Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

METODE OTKRIVANJA SAJBER KRIMINALA PUTEM DIGITALNE FORENZIKE

THE METHODS OF DETECTION CYBER CRIME INTO DIGITAL FORENSICS

Pregledni naučni rad

Mr. sci. Elmedin Ahmić[395]
Prof. dr. Almin Dautbegović[396]
Prof. dr. Nedžad Korajlić[397]

Sažetak

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Razvojem informaciono-komunikacionih tehnologija stvara se sve više mogućnosti sajber-kriminalcima da na lagan način "upadnu" u sistem pojedinca ili kompanija i da načine štetu. U radu će biti opisan razvoj sajber kriminala, oblici zloupotreba i prijevara, te tehnike koje se koriste za otkrivanje počinilaca. Izvlačenje ovih podataka, njihovo tumačenje i prognoziranje, te jednostavno prezentiranje pred sudom, predstavljaju moćan alat u istražnim postupcima. Dakle, nove tehnologije, novi pristup izvršenja krivičnih djela, i otkrivanja istih, inspiracija je za sve istraživače krivičnopravnih i kriminalističkih nauka.

Ciljevi rada (naučni i/ili društveni): Na osnovu uočenog problema istraživanja definisan je i *predmet istraživanja:* predmet rada ima za cilj da objasni metode primjene digitalne forenzike u otkrivanju počinilaca sajber kriminala.

Metodologija/Dizajn: Iako se digitalni dokazi, do prije nekoliko godina u našem okruženju, nisu niti priznavali u sudskim procesima, danas je situacija sasvim druga, jer ovi dokazi ukoliko se prikupe, i obrade na adekvatan način, te prezentiraju uz pomoć propisanih procedura koji se forenzičari moraju pridržavati, tada su dokazi ravnopravni sa ostalim materijalnim dokazima. U konstelaciji sa navedenim, postavljen je sljedeći *problem, a ujedno i hipoteza istraživanja:* Da li je moguće metodama digitalne forenzike obezbjediti relevantne dokaze o počiniocima i krivičnim djelima za sudske postupke validne dokaze sajber kriminala?

Ograničenja istraživanja/rada: Jedan od bitnih faktora ograničenja istraživanja sajber kriminala, predstavlja ubrzani tehnološki razvoj, te samim tim i metode izvršenja izvršilaca, koje su svakim danom sve savremenije, a tehnološka pismenost u Bosni i Hercegovini, ne prati taj korak. Razvojem informacioni tehnologija, zahtijeva prije svega obrazovni sistem prilagođem novim dostignućima, tehnološku pismenost istražitelja itd.

[395] Mr. sci. Elmedin Ahmić, Općinski sud u Travniku, elmedin_ahmic@hotmail.com
[396] Prof. dr. Almin Dautbegović, profesor Krivično-procesnog prava, advokat, aleph.ze@gmail.com
[397]Prof. dr. Nedžad Korajlić, Fakultet za kriminalistiku, kriminologiju i sigurnosne studije Sarajevo, dekan, tppaba@bih.net.ba

Rezultati/Nalazi: Istina je da koliko god uložili u sigurnost, to ne znači da će informacijski sistem biti u potpunosti siguran te da smo oslobođeni problema. U Bosni i Hercegovini do sada nije provedeno relevantno i sveobuhvatno istraživanje o pojavnosti i rasprostranjenosti ovog kriminala. Zato se mora reći da je u sigurnosnom smislu Bosna i Hercegovina nedovoljno istraženo područje. Bosna i Hercegovina nema ni strategiju ni institucije za rješavanje pitanja sajber kriminala i sajber sigurnosnih prijetnji. Ukoliko se obezbijede ulaganja u razvoj ove discipline kako u materijalne tako i u ljudske resurse, trebalo bi da se smanje ozbiljni problemi prijetnji od hakiranja internet stranica do drugih oblika ovog kriminala.
Generalni zaključak: Digitalna forenzika će nastaviti da se razvija i postat će sigurno moćna tehnika za otkrivanje digitalnih dokaza. Da bi taj razvoj bio nesmetan potrebno je da ga prati zadovoljavajuća pravna regulativa i da država ne predstavlja usporavajući faktor.
Opravdanost istraživanja/rada: Tendencije učestalosti izvršenja krivičnih djela iz oblasti sajber kriminala, uzima sve veći primat kako u svijetu, tako i u Bosni i Hercegovini. Zakonska legislativa je prva stepenica u sistematskom pristupu ovom problemu, koji treba u kontinuitetu dorađivati, mijenjati, uporedo sa razvojem tehnološki dostignuća i razvojem istih, kako bi bili na punom tragu izvršiocima ovih krivičnih djela.
Ključne riječi: Sajber kriminal, zakon, istraživanje, krivično djelo, digitalna forenzika, prevencija

Apstract

Reason (s) for writing and research problem (s): By developing information-communication techniques, more and more cyber-criminals are being created to easily "infiltrate" the system of an individual or a company and make damage. The paper will describe the development of cybercrime, forms of abuse and fraud, and technologies used to detect perpetrators. Drawing these data, their interpretation, and forecasting, and simply presenting in court, are a powerful tool in investigative proceedings. Thus, new technologies, a new approach to the perpetration of criminal offenses, and their discovery, is an inspiration for all investigators of criminal law and criminology.
Goals of this paper (scientific and/or social): Based on the identified research problem definition and subject matter of research: the subject of the paper aims to explain the methods of applying digital forensics to detecting cybercriminals.
Methodology/Design: Although digital evidence, even a few years ago in our environment, did not admit it to judicial proceedings, today's situation is quite different, as this evidence is collected and processed in an adequate manner and presented with the help of prescribed procedures that must be respected by forensicists , then the evidence is equated with other material evidence. In the constellation of the above mentioned, the next problem has been raised, and the hypothesis of the research is: Is it possible to provide relevant forensic evidence of perpetrators and criminal offenses of cybercrime to judicial proceedings?
Research/paper limitations: One of the key factors of cyber crime limitation is the accelerated technological development, and thus the execution methods of perpetrators, which are more and more contemporary and technological literacy in Bosnia and Herzegovina, are not following this step. With the development of information technology, I primarily adapt the education system to new achievements, the technological literacy of investigators and so on.
Results/Findings: It is true that as far as security is concerned, this does not mean that the information system will be completely safe and free from the problem. So far, no

relevant and comprehensive investigation into the occurrence and spread of this crime has been carried out in Bosnia and Herzegovina. That is why it has to be said that, in the security sense, Bosnia and Herzegovina is insufficiently explored. Bosnia and Herzegovina has no strategy or institution to address cybercrime issues and cyber security threats. If investment in the development of this discipline is provided both in material and human resources, serious threats from hacking websites to other forms of this crime should be reduced.

General conclusion: Digital forensics will continue to develop and will become a powerful technique for detecting digital evidence. In order for this development to be undisturbed it is necessary to follow a satisfactory legal regulation and not to represent a decelerating factor.

Research/paper validity: The tendency of the frequency of cybercriminal crime is growing in the world, as well as in Bosnia and Herzegovina. Legislative legislation is the first step in the systematic approach to this issue, which needs to be continually updated, altered, alongside the development of technological achievements and development, to be in full swing for the perpetrators of these criminal offenses.

Key words
Cyber Crime, Law, Research, Criminal Offense, Digital Forensics, Prevention

1. Uopšte o sajber kriminalu

Razvojem informatičko-komunikacijskih tehnologija donijele su sa sobom nove oblike društveno neprihvatljivog ponašanja koje se treba na adekvatan način kriminalizirati. I-pak nacionalna zakonodavstva sve više imaju problema za efikasno regulisanje sve većeg broja novih društvenih odnosa koji traže pravnu regulaciju. Posmatrajući savremeno društvo možemo uočiti brojne specifičnosti i ozbiljne probleme koji uglavnom imaju globalnu dimenziju. Do sada je potvrđeno da niti jedan normativni sistem nije uspio do kraja obuhvatiti sve relevatne društvene odnose.

Sa razvojem globalne računarske mreže stvorile su se i dodatne mogućnosti za nove oblike kriminala. Sve češće se pojavljuju pojedinci koji su posebni i tehnički potkovani te možemo reći opsjednuti i osvetoljubivi. Tim osobama se sve teže suprotstaviti i zaustaviti ih.

Naravno zbog lakoće "kretanja" po sajber prostoru pojedinac dobija osjećaj moći i neuhvatljivosti. Ovi osećaji nisu bez razloga, jer stvarno ga je izuzetno teško otkriti u momentu činjenja djela, što, uglavnom, predstavlja i “pravi” trenutak za njegovo identifikovanje i hvatanje. S druge strane, Internet koji je toliko ranjiv i nesiguran zbog ogromnog broja korisnika pretpostavlja se više od tri milijarde korisnika (Internet-Hit-3-Billion-Users, 2014), otvorenosti i neregulisanosti je i idealno skrovište kriminalaca različiti tipova. U ovim okruženjima i sa takvim pojedincima sve se češće pokušavaju izboriti ne samo mnoga nacionalna prava već i međunarodne organizacije, kao i “privatni sektori” ne bi li ublažili negativne posljedice i smanjili gubici koji nastaju zbog kriminalnih aktivnosti.

Tradicionalne kriminalne grupe i organizacije modernizuju se korištenjem ICT, a sajber prostor postaje sredina u kojoj djeluju i koja im istovremeno služi kao mjesto koje je idealno za sakrivanje. Ono postaje i okruženje u kome nastaje poseban tip kriminala – sajber kriminal (Porobić i Bajraktarević, 2012).

1.1. Pojam i definicija sajber kriminala

Možda najpotpuniju definiciju sajber kriminala možemo naći u dokumentu „Kriminal vezan za kompjutersku mrežu“ (Report of Committee II, Workshop on crimes related to the computer network) sa Desetog Kongresa Ujedinjenih nacija, posvećenog prevenciji kriminala i tretmanu počinilaca koji je održan u Beču od 10. do 17. aprila 2000. godine (Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, Wienna, 10-17 April 2000. godine). Radna grupa eksperata u sadržaju izvještaja pod sajber kriminalom podrazumijeva „kriminal koji se odnosi na bilo koji oblik kriminala koji se može izvršavati sa kompjuterskim sistemom i mrežama, u kompjuterskim sistemima i mrežama ili protiv kompjuterskih sistema i mreža“. To je kriminal koji se odvija u elektronskom okruženju. Ako se pod kompjuterskim sistemom podrazumijeva „svaki uređaj ili skup međusobno povezanih uređaja, kojim osigurava ili čiji jedan ili više elemenata osiguravaju, prilikom izvršenja nekog programa, automatiziranu obradu podataka“ (Konvenciju o Sajber criminalu Vijeća Europe, 2011) je očigledno da bez kompjuterskih sistema i kompjuterskih mreža nema ni sajber kriminala. Pojam sajber kriminala je kompleksan i zbog čega ga mnogi smatraju tzv “kišobran terminom“ koji „pokriva“ raznovrsne kriminalne aktivnosti uključujući napade na kompjuterske podatke i sisteme, napade vezane za računare, sadržaje ili intelektualnu svojinu.

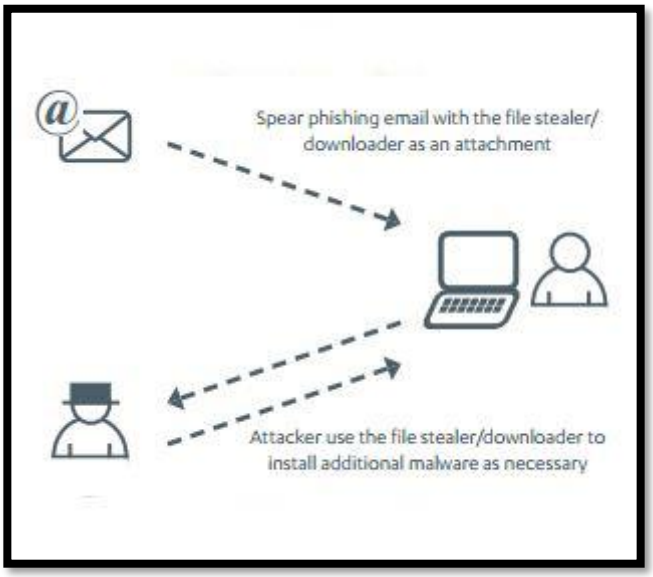
Pravni osnov za postupanje u ovoj oblasti je ustanovljen usvajenjem Konvencije o Sajber kriminalu (usvojena u Budimpešti 23. 11. 2001. g.) koji je preveden kao Konvencija o visokotehnološkom kriminalu ili kao Konvencije o kibernetičkom kriminalu. Također se treba istaći da pod pojmom sajber krivična djela treba svrstati samo krivična djela kod kojih je upotreba kompjutera odnosno kompjuterskog sistema ili kompjuterske mreže bitna za biće krivičnog djela, a ne sva krivična djela u kojima se na neki način kao sredstvo izvršenja pojavljuje kompjuter sa pripadajućom perifernom opremom (Porobić i Bajraktarević, 2012).

1.2. Sajber kriminal

Što važnija postaje mreža u širem značaju za globalno društvo i privredu, to profesionalniji postaju sajber napadači i sajber napadi. Sajber kriminal ima mnogo oblika, te je stoga sve teže se i boriti sa ovom vrstom kriminala. U uobičajene oblike sajber kriminala ubrajamo:

1.2.1. Phishing ili mrežna krađa

Phishing ili mrežna krađa je vrsta prijevare putem koje zlonamjerni pojedinac ili organizacija pokušava doći do osjetljivih, povjerljivih ili tajnih podataka, naravno lažno se predstavljajući. Podaci koji se takvim putem mogu prikupiti su razni - brojevi i PIN-ovi kreditnih kartica, E-mail lozinke, pristupni podaci za razne web servise (Facebook, Skrill, Paypal, Twitter, Ebay) itd.



Grafik 1. Phishing e-mail napad *Izvor: http://securityaffairs.co/wordpress/18206/cyber-crime.html*

Pošiljatelj šalje poruku u kojoj traži od korisnika da odgovori sa pristupnim podacima (lažno se predstavljajući kao službeni kontakt), u svrhu "poboljšanja usluge", ili sprečavanja brisanja korisničkog računa sa određene stranice (Ilustracija 1). Takve poruke gotovo redovito prati slaba pismenost, gramatičke i pravopisne greške. Lažna internetska stranica izgleda skoro identično autentičnoj stranici, ali je URL u adresnoj traci drugi. Kad korisnik upiše podatke na lažiranoj stranici, informacije dolaze do vlasnika lažirane stranice.

Phishing napadi se redovito poboljšaju te uz pomoć razni setova sada koji su dostupni naravno i pojednostavljuju proizvodnju phishing sajtova. Pošiljatelji su u prednosti i mogu lako kroz spam e-mailove da namame žrtve na stranice koje su automatski stvorili, te na kojima mogu da ukradu lične podatke i druge osjetljive podatke. Jedan od načina izbjegavanja ove vrste napada je ignoriranje poveznica danih u e-mailu. Umjesto toga preporučljivo provjeriti adresu navedene internet stranice u preglednik i provjeriti istinitosti

zahtjeva preko te stranice. Korisno je i imati na umu kako ozbiljne organizacije ne kontaktiraju korisnike na ovakve nesigurne i nepouzdane načine.

1.2.2. Hakiranje odnosno zloupotreba internet stranice ili mreže

Razlog hakiranja jesu slabo zaštićene internet stranice iz finansijskih razloga, koje pogoduju napadima i njihovoj „lakšoj" provali te na taj način usmjeravati procese sajber prostora i sigurnosnoj prijetnji kako žele napadači. Naravno takve stranice su itekako pogodne za hakere i njihovo vršenje napada. Za klasični primjer hakiranja neke internet stranice i njihovom društvenom uticaju po sigurnosni problem, predstavićemo u jednom primjeru prepoznatljivog proizvođača video igrica. Tako je Lizard Squad - Hakerska grupa koja je preuzela odgovornost za napad zbog kojeg je PlayStation Network bio offline veći dio dana. Sony je istakao da je riječ isključivo o DDoS[398] napadu i kako korisnički podaci nisu ugroženi.

Ilustracija 1*: *DDos napad na Sony Playstation *Izvor: http://www.mirror.co.uk/news/world-news/sony-hit-playstation-hack-page-4766760*

Stewart Room direktor Cyber Security Challenge je potvrdio za SCMagazine (Scmagazineuk, 2015) da je ovaj najnoviji napad došao u 'rekordnoj' godini za sajber-sigurnost. Vijest o napadu na Sony PlayStation podsjeća još jednom da su prijetnje sajber-sigurnosti raznolike kao što su i stvarne. U 2014. godini zabilježen je rekordan broj napada, a prijetnje su došle sa različitih područja, kao što su krivične prijetnje, prijetnje pod

[398] DDoS je engleska skraćenica za Distributed Denial-of-service attack, i označava sprečavanje pristupa računarskom sistemu korištenjem mnogobrojnih raspršenih resursa koji se većinom nalaze na Internetu.

pokroviteljstvom države, zlonamjerni radnika, a sada i Lizard Squad, čiji motivi i motivacija može biti više od samog hakiranja. Osim što su preuzeli odgovornost za DDoS napad na Sony-eve servere, iz Lizard Squada su na Twitteru poslali i lažnu prijetnju bombom američkoj avio kompaniji American Airlines. Cilj je bio dodatno isprovocirati Sony tako što su došli do podataka o letu na kojem je bio predsjednik Sony Online Entertainment studija, nakon čega je dotični let preusmjeren i prizemljen na najbliži aerodrom.

Ilustracija 2: Prijetnja bombom hakera Lizard Squad na Twitter-u

Glasnogovornik American Airlinesa je potvrdio kako je spomenuti let preusmjeren iz "sigurnosnih razloga".

Ovakvi i slični primjeri nam govore koliku sigurnosnu prijetnju mogu proizvesti ovakvi napadi na određene baze podataka, „hakiranjem“ te na taj način korištenjem tih podataka i svoje svrhe zloupotrebom istih, ucjenama, uticajem na promjeni nekih odluka, i sl. Iz ovog i sličnih primjera, potrebno je upoznati se sa opasnostima, ovakvih upada i računarske mreže, zaštiti ličnih podataka, njihovom zloupotrebljavanju, i kakav uticaj mogu proizvesti ovakvi hakerski napadi i koliku štetu mogu učiniti kako za određene pojedince, tako i na globalnom nivou.

1.2.3. Širenje mržnje i poticanje na terorizam

Trenutno je internet najzastupljeniji medij komunikacije, naročito među mlađim generacijama. Razvojem interneta prijenos informacija se mijenja, te informacija postaje povod za diskusiju na internetskim platformama pri čemu svi korisnici prakticiraju pravo na izražavanje (William i sar., 2011). Da ima razlike između tradicionalnih medija i interneta to možemo vidjeti kroz činjenicu da sadržaji koji pristignu budu provjereni i odobreni prije nego se puste u javnost. Internet je javno mjesto gdje je dovoljno tehnički uvjetovana

radnja (klik miša) da se sadržaj objavi i prenese u javnost, a kontrola nastupa (ako do nje i dođe) a posteriori.

Internet je zapravo prostor bez „granica" a brzina i opseg diseminacije sadržaja teško su zaustavljivi. Razlog i nemogućnost efikasnog kontroliranja interneta je što internet kao globalni medij načelno podložan različitostima pravnog uređenja u svakoj pojedinoj državi, dok je istovremeno nedovoljno regulisan na međunarodnom nivou da bi se moglo izvršiti njegovo uređenje. Zbog svega navedenog autori širenja mržnje mogu putem Interneta besplatno širiti mržnju te „dotaći" veliki broj ljudi u jako kratko vrijeme. Kroz brojne društvene mreže dijele isti interes i motivaciju mogu se povezati te tako ojačati. Također su mehanizmi kontrole nevidljivi pa tako mogu i maloljetnici imati pristup ovakvim sadržajima.

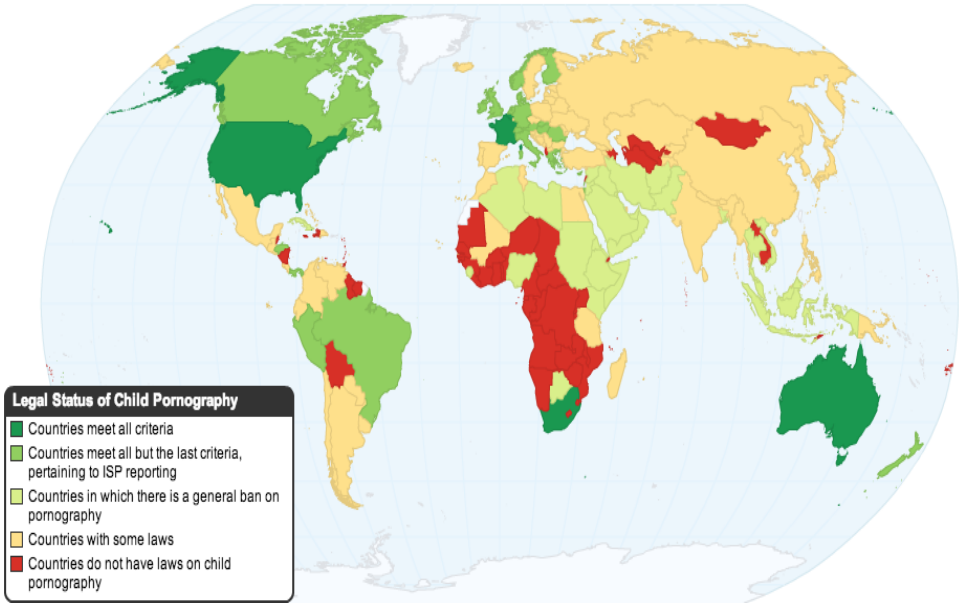
'Novi terorizam i novi mediji' zbog jednostavnosti i anonimnosti komunikacije putem društvenih mreža, sve je teže pratiti jer komunikacije terorista, odnosno protuterorističke jedinica sve je teže zaustaviti jer potencijalne napade dogovaraju na ovaj način. Teroristi se društvenim mrežama najčešće služe za propagandu, radikalizaciju i regrutiranje novih članova te im one omogućuju da 'ciljanoj publici virtualno pokucaju na vrata', odnosno ostvare direktan kontakt s njima i pokušaju ih privući sa svojim idejama. Činjenica da je širenje mržnje i terorizma zabilježeno na novom mediju, neke države smatraju da načela trebaju biti podjednako primijenjena kao npr. u slučaju djeljenja sadržaja (tzv. engl. „share" opcija na društvenim mrežama poput Facebooka) budu jednako kažnjiva kao dijeljenje letaka kojima se poziva na mržnju ili terorizam.

1.2.4. Distribucija dječije pornografije

Danas Internet svjetska informatička mreža koja je ušla u mnoge domove širom svijeta (Dragičević, 1999). Tradicionalni korisnici pornografskih sadržaja sve se više koriste Internetom, što potvrđuje i velik pad interesa za štampana izdanja nekih časopisa. Tako je npr. teksaški pornomagnat Thomas Reedy putem svoje kompanije Landslide Productions Inc. zarađivao oko 1,4 milijuna USD godišnje od pretplate koja je iznosila oko 15 USD u prosjeku po pretplatniku. Riječ je bila o mjesečnoj pretplati koja je korisnicima omogućavala pristup najodvratnijim prizorima spolnih zlopotreba djece koji se uopće mogu zamisliti (Cyber Lolita and Child Rape). Reedy je 2001. godine osuđen na 1.335 godina zatvora, što je prva kazna doživotnog zatvora izrečena za distribuciju dječije pornografije putem Interneta (Rubin, 2003). Premda se s potpunom sigurnošću ne može ustanoviti tačan broj izvora dječije pornografije na Internetu, nesporno je da ona svakodnevno raste. Tom širenju pridonose brojni faktori, od kojih treba izdvojiti anonimnost korisnika te razvoj i razmjernu dostupnost različitih multimedijalnih tehnika kojom i osobe bez posebnog znanja mogu izraditi i distribuirati nezakonite sadržaje.

Obzirom na tako opasnu pojavu, potrebno je zakonsku legislativu razvijati kontinuirano na globalnom nivou kako bi se spriječile zloupotrebe dječijih fotografija eksplicitnog

sadržaja i uopšte zabranila distribucija. Međutim, nije samo zakon koji bi garantovao sigurnost, također je potreban rad policije, pravosudnog sistema i vladajućih struktura koji moraju biti spremni za izvršenje kazni bez tolerancije za svaku povredu tih zakona.



Ilustracija 3: Pravni status dječje pornografije *Izvor: http://findingjustice.org/legal-status-child-pornography/*

Ilustracija 3. prikazuje pravni status dječje pornografije u svijetu. Nevjerovatno je da nešto tako odvratno i grešno, nije međunarodno zabranjeno.

- 5 zemalja zadovoljava sve kriterije.
- 24 zemalje zadovoljava sve, ali ne i ISP izvještaje.
- 68 zemalja imaju neki zakon koji se izričito bavi dječijom pornografijom.
- 92 zemlje nemaju zakona koji se konkretno bavi dječijom pornografijom.

Ova ilustracija, nam jasno govori kako se u svijetu pristupa problemu zaštite i zloupotrebe dječijih eksplicitnih sadržaja, njihovom korištenju, distribuiranju , a prije svega evidentno je mali broj zemalja imaju jasno opredjeljen stav u pravnom smislu kada je u pitanju prevencija i zaštita dječijih prava i sloboda.

2. Digitalna forenzika

Da bi se odgovorilo na visokotehnološki kriminal javila i se potreba za razvojem nove naučne discipline, kao i regulisanje pravnih normi vezanih za uspješno otkrivanje, a zatim i procesuiranje krivičnih djela iz ove oblasti.

Digitalna forenzička istraga predstavlja proces koji korištenjem 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 protivpravnoj aktivnosti i svih okolnosti u vezi sa počiniocem i načinom izvršenja krivičnog djela. Digitalni dokaz u tom slučaju predstavlja digitalni objekat koji sadrži pouzdane informacije koje podržavaju hipotezu. Kako bi se učinjena nezakonita djela dokazala i njihovi počinioci procesuirali i sankcionisali, potrebno je primjeniti procedure digitalne forenzike kao naučne discipline sa izuzetno značajnom praktičnom primjenom. Upravo digitalna forenzika kao relativno nova naučna disciplina (uspostavljena 1999. godine od strane IECO - International Organization on Digital Evidence) obezbjeđuje jedini pouzdani alat za istragu kompjuterskog i mrežnog kriminala, akviziciju i analizu digitalnih podataka i pripremu i prezentaciju digitalnih dokaza pred sudom. U slučaju da je došlo do zloupotrebe IKT (informaciono komunikacijska tehnologija) sistema, odnosno kompjuterskog kriminala ili potrebe za upravljanjem kompjuterskim incidentom, administrativnih zahtjeva ili civilne parnice, odgovore će nam dati digitalna forenzika koja podrazumijeva otkrivanje (pretraga, istraga) i sakupljanje (akviziciju), čuvanje (upravljanje), dokazivanje (analizu) i ekspertsko svjedočenje (prezentaciju) digitalnih dokaza pred sudom (Milosavljević i Grubor, 2009).

Digitalna forenzika je naučna disciplina koja može ponuditi relevantan dokaz odnosno digitalni dokaz. Veliki razvoj IKT-a postavlja velike izazove pred digitalne forenzičare koji moraju imati permanentnu i svakodnevnu edukaciju kako bi bili za korak ispred počinioca koji sprovode protivpravne aktivnosti u digitalnom okruženju. Brzina tehnološkog razvoja uticala je na razvijanje ove mlade naučne discipline, koja zajedno sa paralelnim razvojem drugih nauka, primjenjuje nove metode koje utiču na brzinu, i jednostavnost prikupljanja čvrstih dokaza, istražuje anti-forenzičke aktivnosti, sa ciljem da otkrije istinu u vezi sa učinjenom protivpravnom radnjom. U taksonomiji digitalne forenzike, a u odnosu na predmet forenzičke istrage, digitalnu forenziku možemo podjeliti na: forenziku računarskih sistema, forenziku mobilnih uređaja, forenziku baza podataka i forenziku računarske mreže uključujući i Internet ili kibernetičku forenziku (Marcella i Greenfield, 2002). Treba istaći da je za digitalnog forenzičara od presudne važnosti 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 kao i profilisanje prema drugim IKT sistemima).

Različiti profili kompanija primjenjuju digitalnu forenziku i od policijsko-sudskih i vojno-obaveštajnih aktivnosti, civilnog i bankarskog sektora i osiguravajućih društava. Svi ovi entiteti moraju biti izuzetno oprezni sa podacima kojima raspolažu, jer u protivnom može biti prouzrokovana nemjerljiva šteta zbog industrijske špijunaže, zloupotrebe IKT sistema, ali i nekih drugih oblika protivpravnih postupaka. Procjena je, da šteta od različitih djelovanja visokotehnološkog kriminala, ne uzimajući u obzir njegove potencijalne veze sa organizovanim kriminalom, na godišnjem nivou iznosi oko 200 milijardi dolara (Prlja, 2017).

Da bi se podaci mogli koristiti kao neoborivi i čvrsti dokazi pred sudom digitalna forenzika kompjuterskog sistema obuhvata naučno ispitivanje i analizu podataka sa čvrstih diskova, fajl sistema i prostora za skladištenje podataka. Steve Haily iz Cybersecurity instituta, digitalnu forenziku posmatra kroz postupke dobijanja, očuvanja, identifikacije, tumačenja i dokumentovanja digitalnih dokaza prema propisanim pravilima, pravne procese, postupak očuvanja integriteta dokaza, kao i pružanje stručnog mišljenja pred sudom u vezi sa pronađenim dokazima. Na osnovu navedene definicije može se zaključiti da digitalna forenzika podrazumijeva upotrebu unaprijed definisanih procedura i tehnika za detaljno ispitivanje kompjuterskog sistema, a sa ciljem dobijanja relevantnih digitalnih dokaza. Često u literaturi možemo da pronađemo poistovjećivanje digitalne forenzike kompjuterskog sistema sa procesom oporavka podataka. Ovo je samo djelimično i tačno. Digitalna forenzika oporavlja podatke koje je korisnik namjerno sakrio ili izbrisao, za razliku od slučajno izgubljenih ili izbrisanih, što kao krajnji cilj ima da se obezbjedi validnost oporavljenih podataka za dokaze pred sudom. Forenzičari imaju strogo definisana pravila, pri prikupljanju medijuma (čvrste diskove i sve druge sekundarne medije za skladištenje podataka) za koje sumnjaju da se na njima nalaze digitalni dokazi, osiguravaju ih od bilo kakvih promjena, i iz velike količine digitalnih podataka moraju pronaći relevantne i održive dokaze.

Digitalna forenzika igra veliku ulogu u praćenju potencijalnih počinilaca protivpravnih aktivnosti. To se postiže identifikacijom protivpravne aktivnosti, prikupljanjem dokaza, izgradnjom "lanca nadležnosti nad digitalnim dokazima", analizom dokaza, prezentovanjem pronađenih dokaza, svedočenjem i sve to u okviru vođenja sudskog postupka protiv osumnjičenog. Digitalni dokazi mogu biti oslobađajući, optužujući ili da ukazuju na osnovanu sumnju.

2.1. Digitalni dokaz

Digitalni dokaz počiva kao elektornski podatak, bilo u formi transakcije dokumenta ili neke druge vrste medija, kao što su audio i video snimci. Skoro pa svaka današnja transakcija je digitalozovana u nekom trenutku i postaje digitalni dokaz, npr. podizanje novca sa računa, plaćanje računa na bankama, plaćanje kreditnim karticama itd... U današnjem vremenu gotovo nemoguće je u ovom povezanom svijetu da na neki način ne ostavite elektronski trag putem plaćanja bilo kakve vrste transakcije. Mnogi ljudi danas dijele

svoja svakodnevna dešavanja na socijalnim mrežama kao što su Twitter, Facebook Google+ i mnoge druge. U stanju smo da znamo pored svih slika pjesmi, politički stavova, dnevni događaja, saznamo i njihove lokacije gdje se u trenutku objave nalaze. Prilikom pisanja E-mail poruke ili dokumenta u Wordu ili Notepad-u, vozimo automobil sa uključenim GPS uređajem ili nešto plaćamo preko interneta, mi stvaramo digitalni dokaz. Prilikom surfanja internetom i telefoniranja stvara se digitlani dokaz. To su nam više poznati oblici digitalni dokaza, međutim mnogo puta radimo sve naborojane radnje, a uistinu nismo svjesni da stvaramo digitalne dokaze.

Da bi jedan digitalni dokaz bio prihvaćen od strane suda treba da posjeduje pet osobina:

a) Prihvatljivost – Potrebno je da je u skladu sa određenim pravnim pravilima, prije nego što bude dostavljen sudu. Ukoliko se koristi orginal tada kopija nema značaja, dok je u slučaju korištenja kopije potrebno koristiti najbolju kopiju. S obzirom da se danas može napraviti kopija digitalnog dokaza koja je istovjetna originalu, upotreba kopije je pravno prihvatljiva i ako postoji original. Upravo se u praksi koristi i primjenjuje prezentovanje kopije digitalnog dokaza, da bi se eliminisale sve sumnje vezane za izmjenu tj. zloupotrebu sa originalnim dokazom,
b) Autentičnost - Dokazni materijal mora nedvosmisleno upućivati na krivično djelo i počinioca. 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 i neprihvatljivim za donošenje sudske odluke,
c) Kompletnost – u smislu da dokaz treba da prikaže cjeli slučaj sa svim aspektima bitnim za donošenje sudske odluke. Dokaz mora biti objektivan i prikazati sve bitne okolnosti za sudsko odlučivanje – Ukoliko postoje okolnosti koje mogu biti oslobađajuće tako i one koje se stavljaju na teret počinioca,
d) Pouzdanost –nije dozvoljeno da 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,
e) Vjerodostojnost i razumljivost – dokaz mora biti lako razumljiv i vjerodostojan za sud i stranke u postupku. Nema svrhe pred sud iznositi neke stručne stvari i objašnjavati npr. „memory dump— (sliku stanja memorije u računaru), s obzirom da sud nema obavezu da posjeduje takva stručna znanja pa samim tim neće razumjeti šta to znači (Schweitzer, 2003).

2.2. Forenzička istraga

Kolekcije forenzički alata se koriste za identifikaciju datoteka koje je potrebno pregledati. Prilikom procesa akvizicije alat stvara indeks pojmova koji predstavljaju osnovnu jedinice pretrage. Pojam može biti samo znak ili skupina znakova, alfanumeričkih ili numeričkih, s razmacima na obje strane. Pretraga veličine datoteka ili raspon veličina traženih (Bunting i Wei, 2006) dokumenata vrši se uz pomoć Boolove logike (I, ILI, NILI). Svaki forenzički softver posjeduje specifične ugrađene metode pretrage koje koriste boolovu logiku.

Pojmove je moguće povezati korištenjem boolovih operatora. Kako bi se stvorio traženi izraz ili moglo filtrirati rezultate. Alate za digitalnu forenzičku istragu možemo podjeliti na hardverske i softverske alate. Zatim prema platformi na kojoj rade:

- "Open Source" programi (Sleuthk Kit & Autopsy, SMART....),
- Licencirani programi: (EnCase, Helix3 Enterprise, X-Ways Forensics...).

Zatim prema platformi na kojoj rade:

- Windows platforma: (EnCase , X-Ways Forensics....),
- Linux platforma: (Sleuthk Kit & Autopsy, Helix3 Enterprise...).

Digitalni dokaz ima važnu ulogu na sudu, ali dobijanje takvih dokaza često može biti vrlo teško. Svaki od navedenih alata odgovara određenim potrebama. Njihova upotreba je od velikog značaja kada treba doći do izgubljenih, obrisanih ili oštećenih podataka koje treba povratiti. Danas, kada je broj prevara, zločina i zloupotreba računara veoma veliki, neophodno je imati odgovarajuće alate kojima je lako odgovoriti na potrebe istrage. Ono što prvo treba da svaki alat obezbijedi, jest to da eletronski ili digitalni dokaz bude takav da može da se podnese kao validan dokaz na sudu. Za to je uglavnom neophodno predznanje i obuka u vezi sa radom sa alatima. Glavni nedostatak većine alata je cijena prilikom vraćanja podataka. Eksperti za kompjuterski kriminal naplaćuju po satu, a istraga može trajati i do 10 i više sati. Iako primjena kompjuterske forenzike i alata ima svoje prednosti i nedostatke, pokazalo se da je njihova upotreba opravdana i vrlo korisna u većini slučajeva kada se može primjeniti. Predstavićemo u radu neke od najzastupljenijih alata za otkrivanje sajber prevara, kojim dokumentujemo izvršenje krivičnog djela.

2.2.1. EnCase Forensic

EnCase Forensic je vodeći software i svjetski pružatelj rješenja, usluga i obuke u području digitalne forenzike. Kako bi pratili tempo i trend, forenzički alati koji forenzičari koriste su sve kompleksniji i sa više funkcionalnosti nego ikad prije, a imaju i veću učinkovitost. Dovoljno je samo da se pogleda razlika u dodatnim funkcijama između verzija određeni verzija i može se uočiti ogromna razlika. Prošla su vremena kada se jedan alat koristio samo kako bi stvorili sliku, drugi alat se koristi samo u pretraživanju podataka, treći alat se koristi samo za stvaranje hash datoteka itd. Današnji alati ispunjavaju često zatraženo "pronalazak svih dokaza (i ispisivanje izvještaja)" klikom na dugme. Uspješni i profesionalni forenzičari u jednom trenutku moraju prenijeti svoje rezultate na treću osobu koja ima vrlo ograničeno ili malo razumijevanje računarskih operacija. Te treće strane su obično istražitelji, odvokati, suci, žiri itd. Forenzičar mora objasniti, usmeno i pisanim izvještajima, vrlo mnogo tehnički pojmova u smislu da laik može razumjeti. Potrebno je naravno vrijeme, praksa, znanje, iskustvo i kreativnost. Najviše od svega, to zahtijeva da su spremni poduzeti dodatne napore kako bi izvještaj bio uspješan. Kada se stvori

izvještaj da čitatelji mogu lako čitati i razumjeti, rezultati moraju govoriti sami za sebe (Bunting i Wei, 2006).

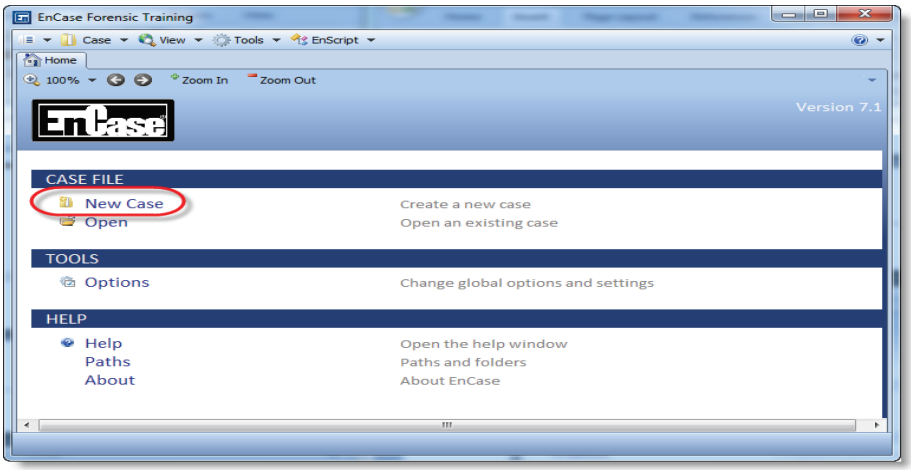
EnCase je alat za kompjutersku forenziku koji je proizveo GuidanceSoftware. Dostupan je advokatskim kancelarijama, a koristi se za prikupljanje podataka, oporavak fajlova, pretragu i parsiranje fajlova. Za korišćenje ovog softvera obično je neophodna specijalna obuka. Podaci otkriveni putem EnCase alata se uspješno koriste u raznim sudovima širom svjeta. EnCase softver omogućava korisnicima da kreiraju boot disk koji će zaštititi podatke od toga da budu upisani na neki sumnjivi disk prilikom procesa pokretanja kompjutera. Jednom kada se kompjuter pokrene i krene sa radom, forenzičar može da krene sa pravljenjem slike diska, bilo pomoću patch kabla ili serial kabla. Kada se slika kreira, EnCase softver omogućava pretraživanje hard diska na neki od sljedećih načina:

- Istraživanje slika sa hard diska pregledom pomoću galerije,
- Istraživanje fajlova korištenjem heksa pogleda (čitanje heksadecimalnih komponenti fajla),
- Pretraživanje cjelokupnog diska na ključne riječi (Advances in Digital Forensics II, 2006).

EnCase alat također posjeduje mogućnost izvještavanja što omogućava istražiteljima da sačuvaju pronađene ključne riječi, slike i da snime lične komentare u formatu koji je lak za izvještavanje. Na taj način, informacije mogu da se odštampaju ili prosljede mail-om pravnim zastupnicima koji su uključeni u slučaj. EnCase predstavlja jedan od najnaprednijih i sveobuhvatnih alata za izvođenje složenih i vremenski zahtjevnih zadataka, kroz višestruke sistemske fajlove i jezike. Nova verzija ovog programa je V7 koja uključuje nove značajke kao što su smartphone modul, eksterni pregled paketa i pristup desetinama EnScripta[399] i aplikacija u App EnCase Central-u.

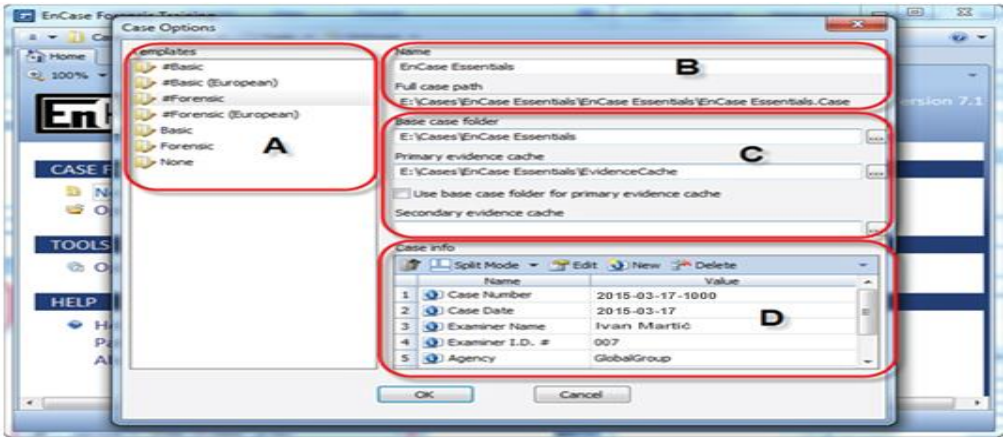
Procesor Manager za dokaze u EnCase Forensic V7 omogućava distribuciju i kontrolu obrade dokaza za jednu ili više EnCase mašine ili EnCase procesor čvorova. Sa dokazima Procesor Managera, može se pojednostaviti, automatizirati, i povećati brzina obrade dokaza i preuzimanja (EnCaseFroensicBrochure, 2014).

[399] EnScript je programski jezik korišten od strane forenzički kompjuterski programa kao što je EnCase.



Ilustracija 4: Shema novog slučaja Izvor: Vlastita izrada

Procesor Manager pruža također istražitelju potpunu kontrolu u preradi dokaza, te osim toga optimiziran je za efikasnije iskorištavanje sistemskih resursa, čime se povećava brzina obrade. Ilustracijom će biti prikazano pravljenje jednog slučaja u EnCase V7:



Ilustracija 5: Pravljenje novog slučaja Izvor: Vlastita izrada

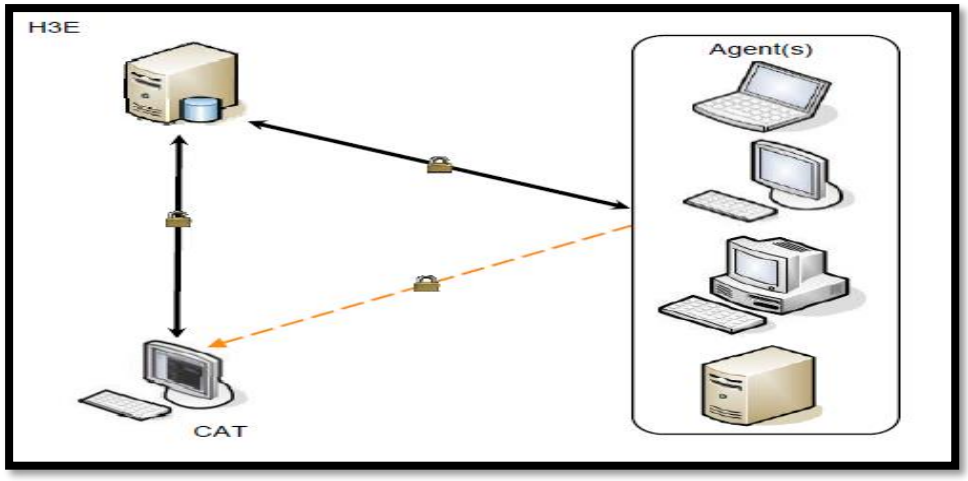
- Opcija A - Kada stvaramo novi slučaj, dobivamo popis dostupnih predložaka (templates). To su unaprijed definirani predlošci koje EnCase prikazuje uz spašene predloške. Na Ilustraciji 5, izabran je Forenzički predložak.
- Opcija B - Ime slučaja je tekst koji se unosi za identificiranje slučaja. U ovoj verziji EnCase V7, slučaj više nije sadržan u jednom fajlu, već je pohranjen unutar mape koja sadrži mnoge komponente. Naziv naveden u ovom polju koristi se za pronalazak predmeta u toj mapi.

- Opcija C - Mapa osnovnog slučaja - To je mjesto gdje se stvara nova mapa slučaja.
- Opcija D - Informacije o slučaju - Informacije o trenutnom slučaju. Ove stavke se prvenstvenstveno koriste za umetanje korisnički definirani podataka u izvještaju.

Forezičari mogu da podese vremensku zonu za svaki dio medija, omogućavajući jednostavno upoređivanje medija sa različitim zonama. Također mogu da sortiraju fajlove u odnosu na 30 različitih polja, uključujući i sva četiri vremenska pokazatelja (kada je neki od fajlova kreiran, kada mu je posljednji put pristupljeno, kada je posljednji put pisano i kada je posljednji put modifikovan), nazive fajlova, putanje, formate i slično. EnCase softver nudi više od 150 filtera, počevši od obrisanih fajlova pa sve do Word dokumenata koji su zaštićeni šifrom. Također ima ugrađenu pomoć koja brzo i jednostavno služi kao korisničko uputstvo (Mediarecovery, 2015). Završna faza forenzičkog ispitivanja je izvještaj, koji mora biti dobro organiziran i prikazan u formatu koji će ciljana publika razumjeti.

2.2.2. Enterprise

Uz pomoć Helix3 Enterprise (H3E) imamo potpunu vidljivost aktivnosti preko cijelog našeg mrežnog sistema, aktivnosti kao što su pristup neovlaštenim podacima, izvlačenje podataka ili stvaranje tajnih tunela. H3E također nam omogućuje da brzo reagujemo i bez otkrivanja korisnika odgovorimo na incidente i prijetnje. Helix3 Enterprise nam omogućuje da brzo otkrijemo, identificiramo, analiziramo, očuvamo izvještaj koji nam daje dokaze i otkriva istinu te štititi svako poslovanje. H3E rješenje je trostruka arhitektura koja se sastoji se od konzole za upravljanje (CAT), Servera i Agenata (H3E Manual, 2015).



Ilustracija: 6: Arhiktertura H3E

Svi podaci koji se razmjenjuju između CAT-a i Agenata prolaze kroz Server, osim za vrijeme prijenosa velikih slikovnih datoteka, kao što su RAM, tada CAT i agenti komuniciraju direktno. Server djeluje kao srednje spremište za sve podatke prikupljene od strane Agenata. Server autentificira i šalje naredbe iz CAT-a za Agente na mreži, a zatim istodobno prosljeđuje odgovore podataka natrag u CAT i pohranjuje ih u unutarnje SQL baze podataka. Verzija Helixa koja se najviše koristi je zasnovana na Ubuntu[400], što obećava stabilnost i laku upotrebu.

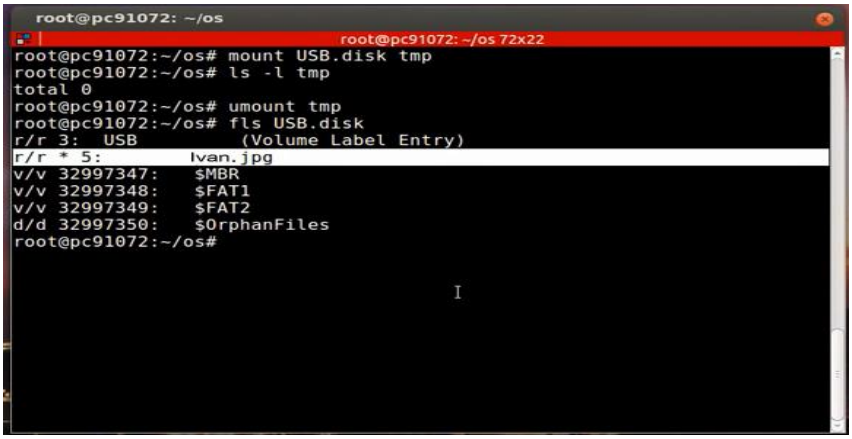
Ilustracija 7: Kontrolna ploča H3 Enterprise

Osnovni paket koji dolazi uz Helix3 sadrži moćan alat za analiziranje mreže, nekoliko anivirus alata, povratak lozinki, rezervne kopije i povratak particije, pretragu MAC particija, istraživanje binarnih fajlova itd. Može se zaključiti iz ovog da je Helix veoma koristan alat. Dual mod je posebno koristan, a to omogućava korisnicima Helix alata da pristupe problemima koji su povezani ne samo za Linux nego i sa Windows sistemom na različite načine. Helix je stabilan, kompletan paket, sa velikim opsegom mogućnosti koje mogu značajno povećati sposobnost odgovora na probleme, prijetnje i incidente iz okruženja. Pri kraju svih potrebnih analiza i pretraga obavlja se stvaranje izvještaja u PDF formatu. Helix3 Enterprise je jednostavan za korištenje i moćno rješenje kako bi se osiguralo poslovanje svakog preduzeća. Ne samo da uz H3E imamo vidljivost na cijeloj infrastrukturi, nego ovaj alat omogućuje pravovremeno reagiranje na incidente i prijetnje koji se mogu izolirati na vrijeme.

[400] Ubuntu je računarski operacijskih sistem nastao kao izvedenica sistema Debian GNU/Linux, koji pak mnoge temeljne komponente preuzima iz projekta GNU i koristi Linux kao jezgru operacijskog sistema.

2.2.3. Sleuth Kit-Autopsy

Sleuth Kit je forenzički alat za analizu i Microsoft i UNIX sistem datoteka i disk slika. Sleuth Kit je open source, što omogućuje istražiteljima da potvrde akcije alata ili ga prilagode na specifične potrebe. Sleuth Kit je razvijen nezavisno od komercijalnih i naučnih organizacija od Brian Carrier-a, koji je također razvio Autopsy Forensic Browser. Sleuth Kit je kolekcija alata za forenzičku analizu sistema pod UNIX-om baziranih na komandnoj liniji (Dowling, 2006). Alati omogućavaju ispitivanje sistemskih fajlova na sumnjivom kompjuteru na nenametljiv način. Alat nije povezan sa operativnim sistemom da bi analizirao sistemske fajlove, također prikazuje obrisane i sakrivene sadržaje.



Ilustracija 8: Prikaz obrisane slike sa USB-a *Izvor: Vlastita izrada*

Ilustracija 9: Oporavak izbrisane slike sa USB-a

Kada se izvodi kompletna analiza sistema, bolje je koristiti alat sa grafičkim okruženjem, a ne sa komandnom linijom. Autopsy Forensic Browser je alat u Sleuth Kit-u sa grafičkim interfejsom koji omogućava lakši tok istrage. Autopsy daje mogućnost menadžmenta slučaja, integritet slike, pretragu po ključnim riječima i ostale automatske operacije. Podržava NTFS, FAT, UFS1, UFS2, EXT2FS, EXT3FS, i ISO 9660 fajl sisteme. Alati mogu biti pokrenuti sa „živog" UNIX sistema tokom odgovora na incident. Ovi alati će prikazati fajlove koji su skriveni i neće modifikovati vrijeme pristupa (Dowling, 2006). Tehnike za pretraživanje dokaza sa ovim alatima su:

- Listing fajlova: Analizira fajlove and direktorije, uključujući imena izbrisanih fajlova i fajlova sa Unicode[401] baziranim imenima,
- Sadržaj datoteka: Sadržaj datoteka mogu biti pregledani u raw, hex, ili ASCII stringovi mogu biti raspakovani,
- Hash baze podataka: Pregled nepoznati fajlova u hash bazi podataka i brza identifikacija da li je dobar ili loš. Autopsy koristi NIST National Software Reference Library[402] (NSRL) bazu podataka u prepoznavanju dobri i loši fajlova,
- Sortiranje po tipu fajla: Sortitranje datoteka po poznatim tipovima. Autopsi može također izvući samo grafičke slike (uključujući minijaturni prikaz), te prikazati sve promjene ekstenzija datoteka koje su se koristile kako bi se sakrio određeni fajl,
- Pretraga po ključnoj riječi: Pretraga se može izvesti pomoću ASCII stringa i regularnih izraza. Pretraživanje je moguće izvesti na punom sistemu ili samo određeni datoteka i prostora. Stringove koji su često traženi možemo jednostavno konfigurirati u Autopsy za automatsko traženje,
- Analiza meta podataka: Meta podaci sadrže detalje o fajlovima i direktorijima. Autopsy dozvoljava pregled detalja bilo koje strukture meta podataka u sistemskom fajlu. Ovo je korisno ukoliko radimo oporavak podataka ili vraćanje izbrisanih sadržaja,
- Detalji slike: Detalji sistemski fajlova mogu biti pregledani uključujući i vremenske aktivnosti. Ovaj način nudi informacije koje su vrlo korisne tokom oporavka podataka (Sleuthkit. org, 2015).

Može se reći da svi ovi alati nude prilično dosta sličnosti, ali u nekim slučajevima EnCase ima malo više mogućnosti. U tom slučaju to sa sobom nosi i cijenu složenosti, a općenito neki korisnici se slažu da EnCase GUI nije tako intuitivan. Naravno, svaki od alata zahtijeva

[401] Unicode je standard za razmjenu podataka usmjeren na prikaz slova na način neovisan o jeziku, računarskom programu ili računarskoj platformi.
[402] Nacionalna referentna knjižnica Software-a (NSRL), je projekt Nacionalnog instituta za standarde i tehnologiju (NIST) koji održava repozitorij poznatog softvera, profila datoteka za uporabu provedbu zakona i drugih organizacija koje se bave računarsko forenzičkim istragama.

obuku ili neko predznanje. Helix, za razliku od ostala dva alata se koristi manje u sudskim procesima, a to proizilazi iz toga što je on namijenjen ne tako zahtjevnim potrebama.

2.2.4. DFRSW Model

DFRWS model je razvijen je između 2001. i 2003. godine pri digitalnoj forenzičkoj istraživačkoj radionici (engl. Digital Forensics Research Workshop). Ovim modelom su obuhvaćene digitalno istražne radnje, definisane klasama. Klase služe za kategorizaciju istražnih radnji po grupama. Modelom su predviđene liste radnji koje mogu da se izvršavaju, a neke od njih su obavezne. Specifičnost ovog okvira je ta, što za svaku pojedinačnu istragu u velikoj mjeri model mora biti redefinisan. Prema ovom modelu postoji ukupno sedam faza u procesu istrage digitalnih dokaza: *identifikacija, čuvanje, sakupljanje, pretraživanje, analiza, prezentacija i odluka.*

2.2.4.1. Identifikacija

Identifikacija u ovom modelu predstavlja osiguranje dokazno značajni elektronski zapisa koji su identifikovani, dostupni i upotrebljivi. Od izuzetne je važnosti da procedure budu jasne, a da bi se one uspješno sprovodile, neophodno je razumijevanje pravnih normi. Cilj ove faze je da se napravi dobar odabir objekata, koje treba prikupiti (fizičke i digitalne) uz što detaljnije dokumentovanje i obrazloženje svake sprovedene aktivnosti. Dokumentacija je prisutna u svim fazama istražnog postupka, ali je pri prikupljanju digitalnih dokaza najvažnija zbog uspostavljanja lanca očuvanja integriteta zapljenjenih dokaza. U tradicionalnom kontekstu prikupljanje podrazumijeva "uzimanje predmeta", a u digitalnom kontekstu se vrši prikupljanje predmeta, također ali sa tom razlikom što ti predmeti nose i "određena stanja"[403] koja mogu da se izgube nakon zapljene ili nestabilnosti elektronskih uređaja (npr. slaba baterija, prekid struje itd...).

Također, digitalni dokazi mogu postojati u velikom broju različitih formi: logovi aplikacija, biometrijski podaci, aplikacijski metadata podaci, logovi Internet servis provajdera, firevall logovi, proksi logovi, logovi mrežnog prometa, logovi sistema za detektovanje upada u sistem, sadržaji podataka iz baze podataka i logovi transakcija, logovi audit programa i mnogi drugi logovi. S obzirom na sve ovo identifikacija svih dostupnih digitalnih dokaza, nije nimalo lagan zadatak. Da bi se proces zapljene što efikasnije izveo, publikovani su i vodiči u kojima su dati praktični savjeti i principi koji su od koristi onima koji se bave digitalnim dokazima. Jedan od njih je "Electronic Crime Scene Investigation: A Guide for

[403] Ta stanja su zapisana u RAM memoriji (engl. Random Access Memory) računara koja sadrže podatke o procesima, informacije o stanju mreže, konekcije sa udaljenim računarom kao i mnoge druge. Kada dodje do isključenja sistema trenutni sadržaj RAM memorije je izgubljen i može samo dio informacija da se povrati.

First Responders"[404] publikovan od strane US Department of Justice 2001. godine u USA kao i „Forensic Examination of Digital Evidence: A Guide for Law Enforcement“ publikovan 2004. godine u USA (Ncjrs, 1999).

2.2.4.2. Prikupljanje i pohrana podataka

Forenzička pohrana naziva se i bitstream slika, zbog toga što predstavlja identičnu bit-po-bit kopiju originalnog dokumenta, datoteke, particije, slike, fotografije ili diska. Prikupljanje podrazumijeva osiguranje i pohranu osjetljivih digitalnih dokaza (dokazi koji se lako mogu izmijeniti ili nestati). Važni koraci kao što su izolovanje sistema od mreže, prikupljanje osjetljivih podataka (koji se mogu izgubiti prilikom isključivanja sistema) identifikovanje sumnjivih procesa na sistemu. U ovoj fazi pravi se kompletna forenzička kopija fizičkog sistema (mirror) na forenzičkom računaru, čime se realizuje pohrana kompletnog digitalnog krivičnog mjesta. Ove forenzičke kopije sadrže cjelokupno digitalno mjesto krivičnog djela za razliku od običnog backup-a koji čuvaju samo dodjeljene podatake (engl. allocated) u digitalnom mjestu krivičnog djela.

U zavisnosti od tipa istrage originalni hard disk može da bude čuvan kao fizički dokaz sve do završetka postupka, a može poslije postupka replikacije biti vraćen u produkciju, ako su u pitanju kritični sitemi. Ova faza je odgovorna za preduzimanje potrebnih mjera kako bi se sačuvali integriteti fizičkih i digitalnih dokaza odnosno njihova nepromjenjivost. Za uspjeh ove faze bitnu ulogu imaju alati i metodi koji se koriste, kao i sama stručnost istražitelja jer se u krivičnom postupku, uglavnom, pokušava to osporiti od suprotne strane. Veliki se broj stručnjaka digitalne forenzike slaže da od ove faze počinje prava digitalna istraga. U ovoj fazi se pravi veći broj dupliranih kopija digitalnih dokaza iz svih izvora, dok se originalni materijal katalogizira i smješta u kontrolisano okruženje u neizmjenjenom stanju. Kopija dobijena odgovarajućim forenzičkim alatima koje smo spomenuli u radu je identična kopija originalnog materijala koja služi za pregledanje ispitivanje i analize u daljim fazama digitalno forenzičke istrage.

2.2.4.3. Pretraživanje

Ukoliko se zna što se otprilike traži, moguće je naravno uvjek lakše nastaviti ovu fazu npr. pretraga po ključnoj riječi, internet pošta (web-mail) "kolačići" (cookies) datumu nastanka ili zadnje promjene datoteka itd... U fazi pretraživanja pronalaze se očigledni djelovi digitalnih dokaza koji odgovaraju tačno određenoj vrsti protivpravne aktivnosti. Ponekad se ova faza izvodi i direktno na terenu (iako je preporuka da se ova faza realizuje u forenzičkoj laboratoriji) da bi se utvrdilo da li je potrebno da se sistem donosi na punu forenzičku analizu i u tom slučaju sistem se podiže u sigurnom okruženju pomoću

[404] 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, dostupno na adresi https://www.ncjrs.gov/pdffiles1/nij/187736.pdf

butabilnog DVD/CD/USB, da bi digitalni dokazi ostali nepromijenjeni. Naprimjer, ukoliko se radi o dječijoj pornografiji, istražni organi će prikupiti sve grafičke slike sa sistema i identifikovaće one koje bi predstavljale potencijalne dokaze. Ukoliko se radi o neovlaštenom upadu na server, istražni organi će tražiti očigledne znakove rootkit instalacija, pregledali bi se logovi aplikacija i vršila bi se pretraga za novim konfiguracionim datotekama. U zavisnosti od vještine osumnjičenog, za protivpravne aktivnosti istražitelji će izvršiti procjenu potrebnih tehnika koje će primjeniti u istrazi.

2.2.4.4. Analiza digitalnih dokaza

Cilj analize digitalnih dokaza jest pronalazak i povezivanje činjenica, njihova interpretacija te prezentacija zaključaka i pronalaska. Ova faza podrazumijeva vrlo detaljnju pretragu padataka koji su identifikovani u prethodnim fazama, te se vrše detaljani pregledi podataka kao što je tekst i njegovo značenje, te specifični formati audio i video zapisa. Ova faza ima i svoje podfaze : Fuzija i povezanost - Tokom istrage, podaci (informacije) se prikupljaju iz mnogih izvora (digitalnih i nedigitalnih). Sami za sebe podaci ne mogu da prenesu priču o istraživanom događaju, već moraju da se fuzionišu da bi se sklopila cijela priča. Primjer fuzije može predstavljati vremenski okvir nekog događaja ili radnje koji se odnosi na određeni slučaj odnosno incident. Svaka protivpravna aktivnost ili incident posjeduje hronološku komponentu gdje događaji ili radnje traju tačno određeni vremenski period. Ovim se dobijaju odgovori na gdje, kada i ponekad, kako se desio forenzički relevantan događaj (Caloyannides, 2004).

2.2.4.5. Prezentacija

Forenzički stručnjak mora na jednostavan način obrazložiti rezultate istrage vodeći računa o tome da se isti mogu ponoviti ili da neko drugi može doći do istih zaključaka. Izvještaj povezuje zaključke analize, dokaze i dokumentaciju, te sadrži vrijeme i datum analize i detaljan opis rezultata. Stvaranje izvještaja je najvažnija faza digitalne forenzike i treba sadržavati detaljnu dokumentaciju alata, procesa i metodologije. Složenost izvještaja ovisi o njegovoj namjeni. Kada je istraga zaključena i slučaj predat sudu, rezultati istrage se prezentiraju odvokatima, tužilaštvu, sudiji ili poroti. Nekada od načina prezentacije umnogome zavisi i tok cijelog slučaja, gdje forenzičar mora biti u stanju na jednostavan način obrazložiti rezultate, a nerijetko odvokati, suci, tužilac ili porota prolaze osnovne kurseve računarske forenzike kako bi što kvalitetnije mogli sudjelovati u sudskom procesu.

2.2.4.6. Odluka

Digitalna forenzika ima isti cilj kao i klasična forenzika, a to je sastaviti istinitu verziju događaja potkrijepljenu dokazima. Ključ provođenja digitalne forenzičke istrage je ne samo postaviti prava pitanja, već i znati interpretirati način na koji računar odgovori na pitanja (Volonino i Anzaldua, 2008). Kao krajnji korak provedenog prikupljanja informacija i

obavljene analize je dokument i odluka vještaka čiji je važni dio jasno napisan u kojemu se povezuju do sada prikupljeni i analizirani podaci u cjelovitu priču. Ako se npr. radi o kriminalu u kojem su ukradene kreditne kartice neke banke, onda se svaki broj računa koji je pronađen mora navesti u izvještaju, a sud će na temelju svih rezultata vještačenja i cjelovite priče donijeti odluku.

3.**Perspektive digitalne forenzike u BiH**

U borbi protiv sajber kriminala prije svega se treba usredočiti na stvaranje pravnih ali i tehničkih preduslova, kao što je primjena i razvoj digitalne forenzike. Kao mudar odgovor za ovaj trend potrebno je pristupiti izgradnji preventivnih mehanizama i ulaganja u naučnu disciplinu kao što je digitalna forenzika. Velika važnost digitalne forenzike ogleda se u situacijama kada se već i dogodio sajber napad, koji nismo uspjeli spriječiti ni mjerama informacijske sigurnosti. Tada nam je digitalana forenzika od velike koristi, jer nam pomaže da pronađemo počinitelje i ono što se dogodilo, te identificira osobe odgovorne za napad pomoću dokaza.

Grafikon 2 : Rangirani oblici organizovanog kriminala kojima vlast treba da daje prioritet *Izvor: Centar za sigurnosne studije, Sarajevo - Studija o organizovanom kriminalu u Bosni i Hercegovin.i*

Kako se na grafikonu 3. može primijetiti, građani smatraju da se manje pažnje u definisanju prioriteta djelovanja u predstojećem periodu treba posvetiti aktivnostima

usmjerenim protiv zloupotrebe autorskih prava i kompjuterskog kriminala. Prema stavovima ispitanika, borba protiv kompjuterskog kriminala za Bosnu i Hercegovinu je trinaesti prioritet u budućem djelovanju vlasti. Ovo su pokazatelji koliko građani, a samim tim i odgovorni, a nestručni ljudi iz ove oblasti, smatraju koliko je važna ili bitna borba protiv sajber kriminala u širem kontekstu i koliki negativan efekat može proizvesti po društvo i privredu.

Istina je da koliko god uložili u sajber sigurnost, to ne znači da će informacijski sistem biti u potpunosti siguran te da smo oslobođeni problema. Međutim, tu opasnost možemo svesti na najnižu moguću mjeru uvodeći sisteme digitalne forenzike. Ipak moramo imati na umu da ni tada nismo sigurni. U Bosni i Hercegovini do sada nije provedeno relevantno i sveobuhvatno istraživanje o pojavnosti i rasprostranjenosti ovog kriminala. Zato se mora reći da je u sigurnosnom smislu Bosna i Hercegovina nedovoljno istraženo područje. Bosna i Hercegovina nema ni strategiju, dok se određene institucije bave otkrivanjem sajber kriminala i sajber sigurnosnih prijetnji. Vijeće ministara još nije usvojilo Akcioni plan za formiranje BIH CERT-a (Computer Emergency Response/Readiness Team – Tim za odgovore na računarske incidente). Izvještaji o krivičnim djelima koje pripremaju organi za provođenje zakona u Bosni i Hercegovini se ne odnose na sajber kriminal. Oni ne daju tačne podatke o broju slučajeva, istragama ili osumnjičenima. Digitalna forenzika i druga tehnička sredstva za borbu protiv sajber kriminala na državnom i međunarodnom nivou su ograničena i nedovoljna. Direkcija za koordinaciju policijskih tijela je određena kao stalno dostupna kontakt tačka 24 sata svih sedam dana u skladu s Konvencijom o sajber kriminalu (Budimpeštanska konvencija), ali za to nedostaju potrebni kapaciteti. Na više mjesta u radu je naglašeno kako se u slučaju primjena digitalne forenzike radi o veoma mladoj naučnoj disciplini, koja svoje opravdanje u investiciona ulaganja imaju u jednoj činjenici, a to je otkrivanju počinioca sajber kriminala. Osnivanje i djelovanje tima za digialnu forenziku zahtijeva znatna sredstva. Potrebno je osigurati osim radnog prostora, opreme, i aktuelne programske alate s nužnim nadogradnjama, te stalno školovanje osoblja. Korišteni programski alati obično trebaju biti licencirani, bilo na ime agencije ili članova tima koji ju koriste.

U razvoju digitalne forenzike najvažniju ulogu imaju ljudski resursi. To podrazumijeva da bi zaposleni morali prvenstveno biti obrazovani sa iskustvom i da stalno rade na sopstvenom usavršavanju koje svakako nije samo iz oblasti informatike. To bi morali biti ljudi čije je znanje na vrlo visokoj ljestvici pravne regulative i informatike. Sadašnje stanje sajber kriminala u Bosni i Hercegovini zahtijeva da se ova naučna disciplina što brže, a i bolje uključi u sve zakonske propise i naravno da se što hitnije primjenjuje kako na tekuće probleme tako i na rješavanje i otkrivanje problema iz prethodni godina.

Kada je u pitanju valjanost digitalnih dokaza nije sporna ukoliko se slučaj rješava po propisima i metodama digitalne forenzike. Dokazi su mnogo ranjiviji od konvencionalnih fizičkih dokaza i zbog toga se prilikom rukovanja potrebno pridržavati određenih smjernica kako ih se ne bi uništilo ili oštetilo. Da se dokazi mogu lako izgubiti može se uočiti pri gašenju kompjutera i transporta u laboratorij radi provođenja temeljite analize. Svi

podaci nastali tokom rada računara, koji nisu pohranjeni na tvrdi disk, time su nepovratno izgubljeni. Naravno i nestručnim rukovanjem dokazi mogu biti oštećeni i tako obezvrijeđeni u potencijalnom sudskom postupku.

4. Zaključak

Digitalna forenzika će nastaviti da se razvija i postat će sigurno moćna tehnika za otkrivanje digitalnih dokaza. Da bi taj razvoj bio nesmetan potrebno je da ga prati zadovoljavajuća pravna regulativa u Bosni i Hercegovini i da ne predstavlja usporavajući faktor. Zemlje zapadne Evrope i SAD su odavno uočile ovu konstataciju i čine sve da pruže pravnu podršku digitalnoj forenzici.

U regulisanju ovog pitanja Bosna i Hercegovina daje određene napore, međutim nedovoljno, iz više razloga. Nadu budi prijedlog zakona o organizaciji i nadležnosti državnih organa za borbu protiv sajber kriminala kojim je predviđeno obrazovanje posebnih organizacionih jedinica koje bi se bavile krivičnim djelima predviđenim tim zakonom. Vjerovatno kao posljedica ovog prijedloga zakona, postoje informacije da će biti formirano posebno odjeljenje policije koje bi se bavilo sajber kriminalom i digitalnom forenzikom (trenutno radi SIPA i njihova Agenciji za forenzična ispitivanja i vještačenja - AFIV), kao i određene aktivnosti FUP. Dok se to sve ne ozvaniči ostaje konstatacija da kasnimo za razvijenim informatičkim državama i da bi se trebalo unaprijediti postojeće stanje. Dok se ne donesu pravni mehanizmi nama ostaje da radimo na unapređenju postojeće metodologije i tehnika. Problem sajber kriminala je kompleksan fenomen. Da bi se zaustavilo moguće širenje sajber kriminala, u zvaničnoj istrazi neophodno je uspostaviti multidisciplinarne timove za istragu, koji se sastoje od digitalnog forenzičara, pripadnika organa unutrašnjih poslova i tužilaštva. Za dokazivanje ovih elemenata neophodno je sprovesti adekvatne istražne radnje, analizirati način, vrijeme izvršenja djela i obim štete pomoću tehnika i alata digitalne forenzike i uspješno procesuirati ta djela u pravnom sistemu. U svemu tome najznačajniji doprinos ima upravo digitalna forenzika kao naučna disciplina koja daje precizne odgovore na pitanja koja se postavljaju kako u rješavanju problema izazvanih kompjuterskim kriminalom tako i u postupku preventivne zaštite mreže i kompjuterski sistema. Digitalna Forenzika nije samo svojstvena agencijama za sprovođenje zakona, nego je njena primjena danas velika i u organizacijama i poduzećima, gdje je potrebno uz metode digitalne forenzike, utvrditi neke činjenice, te dokazati na sudu dokaze koji trebaju biti prihvaćeni. Iako se digitalni dokazi , do prije nepunih nekoliko godina u našem okruženju , nisu niti priznavali u sudskim procesima, danas je situacija sasvim drugačija, jer ovi dokazi ukoliko se prikupe, i obrade spomenutim metodama, te prezentiraju uz pomoć propisanih procedura koji se forenzičari moraju da drže, tada su dokazi ravnopravni sa ostalim materijalnim dokazima.

Ovaj rad je nadamo se obezbjedio dovoljno detaljan opis najznačajnijih aktuelnih kretanja iz digitalne forenzike te može biti primjenljiv i koristan kako studentima za dalja istraživanja iz ovih oblasti, tako i stručnjacima iz sigurnosnih agencija i pravosuđa.

5. Literatura

- Albert J. Marcella i Robert S. (2002). *Greenfield Cyber Forensics,* CRC Press LLC
- Babić, V. (2009). *Kompjuterski kriminal,* Metodologije kriminalističkih istraživanja, razjašnjavanja i suzbijanja kompjuterskog kriminaliteta, Sarajevo.
- Beebe N. L. i Clark J. G. (2005). *A hierarchical*, objective-based framework for the digital investigations process, In Proceedings of the 2005 Digital Forensics Research Workshop. Bajraktarević M.iI Porobić M. (2012). *Cyber crime, pranje novca i finansijske istrage* – Sarajevo.
- Bunting S. i Wei W. (2006). *EnCase Computer Forensics*: The Official EnCE: EnCase Certified Examiner Study Guide, Indianapolis, IN: Wiley Publishing
- Caloyannides M. A. (2004). *Privacy Protection and Computer Forensics Second Edition*, Artech ouse Inc.
- Carrier B. (2002). *Open Source Digital Forensics Tools* - The Legal Argument, @tstake.
- Dragičević, D. (2004). *Kompjuterski kriminalitet i računarski sistemi*, Zagreb.
- Dowling., A. (2006). *Digital Forensics*: A Demonstration of the Effectiveness of The Sleuth Kit and Autopsy Forensic Browser.
- Kruse II G. W. i Heiser G. J. (2010). *Computer Forensics Incidend response essentials*, 14th printing, New York: Addison Wesley.
- Kipper G. (2007). *Wireless crime and forensic investigation*, Auerbach Publications Taylor & Francis Group.
- Leschke T. R. (2010). Shadow Volume Trash: *Recycle Bin Forensics for Windows 7 and Windows Vista Shadow Volumes,* U.S. Department of Defense Cyber Crime Institute.
- Milosavljević M. i Grubor G. (2009). *Istraga kompjuterskog kriminala metodološka* – tehnološke osnove, Univerzitet Singidunum, Beograd.
- McClure S., Scambray J. i Kurtz G. (2006). *Hakerske tajne*: zaštita mrežnih sistema, prevod petog izdanja, Mikro knjiga, Beograd.
- Prlja D. (2017): *Cyber kriminal*, predavanje održano na Pravnom fakultetu Univerziteta u Beogradu, 16.11.2017, dostupno na http//www.prlja.info/sk2008.pdf
- Rubin, J. (2003). *Teacher, doctor nabbed in porn probe Police make plea for resources to stop spread of 'evil'*, Staff reporter thestar.com, with files from Canadian press.
- Schweitzer D. (2003). *Incident Response* - Computer Forensics Toolkit, Wiley Publishing, Inc, Indianapolis
- Volonino L. i Anzaldua, R. (2008). „*Computer Forensics*",Wiley publishing.
- William D., Dopatka, A., Hills, M., Ginette L. i Nash, V. (2011). *Freedom of connection* – Freedom of expression The Changing Legal and Regulatory Ecology Shaping the Internet,
- Konvenciju o Sajber criminalu Vijeća Europe od 23.novembra 2011.godine („Službeni glasnik BiH",broj 06/06 Međunarodni ugovori), Član 1. stav 1.pod a).

- Krivični zakon Federaciji Bosne i Hercegovine,Službene novine Federacije BiH, broj 34/03, Sarajevo , 2003. godine.
- Krivični zakon Republike Srpske, Službeni glasnik Republike Srpske, broj 49, Banja Luka, 2003 godine.
- Krivični zakon Brčko Distrikta , *(Službene glasnik Brčko DC, broj 10/03),* 2003 godine.

Dokumenti i izvještaji:

- Advances in Digital Forensics II: IFIP International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, January 29-February 1, 2006.

Izvori gdje nedostaju autori:

- https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx
- http://www.dedoimedo.com/computers/helix.html 29.01.2015.
- http://www.e-fense.com/h3-enterprise.php 29.01.2015.
- http://www.sleuthkit.org/autopsy/v2/ 20.03.2015.
- http://www.emarketer.com/Article/Internet-Hit-3-Billion-Users-2015/1011602 15.9.2014
- http://www.scmagazineuk.com 20.02.2015.
- http://www.mediarecovery.pl/doc/encase-forensic/Detailed_Product_Description.pdf 17.03.2015.
- https://www.ncjrs.gov/pdffiles1/nij/199408.pdf