ORGANIZOVANI KRIMINAL I DIGITALNA FORENZIKA

Vanja Korać*
Andrej Diligenski*
Dragan Prlja*

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. 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 i koji daju odlučujući odgovor na krivična dela organizovanog kriminala počinjena u sajber prostoru.

KLJUČNE REČI: pravo, informatika, bezbednost, organizovani kriminal, visokotehnološki kriminal, digitalna forenzika, digitalni dokaz, istraga

1. UVOD

"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".[1]

Organizovani kriminal predstavlja veliku pretnju za svako društvo. Podrazumeva vršenje krivičnih dela od strane organizovane kriminalne grupe ili njenih pripadnika. Nemoguće je precizno izračunati finansijsku štetu koju nanosi organizovani kriminal, ali je sasvim sigurno da je ona velikih razmera.

Organizovane kriminalne grupe za krijumčarenje narkotika, falsifikovanje novca, trgovinu ljudima, pranja novca sve više koriste mogućnosti novih tehnologija za ostvarivanje međusobne komunikacije. Predviđa se da će budući period

* Naučni saradnik, Matematički institut.
* Spoljni saradnik Instituta za uporedno pravo.
* Naučni saradnik Instituta za uporedno pravo, email: dprlja@yahoo.com
[1] 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.

visokotehnološkog kriminala karakterisati veće uključivanje organizovanog kriminala u korišćenje računara prilikom distribucije opojnih droga, zloupotrebe dece, zloupotrebe platnih kartica, u prostituciji, trgovini ljudskim organima. U elektronskom transferu novca otvaraju se nove mogućnosti za brzo i pouzdano "pranje novca". Očekuje se i veće uključivanje maloletnih lica u izvršenju težih krivičnih dela, krađa identiteta i zloupotreba u elektronskoj trgovini.[2]

S obzirom na sve veću ulogu novih informaciono-komunikacionih tehnologija (IKT) u svim oblicima organizovanog kriminala, neophodno je cilju ostvarivanja efikasne borbe u suzbijanju ove vrste kriminala razviti i ovladati metodama digitalne forenzike. Kada je u pitanju visokotehnološki kriminal digitalna forenzika se već pokazala, kao jedan od najznačajnih faktora u procesu otkrivanja istine o nedozvoljenim aktivnostima. Digitalna forenzika deluje i preventivno, pošto njeni rezultati pokazuju kako se neka nedozvoljena aktivnost desila, gde su bili propusti i na koji način su se oni desili. Samim tim moguće je predupredi ti iste ili slične nedozvoljene aktivnosti. Primenom digitalne forenzike i implementacijom saznanja ove nauke u mehanizme zaštite IKT, digitalna forenzika postaje bitan elemenat proaktivne zaštite od svih oblika kriminala.

Trka između zakona i njegove primene sa jedne strane i novih tehnologija i njenih primena u svrhu vršenja organizovanog kriminala na drugoj strani i dalje se nastavlja. Prirodna tendencija prava ka konzervativizmu često dolazi u sukob sa životom, s obzirom na njegovu dinamičnost i na sofistirane metode kriminalaca. Brzina takvih promena naročito se ogleda u informatičkoj nauci i tehnologiji, koje su predmet stalnih inovacija i promena.

2. ORGANIZOVANI KRIMINAL I VISOKOTEHNOLOŠKI KRIMINAL

2.1. Oblici organizovanog kriminala i visokotehnološki kriminal

Organizovani kriminal se danas najčešće ispoljava u mnogobrojnim oblicima i sa različitim objektima napada.

Napadi na firme kroz ucenu, krađu (pljačkanje banaka) ili prevare kao što su otimanje teretnih vozila, stečajne prevare, prevare sa osiguranjem ili akcijama.

Napadi na državu i državne institucije kroz nameštanje javnih projekata, falsifikovanje novca, krijumčarenje i proizvodnja neoporezivanog alkohola ili cigareta, krijumčarenje radnika, migranata. Ovim oblikom kriminala bave se i grupe koje potražuju korumpirane javne zvaničnike na visokim položajima, kako bi njihove aktivnosti protekle bez problema ili radi dobijanja upozorenja i informacija o istragama i gonjenjima.

Napadi na pojedince ostvaruju se putem krađa automobila, provala, krađa nakita, zelenašenja sa vrlo visokim kamatama, kompjuterskog hakovanja, prevara kreditnim karticama, ekonomske špijunaže, pronevere, krađe identiteta, itd.

Organizovani kriminal se ispoljava takođe *bez obzira na objekat napada* u vidu atentata, ucena, ilegalnog kockanja, kršenja autorskih prava, prostitucije, trgovine narkoticima, trgovine oružjem i krijumčarenja vojne opreme, krijumčarenja benzina,

[2] *Nacionalna strategija z aborbu protiv organizovanog kriminala*, Sl. Glasnik RS, br. 23/2009.

trgovine organima, naručenih ubistva, falsifikovanja dokumenata, pranja novca, nameštanja sportskih utakmica, krijumčarenja ljudi i trgovina ljudima.[3]

Navedeni objekti napada organizovanog kriminala se manifestuju *u različitim sredinama*. U novije vreme se oblici organizovanog kriminala manifestuju *u sajber svetu i uz pomoć računara kao sredstva izvršenja krivičnih dela*. Razvojem IKT i računarskih mreža, već sedamdesetih godina prošlog veka dolazi do pojave visokotehnološkog kriminala.

Visokotehnološki kriminal ili sajber 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 *Konvenciji o sajber kriminalu Saveta Evrope* računarski sistem je definisan kao svaki uređaj ili grupa međusobno povezanih uređaja kojima se vrši automatizivana obrada podataka. Iz toga proizlazi da bez istih i bez računarskih mreža nema ovog oblika kriminala.[4] *Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala* Republike Srbije definiše visokotehnološki kriminal kao: "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".[5]

2.2. Organizovani kriminal i visokotehnološki kriminal u srpskom pravu

Pod *organizovanom kriminalnom* grupom *Krivični zakonik Republike Srbije* podrazumeva grupu od tri ili više lica, koja postoji određeno vreme i deluje sporazumno u cilju vršenja jednog ili više krivičnih dela za koja je propisana kazna zatvora od četiri godine ili teža kazna, radi sticanja, posredno ili neposredno, finansijske ili druge koristi.[6]

Pojavni oblici organizovanog kriminala zastupljeni u Republici Srbiji, koji su inkriminisani Krivičnim zakonikom su: trgovina narkoticima, iznude, otmice, prinude, teške krađe, razbojničke krađe, razbojništva, trgovina ljudima, nedozvoljen prelaz državne granice i krijumčarenje ljudi, trgovina maloletnim licima radi usvojenja, udruživanje radi protivustavne delatnosti (u ovu grupu krivičnih dela spadaju napad na ustavno uređenje, ugrožavanje teritorijalne celine, ugrožavanje nezavisnosti, priznavanje kapitulacije ili okupacije, pozivanje na nasilnu promenu ustavnog uređenja, ubistvo predstavnika najviših državnih organa, sabotaža, diverzija), udruživanje radi vršenja krivičnih dela (organizovanje grupe koja ima za cilj vršenje krivičnih dela za koje se može izreći kazna zatvora od tri godine ili teža kazna), finansiranje terorizma, organizovanje i podsticanje na izvršenje genocida i ratnih zločina.[7]

Zakonom o organizaciji i nadležnosti državnih organa u suzbijanju organizovanog kriminala, korupcije i drugih posebno teških krivičnih dela obrazovano je posebno tužilaštvo za suzbijanje ove vrste kriminaliteta, kao i sudovi koji će odlučivati u

---

[3] Organizovani kriminal, *Wikipedia*, https://sr.wikipedia.org/wiki/Организовани_криминал, 28.06.2016.
[4] Council of Europe treaties, Details of Treaty No.185, *Convention on Cybercrime*, http://conventions.coe.int/treaty/en/treaties/html/185.htm, 01.07.2016.
[5] *Zakon o organizaciji i nadrežnosti državnih organa za borbu protiv visokotehnološkog kriminaliteta*, Sl. Glasnik RS, br. 61/2005, 23. 10. 2011.
[6] *Krivični Zakonik*, Sl. glasnik RS, br. 85/2005, 88/2005, 111/2009, 121/2012, 104/2013, i 108/2014., član 112 tačka 35.
[7] *Ibidem.*

sporovima vezanim za predmete organizovanog kriminala. Formirana jei posebna služba za suzbijanje organizovanog kriminala u okviru policije, radi otkrivanja i krivičnog gonjenja učinioca krivičnog dela organizovanog kriminala.[8] Ovaj zakon se primenjuje za:

1) krivična dela organizovanog kriminala,

2) krivična dela protiv ustavnog uređenja i bezbednosti Republike Srbije (čl. 310. do 312. Krivičnog zakonika),

3) krivična dela protiv službene dužnosti (čl. 359, 366, 367. i 368. Krivičnog zakonika), kada je okrivljeni, odnosno lice kojem se daje mito, službeno ili odgovorno lice koje vrši javnu funkciju na osnovu izbora, imenovanja ili postavljenja od strane Narodne skupštine, Vlade, Visokog saveta sudstva ili Državnog veća tužilaca,

4) krivično delo zloupotreba službenog položaja (član 359. stav 3. Krivičnog zakonika), kada vrednost pribavljene imovinske koristi prelazi iznos od 200.000.000 dinara

5) krivično delo međunarodni terorizam i krivično delo finansiranje terorizma (čl. 391. i 393. Krivičnog zakonika),

6) krivično delo pranja novca (član 231. Krivičnog zakonika), ako imovina koja je predmet pranja novca potiče iz krivičnih dela iz tač. 1), 3), 4) i 5) ovog člana,

7) krivična dela protiv državnih organa (član 322. st. 3. i 4. i član 323. st. 3. i 4. Krivičnog zakonika) i krivična dela protiv pravosuđa (čl. 333. i 335, član 336. st. 1, 2. i 4. i čl. 336b, 337. i 339. Krivičnog zakonika), ako su izvršena u vezi sa krivičnim delima iz tač. 1) do 6) ovog člana.[9]

Kompjuterska krivična dela regulisana su u srpskom pravu Krivičnim zakonikom u Glavi 27 kao "Krivična dela protiv računarskih podataka" (čl. 298–304a).[10]

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 visokotehnološkog kriminala.[11][12]

Kao što se može uočiti, krivična dela visokotehnološkog kriminala i elementi saradnje sa Tužilaštvom za visokotehnološki kriminal nisu predviđeni *Zakonomo organizaciji inadležnosti državnih organa u suzbijanju organizovanog kriminala, korupcije i drugih posebno teških krivičnih dela*. Stoga je neophodna saradnja između dve specijalne jedinice odeljenja policije i između tužilaštva, radi otkrivanja, gonjenja i na kraju suđenja za krivčna dela organizovanog kriminala počinjena pre svega na internetu. Potrebno je regulisati zakonom i sudsku nadležnost po pitanju izvršenja krivičnih dela organizovanog kriminala na internetu, kako bi se izbegao potencijalni sukob nadležnosti.

---

[8] *Zakon o organizaciji i nadležnosti državnih organa u suzbijanju organizovanog kriminala, korupcije i drugih posebno teških krivičnih*, ("Sl. glasnik RS", br. 42/2002, 27/2003, 39/2003, 67/2003, 29/2004, 58/2004 - dr. zakon, 45/2005, 61/2005 i 72/2009), članovi 2, 4 i 10.

[9] *Ibidem.*

[10] *Krivični Zakonik*, Sl. glasnik RS, br. 85/2005, 88/2005, 111/2009, 121/2012, 104/2013, i 108/2014.

[11] 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 gonjenjemdela VTK bave dva zamenika višeg javnog tužioca u Beogradu, koji su specijalizovani za tu oblast.

[12] *Zakon o organizacijii nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala*, Sl. glasnik RS, br. 61/05.

Zbog specifičnog mesta izvršenja krivičnog dela, potrebno je već uspostavljene metode istrage visokotehnološkog kriminala primeniti i krivična dela organizovanog kriminala. *Glavni cilj istrage visokotehnološkog 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 (zloupotrebe IKT sistema) obezbeđuje metodologija istrage klasičnog kriminala, sa specifičnostima istrage osetljivih, lako promenljivih i po svojoj prirodi posrednih digitalnih dokaza.[13] U otkrivanju i sankcionisanju organizovanog kriminala u sajber prostoru, *digitalna forenzika* je nezamenljiv alat.

3. DIGITALNA FORENZIKA KAO NAUČNA DISCIPLINA

Digitalna forenzika kao relativno nova naučna disciplina 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 ili kada postoji potreba za upravljanjem računarskim incidentom, odgovore će nam dati digitalna forenzika.[14]

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.[15] 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.[16]

Kada je reč o elementima visokotehnološkog kriminala i organizovanog 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.

Tradicionalna forenzika nije imala adekvatan odgovor na sve prisutniju vrstu kriminala vezanu za računarske sisteme, odnosno kriminala koji se odvija na globalnoj mreži internetu. Digitalna forenzika je naučna disciplina koja može ponuditi relevantan dokaz tj. digitalni dokaz u ogovoru na ove vrste krivičnih dela. Razvoj IKT postavlja velike izazove pred digitalne forenzičare, koji moraju 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

[13] Milan Milosavljević, Gojko Grubor, *Istraga kompjuterskog kriminala - metodološko tehnološke osnove*, Beograd, Singidunum 2009. str. 4.
[14] Aaron P., Cowen D., Davis. C., *Hacking Exposed Computer Forensics*, Second Edition, The Mcgraw-Hill Companies, 2010.
[15] Vanja Korać, Dragan Prlja, i Gordana Gasmi, *High Tecnology Criminal and Digital Forensics*, in: Preventing and Combating Cybercrime, Cluj-Napoca, Accent, 2016, str. 85.
[16] Allen B., *Collecting DigitalEvidence 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.

discipline, koja zajedno sa paralelnim razvojem drugih nauka, primenjuje nove metode koje utiču na brzinu i jednostavnost prikupljanja dokaza. Upravo takva složenost problema na koju forenzičari nailaze, uslovili su i specijalizovanje stručnjaka za različite oblasti.

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.

4. 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).[17] *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, 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.).

Principi i standardne operativne procedure digitalne forenzičke istrage gotovo iste kako u zvaničnoj (državnoj) 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.[18]

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. Od značaja je utvrditi*informacije o cilju napada* i eventualno *postojanje uzročno-posledične veze* (direktne ili indirektne) sa ostalim kumulativno počinjenim krivičnim delima.Identifikacijom izvršenja nedozvoljene aktivnosti od strane nadležnih organa, isti iniciraju istragu u pretkrivičnom postupku.

U okviru krivičnog postupka 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, 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

[17] Vanja Korać, Dragan Prlja, i Gordana Gasmi, *High Tecnology Criminal and Digital Forensics*, in: Preventing and Combating Cybercrime, Cluj-Napoca, Accent, 2016, str. 87.
[18] Grubor G., Gotić A., *Korporativna aktivna digitalna forenzička istraga primenom Backtrack – a*, 10. Međunarodni naučni skup Sinergija 2012. Univerzitet Sinergija, 2012.

svih dokaznih postupaka je da se utvrdi činjenično stanje stvari koje odgovara konkretnom slučaju.[19]

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 da dokažu vezu između izvršioca zločina sa samim zločinom. Primeri fizičkih dokaza su: računar, DVD, hard disk, mobilni telefon;

- *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 (npr. log fajlovi), 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;[20]

- *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.

4.1. Digitalna forenzika računarskog sistema

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.[21]

Najveći deo računarske forenzike odnosi se na forenziku računarskih sistema. 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*.[22] 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. Tako je moguće dovesti određene dokaze u vezu sa izvršiocem.

Digitalna forenzika računarskog sistema obuhvata naučno ispitivanje i analizu podataka sa hard diskova, fajl sistema i prostora za skladištenje podataka unutar

[19] Dragan Prlja, Miodrag Savović, *E-mail kao dokazno sredstvo u uporednom pravu*, Strani pravni život, br. 2/2009, str. 71-74.
[20] 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.
[21] Albert J. Marcella, Robert S. Greenfield, *Cyber Forensics*, CRC Press LLC, 2002, str. 317.
[22] Bem D., Huebner E., *ComputerForensic Analysis in a Virtual Environment*, International Journal of Digital Evidence Fall 2007, Volume 6, Issue 2, 2007.

računarskog sistema, da bi se ti podaci mogli koristiti kao neoborivi i čvrsti dokazi pred sudom.[23][24]

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.

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 incidentnog događaja podrazumeva korišćenje digitalno-forenzičkih tehnika i alata za oporavak izgubljenjih podataka (npr. 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.

4.2. Prikupljanje digitalnih dokaza u okviru digitalne forenzičke istrage

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.[25]

Dokaz je ono što razdvaja hipotezu od neosnovane tvrdnje.[26]Dokazom se može potvrditi ili oboriti hipoteza. Stoga je od izuzetne važnosti pitanje njegovog integriteta,

[23] 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.
[24] Alghafli K. A., Jones A., Martin T. A., *Forensic Analysis of the Windows 7 Registry*, Khalifa University of Science, Technology and Research, 2010.
[25] Council of Europe, Recommendation No. R (95) 13, http://www.justice.gov /criminal/cybercrime/ crycoe.htm, 22.06.2016.

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 način, odnosno fizičkim predmetima.[27][28]

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.[29]

Pod pojmom digitalnih dokaza prema definiciji IOCE podrazumeva se 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.[30] [31]

Postandardu SWGDE/IOCE[32] [33] dokazi se mogu klasifikovati u sledeće kategorije:[34]

1. *digitalni dokaz*- informacija od značaja za krivični postupak koja se nalazi ili prenosi u digitalnom obliku;
2. *fizički predmeti kao dokaz*- fizički medijum koji skladišti ili prenosi digitalnu informaciju;
3. *digitalni podaci*- informacije od značaja za krivični postupak koje su povezane sa fizičkim predmetom.[35]

Od značaja za forenzičku analize je razgraničiti značenje pojedinih *pojmova* koji se često koriste kao sinonimi.

1. *Originalni digitalni dokaz*je fizički predmet i/ili podatak sadržan u tom predmetu u vreme zaplene (akvizicije) 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.

---

[26] Manzuik S., Gold A., Gatford C., *Network Security Assessment: From Vulnerability to Patch*, Syngress Publishing, Inc., 2007.
[27] IACIS – International Association of Computer Specialist
[28] Aycock J., *Computer Viruses and Malware* , Springer , Canada, 2006.
[29] Vanja Korać, Dragan Prlja, i Gordana Gasmi, *High Tecnology Criminal and Digital Forensics*, in: Preventing and Combating Cybercrime, Cluj-Napoca, Accent, 2016, str. 93.
[30] 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.
[31] Kornblum J. D., *Exploiting the Rootkit Paradox with Windows Memory Analysis*, International Journal of Digital Evidence Fall 2006, Volume 5, Issue 1, 2006.
[32] Scientific Working Group on Digital Evidence (SWGDE), http://www.swgde.org/, 03.01.2016.
[33] International Organization on Digital Evidence (IOCE), http://www.ioce.org/core.php?ID=1, 03.01.2016.
[34] 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.
[35] Michael Cross, S*cene of the Cybercrime*, Second Edition, Syngress, 2008, str. 628.

2. *Duplikat digitalnog dokaza* je verna digitalna reprodukcija svih objekata podataka sadržanih u originalnom fizičkom predmetu (HDu, CDu itd.).
3. *Kopija digitalnog dokaza* je verna reprodukcija informacija koje su sadržane na originalnom fizičkom predmetu, nezavisno od originalnog fizičkog predmeta.[36]
4. *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, fajlovi zaštićeni šifrom;[37] fajlovi zaštićeni enkripcijom, skriveni fajlovi, kompresovani fajlovi, tabelarni fajlovi, fajlovi baza podataka, kalendar, multimedijski fajlovi (audio, video, grafički fajlovi), adresar, fajlovi elektronske pošte.

O bilo kom tipu visokotehnološkog kriminala da je reč moraju se pronaći*tri tipa dokaza*: vremenski dokazi (pomaže u otkrivanju vremenskih dešavanja), relacioni dokazi (podrazumevaju elemente nedozvoljenih aktivnosti, njihov odnos i pozicije) i funkcionalni dokazi (pružaju uvid u to šta je moguće).

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 bezbednosti ili korporativnim organima ukoliko se incidentna radnja desila u njenim okvirima.

Digitalni dokaz kao element istrage je mnogo ranjiviji od fizičkog, pa je veštom napadaču lakše da ga ukloni. 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.[38] *Digitalni dokazi* su apstraktni i kao takvi mogu se lako izmanipulisati u smislu izmene ili njihovog uklanjanja.

Kada digitalni forenzičar preuzme *ispitivanje digitalnog dokaza*, prave se digitalne kopije za dalju analizu. Praksa je pokazala da je najbolje napraviti četiri digitalne kopije hard drajva pri čemu se na jednu od njih primenjije heširanje sa MD5 ili SHA algoritmom da bi se sačuvao integritet (nepromenjivost) digitalnog dokaza. Pritom se jedna kopija izdvaja i povezuje na forenzički računar da bi se nad njom vršila analiza i ispitivanje. Druge dve kopije služe kao rezervne kopije (backup) za bilo koji nepredviđeni slučaj, a može poslužiti i u analizi pod virtuelnim okruženjem.

Pravila prikupljanja digitalnih dokaza, koja su se kroz praksu pokazala kao vrlo korisna: digitalni forenzičar mora da svede mogućnost ispitivanja originalnog dokaza

---

[36] 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/, 01.07.2016.

[37] 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/, 22.07.2016.

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

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.

Da bi digitalni dokaz bio prihvaćen od strane suda treba da bude:

1. *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;
2. *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;
3. *Kompletan* - u smislu da dokaz treba da prikaže ceo slučaj sa svim 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;
4. *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;
5. *Verodostojan i razumljiv* - za sud i stranke u postupku. Nema svrhe pred sud iznositi slika stanja memorije u računaru ("memory dump"), s obzirom da sud nema obavezu da poseduje takva stručna znanja pa samim tim neće razumeti šta to znači.[39][40]

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. 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.

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

[40] Beek C., *Virtual Forensics*, TenICT proffesionals, 2010, http://securitybananas.com/wp-content/uploads/2010/04/Virtual-Forensics_BlackHatEurope2010_CB.pdf, 11.07.2016.

4.3. Upotreba forenzičkih alata u okviru digitalne forenzičke istrage

Digitalna forenzička istraga podrazumeva *upotrebu različitih forenzičkih alata i tehnika*, odnosno njihovu primenu u toku istrage. Alati se koriste se 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 nalaze primenu pri rekonstrukciji nedozvoljene radnje ili otkrivanju tragova osumnjičenog na računaru.

Izuzetno je bitno da digitalni dokazi sa osumnjičene mašine budu dobijeni ili prikupljeni *forenzičkim alatima koji su prihvatljivi pred sudom*. Isto 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 su utvrđeni merodavni forenzički alati *AccessData FTK Imager* i *EnCase*. Ovo su forenzički alati testirani u NIST-ovoj laboratoriji i prvi priznati u svetu od pravosudnih sistema na Zapadu.[41] U ostalim zemljamakoriste se i drugi alati kao što su *Ilook-IX*[42] (FBI,[43] SAD), *X-Way Forensic*[44] (NPIA,[45] Engleska), *Paraben*[46] (BKA,[47] Nemačka), kao i 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 varirajutipovi 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.

[41] The National Institute of Standards and Technology (NIST), http://www.nist.gov/index.html, 30.04.2016.
[42] Perlustro, http://www.perlustro.com/, 30.04.2016.
[43] Federal Bureau of Investigation, http://www.fbi.gov/, 30.04.2016.
[44] X-Ways Forensics: *Integrated Computer Forensics Software*, http://www.x-ways.net/forensics/, 30.04.2016.
[45] National Policing Improvement Agency, http://www.npia.police.uk/, 30.04.2016.
[46] Paraben Corporation, http://www.paraben.com/, 30.04.2016.
[47] BKA odnosno , Federal Criminal Police Office, http://www.bka.de/, 30.04.2016.

4.4. Specijalizacija i sertifikacija digitalnih forenzičkih procesa i forenzičara

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 se 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)[48] je 2002. godine objavila vodiče za trening "Najbolje prakse računarske forenzike".[49] Američko udruženje direktora laboratorije za zločine ASCLD je predložilo zahteve za ljude koji pregledaju digitalne dokaze u forenzičkim laboratorijama. 2005. godine je objavljen *ISO 17025 standard* pod nazivom "Opšti zahtevi za kompetentnost laboratorija za ispitivanje i eteloniranje laboratorija", u kome se spominje pregled digitalnih dokaza u kontekstu akreditovane discipline pod internacionalnim standardom (ISO 17025; ENFSI 2003).

Razvoj tehničkih standarda iz ove oblasti je izazvao potrebu utvrđivanja standarda u samoj praksi namenjenih pojedincima. S*ertifikacija personala*, koji pregladaju digitalne dokaze imaju sve potrebne veštine da obavljaju svoj posao kompetentno i da prate ispravne procedure, postala je neophodna.

Postoji više nivoa sertifikacija I treninga prema pomenutim standardima:

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.[50]

5. ZAKLJUČAK

Sajber prostor se nažalost zloupotrebljava u svrhu vršenja organizovanog kriminala. 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 digitalna forenzika kao naučna disciplina koja daje precizne odgovore na pitanja koja se postavljaju. Ova naučna disciplina može poslužiti ne samo kaosredstvo prevencije i efikasne borbe u suzbijanju organizovanog kriminala već i u postupku preventivne zaštite računarskih mreža i sistema. Jedan od načina da se izbegnu tragične posledice organizovanog kriminala je

[48] Scientific Working Group for Digital Evidence, *Best practices for Computer Forensics*.
[49] Frank Adelstein, *Live forensics: Diagnosing your system without killing it first*, Communications of the ACM, 49(2), 2006, str. 63–66.
[50] 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.

sticanje novih znanja i ospobljavanje kadrova za što efikasnije prikupljanje digitalnih dokaza i njihovo prezentovanje u sudskim postupcima.

Da bi se zaustavilo moguće širenje visokotehnološkog kriminala i organizovanog kriminala u Srbiji neophodno je uspostaviti multidisciplinarne timove za istragu, koji se sastoje od digitalnog forenzičara, pripadnika organa unutrašnjih poslova i tužilaštva. Potrebno je odrediti jasnu sudsku nadležnost i proširiti inkriminaciju krivičnih dela organizovanog kriminala, koji za mesto izvršenja krivičnog dela imaju sajber prostor.

Moto svakog dobrog inžinjeringa bezbednosti je: *"Bezbednost nije proizvod već proces"* Bruce Schneier.[51]

ORGANIZED CRIMINAL AND DIGITAL FORENSICS

Digital forensic investigation is the process, which by using scientific methods and technologies, develops and tests theories through hypotheses, analyzing digital devices, which are relevant evidence in court proceedings. The aim of such an investigation is to determine the truth about unlawful activity and all the circumstances relating to the perpetrator and manner of execution of criminal act or minor offense. Digital evidence in this case is digital object that contains reliable information to support or refute the hypothesis and give the decisive response to organized crime offenses committed in cyberspace.

KEY WORDS: law, informatics,security,organized crime,high technology criminal, digital forensics, digital evidence,investigation.

[51]Bruce Schneier, "Security Is Not a Product; It's a Process", *Schneier on Security*, https://www.schneier.com/crypto-gram/archives/1999/1215.html, 29.07.2016.