i hijerarhijski prikaz procesa kao kod tlist alatke.[370] Nedostaci su mu ti što ne pruža putanju do izvršnog programa, komandno okruženje pod kojim je startovan proces ili koji je user izvršio određen proces.

370 Mark Russinovich, PsList v1.3, Windows Sysinternals, http://technet.microsoft.com/en-us/sysinternals/ bb896682.aspx, 05.06.2016.

```
Name                  Pid      VM      WS    Priv Priv Pk   Faults   NonP Page
TCMDX64              4500  113924   18792    9468   42720     6174     20  203
  Tid Pri     Cswtch          State      User Time   Kernel Time   Elapsed Time
 4284   8     158723   Wait:DelayExec  0:01:50.261   0:11:35.951   0:57:10.562
  820   8          5     Wait:UserReq  0:00:00.000   0:00:00.000   0:57:09.439
  900   8         61       Wait:Queue  0:00:00.000   0:00:00.000   0:57:09.361
 1036  10       3243     Wait:UserReq  0:00:00.000   0:00:00.000   0:57:09.283
```

Slika 37. Prikaz zauzeća memorije i procesorskog vremena komandom c:\pslist -x

Korisna alatka koja je implementirana u Windows OS može dati detaljan prikaz o procesima i celoj putanji I tako biti forenzičaru od koristi sa dodatnim argumentima koji mogu da izlistaju podatke i snime formate kao što su CSV ili html:

"*wmic /output:wmic.csv process get name,processid,priority,commandline /format:csv*" ili u html formatu što može biti mnogo preglednije:

"*wmic/output:wmic.htmlprocessgetname,processid,priority,commandline /format:hform* "

Ova komanda izlistava ime procesa, id procesa, priorite i putanju do izvršnog fajla što je i prikazano na sledećoj slici:

Node: ZEVS - 86 Instances of Win32_Process

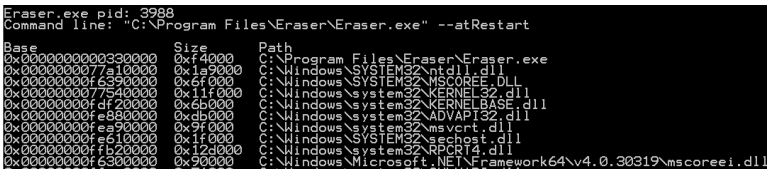
acrotray.exe.	
Property Name	Value
CommandLine	"C:\Program Files (x86)\Adobe\Acrobat 8.0\Acrobat\acrotray.exe" .
Name	acrotray.exe.
Priority	8
ProcessId	2076
.	
agr64svc.exe.	
Property Name	Value
CommandLine	"C:\Program Files\LSI SoftModem\agr64svc.exe".
Name	agr64svc.exe.
Priority	8
ProcessId	1920
.	
AppleMobileDeviceService.exe.	
Property Name	Value
CommandLine	"C:\Program Files (x86)\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe".
Name	AppleMobileDeviceService.exe.
Priority	8
ProcessId	2024

Slika 38. Prikaz procesa na ispitivanom sisemu dobijenog sa wmi komadnom u html formatu

Jako korisna alatka koja može forenzičaru takođe biti od pomoći jeste *ListDLL* , koja je u stanju da prikaže module i DLL-ove koje određeni proces koristi.[371] Osim toga može da da prikaz cele putanje do modula ili DLL-a čak i ako se učitana verzija DLL-a u memoriji razlikuje od DLL-a na disku. To je veoma važno, jer program prikazuje tačno onaj DLL odnosno modul koji se koristi od strane aplikacije. Sa ovim programom moguće je prepoznati neke rootkit-a, trojanaca i drugih malicioznih programa koji koriste tehniku DLL injection. Ti maliciozni programi pokušavaju da učitaju sebe u memorijski

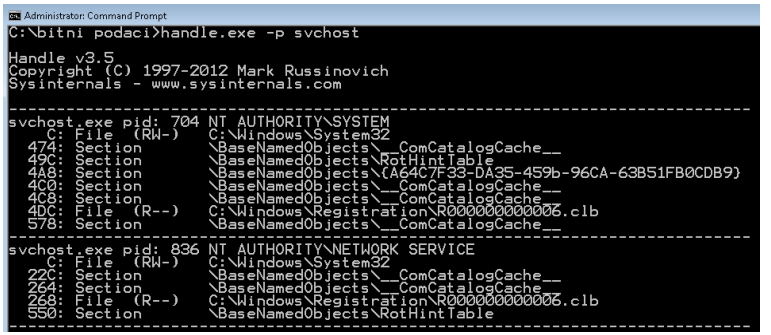
371 Mark Russinovich, ListDLLs v3.1, Windows Sysinternals, http://technet.microsoft.com/en-us/ sysinternals/ bb896656.aspx, 05.06.2016.

prostor startovanog procesa da bi mogli da se startuju i izvrše ali da se ne prikažu u listi procesa jer su zapravo deo nekog drugog procesa. Osim toga moguće je uočiti i programe koji imaju za cilj anti-forenzičke aktivnosti kao na primer "duboko" formatiranje hard diska ili brisanje podataka pri restartu sistema, gašenju itd. Blagovremenim uočavanjem zlonamernog programa moguće je povećati i bezbednost samog sistema i pronaći dokaz koji može biti važan deo konteksta istrage. Na slici je dat primer izlaza komande Listdll u kome se vide imena procesa, Id procesa, na koji način se izvršava iz komandne linije (sa parametrom izvšenja po restartu) i pripadajući DLL-ovi sa putanjama.



Slika 39. Prikaz izlaza komande listdll

Alatka *handle* spada u red jako korisnih forenzičkih alatki za pregledanje procesa.[372] Ova alatka se ne odnosi samo na prepoznavanje fajlova i foldera i njihovih putanja koji su u vezi sa procesima, već prepoznaje i otvorene portove, ključeve u registru bazi, kao i procesorsko vreme. Na taj način ona može da pruži informaciju o tome koje resurse koristi proces dok je aktivan. Na slici je prikazan primer izlaza ovog alata sa komandom koja se odnosi samo na proces svchost "c:\handle.exe -p svchost":



Slika 40. Prikaz Alatke handle

372 Http://technet.microsoft.com/en-us/sysinternals/bb896655.aspx, 05.06.2016.

Dodatno ukoliko je forenzička istraga zahtevala carving proces prvi korak u analizi biće analizirarnj fajl host.data. Treba obratiti pažnju na timestamp-ove koji mogu biti različiti i u tom slučaju se vrši kreiranje time frame tabele, da bi se ustanovilo tačno vreme kreiranja određenih fajlova. U hosts.data fajlu mogu se identifikovati svi startovani i aktivni procesi ispitivanog operativnog sistema. Dodatni korisni forenzički alati za ispitivanje procesa i mrežnih konekcija su Process explorer[373], Hyena[374] Process haker[375].

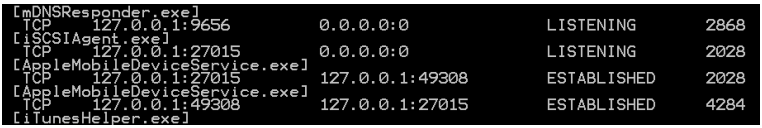
Ukoliko je neka od navedenih alatki pronašla sumnjiv proces forenzičar može doneti odluku o tome da sazna više informacija o tom procesu, a to može uraditi dumpovanjem onog dela memorije koje ispitivani proces koristi. U daljem tekstu biće izloženi neki alati koji mogu da izvuku sadržaj RAM memorije (kao i deo memorije nekog procesa). U forenzičkom ispitivanju taj postupak se zove *memorijska analiza*. Od značaja je da se nepotrebni servisi na računarskom sistemu prilikom njegovog konfigurisanja onemoguće. Tako se ostvaruje dvostruki benefit: dobijanje na performansama i dobijanje na većoj bezbednosti računarskog sistema.

3.1.9. Podaci od značaja privremenog karaktera na Windows-u - mapirani portovi od strane procesa

Značajno je istaći da ukoliko na računarskom sistemu postoji uspostavljena mrežna konekcija ili su otvoreni određeni portovi na sistemu, to znači da iza njih stoje i određeni procesi. Da bi digitalni forenzičar utvdio vezu između portova i procesa neophodni će mu biti određeni alati za tu namenu.

Već pomenuta alatka koja je sastavni deo Windows operativnog sistema (počev od Windows XP) je *netstat* i može pomoći forenzičaru pri uspostavljanju *korelacione veze između procesa i otvorenih portova*. Nakon izlaska dodatnog paketa SP2 (eng. service pack) za Windows XP i dodatnog paketa SP1 za Windows 2003 ova alatka je dobila mogućnost korišćenja novog switch-a "-b" koji su izvršni programi odgovorni za otvaranje porta (u nekim slučajevima mogu biti prikazani i DLL-ovi koji koristi određeni proces).

373 Https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx, 05.06.2016.
374 Http://www.systemtools.com/, 05.06.2016.
375 Http://processhacker.sourceforge.net/, 05.06.2016.

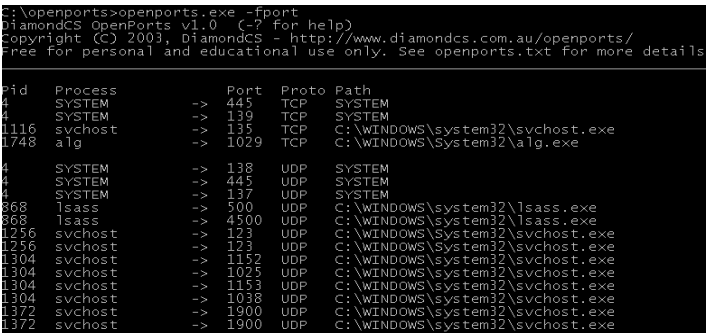


Slika 41. Prikaz komadne netstat sa dodatnim switchem -b (netstat -anob)

Fport je sjajna alatka koja ima jednostavanu upotrebu sa preglednim i razumljivim izlazom.[376] Nedostatak je što ima podršku samo za Windows, Windows NT4, Windows 2000 i Windows XP i što forenzičar mora imati pristup administratorskom nalogu za pokretanje ovog alata.

C:\>fport.exe
Pid Process Port Proto Path
92 svchost -> 135 TCP C:\WINNT\system32\svchost.exe
18 System -> 139 TCP
28 System -> 445 TCP
508 MSTask -> 1025 TCP C:\WINNT\system32\MSTask.exe
345 svchost -> 135 UDP C:\WINNT\system32\svchost.exe
86 System -> 137 UDP

Još jedna jako dobra alatka (sa podrškom za NT4, Windows 2000 i Windows XP) jeste *openports* kompanije DiomondCS koji ima podršku za više izlaznih formata (fport stil, csv stil ili netstat).[377] Prilikom pokretanja ne zahteva administratorske privilegije. Daje prikaz ID procesa, ime procesa, broj porta, tip protokola i putanju do izvršnog programa kao što je prikazano na sledećoj slici:



Slika 42. Prikaz Izlaza programa opentports u f-prot stilu

376 Http://www.mcafee.com/ apps/ free-tools/ termsofuse.aspx?url=/ uk/ downloads/ free-tools/ fport.aspx, 05.06.2016.

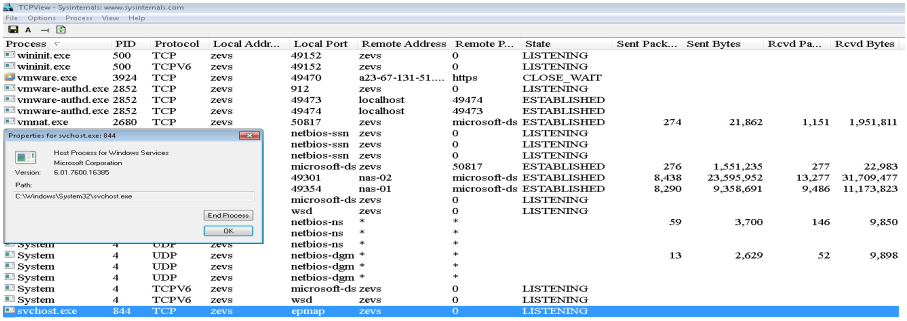
377 Http://www.diamondcs.com.au/openports/, 05.06.2016.

Alat *Tcpvcon* je jedan od najboljih alata kada je reč o istraživanju otvorenih portova i procesa koji iza njih stoje.[378] Ima mogućnost izlaza i u csv formatu. Podržava Windows OS od Windows XP i novije.

```
C:\>tcpvcon.exe -a

TCPView v2.34 - TCP/UDP endpoint lister
Copyright (C) 1998-2003 Mark Russinovich
Sysinternals - www.sysinternals.com

[TCP] C:\WINDOWS\system32\svchost.exe
      PID:      1116
      State:    LISTENING
      Local:    winXPsp2:epmap
      Remote:   winXPsp2:0
[TCP] System
      PID:      4
      State:    LISTENING
      Local:    winXPsp2:microsoft-ds
      Remote:   winXPsp2:0
[TCP] C:\WINDOWS\System32\alg.exe
      PID:      1748
      State:    LISTENING
      Local:    winXPsp2:1029
      Remote:   winXPsp2:0
```

Slika 43. Prikaz izlaza alata tcpvcon

Alat *TcpView* jedan je od najboljih alata ovog tipa i koristi grafički interfejs.[379] Prikazuje detaljne informacije o svim TCP i UDP otvorenim portovima na sistemu, udaljene adrese sa kojima je ta konekcija ostvarena kao i stanje TCP konekcije. Ima podršku za sve Windows OS počev od Windows XP. U paketu se isporučuje i prethodno opisana alatka tcpvcon koja je prilagođena za komandno okruženje.



Slika 44. Prikaz TCPview alata sa apsolutnom putanjom određenog procesa

Naravno forenzičar treba da zna da se ovi alati oslanjaju na API i DLL-ove iz sistema. To znači da ukoliko postoji dodatna sumnja (a ove alatke nisu našle sumnjive portove) treba uzeti u obzir i *dodatno skeniranje portova* od

378 Dostupno kao deo paketa TCPView. Vidi: http://technet.microsoft. com/ en-us/ sysinternals/ bb897437.aspx, 05.06.2016.

379 Mark Russinovich, TCPView v3.05, Windows Sysinternals, http://technet.microsoft.com/en-us/sysinternals/bb897437.aspx, 10.06.2016.

spolja alatima kao što je *NMAP*.[380] Takvim skeniranjem dodatno će se potvrditi da li je sistem bio kompromitovan (od strane nekog exploita ili rootkita) ili nije, odnosno da li mu je bezbednost ugrožena ili ne.

Rootkit kolekcija odnosno komplet (eng. kit) alata, koju koristi zlonamerni napadač, obično se sastoji od trojanskih alata, mrežnih snifera (prisluškivači mreže), skripti za čišćenje logova (eng. log cleaning scripts) kao i programa koji omogućavaju napadaču da ima root (najveće) privilegije na sistemu. U literaturi se mogu naći opisane sledeće mogućnosti ovih rootkit alata:

-skrivanje fajlova i direktorijuma;

-skrivanje procesa;

-skrivanje stavki iz Windows registra (eng. registry) kada je Windows OS u pitanju;

-sprečavanje brisanje fajlova;

-sprečavanje pokretanja antivirusnog sistema.

Rootkitovi se najčešće mogu podeliti na *tri tipa*:

- *tradicionalni* - u ovu grupu rootkitova spadaju programi koji slušaju na nekom TCP/UDP portu čime omogućavaju zlonamernom napadaču skriveni pristup računarskom sistemu tzv. backdoor. Zatim postoje *čistači logova* (eng. log wipers), koji brišu log fajlove da bi se sakrilo prisustvo i aktivnosti zlonamernog napadača. U ovu grupu spadaju i programi dizajnirani da prisluškuju mrežu odnosno da nadgledaju i hvataju mrežne pakete od interesa kao i ddos agenti koji nevidljivo šalju UDP/ICMP pakete sa ciljem zagušenja mreže odnosno obaranja servisa;
- *oni koji se integrišu u kernel* (eng. loadable kernel modules - LKM) *Linux sistema* - LKM je najčešće korišćeni rootkit protiv Linux sistema. Ovi rootkitovi vrše transparentnu izmenu jezgra, izvršavaju preusmeravanje tako što premapiraju sistemske pozive, omogućavaju izvršavanje na daljinu (komandama preko mreže), omogućavaju promiskuitetan režim (eng. promiscous mode, skriveni režim) čime se prikriva mrežni interfejs računarskog sistema na mreži.[381] Ovim rootkit-om moguće je izvršiti kompromitovanje različitih task-ova na računarskom sistemu izmenama identifikacionog korisničkog

380 Http://nmap.org/, 10.06.2016.

381 Postoje određene komande koje omogućavaju jezgru da se prikriju sve informacije o određenom procesu.

broja (eng. user id - UID) na sistemu,[382] efektivnog identifikacionog korisničkog broja (eng. effective user id - EUID)[383] kao i sistemski identifikacioni broj (eng. file system id, FSUID) bilo kog procesa.[384] Ovaj tip rootkit-a se dovodi u pitanje zbog pouzdanost dobijanja dumpa odnosno slike memorije na ispitivanom sistemu. Ovaj problem razmatrao je u radu Bradley Shatz;[385]

- *oni koji se integrišu u kernel Windows sistema* - ova vrsta rootkit-ova implementira određeni Device driver u kernel modu (eng. Device driver kernel mode) na tzv. nultom prstenu procesora (npr. na CPU x86) preko root.sys i pokretačkog program deploy.exe.[386] Ovaj rootkit može kreirati zadnjih vrata (eng. backdoor), skrivati fajlove (npr. komanda dir neće prikazati skrivene zlonamerne fajlove), procese i stavke iz registra (eng. windows registry), presretati aktivnosti sa tastature.

Sa forenzičkog gledišta kada je zlonamerni program tipa rootkit pristutan na računaru, ne može se sa sigurnošću utvrditi kakav on ima uticaj na sistem. Karakteristika ovih zlonamernih programa je da mogu biti inteligentno programirani tj. sa elementima veštačke inteligencije. Ova vrsta programa može da poseduje funkcionalnost prepoznavanja tehnike analize zlonamernih programa, koje sprovodi digitalni forenzičar, kako bi prikrila svoju prisutnost na sistemu odnosno aktivnosti. Forenzička analiza zlonamernih programa podrazumeva – detaljnu analizu programa u smislu identifikovanja izmena koje ovaj zlonamerni program vrši na operativnom sistemu. Ukoliko je zlonamerni program u operativnom sistemu i ukoliko je u kernelu može imati globalni uticaj na ceo sistem. Na primer operativni sistem kreira određeni log fajl i prosleđuje se instrukcija o upisivanju imena tog fajla na fajl sistem. Međutim ovaj proces može biti presretnut od strane zlonamernog programa što može imati za posledicu kreiranje izmenjenih log

382 UID na sistemu ima numeričku vrednost. Preporuka iz bezbednosnih razloga je da vredsnost UID-a za korisničke naloge bude preko 1000. UID sa vrednošću 0 je specijalan i pripada root korisniku koji ima neograničen pristup sistemskim resursima.

383 EUID služi da bi se odredio koji nivo pristupa ima trenutni proces. Kada EUID ima vrednost 0 implicira da taj proces ima neograničen pristup.

384 FSUID se izričito koristi za kontrolu pristupa fajl sistemu. Povezan je sa EUID-om čije se promene propagiraju na FSUID. Uloga FSUID-a je da se dozvoli programima da se samoograniče putem prava na fajl sistemu prema dodeljenom UID-u. Vidi: User identifier, Wikipedia, http://en.wikipedia.org/wiki/User_identifier, 30.03.2016.

385 Leschke T. R., "Cyber Dumpster Diving: $Recycle Bin Forensics for Windows 7 and Windows Vista", U.S. Department of Defense Cyber Crime Conference, 2010.

386 Device drivers posebno na novijim računarskim sistemima Microsoft Windows platformi mogu da se pokrenu u kernel modu (nulti prsten na CPU x86) ili u korisničkom modu (treći prsten na CPU x86). Device driver, Wikipedia, http://en.wikipedia.org/wiki/Device_driver, 31.03.2016.

fajlova. Zato prihvatljivost digitalnog dokaza preuzetog sa sistema na kome je zlonamerni program prisutan, može da varira od slučaja do slučaja i u zavisnosti od tipa zlonamernog programa i njegovog uticaja na sistem.

Jedni od najpoznatijih rootkitova su sledeći: Vanquish,[387] FU Rootkit,[388] WinLogonHijack Rootkit,[389] KIog Rootkit,[390] AFX Rootkit,[391] BootKitBasic RootKit,[392] KNARK,[393] ADORE,[394] Rustock.C, Skynet rootkit i drugi.

Detektovanje prisustava rootkita moguće je ostvariti sa posebnim alatima za tu namenu. Jedan takav alat je i *rootkit revealer* koji je u mogućnosti da detektuje rootkit pretnju na osnovu analiza postojećih sistemskih datoteka i postojećih stavki u Windows registru (razlike ili neslaganja).[395] Može se pokretati iz komandnog moda, iz grafičkog moda ili sa udaljenog sistema preko PSexec-a, koji je sastavni deo PsTools suite-a. Alati za detekciju rootkit-ova otkrivaju one instalirane zlonamerne module, koji presreću osnovne sistemske servise. Na te servise se oslanjaju svi programi kao i sam OS i ukoliko zlonamerni moduli postoje to znači da je ugrožena bezbednost sistema (odnosno da su aktivni određeni špijunski programi, virusi ili drugi zlonamerni programi). U nastavku će biti navedeni još neki alati namenjeni otkrivanju rootkit-a:

- *chkrootkit* (Check rootkit)[396] - otkriva prisustvo rootkita nakon

387 Vanquish rootkit spada u alate koji vrše DLL injection odnosno ubacuju zlonamerni kod (DLL bibliteku) u određeni proces (odnosno u memorijski prostor tog procesa) menjajući mu originalnu funkcju. Realizuje skrivanje fajlova, foldera, stavki iz registarske baze i loguje šifre.

388 FU rootkit je u stanju da sakrije procese, podigne privilegije procesa, mrežne konekcije, mrežne portove, lažira Windows Event Viwer kako bi onemogućio forenzičku analizu i čak je moguće da sakrije drajver uređaja na osnovu DKOM-a (eng. Direct Kernel Object Manipulation) u memoriji. Ovaj sofisticirani rootikih omogućuje LKM da ima direktan pristup kernelovoj memoriji, vršeći izmene nad objektima u memoriji pouzdano se skrivajući.

389 Ovaj rootkit ubrizgava zlonamerni DLL u winlogon.exe kompromitujući Windows funkciju WlxLoggedOutSAS function a posledica je logovanje korisnika u nezaštićenom otvorenom tekstu (eng. plaintext).

390 Ovaj rootkit je zapravo keylogger.

391 Ovaj rootkit koristi ubrizgavanje zlonamernog koda omogućavajući skrivanje procesa, modula, portova, fajlova i registarskih ključeva.

392 Ovaj rootkit je u suštini boot kit koji menja boot sektor sa ciljem onemogućavanja Windows NT bezbednosnog modela. Veoma je mali, podržava Windows 2000, XP, 2003 i pečuje kernel prilikom njegovog podizanja. Omogućava učitavnje dodatnih zlonamernih rootkit alata.

393 Spada u Linux LKM rootkit-ove, http://packetstormsecurity.com/files/download/24853/knark-2.4.3.tgz, 16.05.2016.

394 Spada u Linux LKM rootkit-ove, http://packetstormsecurity.com/files/download/32843/adore-ng-0.41.tgz, 16.05.2016.

395 Mark Russinovich, RootkitRevealer v1.71, Windows Sysinternals, http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx, 16.05.2016.

396 Http://www.chkrootkit.org/download.htm, 25.05.2016.

njegove instalacije na Linux sistemu;
- *rkscan*[397] - je alat koji otkriva LKM rootkitove na Linux sistemima;
- *rkdet (Root Kit Detector)*[398] – karakterističan po tome što se instalira pre nego što se zarazi rootkit-om. Predstavlja tip preventinog alata koji prepoznaje rootkit-ove na Linux sistemima i detektuje špijuniranje paketa (eng. packet sniffer);
- *carbonite*[399] - Linux kernel modul koji izlistava sve procese na nivou kernela otkrivajući LKM rootkitove;
- *rootKit Hook Analyzer*[400]- alat, koji će proveriti da li na Windows OS postoji rootkit instaliran na OS koji se prikačio na sistemske servise kernela;
- *iceSword*[401] - prikazuje skrivene procese i resurse koje Windows explorer nije u stanju da prikaže. Spada u sofisticirane alate, koji se instaliraju pre rootkit infekcije i na preventivni način pruža zaštitu Windows OS.

3.1.10. Podaci od značaja privremenog karaktera na Windows-u - sadržaj privremene memorije

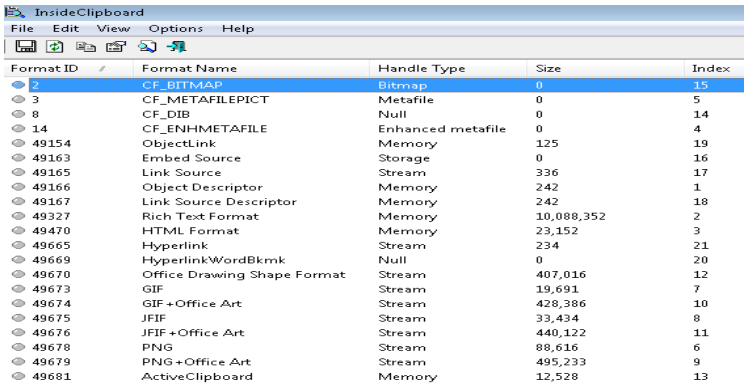
Sadržaj privremene memorije (*clipboard*) predstavlja prostor gde se podaci (tekstualni, binarni) privremeno odlažu za kasniju upotrebu. Većina Windows aplikacija omogućava ovu funkcionalnost kroz svoju EDIT stavku na MENI baru putem CUT COPY i PASTE opcija, odnosno kopiranje i premeštanje dokumenata između aplikacija na Windows sistemu.

Clipboard olakšava kopiranje i premeštanje podataka (objekata) kako u samom dokumentu tako i između samih dokumenata (tekstualnih i binarnih) i između samih aplikacija. Clipboard je predmet forenzičke istrage, pošto podatak kopiran u clipboard ostaje u njemu do gašenja računara ili njegove zamene drugim podatkom. Na primer, ukoliko je na ispitivanom računaru iskopiran određeni tekst, web adresa ili skype konverzacija, pa zatim urađen paste u program u kome se piše elektronska pošta. Tada će ceo kopiran tekst ostati dok se računar ne bude isključio ili dok se korisnik ne odjavi eng. logout, odnosno

397 Http://www.hsc.fr/ressources/outils/rkscan/index.html.en, 25.05.2016.
398 Andrew Daviel, Rkdet, http://vancouver-webpages.com/rkdet/, 25.05.2016.
399 Http://www.mcafee.com/ apps/ free-tools/termsofuse.aspx?url=/us/downloads/free-tools/carbonite. aspx, 27.05.2016.
400 RootKit Hook Analyzer, Resplendence Software Projects Sp, http://www.resplendence.com/hookanalyzer, 27.05.2016.
401 IceSword, Antirootkit.com, http://www.antirootkit.com/software/IceSword.htm, 27.05.2016.

dok ne bude urađen novo kopiranje u clipboard. To je još jedan veliki razlog koji ide u prilog vođenja digitalne forenzičke istrage "uživo", kada je u pitanju krađa intelektualnog vlasništva, prevare, uznemiravanja i itd. *Sadržaj clipboard-a nije "očigledno" vidljiv* ali je prisutan u sistemu što može biti i problem (jer u njemu mogu da se nađu osetljive informacije). Microsoft je napisao članak o tome kako sprečiti web sajtove da imaju pristup clipbaord-u.[402]

Da bi se *prikupile informacije iz clipboarda postoje alati* za tu namenu. Jedan dobar alat koji se pokreće iz komandnog okruženja je *pclip.exe,* koji može da izvuče tekstualni sadržaj iz clipboard-a.[403] Druga alatka je *clipboard,* koja može da se primeni i u Windows i u Linux okruženju i može da izvuče tekstualni sadržaj ili sadržaj fajla.[404] Sjajna alatka koja može da pruži uvid u osnovne clipboard formate, tekst i bitmape je program *InsideClipboard*.[405] Ovaj program pruža mogućnost snimanja fajlova kao sliku. Kao binarni fajl pruža dodatne informacije o fajlu, a mogu se naći i informacije o putanji do fajla, veličini i tipu. Na narednoj slici mogu se videti detalji vezani za objekat u clipboardu (što ukazuje da se radi o slici). Detalji iz clipboarda ukazuju da se radi o tekstu, a ono što je sjajno što ovaj program pruža je i uvid u putanju do samog fajla iz clipboard-a preko "Link source" pregleda.



Format ID	Format Name	Handle Type	Size	Index
2	CF_BITMAP	Bitmap	0	15
3	CF_METAFILEPICT	Metafile	0	5
8	CF_DIB	Null	0	14
14	CF_ENHMETAFILE	Enhanced metafile	0	4
49154	ObjectLink	Memory	125	19
49163	Embed Source	Storage	0	16
49165	Link Source	Stream	336	17
49166	Object Descriptor	Memory	242	1
49167	Link Source Descriptor	Memory	242	18
49327	Rich Text Format	Memory	10,088,352	2
49470	HTML Format	Memory	23,152	3
49665	Hyperlink	Stream	234	21
49669	HyperlinkWordBkmk	Null	0	20
49670	Office Drawing Shape Format	Stream	407,016	12
49673	GIF	Stream	19,691	7
49674	GIF+Office Art	Stream	428,386	10
49675	JFIF	Stream	33,434	8
49676	JFIF+Office Art	Stream	440,122	11
49678	PNG	Stream	88,616	6
49679	PNG+Office Art	Stream	495,233	9
49681	ActiveClipboard	Memory	12,528	13

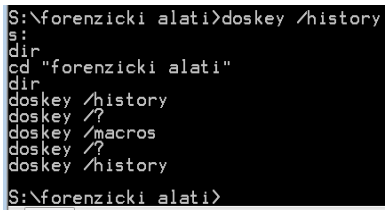
Slika 45. Izgled prozora programa InsideClipboard kada je u pitanju slika

402 How to Prevent Web Sites From Obtaining Access to the Contents of Your Windows Clipboard, Microsoft, http://support.microsoft.com/kb/224993, 27.05.2016.

403 Karl M. Syring, GNU utilities for Win32, http://unxutils.sourceforge.net/, 27.05.2016.

404 Steve.org.uk, Steve Kemp's Homepage, http://www.steve.org.uk/Software/clipboard/, 27.05.2016.

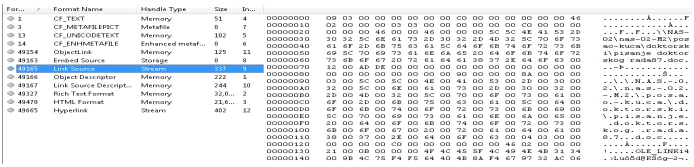
405 Freeware Utilities for Windows, NirSoft, http://www.nirsoft.net/utils/index.html, 29.05.2016.



Slika 46. Izgled prozora programa InsideClipboard sa prikazom putanje

3.1.11. Podaci od značaja privremenog karaktera na Windows-u - istorija pokrenutih komandi

Za digitalnog forenzičara vredan izvor informacija može da bude i istorija pokrenutih komandi na ispitivanom sitemu. Tragovi koji se mogu naći zavise od samog slučaja na primer: upotreba ftp, telnet, mapiranje drajvova razne druge aktivnosti, koje mogu da se dovedu u kontekst ispitivanog slučaja. Alatka *doskey* je sastvani deo OS i upotrebljava se sa switch-om "/history" prikazana je na sledećoj slici:



Slika 47. Prikaz komnde doskey /history

U registarskoj bazi moguće je takođe videti poslednju izvršenu komandu (uvek izvoditi iz proverenog komandnog okruženja):

„HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU"

Alatka koja takođe može pomoći pri dobijanju *istorije logovanja* je alatka *Ntlast.* Oslanja se na auditing politiku o istoriji logovanja. Ukoliko ona nije omogućena, potrebne informacije ova alatka neće pružiti.[406] To je signal administratorima da na sistemu obavezno omoguće auditing, jer u slučaju kompromitovanja sistema moguće je dobiti dragocene informacije. Alatka koja pruža detalje vezane za auditing na sistemu jeste *Microsoft Auditpol.*

406 Http:// www. mcafee. com/ apps/ free-tools/ termsofuse. aspx? url=/ hk/downloads/ free-tools/ ntlast. aspx, 29.05.2016.

Da bi se omogućio ili onemogućio auditing na sistemu to se radi iz dva koraka. *Prvi korak* određuje šta će se kontrolisati i šta će se snimati. To se uređuje grupnom polisom *Audit Policy*. *Drugim korakom* se određuju objekti, korisnici i grupe koje će biti kontrolisane. Na primer, ukoliko je potrebno da se prate svi neuspeli pokušaji pristupa određenom NTFS fajlu ili folderu mora da se podesi *Audit object access* policy na '*failure*'. Grupnoj polisi se pristupa preko konzolnog alata *gpedit.msc*.

Nakon omogućavanja auditinga na sistemu u *event vieweru* pod security opcijom mogu da se vide stanja praćenih aktivnosti. Event viewer-u se može pristupiti preko „*start-run-eventvwr.msc*" i u njemu možemo pregledati događanja na sistemu kroz logove aplikacija, bezbednosne logove (definisane kroz auditing) i sistemske logove, kao i kroz druge logove koji mogu biti specifično definisani (npr. logove perfomansi računarskog sistema).

Bruce Schneier je lepo objasnio značaj auditinga: "Auditing je od vitalnog značaja gde god se bezbednost ozbiljno shvata. Postojanje auditinga omogućava otkrivanje napada na sistem, pomaže da se razume šta se desilo nakon upada u sistem i može poslužiti za dokazivanje nedozvoljene aktivnosti na sudu".[407]

3.1.12. Podaci od značaja privremenog karaktera na Windows-u - mapirani drajvovi i deljeni resursi

Prilikom forenzičkog ispitivanja potrebno je utvrditi koji drajvovi ili mapirani deljeni resursi postoje na sistemu. Mapirani drajvovi mogu biti kreirani od strane korisnika, a mogu biti plod aktivnost zlonamernog korisnika, koji je na neki način iskoristio administratorsku šifru. Ove informacije spadaju u *privremene podatke* i značajne su jer se mogu dovesti u korelaciju sa dobijenim informacijima sa već opisanim alatima.

Najjednostavnija komanda koja se može upotrebiti na Windows sistemima (počev od Windows-a XP) jeste putem *WMI*[408] (eng. Windows Management Instrumentation) komande:

„c:\wmic logicaldisk get name, description,size, freespace, volumename, filesystem, providername"

Ovom komandom dobija se *spisak drajvova* koji se nalaze na sistemu,

---

407 Friedman C.S., *This Alien Shore*, Daw Books INC., New York 1998, http://rose.digitalmidnight.org/temp/books/ CS_Friedman/C.% 20S.% 20Friedman% 20-%20This% 20Alien% 20Shore.pdf, 21.06.2016.

408 Http://msdn.microsoft.com/ en-us/ library/ windows/ desktop/ aa394582%28v= vs.85%29.aspx, 29.05.2016.

tip drajva (mrežni-mapirani, prenosni ili fiksni-lokalni drajv), ime drajva, kapacitet drajva i slobodan prostor, tip fajl sistema i ime mapiranog drajva koji se može na narednoj slici:

Slika 48. prikaz postojećih drajvova na sistemu sa detaljima komadnom wmic

Alatka koju je napravio Harlan Carvey i koja takođe forenzičaru može pomoći pisana je u perlu i prekompajlirana za Windows, zove se *driveinfo.exe*. Njen izlaz skoro isti je kao kod prethodne komade i prikazan na sledećoj slici:

Slika 49. Prikaz izlaza programa driveinfo.exe

U toku istrage takođe će se ukazati potreba za uvidom u deljene resurse ispitivanog računara. Ti podaci se nalaze u registarskoj bazi (eng. registry) pod ključem

"HKEY_LOCAL_MACHINE\System\CurrentConrolSet\Services\lanmanserver\Shares"

Postoji komanda koje je sastavni deo Windows OS i njen izlaz dat je na narednoj slici:

"c:\wmic share list brief"

Slika 50. prikaz deljenih resursa na ispitivanom sistemu komandom wmic

Osim toga korisna alatka sa kojom forenzičar može da proveri omogućene deljene resurse na ispitivnom računaru jeste *Srvcheck* (dostupna iz Windows Server 2003 Resource Kit). Ona nabraja korisnike i korisničke grupe, koje imaju pristup uključujući i nivo pristupa. Forenzičar treba da bude

svestan da ova alatka ima svoje ograničenje tj. može prikazati samo neskrivene deljene resurse.

3.1.13. Podaci od značaja privremenog karaktera na Windows-u - privremeni fajlovi

Za digitalnog forenzičara dodatan izvor relevantnih dokaza mogu sadržati i *privremeni* (eng. temporary) *fajlovi*. Mnoge aplikacije kreiraju privremene fajlove i ostavljaju ih u računaru kada program završi sa radom ili ih brišu po zatvaranju aplikacije. Microsoft definiše privremeni fajl kao "fajl koji služi za privremeno smeštanje informacija da bi se oslobodila memorija za druge namene ili u funkciji bezbednosti za sprečavanje gubitka podataka kada program izvršava neke druge funkcije".[409] To znači da je sa jedne strane omogućeno najbolje iskorišćavanje memorije koja je dodeljena aplikaciji, a sa druge strane obezbeđena je zaštita integriteta podataka od grešaka prilikom memorisanja dokumenata, čak i prilikom naglog prestanka sa radom računara (nestanak struje, a računar je bez UPS-a).

Većina Windows aplikacija kao i sam OS zahtevaju privremeno skladišenje podataka na hard disku. Ovi fajlovi se skladište u *folderu "temp"* i uglavnom (mada ne uvek) ovi fajlovi imaju ekstenziju .TMP. Kada OSu ili programu oni ne budu više trebali brišu se od strane onog ko ih je kreirao (OS ili program). U praksi to nije uvek bio slučaj, što forenzičaru može biti od koristi prlikom ispitivanja računarskog sistema. Na primer, Microsoft office prilikom otvaranja dokumenta automatski određuje gde i kada će se kreirati privremeni fajl. U slučaju regularnog isključivanja računara privremeni fajl se povezuje sa otvorenim dokumentom koji se memoriše i zatvara. U slučaju neregularnog isključivanja Microsoft Office programa privremeni fajl se ne briše što ostavlja prostor za forenzička ispitivanja. *Fajlovi* koji forenzičaru mogu biti *od koristi* su kada je *Microsoft office* u pitanju:[410]

1. *Word: ~wrf0000.tmp*
2. *Word: ~mfxxxxx.tmp*[411]
3. *Word: ~dftxxxx.tmp*

409 Definition of Windows Temporary Files, Microsoft, http://support.microsoft.com/kb/44880, 28.05.2016.

410 Aaron P., Cowen D., Davis. C., *Hacking Exposed Computer Forensics, Second Edition*, The Mcgraw-Hill Companies, 2010.

411 Xxxx predstavlja broj sekvence.

4. *Word: wrf0001.tmp*
5. Kopiranje drugog dokumenta: *~wrcxxxx.tmp*
6. *Word* dokument: *~wrdxxxx.tmp*
7. Fajl privremenog dokumenta**:** *~wrfxxxx.tmp*
8. Rečnik: *~wrixxxx.tmp*
9. *Clipboard*: *~wrlxxxx.tmp*
10. Makroi: ~wrmxxxx.tmp
11. *Word OLE* dokument: *~wroxxxx.tmp*
12. *Scratch* fajl: *~wrsxxxx.tmp*
13. Konvertovani [*foreign*] dokument: *~wrvxxxx.tmp*
14. *PowerPoint*: *pptxxxx.tmp*
15. *Excel*: *~dfxxxx.tmp*

Ispitivanjem ovih fajlova forenzičar može i da oporavi ove podatke, koji mogu da budu potencijalni dokazni materijal. Pomenuti fajlovi se mogu pronaći na različitim lokacijama u zavisnosti od izvršene akcije nad fajlom. Najčešća mesta su u zavisnosti od verzije operativnog sistema:

„c:\Documents and Settings\<Korisnicko ime>\Local Settings\Temp" (Windows XP i ranije verzije)

„c:\Documents and Settings\<Korisnicko ime>\Application Data\ Microsoft\Word" (windows xp i raniije verzije)

„c:\Users\<Korisnicko ime>\AppData\Local\Temp" (ovde se smeštaju privremeni fajlovi od programa koje je pokrenuo korisnik, Windows Vista i kasnije verzije)

"c:\Windows\Temp" (ovde se smeštaju privremeni fajlovi kreirani od strane OS)"

Takođe se mogu naći i na mestima, gde je kreiran sam fajl. Prilikom pretraživanja privremenih fajlova drugih programa (koji mogu biti smešteni na različitim lokacijama) forenzičar treba pregledati i sam folder sumnjive aplikacije, koji može da sadrži veliki broj korisnih informacija od značaja za dalju istragu.

3.1.14. Postojani podaci od značaja na Windows-u - vremenski pečati fajl sistema

U toku digitalne istrage *vreme*, *datum* i *osumnjičeni* predstavljaju

tri ključna elementa.[412] To znači da forenzičar mora da zna kada su fajlovi od forenzičkog značaja kreirani modifikovani ili obrisani i ko je to uradio. To je važno da bi se saznalo šta se dešavalo na sistemu. Većina OS održava tri vremenska pečata (eng. timestampa) za svaki fajl na sistemu, poznatih kao *MAC vremena* (eng. Modified, Accessed, Created).[413] Da bi se dobili vremenski pečati svih podataka na fajl sistemu uglavnom se koristi alatka *dir*. U praksi se pokazalo da komanda „dir" ne daje pregledan listing kao i da nije upotrebljiva na programima koji rade sa tabelama. Kao dobro rešenje je alatka *"find"* koja je ustvari Linux alatka prilagođena za Windows dostupna u sklopu UnxUtils paketa.[414]

Izlaz komande *"c:\find.exe c:\ -printf "%m; %Ax; %AT;% Tx;%TT;%Cx;% CT;% U;% G;%s;%p\n"* je u formatu koji je upotrebljiv na svakom programu koji radi sa tabelama. Može prikazati dozvole nad fajlovima, poslednje vreme i datum pristupa, datum i vreme poslednje izmene kao i datum i vreme kreiranja fajla zatim vlasiništvo, veličinu i punu putanju. Ovaj prikaz se uglavnom koristi u korelaciji sa već utvrđenim sumnjivim procesima i putanjama kao dodatni dokaz prisustva određenog malicioznog fajla. U nastavku sledi tabela sa prikazom *NTFS osobina* pri određenim aktivnostima:

Tablela 6. NTFS osobine

Aktivnost	Vreme kreiranja	Vreme izmene	Vreme pristupa
Izmeštanje (sa volumena)	Ažurira se	Ne menja se	Ažurira se
Izmeštanje (u okviru volumena)	Ne menja se	Ne menja se	Ne menja se
Kopiranje	Ažurira se	Ne menja se	Ažurira se
Cut & paste (seći i dodavati)	Ne menja se	Ne menja se	Ažurira se

Kada je reč o vremenu izmene, sistem beleži vreme poslednje izmene datoteke odnosno kada je datoteka poslednji put sačuvana. Vreme pristupa podrazumeva kada je datoteka poslednji put čitana i na većini OS beleži se samo datum, ne i vreme. Vreme kreiranja je vreme kada se fajl prvi put pojavio na sistemu. Individualne aktivnosti na računaru ostavljaju mnoge tragove pa se iz navedenih vremenskih pečata, koji se odnose na fajlove i foldere, mogu izvući veoma korisne informacije za digitale forenzičare. Na primer, izmeštanje fajla u okviru volume-na ne menja vremena fajlu. Originalno obrisan directory entry je identičan novom directory entry-ju.[415] Na osnovu ove osobine

412 Mohay G., Anderson A., Collie B., Vel O., McKemmish R., *Computer and Intrusion Forensics*, Artech House, Norwood, MA, 2003.

413 Prlja D., *Sajberkriminal*, predavanje održano na Pravnom fakultetu Univerziteta u Beogradu, http//www.prlja.info/sk2008.pdf, 25.04.2012.

414 Karl M. Syring , GNU utilities for Win32, http://unxutils.sourceforge.net/, 29.05.2016.

415 Informacije o fajlovima čuvaju se u *directory entry*. Ove informacije zavise od OS.

forenzičari mogu da odrede gde su fajlovi izmešteni dok god postoji originalan directory entry. Ono što je interesantno primetiti jeste sledeće: fajlovi kopirani u okviru volume-a, ili premešteni sa hard diska na floppy, vreme kreiranja i vreme poslednjeg pristupa se ažuriraju, a vreme poslednje izmene ostaje isto. Za forenzičara značajan podatak jeste da se kod Windows Vista sistema ne prati vreme poslednjeg pristupa.[416] Razlog leži u činjenici da su se time povećale performanse računara. Praćenje vremena poslednjeg pristupa (koje u većini forenzičkih slučajeva nije omogućeno) može se omogućiti izmenom registarskog ključa *"HKLM\System\CurrentControlSet\Control\FileSystem\ NtfsDisableLastAccessUpdate"*.

Takođe forenzičari trebaju biti svesni da *vremena fajlova na sistemu ne moraju uvek biti tačna*. Razloga ima dosta, a glavni koje je NIST izdvojio u svom dokumentu su sledeći:[417]

- računarski sat nema podešeno tačno vreme. Na primer, sat na računaru nije se sinhronizovao sa vremenskim serverom (ntp server);
- vreme ne može biti snimljeno sa očekivanim nivoom detalja. Na primer, izostanak minuta ili sekundi;
- zlonamerni korisnik (napadač) je izmenio vremena nad fajlovima.

Pomenuti vremenski pečati su samo jedna oblast fajla (meta-podatak), koji mogu biti korisni prilikom utvrđivanja redosleda događaja i prirode aktivnosti na sistemu.

3.1.15. Postojani podaci od značaja na Windows-u - informacije o računarskom sistemu, verzija OS i nivo ažuriranosti paketa

Kada se govori o *postojanim podacima* (eng. nonvolatile) misli se na podatke koji ostaju na računaru i *posle reboot-ovanja* ili gašenja računarskog sistema. U njih spadaju i informacije o računarskom sistemu i njegovim komponentama koje mogu biti značajne u toku istrage, jer mogu pružiti dodatan kontekst kada je reč o identifikovanju kompromitovanog odnosno malizioznog računara. U daljem tekstu biće navedeni načini na koje ih forenzičar može upotrebiti da bi prikupio informacije o računarskom sistemu.

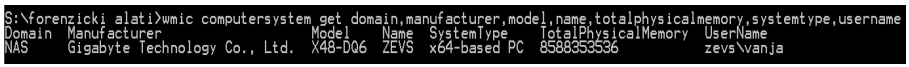
Directory entry sadrži informacije kao što su vlasništvo nad fajlovm, lokacija, veličina, prava pristupa i vremena aktivnosti (kreiranje pristup izmena).

416 Kipper G., *Wireless crime and forensic investigation*, Auerbach Publications Taylor & Francis Group, 2007.

417 National Institute of Justice, *Electronic Crime Scene Investigation. A Guide for First Responder*, 2001, https://www.ncjrs.gov/pdffiles1/nij/187736.pdf, 11.07.2016.

Alatkom *wmic* (forenzički sigurna) možemo dobiti informacije o računarskom sistemu kao što su domen odnosno workgrupa kome sistemu pripada, proizvođač ploče, model ploče, ime računarskog sistema, tip sistema (x86 ili x64,) ukupna RAM memorija i korisnika pod kojim je izvršena ova komanda. Izlaz ove komnde dat je na sledećoj slici:

"c:\wmic computersystem get domain,manufacturer, model,name ,totalphysicalmemory,systemtype,username"

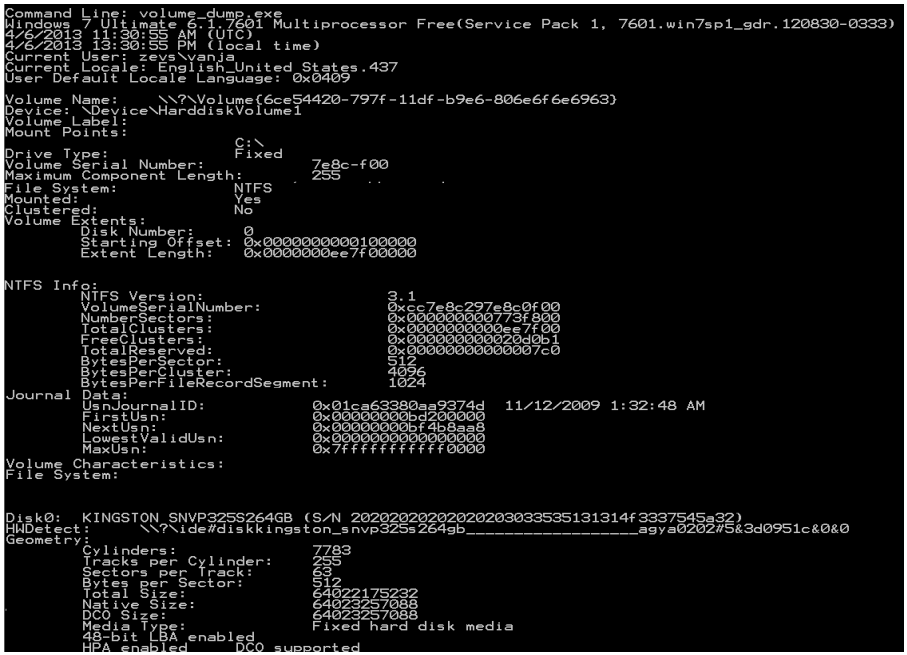


Slika 51. Prikaz detalja koji se odnose na postojeći sistem

Takođe informacije koje se odnose na BIOS računara mogu se dobiti upotrebom sledeće komande:

"c:\wmic bios list full" ili "c:\wmic bios list brief"

Forenzička alatka *volume_dump* iz paketa Forensic Acquisition Utilities (FAU) čiji je autor George M. Garner Jr, je alatka sa kojom možemo dobiti informacije o uređajima za skladištenje podataka kao što su oznaka proizvođača, vendor ID, serijski broj, USN journal informacije i ostale forenzički korisne sistemske informacije koje se odnose na pomenute uređaje. Izlaz ove alatke prikazan je na narednoj slici:



Slika 52. Prikaz izlaza alatke volume_dump

Informacije koje se odnose na prikaz instaliranih zakrpa (eng. hotfix) i servis pekova (eng. service pack) mogu biti prikazani preko *wmi* komandi i njenih argumenata:

"c:\wmic qfe"

Slika 53. Prikaz instaliranih hotfixova i servis pekova sa detaljnima

Ove informacije mogu pomoći administratorima i forenzičarima da ustanove da li je potrebna zakrpa bila instalirana na ispitivanom računaru. To može dati kontekst u daljem toku istrage, odnosno može ukazati na bezbednosni propust, ukoliko je postojao odnosno poboljšati sigurnost ukoliko određena zakrpa ili servis ne postoji na sistemu.

3.1.16. Postojani podaci od značaja na Windows-u - setovanja registra baze

Forenzički gledano *sadržaj ključeva iz registra* kao i *registarski fajlovi* spadaju u *postojane podatke*. Sa logičkog aspekta registarsku bazu podataka, koja se koristi za čuvanje sistemske konfiguracije i detalja o korišćenju, čine ključevi (eng. registry key) koji se mogu pretražiti u programu Registry editor. U fizičkom smislu se sve registarske informacije smeštaju u fajlove tzv. *hive*. U Windows 95 i Windows 98 registarski fajlovi ("hives") se zovu system. dat i user.dat U Windows ME zovu se Classes.dat, User.dat, i System.dat. U Windows NT, Windows 2000, Windows XP, Windows 2003, Windows, Vista i Windows 7 OS postoje nekoliko registarskih fajlova bez ekstenzije, koji su smešteni u folderu "*Windows\System32\Config*" i zovu se *Software, System*, *SAM*, *Security, Default*, a postoji i fajl *ntuser.dat* koji postoji za svaki korisnički nalog i nalazi se u folderu *"Documents and Settings\ime_korisnika"* (Windows XP i 2003) odnosno "*users\ime_korinika\"* (Windows Vista, 7).[418] Hive lista sa registarskim fajlovima na sistemu nalazi se pod ključem *"HKLM\System\ CurrentControlSet\Control\hivelist.*[419] Na forenzičaru je da donese odluku, koje će informacije izvlačiti iz registra i koje će fajlove prikupiti za dodatnu analizu. U određenim slučajevima maliciozni korisnik može biti prijavljen na sistem u toku forenzičkog ispitivanja pa forenzičar može doneti odluku da prati malicioznog korisnika uz očuvanje podataka tj. potencijalnih dokaza značajnih za istragu. Kada se sistem ponovo podiže može doći do određenih izmena nad već pomenutim podacima sa privremenim karakterom (mapirani drajvovi, startovani procesi, servisi i programi) pa te podatke forenzičar mora evidentirati i dokumentovati.

Određena podešavanja u registru bazi mogu da se odraze na forenzičku analizu i istragu. Ove podešene vrednosi u registru spadaju u postojane podatke, ali mogu uticati na način vođenja istrage. Podešena registarska opcija "*Clearpagefileatshutdown*" govori sistemu da izvrši brisanje page fajla kada se radi gašenje računara. *Page fajl* je fajl koji može sadržati vredne forenzičke informacije (šifre, delove konverzacije programa i druge značajne podatke), jer deo memorije nekog procesa (programa) može biti upisan u page fajl. To znači da po isključivanju računara informacije u page fajlu ostaju zapisane na hard disku. Ukoliko se ovaj fajl obriše prilikom isključivanja računarskog

418 Windows registry information for advanced users, Microsoft, http://support.microsoft.com/ kb/256986, 27.05.2016.

419 Registry Hives, Microsoft, http://msdn.microsoft.com/ en-us/ library/windows/ desktop/ ms724877%28v= vs.85%29.aspx, 28.05.2016.

sistema potencijalne vredne informacije mogu teško biti povraćene, a mogu biti i izgubljene. Ukoliko je vrednost *„HKLM\System\CurrentControlSet\ Control\SessionManager\MemoryManagement\ ClearPageFileAtShutdown"* podešena na 1, page fajl neće biti apsolutno obrisan već će biti prepisan sa nulama (eng. overwritten).

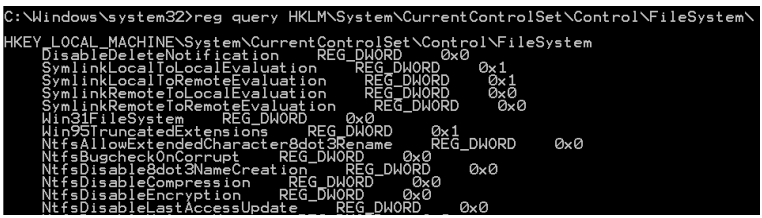
Windows OS poseduje mogućnost *isključivanja praćenja vremena poslednjeg pristupa fajlu* kroz registarsku opciju "*DisableLastAccess*". Prema Microsoftu njegovo podešavanje može uticati na performanse kod high-availability računarskih sistema, dok kod kućnih i kancelarijskih računara (lap top ili desktop) nema uticaja na performanse. Podešava se "*HKLM\System \CurrentControlSet\ Control\ FileSystem\ NtfsDisable Last AccessUpdate*" vrednost na 1. Provera koju vrednost ima DisableLastAccess moguće je uraditi preko alata koji je sastavni deo Microsoft OS (od Windows XP):

"C:\Windows\system32>fsutil behavior query disablelastaccess"

Izlaz komnde može biti DisableLastAccess = 0 ili DisableLastAccess = 1

ili *reg.exe* alatkom (koja se sastvani deo Windows OS od Windows XP) prikazano je na sledećoj slici:

"c:\ reg query HKLM\System\CurrentControlSet\Control\FileSystem\":



Slika 54. Prikaz vrednosti NtfsDisableLastAccessUpdate pomoću komande reg.exe

Treba napomenuti da *postavljena vrednost na 1* znači da je onemogućeno praćenje vremena pristupa fajlu na osnovu akcija čitanja i pregledanja osobina (eng. properties) fajla. Vreme će se menjati ukoliko je došlo do izmena na samom fajlu (npr. prilikom upisa u fajl). Na Windows 2003 ova vrednost u registru nije podešena, na Windows XP ova vrednost nije podešena, na Windows Visti ova vrednost je postavljena na 1, na Windows 7 ova vrednost postoji i postavljena je na 0.

Vrlo važna forenzička informacija može biti i ona koja se odnosi na pristup poslednjem ključu registarske baze. To može indicirati da je ključ menjana vrednost iz nekog razloga. Ta informacija se nalazi u registarskoj

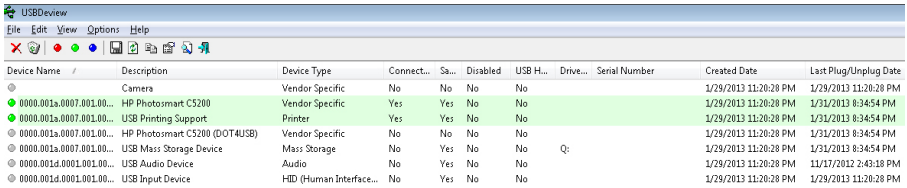
bazi na sledećoj putanji:

"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit"

Alatka *USBDeview* može forenzičaru da pruži dragocene informacije o USB uređajima (u preglednom formatu) koji su priključeni i koji su bili priključeni na sistem.[420] Mesto u registru bazi koje sadrži ove informacije jeste:

"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB"

Dobijene infomacije imaju veliki značaj s obzirom da je moguće ustanoviti odnosno dokazati povezanost određenog perifernog USB uređaja sa ispitivanim sistemom. Mogu se uočiti ime USB uređaja, opis, tip, da li je kontektovan ili nije, serijski broj uređaja, datum konektovanja na sistem i datum poslednje konekcije. Mana je što ne podržava u potpunosti sve USB 3.0 uređaje.[421] Detalje koje ova alatka može da prikaže dati su na sledećoj slici:



Slika 55. Prikaz detalja o USB uređajima sa alatakom USBDeview

Besplatna alatka *Woanware USBDeviceForensics* ima veću USB 3.0 kompatibilnost i omogućava forenzičarima dobijanje navedenih podataka.[422] Od komericijalnih programa tu je *AccessData RegistryViewer.*[423] Besplatan alat *USB Device History EnScript* autora Lance Mueller radi uz komercijalni program Guidance Software -EnCase Forensic.[424] [425]

---

420 USBDeview v2.60 - View all installed/connected USB devices on your system, Nir Sofer, http://www.nirsoft.net/utils/usb_devices_view.html, 26.05.2016.

421 S obzirom da se alatka razvija i da često izlazi njena poboljšana verzija očekuju se poboljšanja kada je reč o kompatibilnostima sa USB 3.0 uređijima.

422 Http://www.woanware.co.uk/?p=280, 28.05.2016.

423 Current Releases - Digital Forensics, AccessData Community, http://www.accessdata.com/support/ product-downloads, 29.05.2016.

424 Lance Mueller, USB device History EnScript, http://www.forensickb.com/2007/07/usb-device-history-enscript.html, 29.05.2016.

425 Mark Simms, *Portable Storage Forensics: Enhancing the Value of USB Device Analysis and Reporting*, http://www.google.rs/ url?sa= t&rct= j&q= &esrc= s&source = web&cd= 5&cad= rja&ved= 0CFkQFjAE&url= http%3A%2F%2Faut. researchgateway. ac. nz% 2Fbitstream% 2Fhandle% 2F10292% 2F4687% 2FSimmsM. pdf% 3Fsequence%

Značajne forenzičke oblasti u registru su i *autostart lokacije* u kojim je definisano automatsko pokretanje aplikacija: pri podizanju sistema, prijavljivanju korisnika na sistem i različitih akcije prilikom korisničkog pokretanja aplikacije. U slučaju da je u registru podešeno da će se prlikom pokretanja aplikacije od strane korisnika izvršiti određena akcija ili pokrenuti drugi program, to korisnik neće znati. Te lokacije nije jednostavno pronaći, ali je moguće. Jedna od takvih alatki je r*eg.exe*, koja je sastavni deo OS, a druga je alatka Marka Rusinovića (Mark Russinovich) i Brajsa Kogsvela (Bryce Cogswell) *Autoruns* koja postoji u GUI i CLI verziji sa istom funkcionalnošću. Alatka daje detaljan prikaz autorun vrednosti iz registra baze.

Autorun lokacije predstavljaju ključeve registarske baze koji aktiviraju programe u toku podizanja sistema.

Uobičajene Autorun lokacije su sledeće:

"*HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce*"

"*HKLM\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run*"

"*HKLM\Software\Microsoft\Windows\CurrentVersion\Run*"

"*HKCU\ Software\Microsoft\Windows NT\CurrentVersion\Windows\Run*"

"*HKCU\ Software\Microsoft\Windows\CurrentVersion\Windows\Run*"

"*HKCU\ Software\Microsoft\Windows\CurrentVersion\Windows\RunOnce*"

" *(Putanja do profila)\Start Menu\Programs\Startup*"

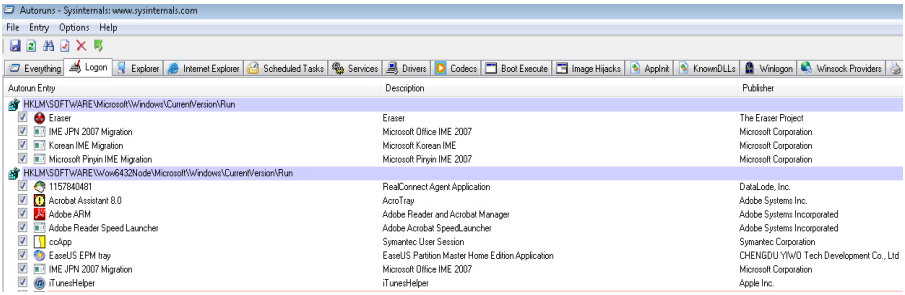
Na primer, moguće je proveriti *oblast raspoređenih poslova* (eng. task scheduler) koja može otkriti zlonamernu aktivnost. Raspoređeni poslovi imaju veliku korisnost za administratore u smislu održavanja sistema i mreže. Ovu funkcionalnost zloupotrebljavaju napadači koji žele da se određeni zlonamerni programi konstantno izvršavaju na sistemu (npr. Conficker-Downadup). Ovaj zlonamerni program ima sposobnost da se propagira kroz mrežu tako što nakon inficiranja određenog računara skenira mrežu tražeći Windows SMB share resurse pokušavajući da izvrši exploit. Forenzički značajan podatak u otkrivanju takvih sigurnosnih pretnji može se naći u log fajlu rapoređenih poslova koji se zove s*chedlgu.txt*. Ovaj fajl čuva zadatke koji treba da se startuju. U registarskoj bazi putanja ovog fajla se može pronaći u:

"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SchedulingAgent"

U Windows XP i Windows 2003 putanja do ovog fajla jeste *"C:*

3D3&ei =lR0MUaP0IeLj 4QTt2IGQDw&usg= AFQjCNFj7 juCv0VaGZfLY0PB2gKz_ gNsYw&bvm=bv.41867550,d.bGE , 01.02.2016.

Windows\SCHEDLGU.TXT”, dok je kod Windows Viste, Windows 7 i kasnije ta putanja *“C:\Windows\Tasks\SCHEDLGU.TXT”*. Ukoliko administrator nije definisao ništa za raspoređene poslove, forenzičar može očekivati da vidi vremena startovanja i stopiranja Task Scheduler servisa. S obzirom da se ovaj servis staruje kada se startuje i sam sistem forenzičar može imati pregled o vremenu pokretanju i gašenju računara. Nažalost puna putanja do izvršnog fajla neće biti prikazana u log fajlu, ali će ovaj log biti pokazatelj vremena kada je određen zadatak bio pokrenut.



Slika 56. Prikaz mogućnosti alatke autoruns

Prikaz raspoređenih poslova moguće je dobiti i alatkom koja je implementirana i u sam Windows sistem koja se zove "*at*".

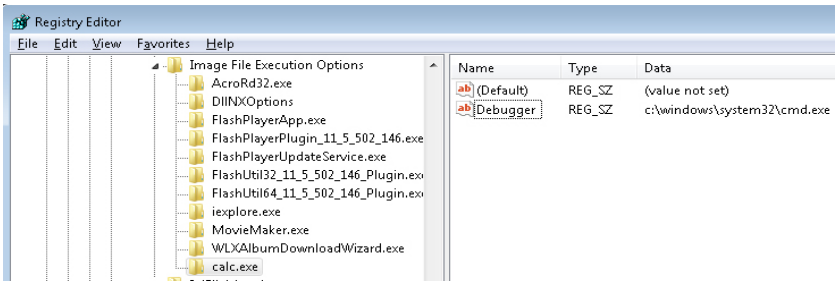
c:\at ,

gde izlaz može biti: “There are no entries in the list.”, ili detalji koji ukazuju na određeni posao koji treba da se obavi.

Važna oblast u registru je mesto gde je moguće sakriti program koji se zapravo startuje (maskiranje). Mesto koje forenzičar treba da ispita je zapravo sledeće:

„HKLM\Software\Microsoft\Windows NT\CurrentVersion\ Image File Execution Options”

Forenzičar treba da ispita da li je na ovom mestu kreiran neki *sumnjiv podključ* sa kreiranim stringom Debugger i vrednošću koja se odnosi na neki sumnjivi program. Na slici je radi demonstracije napravljen podključ sa imenom izvršnog programa calc.exe, kreiran je string sa imenom Debugger i vrednošću koja predstavlja putanju do aplikacije koja će se izvršiti (u ovom primeru je to komandni šel c:\windows\system32\cmd.exe), a to može biti neka maliciozna aplikacija.



Slika 57. Maskiranje izvšenog program preko editor registra baze

Posle pokrenute naredbe calc.exe u start-run-calc.exe otvoriće se komandni šel. Ova demonstracija je značajna jer može postojati zamaskirana maliciozna aplikacija, tako da je preporuka da administratori i forenzičari obavezno pogledaju ovu oblast. Administratori mogu da okriju napad i spreče potencijalne štete, a forenzičari mogu da pronađu dragocene informacije za dalji tok istrage.

Još jedna važna oblast u registarskoj bazi koja može da pruži dragocene informacije jeste *Protected storage oblast*. Podaci na ovom mestu se nalaze u šifrovanom obliku u registarskoj bazi. Alat koji može da dešifruje i oporavi ove podatke je forenzički alat *AccessData FTK*. Pogodan alat za forenzičko istraživanje "uživo" je i *pstoreview.exe*, koji može da omogući pregled ovih zaštićenih podataka (npr. snimljene šifre, imena korisnika u autocomplete formi putem Internet Explorera).[426] Na primer, forenzičar može pronaći šifre i naloge određenih servisa korisnika kao i dodatne podatke usnimljenih preko autocomplet forme (npr. HotMail,[427] Yahoo,[428] MSN,[429] Paypal,[430] Ebay,[431] i dr.).

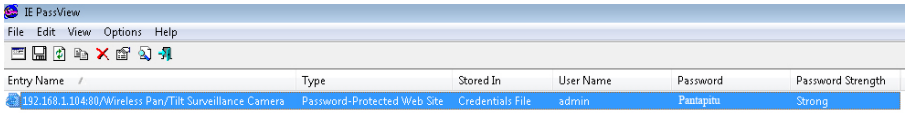
Može se reći da omogućavanje Autocomplete formi na sistemu može biti jedna od bezbednosnih pretnji o čemu je i pisao Brian Krebs u svom članku o hakeru koji je kroz napisani Bot program kontrolisao 1000 računara dobijajući podatke upravo iz autocomplete formi kompromitovanih računara.[432] Ipak treba naglasiti da se od verzije Windows explorera 7 zaštićena oblast za skladištenje više ne koristi za čuvanje naloga i korisničkih šifri i da alat *Passview.exe*[433] nije

426 Http://ntsecurity.nu/toolbox/pstoreview/, 16.05.2016.
427 Http://www.hotmail.com, 16.05.2016.
428 Http://www.yahoo.com, 16.05.2016.
429 Http://www.msn.com, 18.05.2016.
430 Http://www.paypal.com, 16.05.2016.
431 Http://www.ebay.com, 16.05.2016.
432 Brian Krebs, Invasion of the Computer Snatchers, The Washington Post, http://www. washingtonpost. com/wp-dyn/content/article/2006/02/14/AR2006021401342.html, 18.05.2016.
433 IE PassView v1.35 - Recover lost passwords stored by Internet Explorer, Nir Sofer, http:// www. nirsoft.net/utils/internet_explorer_password.html, 16.05.2016.

primenjiv od verzije Internet explorera 6, već je forenzičaru na raspolaganju novi alat *IEpassview.exe.*[434]

Na sledećoj slici je primer u kome su na Windows 7 OS ostali podaci iz Internet Explorera 9 kod korisnika koji toga nije bio svestan, tako da bi zlonamerni korisnik pristupom tom OS mogao dobiti korisničko ime i šifru za prisup IP kameri. To za posledicu može da ima kompromitovanje bezbednosti. Relevantni alati iste namene sa ciljem oporavka šifara iz popularnih internet pretraživača su sledeći:[435]

- PasswordFox[436] - Mozilla Firefox čitač šifri;
- ChromePass[437] - Google Chrome čitač šifri;
- OperaPassView[438] - Opera browser čitač šifri.



Slika 58. Prikaz IE passview programa sa pronađenim korisničim imenom i šifrom na sistemu

Može se primetiti da je korisnost ovih alata dvostruka. Sa jedne strane omogućuje se digitlanom forenzičaru pristup osetljivim infomacijama "uživo" koje mogu biti značajne za dalji tok istrage (pogotovu kada se radi o krađama podataka, neovlašćenom distribuiranju podataka, nestanku osobe), a sa druge strane tim istim alatima moguće je testirati sopstvene slabosti na sistemu, što za posledicu ima povećanje bezbednosti na samom sistemu.[439]

---

434 IE PassView v1.35 - Recover lost passwords stored by Internet Explorer, Nir Sofer, http://www. nirsoft.net/utils/internet_explorer_password.html#DownloadLinks, 16.05.2016.

435 Newsham T., Palmer C., Stamos A., *Breaking Forensics Software: Weaknesses in Critical Evidence Collection*, BlackHat Conference 2007, http://www.defcon. org/images/defcon-15/dc15-presentations/ Palmer_and_Stamos/Whitepaper/dc-15-palmer_stamos-WP.pdf, 11.07.2016.

436 PasswordFox v1.56 - Extract the user names/passwords stored in Firefox, Nir Sofer, http://www. nirsoft.net/utils/passwordfox.html, 16.05.2016.

437 ChromePass v1.37, Nir Sofer, http://www.nirsoft.net/utils/chromepass.html, 19.05.2016.

438 OperaPassView v1.10 - Recover the passwords stored in Opera Web browser, Nir Sofer, http://www.nirsoft.net/utils/opera_password_recovery.html, 18.05.2016.

439 Npr. moguće je uočiti postojeće šifre i osetljive informacije a da korinsik toga nije svestan, što može biti zloupotrebljeno od strane malicioznog korisnika.

3.1.17. Postojani podaci od značaja na Windows-u - tačka za oporavak sistema

Mesto gde se nalaze fajlovi potrebni za oporavak sistema (eng. System Restore Point) nalazi se pod *"c:\System Volume Information*". Ovom mestu nije moguće prići preko Windows Explorera ni sa administratorskim nalogom. Po difoltu sistem restore points kreira se nakon 24h i zadržava se 90 dana kod Windows Vista OS dok se Windows 7 snapshot kreira svakih 7 dana. Oblast u registru koja je odgovorna za sistem restore se nalazi u:

„HKLM\Software\Microsoft\WindowsNT\CurrentVersion\SystemRestore"

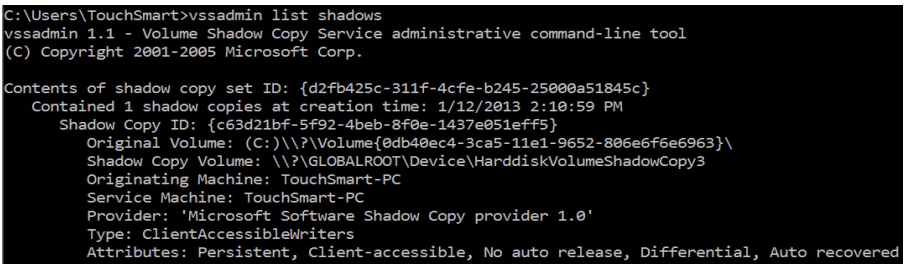
Sistem restore moguće je pokrenuti ručno, dok se automatski pravi pre ažuriranja Windowsa (eng. Windows update), pre instaliranja aplikacije koja poziva Snapshot API, pre restora samog sistema (u slučaju da je izabran pogrešan restore point) i prilikom instaliranja nepotpisanih drajvera (eng. unsigned driver).[440] Za digitalnog forezničara važno je da zna da se proces vraćanja sistema na određeni datum loguje u event logu kao EVENT ID 110 i da VSS (eng. Volume Shadow Copy Service) servis koji odgovoran za restore nadgleda sve fajlove.[441]

Da bi digitalni forenzičar mogao da priđe podacima koje sadrži *"c:\System Volume Information"* i da ustanovi promene, koje su se dešavale na sistemu na raspolaganju su mu određeni alati. Na samom Windows OS postoji alat *vssadmin*. Na primer:

"c:\vssadmin list shadows" izlistaće se sadržaj *"c:\System Volume Information"* odnosno tačke za oporavak sistema pre određene promene.

440 Restore Points, Microsoft, http://msdn.microsoft.com/en-us/library/windows/ desktop/ aa378910 %28v=vs.85%29.aspx, 18.05.2016.

441 Http://msdn.microsoft.com/en-us/library/ windows/ desktop/ aa384649% 28v= vs.85%29. aspx, 18.05.2016.



Slika 59. Prikaz izlaza komande vssadmin

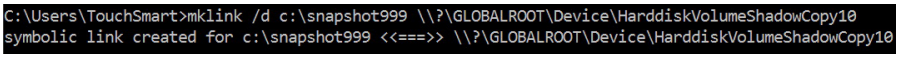
Nakon listanja forenzičaru će biti potrebno da mount-uje određen system restore points na neku svoju forenzičku stanicu.[442] To se radi sa komandom:

"C:\>mklink/d C:\IME_I_LOKACIJA_SIMBOLICKOG_LINKA \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopyXXXXX\"

Na primer:

"C:\>mklink/d C:\snapshot10 \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy10\"

Ukoliko je simbolički link ispravno napravljen biće prikazano kao na slici:

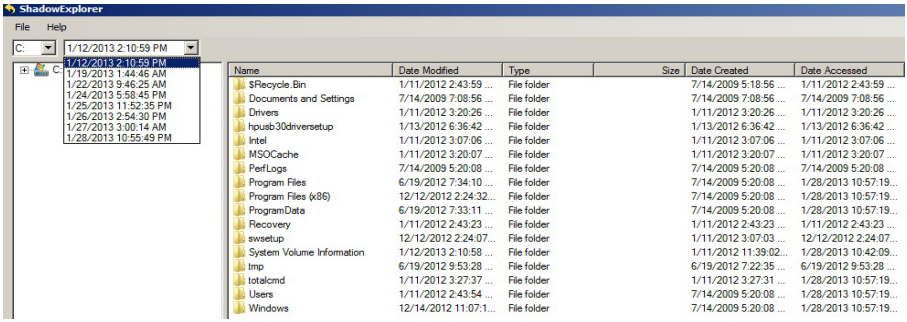


Slika 60. Prikaz kreiranja simboličkog linka na određenu lokaciju

Nakon toga digitalnom forenzičaru će biti omogućeno ispitivanje tih mesta za oporavak sistema. Druga alatka koja daje dosta pregledniji prikaz shadows copy tj. snapshot-a jeste *Shadow explorer* koji funkcioniše na Windows Visti, 7 i 8.[443] Ova alatka dopušta forenzičaru pretraživanje shadows kopije koju kreira VSS, prikazuje datume svih snapshot-ova na sistemu i omogućava preuzimanje prethodnih verzija fajlova i foldera. Prikaz ovog alata dat je na sledećoj slici:

442 Ovaj način pretraživanja po mestima za oporavak sistema više je orijentisan sa post-mortem analizu ili kako neki autori navode postmortem analizu kada se ispituje sumnjivi hard disk.

443 ShadowExplorer, http://www.shadowexplorer.com/downloads.html, 29.05.2016.



Slika 61. Prikaz alata ShadowExplorer

Shadow explorer alatka, kod Windows 7 operativnog sistema, može biti korisna i za oporavljanje prethodnih verzija kompromitovanog ili obrisanog fajla od strane određenih zlonamernih programa tipa ransomware. Da bi čuvanje prethodnih verzija bilo omogućeno na sistemu za određeni drajv to se radi na sledeći način:
System properties - System protection - Protection settings - odabrati drajv i pod tabom Configure odabrati "Restore previous versions of files".

Na samom Windows sistemu moguće je na nekoliko načina onemogućiti kreiranje shadow kopije tj. snapshota sistema ili obrisati snapshot-ove. Jedan od načina je onemogućavnje VSS servisa (eng. Volime Shadows Copy Service), zatim putem opcije Disk Cleanup (koja omogućava brisanje svih snapshot-ova osim trenutnog). Preko opcija System protectio (My computer-system properties-system protection-configure) moguće je onemogućiti VSS servis i brisanje svih postojećih snapshot-ova. Alatkom *Vshadow* koja dolazi sa Shadow Copy Software Development Kit[444] se mogu obrisati svi snapshotovi[445] ukoliko se izvši "*c\vshadow -da*".

Digitalni forenzičar prilikom analize kompromitovanog sistema treba da uzme u obzir da će zlonamerni korisnik pokušati da ukloni tragove. Microsoft VSS funkcionalost je jako dobra po pitanju zaštite podataka na sistemu i ukoliko je ona iz nekog razloga isključena forenzičaru to može biti signal da je sistem kompromitovan (u korelaciji sa dodatnim pokazateljima) odnosno dokaz da je malicizoni korinik pokušao da incidentnu radnju ili nedozvoljenu aktivnost prikrije.

444 Volume Shadow Copy Service SDK 7.2, Microsoft, http://www.microsoft.com/en-us/download/ details.aspx?id=23490, 30.01.2016.

445 Nije samo to jedina namena vssadmin alata. Pomoću njega moguće je takođe izlistati sve snapshot-ove na sistemu, uraditi mount određenog snapshot-a i pristupati mu kroz određeni drajv na sistemu preko Windows Explorera (eng. drive letter) i obrisati sve snapšotove sa komandom.

3.1.18. Postojani podaci od značaja na Windows-u - logovi na sistemu

Prilikom istrage kada, postoje određeni događaji u log fajlovima sa forenzičke tačke gledišta bitno je utvrditi korelacione parametre između više nastalih dešavanja. To je moguće izvući iz određenih logova. Da bi logovi bili priznati na sudu kao validan digitalni dokaz bitna je procedura po kojoj je log prikupljen. Ulaskom u sistem i kopiranjem loga fajla pravi se greška ukoliko se pre kopiranja ne primeni heširanje nad log fajlom. Posle kopiranja potrebno je uraditi još jednom heširanje da bi se potvrdio integritet log fajla. U slučaju poklapanja dobijene dve vrednosti ovaj digitalni dokaz može se upotrebiti na sudu. Log fajl bez heša ne daje garanciju da ga neko nije izmenio i postoji realna mogućnost da takav dokaz ne bude validan na sudu.

Logovi događaja tzv. event log su esencijalni fajlovi u OS. Pružaju uvid u korišćenje naloga na sistemu u svakom trenutku. Postoje sistemski, aplikativni i bezbednosni event logovi. Ranije verzije Windows OS (NT, 2000, XP i 2003) koriste sistem za logovanje poznat kao Event logging.[446] Sistem za logovanje je u Windows Visti i Windows 7 zamenjen novim, koji je izmenio strukturu zapisa o logovanom događaju. Novi format je postao kompleksniji od prethodnog i njegova struktura dostupna je na Microsoft MSDN sajtu.[447] Razlika u strukturi povlači za sobom korišćenje drugog tipa alata za analizu ovih log fajlova.

U zavisnosti na koji način je podešeno evidentiranje događaja na ispitivanom sistemu i na koji način se vrši odgovor na incident odnosno nedozvoljenu aktivnost, svi pristupi sistemu biće evidentirani. Korisničkim nalozima omogućeno je dve vrste pristupa računarima: interaktivni pristup sistemu i pristup deljenim resursima. *Sistemiski log fajlovi* mogu sadržati informacije o korisničkim nalozima koji su korišćeni u maliciozne aktivnosti a mogu ukazati i na to da je korisnički nalog "ukraden" odnosno zloupotrebljen bez znanja vlasnika tog naloga. Na primer, ukoliko se ispitivanom računaru pristupa od spolja (udaljen pristup ispitivanom sistemu može nekada biti jako važan da bi se sačuvali određeni podaci od izmena) i ukoliko je sistem za logovanje ispravno konfigurisan u Security event logu će biti evidentiran

446 Informacije o strukturi generisanih Event logova u ovim OS može se naći na MSDN sajtu. EVENTLOGRECORD structure, Microsoft, http://msdn.microsoft.com/en-us/library/ windows/ desktop/ aa363646%28v=vs.85%29.aspx , 30.01.2016.

447 Windows Event Log Reference, Microsoft, http://msdn.microsoft.com/en-us/library/ windows/ desktop/aa385785%28v=vs.85%29.aspx, 30.01.2016.

svaki pristup od spolja. Lokacija (koja može da se promeni) gde se upisuju programski, bezbednosni i sistemski log fajlovi u Windows OS je definisana u registarskoj bazi na sledećem mestu:

"HKLM\System\CurrentControlSet\Services\Eventlog"

Za Windows Vistu i Windows 7 OS lokacija je *"c:\widows\system32\winevt\logs\"*.

Za Windows XP OS lokacije *"c:\widows\system32\config\"*.

Sistemski event logovi sadrže informacije o različitim delovima OS. Na primer, tu se mogu pronaći informacije o učitanim drajverima, vremenima startovanja i gašenju računara, aktivnosti na CD ili DVD-u i druge aktivnosti. Aplikativni event log je na raspolaganju korisničkim aplikacijama da beleže događaje koji su od značaja za ceo sistem. Na primer, antivirusni program može snimati informacije o ažuriranju, skeniranju ili pronađenom virusu. Bezbednosni event logovi beleže događaje vezane za upotrebu sistemskih resursa. Na primer, beleže se pokušaji koisničkih logovanja, mrežne konekcije, kreiranje otvaranje i brisanje fajlova (po difoltu bezbednosno logovanje nije uključeno).

Posle verzije Windows XP, format logova se promenio sa *.evt* na *.evtx*. Forenzičar treba da zna da svaki event log ima svoj event ID (npr. EVENT ID 540 ukazuje na logovanje dok event ID 538 ukazuje na odjavljivanje), vremenski pečat (eng. timestamp) i broj zapisa. Baza event logova koja daje dodatne informacije o određenom event log-u na osnovu njegovog ID broja nalazi se na sajtu http://www.eventid.net/search.asp.

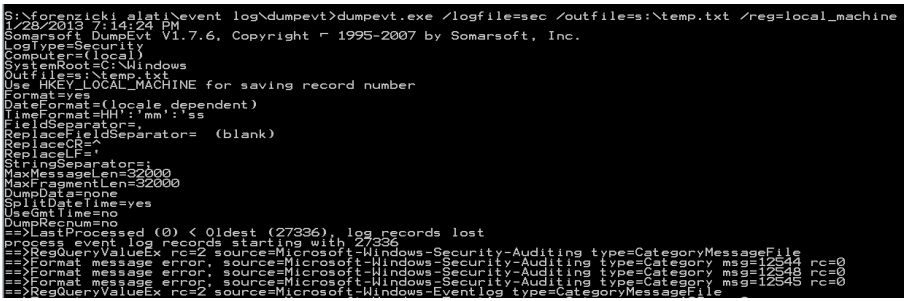
Podatke iz event fajlova moguće je procesirati kroz log parsere (alati koji mogu preko sql komandi procesirati log fajl). Na Windows OS omogućeno logovanje programskih i sistemskih događaja, a da se po difoltu bezbednosni događaji ne loguju (ovaj podatak se odnosi na Windows XP i ranije).[448] Kod Windows Viste i Windows 7 OS važno je uključiti monitoring naloga na sistemu (uspešnih i neuspešnih prijava na sistem) što kao preventivna mera može podići nivo bezbednosti (otkrivajući pokušaje upada u sistem), a forenzičaru pružiti dodatan uvid u dešavanja na kompromitovanom sistemu.

To se radi na sledeći način: "start-run-secpol.msc-localpolicies-auditpolicy- Audit account logon events-properties-čekirati Success and Failure"

"start-run-secpol.msc-localpolicies-auditpolicy-Audit Logon events-properties - čekirati Success and Failure "

448 Detaljno uputstvo kako se na Windows XP omogućava bezbednosno logovanje dostupno je na: http://www.microsoft.com/ resources/documentation/windows/xp/all/proddocs/en-us/ els_ start_ security_ log.mspx?mfr=true, 26.05.2016.

Alati sa kojima se mogu dobiti zapisi iz logova su *psloglist.exe*[449] i *dumpevt.exe*.[450] Moguće je iskopirati sve *.evt fajlove i forenzički ih ispitivati (zavisi koliki nivo privilegije digitalni forenzičar ima na ispitivanom sistemu "uživo"). Na sledećoj slici je prikazana upotreba alatke dumpevt.exe sa ispravnom sintaksom na Windows 7 x64 operativnom sistemu:



Slika 62. Prikaz upotrebe alatke dumpevt.exe
za prikupljanje logova događaja iz sistema

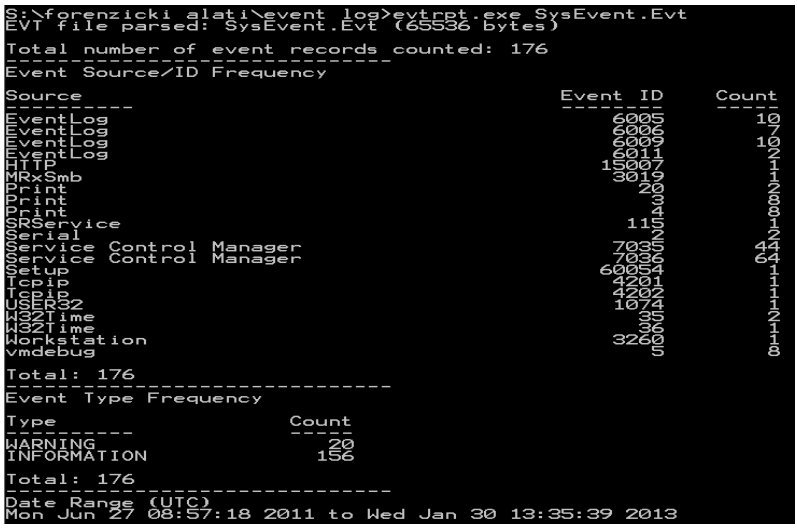
Kada su u pitanju sistemi pre Windows Viste, forenzičar može koristiti alatku (perl skriptu) za analizu log fajlova koja se zove *evtrtp.exe*.[451] Druga alatka koja je na raspolaganju forenzičaru je *grokevt* koja je pogodna za analizu log fajlova.[452] Na sledećoj slici prikazan je izlaz alatke evtrtp koja je dala analizu sysevent.evt fajla:

449 SomarSoft Utilities, SomarSoft, http://www.systemtools.com/somarsoft/?somarsoft.com, 27.05.2016.

450 Http://www.systemtools.com/cgi-bin/download.pl?DumpEvt, 27.05.2016.

451 Dostupno na disku koji se dobija uz knjigu Windows Forensic Analisys od Harlana Carvey.

452 GrokEVT Download, Sentinel Chicken Networks, http://projects.sentinelchicken.org/grokevt/ download/, 30.01.2016.

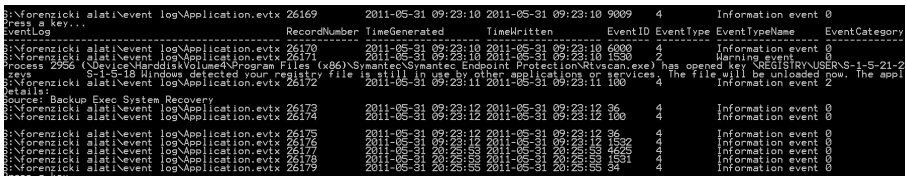


Slika 63. Prikaz analize sysevent.evt log fajla alatkom evtrtp.exe

Alatka *log parser* koja može izvršiti proces evtx fajlova. [453] Njen prikaz dat je na sledećoj slici:

Komanda se upotrebljava sa sql sintaksom:

"logparser.exe "SELECT * from application.evtx" -i:evt"



Slika 64. Izlaza alata log parser izvšenog nad fajlom application.evtx

Osim event log fajlova na računaru je moguće pronaći log fajlove kako od strane sistema tako i od strane aplikacija. Oni mogu biti jako dobar i koristan izvor podataka o dešavanjima na računaru. Windows XP pri instalaciji kreira negde oko 135 log fajlova ili osnovnih tekst fajlova koji rade kao log fajlovi.[454]

453 Log Parser 2.2, Microsoft, http://www.microsoft.com/en-us/download/ details.aspx?id=24659# overview, 05.02.2016.

454 Aaron P., Cowen D., Davis. C., *Hacking Exposed Computer Forensics, Second Edition*, The Mcgraw-Hill Companies, 2010.

Forenzičar u ovim log fajlovima može pronaći vrlo relevantne podatke o tome kada je program prvi put instalilran na sistem, vreme poslednjeg pokretanja programa, na koji način je konfigurisan kada je poslednji put startovan. Međutim nije uvek očigledno na koje se procese ili aplikacije određeni log fajlovi odnose. Ponekad je potrebno da forenzičar pretraži ceo disk u potrazi za *.log fajlovima i da ih ispita ponaosob. U log fajlovima se mogu naći i informacije o mogućim problemima sa određenim programom ili procesom na sistemu. Stoga je blagovremenom reakcijom moguće sprečiti protencijalni bezbednosni problem kako aplikacija tako i celog sistema.

Na Windows XP OS i Windows 2003, lokacija od forenzičkog značaja može biti log fajl koji generiše alatka *Dr. Watson*.[455] Ova alatka skuplja informacije o sistemu i programskim greškama u tekstualni log fajl. Taj fajl može se poslati na analizu stručnjacima za rešavanje problema na sistemu. Ostim toga može biti značajna i forenzičarima prilikom istrage OS.

Nalazi se na lokaciji: *"c:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson*"

Putanja ovog alata je definisana u registarskoj bazi pod slededćim ključem: *"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DrWatson*"

Značajno je reći za alatku Dr. Watston da kada se pojavi određena greška informacije o njoj snimaju se u *fajl drwtsn32.log* fajl. Format ovog fajla sastoji se od putanje programa koja je uzrokovala grešku zajedno sa datumom i vremenom nastanka. Ove informacije su dragocene za istragu pogotovu po pitanju malicioznih programa ili posledica upada na sistem ili zloupotrebe. Ove informacije forenzičar može staviti u kontekst dešavanja na sistemu npr. kada je maliciozni korisnik dobio pristup serveru, koji je proces pokrenut (što može da se vidi iz podataka o vremenu instalirane aplikacije), koji su DLL-ovi su učitani od strane sumnjivog programa koji je izazvao određeno programsko odstupanje (eng. access violation odnosno eng. application exception). Dr. Watson takođe kreira i *crash dump fajl* (user.dump) koji se nalazi u istom direktorijumu baš kao i drwtsn32.log fajl. Ovaj dump fajl može se pročitati sa alatakom *Windbg* koja je deo Microsoft Windows Debugging alata.[456] *Fajl user.dump* sadrži samo poslednje aplikativno odstupanje, a prepisuje se njenim novim nastankom. Ovaj fajl izuzetno je dragocen jer može da sadrži šifre, čiste tekstualne podatke (eng. plain text) ili dešifrovane podatke i podatke koji ukazuju na aktivnost malicioznog korisnika.

---

455 Description of the Dr. Watson for Windows (Drwtsn32.exe) Tool, Microsoft, http://support.microsoft.com/kb/308538, 04.06.2016.

456 Memory Dump Analysis Anthology, Software Diagnostics Services, http://www.windbg.org/, 04.06.2016.

S obzorom da Dr. Watson32 alatka nije dostupna na Windows Vista/ Server 2008/Windows 7/Server 2008 R2 moguće je koristiti podatke koje generiše WER (Windows Error Report). Kada nastane aplikativno odstupanje u event logu će biti pojaviti EVENT ID sa brojem 1000 koji ukazuje da se radi o aplikativnoj grešci. Kada se desi krah aplikacija ili servisa (access violation odnosno application exception) postoje nekoliko lokacija gde forenzičar može pronaći user.dmp fajl.

Ukoliko je aplikacija koja je kontrolisana od strane UAC-a doživela krah (eng. User Access Control) dump će biti smešten na:

"C:\ProgramData\Microsoft\Windows\WER\ReportArchive"

ili

"C:\ProgramData\Microsoft\Windows\WER\ReportQueue" u zavisnosti od toga da li je mode queue podešen ili ne.

Ukoliko je aplikacija koja nije kontrolisana od strane UAC-a doživela krah (eng. User Access Control) dump će biti smešten na:

"C:\Users\Ime_Korisnika\AppData\Local\Microsoft\Windows\WER\ ReportArchive" ili

"C:\Users\ Ime_Korisnika \AppData\Local\Microsoft\Windows\WER\ ReportQueue"

Za forenzičara najlakši način pretraživanja ovih fajlova je sa alatom dir:

*"c:\dir *.*dmp /s ProgramData\Microsoft\Windows\WER\"* i

*"c:\dir *.*dmp /s c:\users\"*

Ovi dump fajlovi mogu da se verifikuju alatkom *dumpchk.exe* o kojoj je već bilo reči, a učitavaju se sa takođe već pomenutom alatkom *windbg.exe*. Log parser Lizard predstavlja odličan alat za analizu logova. Procesira log fajlove koji se odnose na Microsoft OS IIS logovi, sistemske logovi, logove Oracle sistema, apache logovi i formira ih u oblik baze koje je moguće pretraživati kroz select upite.[457]

Kada je reč o tzv. text based logovima, s obzirom na to da .txt format ima mali heder jako je teško nakon njihovog brisanja izvršiti njegovu rekonstruciju. To znači da se sa carving procesom neće moći iz praznog prostora hard diska povratiti kompletan log fajl. Mogu se povratiti segmenti, ali oni nisu validni na sudu ukoliko nemamo sa čim da ih uporedimo. Zato je preporuka da se tzv. text based logovi čuvaju na udaljenoj lokaciji. Forenzičar mora poznavati formate određenih događaja tj. poruka (deny, can not access i dr.) kako bi od dobijenih informacija izvršio korelaciju određenih dešavanja koja su nastala u logu. Log parser Lizard može uraditi

457 Http://www.lizard-labs.com/log_parser_lizard.aspx. 17.07.2016.

korelaciju logova iz više baza na primer iz loga html_access i loga iz baze baze podataka i zato je jako važno da postoji isti timestamp.

Svi ovi opisani logovi mogu biti izuzetno značajni prilikom dokazivanja i potkrepljivanja vremenskog okvira aktivnosti na sistemu. Na primer, napadač je iskoristio ranjivost određenog sistema, izvršio upload malicioznih alata i prilikom pokretanja došlo je do greške application exception. Na osnovu iznetog moguće je pronaći logove pristupa napadača sistemu, logovi pokazuju vreme kada je izvršen upload alata (zajedno sa IP- adresom). Event logovi će ukazati na grešku application exception a Drwatson log bi ukazao na aplikaciju koja je to izazvala. Ove informacije mogu pomoći forenzičaru da učvrsti svoj stav o tome, koje su aplikacije već postojale na sistemu pre pristupa maliciznog korisnika na sistemu, koje je aplikacije on dodao i vreme kada su one pokrenute na sistemu. Sa bezbednosne strane logovi su korisni samo ukoliko se redovno pregledaju.

3.1.19. Postojani podaci od značaja na Windows-u - Recycle bin i obrisani fajlovi

Recycle bin ili korpa za otpatke se može posmatrati metaforično kao kada se zgužvani papiri bace u korpu za otpatke. Papiri su bačeni, ali su još uvek tu. Prema analogiji podaci koji su obrisani sa sistema premeštaju se u oblast Recycel bin i još uvek su prisutni na sistemu. Korisnost *Recycle bina* ogleda se u tome da kada se određeni podatak slučajno obriše moguće je povratiti na njegovu prethodnu lokaciju. Dakle, kada se nešto obriše sa desktopa ili Windows explorera to nije trajno obrisano, već je premšteno u Recycle bin. Recycle bin direktorijum je prisutan u fajl sistemu u korenskom (root) direktorijumu svakog hard diska. Za forenzičku istragu izuzetno je značajan, jer može sadržati dragocene podatke. Postoje razlike u formatu i načinu smeštanja izbrisanih fajlova kod određenih verzija Windows OS. Kod Windows XP OS kada se fajl obriše (ne računajući na komandu del i erase pod komandnim okruženjem) kreira se poddiretktorijum za određenog korisnika u RECYCLER direktorijumu. Naziv ovog poddirektorijuma se imenuje sa korisničkim bezbednosnim identifikatorima SID.

Na primer: *"C:\RECYCLER\S-2-6-26-1839457583-836208765-1990"*

Potrebno je reći da kada se otvori Recycle bin sa desktopa on će direktno pristupiti poddirektorijumu aktivnog korisnika prikazujući obrisani sadržaj. Ukoliko se vrši analiza preko forenzičke slike moguće je dobiti informacije od korisničkim aktivnostima, koliko je često praženjen

Recycle bin i identifikovanje tipa fajlova na osnovu razumevanja formata imenovanja.[458] Na primer, kada se preseli fajl u Recycel bin biće preimenovan prema Microsoft konvenciji imenovanja u:

"D<original drive letter of file><#>.<original extension>"

Ime fajla počinje sa D zatim slovo drajva sa kog je fajl obrisan, broj obrisanog fajl indeksiranog od nule i originalna ekstenzija. Prilikom brisanja fajla kompletna putanja i ime fajla čuva se u *skrivenom fajlu INFO2* koji se nalazi u RECYCLER direktorijumu (ukoliko je u pitanju NTFS) odnosno RECYCLED (ukoliko je u pitanju FAT32). Ovaj fajl sadrži informacije o svim fajlovima koji su trenutno u Recycle binu. Zahvaljujući Keith Jones-u dokumentovan je format INFO2, koji je izuzetno dragocen za forenzičku analizu. Sadrži podatke koji se odnose na svaki fajl iz Recycle bina, ime drajva, vremenski pečat o vremenu nastanka fajla u Recycle binu, veličinu fajla, ime i putanju fajla u ASCII i Unicode formatu.[459] Forenzički alati koji mogu pomoći u dobijanju svih pomenutih informacija iz INFO2 fajla su *Recbin.pl* alat čiji je autor Harlana Carvey, *Rifiuti.exe*[460] čiji je autor Keith Jones ili poboljšana alatka *Rifiuti2.exe.*[461] Ukoliko korisnički poddirektorijum u Recycler direktorijumu sadrži samo desktop.ini fajl i mali INFO2 fajl vreme poslednje modifikacije INFO2 fajla koje može da se dobije pomenutim alatima, jeste vreme kada je Recycle bin ispražnjen. Sa bezbednosnog aspekta administratori i forenzičari moraju biti oprezni sa fajlovima koji se nalaze u Recycler direktorijumu, koji se ne čuvaju pod korisničkim SID poddirektorijumom, kao i sa onim fajlovima koji se ne poklapaju sa pomenutom konvencijom imenovanja obrisanih fajlova.[462] Ovi fajlovi mogu ukazivati na zlonamerne programe (Autorun tipa) ili aktivnosti zlonamernog korisnika sa ciljem prikrivanja fajlova.[463] Forenzičari moraju biti upoznati sa određenim antivirusnim programima

458 How the Recycle Bin Stores Files, Microsoft, http://support.microsoft.com/kb/136517, 27.05.2016.

459 Kopecký K., *Stalking a kyberstalking nebezpečné pronásledování*, study Olomouc, 2010, http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd, 11.07.2016.

460 A Recycle Bin Forensic Analysis Tool., Rifiuti v1.0, Intel security, http://www. mcafee. com/ hk/downloads/free-tools/rifiuti.aspx, 27.05.2016.

461 Alatka Rifiuti2.exe ima podršku za Windows. Lokalizovan na različitim jezicima, strožiju proveru na greške i može prozvesti izlaz u XML format, http://code.google.com/p/rifiuti2/, 27.05.2016.

462 Hauck V. R., Atabakhsh H., Ongvasith P., Gupta H., Chen, H., *Using Coplink to analyze criminal-justice data*, IEEE Computer, Vol. 35 No. 3, 2002, str. 30–37.

463 Pogue C., Altheide C., Haverkos T., *UNIX and Linux Forensic Analysis DVD Toolkit*, Syngress publishing Inc., 2008.

(npr. Symantec Norton Antivirus[464] koji kreira fajl nprotect.log[465]) i mogu korisiti folder Recycler.

Kao što je već spomenuto implementirana arhitektura Recycle bin mehanizma promenjena je od verzije Windowsa XP. Promene omogućuju poboljšanja koja se odnose na dobijanje više korisnih informacija o obrisanim fajlovima kada je u pitanju forenzička analiza. Kod Windows Viste i Windows 7 obrisani fajlovi se i dalje vezuju za korisnički SID kao i kod Windows XP, ali je promenjena lokacija i sada se obrisani fajlovi nalaze u *c:\$Recycle.Bin direktorijumu*. Druga promena odnosi se na imenovanje obrisanog fajla. Nakon što se fajl obriše kreiraju se dva fajla. Prvi fajl tzv. *$R fajl*, predstavlja kopiju sadržaja obrisanog fajla koji će biti preimenovan u "$R" uz seriju od 6 random karaktera i pridruženu ekstenziju (na primer $R3rkd37.doc).[466] Drugi fajl tzv. *$I fajl* ($I3rkd37.doc) je fajl koji sadrži metadate podatke originalnog fajl (obrisanog fajl) sa informacijama sličnim kao kod INFO2 fajla kod Windows XP sistema. Ovaj $I fajl sadrži ime originalnog fajla, veličinu fajla, datum i vreme brisanja fajla.[467]

Dakle rezultat brisanja jednog fajla za posledicu ima kreiranje dva fajla u Recycle binu, što može predstavljati potencijalni problem. Timothy Leschke u svom radu ukazao je upravo na taj problem sa kojim se susreću forenzičari prilikom analize ovih fajlova u Windows Vista i Windows 7 okruženju, a to je generisana velika količina fajlova od strane sistema koje je potrebno analizirati.[468]

Na primer, sprovodi se forenzička analiza na Windows 7 OS u kome je zlonamerni korisnik obrisao 200 različitih fajlova. Od ovih 200 fajlova nastaje 400 fajlova ($R+$I). S obzirom da Windows 7 ima VSS (eng. VOLUME SHADOW COPY SERVICE, o kome je već bilo reči) tj. sistem za arhiviranje stanja sistema (eng. snapshot). Ovi fajlovi će se arhivirati svako veče (ukoliko je sistem konfigurisan da pravi snapshot svaki dan) i posle 30 dana broj fajlova će narasti sa 400 na 12000 fajlova (jer će kopija svakog fajla iz $Recycle.Bin

464 Http://www.symantec.com/index.jsp, 22.04.2016.

465 Ovaj log fajl moguće je pročitati sa alatkom Nprotect viewer kompanije StepaNet Communications Inc. koja je deo paketa DataLifter. StepaNet Communications Inc., http:// stepanet -communications-inc. software. informer.com/, 23.05.2016.

466 Hay B., Bishop M., Nance K., *Live Analysis: Progress and Challenges*, IEEE Security and Privacy, vol. 7, pp. 30-37., Mart 2009, http://nob.cs.ucdavis.edu/ bishop/papers/2009-ieeesp-2/ liveanal.pdf, 22.06.2016.

467 Hay B. Nance K., *Forensics Examination of Volatile System Data Using Virtual Introspection*, SIGOPS Operating Systems Review , Volume 42 Issue 3, ACM, 2008, str. 74–82.

468 Hay B., Bishop M., Nance K., *Live Analysis: Progress and Challenges*, IEEE Security and Privacy, vol. 7, pp. 30-37., Mart 2009. http://nob.cs.ucdavis.edu/ bishop/papers/2009-ieeesp-2/ liveanal.pdf, 22.06.2016.

foldera biti kreirana u svakom novom snapshot-u). Upravljanje tolikom količinom podataka je problem za forenzičara. Na koji način forenzičar na Windows 7 OS može prikupiti dragocene informacije za dalji tok istrage iz Recycle bina i generisanih fajlova od strane VSS mehanizma, biće ilustrovano sledećim primerom.

Pretpostavimo da se radi o malicioznom korisniku za koga se sumnja da je učesnik u distribuiranju fajlova zabranjenog pornografskog sadržaja ili određenih malicioznih alata. On je ove fajlove obrisao kako bi sakrio dokaze nedozvoljene aktivnosti i ti fajlovi su dospeli u Recycle bin. Pod pretpostavkom da je priključio svoj externi USB hard disk na OS radi manipulacije sa fajlovima, OS će instalirati nove drajvere za eksterni USB hard disk. To će biti okidač za VSS mehanizam da kreira snapshot. To znači da svi podaci Recycle bina takođe biti sačuvani u snapshotu. U ovom trenutku ukoliko maliciozni korisnik isprazni Recycle bin sa namerom da se trajno izbrišu kompromitujući falovi to se neće ostvariti. Kopija ovih kompromitujućih fajlova će biti sačuvana u snapshotu. S obzirom da je preostali dokaz arhiviran u snapshotu, sledeći korak forenzičara je realizovanje uspešnog pristupa ovom dokazu kako bi se on detaljno ispitao. O mogućem načinu pristupa snapshotu kroz VSS već je bilo reči.

Fajlove koji su izbrisani iz Recycle bina moguće je potpuno ili delimično oporaviti u *offline forezničkom postupku*. Nakon brisanja fajlova u modernim OS fajlovi nisu zaista obrisani. Umesto toga mesto gde se fajl nalazio fajl sistem obeležava kao raspoloživ za upisivanje drugih fajlova. Sve dok taj rapoloživi prostor nije prepisan (eng. overwriten) drugim fajlom, stari fajl moguće je isčitati specifičnim alatima. Oporavljenje ovakvih fajlova naziva se *karving* (eng. Data carving). Karving podataka podrazumeva tehniku prepoznavanja obrisanih fajlova ili delova fajlova na osnovu hedera podataka. Na primer, ukoliko je obrisan fajl veličine 200 MB i kasnije upisan novi 80 MB fajl u memorijski prostor (koristeći istu početnu memorisku adresu fajla od 200 mb) preostalih 120 MB će predstavljati slek prostor (o kome je već bilo reči) koji može da se identifikuje specijalnim alatima i oporavi deo fajla. Dakle prepisujući izbrisane fajlove drugim informacijama, izbrisani fajlovi će biti nečitljivi „za gotovo sve praktične potrebe".[469] *Defragmentacija* jeste jedan od primera gde se na brz i lak način mogu prepisati podaci. Forenzičar takođe treba da ima na umu da su mnogi sistemi konfigurisani da rade periodičnu defragmenticiju, ali da korisnik može i ručno nju pokrenuti sa ciljem

469 Lee H., Palmbach T., Miller M., *Henry Lee's Crime Scene Handbook*, San Diego: Academic Press, 2001.

prikrivanja dokaza. Forenzičkim ispitivanjem se može prepoznati ta razlika. Jednom prepisani podaci nekada nisu dovoljni za njihovo potpuno uništenje i sa specijalnom forenzičkim alatima moguće je njihovo oporavljanje ili oporavak bar jednog njihovog dela. Postupci sa kojima je moguće *kompletno brisanje fajlova*, a koje forenzičar mora da zna da bi ih prepoznao kao nameru prikrivanja i uništavanja dokaza su sledeći:

1. *Automatski wipe-ing* - U literaturi se navodi da je prepisivanje podataka 10 do 12 puta dovoljno da se onemogući oporavak podataka koristeći sve aktuelne tehnike i alate. Obično se postiže korišćenjem komercijalnih programa koji naizmenično popunjavaju raspoloživ prostor nulama i jedinicama ili upisom slučajnih (eng. random) podataka. Digitalni forenzičar može prepoznati da li je korišćena ova metoda za uništavanje dokaza;
2. *Ručni wipe-ing* (eng. File churning) - Podrazumeva brisanje određenih podataka, kopiranje velike količine „legitimnih" podataka (nekada do popunjavanja hard diska), brisanje tih podataka i postupak defragmentacije, ponovljenih nekoliko puta. Ovaj postupak je teže uočljiv forenzičarima;
3. *Fizičko uništavanje medija* - jedini način definitivnog uništenja podataka jeste fizičko uništenje medija na kom se podatak nalazi.

3.1.20. Postojani podaci od značaja na Windows-u - print spooler fajlovi

Glavna komponenta u Windows okruženju za štampanje je *print spooler* (eng. Simultaneous peripheral operations online). On u privremenom fajlu čuva stranu koju je određena aplikacija poslala na štampanje. Aplikacija i štampač mogu simultano upisivati i isčitavati fajlove u print spooleru.[470] Na primer, kada se fajl šalje štampaču, lokalni printer provajder (localspl.dll) upisuje sadržaj u spool fajl (.spl) i kreira poseban grafički fajl (.emf) za svaku stranu. Za forenzičko ispitivanje je važno ono što *localspl.dll* prati, a to su informacije o korisničkom imenu, imenu fajla (i drugi detalji vezani za dokument koji se šalje na štampu) i smešta ih u *shadow fajl* (.shd). Po difoltu fajlovi .spl i .shd se upisuju u spool folder. U zavisnosti od konfiguracije štampača ovi fajlovi se mogu smeštati u Windows virtualnu memoriju na hard disku ili u keš memoriju operativnog sistema.

470 Aaron P., Cowen D., Davis. C., *Hacking Exposed Computer Forensics*, Second Edition, The Mcgraw-Hill Companies, 2010.

"C:\Windows\System32\spool\PRINTERS"

U zavisnosti od konfiguracije štampanja, a sa obzirom da se ovi fajlovi .spl, .shd i .emf fajlovi brišu nakon što se završi štampanje, forenzičaru će biti potrebno izvlačenje ovih fajlova iz nealociranog prostora. Programa koji to uspešno radi je *AccessData FTK* u post-mortem forenzičkoj analizi.[471] Forenzičar može pronaći ove fajlove ukoliko je postojalo neuspelo štampanje ili je štampanje bilo prekinuto isključivanjem/restartom računara.

Savremeni štampači pogotovu multifunkcionalni uređaji sadrže hard diskove na kojima se čuvaju zapisi o tome ko je štampao, šta je štampano, a neki od njih čuvaju u radnoj memoriji i informacije o poslednjim odštampanim stranicama. Ti podaci se mogu izvući sa specijalnim forenzičkim alatima za takvu namenu, ali takvi podaci nisu kompletni i nemaju se sa čime uporediti. U tom slučaju neophodno je uraditi rekonstrukciju celog fajla da bi dokaz bio prihvatljiv za sud.

3.1.21. Postojani podaci od značaja na Windows-u - fajlovi linkova i najčešće korišćeni fajlovi

Windows fajlovi linkovi (eng. shortcut file) ili prečice za digitalnog forenzičara mogu biti korisni jer mogu sadržati bitne informacije za dalji tok istrage. Ovi fajlovi predstavljaju linkove do određenih fajlova, programa i sistemskih objekata izvan fajl sistema (npr. mrežni uređaji, štampači, skeneri, eksterni diskovi, kamere i druge periferni uređaji). Linkovi čuvaju poslednje vreme pristupa ili izmene ciljnog fajla odnosno datoteke, što može biti od izuzetne koristi kada je ciljni fajl obrisan. To znači da iako datoteka ne može biti oporavljena, link fajl može da pruži informaciju o tome kada je datoteka poslednji put bila prisutna na sistemu. Ovi fajlovi imaju ekstenziju *.lnk* i zbog toga se deklarišu kao LNK fajlovi. U praksi najčešće se nalaze na desktopu OS, u Windows rescent folderu, u Windows start meniju, u omiljenim lokacijama (eng. favourites) internet pretraživača.

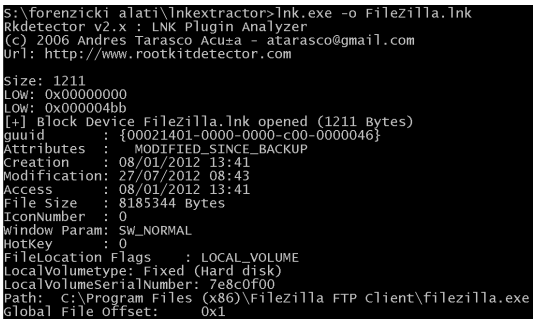
Takođe jedna od značajnih lokacija koja sadrži link fajlove do mrežnih resursa jeste:

"C:\Users\(User Name)\AppData\Roaming\Microsoft\Windows\Recent Items\Network Shortcuts"

Ova lokacija može pokazati forenzičaru kojim fajl serverima je osumnjičeni pristupao i vreme kreiranog linka.

471 Forensic Toolkit (FTK), AccessData Community, http://www.accessdata.com/products/digital-forensics/ftk, 17.05.2016.

Detaljnijim ispitivanjem fajlova linkova forenzičar može steći sliku o tome kako je računarski sistem personalizovan (na koji način korisnik pristupa programima, folderima i fajlovima). LNK fajlovi mogu biti kreirani na različite načine: od strane samog korisnika, prilikom instalacije OS ili u toku instalacije ili izvršenja programa. Jesse Hager je obradio strukturu LNK fajlova i njegov rad se može naći na sajtu Google code.[472] LNK fajlovi sadrže vremenske pečate i sadrže punu putanju fajla do fajla na koga se link odnosi. Ove informacije nisu toliko očigledne pa se zahteva od forenzičara dodatno dekodiranje, na osnovu relevantnog offseta bajta (koji ukazuje da se radi o lnk fajlu). Alatka koja može forenzičaru pomoći u analizi lnk fajla je *JAFAT perl skripta* (koja radi pod Linuxom).[473] Druga alatka koja takođe analizira lnk fajl jeste *linkextractor*[474] koja radi u komandnom okruženju i izlaz fajla dat je na slici:



Slika 65. Prikaz izlaza alata koji analizira LNK fajl

U forenzičkom ispitivanju uvek je korisno pretražiti ove fajlove kako u alociranom tako i u nealociranom prostoru diska i page fajlu. Razlog je taj što se ispitivanjem ovih lnk fajlova može obezbediti povezivanje fajla sa logičkim diskom na kojem je fajl smešten, a zatim na logički disk gde je smešten sam OS. To može indicirati na moguće korišćenje eksternog diska.

Treba naglasiti da *Windows rescent folder* može sadržati dragocene informacije za digitalnog forenzičara, jer se u njemu nalaze prečice do svih fajlova koji su najčešće bili korišćeni. U Windows 7 OS pristup Windows rescent folderu je preko:

---

472 Http:// code.google.com /p/ 8bits/ downloads/ detail? name= The_ Windows_ Shortcut_ File_ Format.pdf&can=2&q=, 18.05.2016.

473 Jake's Archive of Forensic Tools, http://sourceforge.net/projects/jafat/files/lnk-parse/lnk-parse-1.0/, 18.05.2016.

474 Andres and Miguel Tarasco, Lnk Analyzer, Tarasco.org, http:// www. tarasco. org /security/ Lnk_Analyzer/index.html, 18.05.2016.

"C:\Users\(User Name)\AppData\Roaming\Microsoft\Windows\Recent Items"

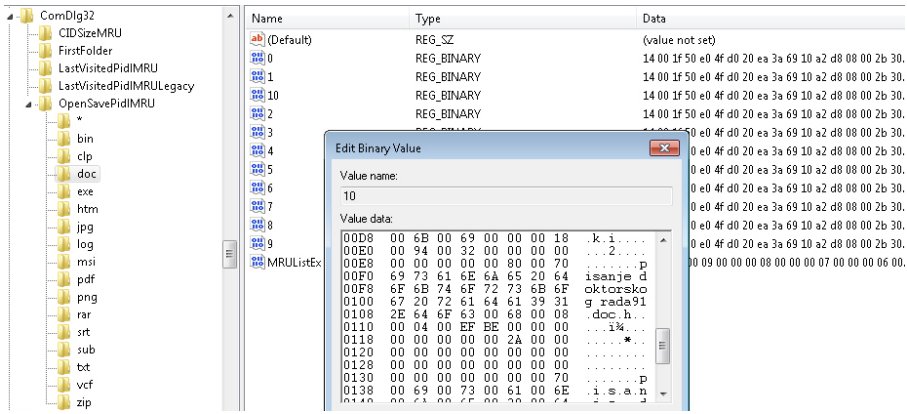
Najčešće korišćene komande u "RUN" baru može se pronaći u Windows registru na sledećem mestu:

"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU"

Ovde se mogu naći korisne informacije o tome koje je komande osumnjičeni koristio putem "RUN-a" (hronološki prikazanih u „DATA" koloni „MRUList" vrednosti). Na novijim OS korisnici sve više koriste bar "Search and programs" koji se ovde ne registruju. Ukoliko forenzičar želi da sazna, koji su se to fajlovi otvarali i snimali pri pokretanju prozora (eng. open/save dialog) to može videti u registarskoj bazi pod sledećim ključem:

"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU"

Treba napomenuti da su vrednosti koje sadrže podključevi u HEX zapisu, ali se mogu videti u ASCII prikazu, što se može primetiti na sledećoj slici:



Slika 66. Prikaz otvaranih fajlova u Windows 7 iz registarske baze

Moguće je kroz registarsku bazu videti i poslednje otvarane foldere na sistemu:

"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU"

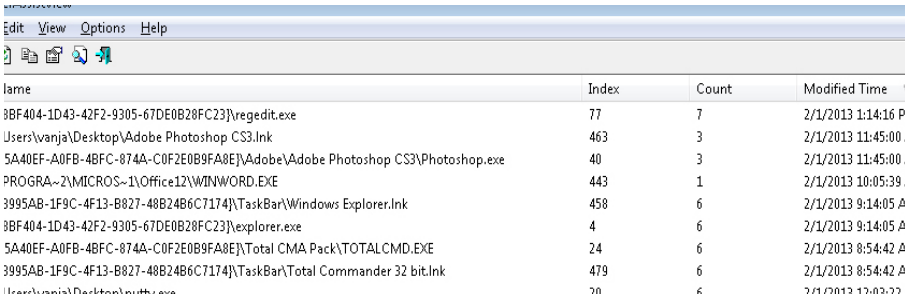
U registarskoj bazi moguće je videti i poslednje otvarane dokumente (kao na primer .bin, .clp, .csv, .doc, .docx, .dotm, .htm, .jpg, .log, .pdf, .png, .rar, .srt, .sub, .txt, .vcf, .xls, .zip). Lokacija koju forenzičar treba da ispita jeste:

"HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion\Explorer\RecentDocs"

Interesantno mesto u registarskoj bazi takođe predstavlja i:

"HKEY_CURRENT_USER\ Software\ Classes\Local Settings\ Software\ Microsoft\ Windows\ Shell\MuiCache" koje sadrži listu otvaranih izvršnih fajlova na sistemu. Ovi podaci mogu biti dragoceni, kako administratoru sistema da ispita bezbednost samih izvršnih fajlova, tako i forenzičaru koji dobija novi izvor podataka u rekonstruisanju zlonamernih aktivnosti. Ukoliko forenzičar želi da sazna detalje o izvršnim fajlovima (.exe) i linkovima koji su se često otvarali na OS to je moguće uraditi altatkom *UserAssistentView*[475] koja vrši dešifrovanje zapisa koji se nalaze u registru bazi pod ključem:

"HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion\Explorer\UserAssist key". Informacije prikupljene ovom alatkom prikazane su na sledećoj slici:



Slika 67. Prikaz informacije dobijene iz registra baze a koje se odnose na ključ UserAssist

Pretraživanje *User Assist ključeva* je korisno u slučaju da na ispitivanom sistemu postoji više korisničkih naloga, s obzirom da prefetch fajl ne može da identifikuje koji je korisnik startovao određenu aplikaciju. Sa UserAssist ključem digitalni forenzičar može doći do informacija, koje ukazuju na određene tipove fajlova i programa kojima je pristupano. Iako ovi podaci nisu konačni (ne mogu se povezati sa tačno određenim datumom

475 UserAssistView v1.02, Nir Sofer, http://www.nirsoft.net/utils/userassist_view.html, 16.05.2016.

i vremenom), ipak mogu ukazati na specifične korisničke aktivnosti. User Assist podključevi su šifrovani ROT-13 algoritmom koja je izuzetno slab prema današnjim standardima.[476] U nastavku sledi tabela koja prikazuje listu istorije sa podključevima u registarskoj bazi.[477]

Tabela 7. Lista istorije sa podključevima u registarskoj bazi

Lista istorije prema tipu	Podključ koji ukazuje na listu istorije
URL-ovi iz Microsoft Internet Explorera	*HKEY_USERS\S-1-5-21-[User Identifier] \Software\Microsoft\ Internet Explorer\TypedURLs*
Datoteke Microsoft Word-a	*HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft\Office\12.0\Word\File MRU*
Datoteke Microsoft Excell-a	*HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft \Office \12.0\Excel\File MRU*
Datoteke Microsoft Power Point-a	*HKEY_USERS\S-1-5-21-[User Identifier] \Software\Microsoft \ Office\12.0\PowerPoint\File MRU*
Datoteke Acrobat Reader-a	*HKEY_USERS\S-1-5-21-[User Identifier] \Software\Adobe\ Acrobat Reader\9.0\AVGeneral\cRecentFiles*
WinRAR datoteke	*HKEY_USERS\S-1-5-21-[User Identifier] \Software \WinRAR \ArcHistory*
Datoteke .GIF	*HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.gif*
Datoteke .JPG	*HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpg*
Datoteke .TXT	*KEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt*
Datoteke .ZIP	*HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft \Windows\CurrentVersion\Explorer\RecentDocs\.zip*
Folderi	*HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\ Folder*
Najskorije korišćena mapirana mreža	*HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft \Windows\CurrentVersion\Explorer\Map Network Drive MRU*
Najskorije korišćen Wallpaper	*HKEY_USERS\S-1-5-21-[User Identifer] \Software \Microsoft \Windows\CurrentVersion\Explorer\Wallpaper\MRU*
Najskorije upotrebljena komanda u RUN dijalogu	*HKEY_USERS\S-1-5-21-[User Identifier] \Software \Microsoft \Windows \CurrentVersion\Explorer\RunMRU*

476 Kunz M., Wilson P., *Computer Crime and Computer Fraud - Report to the Montgomery County Criminal Justice Coordinating Commission*, University of Maryland Department of Criminology and Criminal Justice, USA, 2004.

477 Kruse II G. W., Heiser G. J., *Computer Forensics Incidend response essentials*, 14th printing, New York: Addison Wesley, March 2010.

3.1.22. Postojani podaci od značaja na Windows-u - fajlovi internet aktivnosti

Veoma važan korak u digitalnoj forenzici računarskih sisema jeste ispitivanje internet aktivnosti osumnjičenog vezanih za incidentnu odnosno nedozvoljenu aktivnost. Ove informacije mogu biti dragocene za forenzičko ispitivanje kršenja politike kompanije, korporativne špijunaže, krađa intelektualnog vlasništva i drugih krivičnih dela.

Ovi podaci forenzičaru mogu da pruže značajne informacije, kada je u pitanju istraživanje tragova pristupa internetu na ispitivnom računaru. Praksa je pokazala kada je reč o visokotehnološkom kriminalu da se uglavnom koristi neki od internet aspekta. Upravo zato digitalni forenzičar mora razumeti funkcionosanje interneta i poznavati sva značajna mesta u OS, u kojima se mogu pronaći incidentne/nedozvoljene aktivnosti.

Windows OS isporučuje svoj OS sa svojim internet pretraživačem Internet explorerom (IE).

IE ima svoje dve oblasti značajne za forenzičare gde skladišti svoje podatke. Prva oblast je *index.dat fajl* odnosno baza koju koristi IE pretraživač i keš IE-a. Index.dat fajlovi su struktuirani u *MS IE cache File* (MSIECF) formatu. Ovaj fajl sadrži zapise posećenih URL lokacija, uključujući upite, pristupe web mail servisima i druge bitne podatke za digitalnu istragu. Relevantni tipovi iz strukture index.dat fajla koje će forenzičar identifikovati prilikom rekonstrucije internet aktivnosti su sledeći:

- *Tip REDR* - ovaj tip zapisa o aktivnostima na internetu ukazuje da se radi o redirekciji odnosno da je korisnički internet pretraživač preusmeren na drugu internet lokaciju;
- *Tip URL* - ovaj tip zapisa o aktivnostima na internetu predstavlja skup podataka koji predstavljaju URL adresu ili web sajt koju je korisnik posetio;
- *Tip LEAK* - ovaj tip zapisa o aktivnostima na internetu ukazuje na sajt koji je korisnik posetio.

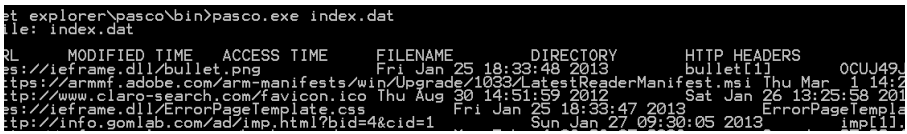
Na Windows XP i Windows 2003 sistemima lokacija koja je od forenzičkog značaja gde se nalazi index.dat fajl jeste:

"c:\Documents and Settings\Ime_Korisnika\Local Settings\Temorary Internet Files\Content.IE5"

Na Windows Visti i Windows 7 ta lokacija je:

"c:\Users\Ime_Korisnika\AppData\Local\Microsoft\Windows\Temorary Internet Files\Content.IE5"

Forenzičaru mogu biti od koristi različiti alati kada je reč o prikupljanju informacija iz index.dat fajla, a najpoznatiji alat za tu namenu je *pasco.exe*[478] autora Keith J. Jones-a, koji može da radi i na obe platforme (Windows i Linux).[479] Izlaz iz ove komande prikazan je na sledećoj slici:



Slika 68. Izlaz Pasco komande

Dobra alatka za prikupljanje podataka iz index.dat fajla je i *libmsiecf*, čiji je autor Joachim Metz. Sastoji se iz dva programa, msiecfinfo i msiecfexport. Msiecinfo prikazuje osnovne podatke iz MSIECF fajla, dok msiecfexport prikazuje detaljnije podatke ovog fajla. Mana je što je alatka dostupna samo za Linux sisteme.

Dragocene podatke forenzičar može dobiti iz privremenih internet fajlova odnosno *keš fajlova* (eng. Internet cache), koji ostaju na računarskom sistemu nakon pristupa korisnika web lokacijama na internetu. Pre nego što se korisniku prikaže stranica kojoj želi da pristupi, računar prethodno preuzima fajlove koji čine tu web stranicu i smešta ih u internet keš na disku, da bi nakon toga bila prikazana na ekranu korisnika. Ukoliko se kontaktira ponovo isti sajt pristupa se keš fajlu (neki internet pretraživači vode evidenciju koliko je puta posećen određeni sajt - kod IE se ti podaci nalaze u fajlu index.dat; u Netscape-u se nalazi u Netscape.hst; kod Mozilla se ti podaci nalazi u _ CACHE_001_). Internet keš predstavlja oblast na hard disku (serija foldera) što znači da sistem sve te upise registruje. Internet keš je osmišljen sa namerom da ubrza vreme prikaza web stranice na ekranu, a sa druge strane obezbeđuje forenzičaru dodatan izvor informacija i dokaza. Naravno korisnik može odrediti veličinu internet keša na 0MB. To znači da se informacije o posetama na internetu ne keširaju. Mogu se i obrisati fajlovi, koji ulaze u sastav keša. To može biti signal forenzičaru da je namera zlonamernog korisnika na sistemu bila prikrivanje nedozvoljenih aktivnosti.

Na Windows XP sistemima ovi fajlovi su na lokaciji:

"c:\Documents and Settings\Ime_Korisnika\Local Settings\Temorary Internet Files\Content.IE5"

478 Pasco v1.0, Intel security, http://www.mcafee.com/hk/downloads/free-tools/pasco.aspx, 15.05.2016.

479 Korać V., *Digital archaeology in a virtual environment*, Arheologija i prirodne nauke, br. 8, Beograd 2013, str. 129-141.

Na Windows Visti i Windows 7 ta lokacija je:

"c:\Users\Ime_Korisnika\AppData\Local\Microsoft\Windows\Temorary Internet Files\Content.IE5"

Za forenzičara je važno da zna da se ovi keš fajlovi smeštaju u jedan od 4 proizvoljno kreirana poddirektorijuma. Informacije koje sadrže ovi foderi su keširani fajlovi kojima mogu da se potvrde aktivnisti na internetu (npr. URL adrese i putanje do određenog fajla) uz korelaciju sa podacima dobijenim iz index.dat fajla.

Dodatne informacije od značaja za istragu se mogu takođe dobiti iz *Omiljenih lokacija* internet pretraživača (eng. Favourites). Ove omiljene lokacije pretstavljaju obeležene lokacije od značaja (eng. Bookmarks) i mogu biti pokazatelj kretanja korisnika na internetu.

Omiljene lokacije ne Windows XP nalaze se na:

"c:\Documents and Settings\Ime_Korisnika\Favorites"

Na Windows Visti i Windows 7 ta lokacija je:

"c:\Users\Ime_Korisnika\Favorites

Omiljene lokacije se pojavljuju nakon kreiranja korisničkog profila i njegovog logovanja na sistem. Ove lokacije predstavljaju skup URL prečica (eng. shortcut). Sadržaj URL prečice se može lako videti text editorom ili izlazom komande "type" na konzoli Windows sistema ili comande "cat" na Linux sistemima. Pored sadržaja URL forenzičar može naći vrednosti kao što su kada je fajl kreiran, modifikovan i kada mu je poslednji put bilo pristupano. To indicira koje je lokacije osumnjičeni posećivao kao i njihovo vreme. Ove informacije mogu biti dragocene prilikom forenzičke istrage. Ulaze u „Omiljene lokacije" unosi i sam sistem, a ne samo korisnik, što se mora uzeti u obzir. Zato je najvažnija informacija zapravo URL adresa lokacije, na koju se prečica iz Omiljenih lokacija odnosi. Dodatan kontekst istrazi mogu pružiti informacije iz *unetih URL adresa* iz trake za pretraživanja (eng. Navigation toolbar). To je lista onih URL ulaza koje je korisnik napravio u prozoru pretraživača. Ta lista se čuva u registarskoj bazi u ključevima i lako je identifikovati.

Lokacije koje forenzičar treba da ispita u registri bazi su:

"*HKCU\Software\Microsoft\InternetExplorer\TypedURLs*"

"HKCU\Software\Microsoft\InternetExplorer\Download"

Upotreba registarskog ključa *TypedURLs* zavisi od verzije Windows OS i IE. Kod IE 6 u ključu će biti upisana vrednost samo ukoliko je IE ugašen na pravilan način (ukoliko je IE proces iexplore.exe "ubijen" iz Taks menadžera neće biti upisa u ključ). Kod IE 8 vrednost će se upisati u ključ u realnom

vremenu nezavisno od toga na koji je način IE ugašen. Kod Windowsa XP sa SP2 i SP3 i Windows Viste podaci o unetim URL adresama se upisuju u ključ TypedURL, dok se kod Windows 7 ovi podaci ne upisuju.[480]

Predhodno razmatranje odnosilo se na internet pretraživač IE, koji dolazi zajedno sa instaliranim Windows OS. Drugi pretraživači (Firefox, Opera, Chrome, Safari, Netscape) koji nisu pretdmet ove knjige, iako i oni funkcionišu na vrlo sličan način ili poseduju sopstveni sistem skladištenja internet fajlova.

Dodatan kontekst istrazi mogu pružiti i fajlovi koji se nazivaju *kolačići* (eng. Cookies). Za digitalnog forenzičara oni predstavljaju izvor dodatnih informacija o internet aktivnostima korisnika. Njihova karakteristika je da korisnik nema punu kontrolu nad njima. To su mali tekst fajlovi koji se skladište na hard disku i dolaze kao posledica internet aktivnosti kroz posete web lokacijama. Njih je moguće otvoriti sa tekst editorom direktno, ali su određena polja šifrovana. Šifrovana polja polja 5 i 6 odnose se na vremenski rok kolačića, a polja 7 i 8 predstavljaju vreme kreiranja kolačića.

U Windows XP sistemima lokacija kolačića je:

"c:\Documents and Settings\Ime_Korisnika\Cookies"

Na Windows Visti i Windows 7 ta lokacija je:

"c:\Users\Ime_Korisnika\AppData\Roaming\Microsoft\Windows\Cookies"

Da bi se uspešno prikazala sva polja neophodno je korišćenje alata. Alat *Galleta*,[481] čiji je autor takođe Keith J. Jones (autor Pasco alata), daje odličan prikaz i izlaz ovog alata učitan u Microsof Excel fajl dat je na sledećoj slici:

VARIABLE	VALUE	CREATION TIME	EXPIRE TIME
ivc	1	Thu Jan 31 14:08:12 2013	Fri Feb 1 14
__utma	132044255.554491166.1359641293.1359641293.1359641293.1	Thu Jan 31 14:08:13 2013	Sat Jan 31 14
__utmb	132044255.2.10.1359641293	Thu Jan 31 14:08:13 2013	Thu Jan 31 1

Slika 69. Prikaz izlaza alata Galleta nakon analize kolačića na Windows 7 OS

Istorija aktivnosti na internetu (eng. Internet History), omogućuje evidentiranje lokacija koje je korisnik posetio sa svog OS u toku pretraživanja interneta. Ispitivanjem internet istorije moguće je obezbediti ključne dokaze u rešavanju slučaja. Istrage koje se odnose na nazakonito korišćenje

480 Kipper G., *Wireless crime and forensic investigation*, Auerbach Publications Taylor & Francis Group, 2007.

481 Galleta v1.0, *Intel security*, http://www.mcafee.com/us/downloads/free-tools/galleta.aspx, 19. 05. 2016.

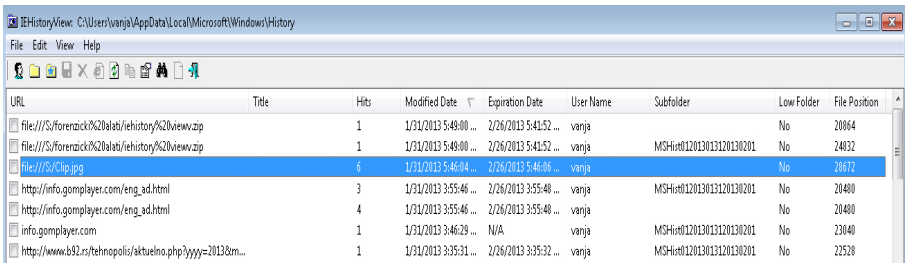
ili nepropisno korišćenje interneta, zahtevaju stručnu analizu informacija sačuvanih od strane internet pretraživača. Te informacije su rezultat internet aktivnosti osumnjičenog. Na primer, istorija aktivnosti može uključivati imena posećenih internet lokacija, FTP sajtova, novinskih grupa (eng. news group). Na osnovu istorije aktivnosti i prethodno opisanih bitnih web elemenata za ispitivanje, forenzičar može rekonstruisati aktivnosti osumnjičenog sa sledećih lokacija:

"c:\Documents and Settings\Ime_Korisnika\Local Settings\History" - odnosi se na Windows XP a na Windows Visti i Windows 7 ta lokacija je:

"*C:\Users\ Ime_Korisnika \AppData\Local\Microsoft\Windows\History* "

Sistem ovde pravi podelu istorije aktivnosti na dnevne i nedeljne. Moguće je pronaći kako one aktivnosti koje se odnose na internet aktivnosti tako i one koje se odnose na pristup fajlovima samog računara (pristup lokalnim fajlovima na hard disku). Internet istorija ima opciju za korisnička podešavanja i difoltno vreme vođenja istorije je 20 dana. Onemogućavanje vođenja istorije forenzičaru može biti signal o prikrivanju potencijalnih dokaznih informacija.

Besplatna alataka I*EHistoryView* čita sve podatke iz istorije datoteka na računaru i prikazuje listu svih URL adresa koje su posećene u poslednjih nekoliko dana u jako preglednom formatu. [482] Na sledećoj slici dat je izlaz alatke IEHistoryView.

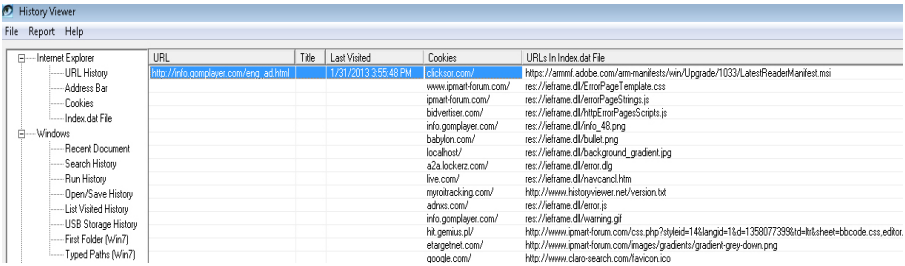


Slika 70. Prikaz izlaza alatke IEHistoryView sa detaljima istorije internet aktivnosti

Druga alatka sa kojom je moguće dobiti informacije vezane ze istoriju internet aktivnosti, ali podržava i druge internet pretraživače i daje dodatne korisne istorijske informacije na ispitivanom sistemu jeste alatka *History*

482 IEHistoryView v1.70 - View Visited Web Sites of Internet Explorer, Nir Sofer, http://www.nirsoft.net/utils/iehv.html, 20.05.2016.

Viewer.[483] Njen izlaz dat je na sledećoj slici:



Slika 71. Prikaz izaz alatke History Viewer

Treba istaći da se postojani podaci na sistemu osim "uživo" mogu prikupiti i analizirati u post-mortem forenzici. Na osnovu iznetih informacija o postojanim podacima može se zaključiti da su za pronalaženje potencijalnih forenzički tragova najznačajnija sledeća mesta na Windows sistemu:

- keš pretraživača;
- metadata fajlovi (eksterni, interni i link fajlovi);
- log fajlovi (logovi događaja programa, bezbednosni logovi i sistemski logovi, logovi programa za komunikaciju);
- obrisani fajlovi;
- Windows registarska baza (informacije o vremenskoj zoni, MRU lista, UserAssist, bežične mreže, USB uređaji, IE, windows šifre, IM programi).

Prilikom forenzičke analize http saobraćaja moguće je identifikovati verziju operativnog sistema (kao i tip OS 32bit ili 64bit), ime i verziju internet pretraživača (Firefox, IE) kroz parametar AGENT http request hedera. Te informacije se mogu dobiti uz pomoć alata Wireshark i na taj način identifikovati zlonamernog napadača.

483 History Viewer, http://www.historyviewer.net/download.htm, 20.05.2016.

3.1.23. Postojani podaci od značaja na Windows-u - fajlovi aktivnosti elektronske pošte

Nedozvoljene aktivnosti mogu biti izvršene slanjem email poruka i mogu biti potpomognute elektronskom poštom. Kada su nedozvoljene aktivnosti izvršene slanjem email poruka to podrazumeva fišing napade, email bombardovanja, slanje spama (distribuiranje nezatraženih email poruka putem elektronske pošte ili preko news grupa[484]). Kada se govori o nedozvoljenoj aktivnosti koja je potpomognuta elektronskom poštom misli se na krađu identiteta, ucene i različite oblike uznemiravanja.

Da bi forenzička istraga bila uspešna forenzičar mora da razume način funkcionisanja elektronske pošte. Elektronska poruka se kreira sa određenim email klijentom (npr. Gmail, Outlook, Yahoo). Email klijent šalje kreiranu elektronsku poruku do MTA (eng. Mail transfer agent) odnosno do email servera na kome je pokrenut servis SMTP (eng. Simple mail transfer protocol). MTA pronalazi odgovarajući mail server za primaoca elektronske poruke i prenosi je. Kroz svaki MTA koji elektronska poruka prođe pridoda joj se vremenski pečat. Upravo ovi vremenski pečati su od izuzetne važnosti u forenzičkoj istrazi.

Primer: „*Apr 21 06:16:27 turing sendmail[29573]: r3L4GOmb029573: from=<yqxadathqk@assupport.eu>, size=1059, class=0, nrcpts=1, msgid=<001 001ce3e46$e4b39410$94bb4ebd@systemro7vpq>, proto=SMTP, daemon=MTA, relay=triband-del-59.177.175.107.bol.net.in [59.177.175.107]* "

U poslednjem koraku primalac kontaktira svoj email server koristeći određeni protokol za pristup elektronskoj pošti na serveru (npr. POP3, IMAP) i preuzima elektronske poruke svojim email klijentom. Važni forenzički parametri elektronske pošte nalaze se u email hederu (zaglavlju poruke) i na osnovu njih moguće je identifikovanje primaoca, pošiljaoca i servere (SMTP provajdere):

Received: from - na strani provajdera sa kog se šalje email sadržaće ID poruke, IP adresu sa koje je poslat email i ime samog provajdera:

Message-ID: <20090225142225.22087.mail@**email.provider1.com**>

Received: from [**22.22.222.222**] by **email.provider1.com** via HTTP; Wen, 25 Feb 2009 14:22:25 PST

Na strani provajdera pošiljaoca prilikom transfera poruke provajderu primaoca sadržaće adresu primaoca, adresa provajdera koji prima poštu,

484 Korać V., *Spam*, Arheologija i prirodne nauke, br.1/2006, Beograd, str. 137-150.

vreme, povratnu putanju pošiljaoca, adresa provajdera sa kog se šalje elektronska poruka:

Delivered-To: primalac@gmail.com

Received: by 216.58.214.101 with SMTP id e3cs235nzb; Wen, 25 Feb 2009 14:22:27 PST -0800 (PST)

Return-Path: pošiljaoc@**email.provider1.com**

Received: from **email.provider1.com** (**email.provider1.com** [111.111.11.111]) by mx.gmail.com with SMTP id h18si826631rnb; Wen, 25 Feb 2009 14:22:27 -0800 (PST)

X-mailer : Aplikacija koja je korišćena za kreiranje elektronske pošte;

Sender – email upotrebljena adresa, gde se uz polja from i replay-to polja može videti da li je neko menjao podatke;

Na osnovu forenzičke analize aktivnosti elektronske pošte forenzičar treba da dobije odgovore na pitanja: ko je poslao email, kada je email poslat i odakle je poslat. Email dokazi se obavezno pregledaju na računaru koji nije povezan sa internetom, odnosno namenjen za offline ispitivanje. Razlog je taj što ukoliko je podešena potvrda o pročitanom emailu, nakon pregledanja emaila poslaće se pošiljaocu informacija da je email pročitan, što može ugroziti istragu (u slučaju da je računar na kome se vrši ispitivanje povezan sa internetom).

Na osnovu podataka koji se dobijaju forenzičkim ispitivanjem fajlova elektronske pošte moguće je locirati računar sa kog je maliciozni korisinik izvršio incidentnu odnosno nedozvoljenu aktivnost. Zaglavlje elektronske pošte (eng. email header) može sadržati veoma važne informacije kao što su jedinstveni identifikacioni brojevi, IP-adrese servera sa kog je slana elektronska pošta kao i vreme slanja. Pregledanje zaglavlja elektronske pošte može biti izvedeno iz grafičkih email klijenta ili klijenata komandnog okruženja i iz webmail klijenata. Istraživanje elektronskih poruka se bazira na pristupu ispitivanom (kompromitovanom) računaru uz prikupljanje dokaza. Upotrebom email klijenta sa ispitivanog računara mogu se pronaći i iskopirati dokazi iz elektronske poruke. Mogu se pronaći zaštićeni i šifrovani dokumenti. Sve emailove koji sadrže potencijalne dokaze neophodno je odštampati.

Način prikupljanja zaglavlja iz grafičkih email klijenata:

- *Microsoft Outlook* – Potrebno je otvoriti ispitivanu poruku, odabrati opciju "Message Options", selektovati sve i iskopirati heder u određeni tekstualni editor;
- *MS-Outlook Express* - Otvoriti ispitivanu poruku, odabrati opciju "message properties ", odabrati "Message Soruce", iskopirati heder u

određeni tekstualni editor;

- *Web orijentisani servisi* za poštu (eng. Webmail) tipa Yahoo, snimaju IP-adrese sistema (u zaglavlje poruke) sa kojih je sastavljana elektronska pošta. [485] U daljem tekstu daje se prikaz načina prikupljanja email zaglavlja (eng. header) u forenzičkoj praksi iz najkorišćenijih webmail klijenata:
    - *prikaz i kopiranje email hedera u Gmail-u*[486] - potrebno je ulogovati se u Gmail, otvoriti ispitivanu poruku, odabrati opciju "MORE", zatim odabrati opciju "SHOW ORIGINAL", selektovati ceo heder, kopirati i snimiti sve u određeni fajl;
    - *prikaz i kopiranje email zaglavlje u AOL-u*[487] u praksi - potrebno je ulogovati se u AOL, otvoriti ispitivanu poruku odabrati link "DETAILS", selektovati ceo heder, kopirati i snimiti sve u određeni fajl;
    - *prikaz i kopiranje email hedera u Yahoo mail-u*[488] - potrebno je ulogovati se u Yahoo mail, otvoriti ispitivanu poruku, odabrati "FULL HEADER", selektovati ceo heder, kopirati i snimiti sve u određeni fajl;
    - *prikaz i kopiranje email hedera u Hotmail-u*[489] - potrebno je ulogovati se u Hotmail, kliknuti desnim klikom na ispitivanu poruku, odabrati "VIEW MESSAGE SOURCE", selektovati ceo heder, kopirati i snimiti sve u određeni fajl.

Kada je reč o telu poruke (eng. Message Body) ono sadrži isključivo podatke koje je pisao pošiljalac (u smislu nema dodatih podataka od strane servera kao kod zaglavlja poruke). Iako je telo poruke u tekstualnom obliku, email klijenti ili serveri njih mogu sačuvati u binarnom formatu. Zato je jako važno da se koriste specijalizovani alati za forenzičku analizu elektronske pošte koji mogu da procesiraju različite formate fajlova i baza u kojima se smeštaju elektronske poruke. Treba napomenuti da korisnici kroz telo poruke mogu biti prevareni na osnovu lažnog linkovanja veb adrese na neku zlonamernu veb stranu. Napredni fišing napadi kreiraju dodatno lažne title tagove (daje opis linka kada korisnik pređe mišem preko njega) tako da prikazana adresa linka izgleda kao da je originalna.

U nastavku će biti prikazane određene karakteristike najkorišćenijih

485 Http://www.yahoo.com, 29.05.2016.
486 Http://www.gmail.com, 29.05.2016.
487 Http://www.aol.com/, 30.05.2016.
488 Http://www.yahoo.com/, 30.05.2016.
489 Http://www.hotmail.com/, 30.05.2016.

emal klijenata (Microsoft Outlook, Microsoft Outlook Express, Windows mail, Mozilla thunderbird i webmail) koji su od važnosti za forenzičku istragu.

1. Microsoft Outlook – ovaj klijent smešta elektronsku poštu u fajl sa .PST ekstenzijom. Arhiva elektronske pošte se nalazi na sledećim lokacijama:

Kod Windows XP i ranijih OS u folderu

<korisničko_ime>\LocalSettings\Application Data\Microsoft\Outlook

Kod Windows Vista i kasnijih OS

<korisničko_ime>\AppData\Local\Microsoft\Outlook

Registarski ključevi koji ukazuju koje su arhive korišćene smešteni su u:

„HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windo

ws Messaging Subsystem\Profiles\Outlook“

Veličina arhive može biti do 20 GB.

2. Microsoft Outlook Express - ovaj klijent smešta elektronsku poštu u fajl sa .DBX ekstenzijom (folder.dbx je indeksni fajl)

Pre Windows Viste ovaj klijent dolazio je instaliran sa OS.

Arhiva elektronske pošte se nalazi na sledećim lokacijama:

<korisničko_ime>\Local Settings\Application Data \Identities\ <GUID>\ Microsoft

Outlook Express

Forenzički značajan je *fajl cleanup.log* koji govori o vremenu poslednjeg pakovanja. Obrisane poruke su označene sa „deleted“. Moguće je pronaći obrisane .DBX fajlove u nealociranom prostoru.

3. Windows Mail - ovaj klijent smešta elektronsku poštu u fajl sa .EML ekstenzijom (.FOL predstavlja indeksni fajl). Dolazi instaliran sa Windows Vista OS. Arhiva elektronske pošte se nalazi na sledećim lokacijama:

<korisničko_ime>\AppData\Local\Microsoft\Windows Mail

Obrisana elektronska pošta smešta se u “Deleted Items” folder u „locale store“, postojie kao individualni .EML fajlovi i ne brišu se po difoltu.

4. Mozilla Thunderbird - ovaj klijent smešta elektronsku poštu u fajl INBOX nema ekstenzije (.msf predstavlja indeksni fajl). Arhiva elektronske pošte se nalazi na sledećim lokacijama:

Kod Windowsa XP:

C:\Documents andSettings\[Korisničko Ime]\ApplicationData\Thunderbird

Profiles\<random 8 karaktera>.default\Mail\Local Folders

Kod Windows Vista i Windows 7 OS:

C:\users\[Korisničko ime]\Application Data\Thunderbird\Profiles\<

random 8 karaktera>.default\Mail\ Local Folders

Ukoliko je portable verzija nalazi se pod

„\Data\Profile\mail\ime_servera\"

Proces pakovanje (eng. compaction) se sprovodi ručno (auto proces je onemogućen po difoltu). Folderi imaju limit od 4GB.

5. *Webmail* - Elektronska pošta je uobičajeno smeštena na serveru provajdera (eng. ISP – Internet Service provide), osim ukoliko klijent koristi POP3 ili IMAP protokol za pristup pošti. To može biti od koristi forenzičaru čime se znatno ubrzava proces istrage. Mogu se dobiti korisničke IP-adrese i informacije o pretplatniku (npr. ADSL pretplatnik ili pretplatnik kablovskog interneta). Značajno je istaći da je moguće oporaviti keširane fajlove.

Posle prikupljenih heder i body informacija iz email poruka sledi njihovo ispitivanje i praćenje tragova kao što su: povratne putanje, email adrese primaoca, tip servisa za slanje elektronske pošte, ime servera elektronske pošte, jedinistveni identifikacioni broj elektronske pošte, datum i vreme slanja elektronske pošte, informacije o prikačenim fajlovima (eng. attachment) pretraživanje tela poruke prema određenom stringu i druge korisne informacije od značaja za istragu. Potrebno je utvrditi da li su poruke sačuvane na lokalnom računaru ili su ostavljene na serveru. Računari koji predstavljaju email servere smeštaju elektronsku poštu na dva načina u fajl ili u bazu podataka.

Forenzički značajni *fajlovi* su *.pst* i *.ost* (Microsoft Outlook) fajlovi koji mogu sadržati sačuvane elektronske poruke, kalendarska dešavanja kao i raspored obaveza. Pst fajlovi koriste se pri upotrebi POP3, IMAP i web orijentisanih email naloga.[490] OST fajlovi se zapravo koriste ukoliko se upotrebljava Exchange nalog u offline režimu i predstavljaju kopije objekata sa servera. Kada su u pitanju web orijentisni fajlovi elektronske pošte forenzičar treba da istraži fajlove i foldere koji se odnose na history, kolačiće, keš, i privremene fajlove (eng. Temp files). Kada se forenzička istraga odnosi na ispitivanje elektronske pošte dodatno će se koristiti i mrežni logovi da bi se potvrdila email ruta. Na primer, konsultovani će biti logovi sa rutera, logovi dolaznog i odlaznog saobraćaja na email serveru, fajervol logovi. Forenzički posmatrano POP3 predstavlja clear text tip protokola i sav saobraćaj koji ide kroz POP3 prolazi kao čist tekst (clear text). Tamo gde postoji POP3 a gde nije ssl omogućen zlonamerni napadači samo kroz prisluškivanje saobraćaja mogu izvući poverljive podatke (na primer šifra od email naloga). Sa stanovišta

490 Introduction to Outlook Data Files (.pst and .ost), Microsoft, http://office.microsoft.com/en-001/outlook-help/introduction-to-outlook-data-files-pst-and-ost-HA010354876.aspx, 28.05.2016.

bezbednosti potrebno je poznavati koji protokol na kom portu radi i na koji način, da bi se osigurala bezbednost informacija u organizaciji. Forenzičari se prilikom analize email komunikacije u organizacijama uglavnom susreću sa enkriptovanom POP3 komunikacijom. To znači da mrežni paketi koji putuju kroz mrežu preko 995 porta sugerišu da se radi o zaštićenoj email komunikaciji. Sledeći zadatak za forenzičara jeste pronalaženje načina da se ti kriptovani podaci isčitaju nakon njihovog prikupljanja. S obzirom na to da forenzičar ima ovlašćenja da radi na elementima IT infrastrukture od strane organizacije koja ga je angažovala može legitimno da dobije email sertifikat sa kojim može da se izvrši dekripcija prikupljenih paketa preko 995 porta. Na taj način će se dobiti clear text forma poruke. Ukoliko je istraga većih razmera sudija izdaje nalog da ISP može prikupiti sve mrežne pakete tipa Incoming i Outgoing koji se odnose na javne IP adrese organizacije gde se radi forenzička istraga.

Case study: Korisnički inbox email naloga je kompromitovan

Korisnik je dobio informaciju od GMAILa da se neko logovao sa drugim veb pretraživačem u njegov inbox. Korisnik u tom slučaju kontaktira IT podršku. Treba pokrenuti inicijalni forenzički odgovor da bi se pokupio digitalni dokaz sa identifikovanjem nedozvoljene aktivnosti i da bi se preduzele mere da se ista aktivnost ne bi ponovila. U ovom slučaju informacija koju će se proslediti korisniku jeste da hitno promeni šifru. Forenzički istražitelj preuzima digitalne dokaze i transportuje ih bezbedno do forenzičke laboratorije. Zatim sledi kreiranje 2 bitstream kopije originalnog hard diska uz kreiranje SHA heš vrednosti radi obezbeđivanja integriteta. Posle toga vrši se ispitivanja fajlova prikupljenih iz bitstream imidža.

Prema odredbi člana 4. stav 1. Zakona o elektronskom dokumentu („Sl. glasnik RS“, br. 51/2009), elektronskom dokumentu ne može se osporiti punovažnost ili dokazna snaga samo zato što je u elektronskom obliku. U praksi se zbog toga često pogrešno smatra da se svaki fajl u elektronskom obliku tumači kao dokaz. Na forenzičkom istražitelju ili licenciranom digitalnom veštaku je da dokaže da na primer email može biti uzet kao digitalni dokaz samo ako je prikupljen sa hederom, sa telom poruke i sa dokumentovanom procedurom inicijalnog forezičkog odgovora. Samo na taj način email i može biti uzet kao digitalni dokaz u ispitivanom slučaju.

Najupotrebljavaniji forenzički alati koji se koriste prilikom forenzičkog

ispitivanja elektronske pošte su: *AccessData's FTK*,[491] *EnCase Forensic*,[492] *Paraben E-mail Examiner*, [493] *FINALeMAIL*,[494] *DBXtract*,[495] *Fookes MailBag Assistant*.[496] [497] Za forenzičku istragu je važno i da se izvrši analiza spam foldera ispitivanog email klijenta zlonamernog napadača, da bi se ustanovilo da li spam poruka sadrži i nešto više osim spama. Zlonamerni napadači koriste i određene servise kao što je spam mimic koji služi za enkodiranje određenog teksta u vidu spam poruke, koja ne sadrži ni jedan string onoga što je uneto. [498] Takav dobijeni string može se dekodirati u decode prozoru spam mimica. Ovaj servis spam mimic je korišćen od strane zlonamernih napadača za prenošenje određenih poruka kroz lažne profile a forenzičar može takođe da proveri na tom servisu da li određena poruka u spam folderu sadrži zapravo neke druge informacije.

3.2. FORENZIČKI ODGOVOR NA NEDOZVOLJENU / INCIDENTNU AKTIVNOST „UŽIVO" NA LINUX PLATFORMI

Linux je besplatan UNIX orijentisan OS otvorenog koda (eng. open source). Izvorno kreiran od strane Linus Torvaldsa uz pomoć programera iz celog sveta. Postoje različite verzije Linuxa koje se nazivaju distribucije i najprisutnije su Red Hat, Centos, Fedora, Debian, Suse, Ubuntu, Kubuntu, Slackware. Svaka od njih ima svoje prednosti i mane. Ove distrbucije se međusobno razlikuju i prema tipovima. Postoje serverske, desktop i live distribucije. *Serverske distribucije* su primarno orijentisane na biznis okruženje (mada mogu da se konfigurišu i da budu odgovarajuće i za kućnu upotrebu). *Desktop distribucije* su pogodne više za kućnu upotrebu, podrazumevaju grafičko okruženje i veliki broj aplikacija. *Live distribucije* podrazumevaju butabilne verzije OS, koji se učitavaju direktno u RAM memoriju i rade nezavisno od postojećeg računarskog OS.

Forenzičar mora da zna način na koji Linux podiže svoj OS (eng linux

491 Forensic Toolkit (FTK), AccessData Community, http://www.accessdata.com/products/digital-forensics/ftk, 28.05.2016.

492 EnCase Forensic, Guidance Software, http://www.guidancesoftware.com/encase-forensic.htm, 28.05.2016.

493 Email Examiner, Paraben, http://www.paraben.com/email-examiner.html, 28.05.2016.

494 Http://www.finaldata.com/Products/?s=PRD&c=6&n=21, 29.05.2016.

495 DBXtract, OEHelp.com/DBXtract, http://www.oehelp.com/dbxtract/, 29.05.2016.

496 Fookes Software, http://www.fookes.com/mailbag/, 29.05.2016.

497 Prlja D., Reljanović M., *Visokotehnološki kriminal - uporedna iskustva*, Strani pravni život, br. 3/2009, str. 161-184.

498 Http://www.spammimic.com/, 27.07.2016.

boot sequince). Boot sekvenca otpočinje učitavanjem kernela. Uobičajeno slika kernela (eng. kernel image) se nalazi po difoltu u /boot direktorijumu. Takođe link ka slici kernela se nalazi u /boot direktorijumu i referencira se iz konfiguracionog fajla linux loadera LILO (/etc/lilo) ili GRUB (/etc/grub.conf). Poslednji korak jeste inicijalizacija. Fajlovi koji kontrolišu inicijalizaciju nalaze se u fajlu /etc/inittab. Fajl odgovoran za započinjanje procesa jeste /sbin/init. Tada se inicijalizuje runlevel i startup skripte kontrolisane od strane terminalskog procesa. Kada je reč o Linux fajl sistemu potrebno je istaći da Linux sve uređaje tretira kao fajlove i njih smešta u *folder /dev*. Za forenzičara je bitno da zna da većina Linux distribucija ima organizovane fajlove sa sličnom strukturom direktorijuma:

Tabela 8. Linux struktura direktorijuma

/bin	Zajedničke izvršne komande na nivou sistema
/boot	Potrebni fajlovi prilikom podizanja sistema uključujući slike kernela zajedno sa linkovima koji na njih upućuju definisanih u LILO ili GRUB
/usr	Lokalni programi, biblioteke, igre
/var	Logovi i drugi promenljivi fajlovi
/dev	Interfejs fajlovi koji omogućavaju jezgru (kernelu) da komuniciraju sa hardverom i fajl sistemom
/home	Direktorijumi svih korisnika na sistemu sa ličnim korisničkim i konfiguracionim fajlovima
/mnt	Priključna tačka za spoljašnje, udaljene i i Mount points for external, remote, i prenosive fajl sisteme
/etc	Konfiguracioni fajlovi i skripte za administraciju
/root	Direktorijum root korisnika
/sbin	Administrativne izvršne komande koje treba da budu dostupne samo root-u odnosno administratoru
/lib	Osnovne sistemske biblioteke
/opt	Opcioni i drugi programi

Osnovne komande koje forenzičaru mogu pomoći za dobijanje osnovnih informacija o ispitivanom sistemu su sledeće:

#uname - a - pokazuje ime računara i verziju Linuxa
#ls - prikazuje spisak fajlova
#ls -l - pokazuje spisak fajlova sa njihovim dozvolama
#ls -ul ime_fajla - daje vreme pristupa fajlu
#cp - kopira fajlove
#mv - premešta fajlove
#chmod - izmena dozvola nad fajlovima
#ps - prikazuje pokrenute procese

#netstat -s - prikazuje informacije i protokole
#ifconfig - prikazuje informacije o mrežnim uređajima na sistemu
#find - pretražuje informacije na sistemu
#grep - pretražuje fajlove ili pretražuje ključne reči
#less - izlistava sadržaj fajla
#more - izlistava sadržaj fajla
#cat - izlistava sadržaj fajla
#diff - daje poređenje dva fajla
#df - daje prikaz mount- ovanih fajl sistema

Na Linuxu, da bi neki fajl sistem mogao da se koristi mora biti *montiran* - dodeljen (eng. mount) sistemu. Svi fajl sistemi na particijama koji su definisani tokom instalacije Linux OS će biti automatski montirani prilikom svakog podizanja sistema.

Forenzičar mora da zna da podaci mogu biti upisani na uređaj (eng. device), iako sam uređaj nije montiran. Periferne uređaje za skladištenje podataka uređaj prepoznaje kao SCSI uređaje. Ukoliko se koristi IDE disk na primarnom kontroleru kao master sistem će ga nazvati "hda" ukoliko je priključen kao slave nazvaće se "hdb", dok će na sekundarnom kontroleru oni biti "hdc" i "hdd". Da bi se videla kompletna lista raspoloživih particija na sistemu koristi se komanda: *#fdisk -l /dev/hda*

Svaka particija ima svoje dodeljeno Linux ime. Oznaka „*" označava da se radi o bootabilnoj particiji. Izlaz fdisk komande uključuje i informacije o početnom i poslednjem cilindru svake particije, kao i broj blokova koji sadrže, ID particije i tip fajl sistema.

Forenzičar tokom istrage mora voditi računa o tome da sledi sledeće mere predostrožnosti kao što su:

- izbegavanje pokretanja programa na kompromitovanom računarskom sistemu;
- ne sme pokretati programe koji mogu izmeniti metadata podatke o fajlovima i direktorijumima;
- dokumentovanje svih preduzetih aktivnosti i rezultata tokom istrage;
- izračunavanje hash vrednosti podataka da bi bio obezbeđen integritet nad podacima.

Kao što je već bilo opisano za očuvanje podataka na „živom" sistemu često je potrebno da se blagovremeno utvrdi da li postoji određena incidentna/nedozvoljena aktivnost. Na primer, maliciozni program može ugroziti kako bezbednost samog sistema tako i sistema sa kojima je povezan. Odgovor

"uživo" na incidentnu/nedozvoljenu aktivnost na Linux platformi uz svoje specifičnosti vrlo je sličan kao i odgovor "uživo" na Windows paltformama. S obzirom da je značaj prikupljanja podataka kako onih postojanih tako i onih sa privremenim karakterom već opisivan u daljem tekstu će biti opisivani alati koji se odnose na njihovo prikupljanje na Linux platformi. Baš kao i kod forenzičkog ispitavanja Windows sistema za forenzičara je neophodno da ima svoj "komplet" alata za prikupljanje privremenih podataka (eng. volatile data) sa komporomitovanog sistema. Razlog je taj što određene komande na kompromitovanom sistemu mogu biti takođe ugrožene pa se ne mogu smatrati pouzdanim i interakcija sa ispitivanim sistemom svodi se na minimalnu. Korišćenjem sopstvenih alata moguće je otkriti dragocene podatke koji su skriveni određenim malicioznim programom (npr. rootkitom). Naravno u nekim slučajevima kada se radi rootkitu koji se učitava kao modul u kernel (eng. Loadable Kernel Module - LKM), ovi alati neće dati očekivane rezultate pa će biti potrebno uraditi forenzičko ispitivanje memorije i fajl sistema.

Linux ima dobru alatku koja može snimati pokrenute komadne i njihove izlaze, čime se lako dokumentuje ono što se radilo na živom sistemu. To je alatka "*Script*", koja kešira podatke u memoriji i upisuje sve informacije prilikom njenog prekida u fajl typescript. Ukoliko je potrebno snimanje posle svake komande alataka se upotrebljava sa switchom "-f".

#script ili #script -f

Pre pokretanja bilo kojih komandi na ispitivanom Linux sistemu iz pouzdanog komandnog okruženja (eng. command shell) pokreće se alatka *script* (prethodno iskompajlirana u proverenom okruženju).[499]

Baš kao što je bilo prikazano kod prikupljanja podataka sa Windows platforme može se pokrenuti netcat odnosno cryptcat komanda.[500] To se radi u slučajevima kada ne smemo isključiti računar, a nema mogućnosti da se računar poveže na uređaj za neprekidno napajanje ili externi hard disk. Forenzičar u tom slučaju pravi forenzičku kopiju hard diska koristeći transfer preko mreže (pod uslovom da postoji LAN mrežni priključak). To se radi upotrebom alatke dd u kombinaciji sa alatkom netcat čime se omogućava prenos kompletnog sadržaja hard diska tj. njegove bitstream kopije kroz

499 Šel eng. shell predstavlja interfejs između jezgra OS i korisnika. Ima veliki broj funkcijia od kojih se ističu interpretacija komandne linije, pokretanje programa, ulazno-izlazna redirekcija, međusobno povezivanje komandi (eng. pipe) i shell programiranje. Najpoznatiji shell komandni interpreteri su Bourne shell (sh), C shell (csh), Bourne-again shell (bash), Korn shell (ksh).

500 Ukoliko se želi obezbediti slanje podataka sa ispitivanog računara na forenzičku radnu stanicu može se koristiti *Netcat* sa enkripcijom koji se zove cryptcat. Cryptcat koristi poboljšanu verziju Twofish blokšifarsku enkripciju sa simetričnim ključem. Twofish, Schneier on Security, http://www.schneier.com/twofish.html, 30.05.2016.

mrežu na udaljeni forenzički računar.

#dd if=/dev/hda bs=16065b | netcat targethost-IP 9898 (ispitivan računar sa kog se šalju informacije sektor po sektor uz pomoć netcat alatke)

#netcat–l –p 9898 | dd of=/dev/hdc bs=16065b (forenzička radna stanica na kojoj je pokrenuta alatka netcat u modu slušanja koja može biti ili Linux ili Windows)

Na taj način izvršena je akvizicija odnosno duplikacija hard diska.

Sa komandom CTRL-C prekida se netcat sesija. Sledeće što treba uraditi je da se nad dobijenim podacima generiše hash vrednost SHA-1 ili SHA-256. Isto tako treba iskopirati i dobijeni typescript fajl i nad njim izvršiti generisanje hash vrednosti.

Da bi se dobili odgovori na pitanja "ko, šta, gde, kada i kako" se desila incidentna/nedozvoljena aktivnost potrebno će biti prikupiti sledeće podatke:

Podaci sa privremenim karakterom:

- Sistemsko vreme i datum
- Postojeće mrežne konekcije
- Otvoreni TCP i UDP portovi
- Izvršni fajlovi koji otvaraju TCP i UDP portove
- Pokrenuti procesi
- Otvoreni fajlovi
- Interna tabela rutiranja
- Učitani moduli u kernel LKM
- Pridruženi fajl sistemi (eng. mounted file systems)

Postojani podaci od značaja:

- Verzija OS i nivo ažuriranosti paketa
- Vremenski pečati fajl sistema
- Ulogovani korisnici na sistem
- Istorija logovanja na Linux sistem
- Logovi na sistemu
- TCP Wrappers
- Korisnički nalozi
- Korisnički fajl sa istorijom izvršenih komandi
- Sumnjivi fajlovi

3.2.1. Podaci od značaja privremenog karaktera na Linux-u -sistemsko vreme i datum

Sistemsko vreme i datum se dobija upotrebom komande koja označava i početak forenzičkog prikupljanja vremena:

#date a izlaz ove komande je: Sun Feb 3 13:54:31 CET 2013

Upotrebom forenzičke netcat komande to se radi na sledeći način:

#netcat -v -l -p 9898 > datum_komprimitovanog_rucunara

#/mnt/cdrom/date -u | /mnt/cdrom/netcat ip_adresa_forenzicke_ radne_stanice 9898

#sha256sum datum_komprimitovanog_rucunara > datum_ komprimitovanog_ rucunara.sha256

Po završetku forenzičkog prikupljanja preporuka je da se markira i vreme završetka prikupljanja podataka sa kompromitovanog računara.

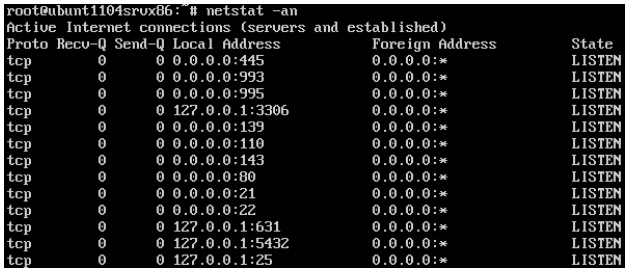
#netcat -v -l -p 9898 > vreme_kraj_komprimitovanog_rucunara

#/mnt/cdrom/date -u | /mnt/cdrom/netcat ip_adresa_forenzicke_ radne_stanice 9898

#sha256sum vreme_ kraj_ komprimitovanog_ rucunara > vreme_ kraj_ komprimitovanog_rucunara.sha256

3.2.2. Podaci od značaja privremenog karaktera na Linux-u - postojeće mrežne konekcije

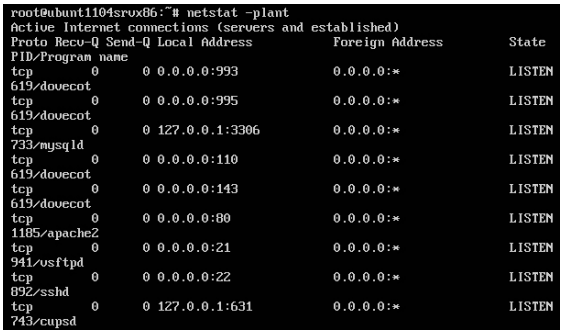
Podaci postojeće mrežne konekcije su važan pokazatelj aktivnosti na ispitivanom sistemu. Na osnovu ovih podatka forenzičar može utvrditi da li je zlonamerni korisnik još uvek priključen na sistem i koji port koristi. Pored toga moguće je ustanoviti i inicijalnu tačku upada odnosno omogućene (eng. enable) ranjive servise na sistemu, koji mogu biti kompromitovani i omogućiti upad u sistem. Komanda koja može da izlista postojeće mrežne konekcije jeste *#netstat -na komanda* i prikazana je na sledećoj slici:



Slika 72. Prikaz izlaza komande netstat -an

3.2.3. Podaci od značaja privremenog karaktera na Linux-u - otvoreni TCP i UDP portovi

Forenzičko ispitivanje otvorenih portova (TCP i UDP) na sistemu je fokusirano na detektovanje ranjivih portova ili zadnjih vrata (eng. backdoor) uspostavljenih na sistemu, koji omogućuju realizovanje indicentne/ nedozvoljene aktivnosti.[501] Komanda *#netstat –plant* daje prikaz portova, IP-adresa, procesa i ID-a, koji je odgovoran za otvaranje određenog porta.



Slika 73. Prikaz izlaza komande netstat -plant

Forenzičar može pomoću netcata prikupiti na živom sistemu ove informacije na sledeći način:

#netcat -v -l -p 9898 > open_port_TCP_UDP_komprimitovanog_racunara

#/mnt/cdrom/netstat -plant | /mnt/cdrom/netcat ip_adresa_forenzicke_radne_stanice 9898

#sh256sum open_port_TCP_UDP_kompromitovanog_racunara >

501 Može se očekivati da se na sistemu pored TCP i UDP portova pojavi i RAW port i treba znati da se on odnosi na Linux kernel.

open_ port_ TCP_ UDP_kompromitovanog_racunara.sh256

Najbolji način zaštite otvorenih portova (jer nose potencijane rizike upada u sisem) je da se otvore samo oni portovi, koji su potrebni za pravilno funkcionisanje sistema. Servise koji rade na nepotrebnim portovima treba izbaciti iz sistema, čime se povećava bezbednost samog sistema.

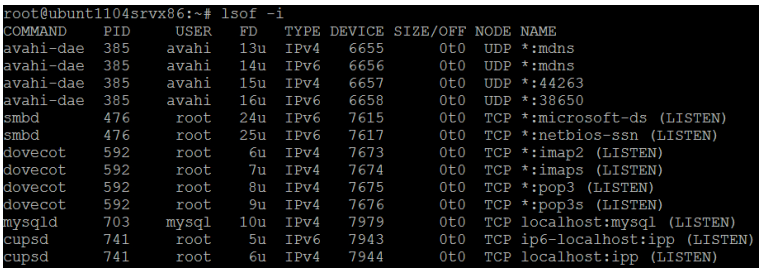
3.2.4. Podaci od značaja privremenog karaktera na Linux-u - izvršni fajlovi koji otvaraju TCP i UDP portove

U Windows okruženju prikazana je alatka *fport.exe* koja je linkovala otvoreni port sa startovanim procesom. Pod Linuxom to se može uraditi sa alatom koji se zove *lsof* (eng. List Open Files) koja daje listu aktivnih procesa.[502] Karakteristika ove alatke je da daje ne samo prikaz procesa koji otvara određeni port, već daje prikaz fajlova koji pokreću određeni proces. U slučaju da je zlonamerni napadač kompromitovao sistem i preneo određene maliciozne fajlove, on će maliciozne fajlove pokušati da sakrije od sistema, markirajući ih kao skrivene. Sledeće što će uraditi je kreiranje procesa, koji će nakon otvaranja fajla raskinuti vezu sa fajlom tzv. unlink, a proces će nastaviti da izvršava zlonamerne aktivnosti. Programi tipa "ls" neće prikazati ove informacije o fajlu i procesu, jer su sakriveni od administratora.

Stoga je veoma važno da forenzičar ili administrator poznaju ograničenja programa koje upotrebljavaju. Lsof je program koji će pružiti detaljne informacije o fajlovima uključujući i fajlove sa raskinutim vezama. Poznavanje dostupnih alata i odabir pravog je od ključne važnosti kako za forenzičko ispitivanje tako i za ustpostavljanje bezbednog sistema.

Može se koristiti kao #lsof -n , gde se daje detaljan prikaz o fajlovima, procesima i portovima na sistemu. Pretraga se može suziti na one procese, koji se odnose na TCP i UDP internet socket-e prikazanoj na sledećoj slici sa komandom "#lsof -i":

502 Information Security Archive, CERIAS, http://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/lsof/, 30.05.2016.



Slika 74. Prikaz izlaza komande lsof -i

Upotreba ove komande na forenzički ispravan način kojim se mogu prikupiti sve informacije o svim procesima na sistemu, otvorenim portovima i fajlovima je sledeća:

#netcat -v -l -p 9898 > lsof_komprimitovanog_racunara

#/mnt/cdrom/lsof -n -P -l | /mnt/cdrom/netcat ip_adresa_forenzicke_radne_stanice 9898

#sh256sum lsof_ kompromitovanog_ racunara > lsof_ kompromitovanog_ racunara.sh256

Podatke dobijene pomoću netstat i lsof komandi treba međusobno uporediti, jer u njihovim razlikama forenzičar može pronaći skrivene procese od strane kernela sa LKM-om. Analiza LKM-a spada u posebnu oblast, koja nije predmet ove knjige. Blagovremenim uočavanjem sumnjivih portova od strane digitalnog forenzičara dobiće se dodatni podaci o incidentnoj/nedozvoljenoj aktivnosti, a uočavanjem od strane administratora moguće će biti sprečiti nanošenje dodatne štete na sistemu.

3.2.5. Podaci od značaja privremenog karaktera na Linux-u - pokrenuti procesi i servisi

Da bi sistem bio bezbedan mora se znati koji su procesi i servisi pokrenuti na njemu. Pokrenute procese mogu se videti u Linuxu na nekoliko načina. Jedan je korišćenjem komade "Ps". *#ps -auxwww* je komanda, koja izlistava sve procese na sistemu sa pripadajućim korisnicima koji su ga startovali.

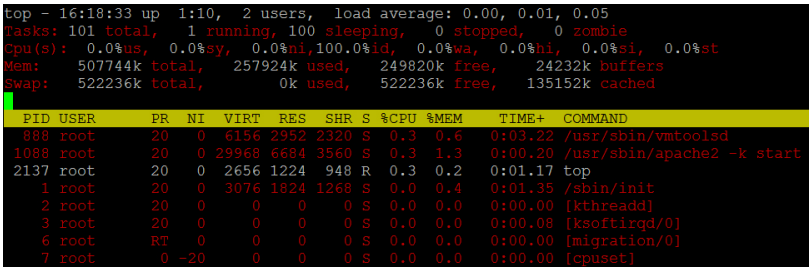
INETD je proces, koji upravlja standardnim internet servisima na

sistemu. Startuje se podizanjem sistema i koristi konfiguracioni fajl u kome je definisano, koje servise treba da omogući. Glavni konfiguracini fajl, koji inetd koristi je /etc/inetd.conf (mesto ime zavisi od tipa Linux distribucije). Za bezbednost sistema je važno da se razume na koji način inetd radi i koje informacije on sadrži u konfiguracionom fajlu.[503]

Drugi način je pokretanje komande "top": #top

Program top će generisati ceo ekran sa spiskom postojećih procesa, koji se stalno ažuriraju prema stepenu iskorišćenja CPU-a. Na vrhu ovog spiska nalaze se podaci o: vremenu podizanja OS, broju pokrenutih procesa na sistemu, statistici raspoložive memorije, swap prostoru. Prikaz se može formatirati na različite načine sa tasterom "SHIFT+o" tako da se procesi mogu sortirati prema zauzeću CPU (SHIFT+p), memorije (SHIFT+m), swap-a, ID-u procesa itd. Radi lakšeg uočavanja procesa koji su aktivni koristi se taster "z", koji boji sve procese u crveno. Belom bojom su obojeni procesi koji su najintenzivniji prema definisanim parametrima. Prikaz startovanog procesa od strane određenog korisnika:

#top -u sumnjivog_korisnika



Slika 75. Prikaz izlaza top komande

Za forenzičare je važan prikaz apsolutnih putanja startovanih procesa, koji se izlistava *tasterom "c"* nakon pokretanja top komande. U praksi se desio sledeći slučaj: Http server organizacije je prestao odjednom sa radom. Analizom podataka na serveru došlo se do zaključka da nije bilo napada, već je http server Zope bio ažuriran sa bagovitim fajlovima i generisao je veliku količinu log fajlova, koji su zauzeli 100% prostora na disku. Analizom top komande došlo se do procesa, koji je generisao greške i fajl u koji je te greške upisivao. Nakon zaustavljanja top procesa, brisanjem prepunjenog log fajla i korigovanjem bagovanih fajlova Zope http server uspešno je startovan i

503 Marcella A. J., Greenfield S. R., *Cyber Forensics*, CRC Press LLC, 2002.

problem je bio rešen.

Pokrenute servise na sistemu možemo utvrditi i pomoću komadne:

#service --status-all

#ps -A

3.2.6. Podaci od značaja privremenog karaktera na Linux-u - otvoreni fajlovi

Komandom lsof može se dobiti lista otvorenih fajlova na sistemu. Za forenzičko ispitivanje ovo mogu biti dragoceni podaci. Na primer, mogu se uočiti skriveni fajlovi odnosno maliciozni alati (npr. password crackeri, exploiti i drugi maliciozni programi), koji mogu iskoristiti resurse samog servera uperene kako protiv sami korisnika na sistemu tako i protiv drugih sistema (npr. za distribuciju ili hostovanje, dečije pornografije, za distribuciju sadržaja zaštićenih autorskim pravima i mnoge druge vrste visikotehniloškog kriminala).

Komande koje forenzičaru mogu biti od koristi su sledeće:

#lsof -u root prokazuje sve otvorene procese i otvorene fajlove od strane root korisnika

#lsof -p 3333 prikazuje sve otvorene fajlove od strane procesa sa ID 3333

#lsof /var/log/auth.log prikazuje proces koji otvara određeni fajl kao na sledećoj slici:

```
root@ubunt1104srvx86:/var/log# lsof /var/log/auth.log
COMMAND  PID   USER   FD   TYPE DEVICE SIZE/OFF   NODE NAME
rsyslogd 366 syslog    1w   REG    8,1     7300 665417 /var/log/auth.log
root@ubunt1104srvx86:/var/log#
```

Slika 76. Prikaz izlaza lsof komande nad fajlom /var/log/auth.log

#lsof /home se može pokazati kao korisna informacija, ukoliko sistem prikazuje grešku zauzeća (eng. Device or resource busy), jer može prikazati koji su procesi odgovorni za montiranje tačke /home na sistem.

3.2.7. Podaci od značaja privremenog karaktera na Linux-u - interna tabela rutiranja i keš tabele

Da bi administrator ili forenzičar ustanovili da li je ruting tabela menjana iz istih navedenih razloga kao kod podataka od značaja privremenog karaktera na Windowsu, to je moguće obaviti a netstat komandom (ili sa route komandom) kao na slici: #route ili #netstat –nr

```
root@ubunt1104srvx86:~# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.1.0     0.0.0.0         255.255.255.0   U         0 0          0 eth0
0.0.0.0         192.168.1.1     0.0.0.0         UG        0 0          0 eth0
```

Slika 77. Prikaz izlaza komande netstat -rn

ARP (eng. Address Resolution Protocol) je TCP/IP protokol, koji se koristi da pretvori IP-adresu u fizičku adresu odnosno MAC adresu. Za digitalnog forenzičara značajno je ispitivanje ARP keša ispitivanog računara, jer je moguće identifikovati druge sisteme koji su trenutno ili nedavno uspostavili vezu sa ispitivanim računarom. Informacije prikupljene putem ARP keša se koriste za otkrivanje dodatnih računara na mreži, koji su možda kompromitovani kao posledica incidentnih/nedozvoljenih aktivnosti. Sa stanovišta bezbednosti posmatranje ispitivanje ARP keša koristi se i za identifikovanje sumnjivih računarskih sistema na mreži, koji mogu biti korišćeni za pokretanje internih napada u mreži. Da bi se na sistemu prikazao sadržaj ARP keša koristi se komanda “arp”: #/mnt/cdrom/arp

```
[root@turing ~]# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
147.91.96.190            ether   a0:f3:c1:a2:0c:05   C                     eth0
147.91.96.208            ether   a0:f3:c1:a2:41:b3   C                     eth0
147.91.96.148            ether   00:19:99:d3:90:33   C                     eth0
147.91.96.149            ether   00:19:99:e4:cf:d6   C                     eth0
147.91.96.146            ether   50:26:90:a1:46:f6   C                     eth0
```

Slika 78. Prikaz ARP keša komandom arp

Ova komanda prikazaće sve IP-adrese, koje su konektovane ili bile konektovane sa ispitivanim računarom.

Forenzičar pomoću netcata može prikupiti na živom sistemu ove informacije na sledeći način:

#netcat -v -l -p 9898 > ARPkeš_komprimitovanog_racunara

#/mnt/cdrom/arp | /mnt/cdrom/netcat ip_adresa_forenzicke_radne_

stanice 9898

#sh256sum ARPkeš_komprimitovanog_racunara > ARPkeš_ komprimitovanog_ racunara.sh256

Trenutno aktivne rute na sistemu čuvaju se u tzv. ruting kešu odnosno ruting keš tabeli (eng. kernel route cache table). Ruting keš tabela se razlikuje od ruting tabele. Naime, *ruting keš tabela* prikazuje trenutno aktivne (uspostavljene) rute na sistemu. *Ruting tabela* se koristi za donošenje odluke oko rutiranja, a ruting keš tabela daje prikaz ruta koje su uspostavljene. Upravo to može biti značajno za forenzičku istragu, jer prikupljene informacije iz ruting keš tabele mogu pomoći u otkrivanju računara na mreži ne samo onih koji su možda kompromitivani, nego i onih sa kojih je incidentna/ nedozvoljena aktivnost izvršena. Sa stanovišta bezbednosti, prikupljanje informacija iz ruting keš tabele može se koristi i za identifikovanje sumnjivih računarskih sistema na mreži koji mogu biti korišćeni za pokretanje internih napada u okviru mreže. Ruting keš tabela (eng. Kernel route cache table) daje prikaz izvorne adrese (eng. source) i odredišne adrese (eng. destination), mrežni izlaz (eng. gateway) i interfejs koji se koristi da bi se veza uspostavila.

Na Linux sistemima ispitivanje rute keša može se dobiti pomoću komande "route":

#route -Cn

```
root@emis:~# route -Cn
Kernel IP routing cache
Source          Destination     Gateway         Flags Metric Ref    Use Iface
66.249.76.226   147.91.102.6    147.91.102.6    l     0      0       49 lo
147.91.102.6    66.249.76.162   147.91.102.1          0      0        1 eth0
147.91.102.6    66.249.76.226   147.91.102.1          0      0        7 eth0
147.91.102.6    66.249.76.14    147.91.102.1          0      0       14 eth0
147.91.102.6    147.91.96.2     147.91.102.1          0      2        0 eth0
147.91.102.6    147.91.96.2     147.91.102.1          0      0        4 eth0
192.168.2.4     192.168.2.255   192.168.2.255   ibl   0      0       11 lo
```

Slika 79. Prikaz sadržaja Ruting keš tabele

Forenzičar pomoću netcata može prikupiti na živom sistemu ove ruting keš informacije na sledeći način:

#netcat -v -l -p 9898 > ruting_kes_tabela_komprimitovanog_racunara

#/mnt/cdrom/route -Cn | /mnt/cdrom/netcat ip_adresa_forenzicke_ radne_stanice 9898

#sh256sum ruting_kes_tabela_komprimitovanog_racunara > ruting_ kes_tabela _komprimitovanog_ racunara.sh256

3.2.8. Podaci od značaja privremenog karaktera na Linux-u - učitani moduli u kernel LKM

Ukoliko postoji osnovana sumnja da je postojeći kernel ispitivanog sistema kompromitovan određenim rootkitom odnosno trojancem potrebno će biti izlistati učitane module u kernel. To se može uraditi na sledeće načine:

#netcat -v -l -p 9898 > moduli_komprimitovanog_racunara

#/mnt/cdrom/cat /proc/modules | /mnt/cdrom/netcat ip_adresa _ forenzicke_ radne_ stanice 9898

#sh256sum moduli_komprimitovanog_racunara > moduli_ komprimitovanog_ racunara.sh256

ili sa proverenom komandom lsmod:

#netcat -v -l -p 9898 > moduli_komprimitovanog_racunara

#/mnt/cdrom/lsmod | /mnt/cdrom/netcat ip_adresa_forenzicke_ radne_stanice 9898

#sh256sum moduli_ komprimitovanog_racunara > moduli_ komprimitovanog_ racunara.sh256

Izlaz komande lsmod prikazan je na sledećoj slici:

```
root@ubunt1104srvx86:~# lsmod
Module                  Size  Used by
vesafb                 13449  1
snd_ens1371            24722  0
gameport               15027  1 snd_ens1371
snd_rawmidi            25269  1 snd_ens1371
snd_seq_device         14110  1 snd_rawmidi
snd_ac97_codec        105614  1 snd_ens1371
ac97_bus               12642  1 snd_ac97_codec
snd_pcm                80244  2 snd_ens1371,snd_ac97_codec
ppdev                  12849  0
vmw_balloon            12729  0
psmouse                59039  0
snd_timer              28659  1 snd_pcm
```

Slika 80. Prikaz trenutno učitanih modula u kernel komandom lsmod

Ono što forenzičar treba da ima na umu je, da u praksi postoje određene tehnike kojima se maliciozni modul može učitati u kernel i sakriti ga nakon toga. Jedan takav rootkit zove se Knark (više informacija o Knarku[504] može se saznati na SANS[505] sajtu). Nakon skrivanja učitanog modula ne postoji šansa da se on otkrije forenzičkim ispitivanjem "uživo".

504 Jonathan Clemens, CCP, CISSP, IDFAQ: Knark: Linux Kernel Subversion, Corporate Information Security, Intel, http://www.sans.org/security-resources/idfaq/knark.php, 30.05.2016.

505 SANS Institute, http://www.sans.org/, 30.05.2016.

3.2.9. Podaci od značaja privremenog karaktera na Linux-u - dump memorije i memorijskih procesa

Da bi forenzičar mogao da analizira memoriju sa kompromitovanog računara potrebno je da se "snimi" (eng. capture) fizička memorija, o čemu je već ranije bilo reči u delu koji govori o Dump-u memorije na Windows OS. Kada se vrši "snimanje" memorije takođe se i remeti trenutno stanje memorije, a razlog je pokretanje programa i čitanje podataka. Dodatan problem predstavlja upisivanje fajla sa snimljenim stanjem fizičke memorije. To znači da će bilo koji izlaz fajla biti keširan u memoriji, zamenjujući možda veoma važne informacije značajene za digitalnu istragu. Zato *korišćenje forenzičkog računara* jeste najbolji način da se sačuvaju podaci sa minimalnim uticajem na memoriju. Kada je reč o "snimanju" memorije forenzičar se susreće sa jednim problemom: potrebom da se sačuva što veća količina veoma promenljivih podataka, ali se sa njihovim prikupljanjem mogu uništiti dodatni dokazi. Odluka forenzičara mora biti takva da značaj prikupljenih podataka mora biti veći od značaja onih podataka koji će se izgubiti. Procena toga zavisi od iskustva samog forezničara.

Zbog obaveznog dokumentovanja celog postupka preporuka je da se prikupe osnovne informacije o memoriji. Fajl koji sadrži ove podatke jeste /proc/meminfo. To se radi na sledeći način:

#netcat -v -l -p 9898 > mem_info_komprimitovanog_racunara

#/mnt/cdrom/cat < /proc/meminfo | /mnt/cdrom/netcat ip_adresa_ forenzicke_ radne_ stanice 9898

#sh256sum mem_info_komprimitovanog_racunara > mem_ info_ komprimitovanog_ racunara.sh256

Najjednostavniji način, mada ne i univerzalan, za "snimanje" kompletne fizičke memorije na Linux sistemima je pokretanje proverene statički kompajlirane *dcfldd komande*.[506] Dcfldd format predstavlja zapravo dd koji je proširen sa dodatnim funkcionalnostima kao što je hešing on-the-fly. Može da se koristi i za kreiranje bitstream kopije hard diska. Nakon što se kreira bitstream kopija (ili bilo koji vid akvizicije) mora se primenti hešing algoritam i na bitstrim kopiji i na originalnom dokazu da se potvrdi poklapanje vrednosti heša a ova alatka radi heširanje za vreme kopiranja na svakom bajtu.[507]

#netcat -v -l -p 9898 > fiz_mem_komprimitovanog_racunara

#/mnt/cdrom/dcfldd < /dev/mem | /mnt/cdrom/netcat ip_ adresa_

506 Http://dcfldd.sourceforge.net/, 30.05.2016.

507 Korać V., *Digital archaeology of volatile data on Linux platform*, Arheologija i prirodne nauke br. 9/2014, Beograd, str. 205-217.

forenzicke_ radne_stanice 9898

#sh256sum fiz_mem_komprimitovanog_racunara > fiz_ mem_ komprimitovanog_ racunara.sh256

Ovaj postupak funkcioniše na Linux sistemima međutim neki od Unix sistema (npr. FreeBSD, Solaris) tretiraju fizičku memoriju na drugačiji način, što za posledicu može imati nekompletan sadržaj fizičke memorije.[508] Postoji alatka "*memdump*" u okviru The Coroner's Toolkit-a (TCT)[509] koja uspešno razrešava pomenuti problem koristići pritom minimalno memorije. Forenzički ispravan način primene ovog progama je na sledeći način:

#netcat -v -l -p 9898 > fiz_mem_komprimitovanog_racunara

#/mnt/cdrom/memdump | /mnt/cdrom/netcat ip_adresa_forenzicke_ radne_stanice 9898

#sh256sum fiz_mem_komprimitovanog_racunara > fiz_ mem_ komprimitovanog_ racunara.sh256

Sadržaju fizičke memorije može se pristupiti i preko *fajla /proc/kcore*. Ovaj fajl sadrži podatke iz fizičke memorije koji se nalaze u ELF[510] core fajl formatu. Opšte je mišljenje da je vrlo preopručljivo prikupiti sadržaj ovog fajla, pored sirovih (eng. raw format) podataka iz memorije. Razlog je što se ovaj format može ispitati sa GNU debbuger-om tzv. GDB uz pomoć "System map" fajla i slike kernela iz /boot direktorijuma.[511] Ovaj postupak opisao je Mariusz Burdach u svojim radovima.[512] [513] [514] [515]

Kada je o memoriji reč forenzički je značajan i *swap prostor* na sistemu.

---

508 Home page The United States Department of Justice, *Reporting Computer related crime,* http://www.justice.gov/criminal/cybercrime/intl.html, 22.06.2016.

509 The Coroner's Toolkit (TCT) predstavlja kolekciju forenzičkih alata čiji su autori Wietse Venema i Dan Farmer. The Coroner's Toolkit (TCT), http://www.porcupine.org/forensics/tct.html, 05.04.2016.

510 ELF - Executable and Linking *Format.*

511 5.2.14. /proc/kcore, Red Hat Enterprise Linux, https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Enterprise_Linux/5/html/Deployment_Guide/s2-proc-kcore.html, 05.04.2016.

512 Mariusz Burdach, Detecting Rootkits And Kernel-level Compromises In Linux, http://www. symantec.com/connect/articles/detecting-rootkits-and-kernel-level-compromises-linux, 05.04.2016.

513 Mariusz Burdach, Forensic Analysis of a Live Linux System, Pt. 2, http://www.symantec.com/ connect/articles/forensic-analysis-live-linux-system-pt-2, 05.04.2016.

514 Ivaniš N., *Digitalna forenzicka istraga u virtuelnom okruženju*, master rad, Univerzitet Singidunum 2011.

515 Jakobsson M., Ramzan Z., *Crimeware: Understanding New Attacks and Defenses*, Addison Wesley Professional, 2008.

Swap prostor predstavlja prostor u kome se delovi memorije *stranice*[516] (eng. pages) privremeno smeštaju u slučaju potrebe oslobađanja dela RAM memorije[517] (ili je sistemu potrebno više memorije nego što je raspoloživo postojećim RAM-om). Zbir RAM memorije i swap memorije predstavlja ukupuno količinu virtuelne memorije na sistemu. Swap prostor može postojati u formi swap particije (što je preporučljivo), swap fajla ili kombinaciji swap fajla i particije. Ovaj prostor može sadržati značajne informacije za forenzičku istragu (iako sistem retko swap-uje). Swap prostor se može jednostavno iskopirati korišćenjem alata "dd" ili "cat" nad swap particijom ili fajlom uz pomoć "netcat" alatke i posle pretraživati određenim alatima u potrazi za određenim stringom (npr. hexdump).[518]

Dump memorije startovanih procesa moguće je uraditi pomoću alatke *pcat* koja se nalazi u sastavu pomenutog The Coroner's Toolkit-a (TCT).[519]

Forenzički ispravna upotreba ove komande je:

#netcat -v -l -p 9898 > pcat_komprimitovanog_racunara

#/mnt/cdrom/pcat proc_id | /mnt/cdrom/netcat ip_adresa_forenzicke_radne_stanice 9898

#sh256sum pcat_komprimitovanog_racunara > pcat_komprimitovanog_ racunara.sh256

Za forenziku memorije značajna je alatka Inception koja radi pod Linuxom. Inception može da prikupi privremeni heš šifre zaključane sesije operativnih sistema (Windows, Mac, Ubuntu). Radi preko DMA (direct memory access) interfejsa kao što je FireWire, Thunderbolt, ExpressCard, PCMCI Card, PCI/PCIe HW interfaces. U DMA port, na primer firewire može se ubaciti konekcija sa forenzičke radne stanice i kroz alat Inception izvrši se ulazak na bilo koji operativni sistem. U prvih 4 GB ram memorije pretražuje lokacije heša privremene lock sesije Osa, zatim briše taj heš i nakon toga moguće je ulazak na zaključani OS. Uslov da bi ulazak na operativni sistem bio uspešno izveden je da ispitivani računar ima maksimalno 4 GB ram memorije. Ne može se izvesti forenzika memorije preko USB porta (Verzije OS X > 10.7.2 i Windows > 8.1 onemogućavaju FireWire DMA na zaključanom

516 U Linux sistemima RAM memorija se deli na delove memorije koji se nazivaju stranice (eng. pages).

517 Kernel može da izmešta na swap prostor one delove memorije koji se manje koriste (neaktivne) i da tu oslobođenu memoriju dodeli tekućem programu odnosno procesu kome je potrebna memorija.

518 Linux / Unix Command: hexdump, http://linux.about.com/library/cmd/blcmdl1_hexdump.htm, 05.04.2016.

519 Http://www.porcupine.org/forensics/tct.html, 05.04.2016.

operativnom sistemu i na taj način onemogućena je upotreba Inception alata, ali je ona moguća u slučaju da je korisnik ulogovan.

Poznavanje načina na koji sistem upotrebljava memoriju (keširanje fajlova i stranice sa virtuelnom memorijom eng. memory page čiji je cilj poboljšanje performansi računara), veoma je važan za analizu same memorije. Iz navedenog proizlazi da se mogu pronaći i identifikovati značajni delovi memorije na sistemu, koji su od značaja digitalnu istragu.

3.2.10. Podaci od značaja privremenog karaktera na Linux-u - montirani fajl sistemi

Za forenzičko ispitivanje važno je da se ustanove koji su fajl sistemi montirani (eng. mounted) u ispitivanom operativnom sistemu. Postoje određene komande kojima se to može ustanoviti.

Prva komanda je *mount* komanda:

#mount čiji izlaz prikazuje uređaje (npr. hard disk) tačku montiranja i tip fajl sistema.

Druga komanda jeste *df* komanda:

#df čiji izlaz prikazuje montirane uređaje, tačku montiranja, veličinu i raspoložive kapacite i veličinu zauzeća.

```
root@ubunt1104srvx86:~# df
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/sda1             20125340   2225092  16877940  12% /
none                    247256       200    247056   1% /dev
none                    253872         0    253872   0% /dev/shm
none                    253872       444    253428   1% /var/run
none                    253872         0    253872   0% /var/lock
```

Slika 81. Izlaz df komande

Prethodne dve komande ne mogu videti montirane deljene resurse mrežnog fajl sistema ili skraćeno NFS (eng. Network File System). Komanda koja može prikazati NFS deljen resurse jeste *showmount*:

#showmount -a localhost ili showmount -e koja pokazuje exportovane sisteme

#showmount -a localhost

All mount points on localhost:

192.168.1.104:/nfs/slike

192.168.1.101:/nfs/filmovi

Prikazuje spisak računarskih sistema koji su konektovani na lokalni

sisteme, njihove tačke pristupa. Ova komanda forenzičarima može omogućiti prikupljanje dragocenih podataka na ispitivanom OS, pogotovu kada je u pitanju neovlašćena distribucija zaštićenih autorskih dela ili zabranjenih pornografskih sadržaja.

3.2.11. Postojani podaci od značaja na Linux-u - verzija OS i nivo ažuriranosti paketa

Za forenzičku istragu značajno je saznati o kojoj se verziji OS radi (i koja je verzija kernel u pitanju) da bi se primenio forenzički alat adekvatan verziji Linux OS. Verzija OS na većini Linux distribucije može se dobiti alatom uname sa *switchem "-a"*:

#uname -a koji izlistava ime računara, verziju kernela, Linux distribuciju, vreme i tip sistema (x86 ili x64), ali ne izlistava verziju Linux distribucije

#Linux ubunt1104srvx86 2.6.38-8-generic-pae #42-Ubuntu SMP Mon Apr 11 05:17:09 UTC 2011 i686 i686 i386 GNU/Linux

Na primer, na Debian i Ubuntu distribucijama moguće je videti i verziju Linux distribucije alatom "*lsb_release*"sa switch-em "-a":

 # lsb_release -a koji daje sledeći izlaz:

Description: Ubuntu 11.04

Release: 11.04

Codename: natty

Na Red Hat distribuciji verziju Linux distribucije moguće je videti izlistavanjem fajla "*/etc/redhat-release*" sa alatkom "*cat*"

#cat /etc/redhat-release koji daje sledeći izlaz:

Red Hat Enterprise Linux Server release 6.3 (Santiago)

Nivo ažuriranosti paketa (eng. patch level) je teže dobiti i razlikuje se od distribucije do distrbibucije. Na Red Hat distribuciji moguće je dobiti spisak instaliranih paketa komandom "*rpm -qa*"

 # rpm -qa koji daje sledeći izlaz:

libXxf86misc-1.0.2-1.el6.x86_64

openjpeg-libs-1.3-9.el6_3.x86_64

libcroco-0.6.2-5.el6.x86_64

evolution-data-server-doc-2.28.3-15.el6.noarch

libSM-devel-1.1.0-7.1.el6.x86_64

...

Na Ubutntu ili Debian distribuciji nivo ažuriranosti moguće je dobiti komandom:

#dpkg --get-selections koji daje sledeći izlaz:

adduser install
apache2 install
apache2-mpm-prefork install
apache2-utils install
apache2.2-bin install
apache2.2-common install
apparmor install

Prikupljanjem ovih informacija moguće je dobiti vrlo korisne početne informacije o bezbednosti sistema odnosno njegovoj ranjivosti na osnovu instaliranih paketa.

3.2.12. Postojani podaci od značaja na Linux-u - vremenski pečati fajl sistema

Vremenski pečati fajlova na sistemu se mogu dobiti na različite načine. Jedan od načina je korišćenje alata "*stat*". Ako su potrebne informacije o nekom fajlu (npr. o dozvolama nad fajlom, datumu i vremenu poslednjeg pristupa fajlu, datumu i vremenu poslednje izmene fajla, datumu i vremenu promene inoda, o vlasništvu nad fajlom, o veličini fajla i putanji do fajla), moguće je dobiti ih na sledeći način:

#stat /etc/passwd dobija se izlaz:

File: `/etc/passwd'
Size: 1467 Blocks: 8 IO Block: 4096 regular file
Device: 801h/2049d Inode: 1058850 Links: 1
Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)
Access: 2013-02-03 17:13:19.650908871 +0100
Modify: 2013-02-03 17:13:19.610908872 +0100
Change: 2013-02-03 17:13:19.618908872 +0100

Ukoliko forenzičar želi dobiti ove podatke za sve fajlove koji se nalaze u sistemu u čitljivom formatu mora se pretražiti ceo fajl sistem a to se može uraditi na sledeći način:

 # find / -printf «%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%U;%G;%s;%p\n»

Izlaz ove komande su informacije o fajlovima razdvojene sa «;» u formatu koji je kompatibilan sa većinom programa koji rade sa tabelama (npr.

Microsoft Excel)

«755;02/04/2013;14:43:12.0258794640;07/07/2011;07:59:13.3346548330;07/07/2011;07:59:13.3346548330;0;0;4096;/usr/src/linux-headers-2.6.38-8/scripts/basic»

Forenzičar treba da zna da Linux ne poznaje vreme kreiranja fajla, već vreme promene «inoda» poznato kao «ctime» i ono je najbliže vremenu stvaranja (eng. creation time).

Prikupljene informacije treba se koristiti u korelaciji sa dobijenim podacima iz prethodnih postupaka da bi se dobila što potpunija slika o mogućem incidentu odnosno nedozvoljenoj aktivnosti. Na primer, može se desiti da je izlaz komande «lsof» izlistao određene skrivene foldere koji se nisu prikazali u pomenutoj pretrazi (find /), što forenzičaru može biti indicija da se radi o kompromitovanom kernelu. U tom slučaju najbolje je uraditi forenzičku duplikaciju i analizirati skrivene fajlove i foldere. Forenzičar može primetiti kada su fajlovi /etc/passwd i /etc/shadow menjani, što može biti dragocen forenzički podatak jer se odnosi na korisničke naloge i šifre na sistemu. Svi ovi fajlovi su od krucijalnog značaja za bezbednost sistema. Više o ovom fajlu govoriće se u delu o korisničkim nalozima na sistemu.

Prikupljeni podaci mogu ukazati i na prisutvo određenih *perl modula* koji nisu instalirani od strane administratora pa bi forenzički fokus mogao da bude i njihova analiza. Najjednostavniji način izlistavanja perl modula na sistemu je sa alatkom «*instmodsh*»:

instmodsh ova interaktivna komanda ima sledeći izlaz:

Available commands are:
l - List all installed modules
m <module> - Select a module
q - Quit the program
cmd? l
Installed modules are:
Perl
cmd?

Treba naglasiti da bi određeni maliciozni program funkcionisao (pod pretpostavkom da se oslanja na određene perl module) perl moduli ne smeju biti sakriveni već moraju biti vidljivi malicioznom programu.

3.2.13. Postojani podaci od značaja na Linux-u - checksum fajl sistema

Jedan od načina da se proveri *integritet sistemskih fajlova* ili prikupljenog *imidža hard diska* sa ispitivanog računara jeste korišćenje SHA-1 ili *SHA-256 heširanja* nad njima. Prema Wang Xiaoyun sa Beijing's Tsinghua University i Shandong University of Technology postoje tri pravila koja se odnose na forenzička heširanja:[520]

1. Ne može se predvideti heš vrednost fajla ili uređaja;
2. Ne postoji ista heš vrednost za dva različita fajla (u istraživanju kolizije su nastale upotrebom superračunara);
3. Ukoliko se bilo šta promeni u fajlu ili uređaju, heš vrednost se mora promeniti.

SHA-1 i SHA-256 je zamena za MD5 i CRC-32. MD5 se više ne koristi. U MD5 i u SHA-1 su se desile kolizije, odnosno dva različita fajla su imala istu vrednosti. Kolizije su retke međutim i uprkos nedostacima MD5 i SHA-1, oba algoritma za heširanje su korisni za utvrđivanje *integriteta digitalnih dokaza* prikupljenih iz fajlova ili uređaja za skladištenje podataka. Ukoliko se sumnja na koliziju preporuka je da se radi byte-by-byte poređenje da se utvrdi da li su svi bajtovi identični.[521]

Kreiranje heš vrednosti nad svim sistemskim fajlovima sistem administratoru može pomoći pri kasnijem detektovanju izmenjenih fajlova na sistemu i time preventivno delovati na bezbednost postojećeg sistema. Digitalnom forenzičaru je na raspolaganju i heš baza poznatih sistemskih fajlova na NIST sajtu u okviru projekta "National Software Reference Library", koji se mogu uporediti sa prikupljenim fajlovima sa ispitivanog sistema.[522] Time se štedi vreme potrebno za forenzičku istragu, jer pomenuta baza eliminiše poznate sistemske fajlove i uzimaju se u obzir samo oni izmenjeni i nepoznati. Forenzičar može izgraditi sopstven bazu kao na primer bazu malicioznoih programa (poznatih password crackera ili exploita) i uporediti sa fajlovima na ispitivanom računaru. Ukoliko se nađu fajlovi koji se poklapaju to zapravo znači da na sistemu postoji takav maliciozni fajl. Izračunavanje hash vrednosti svih fajlova na Linux sistemu moguće je na sledeći način:

 # find / -xdev -type f -exec sha256sum -b {} \; > svi_fajlovi.sha1

520 Marshall A. M., Digital Forensics - Digital Evidence in Criminal Investigation, JohnWiley & Sons, Ltd 2008.

521 Marković S., *Digitalna forenzika Linux fajl sistema*, master rad, Univerzitet Univerzitet Singidunum, 2010.

522 Http://www.nsrl.nist.gov/, 29.05.2016.

Izlaz ove komande jeste SHA-256 256-bitna hash vrednost i putanja do fajla:

*dc216ac4a4c232815731979db6e494f315b507dd */home/vanja/.bash_logout*

*7a2dd812db7465d93fd0c0567123ef7a4d7c86ed */home/vanja/.bashrc*

*3a08ac3ce95404186b72647d7a88bf18a06acf98 */boot/vmlinuz-2.6.38-8-generic-pae*

*45ba33a6642c9994c2bb09564b4dd2c2224f2ed8 */boot/vmcoreinfo-2.6.38-8-generic-pae*

*fb9eb00af37da053c29e31206a7eb3e13031117b */boot/initrd.img-2.6.38-8-generic-pae*

*352afe195c4484eb80e6f7fef9a377c3d3d72580 */boot/System.map-2.6.38-8-generic-pae*

*86d46047f90cce4984bfd0dbbd7e12cec897c812 */boot/grub/ohci.mod*

Postoji i alatka *sha256deep* kojom se može uraditi SHA-256 heširanje na sistemu:

#sha256deep -r -s /ispitivani_direktorijum > hash_direktorijum.sha256

Ovom alatkom lako se mogu utvrditi razlike u heš vrednostima na sledeći način:

#sha256deep -r -X hash_direktorijum.sha256 /ispitivani_direktorijum

Alatka će imati izlaz samo ukoliko se pronađu razlike u heš vrednostima. Sa stanovišta bezbednosti sistema ova alatka ima veliku upotrebnu vrednost, jer se mogu utvrditi podaci koji su izmenjeni na sistemu.

3.2.14. Postojani podaci od značaja na Linux-u - ulogovani korisnici na sistem

Informacija o tome, koji su korisnici trenutno ulogovani na sistem čuva se u */var/run/utmp*, ali nije u čitljivom obliku već u binarnom. Najbolje je koristiti komandu "w" koja daje sledeći izlaz na sistemu:

 # w

9:38:16 up 1 day, 4:28, 2 users, load average: 0.00, 0.01, 0.12

USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT

root tty1 Sun15 27:46m 0.27s 0.21s bash

root pts/0 zevs.local 11:47 0.00s 1.51s 0.00s w

Ova komanda prikazuje korisnike koji su trenutno ulogovani (na konzoli *tty* ili preko pseudo terminala *pts* na primer ssh, xterm, screen) na Linux sistemu. Moguće je trenutno ulogovane korisnike videti uz pomoć

komande last:

#last -f /var/run/utmp

Problem za forenzičara postoji, ukoliko je napadač pokrenuo određeni program za prikrivanje svoje prave IP-adrese, kojom se prijavio na sistem (npr. određene Antilog skripte).[523] U tom slučaju jedini način da se utvrdi prava IP-adresa je detaljna pretraga nakon dupliciranja hard diska.[524]

3.2.15. Postojani podaci od značaja na Linux-u - istorija logovanja na Linux sistem

Istorija validnih korisničkih prijava i odjava sa Linux sistema čuva se u binarnom fajlu */var/log/wtmp*, a neuspela logovanja na sistem čuvaju se u binarnom fajlu */var/log/btmp*.

Ovaj fajl čuva podatke iz prošlosti o prijavljivanju na sistem, odjavljivanju sa sistema, gašenju sistema i restartovanju sistema sa prikazanim vremenom.

U toku "uživo" forenzičkog ispitivanja ovi podaci se mogu videti alatkama *last* i *lastlog*. Lastlog čuva svoj sadržaj u fajlu /var/log/lastlog.

 # last daje izlaz:
root pts/0 zevs.local Mon Feb 4 20:24 still logged in
reboot system boot 2.6.38-8-generic Mon Feb 4 20:22 - 20:24 (00:02)
root pts/0 zevs.local Mon Feb 4 11:47 - down (08:34)
root pts/0 zevs.local Sun Feb 3 17:11 - 11:01 (17:50)
root pts/0 zevs.local Sun Feb 3 15:54 - 17:06 (01:12)
root pts/0 zevs.local Sun Feb 3 15:09 - 15:53 (00:44)
root tty1 Sun Feb 3 15:08 - down (1+05:13)
root tty1 Sun Feb 3 15:08 - 15:08 (00:00)
reboot system boot 2.6.38-8-generic Sun Feb 3 15:07 - 20:22 (1+05:14)

Ukoliko bi forenzičar hteo da pročita fajl o neuspešnim logovanjima na sistem sa alatima *cat* ili *vi* dobio bi nerazumljiv tekst. Način na koji forenzičar (ili administrator) može doći do podataka koji se odnose na neuspešna logovanja na sistem je sa komadnom *last*:

#last -f /var/log/btmp

523 Http://www.packetstormsecurity.org/UNIX/penetration/log-wipers/, 27.05.2016.
524 Haruyama T., Suzuki H., One-byte Modification for Breaking Memory Forensic Analysis, BlackHat Europe, Mart 2012.

[root@turing ~]# last -f /var/log/btmp
miska ssh:notty localhost Tue Feb 12 18:38 gone - no logout
miska ssh:notty localhost Tue Feb 12 18:38 - 18:38 (00:00)
pera ssh:notty localhost Tue Feb 12 18:34 - 18:34 (00:00)
root ssh:notty localhost Tue Feb 12 18:18 - 18:34 (00:15)
vanja tty1 :0 Tue Feb 12 18:15 gone - no logout

Alatka *lastlog* daje podatke o korisničkom imenu, portu, vremenu poslednje prijave na sistem:

#lastlog

Username	*Port*	*From*	*Latest*
root		*pts/0*	*zevs.local*	*Mon Feb 4 20:24:45 +0100 2013*
daemon				***Never logged in***
bin				***Never logged in***
sys				***Never logged in***
sync				***Never logged in***

Informacije koje forenzičar može otkriti opisanim alatkama su sledeće: koji su korisnici i kada bili prijavljeni (ili su još uvek) na sistem, sa kojom IP-adresom i preko kog terminala. Osim toga može se videti i vreme kada je sistem bio restartovan. Ove informacije mogu pomoći forenzičarima i administratorima, da otkriju da li neko koristi naloge za koje nije ovlašćen. Pažljivom analizom moguće je otkriti malicioznog korisnika i njegovu pravu IP-adresu. Forenzičkom analizom moguće je otkriti *datapipe* alate koji omogućuju radirekciju portova sa namerom zaobilaska firewala na sistemu.[525] Analizom pomenutih fajlova moguće je pravovremeno uočiti određene bezbednosne pretnje i time sprečiti nastanak veće štete, a forenzičarima pružiti dragocene podatke za dalji tok istrage.

3.2.16. Postojani podaci od značaja na Linux-u – logovi na sistemu

Syslog je standard za logovanje na Linux sistemima. Kao što Windows ima svoj event loging mehanizam tako Linux ima svoj sistem za logovanje koji izvršava logove prema određenom tipu. Može se koristi za upravljanje računarskim sistemom, za nadzor bezbednosti na sistemu kao i za pružanje

525 Neke od ovih alata moguće je naći na: http://packetstormsecurity.com/search/files/?q=datapipe, 29.05.2016.

generalnih informacija za analizu i otklanjanje grešaka. Syslog je zapravo centralizovan sistem za praćenje događaja. Ima svoj proces (eng. daemon) koji sluša poruke koje generišu drugi programi (ili serveri na internetu) i skladišti ih prema konfiguracionom fajlu /etc/syslog.conf odnosno /etc/rsyslog.conf.[526] Ono što je važno za forenzičara je da su u ovom konfiguracionom fajlu opisani *podsistemi*, koji generišu poruke za logovanje i putanje do fajla u kome će se te poruke smestiti. Podsistemi su sledeći: auth i authpriv (odnosi se na proveru sigurnosnih događaja i proveru identiteta), cron (odnosi se na raspored poslova na sistemu), daemon (odnosi se na servise odnosno daemon procese na sistemu), kern (odnosi se na informacije iz kernela tj. jezgra sistema), lpr (odnosi se na podsistem za štampanje), mail (odnosi se na podsistem za elektronsku poštu), news (odnosi se na podsistem za vesti), sysloguser (odnosi se na interne poruke), uucp (odnosi se na komunikacioni podsistem Unix to unix) i od local0 do local7 (za lokalnu upotrebu).

Format svakog reda u okviru konfiguracionog fajla syslog.conf je:

izvor_poruke.prioritet[;izvor_poruke.prioritet][TAB][putanja do log fajla]

Vrednosti prioriteta moguće su sledeće:

- *debug, info* - spadaju poruke informacionog karaktera (ne zahtevaju dodatne akcije od strane administratora);
- *notice* - spadaju poruke sa većim značajem i nisu u pitanju greške (ne zahtevaju hitno reagovanje, ali ih treba pratiti);
- *warning* - ne predstavljaju greške, ali ukazuju da greška može da nastane ukoliko se određena akcija ne preduzme (npr. kada je zauzeće fajl sistema prešlo 90%);
- *error i critial* - poruke koje zahtevaju hitnu intervenciju administratora (npr. prekid mrežne konekcije);
- *emmerg* - poruke o greškama koje mogu dovesti do prestanka rada celog sistema (osim preduzimanja administratorskih intervencija, obaveštava se i tehničko osoblje).

Na primer, ukoliko u konfiguracionom fajlu stoji *.info;mail.none, znači da će sistem logovati sve osim onoga što stoji uz none. U ovom slučaju znači da se ne loguju informacije o mailu.

Tu se nalaze sledeće važne putanje do log fajlova:

- */var/log/messages* - pokazuje globalne sistemske informacije. Od značaja je za bezbednost jer prikazuje informacije o uspešnoj autentifikaciji komande *sudo*, koja pruža sveobuhvatne audit

526 U zavisnosti od Linux distribucije i verzije /etc/syslog.conf je kod RedHat-a 5, dok je kod RedHata 6, CentOS-a, Debiana i njegovih derivata kao što su Ubuntu i Kubuntu sistem konfiguracija sistema za logovanje nalazi se u /etc/rsyslog.conf.

informacije. Sudo komanda omogućava korisniku sa sudo privilegijama da izvrši komandu u ime root-a ili nekog drugog korisnika. Sudo konfiguracioni fajl se nalazi "/etc/sudoers". Po difoltu korišćenje sudo komande zahteva autentifikovanje korisnika sa sopstvenom šifrom (ne root šifra). Nakon uspešne autentifikacije, ažuriraju se vremenski pečati i korisnik može koristiti sudo komandu bez šifre u kratkom periodu (5 minuta po difoltu), odnosno onoliko koliko se definiše u konfiguracionom "/etc/sudoers" fajlu.

- */var/log/secure* - prikazuje informacije o proveri identiteta upućenih na mrežne servise OS, kao i informacije o korisniku koji je koristio komandu "su" (eng. substitute user), kako bi na najjednostavniji način promenio vlasništvo trenutne (ulogovane) sesije u root ili nekog drugog korisnika.[527] Ovde se mogu pronaći dragocene informacije, kako o korisnicima koji su izvršili "sudo" komande, tako i nazivi samih komandi. Sa stanovišta bezbednosti je preporučljivo da se od administratora zahteva korišćenje sudo-a, pre upotrebe određene komande. Time se omogućava i proaktivna zaštita od neprikladnih i neovlašćenih aktivnosti. SUDO konfiguracioni fajl treba adekvatno podesiti, kako i sami administratori ne bi zaobišli odgovornost i sistem za analizu logova (kao npr. definisanje određenih komandi i šelova koje smeju da koriste).
- */var/log/maillog* - pokazuje informacije koje se odnose na mail server.
- */var/log/cron/* - pokazuje informacije o stanju raspoređenih poslova (eng. scheduled task).
- */var/log/spooler* - pokazuje događaje koji se odnose na servise UUCP ili NNTP.
- /*var/log/boot.log* - prikazuje informacije koje se prikazuju na ekranu pri podizanju sistema.

Informacije od značaja koje forenzičar može pronaći se mogu podeliti u nekoliko grupa:

1. *uspešna korisnička logovanja* - mogu se pronaći u log fajlovima pod nazivima "Accepted password", "Accepted publickey", „session

527 Korišćenjem komande "su" se na više korisničkih sistemima osvaruje veća bezbednost, kada je u pitanju upravljanje sistemom od strane administratora. U praksi to znači da postoji mnogo manji potencijal za slučajne ili zlonamerne štete, jer se administrator na sistem može prijaviti kao običan korisnik (koji ima ograničene sistemske privilegije) i obavljati rutinske poslove, koji ne zahtevaju root privilegije. U slučaju kada je potrebno korišćenje root privilegija sa komandom "su" može se prebaciti na root nalog.

opened";
2. *neuspešna korisnička logovanja* - mogu se pronaći u log fajlovima pod nazivima "authentication failure", "failed password";
3. *odjajvljivanje korisnika sa sistema* - može se pronaći pod nazivom "session closed";
4. *izmena korisničkog naloga ili brisanje* - može se pronaći u log fajlovima pod nazivima "password changed", "new user", "delete user";
5. *upotreba SUDO komandi* - može se pronaći u log fajlovima pod nazivima "sudo: … COMMAND=…","FAILED su";
6. *otkazivanje servisa* - može se pronaći pod nazivima „service failed" ili „service failure".

Sve prethodno opisani fajlove, koji mogu sadržati pomenute dragocene podatke za forenzičku istragu potrebno je prebaciti alatkom „*netcat*" ili „*cryptcat*" na forenzičku radnu stanicu za dalju analizu. Ovi fajlovi su veoma značajni kako forenzičaru tako i administratoru sistema za kontrolu bezbednosti.

Treba znati da se generisani *syslog log* sastoji od 5 polja (datum, vreme, ime računara, proces koji je inicirao događaj sa ID procesa i poruka). Na osnovu ispitivanja ovih fajlova moguće je ustanoviti određene incidentne/nedozvoljene aktivnosti (upad u sistem preko određenih exploita nad ranjivim servisima, neovlšćeno korišćenje tuđeg naloga, DoS napadi). S obzirom da ovi logovi mogu sadržati dragocene dokaze i sami mogu biti meta napada. Na primer, DoS napadom moguće je onesposobiti syslog server tako da se hard disk prepuni logovima (100% zauzeća), da više ne vrši funkciju logovanja.

Jedan od načina na koji administrator može zaštititi syslog server je: kroz njegovo izdvajanje na posebnu privatnu mrežu u okviru postojeće mreže, kreiranje firewall-a sa dozvolama za pristupanje serveru samo onih računarskih sistema koje je potrebno pratiti kao i izdvajanja log fajlova na posebne fajl sisteme odnosno particije. Dodatno je potrebno postaviti okidače (eng. triggers) nad logovima sa automatskim slanjem maila administratoru u slučaju da je ispunjen trigger kriterijum. Jedan takav alat jeste *Swatch*.[528]

Za povećanje proaktivne zaštite u cilju praćenja izvršenih komandi na sistemu preporučljivo je pokretanje *"Accton"* servisa. Razlog je, što će nakon upada na sistem zlonamerni napadač pokušati da ukloni dokaze izvršenja komandi i to uglavnom brisanjem bash_history fajla. Međutim, moguće je uključiti na sistemu proces praćenja svih izvršenih komandi, čime se omogućava uvid u svaku izvršenu komandu uključujući njen uticaj na CPU

528 Simple Log Watcher, http://sourceforge.net/projects/swatch/, 28.05.2016.

i na memoriju. Time će se omogućiti praćenje svih izvršenih komandi na računaru, kao i vreme izvršenja od strane korisnika. Potrebno je instalirati paket *Psacct* koji sadrži nekoliko alata za praćenje aktivnosti i to su:

ac (prikazuje koliko su vremena korisnici na sistemu logovani);

lastcomm (prikazuje informacije o prethodno izvršenim komandama, a podrazumeva se da je accton omogućen kao servis);

acct (uključuje ili isključuje servis za praćenje komandi);

sa (sumira informacije o prethodno izvršenim komandama, a podrazmeva se da je omogućen accton servis).

Acct servis se na Debianu i Ubuntu Linux sistemima startuje automatski po difoltu, dok je kod Red Hata, Fedore i Centos sistema potrebno ručno pokrenuti servis.

3.2.17. Postojani podaci od značaja na Linux-u – TCP Wrappers

TCP Wrappers predstavlja program, koji se obavija oko TCP-a i ima ulogu poboljšanja zaštite. Bez TCP Wrapper-a, povezivanje na određeni port izvodilo bi se bez ikakve zaštite, tako što bi inetd pronalazio port i odgovarajući servis bi se pokrenuo. Koncept sa TCP Wrapper-om podrazumeva da se prilikom uspostavljanja veze sa portom poziva poseban program (tcpd), koji može da izvrši određene provere pre pozivanja pravog „daemon-a". Wrapper na sistemu može da kontroliše pristup TCP i UDP servisima. Provere koje TCP Wrapper obavlja, a koje forenzičaru mogu biti od pomoći prilikom ispitivanja zlonamernih aktivnosti su sledeće:

- vrši logovanje svih zahteva uz pomoć syslog-a (što može pomoći forenzičaru da se vidi sa kojim je portom uspostavljena veza na sistemu);
- izvršava „double reverse DNS lookup" za proveru izvorne adrese;
- vrši proveru zahteva u odnosu na /etc/hosts.allow i /etc/hosts. deny fajlove i ukoliko zahtev bude odobren, dozvoljava se pristup (forenzičaru može pomoći oko ispitivanja zlonamernog napada na system, kao i uspostavljanju veće zaštite na sistemu).

Treba naglasiti da je za dobru zaštitu sistema (bilo da je reč organizaciji ili kućnim računarima), važan stav po kome je sve zabranjeno osim onog što je eksplicitno dozvoljeno. To znači da bi u fajlu /etc/hosts. deny bio zabranjen sav saobraćaj dok bi u /etc/hosts.allow eksplicitno bio dozvoljen onaj potreban.

Na primer, izvod iz loga /var/log/messages na RED HAT Enterprise Linux OS:

- *Oct 23 22:15:35 toledo sshd[14558]: ROOT LOGIN REFUSED FROM xxx.xxx.15.133*, može pružiti korisne informacije kao što su: vreme i datum pokušaja prijavljivanja na sistem, ime računarskog sistema (domaćina), servis (ssh) i korisnički nalog sa kojim je pokušana prijava i IP-adresa sa koje je pokušana prijava.

Drugi primer u kome je snimljeno uspešno povezivanje servisa:

- *Sep 16 21:36:29 toledo in.tftpd[614]: connect from xxx.xxx.15.133*

Ovaj zapis iz /var/log/messages ukazuje da je računar sa IP-adresom xxx.xxx.15.133 povezan na TFTP servis ispitivanog računara. Na osnovu ovih logova forenzičar može utvrditi korelaciju između dobijanja pristupa računarskom sistemu i pristupu određenim fajlovima na njemu.

3.2.18. Postojani podaci od značaja na Linux-u - korisnički nalozi

Spisak korisnika, koji postoje na sistemu nalazi se u fajlu */etc/passwd* fajlu. Forenzičkim ispitivanjem može se utvrditi, koji je nalog kompromitovan na sistemu odnosno pridodat za kompromitovanje sistema.

Izgled /etc/passwd fajla na sistemu:

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
vanja:x:1000:1000:vanja korac,,,:/home/vanja:/bin/bash

Forenzičar treba da obrati pažnju na korisnike sa ID userom i grupom "'0" i mestom za njihov home. Ukoliko postoji korisnik u fajlu /etc/passwd:

sumnjivi_korisnik:x:0:0:vanja korac,,,:/:/bin/bash, to znači da sumnjivi_ korisnik ima root privilegije na sistemu, što je administratoru znak za uzbunu a digitalnom forenzičaru dragoceni podatak za dalji tok istrage.

3.2.19. Postojani podaci od značaja na Linux-u - korisnički fajl sa istorijom izvršenih komandi

Korisnički fajlovi sa istorijom izvršenih komandi vrlo su značajni forenzički podaci, jer mogu pružiti dragocene dokaze o načinu komprimitovanja kako samog sistema tako i drugih sistema. Drugim rečima, daju podatke o upotrebljenoj hakerskoj metodologiji. Bash šel istorija izvršenih komandi se nalazi u fajlu *.bash_history.* Forenzičar može pronaći postojeće .bash_history fajlove na sledeći način:

 # find / -type f -name .bash_history

3.2.20. Postojani podaci od značaja na Linux-u - fajlovi sa SUID, SGID, sticky bitovi i prava nad fajlovima

Prava pristupa fajlovima i folderama na Linux sistemu definisana su setom dozvola. Ove dozvole ukazuju programu o pravima pristupa korisnika ili grupe određenom folderu ili fajlu. Setom je definisano da li program, proces ili korisnik može pristupiti određenom fajlu ili folderu. Postoje tri tipa pristupanju fajla odnosno folderu "r" (odnosi se na čitanje fajla ili izlistavanje direktorijuma), "w" (odnosi se na upisivanje u fajl odnosno direktorijum), "x" (odnosi se na izvršavanje fajla odnosno prolaz kroz direktorijum), za tri različite grupe u, g, o (korisnik odnosno vlasnik fajla eng. user "u", grupa eng .group "g" i ostali eng. other "o").

Pored pomenutih standardnih prava pristupa fajlovima i folderima (prava čitanja eng. read, pravo upisa eng. write, pravo izvršenja eng. execute) na Linux sistemima mogu postojati i *specijalna prava pristupa*. Ona se određuju posebnim bitovima: *SUID bit, SGID bit i Sticky bit.*

Kada se izvršni fajl pokrene on radi u vlasništvu korisnika koji je inicirao izvršenje. To znači da ukoliko je korisnik "test" pokrenuo komandu "ls" odgovarajući proces će se pokrenuti u vlasništvu korisnika "test".

SUID bit (Set User ID bit), menja ovo ponašanje na sledeći način. Ukoliko je *SUID bit* postavljen na određeni program (izvršni fajl) to znači da će se taj program pokrenuti u ime vlasništva fajla bez obzira na to ko fajl pokreće. Na primer, ukoliko je korisnik "test" pokrenuo program "demo", čiji je vlasnik korisnik root, program će se pokrenuti u ime korisnika "root" (pod uslovom da je podešen *SUID bit*). Ovaj koncept je koristan u administraciji aplikacija/spkripti, da bi se dozvolilo određenim aplikacijama/skriptama koje su pod root vlasništvom da mogu biti izvršene od strane korisnika. Koncept

podrazumeva i izvršenje na ovakav način samo nad skriptama, čije je izvršenje u potpunosti poznato. To znači da iako je korisniku dozvoljeno da izvrši ove skripte odnosno programe kao root, korisnici mogu da sa njima urade jedino ono za šta su ovi programi odnosno skripte dizajnirani da urade. Na primer, ukoliko je skripta dizajnirana tako da se vrši bekapovanje odnosno kopiranje 10 fajlova sa jednog mesta na drugo, korisnik bi imao samo pravo da izvrši ovaj scenario, a ne i da izvrši bilo kakvu promenu nad skriptom (jer nema prava upisa). Ovo je odlično rešenje, da se omogući korisnicima da se izvedu važni bekapi koristeći skriptu, koja ima samo određenu namenu podešenu sa *SUID* odnosno *SGID* bitom. Međutim ovo može predstavljati i potencijalni bezbednosni rizik. S obzirom da se skripta sa *SUID bit*-om izvršava u ime root-a postoji opasnost od zlopotrebe. Maliciozni korisnik može proslediti određene parametre toj skripti i zloupotrebiti ih, što može dovesti do činjenja velike štete na sistemu. Preporuka je da se broj fajlova sa SUID privilegijama na sistemu svedu na minimum, a da administratori budu svesni koji su to fajlovi i da oni budu dobro čuvani.

SGID bit može da se podešava na fajlovima i na folderima, ali sa različitim značenjem. Ukoliko se *SGID bit* upotrebljava nad *fajlovima*, ti fajlovi se izvršavaju u ime vlasnika grupe pokrenutog fajla bez obzira ko je izvršio pokretanje fajla. *SGID bit* setovan na *direktorijumu* koristi se za kreiranje zajedničkih direktorijuma u okviru rada na zajedničkom projektu. Na primer, više korisnika jednog projekta rade zajedno i svi pripadaju grupi "*projekat*". Preptostavimo da se zajednički folder zove "*projekatIII400*". Zahtev je da se u toku trajanja projekta moraju deliti međusobno fajlovi i svi moraju imati uvid u sve kreirane fajlove. Ovo se može jednostavno uraditi obezbeđivanjem dozvola za čitanje na nivou grupe. Problem nastaje prilikom kreiranja fajla, jer će on pripadati primarnoj grupi korisnika, koji je kreirao fajl. To znači da kada različiti korisnici budu kreirali njihove fajlove u folderu "*projekatIII400*" ovi fajlovi neće imati vlasništvo grupe "*projekat*". Da bi se ovaj problem prevazišao, folder "*projekatIII400*" se setuje sa vlasništvom grupe "projekat" i podešava mu se specijalno pravo prostupa odnosno *SGID bit*. To znači da kada korisnici u ovom folderu budu kreirali fajlove i foldere svi oni će pripadati grupi "*projekat*".

Sticky bit se odnosi samo na direktorijume. Ukoliko korisnik želi da kreira ili obriše fajl odnosno direktorijum u nekom direktorijumu za to mu je potrebno pravo upisa nad tim direktorijumom. Na primer, privremeni direktorijum /tmp predstavlja direktorijum za privremeno smeštanje fajlova i direktorijuma. Da bi svi korisnici u njemu mogli da kreiranju i brišu

privremene fajlove on mora da bude podešen tako da dopušta sva prava (čitanje, upis, izvršenje) na sva tri nivoa (vlasnik, grupa, ostali). Problem će nastati, ukoliko svi korisnici imaju pravo upisa nad /tmp direktorijumom, pošto to znači da oni mogu i izbrisati bilo koji fajl u tom direktorijumu, a ne samo svoj. Ovaj problem se rešava podešavanjem specijalnog prava *Sticky bit*-a nad direktorijumu (npr. /tmp), čime se omogućava da svako može da kreira fajl u njemu, ali korisnik može obrisati samo onaj fajl koji je u njegovom vlasništvu. Fajlovi koji nisu u vlasništvu korisnika, korisnik ne može obrisati.

Prema tome otkrivanje svih izvršnih fajlova na sistemu, koji mogu biti pokrenuti u ime drugog korisnika, naročito onih sa root privilegijama, su kritični za bezbednost sistema i vrlo važni kada je forenzička istraga u pitanju. Digitalni forenzičar može pronaći upravo one fajlove koji su zloupotrebljeni na sistemu od strane malicioznog korisnika.

Dozvole nad fajlovima kao što je rečeno koriste se za kontrolu pristupa resursima. *Prava pristupa* definišu se sa četiri oktalne cifre. Odnos bitova svake oktalne cifre i prava pristupa može se predstaviti na sledeći način:

Prava pristupa:		Brojčana vrednost
SUID, r	=	4
SGID, w	=	2
Sticky, x	=	1

Prve tri oktalne cifre se odnose na specijalna prava pristupa (SUID, SGID, Sticky) a ostale se odnose na prava pristupa određenih kategorija korisnika (vlasnik-korisnik, grupa, ostali).

Na primer:

rwxr--r-- = 744

rwsr-xr-x = 4755 (SUID bit setovan)

rwxr-sr-x = 2755 (SGID bit setovan)

rwxrwxrwt = 1777 (Sticky bit setovan)

Pravilnim podešavanjem prava pristupa moguće je ograničiti pristup određenim informacijama. Ukoliko prava nisu ispravno podešena svako ko pristupi sistemu moći će da radi šta hoće na njemu.

U nastavku biće prikazani načini pronalaženja fajlova koji imaju podešena specijalna prava pristupa i oni koji mogu biti od značaja za digitalnog forenzičara.

Pronalaženje svih fajlova pod root vlasništvom sa podešenim SUID bit-om:

#find / -user root -perm -4000 -print

Pronalaženje svih fajlova pod root vlasništvom sa podešenim SGID bit-om

#find / -group root -perm -2000 -print

Pronalaženje svih fajlova pod root vlasništvom sa podešenim Sticky bit-om

#find / -group root -perm -1000 -print

Pronalaženje svih fajlova sa podešenim SUID i SGID bit-om

#find / -type f \(-perm +4000 -o -perm +2000 \) -exec ls -l {} \; 2>/dev/null

ili

 # find / -perm +6000 -type f -exec ls -ld {} \;

Pronalaženje svih fajlova bez vlasništva (mogući iskopirani maliciozni programi):

#find / -nouser -print

Pronalaženje svih fajlova bez grupe (mogući iskopirani maliciozni programi):

#find / -nogroup -print

Pronalaženje svih simboličkih linkova na sistemu i mesta na koja ukazuju:

#find / -type l -ls

Sve navedene komande imaju za cilj pronalaženja niza fajlova koji mogu biti predmet detaljne forenzičke i bezbednosne analize. Iz navedenog proizlazi da bi ključne informacije bile pravilno zaštićene, veoma je važno pravilno razumeti upotrebu kako dozvola nad datotekama tako i specijalnih prava pristupa.

3.2.21. Postojani podaci od značaja na Linux-u - sumnjivi fajlovi

Ukoliko se forenzičko ispitivanje radi samo "uživo", sumnjive fajlove moguće je prebaciti na forenzičku radnu stanicu koristeći alat *netcat*.

Na forenzičkom radnoj stanici pokreće se:

#cryptcat -v -l -p 9898 > ime_sumnjivog_fajla

Na ispitivanom računaru pokreće se:

#cat ime_sumnjivog_fajla | cryptcat IP_adresa_Forenzickog_racunara 9898

U slučaju da se radi o kompromitovanom kernelu, potrebno je uraditi i forenzičku duplikaciju da bi forenzičar bio siguran da alati koje bude upotrebio neće biti kompromitovani. Specifičnost kod Linuxa u odnosu na Windows je kod izvršnih fajlova. U Windows OS izvršni fajl je zaključan i

ne može biti obrisan dok se izvršava u memoriji, što predstavlja benefit za forenzičku istragu. Kod Linux OS, nakon pokretanja malicioznog fajla (npr. spomenutog pipe programa koji služi za redirekciju portova), moguće je obrisati binarni fajl.

To za istragu znači sledeće: ako se računar isključi biće izgubljen fajl, koji se nalazio u memoriji i neće više biti mogućnosti za njegovu kasniju analizu. Folder "/*proc*" može pomoći forenzičaru da se to ne bi desilo. Ovaj folder se ne nalazi na hard disku, već u memoriji. Njegov sadržaj upućuje na startovane procese i druge informacije o sistemu.

Folderi imenovani brojevima ukazuju na ID startovanog procesa u memoriji. Ovaj podatak može biti dragocen, ukoliko je forenzičar ustanovio o kom malicioznom procesu se radi. U tom folderu nalazi se i podfolder „*fd*", koji sadrži sve otvorene fajlove koji se odnose na taj maliciozni proces. Na primer, zlonamerni korisnk je upotrebio alat sniffer za prikupljanje šifara na sistemu, alat je startovao proces sa ID 666. To znači da će forenzičar dokaze moći u folderu „*/proc/666*" i u folderu „*/proc/666/fd*" da nađe reference, koje ukazuju na fajlove otvarane od alata sniffera i fajl u kome su se smeštale prikupljane šifre.

Forenzički odgovor „uživo" ne može dati adekvatne rezultate, ali može barem dati dobru predstavu tome šta se desilo. Dodatne analize moguće je uraditi mrežnom forenzikom, a kasnije forenzičkom duplikacijom, post-mortem forenzikom (analiza fajlova: slika, audio video fajlova, arhiva i dokumenta).

3.3. SOFTVERSKI FORENZIČKI ALATI ZA INICIJALNI ODGOVOR I ALATI ZA OPORAVAK PODATAKA I PARTICIJA

3.3.1 Alati inicijalnog odgovora za Windows sisteme

Forenzički inicijalni odgovor potrebno je da realizuje stručna osoba ili tim koji prvi dolazi na scenu nedozvoljene/incidentne aktivnosti. Tom prilikom se vrši analiza i prikupljaju informacije o aktivnosti koja je identifikovana ili koja je izvršena. Najčešće osobe koje realizuju forenzički inicijalni odgovor su sistem administratori, mrežni administratori i oni su u organizaciji vrlo značajni kako za prenošenje „svesti o bezbednosti", tako i za poznavanje procedura forenzičke istrage, jer oni moraju očuvati digitalni dokaz na licu mesta. Svaka akcija koja se uradi, može da ugrozi integritet digitalnog dokaza.

First responder Toolkit mora da sadrži: [529] [530] [531]

- Alate za dokumentaciju – kamere, tagovi za kablove, stikeri, notepad, notepad++ alatke za prikazivanje koda pythona i C koda u različitim poljima za identifikovanje funkcija, klasa, promenljivih, konstanti itd;

- Alate za demontažu i rastavljanje uređaja – odvrtači, klješta, sekač za žicu;

- Pribor za pakovanje i transport antistatik vrećice, vezice za kablove, torbe za originalne dokaze, trake za dokaze, čvrste kutije;

- Ostali alati – rukavice, lupa, papir za štampanje, floppy disk;

- Prenosni računar sa programskim i hardverskim alatima sa konektorima i write blokerima.

- Uređaj za neprekidno napajanje na koji bi ispitivani uređaj mogao biti povezan kako ne bi prestajao sa radom prilikom transporta do forenzičke laboratorije ukoliko je to neophodno;

- Komplet osnovnih alata za inicijalni odgovor.

Tabela 9. Forenzički alati za inicijalni odgovor na Windows sistemima

Ime alata	Namena	Izvor
date i time	Prikazuje datum i vreme na sistemu	Implementirano u Windows OS
cmd.exe	Komandno okruženje za Windows OS NT/2000/2003//2008/ XP/Vista/7	Implementirano u Windows OS
psloggedon	Alat koji prikazuje sve povezane korisnike na sistem (lokalne i one koji koriste deljene resurse)	Dolazi u sklopu pstools-a i dostupno je na: http://technet. microsoft. com/en-us/ sysinternals/ bb896649_

529 Mane Piperevski, Workshop ICT Forensics Investigation – module 1, Piperevski & Associates, Beograd 2016.
530 EC-Council press, Computer forensics Investigation procedures and response, Cengage Learning, USA, 2010. Chapter4 pp 4-4 - 4-5
531 CHFI Module V - First Responder Procedures, EC-Council, http://www.s lideshare. net/ desmond. devendran/file000118, 22.07.2016.

logonsessions	Alat koji prikazuje detalje u vezi sa postojećim sesijama, tip autentifikacije, aktivne procese i tip logovanja korisnika na sistem	Dostupno na: http://technet.microsoft.com/en-us/sysinternals/bb896769.aspx
net session	Prikazuje ime udaljenog korisnika, koji koristi deljene resurse i IP-adresu. Da bi komanda radila mora je koristiti korisnik sa administratorskim pravima	Implementirano u Windows OS
net accounts	Daje prikaz postavki naloga	Implementirano u OS
net file	Daje prikaz otvorenih fajlova od strane udaljenih korinsika	Implementirano u OS
net share	Daje prikaz lokalno deljenih resursa dostupnih na mreži	Implementirano u OS
net start	Prikazuje spisak servisa I njihove statuse	Implementirano u OS
net use	Prikazuje udaljene deljene resurse sa kojima je sistem trenutno povezan	Implementirano u OS
net user	Daje spisak svih korisničkih naloga	Implementirano u OS
net view	Daje prikaz računara u lokalnom domenu	Implementirano u OS
Route print	Daje prikaz ruting tabele na lokalnom sistemu	Implementirano u OS
Netusers	Prikazuje detalje vezane za poslednje vreme logovanja korisnika na sistem	Dostupno je na: http://www.systemtools.com/cgi-bin/download.pl?NetUsers
rasusers	Prikazuje listu korisnika na domenu ili lokalno na server koji imaju privilegije udaljenog pristupa preko Routing and Remote Access-a na server	Sastvani je deo Resource Kit utility-a za servere NT, 2000, 2003, 2008
netstat -anr	Izlistava sve aktivne portove TCP i UDP (koji su u režimu slušanja) i trenutne konekcije sa tim portovima	Implementirano u OS
fport	Izlistava sve otvorene TCP/IP I UDP i mapira ih prema aplikaciji koja je vlasnik tog porta. Služi za brzo identifikovanje nepoznatih otvorenih portova i aplikaciju koja je povezana sa tim portom	Kompatibilna je sa Windows NT/2000/XP http://www.mcafee.com/us/downloads/free-tools/fport.aspx
Pslist	Izlistava i daje detaljan opis svih startovanih procesa na sistemu	Dolazi u sklopu pstools-a: http://technet.microsoft.com/en-us/sysinternals/bb896649

ListDLLs	Izlistava sve DLL biblioteke koje su učitane u procese u sistemu. Alat omogućava listanje svih dll biblioteka u svim procesima, samo u određenom procesu ili lista procese sa određenom dll bibliotekom	http://technet.microsoft.com/en-us/sysinternals/bb896656
nbtstat –c	Svaki računar koji je konfigurisan sa Netbios-om dodeljuje mu se jedinstveno ime sa kojim komunicira sa ostalim računarima u mreži. Daje informacije o statistici NetBt protokola, lokalnu i udaljenu tabelu sa NetBios imenima i keširana Netbios imena koja traju samo određeni period npr 10 minuta. Te informacije pripadaju nestabilnim (eng. volatile) podacima. Ovim alatom mogu se prikupiti informacije iz keša, koje mogu pokazati konekcije koje su postojale na ispitivanoj mašini. Sa parametrom -c prikazuje trenutni NetBIOS keš koji sadrži imena udaljenih računara i IP-adrese	Implementirano u Windows OS
arp –a	Mapira MAC adrese u IP-adrese sistema sa kojima ima komunikaciju	Implementirano u Windows OS
At	Daje prikaz odloženih komandi ili operacija na sistemu koje treba da se izvrše	Implementirano u OS
kill	Prekida proces	Sastvani je deo Resource Kit utility-a za servere NT, 2000, 2003, 2008
md5sum.exe	Kreira MD5 heš vrednost za određeni fajl	Win9x/ME/NT/2000/XP/Vista/7 http://www.pc-tools.net/win32/md5sums/
sha256sum.rexe	Kreira SHA256 heš vrednost za određeni fajl	http://www.labtestproject.com/files/win/sha256sum/sha256sum.exe
Rmtshare	Može prikazati i kreirati deljene foldere na udaljenom računaru	Sastvani je deo Resource Kit utility-a za servere NT, 2000, 2003, 2008 ali nije kompatibilan sa njihovim x64 bitnim verzijama
nc.exe	Netcat obezbeđuje kanal za komunikaciju između dva sistema	http://netcat.sourceforge.net/, http://www.downloadnetcat.com/, http://nmap.org/ncat/
cryptcat	Obezbeđuje šifrovan kanal za komunikaciju između dva sistema	http://sourceforge.net/projects/cryptcat/files/

PsLogList	Iščitava sadržaj iz event loga	Dolazi u sklopu pstools-a: http://technet.microsoft.com/en-us/sysinternals/bb896649
Ipconfig	Prikazuje konfiguracione informacije postojećih interfejsa na sistemu	Implementirano u OS
PsInfo	Prikazuje informacije o lokalnom sistemu	Dolazi u sklopu pstools-a: http://technet.microsoft.com/en-us/sysinternals/bb896649
PsFile	Prikazuje fajlove koji su otvoreni sa udaljenog sistema	Dolazi u sklopu pstools-a: http://technet.microsoft.com/en-us/sysinternals/bb896649
PsService	Prikazuje status konfiguraciju i zavisnost od nekog servisa (procesa) i omogućava kontrolu servisa (startovanje, stopiranje, pauziranje i restartovanje)	Dolazi u sklopu pstools-a: http://technet.microsoft.com/en-us/sysinternals/bb896649
Volume_dump.exe	Alatka za prikupljanje informacija o drajvovima na sistemu i prikazuje USN journals informacije	Dolazi u sklopu Forensic Acquisition Utilities (FAU) paketa dostupnog na: http://gmgsystemsinc.com/fau/03ddecb5-8262-4022-aaff-6559424ff8fc/fau-1.3.0.2390a.zip
dd.exe	Linux alatka prilagođena za Windows čiji je autor George Garner. Svrha ovog programa jeste konverzija i kopiranje fajlova (kopira zadati ulazni fajl u određeni izlazni fajl uz moguće konverzije)	Dolazi u sklopu Forensic Acquisition Utilities (FAU) paketa dostupnog na: http://gmgsystemsinc.com/fau/03ddecb5-8262-4022-aaff-6559424ff8fc/fau-1.3.0.2390a.zip

Ntlast	Prikazuje informacije iz bezbednosnih logova na sistemu	Dostupno na http://www.mcafee.com/us/downloads/free-tools/ntlast.aspx
auditpol	Ovaj alat može da prikazuje i vrši izmenu trenutnih sistemskih i korisničkih bezbednosnih postavki	Sastvani je deo Resource Kit utility-a za servere NT, 2000, 2003, 2008 ali nije kompatibilan sa njihovim x64 bitnim verzijama
doskey	Prikazuje listu izvršenih komandi na sistemu u okviru cmd.exe shella	Implementirano u OS
Uptime	Prikazuje vreme neprekidnog rada računarskog sistema	http://support.microsoft.com/kb/232243
Pwdump6	Dump heš vrednosti iz SAM baze sa ciljem oporavka šifri	http://www.foofus.net/~fizzgig/pwdump/
Dumpel	Dump logova na NT i Win 2000	Sastvani je deo Resource Kit utility-a za servere NT, 2000

3.3.2. Windows alati za oporavak podataka

Prilikom forenzičke istrage računarskih sistema forenzičari se vrlo često susreću sa zaključanim sistemima za koje nemaju ulazne kredencijale. Postoje različiti načini ulaska na računar zlonamernog napadača koji je obezbeđen šifrom a jedan od njih biće izložen u tekstu koji sledi.

Prvo se utvrdi koja je verzija operativnog sistema i za nju se obezbedi instalacioni disk (na primer OS Windows 7 pro x64). Potom se pokreće računar sa instalacionog diska i odabere opcija *Repair Your Computer*. Sledeći ekran koji će se pojaviti prikazaće listu postojećih operativnih sistema i slovo koje mu je dodeljeno (njega zapamtiti ili zapisati). U sledećem ekranu treba odabrati od ponuđenih opcija *command prompt* i pokrenuti alatku *regedit*. U samom Registry-ju treba odabrati kategoriju HKEY_LOCAL_MACHINE i kroz *File* tab pod opcijom *Load Hive* učitati *„E:\Windows\System32\config*" i odabrati Registry repozitorijum Software. Potom se odabere ime za *Key* name: *testiranje* na Load hive prozoru. Nakon uspešnog unosa ime testiranje pojaviće se pod :
HKEY_LOCAL_MACHINE\testiranje\Microsoft\Windows\NT\

CurrentVersion\Image File Execution Options
Desnim klikom na *Image File Execution Options* treba odabrati *New-Key* i upisati „*utilman.exe*“
Desnim klikom na „*utilman.exe*“ treba odabrati dodavanje *New-String* vrednosti sa imenom *Debugger*
Desnim klikom na *Debugger* treba odabrati izmenu i uneti u polje za vrednost (Value Data) *cmd.exe*
Nakon toga se restartuje operativni sistem kome ne znamo šifru. Klikom na *easy of access* dobija se command prompt i možemo promeniti administratorsku šifru.
C:\Windows\system32>net user testiranje testiranje /add
The command completed successfully.
C:\Windows\system32>net localgroup Administrators testiranje /add
The command completed successfully.
U većini slučajeva forenzičaru je značajnije dobijanje pristupa i otkrivanje šifri naloga koji se nalaze na sistemu od same promene šifre. To se radi uz pomoć powershell skripti sa kojom je moguće uraditi dump heševa šifri postojećih naloga iz SAM database i posebnih alata za dekriptovanje heševa. Upotrebom Nishang powershel skripti jedan je od načina prikupljanja heš vrednosti šifri postojećih korisnika na sistemu.
C:\Windows\system32>powershell (ulazak u powershell okruženje)
PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned (postavljanje polise da skripte mogu da se izvrše)
PS H:\nishang> Import-Module .\nishang.psm1 (importovanje nishang modula)
PS H:\nishang> . .\Gather\Get-PassHashes.ps1 (učitavanje skripte)
PS H:\nishang> Get-PassHashes (dobijanje NTLM heš vrednosti šifre)
Administrator:500:aad3b435b54404eeaad3b435b51404ee:31d6cfe0d16ae931b73c58d7e0c089c0:::
Guest:501:aad3b435b51404e3aad3b435b51404ee:31d6cfe0d165e931b73c59d7e0c089c0:::
marwin:1000:aad3b435b51404e6aad3b435b51404ee:b48dd2d80629860d7b6e0689508ca0ed:::
vanja:1001:aad3b435b51404eeaa73b435b51404ee:b48dd2d87d29860d7b6e0689508ca0ed:::
jasmina:1002:aad3b435b51404eea9d3b435b51404ee:b1c46c8199fe93ce7f968b4b1fbc8af3:::
Kada forenzičar izvrši prikukpljanje heš vrednosti (NTLM hash) naloga, sledi postupak dešifrovanja sa posebnim alatima. Za forenzičku istragu je jako važno da se otkrije ta šifra zato što je vrlo verovatno da je zlonamerni

napadač istu šifru upotrebljavao na nekoliko drugih servisa (email, webmail, i za mobilne uređaje koje poseduje) gde ima naloge. Ovaj postupak se može uraditi i na forenzičkoj kopiji koja se importuje u virtuelnu mašinu.
Brojevi koji su uz imena naloga označavaju ID korisnika. 500 označava se ID administratora lokalni korisnik koji bude kreiran počinje od broja 1000.
Jedna od alatki koju forenzičari koriste za otkrivanje šifri na osnovu NTLM heš vrednosti (podržava veliki broj tipova heša) zove se hashcat. Starije verzije su se delile na hashcat koji koristi CPU i oclhashcat koji koristi GPU za izvršavanje postupka dekriptovanja. U novijoj verziji hashcat 3 te dve verzhije su integrisane u jednu. Upotrebom GPU za dekriptovanje heša uz pomoć Hashcat-a operacije se procesiraju stream base tj. procesira veliki broj operacija u paraleli, dok se upotrebom CPUa operacije procesiraju kao block base tj. redno što je daleko sporiji postupak. Primer postupka dekriptovanja heša šifre koja sadrži 10 numeričkih cifara.
C:\>Hashcat64.exe –m 1000 –a 3 ntlm.txt ?d?d?d?d?d?d?d?d?d?d

Nakon dobijanja potrebnih privilegija forenzičar može da izvrši postupak prikupljanja podataka sa forenzičkim alatima.

Čest je slučaj da mobilni uređaji, digitalne kamere, digitalni fotoaparati ili smart uređaji koriste SD kartice za smeštanje multimedijalnih podataka ili operativnih sistema. Prilikom analize sadržaja ili nakon oporavka podataka sa SD kartice mogu se dobiti vrlo važne informacije kako o samom hardveru SD kartice kroz print out u vidu jedinstvenog ID koda (isto važi i za HDD, SSD). Na osnovu ovih kodova proizvođača moguće je saznati, gde je ova kartica prodata, kom distributeru je prodata. Nakon kontakta distrubutera može se saznati u kojoj je radnji bila prodata ili kom pravnom ili fizičkom licu je prodata kartica. Na taj način moguće je doći do zlonamernog napadača. Kada je reč o alatima za oporavak podataka treba reći da su oni generalno ograničeni, jer se oslanjaju na fajlove koji imaju netaknuta zaglavlja. Kada se prikupljaju podaci iz slek prostora koji sadrži fragmente fajlova, ti fragmeti mogu biti oporavljeni ali retko mogu biti rekonstruisani u kompletne fajlove. Kada mali fajl prepisuje veliki fajl moguće je oporaviti veći deo velikog fajla iz slek prostora. Značajne forenzičke alatke sa kojima je moguć proces oporavka podataka na Windows OS prikazani su u tabeli.

Tabela 10. Forenzički alati za oporavak podataka na Windows OS

Ime alata	Podržana verzija Microsoft Windows OS[2]
foremost	Radi pod Linuxom i podržava sve Windows fajl sisteme pri oporavljanju podataka
scalpel	Radi pod Linuxom i podržava sve Windows fajl sisteme pri oporavljanju podataka
Undelete	Windows server 2008, Windows server 2003, Windows 8, Windows 7, Windows Vista, Windows XP (ne podržava Windows Vista Business i Vista Enterprise)
Active@ UNDELETE	Windows XP, Windows Vista, Windows 7, Windows 8, Windows server 2003, Windows server 2008.
Active@ UNERASER	Windows 8, Windows 7, Windows Vista, Windows, XP, Windows 95, Windows 98, Windows Me, Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server, Windows NT 4.0 Workstation, Windows NT 4.0 Server, MS-DOS / PC-DOS.
BadCopy pro	Windows 9x, Windows Me, Windows 2000, Windows NT, Windows XP, Windows 2003, Windows Vista, Windows 7.
DiskInternals Uneraser	Windows 2000, Windows XP, Windows 2003, Windows 2008 Server, Windows Vista, Windows 7, Windows 8.
Edata Unerase	Windows 7, Windows Vista, Windows ME, Windows NT, Windows 2000, Windows XP, Windows 2003
Easy-Undelete	Windows 95OSR2, Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP, Windows 2003, Windows Vista
File Recover	Windows XP SP3, Windows Vista, Windows 7, Windows 8
File-saver	Windows 95, Windows 98, Windows NT, Windows 2000, Windows ME, Windows 2003, Windows XP, Windows Vista and Windows 7
File scavenger	Windows 8, Windows 7, Windows Vista, Server 2012, Windows 2008, Windows 2003, Windows 2000, Windows NT, Windows XP
Handy recovery	Windows 9x, Windows Me, Windows NT, Windows 2000, Windows XP, Windows 2003, Windows Vista, Windows 7
Mycroft	Windows 95, Windows 98, Windows ME, Windows XP, Windows 2000, Windows NT
PC INSPECTOR File Recovery	Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP
Recover my files	Windows 2003, Windows XP, Windows Vista, Windows 7, Windows 8
Recover4all Professional	Windows 8, Windows 7, Windows Vista, Windows XP, Windows 2000, Windows ME, Windows 98, Windows 2008, Windows 2003 Server
Search and recover	Windows 8, Windows 7, Windows Vista, Windows XP, Windows 2000
WinUndelete	Windows 98, Windows 2000, Windows 2003, Windows 2008, Windows XP, Windows Vista, Windows 7, Windows 8
Getdataback	Windows Server 2003, 2008, 2012, XP, Vista, Windows 7, Windows 8, Windows 10, 32 or 64-bit, podržava sve Windows fajl sisteme a nova verzija podržava i Linux EXT
photorec	Sve verzije Windows i Linux sa kernelom 2.6.18 ili većom x32 i x64

U carving procesu analizira se svaki sektor napravljene forenzičke kopije i izvlači se iz praznog prostora odnosno slek prostora, informacije koje je potrebno rekonstruisati sa ciljem dobijanja fajlova koji su bili obrisani. Alatke *foremost* [532] i *scalpel* [533] mogu da izvlače fajlove iz prostora markiranog kao obrisan sa shift+del. Pripadaju besplatnim alatima i rade u

532 Http://foremost.sourceforge.net/, 17.08.2016.

533 Https://github.com/sleuthkit/scalpel, 17.08.2016.

Linux komandnom okruženju. Sa ovim alatima iz forenzičkih kopija koje su u formi imidža, moguće je izvući obrisane fajlove. Pre upotrebe neophodno je editovati konfiguracione fajlove /etc/foremost.conf i /etc/scalpel.conf da bi se odabrali tipovi fajlova (.jpg, .pdf, .xls, .doc) koje procesiraju ovi alati.

Primer upotrebe alata foremost i scalpel :

#foremost –v –c /etc/foremost.conf -i /home/forenzicka_kopija/imidz_ hard_disk.dd –o /home/carving_podaci_foremost/

#scalpel –b –c /etc/scalpel/scalpel.conf -i /home/ forenzicka_ kopija/ imidz_ hard_ disk.dd –o /home/ carving_podaci_scalpel/

Ukoliko zlonamerni napadač izbriše sa CCleanerom sve informacije koji ukazuju o upotrebljenim zlonamernim alatima informacije se mogu povratiti sa ovim alatima jer one omogućuju carving tačno targetiranih podataka. Kada se u konfiguracionom fajlu alata postavi string u heksadecimalnoj formi onoga što se pretražuje moguće je da se traženo pronađe i da se prikupi kao digitalni dokaz.

Undelete - oporavlja podatke koji se ne mogu izvući iz korpe za otpatke (eng. Recycle bin).[534] Tipovi podataka koji se mogu oporaviti koristeći undelete alat su: deljeni podaci (eng. shard files), prethodne verzije Microsoft office fajlova, veliki fajlovi koji nisu mogli da uđu u korpu za otpatke, određeni fajlovi koji se kreiraju i brišu od strane aplikacija i fajlovi izbrisani korišćenjem komandne linije. Podržava sledeće OS (32 bitne i 64 bitne): Windows server 2008, Windows server 2003, Windows 8, Windows 7, Windows Vista, Windows XP. Ne podržava Windows Vista Business i Vista Enterprise.

Active@ UNDELETE - oporavlja podatke koji su obrisani iz korpe za otpatke, formatirane podatke sa hard diska, floppy diska, sa basic i dynamic Volume-a, sa hardverskog i softverskog RAID niza (RAID0 i RAID5).[535] Podržava kompresovane, kriptovane i fragmentirane fajlove. Pored hard diskova program ima podršku za oporavak podataka sa prenosnih uređaja kao što su CompactFlash, Secure Digital, SmartMedia, Sony memory stick, Zip drajv i USB drajv. Moguće je oporaviti obrisane podatke sa sledećih fajl sistema FAT12, FAT16, FAT32, NTFS, NTFS5 i EFS. Podržava sledeće OS (32 bitne i 64 bitne) Windows XP, Vista, Windows 7, Windows 8, Windows server 2003, Windows server 2008.

Active@ UNERASER - oporavlja podatke (fajlove i foldere), koji su

534 Undelete Home, http://www.condusiv. com/ home-use/ undelete/ home-edition/ ?SID=8&rid= 106504, 23.04.2016.

535 Active UNDELETE 11 - Data Recovery Toolkit, http://www.active-undelete.com/, 24.05.2016.

obrisani na FAT12, FAT16, FAT32, NTFS fajl sistemu.[536] Moguće je oporaviti fajlove sa obrisanih ili formatiranih particija. Podržava kompresovane, kriptovane i fragmentirane fajlove. Nije neophodno instaliranje na sistem već se može pokrenuti i sa USB prenosnog drajva i ima podršku za DOS sisteme. Podržava sledeće OS: Windows 8, Windows 7, Windows Vista, Windows XP, Windows 95, Windows 98, Windows Me, Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server, Windows NT 4.0 Workstation, Windows NT 4.0 Server, MS-DOS / PC-DOS.

BadCopy pro - oporavlja izgubljene i oštećene podatke sa floppy drajva, CD-R, CD-RW, DVD-ROM, DVD+/-R/W, Digial Media, zip drajva i diskova.[537] Ne upisuje podatake na originalan disk već snima oporavljene informacije u zadati direktorijum. U stanju je da oporavi podatke iz sesija sa višesesijskih CD-a i DVD-a. Podržava sledeće OS: Microsoft Windows 9x/Me/2000/NT/XP/2003/Vista/7.

DiskInternals Uneraser - oporavlja oštećene podatke (dokumente, fotografije, mp3 i zip), foldere i oštećene diskove.[538] Uspeva da oporavi i izgubljene fajlove koji su posledica napada virusa ili zlonamernog korisničkog ponašanja. Od uređaja podržava SD, microSD, Compact Flash, SONY Memory Stick, xD i MMC. USB flash drives. Od fajl sistema podržava NTFS, exFAT, FAT12/16/32, Ext2, Ext3, Ext4, Reiser, Reiser4, UFS i skrivene NTFS FAT12/16/32, kao i kompresovane NTFS i NTFS5 i šifrovan NTFS5. Prepoznaje lokalizovana imena sa podrškom za duge nazive u FAT12, FAT16 i FAT32. Podržava sledeće OS: Microsoft Windows 2000, XP, 2003, 2008 Server, Vista, Windows 7, 8.

Edata Unerase - oporavlja izbrisane fajlove, fajlove koji su izbrisani iz korpe za otpatke kao i izgubljene podatke nakon formatiranja hard diska, nakon infekcija virusa, neplaniranog gašenja računara ili nakon otkaza programa.[539] Ima dva metoda pretrage. Brzo skeniranje fajl sistema koje traži samo obrisane fajlove i kompletno skeniranje koje pretražuje obrisane i izgubljene fajlove. Od uređaja podržava hard diskove, floppy drajvove, Memory sticks, USB flash drajvove, Zip drajvove, Compact Flash kartice, SmartMedia kartice. Od fajl sistema podržava FAT12/16/32 and NTFS. Podržava sledeće OS: Microsoft Windows 7/Vista/ME/NT/2000/XP/2003.

Easy-Undelete - oporavlja nestale fajlove i foldere na NTFS, FAT32,

536 Active UNERASER, http://www.uneraser.com/, 24.05.2016.

537 BadCopy Pro™ (since 1996) - Recover Corrupted or Lost Data in Minutes!, Data Recovery Software, http://www.jufsoft.com/badcopy/, 24.05.2016.

538 Have you deleted a file you need?, DiskInternals, ltd., http://www.diskinternals.com/uneraser/, 24.05.2016.

539 eDATA Unerase™ Professional Edition, http://www.octanesoft.com/data_recovery.html, 24.05.2016.

FAT16 i FAT12 fajl sistemima i može prikazati izgled slike (Jpeg, PNG, TIFF, GIF, BMP, ICO, TGA, PCX, WBMP, PNM) ili binarnog fajla pre oporavka (heksadecimalni prikaz).[540] Podržava hard diskove, memorijske kartice, USB flash drajvove, Zip drajvove. Pokreće se bez instaliranja. Podržava sledeće OS: Microsoft Windows 95OSR2, 98, ME, NT, 2000, XP, 2003 i Vista.

File Recover - oporavlja obrisane fajlove, fajlove koji su nestali prilikom pražnjenja korpe za otpatke, fajlove nakon akcija brisanja koja zaobilaze korpu za otpatke (SHIFT+DELETE, brisanje iz komandnog okruženja, brisanje prevelikih fajlova i korišćenje programa za brisanje koji zaobilaze korpu za otpatke).[541] Ukoliko je fajl parcijalno prepisan ovaj program će pokušati rekonstrukciju preostalog sadržaja. Moguće je korišćenje batch moda (oporavak više fajlova odjednom) prilikom oporavka podataka. Podržava hard diskove, floppy drajvove, memorijske kartice, USB flash drajvove, Zip drajvove. Podržava FAT16, FAT32, ExFAT i NTFS fajl sisteme. Podržava sledeće OS: Microsoft Windows XP SP3 (samo 32bit verziju), Microsoft Windows Vista (32bit i 64bit verzije), Microsoft Windows 7, Microsoft Windows 8 (32bit i 64bit verzije).

File-saver - oporavlja fajlove obrisane od malicioznog programa ili fajlove koji su ispražnjeni iz korpe za otpatke.[542] Poseduje mogućnost provere uspešnosti oporavka izbrisanih fajlova. Može oporaviti neograničeni broja fajlova. Podržava hard diskove, floppy diskove i kartice digitalnih kamera. Podržava FAT16, FAT32, ExFAT i NTFS fajl sisteme. Od OS podržava: Microsoft Windows 95, Windows 98, Windows NT, Windows 2000, Windows ME, Windows 2003, Windows XP, Windows Vista and Windows 7.

File scavenger - oporavlja digitalne fotografije sa većine medija.[543] Može da oporavi fotografije koje su oštećene ili uništene od strane virusa ili slučajnim brisanjem iz Windows Explorera, korpe za otpatke, komandnog okruženja. Ima podršku za kompresovane diskove, osnovne i dinamičke diskove. Moguće je čak oporavati formatirane drajvove, oštećene raid nizove, oštećene particije (preko funkcije Defunct Volume search) i oporaviti podatke sa oštećenih diskova, koji sadrže loše sektore ili oštećene particije. Program je moguće pokrenuti sa floppy diska ili USB drajva ili ga instalirati na sistem. Od OS podržava: Microsoft Windows 8, 7, Vista, Server 2012/2008/2003/2000, NT i XP (32- and 64-bit).

---

540 Http://www.easy-undelete.com/, 24.05.2016.

541 PC Tools Utility, http://www.pctools.com/file-recover/, 24.05.2016.

542 File-Saver, http://www.recovery-magic.com/undelete/affiliate.aspx, 24.05.2016.

543 File Scavenger Version 5.2, Data Recovery Software & Services, http://www.quetek.com/prod02.htm, 24.05.2016.

Handy recovery - oporavlja fajlove sa hard diskova i floppy diskova kao i slika sa medija CompactFlash, SmartMedia, Multimedia, Secure Digital.[544] Program može oporaviti fajlove koji su obrisani, oštećeni malicioznim programom, padom sistema, programskom greškom i može oporaviti podatke nakon formatiranja particije. Oporavlja podatke izbrisane iz korpe za otpatke kao i kompresovane i šifrovane na NTFS-u. Pretraživanje izbrisanih fajlova je slično kao kod Windows Explorera. Moguće je snimanje fajlova na druge diskove uz oporavak čitavih stabla foldera. Od fajl sistema podržava FAT12/16/32/64(ExFAT), NTFS/NTFS 5, EFS, HFS/HFS+. Od OS podržava: Microsoft Windows 9x/Me/NT/2000/XP/2003/Vista/Win7.

Mycroft - ovaj alat je brz i efikasan pretraživač. Pomaže digitalnom forenzičaru da izvrši brzu pretragu za određenim pojmovima nakon zaplene hard diska.[545] Pre započinjanja pretrage ovaj program zaključava hard disk, da bi sprečio bilo kakve promene informacija na ispitivanom hard disku. Prema dostupnim podacima brzina pretrage iznosi 5MB/sec.[546]

PC INSPECTOR File Recovery - ova alatka može biti od koristi u slučaju oštećenja boot sektora, obrisanih fajlova ili particija.[547] Od particija podržava FAT 12/16/32 i NTFS. Moguće je oporaviti podatke sa originalnim vremenom i vremenskim pečatom. Pored toga moguće je oporaviti fajlove na mrežnim drajvovima. U stanju je da oporavi podatake koji su bez hedera. Od OS podržava: WINDOWS 95/98/ME/NT/2000/XP.

R-Undelete - ovaj alat može oporaviti fajlove sa bilo kog validnog logičkog diska vidljivog od strane OS.[548] Može oporaviti fajlove sa oštećenih ili izbrisanih particija. Oporavlja podatke koji su izbrisani bez slanja u korpu za otpatke, izbrisani iz korpe za otpatke, obrisani od strane malicioznog programa ili nakon naglog isključenja OS (nestanak struje). Podržava kreiranje image-a, što je korisno u slučaju da hard disk sadrži bad sektore koji narastaju. Može oporaviti podatke sa sledećih fajl sistema: FAT (FAT12, FAT16, FAT32, exFAT), NTFS, NTFS5. Od OS podržava: Windows 2000 /XP /2003 /Vista /2008 /Win7 /Win8.

Recover my files - oporavlja obrisane podatke, koji su ispražnjeni iz korpe za otpatke, podatke koji su formatirani ili oštećeni na hard disku

544 Handy Recovery, http://www.handyrecovery.com/, 24.05.2016.

545 Http://www.dibsusa.com/, 24.05.2016.

546 Huebner E., Bem D., Wee K. C., *Data hiding in the NTFS file system*, Digital Investigation 3, Elsevier, October 2006, ftp://163.13.201.222/ Prof_Liang/%E6%95% B8%E4%BD%8D% E9%91% 91%E8%AD%98/Volume%203%20%282006%29/Supplement%201/Issue%204/ Pages%20211-226.pdf, 21. 06. 2016.

547 PC INSPECTOR, http://www.pcinspector.de/default.htm?po=1&language=1, 24.05.2016.

548 R-Undelete, http://www.r-undelete.com/, 04.06.2016.

usled aktivnosti malicioznih programa ili nakon iznenadnog isključenja računara.[549]Moguće je oporaviti dokumente, fotografije, video i muzičke fajlove i mailove. Podržava hard diskove, memorijske kartice, USB flash drajvove, Zip drajvove, floppy diskove i druge prenosne medije. Može oporaviti podatke sa sledećih fajl sistema: FAT (FAT12, FAT16, FAT32), NTFS, NTFS5. Od OS podržava: Windows 2003/XP/Vista/Windows 7/Windows 8.

Recover4all Professional - oporavlja podatke slučajno obrisane na Windows sistemu, bez obzira da li su podaci izbrisani iz korpe za otpatke ili su obrisani direktno.[550] Da bi se sprečilo prepisivanje fajlova ova alatka ne zahteva instalaciju i može biti pokrenuta direktno sa floppy diska, USB diska ili flash drajva. Ima podršku za oporavljanje svih tipova dokumenata, slika, muzičkih i video fajlova. Podržava NTFS i FAT fajl sisteme kompresovane drajvove i fajlove, sve RAID nivoe kao i GPT.[551] Od uređaja podržava hard diskove, prenosne diskove, Zip drajvove, floppy diskove, memorijske kartice (CompactFlash, SmartMedia, SecureDigital, Memory Stick). Od OS podržava: Windows 8/7/Vista/XP/2000/ME/98/2008 i 2003 Server.

Search and recover - brzo oporavlja obrisane podatke, foldere, muzičke i video fajlove, slike, programe, web stranice, email poruke u Microsoft Outlook i Outlook express klijentima, Netscape mail, Thunderbird i Eudora.[552] Poseduje proširenu podršku za oporavak Outlook podataka (oporavak obrisanih taskova, kontakata, beležnica "eng. notes" i dnevnika). Omogućuje snimanje oporavaljenih podataka direktno na CD ili DVD. Da bi sprečio gubitak podataka ovaj alat može se pokrenuti sa CD-a. Pored toga moguće je oporaviti podatke sa hard diskova, memorijskih kartica, flash drajvova, CD-a, DVD-a. Od OS podržava: Windows8/7/Vista/XP/2000 (32-bit i 64-bit).

WinUndelete - oporavlja podatake sa hard diskova, floppy diskova, Zip drajvova, Jaz diskova, prenosnih diskova, memorijskih kartica.[553] Oporaviti podatke nakon pražnjenja korpe za otpatke kao i one podatke koji nisu ni prosleđivani korpi za otpatke (obrisani iz DOS komandnog okruženja, SHIFT+DEL), podatke obrisane od strane malicioznih programa. Podržava FAT12/16/32, NTFS i NTFS 5. Može prikazati slike, običan tekst (eng. plain text) i Microsoft dokumente pre oporavka. Od OS podržava: Windows® 98/2000/2003/2008/XP/Vista/7/8 (32-bit & 64-bit).

549 Need File Recovery or Hard Drive Data Recovery software?, GetData, http://www. recovermyfiles. com/, 04.06.2016.

550 The Recover4all data recovery software, http://www.recover4all.com/, 04.06.2016.

551 GUID Partition Table, više o GPT može se naći na Microsoftovom sajtu: Windows and GPT, http://msdn. microsoft.com/en-us/library/windows/hardware/gg463525.aspx , 04.06.2016.

552 Search and Recover, http://www.iolo.com/search-and-recover/, 04.06.2016.

553 WinUndelete, http://www.winundelete.com/, 04.06.2016.

GetDataBack – odličan alat za oporavljanje podataka sa hard diskova, SSD, fleš kartica i sa USB fleš diskova.[554] Jednostavan je za upotrebu i može da oporavi ime fajla i strukturu direktorijuma. Radi pod Windows Server 2003, 2008, 2012, XP, Vista, Windows 7, Windows 8, Windows 10, 32 or 64-bit. Od fajl sistema podržava NTFS, FAT12, FAT16, FAT32, EXT, EXT2, EXT3, EXT4.

Photorec – odličan besplatan alat koji može oporaviti podatke sa sledećih fajl sistema FAT, NTFS, exFAT, ext2/ext3/ext4, HFS+. Oporavlja podatke sa hard diskova, CD-ROMa, memorijskih kartica (CompactFlash, Memory Stick, Secure Digital/SD, SmartMedia, Microdrive, MMC), USB diskova, sa DD raw imidža, sa EnCase E01 imidža.[555] Namenjen je oporavku digitalnih slika i ostalih fajlova. Podržava preko 440 fajl formata.

3.3.3. Linux alati za inicijalni odgovor

Master boot record (MBR) predstavlja prvih 512 bajtova uređaja za skladištenje podataka (npr. hdd, ssd) i u njemu se nalazi bootloader operativnog sistema i tabela particija. MBR igra važnu ulogu prilikom bootovanja operativnog sistema, jer zapis MBR je prvo što se isčitava od strane BOOTSTRAP-a zapisanog u BIOS-u. Uređaj za skladištenje podataka je podeljen na particije. Razlikujemo primarnu (eng. primary) i proširenu (eng. extended) particiju. MBR sadrži zapis o tome na koji je način disk particionisan. Na primarnoj particiji smešta se operativni sistem i on nosi oznaku „A“ što označava da je particija aktivna. Proširena particija služi za smeštanje podataka. MBR je nezavistan od operativnog sistema.

Sa forenzičke tačke gledišta ukoliko želimo kod Linux OS da izvršimo analizu MBR zbog sumnje na moguću infekciju ili prisutnosti zlonamernog koda najpre se vrši bekapovanje MBR-a sledećom komandom:

#dd if=/dev/sda of=/path/mbr-backup bs=512 count=1

U slučaju da je potrebno izvršiti restore MBRa to se radi sa sledećom komandom:

#dd if=/putanja/mbr-backup of=/dev/sda bs=512 count=1

Od krucijalne važnosti je da forenzičar poznaje strukturu MBRa jer upravo to je ono što je predmet analize. Forenzičku analizu MBRa moguće je raditi u HEX editoru nad forenzičkom kopijom digitalnog dokaza koja je u formi bit-stream imidža. Na osnovu analize MBRa moguće je identifikovati

554 Https://www.runtime.org/data-recovery-software.htm, 22.07.2016.

555 Http://www.cgsecurity.org/wiki/PhotoRec, 22.07.2016.

sve adresirane podatke i njihovu ulogu (regularna/zlonamerna).

Tabela 11. Forenzički alati za inicijalni odgovor na Linux sistemima

Ime alata	Namena	Izvor
Nc	Netcat obezbeđuje kanal za komunikaciju između dva sistema	http://netcat.sourceforge.net/
dd, dcfldd	Svrha ovog programa jeste konverzija i kopiranje fajlova (kopira zadati ulazni fajl u određeni izlazni fajl uz moguće konverzije)	DD implementiran u sistem a poboljšana verzija dostupna na http://dcfldd.sourceforge.net/
date	Prikazuje datum i vreme na sistemu	Implementirano u sistem
Cat	Služi sa prikaz i povezivanja fajlova	Implementirano u sistem
pcat	Može dati prikaz svih procesa koji se nalaze u memoriji	Sastavni je deo TCT kompleta alata dostupnog na http://www.porcupine.org/forensics/tct.html
netstat	Daje prikaz trenutno aktivnih mrežnih konekcija	Implementirano u sistem
netstat -nr	Daje prikaz kernel IP-ruting tabele	Implementirano u sistem
arp	Daje prikaz ARP keša na sistemu	Implementirano u sistem
route	Takođe daje prikaz IP-ruting tabele	Implementirano u sistem
route -Cn	Daje prikaz ruting keša	Implementirano u sistem
dmesg	Daje informacije o hardveru na sistemu koje dobija od strane ring bafera jezgra	Implementirano u sistem
Ls	Izlistava sadržaj direktorijuma	Implementirano u sistem
fdisk -l /dev/???	Fdisk je alatka sa koja služi za rad sa particijama na linux. Pokrenuta sa switchem i određenim uređajem daje informacije o particijama	Implementirano u sistem
Script	Pomoću ove komande moguće je dokumentovanje pokrenutih komandi	Implementirano u sistem
ps -auxwww	Izlistava sve startovane procese prema pripadajućem korisniku	Implementirano u sistem
memdump	Pomoću ove alatke moguće je uraditi dump memorije	Dostupan TCT sajtu http://www.porcupine.org/forensics/tct.html
Df	Daje prikaz montiranih uređaja, tačku montiranja, veličinu, raspoloživ kapacitet i zauzeće uređaja	Implementirano u sistem
showmount	Daje prikaz NFS deljenih resursa na serveru	Implementirano u sistem

3.3.4. Linux alati za oporavak podataka

E2undel - ova alatka može se primeniti na Linux OS sa ext2 fajl sistemom.[556] Sastoji se od biblioteke koja može oporaviti obrisane fajlove prema imenu. Nakon oporavka podataka treba proveriti tri dela fajla: sadržaj fajla, metadata podatke o fajlu (datum i vreme kreiranja, vlasništvo i prava) i ime fajla. Ne podržava ext3, ReiserFS, XFS i JFS.

R-Linux - ova alatka može se primenti na Linux OS sa ext2, ext3, ext4 fajl sistemom sa kernelom 2.6 i iznad.[557] Ova alatka prepoznaje lokalna imena i može sačuvati oporavljene podatke na disku koji je vidljiv od strane operativnog sistema. Jednostavna je za upotrebu, oporavlja podatke sa diska koji imaju loše sektore, podatke koji su obrisani od strane malicioznog programa, nestale podatke usled kraha sistema ili iznenadnog isključenja.[558] Ova alatka može pomoći ukoliko je došlo do promene ili oštećenja particije na sistemu tako što će pokušati pronaći prethodnu particiju i oporaviti podatke koji se na njoj nalaze.

Stellar Phoenix Linux Data Recovery - oporavlja izgubljene ili nepristupačne podatke sa Linux fajl sistema EXT4, EXT3, EXT2 i Windows FAT12, FAT16, FAT32 fajl sistema.[559] Može oporavljati fajlove, direktorijume i particije kao posledice slučajnog formatiranja, gubitka particije, oštećenja fajlova ili delovanje malicioznog programa. Poseduje automatizovani čarobnjak koji istraživača vodi kroz tri koraka: procena, analiza i oporavak. Ova alatka poseduje samo funkcije čitanja. Oporavljeni podaci mogu da se smeštaju na prenosne uređaje.

3.3.5. Oporavak obrisanih Windows i Linux particija

Oporavak obrisanih particija je proces procene i izvlačanje obrisanih particija. Ovaj proces je jako važan kada je reč o oporavljanju podataka. Oporavljanje može da podrazumeva oporavljanje slučajno obrisane particije, od strane virusa, usled otkazivanja programa ili čak sabotaže. U nastavku će biti prikazani programi koji služe za oporavak particija.

---

556 E2undel, http://e2undel.sourceforge.net/, 04.06.2016.

557 Free Linux Recovery for Windows | for Linux, http://www.r-tt.com/free_linux_recovery/, 04.06.2016.

558 U ovom slučaju pravio bi se imidž celog hard diska i fajlovi bi se dalje procesirali kroz napravljeni imidž.

559 Stellar Phoenix Linux Data Recovery, http://www.stellarinfo.com/linux-data-recovery.htm, 28.05.2016.

Acronis Recovery expert - je sastavni deo paketa Acronis Disk Director Suite koji služi za kompletnu zaštitu korisničkih podataka, omogućujući oporavak obrisanih ili izgubljenih particija.[560] Štiti sistem od hardverskih i programskih grešaka i malicioznih napada. Može da radi nezavisno tako što se pokreće sa butabilnog CD-a ili diskete omogućujući oporavak particija čak iako sistem ne može da se bootuje. Podržava sledeće fajl sisteme FAT16, FAT32 ,NTFS , Ext2, Ext3, ReiserFS3, Linux SWAP. Od OS podržava: (x86 i x64) Windows 7, Windows Vista, Windows XP.

Active@ Disk image - uz pomoć ove alatke moguće je uraditi bekap i oporavak, kako celog hard diska tako i pojedinačnih FAT, NTFS particija.[561] Ovaj alat ima mogućnost pregleda fajlova i foldera unutar napravaljenog imidža pre oporavka podataka. Može se pokrenuti sa DOS diskete, CD-roma, DVD-a ili USB flash. Daje prikaz kompletnog HDD-a, particija i informacija o imidžu diska. Mogućnost kreiranja kompresovanog i nekompresovanog raw imidža fizičkog hard diska (sector by sector). Od fajl sistema podržava FAT12, FAT16, FAT32, NTFS i HTFS5. Od OS podržava: Windows 8 / 7 / Vista / Server 2003 / Server 2008 / XP /Small Business Server 2011.

Active@ Partition Recovery - oporavlja obrisanu particiju (primarnu ili prošerenu) samo u slučaju da njena lokacija nije prepisana.[562] Može kreirati bekape MBR, tabele Particija i Volume boot sektore. Pomaže pri oporavku nesistemskih particija. Ima mogućnost automatskog korigovanja BOOT.INI fajla i boot sektora da bi sačuvao bootabilnost sistema. Može popraviti MBR i održati integritet particije. Podržava diskove veće od 2TB. Od fajl sistema podržava FAT12, FAT16, FAT32, exFAT, NTFS, Apple HFS+, FreeBSD Unix UFS i Linux ExtFs. Od OS podržava: (x86 i x64) Windows 2000/XP/Server 2003/2008/Vista/Windows 7/ Windows 8.

DiskInternals Partition recovery - oporavlja podatke i particije.[563] Ne zahteva posebne veštine, jer program dolazi sa vodičem korak po korak (eng. wizard step-by-step). Oporavlja podatke sa oštećenih, obrisanih i reformatiranih particija. Program skenira svaki sektor na disku. Oporavlja podatke sa virtuelnih diskova VMware[564] (uključujući imidže, koji su smešteni na udaljenom ESX serveru), Oracle VirtualBox,[565] Microsoft

560 Http://www.acronis.com/homecomputing/products/diskdirector/#requirements, 28.05.2016.
561 Http://www.disk-image.com/, 28.05.2016.
562 Http://www.partition-recovery.com/, 28.05.2016.
563 Http://www.diskinternals.com/partition-recovery/, 28.05.2016.
564 Http://www.vmware.com/, 28.05.2016.
565 Https://www.virtualbox.org/, 28.05.2016.

VirtualPC,[566]Parallels,[567] bez potrebe instalacije virtuelne mašine. Oporavljene podatke program može narezati na CD ili DVD ili exportovati putem FTP-a. Od fajl sistema podržava FAT12, FAT16, FAT32, VFAT, NTFS, NTFS4, NTFS5, Ext2, Ext3. Od OS podržava Microsoft Windows 95, 98, ME, NT, 2000, XP, 2003 Server, Vista, Windows 7, 2008 Server.

GetDataBack - oporavlja izgubljene, obrisane, oštećene, formatirane ili reformatirane podatke.[568] Oporavlja oštećene particije na hard disku, oštećen boot sektor i FAT/MFT.[569] Podržava Unicode što omogućava oporavak fajlova sa imenima enkodovanih sa nestandardnim setom karaktera (kao na primer japanski, kineski, korejski, ruski i grčki set karaktera).[570] Ima podršku za sve FAT i NTFS fajl sisteme. Od OS podržava: Windows 95, 98, ME, NT, 2000, XP, 2003, Vista, Windows 7 ili Windows 8.

Testdisk - oporavlja izgubljene particije i omogućava povratak butabilnosti diska kada on postane nebutabilan, kao posledica neke programske neispravnosti, aktivnosti zlonamernog programa, ljudske namere ili greške.[571] Može oporaviti MFT, boot sektore kao i FAT tabelu. Od fajl sistema podržava FAT12/FAT16/FAT32, exFAT, NTFS, ext2/ext3/ext4. Primena ove alatke u različitim digitalno forenzičkim ispitivanjima imidža prikazana je na sajtu CGIsecurity.[572] Od OS podržava: DOS, Windows 95, Windows 98, Windows (NT4, 2000, XP, 2003, Vista, 2008, Windows 7 (x86 & x64), Linux, FreeBSD, NetBSD, OpenBSD, SunOS i MacOS X.

Svi navedeni programi koji se bave oporavkom podataka osim što doprinose prikupljanja dragocenih informacija za forenzičku istragu predstavlja i veoma važan element u strategiji zaštite samih podataka.

---

566 Http://www.microsoft.com/windows/virtual-pc/, 28.05.2016.

567 Http://www.parallels.com/, 28.05.2016.

568 Http://www.runtime.org/data-recovery-software.htm, 28.05.2016.

569 MFT (eng. Master File Table) predstavlja mesto gde se nalaze informacije o svim fajlovima i direktorijumima u okviru NTFS fajl sistema. Sadrži listu zapisa sa informacijama za pronalaženje podataka na disku kao i njihova vremena i datume kreiranja, poslednjih izmena i poslednjih pristupa.

570 Preporuka je da se oporavak podataka vrši na minimum Windows XP sistemu jer Windows 98 i Windos ME ne podražavaju u potpunosti Unicode.

571 TestDisk, Data Recovery, TestDisk, http://www.cgsecurity.org/wiki/TestDisk, 28.05.2016.

572 TestDisk and PhotoRec in various digital forensics testcase, http://www.cgsecurity.org/wiki/ TestDisk_and_PhotoRec _in_various _digital_forensics _testcase# Digital_Forensics_Tool_Testing_Images, 28.05.2016.

3.4. DIGITALNO FORENZIČKI KOMPLETI ALATA ZA WINDOWS I LINUX SISTEME

U današnje vreme forenzički programi se najčešće koriste za prikupljanje dokaza, kako u krivičnim postupcima, tako i u korporativnim istragama. Sa jedne strane umanjuju rizike koji mogu nastati sa ispitivanjem medija u njegovom prirodnom okruženju, a sa druge pružaju mogućnost brzog preteraživanja i pregledanja. Pomenuti rizici podrazumevaju izmenu kritičnih metadata podataka kao što su datumski i vremenski pečati pristupanim ili obrisanim fajlovima prilikom forenzičke analize. Zato mnogi forenzički alati obezbeđuju *zaštitu integriteta nad prikupljenim dokazima* pomoću heširanja (SHA1, SHA-256), da bi se osiguralo da su dokazi koji se iznose pred sud ostali ne promenjeni nakon prikupljanja. To znači da provosnudni organi prilikom sprovođenja zakona u velikoj meri zavise i od forenzičkih programa kojima se vrši prikupljanje, analiza i očuvanje kritičnih dokaza. Zato je od suštinske važnosti da se upotrebljavaju samo provereni i bezbedni forenzički alati. Postoji veliki broj radova koji se bave problemima i slabostima koji se odnose na forenziče alate.[573]

Digitalno forenzički kompleti alata predstavljaju skup alata koji mogu realizovati više elemenata forenzičkog procesa. To znači da kompletom mogu biti obuhvaćeni procesi pravljenja forenzičkih kopija, dokaza i njihova verifikacija, oporavak izbrisanih ili izgubljenih particija ili podataka, dešifrovanje zaštićenih fajlova, analiza podataka, dokumentovanje pronađenih dokaza i kreiranje izveštaja. Postoji preko 150 različitih automatizovanih alata koji se koriste prilikom istrage visokotehnološkog kriminala.[574] [575]

Sa aspekta platforme na kojoj rade mogu se podeliti na komplete alata koji rade pod Windows ili Linux operativnim sistemom. Sa aspekta koda kompleti se mogu podeliti na one sa otvorenim kodom i na one koji se licenciraju. U komplete koji rade na Windows OS spadaju: Accessdata FTK,

---

573 Tim Newsham, Chris Palmer i Alex Stamos sa radom "Breaking Forensics Software: Weaknesses in Critical Evidence Collection", Microsoft, *Microsoft Hyper-V*, http://www.microsoft.com/en-us/server-cloud/ hyper-v-server/; Chris Ridder sa radom "Evidentiary Implications of Potential Security Weaknesses in Forensic Software" Milanović Z., Milanović T., *Digitalna anti-forenzika kao kriminogeno sredstvo zaštite kiber kriminala*, Ziteh - Udruženje sudskih veštaka za informacione tehnologije It veštak, 2010.; Ryan Harris sa radom „Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem", Milosavljević M., Grubor G., *Digitalna forenzika računarskog sistema*, Univerzitet Singidunum, Beograd 2009.

574 Http://www.cftt.nist.gov/project_overview.htm, 29.05.2016.

575 Milanović Z., Milanović T., *Digitalna anti-forenzika kao kriminogeno sredstvo zaštite kiber kriminala*, Ziteh - Udruženje sudskih veštaka za informacione tehnologije It veštak, 2010.

Guidance Encase forensic, Ilook investigator, X-way forensic. U komplete koji rade pod Linux OS spadaju: The Sleuth kit, Autopsy, Penguin Sleuth, The Coroner's Toolkit (TCT), Helix. Najvažniji forenzički kompleti biće navedini u sledećoj tabeli i biće opisani u nastavku rada.

Tabela 12. Forenzički kompleti alata

Naziv forenzičkog alata	*Web sajt*	*Okvirna cena*
ENCASE forensic	http://www.guidancesoftware.com	4000$
ILOOK Investigator	http://www.perlustro.com/	2200$
The Sleuth kit, Autopsy forensic browser	http://www.sleuthkit.org/	Open Source - besplatan
AccessData Forensic Toolkit (FTK)	http://www.accessdata.com/	5500$
Penguin Sleuth	http://www.penguinsleuth.org/	Open Source – besplatan
The Coroner's Toolkit (TCT)	http://www.porcupine.org/forensics/tct.html#features	Open Source – besplatan
Helix Live CD	http://www.e-fense.com/helix	Starije verzije su besplatne ali nemaju podršku
Knoppix-STD 0.1	http://s-t-d.org/index.html	Open Source – besplatan
LiveWire Investigator	http://www.wetstonetech.com/cgi-bin/shop.cgi?view,14	9000$
The ProDiscover Family	http://www.techpathways.com	8000$
X-ways Forensics	http://www.x-ways.net/forensics/index-m.html	1500$

3.4.1. ENCASE forensic

Ovaj set alata ujedno predstavlja industrijski standard i kompletno rešenje za digitalnu računarsku istragu baš kao i AccessData FTK. Ovim alatom moguće je sprovesti efikasno prikupljanje podataka na forenzički ispravan način, tako da se proces može ponoviti i odbraniti pred sudom. Omogućava istraživačima prikupljanje podataka sa velikog broja uređaja, otkrivanje potencijalnih dokaza kao i izradu detaljnih izveštaja o svojim nalazima, održavajući pritom integritet nad dokazima. Postoji više verzija ovog alata koje mogu biti namenjene za privatan sektor ili za pravosuđe u zavisnosti od potreba i načina upotrebe. Encase komplet deli se na Mobile Encase i na Classic Encase.Mobile dolazi sa neophodnim adapterima i sa hardverom koji je potreban za pristup velikom broju modela mobilnih telefona. Classic Encase dolazi u formi servera i klijenta. Server je namenjen kreiranju bitstream kopija sa udaljenog mesta na kome se pokrene klijent.

Kada je reč o prikupljanju podataka ovaj set alata može prikupljati podatke sa servera, radnih stanica i tableta iz RAM memorije ili sa diskova čuvajući lako izmenjive podatke bilo gde na mreži bez ometanja poslovanja. Podrazumeva sigurnu istragu i analizu prikupljenih podataka preko LAN/WAN mreže sa centralne forenzičke lokacije (npr. kod Enterprise Encase rešenja). Od tipova podataka obuhvata dokumente, slike, internet artefakte, web istoriju i keš, rekonstruisanje HTML stranica, chat sesije, kompresovane fajlove, bekap fajlove, log i eventlog fajlove, šifrovane fajlove, fajlove sa RAID-a nizova kao i elektronsku poštu. Podržani formati elektronske pošte su Mbox (Unix), Netscape, AOL (ver 6,7,8,9), Yahoo, MSN Hotmail, Microsoft Outlook i Microsoft Outlook express.

Set alata kreira bit-by-bit sliku. Proizveden binarni duplikat identičan je originalu i verifikuje se generisanim hash vrednostima. U stanju je da oporavlja podatke i particije, detektuje obrisane fajlove, vrši analizu potpisa fajlova (eng. file signature) i heš vrednosti, pa čak i iz kompresovanih fajlova i sa nealociranog prostora. Digitalni istraživači mogu pregledati rezultate nakon što se podaci prikupe. Kada je jednom slika (eng. image) kreirana (podržava VMWARE, DD, Safeback v2), istraživači mogu pretraživati i analizirati više drajvova odjednom. U okviru Encase alata implementirana je NSLR (eng. The National Software Reference Library) biblioteka sa heš vrednostima poznatih fajlova čime se značajno smanjuje vreme i količina podataka potrebnih za analizu.[576] Prisutna je podrška za prikaz više od 100 fajlova u njihovoj prirodnoj formi, ugrađena je podrška za pregled registra baze, integrisan je prikazivač za fotografije, a rezultati pregleda mogu se vide na vremenskoj osi odnosno kalendaru. Sa bezbednosne tačke gledišta vrši auditing računara u slučaju kompromitovanja napadom zero-day (eng. zero-day attack), a takođe prepoznaje rootkit programe koji se odnose na Windows kernel i sanira njihove posledice.[577]

Poseduje mogućnost programiranja skripti za ovu alatku upotrebom Enscript programskog jezika što forenzičarima može pomoći da automatizuju specifične vrste pretraživanja i analiza. EnCase uspešno zaobilazi BitLocker zaštitu postavljenu u Vista OS kao i starije PGP zaštite.[578] Generisani izveštaji sadrže listu svih fajlova i foldera, detaljnu listu posećenih URL adresa sa

576 National Software Reference Library, (NSRL) Project Web Site, http://www.nsrl.nist.gov/, 29.05.2016.

577 Zero-day napad predstavlja napad određenim programom (zero-day exploit) koji iskorišćava ranjivost računarskog programa (servisa) koja nije prepoznata od strane programera. Zero-day exploit predstavlja program koji koristi sigurnosni propust da bi se izvršio napad.

578 Nestler V., Conklin W. A., White G., Hirsch M., Principles of Computer Security: CompTIA Security and Beyond Lab Manual, Second Edition, The McGraw-Hill Companies 2011.

datumima i vremenima pristupa. Pruža detaljne informacije o hard disku kao i detalje o prikupljanju podataka. Za autenfikaciju svih novijih EnCase verzija upotrebljava se USB dongle drive, koji predstavlja ključ sa kojim se program otključava.

3.4.2. ILOOK Investigator

ILOOK spada među prve komplete alata namenjenih dokazima na sudu u svetu. Bavi digitalnom forenzikom na Windows sistemima. Do verzije 8 ovaj komplet je bio isključivo namenjen pravosudnim organima kao i vojsci, ali od verzije IX ovaj alat je dostupan i kao komercijalan proizvod. Poseduje sopstveni alat za kreiranje forenzičke kopije ne samo za Intel sisteme već podržava 18 različiti procesora. U funkciji analize poseduje napredne tehnike pretrage i pregleda slike diska sa kompromitovanog računara. Može da vrši pretraživanje slike diska dobijenih drugim programima za pravljenje forenzičke kopije (bit po bit kopije) kao na primer: Encase imidž fajlove, Safeback imidž fajlove, ISO imidž fajlove, VMware virtuelni disk fajlovi. Ima mogućnost kreiranja hash za imidž fajlove CRC32, MD5, SHA1. Podržava veliki broj fajl sistema kao na primer: FAT 12/16/32/32x, VFAT, NTFS 4/5, NTFS 4/5 Compressed, HFS, HFS+, Ext2, Ext3, ReiserFS 1/2/3, SysV-AFS, SysV-EAFS, SysV-HTFS, Novell NWFS, Novell NWFS Compressed, VMDK (VMWare Drive Mount disk), Microsoft Virtual PC disk, CDFS, ISO 9660, ISO 9660, i UDF. ILOOK podržava puno UNICODE pretraživanje. Poseduje pretraživanje u različitim modovima (standardna, indeksirana i bulk pretraga). Može vršiti analizu potpisanih fajlova (eng. file signature) i heš vrednosti (podržava CRC32, MD5, SHA1). Poseduje funkciju hash deduplikacije (u slučaju učitavanja više slika odjednom) koja uklanja duplirane fajlove čime se može značajno ubrzati pretraživanje. Može se implementirati i Hashkeeper [579] kreiran od strane U.S. National Drug Intelligence Center (NDIC)[580] ili NIST NSRL baza, čime bi se vreme za pretraživanje smanjilo eliminišući poznate fajlove.

Poseduje i granularano izvlačenje fajlova sa kojim možemo da izdvojimo odgovarajući deo fajl sistema za pretragu. Poseduje mogućnost oporavka oštećenih i izbrisanih fajlova kao i Orphaned FAT direktorijuma.

579 Hashkeeper predstavlja veliku bazu podataka u Ms Access formatu koja sadrži 69 miliona potpisanih fajlova. Ova baza u sebi sadrži heš vrednosti bezbednih i zlonamernih fajlova čime mogu da se prepoznaju šifrovani programi, fajlovi sa zabranjenim pornografskim sadržajima i programi koji služe za prikrivanje zlonamernih aktivnosti (eng. staganonography programs).
580 The Department of Justice, http://www.justice.gov/archive/ndic/, 28.05.2016.

Ima ugrađen hex editor sa mogućnošću pretraživanja. Može prikazati događaje iz Event viewer-a na vizuelnoj mapi prema tipu događaja na vremenskoj osi.

Podržani formati za rekonstrukciju elektronske pošte i attachmenta su MBox, mbx, PST, OST, EML, EMLX, DBX, AOL, Lotus NOTES. Poseduje naprednu tehniku oporavka elektronske pošte iz MS Outlook-a. Takođe može uraditi rekonstrukciju internet keša. Poseduje pretraživač registarske baze sa pronalaženjem skrivenih registarskih ključeva. Poseduje mogućnost programiranja skripti za ovu alatku (moguće je razviti sopstvenu .NET aplikaciju koja može da se integriše u ILOOK). Od novina prisutna je funkcija analize fajlova koja detektuje slike i filmove zabranjenog sadržaja na osnovu prepoznavanja ljudskih formi. Može detektovati i šiframa zaštićene fajlove. Sa bezbednosne tačke gledišta poseduje mogućnost detekovanja malicioznih programa kao štu su virusi i trojanci.

ILOOK generiše detaljne izveštaje bilo da se radi o slučaju ili o dokazima. Počev od verzije 7 ILOOK klasifikuje dokaze prema virtuelnim kategirijama. Dokazi iz virtuelne kategorije mogu biti dodeljene različitim izveštajima prema tipu, i snimljeni u 7 različitih formata (PDF, HTML, MHT, RTF, Excel, TEXT, CSV) ili poslati mailom.

3.4.3. The Sleuth kit, Autopsy forensic browser

The Sleuth kit (TSK) i Autopsy forensic browser predstavljaju Linux orijentisane komplete alata za forenzička istraživanja čiji je autor Brian Carrier. TSK i Autopsy su otvorenog koda i rade na Unix platformi. TSK sadrži kolekciju Linux alata namenjenih komandnom okruženju za forenzičku analizu, dok Autopsy predstavlja grafički interfejs nad tim alatima za forenzičku analizu iz komandnog okruženja (koji pripadaju TSK). Sa ovim alatima moguće je istraživati fajl sisteme kao i logičke diskove (eng. volume). Ovi alati mogu služiti za analizu Windows i Linux fajl sistema. Mogu da analiziraju raw (dd), expert witness (encase) i AFF fajl sisteme i slike diskova podržavajući NTFS, FAT, UFS1/2, ext 2/3 i ISO 9660 fajl sisteme (čak iako OS na ispitivanom računaru ne podržava fajl sisteme). TSK takođe može oporaviti slak prostor na disku. Autopsy je HTML orijentisan tako da se njemu može prići sa bilo koje plaftorme uz pomoć HTML pretraživača. Interfejs kod Autopsy je u formi fajl menadžera i pokazuje detalje o obrisanim fajlovim i strukturi fajl sistema.

U nastavku slede kategorije alata koji su deo ovih kompleta:

- *alati koji se odnose na fajl sistem* - ovi alati procesiraju generalne informacije o fajl sistemu (npr. raspored blokova, veličinu i boot

blokove, labele). Jedna takva alatka jeste fstat.

- *alati koji se odnose na nazive datoteka* - ovi alati procesiraju strukturu imena fajlova koji su locirani u direktorijumu višeg reda (eng. parent direcotory). U ove alate spadaju ffind koji pronalazi dodeljena i neraspoređena imena datoteka na koje ukazuju određen metadata strukture i alatka fls koja izlistava dodeljena i obrisana imena datoteka u direktorijumu.
- *alati koji se odnose na metadata strukture* - ovi alati procesiraju metadata strukture koje sadrže detalje o fajlovima. Primeri ovih struktura su: zapisi direktorijuma u FAT, MFT zapisi u NTFS i inodi u Ext i UFS fajl sistemima. U ove alate spadaju icat (prikazuje sadržaj blokova dodeljenih određenom inodu), ifind (može da ustanovi koji inod sadrži određeni blok), ils (izlistava metadata strukture i njihov sadržaj u formatu gde je razgraničenje „vertical bar" odnosno „|"), istat (prikazuje statistiku i detalje u lako razumljivom formatu o određenoj metadata strukturi npr. o broju inoda). Cilj upotrebe ovih alata je da se dobije kopija fajla bez upotrebe API komandi (CreateFile, CopyFile i drugi) koje rootkit može da onemogući skrivanjem ili sprečavanjem pristupa fajlu.[581]
- *alati koji se odnose na jedinice podataka* (eng. data unit) - ovi alati procesiraju jedinice podataka prema mestu gde je uskladišten sadržaj fajla. Na primer: klasteri u FAT i NTFS fajl sistemu i blokovi u ext i UFS sistemima. U ove alate spadaju dcat (izvlači sadržaj određene jedinice npr. bloka podatka), dls (izlistava sadržaj obrisanog bloka na disku i može izvući nealociran prostor fajl sistema), dstat (prikazuje statistiku o bloku podataka u lako razumljivom formatu), dcalc (izračunava gde se podaci iz slike nealociranog prostora, dobijenih alatom dls, nalaze na originalnoj slici).
- *alat za upravljanje medijuma "mmls"*- ova alatka procesira sliku diska i analizira strukturu particija. Pronalazi skrivene podatake između particija, daje prikaz rasporeda diska uključujući i nealociran prostor. Izlaz ove alatke identifikuje tip particije i dužinu što olakšava postupak upotrebe dd kako bi se izvukla particija. Izlaz je sortiran na osnovu početnog sektora, pa je lako identifikovati praznine u rasporedu.
- *imidž fajl alatke* - ovi alati prikazuju detalje koji se odnose na imidž

581 National Institute of Standards and Technology, *Secure Hash Standard*, FIPS PUB 180, May 1993.

fajl. Alatka img_stat prikazuje detalje o formtu imidž fajla, dok img_cat prikazuje raw sadržaj imidž fajla.

TSK kao i Autopsy kompleti sadrže dodatne korisne alate kao na primer *mactime*. Mactime na osnovu rezultata dobijenih alatim „fls" i „ils" može kreirati vremesku osu o aktivnostima kako raspoređenih tako i nealociranih fajlova (vreme pristupa izmene i promene).[582]Alat Hfind (koristi binarni algoritam za traženje md5 heš vrednosti u već pomenutima bazama NIST NSRL i HashKeeper) i može skratiti vreme potrebno za analizu fajlova eliminišući poznate dobre fajlove, a identifikujući loše na osnovu poređenja sa bazom.[583]

Ovi forenzički kompleti pokrivaju post-mortem analizu i u tom slučaju moraju se pokrenuti iz pouzdanog i proverenog okruženja (npr. forenzička laboratorija) i analizu "uživo", u tom slučaju ovi kompleti se pokreću sa CD-a u nepouzdanom okruženju (što se radi u slučajevima odgovora na incident kada je on potvrđen). Nakon što je incident potvrđen istražitelj može da sprovede post-mortem analizu. Ovi alati poseduju dobre tehnike pretraživanja potenicijalnih dokaza sa UNICODE podrškom. Moguće je: prikazivanje fajlova i direktorijuma uključujući i imena obrisanih fajlova, pretraživanje sadržaja fajla u raw ili hex formatu izvlačeći ASCII string. Kada su nepoznati fajlovi u pitanju forenzičar može vršiti njihovo poređenje u heš bazama (NIST NSRL ili HashKeeper), da bi se potvrdilo da li se radi o poznatim dobrim ili malicioznom fajlovima. Sortiranje fajlova se radi prema njihovim internim potpisima. Ujedno se vrši i upoređenje ekstenzija fajla sa tipom fajla da bi se identifikovali fajlovi sa promenjenim ekstenzijama (gde je bio cilj da se fajl sakrije).

3.4.4. AccessData Forensic Toolkit (FTK) i Ultimate Toolkit (UTK)

Ovaj digitalno forenzički komplet alata koristi se od strane pravosuđa, vladinih agencija i korporacija širom sveta. Dizajniran je za detaljno pronalaženje i ispitivanje računarskih dokaza prilikom digitalne forenzičke istrage visokotehnološkog kriminala. Sa ovim kompletom moguće je izvršiti prikupljanje, oporavak fajlova, indeksiranje podataka kao i oporavak podataka na najnižem nivou (eng. data carving). Sadrži moćne alate za pretraživanje, filtriranje fajlova i njihovu analizu. FTK je prepoznat i kao vodeći forenzički alat kada je u pitanju

582 Jones R., *Internet Forensics*, O'Reilly Media, 2005.

583 U 2012 godini NDIC je ostao bez finansiranja i zatvorio je svoja vrata 16.juna 2012 pa je dostupnost i budućnost Hashkeep-era neizvesna, http://www.whiteoutpress.com/articles/q22012/after-19-years-of-waste-nat-drug-intel-center-closes/, 28.05.2016.

analiza elektronske pošte. FTK uključuje, FTK imager (program sa kojim se prave forenzička kopija ispitivanog hard diska i forenzičke slike), KFF heš biblioteka, prikazivač registarske baze (eng. Registry viewer[584]) kao i 50-100 klijentskih DNA (DNA ili Distributed Network Attack)[585] licenci za oporavak šifara. On može praviti forenzičke slike, čitati slike dobijenih drugim alatima (npr. ENcase). Takođe može prikupiti zaključane sistemske fajlove (SAM/System/NTuser). Sa svojom optimizovanom dtsearch funkcijom izuzetno brzo sprovodi indeksiranje i pretraživanje nad velikim skupovima podataka. Koristi MD5 i SHA-1 haširanje za verifikaciju fajlova. Sud priznaje kao valjani dokaz slike odnosno imidže diskova napravljene sa programom FTK Imager (ne odnosi se na FTK Imager Lite). Takođe, AccessData FTK podržava veliki broj postojećih formata za pravljenje forenzičkih kopija. To znači da on može otvoriti i imidže kreirane sa EnCase alatom, SMART alatom i drugih alata pa čak i .vmdk fajlove, koji predstavljaju slike radnih memorija sa virtualnih mašina.

Ultimate Toolkit uključuje kompletan FTK, alat za oporavak šifara (PRTK - Password Recovery toolkit), prikazivač registarske baze, Wipedrive pro, Microsoft NT login access utility kao i Novel utility. Sadrži komponente za oporavak izgubljenih ili zaboravljenih šifara. Ima mogućnost analiziranja celog hard diska u potrazi za šifrovanim i zaštićenim podacima. Poseduje module za analizu i dešifrovanje registarskih podataka, kao i module za čišćenje hard diska. Nema mogućnost rada sa skriptama kao Encase. Da bi se ovi proizvodi mogli koristiti neophodna je upotreba USB security key (koji se još naziva i dongle) baš kao i kod pomenutog Encase alata. Za svoje proizvode kompanija nudi trening i demo verziju, koja može biti skinuta sa zvaničnog sajt kompanije.

3.4.5. Penguin Sleuth

Ovaj komplet alata je ustvari bootabilna Linux distribucija zasnovana na Knopix sistemu prilagođena forenzičaru. Uključuje različite komplete alata kao što su TCT (The Coroner's Toolkit), Autopsy i TST (The Sleuth Kit) kao i alate za skeniranje virusa i skeniranje sistema na ranjivost (eng. penetration test). Može se koristiti iz komandnog ili iz grafičkog okruženja. Omogućeno je pregledanje uživo (eng. live privew) kompromitovanog računara bez izmene

584 Accessdata Registry viewer omogućava pristup zaštićenom "Storage sistem provider" ključu koji sadrži šifre elektronske pošte, internet šifre i podešavanja. Ovaj alat pravi izveštaj sa dragocenim podacima iz registarskih ključeva koji su od interesa za istragu.

585 DNA predstavlja novi pristup u procesu oporavka šifrom zaštićenih fajlova. U prošlosti se za oporavak koristila snaga jedne mašne, dok se sa novim DNA pristupom koristi snaga svih za to licenciranih mašina na mreži.

nad dokazima kada je u pitanju EXT2, FAT32 i NTFS4.

Ernest Baca je uradio studiju provere Knoppix distribucije za pregled "uživo" na računaru sa EXT3 ili reiserfs instaliranim particijama i zaključeno da se kao posledica javlja promena MD5 hash vrednosti particije.[586] Treba biti posebno oprezan prilikom ispitivanja kompromitovanog Linux računara. Razlog leži u tome što će Knoppix pokušati da koristi swap prostor, a on može sadržati potencijalne dokaze koji u tom slučaju mogu biti izmenjeni. Forenzički alati ovog kompleta su sledeći:

Sleuth Kit - forenzički alati komandnog okruženja;
Autopsy - grafički deo Sleuth kit;
Dcfldd - unapređena verzija DD Imaging alata sa ugrađenim heširanjem;
Foremost[587] - alat komandnog okruženja za oporavak podataka;
Air (Automated Image and Restore) - grafički interfejs za (dd ili dc3dd)[588] za kreiranje forenzičkih slika;
Md5deep[589] - program za MD5 heširanje;
Netcat - obezbeđuje kanal za komunikaciju između dva sistema;
Cryptcat - obezbeđuje šifrovan kanal za komunikaciju između dva sistema.
NTFS alati kompleta PSK:
Qtparted - grafički alat za particionisanje;
Regviewer - alatka za prikaz windows registarske baze.
Bezbednosni alati kompleta PSK:
Etherape - grafička alatka za nadgledanje mrežnog saobraćaja;
Clamv - antivirusni skener;
Nikto2[590] - bezbednosni skener za web server;
Snort[591] - alatka komandnog okruženja za detekciju upada u mrežu (po difotlnim pravilima);
John the Ripper - password cracker komandnog okruženja;
Rkhunter[592] - alatka komandnog okurženja koja pretražuje znakove prisustva rootkit programa;

586 Ernest Baca, The Penguin Sleuth Kit, http://www.penguinsleuth.org/linuxforensics/pensleuth.html, 29.05.2016.
587 Foremost, http://foremost.sourceforge.net/, 30.05.2016.
588 Unpređena dd verziija od strane Jesse Kornblum iz DoD Cyber Crime centra omogućava heširanje sa algoritmima MD5, SHA-1, SHA-256, and SHA-512.
589 Http://md5deep.sourceforge.net/, 30.05.2016.
590 Nikto2, CIRT.net, http://www.cirt.net/nikto2, 30.05.2016.
591 Http://www.snort.org, 30.05.2016.
592 Http://rkhunter.sourceforge.net/, 30.05.2016.

Ethereal - alatka za analizu saobraćaja na mreži;
FWBuilder - grafički firewall program;
Nessus - grafički skener ranjivosti sistema;
Chkrootkit[593] - alatka komandnog okurženja koja pretražuje znakove prisustva rootkit programa.

3.4.6. The Coroner's Toolkit (TCT)

Primarno je razvijen za UNIX sisteme od strane Dan Farmer i Wietse Venema, može izvesti prikupljanje i analizu podataka i na diskovima koji nisu pod Unix fajl sistemom.

Alati koji su sastvani deo TCT kompleta su:

– *grave-robber* - ova alatka služi za prikupljanje podataka;
– *alati pisani u C-u* o kojima je bilo reči u prethodnim kompletima (ils, icat, pcat, mactime);
– *unrm& lazarus* - ovi alati služe oporavak obrisanih fajlova;
– *findkeytool* - alatka koja služi za oporavak šifarskih ključeva iz pokrenutog procesa ili fajla.

3.4.7. Helix Live CD

Starije verzije Helixa predstavljaju prilagođenu Knoppix live Linux distribuciju za forenzičku istragu, dok su novije bazirane na Ubuntu live distribuciji. Forenzičar podiže Linux okruženje koje podrazumeva prilagođen Linux kernel, detektovanje hardvera kao i prisustvo mnogih forenzičkih programa i programa za odgovor na incidentnu aktivnost. Ovaj program nema uticaja na računar, koji se ispituje što predstavlja forenzički ispravan pristup. Program neće uraditi automatski (eng. mount) priključak na swap prostor, kao što neće priključiti ni bilo koji konektovan uređaj na ispitivani sistem. Karakteristika ovog kompleta je što sadrži spoj Windows funkcionalnosti, koja se ogleda prilikom prikupljanja lako izmenjivih podataka uživo sa Windows sistema (program se pokreće kao standardna Windows aplikacija) i Linux funkcionalnosti sopstvenog butabilnog OS koji se koristi u sveobuhvatnoj post-mortem analizi. Upotrebom HELIX Live cd (HELIX 2009 r1) može se izvršiti kreiranje „live" forenzičke kopije računarskog sistema dok je računar upaljen i ovaj alat predstavlja zapravo toolkit inicijalnog forenzičkog odgovora. Na

593 Http://www.chkrootkit.org/download.htm, 30.05.2016.

osnovu svoje funkcionalnosti HELIX radi na dva načina kao Windows live (u komandnom ili grafičkom okruženju) i kao bootabilna linux distribucija. Treba napomenuti da rad u grafičkom okruženju HELIXa zahteva više resursa nego rad u komandnom okruženju. Sadrži toolkit windows alata koji omogućuje da se izvrši remote tcp konekciju na ispitivan računar bez dodavanja uređaja i da se kroz mrežu uradi digitalna kopija hard diska ili kopiranje digitalnih dokaza.

Najvažniji alati koji su deo Helix kompleta su sledeći:

- *WFT, WTF2* (Windows Forensics Toolchest) - autora Monty McDougal, omogućava ponovljiv automatizovan proces forenzičkog odgovora uživo, odgovora na incident i procenu bezbednosti na Windows sistemima na osnovu prikupljenih bezbednosno relevantnih informacija sa sistema.[594] Generiše izveštaj u HTML formatu.[595]

- *IRCR2* (Incident Response Collection Report) – čiji je autor John McLeod, je skripta koja omogućava prikupljanje i analizu forenzičkih podataka na Windows OS.[596] Slična je alatu TCT (Farmer i Vanema) i orijentisana je više prikupljanju nego analizi prikupljanja podataka. Prikupljeni podaci se nakon incidentne radnje šalju digitalnom forenzičaru na dodatne analize.

- *FRU* (First Responder Utility) - autora Harlan Carvey, omogućava forenzičarima da izbegnu nepraktičnost netcata kada je u pitanju prikupljanje podataka uživo sa ispitivanog sistema.[597] Sastoji se iz dve komponente, serverske i klijentske. Za funkcionisanje na Windows OS potrebni su određeni dll-ovi, jer je kod originalne skripte pisan u perlu i potom kompajliran za Windows okruženje.

- *Nigilant32* - autora Matthew Shannon iz Agilant Risk Managemet, omogućava forenzičaru da pregleda hard disk, napravi sliku memorije i uradi snimak stanja (eng. snapshot) trenutno pokrenutih procesa i otvorenih portova na sistemu. Ima mali uticaj na sistem i zauzima manje od 1MB memorije kad se učita. Podržava Windows 2000, XP i 2003.

- *FRED* (First Responder's Evidence Disk) - autora Jesse Kornblum, predstavlja skriptu za odgovor na incident. Slična je alatki IRCR. Orijentiasna je ka prikupljanju lako izmenjivih podataka na Windows OS bez modifikovanja ispitivanog sistema. Ova alatka od Helix verzije 2 nije prisutna u kompletu.

---

594 Http://www.foolmoon.net/security/wft/index.html, 30.05.2016.

595 Kanellis P., Kiountouzis E., Kolokotronis N., Martakos D., *Digital Crime and Forensic Science in Cyberspace*, Idea Group Inc, 2006, str. 217-242.

596 IRCR, SourceForge, http://ircr.sourceforge.net/, 30.05.2016.

597 Alatka netcat u većini slučajeva funkcioniše odlično, međutim kada naraste broj komandi koje treba primeniti (npr. može doći do grešaka prilikom kucanja) postaje nepraktična.

- *SecReport* (Security Reports) - služi za prikupljanje bezbednosnih informacija na ispitivanom sistemu. Moguće je vršiti poređenja rezultata dva sistema ili istog sistema ali sa različitim vremenima. Poseduje grafičko okruženje. Informacije koje prikuplja su sledeće: hard diskovi, procesor, ostali uređaji, podešavanja page fajl setovanja, otvoreni portovi, instalirane zakrpe, programi, servise, konfiguracija event loga, mrežna konfiguracija, bebednosna (eng. audit) konfiguracija.

- *Prikazivače različitih namena* - u ovom kompletu mogu se naći prikazivači, messenger šifara, šifara za korišćenje elektroneske pošte, mrežne šifre, zaštićena područja, registarske baze, istorije IE, IE šifre, Outlook PST šifre, kolačiće IE i Mozille, polja prekrivena asterisk znacima "******".

- *Pouzdano komandno okruženje* - omogućava komandu šel koja je pouzdana i proverena za vršenje forenzičkog prikupljanja podataka.

- *MD5 Generator* - generiše MD5 heš za prikupljene podatake.

- *PC inspector File Recovery* - alatka kompanije Convar. Služi za oporavak podataka sa FAT 12/16/32 i NTFS-a. [598] Automatski pronalazi particije čak i ako je boot sektor kod FAT particije (ne odnosi se na NTFS) obrisan ili oštećen. Oporavlja podatke sa originalnim vremenskim i datumskim pečatima. Omogućeno je i snimanje oporavljenih podataka na mrežni disk. Podržava sledeće formate podataka: arj , avi , bmp , cdr , doc , dxf , dbf , xls , exe gif , hlp , html , htm , jpg , lzh , mid , mov , mp3 pdf , png , rtf , tar , tif , wav , zip. Od OS podržava: Windows 95/NT/98/Me/2000/XP.

Windows Systernals Rootkit Revealer - autori ove alatke su Bryce Cogswell i Mark Russinovich.[599] Poseduje naprednu tehniku pretraživanja rootkita na sistemu (bilo da je reč o korisničkom ili kernel modu rootkita). Najnovija verzija nije komandno orijentisana. Podržava Windsows XP (32-bit) i Windows server 20003 (32-bit).

3.4.8. Knoppix-STD 0.1

Ovaj komplet alata predstavalja kolekciju više stotina bezbednosnih alatki otvorenog koda. Spada u live Linux distrabucije, što znači da se pokreće sa bootabilnog diska u memoriji bez promene OS na računaru. Upotrebljava se za oporavak podataka u post-mortem analizi ili nad zaključanim računarima. Ovaj komplet alata pruža i mogućnost izvođenja procene ranjivosti sistema

598 Convar.de.com, http://www.convar.de/ , 30.05.2016.

599 Mark Russinovich , RootkitRevealer v1.71, Windows Sysinternals, http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx, 16.04.2016.

kao i penetraciono testiranje (simulacija napada na sistem sa ciljem procene sigurnosti računarskog sistema ili mreže).

Značajni forenzički alati koji dolaze u sklopu ove distribucije su sledeći:

- *sleuthkit:* komplet o kome je već bilo reči;
- *autopsy:* komplet o kome je već bilo reči;
- *biew*: binarni prikazivač;
- *bsed*: binarni editor;
- *dcfldd*: US DoD Computer Forensics Lab verzija dd;
- *fenris:* alat za debagovanje koda, dekompajliranje;
- *fatback*: oporavak FAT;
- *foremost*: oporavak specifičnih tipova fajlova sa slike diska;
- *ftimes*: system baseline tool (be proactive);
- *galleta*: oporavaka kolačića iz IE;
- *mac-robber*: TCT's graverobber napisan u C;
- *md5deep*: izvšenje md5 heširanja nad vise fajlova/direktorijuma;
- *memfetch*: prikupljanje dump-a memorije;
- *pasco*: pretraživanje IE index.dat fajla;
- *photorec*: prikupljanje fajlova grab fajla iz digitalnih kamera;
- *readdbx*: konvertovanje Outlook Express .dbx fajlova u mbox format;
- *readoe*: konvertovanje celog Outlook Express direktorijuma u mbox format;
- *rifiuti*: pretraživač Windows Recycle Bin INFO2 fajlova;
- *secure_delete*: securely delete files, swap, memory; i
- *testdisk*: testiranje i oporavak nestalih particija.

Ids – alati za detektovanje upada na sistem su:

- *snort 2.1.0*: IDS;
- *ACID*: web interfejs za snort;
- *barnyard*: brzo procesiranje snort logova;

- *oinkmaster*: ažuriranje snort definicija;
- *bro*: mrežni IDS;
- *prelude*: mrežni i lokalni IDS;
- *logsnorter*: praćenje logova;
- *swatch*: praćenje bilo kakvog fajla:
- *sha1sum; i*
- *md5sum.*

Alati za procenu ranjivosti na sistemu su:

- *amap 4.5:* mapira startovane programe na udaljenom računaru;
- *chkrootkit 0.43*: vrši pretraživanje pristustva rootkita;
- *clamAV:* antivirusni skener;
- *hydra:* brute force alatka;
- *nbtscan:* skeniranje SMB mreže;
- *nessus 2.0.9:* alatka za skeniranje ranjivosti na sistemu;
- *nikto:* skener web ranjivosti; i
- *screamingCobra*: skener web ranjivosti.

3.4.9. LiveWire Investigator

Predstavlja sveobuhvatan komplet alata za digitalnu forenziku. Poseduje veliki broj opcija kako za prikupljanje podataka i za njihovu analizu. Pogodan je za forenziku "uživo", u stanju je da prikuplja podatke uključujući i stanje "running state", dok sistem nastavlja da radi. Poseduje automatsko logovanje i kreiranje izveštaja za sve pokrenute istražne aktivnosti. Prikuplja i snima trenutno aktivno stanje sistema "running state" i poseduje mogućnost kreiranja slike fizičke memorije. Uživo može da pregleda registarsku bazu. Prikuplja ključne informacije o startovanim programima, procesima, mrežnim konekcijma, prenešenim podacima. U stanju je da mapira mreže, procenjuje ranjivosti na sistemu, prikuplja dokaze direktno sa ispitivanog računara, kao i da vrši skeniranje na maliciozne programe. Od OS podržava: Windows NT4, 2000 pro, XP, 2003 server, Vista.

3.4.10. The ProDiscover Family

Prodiscover Family predstavlja sveobuhvatan komplet za digitalnu forenziku i podrazumeva dva paketa alata: Prodiscover forensic paket i Prodiscover incident response paket. Namenjen je pravosudnim organima.

Prodiscover forensic paket služi za prikupljanje, analizu, upravljanje i kreiranje izveštaja o digitalnim dokazima. Prilikom prikupljanja za analizu podataka kreira se bit-stream slika originalnog diska uključujući i skrivenih prostora HPA (eng. Host protected area).[600] Moguća je pretraga fajlova, metadata podataka i celog diska uključujući slek prostora i HPA. Može čitati slike raw (.dd) formata i Encase formata. Podržava sve verzije Windows OS sa podrškom za fajl sisteme FAT 12/16/32/exFAT, NTFS, SUN Solaris UFS, Linux Ext 2/3/4, i Mac OSX HFS+, uključujući dinamičke diskove i programski RAID. Moguća je upotreba Proscript-a i Perla-a, a moguće je automatizovanje procesa istrage.

Prodiscover incident response paket pretvara Prodiscover forensic u klijent server aplikaciju koja omogućava pregled diska, prikupljanje slike diska i analizu preko TCP/IP mreže. Sadrži i dodante napredne alate za odgovor na sajber napade. U stanju je da brzo identifikuje upade na sistem bez gašenja sistema. Dozvoljava forenzičaru da prikupi sadržaj fizičke memorije sa "živog" sistema. Odlikuje se posedovanjem najmodernijeg sistema za verifikaciju podataka. Omogućena je potpuna indeksirana pretraga, mountovanje „uživo", kreiranje slika svega na ispitivanom Windows OS uključujući Volume shadow copy. Može obavljati neograničen broj istovremenih kreiranja slika sistema. Uz pomoć ovog seta alata moguće je utvrditi da li je sistem kompromitovan i omogućava prikupljanje potrebnih dokaza da se to i dokaže. Istraživanje može obuhvatati kreiranje slike fizičkog diska ili memorije.

Ovaj komplet u stanju je pronaći sve podatke koji se nalaze na ispitivanom disku u forenzički ispravnom maniru, čak i one koji se nalaze u HPA oblasti diska bez izmene podataka. Za obezbeđenje integriteta kreiraju se heš potpisi (MD5, SHA-1, SHA-256) za sve fajlove i moguće je njihovo poređenje sa određenom bazom poznatih fajlova. Ima funkciju izvlačenja EXIF informacija iz JPEG fajlova.[601] Prodiscover incident response zahteva

600 HPA predstavlja deo hard diska skriven od OS a samim tim i od korisnika. Uglavnom se koristi od strane proizvđača računara da bi se tu smestili podaci sa održavanje ili oporavak sistema. Naravno zlonamerni korisnici tu oblast mogu da iskoriste za skrivanje podataka. Za proveru postojanja HPA na disku moguće je koristiti i Brian Carrirer-vu Sleuth kit alatku disk_stat.

601 Exchangeable image file format (Exif) predstavlja standard koji opisuje format slike, zvuka, snimljenih digitalnim kamerama. Ovaj standard obuhvata metadata podatke (npr. datum i vreme, opis, copyright informacije, tip kamere i njena podešenost i dodatni podaci).

instaliranje serverskog apleta (PDServer program) na ispitivanom računaru da bi se realizovao postupak prikupljanja podataka, što ga čini prihvatljivim više korporativnom okruženju nego za istrage pravosudnih organa.

3.4.11. X-ways Forensics

X-Ways Forensics predstavlja forenzičko radno okruženje za digitalnu istragu računarskih sistema. Podržava Windows XP/2003/Vista/2008/7*, 32 Bit/64 Bit. Podržava veliki broj opštih kao i specifičnih funkcija za forenzičku istragu. Podržava kloniranje diskova i pravljenje slike originalnog diska bez izmene podataka. Od fajl sistema podržava: FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4, Next3, HFS, HFS+/HFSJ/HFSX, ReiserFS, Reiser4, XFS, UFS1, UFS2, CDFS/ISO9660/Joliet, UDF, GPT, Windows dinamičke diskove i LVM2.[602] Može čitati slike formata raw (.dd), ISO, VHD i VMDK i encase (.E01). Obezbeđuje kompletan pristup diskovima, RAID-u i slikama većim od 2TB. Ima funkciju pregledanja i dumpa fizičke memorije za OS Windows 2000, XP, Vista, 2003 Server, 2008 Server, Windows 7, a može prikupiti i virtuelnu memoriju startovanih procesa. Poseduje različite tehnike oporavljanja podataka koji obezbeđuju brzinu. Ova alatka vrši prikupljanje podataka iz slek prostora, slobodnog prostora. Kreira katalog fajlova i direktorijuma za sve medije. Izračunava hep vrednosti za sve fajlova sa dostupnim algoritmima CRC32, MD4, ed2k, MD5, SHA-1, SHA-256, RipeMD.[603] Ima podršku da importuje NSRL RDS 2.x, HashKeeper, i ILook hash za potrebe deduplikacije poznatih fajlova i pronalaženja onih malicioznih. Poseduje odlično simultano fizičko i logičko pretraživanje kao i zaštitu od upisivanja da bi se obezbedio integritet podataka. Raspolaže sa funkcijom analize elektronske pošte prikupljene iz sledećih formata: Outlook (PST, OST), Exchange EDB, Outlook Express (DBX), AOL PFC, Mozilla (including Thunderbird), generic mailbox (mbox, Unix), MSG, EML. Vrši automatsku detekciju zaštićenih MS Office i pdf fajlova kao i detekciju slika u njima sa funkcijom Skin color detection koja služi za ubrzavanje pronalaženja tragova dečije pornografije. Ova alatka poseduje i veliki broj prikazivača različitih namena: prikazivač registarke baze (za sve Windows verzije) sa generisanjem registarskog izveštaja, prikazivač even logova (.evt, .evtx), shortcut fajlova

602 WAN Optimization and Data Reduction, CTERA, http://www.ctera.com/ products/ technology/ next3-file-system, 29.05.2016.

603 Antoon Bosselaers, The hash function RIPEMD-160 , What is RIPEMD-160?, http://homes. esat. kuleuven.be/~bosselae/ripemd160.html, 29.05.2016.

(.lng), windows prefetch fajlova, raspoređenih zadataka (.job), wtmp/utmp/btmp logova, Outlok imenika, Firefox istoriju, Firefox download, Chrome istoriju, Chrome arhiviranu istoriju, podatke o Chrome logovanjima, Safar cache, Skype bazu podataka sa kontaktima i prenešenim fajlovima. Izvlačenje metadata podataka iz velikog broja različitih tipova podataka kao što su: MS Office, OpenOffice, StarOffice, HTML, MDI, PDF, RTF, WRI, AOL PFC, ASF, WMV, WMA, MOV, AVI, WAV, MP4, 3GP, M4V, M4A, JPEG, BMP, THM, TIFF, GIF, PNG, GZ, ZIP, PF, IE cookies, DMP memory dumps, hiberfil.sys, PNF, SHD & SPL printer spool, tracking.log, .mdb MS Access database, manifest.mbdx/.mbdb iPhone backup. Ima mogućnost detektovanja HPA prostora na disku. Ima mogućnost dekompresovanja kompletnog hiberfil.sys fajla. Nakon prikupljenih podataka i pronađenih dokaza alatka izrađuje detaljan izveštaj o nalazima.

X-ways winhex je forenzička alatka (znatno jefitinija) i digitalnom forenzičaru može koristiti kao hex editor, disk editor ili RAM editor zajedno sa ostalim funkcijama programa kao što su spajanja, odvajanja, kombinovanja i procene fajlova.[604] Ovaj program poseduje funkciju brzog pretraživanja i funkciju zamene, šablon za uređivanje, enkripciju, funkciju izmene fajlova, mehanizam za pravljenje rezervnih kopija, mogućnost pravljenja slike diska, kloniranje diska i štampanje. Od strane disk editora podržani su flopy diskovi, hard diskovi CD i DVD drajvovi. Podržava kreiranje heš vrednosti za veliku količinu fajlova (CRC32, MD4, ed2k, MD5, SHA-1, SHA-256, RipeMD). Ova alatka služi za prikupljanje i analizu dokaza, jer pored mogućnosti za kopiranje i verifikaciju dokaza, sadrži i HEX editor koji omogućava analizu podataka.

604 Software Products, X-Ways, http://www.x-ways.net/winhex/, 23.04.2016.

4. DIGITALNA FORENZIKA I MERE ZAŠTITE U ORGANIZACIJAMA

Ranjivosti sistema predstavljaju hardverske i programske slabosti u vidu grešaka ili loše konfiguracije koje zlonamerni korisnik može kompromitovati. Upravljanje konfiguracijom, zakrpama i bezbednošću na sistemu su od pojedinačnih disciplina evoluirali u jedan IT problem koji se danas naziva upravljanje ugroženošću.[605]

Nijedan sistem nije 100% siguran i svaki ima svoje ranjivosti. Razlozi leže u toj činjenici što, iako nema u datom momentu na sistemu prepoznatih programskih propusta, uvek su mogući problemi vezani za bezbednosna podešavanja na sistemu ili zloupotrebe funkcija programa. Zbog velikog broja slabosti svojstvenih bezbednosnim podešavanjima na sistemu, zajedno sa mogućnostima zloupotrebe programskih funkcija i programskim propustima, u svakom trenutku postoje desetine i stotine ranjivosti na samo jednom računarskom sistemu.

Ove ranjivosti imaju čitav niz različitih karakteristika. Neke od njih jednostavne su za zloupotrebu (eng. exploit), dok su za druge zloupotrebe ranjivosti potrebni određeni preduslovi. Sa nekim exploitima dobijaju se admin tj. root privilegije dok sa drugim mogu obezbeđivati samo pristup sistemu sa difoltnim privilegijama. Upravo je *analiza ranjivosti na sistemima* jako značajna sa stanovišta zaštite, da bi organizacije mogle da znaju koji su propusti prisutni na sistemima, koliko je teško napadaču da ih iskoristi i kakve bi posledice mogli da izazovu. Bezbednost na sistemima može se sagledati i kroz moto Erica Cole-a: „Prevencija je idealna, ali je detekcija obavezna".[606] [607] Dakle, kada je zaštita u pitanju kako u organizaciji tako i u kućnim sistemima postoje dve ključne komponente: prevencija i detekcija.

Većina organizacija zaštitu na svojim sistemima fokusira na prevenciji, ali ne i na detektovanju zlonamernih aktivnosti. Na primer većina kompanija na svojim sistemima ima instalirane firewall-ove koji deluju preventivno. U tom slučaju mogu da se jave dva problema. Prvi je taj da organizacija ne može da spreči kompletan saobraćaj, što na neki način otvara mogućnost za

605 Mrdović S., Huseinović A., Zajko W., *Combining Static and Live Digital Forensic Analysis in Virtual Environment*, Information, Communication and Automation Technologies, ICAT 2009, XXII International Symposium, 2009, http://people.etf.unsa.ba/~smrdovic/publications/ICAT2009-Mrdovic_ Huseinovic_ Zajko.pdf, 22.06.2016.

606 Eric Cole i Stephen Northcutt, Honeypots: *A Security Manager's Guide to Honeypots*, http://www. sans. edu/research/security-laboratory/article/honeypots-guide, 11.06.2016.

607 Eric Cole, How to secure your company, Computerworld, http://www.computerworld.com/s/article/ 82515/How_to_secure_your_company?nlid=SEC2, 11.06.2016.

potencijalni napad. Drugi problem leži u činjenici da preventivni mehanizmi nisu prilagođeni ili nisu ispravno konfigurisani pa samim tim pružaju minimalnu ili nikakvu zaštitu. Uspostavljanjem samo preventivne mere nije dovoljno da se spreči svaki napad, u tom slučaju ključno je da oraganizacija uspostavi svoju odbranu na takav način da prepozna pretnju napadača blagovremeno, pre nego što se desi kompromitovanje sistema.

Kada se radi o nedozvoljenoj aktivnosti tipa upada u računarski sistem, napadač će uvek ići linijom manjeg otpora. Upravo zato je izuzetno važno da organizacija (kao i vlasnici kućnih računara) razume svoje slabosti na sistemima i da se ne koncentriše samo na jednu oblast zaštite. Na primer, nikada se ne treba oslanjati samo na antivirusni program sa ciljem detektovanja malicioznih programa iz više razloga. Prvo malicizni programi se brzo razvijaju i sistem može sadržati maliciozni program, a da ga antivirus kao takvog ne prepoznaje, jer još nije uvršćen u antivirusnu bazu podataka. Drugo veliki broj malicioznih programa ima načine da onemoguće antivirusnu zaštitu na sistemu tako da skener na maliciozne programe ništa ne prijavljuje. Veliki broj regularnih programa se koristi na nedozvoljen način u svrhu ostvarivanja nedozvoljenih aktivnosti.

FTP server jeste regularan program, koji može biti instaliran od strane zlonamernog napadača sa ciljem hostovanja i distribucije nedozvoljenog materijala. Antivirusni program ga neće detektovati kao maliciozan (pošto izgleda kao regularna aplikacija), jer ne ispituje način na koji se program koristi.[608]

Zaštita se postiže neprekidnim ciklusom otkrivanja slabosti i njenim ispravljanjem. Samo ukoliko postoji jasan stav o razumevanju bezbednosti računarskih sistema u okviru organizacije i plan da se bezbednosni rizici smanje, mogu se prevazići bezbednosni problemi.

Sa stanovišta bezbednosti najvažniji cilj je pronaći najslabiju kariku i zakrpiti je (eng. patching), pre nego što je iskoristi zlonamerni napadač. To predstavlja termin *prozor ranjivosti* (eng. Window of Vulnerability), koji se odnosi na upravljanje ranjivostima na sistemima. Pored toga se odnosi na vremenski period u kome je sistem ranjiv na određeni bezbednosni propust, konfiguracioni problem ili neki drugi faktor koji smanjuje bezbednost na sistemu. Prema Manzuiku Goldu i Gatfordu razlikujemo *dva prozora ranjivosti*:[609]

608 McRee R., *Memory Analysis with DumpIt and Volatility*, ISSA Journal, September 2011.

609 Mrdović S., Huseinović A., Zajko W., *Combining Static and Live Digital Forensic Analysis in Virtual Environment*, Information, Communication and Automation Technologies, ICAT 2009, XXII International Symposium, 2009, http://people.etf.unsa.ba/~smrdovic/publications/ICAT2009-Mrdovic_ Huseinovic_ Zajko.pdf, 22.06.2016.

1. *Nepoznati prozor ranjivosti* - obuhvata vreme od otkrivanja ranjivosti do momenta kada je sistem obezbeđen od te ranjivosti tj. pečovan;
2. *Poznati prozor ranjivosti* - obuhvata vreme od kada je proizvođač (eng. vendor) objavio zakrpu, do momenta kada je sistem obezbeđen od ranjivosti tj. pečovan.

Iako većina organizacija obraća pažnju na poznati prozor ranjivosti izračunavanje nepoznatog prozora ranjivosti je dragoceno za planiranje strategije za ublažavanje štete.

Krajnji cilj je da se zakrpi dovoljan broj ranjivosti na sistemu koji će odbiti zlonamernog napadača zbog neuspešnih pokušaja upadanja na sistem. Većina proizvođača programa ili hardvera nude zakrpe preko svojih mailing listi, koji se odnose na bezbednost:

Tabela 13. Bezbednosne liste

Naziv Liste	Web sajt liste	Opis
Microsoft Security Bulletins	http://technet.microsoft.com/en-us/security/bulletin	Ovo je Microsoft bilten lista koja se tiče bezbednosti, a preko koje se dobijaju informacije o pitanjima i problemima koji se odnose Microsoft proizvode.
Bugtraq	http://seclists.org/bugtraq/	Jedna je od prvih bezbednosnih mailing listi. Ukoliko se problem pojavi skoro uvek će biti postavljen na ovoj listi.
VulnWatch	http://seclists.org/vulnwatch/	Nije diskusiona lista već se bavi samo objavljivanjem sigurnosnih problema.

Osim u izuzetno malom broju slučajeva nikada se ne mogu ukloniti svi propusti na sistemu. Zbog toga je cilj da se ukloni i ublaži najveći broj rizika, koji će odbiti napadača ili da se napadač blagovremeno otkrije i spreči šteta. Veliki broj organizacija ne preduzima adekvatne bezbednosne mere sve dok im se ne desi kompromitovanje sistema odnosno nastanak štete. Suština je ta da ukoliko se bezbednosni problem otkrije na vreme manje će štete imati organizacija odnosno vlasnik računara. Što je više vremena proteklo od detektovanja napada vreme za saniranje raste, nastala šteta je veća.

Zaštita od zlonamernih napadača zahteva stalnu pažnju i nadzor, jer većina organizacija koje su priključene na internet neće biti u stanju da spreče svaki napad. Izuzetno je važno da se napadač koji je uspeo da iskoristi određeni propust na sistemu otkrije što pre.

Na sledećem primeru vidimo koliko je važno da osim preventivnih

mera postoje i mere za detekovanje. Jedna organizacija može mnogo da izgubi ukoliko njene ponude i spiskovi klijenata, budu dostupni javnosti. Stoga se postavilo pitanje procene bezbednosnih rizika. Predlog za procenu bezbednosti, nije naišao na odobrenje iz razloga što kompanija nije imala nikakvih bezbednosnih povreda u poslednje tri godine. Na pitanje: koliko su imali napada na sajt? Odgovor je bio da napadi nisu detektovani, jer nisu ni tražili napade. Način na koji su utvrdili da su napadani jeste na osnovu korisničkih žalbi ili na osnovu ometanja servisa, što je za organizaciju bilo definisano kao minimalno ometanje pa se nije dovodilo u vezu sa povredom bezbednosti. To znači da je za organizaciju jedini način utvrđivanja povrede bezbednosti bio ukoliko dođe do prekida servisa. To dalje implicira da je napadač mogao da upadne u računarski sistem organizacije i preuzme sve osetljive fajlove i iskoristi ih sa ciljem krađe klijenata. To u organizaciji ne bi primetili, jer napad nije ugrozio njihov servis. Posle određenog perioda javio se problem sa storidžom, a pripisan je korisnicima koji kopiraju velike količine fajlova. Nakon forenzičkog ispitivanja konstatovano je sledeće: sistem za skladištenje podataka bio je prepun hakerskih alata i raznih exploita na sistemu, pronađeni su i maliciozni programi tipa trojanaca na čak 13 servera, pogrešno konfigurisan firewall i nedostatak nadziranja log fajlova i mrežnih aktivnosti.[610] Pronađeno je i 5 naloga sa administratorskim privilegijama, ali se nije znalo kome pripadaju. Iz svega se može zaključiti da je ova organizacija bila ozbiljno ugrožena, a da toga nisu bili svesni. Ispravljanje ovog problema trajalo je blizu 8 meseci i koštalo je organizaciju preko 150.000 evra. Da je organizacija imala odgovarajuće procedure vezane za bezbednost sistema, nakon prvog upada zlonamernog napadača u sistem, napadač bi bio uhvaćen i organizaciji bi trebalo nekoliko sati da se očisti i zakrpi svoje ranjivosti.

Sistem pored zaštitnih barijera mora da ima i sistem za detekovanje upada (IDS), koji zajedno sa forenzičarem predstavlja proaktivan pristup u bezbednosti sistema. To je ono čemu teži veliki broj organizacija, ali nažalost veliki je broj organizacija koje ne pridaju veliki značaj IDS-u i forenzičkoj analizi dok se ne desi veća šteta. Velike ogranizacije koriste mamce tj. *hanipotove* (eng. Honeypot) kao vid proaktivnosti na svojim nezaštićenim delovima mreže sa ciljem proaktivnog detektovanja upada na sistem. Sistem Honeypot jeste osmišljen da se u produkcijskim sistemima uhvati zlonamerni napadač

610 U većini slučajeva postojanje sistema za logovanje aktivnosti na mreži predstavlja i jedini način na osnovu koga je moguće utvrditi da li je u toku komprimitovanje sistema ili je već iskompromitovan. Samo ako se zna šta se dešava na mreži moguće je pravilno se odbraniti od napada. U većini slučajeva organizacije koje ne nadziru svoje logove rizikuju da će biti kompromitivane i da će doživeti poslovni krah.

pre nego što izvrši zlonamernu aktivnost. On simulira naizgled ranjive servise na primer na Windows serveru podignuta ranjiva verzija IIS-a.[611] Kada zlonamerni napadač skenira mrežu i pronađe server koji poseduje ranjiv servis on će pokušati da izvrši exploit nad tim servisom sa ciljem dobijanja neovlašćenog pristupa operativnom sistemu. Primer jedne honeypot platforme jeste T-Pot razvijena od strane Deutsche Telekom-a.[612] Implementacija je jednostavna jer instalacija dolazi u .iso fajlu. Poseduje mogućnost analiziranja logova od nastalih dešavanja na sistemu. Drugi korisni honeypot paket jeste Valhala Honeypot instalira se na Windows sisteme.[613] Simuliraju se servisi kao na primer http servis, ftp servis iako on realno ne postoji na sistemu.

U situacijama kada se vrši ciljani napad i ukoliko je neophodno uraditi forenziku ili sprečiti takvu vrstu napada ili ublažiti zlonamernu aktivnost, može se upotrebiti i honeynet project.[614] Ovaj projekat dozvoljava da se na postojećim veb serverima u okviru organizacije postave veb strane koje će biti indeksirane od strane google engine-a. Na taj način ukoliko zlonamerni napadač šalje upit za pretraživanje direktorijuma sa osetljivim podacima ili login stranama, dobiće URL linkove na koje će pokušati da pristupi. Zapravo ti URL-ovi nisu zvanični URL-ovi organizacije već se nalaze na prikrivenoj lokaciji na veb serveru. Na taj način moguće je otkriti source IP adresu koja je pokušala da pristupi osetljivim lokacijama.

Zlonamerni napadači koriste google ili bing sa naprednim operatorima da dobiju tačno tražene rezultate od određenog veb servera:

inurl:, link:, related:, site: intitle:type

Primer pronalaženja svih .doc fajlova koji se nalaze na sajtu mi.sanu.ac.rs

www.mi.sanu.ac.rs filetype:doc

Primer pronalaženja svih .pdf fajlova koji se nalaze na sajtu viminacium.org.rs

filetype:pdf site:viminacium.org.rs

Zlonamerni napadači najčešće koriste sledeću pretragu za pronalaženje URLova na kojima se nalazi login forma:

intittle:login site:turing.mi.sanu.ac.rs

Kada pronađe login formu zlonamerni napadač će pokušati da detektuje koji je servis u pitanju da bi proverio da li za njega postoji određeni exploit ili će pokušati da izvrši bruteforce login napad sa ciljem dobijanja neovlašćenog pristupa servisu. Ukoliko postoji IDS tipa SNORT moguće je detektovati takav napad zbog velike količine login paketa za kratak vremenski interval sa jedne IP

611 Microsoft veb server razvijen za Windows OS zove se IIS -Internet Infromation Services.
612 Http://dtag-dev-sec.github.io/mediator/feature/2015/03/17/concept.html, 17.08.2016.
613 Https://sourceforge.net/projects/valhalahoneypot/, 17.08.2016.
614 Https://www.honeynet.org/, 17.08.2016.

adrese. Ukoliko postoji određeni honeypot na serveru on bi registrovao pristup određenom traženom fajlu i te informacije bi forenzički bile korisne ukoliko se one koriste u korelaciji sa dodatnim elementima zlonamerne aktivnosti.

Kada je u pitanju bezbednost sistema ne postoji "*srebrni metak*" kao jedinstveno zaštitno rešenje. Potrebno je imati pristup zaštiti u više nivoa. Na primer, firewall je dobar za početak, ali nije konačno rešenje. Tek nakon dodavanja sistema za nadziranje IDS: većeg broja firewalla, aktivnog nadziranja logova, forenzičkog nadziranja, antivirusne zaštite, zaštićenog dial-up pristupa, VPN pristupa, kriptografski zaštićene komunikacije u okviru organizacije, upotrebe jakih šifara, liste za kontrolu pristupa i upotrebne analize ranjivosti, može se govoriti o sigurnoj mreži i sigurnim računarskim sistemima.

Ovakav pristup koji ima više mehanizama zaštite naziva se zaštita u više nivoa (eng. defense in depth). Hanipot predstavlja postavljanje ranjivog računara (sa minimumom sigurnost) na posebnom delu mreže kao mamac, koji će privući potencijalnog napadača.[615] Cilj je nadziranje malicioznih aktivnosti programa ili napadača, kako bi organizacija spremno odgovorila na takve aktivnosti.[616]

Potrebno je ukazati i na to da ne postoji način da se računarski sistemi pravilno zaštite, ukoliko se ne zna protiv čega je usmerena zaštita. Samo pravilnim razumevanjem nedozvoljenih aktivnosti, načina na koji se napadi dešavaju, šta maliciozni korisnici (napadači) rade kako bi kompromitovali sistem, učenjem od forenzičkih događaja i analizom ranjivosti računarskih sistema i odgovornošću zaposlenih, organzacija može da sprovede zaštitu na pravi način.

Ukoliko se proaktivna analiza ranjivosti (bezbednosno skeniranje sistema) sprovodi u redovnim intervalima, uz dokumentovanje ranjivosti na dosledan i metodičan način, organizacija će biti svesna svojih potencijalnih bezbenosnih propusta od kritičnih do onih manje važnih.[617] Samo će dobro pripremljeni računarski sistemi koji podrazumevaju proaktivni pristup zaštite zajedno sa uspostavljenom bezbednosnom politikom (in-depth) i procedurama biti odbranjeni od napadača (ili će ga odvratiti, sprečiti ili brzo detektovati), a organizacija neće pretrpeti gubitak (ili će on biti mali).

615 Nikačević V., *Korporacijska istraga kompjuterskog kriminala sa implementacijom sigurnosne politike*, Ziteh - Udruženje sudskih veštaka za informacione tehnologije It veštak, 2010.

616 Spernow je opisao na koji način Microsoft upotrebljava hanipot kao proaktivni element zaštite sa ciljem otkrivanja i sprečavanja upada. Nikolić K. L., *Suzbijanje visokotehnološkog kriminala*, Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, Beograd 2010.

617 McDougal M., *Windows Forensic Toolchest (WFT)*, 2005, http://www.foolmoon.net/security/, 11.07.2016.

Snorby u kombinaciji sa Snort servisom predstavlja unapređen IDS sistem.[618] Snort je jedan servis koji Snorby program koristi. Ovaj program prikuplja logove iz Snorta, a na osnovu svojih signatura vrši komparaciju koja se prikazuje u logovima, da li je prepoznat određeni tip napada (ako jeste šalje se alert) kao što to antivirusni sistemi rade.[619] Snorby predstavlja zapravo veb aplikaciju koja služi za praćenje bezbednosti na mreži koja se oslanja na popularne IDS sisteme kao što su Snort, Suricata[620] i Sagan[621]. Snorby ima mogućnost da vrši kategorizaciju svih paketa. Sa forenzičke tačke dobar način okrivanja exploita koji se koriste u mreži je upotreba Snort događaja kroz Suricatu uz korišćenje pravila EmergingThreats i ET PRO rulesets.[622] Uz pomoć alatke tcpreplay forenzičar dobija mogućnost upotrebe pretnodno prikupljenog saobraćaja u libpcap formatu.[623] Na taj način forenzičar vrši simuliranje zlonamernog saobraćaja na mrežni interfejs senzora kako bi se prepoznale pretnje. Primer :

#tcpreplay –i eth0 /home/dump_mreza_1/dump_mreze_1.pcap

4.1. PRIMERI RANJIVOSTI I NAČINI ZLONAMERNOG ISKORIŠĆAVANJA SISTEMA

U daljem tekstu biće navedene najčešće ranjivosti sa kojima se suočavaju kako administratori sistema tako i forenzičari pri analizi incidentnih i nedozvoljenih aktivnosti. Prikazane ranjivosti ne obuhvataju sve moguće ranjivosti, ali mogu služiti kao polazna tačka za organizacije (vlasnike računarskih sistema), koje žele da obezbede svoje mreže i računarske sisteme. Ne treba da čudi što su mnoge prikazane ranjivosti iste baš kao i one publikovane od strane SANS (System, Administration Networking, and Security) instituta i FBI istraživanja.[624] SANS je napravio odličnu klasifikaciju kroz top 20 najčešćih ranjivosti koje se odnose na OS Linux i Windows. Lista u ovoj knjizi obuhvata većinu SANS ranjivosti uz pridodate druge ranjivosti, koje su prisutne na računarskim sistemima. Prikazane ranjivosti

618 Https://github.com/Snorby/snorby/, 17.08.2016.
619 Https://www.snort.org/, 17.08.2016.
620 Https://suricata-ids.org/, 17.08.2016.
621 Https://suricata-ids.org/, 17.08.2016.
622 Mane Piperevski, Workshop ICT Forensics Investigation – Lab module 3, Piperevski & Associates, Beograd 2016.
623 Http://tcpreplay.synfin.net/wiki/tcpreplay/, 17.08.2016.
624 SANS lista klasifikovanih ranjivosti. CIS Critical Security Controls, SANS Institute, http://www. sans.org/top20/2005/#w5, 26.04.2016.

moguće je otkriti na osnovu analize ranjivosti (ili testom penetracije). Neke od prepoznatih ranjivosti mogu direktno da kompromituju sistem, dok je uz pomoć drugih moguće dobijanje korisnih informacija koje napadaču mogu pomoći da organizuje napad.

Neke od ranjivosti se odnose na većinu OS, a neke su specifične za Linux odnosno za Windows OS. U daljem tekstu biće opisane prepoznate ranjivosti, uz predložene adekvatne protivmere da bi se ranjivost otklonila, a sistem zaštitio.

4.1.1. Opšte ranjivosti

1. *Podrazumevane (eng. default) instalacije OS i aplikacija* nose sa sobom velike bezbednosne rizike. Na primer, mogu se pojaviti nezaštićeni korisnički nalozi (npr. nalozi bez šifre). Dešava se da se sistemi isporučuju sa korisničkim nalozima bez šifara ili sa poznatim fabričkim šiframa ili sa aktivnim gost (eng. guest) nalogom bez šifre. U slučaju da korisnici zaborave da postave šifru odnosno promene podrazumevnu šifru, to daje prostora zlonamernim napadačima da lako realizuju upad u računar. Opasnost leži u činjenici da potencijalni napadač može dobiti kompletnu kontrolu nad sistemom. Jednostavnim pristupom sistemu (preko nezaštićenog naloga npr. guest) i pokretanjem nekih od exploit alata na sistemu sa ciljem dobijanja pune kontrole nad sistemom, sistem može biti kompromitovan. Čak i ako administrator promeni šifru difoltnog naloga, taj nalog će i dalje biti meta zlonamernog napadača koji će uz pomoć upotrebe "brute force" alata pokušati da pogodi šifru.

   Rešenje: *Na svakom računarskom sistemu obavezno promeniti root šifru (na Linuxu), odnosno preimenovati administratorski nalog i promeniti adminisratorsku šifru, onemogućiti guest nalog, prekontrolisati sve postojeće naloge (obrisati sve defaultne naloge) i podesiti nove šifre, pre puštanja sistema u produkciju. Savet je da se sa programima za proveru šifara otkriju slabe šifre na sistemu i blagovremeno ih treba promeniti.*

2. *Instalirani servisi na default OS* - U praksi je čest slučaj da se pri instalaciji programa ili OS, instaliraju i startuju servisi bez znanja onog ko vrši instalaciju. Na primer, određene Linux distribucije po difoltu instaliraju servise (npr. Sendmail, rstat, FTP), koji nisu

podrazumevano nužni, a koji predstavljaju potencijalnu ranjivost na sistemu. Na Windows NT sistemima difoltna instalacija ponuđena je sa servisom IIS (Internet Information Server). Fluktuacija sistem administratora u organizaciji je vrlo česta pa novi administrator sistema ne može identifikovati sve servise koji rade na sistemima pa samim tim ne može imati uvid u njihove ranjivosti.

Rešenje: *Analizom ranjivosti (ili pentracionim testom) moguće je otkriti servise kojih administrator nije bio svestan. Potrebno je detaljno proučiti dokumentaciju programa ili sistema koje je potrebno instalirati. Novi administrator sistema treba da utvrdi koji su servisi pokrenuti na sistemu za koji će biti odgovoran. Potrebno je periodično vršiti skeniranje servera sa port skenerima za proveru da li postoje novi servisi. Na firewall je potrebno blokirati sve nepotrebne portove, kako bi se sprečio zlonamerni napad na servis koji je greškom pokrenut.*

3. *Upotreba nezaštićene komunikacije (eng. clear text , eng. unencrypted data)* - Servisi na sistemu konfigurisani da prenose sve informacije u čistom tekstu predstavljaju ranjivost sistema i mreže. To znači da se informacije koje putuju kroz mrežu prenose u nezaštićenom obliku. Mnogi HTTP serveri koriste BASIC autentifikacioni mehanizam. To je vrlo jednostavna šema koja koristi base64 način kodiranja cleartext formata korisničkih imena i šifri. Ukoliko je zlonamerni napadač u mogućnosti da prati HTTP saobraćaj (npr. sniffer) može ukrasti imena korisnika i šifre dekodiranjem tih base64 zaštićenih podataka, da bi obezbedio neovlašćen pristup sistemu. Protokoli koji koriste clear tekst komunikaciju odnosno nemaju u sebi podržanu enkripciju i sav saobraćaj se može pročitati iz fajla (pcap – packet caputre) u kome su smešteni „hvatani“ paketi. [625] U ove protokole spadaju FTP (port 20-data/21-control), Telnet (port 23), SMTP (port 25), HTTP (port 80), POP3 (port 110), IMAPv4 (port 143), NETBIOS (port 139/445), SNMP (port 161/162), SQLnet (port 1521).

   Rešenje: *Izbegavati upotrebu servisa koji omogućavaju komunikaciju u čistom tekstu. Umesto njih upotrebljavati servise koji omogućuju zaštićenu komunikaciju (npr. SSH i HTTPS, HTTP over TLS/SSL).*

625 Linux sistemi ostvaruju „hvatanje“ paketa (packet caputre) uz pomoć libpcap biblioteke, a Windows sistemi koriste prilagođenu verziju biblioteke libpcap koja se zove WinPcap.

Segmentiranja mreže sa korišćenjem VLAN-ovim (eng. virtual local area networks) na svičevim i ruterima može pomoći u zaštiti od sniffera. Da bi mrežni saobraćaj bio bolje zaštićen upotrebljavaju se protokoli koji podržavaju enkripciju kao što je SSH , SFTP HTPS i dr. Kada se protokoli koji koriste clear text komunikaciju konfigurišu da upotrebljavaju enkripciju SSL/TLS oni rade preko drugih portova u tom slučaju HTTPS koristi port 443, FTP 989-data/990-control, Telnet koristi port 992, IMAP koristi port 993 POP3 koristi port 995 SMTP sa SSL koristi port 465, SMTP sa TLS koristi port 587.

4. *Ranjivosti zbog dozvola nad fajlovima (eng. file permissions)* - Upotreba neodgovarajućih dozvola nad fajlovima može biti potencijalni bezbednosni problem iz nekoliko razloga. Kao prvo dozvole nad fajlovima ne određuju samo pristup nekom fajlu, nego i mogućnost pokratanja programa na sistemu. Drugo, određeni programi su pokrenuti u ime korisnika sa najvećim privilegijama, pa se lošim konrifgurisanjem privilegija nad ovim programima može desiti da napadač dobije veća prava pristupa. U praksi se dešava da su određeni programski direktorijumi podešeni tako da grupa "everyone" ima sva prava (pod Windows i pod Linuxom bi to bila grupa „other"), što ostavlja zlonamernim napadačima otvorena vrata na sistemu.

   Rešenje: *Periodično pregledati dozvole nad fajlovima i folderima i postaviti ih na najrestriktivniji mogući nivo koji omogućuje neophnodnu operativnost u mreži sa deljenim resusrima.*

5. *Ranjivost usled korišćenja slabih šifri* - Jedna od najvećih ranjivosti na sistemu je upotreba slabih šifri za autentifikaciju i slabih autentifikacionih metoda. I pored postojanja načina da se zapamte jake šifre u praksi je čest slučaj da korisnici izaberu nebezbedne šifre koje se lako pamte. Razlog je uglavnom nedostatak svesti o bezbednosti kod korisnika. Novi tzv. crack-password progarami su u stanju da razbiju šifru koja se nalazi u rečniku za manje od minuta. Ovi programi takođe su u stanju da lako razbiju i male modifikacije sa rečima iz rečnika (npr. dodavanjem broja ispred ili iza reči, permutacija reči unazad). Čest je slučaj da korisnici upotrebljavaju još jednostavnije šifre kao na primer: imena, datumi, sportski timovi i druge činjenice koje se mogu lako pretpostaviti, čineći šifre još ranjivijim. U praksi se

dešavaju i situacije u kojima se najmoćnijim nalozima (admin, root) daju slabe šifre da bi više administratora moglo da zapamti tu šifru ili se šifre ne ažuriraju na redovnoj osnovi.

Rešenje: *Svaki administrator mora da ima svoj nalog koji pripada grupi "administrators" (kod Windows sistema), odnosno prijava administratora na svoj nalog i upotreba komande „su" odnosno „sudo" prilikom izvršenja admin operacija (kod Linux sistema). Korisnici i administratori moraju da odaberu jake šifre koja sadrži upotrebu velikih i malih slova, brojeva i znakova sa minimum 10 karaktera bez upotrebe reči iz rečnika. Šifra se mora podesiti da ističe često (u zavisnosti od pristupa osetljivim informacijama) uz sprečavanje upotrebe starih šifri. Ima dosta alata za testiranje šifri koji se mogu naći na internetu, a najčešće korišćeni su L0phtCrack*[626] *i John the Ripper.*[627] *Na Windows računarskim sistemima u politici administriranja sistema potrebno je zahtevati upotrebu jakih šifri (eng. strong password enforcement). Postupak je prikazan u Microsoft dokumentu „Strong Password Enforcement and Passfilt.dll".*[628] *Da bi se dodatno zaštitila SAM (Security Accounts Management) baza*[629] *na Windows sistemima moguće je upotreba SysKey alatke prema preporuci Microsofta.*[630] *Cilj upotrebe ove alatke jeste dodavanje drugog sloja zaštite nad heširanim šiframa. Na starijim Linux sistemima (kao na primer Slackware 2.3, Slackware 3.0) obavezno treba omogućiti shadowing šifri (čime se omogućava pristup heširanim šiframa samo root korisniku) uz pomoć Shadow Suite-a.*[631] *Kad je reč o autentifikacionom problemu treba istaći da se u praksi većina sistema oslanja na upotrebu korisničkih imena i šifri, matičnih brojeva ili kolačića kao autentifikacionih mehanizama. U praksi forenzičke analize zlonamerni napadači su lako zaobilazili pomenute autentifikacione mehaizme i dobijali neovlašćen pristup nalogu, podacima i servisima. Ključ za poboljšanje bezbednosti na sistemu jeste upotreba jakih autenfikacionih mehanizama kao što je postojanje PKI,*

626 L0phtCrack, http://www.l0phtcrack.com/, 11.06.2016.

627 John the Ripper password cracker, http://www.openwall.com/john/, 11.06.2016.

628 Strong Password Enforcement and Passfilt.dll, Microsoft, http://msdn.microsoft.com/en-us/library/ windows/desktop/ms722458%28v=vs.85%29.aspx, 11.06.2016.

629 SAM baza sadrži kopije heš vrednosti korisničkih šifri.

630 How to use the SysKey utility to secure the Windows Security Accounts Manager database, Microsoft, http://support.microsoft.com/kb/310105, 11.06.2016.

631 Getting the Shadow Suite, History of the Shadow Suite for Linux, http://www.tldp.org/HOWTO/ Shadow-Password-HOWTO-3.html, 11.06.2016.

korišćenje digitalnih sertifikata, smart-kartica, jednovremenskih šifri, dvofaktorske autentifikacije (nešto što korisnik ima-Token i nešto što korisnika zna-PIN), ili trofaktorske autenfikacije (nešto što korisnik ima-Token, nešto što korisnika zna-PIN, i nešto što jeste - biometrija) u zavisnosti od osetljivosti podataka na sistemu. Pomenuti mehanizmi za proveru identiteta su odlični primeri za poboljšanje bezbednosti na sistemu ali su veoma skupi i složeni za implementaciju pa je to jedan od razloga što nisu dostupni na većini sistema.

6. *Ranjivost usled korišćenja šifri koje ne ističu* - Postavljanje šifri koje ne ističu predstavljaju bezbednosni propust. Time se omogućava napadaču efikasniji brute force napad na šifre. Ovaj napad može imati više uspeha ukoliko je na sistemu podešeno da lozinka ne ističe.

   Rešenje: *Podesiti isticanje korisničkih šifri. Ukoliko se korisnički nalog ne koristi treba ga obrisati ili onemogućiti. Kod Microsoft Windows OS, ukoliko je u pitanju nalog koji je ugrađen u sistem kao na primer IUSR_ ili IWAM_, treba podesiti za njih opciju "User cannot change password" da se prikazuje kao ranjivost u izveštaju (Microsoftova preporuka je da se sistemskim nalozima zabrani izmena šifri). Sa druge strane treba omogućiti isticanje šifri nečekiranom opcijom "Password never expires".*

   Za Microsoft Windows Vistu, Microsoft Windows Server 2008 postupak je sledeći:
   1. Otvoriti Windows Control Panel;
   2. Odabrati "Administrative Tools";
   3. Da bi se promenile domain-wide lockout policy, odabrati "Domain Security Policy" (ili "Domain Controller Security Policy") ukoliko je računar domenski kontroler. U slučaju da se ova politika menja na lokalnom računaru odabrati "Local Security Policy";
   4. Proširiti folder "Account Policies" i odabrati "Password Policy";
   5. Podesiti Maximum Password Age. Ova vrednost predstavlja maksimalnu dužinu trajanja šifre. Preporučena vrednost može kreće se između 30 i 90 dana u zavisnosti od privilegija naloga;
   6. Restartovati sistem da bi se efekti primenili.

   Za Microsoft Windows 2000 Server, Microsoft Windows Server 2003 postupak je sledeći:

1. Otvoriti "Administrative Tools" iz Control panel-a;
2. Dva puta kliknuti na "Active Directory Users and Computers";
3. Dva puta kliknuti na željenog korisnika;
4. Kliknuti na "Account" tab;
5. Odčekirati "Password never expires".

Za Microsoft Windows XP Professional i Windows 2000 Professional postupak je sledeći:

1. Desni klik na "My Computer";
2. Odabrati opciju "Manage";
3. Otvoriti folder "Local Users and Groups";
4. Otvoriti folder "Users";
5. Dva puta kliknuti na željenog korisnika;
6. Odčekirati "Password never expires".

Za Microsoft Windows NT postupak je sledeći:

1. Kliknuti na dugme "Start" na Task Bar-u;
2. Odabrati folder "Programs";
3. Odabrati folder "Administrative Tools";
4. Odabrati "User Manager";
5. Dva puta kliknuti na željenog korisnika;
6. Odčekirati "Password never expires".

Kod Linux OS upravljanje isticanjem korisničkih šifri radi se sa alatom „chage":

chage –M dužina_dana korisničko_ime

7. *Ranjivosti CGI (eng. common gateway interface)* - mogu se pronaći na velikom broju web servera.[632] CGI programi omogućuju interaktivnost na web stranici kroz prikupljanje informacija, pokretanje programa ili pristupanje direktorijumima i fajlovima. S obzirom da se CGI programi pokreću sa istim privilegijama kao i web server program to za posledicu može imati da zlonamerni napadač koji zloupotrebi ranjiv CGI može izmeniti ili obrisati web strane, pristupiti osetljivim informacijama ili komrpomitovati sistem.

632 CGI je vrsta programskog jezika kojeg programeri koriste da bi se prikazalo i isčitalo ono što se unosi u web pretraživač (eng. web browser) i omogućava pravljenje dinamičkih web strana. U stvari predstvalja jedan od načina za programe i skripte na serveru kako da komuniciraju sa web pretraživačima.

Rešenje: Web *servisi ne smeju da se pokreću u ime administratora ili roota. Programski interpretori kao što su „perl" i „sh" ne smeju se nalaziti u direktofijumu CGI programa. Njihovom ostavljanjem zlonamerni napadači mogu izvršiti maliciozne CGI skripte. Treba vršiti analize ranjivosti sa ciljem pronalaženja ranjivih CGI programa i primenom adekvatne zakrpe sistem će se zaštititi od pomenute potencijalne ranjivosti.*

8. *FTP i Telnet ranjivosti* – Korišćenje ftp i telenet servisa predstavlja potencijlni bezbednosni problem, zbog uspostavljanja nezaštićene komunikacije. U praksi je čest slučaj da sistemi sa omogućenim FTP servisom dopuštaju anonimno logovanje (preko usera anonymous). Korisnik anonymous ima isključivo privilegije za čitanje, ali svako pravo čitanja može se zlupotrebiti za sticanje dodatnih informacija potrebnih zlonamernom napadaču za kompromitovanje sistema. Nepravilnim konfigurisanjem korisnik anonymous može da dobije prava upisa ili čak mogućnost da pristupa direktorijumima van FTP okruženja (npr. u pod Linuxom /etc/passwd, /etc/shadow ili pod Windowsom /winnt/repair/sam.*). Dodatno mnoge verzije FTP servera imaju ranjivosti koje mogu da dovedu do kompromitovanja računarskog sistema. Na primer, određena verzija WFTP servera je imala ranjivost na nekoliko buffer overflows napada sa kojima bi zlonamerni napadač nakon izvršenog koda dobio pristup strukturi fajlova i direktorijum na sistemu.[633]

   Rešenje: *Ukoliko telnet i FTP servisi nisu potrebni na sistemu njih treba ukloniti nakon difoltne instalacije sistema. Umesto njih koristiti SSH i SFTP servise koji obezbeđuju zaštićenu (šifrovanu) komunikaciju. U cilju povećanja bezbednosi bitno je da administratori na sistemu ograniče login pristup sistemu za pomenute aplikacije prema IP-adresama uz pomoć TCP Wrapper-a ili upotrebe Denyhost programa.*[634]

9. *ICMP ranjivost* – ICMP je čuven na osnovu korišćenja ping i traceroute (ili tracert) alata (koji generiše icmp pakete) i mnogi drugih DOS alata. Ranjivosti ICMP se vezuju za dobijanje informacije o mrežnoj masci, vremenskih pečata i drugih korisnih informacija. U praksi je čest slučaj da se ICMP saobraćaj ne blokira u organizacijima u okviru

633 Davidovac Z., Korać V., *Vulnerability management and patching it systems*, Arheologija i prirodne nauke, br. 6, 2011, str. 129-144.

634 DenyHosts, http://denyhosts.sourceforge.net/, 15.06.2016.

svojih rutera i firewalla. Razlog je taj što se ping i traceroute alati koriste za rešavanje mrežnih problema na računarima ili mrežnim uređajima (provera rada mrežnih kartica) i detektovanje mesta gde nastaju greške u mrežnoj komunikaciji. Napadači su preko ping komandi u mogućnosti da identifikuju potencijalne mete.

ICMP protokol može uz pomoć solicitation paketa da preda informaciju o gateway klijentima na osnovu koje će oni zapisati novu rutu u ruting tabeli u okviru svoje IP konfiguracije. U tom slučaju zlonamerni računar izvodi man in the middle napad, lažno se predstavljajući klijentu kao gateway, a gateway se predstavlja kao klijent. Na taj način vrši se rerutiranje paketa i zlonamerni računar prikupljajući sve pakete vrši prisluškivanje saobraćaja. Takođe ICMP se može zloupotrebiti za prenošenje podataka što predstavlja napad tipa curenje informacija. Onemogućavanjem upotrebe ICMP komunikacije u bezbednosnom smislu otežaće se skeniranje mreže od strane zlonamernih napadača. Određeni programi za skeniranje mreže su konfigurisani da ne skeniranju sisteme koji ne reaguju na pingovanja.

Rešenje: *Upotrebu ICMP komunikacije bi trebalo zabraniti na ruteru i firewallu u okviru organizacije. Ukoliko je ona neophodna zbog potreba rešavanja mrežnih problema, treba je ograničiti samo na određene računarske sisteme. Na OS to se može uraditi na prikazane sledeće načine.*

Za Windows 2000 onemogućavanje ICMP timestamps odgovora vrši se uz pomoć IPSec filter-a na osnovu definisanja i primene IP filter liste koja blokira ICMP types 13 (timestamp request) ICMP type 14 (timestamp response). Mogućnost blokiranja ICMP timestamps preko podešavanja u okviru "Networking and Dialup Connections" nije moguće. Detaljan opis korišćenja IPSec IP filter listi pod Windows 2000 prikazano je u Microsoft dokukmentu „How to use IPSec IP filter lists in Windows 2000“.[635]

Za Windows XP i Windows 2003 onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows firewalla:

1. Network Connections control panel;
2. Desni klik na Network adapter i odabrati opciju “properties”;
3. Odabrati tab “Advanced”;

635 How to use IPSec IP filter lists in Windows 2000, Microsoft, http://support.microsoft.com/kb/313190, 15.06.2016.

4. Pod Windows Firewall box-om, izabrati “Settings”;
5. Selektovati tab “General”;
6. Omogućiti firewall selektovanjem opcije “on (recommended)”;
7. Odabrati tab “Advanced” tab;
8. U ICMP box-u, odabrati opciju “Settings”;
9. Deselektovati opciju “Allow incoming timestamp request”;
10. Odabrati opciju “OK” i snimiti podešavanja za ICMP Settings;
11. Odabrati opciju “OK” i snimiti podešavanja za Windows firewall dijaloga;
12. Odabrati opciju “OK” i izaći iz internet adapter dijaloga.

Za Microsoft Windows Vista i Microsoft Windows Server 2008 onemogućavanje ICMP timestamps odgovora vrši se preko komandne linije alatom „netsh“:

1. Otvoriti Windows Control Panel;
2. Odabrati “Windows Firewall”;
3. Odabrati “Change Settings”;
4. Omogućiti fajervol odabirom opcije “on (recommended)”;
5. Otvoriti Command Prompt;
6. Ukucati komandu “netsh firewall set icmpsetting 13 disable”.

Više detalja oko podešavanja firewalla izloženo je u Microsoft-ovoj dokumentaciji.[636] Najefikasniji i najjednostavniji način onemogućavanja ICMP komunikacije je konfigurisanje firewalla da blokira dolazne i odlazne ICMP pakete tipa ICMP 13 (timestamp request) i tipa ICMP 14 (timestamp response).

Za Linux OS:

Nažalost na Linuxu nije moguće modifikacijom parametra kernela preko sysctl (kao kod OpenBSD) ili preko /proc/sys/net/ipv4 interfejsa onemogućiti ICMP timestamp responses, već se to radi uz pomoć firewalla iptables.[637]

Na primer:

ipchains -A input -p icmp --icmp-type timestamp-request -j DROP
ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP

636 Http: //www. microsoft. com/ resources/ documentation/ windows/ xp/ all/ proddocs/ en-us/ hnw _understanding _firewall. mspx?mfr =true, 15.06.2016.

637 Kod OpenBSD sistema onemogućavanje ICMP timestamp odgovora (eng. responses) se vrši podešavanjem “net.inet.icmp.tstamprepl” varijable na nulu: # sysctl -w net.inet.icmp. tstamprepl=0.

10. *Ranjivosti usled nedostatka monitoringa i detekcije upada* - Nedostatak monitoringa i detekcije upada za posledicu može imati neprimećeno testiranje slabosti računarskih sistema ili neprimetan upad na sistem od strane napadača. U praksi česta su sledeća tri slučaja: ne vrši se monitoring ili nepostoji sistem za detektovanje upada, sistem za detekciju postoji, ali nije pravilno konfigurisan i sistem za nadziranje postoji, ali se ne proverava redovno. Ukoliko se ne detektuju pokušaji upada na sistem napadač može upotrebljavati veliki broj alata (npr. brute-force napad), dok ne prepozna određene slabosti na sistemu, da bi na kraju izvršio i kompromitovanje sistema.

    Rešenje: *Postojanje odgovarajućeg sistema za praćenje i detekcije upada su od suštinskog značaja za bezbednost sistema.*

11. *Ranjivosti SMTP (Simple Mail Transport Protocol) servisa* - SMTP predstavlja osnovni protokol sloja aplikacija za elektronsku poštu, koji koristi uslugu pouzdanog transfera podataka protokola TCP.[638] Definisan je u dokumentu RFC 821.[639] Postoji veliki broj implementacija SMTP servisa (npr. Sendmail, Postfix, Qmail, Novell GroupWise, Exim, Novel Netmail, Microsoft Exchange Server). Sve implementacije imaju svoje ranjivosti i u praksi su se pokazale sličnim. Ranjivost Sendmail SMTP implementacije biće prikazana u daljem tekstu. U praksi iskorišćavanje SMTP ranjivosti realizuje se sa exploitima koji mogu da izvode prepunjavanje bafera (eng. buffer overflow), slanjem spam poruka kao i onemogućavanjem servisa.

    Rešenje: *Upotreba najnovijih implementacija SMTP servisa. Konstantno praćenje informacija koje se odnose na ranjivost i primenu poslednjih zakrpa za SMTP servis.*

12. *Ranjivost usled postojanja pokaznih tj. fajlova primera (eng. sample files) na web serveru* - U praksi sa instalacijom web servisa po difoltu dolaze i fajlovi sa primerima za pomoć pri instalaciji i konfigurisanju servisa.

638 SMTP, Wikipedia, http://sr.wikipedia.org/sr/SMTP, 17.06.2016.
639 Jonathan B. Postel, SIMPLE MAIL TRANSFER PROTOCOL, http://tools.ietf.org/html/rfc821, 17.06.2016.

Microsoft IIS,[640] Apache,[641] Adobe ColdFusion,[642] Oracle iPlanet Web Server,[643] i drugi web serveri dolaze sa pomenutim pokaznim fajlovima. Ovi fajlovi iako su veoma korisni administratorima za konfiguraciju servisa i programerima za razvoj web servisa, mogu biti ranjivi kao na primer IIS Showcode.asp.[644] Zlonamerni napadači kompromituju poznati kod iz pokaznih fajlova tako da on izvršava neautorizovane funkcije. S obzirom da napadači poznaju lokacije ovih fajlova na sistemima, mogu planirati precizan napad na njih.

Rešenje: *Najbolja odbrana ovih fajlova je njihovo uklanjanje sa web servera. Ipak, ukoliko su oni neophodni treba izvršiti njihovo premeštanje na druge lokacije tako da ne budu na produkcijskim sistemima. Dodatno izvršiti skeniranje ranjivosti sa ciljem identifikovanja slabosti koje se odnose na web servise.*

13. *Ranjivost usled pristustva virusa i skrivenog malicioznog koda* - Bezbednosne pretnje od virusa variraju u zavisnosti od tipa zlonamernih aktivnosti koje će se izvršiti. Dok neki virusi donose samo jednostavne neprijatnosti, drugi omogućavaju neautorizovan pristup računarskom sistemu, onemogućavaju servise i mnoge druge nedozvoljene aktivnosti. Kada su virusi u pitanju široko rasprostranjeni problem nastao je zbog sposobnosti napadača da vešto sakriju maliciozni kod. Na taj način korisnik nesvesno izvršava ovaj kod čime može biti ugrožena bezbednost sistema ili mreže u okviru organizacije. Antivirusni skeneri su prilično napredovali, ali njihova efikasnost je bazirana na ažuriranosti virusnih definicija. Problem se javlja kada se pojavi novi virus koji nije uvršćen u antivirusne definicije. Antivirusni skener ga neće prepoznati i on može biti propušten. Antivirusni alati koji primenjuju heuristističan pristup i sandbox za pronalaženje novih nedefinisanih virusnih pretnji. *Heuristika* podrazumeva sistemsku pretragu na zlonamerne kodove ili programe koji liče ili koji bi mogli biti virusi. *Sandbox* pristup podrazumeva izvršavanje koda u strogo konrolisanom okruženju (karantin) ispitujući njegove aktivnosti.

640 Http://www.iis.net/, 17.06.2016.
641 HTTP Server Project, Apache, Http://httpd.apache.org/, 17.06.2016.
642 Adobe ColdFusion, http://www.adobe.com/products/coldfusion-family.html, 17.06.2016.
643 Oracle, http://www.oracle.com/ technetwork/ middleware/ iplanetwebserver - 098726.html, 17.06.2016.
644 NT IIS Showcode ASP Vulnerability, Security Focus, http://www.securityfocus.com/ bid/167, 17.06.2016.

Ukoliko je program prepoznat kao virus on se pakuje u karantin i šalje se upozorenje o virusu. Heuristika i sandbox su od velike pomoći za prepoznavanje virusa koji još nisu uvršćeni u najnovije virusne definicije. Pomenuto skrivanje malicioznog koda je u direktnoj vezi sa virusima. Napadač može prevariti korisnika tako da korisnik nije svestan da je pokrenuo zlonamerni kod i omogućio napadaču pristup internoj mreži ili sistemu. Na primer, napadači mogu da sakriju zlonamerni JAVA ili Active X kod na udaljenom web serveru. Prilikom pretraživanja strana na malicioznom web serveru korisnik neznajući pokreće zlonamerni kod čime kompromituje sistem. U praksi je čest slučaj da je zlonamerni kod ubacivan u elektronske poruke ili atačmente poruka. Izvršenjem tih kodova ili skripti iz elektronski poruka otvara se pristup, kako direktan pristup samom sistemu omogućujući napadaču zaobilaženje firewalla i drugih vidova kontrole, tako i indirektan pristup internoj mreži.

Rešenje: *Uklanjanje ranjivosti ovog tipa podrazuma slojevit pristup zaštiti. Na prvom mestu je edukacija korisnika o riziku koji nosi otvaranje elektronske pošte nepoznatog porekla. Postojanje antivirusnog servera sa heurističnim skeniranjem pozicioniranim na tački pristupa mreži (na samoj granici) na mestu gde može da se skenira sva elektronska pošta, atačmenti i internet download pre njihovog ulaska u mrežu. Zaštita na osnovu upotrebe slojevitog skeniranja (heuristika, desktop skeniranje, skeniranje gateway-a) povećavaju šanse za zaustavljanje onih virusa koji su zaobišli prvu ili drugu liniju odbrane od virusa. Dodatno, treba onemogućiti pokretanje udaljenih (eng. remote) JAVA i Active X skripti na veb pretraživačima. Potrebno je koristiti alate za onemogućavanje izvršenja zlonamernih programa u cilju zaštite sistema. Alatka Cryptoprevent – onemogućuje da se Cryptlocker i Cryptowall izvršavaju na Windows operativnom sistemu.* [645] *Radi u nekoliko modova: klasična zaštita (basic) – gde su podešena samo osnovna pravila za zaštitu od Cryptolockera, default mod u kome je podešen optimalan mod zaštite, ali nema mogućnost zaštite od novijih verzija zlonamernih programa (pogodan za većinu kućnih okruženja), i maximum protection mod koji je za preporuku gde je bezbednost na prvom mestu. U ovom modu sistem je zaštićen i od novijih verzija ovih zlonamernih programa ali zbog svoje restriktivnosti može na operativnom sistemu zabraniti određene servise, instaliranja određenih drajvera i dr. S obzirom da zlonamerni paketi mogu doći kroz tzv. wrapper*

645 Https://www.foolishit.com/cryptoprevent-malware-prevention/

fajlove (paketi koji sadrže istovremeno regularan program i zlonamerni program tako da se prilikom instalacije regularnog programa instaliraju i zlonamerni programi u skrivenoj formi), ukoliko je neophodna maksimalna zaštita od ovih zlonamenrih programa preporučeno je podešavanje maximum protection mod. Upotreba dodataka na internet pretraživačima (IE, Firefox) kao na primer Noscript, koja nudi kontrolu nad izvršavanjem skripti na korisničkom internet pretraživaču takođe je korisna sa aspekta zaštite.[646] *Na taj način moguće je sprečiti izvršenje zlonamernih skripti. Dodatno upotrebom ekstenzija za onemogućavanje prikazivanja sadržaja sa reklamama sprečiće se njihovo prikazivanje. Na taj način povećaće se zaštita na sistemu, jer u praksi se pokazalo da se veliki broj zlonamernih programa instalirao kroz određene reklamene prozore. Ekstenzija Adblock Plus je dobra alatka za sprečavanje prikazivanja marketninških banera, zlonamernih programa i blokira kolačiće za praćenje (eng. tracking cookie).*[647] *Takođe korisno je i ručno pretražiti koji su to plug-inovi ili add-in-ovi i obrisati ih, što je teži način njihovog uklanjanja jer se prikrivaju sa prepoznatljivim imenima. To se može ustanoviti sa alatkom CCleaner koja može da pruži informacije o instaliranim plug-in-ovima na postojećim internet pretraživačima (podržani su gotovo svi značajni pretraživači) na sistemu u vidu parametara opisa i izdavača. Ukoliko informacija o izdavaču ne postoji ili je unknown velika verovatnoća je da se radi o neželjenom dodatku ili zlonamernom programu.*

4.1.2. Ranjivosti na Windows sistemima

1. *Postojanje UNICODE ranjivosti na IIS serveru kod OS Windows NT i Windows 2000.* IIS predstavlja web server koji je prisutan na Microsoft Windows familiji servera.[648] Nekoliko crva tipa Red Worm, Red Worm II i Nimda, su isprogramirani da zloupotrebe IIS Unicode ranjivost. Iskorišćavanjem ovih ranjivosti osim omogućavanja napadačima administratorskih privilegija, moguće je pokretanje zlonamernog koda na kompromitovanom sitemu sa eskaliranjem daljeg kompromitovanja. UNICODE ranjivosti se mogu vizuelno otkriti u log fajlovima zbog karakterističnog znaka „%“ praćenog

646 Https://noscript.net/, 16.08.2016.
647 Https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/, 17.08.2016.
648 Marvin Marin, Malware FAQ: Windows NT UNICODE Vulnerability Analysis, SANS, http://www. sans.org/security-resources/malwarefaq/wnt-unicode.php, 17.06.2016.

brojevima kao na primer „%255a“ ili „%a1%1a“ (kao NIMDA crva).[649]

Rešenje: *Sisteme je moguće zaštiti od ovih ranjivosti instaliranjem najnovijih bezbednostnih update-a i service pack-a. Preporuka je da se ne koriste difoltna imena za direktorijume i deljene resurse prilikom instalacije IIS-a uz pažljivo postavljanje dozvola na direktorijumima. Treba onemogućiti sve nepotrebne funkcije i ekstenzije u okviru IIS-a.*[650]

2. *Programske ranjivosti* - Predstavljaju opštu kategoriju koja se odnosi na programske greške ili propuste koji omogućavaju napadačima da izvrše kompromitovanje sistema. Na primer, ranjivost Compaq Web-Based Management buffer overflow može da omogući napadaču da iskopira SAM fajl na Windows serveru 2000 van direktorijuma „system repair“.[651] Ako se ova programska ranjivost prepozna na vreme i program zakrpi, to će zaštiti sistem od potencijalnog kompromitovanja izazvanog propustom u pomenutom programu.

   Rešenje: *Treba vršiti analize ranjivosti sa ciljem prepoznavanja instaliranih programa na sistemu da bi se ustanovilo da li za instalirane programe postoji exploit koji može da dovede do kompromitovanja sistema. Ukoliko se pronađe takav program primenom adekvatne zakrpe sistem će se zaštititi od pomenute potencijalne ranjivosti.*

3. *Ranjivost ISAPI (eng. Internet Server Application Programming Interface) extension prepunjavanje bafera (eng.buffer overflows)*[652] - Neke od ISAPI aplikacija realizovane preko ISAPI ekstenzija su:[653]
   -ASP (eng. Active Server Pages),[654] standardno je instaliran na IIS;

649 Tom Rodriguez, IDFAQ: What are unicode vulnerabilities on Internet Information Server (IIS)?, SANS, http://www.sans.org/security-resources/idfaq/iis_unicode.php, 17.06.2016.
650 Tom Rodriguez, IDFAQ: What are unicode vulnerabilities on Internet Information Server (IIS)?, SANS, http://www.sans.org/security-resources/idfaq/iis_unicode.php, 17.06.2016.
651 Nelson B., Phillips A., Steuart C., *Guide to Computer Forensics and Investigations – fourth edition, Fourth Edition*, Course Technology, Cengage learning, Boston, 2010.
652 IBM X-Force Exchange, http://www.iss.net/security _center/ reference/ vuln/HTTP _IIS_ Index _Server_Overflow.htm, 17. 06. 2016.
653 Internet Server Application Programming Interface, Wikipedia, http://en.wikipedia.org/ wiki/ Internet_ Server_Application_Programming_Interface, 17.06.2016.
654 Active Server Pages, Wikipedia, http://en.wikipedia.org/wiki/Active_Server_Pages, 31.03.2016.

-ASP.NET,[655] standardno je instaliran od verzije IIS 6.0 pa nadalje;

-ColdFusion,[656] poslednja verzija može se instalirati na IIS;

-Perl ISAPI (Perliis),[657] besplatan je za instalaciju;

-PHP,[658] besplatan je za instalaciju.

Primer za prepunjavanje bafera bi se mogao opisati na sledeći način: program očekuje da se unese maksimalno 90 karaktera i ukoliko on za input dobije 5000 karaktera postavlja se pitanje kako će program odnosno kod da reaguje na to. Iskorišćavanjem ISAPI ranjivosti moguće je dobiti punu putanju do web root direktorijuma kao što je to slučaj kod ranjivosti „Microsoft IIS HTR ISAPI Extension Buffer Overflow".[659]

Rešenje: *Treba vršiti analize ranjivosti sa ciljem prepoznavanja ranjivosti na IIS servisu, koji mogu da dovesti do kompromitovanja sistema. Ukoliko se ona pronađe primenom adekvatne zakrpe za sistem ili bezbednosnog update-a, sistem će se zaštititi od pomenute ranjivosti.*

4. *Ranjivost RDS-a (eng. Remote Data Service, komponente MDAC-a, eng. Microsoft Data Access)*[660] [661] - predstavlja bezbednosni propust u okviru Microsoft IIS-a (eng. Internet information server). Ukoliko se bezbednosni propust ne prepozna na vreme i ne zakrpi može doći do kompromitovanja web servera, kao što su to učinili crvi tipa Nimda i Code red.[662] Napadač može pokrenuti komande na udaljenom sistemu bez direktnog pristupa. Zloupotrebu ove ranjivosti prema Microsoftu moguće je prepoznati iz IIS "POST" logova na osnovu postojanja "/msadc/msadcs.dll" stavki.

Rešenje: *Da bi se izvršila adekvatna zaštita treba ispratiti uputstva data*

655 ASP.NET, Wikipedia, http://en.wikipedia.org/wiki/ASP.NET, 31.03.2016.

656 Adobe ColdFusion, Wikipedia, http://en.wikipedia.org/wiki/Adobe_ColdFusion, 31.03.2016.

657 Perl, Wikipedia, http://en.wikipedia.org/wiki/Perl, 31.03.2016.

658 PHP, Wikipedia, http://en.wikipedia.org/wiki/PHP, 31.03.2016.

659 Rapid, https://www.rapid7.com/db/vulnerabilities/http-iis-0013, 17.06.2016.

660 GIAC, http://www.giac.org/paper/gsec/19/vulnerability-microsoft-data-access-components-mdac-internet-information-server-iis/ 101517, 31.12.2016.

661 Microsoft Data Access Components, Wikipedia, http://en.wikipedia.org/ wiki/Microsoft _Data_ Access_Components, 31.03.2016.

662 Nimda, Wikipedia, http://en.wikipedia.org/wiki/Nimda, 24.04.2016.

od strane Microsofta,[663] *ili preporuku iz SANS dokumenta "Copyright SANS Institute".*

5. *Nezaštićeni deljeni mrežni resursi realizovani preko NETBIOS-a* - Deljenje resursa na NT sistemima je ranjivost baš kao i na Linux sistemima. Komunikacija sa deljenim resursima se obavlja preko portova 135-139. Na Windows 2000 port za komunikaciju je 445. Preko ovih portova dobijaju se informacije o broju korisnika, otvorenim deljenim resursima i sistemske informacije. Putem ovih portova zlonamerni napadač može zloupotrebljavati „NET" komande kako bi došao do informacija koje mogu poslužiti za dalju zloupotrebu. U praksi je čest slučaj da se deljeni resursi zloupotrebljavaju u svrhu prostora za skladištenje nedozvoljenog sadržaja.

   Rešenje: *Svi neopotrebni portovi bi trebali biti onemogućeni na firewallu spolja, a administrator bi posebno morao da proveri da li su portovi 135-139 i 445 zatvoreni.*

6. *Null session ranjivost* - Curenje informacija (eng. leakage) preko konekcije null sesije (eng. null session). Konekcija null sesije poznata je kao anonimno logovanje (eng. anonymous logon). Predstavlja mehanizam koji omogućava korisniku da anonimno preuzima informacije sa mreže ili da se anonimno autentifikuje na sistem.[664] Null sesije iskorišćavaju greške u CIFS (eng. Common Internet file system)/SMB (eng. Server Messaging Block). Nul sesija zahteva pristup preko porta TCP 139 ili TCP 445. Pogođeni sistemi su Microsoft Windows NT, 2000 and XP.
   Na koji način otkriti ovu slabost? Najbolji način je testirati sistem konektovanjem preko Null sesije sa sledećim komandama (u zavisnosti od tipa NT sistema):

*NET USE \\ime ili adresa računara\IPC$ * /USER:*

663 Microsoft Security Bulletin MS01-044 - Critical, Microsoft, http://technet.microsoft.com/en-us/security/bulletin/ms01-044, 24.04.2016.

664 Pod Windows 2000 mnoštvo lokalnih servisa radi pod nalogom LocalSystem koji se koristi za razne kritične sistemske operacije. Kada jedan računar treba da prezume podatke iz drugog računara (npr. pristup deljenim resursima i ostali network neighborhood funkcionalnosti) nalog LocalSystem će otvoriti nul sesije za drugi računar. Specifičnost je ta da taj nalog LocalSystem ima gotovo neograničene privilegije i nema šifre (što znači da se na sistem i ne može logovati preko LocalSystem naloga). Opasnost je ta što zlonamerni korisnici mogu da iskoriste neki exploit i da se prijave na nul sesiju da bi dobili pristup ciljanom računarskom sistemu.

*NET USE \\ime ili adresa računara\IPC$ * /USER:""*
NET USE \\ime ili adresa računara\IPC$ "" /USER:""

Ili iz linuxa: *# smbclient \\\\target\\ipc\$ "" –U ""*

Navedena sintaksa podrazumeva kontekovanje na skriveni Inter-procesni komunikacioni share (IPC$) ciljanog računara preko anonimnog korisničkog naloga (/u:""), koji je ugrađen u sistem sa blanko šifrom (""). Ukoliko je odgovor "connection failed" sistem nije ugrožen na ovaj tip slabosti. Ukoliko odgovora nema ili je odgovor "command was successfull" sistem je ranjiv. Ukoliko je sistem ranjiv napadač može pristupiti skrivenim deljenim resursima (eng. shares). Napadač može saznati postojeće korisničke naloge i grupe, njihov status, imena računara, registarska podešavanja, postojeće deljene resurse i računarske i korisničke bezbedonosne identifikatore (eng. Security Identifiers, SID) i druge informacije koje mogu pomoći da se organizuje zlonamerana aktivnost. U praksi napadači koriste i dodatne alate kao što su Wininfo i NAT (netbios auditing tool), kako bi saznali korisnička imena na ciljanom serveru i izvršili dictinary napad, a neretko se za napad na Windows NT koristio i sid2user alat.[665]

Rešenje: *Onemogućiti logovanje anonimnih korisnika. Na ovaj način će se zabraniti pristup informacijama anonimnim korisnicima, kojima eksplicitno nije dozvoljen pristup uključujući grupu Everyone i korisnike nulte sesije. Ova restrikcija može imati implikacija na sinhronizovanje sa domenom ili drugim servisima pa je pre upotrebe treba testrati na postojeće okruženje.*

Postupak za Microsoft Windows NT:

a. Izmena registarstkog ključa:
„HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\“
sa sledećim podešavanjima:
Value Name: RestrictAnonymous
Data Type: REG_DWORD
Data Value: 1
Posle ovih podešavanja neophodan je restart računarskog sistema.

Postupak za Microsoft Windows 2000:

665 Evgenii B. Rudnyi, http://evgenii.rudnyi.ru/programming.html#sid2user, 17.06.2016.

a. Izmena registarstkog ključa:
„*HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa*“
sa sledećim podešavanjima:
Value Name: RestrictAnonymous
Data Type: REG_DWORD
Data Value: 2

b. Dodatno otvoriti „Local Security Settings“ postaviti sledeće podešavanje:
Local Security Settings - Local Policies- Security Options-Additional restrictions of anonymous connections:No access without explicit anonymous permissions.
Posle ovih podešavanja neophodan je restart računarskog sistema.

Postupak za Microsoft Windows XP:

a. Izmena registarstkog ključa „*HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa*“
sa sledećim podešavanjima:
Value Name: RestrictAnonymous
Data Type: REG_DWORD
Data Value: 1
Value Name: RestrictAnonymousSAM
Data Type: REG_DWORD
Data Value: 1
Value Name: EveryoneIncludesAnonymous
Data Type: REG_DWORD
Data Value: 0

b. Izmena registarstkog ključa „*HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters*“
sa sledećim podešavanjima:
Value Name: RestrictNullSessAccess
Data Type: REG_DWORD
Data Value: 1
Value Name: NullSessionPipes
Data Type: REG_MULTI_SZ
Data Value: "" (prazan string bez navodnika)

c. Dodatno otvoriti „Local Security Settings“ postaviti sledeće podešavanje:

Security Settings - Local Policies - Security Options - Network access: Allow anonymous SID/Name translation: Disabled

Posle ovih podešavanja neophodan je restart računarskog sistema. Treba napomenuti da onemogućavanje „NULL sessions" može imati uticaj na funkcionalnost, kao i na neke mrežne programe.[666]

Postupak za Microsoft Windows 2003:

a. Izmena registarskog ključa *„HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\"*
   sa sledećim podešavanjima:
   Value Name: RestrictAnonymous
   Data Type: REG_DWORD
   Data Value: 1
   Value Name: RestrictAnonymousSAM
   Data Type: REG_DWORD
   Data Value: 1
   Value Name: EveryoneIncludesAnonymous
   Data Type: REG_DWORD
   Data Value: 0
   Value Name: TurnOffAnonymousBlock
   Data Type: REG_DWORD
   Data Value: 0
b. Izmena registarskog ključa *„HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\"*
   sa sledećim podešavanjima:
   Value Name: RestrictNullSessAccess
   Data Type: REG_DWORD
   Data Value: 1
   Value Name: NullSessionPipes
   Data Type: REG_MULTI_SZ
   Data Value: "" (prazan string bez navodnika)
c. Dodatno otvoriti „Local Security Settings" i postaviti sledeće podešavanje:
   Security Settings - Local Policies - Security Options - Network access: Allow anonymous SID/Name translation: Disabled
   Posle ovih podešavanja neophodan je restart računarskog sistema.

666 Efekti onemogućavanja NULL sesije objašnjeni su u Microsoft članku: *The effects of removing null sessions from the Microsoft Windows 2000 and Microsoft Windows NT environment,* http://support. microsoft. com/kb/890161, 19.06.2016.

Treba napomenuti da onemogućavanje „NULL sessions“ može imati uticaj na funkcionalnost, kao i na neke mrežne programe.[667]

Postupak za SAMBU na Linuxu:

Da bi se onemogućilo anonimno logovanje na SAMBU neophodno je modifikovati konfiguracioni fajl SAMBA servera „smb.conf“ sa sledećim podešavanjima:

guest account = nobody
restrict anonymous = 1

Obavezno proveriti da li postoji korisnik sa imenom „nobody“.

7. *Slabost heširanja u SAM (eng. Security accounts manager) bazi putem LAN menadžer heša (eng. Lan manager hash - LM hash)* - Windows generiše i skladišti šifre korisničkih naloga na dva različita načina, poznatog kao *heširanje*. Ukoliko se postavlja šifra čija je dužina ispod 15 karaktera, Windows generiše dve heš vrednosti LM heš i Windows NT heš šifre. Ove heš vrednosti se smeštuju u SAM bazu lokalno-ili u Aktvini direktorijum. LM heš je slabiji u poređenju sa NT heš i zato je skloniji–bržem brute-force napadu.[668] Zato je preporuka da se onemogući u Windows, čuvanje LM heš vrednosti šifri.

   Rešenje: *Detaljno uputstvo koje se odnosi na sprečavanje Windows OS da skladišti LM heširane šifre u aktivni direktorijum i lokalnu SAM bazu prikazano je u Microsoft članku „How to prevent Windows from storing a LAN manager hash of your password in Active Directory and local SAM databases“.*[669] *Verzije Windowsa na koji se članak odnosi su: Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows Server 2003.*

8. *Remote Administration Services* - Ova ranjivost potiče od načina upravljanja udaljenih sistema od strane administratora sistema. Ovi

667 Uticaji onemogućavanja NULL sesije objašnjeni su i u Microsoft članku: *Client, service, and program issues can occur if you change security settings and user rights assignments,* Microsoft, http:// support. microsoft.com/kb/823659, 19.06.2016.

668 How to prevent Windows from storing a LAN manager hash of your password in Active Directory and local SAM databases, Microsoft, http://support.microsoft.com/kb/299656, 31.03.2016.

669 How to prevent Windows from storing a LAN manager hash of your password in Active Directory and local SAM databases, Microsoft, http://support.microsoft.com/kb/299656, 19.06.2016.

sistemi upravljanja na daljinu iako su relativno sigurni imaju svoje ranjivosti. U praksi su najčešće upotrebljavani sistemi za udaljeno administriranje sistema: Symantec PcAnywhere,[670] Radmin,[671] DameWare Remote Support,[672] TeamViewer,[673] RealVNC.[674] Kompromitovanje ovih servisa prema forenzičkoj praksi najčešće je posledica kompromitovanja nedovoljnih ili loše konfigurisanih bezbednosnih kontrola uz upotrebu određenih exploita kako bi zlonamerni napadači dobili administratorske privilegije.

Rešenje: *Treba upotrebljavati samo bezbedne sisteme za udaljeno administriranje. Takvi sistemi moraju da omoguće zaštićenu komunikaciju (šifrovanu), sa podrškom za jaku autentifikaciju, mogućnost zaključavnja naloga nakon određenog broja neuspelih logovanja uz podršku za logovanje neautoruzovanih pokušaja. Potrebno je podesiti da se od korisnika računarskog sistema očekuje potvrda da prihvata udaljeno administriranje kao i ograničavanje programa na samo IP-adresu administratorske radne stanice.*

4.1.3. Ranjivosti na Linux sistemima

1. *Prepunjavanje bafera RPC (eng. Remote procedure call, RPC buffer overflows) servisa* - Ovi RPC servisi omogućavaju programima sa jednog računara da izvršavaju programe na nekom drugom računaru. Koriste se za pristup mrežnim servisima, kao na primer NFS. Greške i ranjivosti u RPC-u mogu biti aktivno eksploatisane. Postoje i dokazi da je prilikom izvršavanja DDoS napada tokom 1999. g. i početkom 2000. g. izvršeno upravo preko računara sa kompromitovanih RPC servisa.[675]

   Rešenje: *Ograničiti upotrebu RPC servisa samo na računare koji nemaju pristup internetu. Ukoliko su neophodni na firewallu blokirati pristup RPC servisima tako da napadači ne mogu pristupati tom*

670 Http://www.symantec.com/pcanywhere, 19.06.2016.
671 Remote Control Software, Radmin, http://www.radmin.com/, 19.06.2016.
672 DameWare, http://www.dameware.com/, 19.06.2016.
673 Team Viewer, http://www.teamviewer.com/sr/, 19.06.2016.
674 RealVNC, http://www.realvnc.com/, 19.06.2016.
675 Georgijević U., *Istražne metodologije, tehnike i alati za digitalnu forenzičku istragu*, master rad, Fakultet za informatiku i menadžment, Univerzitet Singidunum 2010.

servisu. Zaštitu od napada na RPC servis iz unutrašnje mreže moguće je ostvariti kroz onemogućavanje ovog servisa na sistemima gde on nije potreban. Na sistemima kojima je neophodan RPC servis obavezno je vršiti redovno ažuriranje i krpljenje servisa. Analizom ranjivosti na redovnoj osnovi moguće je otkriti ranjivu verziju RPC servisa.

2. *Sendmail ranjivosti* - Sendmail je program koji procesira odnosno prima, šalje i prosleđuje elektronsku poštu na Linux OS. S obzirom na njegovu široku rasporstranjenost vrlo često je na meti napadača. Tokom godina upotrebe pronađene su neke slabosti vezane za Sendmail, koje mogu napadaču da omoguće pokretanje komadi bez direktnog logovanja na kompromitovani računar i tako punu kontrolu nad računarom. U praksi prepoznata su tri najčešća exploita: exploit sa kojim se šalje spam, exploit koji šalje fajl sa šiframa i exploit koji izvršava DoS napad. Na primer: napadač šalje osmišljenu email poruku sa zlonamernim kodom na server na kome se nalazi Sendmail, Sendmail procesira tu poruku kao instrukciju u kome se zahteva slanje fajla sa šiframa, Sendmail šalje fajl sa šiframa napadaču na njegov računar gde će moći da razbije šifre.

   Rešenje: *Osavremenjivanje Sendmail-a poslednjom verzijom ili primena zakrpa (eng. patches) za postojeći Sendmail servis. Ne pokretati Sendmail servis u demon modu (eng. daemon mode) isključivanjem -bd switcha na računarima koji nisu podešeni kao mail serveri niti kao serveri za slanje pošte. (eng. mail relay server).*[676]

3. *Slabosti BIND (The Berkeley Internet Name domain) programa* - Bind je najrasprostranjeniji način implementacije DNS-a (eng. Domain name service) na osnovu koga se lociraju svi sistemi na internetu prema njihovim imenima kao na primer www.mi.sanu.ac.rs, bez potrebe da se znaju određene IP-adrese. Ovaj sistem koristi DNS da bi izvršio prevođenje imena računara u IP-adrese i obrnuto. S obzirom da su DNS servisi od krucijalnog značaja za normalno funkcionisanje interneta, njihova dostupnost na internetu ih čini omiljenom metom napadača. Prema SANS institutu u anketi koja je rađena 1999 godine čak 50% svih DNS servera, koji su povezani na

676 Hal Pomeranz, Deer Run Associates, Improving Sendmail Security by Turning it Off, http://www. deer-run.com/~hal/sysadmin/sendmail.html, 19.06.2016.

internet su imali ranjive verzije BIND servisa. Primer BIND napada: napadač briše sve logove na sistemu, instalira alate koje će mu omogućiti administratorska prava. Potom kompajlira i instalira IRC alate i alate za skeniranje mreže u potrazi za dodatnim sistemima koji imaju ranjive verzije BIND servisa. Za manje od minuta moguće je zloupotrebiti stotine udaljenih računarskih sistema što za posledicu nosi dalje kompromitovanje ostalih sistema. Ovaj primer ilustruje na koji način ranjivost DNS servera odnosno BIND-a, koji je odgovoran za realizaciju DNS-a, može da napravi potpuni haos. Korišćenje zastarelih verzija BIND-a nosi sa sobom i rizik zloupotrebe putem buffer overflow eksploita čime napadač može dobiti neovlašćeni pristup računarskom sistemu, a česti su i DoS napadi na ovaj servis.

Rešenje: *Osavremenjivanje Binda-a poslednjom verzijom ili primena zakrpa (eng. patches) za postojeći BIND servis. Preporuka je da se BIND servis pokreće u ime neprivilegovanog korisnika iz bezbednosnih razloga u slučaju nekog budućeg udaljenog napada. Preporuka je da se BIND realizuje u izolovanom (chroot) direktorijumskom okruženju zbog zaštite od budućih udaljenih napada.*[677] *To znači da ukoliko neko uspe da izvrši udaljeni napad na BIND servis najviše što će moći je manipulisanje sa fajlovima u direktorijumu u kome je BIND zaključan.*

4. *Slabosti DNS servisa* - DNS servis na osnovu svoje izloženosti može uticaj na bezbednost sistema. Kao što je već pomenuto sistemi koriste DNS za prevođenje imena računara u IP-adrese i obrnuto. U praksi je slučaj da su serveri konfigurisani na takav način da šalju veliki broj informacija o svojoj mreži. Na primer, DNS može biti tako konfigurisan da putem transfera zone sistema, napadač dobije informacije i o kompletnom domenu. Dodatno DNS rekordi mogu sadržati informacije kao što su adrese internih servera, tekstualni opisi servera, imena sekundarnih sistema kao i uloge određenih servera što može pomoći napadaču da organizuje napad.

677 Podešavanje Chroot okruženja podrazumeva da se za određeni program kao na primer za BIND folder proglasi za koren fajl sistema na primer "/isolation" umesto "/"). To znači da program koji radi u chroot okruženju ne vidi realan fajl sistem tj. "/", već samo taj izolovan folder "/isolation" i samim tim ne može da se nanese šteta OS u slučaju kompromitovanja izolovanog servisa. To znači da program koji radi u izolovanom chroot-ovanom okruženju, ukoliko želi da pristupi folderu /var/named, on će zapravo pristupiti folderu /isolation/var/named.

Rešenje: *Analizom ranjivosti potrebno je utvrditi koje informacije se šalju od strane DNS servera da bi se onemogućilo slanje suvišnih informacija, koje za posledicu imaju povećanje rizika od napada. Neophodno je konfigurisanje DNS servera tako da se ograniči transfer zone samo za određene IP-adrese koje zahtevaju ažuriranje zonskih informacija.*

5. *Upotreba "trust" komandi (eng. r commands ili relationship trust commands)*. Ukoliko je korisnik ulogovan na server koji sa drugim serverima ima uspostavljen "trust" odnos, korisnik može da se slobodno prijavljuje na te servere bez re-autentifikacije uz pomoć komandi rlogin (remote login), rsh (remote shell), rcp (remote copy).[678] Ove komande ne zahtevaju potvrdu identiteta što znači da korisnik ne mora ponovo da kuca šifru. Sa stanovišta praktičnosti "trust " odnos je odlična ideja, ali sa stanovišta bezbednosti predstavlja veliku potencijalnu opasnost. Ukoliko napadač dobije kontrolu na bilo kom računarskom sistemu koji je u "trust" odnosu, on može da dobije pristup svim drugim računarskim sistemima, koji imaju "trust" odnos sa kompromitovanim sistemom.

   Rešenje: *Proveriti da li postoji fajlovi .rhosts i i /etc/hosts.equiv . Ukoliko postoje onemogućiti upotrebu "trust" komandi editovanjem fajla /etc/inetd.conf.*

6. *LPD (eng. remote print protocol daemon)* - Ovaj servis (in.lpd) se upotrebljava za interakciju Linux korisnika sa lokalnim štampačem preko porta TCP 515. U praksi se pokazalo (npr. Solaris 2.6-8 Linux) da je buffer overflow ranjiv, što za posledicu može napadaču da donese root privilegije na računarskom sistemu u slučaju kompromitacije ovog servisa.

   Rešenje: *Sistem je ranjiv ukoliko nije odrađeno patchovanje ranjive verzije lpd. Zaštita se izvodi instaliranjem poslednje verzije ovog servisa ili patchovanjem lpd ranjive verzije. Ukoliko ovaj servis nije neophodan treba ga ukloniti sa sistema onemogućavanjem print servisa u /etc/inetd.conf i blokiranjme porta 515.*

678 Umesto zahteva za korisničkim imenom i šifrom udaljenom računaru je dovoljno samo definisana "trust" IP-adresa.

7. *Sadmind i Mountd* - Sadmind je Solarisov program koji omogućava udaljeni pristup računarskom sistemu i služi za admistriranje računarskog sistema (ima i svoj grafički interfejs). Izvršava sa na serveru uz pomoć klijentskog programa koga kontroliše sam korisnik. Mountd kontroliše pristup deljenim datotekama na mreži preko NFS na Linux sistemima. Ovi programi su ranjivi pa bi napadač preko exploita mogao da izazove buffer overflow i tako dobije root privilegije. Ovo je bio jedan od glavnih načina na koji su organizovani DDoS napadi na CNN, Yahoo i druge sajtove.[679]

   Rešenje: *Instaliranje poslednjih zakrpa za sadmind i mountd.*

8. *Upotreba difoltnih SNMP stringova* - SNMP (eng. The simple network management protocol) je protokol koji se najčešće koristi kao način praćenja i upravljanja uređajima na mreži (npr. rutera, switcheva, štampača, računara i ostalih mrežnih uređaja). Svrha upotrebe ovog protokola je dobijanje statusa, performansi i dostupnosti uređaja koji se prati. Koristi nešifrovan "community string" kao jedini autentifikacioni mehanizam, što je ujedno i velika slabost ovog protokola. Difoltna vrednost community stringa zavisi od proizvođača same mrežne opreme i uglavnom je postavljena na "public" (sa pravima čitanja) ili "private" (sa pravima čitanja i upisa). Ako napadač dobije pravo upisa na uređaju moguće su zloupotrebe u vidu rekonfiguracije samog uređaja, isključivanja uređaja ili instaliranja neautorizovanih servisa koji omogućuju "zadnja vrata" (eng. back door). Prisluškivanjem SNMP saobraćaja potencijalni napadač može otkriti mnogo, kako o strukturi same mreže tako i o računarskom sistemu i njegovim pridruženim uređajima kako bi što bolje planirano napad i fingirao cilj. Iako SNMP nije karakterističan samo za Linux već se koristi i na Windows računarskim sistemima, u praksi se pokazalo da je najviše napada bila upravo na Linux računarskim sistemima zbog loše SNMP konfiguracije.

   Rešenje: *Pri konfigurisanju izabrati jake šifre (community strings) sa većim brojem karaktera*[680]*, postaviti SNMP bazu podataka (eng.*

679 Grubor G., Funkcionalni model istrage kompjuterskog kriminala, Ziteh 2010.

680 Korišćenje jakih šifara podrazumeva upotrebu alfa-numeričkih karaktera dužine najmanje 10 karaktera uključujući velika i mala slova (eng. case sensitive).

management information base - MIB)[681] *na read only. SNMP pristup blokrati na firewallu, vršiti njegovu kontrolu kroz pristupne liste (eng. Access control list) na internim i eksternim ruterima.*

9. *Globalno deljenje fajlova (eng. global file sharing)* - Globalno deljenje fajlova na mreži podrazumeva deljenje datoteka između računara koji koriste Network Neighborhood (kod Microsoft Windows računara) ili NFS (kod Linux računara). Pristup prema podrazumevanoj postavci je za čitanje i pisanje (eng. read-write). To znači da svako na istoj mreži može pristupiti svim fajlovima. Na početku mreže su bile relativno male, ali sada kada je nastala globalna mreža internet, to nosi rizik da bilo ko može pristupiti fajlovima koji se dele na mreži. Najveća opasnost je za kućne korisnike koji imaju direktan pristup internetu preko modema (adsl modemi, kablovski modemi, telefonski modemi). Napadači mogu dobiti pristup ličnim podacima korisnika (npr. brojevima kreditnih kartica, tekućim računima, šiframa email naloga, itd).

   Rešenje: *Potrebno je pažljivo odrediti podatke za deljenje na mreži i osigurati da se podaci dele samo sa onima kojima su namenjeni.*

10. *Ranjivosti IMAP i POP* - Internet message access protocol (eng. IMAP)[682] i Post Office Protocol (eng. POP)[683] su najčešće korišćeni email protokoli koji korisnicima omogućavaju naprednije mogućnosti prilikom pristupanja svojim email nalozima sa udaljenih lokacija. IMAP i POP servisi takođe imaju svoje slabosti. Zaštitni zidovi obično su konfigurisani da propuštaju ove servise. Opasnost se krije u tome što napadači mogu da dobiju pristup internoj mreži i da kompromituju IMAP i POP mail server. Ukoliko je napad bio uspešan moguće je da preuzmu kontrolu nad sistemom.

---

681 MIB opisuje strukturu upravljanja podacima za određeni SNMP uređaj, http://en.wikipedia.org/ wiki/ Simple_ Network _Management_Protocol, 04.04.2016.

682 Ovaj protokol predstavlja protokol kojim se omogućava pristup email porukama na udaljenom serveru putem korisničkog lokalnog klijenta. Internet Message Access Protocol, Wikipedia, http://en .wikipedia. org/wiki/ Internet_Message_Access_Protocol, 26.04.2016.

683 Ovaj protokol predstavlja protokol za prenos elektronske pošte preko IP mreža (primanje email poruka sa udaljenog servera na lokalni email klijent korisnika), razvijan je kroz nekoliko verzija i trenutna verzija je POP3, http://sh.wikipedia.org/ wiki/ Post_ Office_Protocol, 19.06.2016.

Rešenje: *Analizom ranjivosti moguće je detektovati prisutnost ranjivih IMAP i POP servera. Ove servise treba postavljati samo na sistemima namenjinim za poštu odnosno mail serverima, ukoliko za njima ne postoji potreba treba ih ukloniti sa sistema. Treba redovno instalirati zakrpe koje se pojavljuju za pomenute servise odnosno, osvežavati ih najnovijim verzijama.*

11. *Ranjivosti na NFS-u (Network File system)* - NFS se koristi za deljenje fajlova i drajvova na Linux fajl sistemima. Eksportovani NFS sistemi koji su dostupni spolja (putem interneta) su potencijalna meta za napadače. Kompromitovanje NFS deljenih resursa od strane napadača može biti prouzrokovano lošim konfigurisanjem NFS dozvola. Posledica može biti takva da napadač može pristupiti osetljivim informacijama ili dobiti dozvole upisa na NFS sistem. Na primer, napadač može da unese ili izmeni .rhosts fajl u kome dodeljuje za svoju IP-adresu pristup sistemu putem rlogin-a. Postojanje ranjivosti NFS servisa zavisi od verzije nfsd-a, a one kritične omogućuju zlonamernom napadaču pristup fajl sistemu sa root privilegijama.

    Rešenje: *Ukoliko je NFS neophodan treba proveriti da li je ispravno konfigurisan. Portove koji se koriste za NFS (port 2049) treba blokirati na firewallu i filtrirati na ruteru. Dozvole za kontrolu pristupa moraju biti podešene na odgovarajući način (treba izbegavati korišćenje „no_root_squash" opcije). Treba vršiti periodičnu analizu ranjivosti, pratiti publikovane NFS ranjivosti i instalirati najnovije sigurnosne zakrpe za NFS servise.*

Treba spomenuti da postoji nekoliko besplatnih servisa koji publikuju nove ranjivosti koje se pojave. Sajtovi kao što su Security Focus,[684] The Computer Security Division of the National Institute for Standards and Technologies (NIST) ICAT,[685] sadrže pretraživače baze ranjivosti. Pretražive baze omogućuju administratorima da pretražuju nove ranjivosti koje se odnose na proizvode koji se koriste na sistemima. Mnogi od ovih pretraživanja omogućuju predefinisano pretraživanje prema određenim kriterijumima. Na primer prema OS, programu, značajnosti, datumu i drugim kriterijumima.

684 Security Focus, http://www.securityfocus.com/, 19.06.2016.
685 National Vulnerability Database (NVD), http://nvd.nist.gov/, 19.06.2016.

4.2. NAJČEŠĆI NAČINI ZLONAMERNOG ISKORIŠĆAVANJA SISTEMA

U prethodnoj klasifikaciji prikazane su prepoznate ranjivosti koje su prisutne na sistemima i načini njihove prevencije.

U daljem tekstu biće navedeni najčešći načini zlonamernog iskorišćavanja ranjivosti na sistemima: upad na sistem sa ciljem dobijanja pristupa, dobijanje privilegija i onemogućavanje servisa.

4.2.1 Upad na sistem sa ciljem dobijanja pristupa

Upad na sistem podrazumeva dobijanje pristupa kroz iskorišćavanja ranjivosti sistema kao i dobijanje privilegija na sistemu. Zlonamerno dobijanje pristupa na sistemu najčešće se ostvaruje na sledeći načine:

1. napad na OS: kada je reč o napadu na OS glavne slabosti koje su predmet iskorišćavanja su servisi i otvoreni portovi. Što je više servisa otvorenih portova to je više pristupnih tačaka na sistemu. Na osnovu ovakvog gledišta difoltna instalacija OS treba da ima što manje pokrenutih servisa (samo neophodnih) i otvorenih portova (ukoliko je potreban veći broj mogu se naknadno instalirati servisi). Nažalost u realnosti to nije slučaj. Difoltna instalacija sadrži veliki broj startovanih servisa i otvorenih portova. Razlog za instaliranje velikog broja servisa pri difoltnoj instalaciji OS, koji sa sobom nosi ogroman bezbednosni rizik jeste materijalan. Cilj proizvođača jeste da korisnik OS može da instalira i konfiguriše sistem sa najmanje napora (ukoliko postoji problem zove se tehnička podrška proizvođača, a ona je skupa). To znači da sa jedne strane imamo smanjenje troškova za proizvođača, a sa druge strane imamo veću funkcionalnost na sistemu i veće zadovoljstvo korisnika prilikom instalacije sistema (instalirano je i šta je potrebno i šta nije). Sa gledišta proizvođača to je prihvatljivo, ali sa stanovišta bezbednosti nije. Dodatan problem leži u činjenici da korisnici računarskih sistema nisu dovoljno svesni ranjivosti sistema koje koriste. U organizacijama takođe smatraju da je instaliranjem OS na računaru posao završen i ne primenjuju krpljenje i ažuriranje sistema (eng. update), koje se preporučuje na dnevnom nivou.[686] Rezultat jeste organizacija sa zastarelim OS, koji ima veliki broj ranjivosti odnosno veliki bezbednosni rizik.

2. napad na instalirane programe na sistemu: Kada je reč o napadima na

686 Nelson B., Phillips A., Enfinger F., Steuart C., *Guide To Computer Forensics And Investigations*, *second edition*, Thomson Course Technology, Boston, 2006.

programe instalirane na sistemu postoji više uzroka. Najpre u samom razvoju programa nije posvećena dovoljna pažnja bezbednosti. U praksi programeri koji razvijaju programe susreću se sa postavljenim vrlo kratkim rokovima za realizaciju programa. To znači da se testiranja ne vrše dovoljno detaljno. Dodatni problemi za bezbednost nastaju prilikom povećavanja funkcionalnosti i kompleksnosti programa pa su šanse za testiranje svih funkcija još manje. Zloupotreba funkcionalnosti otvara vrata za kompromitovanje bezbednosti na sistemu. Na primer, jedan email klijent može da sadrži funkciju koja omogućuje direktno isčitavanje HTML poruke za korisnika. Napadač ovo može da iskoristi tako što osmisli lažnu poruku koja u HTML izgleda regularno, ali koja sadrži hyperlink koji vodi do zlonamerne web stranice kada korisnik klikne na nju.[687] Drugi problem koji se odnosi na programe je nedovoljno ispitivanje programa kada su u pitanju greške (eng. error-checking). Jedan od razloga za veliki broj bezbednosnih propusta u programima je upravo nedostatak ispitivanja grešaka. Buffer overflow je jedan od primera ovog problema i tu ranjivost može zloupotrebiti napadač da dobije pristup sistemu, privilegije, a može i da onemogući servise na sistemu. Napad tipa buffer overflow nastaje kada napadač pokušava da uskladišti veći broj podataka u bafer memoriju u odnosu na onu koji je programer predvideo prouzrokujući prelivanje podataka sa malicioznim kodom u druge bafere (primer za prepunjavanje bafera mogao bi se ilustrovati na sledeći način: program očekuje niz od 80 znakova, a korisnik unese 300). Kada se izvrši ovaj kod napadač može da dobije potpunu kontrolu nad sistemom. Jako dobar rad autora Aleph One-a, koji opisuje ranjivost tipa buffer overflow jeste „*Smashing the Stack for Fun and Profit*"[688] objavljen u online časopisu Phrack[689] koji se bavi problemima vezanom za bezbednost na računarskim sistemima.[690] Sql injection napad se odnosi na serverski deo infrastrukture gde servis procesira zahteve od strane klijentske strane očekujući regularnu formu vrednosti. Međutim, ukoliko zlonamerni napadač, umesto očekivane regularne vrednosti, na database sloju unese sql injection string reč je o sql injection napadu. Digitalni dokaz koji forenzičar treba da pronađe je zlonamerni sql string, koji ukazuje da se radi o sql injection napadu. Može se pronaći u logovima koji mogu da budu

687 Menz M., Bress S., *The fallacy of software write protection in computer forensic*, 2004, http://www.mykeytech.com/SoftwareWriteBlocking2-4.pdf, 11.07.2016.

688 BugTraq, r00t, i Underground.Org, Smashing The Stack For Fun And Profit, http://www-inst.eecs.berkeley.edu/~cs161/fa08/papers/stack_smashing.pdf, 20.06.2016.

689 Phrack Staff, http://www.phrack.com/, 20.06.2016.

690 Marchany R., *The top 10/20 Internet security vulenrabilities*, Va Tech Computing center, The Sans institute, Covits, 2000. http://www.slideshare.net/ amiable_indian/the-top-1020-internet-security-vulnerabilities-a-primer, 22.06.2016.

locirani na različitim lokacijama. Kao prvo mesto gde forenzičar treba da izvrši pretragu za digitalnim dokazom, jeste log fajl access_log na veb serveru. Ovaj log fajl sadrži svaki http zahtev koji dolazi za veb servis u vidu hedera i body-ja. Na taj način moguće je identifikovati aktivnost određenog korisnika. Drugo važno mesto koje je potrebno pretražiti jeste log baze podataka jer ona sadrži sve upite koji su upućivani samoj bazi. Međutim u bazi se ne nalaze IP adrese koje su izvršavale upit ukoliko ne postoje zaštitini mehanizmi u formi veb aplikativnih fajervolova. Na taj način u logu se čuva upit poslat ka bazi podataka i vrši se provera stringove u formi regularnih izraza (source IP i upit koji je poslat veb serveru). Dodatno za bazu podataka treba uključiti audit logove u log menadžment sistemu kako bi se obezbedili dovoljni tragovi za forenzičku istragu.

Microsoft je napravio odličan shell (komandno okruženje) po uzoru na Linuxov koji se zove Powershell. Glavna mana Powershell-a je što ne može pametno da identifikuje koja je zlonamerna, a koja je dobra skripta. Na primer ukoliko postoji zlonamerna skripta koju sistem identifikuje kao lošu, ali ako njoj zlonamerni napadač modifikuje samo način izvršenja, ta skripta će se izvršiti jer prema pattern matchingu neće biti prepoznata više kao loša. Dodavanje zaštite u vidu postavljanja digitalnog potpisa na skriptu opet nije garant sigurnosti određenog programa. Zlonamerni napadači mogu da ukradenom kreditnom karticom kupe digitalni sertifikat za digitalno potpisivanje od Public certification authority. Ukoliko se sa takvim sertifikatom izvrši potpisivanje zlonamernog koda, većina antivirusa neće dati informaciju o tome da je ta potpisana skripta zlonamerna. Na primer slučaj Comodo (CA) je bio kompromitovan 2011. godine, a on predstavlja public certification authority koji izdaje digitalne sertifikate za google.com, facebook.com. Zlonamerni napadač je bio u prilici da iznova izdaje digitalne sertifikate za te domene neograničen broj put. Ovi sertifikati su se koristili za kreiranje lažnih veb servera. Kada korisnik takvom veb serveru pristupa ne može da posumnja u originalonst sajta jer je https potpisan sa public site authority. Nakon što korisnik ostavi svoje korisničko ime i šifru, lažni server preusmerava korisnika na pravi, ali je prethodno pokupio korisničke podatke.

3. napad na skripte i primere programa: Napadi na skripte i probne programe posebno se odnose na Linux sisteme. Razlog leži u činjenici da prilikom instaliranja OS ili programa proizvođač distribuira i probne fajlove tj. skripte i programe za bolje razumevanje sistema i za budući razvoj programa. Sa stanovišta programera koji razvija programa ovakav pristup je dragocen,

jer se vreme potrebno za razvoj drastično smanjuje, ali nosi rizik po pitanju bezbednosti. Najveća prisutnost ovih probnih skripti je u oblasti web razvoja. Na primer, prethodne verzije Apache web servera su dolazile sa probnim skriptama od kojih je većina imala ranjivosti. Dodatan problem predstavlja i veliki broj predefinisanih skript alata, koji dolaze u sklopu web pretraživača koji omogućuju ljudima da sa malo programerskog znanja razvijaju programe za kratko vreme. Rezultat je takav da program radi, ali ono što je u pozadini jeste veliki bezbednosni problem. Skripte mogu biti pune nepotrebnog koda, a testiranje na greške je izostalo što otvara vrata potencijalnom napadaču. Primera ima mnogo a jedan koji može da ilustruje bezbenosni problem jeste difoltna instalacija web sajta koji dolazi sa IIS (eng. Internet Information Services, bivši Internet Information Server). Nakon instaliranja alati za udaljenu administraciju su dostupni na glavnoj strani. Ovi alati mogu biti zloupotrebljeni od strane napadača da kompromituju sistem.

4. napadi usled loše konfiguracije (sistema, programa, servisa, firewalla): Napadi zbog pogrešne konfiguracije nisu retka pojava. Primera u forenzičkoj praksi ima mnogo: sistem administrator pokušavajući da podesi sistem uključuje gomilu opcija dok ne proradi ono što želi da iskonfiguriše. Međutim zbog uključivanja velikog boja opcija nikada neće razumeti šta one rade i samim tim neće biti uklonjen višak nepotrebnih opcija koje predstavljaju potencijalnu bezbednosnu pretnju. Da bi se kompjuter konfigurisao ispravno i da bi se smanjili potencijalni bezbednosni rizici neophodno je ukloniti servise i programe sa sistema koji nisu potrebni. Ovo je oblast na koju se treba dodatno skoncentrisati, jer se ona može kontrolisati dobrom administracijom. Upad na sistem radi dobijanja pristupa nije samo po sebi cilj, već je cilj da se obavi niz zlonamernih aktivnosti na serveru. Najčešće posle dobijenog pristupa napadač vrši upload (određenih malicioznih programa, fajlova, ilegalnih fajlova) ili download (osetljivih informacija) sa kompromitovanog sistema. U forenzičkoj praksi uglavnom se dešava da napadač učitava program na sistemu koji služi za: dobijanje većih privilegija na sistemu, onemogućavanje servisa, kompromitovanje drugih računara u mreži ili van nje, podešavanje zadnjih vrata za ponovni pristup sistemu (gde je najjednostavniji način dodavanje novog korisničkog naloga na sistem, preko kreiranja zadnjih vrata po određenom portu npr. „*Back Orifice*“ do sofisticiranih trojanskih verzija logon deamon-a koji imaju skrivene mogućnosti logovanja određenog korisnika na sistem sa root privilegijama).

4.2.2. Dobijanje privilegija na sistemu

Jedan od ciljeva napada na sistem jeste i dobijanje privilegija na njemu, bilo kao root (na Linux OS) bilo kao administrator (na Windows OS). Dobijanje privilegija najčešće se ostvaruje upotrebom lokalnog ili udaljenog exploita. Da bi napadač upotrebio lokalni exploit mora da ima pristup sistemu sa standarnim privilegijama i pomoću njega dobija admin, tj. root privilegije. Udaljeni exploit je skoro isti kao i lokalni samo što napadač ne mora da ima pristup računarskom sistemu već može da ga pokrene sa bilo koje internet lokacije. U izuzetno retkim slučajevima napadač može direktno da dobije najveće privilegije, ali u većini slučajeva napadač mora da ima ili da dobije pristup sistemu, pa tek onda može da povećava svoje privilegije na njemu. Na primer, u forenzičkoj praksi čest je sledeći scenario na Windows OS: napadač može da pristupi sistemu kroz nalog Gost (eng. Guest) i na taj način prikupljajući dodatne informacije koje je zajedno sa određenim alatima iskoristio za dobijanje administratorskog pristupa na Windows OS. Preporuka je da se na sistemima zabrani upotreba gostujućih naloga i da se vrši revizija korisničkih naloga kako bi se detektovali sumnjivi nalozi (jer napadač može sa dobijenim privilegijama kreirati maliciozni nalog preko koga bi mogao da ima normalan pristup sistemu).

Administratori trebaju posebno voditi računa kada koriste svoje kredencijale u organizaciji prilikom logovanja na korisničke računare, jer zlonamerni napadači zloupotrebljavaju alatku Windows Credentials Editor (WCE) da bi prikupili kredencijale sistem administratora.[691] Od trenutno ulogovanog administratora koji je prijavljen na sistem lokalno ili udaljeno, ova alatka prikuplja cleartext, korisničko ime i šifru. Na taj način zlonamerni napadač može da dođe do administratorskih privilegija na operativnom sistemu. Ovaj program je izvršni, ne instalira se, ali ga detektuju antivirusni programi. Na alat mimikatz forenzičari trebaju da obrate pažnju ukoliko prilikom istrage naiđu na njega, jer se on takođe upotrebljava za prikupljanje administratorskih kredencijala da bi se dobile administratorske privilegije na sistemu. [692]

691 Http://www.ampliasecurity.com/research/windows-credentials-editor/, 18.08.2016.
692 Https://github.com/gentilkiwi/mimikatz, 17.08.2016.

4.2.3. Napadi sa ciljem onemogućavanja servisa

Cilj ovih napada je da na sistemu blokiraju servise ili raspoloživost resursa namenjenih korisnicima. Na primer, blokiranje korisnika da posete određeni sajt, zaključavanje korisničkih naloga. Napadi ovog tipa se relativno lako obavaljaju na internetu, jer ne zahtevaju prethodni pristup sistemu.

4.2.4. Napad tipa man-in-the middle

Svrha ovog napada jeste prerutiranje saobraćaja odnosno uspostavljanje saobraćaja na takav način da svi paketi prolaze kroz računar zlonemenog napadača. Na tom principu se realizuje ARP poison napad tako da zlonamerni napadač može vršiti izmenu mrežnog saobraćaja on-the-fly. Na primer, kada je DNS saobraćaj u pitanju, (DNS paketi funkcionišu po principu zahtev-odgovor) u odgovoru DNS servera nalazi se IP adresa određenog FQDN URL zahteva iniciranog od strane korisnika. U tom slučaju kada korisnik ukuca u internet pretraživaču yahoo.com, njegov računar šalje upit DNS serveru za dobijanje IP adrese yahoo.com, međutim, zlonamerni napadač može taj odgovor da izmeni i da odgovor od DNS servera bude modifikovan kada prosleđuje IP adresu yahoo.com a da prosledi IP adresu zlonamernog računara. U tom slučaju kucanjem yahoo.com korisnik koji je žrtva man-in-the-middle napada, kao rezultat može da dobije pristup određenoj lažnoj internet stranici, a ne originalnoj stranici yahoo.com. Zlonamerni napadači koriste u tu svrhu alate tipa social engenering toolkit (na primer Lucy) kako bi kreirali lažne izglede sajta (gmail, yahoo, facebook) i simulirali login forme sa ciljem prikupljanja korisničkih kredencijala.[693] Realizovanjem ovog napada zlonamernom napadaču je otvoren put za sprovođenje i drugih opisanih napada. Zato je važno da korisnici obavezno obraćaju pažnju na URL-ove koje koriste prilikom surfovanja, a naročito prilikom logovanja gde ostavljaju svoje kredencijale.

4.2.5 Rizici koje nosi korišćenje TOR mreže

Sa stanovišta digitalne forenzike poznavanje Onion rutiranja je jako važno kada se procesiraju slučajevi nedozvoljene aktivnosti gde je korišćena TOR mreža za prikrivanje ilegalnih aktivnosti. Takođe sa stanovišta bezbednosti u okviru organizacije zbog mogućih curenja informacija važno

693 Http://www.lucysecurity.com/, 17.08.2016.

je da se na vreme prepozna korišćenje TOR mreže.

Veliki je broj razloga za postizanje zaštite identiteta na internetu kako za pojedince tako i za servise. Oni se kreću od izbegavanja cenzurisanja interneta i njegovih servisa preko objavljivanja određenih osetljivih informacija, bezbednije komunikacije novinara i njihovih izvora, pa do prikrivanja ilegalnih aktivnosti cyber kriminala. S obzirom na to da IP komunikacija nije predviđena za anonimnost, jer obe strane u komunikaciji moraju znati IP adresu onog sa kojim komuniciraju, da bi se komunikacija mogla ostvariti. U tom slučaju kada je adresa poznata poznat je i naš digitalni otisak – IP identitet. Rešenje je došlo iz NSA projekta u vidu tzv. Onion rutiranja (TOR je akronim od The Onion Routing) gde se umesto uspostavljanja direktne komunikacije sa servisom određenog servera, komunikacija realizuje preko određenog broja nodova odnosno čvorova. Za svaki HOP kreira se posebna „koverta" u koju se smešta paket koji se prosleđuje sledećem nodu u vidu paketa. Koliko ima HOPova toliko ima i koverata analogno slojevima crnog luka (Onion). Prvi nod može da otkrije samo prvu kovertu, čime se otkriva putanja do sledećeg noda kome se prosleđuje paket i tako dok se ne dođe do poslednjeg noda u TOR mreži koji jedini vidi informaciju o tome ka kom serveru treba da se pošalje paket. To znači da svaki nod zna samo za prethodni i naredni nod, odnosno „nije svestan" krajnje i početne destinacije, sem prvog kome je poznata samo početna destinacija i poslednjeg kome je poznata samo krajnja destinacija. Korisnikov računar koji se prijavljuje na TOR mrežu naziva se TOR klijent, a sama TOR mreža sastoji se od TOR nodova koji mogu da budu tzv. TOR releji koji služe sa pojačavanje propusnog opsega TOR mreže ili igraju ulogu direktorijum servera koji sadrži listu svih aktivnih javnih TOR releja ili ulaznih i izlaznih releja. Uspostavljanje pouzdanog kanala realizuje se kroz TLS koji ima različite varijante korišćenja u TORu: RSA, DiffieHelman i ECC služe za razmenu ključeva, a po uspostavljanju kanala koristi se AES za šifrovanje koverti zbog brzine u šifrovanju dok se heširanje koristi za obezbeđivanje integriteta poruke, jer je finalni čvor kritičan gde može da se kompromituje komunikaciju sa servisom. TOR izlazni relej ima svoj rejting. Visok rejting podrazumeva relej koji može da procesira veliki broj konekcija koje trebaju da izađu iz TOR mreže.

Nakon uspostavljanja pouzdanog kanala sa prvim nodom putanja se proširuje do poslednjeg noda koji pristupa traženom servisu. Ideja je da ni jedan od TOR nodova/releja nema kompletnu informaciju o klijentu i servisu kome se pristupa i niko ne zna kompletnu putanju poslatog paketa sa podacima. Difoltna vrednost za broj HOPova je 3 (manji broj manja

anonimnost, veći broj smanjuje performanse jer se prenošeni sadržaj dešifruje i šifruje na svakom releju kako pri odlaznom tako i pri dolaznom saobraćaju). Kritične tačke TOR mreže:

- Poslednji HOP sadrži potpuno otvoren paket jer nije enkriptovan u TOR-u. To znači da postoji mogućnost, ukoliko zlonamerni napadač prisluškuje, da bude pročitan payload paketa koji izlazi iz poslednjeg noda. TOR napadači u praksi najčešće igraju ulogu izlaznog releja iz razloga što se to mesto gde se raspakuje konačni paket u kome se vidi i kom servisu se pristupa i sam payload. Rešenje može da bude u vidu upotrebe enkripcije na aplikativnom sloju u vidu https (ako je u pitanju veb servis). To znači ako je payload šifrovan na aplikativnom sloju onda je anonimnost relativno osigurana, ukoliko nije onda se vide svi podaci poslati ka servisu i šta se dobija od servisa, što može dovesti do kompromitovanja anonimnosti.
- Ukoliko se prisluškuje prvi HOP može se doći do informacija da je određen računar TOR klijent i da koristi uslugu TOR mreže, ali ne može se saznati šta se šalje i kome se šalje. Na taj način bez obzira što je saobraćaj šifrovan i ne može se videti kome korisnik pristupa, korisnik dobija etiketu kao „sumnjiv" što može za posledicu da nosi primenu drugih elemenata nadgledanja korisnika. Sa druge strane provajderi mogu filterima blokirati pristup TOR mreži na osnovu detektovanja da korisnik pristupa TOR releju. Rešavanje ovog problema se svodi na postavljanje tzv. mostova koji predstavljaju isto TOR releje samo nisu javno dostupni. Svakako, nema garancije da neki od tih mostova neće vrlo brzo biti kompromitovani.
- U praksi se dešava da pored regularnih volonterskih relej servera postoje nameski relej serveri iza koji se kriju ili zlonamerni napadači koji ugrožavaju postizanje anonimnosti ili istražitelji koji rade u skladu sa zakonom čiji je cilj razotkrivanje nečije anonimnosti. To znači da nema apsolutne garancije da TOR relej nije pod kontrolom nekoga ko želi razotkriti korisničku anonimnost.
- Analiza saobraćaja - ukoliko napadač ima pristup ulaznoj i izlaznoj tački analizom saobraćaja moguće je mečovanjem povezati određenog korisnika sa servisom kome pristupa i na taj način saznati IP adresu koju korisnik ima. Murdoch S. i Danezis D. sa Camridge univerziteta na konferenciji IEEE Symposium on Security and Privacy 2005 u Oaklandu (Kalifornija) objavili su članak pod naslovom „*Low-Cost Traffic Analysis of Tor*" koji govori slabosti Tor mreže na

analizu saobraćaja.[694] Tehnika koja je opisana u radu omogućuje zlonamernom napadaču koji ima pristup ograničenom delu TOR mreže da otkrije nodove preko kojih je ostvarena anonimna veza, čime se kompromituje anonimnost korisnika. Ovo nije jednostavan postupak, jer napadač mora da ima pristup ulaznoj i izlaznoj tački. Da bi se ova šansa smanjila bira se da ulazna i izlazna putanja ne budu u istom autonomnom sistemu, jer se time smanjuje šansa da je uspostavljeno kolo pod kontrolom istog provajdera i samim tim manja je šansa da napadač ima pristup dvema kritičnim tačkama.[695]

- DNS upiti se šalju bez korišćenja TOR posrednika pa se na taj način može otkriti DNS upit TOR klijenta. Upotreba Pivoxy servera ili torify naredbe TOR programskog paketa omogućuje ispravljanje ovog nedostatka. Takođe, programi koje koriste SOCKS5 server, a koji omogućuje upite koji se baziraju na imenu, mogu usmeravati DNS zahteve preko TOR mreže pri čemu se pretraživanje zapisa (eng. lookup) realizuje na izlaznom čvoru pa DNS zahtevi ostvaruju jednaku nivo anonimnosti kao i ostali promet na TOR mreži.[696]

Istraživači francuske inženjerske škole ESIEA pronašli su određene ranjivosti na TOR mreži i u laboratorijskom okruženju uspeli da aktiviraju kreirani exploit dobijajući sistemske privilegije na kompromitovanom računarskom sistemu. Na taj način moguće je dobijanje kontrole nad mrežom nakon što su releji inficirani zlonamernim programom.[697] Pošto uspostave administratorske privilegije nad zaraženim relejima, primenjuju dvostruki napad: lokalizovana zagušenja, koji podrazumeva slanje velikog broja zahteva prema neinficiranim relejima, a zatim se okreće paket sa virusom, implementiran u zaraženim relejima, koji se priloži nezaraženim serverima u petlji kola da ih popuni.[698] 2013. godine je objavljeno da je NSA kreirala

694 Steven J. Murdoch, George Danezis, *Low-Cost Traffic Analysis of Tor, IEEE Symposium on Security and Privacy* 2005, Oakland, California, USA, May 8 – 11, 2005, http://sec.cs.ucl.ac.uk/users/ smurdoch/ papers/ oakland05torta.pdf, 10.08.2016.

695 Zoran Čiča, *Tor Network - How to Achieve Anonymity?,* ICT security 2016 conference, Belgrade, 2016.

696 CARNet, *Tor - mreža za anonimnost*, CCERT-PUBDOC-2007-07-197, Revizija v1.1, str.13-14., 2007, http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-07-197.pdf, 10.08.2016.

697 The hacker News, *Tor anonymizing network compromised by French researchers*, http://thehackernews.com/2011/10/tor-anonymizing-network-compromised-by.html, 10.08.2016.

698 Nada Staletić, Predrag Staletić, Aleksandar Simović, *Sigurnost Tor mreže u zaštiti identiteta na Internetu,* INFOTEH-JAHORINA Vol. 13, str 913 - 917, 2014, http://infoteh. etf.unssa. rs.ba/zbornik/2014/radovi/RSS-6/RSS-6-5.pdf, 08.08.2016

tehniku kodnog naziva EgotisticalGiraffe sa kojom je moguće dešifrovanje kriptovanih podataka na TOR mreži preko ranjivih verzija Firefox programa koji su prilagođeni u TOR aplikaciju.

Zloupotrebe TOR mreže:

- Upotreba TOR mreže za prenos velikih količina podataka od strane korisnika čime se vrši zagušenje saobraćaja i drastičan pad performansi,
- korišćenje TOR mreže za distribuiranje spam elektronske pošte (prema difoltnim podešavanjima TOR browsera onemogućen je port 25 koji koristi SMTP server za distribuiranja elektronske pošte),
- TOR omogućuje osim prikrivanja korisničkih identiteta i prikrivanja samih servisa. Tipičan primer u praksi je njihova zloupotreba sa ciljem prikrivanja ilegalnih radnji. Primeri ilegalne kockarnice, sajtovi dečije pornografije, distribucija narkotika itd.

Uz pomoć TOR internet pretraživača može se ući u skriveni tzv. Uncensored Hidden Wiki portal. Na ovom portalu nalaze se linkovi za ulaz na Darknet servise. Adresa je nepromenjena par godina *http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page*.

Većina servisa nose bezbednosni rizik za mašinu sa koje se pristupa. Na njemu se mogu naći veliki broj ilegalnih usluga koje se nude (malware kao servis, pay pal račun sa dobrim balansom, brojevi ukradenih kartica kao lažni servisi od strane raznih tajnih službi). Može se uočiti da se plaćanje ilegalnih servisa vrši sa bitcoinima.

Sa stanovišta bezbednosti ukoliko organizacija želi da onemogući upotrebu TOR saobraćaja preporuka je da zabrani instaliranje TOR klijenta u orgnizaciji, a ne da kroz filtriranje dolaznog i odlaznog saobraćaja vrši njegovo ograničavanje.

Nepažljivom upotrebom TOR pretraživača može se izgubiti anonimnost. Na primer, ukoliko korisnik želi da sakrije svoj digitalni otisak sa ciljem anonimnog pristupanja svom nalogu na twtitter-u, facebook-u ili svom nalogu za email, ne treba da koristi TOR pretraživač za svoje postojeće naloge. Onaj ko vrši nadgledanje servisa ima informaciju koji digitalni otisak pristupa određenom nalogu i u momentu kada da je korisnik pristupio svom nalogu preko TOR mreže, ta komunikacija dobija etiketu „sumnjiva". Komunikacija dalje može da se nadgleda, jer se sad poznato za koga se vezuje ta komunikacija, pošto korisnik pristupa svom nalogu (na taj način korisnik nije prikrio svoj digitalni otisak, već je ga je otkrio). Za povećanje nivoa anonimnosti preporuka je dakle da se ne pristupa svojim nalozima kojima se pristupa van TOR mreže, već je potrebno kreirati namenski

identitet koji važi samo na TOR mreži, da se on ne bi vezivao za korisnika. Prilikom kreiranja namenskog identiteta izbegavati sličnosti identiteta sa originalnim identitetom i njegove konfiguracije koje su bile na drugim mrežama, da se ne može iz korelacije tih podataka zaključiti korisnički identitet. Dodatno, prilikom korišćenja usluge TOR mreže, ne koristiti drugu mrežnu komunikaciju izvan TOR mreže jer to sa sobom nosi mogućnost otkrivanja identiteta. Na primer otvaranje dokumenata tipa pdf, excel, word koji u sebi sadrže aktivne linkove mogu aktivirati mrežnu komunikaciju prilikom njihovog otvaranja i na taj način kompromitovali originalnu IP adresu pošto se ti podaci šalju nezavisno od TOR mreže (zaobilaze se TOR podešavanja). Jedan od primera je bagovit dodatak na pretraživaču Adobe Flash koji omogućava slanje IP adrese zaobilazeći TOR podešavanja.

NSA čiji je projekat Onion rutiranje poseduje svoje TOR čvorište sa linkovima ogromne propusne moći i velikog rejtinga, tako da skoro sve komunikacije izlaze kroz njega, a s obzirom na to da poseduju tehnologiju koja omogućava dinamičko menjanje geo IP adresa (posedovanje IP adresa sa različitih geografskih lokacija), neće se znati da li je TOR izlazni nod iz Evrope, Azije, Afrike. Može se reći da sve izlazi iz jednog noda koji je vlasništvo NSA i na taj način sve je nadgledano. Jedino se javlja problem identifikacije vlasnika paketa, ali i to se može obezbediti na osnovu TCP state sesija koje provajderi moraju da čuvaju izvestan vremenski period i upotrebe big data mining tehnologije sa naprednim algoritmom identifikacije.[699] [700]

Može se zaključiti da TOR mreža može obezbediti zaštitu anonimnosti od strane tzv. lowprofile napadača (marketinške agencije, zlonamerni napadači, pojedinci), ali ne obezbeđuje zaštitu anonimnosti od strane bezbednosnih službi.

---

699 Obaveza zadržavanja podataka od strane provajdera u Republici Srbiji zasnovana je na Zakonu o elektronskim komunikacijama (čl. 128) i traje 12 meseci. Zakon o elektronskim komunikacijama, Sl. glasnik RS", br. 44/2010, http:// www. rra. org. rs/ uploads/ useruploads/ PDF/ 4360-zakon_ o_ elektronskim_ komunikacijama.pdf, 23.08.2016.

700 Nemačka je krajem 2015. godine usvojila *Zakon o zadržavanju podataka*. Ovim zakonom su u značajnoj meri skraćeni rokovi zadržavanja podataka od strane provajdera. Provajderi sada imaju obavezu da čuvaju sledeće podatke: 1) *podatke koji se odnose na telefoniranje* (pozivni brojevi, koji je broj pozivan i koji broj se poziva, vreme početka i kraja razgovora) i *podatke koji se odnose na kompjutere* (*IP-adrese* priključaka) za vreme od *10 nedelja*; 2) *podatke o baznim stanicama mobilnih telefona* (sa kog broja, kada i koliko je i sa kojim brojem telefonirao) za vreme od *4 nedelje*; 3) pristup zadržanim podacima mora biti sudski odobren; 4) podaci o lekarima, advokatima, novinarima su izričito isključeni iz područja delovanja ovog zakona; 5) E-mejl saobraćaj i sadržaji razgovora su izričito isključeni iz područja delovanja ovog zakona. Gesetz zur Einführung einer Speicherfrist und einer Höchstspeicherfrist für Verkehrsdaten, vom 10. Dezember. 2015., http://www. bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl#__ bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s2218.pdf%27%5D__1463939728226, 23.08.2016.

4.3. ZAŠTITA U OKVIRU ORGANIZACIJE I ODGOVORI NA NEDOZVOLJENE ILI INCIDENTNE AKTIVNOSTI

Kada je reč o zlonamernom iskorišćavanju (eng. exploit) računarskog sistema podrazumeva se: dobijanje pristupa na iskorišćenom sistemu, većih prava na sistemu i uskraćivanje servisa na kompromitovanom sistemu. Sve tri pomenute zlonamerne aktivnosti su korisne za malicionznog korisnika (napadača) i zavise od tipa napada koji se želi postići. U praksi postoje slučajevi gde se ove aktivnosti kombinuju jedna sa drugom. Na primer, kada napadač kompromituje korisnički nalog da bi imao pristup sistemu. Međutim, pošto nema „administratorske" privilegije ne može doći do osetljivih informacija niti instalirati zlonamerne programe. U tom slučaju napadač bi izvršio i drugi napad tj. zlonamernu aktivnost, koja za cilj ima dobijanje administratorskih privilegija da bi dobio pristup osetljivim informacijama i instalirao zlonamerne programe.

Na osnovu velikog broja izveštaja vodećih kompanija koje se bave bezbednošću na internetu može se ustanoviti, da se kompromitovanje računarskih sistema izvodi sve više na sofisticiranije načine (brisanje podataka, šifrovanje podataka, manipulacije sa vremenom i datumima, manipulacija sa meta podacima i upotreba antiforenzičkih programa). Korišćenje nebezbednih mreža može da ima za posledicu kompromitovanje računarskih sistema koji ih koriste.[701] Veliki broj napada je realizovan na osnovu iniciranja od strane samih korisnika primeri su fišing napadi, korišćenje malicioznih sajtova i metode socijalnog inženjeringa. Fokus treba usmeriti na aktivnosti zaštite pre nastupanja nedozvoljene aktivnosti (priprema za protipravne aktivnosti), kao i edukovanja što većeg broja krajnjih korisnika po pitanju bezbednog korišćenja računarskih sistema. Na primer, zaštita od napada socijalnog inženjeringa treba usmeriti na edukaciju službenika u organizaciji. To znači da ukoliko se sumnja u identitet određene osobe (npr. poziv telefonom), toj osobi treba postaviti specifična pitanja koja će otkloniti sumnje u identitet ili otkriti zlonameran pokušaj. U praksi se pokazalo da se određeni napadači dobro pripremaju za napad, tipa socijalnog inženjeringa, detaljno proučavajući organizaciju koju žele da napadnu. Tako da ukoliko postoji i mala sumnja treba obavestiti pretpostavljenog radi dodatnih provera.

Korisnici računarskih sistema takođe treba da vode računa i o tome da kada unose svoje šifre na računarske sisteme, da nemaju nikoga iza sebe

701 Najeveći broj napada u mreži se realizuje preko layer 2 napada i putem DNS napada. U layer 2 napade spada VLAN hoping, napadi na MAC adrese, DHCP napadi, ARP napadi, napadi obmane a u DNS napade spada DNS hijacking, hijacking HTTP sesije.

koji može gledati unos šifre. Treba zabraniti čuvanje šifri na papirićima pored računara. Da bi se zaštitili od napada pogađanja korisničkih šifri, nikada kao šifre ne treba upotrebljavati datume rođenja, porodična ili imena bliskih osoba, imena kućnih ljubimaca. Upotreba šifri iz rečnika takođe može biti komprimitovana „*dictionary*" napadom. Ukoliko se koristi neka reč iz rečnika zbog veće zaštite, nju je bolje modifikovati (npr. reč „projektant" modifikovati u „pr0j3kt4nt" ili upotrebljavati određene fraze npr. „kolikojesati?21h"). Napadi na korisničke šifre mogu biti izvedeni sa tzv. brute-force napadom, a zaštita od ovih napada najbolja je upotrebom dugačkih šifri, različitih znakova, brojeva, velikih i malih slova. Ukoliko napadaču treba dosta vremena da pogodi šifru vrlo je verovatno da će odustati. Korišćenje fraza za šifre je dobra opcija za njenu bezbednost. USB flash koji se koristi za upisivanje „osetljivih informacija" ili za smeštanje virtuelnih mašina ne treba davati na pozajmicu čak i ako su podaci obrisani sa njega. Neko ko ima znanja za korišćenja prikazanih forenzičkih alata može povratiti obrisane podatke kako sa fajl sistema samog USB flash-a tako i obrisane podatke iz samih virtuelnih mašina. Na taj način može doći do kompromitovanja korisničkog naloga, ucena ili izvlačenja informacija za primenu socijalnog inžinjeringa.

Zaštita od već pomenutih fišing napada je u praksi veoma jednostavna. Ukoliko se od korisnika traži da ostave lične podatke na određeni sajt, treba obavezno pogledati URL adresu sajta. Na primer, pretpostavljate da treba da se nalazite na Yahoo.com sajtu a URL adresa pokazuje YAHOOHOHO.com. To znači da je sajt lažan, jer na pravom Yahoo.com sajtu URL adresa može samo da bude Yahoo.com.

Mnogi stručnjaci smatraju da je ideja IPS (prevencije) superiornija od detekcije upada IDS. Foster i Wislon napominju da sve dok su napadači, odnosno upadi i dalje uspešni potreba za detektovanjem upada je više nego očigledna.[702] Da bi se sprečavalo ponavljanje upadanja, ili napada na sisteme neophodna je *računarska forenzika*, koja bi utvrdila najpre zašto je došlo do napada ili upada i na koji način. Dakle računarska forenzika predstavlja i integralni deo zaštite od upadanja na računarski sistem. Uspešna zaštita u okviru organizacije se može ostvariti kroz postojanje kadrova koji se bave upravljanjem incidentom i upravljanjem rizikom uz obavezno postojanje zaposlenog digitalnog forenzičara. To za posledicu ima smanjenje vremena potrebnog za zaštitu.[703] Takvim sistemom se upravlja kroz postojanje organizacionih, upravnih i tehničkih mera.

---

702 Milosavljević M., Grubor G., *Digitalna forenzika*, Univerzitet Singidunum, Beograd, 2008.

703 Vreme zaštite = vreme detekovanja + vreme odgovora

Prava zaštita podrazumeva prevenciju (prava pristupa, kriptografska zaštita i fajervoli) zajedno sa detekcijom (detektovanje incidenta odnosno nedozvoljene aktivnosti) i reakciju odnosno odgovor na incidentnu radnju (rukovanje incidentom).

Većina organizacija reaguju samo na bezbednosne pretnje i uglavnom te reakcije dolaze nakon što je šteta već učinjena. Ključ infomacione bezbednosti leži upravo u proaktivnom pristupu bezbednosnim pretnjama što podrazumeva uklanjanje bezbednosnih ranjivosti pre nego što one budu iskorišćene od strane potencijalnog napadača.[704] Poželjno bi bilo da organizacije prave bazu bezbednosnih incidenata kako zbog statistike tako i zbog definisanja obrazaca poklapanja kako se incidenti ne bi ponavljali. Trenutno u Srbiji nedostaje nacionalni CERT, gde bi se nalazila baza poznatih bezbednosnih incidenata, na osnovu koje bi se distribuirale smernice, u vezi sa bezbenosnim problemima na koje treba obratiti više pažnje, kako bi se efikasnije suzbijale nedozvoljene aktivnosti i sprečavalo njihovo ponavljanje.

4.3.1. Detektovanje incidentnih odnosno nedozvoljenih aktivnosti

Detekcija upada prema NISTu (eng. The National Institute of Standards and Technology)[705] definiše se kao: „proces praćenja i analize događaja, koji se javljaju u računarskom sistemu ili na mreži, sa ciljem prepoznavanja znakova upada koji se definišu kao pokušaji da se kompromituju poverljivost, integritet, raspoloživost ili da se zaobiđu mehanizmi zaštite računarskih sistema ili mreže".[706] Alati kojima se detektuju ugrožavanje bezbednosti sistema mogu upozoriti administratore (sistema i mreže) mnogo brže nego da se njihova identifikacija vrši manuelno. *Sistem za detekciju upada* (eng. intrusion detection system - IDS) predstavlja program koji automatizuje proces detekcije upada. *Sistem za prevenciju upada* (eng. Intrusion prevention

704 Phillip G. Bradford i Ning Hu svom radu *„A Layered Approach to Insider Threat Detection and Proactive Forensics"* su predstavili mogućnost upotrebe peroaktivne forenzike u otkrivanju insajderskih napada uz pomoć sistema za online praćenje korisničkih aktivnosti koje se odnose na otkrivanje potencijalnih zloupotreba računarskih sistema. Milosavljević M., Grubor G., *Istraga kompjuterskog kriminala - metodološko tehnološke osnove*, Univerzitet Singidunum 2009.

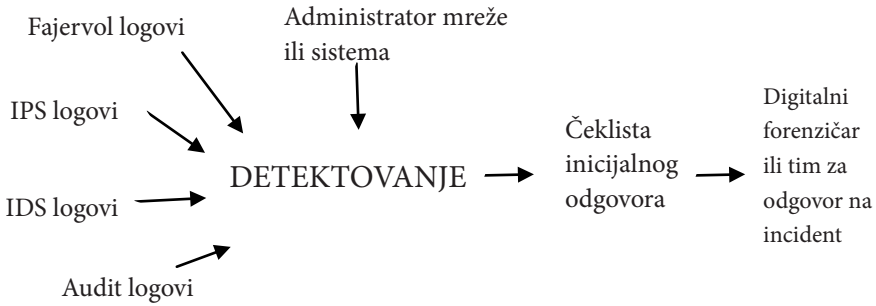
705 The National Institute of Standards and Technology (NIST), http://www.nist.gov/index.html, 30.05.2016.

706 Baiju Shah, *How to Choose Intrusion Detection Solution, Version 1.2e*, SANS Institute InfoSec Reading Room 2001, http://www.sans. org/ reading_ room/ whitepapers/ detection/ choose – intrusion - detection-solution_334.pdf , 25.03.2016.

system, skraćeno IPS) ima sve mogućnosti sistema za detekciju upada i može pokušati da zaustavi mogući incident.[707]Ukoliko se onemoguće preventivne funkcije IPS-a on će funkcionisati kao IDS. Za razliku od manuelne provere administratori će na upozorenja, koja alati budu generisali, brzo odreagovati i proveriti sumnjive aktivnosti. IDS sistemi su veoma važne kompomente bezbednosti, ali oslanjajući se samo na njih to neće biti garant kompletne bezbednosti na sistemima i mreži. Potrebno je dakle da se stalno pretražuju znakovi bezbednosnih incidenata koji se mogu prepoznati u vidu:

-sumnjivih stavki u logovima;
-upozorenja od strane IDS;
-upozorenja od strane IPS;
-prisustva neobjašnjivih korisničkih naloga na sistemu ili mreži;
-prisustva sumnjivih fajlova sa nepoznatim ekstenzijama na sistemu;
-neobjašnjivog modifikovanja foldera i fajlova;
-prisustva neuobičajenih servisa;
-otvorenih nestandardnih portova;
-nepredvidivog ponašanja sistema;
-velike količine primljenih paketa (u odnosu na očekivanu);
-nedostupnosti drajvovima na sistemu.

Pomenuti znakovi su najosnovniji indikatori potencijalnog ugrožavanja sistema koji se moraju proveravati, a opširiniji spisak indikatora biće izložen u daljem tekstu.



Slika 75. Detektovanje incidentne radnje

707 Michaud, D. J., *Adventures in Computer Forensics*, Information Security Reading Room, SANS Institute 2001, https://www.sans.org/reading-room/whitepapers/incident/adventures-computer-forensics-638., 11.07.2016.

Mora se istaći da se rana detekcija upada može detektovati kroz pregledanje kako pomenutih sistemskih logova tako i sigurnosnih logova za praćenje aktivnosti (eng. audit log). Koji sve procesi mogu biti praćeni zavisi od *auditing konfiguracije* na samom sistemu. Audit log može sadržati sledeće informacije:

-specijalne operacije kao na primer promene šifre;
-administrativne aktivnosti na sistemu;
-kreiranje i brisanje objekata u sistemu;
-prijavljivanje na sistem i odjavljivanje;
-da li je događaj bio uspešan ili nije i kada se dogodio;
-čitanje i otvaranje fajlova;
-upis ili izmena fajla;
-ime korisnika koji je inicirao aktivnost.

U zavisnosti od potrebnog nivoa bezbednosti podešava se i nivo auditinga. Potrebno je naći dobar balans između potrebnog nivoa bezbednosti i performansi računara sa mogućnostima procesiranja dobijenih informacija. Auditing log može da se napuni velikom količinom nepotrebnih informacija pa se može pojaviti problem da se izdvoje i pronađu bitne informacije i podaci.

Sistemi za detekciju upada IDS (eng. intrusion detection system) mogu biti i uređaji ili programi koji detektuje neovlašćeno korišćenje ili napada na računar ili na mrežu.[708] IDS funkckonišu na osnovu korelacionih pravila na osnovu čega je moguće prepoznati paket sa zlonamernim kodom. Mogu biti mrežno ili računarski orijentisani i kombinovani.[709] Upadi se mogu posmatrati kao pokušaji kompromitivanja integriteta, poverljivosti (tajnosti) i dostupnosti informacija odnosno podataka kroz zaobilaženje bezbednosnih mehanizama informaciono komunikacionih sistema.

Prema tome detekcija može da se radi ručno putem pregledanja log fajlova, automatski ili kombinovano. Upozorenje na incident može

708 Garfinkel S., *The Advanced Forensic Format 1.0*., 2005, http://stuff.mit.edu/afs/ sipb/user/ simsong/ afflib/affdoc.doc, 22.06.2016.

709 Računarski orijentisani IDS procesira kontrolne podatke kao i log datoteke i može da utiče na perfomanse računarskog sistema. Na primer, računarski orijentisani IDS će uhvatiti zlonamerne korisnike koji su se ulogovali direktno na sistem, ali će propustiti mrežne aktivnosti. Mrežno orijentisani IDS procesira podatke na mrežnom segmentu iako je lako primenjiv susreće se sa mnogobrojnim problemima (npr. lažni alarmi zahteva se postojanje velikog broja senzora). Mrežno orijentisan IDS propustiće zlonamerne aktivnosti pojedinca na ulogovanom računaru ali će primetiti napade usmerene na više računara. Kombinovani IDS koristi najbolje iz prethodna dva sistema.

doći od strane IPS-a, IDS-a, krajnjih korisnika, tehničke podrške, sistem administratora i drugih sistema za zaštitu.

Sistemi za detektovanje upada (IPS i IDS) na računarske sisteme ustvari pokušavaju da definišu i detektuju abnormalna ponašanja i aktivnosti koje nisu u skladu sa normalnim aktivnostima. Korišćenjem ovakvih sistema pruža mogućnost rane detekcije pokušaja upada na računar ili u mrežu. Sistemi omogućavaju proveru različitih tipova aktivnosti kao na primer: detektovanje upada ili pokušaja upada na sistem, detektovanje zamaskiranog napadača (eng. masquerading) detektovanje pokušaja testiranja upada (eng. penetrating) od strane legitimnih korisnika na sistemu, detektovanje odliva informacija (eng. leakage) od strane legitimnih korisnika na sistemu, detekcija trojanaca, virusa i napada odbijanja servisa. Profesor Robert Kaufman ističe četiri glavne metode na kojima treba da se bazira sistem za detekciju upada:[710] [711]

- *profilisanje korisnika* - podrazumeva kreiranje profila za svakog korisnika prema njegovim najčešće sprovođenim akcijama. Taj profil će predstavljati korisnički identitet, odnosno obrazac ponašanja koji se posmatra i uspost ʾja nakon određenog vremenskog perioda. Na primer, svaki korisnik ima običaj da, koristi samo određene komande, pristupa istim fajlovima, prijavljuje se u određeno vreme sa određenim učestalostima i izvršava iste programe.[712] Iz navedenog proizlazi da će se korisnički profil kreirati na osnovu ovih aktivnosti i mora se održavati učestalim ažuriranjima.

- *profilisanje napadača* - podrazumeva kreiranje napadačkog profila odnosno definisanje aktivnosti koje će napadač preduzeti ukoliko ostvari neovlašćeni pristup. Tehnika profilisanja počinioca zlonamernih aktivnosti bazira se na analizi prirode dela i načina izvršenja dela. Analiziraju se antropološke, biološke, psihološke, demografske i lične karakteristike potencijalnih počinilaca i upoređuju se sa prethodnim, sadašnjim i naknadnim osobinama načina izvršenja dela. Ove informacije se kombiniju sa drugim

---

710 Garfinkel S., *Anti-Forensics: Techniques, Detection And Countermeasures*, In Proceedings Of The 2nd International Conference On I-Warfare And Security (Iciw), Naval Postgraduate School, Monterey, Ca, March 8-9, 2007.

711 Garfinkel S., Malan D., Dubec K., Stevens C., Pham C., *Disk imaging with the advanced forensics format, library and tools*, The second Annual IFIP WG 11.9 International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, USA, January 20-February 1, 2006.

712 Tipovi aktivnosti koji mogu da se snimaju uključuju iskorišćenost CPU i I/O, vreme uspostavljanja konekcije i dužina trajanja i broj uspostavljanjih konekcija, lokacija korišćenja, korišćene komande, upotreba maila, upotreba komplajlera i editora, pristup i izmena fajlova i foldera, greške i mrežne aktivnosti.

relevantnim podacima i fizičkim dokazima i upoređuju sa karakteristikama poznatih tipova ličnosti i mentalnih abnormalnosti. Na osnovu svega toga pravi se opis potencijalnog počinioca.[713] [714] Na primer, ukoliko je napadač ostvario neovlašćeni pristup na sistem najčešće korišćena akcija je proveravanje trenutno prijavljenih korisnika na sistemu i istraživanje fajlova direktorijuma i aktivnih servisa. Profilisanje treba da obuhvatiti i insajderske aktivnosti, koje se odnose na sticanje pristupa od strane legitimnih korisnika na sistemu i datotekama za koje nisu ovlašćeni. Problem profilisanja je što je teško definisati sve moguće profile i bezbednosne incidente. Ponekad su aktivnosti novog korisnika koji se upoznaje sa sistemom vrlo slične sa aktivnostima zlonamernog napadača.

- *analiza potpisa* (eng. signature analysis) - kao što svaki pojedinac ima jedinstveni pisani potpis koji se može koristiti u svrhu identifikacije, pojedinci takođe imaju i potpis kucanja "eng. typing signature". Vreme koje je potrebno da se otkucaju određeni parovi ili trojke slova mogu se meriti (kolekcija tih digrafa ili trigrafi). Ti parovi zajedno formiraju jedinstvene kolekcije na osnovu kojih se pojedinac može profilisati sa ciljem identifikacije. Ova tehnika zahteva specijalnu opremu i na nju se ne može u potupunosti osloniti kao na jedini faktor pri kontroli pristupa (baš kao što to navode Bergadano, Gunetti, Picardi).[715]

- *otisak napada* (eng. attack signature) - podrazumeva prepoznavanje konkretnih aktivnosti ili akcija kao pokazatelja napada na sistem.[716] Na primer, pokušaj da se iskoriste ranjivosti na sistemu (bezbednosne rupe eng. security hole) korišćenjem exploit programa. Najčešći tipova ranjivosti koji se zloupotrebljavaju su pogrešna konfiguracija sistema ili servisa (eng. misconfiguration), podrazumevana konfiguracija sistema ili servisa (eng. default configuration), ranjivosti na prepunjavanje bafera servisa ili aplikacije (eng. buffer overflow), ranjivost na sql inekciju servisa (eng. sql injection),

---

713 Mirjana Drakulić, Ratimir Drakulić, *Cyber kriminal, Prezentacija*, Fakultet organizacionih nauka, Beograd, 2011, http://www.google.rs/url?sa =t&rct=j&q=&esrc=s&source=web&cd= 1&ved= 0CDMQFjAA &url =http%3A%2F%2Fposlis.fon.bg.ac.rs%2Findex.php% 3Foption%3Dcom_ docman% 26task% 3Ddoc_download% 26gid% 3D295% 26Itemid%3D14&ei =QjttUfLgIsnkswawmoDIDg&usg =AFQjCNGqrl Dyeh9PUTyZ42pif5r8eyS11Q&bvm=bv.45175338,d.Yms&cad=rja, 24.03.2016.

714 Kaufman R. J., Intrusion Detection and Incident Response IS 3523 course,UTSA Spring, 2012.

715 Georgijević U., *Integrisani model procesa digitalne forenzičke istrage*, Ziteh - Udruženje sudskih veštaka za informacione tehnologije It veštak, 2006, http://www.itvestak.org.rs/ziteh_06/Radovi/ZITEH%2006-R07.pdf, 22.06.2016.

716 Kaufman J. Robert, *Intrusion Detection and Incident Response IS 3523 course*, UTSA Spring 2012, http://faculty.business.utsa.edu/rkaufman/IDLsn4.ppt, 24.03.2016.

XSS ranjivost servisa (eng. cross-site scripting).[717] Problem je u tome, što metodi napada ne mogu biti poznati tako da se novi otisci napada konstantno kreiraju pa je sistem za detekciju upada potrebno često ažurirati.

Kada se primenjuju pomenuti sistemi za praćenje aktivnosti (eng. monitoring) postavlja se pitanje očuvanja privatnosti od strane pojedinca. Ukoliko monitoring primenjuje organizacija je u obavezi da obavesti pojedinca da su njihove aktivnosti predmet monitoringa. Na primer, računarski sistemi vladinih organizacija u SAD poseduju banere upozorenja. Koordinacioni centar CERT (CA-92:19) preporuke od Američkog odeljenja za pravosuđe po pitanju praćenja otkucaja na tastaturi (eng. monitor keystrokes) kao metod zaštite računarskih sistema od neovlašćenog pristupa, ali se korisnik mora eksplicitno upozoriti u formi upozoravajućeg banera.[718]

Prema forenzičkoj praksi ukoliko je napadač ostvario neovlašćeni pristup na sistemu uz ostvarivanje root, odnosno admin privilegija, prepoznate su sledeće aktivnosti koje mogu da izazovu mnogo štete:

- dodavanje sebe tj. zlonamernog korisnika za budući pristup sistemu;
- dodavanje kompromitovanog sistema u botnet kolekciju za korišćenje u napadu na druge sisteme;
- korišćenje kompromitovanog sistema kao proxy servera za kompromitovanje drugih sistema;
- instaliranje rootkit alata za lakši povratak na sistem uz dobijanje kompletne kontrole nad sistemom;
- permanentna krađa informacija;
- upotreba sistema za skladištenje zabranjenog materijala; i
- onesposobljvanje sistema ili uništavanje svih informacija na njemu.

Napad na DHCP server predstavlja napad određenim paketima tzv. DORA procesa (discover, offer, request, acknowledge). Dobijanje DHCP adrese realizuje se kroz DORA proces koji podrazumeva razmenu 4 paketa, da bi se dobila IP adresa od DHCP servera. Prilikom forenzike mrežnih paketa pojaviće se veliki broj paketa iz DORA procesa tipa discover i offer. Discover je paket kojeg na mreži klijent šalje zajedno sa broadcast-om kako bi pronašao DHCP server. Nakon toga klijent dobija offer paket iz dhcp servera i odgovara

717 Napadi tipa Cross site scripting (XSS) nastaju kada zlonameni napadač na web sajt unosi takve maliciozne podatke da aplikacija izvršava nešto što nije predviđeno. U praksi ranjivosti na XSS su se prepoznale u određenim funkcijama web sajta (npr. pretraživač na sajtu, forme za logovanja, polja za komentare).

718 Http://cpsr.org/prevsite/cpsr/privacy/computer_security/cert_keystroke_monitoring.txt/, 27.05.2016.

sa request paketom. Kao odgovor od dhcp servera klijent dobija acknowledge paket koji sadrži informacije o IP adresi, DNS, gateway itd. Prilikom DHCP starvation attack-a zlonamerni napadač preko mrežne kartice broadcast-uje discover DHCP pakete u velikoj količini. Na taj način kada DHCP server primi te pakete za svaki novi paket on vrši rezervaciju IP adrese određenog poola. U slučaju da je pool veličine 250 adresa i ukoliko se kroz lažne pakete rezerviše svih 250 adresa, taj DHCP server ne može više da opslužiri regularne korisnike na mreži. Otkrivanje je moguće jedino forenzičkom analizom mrežnih paketa na osnovu koje će se utvrditi veliki broj generisanih discover DHCP paketa. Forenzička istraga mrežnih paketa podrazumeva „hvatanje", skladištenje i analizu mrežnih aktivnosti. To znači da su u fokusu samo mrežni događaji. Da bi se izvršila forenzička analiza mrežnih paketa forenzičar mora da prikupi mrežni saobraćaj. Jedan od načina je preko SPAN porta. SPAN port je port mrežnog uređaja koji prima kopije mrežnih paketa iz svih portova mrežnog uređaja. Sistemi za sniffing paketa (IDS sistemi, sistemi za sniffing) se priključuju na taj span port da bi prikupljali pakete sa svih portova. Uslov je postojanje upravljivog SPAN porta na mrežnom uređaju (switch, ruter). Postoje i drugi načini kod kojih se prikupljanje mrežnih paketa vrši pasivno (kroz kabl) uz pomoć specifičnih habova specijalne namene. Nakon što forenzičar prikupi informacije analizira se prikupljeni mrežni saobraćaj i generiše se izveštaj sa pronađenim bitnim mrežnim događajima (npr. prenošenje osetljivih podataka preko ICMP saobraćaja, brute force na određeni nalog). [719] U praksi se dešava da se informacije o mrežnim događajima sa mrežnih uređaja ukrštaju sa informacijama koje se mogu dobiti i iz radne memorije operativnih sistema koje se odnose na mrežne događaje. Alat za pretraživanje paketa prema kategorijama je Whireshark. Na taj način prilikom DHCP starvation napada možemo saznati ime računara, IP adresu računara koji je vršio broadcast velikog broja lažnih DHCP paketa (DHCP koristi za server UDP port 67, a za klijenta UDP port 68). Forenzičkom analizom ICMP paketa (npr. sumnjiva količina i veličina ICMP paketa) alatima, moguće je utvrditi da li su određene osetljive informacije slate preko ICMP paketa. IDS sistemi ne analiziraju ICMP pakete prema sadržaju, već je to moguće uz pomoć forenzičke analize uz pomoć namenskih alata kao što je Whireshark. Takođe ovim alatom je moguće detektovanje i IP spoofing napada. Kod ove vrste napada vrši se izmena source IP adrese mrežnog paketa na mreži. IP spofing tj. uređaj koji lažira svoju IP adresu jednostavno se detektuje na osnovu forenzičke analize saobraćaja

719 ICMP – osim što je dijagnostički protokol (PING) može se zloupotrebiti sa ciljem prenošenja podataka.

određenog switcha gde se prema source adresi može uočiti koja je lažna.

Forenzičkom istragom mrežnih paketa moguće je identifikovati i autentifikacione napade. Prilikom komunikacije između korisničkog računara koji je delegiran određenom domenu u lokalnoj mreži na primer logovanje sa korisničkim imenom i šifrom na domen, šalje se autentifikacioni paket domenskom kontroleru da se potvrdi ispravnost korisničkog kredencijala i odobri ili odbije pristup sistemu. Ova komunikacija koja se uspostavlja između korisničkog računara i domen kontrolera je izuzetno bitna sa stanovišta bezbednosti. Ukoliko neko presretne te pakete i realizuje njihovu reprodukciju može dobiti neovlašćeni pristup sistemu (stari domenski kontroleri su imali tu slabost). U okruženju sa savremenim domenskim kontrolerima to nije izvodljivo. Međutim i dalje postoji slabost na brute force autentifikacione napade. Ono što forenzika može da otkrije jeste da li je neko pokušavao da izvede ovakvu vrstu napada. U tom slučaju zlonamerni napadač generiše veliki broj paketa koji se šalju domen kontroleru. I u ovom slučaju koristi se alat za inspekciju mrežnih paketa Whireshark. Na taj način u njemu se može identifikovati određena TCP sesija u kojoj se generiše velika količina autentifikacionih paketa i na osnovu te analize doći do IP adrese sa koje se oni generišu odnosno sa koje je pokrenut brute force napad. U skladu sa ispravnom forenzičkom procedurom takođe potrebno je primeniti hešing algoritam na fajl koji sadrži kolekciju mrežnih paketa zbog utvrđivanja integriteta mrežnih paketa da bi se sprečilo manipulisanje sa sadržajem mrežnih paketa (izmena IP adresa u postojećem fajlu kroz namernu reprodukciju lažnih paketa sa lažnim IP adresama). Prilikom istrage mrežnih paketa forenzičar može pronaći zlonamerni program ili IP adresu sa koje je zlonamerni program komunicirao sa upravljačkim centrom. Moguće je saznati IP adrese i domene koji se koriste od strane zlonamernog programa. Dodatno kroz forenziku mrežnih paketa moguće je otkriti ranjivost koja je bila zloupotrebljena na korisničkoj strani, odakle je zlonamerni program imao komunikaciju (npr. u slučaju Ransomware zlonamernog programa).

Prednosti detekcije upada u sistem su višestruke: markiraju se napadi koje nisu sprečeni drugim sredstvima, sprečavaju se dalje širenja štete na računarskim sistemima ili u mreži nakon nastanka incidentne radnje (npr. nakon upada hakera na server), dokumentuju se postojeće pretnje i poboljšava se kvalitet, kontrola administracije i dizajn bezbednosti odnosno mehanizmi za detektovanje incidentne radnje koja aktivira odgovor na incident. Sve pomenuto ima za cilj kreiranje bezbednijeg funkcionisanja mreže i operacija

na računarima. Poseban *značaj detekcije upada u digitalnoj forenzici* je da se sa jedne strane utiče na poboljšanje bezbednosti u informacionim sistemima, a sa druge strane ti rezultati pomažu u procesuiranju incidentne/nedozvoljene aktivnosti. Bitno je istaći da se vreme zaštite izračunava na osnovu vremena potrebnog za detekciju i vremena reakcije na incidentnu/nedozvoljenu aktivnost.

4.3.2. Indikatori incidentnih odnosno nedozvoljenih aktivnosti

Za samu istragu veoma je važna inicijalna procena digitalnog istraživača koji mora da sagleda sve simptome incidentne aktivnosti, da bi se dobio odgovor na pitanje da li je u pitanju sistemski problem ili incidentna/nedozvoljena aktivnost. To za rezultat podrazumeva potvrđivanje da se radi o incidentu, identifikaciju incidenta i prijavljivanje incidentne radnje odnosno nedozvoljene aktivnosti. U daljem tekstu biće izneti neki od najčešćih *potencijalnih indikatora incidentne odnosno nedozvoljene aktivnosti* u praksi:

- -neobjašnjivo visoka iskorišćenost opreme (računarskih stanica, serverskih stanica, mrežnih resursa, storidža);
- -pojava upozorenja/alarma od strane sistema za detekciju napada IDS, firewall-a ili network trap dna sistema, može registrovati napad spolja ili izunutra;
- -veliki broj neuspešnih logovanja na sistem;
- -neobjašnjiva upozorenja ili alarmi firewall-a na OS;
- -logovanje putem skrivenih ili difoltnih korisničkih naloga (npr. guest);
- -registrovana neuobičajeno velika aktivnost na mreži ili na sistemu tokom neradnih sati;
- -izmenjeni datumi na fajlovima;
- -izmenjeni korisnički profil za logovanje;
- -neobjašnjivo zaključavanje korisničkih naloga;
- -izmenjena korisnička lozinka bez znanja korisnika;
- -pronađeno je postojanje novih SUID i SGID programa;
- -mrežni senzori detektuju neuobičajeno visoki nivo mrežne aktivnosti;
- -prisustvo novih naloga na sistemu, koji nisu kreirani od strane sistem administratora;
- -postojanje nepoznatih datoteka ili izvršnih fajlova;
- -neobjašnjivi oštećeni fajlovi ili servisi;
- -neobjašnjive promene u fajlovima ili dozvolama za pristup

direktorijuma;
-neobjašnjive promene privilegija;
-neobjašnjivi gubici osetljivih i kritičnih podataka;
-izmene web stranica na web serveru;
-postojanje hakerskih alata na sistemu (npr. exploiti, snifferi);
- izbrisani ili prazni log fajlovi;
- drastično smenjene performanse računara;
-obaranje računarskog sistema (nemogućnost bootovanja, iznenadna restartovanja računara, zamrzavanje, iznenadno isključivanje);
-detektovanje otvorenih backdoor portova na sistemu;
-neobičan način korišćenja programa kao na primer kompajliranja programa na korisničkom nalogu, koji ne pripada nalogu programerskog profila;
-na osnovu izveštaja o protoku saobraćaja na mreži generisanog od davaoca internet usluga;
-konstantno onemogućavanje normalnog rada antivirusnog programa;
-nemogućnost instaliranja novih aplikacija;
-aplikacije koje su najčešće korišćene nisu funkcionalne;
-nepravilan rad task menadžera (nemoguće je pokrenuti task menadžer);
-nemogućnost normalnog izvršavanja registry editora (pri pokretanju se zamrzava ili se zatvara);
-otvaranjem internet pretraživača vrši se redirekcija na nepoznate sajtove;
-izmena ili dodavanje sistemskih programa bez znanja administratora;
-prisustvo novog korisnika, na već instaliranom na email sistemu;
-prisustvo zabranjenog pornografskog sadržaja; i
-nestanak/krađa računara ili mrežne opreme.

4.3.3. Odluke koje se odnose na rešavanje incidentne odnosno nedozvoljene aktivnosti

Pre nego što se donese konkretna odluka o odgovoru na incidentnu/nedozvoljenu aktivnost, moraju se uzeti u obzir sve okolnosti i okruženje u kome se ona desila. Ukoliko se incidentna/nedozvoljena aktivnost desila u nekoj organzaciji, bitno je ustanoviti njene prioritete prema značajnosti. Na primer: vraćanje OS u operativno stanje, obezbeđivanje integriteta podataka,

procena efekta incidentna/nedozvoljene aktivnosti, prikupljanje dokaza. Potrebno je detaljno razmotriti prirodu incidenta/nedozvoljene aktinosti, da bi se razumelo na koji način se desila incidentna/nedozvoljena aktivnost i primeniti odgovarajuće zaštitne mere nad pogođenim računarskim sistemom. Treba utvrditi da li postoje sistemski uzroci incidentne odnosno nedozvoljene akivnosti (npr. nedostaci standarda, nepoštovanje standarda, nepoštovanje procedura itd.). Potrebno je predvideti i oporavak, kako kompromitovanog računara tako i onog koji je bio pod uticajem nedozvoljene aktivnosti. To za posledicu može imati upotrebu starijih verzija podataka, ranije stanje OS (eng. restore point) ili programa, koji obezbeđuju normalnu operativnost sistema. Neophodno je definisati odgovarajuće primene ispravki (eng. patch) nad OS sa ciljem onemogućavanja ranjivosti nad računarskim sistemima i treba odrediti odgovorna lica. Napominjemo da se sve vrste ispravki moraju prethodno testirati pre nego što se upotrebe na produkcionim sistemima. Osobe određene za ispravljanje sistemskih problema moraju da kontrolišu i prate napredak neophodnih ispravki.

Pored toga vrši se kontrola da li su primenjena zaštitna sredstva i kontramere bile efikasne, odnosno vrši se provera da li se nad svim kompromitovanom računarskim sistemima izvršila pravilna primena zaštitnih mera. Kada se incidentna/nedozvoljena aktivnost konstatuje u organizaciji (čak iako je odgovor na incident bio efikasan) potrebno će biti ažuriranje *bezbednosne politike*, kako bi se smanjio rizik od budućih incidenata odnosno nedozvoljenih aktivnost i utvrdile neophodne procedure, koje će budući odgovor učiniti efikasnijim. S obzirom da dogovorena adekvatna rešenja, kada je u pitanju nedozvoljena aktvnost, skoro uvek zahtevaju više resursa nego što je raspoloživo, treba uzeti u razmatranje i realizaciju proaktivne zaštite na OS.

Na donošenje rešenja takođe utiče i način na koji je izvršena incidentna/nedozvoljena aktivnost. Ukoliko je sistem kompromitovan, zlonamerni napadač može prići računarskom sistemu ili mreži preko kompromitovnih servisa (eng. vulnerable services), preko zadnjih vrata (eng. backdoors) ili putem važećih kredencijala (eng.credentials). Ukoliko se nedozvoljena aktivnost realizovala na osnovu *ranjivosti servisa* rešenja će da obuhvataju i razmatranje mrežnih protivmera, vršenje skeniranja ranjivosti OS i instaliranje zakrpa (eng. patches) i ispravki (eng. fixes). Ukoliko se nedozvoljena aktivnost realizovala na *osnovu zadnjih vrata*, rešenje će obuhvatiti i razmatranje mrežnih protivmera, detaljnu proveru računarskog sistema, vršenje skeniranja ranjivosti OS i instaliranje zakrpa (eng. patches) i ispravki (eng. fixes). Ukoliko je nedozvoljena aktivnost realizovana na osnovu

važećih *kredencijala*, rešenjem će se zahtevati izmena svih šifara na sistemu kao i primena nove autentifikacione šeme.

4.3.4. Forenzički odgovor na incidentnu/nedozvoljenu aktivnost

Odgovor na incidentnu/nedozvoljenu aktivnost može da postoji samo ako se ona uspešno bude detektovala. Prilikom prvog odgovora (forenzičkog ili tima u okviru kompanije) na incidentnu/nedozvoljenu aktivnost potrebno je doneti odluku o tome da li da se kompromitovani računar isključi ili da ostane uključen.[720] Ovo je vrlo teška odluka, jer nestabilni podaci (eng. volatile data) prilikom isključivanja računara mogu biti izgubljeni, pošto se nalaze u memoriji računara, stanjima mrežnih konekcija i stanjima startovanih procesa.[721]Takođe gašenje sistema može ne samo da utiče i na mogućnost izvođenja imidžinga, već može da promeni podatke koji se nalaze u OS.

Većina sistema se može isključiti na dva načina:

- *regularan shutdown* - podrazumeva uklanjanje operativnih aktivnosti sa sistema (zatvaranje otvorenih fajlova, brisanje privremenih fajlova, mogućnost brisanja swap fajla). Shutdown može inicirati i uklanjanje malicioznog materijala (uklanjanje rootkita koji je bio u memoriji ili trojanca, koji može da ukloni dokaze o malicioznim aktivnostima). Izvodjenje shutdown operacije je moguće sa korisničkim nalogom, koji ima dovoljno privilegija;

- *isključenjem napojnog kabla iz struje ili vađenjem baterije* (iz lap topa ili drugog prenosnog uređaja) - ovim postupkom moguće je sačuvati swap fajlove, privremene fajlove i ostale informacije koje mogu biti izmenjene ili obrisane regularanim shutdown-om. Mana ovog postupka je što naglim gubitkom struje fajlovi (najčešće su to otvoreni fajlovi ili fajlovi kojima je prustupljeno) na nekim OS mogu da se oštete. Za neke korisničke uređaje kao što su PDA ili mobilni telefoni uklanjanje baterije može za posledicu da ima

720 Postoje različiti tipovi timova za odgovor na incidentnu odnosno protipravnu aktivnosti (eng. computer security incident response team ili skraćeno CSIRT). Na primer postoje interni CSIRT timovi u okviru samih organizacija kao što su banke, korporacije, univerziteti i vladine organizacije. Zatim postoje nacionalni CSIRT timovi koji pružaju usluge na nivou cele države kao na primer Japanski CSIRT tim (eng. Japan computer emergencz response team coordination center ili skraćeno JPCERT/CC). U svetu postoje i centri za analizu sintetizovanih podataka (prikupljenih podataka), koji određuju trendove i modeluju incidentne aktivnosti da bi se predvidele buduće aktivnosti i pružili rana upozorenja. Takođe postoje i CSIRT provajderi koji nude svoje usluge odgovora na incidentnu odnosno protipravnu aktivnost na zahtev klijenata.

721 Leschke T. R., Shadow Volume Trash: $Recycle.Bin Forensics for Windows 7 and Windows Vista Shadow Volumes, U.S. Department of Defense Cyber Crime Institute, 2010.

gubitak podataka.[722]
Stoga forenzičar prilikom donošenja odluke o isključivanju računarskog sistema mora dobro poznavati karakteristike ispitivanog OS kao i vrstu podataka koje treba da sačuva. Takođe potrebno je voditi računa prilikom preuzimanja opreme kao na primer USB aktivnog hard diska ili SD kartice, jer se struktura fajl sistema može narušiti, a samim tim i integritet digitalnog dokaza. Ukoliko se nepažljivo postupi (izvlačenje aktivnog hard diska ili izvlačenje SD kartice na koju se aktivno upisuju podaci) moguće je da hardver za smeštaj podatka prilikom ponovnog aktiviranja pokrene rebuild proces koji može uništiti podatke koji se trenutno nalaze na njemu. Zbog toga se sve aktivnosti moraju detaljno dokumentovati i sprovoditi u skladu sa procedurama za forenzički inicijalni odgovor.

Ukoliko inicijalni odgovor vrši forenzički tim, vrlo je važno da se obezbedi *zaštićena komunikacija* između članova tima. U praksi se dalje vrše *intervjui* sa odgovarajućim osobljem da bi se dobile relevatne informacije o incidentnoj/nedozvoljenoj aktivnosti. Bitno je da se na osumnjičenom računaru na forenzički prihvatljiv način pregledaju svi mogući izvori informacija uključujući firewall, uređaje za nadgledanje mreže, svičeve i rutere. Svi računarski sistemi u mreži kao i mrežni uređaji su sumnjivi dok se ne sazna stvarna razmera incidenta. Cilj ove faze je da se prikupi što više informacija da se utvrdi da li se incidentna radnja zaista desila. Ako se desila incidentna radnja bitno je ispitati, u kolikoj meri će se to odraziti na poslovanje organizacije odnosno da li spada u nedozvoljenu aktivnost nakon čega bi otpočela zvanična istraga. Potrebno je izvršiti procenu obima incidentne radnje, izdvojiti neophodne resurse i definisati neophodan nivo stručnosti potreban za odgovor na nju.
U praksi se primenjuju sledeći *koraci u odgovoru na incidentnu radnju*:

-ograničava se obim i intezitet incidentne radnje;
-proveravaju se integriteti računara na mreži;
-proveravaju se integriteti svih mrežnih uređaja;
-proveravaju se integriteti svih firewall i direktorijuma na sistemu (cheksum);
-porede se sistemski fajlovi sa onima iz bekapa ili iz inicijalnih distribucija;
-uklanjaju se pojedinci koji predstavljaju potencijalnu pretnju;
-vrši se isključivanje osumnjičenog ili ciljanog računara sa mreže ili

722 National Institute of Justice, *Electronic Crime Scene Investigation. A Guide for First Responder,* 2001, https://www.ncjrs.gov/pdffiles1/nij/187736.pdf, 11.07.2016.

mrežnog uređaja;

-izbegava se logovanje na kompromitovan računar kao administrator (Windows OS) odnosno kao root korisnik (Linux OS); i

-vrši se promena šifara na svim računarima koji nisu kompromitovani, ali koji se nalaze u istoj mreži kao i kompromitovan računar.

Koraci odgovora na incident mogu se grupisati na sledeći način:

- *otkrivanje i prijava incidentne aktivnosti* - za forenzičku istragu značajno je ko je otkrio problem (korisnik, vlasnik programa, vlasnik sistema itd.);
- *potvrda da se radi o incidentu ili nedozvoljenoj aktivnosti* - za forenzičku istragu značajno je da li se radi o korisničkim, programskim, sistemskim incidentima (greškama) ili nedozvoljenoj aktivnosti;
- *pokretanje istrage* (korporacijske ili javne) u zavisnosti od tipa maliciozne aktivnosti (DDoS napad, neovlašćeni pristup ili izmena podataka, neovlašćeno mrežno ispitivanje, upotreba zlonamernih programa);
- *oporavak kompromitovanih resursa* - ukoliko je potrebno oporavak ugroženih sistema; i
- *izveštaj i preporuke za buduću zaštitu* - identifikovanje slabosti u mreži i na sistemima, i preporuke za poboljšanje bezbednosti.

Navedeni koraci *dokumentuju* se putem *čekliste inicijalnog odgovora*. Bitno je da se vodi računa da se ne ugrozi digitalno mesto zločina. Fokus treba da bude usmeren na sledeće kritične detalje: trenutni datum i vreme, ko izveštava o incidentnoj aktivnosti, tip incidentne aktivnosti, kada se ona desila, koji je program odnosno uređaj obuhvaćen incidentnom aktivnošću, kontakti osoba iz organzacije koji su obuhvaćeni digitalnom istragom.

Ukoliko je faza pripreme za incidentnu/nedozvoljenu aktivnost dobro realizovana ova faza će biti u mogućnosti da smanji vremenski okvir od detektovanja incidentne aktivnosti do potvrde da li se radi o incidentnoj ili nedozvoljenoj aktivnosti (ako je potvrđena u tom slučaju se pokreće zvanična istraga), kao i da se tačno i brzo odredi obim incidenta.

Potrebno je istaći da čak i najspremnije organizacije po pitanju bezbednosti mogu biti suočene sa nedozvoljenim aktivnostima kao što su: dela prevare, krađe, upada u računarske sisteme, finansijske prevare, krađa intelektualne svojine, DDoS napadi, podmetanje malicioznih programa itd.

Incidenti u okviru orgranizacije uglavnom se odnose na sledeće probleme:

- gubitak ili curenje osetljivih (poverljivih) podataka;

- neprihvatljivo korišćenje računarskih resursa od strane zaposlenih;
- širenje malicioznih programa (npr. virusi, crvi, špijunski programi);
- računarski upadi spolja;
- napadi tipa odbijanja servisa (na primer DoS, DDoS);
- manipulacija dokazima;
- prekid radnog odnosa sa zaposlenim koji je na ključnoj poziciji u IKT sistemu predstavlja vrlo ozbiljan sigurnosni problem; i
- istraga nad drugim zaposlenim licima u IKT sistemu.

U odgovoru na incidentnu aktivnost u zavisnosti od obima i tipa incidenta i veličine organizacija učestvuje veliki broj lica. Tu se pre svega misli na korporacijiski tim za odgovor na incident (kod velikih kompanija) ili digitalnog forenzičara (kod manjih kompanija), vlasnika ili programera aplikacije, stručnjaka za bezbednost informacija, administratora sistema, administratora zaštitinih barijera, mrežnog admministratora. U zavisnosti od tipa incidenta mogu da učestvuju lica iz različitih oblasti kao što su menadžeri poslovnih organizacija, advokati, tužioci, nadležni državni organi, kadar tehničke podrške i krajnji korisnici odnosno vlasnici sistema. Iz tog razloga je veoma važno da osoblje koje radi kao tehnička podrška edukuje razume na koji način napadači napadaju računarske sisteme i da mogu da uoče napade putem nadzora mrežnih aktivnosti.

*Forenzički odgovor na incidentu radnju/nedozvoljenu aktivnos*t podrazumeva ispunjavanje velikog broja različitih *ciljeva* kao što su:

- koordinisan odgovor na incident svih timova koji rade na istrazi;
- oporavak servisa na bezbedan način;
- dobijanje odgovora na pitanje da li se incident dogodio ili nije (da li je reč o nedozvoljenoj aktivnosti);
- prikupljanje preciznih informacija o incidentnim aktivnostima;
- procenjuje se obim i troškovi incidenta/nedozvoljene aktivnosti;
- izvođenje oporavka podataka ili informacija nakon izazvane štete ili gubitka;
- uspostavljanje kontrole nad pronalaženjem i pravilnim rukovanjem digitalnim dokazima;
- identifikovanje izvora napada i motivacije (da li je tip zlonamerne aktivnosti poznat javnosti);
- poštovanje prava na privatnost u skladu sa propisima;
- svođenje na minimum ometanja tekućeg poslovanja u mrežnom okruženju;
- omogućavanje sudskog postupka ili disciplinskog postupka (u

okviru kompanije postupak protiv učinioca);
- obezbeđivanje tačnih i pravovremenih izveštaja sa preporukama;
- smanjivanje izloženosti tj. ugroženost vlasničkih podataka;
- zaštita imovine i ugleda organizacije;
- edukacija rukovodećeg menadžmenta u cilju bolje sagledavanja i razumevanja bezbednosti; i
- pomoć oko bržeg detektovanja i/ili sprečavanja incidentnih/ nedozvoljenih aktivnosti u budućnosti (učenjem kroz iskustva, izmenama politika i procedura u organizacijama).

4.3.5. Politika bezbednosti

Formulisanje sveobuhvatne i efikasne politike bezbednosti (interno pravilo) predstavlja ideal bezbednosti računarskih sistema i mreža. Ona treba da bude prilagođena jedinstvenim karakteristikama organizacije uz obezbeđenje prihvatljive privatnosti zaposlenih. Prema Shimonskom svrha bezbednosne politike je da se formalno navedu ciljevi, pravila i formalne procedure, uz pomoć kojih je moguće definisati opšti bezbednosni položaj i bezbednosnu arhitekturu organizacije.[723] Pored toga Shimonski ukazuje da bezbednosna politika mora sadržati i *sedam važnih funkcija*: 1. mora biti razumljiva, 2. mora biti realna, 3. mora biti dosledna, 4. mora biti primenjiva, 5. mora biti dokumentovana, distribuirana i pravilno prezentovana, 6. mora biti fleksibilna, 7. mora biti periodično preispitivana.[724]

Prema Wylupskom-u, Champion-u i Grant-u politika bezbednosti treba da obuhvati i procedure od strane IT koje za cilj imaju preispitivanje bezbednosti, posebno onih elemenata koji utiču na produktivnost i privatnost zaposlenih.[725]

Bezbednosna politika se formira prema definisanoj imovini (hardver, programi, ljudski resursi) i procenjenom riziku. Jednu dobru *strategiju za definisanje imovine* (eng. assets), procesa u toku i procenu rizika predložio je Danchev u radu „*Building and implementing a successful information security policy*". Imovina i procesi u toku moraju biti definisani kako bi se osigurala

723 Nolan R., Baker M., Branson J., Hammerstein J., Rush K., Waits C., Schweinsberg E., *First Responders Guide to Computer Forensics: Advanced Topics*, Software Engeneering Institute Carnegie Mellon, 2005.

724 *Ibidem.*

725 Nikačević V., *Korporacijska istraga kompjuterskog kriminala sa implementacijom sigurnosne politike*, Ziteh - Udruženje sudskih veštaka za informacione tehnologije It veštak, 2010.

njihova zaštita.[726] Potrebno je prvo ustanoviti koja se imovina štiti, a zatim se vrši procena potencijalnih rizika. Predlaže se kreiranje lista imovne prema prioritetima na osnovu kritičnosti za organizaciju (kategorije, sistemi, i procesi). Procesom analize rizika potrebno je obuhvatiti, hardver, programe i mrežu. Pod *hardverom* se podrazumevaju svi serveri, radne stanice, prenosivi računari, prenosivi hard diskovi i drugi prenosni uređaji koji služe za skladištenje podataka (CD, DVD, BRD, USB flash i dr.). Kada je reč o *mreži* koja obezbeđuje spoljni pristup (zaposlenima, korisnicima ili partnerima) neophodno je razmotriti bezbednost tačke pristupa mreži organizacije, bez obzira da li je reč o dial-up ili VPN pristupu. Shodno navedenom neophodno je ograničiti pristup specifičnim programima, servisima ili serverima uz limitirano trajanje šifre. Neažurirani programi, servisi i sistemi mogu dovesti do ranjivosti sistema pa je neophodno politikom definisati i period skeniranja sistema na ranjivosti kako bi incidentne aktivnosti bile blagovremeno identifikovane. U praksi potencijalne bezbednosne pretnje mogu se pojaviti upotrebom *nezaštićenih programa*, fajl šering programa (vuze, morpheus, kaza, E-donkey, torrent, e-mule i dr.), instant čat programa, progama za zabavu i drugih besplatnih programa nepoznatog izvora. Zato je potrebno izvršiti procenu rizika, identifikovati digitalnu imovinu i definisati nivoe pristupa sa principom dovoljnih privilegija neophodnim za obavljanje potrebnih aktivnosti. *Digitalna imovina* može obuhvatati i informacije iz organizacije (vlasničke podatke, korisničke podatke), intelektualna vlasništava i pristup servisima (npr. email, internet i dr.). Politikom treba obuhvatiti i *kreiranje grupa i privilegija* svih onih koji koriste digitalnu imovinu u okviru organizacije na osnovu pozicije u organizaciji. Cilj kreiranja grupa jeste upravljanje pristupom informacijama uz pomoć autentifikacije, autorizacije i privilegija. *Autentifikcija* daje odgovor na pitanje ko se prijavljuje na sistem, *autorizacija* daje odgovor na pitanje šta želimo, a *privilegije* daju odgovor na pitanje zašto želimo (čitanje, pisanje, izvršenje).[727]

Upravljanje rizicima u okviru bezbednosne politike mora se posvetiti posebna pažnja. Prema Danchev-u rizici su podeljeni na: fizičke bezbednosne pretnje (zloupotreba šifri, virusna zaštita, prenosni uređaji, upravljanje incidentom) i internet pretnje (web pretraživanje, email, instant messaging, download programa i otvaranje fajlova). Upotreba šifri i njihova bezbednost mora biti pažljivo razmotrena.

Upotreba šifri treba da ima sledeće karakteristike:

726 Nolan R., Sullivan C. O., Branson J., Waits C., *First Responders Guide to Computer Forensics*, CERT Training and Education, Carnegie Mellon University, March 2005

727 *Ibidem.*

- mora da bude jedinstvena (jedan nalog jedna šifra);
- za šifru ne upotrebljavati porodična imena, kućne ljubimce, matični broj;
- dužina šifre ne sme biti manja od 10 karaktera;
- šifra mora sadržati osim slova i brojeve i znakove;
- promenjena šifra ne sme biti slična prethodnoj, tako što joj se pridoda broj na kraju (doktorskiR2D$ ne sme postati doktorskiR2D$1);
- šifra na sistemu i na svim programima treba biti podešena, tako da automatski ističe posle određenog (definisanog vremena); i
- ukoliko je moguće treba kreirati infrastrukturu sa javnim ključevima i upotrebljavati dvofaktorske ili trofaktorske mehanizme autentifikacije.

Kada je reč o *virusnoj zaštiti* Danchev predlaže da se u bezbednosnoj politici eksplicitno definišu ponašanja zaposlenih na računarskim sistemima i na internetu kako bi se izbeglo izlaganje virusima. Preporuka je da se fajlovi i programi nepoznatog izvora nikada ne otvaraju. Svaki fajl ili program se mora skenirati ažuriranim antivirusim programom pre njegovog otvaranja bez obzira na ekstenziju koju ima, a najmanje jednom nedeljno neophodno je izvršiti antivirusno skeniranje kompletnog sistema (sa prethodno ažuriranim antivirusnim definicijama). Onemogućivanje antivirusnog programa treba biti zabranjeno osim u izuzetnim slučajevima usled privremenih intervencija nadležnih IT stručnjaka.

Upotreba prenosnih uređaja (USB flash, DVD, CD, floppy itd.) mora biti kontrolisana i ograničena na sisteme u okviru ogranizacije. Politikom treba onemogućiti pristup prenosnim medijima koji nisu vlasništvo organizacije. U izuzetnim slučajevima kada je nephodan pristup, uz nadzor IT stručnjaka i sa prethodnom proverom mogućih malicioznih programa, mogućno bi bilo korišćenje prenosnih uređaja.

Proces obavljanja periodičnog *sistemskog bekapa* i njegova verifikacija kao i održavanje računarskih sistema moraju biti obuhvaćeni bezbednosnom politikom.

S obzirom da svaki bezbednosni upad ima svoje specifičnosti u svojoj bezbednosnoj politici organizacija mora da ima prethodno definisan i implementiran *plan inicijalnog odgovora* koji pruža uvid u načine odgovora na ranjivost. Organizacija treba da ima u pripravnosti spreman tim obučenih kadrova sa mogućnošću upotrebe forenzičkih tehnologija za praćenje zloupotrebljenog exploita ili druge zlonamerne aktivnosti.

Za *Internet rizike* (web pretraživanje, email, instant messaging, download programa i otvaranje fajlova) prema Danchevu neophodno je politikom pažljivo odrediti prihvatljivu upotrebu svake aktivnosti, koje mogu

dovesti do kompromitovanja bezbednosti. Neophodno je definisati kada i na koji način zaposleni mogu da pretražuju web, downloaduju fajlove, otvaraju fajlove, koriste email i druge servise. Bezbednosni rizici moraju biti jasno određeni, a aktivnosti moraju biti praćene u slučaju neodgovarajućih ili nedozvoljenih aktivnosti.

Udaljeni pristup putem VPN forme ili bežičnim putem jeste dobar za produktivnost, ali bez kontrole sistema i mreža organizacija se izlaže bezbednosnim pretnjama. Sistemi koji koriste VPN obavezno moraju biti zaštićeni firewallom i redovno ažuriranim antivirusnim programom, jer bez njih su i sistem i mreža ranjivi na upade. Korišćenjem WI-FI tehnologije računarski sistemi mobilnih korisnika (eng. Lap top users) u bezbednosnom smislu potencijalno ranjivi i zlonamerni napadači mogu da iskoriste ranjivosti (npr. da ukradu podatke, unesu viruse, šire spam, izvrše DoS napadi). Najveći broj zloupotreba WI-FI ranjivosti se dešava prilikom korišćenja javnih hotspot lokacija. Prema istraživanju Wireless Broadband Alliance (WBA)[728] u saradnji sa Informa[729] organizacijom, početkom 2011. godine registrovano je 1.3 miliona javnih hotspot-ova sa tendencijom rasto na 5.8 miliona do 2015. godine.[730] Ova statistika govori da će izloženost bezbednosnom riziku mobilnih korisnika biti u sve većem porastu. Bezbednosnom politikom treba onemogućiti pristup mreži mobilnim uređajima koji nisu pod kontrolom organizacije odnosno u njenom vlasništvu.

Može se reći da dobra bezbednosna politika u organizaciji zapravo predstavlja uspostavljanje balansa između potreba korisnika i rizika koje te potrebe nose sa jedne strane i zaštite i prihvatljive privatnosti sa druge strane. Politika bezbednosti mora biti dostupna svim zaposlenima u elektronskom ili papirnom obliku. Prilikom njenog distribuiranja zaposleni treba da svoju saglasnost o pridržavanju u skladu sa bezbednosnom politikom potvrde svojim potpisom. Značajnije dopune, izmene i brisanja se prosledjuju obaveštenjima u formi maila, govornom poštom i drugim sredstvima obaveštavanja. Politikom je potrebno jasno i precizno definisati prihvatljive aktivnosti, nedozvoljene aktivnosti i lične aktivnosti zaposlenih (odobrenih uz saglasnost odgovarajućeg hijerarhijskog nivoa). Osim toga je potrebno izraditi precizne liste i procedure sprovođenja disciplinskih postupaka u slučaju kršenja bezbednosne politike. Reviziju bezbednosne politike treba vršiti prema definisanom vremenskom periodu. Njen cilj jeste ispravka i

728 Wireless Broadband Alliance (WBA), http://www.wballiance.com/, 29.05.2016.

729 Informa, http://www.informa.com/, 29.05.2016.

730 Global public Wi-Fi hotspots to hit 5.8 mln in 2015, Telecompaper, http://www.telecompaper.com/ news/global-public-wi-fi-hotspots-to-hit-58-mln-in-2015--837903, 29.05.2016.

eliminisanje što većeg broja ranjivosti na sistemima i mreži nakon stečenih novih znanja iz incidentnih aktivnosti i odgovora na njih.

4.3.6. Formulisanje strategije odgovora

Strategija odgovora mora biti obuhvaćena bezbednosnom politikom. Podrazumeva uključivanje nadležnih lica odnosno donosioca odluka u organizaciji. Važno je razumeti karakter incidenata, što podrazumeva svesnost, sagledavanje potencijalnog uticaja na poslovanje, moguće počinioce i razumevanje načina na koji se način desila nedozvoljena aktivnost. Da bi strategija odgovora pružila zadovoljavajuće rezultate neophodno je njome obuhvatiti osobu, koja će biti odgovorna za formulisanje strategije odgovora. Osim toga potrebno je odrediti i pojedince koji će učestvovati u realizaciji uspostavljene strategije odgovora na nedozvoljenu aktivnost. Važno je odrediti prioritete organizacije i koliki je njihov uticaj na odgovor na nedozvoljenu aktivnost, kao i definisati izvodljive opcije odgovora u odnosu na prioritete.

Treba uzeti u obzir sledeće faktore koji direktno utiču na strategiju odgovora na nedozvoljenu aktivnost:

-kolika je ugroženost kompromitovanog sistema;

-koji je tip incidentne radnje u pitanju - (npr. DoS napad, krađa, distribucija nedozvoljenog sadržaja, ugrožavanje privatnosti, vandalizam);

-da li će se pokretati interna ili javna istraga;

-osetljivost podataka;

-da li je nedozvoljena aktivnost poznata javnosti;

-nivo postignutog neovlašćenog pristupa od strane zlonamernog napadača;

-ko su počinioci - unutrašnji ili spoljašnji napadači;

-veština napadača;

-koliki je vremenski zastoj na sistemu i koliko se on može tolerisati (npr. ukoliko je kompromitovanjem serverera onemogućen neki bitan servis, donosi se odluka na koji način će se server povratiti u operativno stanje tj. da li će se oporavak realizovati on-line ili post-mortem);

-klasifikovanje kompromitovanog računara (da li je u pitanju server ili radna stanica korisnika);

-procena ukupnog gubitka; i

-koliki su preostali raspoloživi resursi za rešavanje nedozvoljene aktivnosti.

Ovom strategijom potrebno je definisati ko treba da bude uključen u donošenju odluka i ko treba da rukovodi i da realizuje odgovor na nedozvoljenu aktivnost i korake koje treba sprovesti. Organizacija može

da iskoristi bezbednosne incidente i kao sredstvo za obuku i za reviziju bezbednosne politike.

4.3.7. Nedostaci forenzičkog odgovora „uživo“ i najčešće forenzičke greške

Odgovor “uživo “ zahteva upotrebu pripremljenih alata za odgovor “uživo”, ali oni nisu apsolutno nezavisni od OS. Takođe zahteva se postojanje decentralizovanih off-site lokacija (eng. off-site location) za odgovor na nedozvoljenu aktivnost.[731] Podrazumevana je obuka lica koja će da realizuju off-site odgovor na nedozvoljenu aktivnost. Prilikom prikupljanja uživo doći će do promene vremenskih pečata (eng. stamps) datuma i vremena prikupljanih podataka (npr. vreme pristupa fajlu).

Neophodna je međusobna interakcija za dobijanje brojeva portova, broja particija i imena log fajlova i korisničke konfiguracije. Zahteva se administratorsko logovanje na svakoj konzoli.

Nije dozvoljena forenzička duplikacija "uživo". Dobijene informacije odnosno izlazi dobijeni forenzičkim alatima nisu uvek dobro organizovani i pregledni. Odgovor "uživo" nije moguće uvek realizovati.

Najčešće greške mogu se grupisati na sledeći način:

- *kršenje zakona* (neovlašćeno oduzimanje ili zaplena, prikupljanje dokaza, upotreba nelicenciranih programa kao i posedovanje ilegalnih programa);
- *uništavanje dokaza* (kroz pokušaj oporavka podataka, patchovanje sistema ili izmenom vremenskih i datumskih pečata nad dokazima na sistemu ili "ubijanje" zlonamernog procesa, improvizovanje forenzičkih procedura od strane sistem administratora zbog ne poznavanja procedure forenzičkog prvog odgovora, prilikom dobijanja infekcije isključivanje iz napajanja je pogrešno – svakim isključenjem ili rebotovanjnem sve što je u radnoj memoriji se briše);
- *neuspešno održavanje kompletne dokumentacije* (ne beleženje preduzetih koraka na sistemu, ne dokumentovanje procesa prikupljanja podataka, neuspešno dokumentovanje pronađenih

731 Kada se govori o off-site lokaciji misli se na off-site zaštitu podataka što podrazumeva slanje kritičnih podataka sa glavne lokacije odnosno van glavne lokacije tj. off-site lokacije. Može da se transportuje pomoću prenosivih medija za skladištenje podataka (npr. magnetne trake, optički uređaji i dr.). Off-site data protection, Wikipedia, http://en.wikipedia.org/wiki/Off-site_data_protection, 16.03.2016.

dokaza u forenzičkom maniru);
- *neuspešno kontrolisanje pristupu digitalnim informacijama*;
- *potcenjivanje obima incidentne radnje* odnosno nedozvoljene aktivnosti (podcenjivanje količine dokaza koji se mogu pronaći);
- *neblagovremena i neprecizna prijava incidentne radnje*, odnosno nedozvoljene aktivnosti (neuspešna prijava preciznim informacijama donosiocima odluka, na primer prijava pogrešnog vremena ili vremenske zone);
- *neuspešno ili neblagovremeno obezbeđivanje tačnih informacija* (predugo čekanje na prijavu incidenta); i
- *ne postojanje plana za odgovor na incidentnu radnju* odnosno nedozvoljenu aktivnost.

Da bi se navedene forenzičke greške eliminisale ili bar smanjile na prihvatljiv nivo u okviru organizacije neophodno je postojanje plana, kontrolisanje njegovog sprovođenja, dokumentovanje svih preduzetih forenzičkih mera i izveštavanje. Međutim čak iako se poštuju navedena upozorenje koja se odnose na greške, istraga može da se završi bez hvatanja počinioca, suđenja i sankcionisanja.

Razlozi su sledeći:[732] [733]

-gubljenje traga - jer je prošlo suviše vremena od incidenta i nema dokaza;

-nekompletno logovanje ili ga uopšte nema;

-cena istrage je veća nego gubici nastali usled incidenta, pa nije rentabilno nastaviti istragu;

-velik prostor skrivanja počinioca (internet), a incident se dogodio samo jedanput, sa malo ili bez imalo dokaza;

-incident nije sasvim određen - nije jasno da li je ili nije bezbednosni incident;

-ne može se nedvosmisleno ukazati na počinioca;

-nema dovoljno dokaza da se nedvosmisleno dokaže slučaj;

-postojanje političkog ili nekog drugog pritiska da se istraga zaustavi; i

-zataškavanje istrage.

732 Malin C. H., Casey E., Aquilina J. M., Malware Forensics - Investigating and Analyzing Malicious Code, Syngress 2008.

733 APWG, *Phishing Activity Trends Report, 3rd Quarter (July – September 2012)*, 2013, http:// www. apwg. org/download/document /84/apwg_trends_ report_q3_2012.pdf, 20.06.2016.

5. ZAKLJUČAK

Svakodnevno raste značaj i razvoj novih tehnologija, ali se istovremeno povećava i opasnost od visokotehnološkog kriminala. Problem visokotehnološkog kriminala je kompleksan fenomen. S obzirom da počinioci tih dela imaju potrebna znanja i koriste sofisticirane tehnike za njihovo izvršenje, sve im je teže ući u trag i nesumnjivo dokazati elemente krivičnog dela. Digitalna forenzika je nauka koja jedinstveno kombinuje informatičke discipline sa pravom i na taj način omogućuje efikasniju borbu sa visokotehnološkim kriminalom. Prirodna tendencija prava ka konzervativizmu često dolazi u sukob sa životom, s obzirom na njegovu dinamičnost. Brzina takvih promena naročito se ogleda u informatičkoj nauci i tehnologiji, koje su predmet stalnih inovacija i promena. Na primer, napredak u dizajnu operativnog sistema i hardvera prati i napredak upotrebe novih zlonamernih tehnika i alata, što postavlja za digitalnu forenziku veliki izazov, jer prevashodno mora da drži korak sa stalnim promenama.

Da bi se zaustavilo moguće širenje visokotehnološkog kriminala neophodno je uspostaviti multidisciplinarne timove za istragu, koji se sastoje od digitalnog forenzičara, pripadnika organa unutrašnjih poslova i tužilaštva. Za dokazivanje elemenata ovih specifičnih krivičnih dela, njihovih izvršioca i uzročno-posledičnih veza, neophodno je nesumnjivo i sa velikom preciznošću detektovati napad na računarski sistem, sprovesti adekvatne istražne radnje, analizirati način, vreme izvršenja i obim štete pomoću tehnika i alata digitalne forenzike poštujući odredbe nacionalnih i međunarodnih propisa. U svemu tome veliki doprinos ima upravo digitalna forenzika kao naučna disciplina koja daje precizne odgovore na pitanja koja se postavljaju kako u rešavanju problema izazvanih visokotehnološkim kriminalom tako i u postupku preventivne zaštite računarskih mreža i sistema.

Digitalni podaci u računarskom sistemu i mreži, a naročito na internetu veoma su osetljivi na potencijalne zloupotrebe. Digitalna forenzička istraga, digitalni dokazi, njihovo prikupljanje i analiza na forenzički ispravan način opisani su u ovoj knjizi sa namerom da se znanja iz oblasti digitalne forenzike prate i proširuju. Motivi visokotehnoloških kriminalaca najčešće su u materijalnim, a ređe nematerijalnim razlozima. Oni nastoje da uz pomoć najnovijih metoda i malicioznih programa prikrivaju svoje prisustvo na računarskom sistemu. Tragovi kompromitovanja računarskog sistema upravo se otkrivaju forenzičkim alatima, razmatranim u okviru ove knjige. Nastojali smo da predstavimo forenzičke metode, alate i njihovu primenu sa ciljem

pronalaženja dokaza prihvatljivih na sudu u skladu sa važećim propisima. Posebnu pažnju smo posvetili predstavljanju načina i ograničenja prikupljanja postojanih i brzo promenljivih podataka na Windows i Linux platformama. U knjizi je dat prikaz softverskih forenzičkih alata za inicijalni odgovor, pojedinačnih alata za oporavak podataka i particija i prikaz forenzičkih kompleta alata koji mogu realizovati više elemenata forenzičkog procesa.

Jedan od ciljeva knjige bio je da se prikaže gde i kako se mogu pronaći digitalni dokazi, koji potvrđuju nedozvoljenu aktivnost koja se realno može dogoditi, a koja je u vezi sa računarskim sistemom ili mrežom. Predstavili smo primere najčešćih ranjivosti na Windows i Linux sistemima i načine zlonamernog iskorišćavanja sistema koji su otkriveni kroz procese forenzičke istrage i analize. Prikazani su ranjivi servisi koji mogu ugroziti bezbednost sistema i predložene su adekvatne mere proaktivne zaštite. Kada je reč o zaštiti, treba napomenuti da ne postoji jedinstvena tehnologija - srebrni metak, koji može rešiti sve bezbednosne probleme u organizaciji. Ukoliko se u životu želi postići određeni cilj, mora se naporno raditi uz mnogo odricanja. U tom smislu ni postizanje maksimalne zaštite nije izuzetak. Realizovanje prihvatljivog nivoa bezbednosti u organizaciji zavisi od uloženih resursa. Većom upotrebom proceduralnih i tehničkih zaštitinih mera, povećava se zaštita sistema, a time i nivo bezbednosti u celoj organizaciji.

Pravilnom i redovnom upotrebom alata sa kojima se vrše skeniranja i logovanja ranjivosti na sistemima, uz prisustvo forenzičkog stručnjaka, moguće je dobiti detaljan uvid u nezakonite procese na sistemu i sprečiti da se dogode dalje nedozvoljene aktivnosti u okviru mreže ili određenog računarskog sistema. Integrisanjem rezultata proaktivne digitalne forenzike zajedno sa sistemima preventivne zaštite, detekcije i analize ranjivosti, kao i primenom višeslojne arhitekture zaštite uz pravovremeni odgovor na incidentne/nedozvoljene aktivnosti, moguće je povećati bezbednost sistema i ostvariti optimalan nivo zaštite adekvatan definisanoj bezbednosnoj politici.[734]

Konačno, knjiga je obezbedila koncizan, ali dovoljno detaljan opis najznačajnijih aktuelnih kretanja u okviru digitalne forenzike i implikacije u više različitih oblasti - informatičke nauke, pravne nauke, bezbednosti i kriminologije. Vrlo je verovatno da će istraživanja opisana u knjizi biti izuzetno primenljiva i koristan resurs istraživačima, studentima i stručnjacima iz različitih oblasti. S obzirom da je u knjizi opisano korišćenje forenzičkih alata, sa brojnim primerima primene u praksi (na terenu i u laboratorijama), to ovu

734 Korać V., Infrastruktura sa javnim ključevima u funkciji zaštite informacionog toka i elektronskog poslovanja, Arheologija i prirodne nauke, specijalna izdanja, Centar za nove tehnologije, 2010.

knjigu čini upotrebljivom i profesionalcima u pravosudnim organima, policiji i kompanijama, koje svakodnevno obavljaju poslove digitalne forenzike računarskih sistema. Sve što je u knjizi prikazano namenjeno je isključivo za istraživanje i unapređenje bezbednosti računarskih sistema, prevenciju i suzbijanje visokotehnološkog kriminala tako da se autori na ovaj način ograđuju od eventualnih zloupotreba prikazanih alata i tehnika.

6. REČNIK POJMOVA I IZRAZA

Active content	Eng. aktivni sadržaj. Interaktivni ili animirani sadržaj koji se koristi na web lokacijama. On uključuje ActiveX kontrole i dodatne uređaje web pregledača koji predstavljaju male programe čija je upotreba na internetu rasprostranjena. Pregledanje weba može postati zabavnije zahvaljujući aktivnom sadržaju jer on obezbeđuje trake sa alatkama, podatke o akcijama, video zapise, animirani sadržaj itd.
Adware	Oglašivački softver ima velike sličnosti sa spajverom iz razloga što obe vrste programa se baziraju na prikupljanju informacija o korisniku u njegovim navikama. Razlika je u tome što je advere više marketinški orijentisan. Prikupljene informacije se šalju kompanijama koje se bave posebnom vrstom marketinga (engl. behavioural marketing) koja se bavi analizom i praćenjem korisničkih navika prilikom web pretraživanja i oglašavanja. Javlja se u obliku iskačućih prozora (eng. pop-ups) kao reklamni oglas ili preusmeravajući web browser na određene web lokacije sa namerom da korisnika navedu na kupovinu. Ova vrsta programa će praćenjem korisničkih navika pokušati da se uklopi u kontekst onoga što korisnik radi. Npr. ako korisnik pretražuje na internetu reč potter rezulatat može biti neželjena reklama za knjigu o Harry Potteru. Neki adveri su nepošteni i zbog toga mogu da se klasifikuju kao špijunski program. Razlog je što ova vrsta programa osim što prikuplja podatka može i dalje da prenosi informacije o korisnicima što može biti deo opet marketinške svrhe. Instaliraju se uglavnom kao samostalni programi i uglavnom dolaze uz besplatne programe, tako što većina korisnika ne čita uslove upotrebe programa (eng. EULA ili End User Licence Agreement – predstavlja ugovor o licenci softvera, za krajnjeg korisnika) kojeg instalira i prihvata dalju instalaciju po predloženim uslovim što prouzrokuje instaliranje i adware programa. Često dolazi sa integrisanim spajverom ili drugom malicioznim programom koji ugrožava privatnost korisnika (špijunirajući korisnički osetljive podatke). Takođe kao i spajver programi, prisustvo adwera utiče na performanse računarskog sitema i oni nemaju samo-replicirajuću osobinu. Uklanjaju se sa računara alatima za uklanjanje malicioznih programa ili pomoću naprednijih antivirusnih programa.
Auditing	Praćenje tragova aktivnosti na sistemu.
Backdoor	Eng. zadnja vrata - predstavlja metod zaobilaženja normalne autentifikacije putem neprimećenog obezbeđivanja daljinskog pristupa računaru. Jedna posebna vrsta zadnjih vrata je RAT alat za daljinsku administraciju (eng. Remote access trojan). Ovaj alat omogućuje daljinsko nadgledanje i upravljanje i pristup računaru. Mogu biti instalirani od strane korisnika (za daljinski pristup od kuće ili da se dozvoli help desk-u) ili neprimetno od strane nekog malicioznog programa (da se nanese šteta ili ukradu informacije).
Benefit	Prednost, korist.
BIOS	Eng. basic input/output system, osnovni ulazno-izlazni sastav. Standardni kompjuterski program, koji se prvi pokreće nakon uključenja računara IBM, PC. BIOS postavlja osnovne radne parametre računara i pronalazi i učitava operacijski sastav u radnu memoriju (RAM).
Botnet mreža	Umreženi računari namenjenih distribuciji nelegalnih sadržaja ili piraterije.

CERT	Eng. Computer emergency response teams. Tim za reagovanje na sajber pretnje. U knjizi se upotrebljava I kao standardi od CERT Division of the Software Engineering Institute Univerziteta Carnegie Mellon.
Cloud computing	Tip je virtuelnog okruženja. Korisnik dobija pristup računaru koji je smešten na udaljenom serveru. Sistem omogućava korisniku bezbedan i udoban rad. Prednost ovog sistema je što korisnik ne mora da razmišlja gde mu se nalazi računar, a podaci su mu uvek na raspolaganju. Ne mora da brine ni održavanju tog računara, a može imati na raspolaganju i ogromnu količinu prostora. Postupak uspostavljanja konekcije sa virtuelnom mašinom je jednostavan. Postoje određeni programski klijenti koji su zaduženi za realizaciju ove konekcije prema serveru koji je priključen na javnu mrežu. Posle uspešnog postupka autentifikacije korisnik pristupa svojoj virtuelnoj mašini.
Clickjacking	Tehnika prevare web korisnika iskorišćavajući neki sigurnosni propust na sistemu ili iskorišćavajući ranjivost nekog web pretraživača sa ciljem otkrivanja poverljivih informacija ili prezuzimanja kontrole nad računarom. To se realizuje tako što korisnik klikne na naizgled bezazlenu stranicu i počinje da se izvršava neki kod ili skripta bez znanja korisnika. Zapravo „dugme“ odnosno link koji je bio kliknut počinje da obavlja neku drugu funkciju, a ne onu za koju je korisnik bio obavešten. Npr. korisnik može da primi mail sa linkom za neki video zapis, ispod koje stoji skrivena druga stranica npr ebay.com. Kada korisnik pokuša da klikne na „play“ zapravo kliknuće na „buy“ na ebay aukciji. Isto tako dešavale su se ove vrste prevara čime se omogućivalo uključivanje web kamera i mikrofona kroz Adobe Flash Player za koji je ubrzo objavljena sigurnosna zakrpa.
Clipboard	Sadržaj privremene memorije.
CPU	Eng. Central processing unit. Procesor, izvršna jedinica u računarstvu. Prima i izvršava instrukcije iz odgovarajuće memorije. Kada se kaže procesor, misli se na centralni procesor, koji je jedan od najvažnijih elemenata računara.
Crv	Zlonamerni program, koji ima samoreplicirajuću osobinu kroz računarske mreže. Za razliku od računarskih virusa kojima je neophodno da se prikače (eng. attach) na postojeći program, crv je samostalan i širi se od računara do računara kroz mrežu i ne oslanja se na druge izvršne kodove (nije potreban program domaćin da bi radio). Mogu da se šire putem elektronske pošte (na primer ukoliko se e-mail adresar zarazi crvom, repliciraće se kroz sve kontakte iz adresara i izvršiće zarazu email adresara tih kontakata), deljenih datoteka (eng. file sharing) ili internet servisa koristeći različite tipove protokole u komunikaciji (FTP, HTTP, P2P). Uvek izazivaju neku štetu na mreži kao na primer trošenje hardvereskih resursa što u nekim slučajevima može da preraste u obaranje servisa. Računarski crvi se mogu ukloniti korišćenjem alata za uklanjanje zlonamernih programa.
Cyber grooming	Sajber manipulacija, vrsta psihološke manipulacije koja se obavlja na internetu preko sinhronih i asinhronih komunikacionih platformi (javne chat pričaonice, internet sajtovi za upoznavanje, instant messengeri i VOIP servisi tipa ICQ i Skype) i u novije vreme putem društvenih mreža (facebook, twitter, myspace).
DFIP	Termin koji se odnosi nba digitalno forenzičke istražitelje tj. profesionalce potpuno obučene i sa velikim iskustvom, koji striktno poštuju metode pravila i procedure digitalno-forenzičke istrage.

Direktorijum	Predstavlja je katalog strukturu sistema datoteka (npr. sadržaj diska u DOS sistemima), koja sadrži reference prema ostalim računarskim datotekama i često prema drugim direktorijumima. U Windows OS sinonim je za termin folder.
DNS	Eng. Domain Name System. Omogućava komunikaciju između pojedinih računara u nekoj mreži (a pre svega na internet mreži) se zasniva na principu IP-adresa koje su izgrađene ciframa kao npr. 156.480.22.34. DNS je u stvari jedna baza podataka u kojoj su upisana sva imena i odgovarajuće IP-adrese pojedinih računara, te grupa funkcija koje omogućavaju prevođenje istih.
DoS	DoS napad (eng. distributed denial-of-service, napad odbijanjem usluga) predstavlja napad na neki servis informaciono komunikacionog sistema (najčešće web servis) sa ciljem da se korisnicima onemogući njegovo korišćenje. Pokretanje ove vrste napada sa jedne mašine nije dovoljno da se izgeneriše velika količina internet saobraćaja da bi mogao da se obori veliki sajt i lako se može izblokirati računar sa kog se to pokušava prostim prekidom konekcije sa tim računarom. DoS napad može se izvršiti na lokalnom računaru ili sa udaljene lokacije. Međutim, ukoliko u napadu učestvuje veliki broj zombi računara na ciljani servis, može se desiti da se uspešno realizuje napad. Koordinisan DoS napad u kome učestvuju ogroman broj mreža zombi računara naziva se DDOS napad ili distribuiran DoS napad. Te mreže zaraženih računara (zaraženih nekim zlonamernim programom npr. trojanskim konjem ili crvom ili backdoorom) nalaze se pod kontrolom zlonamernog napadača i mogu se zloupotrebiti na takav način da svi računari istovremeno pošalju veliki broj specifičnih zahteva na neku IP-adresu čim uspešno mogu da realizuju napad npr. obaranje web servisa. Ovi napadi su vrlo problematični i u današnje vreme najčešće se izvode putem tzv. botneta. Veliki broj instalacija operativnih sistema ostala je na onoj osnovnoj formi (sveža instalacija) bez instaliranja sigurnosnih zakrpa (eng. patch) i kao takva postaje podložna napadima crva, što govori o ozbiljnosti ovog problema. Iz prakse može se reći da su najugroženiji oni računari koji su neprekidno na internetu i imaju stalnu IP-adresu (eng. static IP).
Dropper	Eng. kapalica. Predstavlja program koji sadrži neku zlonamernu komponentu koji je dizajniran da "instalira" neku vrstu malvare-a (virusa, spajvera, backdoora, itd.) na određenom sistemu. Dropper može biti samostalan ili izveden iz dve faze. Kod samostalog maliciozni kod se nalazi u njemu samom na takav način da se izbegne njegovo otkrivanje antivirusnim ili antimalver programima. Kada se radi o dvofaznom u prvoj fazi dropper downloaduje malver na ciljni računar a u drugoj fazi ga aktivira.
Enterprise rešenja	Eng. poslovna rešenja.
Ethernet	Danas najčešće korištena tehnologija za lokalne mreže (LAN).
Exploit	Zloupotreba. Zloupotreba ranjivosti, zlonamerno iskorišćavanje računarskog sistema računarskog sistema.

Fišing	Eng. Phishing – predstavlja način prevare korisnika računara u cilju otkrivanja ličnih ili finansijskih informacija putem lažne e poruke ili Web lokacije. Uobičajena phishing prevara na mreži počinje e porukom koja izgleda kao zvanično obaveštenje iz pouzdanog izvora, kao što je banka, preduzeće koje se bavi kreditnim karticama ili ugledni prodavac na mreži. Primaoce e poruka upućuje na lažnu web lokaciju gde se od njih zahteva da unesu lične podatke, kao što su broj računa ili lozinka. Ove informacije se nakon toga obično koriste za krađu identiteta.
Firewall	Eng. zaštitni zid. Firewall prati odlazni i dolazni saobraćaj koji prati i snima u log fajlove mrežni saobraćaj.
Farming	Eng. Pharming - predstavlja način imitiranja drugog računara radi neovlašćenog upada i prevare sa kreditnim karticama. Farming je sličan fišingu, jer predstavlja sistem krađe poverljivih informacija, brojeva računa ili kreditnih kartica koristeći se lažnim web sajtovima. Predstavlja sofisticiraniji vid prevare od fišinga. Razlikuje se po tome što kod farminga nema 'mamca' na koji treba kliknuti (vec se realizuje samovoljnim odlaskom na web adresu). Dovoljno je da se otvori neki email i na taj način će se računar zaraziti nekim zlonamernim programom (virus, trojanac, keylogger) koji će krasti informacije sa računara. Na primer ukoliko korisnik želi da ode na sajt svoje banke, instalirani zlonamerni program će korisnika redirektovati na lažni sajt (a da korisnik toga nije svestan) koji izgleda isto kao i sajt banke i ukoliko korisnik ne prepozna da je redirektovan na lažni sajt uneće sve svoje podatke. Web sajtovi koriste imena domena kao svoje adrese na internetu, dok je njihova stvarna lokacija određena IP-adresom. Kada korisnik unese ime domena u svom web pretraživaču, ime domena se preslikava u neku IP-adresu putem DNS servera. Tada se web pretraživač povezuje na server sa tom IP-adresom i prezuma podatke sa Web strane. Ukoliko je korisnik posetio određeni sajt, podaci o DNS ulazu se pamte u DNS kešu korisničkog računara tako da se ne mora ponovo pristupati DNS serveru svaki put ukoliko korisnik želi da poseti taj isti određeni sajt. Zlonamerni program (koji se instalirao putem emaila zaraženog virusom) koji služi za farming, ustvari vrši izmenu DNS ulaza ili host fajla na korisničkom računaru i time se postiže automatsko prelikavanja određenog sajta u zlonamernu (farming) web adresu. Još veća opasnost je ukoliko se zaraze DNS serveri jer za posledicu može da se ima zlonamerno preusmeravanje velikog broja korisnika.
GB	Gigabajt
GBps	Eng. Gigabits per second. Gigabita po sekundi. Gigabit je merna jedinica za brzinu prenosa podataka u računarstvu i komunikacijama. 1 Gbps = 1,000 Mbps
Heširanje	Načini na koje Windows generiše i skladišti šifre korisničkih naloga.
Hibridi	Zlonamerni programi, kojima se ne može sa sigurnošću utvrditi kom tipu zlonamernog programa pripadaju. Razvojem programerskih paketa olakšava se stvaranje hibridnih malvara koji imaju karakteristike takve da odgovaraju karakteristikama različitih tipova zlonamernih programa. Npr. dešava se da neko isprogramira trojanca, koji ima samorepliciraju̇cu osobinu kao virus a da stvara backdoor.
Hive	U fizičkom smislu se sve registarske informacije smeštaju u fajlove tzv. hive.
host	Fizička mašina. Termin se upotrebljava i za komunikaciju sa virtuelnim mašinama, kao glavna mašina tj. računar.

IKT	Informaciono-komunikacionih tehnologije.
IMEI	Eng. The International Mobile Station Equipment Identity. Predstavlja jedinstveni broj (15 serijski broj ili 16 serijski broj IMEISV) koji je dodeljen svakom mobilnom telefonu (GSM, WCMDA, iDEN) i satelitskiom telefonu. IMEI broj se upotrebljava kao identifikacijski broj u GSM mrežama, kojima operator dopušta ili ne dopušta pristup mobilnoj mreži. Ako operator mreže zabrani pristup mreži pojedinom IMEI broju, tada se taj telefon iako ima ispravnu SIM karticu ne može upotrebljavati.
Integritet	Nepromenjenost npr. hard diska, podataka.
Kernel	Jezgro sistema.
Logičke bombe	Predstavljaju deo koda nekog programa koji pokreće zlonamernu funkciju (akciju) u određeno vreme ili datum ili kada određeni uslovi budu ispunjeni. Sastoje se od dva dela payloada i okidača (eng. trigger). Payload predstavlja nosilac komponente gde se definišu akcije koje će biti izvedene. Drugi deo čini funkciju za okidanje koja je definisana vremenom ili događajem prilikom koga će se biti izvršena nosiva komponenta. Logičke bombe su uglavnom delovi nekog virusa jer predstavljaju principe delovanja a ne celokupan mehanizam.
Lokardov zakon	Prilikom svakog kontakta dva objekta, postoji neka razmena materije, tj. Svaki kontakt ostavlja trag.
MAC adresa	Eng. Media Access Control Address. Predstavlja jedinstven broj hardvera na mrežnoj kartici, kojim se vrši identifikacija uređaja ili interfejsa na lokalnoj LAN mreži.
Malware	Eng. „maliciozni“ ili „zlonamerni“ softver. Pojam se odnosi na program koji je ubačen u sistem sa nemerom kompromitovanja poverljivosti, integriteta podataka, aplikacija ili OS.
MB	Megabajt
MD5, SHA-1, SHA-256 algoritmi	Algoritmi za heširanje su korisni za utvrđivanje integriteta digitalnih dokaza prikupljenih iz fajlova ili uređaja za skladištenje podataka.
Meta podaci	Npr. imena istraživača, beleške istraživača ili hash vrednosti. U digitalnoj forenzičkoj istrazi metadata podaci označavaju podatke o podacima.
Mount	Eng. Dodeliti. Na Linuxu, da bi neki fajl sistem mogao da se koristi mora biti mountiran - dodeljen sistemu.
Monitoring	Eng. praćenje aktivnosti na sistemu.
NIST	National Institute of Standards and Technology, američki Institut za standarde i tehnolgiju.
OS	Operativni sistem. Misli se na Windows ili Linux.
Outsourced programi	Programi koji se prave za ime i račun određene kompanije od strane neke druge kompanije. Eng. Outsourcing – ustupanje, izdvajanje, odnosi se na ustupanje poslova, funkcija, procesa firmama ili trećem licu.
Patch	Zakrpa, ispravka.
Protected storage area	Eng. Zaštićena oblast za skladištenje. Predstavlja oblast memorije, gde se osetljive korisničke informacije smeštaju. Kada je sistem isključen informacije se čuvaju u registarskoj bazi u šifrovanom obliku, dok se korisnik ne prijavi na sistem, kada se te informacije prebacuju u memoriju. Te informacije su šifre i podaci iz autocomplete forme Internet Explorera ili Outlook imena naloga i šifre, koji služe za odloženu upotrebu.

Proxy server	Računar koji stoji između klijenta i glavnog servera kao posrednik i omogućava posredan pristup sadržajima na internetu (najčešće web stranica).
Rabbit	Predstavlja posebnu podgrupa crva. Dobio je naziv po tome što mu je glavna osobina neverovatno brzo umnožavanje. Postoje dve vrste rabbita. Prva predstavlja program koji pokušava do potroši sve sistemske resurse kao na primer prostor na hard disku. Jedan od primera je i „forks bomb" , koji generiše veoma brzo veliki broj procesa (stvarajući procese sa beskonačim petljama) kako bi se iskoristio sav raspoloživ prostor na disku ili u memoriji. Kada se to desi postaje nemoguće pokrenuti novi program na sistemu. Druga vrsta zečeva je zapravo posebna vrsta crva koja predstavlja samostalan program koji se replicira mrežnim putem sa računara na računar ali tako da briše svoj originalni primerak nakon replikacije tj. na mreži postoji samo jedna kopija zeca (retko se dešavaju u praksi).
RAM memorija	Eng. Random Access Memory. Memorija računara koja sadrže podatke o procesima, informacije o stanju mreže, konekcije sa udaljenim računarom kao i mnoge druge.
Reboot	Gašenje računarskog sistema.
Redirekcija	U bukvalnom smislu upućivanje sa jednog mesta na drugo. U tehničkom smislu na primeru HTML-a, ako neko u tuđem HTML fajlu napiše kod i nakon ucitavanja istog, prebaci na neku drugu stranicu. Isto važi i za URL. Ukoliko se promeni putanja URL adrese, doći će se na potpuno drugu.
Registar baza	Sa logičkog aspekta registarsku bazu podataka se koristi za čuvanje sistemske konfiguracije i detalja o korišćenju. Čine je ključevi (eng. registry key) , koji se mogu pretražiti u programu Registry editor.

Rootkit	Program koji omogućava privilegovan pristup računaru/serveru od strane zlonamernog korisnika, aktivno krijući svoje prisustvo od administratora, u cilju narušavanja standardne funkcionalnosti operativnog sistema ili drugih aplikacija. Termin rootkit nastao je spajanjem reči "root" (što u linux terminologiji predstavalja tradicionalni naziv za privilegovanog korisnika računara/servera), a reč "kit" (eng. Komplet, koji se odnosi na programske komponente koje implementiraju ovaj alat). Neke od najkorišćenijih funkcija rootkit programa su sledeće: onemogućavanje logovanja aktivnosti, obezbeđivanje zadnjih vrata za ponovni ulazak na sistem, uklonjanje ili prikrivanje dokaza o inicijalnom ulasku u sistem, skrivanje sadržaja određenih fajlova, skrivanje fajlova i direktorijuma, prikupljanje informacija (šifre, korisnička imena, postojeći računari u mreži). Primer rootkit implementacije: napadač nakon iskorišćenja poznatih ranjivosti na sistemu (nekim od exploita) ili dobijanjem lozinke (razbijanjem zaštite ili putem socijalnog inženjeringa), dobija privilegovan pristup i mogućnost instaliranja rootkita. Rootkit omogućava napadaču da maskira tekući upad i održava privilegovan pristup računaru zaobilezeći mehanizme autentifikacije i autorizacije. Iako može da se koristi za različite namene termin "rootkit" ima negativne konotacije zbog njegove povezanosti sa zlonamernim programima koji utiču na sistem i sa krađom lozinki bez znanja administratora ili korisnika. Jako je teško otkrivanje rootkit-a jer je u stanju da zaobiđe program koji je namenjen da ga pronađe. Metode detekcije uključuju i korišćenje alternativnih operativni sistema, poređenjem hash vrednosti samog sistema - skeniranjem i analizom stanja memorije. Uklanjanje može biti komplikovano ili praktično nemoguće, naročito u slučajevima kada se rootkit implemetnira u samo jezgro, pa je jedino rešenje reinstalacije operativnog sistema. Jedan od projekata koji je usmeren na pronalaženju rootkita pod Linux operativnim sistemima je i Rootkit hunter.
Slek prostori diska	U upotrebi su kao sinonimi u literaturi I različiti termini poput fajl slek, RAM slek i drajv slek. Slek označava slobodan prostor. Izbrisani podaci ostavljaju tragove u nealociranim i slek prostorima diska, a odsustvo podataka ukazuje na antiforenzičku aktivnost i predstavlja osnovu za sumnju u nedozvoljene aktivnosti.
Sniffing	Eng. njuškanje. Uređaj koji je posebno dizajniran da prisluškuje mrežu ili da razotkrije lozinke.
Socijalni inženjering	Predstavlja upotrebu različitih psiholoških metoda sa ciljem uveravanja u lažni identitet napadača i iskorišćavanje situacije da se daju one informacije, koje nikad oštećeni ne bi dali.
Spam	Neželjena pošta.

Spyware	Spajveri ili špijunski programi predstavljaju oblike zlonamernih programa koji se instaliraju tajno na računarski sistem. Prikupljaju i šalju informacije zlonamernom napadaču, o upotrebi i drugim poverljivim i ličnim podacima korisnika. Predmet prikupljanja može biti bilo šta što potencijalno ima vrednost, a primera ima mnogo: korisnička imena, lozinke, e-mail adrese, brojevi kreditnih kartica, brojevi bankovnih računa, licence računarskih programa, praćenje posećenosti internet stranica, usporavanje internet veze, negativan uticaj na funkcionalnost programa računarskih sistema, izmene vezane za podešavanja bezbednosnih parametara računara (postavljajući ih na najniže vrednosti ili onemogućavanja istih), menjanje početne stranice web pretraživača u novu najčešće zaraženu, kao i mnoge druge osetljive i privatne informacije. Računar se može zaraziti spajverom na različite načine kao što su: besplatna online skeniranja sistema, razni dodaci web pretraživaču u vidu pluginova ili add-ona, kroz pristup sumnjivim sajtovima ili slikama pa čak i preko nekih pretraživača, a mogu biti prikačeni kao deo nekog programskog paketa pri instaliranju na sistem. Nisu isto što i virusi (koji takođe mogu da prikupljaju ovakve informacije), zato što nemaju osobinu samo repliciranja. Pojavljuju se i u obliku keyloggera kao podvrsta špijunskih programa, koji pasivno snimaju aktivnost na tastaturi (kucanje na tastaturi). Znači pored toga što rade sve dosad navedeno, u stanju su da vrše i periodična snimanja ekrana (eng. screenshot) definisana vremenski ili na korisnikov klikom miša (što korišćenje virtuelnih tastatura kao vid zaštite od špijuniranja nije adekvatno, jer se snima svaki klik po virtuelnim tipkama i to se beleži snimkom ekrana), pregledanje sadržaja međumemorije (eng. clipboard, deo memorije u koji se privremeno smešta isečeni ili kopirani tekst ili grafički objekat), praćenje unosa u web pretraživače, praćenje konverzacije messaging programa (windows messenger, skype i dr.), praćenje svih otvaranih prozora na sistemu kao i datoteka i to sve praćeno snimkom ekrana. Uklanjaju se korišćenjem antispajver alatima ili nekim antivirusnim programima koji imaju integrisanu antyspaware pretragu.
Storidž (sistemi)	Eng. memorija. Storidž sistemi omogućavaju skladištenje velikih količina podataka.
Stringovi	Eng. string. Na srpskom znače niska. Predstavljaju znakovni tip ili lanac podaka i skladištenje u memoriji. Skladište se tako što svaki simbol predstavlja korišćenje neke numeričke vrednosti.
(Network) Switch	Eng. mrežni prekidač. Aparat koji na mreži spaja različite uređaje te paketno prima, obrađuje i prosleđuje podatke na konačni uređaj. Za razliku od manje naprednih mrežnih čvorova, mrežni prekidač prosleđuje podatke ka jednom ili više uređaja kome su isti potrebni, a ne emituje te podatke iz svakog od njegovih portova.
TCP/IP	Eng. Transmission Control Protocol/Internet Protocol. Je uobičajena oznaka grupe protokola koja se još naziva IP grupa protokola. Omogućuje komunikaciju preko raznih međusobno povezanih mreža i danas je najrasprostranjeniji protokol na lokalnim mrežama, a takođe se na ovom protokolu zasniva i globalna mreža internet.

Trojanski konj (trojanac)	Predstavlja program koji se na prvi pogled čini kao koristan, ali tajno obavlja i neke zlonamerne operacije (da ukrade informacije ili šteti sistemu). Jednom kad se instalira omogućuje zlonamernom korisniku udaljeni pristup računarskom sistemu da bi mogao da obavi kriminalne aktivnosti. Može služiti da se ukradu osetljive informacije, da simulira proxy (eng. trojan proxy). Može se pojaviti i u formi trojan dialer-a (eng. dialers, zlonamerni programi koji pomoću modema pozivaju „premium-rate" putem veoma skupog uspostavljanja veze i cena impulsa) telefonske brojeve da bi se time ostvarila materijalna korist. Naravno postoje i špijunske forme trojanaca koji špijuniraju računarski sistem (eng. trojan spy), obaveštavaju napadača o aktivnostima korisnika na računaru (eng. trojan notifiers). Pored toga mogu i da evidentiraju aktivnost na tastaturi (eng. keylogging samo što ovaj tip keylogging-a nije samostalan kao kod spajvera). Karakteristika im je da se ne kopiraju sami i ne vrše zarazu fajlova, već to izvodi osoba koja ih je stvorila i preuzela kontrolu nad kompromitovanim računarom. Mogu se ukloniti ručno ili pomoću antivirusnog programa.
Umbrella termin	Eng. kišobran termin. Opšti termin.
USN Journal	Skraćeno od Update Sequence Number Journal - predstavlja funkciju u operativnom sistemu koja snima promene na NTFS volume-u. Svrha USN journal-a jeste da loguje sva ažuriranja fajlova i foldera na volume-u. Zadržava se zapis operacija sistema datoteka koji se može iskoristiti za oporavak oštećenja usled neplaniranog pada sistema.
Vendor	Eng. proizvođač.
Virtuelna mašina	Predstavlja kreirano okruženje od strane programskog paketa za virtuelizaciju koja poseduje simulirani skup hardvera (procesor, hard disk, memorija, mrežni uređaji i drugih komponenti) i sopstveni sistemski i aplikativni program.
Zaštitni prstenovi	U računarstvu hijerarhijska oblast zaštite se obično naziva zaštitni prstenovi, koji predstavljaju mehanizme zaštite podataka i funkcionalnosti od grešaka i zlonamernog ponašanja. Računarski operativni sistemi omogućuju različite nivoe pristupa resursima. Zaštitni prsten je jedna od dve ili više hijerarhijskih nivoa ili slojeva privilegija unutar arhitekture računarskog sistema. Prstenovi su organizovani hijerarhijski od najopvlašćenijih (obično su obeleženi brojem 0) do najmanje privilegovanih (obleleženi su većim brojevima). Na većini operativnih sistema nulti prsten je nivo sa najvećim privilegijama i na najdirektniji način ima interakciju sa fizičkim hardverom kao što je CPU i memorija.
ZKP	Zakonik o krivičnom postupku.
Zombi	Zlonamerni program, koji računarski sistem stavlja pod kontrolu zlonamernog napadača bez znanja vlasnika tog računarskog sistema. Uglavnom se koristi za lansiranje zlonamernog DoS napada.

7. LITERATURA

Aaron P., Cowen D., Davis. C., *Hacking Exposed Computer Forensics, Second Edition*, The Mcgraw-Hill Companies, 2010.

Acunetix Ltd., *Acunetix Web Vulnerability Scanner, Manual v. 4.0*, Acunetix Ltd, 2006. Izvor: http://www.acunetix.com/vulnerability-scanner.

Ahmad D., Dubrawsky I., Flynn H., Grand J., Graham R., Johnson N. L., Kaminsky D., Lynch F. W., Manzuik S. W., Permeh R., Pfeil K., Russell R., *Hack Proofing Your Network, Second Edition*, Syngress Publishing, Inc, Rockland, MA, 2002.

Alghafli K. A., Jones A., Martin T. A., *Forensic Analysis of the Windows 7 Registry*, Khalifa University of Science, Technology and Research, 2010.

Allen B., *Collecting Digital Evidence from Intrusion Detection System*, CGS 5132 - Computer Forensics II, 2002. Izvor: http://www.authorstream.com/ Presentation/ Kliment-24060-allen-Collecting-Digital-Evidence-Intrusion-Detection-Systems-designed-forensic-use-as-Entertainment-ppt-powerpoint/.

Altheide C., Carvey H., *Digital Forensics with Open Source tools*, Elsevier, Waltham USA, 2011.

Ansonand S., Bunting S., *Mastering Windows Network Forensics and Investigation*, Sybex, 2007.

APWG, *Phishing Activity Trends Report, 3rd Quarter (July – September 2012)*, 2013. Izvor : http://www.apwg.org/download/document /84/apwg_trends_ report_q3_2012.pdf.

Ashcroft J., Electronic Crime Scene Investigation - A Guide for First Responders, U.S. Department of Justice, 2001. Izvor : https://www.ncjrs.gov/ pdffiles1/ nij/187736.pdf.

Aycock J., *Computer Viruses and Malware* , Springer , Canada, 2006.

Baker S., Green P., Meyer T., Cochrane G., *Checking Microsoft Windows Systems for Signs of Compromise version 1.3.4*, 2005. Izvor: http://www.oucs.ox.ac.uk/network/ security/documents/win_intrusion.pdf.

Bajeglav T., Dimitrijević N., *Istraga aktivnog kompjuterskog incidenta*, Ziteh - Udruženje sudskih veštaka za informacione tehnologije It veštak, 2004. Izvor : http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-02.pdf.

Barrett D., Kipper G., *Virtualization and Forensics – A digital forensic Investigator's guide to Virtual Environments*, Elsevier Inc., USA, 2010.

Beebe N. L., Clark J. G., *A hierarchical, objective-based framework for the digital investigations process*, In Proceedings of the 2005 Digital Forensics Research Workshop, pp. 146-166, 2005.

Beek C., *Virtual Forensics*, TenICT proffesionals, 2010. Izvor: http://securitybananas.com/ wp-content/ uploads/ 2010/04/Virtual-Forensics _Black HatEurope2010_CB.pdf.

Bem D., Huebner E., *Computer Forensic Analysis in a Virtual Environment*, International Journal of Digital Evidence Fall 2007, Volume 6, Issue 2, 2007.

Bergadano F., Gunetti D., Picardi C., *User Authentication through Keystroke Dynamics*, ACM Transactions on Information and System Security, Vol. 5, No. 4, pp. 367-397, November 2002.

Bradford P. G., Hu N., *A Layered Approach to Insider Threat Detection and Proactive Forensics*, 21st Annual Computer Security Applications Conference, Applied Computer Security Associates (ACSA), 2005. Izvor: http://www.acsac.org/ 2005/techblitz/hu.pdf.

Brown C., *Computer Evidence - Collection and Preservation*, Thomson Delmar Learning, Charles River Media, Inc, Hingham, Massachusetts, pp. 213-218, 2006.

Bunting S., Wei W., *EnCase Computer Forensics: The Official EnCE: EnCase Certified Examiner Study Guide,* Indianapolis, IN: Wiley Publishing, 2006.

Burdach M., *Detecting Rootkits And Kernel-level Compromises In Linux*, Symantec, Novembar 2004. Izvor: http://www.symantec.com/ connect /articles /detecting-rootkits-and-kernel-level-compromises-Linux).

Burdach M., *Forensic Analysis of a Live Linux System, Pt. 2*, Symantec, April

2004. Izvor: http://www.symantec.com/ connect/ articles/ forensic -analysis-live-Linux-system-pt-2.

CARNet, *Tor - mreža za anonimnost*, CCERT-PUBDOC-2007-07-197, Revizija v1.1, str.13-14., 2007. Izvor: http://www.cis.hr/www.edicija/ LinkedDocuments/CCERT-PUBDOC-2007-07-197.pdf.

Carrier B., *Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers,* International Journal of Digital Evidence, Winter 2003.

Carrier B., *File System Forensic Analysis*, Addison Wesley Professional, 2005.

Carrier B., *Open Source Digital Forensics Tools - The Legal Argument*, @tstake, 2002. Izvor : http://www.digital-evidence.org/papers/opensrc_legal.pdf.

Carrier B., Spafford H. E., *Getting Physical with the Digital Investigation Process*, International Journal of Digital Evidence Fall 2003, Volume 2, Issue 2, 2003.

Carroll O. L., Brannon S. K., Song T., *Vista and BitLocker and Forensics! Oh My!*, Computer Forensics, Volume 56 Number 1, January 2008.

Carvey H., Altheide C., *Tracking USB storage: Analysis of Windows artifacts generated by USB storage devices*, Digital Investigation 2, pp. 94-100, Elsevier Academic Press, Burlington, MA 2005. Izvor: http:// www.sciencedirect.com/ science/article/pii/S1742287605000320/ pdfft?md5=b4d986c553c49a983e66ae2b68a0c4a6&pid=1-s2.0-S1742287605000320-main.pdf.

Carvey H., *Pearl scripting Live Response, Forensic Analysis, and Monitoring*, Syngress Publishing, Inc 2007.

Carvey H., *Windows Forensic Analysis DVD Toolkit 2E*, Elsevier, Inc. 2009.

Carvey H., *Windows Forensic Analysis DVD Toolkit*, Elsevier, Inc. 2007.

Carvey H., *Windows Forensics and Incident Recovery*, Addison Wesley, 2004.

Casey E., *Digital Evidence and Computer Crime - Forensic Science, Computers and the Internet*, Second Edition, Academic Press 2004.

Casey E., *Digital Evidence and Computer Crime - Forensic Science, Computers and the Internet*, third Edition, Elsevier Academic Press, 2011.

Casey E., *Digital Evidence and Computer crime*, Academic press, San Diego 2000.

Casey E., *Handbook of Digital forensics and investigation*, Elsevier Academic Press, Burlington, 2010.

Chad Steel, Windows Forensics: The Field Guide for Corporate Computer Investigations, John Wiley & Sons 2006.

Chaouchi H., Laurent-Maknavicius M., *Wireless and Mobile Network Security, Security Basics, Security in On-the-shelfand Emerging Technologies*, ISTE Ltd and John Wiley & Sons, Inc. USA, 2009.

Ciardhuáin O. S., *An Extended Model of Cybercrime Investigations*, International Journal of Digital Evidence. Summer 2004, Volume 3, Issue1, 2004. Izvor: https://utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf.

Citrix, *Citrix Xenserver,* Izvor : http://www.citrix.com/English/ps2/ products/ product.asp?contentID=683148.

Clarke N., *Computer Forensics A Pocket Guide*, IT Governance Publishing, United Kingdom, 2010.

Cole E., *Hackers Beware*, New Riders Publishing, 2002.

Communication from the Commission to the Council, The European Parliament, The Economic and Social Committee and Committee of the regions, *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, 2012. Izvor : http://europa.eu.int.

Computer Crime and Intellectual Property Section Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, United States Department of Justice, 2002. Izvor: http://www.justice.gov/ criminal/cybercrime/searching.html.

Convention on cybercrime, Council of Europe, Budapest novembar 2001. Izvor: http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc.

Council of Europe, Recommendation No. R (95) 13, Izvor: http://www.justice.gov/ criminal/cybercrime/crycoe.htm.

Cross M., *Scene of the Cybercrime*, Second Edition, syngress, 2008.

Danchev D., *Building and implementing a successful information security policy*, 2003. Izvor : http://www.Windowsecurity.com/pages/security-policy.pdf.

Dart K. A., *Deleted Files Can Be Recovered*, February 24, 2008. Izvor: http://www.akdart.com/priv9.html.

Davidovac Z., Korać V., *Vulnerability management and patching it systems*, Arheologija i prirodne nauke, br. 6, str. 129-144, Beograd, 2011.

Davis N., *Live Memory Acquisition for Windows Operating System : Tools and Techniques for analyses,* Eastern Michigan University, 2008. Izvor: http://www.emich.edu/ia/pdf/research/Live%20Memory%20Acquisition%20for%20Windows%20Operating%20Systems,%20Naja%20Davis.pdf.

Digital Forensics Research Workshop, *A road map for digital forensics research*, Technical report, Digital Forensics Research Workshop, 2001.

Drakulić M., Drakulić R., *Cyber kriminal*, Fakultet organizacionih nauka u Beogradu. Izvor: http://www.bos.rs/cepit/idrustvo/sk/cyberkriminal.pdf.

Ec-Council Press, *Computer Forensics: Investigating Data and Image files*, Course Technology Cengage learning, USA, 2010.

Ec-Council Press, *Computer Forensics: Investigating hard disks, file and operating systems*, Course Technology Cengage learning, USA, 2010.

Ec-Council Press, *Computer Forensics: Investigation procedures and response*, Course Technology Cengage learning, USA, 2010.

Farmer D. J., *A Windows Registry Quick Reference. eptuners.com,* October 2007. Izvor: http://www.eptuners.com/forensics/A%20Windows%20Registry%20Quick%20Reference.pdf.

Farmer D., Venema W., *Forensic discovery*, Pearson Education Inc, Crawfordsville, 2008.

Fogie S., *VOOM vs The Virus (CIH)*, 2004. Izvor: http://voomtech. com/downloads /Shadow%20Eval%20-%20Fogie.pdf.

Forensics science communications, *Digital Evidence : Standards and Principles*, Scientific Working Group on Digital Evidence (SWGDE)

International Organization on Digital Evidence (IOCE), Volume 2 - Number 2, April 2000. Izvor: http://www.fbi.gov/about-us/lab/forensic-science-communications/ fsc/ april2000/ swgde.htm/.

Foster M., Wilson J. N., *Process Forensics: A Pilot Study on the Use of Checkpointing Technology in Computer Forensics*, International Journal of Digital Evidence, Volume 3, Issue 1, 2004.

Frank Adelstein, *Live forensics: Diagnosing your system without killing it first*, Communications of the ACM, , 49(2) pp. 63–66, 2006.

Friedman C.S., *This Alien Shore*, Daw Books INC., New York 1998. Izvor: http://rose.digitalmidnight.org/temp/books/CS_Friedman/C.%20S.%20Friedman%20-%20This%20Alien%20Shore.pdf.

Garfinkel S., *Anti-Forensics: Techniques, Detection And Countermeasures*, In Proceedings Of The 2nd International Conference On I-Warfare And Security (Iciw), Naval Postgraduate School, Monterey, Ca, March 8-9, 2007.

Garfinkel S., Malan D., Dubec K., Stevens C., Pham C., *Disk imaging with the advanced forensics format, library and tools*, The second Annual IFIP WG 11.9 International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, USA, January 20-February 1, 2006.

Garfinkel S., *The Advanced Forensic Format 1.0.*, 2005. Izvor: http://stuff.mit.edu/afs/sipb/user/simsong/afflib/affdoc.doc.

Georgijević U., *Integrisani model procesa digitalne forenzičke istrage*, Ziteh - Udruženje sudskih veštaka za informacione tehnologije It veštak, 2006. Izvor: http://www.itvestak.org.rs/ziteh_06/Radovi/ZITEH%2006-R07.pdf.

Georgijević U., *Istražne metodologije, tehnike i alati za digitalnu forenzičku istragu*, master rad, Fakultet za informatiku i menadžment, Univerzitet Singidunum 2010.

Grubor G., *Funkcionalni model istrage kompjuterskog događaja*, Udruženje IT Veštak, 2004.

Grubor G., *Funkcionalni model istrage kompjuterskog kriminala*, Ziteh 2010.

Grubor G., Galetin A., *Digitalna forenzička istraga u korporacijskoj zaštiti*

informacija, Singidunum Revija, 2010.

Grubor G., Gotić A., *Korporativna aktivna digitalna forenzička istraga primenom Backtrack – a*, 10. Međunarodni naučni skup Sinergija 2012. Univerzitet Sinergija, 2012.

Harms K., *Forensic Analysis of System Restore Points in Microsoft Windows XP*, Mandiant Corporation, 2006. Izvor: http://citeseerx.ist.psu.edu/ viewdoc/ download?doi=10.1.1.84.4474&rep=rep1&type=pdf.

Harris R., Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem, Journal Digital Investigation: The International Journal of Digital Forensics & Incident Response, vol. 3, pp. 44-49, 2006.

Harrison W., Heuston G., Morrissey M., Aucsmith D. Mocas S., Russelle S., *A Lessons Learned Repository for Computer Forensics*, International Journal of Digital Evidence, Vol. 1 No. 3, 2002. Izvor: http://www. ijde.org /docs/ 02_fall_art2.html.

Haruyama T., Suzuki H., *One-byte Modification for Breaking Memory Forensic Analysis*, BlackHat Europe, Mart 2012.

Hauck V. R., Atabakhsh H., Ongvasith P., Gupta H., Chen, H., *Using Coplink to analyze criminal-justice data*, IEEE Computer, Vol. 35 No. 3 pp. 30–37, 2002.

Hay B. Nance K., *Forensics Examination of Volatile System Data Using Virtual Introspection*, SIGOPS Operating Systems Review , Volume 42 Issue 3, ACM, pp. 74–82., 2008.

Hay B., Bishop M., Nance K., *Live Analysis: Progress and Challenges*, IEEE Security and Privacy, vol. 7, pp. 30-37., Mart 2009. Izvor: http://nob. cs.ucdavis.edu/ bishop/papers/2009-ieeesp-2/liveanal.pdf.

Home page The United States Department of Justice, *Reporting Computer related crime.* Izvor: http://www.justice.gov/criminal/cybercrime/ intl.html.

Huebner E., Bem D., Wee K. C., *Data hiding in the NTFS file system*, Digital Investigation 3, Elsevier, October 2006. Izvor: ftp://163.13.201.222/ Prof_ Liang/%E6%95%B8%E4%BD%8D%E9%91%91%E8%AD%98/ Volume%203%20%282006%29/Supplement%201/Issue%204/

Pages%20211-226.pdf.

Ivaniš N., *Digitalna forenzicka istraga u virtuelnom okruženju*, master rad, Univerzitet Singidunum 2011.

Jakobsson M., Ramzan Z., *Crimeware: Understanding New Attacks and Defenses*, Addison Wesley Professional, 2008.

Johnson T. A., *Forensic Computer Crime Investigation*, Taylor & Francis Group, LLC, 2005.

Jones R., *Internet Forensics***,** O'Reilly Media, 2005.

Kanellis P., Kiountouzis E., Kolokotronis N., Martakos D., *Digital Crime and Forensic Science in Cyberspace*, Idea Group Inc, pp. 217-242, 2006.

Kaufman R. J., *Computer Incident Response*, Texas Security Symposium Agenda, San Antonio TX, 2003.

Kaufman R. J., *Intrusion Detection and Incident Response IS 3523 course*,UTSA Spring, 2012.

Keith J. J., Bejtlich R., Curtis W. R., *Real Digital Forensics Computer Security and Incident Response*, Addison-Wesley, 2006.

Keith J. J., *Forensic Analysis of Microsoft Windows Recycle Bin Records,* Foundstone.com, April 2003.

Kent K., Chevalier S., Grance T., Dang H., *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800-86, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930, August 2006.

Kipper G., *Wireless crime and forensic investigation*, Auerbach Publications Taylor & Francis Group, 2007.

Klevinsky T. J., Laliberte S., Gupta A., *Hack I.T.: Security Through Penetration Testing*, Addison Wesley, 2002.

Kopecký K., *Cyber grooming danger of cyberspace*, study, Olomouc, 2010.

Kopecký K., *Stalking a kyberstalking nebezpečné pronásledování*, study Olomouc, 2010. Izvor: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd.

Korać V., "*Digital archaeology in a virtual environment*", Arheologija i

prirodne nauke, br. 8, str. 129-141, Beograd, 2013.

Korać V., *Infrastruktura sa javnim ključevima u funkciji zaštite informacionog toka i elektronskog poslovanja*, Arheologija i prirodne nauke, specijalna izdanja, Centar za nove tehnologije, Beograd, 2010.

Korać V., *Prevencija širenja virusa kroz autorun funkciju operativnog sistema*, Arheologija i prirodne nauke br.4, str. 103-107, Beograd, 2008.

Korać V., *Zaštita usb prenosnog drajva i operativnog sistema od zlonamernog koda tipa autorun.inf*, Zbornik Radova - Forum BISEC 2010, II konferencija o bezbednosti, str. 77-82, Univezitet Metropolitan, Fakultet informacionih tehnologija, Beograd, 2010.

Korać V., *Spam*, Arheologija i prirodne nauke, br.1, Centar za nove tehnologije str. 137-150, Beograd, 2006.

Korać V., *Digitalna forenzika kao arheologija podataka u visokotehnološkom kriminalu*, Monografija, časopis Arheologija i prirodne nauke, specijalna izdanja 6, Centar za nove tehnologije Viminacium, Arheološki institut, Beograd, 2013.

Korać V., *Digital archaeology of volatile data on Linux platform*, Arheologija i prirodne nauke, br. 9, pp. 205-216, Beograd, 2014.

Korać V., Prlja D., Gasmi G., »*High technology criminal and digital forensics*«, u: »*Preventing and Combating Cybercrime*«, The International Conference - Thematic Proceedings, p. 85-100, Accent, Cluj-Napoka, Romania, 2016.

Kornblum J. D., *Exploiting the Rootkit Paradox with Windows Memory Analysis*, International Journal of Digital Evidence Fall 2006, Volume 5, Issue 1, 2006.

Kornblum J. D., *The Linux Kernel and the Forensic Acquisition of Hard Disks with an Odd Number of Sectors*, International Journal of Digital Evidence, Volume 3, Issue 2, 2004.

Kruse II G. W., Heiser G. J., *Computer Forensics Incidend response essentials*, 14th printing, New York: Addison Wesley, March 2010.

Kunz M., Wilson P., *Computer Crime and Computer Fraud - Report to the Montgomery County Criminal Justice Coordinating Commission*, University of Maryland Department of Criminology and Criminal

Justice, USA, 2004.

Lee H., Palmbach T., Miller M., *Henry Lee's Crime Scene Handbook*, San Diego: Academic Press, 2001.

Leschke T. R., "*Cyber Dumpster Diving: $Recycle Bin Forensics for Windows 7 and Windows Vista*", U.S. Department of Defense Cyber Crime Conference, 2010.

Leschke T. R., *Shadow Volume Trash: $Recycle.Bin Forensics for Windows 7 and Windows Vista Shadow Volumes,* U.S. Department of Defense Cyber Crime Institute, 2010.

Ligh M. H., Adair S., Hartstein B., Richard M., *Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code*, Wiley Publishing, Inc., Indianapolis, Indiana, 2011.

Lillard T. V., *Digital forensics for network, Internet, and cloud computing - A forensic evidence guide for moving targets and data*, Elsevier Inc, USA, 2010.

Malin C. H., Casey E., Aquilina J. M., *Malware Forensics - Investigating and Analyzing Malicious Code*, Syngress 2008.

Manzuik S., Gold A., Gatford C., *Network Security Assessment: From Vulnerability to Patch*, Syngress Publishing, Inc., 2007.

Marcella A. J., Greenfield S. R., *Cyber Forensics*, CRC Press LLC, 2002.

Marchany R., *The top 10/20 Internet security vulenrabilities*, Va Tech Computing center, The Sans institute, Covits, 2000. Izvor: http://www.slideshare.net/amiable_indian/the-top-1020-internet-security-vulnerabilities-a-primer.

Marković S., *Digitalna forenzika Linux fajl sistema*, master rad, Univerzitet Univerzitet Singidunum, 2010.

Marshall A. M., *Digital Forensics - Digital Evidence in Criminal Investigation*, JohnWiley & Sons, Ltd 2008.

Matijašević J., Ignjatijević S., *Kompjuterski kriminalitet u pravnoj teoriji, pojam, karakteristike, posledice*, Infoteh-Jahorina Vol. 9, Ref. E-VI-8, pp. 852-856, March 2010.

McAfee, *Defeat Ransomware: Ensure Your Data Is Not Taken Hostage*,

Solution Brief, Intel Corporation or McAfee, Inc., 2016. Izvor: http://www. mcafee.com/ us/resources/solution-briefs/sb-quarterly-threat-q1-2015-2.pdf.

McDougal M., *Windows Forensic Toolchest (WFT)*, 2005. Izvor: http://www.foolmoon.net/security/.

McQuade III S. C., *Encyclopedia of Cybercrime*, Greenwood Publishing Westport, Connecticut, 2009.

McRee R., *Memory Analysis with DumpIt and Volatility*, ISSA Journal, September 2011.

Menz M., Bress S., *The fallacy of software write protection in computer forensic, 2004.* Izvor: http://www.mykeytech.com/SoftwareWriteBlocking2-4.pdf.

Michaud, D. J., *Adventures in Computer Forensics*, Information Security Reading Room, SANS Institute 2001. Izvor: https://www.sans.org/reading-room/ whitepapers/incident/adventures-computer-forensics-638.

Microsoft, *Microsoft Hyper-V*, Izvor: http://www.microsoft.com/en-us/server-cloud/ hyper-v-server/.

Milanović Z., Milanović T., *Digitalna anti-forenzika kao kriminogeno sredstvo zaštite kiber kriminala*, Ziteh - Udruženje sudskih veštaka za informacione tehnologije It veštak, 2010.

Milosavljević M., Grubor G., *Digitalna forenzika računarskog sistema*, Univerzitet Singidunum, Beograd 2009.

Milosavljević M., Grubor G., *Digitalna forenzika*, Univerzitet Singidunum, Beograd, 2008.

Milosavljević M., Grubor G., *Istraga kompjuterskog kriminala - metodološko tehnološke osnove*, Univerzitet Singidunum 2009.

Mohay G., Anderson A., Collie B., Vel O., McKemmish R., *Computer and Intrusion Forensics*, Artech House, Norwood, MA, 2003.

Mrdović S., Huseinović A., Zajko W., *Combining Static and Live Digital Forensic Analysis in Virtual Environment*, Information, Communication and Automation Technologies, ICAT 2009, XXII International Symposium, 2009. Izvor: http://people.etf.unsa.ba/~smrdovic/

publications/ICAT2009-Mrdovic_ Huseinovic_ Zajko.pdf.

Nada Staletić, Predrag Staletić, Aleksandar Simović, *Sigurnost Tor mreže u zaštiti identiteta na Internetu,* INFOTEH-JAHORINA Vol. 13, str 913-917, 2014. Izvor: http://infoteh.etf.unssa.rs.ba/zbornik/2014/radovi/RSS-6/RSS-6-5.pdf.

National Institute of Justice, *Electronic Crime Scene Investigation. A Guide for First Responder,* 2001. Izvor: https://www.ncjrs.gov/pdffiles1/nij/187736.pdf.

National Institute of Standards and Technology, *Secure Hash Standard*, FIPS PUB 180, May 1993.

National Policing Improvement Agency, *Core Skills in Data Recovery & AnalysisCourse Reference Book V2.01*, Bradford, UK, maj 2007.

Nelson B., Phillips A., Enfinger F., Steuart C., *Guide To Computer Forensics And Investigations*, *second edition*, Thomson Course Technology, Boston, 2006.

Nelson B., Phillips A., Enfinger F., Steuart C., *Guide to Computer Forensics and Investigations, third edition,* Thomson Course Technology, Boston, 2008.

Nelson B., Phillips A., Steuart C., *Guide to Computer Forensics and Investigations – fourth edition, Fourth Edition*, Course Technology, Cengage learning, Boston, 2010.

Nestler V., Conklin W. A., White G., Hirsch M., *Principles of Computer Security: CompTIA Security and Beyond Lab Manual, Second Edition*, The McGraw-Hill Companies 2011.

Newsham T., Palmer C., Stamos A., *Breaking Forensics Software: Weaknesses in Critical Evidence Collection*, BlackHat Conference 2007. Izvor: http://www.defcon. org/images/defcon-15/dc15-presentations/Palmer_and_Stamos/Whitepaper/dc-15-palmer_stamos-WP.pdf.

Nikačević V., *Korporacijska istraga kompjuterskog kriminala sa implementacijom sigurnosne politike*, Ziteh - Udruženje sudskih veštaka za informacione tehnologije It veštak, 2010.

Nikolić K. L., *Suzbijanje visokotehnološkog kriminala*, Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, Beograd 2010.

Nolan R., Baker M., Branson J., Hammerstein J., Rush K., Waits C., Schweinsberg E., *First Responders Guide to Computer Forensics: Advanced Topics*, Software Engeneering Institute Carnegie Mellon, 2005.

Nolan R., Sullivan C. O., Branson J., Waits C., *First Responders Guide to Computer Forensics*, CERT Training and Education, Carnegie Mellon University, March 2005

One A., *Smashing the Stack for Fun and Profit, Phrack,* Volume 7, Issue 49, 1996.

Pogue C., Altheide C., Haverkos T., *UNIX and Linux Forensic Analysis DVD Toolkit*, Syngress publishing Inc., 2008.

Popek J. G., Goldberg P. R., *Formal requirements for virtualizable third generation architectures,* Communications of the ACM 17 (7), pp. 412–421. 1974.

Prlja D., Reljanović M., *Pravna informatika*, Pravni fakultet Univerziteta Union, Beograd, 2014.

Prlja D., Reljanović M., *Visokotehnološki kriminal - uporedna iskustva*, Strani pravni život, br. 3/2009, pp. 161-184., 2009.

Prlja D., *Sajberkriminal*, predavanje održano na Pravnom fakultetu Univerziteta u Beogradu, Izvor: http//www.prlja.info/sk2008.pdf.

Prlja D., Savović M., *E-mail kao dokazno sredstvo u uporednom pravu*, Strani pravni život, br. 2/2009, pp. 71-85., 2009.

Prlja D., Korać V., Diligenski A., »*Maloletnici i sajber kriminal*«, u: »*Maloletnici kao učinioci i žrtve krivičnih dela i prekršaja*«, Institut za kriminološka i sociološka istraživanja, str. 349-365, Beograd, 2015.

Prosise C. Mandia K, *Incident response and computer forensics*, second edition, The McGraw-Hill Companies 2003.

Steven J. Murdoch, George Danezis, *Low-Cost Traffic Analysis of Tor*, IEEE Symposium on Security and Privacy 2005, Oakland, California, USA, May 8 – 11, 2005. Izvor: http://sec.cs.ucl.ac.uk/users/smurdoch/papers/oakland05torta.pdf.

The hacker News, *Tor anonymizing network compromised by French researchers*, Izvor: http://thehackernews.com/2011/10/tor-anonymizing-network-compromised-by.html.

8. BIOGRAFIJE AUTORA

VANJA KORAĆ

Vanja Korać rođen je 1976. godine u Beogradu. Osnovnu i srednju školu završio je u Beogradu. Visoko obrazovanje stekao je na Fakultetu za poslovnu informatiku Univerziteta "Singidunum" 2005. godine u Beogradu, na smeru programiranje i projektovanje, gde dobija zvanje diplomirani inženjer informatike. Nakon uspešno završenih specijalističkih studija na Fakultetu za poslovnu informatiku Univerziteta "Singidunum" u Beogradu, smer bezbednost informacionih sistema i elektronskog poslovanja 2006. godine stekao stekao je diplomu specijaliste za bezbednost informacionih sistema i elektronskog poslovanja, sa zvanjem specijalista za bezbednost elektronskih komunikacija i elektronskog poslovanja.

Magistarske studije na fakultetu za poslovnu informatiku Univerziteta "Singidunum" završio je 2008. godine odbranom magistarskog rada sa temom "*Infrastruktura sa javnim ključevima u funkciji zaštite informacionog toka i elektronskog poslovanja*", gde dobija zvanje magistra informatike. 2011. godine odobrena mu je tema za izradu doktorske disertacije od strane Centra za multidisciplinarne studije Univerziteta u Beogradu pod naslovom : "*Digitalna forenzika u funkciji zaštite informacionog sistema baziranog na Linux i Windows platformama*". 2014. godine odbranio je doktorski rad pod nazivom "*Digitalna forenzika u funkciji zaštite informacionog sistema baziranog na Linux i Windows platformama*" u Rektoratu Beogradskog Univerziteta.

Od 2007-2011, radio je kao IT saradnik u školi od posebnog nacionalnog značaja - Matematičkoj gimnaziji kao rukovodilac računarskog centra,

gde je rukovodio projktom kompletnog umrežavanja škole prilikom njene rekonstrukcije.

Takođe, kao saradnik Arheološkog instituta SANU zadužen je za administriranje mreže i sistema na lokalitetu Viminacium. Bio je angažovan na projektima :

- 2008. FP6 projekat: ADHOCSYS ("*Wireless Ad-Hoc Broadband Monitoring System*");

- 2008-2010 Projekat 144018 pri Ministarstvu za nauku Republike Srbije ("*Napredne metode u kriptologiji i procesiranju informacija*").

Zaposlen je u Matematičkom institutu SANU kao naučni saradnik. Trenutno je angažovan na projektu Ministarstva za nauku Republike Srbije:

- 2010- III 47018 - IRS - *Viminacium, rimski grad i legijski vojni logor - istraživanje materijalne i duhovne kulture, stanovništva, primenom najsavremenijih tehnologija daljinske detekcije, geofizike, GIS-a, digitalizacije i 3D vizuelizacije*.

Od 2015. godine angažovan je na projektu saradnje između MISANU i Telekom Srbije: Razvoj i implementacija pravila za IT bezbednost i zaštitu.

Digitalno forenzičku obuku Information and Communication Technology Forensics Investigation je završio na Septia Academy 2016. godine u Beogradu. Objavljene knjige i radovi su iz oblasti kompjuterskog kriminala, zaštite računarskih sistema, digitalne forenzike, elektronske uprave.

DRAGAN PRLJA

Dragan Prlja rođen je u Ostojićevu 1959. godine, a diplomirao je, magistrirao i doktorirao na Pravnom fakultetu Univerziteta u Beogradu na međunarodnopravnom smeru.

Zaposlen je kao naučni saradnik u Institutu za uporedno pravu u Beogradu.

Predavač je na više fakulteta na predmetima vezanim za upotrebu informacionih tehnologija u oblasti prava.

Objavio je više od 25 knjiga i preko 100 naučnih radova iz oblasti kompjuterskog kriminala, elektronske trgovine, elektronske uprave, zaštite podataka, i pravne informatike.

ANDREJ DILIGENSKI

Andrej Diligenski rođen je u Beogradu 1984. godine, gde je diplomirao na Pravnom fakultetu Univerziteta u Beogradu na međunarodnopravnom smeru. Specijalističke master studije je završio u Beču u oblasti informatičkog prava i prava informacionih tehnologija na temu "Implementacija elektronske uprave - poređenje Austrije i Srbije" („Umsetzung von E-Government" - Ein Vergleich zwischen Österreich und Serbien). Trenutno radi na izradi doktorske disertacije na Pravnom fakultetu u Beču na temu "Zaštita podataka u telekomunikacionom pravu Crne Gore" (Datenschutz im Telekommunikationsrecht Montenegros). Pored toga je i sertifikovan menadžer za informacionu sigurnost (information security manager) po svetskom standardu ISO 27001 od strane austrijskog sertifikacionog tela CIS. Sertifikovan je i od austrijskog sertifikacionog tela ARGE DATEN kao poverenik za zaštitu podataka.

Zaposlen je kao menadžer upravljanja informacijama u osiguranju Zürich u Beču. Radio je i kao poverenik za zaštitu podataka firme Simacek Facility Management Group GmbH u Beču. Saradnik je na više instituta, između ostalih instituta Evropski centar za elektronsku trgovinu i internet pravo, Ludwig Boltzmann Institut za ljudska prava u Beču. Spoljni saradnik je i Instituta za uporedno pravo u Beogradu. Učestvovao na projektu "EU-Twinning Projekt- Implementation of personal data protection strategy in Montenegro". Objavio je više naučnih radova i blogova između ostalih "Pravni aspekti neutralnosti internet mreže", "Fejsbuk i zaštita podataka u EU", "Zaštita podataka kod mergers & acquisitions", "Iznajmljivanje stana i zaštita podataka", "Uvođenje poverenika za zaštitu podataka unutar firme".

CIP - Каталогизација у публикацији - Народна библиотека Србије, Београд

343.983:004

КОРАЋ, Вања, 1976-
Digitalna forenzika / Vanja Korać, Dragan Prlja, Andrej Diligenski. -
Beograd : Centar za nove tehologije Viminacium : Arheološki institut :
Institut za uporedno pravo, 2016 (Beograd : Digital Art Company). - 418
str. : ilustr. ; 23 cm

Slike autora. - Tiraž 300. - Rečnik pojmova i izraza: str. 391-399. -
Biografije autora: str. 415-418. - Napomene i bibliografske reference uz
tekst. - Bibliografija: str. 401-413.

ISBN 978-86-87271-34-0 (CNTV)

1. Прља, Драган, 1959- [аутор] 2. Дилигенски, Андреј, 1984- [аутор]
а) Вештачење - Рачунарски системи
COBISS.SR-ID 226520844