KOMPJUTERSKA FORENZIKA – ŠIROKI ASPEKTI PRIMJENE
COMPUTER FORENSICS - BROAD ASPECTS OF ITS APPLICATION

Ćosić Jasmin, *Ministarstvo unutrašnjih poslova Unsko-sanskog Kantona, Bihać*
Bača Miroslav, *Sveučilište u Zagrebu, Fakultet organizacije i informatike, Varaždin, Republika Hrvatska*

Sadržaj – *Kompjuterska forenzika je grana forenzičke nauke, koja se bavi legalnim metodama prikupljanja i obradom digitalnih dokaza pohranjenih na računaru (ili drugom nosiocu digitalnih podataka). Kompjuterskom forenzikom se ispituju svi mediji za pohranu i prenos podataka u cilju pronalaženja i analiziranja dokumentacije ili drugih digitalnih dokaza, a vezano za neke nelegalne aktivnosti. Danas je pojam kompjuterska forenzika prerastao u digitalna forenzika , jer se pored računara kao sredstva izvršenja, sve više pojavljuju i drugi digitalni uređaji kao što su digitalni fotoaparati, digitalne kamere, mobilni telefoni, pametni telefoni, personalni digitalni asistenti i sl. Digitalna forenzika nije više vezana samo za laboratorije u policijskim i sigurnosnim agencijama, nego je svoju primjenu našla i van tog područja. U ovom radu autori su obradili upotrebu digitalne forenzike, ne samo u agencijama za sprovođenje zakona , nego i u široj upotrebi, internim istragama u firmama, osiguravajućim društvima i bankama.*

Abstract – *Computer forensic is a branch of forensic science, dealing with legal methods of collection and processing of digital evidence stored on a computer (or other digital data carrier). Computer forensics is used to examine all the media for storing and transferring data in order to locate and analyze documents or other digital evidence related to some illegal activities. Today, the term computer forensics evolved into a digital forensics, because along the computer as a tool, the other digital devices such as digital cameras, mobile phones, smart phones and personal digital assistants are used too. Digital forensics is no longer associated only to a laboratory in police and security agencies, but it is also used outside that area. In this paper, the authors describe a digital forensics process, not only in law enforcement agencies, but also in widespread use, internal investigations in companies, insurance companies and banks.*

KLJUČNE RIJEČI: kompjuterska forenzika, digitalna forenzika, digitalni dokazi, kompjuterski kriminal, sajber kriminal

KEY WORDS: computer forensic, digital forensic, digital evidence, computer crime, cyber crime

1. KOMPJUTERSKA/DIGITALNA FORENZIKA

Danas postoji mnogo definicija digitalne forenzike i digitalnog dokaza. Jedna od njih je "digitalna foreznika se može definisati kao primjena nauke i inženjerstva ka rješavanju legalnih problema digitalnih dokaza" [1]. Prema autorima Pollit i Whiteledge [2] "digitalna forenzika je nauka o prikupljanju, čuvanju, ispitivnanju, analiziranju i prezentiranju relevantnih digitalnih dokaza za upotrebu u sudskom procesiranju.
Kompjuterska forenzika, je dio forenzičke nauke koji se odnosi na obradu legalnih dokaza pronadjenih u računara i digitalnim medijima za pohranu podataka.
Sam pojam „forenzika" je nastao od latinske riječi „*forensi"* što znači „*na otvorenom prostoru ili javno*", a što dolazi od riječi „forum" koja upućuje na lokaciju (javne površine koje su se upotrebljavale za sudjenja ili neke druge javne poslove). Značenje je kasnije preraslo u „ znanstveni testovi i tehnike koje se upotrebljavaju za otkrivanje kriminala" [3]

Kompjuterski forenzičari istražuju sve medije za pohranu podataka (FDD,HDD,USB Drives, CD/DVD ROM, Tape drives itd.) u cilju pronalaženja i analiziranja dokumentacije ili drugih digitalnih dokaza. Pojam kompjuterska foreznika se veže za malo „ranije vrijeme" kada nije postojao internet u ovakvom obliku i kada nije postojala globalizacija mreža koju danas imamo. Kada govorima sa aspekta današnjice, govorićemo o „*cyber forenzici"*, jer se mjesto izvšenja krivičnog djela nemože više vezati za računar i stol na kom se taj računar nalazio u momentu izvšenja toga djela. Istrage se proširuju u virtualni svijet, u svijet interneta, mreža, i dalje proširuju na ostale digitalne uređaje (gsm, gps, digitalne fotoaparate, digitalne kamere, „smart" telefone, PDA i sl.)

Pojam "digitalni dokaz" podrazumjeva bilo kakav relevantan podatak dovoljan da dokaže kriminalno djelo na kompjuterskm ili mrežno mediju za pohranu podataka, uključujući uzorke teksta, slike, videa, glasa.
Digitalni kompjuterski dokaz čini gomila posrednih stvarnih dokaza, od kojih se ni jedan ne smije isključiti iz bilo kog razloga. Dokazi moraju biti potpuni, da se međusobno dopunjuju (da su isprepleteni) i da nemaju tzv. pukotina za donošenje zaključaka, odnosno za utvrđivanje čvrstog dokaza[4].

Prema „The Scientific Working Group on Digital Evidence (SWGDE[1])"[5] termin „dokaz" se upotrebljava za „nešto materijalno" što će biti priznato od strane suda. Ono mora biti prikupljeno na legalan i zakonit način. Neki objekat (podataka ili materijalna stvar) postaje dokazom jedino, kada

[1] SWGDE - The *Scientific Working Group on Digital Evidence*

u njega povjeruje službena provedba zakona.Prema istoj organizaciji , pojam digitalnog dokaza predstavlja svaka informacija ili dokaz koji ima vrijednost koja je smještena ili transmitirana u digitalnoj formi.

Kompjuterska forenzika je veoma bitna za uspješno procesuiranje kriminalaca u oblasti kompjuterskog kriminala. Proces digitalne istrage mora otpočeti i svo vrijeme se provoditi na zakonit način . To znači da se tokom cijele forenzičke istrage moraju poštovati određeni principi kako bi digitalni dokaz bio prihvaćen od strane suda. Proces digitalne istrage će biti uspješan ukoliko se poštuju određena pravila.
Danas su mnogi autori razvili modele i okvire za uspješne forenzičke istrage. Najpoznatiji su :

- Lee`s model
- Casey model
- DFRW framework
- Reith, Carr and Gunch model
- Kruss & Heisser model
- USDOJ model
- Ciardhuain Extended model [6]

Karakteristika Lee`s, Casey i DFRW[2] modela je da su bazirani na 3 faze [7]:

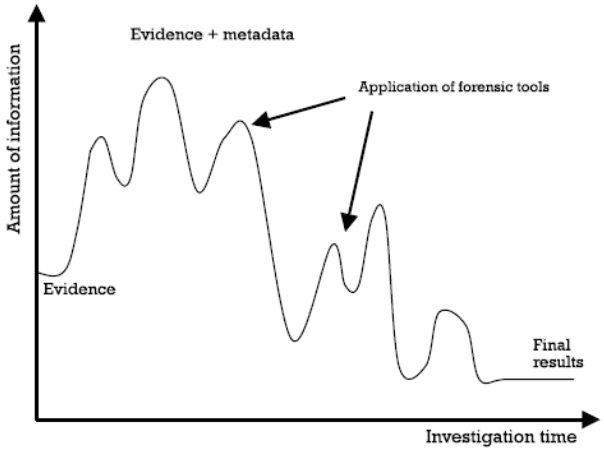
- Indentifikacija (prepoznavanje), prikupljanje i čuvanje
- Ispitivanje i analiza
- Prezetiranje i izvještavanje

Reith, Carr & Gusch i Kohn, Eloff & Oliver [8] su model proširili sa planom i pripremom, te širenjem znanja, dok je Ciardhuaian napravio najkompletniji model koji se sastoji od 13 faza koje su nazvane „aktivnosti“: svjesnost, autorizacija, planiranje, notifikacija, pretraga i identifikacija, prikupljanje, transport, skladištenje, pretraga, hipoteza, prezentiranje, dokazivanje/odbrana, diseminacija[6] .

Svi modeli istražiteljima, sudskim vještacima treba da ponude :

- Prihvaćanje i prihvatljivost
- Pouzdanost
- Ponovljivost
- Integritet
- Uzrok i posljedicu
- Dokumentiranost [7]

Tokom forenzičke istrage moraju biti ispoštovani svih 6 načela. Količina podataka koji se procesiraju je ogromna, pretraga nekada može da traje i danima i sedmicama, analiziraju se terabajti podataka, a da na samom izlazu imamo svega nekoliko megabajta podataka koje mogu pomoći istražiteljima.
Na slici br.1 vidimo odnos između količine podataka koji ulaze u sistem forenzike i podataka koje imamo na izlazu kao rezultat istrage. Evidentno je da se u velikom vremenskom periodu analiziraju ogromne količine podataka, koje u konačnici rezultiraju malim finalnim rezultatom.



Slika 1: Količina obrađenih informacija tokom forenzičke istrage

2. ŠIROKI ASPEKTI PRIMJENE DIGITALNE FORENZIKE

Često se postavlja pitanje zašto je forenziča istraga bitna i koji je vitalni interes za širu upotrebu ? Do prije nekoliko godina “ekskluzivno pravo” na digitalnu forenziku su imale Agencije za provođenje zakona i forenzika je bila vezana za njihove velike skupe i robusne laboratorije. Razvojem internet i IKT-a istrage su su proširile na sajber prostor i mreže, a razvojem tzv.”embeded sistema” kao što su gsm , pametni telefoni, personalni asistenti, gps uređaji , digitalni fotoaparati, digitalne kamere i sl. Nestala je kompjuterska , a nastala digitalna forenzika.

2.1 FORENZIKA U AGENCIJAMA ZA SPROVOĐENJE ZAKONA

Kompjuterski kriminal nije uvijek predstavljao akt kršenja formalnog prava. Prema nekim izvorima [9] prve inicijative da se „upostavi „ pojam kompjuterskog kriminala, datiraju još od 1977 godine, a inicijativa je potekla od U.S. Senate Government Operations Committee-a. Studija je pokušala skrenuti pažnju na nekoliko problema koji se mogu desiti u upotrebi kompjuterskih programa. Interpol [10] je bio prva medjunarodna organizacija koja je se bavila problemom kompjuterskog kriminala i legislative. U izvještaju sa njihove konferenciji 1981.godine, obrađen je problem kompjuterskog kriminala , te legislative, identificirani su potencijalni problemi.

Vijeće Europe je 1985 uspostavilo još jedan komitet sastavljen od eksperata , kako bi se razgovaralo o kompjuterskom kriminalu. 1989.godine donešene su i konkretne preporuke.
UN je 1990.godine donio i rezoluciju o kompjuterskom kriminalu, na 8.kongresu održanom na Kubi. Rezolucija je postala veoma bitan element kod pisanja strategija ili Zakona o kompjuterskom kriminalu u EU, skoro sve zemlje iz Europe su potpisale ovu rezuliciju (BiH je potpisala 2006.godine).

[2] DFRW- *The Digital Forensic Reasearch Working Group*

Potrebu za ovim je nametnula činjenica da je već krajem 70-tih godina već bilo nekoliko stotina (preko 500) krivičnih djela učinjenih uz pomoć računara ili kompjuterskih tehnologija. Sredinom 80-tih nastaje kompjuterska forenzika u SAD , koja se bavi sa prikupljanjem, dokumentiranjem i isporučivanjem „digitalnih dokaza“ za potrebe sigurnosnih agencija i sudova.
90-te donose eskalaciju kompjuterskog kriminala i nastanak pojma „cyber forenzika“.S obzirom na ekspanziju interneta i globalizaciju lokalnih mreža, te nagli razvoj IKT-a s kraja 90-tih godina, klasične laboratorije su postale tijesne za „vještačenja“, te su se forenzičari morali preseliti u cyber prostor.

Znači, nije bilo dovoljno offline pregledavanje „zaplijenjenog“ hardware-a , nego su se počinioci morali hvatati na djelu, znači on-line u vrijeme samog izvršenja. Tako je nastala i „cyber forenzika“, kao kompleksnija i savršenija od kompjuterske forenzike. Njena kompleksnost se ogleda u tome da se sada dokazi pronalaze u kompjuterskim mrežama, na internetu, u drugim dijelovima svijeta. Sve se dešava on-line, na mreži, u realnom vremenu, prate se upadi, zloupotrebe, pregledavanje zabranjeih sadržaja na internetu, dilanje, maliciozno ponašanje software-a, te aktivnost vlasnika takvog software-a.

Koliko je cyber kriminal u svijetu uzeo maha, govori nam podatak da je 2004.godina bila prekretnica i da je u toj godini „zarađeno“ preko 105 milijardi USD putem cyber kriminala , što je mnogo više nego što su prihodi od prodaje droga bili u toj godini .
Po statistikama, najmanje krivičnih djela je iz oblasti „presretanja komunikacija“,dok je najviše „upada u sisteme“ i „širenja virusa i crva“.
Istraživanja koja sprovodi FBI zajedno sa CSI[3], pokazala su da je čak 90 % od ispitanika (korporacija, banaka, vladinog sektora) bilo na neki način izloženo nekoj od vrsta napada. Gubici su izraženi u stotinama miliona dolara. Najveći problem je izazivan širenjem virusa (85 % ispitanika), od toga „svega“ 25% napada došlo je iz vana. Od ukupnog broja ispitanika „svega“ 8% priznalo je da su im ukradeni vazni podaci. Statistički gledano kod 79% od ukupnog broja, problem su napravili uposlenici, koristeći internet u privatne svrhe, skidanjem piratskog software-a odnosno korištenjem elektronske pošte.

BiH je uvidjevši opasnost od širenja interneta i svih ovih opasnosti koje idu sa tim, i obaveza koje je morala ispuniti prema EU, inkriminisala u Kazneni Zakon Federacije BiH i Krivični Zakon Republike Srpske, nekoliko članova koja tretiraju ovu oblast. Na tabelama 1 i 2 vidimo na koji način Krivični zakoni u BiH tretiraju oblast kompjuterskog kriminala. [11]

Tabela 1: Članovi iz Krivičnog zakona FBIH koji tretiraju oblast kompjuterskog kriminala

Član	Djelo	Minimalna kazna	Maksimalna kazna
Član 393	Oštećenje računalnih podataka i programa	Novčana	5 godina zatvora
Član 394	Računalno krivotvorenje	Novčana	5 godina zatvora
Član 395	Računalna prijevara	6 meseci zatvora	12 godine zatvora
Član 396	Ometanje rada sustava i mreže elektronske obrade podataka	Novčana	3 godine zatvora
Član 397	Neovlašćeni pristup zaštićenom sustavu i mreži elektronske obrade podataka	Novčana	5 godina zatvora
Član 398	Računalna sabotaža	1 godina zatvora	8 godina zatvora

Tabela 2: Članovi iz Kivičnog zakona Republike Srpske koji tretiraju oblast kompjuterskog kriminala

Član	Djelo	Minimalna kazna	Maksimalna kazna
Član 176	Neovlašceno korišcenje licnih podataka	Novčana	1 godina zatvora
Član 238	Neovlašceno ulaženje u zašticenu kompjutersku bazu podataka	1 godina zatvora	8 godina zatvora
Član 271	Upad u kompjuterski sistem	6 meseci zatvora	10 godine zatvora
Član 276	Falsifikovanje kreditnih kartica i kartica za bezgotovinsko placanje	Novčana	10 godine zatvora

[3] CSI - *Computer Security Institute*

2.2 FORENZIKA U KORPORATIVNIM ISTRAGAMA

Često se postavlja pitanje u kakvoj su korelaciji Sigurnost informacionih sistema i Digitalna forenzika. Može se reći da digitalne forenzika nastupa kada zakaže politika sigurnosti i kada se desi "upad" u kompjuterski system preduzeća ili kada se desi neki drugi sigurnosni incidente koji narušava politiku sigurnosti IS-a. Često se dešava da korporacije u slučajevima kada zakažu interne istrage i kada se slučaj nemože riješiti iznutra, angažiraju stručnjake za digitalnu forenziku i sudske vještake kao pomoć izvana. U razvijenim zemljama svijeta gdje je veoma rapostranjena industrijska špijunaža, često su tzv. "intruderi" , osobe koje su zaposlene i špijuniraju poduzeća i direktno iz informacionih sistema ciljanih preduzeća šalju izvještaje nalogodavcima. Ovi izvještaji su obično kriptovani, šifrirani ili se koristi steganografija kao metoda izvršenja ovakvih dijela. Ovdje je nužna upotreba digitalne forenzike I angaživanje specijaliziranih stručnjaka na otkrivanju ovih počinitelja.

2.3 FORENZIKA U FINANCIJSKIM INSTITUCIJAMA

Forenzika u financijskim se obično veže za:

- Forezniku u osiguravajućim društvima i
- Forenziku u bankarskom sektoru [12]

Ove institucije veoma često imaju potrebu i interes da se otkriju i procesuiraju izvršioci krivičnih dijela iz oblasti kartičnog poslovanja, auto-osiguranja, medicinskog osiguranja-prevare i falsifikovanje liječničkih nalaza i sl.
Veoma čest slučaju u praksi je falsifikovanje fotografija i nalaza sudskih vještaka u saobraćajnim nesrećama, gdje je pričinjena veća materijalna šteta i gdje se žele izvući veće svote novaca od osiguravajućih društava. Interes bankarskog sektora je brzo otkrivanje i procesuiranje zbog nadoknade štete prestupnika u kartičnom plaćanju, kao i "hacker-a" koji su činili upade u bankarske sisteme sa ciljem nezakonitog sticanja materijalne dobiti. Cilj rekonstrukcije ovih djela je utvrditi na koji nači se djelo dogodilo, te pravilna rekonstrukcija detalja.[13]
Ovdje banke pored policijskih istraga, vode uporedo svoje interne istrage gdje se privatno angažiraju stručnjaci za ovu vrstu forenzike kako bi se slučaj što prije okončao i nadoknadila materijalna šteta.

3. ZAKLJUČAK

Danas računari posjeduju mogućnosti memorisanja ogromnih količina podataka, na personalnim računarima je to reda stotina megabajta, a u poduzećima i firmama i reda terabajta. Forenzičkim metodama se ti podaci prikupljaju, analiziraju i donose se određeni zaključci na osnovu kojih se daju i određene preporuke, zavisno od razloga vođenja istrage. Analiza gomile podataka vremenski i financijski je zahtjevan posao i potrebno je dobro poznavanje problematike, ali i računara i programa koji se koriste.

Forenzika računara nije samo svojstvena Agencijama za sprovođenje zakona (policiji), nego je njena primjena danas velika i u organizacijama i preduzećima, gdje je potrebno uz pomoć naučnih metoda (forenzičkih metoda) , utvrditi neke činjenice, te do i dokazati na način da sudstvo prihvati takve dokaze.
Iako se digitalno dokazi , do prije nepunih nekoliko godina u našem okruženju , nisu niti priznavali u sudskim procesima, danas je situacija sasvim drugačija, te ovi dokazi ukoliko se prikupe, obrade i prezentiraju uz pomoć propisanih procedura, postaju ravnopravni sa ostalim materijalnim dokazima. Razvijene zemlje svijeta , SAD, Japan ali i Europa sve više pridodaju značaja ovoj problematici, i sve više se vrši edukacija sudija, tužioca, te i samih informatičara temama digitalnog dokaza, računarske ali i cyber forenzike.

3. LITERATURA

[1] A.Sammes, B.Jenkinson, Forensic Computing A Practitioners Guide. Springer-Verlag, New York; 2000

[2] M.Pollit, A. Whiteledge, Exploring big Haystacks, Data Mining and Knowledge Management, Advances in Digital Forensic II.IFIP, 2006

[3] S.Peisert ,M. Bishop, K.Marzullo, „Computer Forensics in Forensis" , ACM

[4] *IOCE Princips & Definitions*, IOCE 2. Conference, Marriott Hotel, London, 1999.

[5] Digital Evidence:Standard and Principles: http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm, (pogledano 15.01.2010.g.)

[6] S.Ciardhuain, An extended model of cybercrime investigation, Internation Journal of Computer Science and Network Security, Vol.9 , 2009

[7] E.Casey , Digital Evidence and Computer Crime, San Diego: Academic Press, 2004

[8] M. Kohn ,JHP. Elof , MS. Oliver ,Framework for a Digital Forensic Investigation, Proceeding of the ISSA 2006 from Insight to Forensight Conference, South Africa, 2006

[9] Cybercrime law, A brief history of Computer Crime Legislation, www.cybercrimelaw.net (pogledano 01.10.2009.g.)

[10] Interpol, www.interpol.int, (pogledano 01.12.2009.g.)

[11] J.Ćosić, Kompjuterski kriminal, INFO 119, 2007, str. 96-97

[12] M.Coloyannides, Privacy Protection and Computer Forensics SE, Artech House, 2004

[13] M.Bača, Uvod u računarsku sigurnost, Narodne novine, Zagreb, 2004