Digitalna antiforenzika – manipulacija procesom digitalne istrage

Jasmin Ćosić, *Ministarstvo unutrašnjih poslova, Bihać, Bosna i Hercegovina*, Zoran Ćosić, *Statheros ltd., Kaštel Stari, Hrvatska*

***Sadržaj* — U radu je napravljen pregled i definisana je digitalna antiforenzika, nadolazeća tehnologija koju upotrebljavaju cyber kriminalci kako bi digitalne dokaze prikrili, uništili, promjenili, te time onemogućili zvaničnoj digitalnoj forenzici rješavanje djela iz oblasti kompjuterskog kriminala. Digitalnu antiforenziku koriste i legitimni korisnici koji jednostavno žele da budu ostavljeni na miru u cyber prostoru i zaštite svoju privatnost. U radu će biti predstavljeni neki od alata i metoda koje se koriste u digitalnoj antiforenzici, a u cilju stvaranja okvira za bolje razumjevanje ovog problema.**

***Ključne riječi* — digitalna antiforenzika, digitalna forenzika, enkripcija, privatnost, steganografija, digitalni dokazi**

I. UVOD

Lokardov princip razmjene („Locard exchange princip“), podrazumjeva da bilo tko ili bilo što, što je bilo na mjestu počinjenja djela sa sobom je ponijelo dio mjesta počinjenja djela ili je ostavilo trag svoje prisutnosti. Uvijek je aktuelan trougao žrtva-osumnjičeni-mjesto počinjenja djela [1]. Isti princip se može upotrijebiti i kod krivičnih djela iz oblasti kompjuterskog kriminala.

U ovim slučajevima istražitelji zaduženi za kompjuterski kriminal upotrebljavajući znanstvene metode i alate pokušavaju pronaći dokaze (digitalne dokaze) da je djelo zaista i učinjeno. U ovom poslu im pomaže digitalna forenzika - nauka o prikupljanju, čuvanju, ispitivanju, analiziranju i prezentiranju relevantnih digitalnih dokaza za upotrebu u sudskom procesiranju [2] Kriminalci upotrebljavaju antiforenzičke metode kako bi dokaze prikrili, uništili, promjenili, te time onemogućili otkrivanje ovih djela – digitalnom antiforenzikom se bore protiv procesa digitalne forenzike.

Ne postoji mnogo radova napisanih na ovu temu iz prostog razloga što je još uvijek nejasno što je to antiforenzika ? Nekoliko objavljenih radova je tretiralo ovu oblasti, te su vršene neke analize i pokusi. Digitalna forenzika je nauka - naučna disciplina i kao takva je priznata i prihvaćena u naučnim krugovima, međutim digitalnu antiforenziku koriste najčešće kriminalci i do sada je ostala na nivou tehnike i metoda. Ono što je evidentno, a što se u radovima malo pominje je da se neke od ovih tehnika sve više koristi i u sasvim legalne svrhe. Pri tome se misli na korisnike koji žele iz nekih razloga da ostanu anonimni ili da sačuvaju svoju privatnost u cyber prostoru ili iz jednostavnog razloga žele da dodatno sačuvaju i zaštite svoje lične podatke.

U radu će autor definirati antiforenziku, pobrojati tipove antiforenzike , i na kraju dati pregled alata koji se koriste u ove svrhe.

Jasmin Ćosić, Ministarstvo unutrašnih poslova Unsko-sanskog kantona, 502.V.bbr br.2, 77000 Bihać, Bosna i Hercegovina (telefon: +387/61/790-484, e-mail: jasmin.cosic@mupusk.gov.ba)

Zoran Ćosić, Statheros ltd., Kaštel Stari, CEO, e-mail: zoran.cosic@statheros.hr

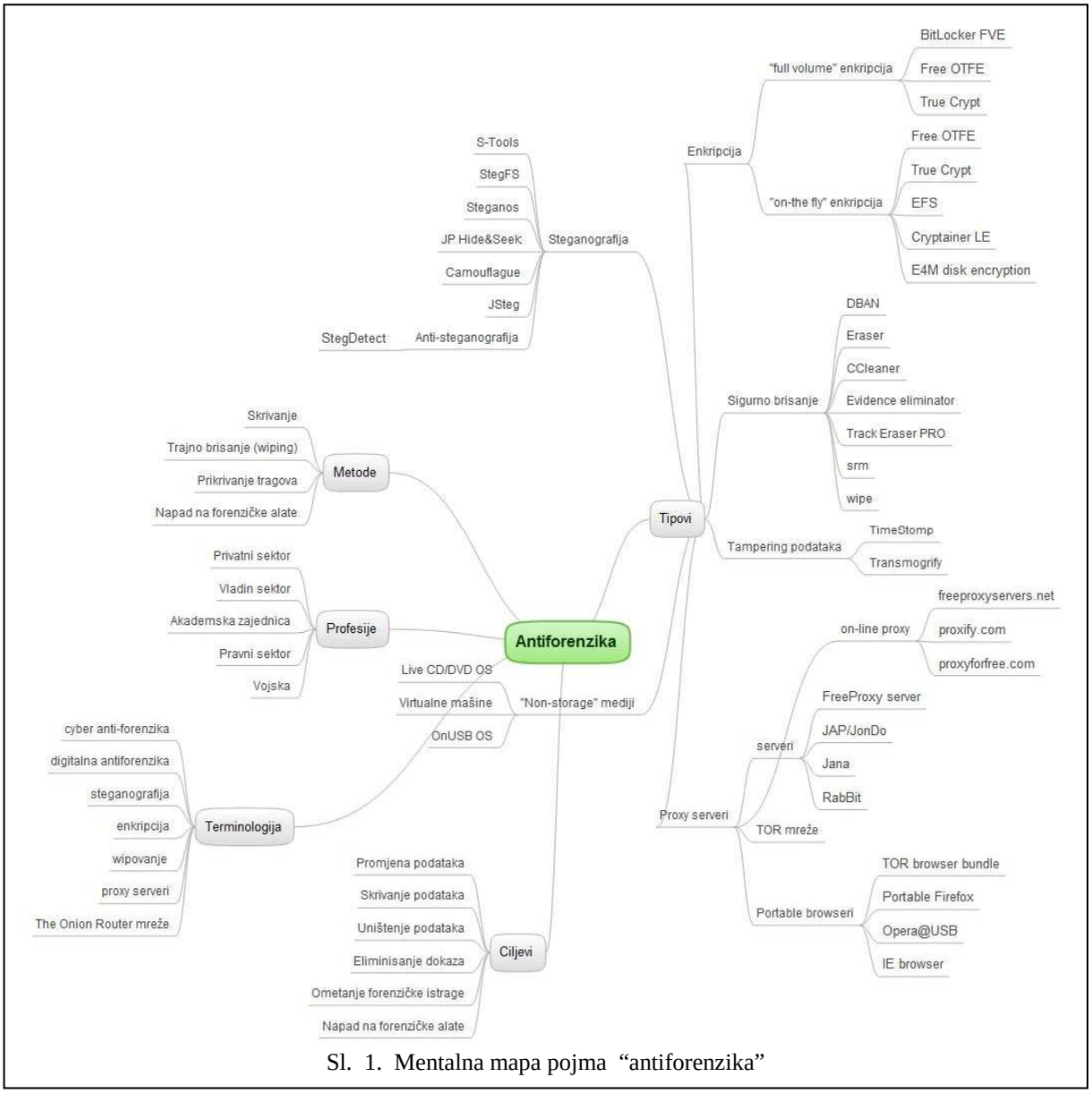
II. DEFINICIJA ANTIFORENZIKE

Ne postoji jasna i koncizna definicija digitalne antiforenzike. Neki autori su se bavili ovim problemom u posljednjih nekoliko godina, te su definirali antiforenziku sa aspekta i na osnovu definicije digitalne forenzike. Tako je prema [3] digitalna antiforenzika metoda koja se upotrebljava za prevenciju (ili protiv) naučnih metoda koje se upotrebljavaju u građanskom ili krivičnom zakonodavstvu, a koje se provode od strane policijskih agencija u kriminalno-pravnom sistemu [3]. Neki autori definiraju antiforenziku kao „jednostavan alat za razbijanje ili izbjegavanje detekcije“ [4] Peron i Legarty [5] definiraju digitalnu antiforenziku kao proces limitiranja identifikacije, prikupljanja, upoređivanja i provjere valjanosti elektronskih podataka, u cilju sprečavanja kriminalističke istrage. Za digitalnu antiforenziku se može reći da je to set taktika i mjera koje poduzima netko tko želi da osujeti proces digitalne istrage [6].

Ukoliko promatramo digitalnu antiforenziku sa aspekta osnovne namjene, a ne udaljavajući se pri tom od činjenice da se radi o tehnikama i tehnologiji možemo reći da je digitalna antiforenzika: *skup metoda i tehnika čija je osnovna namjena kompromitovanje procesa digitalne forenzike, manipulacija sistemom, te narušavanje integriteta digitalnih dokaza.*

III. METODE I ALATI

Prvobitna namjera digitalne antiforenzike je bila skrivanje, promjena, zaštita i uništenje podataka (potencijalnih digitalnih dokaza) , te ometanje samog procesa digitalne forenzike napadom na forenzičke alate.



Sl. 1. Mentalna mapa pojma "antiforenzika"

Gledajući sa tog aspekta metode i alati se mogu podjeliti na:

1. *Steganografija*
2. *Kriptografija*
3. *Sigurno brisanje podataka*
4. *Tampering podataka i napad na forenzičke alate*
5. *Skrivanje iza proxy-ja*

A. Steganografija

Nastanak i prva upotreba steganografije seže još u daleku prošlost u vrijeme starih Grka. Sam pojam predstavlja kovanicu riječi *steganos* (grčki prikriveno) i *graphein* (grčki pisati), što bi u prevodu značilo "*skriveno pisanje*". U to vrijeme, kada su željeli poslati skrivenu poruku, stari grci bi glasniku obrijali glavu, na nju istetovirali poruku, zatim čekali da mu naraste kosa i onda ga slali da na taj način prenese tajnu poruku. U II svjetskom ratu se upotrebljavala "nevidljiva" tinta sačinjena od voćnog soka, urina, mlijeka ili vinskog sirćeta sa kojom su se pisale poruke koje su trebale biti nevidljive. Kada bi se papir na kom je napisana takva poruka zagrijao, tinta bi potamnila i poruka bi bila čitljiva. Proces steganografije se odvija na taj način da se skrivena poruka umetne u neki transportni posrednik, koji se zove nosilac. Skrivena poruka je proširena u nosiocu i formira se steganografski posrednik. Nakon toga se dodaje steganograski ključ kako bi se fajl dodatno kriptovao [7]. Dodatno, TCP/IP protocol ima određene slabosti koje se mogu iskoristiti za tzv."prikriveno komuniciranje" putem privatnih ili čak

javnih mreža. Ove propuste u protokolu koriste zlonamjerni korisnici koji prenose tajne poruke, a ne žele da budu otkriveni. Antiforenzički alati koriste razne metode i mehanizme skrivanja. Neki skrivaju podatke u tzv."slack" i "nealociranom" prostoru na hard-disku računara, dok drugi koriste kriptovane ili skrivene particije ili čak emuliraju tzv."bad sektore" i tu skrivaju podatke. Danas postoji na desetine alata za steganografiju, za svaki operativni system, a najpoznatiji su S-tools, StegFS,Steganos, JPHide&Seek.

B. Kriptografija

Za razliku od steganografije, kriptografija se koristi za dodatno šifriranje a ne skrivanje podataka. Za podatke se zna da su tu ali su bez upotrebe posebnog ključa nečitljivi i neupotrebljivi. Za kriptografiju se u forenzičkoj praksi smatra da je prava noćna mora za forenzičare. Danas mnoge aplikacije već same po sebi imaju određene alate za šifriranje datoteka, ali najčešća podjela profesionalnih alata je na tzv. alate za šifriranje „u letu" (*on-the fly*) i alate za „potpuno šifriranje" (*full encryption*). Razlika je u tome što su tzv. alati za širfiranje u letu ili alati za šifriranje u realnom vremenu mnogo brži i jednostavniji za korištenje - pristup datoteci je moguć odmah nakon unosa ključa, dok se kod potpune enkripcije šifrira cijeli disk i to bit po bit što ponekad zna biti jako sporo i oduzima mnogo dragocjenog vremana. Najčešće korišteni alati za šifriranje „on the fly" su: FreeOTFE, TrueCrypt, EFS, Cryptainer LE, dok su tzv. FVE („Full Volume Encryption") alati: TrueCrypt, BitLocker FVE, FreeOTFE.

Kriptovana internet bazirana komunikacija (SecureSockets Layer, Transaction Layer Security, virtual private networks, IEEE 802.11 secure wireless networks) može učiniti analizu saobraćaja i sadržaja koji se prenose tim kanalima skoro nemogućom [8] te je stoga zlonamjerni korisnici koriste veoma često.

C. Trajno brisanje podataka

Alati i metode za trajno brisanje podataka postoje već godinama još iz doba DOS-a i UNIX-a. Suština rada svih je da se baziraju na jednom od mnogih algoritama koji na prostor gdje se nalaze (ili su se nalazili) podaci, prepisuje slučajni niz 1 i 0 i to od 1 – 35 prolaza. Postoji mnogo sigurnosnih standarda koje je nametnula SAD, Canada, Njemačka, ali i Rusija i druge razvijene zemlje, a svakako su najpoznatiji *Bruce Schneier's algorithm, Canadian OPS-II, DoD 5220.22 M, Gutmann's algorithm, German VSITR ali I Russian GOST p50739-95, US Army AR380-19 S Air Force 5020.*

Svi današnji programi koji su dostupni na internetu koriste neke od pobrojanih algoritama. Prema nekim tvrdnjama dovoljan je 1 prolaz preko diska sa ovim programima I podaci su nepovratano izgubljeni. Većina algoritama podržava prepisivanje 3-7 puta, dok Gutmanov algoritam podržava 35-struko prepisivanje slučajnih sadržaja (0 I 1) preko mjesta na disku gdje su se nalazili obrisani podaci. Gutmanov algoritam je možda i najnapredniji jer se sastoji iz čak 35 prolaza i osigurava punu zaštitu od vraćanja obrisanih fajlova, ali cijena koja se ovdje mora platiti je vrijeme potrebno za ovu operaciju. Neki od poznatih programa su : *Acvite@KillDisk, Secure Erase, Eraser, Data Wiper Advanced File Shredder , DBAN (Darik s boot and nuke).* Programe je moguće koristiti za brisanje cijelog hard-diska, dijelova prostora na disku, čak i slobodnog, nealociranog prostora na kojem trenutno nema podataka (gdje ih je bilo ranije) [9].

D. Napad na forenzičke alate

Ova metoda podrazumjeva napade i varanje alata koje koriste forenzičari u digitalnim istragama, na način da se sakriju aktivnosti, promjene neke sistemske vrijednosti na računaru i sl. Jedan od načina je korištenje alata koji brišu sve tragove aktivnosti korisnika kako na računaru, aplikativnim programima, tako i na internetu. Programi kao što su *Evidence eliminator, TrackEraser, Window Washer* potpuno uklanjaju sve tragove aktivnosti korisnika – historiju browsanja, keš memoriju, slack i nealocirani prostor na disku. Ovim se onemogućuje pronalaženje ovih aktivnosti od strane istražitelja zaduženih za digitalne istrage. Također, čest slučaj u praksi je i korištenje alata za promjenu sistemskog datuma i vremena kreiranja, modificiranja, pristupa i ažuriranja fajlova na NTFS sistemu. U ove svrhe se koristi veoma opasan alat *"TimeStomp"*[1] koji veoma lako može da zavara i najpoznatije alate za digitalnu forenziku i učini digitalne dokaze neprihvatljivim od strane suda.

Program *"Transmogrify"* omogućava korisniku da mjenja zaglavlje datoteka, tako da je moguće zaglavlje .jpg slike staviti u .doc fajl ili obrnuto, a u cilju zavaravanja rada *EnCase, FTK* ili drugih forenzičkih programa.

Još jedan način onemogućavanja rada forenzičkih alata je skrivanje podataka u tzv. "slack" prostor na hard disku. Za ove svrhe se koristi alat *"Slacker"*.

E. Proxy serveri i anonimnost

U digitalnim istragama pored kompjuterske forenzike, veoma čest je slučaj da se informacije traže i od davaoca internet usluga – ISPa. Najčešće je potrebno saznati IP adresu računara za koji se sumnja da je korišten u nelegalne svrhe. U cilju skrivanja stvarne IP adrese koja im je dodjeljena od strane lokalnog ISPa, zlonamjerni korisnici veoma često koriste proxy servere. Umjesto da se direktno pristupa serveru na kom se nalazi traženi resurs na internetu, ovom metodom se istura proxy server i njegova IP adresa, dok stvarna adresa korisnika ostaje zaštićena (zna je samo proxy). U cilju još jače zaštite koriste se i nizovi proxy servera.

Čest slučaj je da se koriste on-line proxy serveri , od kojih su napoznatiji (*proxify.com, freeproxyservers.net* i sl.) ali i serveri koji se instaliraju lokalno na računarima (*Jana, FreeProxyServer, RabBit* i sl.)

F. TOR, Portable browseri i operativni sistemi

Jedan od načina koji se koristi kako u antiforenzičke svrhe tako i u legalne svrhe a u cilju sačuvanja privatnosti i anonimnosti prilikom surfanja na internetu je TOR (*The*

[1] „TimeStomp" – je program koji je dio „Metasploit Framework-a", a čija je namjena promjena originalnog „time-stampa" u NTFS fajl sistemu.

Onion Router). TOR je mreža virtualnih tunela – otvorena i slobodna mreža koja pomaže u borbi protiv tzv.“analize saobraćaja“ [10]. Ideja TOR mreža je da se koriste rute koje je teško pratiti i da se nakon određenog vremena brišu „otisci prstiju“. Svaki puta se kreira nova ruta među korisnicima TOR-a i time se onemogućava snifanje , presretanje paketa i analiza takvog saobraćaja. TOR danas ima dvojaku funkciju, koriste ga cyber kriminalci ali i legitimni korisnici (*novinari, blogeri, vojska, vladine agencije i institucije*) a sa ciljem sačuvanja konzistentnosti i zaštite kako IP adresa, tako i privatnosti.

Danas je veoma čest slučaj i korištenje tzv. mini ili portable browsera koji se pokreću sa USB memorijskih čipova ili MMC/SD memorijskih kartica. Ovim se omogućuje da se browser pokreće i kompletan softver se nalazi u radnom memoriji (RAM) računara, što znači čim se završe aktivnosti na internetu i USB memorija odvoji od računara , nestaju i eventualni tragovi. Danas postoji na desetine ovakvih browsera a najpoznatiji su : *TOR browser bundle, Portable Firefox, Portable IE, Opera@USB* i sl. Svi omogućavaju tzv. „silent mode„ ili „private browsing“.

U cilju dodatne zaštite koriste se i posebne tzv.“LIVE“ verzije operativnih sistema. Suština funkcioniranja takvih operativih sistema je da se isti ne istaliraju lokalno na računaru (na tvrdom disku računara), nego se pokreću direktno sa CD/DVD medija ili nekog drugog prenosnog medija (USB stick, MMC, SD ili neka druga prenosna memorija), te se kompletni izvršavaju i nalaze u RAM memoriji računara. Gašenjem računara brišu se svi tragovi ikakvih aktivnosti na računaru i skoro pa je nemoguće pronaći ikakav dokaz na takvom sistemu. Najčešće su verzije raznih Linux distribucija (*Knoppix, BackTrack, Ubuntu, Fedora,SuSe,Windows PE, Anonym.OS* i sl) . Potpuniji pregled se nalazi na [11]

IV. ZAKLJUČAK

Ovim radom se pokušala skrenuti pažnja na metode i alate koje čine antiforenziku, pobrojani su i opisani neki-najvažniji dok se iz dana u dan razvijaju sve noviji i sofisticiraniji alati. Cilj je bio da se definiraju pojmovi i napravi pojašnjenje kako bi se indvidualno mogao kreirati okvir za eventualno bolje razumjevanje ili borbu protiv ovih metoda. Daljnji rad i istraživanje će biti usmjereno na razvoj strategije za borbu protiv ovih alata i metoda.

LITERATURA

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

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

[3] R.Harris, „Arriving at an anti-forensic consensus:Examination how to define and control the anti-forensic problem“, Digital investigation 3S, ELSEVIER, p.44-49 , 2006.

[4] LC.Fosters, V.Liu, Catch me if you can...In:Blackhat briefings 2005, dostupno na www.blackhatcom/presentations/bh-usa-05/bh-us-05-foster-liu-update.pdf, 2005.

[5] CSJ Peron, M.Legarty, Digital antiforensic:emerging trends in data transformation techniques, www.seccuris.com/documents/papers/Seccuris-Antiforensics.pdf.

[6] G.C.Kessler, Anti-Forensics and the Digital Investigators, Proceeding of the 5th Australian Digital Forensic Conference, 2007.

[7] Ć.Jasmin, M.Bača, „Steganography and its implication on forensic investigation“, INFOTEH Jahorina,B&H, 2010.

[8] Casey, E., „*Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*“ (2nd ed.). London: Elsevier Academic Press,2004.

[9] Ć.Jasmin, “Sigurno brisanje podataka”*INFO br.141, p.24-25, Sarajevo, 2009*.

[10] TOR:Anonimity on line: http://www.torproject.org/index.html.en , pogledano 01.09.2010.g

[11] The Live CD list: http://www.livecdlist.com/ (pogledano dana 01.09.2010)

ABSTRACT

This paper made review and define the digital antiforensic , upcoming technologies used by cyber criminals to conceal digital evidence, destroyed, changed, and thereby prevent the official resolution of digital forensics work in the field of computer crime, but legitimate users who simply want to be left alone in cyberspace and protect their privacy. Also in the paper is presented some of the many tools and methods used in antiforensic, all in order to create a framework for better understanding of this problem.

DIGITAL ANTIFORENSIC-MANIPULATION WITH DIGITAL INVESTIGATION PROCESS

Jasmin Ćosić, *IT Section, Ministry of Interior of Una-sana canton, Bihać, B&H*

Zoran Ćosić, *Statheros ltd., Kaštel Stari, Croatia*