

UNIVERZITET „SINGIDUNUM“

Departman za posleddiplomske
MASTER STUDIJE

Studijski program:
Savremene informacione tehnologije

MASTER RAD

Značaj digitalne forenzičke istrage u upravljanju
kompjuterskim incidentom unutar organizacije

Mentor:
Doc. dr Gojko Grubor

Kandidat:
Slađan Ilić 410311/10

Sažetak

Digitalna forenzika je relativno nova naučna disciplina koja nalazi svoje mesto u pravosudnom sistemu. Prate je brojni izazovi, uključujući brze promene računarskih i digitalnih uređaja, kao i sve sofisticiranijih napada na računarske sisteme i mreže i rapidni porast zloupotreba IKT sistema i kompjuterskog kriminala. Digitalna forenzička nauka ili digitalna forenzika uključuje otkrivanje i sakupljanje (akviziciju), čuvanje (upravljanje), dokazivanje (analizu) i ekspertske svedočenje/veštačenje (prezentaciju) digitalnih podataka, u cilju izgradnje čvrstih dokaza i svedočenja pred sudom, u slučajevima zloupotrebe IKT sistema ili kompjuterskog kriminala, civilne parnice, ili administrativnih zahteva.

Jedan od ključeva uspeha na polju digitalne forenzičke istrage je razumevanje i efikasnost u upotrebi svih alata koji su na raspolaganju. Takođe se naglašava posvećivanje vremena, prevelikih napora, u izboru i podešavanju alata kako bi ih učinili najefikasnijim za odgovarajući posao. U većini slučajeva, svaki alat se fokusira na specifičan cilj. Na primer, neki alati sakupljaju informacije o mreži i mrežnim domenima, a nekima je cilj da iskoriste osetljivost. Najvredniji i najkorisniji su uglavnom oni alati koji su multifunkcionalni i prikladni za upotrebu u više različitih scenarija.

Ključne reči: digitalna forenzika, kompjuterski kriminal, digitalni podatak, IKT sistem.

Abstract

Digital forensics is a relatively new scientific discipline that finds its place in the justice system. Followed by a number of challenges, including rapid changes in computer and digital devices, as well as all the frequent attacks on computer systems and networks and the rapid growth of ICT systems misuse and computer crime. Digital forensic science or digital forensics involves the discovery and collection (acquisition), preservation (control), verification (analysis) and expert testimony/expert (presentation) digital data, in order to build solid evidence and testimony in court, in cases of misuse of ICT systems or computer crime, civil litigation or administrative requirements.

One of the keys to success in digital forensic investigation is the understanding and efficiency in the use of all tools that are available. It also highlights the dedication of time, too much effort in selection and configuration tools to make them most effective for a suitable job. In most cases, each tool focuses on a specific goal. For example, some tools collect information about the network and network domains, while others aim to exploit the vulnerability. The most valuable and most useful tools are generally those that are multifunctional and suitable for use in different scenarios.

Keywords: digital forensics, computer crime, digital data, the ICT system.

SPISAK SLIKA

Slika 1. Primer prozora u WinHex alatu Northon Comander-a.....	21
Slika 2. Tipovi hardverskih blokatora.....	32
Slika 3. Sakupljanje podataka sa klasičnih 3,5 inča IDE diskova.....	33
Slika 4. Sakupljanje podataka sa klasičnih 3,5 inča SATA diskova.....	34
Slika 5. Sakupljanje podataka sa 2,5 inča notebook diskova.....	34
Slika 6. Sakupljanje podataka sa fleš memorije i mikrodiskova.....	35
Slika 7. PCCard (PCMCIA) adapter.....	35
Slika 8. Ikona instaliranog EnCase forenzičkog alata na desktopu.....	41
Slika 9. Otvaranje novog slučaja u EnCase forenzičkom alatu.....	41
Slika 10. Izgled Caine radnog okruženja.....	43
Slika 11. Prikaz instalacije FTK alata verzije 2.0.....	44
Slika 12. Prikaz otvorenog hard diska.....	46
Slika 13. Preuzimanje podataka sa računara preko USB-a koji poseduje COFEE...48	
Slika 14. Helix 3 Pro LiveCD – prikaz Helix boot menija.....	49
Slika 15. Spoljašnji izgled jednog USB fleša.....	56
Slika 16. Izveštaji koje je keylogger slao na e-mail osumnjičenom.....	68
Slika 17. Sadržaj USBSTOR ključa.....	69
Slika 18. Ikonica EnCase alata za digitalnu forenziku.....	71
Slika 19. Pokretanje novog slučaja u EnCase alatu.....	72
Slika 20. Dodavanje dokaznog materijala.....	72
Slika 21. Selekcija USB memorijskog uređaja kao dokaznog materijala.....	73
Slika 22. Oporavak foldera sa FAT fajl sistema opcijom Recover Folders.....	74
Slika 23. Oporavljeni folderi	74
Slika 24. Prikaz izabranih foldera za oporavak.....	75
Slika 25. Kopiranje (oporavak) izbrisanih foldera.....	76
Slika 26. Oznaka „\$“ koja će se nalaziti kao prvo slovo naziva oporavljenog fajla....	76
Slika 27. Prikaz uspešno oporavljenih fajlova.....	77

Slika 28. Prikaz Keylogger-a oporavljenog sa osumnjičenog USB uređaja.....	78
Slika 29. Početna i završna heš vrednost.....	79
Slika 30. Export izveštaja.....	79
Slika 31. Export izveštaja u HTML formatu.....	80
Slika 32. Prikaz HTML izveštaja otvorenog u pretraživaču Mozilla Firefox-u.....	80

SADRŽAJ:

1. Metodologija.....	8
1.1 Uvodne napomene i obrazloženje rada.....	8
1.2 Predmet istraživanja.....	10
1.3 Ciljevi i zadaci istraživanja.....	11
1.4 Hipotetički okvir istraživačkog rada.....	12
1.5 Metodi, tehnike i tok istraživačkog procesa.....	13
2. Forenzički alati.....	16
2.1 Uvod.....	16
2.2 Razvoj forenzičkih alata.....	17
2.3 Opšte karakteristike.....	18
2.3.1 Tehnike i alati za akviziciju digitalnih podataka.....	20
2.3.2 Validacija i diskriminacija podataka.....	22
2.3.3 Ekstrakcija digitalnih podataka.....	23
2.3.4 Rekonstrukcija osumnjičenog diska.....	26
2.3.5 Izveštavanje o digitalnim dokazima.....	28
2.4 Hardverski forenzički alati.....	29
2.4.1 Blokatori upisa i drugi forenzički alati.....	30
2.5 Softverski forenzički alati.....	38
2.5.1 Forenzički alati komandne linije.....	38
2.5.2 Softverski forenzički alat EnCase v4 GUI tipa.....	40
2.5.3 CAINE.....	42
2.5.4 DriveSpy.....	43
2.5.5 Forensic Toolkit.....	43
2.5.6 Forensic Data Recovery.....	44
2.5.7 Computer Online Forensic Evidence Extractor (COFEE).....	46
2.5.8 Helix.....	48
2.6 Validacija i testiranje forenzičkih alata.....	49
2.6.1 Metodologija ispitivanja validnosti forenzičkih alata.....	50
<i>Razvoj specifikacija procesa za ispitivanje alata.....</i>	<i>50</i>
<i>Proces testiranja softverskih forenzičkih alata.....</i>	<i>50</i>
<i>Procedura za validaciju forenzičkih alata.....</i>	<i>52</i>
2.7 Forenzika USB Flash memorijskog uređaja.....	54
2.7.1. Uvod.....	54
2.7.2. USB flash memorija.....	55
<i>Poreklo i razvoj flash memorije.....</i>	<i>56</i>
<i>Princip rada flash memorije.....</i>	<i>57</i>
<i>Posebna ograničenja.....</i>	<i>59</i>
<i>Razvoj flash fajl sistema.....</i>	<i>60</i>
<i>Kapacitet flash memorije.....</i>	<i>60</i>
<i>Brzina flash memorije.....</i>	<i>60</i>

<i>Oštećenje podataka na flash memoriji.....</i>	<i>61</i>
2.8. Korišćenje USB flash memorije u praksi.....	61
2.8.1. Prenos ličnih podataka.....	61
2.8.2. Automatsko prikupljanje podataka.....	62
2.8.3. Širenje zlonamernog softvera.....	62
2.8.4. Forenzički alat.....	63
2.8.5. Sigurnost podataka na flash memorijama.....	63
2.9. Forenzika USB uređaja.....	64
2.9.1. Utvrđivanje relevantnih činjenica.....	64
2.9.2. Izrada procene uspešnosti.....	65
2.9.3. Kreiranje kopije podataka.....	65
2.10. Studija slučaja (<i>Case Study</i>).....	66
2.10.1. Scenario kompjuterskog incidenta.....	67
2.10.2. Oporavak podataka sa USB flash uređaja (pronalazak baze podataka i <i>keylogger</i>).....	70
3. Zaključak.....	82
4. Literatura.....	84

1 METODOLOGIJA NAUČNOG ISTRAŽIVANJA

1.1 Uvodne napomene i obrazloženje rada

Računarska forenzika ili kako je još nazivamo *digitalna forenzika* je grana forenzičke nauke koja se bavi prikupljanjem, pretraživanjem, zaštitom i analizom dokaza u digitalnom obliku te uključuje njihovu prezentaciju kao materijalnih dokaza u kasnijim eventualnim sudskim postupcima.¹

Jedan od ključeva uspeha na polju digitalne forenzičke istrage je razumevanje i efikasnost u upotrebi svih alata koji su na raspolaganju. Takođe se naglašava posvećivanje vremena, prevelikih napora, u izboru i podešavanju alata kako bi ih učinili najefikasnijim za odgovarajući posao. U većini slučajeva, svaki alat se fokusira na specifičan cilj. Na primer, neki alati sakupljaju informacije o mreži i mrežnim domenima, a nekima je cilj da iskoriste osetljivost. Najvredniji i najkorisniji su uglavnom oni alati koji su multifunkcionalni i prikladni za upotrebu u više različitih scenarija.

Digitalna ili *kompjuterska istraga* obuhvata postupak dolaženja do podataka (*digitalnih dokaza*) i utvrđivanja vremena kada su bili uneti, modifikovani, distribuirani, korišćeni, uskladišteni, sklonjeni, kao i vremena kada su fajlovi bili kreirani, postavljeni, punjeni, modifikovani ili kada im se pristupilo. Digitalnim dokazom se smatra svaka informacija koja ima dokazujuću vrednost i koja je uskladištena ili prenesena u binarnoj formi i na koju se sud može osloniti. Nakon sakupljanja, akvizicije i validacije podataka sa “osumnjičenog/korumpiranog” računara, koriste se forenzički alati za identifikaciju i analizu digitalnih podataka. U fazi akvizicije i analize, podaci se ispituju radi identifikacije i otkrivanja dokaza.

Postoji veliki broj alata za digitalnu forenzičku istragu i analizu. Neki od njih su multifunkcionalni, dok se drugi odnose na specifične oblasti. Prilikom istrage i analize mora se jasno utvrditi koji alati će u najkraćem vremenskom periodu pomoći u

¹ <http://sigurnost.lss.hr/documents/LinkedDocuments/NCERT-PUBDOC-2010-05-301.pdf>, od utorka 18.09.2011. god.

postizanju odgovarajućeg cilja. To proističe iz aktuelnosti tzv. žive forenzike, *online* hitnog odgovora na incident. Alati se mogu podeliti u nekoliko grupa, pri čemu, po funkcijama koje obavljaju, ne moraju striktno da pripadaju samo grupi u koju su svrstani.

To su:

- multifunkcionalni alati;
- alati za napad i pregled sistema na *net-u*;
- otvoreni kod/sistemske alati;
- alati za kreiranje lozinke;
- alati za retorički i incidentni odgovor;
- alati za dupliranje odredišta;
- alati za inspekciju sistema na mreži;
- alati za inspekciju mreže;
- alati za pomoć u istraživanju incidenata;
- alati koji pomažu rekonstrukciju Internet aktivnosti;
- uopšteni uređivači i pregledači.

Od svih grupa alata koji su navedeni, u ovom radu biće samo neki objašnjeni i analizirani.

U prvom delu rada dati su razlozi istraživanja, osnovne metodološke postavke, ukazano je na značaj i aktuelnost istraživanja, a zatim su izneti predmet istraživanja, uspostavljeni ciljevi, polazišta i hipoteze i opisana struktura rada.

U drugom delu rada opisano je više forenzičkih alata, kao i njihove mogućnosti, prednosti i mane. Opisani su hardverski i softverski forenzički alati, opisane su osnovne, zahtevane funkcionalnosti softverskih forenzičkih alata tokom istrage. Opisane su funkcionalnosti sledećih forenzičkih alata: *EnCase*, *CAINE*, *DriveSpy*, *FTK*, *Forensic Data Recovery*, *COFEE* i *Helix*. Takođe, opisan je USB fleš memorijski uređaj, poreklo i razvoj fleš memorije, princip rada, kapacitet i brzina fleš memorije. Eksperimentalno je urađena studija slučaja i scenario kompjuterskog

incidenta na korporacijskom nivou, kao i sam oporavak podataka sa USB fleš uređaja.

Treći deo rada – Zaključak koji sadrži rezime rada i rezultate istraživanja u kome su dati prikazi forenzičkih alata koji su korišteni u ovom radu. Zatim, poreklo i razvoj fleš memorije, princip rada, razvoj, kapacitet i brzina fleš memorije, kao i scenario kompjuterskog incidenta na korporacijskom nivou i proces oporavka podataka sa USB flash uređaja. Time su potvrđene postavljene hipoteze.

1.2 Predmet istraživanja

U ovom radu predmet istraživanja je analiza i upotreba softverskih forenzičkih alata u cilju predstavljanja značaja digitalne forenzike za što bolju istragu kompjuterskog incidenta na nivou organizacije. Još jedan od predmeta istraživačkog rada jeste upoznavanje sa USB fleš memorijskim uređajima, analiza i uspešan oporavak izbrisanih podataka sa USB fleš memorijskog uređaja uz pomoć *EnCase* softverskog forenzičkog alata za digitalnu forenzičku istragu, gotovo nezamenljivog u borbi protiv zloupotreba IKT sistema i kompjuterskog kriminala, koji predstavlja veliki problem današnjice.

U prvom delu rada izneti su razlozi istraživanja, osnovne metodološke postavke, sa fokusom na značaj i aktuelnost istraživanja, a zatim izneti predmet istraživanja, uspostavljeni ciljevi i polazišta, postavljene hipoteze i opisana strukturu rada.

U drugom delu rada opisani su forenzički alati, poreklo, razvoj i princip rada fleš memorije, kao i sam tok forenzičke istrage. Opisani su hardverski i softverski forenzički alati, kao i osnovne, zahtevane funkcionalnosti softverskih forenzičkih alata u svakom pojedinačnom delu istrage. Poseban značaj je dat događaju kompjuterskog incidenta na korporacijskom (organizacijskom) nivou, kao i sam oporavak podataka sa USB fleš uređaja, softverskim forenzičkim alatima koji se najviše i najčešće koriste za potrebe prikupljanja dokaza u toku forenzičke istrage.

Treći deo rada se odnosi na zaključak u kome je dat rezultat/prikaz značaja primene u istrazi kompjuterskog incidenta više softverskih forenzičkih alata, njihove osnovne funkcije, prednosti i mane. Nastanak i razvoj fleš memorije i sam način rada

fleš memorije posebno su pogodni za distribuciju malicioznih programa, zloupotrebe i različite oblike kompjuterskog kriminala. Studijom slučaja i scenarijom kompjuterskog incidenta na korporacijskom nivou, kao i samim oporavkom podataka sa USB flash uređaja potvrđene su postavljene hipoteze o neophodnosti primene forenzičkih tehnika i alata za otklanjanje stvarnih uzroka incidenta.

Pre svega treba znati da je računarska (kompjuterska, digitalna) forenzika postupak prikupljanja i analize podataka na način da se ne utiče na njihovu originalnost ili uništenje, što je više moguće, u svrhu rekonstrukcije podataka ili događaja koji su se u prošlosti dogodili na nekom kompjuterskom sistemu. Razumevanje, kao i samo poznavanje forenzičkih alata može biti od velike pomoći u proceni distribucije informacija, načina gubitka ili uništavanja, ali za forenzičara je najbitnije da dođe do njih i očuva njihov integritet u procesu akvizicije, analize i izgradnje čvrstih digitalnih dokaza.

1.3 Ciljevi i zadaci istraživanja

Glavni cilj ovog istraživačkog rada je da se prikaže značaj digitalne forenzike i softverskih forenzičkih alata i tehnika u upravljanju kompjuterskim incidentom. Posebno je dat akcenat na to, da mogući dokazi prikupljeni preko forenzičkih metoda i alata u analizi kompjuterskog incidenta u organizaciji, budu neoborivi u slučaju sudskog postupka, ako do njega dođe.

1. *Poseban cilj* je da se dokaže upotrebna vrednost i neophodnost primene digitalne forenzike u rešavanju slučajeva kompjuterskog incidenta/kriminala u organizaciji pre (ne)angažovanja zvaničnih organa istrage. Za forenzičku analizu je potrebno izdvojiti dosta vremena i napora, obezbediti zaštitu integriteta i dostupnosti i primeniti sve standardne operativne procedure u procesu digitalne forenzičke istrage, koja je veoma kompleksna, vremenski zahtevna i stresna, jer se najčešće radi u određenom i ograničenom vremenskom periodu.
2. *Poseban cilj* rada je dokazati mogućnost praktične primene digitalne forenzičke nauke, tehnika i alata u analizi kompjuterskog incidenta na korporacijskom nivou, kroz oporavak podataka sa USB fleš uređaja uz pomoć *EnCase* softverskog

forenzičkog alata i otkrivanje malicioznog koda (trojanca *keylogger-a*) za krađu bankarskih podataka.

Na *Internet* tržištu postoji veliki broj komercijalno dostupnih digitalnih forenzičkih alata sa brojnim opcijama rešenja za različite forenzičke zadatke. Ovi alati često mogu zbuniti digitalnog forenzičara, pri izboru pravog alata za konkretni slučaj. Forenzička praksa podjednako zahteva da forenzičar raspolaže sa setom raznovrsnih alata za određene namene, ali i specifičnim namenskim alatima koji su generalno bolji za rešavanje namenskih zadataka. Glavni zadaci su, da se definišu i verifikuju ključne funkcionalnosti alata i procene upotrebne vrednosti.

1.4 Hipotetički okvir istraživačkog rada

Hipotetički okvir istraživanja sastoji se od sledećeg:

Opšta hipoteza: Digitalna forenzička istraga kompjuterskog incidenta u potpunosti zavisi od primenjene forenzičke tehnike (metoda) i tipa forenzičkog alata. Softverski digitalni forenzički alati su relativno jeftiniji više dostupni prosečnoj organizaciji, nego hardverski alati, a mogu se podeliti na više načina, zavisno od kriterijuma klasifikacije. U odnosu na tip interfejsa softverski forenzički alati se dele na:

- digitalne forenzičke alate komandne linije i
- digitalne forenzičke alate sa GUI (*Grafical User Interface*) interfejsom.

U odnosu na programski kod, softverski digitalni forenzički alati se dele na:

- digitalne forenzičke alate zatvorenog koda i
- digitalne forenzičke alate otvorenog koda.

Izbor najboljeg forenzičkog alata i tehnike za istragu kompjuterskog incidenta, uvek je poseban izazov za korporacijskog forenzičara. Pored velikog izbora digitalnih forenzičkih alata, ne može se govoriti o najboljem digitalnom forenzičkom alatu. Specijalizovani forenzički alati koriste se za samo određenu vrstu fajlova ili obavljaju

samo jedan zadatak digitalne forenzičke istrage. Ovi alati su namenski i pouzdaniji te mnogo efikasnije obavljaju specifičan zadatak nego neki univerzalni alati.

Sa druge strane, sa adekvatnim skupom raznovrsnih digitalnih forenzičkih alata, forenzičar može brže i konformnije završiti više različitih zadataka digitalne forenzičke istrage.

Najbolje je rešenje da digitalni forenzičar sam, na bazi predistražnih podataka i informacija o slučaju, izvrši izbor adekvatnih alata za konkretan slučaj, uključujući skup alata za izvršenje što više digitalnih forenzičkih zadataka na terenu kao i specijalizovane alate za detaljno i precizno izvršavanje karakterističnog forenzičkog zadatka.

Radna hipoteza: Generalno, digitalni forenzički alati zatvorenog koda pred sudom mogu biti priznati kao alati za akviziciju i analizu digitalnih podataka pod uslovom da su naučno potvrđeni, da im je poznat stepen greške koju unose i da mogu po zahtevu suda ponoviti proces izgradnje čvrstih digitalnih dokaza bez narušavanja integriteta, akvizicijom prikupljenih digitalnih podataka. EnCase i FTK softverski alati zatvorenog koda, najšire su prihvaćeni u forenzičkoj zajednici. EnCase je prvi forenzički alat naučno verifikovan i priznat od pravosudnih sistema gotovo u celom svetu, što je dobar razlog za primenu u korporacijskoj digitalnoj forenzičkoj istrazi.

FTK je skup forenzičkih alata koji nudi najveći broj funkcionalnosti za rešavanje većine forenzičkih zadataka u procesima akvizicije i analize digitalnih podataka. Forenzička prihvatljivost u praksi digitalne forenzičke istrage slučajeva kompjuterskog incidenta/kriminala može se evaluirati verifikacijom deklariranih funkcionalnosti na istim i kontrolisanim slučajevima akvizicije (imidžovanja) i analize digitalnih podataka i komparacijom sa funkcionalnim ispitivanjem sličnog seta priznatih forenzičkih alata drugog tipa (zatvoreni/otvoreni kod, komandna linija/GUI interfejs).

1.5 Metodi, tehnike i tok istraživačkog procesa

Metoda naučnog istraživanja je sistematski, kritički, kontrolisani i ponovljivi proces sticanja novih znanja, neophodnih za identifikovanje, određivanje i rešavanje naučnog problema. U naučnom istraživanju u ovom radu primenjeni su sledeći glavni principi:

- *sistematičnost* - dobra uređenost istraživačkog postupka i obezbeđivanje prirodnog i logičkog sleda procesa istraživanja,
- *kontrolisanost* - sprovođenje istraživanja u što moguće boljim i nadziranim uslovima, kako bi se isključila/smanjila alternativna rešenja i
- *kritičnost* - sve važne tvrdnje o pojavama, procesima, odnosima i svojstvima moraju se ozbiljno, iskreno i strogo procenjivati, proveravati i obrazložiti.

Na osnovu podele naučnog istraživanja prema prirodi istraživanja na - *teorijska i empirijska*, prema cilju istraživanja na - *fundamentalna i primenjena* i prema funkciji istraživanja na - *eksplorativna i usmerena na proveravanje hipoteza*, u ovom istraživačkom radu primenjena su uglavnom *fundamentalna, primenjena i istraživanja usmerena na proveravanje hipoteza*. *Fundamentalna* istraživanja primenjena su radi sticanja novih znanja o ovoj oblasti, a *primenjena i istraživanja usmerena na proveravanje hipoteza* - radi sticanja novih znanja i rešavanja hipotezom postavljenih zadataka u ovom radu.

U ovom istraživačkom radu korišćeni su različiti alati i metode istraživanja i verifikacije procesa digitalne forenzičke istrage da bi se došlo do određenih saznanja, otkrili i izložili naučni principi, koji se primenjuju u digitalnoj forenzici.

Od *opšte naučnih* metoda korišćene su statistička metoda, metoda modelovanja i analitičko-deduktivna metoda. Takođe su korišćene *osnovne, opšte metode društvenih nauka*: pozitivistička metoda, metoda razumevanja, komparativna metoda, metoda idealnih tipova, metodološki funkcionalizam i strukturalizam i dijalektičke metode.

Od *posebnih naučnih* metoda i tehnika primenjene su: analitičko-sintetička metoda, metoda apstrakcije i konkretizacije, metoda generalizacije i specijalizacije, metoda klasifikacije, logičke metode indukcije i dedukcije, kao i metoda spoznaje i dijalektičkog jedinstva indukcije i dedukcije.

Tehnike istraživanja predstavljaju sistematsko i svrsishodno jedinstvo postupaka i instrumenata. Ovaj deo naučnog metoda podrazumeva: *ocenu, sređivanje, obradu podataka i zaključivanje* na osnovu njih. U tom smislu, postoji povezanost i međuzavisnost između metoda prikupljanja i obrade podataka, odnosno dokaznih materijala i informacija do kojih se došlo istraživanjem.

Tok istraživanja, kao prvi logični korak uključuje prikupljanje literature o metodologiji naučnog istraživanja i digitalnoj forenzičkoj istrazi sa težištem na softverske forenzičke alate, zatim, istraživanje literaturnih podataka i materijala preuzetih iz raznih izvora, kroz faze otkrivanja, opisivanja i objašnjavanja određenih faza analize forenzičkih alata i digitalne forenzičke istrage. Rad je struktuiran u određene celine i svaka od njih konkretno objašnjava glavne faze i procese korporativne digitalne forenzičke istrage kompjuterskog incidenta.

U prvom poglavlju je objašnjena metodologija rada, uvodne napomene i obrazloženje rada, u kome je objašnjen pojam digitalne forenzike. Zatim, predmet istraživanja i ciljevi i zadaci istraživanja u kojima se nešto više govori o forenzičkim alatima. Hipotetički okvir istraživanja rada koji se sastoji se od opšte hipoteze i radne hipoteze. Zatim, su objašnjene metode, tehnike i tok istraživačkog procesa rada.

Drugo poglavlje govori o forenzičkim alatima, samom razvoju forenzičkih alata i njihovim karakteristikama, tehnikama i alatima za akviziciju digitalnih podataka. Zatim o validaciji, diskriminaciji i ekstrakciji digitalnih podataka, rekonstrukciji osumnjičenog diska i izveštavanju o digitalnim dokazima, hardverski forenzičkim alatima, blokatorima upisa i drugim forenzičkim alatima. Softverskim forenzičkim alatima, kao što su *EnCase, FTK, DriveSpy, Caine, Helix, Cofee, Forensic Data Recovery*. Validaciji i testiranju navedenih forenzičkih alata, kao i metodologiji ispitivanja validnosti istih. Objašnjen je nastanak i poreklo fleš uređaja, urađena je rekonstrukcija kompjuterskog incidenta na korporacijskom nivou, kao i sam oporavak podataka sa USB flash uređaja uz pomoć EnCase softversko-forenzičkog alata.

U trećem poglavlju dati su zaključci o digitalnoj forenzici kao nauci, softverskim forenzičkim alatima, razvoju i karakteristikama forenzičkih alata i fleš memorijskih uređaja i argumentima koji potvrđuju postavljene hipoteze.

2 FORENZIČKI ALATI

2.1 Uvod

Digitalna forenzika je relativno nova naučna disciplina koja nalazi svoje mesto u pravosudnom sistemu. Prate je brojni izazovi, uključujući brze promene računarskih i digitalnih uređaja, kao i sve sofisticiranijih napada na računarske sisteme i mreže i rapidni porast zloupotreba IKT sistema i kompjuterskog kriminala. Digitalna forenzička nauka ili digitalna forenzika uključuje otkrivanje i sakupljanje (*akviziciju*), čuvanje (*upravljanje*), dokazivanje (*analizu*) i ekspertsko svedočenje/veštačenje (*prezentaciju*) digitalnih podataka, u cilju izgradnje čvrstih dokaza i svedočenja pred sudom, u slučajevima zloupotrebe IKT sistema ili kompjuterskog kriminala, civilne parnice, ili administrativnih zahteva².

Najveći deo digitalne forenzike odnosi se na forenziku računarskih sistema, ili kompjutersku forenziku, bilo da su računari samostalni ili umreženi. Digitalna forenzika računarskog sistema obuhvata naučno ispitivanje i analizu podataka iz čvrstih diskova (HD), fajl sistema i drugih medija i prostora za skladištenje podataka u računarskom sistemu, tako da se podaci mogu koristiti kao čvrsti i neoborivi dokazi pred sudom. „Krajnji cilj jeste da se pokaže kako digitalni dokazi mogu da se koriste da se rekonstruiše zločin ili incident, identifikuju osumnjičeni, uhapsi kriv, oslobodni nevin, i da se razumeju motivi kriminalaca“³.

Ranih 90-tih razvijeni su prvi alati za istragu i ispitivanje digitalnih podataka. IACIS (*Information Association of Computer Investigative Specialists*) organizuje obuku za digitalnu forenzičku istragu. Za uspešnu forenzičku istragu potrebno je dobro poznavati različite platforme: *DOS*, *MS-DOS*, *Windows 9x/NT/2000/XP/Vista*, *UNIX/Linux*, *Machintosh* i dr. Značajne resurse za digitalnu forenzičku istragu predstavlja mreža eksperata za digitalnu forenziku računarskih sistema i drugih profesionalaca i održavanje kontakata putem *e-mail* poruka sa specijalistima različitih disciplina [3].

² Grubor G., Milosavljević M. (2007), „*Digitalna forenzika*“, Univerzitet Singidunum, Beograd, str. 3

³ Casey Eoghan, (2004), „*Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*“, Second Edition, Great Britain, str. 20

Brojni savremeni forenzički alati koriste se istovremeno i za akviziciju i analizu digitalnih podataka. Dele se u dve glavne kategorije: hardverskih i softverskih alata. Kriterijumi za izbor adekvatnog specijalizovanog alata, ili seta forenzičkih alata, značajnija su pitanja za svakog forenzičara, nego preporuke pojedinačnih forenzičkih alata.

Forenzički alati se neprestano razvijaju, modernizuju, popravljaju i reklamiraju. Zato je korisno proveriti *web* lokacije poznatih proizvođača i videti kakve su karakteristike forenzičkih alata poslednje generacije⁴. Savremeni softverski forenzički alati sa GUI interfejsom mogu zahtevati znatne resurse računarskog sistema o čemu treba razmišljati kod nabavke forenzičkog alata.

Da bi se obezbedio neophodni integritet digitalnih podataka, kao i poznavanje stepena greške koju alat unosi, potrebno je poznavati pouzdanu metodu testiranja validnosti forenzičkog alata.

2.2 Razvoj forenzičkih alata

Evolucija alata za digitalnu forenzičku istragu – akviziciju i analizu:

- Prvi forenzički alati su pomagali u ispitivanju privremeno oduzetih računara i to na nivou heksadecimalnog zapisa;
- U 1990-tim na raspolaganju su bili specijalizovani forenzički alati:
 - **DD (Unix)** za kopiranje i konverziju sirovih digitalnih podataka na niskom nivou;
 - **Safeback** za uzimanje imidža diska, razvijen za IRS;
 - **EnCase** set forenzičkih alata sa GUI i interfejsom komandne linije;
 - **Sleuthkit** kolekcija alata baziranih na *Unix* i *Windows* platformama;
- *Mrežni alati*, koji su se razvili u periodu od 2002-2003, koji nisu specifični za digitalnu forenziku:
 - **Carnivore** (FBI) korisnički prilagodljiv snifer paketa koji može monitorisati sav *Internet* saobraćaj ciljanog korisnika;

⁴ Casey Eoghan, (2004), „*Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*“, Second Edition, Great Britain, str. 32

- **Carnivore** i nova verzija DCS-1000, nisu korišćeni u FBI. FBI je koristio nepoznati komercijalni proizvod za nadgledanje *Interneta* 30 puta u istragama u tom periodu.
- Glavni problemi sa forenzičkim alatima su:
 - bagovi u softveru,
 - promene u OS i hardveru računara,
 - kompleksnost,
 - nedostatak standarda i razvoj standarda,
 - alati sa otvorenim izvornim kodom,
 - počelo testiranje forenzičkih alata.
- Istraživanje i iskustva iz prakse su potvrdila da su najveći nedostaci savremenih forenzičkih alata:
 - bagovi (15%),
 - nedostatak standarda (10%),
 - interoperabilnost (8%),
 - automatizacija (6%) i
 - formalno testiranje (4%).

2.3 Opšte karakteristike

Opremanje digitalne forenzičke laboratorije za terenske i stacionirane uslove nije ni malo lak zadatak, treba odrediti koji su forenzički alati najfleksibilniji, najpouzdaniji i najrentabilniji za obavljanje posla. Tako softverski alati moraju biti kompatibilni najmanje sa sledećom generacijom OS. Na primer, uvođenjem NTFS fajl sistema u *Windows NT OS*, forenzičari su imali velike probleme.

Proizvođači forenzičkih softverskih alata morali su revidirati svoje alate za analizu novog fajl sistema. Uspostavljanje i održavanje digitalne forenzičke laboratorije uključuje formiranje softverske biblioteke – repozitorijum, koji sadrži starije verzije forenzičkih alata, OS i drugih programa kao što su stare verzije *Windows* i *Linux OS*.

Ako nova verzija forenzičkog softvera fiksira jedan bag, ali unese drugi, forenzičar može koristiti prethodnu fiksiranu verziju⁵.

Za digitalnu forenzičku akviziciju i analizu potrebno je obezbediti adekvatne forenzičke hardverske i softverske alate - specifične forenzičke alate, ili softverski set alata, koji obezbeđuje izvršavanje nekoliko zadataka istovremeno. Sa setom forenzičkih alata forenzičar može po potrebi koristiti alate sa komandnom linijom, ili GUI interfejsom.

Kod nabavke forenzičkog alata uvek treba imati na umu vrste fajlova i podataka, koje alat treba da analizira. Uvek se preporučuje namenski alat specijalizovan za određenu vrstu podataka, na primer, za *MS Access* bazu ili *e-mail* poruke, nego neki univerzalni alat koji između ostalog analizira i ove podatke, zato što su strogo namenski alati pouzdaniji za tu konkretnu funkciju. Takođe, forenzičar koji poseduje višenamenski skup alata, na primer tipa *FTK*, koji omogućava obavljanje više različitih zadataka forenzičke istrage, može brže i konfornije sa jednim alatom završiti sve raznovrsne zadatke. Razumno rešenje je da forenzičar za terenski rad obezbedi rentabilan skup alata koji izvršava što veći broj tipičnih forenzičkih zadataka, sa određenim specijalizovanim alatima koji brže i tačnije izvršavaju datu funkciju. Za nabavku forenzičkog softvera potrebno je evaluirati karakteristike potencijalnih alata kao što su:

- OS na kojem forenzički alat radi,
- mogućnost rada verzije alata na jednom ili više OS i da li proizvode iste rezultate u višenamenskom radu,
- mogućnost analize više fajl sistema kao što su *FAT*, *NTFS*, *Ex2fs*,
- mogućnost korišćenja nekog programskog alata za automatizaciju funkcija i zadataka koji se u alatu ponavljaju,
- mogućnost automatizovanog obavljanja nekih funkcija, koje mogu smanjiti vreme analize podataka,
- reputacija proizvođača alata i dr.

⁵ Grubor G., Milosavljević M. (2009), „Istraga kompjuterskog kriminala“, Univerzitet Singidunum, Beograd, str. 161

2.3.1 Tehnike i alati za akviziciju digitalnih podataka

Akvizicija digitalnih podataka prvi je zadatak u forenzičkoj istrazi računara i podrazumeva pravljenje fizičke kopije *bit-po-bit* originalnog (osumnjičenog, ispitivanog) diska računara. Sama procedura sprečava korupciju i oštećenje digitalnih podataka na originalnom disku. Forenzički alati za akviziciju digitalnih podataka treba da obuhvataju sledeće funkcije:

- kopiranje podataka sa fizičkog diska,
- kopiranje podataka sa logičkog diska/particija,
- formatiranje akvizicijskih podataka,
- akvizicija komandnom linijom,
- akvizicija sa GUI alatima,
- udaljena akvizicija i
- verifikacija.

Za akviziciju podataka *bit-po-bit* sa originalnog na forenzički disk postoje hardverski i softverski forenzički alati. Primeri hardverskih alata za uzimanje fizičke slike računara su: *Image MaSSter Solo 2 Forensic* komponenta sa *firmware* programom (*Intelligence Computer Solutions Inc.*) koji može samostalno kopirati podatke sa originalnog na forenzički disk. Sve druge aplikacije za akviziciju digitalnih podataka zahtevaju kombinaciju hardverskih i softverskih komponenti. Na primer, *EnCase* alat ima za akviziciju digitalnih podataka *DOS* program *En.exe* i jednu funkciju u svojoj *GUI Windows* aplikaciji. Za akviziciju podataka sa *En.exe* programom zahteva se da računar radi sa *MS-DOS* operativnim sistemom (OS), ima 12V konektor za napajanje, IDE ili SCSI kabl za povezivanje. *Windows* aplikacija *EnCase* alata zahteva upotrebu blokatora upisivanja podataka na originalni disk, kao što je *FastBloc* za sprečavanje *Windows* OS da pristupi i korumpira originalni disk [5].

"Praćenje sistema i pokušaj povratka izbrisanih podataka korišćenjem raznih alata će vam pomoći da razumete šta se dešavalo u tačno određenom trenutku na računaru, to je slično kao praćenje instrument table na vozilu koje će vam pomoći da shvatite šta se dešava sa vozilom sve vreme"⁶.

⁶ *Sinchak Steve, (2004), „Hacking Windows XP“, United States of America, str. 159*

U procesu akvizicije podataka softverskim alatima postoje dva metoda kopiranja:

- fizičko kopiranje celog fizičkog diska i
- logičko kopiranje particija diska.

Većina softverskih alata za akviziciju uključuje jednu ili obe ove funkcije. Formati koji su na raspolaganju za akviziciju diskova variraju od potpuno sirovih podataka u binarnom zapisu do kompresovanih podataka specifičnih za proizvode. Sirovi podaci su direktna kopija diska. Primer imidža sirovih podataka je izlaz *UNIX* i *Linux* šel **dd** komandne linije. Primer formata sirovih podataka je jednostavna *bit-po-bit* kopija fajla podataka, particije diska, ili celog diska. Alat za akviziciju sirovih podataka može kopirati podatke sa jednog diska na drugi disk, ili u jedan ili više segmentiranih fajlova podataka⁷. Pošto je ovo zaista neizmenjena kopija, forenzičar može gledati sadržaj sirovih podataka imidža fajla sa heksadecimalnim editorom kao što su *HexWorkshop* ili *WinHex*. Heksadecimalni editori, poznatiji kao diskeditori, kao što je *Northon DiskEdit*, obezbeđuju čitanje podataka u heksadecimalnom zapisu i otvorenom tekstu (Slika 1).



Slika 1. Primer prozora u WinHex alatu Northon Comander-a

⁷ Grubor G., Milosavljević M. (2007), „Digitalna forenzika“, Univerzitet Singidunum, Beograd, str.58

Većina forenzičkih alata za akviziciju može praviti manje segmentirane fajlove. Ovakvi forenzički alati su na primer *SafeBack (NTI)*, *X-Ways'*, *Replica* i *EnCase*. Namena uzimanja segmentiranih podataka sa diska je da se podaci mogu skladištiti na manje forenzičke medijume, kao što su CD-ROM, DVD-ROM ili USB *Flash* memorija.

Vendorski specifikovani formati nalaze se u alatima kao što su: *EnCase*, *SafeBack*, *ASR Data SMART*, *X-Ways*, *WinHex Forensic* i *Replica*; forenzički alat za uzimanje imidža diska (DII) i *SavePort* komanda *DriveSpy* alata. Neki od ovih alata mogu napraviti *bit-po-bit* imidž fajlova sa kompresovanim ili nekompresovanim podacima. Kompresija imidža podataka može značajno smanjiti potreban kapacitet forenzičkog diska (do 50%). Na primer, podaci sa 30GB HD mogu se kompresovati na HD od 16 ili 17GB. Ako su originalni podaci već kompresovani (npr., ZIP, JPEG ili GIF fajlovi), forenzički alati ih više ne mogu kompresovati [2].

Neki savremeni forenzički alati mogu izvršiti akviziciju podataka na daljinu, preko računarske mreže. Svi savremeni forenzički alati obezbeđuju metod za verifikaciju tačnosti procesa kopiranja podataka sa originalnog na forenzički disk.

2.3.2 Validacija i diskriminacija podataka

Validacija i diskriminacija podataka elementarni su procesi u radu sa digitalnim podacima. Osnovne funkcije procesa validacije i diskriminacije podataka su:

- heširanje,
- filtracija i
- analiza hedera fajlova.

Proces validacije obezbeđuje integritet kopiranih podataka i omogućava njihovu diskriminaciju na dokazujuće i nedokazujuće podatke. Validacija podataka obezbeđuje se uzimanjem heš (sažetka) vrednosti nekim od raspoloživih algoritama, kao što su *CRC32*, *MD5*, *SHA1*, *SHA256*, *SHA384* ili *SHA512*. Ova funkcija uzimanja heš vrednosti kopiranih imidž podataka standardna je karakteristika gotovo svih savremenih forenzičkih alata. Preporučuje se uzimanje heš vrednosti celog

diska, kao i svakog fajla na disku. Takve heš vrednosti su jedinstvene vrednosti podataka, kao otisak prsta za čoveka i obezbeđuju integritet podataka od prvog uzimanja heš vrednosti [5].

Proces diskriminacije, uključujući sortiranje, pretraživanje i analizu svih ispitivanih digitalnih podataka, obezbeđuje izgradnju digitalnih dokaza. Namenjen je za filtriranje -uklanjanje standardnih dobrih podataka od sumnjivih podataka. U dobre podatke spadaju poznati fajlovi kao što su sistemski (OS) i uobičajenih aplikativnih programa (*MS Word, Adobe* i slika). Većina forenzičkih alata obezbeđuje tri metoda diskriminacije podataka:

- Nekoliko softverskih forenzičkih alata mogu integrisati skup heš vrednosti poznatih fajlova. Ovi alati upoređuju poznate fajlove sa istim na osumnjičenom disku i ako se ne poklapaju upozoravaju forenzičara da je fajl sumnjiv. Na ovaj način alat može značajno smanjiti količinu podataka za analizu i izvlačenje dokaza.
- Drugi metod za diskriminaciju podataka je analiza i verifikacija informacija iz hedera svih tipova poznatih fajlova. Na primer oznaka **JFIF** (*JPEG File Interchange Format*) ugrađena je ispred svih JPEG fajlova.
- Treća grupa alata omogućava dodavanje jedinstvenih heš vrednosti podataka hedera u bazu podataka alata, što poboljšava funkciju diskriminacije u fazi analize. Pretraživanjem i upoređivanjem hedera alat može locirati fajlove koji mogu biti namerno izmenjeni. Ova funkcija može se koristiti za lociranje skrivenih fajlova.

2.3.3 Ekstrakcija digitalnih podataka

Ekstrakcija digitalnih podataka sa forenzičkim alatima ima zadatak oporavka podataka u forenzičkoj istrazi i zahtevniji je za upravljanje od svih ostalih funkcija alata. Oporavak podataka je prvi korak u fazi analize ispitivanih podataka. Proces ekstrakcije digitalnih podataka obuhvata više koraka:

- opservacija podataka,
- pretraživanje sa ključnom reči,
- dekompresija podataka iz fragmenata izbrisanog fajla,
- dešifrovanje šifrovanih fajlova podataka i
- označavanje (markiranje) digitalnih dokaza.

Opservacija podataka: Većina forenzičkih alata obezbeđuje funkciju posmatranja podataka, a kako se i u kojem formatu podaci vide, zavisi od alata. *DriveSpy (DII-Digital Intelligence Inc.)*, na primer, obezbeđuje gledanje logičke particije osumnjičenog diska i heksadecimalnog zapisa podataka u klasterima i sektorima diska. Alati kao što su *FTK, EnCase, Smart iLook, ProDiscover* i dr., nude nekoliko različitih načina posmatranja podataka, uključujući posmatranje logičke strukture fajlova i foldera (direktorijuma) na disku. Ovi alati, takođe, pokazuju alocirane (dodeljene) klastere sa podacima fajlova i nealocirane (nedodeljene) oblasti diska. Posmatranje podataka u njihovom normalnom (prirodnom) formatu, znatno olakšava analizu i donošenje zaključaka relevantnih za istragu [3].

Pretraživanje po ključnoj reči: uobičajeni je zadatak u ispitivanju računara. Ovim se oporavljaju ključni podaci. Ključnu reč u istrazi određuje forenzičar na bazi raspoloživih podataka o karakteru krivičnog dela kompjuterskog kriminala. Standardni pretraživači na bazi ključne reči obično generišu suviše informacija, pa je potrebno ispitati da li forenzički alat dopušta kombinaciju ključnih reči, što znatno skraćuje vreme pretraživanja. Takođe, treba ispitati da li su alati selektivni u izboru tipa pretraživanih podataka, na primer, samo za *e-mail* poruke. Neki forenzički alati vrše indeksiranje svih reči na disku. Ovo obezbeđuje *FTK* alat koristeći binarno indeksiranje (tzv. b-stablo) sa *dtSearch* funkcijom, koja obezbeđuje trenutno pronalaženje ključne reči i znatno ubrzava proces analize.

Dekompresija podataka: *FTK* takođe može dekompresovati arhivske fajlove, kao što su *ZIP, MS PST i OST e-mail* folderi i indeksirati njihov sadržaj. Drugi alat – *iLook* ima ograničene kapacitete za indeksiranje i nudi samo nekoliko ključnih reči od interesa za pretraživanje. Ovaj alat kreira fajl b-stabla indeksa koji se može gledati po kompletiranju pretraživanja sa ključnom reči.

Rekonstrukcija fragmenata fajlova obrisanih sa osumnjičenog diska (*USA, carving; eng. salvaging*) značajan je deo procesa forenzičke istrage. Ekstrakcija podataka iz nealociranih prostora diska postala je uobičajen zadatak za forenzičara. *DriveSpy* alat može locirati podatke, ali zahteva mnogo manuelnog rada i metoda za kopiranje klastera u novi fajl. Napredniji forenzički alati, kao što su *EnCase*, *FTK*, *ProDiscover*, *iLook* i drugi GUI tipa alati, imaju ugrađene funkcije koje automatski rekonstruišu fragmentirane podatke. *Data Lifter* i *Davory* alati specifično su dizajnirani da rekonstruišu fajlove poznatih podataka iz eksportovanog nealociranog prostora diska. *Data Lifter* ima interaktivne funkcije koje omogućavaju da forenzičar doda druge jedinstvene vrednosti podataka hedera u bazu alata [2].

Dešifrovanje šifrovanih fajlova podataka glavni je izazov za forenzičara u ispitivanju računara, pored analize i oporavka podataka. Šifrovan može biti ceo disk, particija diska ili individualna poruka. Većina *e-mail* servisa, kao *MS Outlook*, obezbeđuje zaštitu šifrovanjem *PST* foldera ili individualnih poruka. Mehanizmi za šifrovanje rangiraju od specifičnih za određenu platformu – *EFS* u *MS Windows XP* OS do *TTPS (Trusted Third Party Provider Service)* proizvoda – *PGP* ili *GnuPG*. Sa aspekta forenzičara šifrovani fajlovi i sistemi su problem. Mnogi forenzički alati tipa *FTK* za oporavak *password*-a mogu generisati potencijalnu listu za napad rečnikom na *password*. Postoji izvesna šansa da je *password* upisan u privremeni fajl, ili sistemski fajl na osumnjičenom disku, kao što je *Pagefile.sys*. *FTK* alat generiše listu *password* i šalje je u *AD Password Recovery Toolkit (PRTK)* rečnik. *PRTK* prvo otvara listu rečnika *password*-a za šifrovane fajlove. Ako ovaj napad ne uspe ostaje kryptoanalitički napad brutalnom silom, koji zahteva veliku računarsku moć i višeprocesorske mašine.

Označavanje digitalnih dokaza vrši se posle lociranja podataka – glavnog zadatka u ispitivanju računara. Cilj označavanja podataka je da se forenzičar može po potrebi pozvati na označene podatke. Većina forenzičkih alata koriste funkciju označavanja digitalnih podataka za ubacivanje liste u generator za izveštavanje, koji proizvodi tehnički izveštaj o nalazima ispitivanja računara. Primer jednostavnog generatora za izveštavanje je *log* fajl kojeg kreira *DriveSpy* alat. Pošto je ovo alat komandne linije šel tipa, on može memorisati ključne reči za pretraživanje sa ekrana, ali ako se koristi *Output* komanda *DriveSpy* kopira izlaz ekrana generisan funkcijom traženja ključne

reči u *log* fajl. Za posmatranje i analizu rezultata pretraživanja po ključnoj reči, treba ih izvući iz *DriveSpy* alata i otvoriti *log* fajl editorom teksta.

Forenzički alati GUI tipa, kao što su *FTK*, *iLook*, *ProDiscover* ili *EnCase* imaju opciju označavanja digitalnih dokaza koje forenzičar identifikuje. Kada se podigne generator za izveštavanje u *FTK* ili *EnCase* alatu, identifikatori (oznake) digitalnih dokaza se unose u izveštaj. *FTK* i *iLook* generišu izveštaj u *HTML* formatu koji se može čitati u bilo kojem *web* pretraživaču. *EnCase* generiše izveštaj u *RTF* formatu dokumenta i može se čitati u većini *MS Word procesora*⁸.

2.3.4 Rekonstrukcija osumnjičenog diska

Ova funkcija u forenzičkim alatima namenjena je da se regeneriše (re-kreira, ili rekonstruiše) osumnjičeni disk, što se tipično radi sa fizičkog duplikata osumnjičenog HD. Prvi razlog za rekonstrukciju događaja na osumnjičenom računaru je da po zahtevu suda forenzičar može podići osumnjičeni računar i pokazati šta se dogodilo u toku kompjuterskog incidenta, ili krivičnog dela. Drugi razlog za dupliranje osumnjičenog diska je da se napravi identična kopija za potrebe drugih forenzičara-odbrane, veštačenja. Ako je fizička kopija osumnjičenog računarskog sistema uzeta prema propisanoj proceduri akvizicije i sa prihvatljivim i pouzdanim forenzičkim alatom, ta imidž kopija (duplikat) uobičajeno se smatra originalom osumnjičenog računara. Kopirani forenzički disk je tačni *bit-po-bit* duplikat osumnjičenog originalnog diska. Osnovne funkcije u procesu rekonstrukcije osumnjičenog diska mogu biti:

- kopiranje sa diska na disk,
- kopiranje sa fizičkog imidža na disk,
- kopiranje particije na particiju i
- kopiranje imidža particije na particiju.

Postoji nekoliko načina za rekonstrukciju forenzičke *bit-po-bit* kopije osumnjičenog diska. Pod idealnim uslovima najbolji metod forenzičkog dupliranja diska je obezbeđivanje HD istog modela i proizvođača kao što je originalni osumnjičeni HD.

⁸ Grubor G., Milosavljević M. (2009), „Istraga kompjuterskog kriminala“, Univerzitet Singidunum, Beograd, str. 166

Ako je osumnjičeni HD novije generacije, nije teško pronaći isti tip, ali za starije proizvode to nije uvek moguće.

Najjednostavniji metod dupliranja diska je korišćenje alata koji vrši direktno kopiranje sa originalnog na forenzički disk. Na raspolaganju je više alata koji to omogućavaju, a besplatan je *Linux dd Shel command*. Ovaj dinamični alat ima, međutim, veliki nedostatak pri kreiranju radnog duplikata sa originalnog diska: forenzički disk mora biti identičan originalnom disku po *CHS* (cilindri, sektori, tragovi) podacima. Ako nije na raspolaganju identičan HD, forenzička radna stanica mora omogućiti da se iz *BIOS*-a manipuliše sa *CHS* podacima da bi se uparili sa originalnim vrednostima. Treba znati da *firmware* forenzičkog diska može uticati na korektnost ove tehnike. Neki alati mogu meriti geometrijske izmene osumnjičenog diska prema forenzičkom HD. Za većinu forenzičkih alata forenzički disk mora biti najmanje jednak, ili veći po kapacitetu od osumnjičenog diska.

Za kopiranje sa diska na disk brži su hardverski nego softverski alati za dupliranje diska. Sledeći alati prilagođavaju geometriju *CHS* forenzičkog diska prema geometriji *CHS* originalnog diska:

Hardverski duplikatori:

- Logicube Forensic SF-5000,
- Logicube Forensic MD5,
- Image MaSStar Solo 2 Forensic HD Duplicator.

Softverski duplikatori:

- SafeBack,
- SnapCopy.

Za kopiranje sa imidža na disk i imidža na particiju na raspolaganju su brojni alati, ali su znatno sporiji u prenosu podataka. Neki alati koji vrše kopiranje sa imidža na disk su:

- SafeBack,
- Snap Back i
- EnCase.

Sva tri alata imaju specifične formate podataka koji se mogu restaurirati samo sa istom aplikacijom koja ih je generisala. Na primer, *SafeBack* imidž može se restaurirati samo sa istim alatom, ako na glavnom pretresu sudija zahteva da forenzičar demonstrira kako radi računar osumnjičenog. Za ovu demonstraciju forenzičar mora imati proizvod koji zaklanja (*shadows*) osumnjičeni disk i sprečava upisivanje/izmenu podataka na njemu. Ova tehnika zahteva hardverski uređaj kao što je *Voom Technologie's Shadow Drive*, koji spaja osumnjičeni HD na IDE port samo za čitanje, a drugi HD na port za čitanje-pisanje. Ovaj HD na portu za čitanje-pisanje označava se kao zaklonjen HD. Kada se *Voom* uređaj sa ova dva HD poveže na računar, forenzičar može pristupiti i podizati aplikaciju na osumnjičenom HD. Svi podaci koji bi se normalno upisivali na osumnjičeni disk, preusmeravaju se na zaklonjeni disk.

2.3.5 Izveštavanje o digitalnim dokazima

Da bi se proces forenzičke analize i ispitivanja diska kompletirao, potrebno je generisati izveštaj o ispitivanju. Pre pojave forenzičkih alata koji rade na *Windows* OS, ovaj izveštaj je zahtevao kopiranje podataka sa osumnjičenog diska i manuelnu ekstrakciju dokaza. Posle ekstrakcije dokaza, forenzičar ih kopira u poseban program kao što je neki *Word* procesor, da bi se generisao izveštaj. Problem je bio sa ubacivanjem podataka koji se ne mogu čitati u *Word* procesoru, kao što su baze podataka, grafički prikazi i dr., što je forenzičar morao odštampati i prilagoditi uz izveštaj [2].

Savremeni forenzički alati mogu generisati elektronski izveštaj u različitim formatima - *Word* dokument, *HTML* ili *PDF*. Osnovne funkcije procesa izveštavanja su:

- log izveštaj i
- generator za izveštavanje.

Kao deo procesa validacije, potrebno je dokumentovati korake preduzete za dobijanje podataka sa osumnjičenog diska. Većina forenzičkih alata može generisati izveštaj o aktivnosti, poznat kao log izveštaj, koji se može dodati konačnom izveštaju

forenzičara kao dodatni dokument o tome koji su koraci preduzeti u toku ispitivanja. Ovi podaci mogu biti korisni ako se zahteva ponavljanje ispitivanja. Za slučaj koji zahteva direktan uvid, *log* izveštaj potvrđuje koje aktivnosti su izvršene, a koji rezultati su dobijeni iz originalne analize i ispitivanja računara. Sledeći alati su samo neki od onih koji obezbeđuju log izveštaje: *FTK*, *iLook*, *X-Ways Forensic*, *DriveSpy*.

2.4. Hardverski forenzički alati

Kako se brzo menjaju informaciono komunikacione tehnologije IKT sistema, tako se zahteva veći izbor softverskih forenzičkih alata za hardver. Većinu hardverskih komponenti savremenih računara proizvođači isporučuju sa srednjim vremenom otkaza od oko 18 meseci. Kako se forenzički hardverski alati, radne stanice i serveri koriste intenzivno, zamenu i obnavljanje treba planirati najmanje svake dve godine. Većina snabdevača računarskih sistema i komponenti nude širok asortiman forenzičkih radnih stanica, koje korisnik može prilagoditi svojim potrebama. Generalno, forenzičke radne stanice mogu se podeliti u sledeće tri kategorije:

- Stacionarna radna stanica: računarski sistem sa nekoliko kućišta za eksterne HD i mnogo perifernih uređaja visokih performansi;
- Portabl radna stanica: laptop računar sa ugrađenim LCD monitorom i skoro istim brojem kućišta i perifernih uređaja kao stacionarna radna stanica;
- Prenosna radna stanica: obično laptop ugrađen u transportnu torbu sa manjim brojem perifernih uređaja.

Digitalna forenzička laboratorija policijske agencije treba da ima što veći broj različitih forenzičkih alata, softvera i hardvera da bi izvršila sve potencijalne zadatke istrage kompjuterskog kriminala. Ako je moguće treba imati po nekoliko (2-3) konfiguracije PC za istovremeni rad na različitim slučajevima, zatim kompletirati repozitorijum softvera i hardvera sa svim prethodnim verzijama aktuelnih platformi.⁹

Preporuke za nabavku/izgradnju forenzičke radne stanice korisno je razmotriti pre donošenja odluke. Odrediti gde će se vršiti akvizicija podataka, pa ako je to na primer, na terenu:

⁹ Grubor G., Milosavljević M. (2007), „Digitalna forenzika“, Univerzitet Singidunum, Beograd, str. 63

- obezbediti blokator upisivanja, preko *Fire Wire* i USB 2.0 - blokator tipa *Fire Chief* (DII) i forenzički Laptop računar.
- Za redukciju hardvera koji se nosi, može se koristiti *Wiebe Tech Forensic Drive Dock* sa regularnim *Drive Dock Fire Wire* mostom.

2.4.1 Blokatori upisa i drugi forenzički alati

Značajan aspekt digitalnih dokaza koji ga razlikuje od fizičkih i drugih tipova dokaza je što se može kopirati do najsitnijih detalja - bajtova. Za razliku od, na primer, vatrenog oružja, digitalni dokaz se prvo kopira, a zatim se analiza vrši na kopiji. Dakle, kopija, a ne original, je „najbolji dokaz“ u digitalnoj forenzičkoj analizi. Forenzičar može napraviti tačnu fizičku kopiju čvrstog diska, dok balističar ne može napraviti duplikat vatrenog oružja. Otuda je akvizicija podataka iz osumnjičenog računara, pravljenjem fizičke kopije (imidža) osumnjičenog računara, najznačajnija faza digitalne forenzičke istrage.

Akvizicija digitalnih dokaza sa hardverskom tehnologijom uključuje:

- blokatori upisivanja,
- razni adapteri,
- CD/DVD diskovi za akviziciju,
- SCSI diskovi i optički kanali.

Blokatori upisivanja su hardversko-softverski uređaji za sprečavanje upisivanja podataka na ispitivani disk. U izgradnji, ili nabavci radne stanice za digitalnu forenzičku akviziciju i analizu treba obavezno planirati nabavku blokatora upisivanja u softverskoj, ili hardverskoj izvedbi. Blokatori upisivanja sprečavaju forenzičare da slučajno upisuju podatke na ispitivani disk koji sadrži digitalne dokaze.

Softverski blokatori upisivanja uobičajeno se koriste kada nisu na raspolaganju hardverski blokatori i predstavljaju racionalnu alternativu. Softverski blokatori upisivanja, kao što su *PDBlock* (DII), tipično radi u *šel modu* kao što je *DOS*. Kada se koristi *PDBlock*, potrebno je znati da se menja *Interrupt 13* u *BIOS-u* ispitivanog računara, što sprečava bilo kakvo upisivanje u specifikovani disk. Ako pokuša upisivanje podataka na blokirani disk, javlja se alarm koji upozorava da se upisivanje

ne može izvršiti. Ovaj alat se ne može koristiti sa *Windows* i *MS DOS*, nego samo u osnovnom *DOS* modu [3].

Sa hardverskim blokatorom upisivanja spaja se ispitivani disk sa dokazima na forenzičku radnu stanicu i pokreće OS na uobičajen način. Hardverski blokatori upisivanja idealni su za GUI forenzičke alate, jer sprečavaju svaki pokušaj *Windows/Linux* OS da upisuje podatke na blokirani disk, kao što su *Windows* aplikacije, ili *Windows Explorer* da otvara fajlove, ili *Word* da ih čita. Ako se kopira *Word Windows* podatak na blokirani disk, prozor pokazuje da je kopiranje uspešno izvršeno. Međutim, blokator upisivanja u stvari prepíše i nulira sve te podatke. Kada se na radnoj stanici potraži kopirani fajl na blokiranom disku, tamo ga neće biti.

Postoje hardverski blokatori upisivanja koji se povezuju na računar kroz *FireWire*, USB 2.0 i SCSI kontroler. Većina ovih blokatora upisivanja omogućava forenzičaru da ukloni i ponovo spoji disk bez isključivanja (*shut down*) forenzičke radne stanice, što skraćuje vreme procesiranja ispitivanog diska.

Razlika između softverskih i hardverskih blokatora zapisivanja zavisi od definicije hardvera i softvera. Stvarno blokiranje upisivanja hardverom vrši se sa hardverskom komponentom, kako samo ime implicira, koja se ne može reprogramirati posle implementacije dizajna. Međutim, zbog kompleksnosti komunikacionih protokola (kao što su IEEE 1394-FireWire, USB2.9 i.t.d.), često je nepraktično implementirati čiste hardverske blokatore upisivanja.

Generalno, ono što se podrazumeva pod stvarnim hardverskim blokatorom zapisivanja, u stvari se vrši pomoću kombinacije jednog ili više mikroprocesora i hardverske logike u jednom kolu ili čipu. Ovi programi nazivaju se *firmware*, relativno su mali i na njihovu funkciju ne utiče rad OS, pošto se standardni komunikacioni protokoli podešavaju nezavisno od bilo kojeg OS datog računara. Ovo je, sa aspekta forenzičara, osnovna prednost metoda hardverskih blokatora upisivanja u odnosu na softverske.

Korišćenjem hardverskih blokatora upisivanja mogu se skinuti digitalni podaci sa brojnih tipova čvrstih diskova:

- IDE čvrsti diskovi od 3,5 inča, klasični sa 40-pinskim IDE konektorom,
- SATA čvrsti diskovi od 2,5 i 3,5 inča, koji postaje preovlađujući u svim desktop i većini *notebook* računarima,
- *Notebook* čvrsti diskovi od 2,5 inča preovlađivali su u ovim računarima od početka proizvodnje do nedavno,
- PCMCIA (PCCard) čvrsti diskovi, koji nisu šire prihvaćeni,
- 1,8 inča *Toshiba* čvrsti diskovi, koji se koriste u originalnom iPod i široko se koriste,
- 1,8 inča *Hitachi* čvrsti diskovi, koji se retko sreću u praksi,
- Kompaktni fleš i mikrodiskovi, koji se preovlađujuće koriste u digitalnim kamerama i u nekim iPod uređajima,
- SCSI čvrsti diskovi, koji se preovlađujuće koriste specijalno u starijim *Machintosh* i računarima sa visokim performansama,
- Optički čvrsti diskovi (*Fiber Chanel*),
- ZIF kablovski diskovi koji se koriste u video iPods i postaju preovlađujući u upotrebi.

Osnovni tipični blokatori većinom izledaju kao na *slici 2*.



Slika 2. Tipovi hardverskih blokatora

Komplet blokatora upisivanja i adaptera za sakupljanje podataka sa klasičnih 3,5 inča IDE diskova (*Slika 3*), obuhvata:

- forenzički ComboDock koji se priključi na klasični 3,5 inča IDE čvrste diskove,
- FireWire +USB host pristup,
- paralelni 40-pinsku IDE konekciju,
- obezbeđuje blokirano upisivanje i
- brojne forenzičke karakteristike.



Slika 3. Sakupljanje podataka sa klasičnih 3,5 inča IDE diskova

Komplet blokatora upisivanja i adaptera za sakupljanje podataka sa 3,5 inča SATA čvrstih diskova obuhvata (Slika 4):

- forenzički SATADock,
- priključuje se na 3,5 inča SATA čvrsti disk,
- FireWire +USB pristup host računaru,
- SATA konektor,
- obezbeđuje blokirano upisivanje i
- brojne forenzičke karakteristike.



Slika 4. Sakupljanje podataka sa klasičnih 3,5 inča SATA diskova

Komplet blokatora upisivanja i adaptera za sakupljanje podataka sa 2,5 inča notebook čvrstih diskova obuhvata, (Slika 5):

- Forensic Notebook DriveDock,
- priključuje se na 2,5 inčne čvrste diskove,
- priključuje se na FireWire +USB pritupe host računaru,
- obezbeđuje blokirano upisivanje i
- brojne forenzičke karakteristike.



Slika 5. Sakupljanje podataka sa 2,5 inča notebook diskova

Blokatori upisivanja i 1- inčni adapter za akviziciju digitalnih podataka sa fleš memorija i mikrodiskova povezuju se paralelno na forenzički ComboDock, (Slika 6).



Slika 6. Sakupljanje podataka sa fleš memorije i mikrodiskova

PCCard (PCMCIA) adapter, relativno redak, povezuje se paralelno, polarizuje se kroz montažnu stranu šinskog slotu. Nema polarizacije pinova na konektoru. Povezuje se na forenzički *ComboDock*, (*Slika 7*).



Slika 7. PCCard (PCMCIA) adapter

Akvizicija podataka sa CD/DVD diskova za razliku od čvrstih diskova može imati varijacije. Imidži kreirani sa optičkih diskova mogu neznatno varirati svaki put kada se imidž uzima, čak i kada se koriste isti disk i optički disk. Ovo je posledica brojnih faktora, kao što je prisustvo čestica prašine, ili ogrebotina i korišćenja manje robusnih algoritama sklonih greškama od onih koje koriste kontroleri čvrstih diskovi¹⁰. Razmatrajući ove faktore svaka forenzička istraga koja uključuje dokaze na optičkim medijima treba da ima četiri sledeća cilja:

1. Da se izvrši akvizicija imidža fajlova sa diska koji se mogu čitati i analizirati softverskim forenzičkim alatima dizajniranim za tu namenu. Za ovu operaciju postoje brojni alati na raspolaganju: *FTK*, *EnCese*, *iLook*, *xWay Forensic* itd.

¹⁰ Grubor G., Milosavljević M. (2009), „Istraga kompjuterskog kriminala“, Univerzitet Singidunum, Beograd, str. 178

2. Da se obezbedi dokaz da originalni podaci na disku nisu izmenjeni u toku kopiranja. Ovo se postiže korišćenjem forenzički poverljivog softvera za uzimanje imidža diska, što zadovoljava *CD/DVDImager*. Forenzički alati sa otvorenim izvornim kodom na bazi Linux OS za uzimanje imidža su *DD* i *CDRDAO*, koji su od velikog poverenja u forenzičkoj zajednici. Forenzičar često mora da isproba nekoliko alata pre nego što uspešno napravi imidž neobičnog, ili problematičnog optičkog diska. *DD* i *CDRDAO* alati uspešni su za najveći broj optičkih diskova u upotrebi.
3. Da se obezbedi dokaz da fajlovi sa imidža diska nisu izmenjeni posle inicijalnog kreiranja. Ovo se obezbeđuje kreiranjem heš vrednosti uzetog imidža. Uzimanjem drugog heša imidža diska posle forenzičke analize, može se dokazati da imidž nije menjan u toku ispitivanja.
4. Da se obezbedi upoređivanje imidža diska sa fizičkim dokazom. *CD/DVDImager* uzima sliku svakog diska i skladišti je sa imidžom diska. Heš vrednost fajla imidža takođe se generiše tako da forenzičar može kasnije potvrditi da slika nije bila izmenjena.

Dobra praksa forenzičke akvizicije i analize je da se otštampa kopija fajla izlaznog heša posle sesije akvizicije podataka i da se ova kopija forenzički markira i čuva u odvojenoj bezbednoj lokaciji. Na taj način forenzičar kasnije može potvrditi da nije bilo izmena na imidžu posle akvizicije. Ako neko pristupi log datoteci heš vrednosti, može izmeniti i fajl i heš log. Dakle, papirna kopija ojačava forenzički lanac čuvanja dokaza¹¹.

RedPort alat za akviziciju sa SCSI i optičkih kanala razvijen je u saradnji sa ATTO i sprečava upisivanje na diskove. Radi na nivou host računara, a ne u nekom spoljnom mostu. Portovi se identifikuju sa crvenim trakama.

Uređaj *RP-PCIE-SCSI* = Atto'sEPCI-5DRO-BR1 (a.k.a. EPCI-UL5D) automatski blokira upisivanje svakog priključenog SCSI diska, za bezbedno izvlačenje podataka

¹¹ Grubor G., Milosavljević M. (2007), „Digitalna forenzika“, Univerzitet Singidunum, Beograd, str.68

samo sa opcijom "čitanje". Koristi Brzi Ultra SCSI interfejs za podršku starijih SCSI proizvoda. Ima brzinu prenosa podataka do 320MB/sec po kanalu. Može da radi na dva nezavisna SCSI kanala. Posедуje x4PCI Express priključivanje na host računar. Koristi naprednu ADS (*Advanced Data Streaming*) tehnologiju i ima drajvere za podršku Windows i Linux OS. Podržava do 30 SCSI bus IDs i može da radi preko kabla do 12m dužine. Usaglašen je sa RoHS.

RP-PCIE-FC = Atto'sCTFC-42RO-BR1 (a.k.a. Celerity FC-42ES) automatski blokira upisivanje u svaki prključeni *FiberChanel* uređaj, za bezbedno izvlačenje podataka samo sa opcijom "čitanje". Sadrži 4GB-tni dvo-kanalni *FiberChanel*-host računar adapter sa brzinom prenosa podataka do 800 MB/sec u punom duplex modu. Brzina prenosa x8PCI Express (PCIe) za konekciju sa hostom je 2GB/sec. Koristi ADS tehnologiju i ima drajvere za podršku Widows i Linux OS. Kompatibilan je sa 2GB i 1GB starijim *FibreChanel* prozvodima. Uključuje dva 4Gb LC SFPa. Usaglašen je sa RoHSC.

2.5 Softverski forenzički alati

Softverski forenzički alati grupišu se u dve osnovne kategorije:

- Aplikacije komandne linije i
- GUI (Graphics User Interface) aplikacije.

Neki alati namenjeni su za izvršavanje jednog zadatka, kao što je *SafeBack* (*NTI-National Technology Inc.*) alat na bazi DOS komandne linije namenjen za akviziciju podataka sa diska. Primeri GUI tipa alata su: *EnCase* (*Guidance Software*¹²) i *FTK* (*Access Data*¹³), namenjeni za obavljanje više forenzičkih funkcija. Većina GUI alata tipično može izvršiti većinu zadataka akvizicije i analize digitalnih podataka u računarskom sistemu.

¹² <http://www.guidancesoftware.com/forensic.htm>, od petka 09.09.2011. god.

¹³ <http://accessdata.com/products/forensic-investigation/ftk>, od subote 03.12.2011. god.

Značajan aspekt softverskih forenzičkih alata je sposobnost potpunog kopiranja ili uzimanja fizičke (eng. *mirror*) slike *bit-po-bit* osumnjičenog diska. Ovaj se proces često naziva uzimanje imidža (eng. *imaging*) osumnjičenog diska (ili drugog medijuma) sa potencijalnim dokazima. Većina GUI alata mogu čitati i analizirati imidž fajlove i originalne diskove, kao što su najpoznatiji softverski forenzički alati: *EnCase*, *FTK*, *X-Ways Forensic*, *Forensic Data Recovery*, *Helix* i drugi.

2.5.1 Forenzički alati komandne linije

Forenzički alati sa komandnom linijom *MS DOS* za *IBM PC* fajl sisteme bili su prvi alati za analizu i ekstrakciju podataka sa flopi i čvrstog diska. Prvi među tim alatima bio je *Norton DiskEditor*. Kako su vremenom rasle potrebe razvijeni su forenzički programi za *DOS*, *Windows*, *Apple*, *Net Ware* i *UNIX OS*. Neki od ovih softverskih alata može izvući podatke iz nezauzetog (*slack*) prostora i nealociranih (slobodnih) prostora fajl sistema; drugi su namenjeni samo za izvlačenje izbrisanih fajlova. Savremeni forenzički programi su mnogo robusniji, mogu pretraživati po ključnoj reči ili karakteru, računati heš vrednost, oporaviti izbrisani fajl, izvršiti analizu fizičkog i logičkog diska i još mnogo toga [2].

Jedna od osnovnih prednosti alata komandne linije je što zahtevaju malo sistemskih resursa i većinom zauzimaju jedan butabilni flopi disk. Većina ovih alata proizvodi izveštaj u tekst formatu.

Forenzički alati komandne linije ograničeni su što ne mogu pretraživati arhivske fajlove kao što su *ZIP* (*.zip*, *.rar*) i kabinetske (*.cab*) fajlove. Obično rade samo na *MS FAT* fajl sistemu, izuzev *MS DOS* alata *NTFS DOS* (*SysInternals*) koji ekstrahuje podatke iz *NTFS* fajl sistema.

Neki forenzički alati komandne linije dizajnirani su specifično za *DOS/Windows* platforme: *NTI*, *Mars Ware*, *Ds2dump* i *ByteBack*, a drugi za *Machintosh* i *UNIX/Linux* platforme (tzv. *nix* platforme). Forenzički alat komandne linije, koji je na raspolaganju u *Windows 2000* i *XP OS*, *Dir* komanda koja pokazuje vlasnika fajla u računaru sa više korisnika, ili u računarskoj mreži. Aktivira se sledećim koracima:

- Otvoriti *Start*, zatim *Run* i ukucati *cmd* za otvaranje šela komandne linije.
- Ukucati *cd* koji vraća na *rut* direktorijum.
- Ukucati *dir/q>C:\Filowner.txt*.
- Koristiti bilo koji tekst editor za otvaranje *C:\Filowner.txt* i čitanje rezultata.

Forenzički alati komandne linije *UNIX/Linux* rade na brojnim *nix* platformama, koje se značajno razlikuju od *DOS/Windows* sistema. Dugi niz godina *nix* platforme nisu šire prihvaćene, ali su pojavom *GUI* tipa *nix* platformi postale znatno popularnije kod individualnih korisnika i u poslovnim sistemima. Neki od alata koji rade na *nix* platformama su *SMART (ASR Data)*, *TCT (The Coroner's Toolkit)*, *TCT Autopsy* i *SleuthKit*. Svi alati komandne linije zahtevaju veliko razumevanje *MS DOS* komandi i različitih fajl sistema.

Forenzički alati sa *GUI* interfejsom pojednostavljuju forenzičku akviziciju i analizu. Međutim, potrebno je poznavati i koristiti alate komandne linije, pošto neki *GUI* forenzički alati ne mogu otkriti svaki dokaz. Većina *GUI* alata dolazi u setu alata za više zadataka (*EnCase*, *FTK*). *GUI* alati imaju nekoliko prednosti: jednostavna upotreba, mogućnost obavljanja više zadataka i ne zahtevaju učenje starijih OS.

Nedostaci *GUI* forenzičkih alata su:

- zahtevaju velike računarske resurse (*RAM* memoriju),
- proizvode nekonzistentne rezultate zbog tipa korišćenog OS (npr., *Win XP Professional*, ili *Home Edition*),
- stvaraju zavisnost forenzičara da koristi samo jedan alat,
- u nekim situacijama ne rade pa se zahteva alat komandne linije u kompletu alata.

2.5.2 Softverski forenzički alat EnCase v4 GUI tipa

EnCase je najpoznatiji i prvi prihvaćeni softverski alat zatvorenog programskog koda, namenjen forenzičkoj istrazi digitalnih dokaza, koji je proizvela firma *Guidance Software*. Smatra se jednim od najboljih i najčešće korišćenih softverskih forenzičkih alata. Na osnovu ovog softvera, kompanija *Guidance*

Software je postala jedna od tri najveće svetske IT kompanije. EnCase program omogućava i olakšava forenzičku istragu, akviziciju i analizu dokaznog materijala. EnCase se danas koristi kao najnapredniji sigurnosti alat, a kao standard su ga prihvatile i neke vodeće kompanije i organizacije kao što su *Rolls Royce* i *NATO*. Isto tako, ovaj alat je rasprostranjen i koristi se pri primeni zakona u komercijalnim preduzećima za analizu i akviziciju podataka. Smatra se jednim od najboljih, i svakako je jedan od najčešće korištenih alata. EnCase kao alat omogućava i olakšava sudskim veštacima i stručnjacima iz IT okruženja istraživanje slučajeva, akviziciju i analizu dokaza i dokaznog materijala. EnCase ima kvalitetan grafički interfejs, koji omogućava bolji i lakši pregled različitih fajlova kao što su izbrisani (*deleted*) fajlovi, „slack“ i nealocirani prostori fajla „*unallocated data*“. Ono što je svakako najvažnije za forenzičara, jeste da nema mogućnost izmene podataka preuzetih sa korumpiranog računara sa EnCase alatom [2].

Interfejs: EnCase verzija 4 je mnogo urednija od svoje prethodne verzije 3, a najnovija verzija još je bolja. EnCase je organizovan po tabovima i postoji mogućnost prikazivanja većeg broja slučajeva, pri čemu je svaki slučaj organizovan u okviru svog foldera. Tabovi se mogu lako dodavati i uklanjati otvaranjem View menija.¹⁴

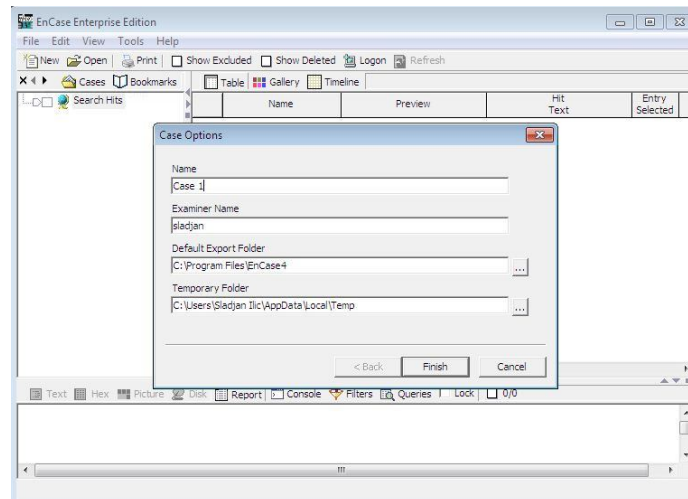
Navigacija: U ovom atributu alata opisano je kako se kreira novi slučaj, dodaje i prikazuje dokazni materijal. Nakon što je EnCase instaliran, na desktopu se pojavljuje ikona (Slika 8). Duplim klikom otvara se EnCase verzija 4 za Windows.



Slika 8. Ikona instaliranog EnCase forenzičkog alata na desktopu

¹⁴ Grubor G., Milosavljević M. (2009), „Istraga kompjuterskog kriminala“, Univerzitet Singidunum, Beograd, str. 181

Klikom na dugme *New* pojavljuje se dijalog za kreiranje novog slučaja (*New Case*). Unose se informacije kao što su ime slučaja, ime istraživača, *export* folder i folder za privremene (*temporary*) fajlove. Klikom na dugme *Finish* kreiran je novi prazan slučaj (*Slika 9*).



Slika 9. Otvaranje novog slučaja u EnCase forenzičkom alatu

Trebalo bi voditi računa o takozvanom *Case Menagement*-u koji podrazumeva dodeljivanje imena slučajevima, ostavljanje prostora na disku za skladištenje dokaznog materijala, imenovanje foldera za *temporary* fajlove i dr. *Case Menagement* je osnova forenzičke istrage dokaza.

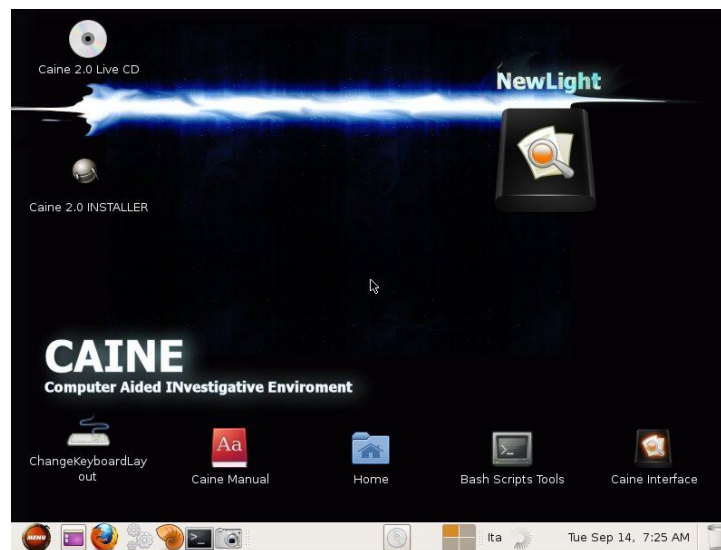
EnCase se prilagođava analitičaru koji možda ne želi ili nema potrebu da zna detalje o hard diskovima i strukturama podataka operativnog sistema. *EnCase* može analizirati skoro svaki popularan fajl sistem, uključujući *NTFS*, *FAT32* i *EXT2*. Ovo ga čini veoma prilagodljivim alatom za organizacije sa više platformi.

2.5.3 CAINE

Caine (*Computer Aided INvestigative Environment*) je program italijanske proizvodnje kreiran za potrebe digitalne forenzike. Koji na jednom mestu sadrži veliki

broj dostupnih besplatnih forenzičkih softvera i pojavio se kao besplatna alternativa, nakon što je *Helix* distribucija postala komercijalna [10].

Caine (Slika 10), kao i *Helix* sadrži u sebi veliki broj alata na *live Linux* distribuciji i alate koji su namenjeni *Windows* operativnim sistemima. Prednost *Caine*-a je u tome, što se sa zvaničnog sajta, koji prati i učestvuje u razvoju, može preuzeti instalaciona verzija koja je namenjena podizanju sa USB fleš uređaja.¹⁵



Slika 10. Izgled Caine radnog okruženja

2.5.4 Drivespy

DriveSpy je alat namenjen za digitalnu forenziku za *DOS* operativni sistem, koji je razvijen od strane kompanije *Digital Intelligence*. Alat je veoma popularan, zauzima malo kapaciteta, to je alat koji proširuje osnovne *MS-DOS* funkcije. Dodatne funkcije su kreiranje MD5 heš vrednosti na kopirani disk ili particiju. Jedina mana je u tome što nema razvijen grafički interfejs. Aktuelna verzija *DriveSpy* 3.0, sadrži dodatak koji pokreće upravljačke programe i omogućava rad sa USB fleš prenosnim uređajima, koje do sada nije prepoznavao *DOS* operativni sistem¹⁶.

¹⁵ <http://www.caine-live.net/>, od subote 01.10.2011. god.

¹⁶ <http://www.digitalintelligence.com/software/disoftware/drivespy/>, od utorka 04.10.2011. god.

2.5.5 Forencis Toolkit

Forencis Toolkit (FTK) je softver za kompjutersku forenziku koji je proizveden od strane kompanije *AccessData*. FTK je priznat širom sveta kao alat koji je zastupljen u istragama kompjuterskog kriminala. Prihvaćen je od strane suda kao alat čija platforma omogućava najsavremenije računarske forenzičke analize i dokaze, dešifrovanje lozinki, izbrisane poruke elektronske pošte i ima veoma jednostavno i prilagodljivo korisničko okruženje, kao i sam grafički interfejs (*Slika 11*).

Alat, takođe, uključuje samostalni disk *imaging* koje se zove *FTK Imager*. *FTK Imager* je možda i najpoznatiji alat za kopiranje "*bit po bit*". On čuva imidž hard diska u jednom fajlu ili segmentima koji se mogu kasnije obnoviti. Izračunava MD5 heš vrednosti i potvrđuje integritet podataka pre zatvaranja datoteke. Kao rezultat dobija se *DD raw image*.¹⁷

Najnovija verzija FTK alata je FTK 3.0, poznat po svom radnom okruženju, koji omogućava preciznu analizu poruka elektronske pošte i prilagodljivih prikaza podataka. FTK predstavlja alat koji se može prilagođavati potrebama organizacije. *Forencis Toolkit v3.0* je sada najnapredniji forenzički alat, sa mnoštvom funkcija.¹⁸



Slika 11. Prikaz instalacije FTK alata verzije 2.0

¹⁷ <http://en.wikipedia.org/wiki/FTK>, od subote 22.10.2011. god.

¹⁸ <http://accessdata.com/products/forensic-investigation/ftk>, od subote 22.10.2011. god.

2.5.6 Forensic Data Recovery

Forensic Data Recovery je alat koji poseduje skup tehnika i delova digitalne forenzike. Njegove metode i analize se mogu koristiti na sudu, ili u svrhu spašavanja izgubljenih ili izbrisanih datoteka. Neki sudski veštaci upotrebljavaju ovaj alat za spašavanje izbrisanih podataka i samu analizu korumpiranog računara. Ako osumnjičeni izbriše datoteke, poruke elektronske pošte ili medije koji sadrže dokaze o kompjuterskom kriminalu, forenzičari mogu da izvrše potpuni oporavak ili samo oporavak delova izbrisanih podataka u svrhu korišćenja dokaza na sudu [12].

Forensic Data Recovery posjeduje i jednu manu, a to je nemogućnost da povрати sve izgubljene ili izbrisane podatke sa računara ili hard diska. Neke vrste podataka koje su izbrisane korišćenjem specifičnih metoda nisu dostupni za oporavak. Takođe, se može videti i nemogućnost povratka podataka sa hard diskova koji imaju veliko fizičko oštećenje (*Slika 12*).

Kada korisnik briše datoteku sa hard diska računara, podaci se sastoje od datoteka koje ne mogu biti uništene. Iako, se operativni sistem više ne seća gde je bila locirana datoteka, ako korisnik ili program mogu da ga pronađu, podaci će i dalje biti dostupni. Ako je datoteka izbrisana na neki specifičan način, metapodaci ili osnovne informacije o datoteci će ostati zapamćeni unutar operativnog sistema.

Ovaj alat mogu koristiti i drugi korisnici za oporavak i spašavanje slučajno izbrisanih podataka koji su im važni ili potrebni za posao. Neprofesionalni korisnici koji ne znaju mnogo o radu sa ovom vrstom alata, mogu da povrate podatke sa svog računara uz pomoć nekih besplatnih programa koji su dostupni sa Interneta, kao što su *Stellar Data Recovery*, *EASEUS Partition Recovery*, *Restoration* i drugi softveri uz pomoć kojih se mogu povratiti izbrisani podaci, oštećene particije ili druge izgubljene datoteke¹⁹.

Mnoge svetske škole imaju osnove digitalne forenzike kao jedan od predmeta iz oblasti informatike, koji zahteva minimalni nivo znanja. Neki univerziteti nude

¹⁹ http://www.ehow.com/about_6702877_forensic-data-recovery.html, od subote 22.10.2011. god.

online kurseve o informacionim sistemima, kompjuterskom kriminalu i digitalnoj forenzici koji su dostupni preko *Interneta* [8].



Slika 12. Prikaz otvorenog hard diska

2.5.7 Computer Online Forensic Evidence Extractor

Agencije za sprovođenje zakona širom sveta se suočavaju sa zajedničkim problemom u borbi protiv kompjuterskog kriminala, dečija pornografija, krađe identiteta, *online* prevare, i sl. Ove agencije moraju snimiti važne dokaze sa računara na mestu istrage pre nego što se računar ugasi i ti podaci budu izgubljeni. "Živi" dokazi, kao što su aktivni procesi koji se odvijaju u sistemu i mrežni podaci su nestabilni i mogu biti izgubljeni u procesu isključivanja računara. Stoga je *Microsoft* da bi rešio ovaj problem kreirao *COFEE (Computer Online Forensic Evidence Extractor)*²⁰.

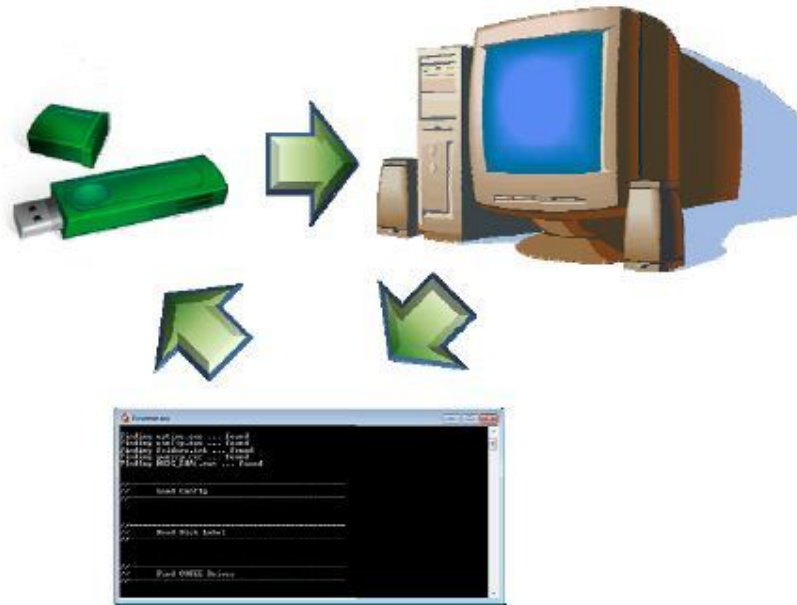
Computer Online Forensic Evidence Extractor (COFEE) je forenzički alat, koji je kreirao *Microsoft* i koji je isključivo namenjen za upotrebu od strane agencija za sprovođenje zakona i suzbijanje kompjuterskog kriminala [3].

²⁰ <http://www.microsoft.com/industry/government/solutions/cofee/default.aspx>, od petka 28.10.2011. god.

COFEE je veoma brz alat, lak za upotrebu, koji sadrži veliki broj forenzičkih mogućnosti, sadrži 150 komandi koje pojednostavljaju i ubrzavaju proces preuzimanja podataka sa korumpiranog računara. Zahteva veoma malo memorije (15MB) i to je veličina koja se može instalirati na USB fleš disk koji koriste policijski službenici. USB disk na koji se instalira *COFEE* bi trebao da sadrži minimum 1GB memorije ili više, i preporučuje se FAT32 fajl sistem. *COFEE* se može koristiti na licu mesta tj. mestu istrage, alat je veoma lak za korišćenje, pouzdan je i ne zahteva velika ulaganja. A može prikupiti nestabilne žive dokaze, koji se mogu izgubiti prilikom gašenja računara. Da je lak za korišćenje potvrđuje činjenica da ga mogu koristiti policajci sa minimalnim informatičkim znanjem, potrebno je 10-ak minuta da se kroz priručnik nauči upotreba ovog alata. Samim tim, ovaj alat omogućava da policajci koriste iste forenzičke mogućnosti kao eksperti digitalne forenzike, da prikupe važne dokaze, a da ne urade nista drugo osim jednostavnog stavljanja USB uređaja na računar (*Slika 13*). *COFEE* može da locira delove hard diska koji su kompjuterski kriminalci koristili za krađu identiteta, *online* prevare, dečiju pornografiju i druge slične zločine. Ovaj potpuno prilagodljivi alat omogućava kreiranje izveštaja u jednostavnom *HTML* formatu koji se kasnije može veoma lako tumačiti i koristiti kao dokaz za dalju istragu i krivično gonjenje osumnjičenog pred sudom. Ovaj alat koji je potpuno besplatan koriste agencije za sprovođenje zakona u 187 zemalja širom sveta.

COFEE zahteva *Windows XP* operativni sistem. Na drugim OS nije testiran, ali prema rečima *Microsoft*-a i ljudi koji rade na razvoju ovog programa, sledeće godine biće objavljena verzija koja će imati potpunu podršku *Windows Vista* i *Windows 7* operativnog sistema.²¹

²¹ <http://digiex.net/downloads/download-center-2-0/applications/2812-cofee-microsoft-forensic-tool-download.html>, od petka 28.10.2011. god.



Slika 13. Preuzimanje podataka sa računara preko USB-a koji poseduje COFEE

2.5.8 Helix

Helix je komercijalna *Linux* distribucija bazirana na *Ubuntu* odnosno *Debianu* namenjena radu u oblasti IT sigurnosti, prvenstveno za digitalnu forenziku. Koristi *GNOME* grafičko okruženje i posjeduje mnoštvo forenzičkih alata. [6]

Aktuelna verzija *Helix 3* dostupna je u tri varijante i to:

- *Helix 3 Pro*,
- *Helix 3 Live Response* i
- *Helix 3 Enterprise*.

Helix 3 Pro je najnoviji član *Helix 3* grupe proizvoda, pokreće se sa *LiveCD*-a i služi za klasičnu forenzičku istragu i analizu. Prikaz *Helix boot* menija je prikazan na slici 14.

Helix 3 Live Response namenjen je prikupljanju podataka koji se nalaze u memoriji i pokreće se sa *USB drive*-a.

Helix 3 Enterprise namenjen je mrežnom okruženju gde je potrebno preventivno delovati, ali i vršiti analizu rizičnih ponašanja, kršenja pravila i hakerskih napada.

Prethodna verzija *Helix* distribucije bila je besplatna što je uticalo na široku rasprostranjenost ove distribucije²².



Slika 14. Helix 3 Pro LiveCD – prikaz Helix boot menija

2.6 Validacija i testiranje forenzičkih alata

Krajnji cilj svake digitalne forenzičke istrage, akvizicije i analize podataka jeste ekstrakcija čvrstih digitalnih dokaza koji optužuju, ili oslobađaju osumnjičenog i svedočenje pred sudom. Da bi digitalni dokaz bio prihvatljiv za sud, forenzičar mora biti spreman da, po zahtevu sudije, testira i vrednuje forenzički softverski alat sa kojim su dokazi procesirani u celom lancu istrage.

²² <http://hr.wikipedia.org/wiki/Helix>, od utorka 01.11.2011. god.

2.6.1. Metodologija ispitivanja validnosti forenzičkih alata

Metodologiju ispitivanja forenzičkih alata razvio je *NIST*²³. Ova metodologija je pokretana sa funkcionalnostima forenzičke istrage i ispitivanja digitalnih podataka. Aktivnost forenzičke istrage se deli u diskretne funkcije ili kategorije, kao što su zaštita upisivanja na HD, uzimanje imidža diska, pretraživanje nizova podataka itd. Trenutno je razvijena i ispitana metodologija za uzimanje imidža diska, a u toku je razvoj metodologije za ispitivanje softverskih alata za blokiranje upisivanja na disk. Sledeća kategorija za razvoj metodologije ispitivanja su alati za oporavak izbrisanih fajlova [3].

U prvoj razvijenoj metodologiji ispitivanja alata za uzimanje imidža čvrstog diska ispitani su *Linux dd* i *SafeBack*. Iz kategorije blokatora upisivanja testiran je alat *RCMP hdl*.

Razvoj specifikacija procesa za ispitivanje alata

Posle kategorije alata i jednog alata iz kategorije za ispitivanje, razvija se proces za ispitivanje alata sa sledećim fazama:

- Razvoj dokumentovanih zahteva od strane iskusnih forenzičara i specijalista za testiranje i kriterijuma i slučajeva za testiranje, tzv. specifikacija kategorije alata.
- Specifikacija kategorije alata se postavlja na web stranicu za direktnu, višestruku reviziju kompjuterske forenzičke zajednice i javne komentare drugih interesnih grupa.
- Relevantni komentari i povratne informacije se ugrađuju u specifikaciju.
- Dizajnira se radno okruženje za kategoriju alata.

Proces testiranja softverskih forenzičkih alata

Posle razvoja specifikacije kategorije alata i izbora alata, tim za testiranja izvršava sledeći proces testiranja alata:

²³ *NIST – eng. National Institute of Standards and Technology*

- Nabavlja alat za testiranje,
- Revidira celu dokumentaciju,
- Selektuje relevantne slučajeve za testiranje, zavisno od nominalnih karakteristika alata,
- Razvija strategiju testiranja,
- Testira alat,
- Izrađuje izveštaj o testiranju,
- Supervizorsko telo pregleda izveštaj o testiranju,
- Isporučioc/proizvođači alata pregledaju izveštaj o testiranju,
- Postavljaju alat na web stranicu,
- Nadležni entitet postavlja izveštaj o testiranju na web lokaciju.

NIST je razvio opšti pristup za testiranje kompjuterskih forenzičkih alata, sa opštim kriterijumima za testiranje. Generalno, nedostaju standardi ili specifikacije koje opisuju šta forenzički alati treba da rade i šta treba da imaju da bi prošli strogu proceduru pravosudnog procesa.

NIST kriterijumi za validaciju i testiranje forenzičkih alata bazirani su na standardnim metodama testiranja *ISO 17025* - kriterijumima za testiranje komponenti za koje ne postoje standardi. Forenzička laboratorija mora zadovoljavati sledeće kriterijume i održavati preciznu evidenciju:

- Uspostaviti kategorije kompjuterskog forenzičkog alata: grupisati softverske alate prema ekspertski specifikovanim kategorijama, na primer, forenzički alati dizajnirani za izvlačenje podataka, alati za praćenje traga *e-mail* poruka itd.,
- Identifikovati zahteve za svaku kategoriju kompjuterskih forenzičkih alata: za svaku grupu opisati tehničke karakteristike, ili funkcije koje forenzički alati moraju imati u toj kategoriji.
- Razviti proceduru testiranja za verifikaciju alata: na bazi zahteva razviti proceduru za testiranje kojom se dokazuje, ili opovrgava navedena mogućnost forenzičkog alata u odnosu na zahteve. Na primer, forenzički alat za oporavak podataka mora biti sposoban da izvuče podatke iz *RAM slack* prostora fajla.
- Identifikovati slučaj za testiranje: pronaći i razviti tipove slučajeva za ispitivanje sa forenzičkim alatom. Identifikovati informacije za izvlačenje iz uzorka diska ili

drugog medija. Na primer, koristiti imidž zatvorenog test fajla koji je generisan sa poverljivim forenzičkim alatom za testiranje novog forenzičkog alata u istoj kategoriji i videti da li su rezultati isti.

- Uspostaviti i razviti metod testiranja: razmatrajući namenu i dizajn alata, specifikovati metod kako testirati forenzički alat i kakve instrukcije treba da ga prate.
- Izveštaj o rezultatima testiranja: opisati rezultate testa u izveštaju koji je u skladu sa *ISO 17025* standardom, koji zahteva da izveštaj o testiranju mora biti tačan, jasan, nedvosmislen i objektivan.

Drugi standard, *ISO 5725*, zahteva tačnost za sve aspekte procesa testiranja alata, što znači da rezultati testiranja moraju biti ponovljivi i reproduktivni. Ponovljivost rezultata znači da ako forenzičar radi sa jednim alatom u istoj laboratoriji i na istoj mašini, alat mora generisati jednak rezultat. Reproductivnost rezultata znači da ako forenzičar radi sa jednim alatom u različitoj laboratoriji i na različitoj mašini, alat mora generisati jednak rezultat – izvući iste informacije [3].

Procedura za validaciju forenzičkih alata

- Izvlačenje i ispitivanje dokazujućih podataka sa jednim alatom.
- Verifikacija dobijenih rezultata izvršavanjem istih zadataka sa sličnim softverskim forenzičkim alatom.
- Za zadovoljenje kriterijuma za validaciju forenzičkog softverskog, ili hardverskog alata, potrebno je koristiti najmanje dva alata.
- Analitički alat za upoređivanje rezultata primene oba forenzička alata, mora biti dobro ispitan i verifikovan.
- Forenzičar mora dobro poznavati korišćeni forenzički alat i imati poverenje u njegove performanse, u slučaju zahteva sudije za neko obrazloženje.

Kao najjednostavniji metod za verifikaciju novog forenzičkog alata i upoređivanje rezultata za korišćenje disk editora, kao što je *Norton DiskEdit*, *HexWorkShop* ili *Win Hex*, koji omogućavaju čitanje podataka u sirovom formatu, tipično prikazuju fajlove, hedere fajlova, fajl slack prostor, *RAM slack* i druge podatke na fizičkom disku.

Problemi mogu biti kod ispitivanja kompresovanih fajlova (*ZIP* ili *PST MS Outlook* fajlova).

Za validaciju novog forenzičkog alata sa pouzdanim GUI forenzičkim alatima tipa *FTK* i *EnCase*, primeniti sledeću proceduru:

- Izvršiti ispitivanje digitalnih dokaza sa jednim GUI forenzičkim alatom.
- Izvršiti isto ispitivanje sa disk editorom (*Win Hex* ili *HexWorkShop*) i verifikovati da li GUI forenzički alat vidi iste podatke na istom mestu na testiranom ili imidžu osumnjičenog diska.
- Kada se fajl oporavi, odrediti heš vrednost u GUI alatu i u disk editoru, a zatim uporediti vrednosti i verifikovati integritet fajla.
- U većini slučajeva *FTK* i *EnCase* forenzički alati služe kao referentni pouzdani alati za verifikaciju drugih forenzičkih alata, jer su široko priznati u pravosudnim sistemima brojnih država.
- Postoje brojni forenzički alati koji mogu uspešno dopuniti kapacitete *FTK* i *EnCase* alata i treba ih koristiti.

Ažuriranje zakrpe (fiksiranje, pečovanje), ili nadogradnja postojećeg alata, potrebno je takođe verifikovati, da bi se sprečila korupcija digitalnih dokaza. Ako se utvrdi da novo fiksiranje, ili nadogradnja nisu pouzdani, taj se alat ne može koristiti za forenzičku akviziciju i analizu digitalnih podataka, dok se problem ne otkloni.

Prva mogućnost je da se generiše izveštaj o grešci i dostavi snabdevaču, koji treba da dostavi novu fiksiranu zakrpu. Sledeći korak je nova runda testiranja validnosti pečovanog/nadograđenog alata²⁴.

Najbolji način da se testiraju novi pečevi i nadogradnja je formiranje HD za testiranje i skladištenje podataka u nekorišćeni prostor alociran za fajl, odnosno u fajl *slack* prostor. Zatim treba koristiti softverski forenzički alat za izvlačenje tih podataka. Ako je moguće izvući podatke sa forenzičkim alatom i verifikovati rezultat sa drugim alatom, to znači da je alat pouzdan [3].

²⁴ Grubor G., Milosavljević M. (2007), „Digitalna forenzika“, Univerzitet Singidunum, Beograd, str. 90

Kako se vremenom razvijaju i forenzički alati, potrebno ih je regularno fiksirati novim zakrpama i nadograđivati novim verzijama. Pri tome treba primenjivati navedenu proceduru za ispitivanje validnosti nove verzije softverskog ili hardverskog alata.

2.7 Forenzika USB Flash memorijskog uređaja

2.7.1 Uvod

Digitalna forenzika je relativno nova naučna disciplina koja nalazi svoje mesto u pravosudnom sistemu. Prate je brojni izazovi, uključujući brze promene računarskih i digitalnih uređaja, kao i sve sofisticiranijih napada na računarske sisteme i mreže i rapidni porast zloupotreba IKT sistema i kompjuterskog kriminala.

U ovom radu ćemo govoriti o USB fleš memorijskim uređajima i procesu oporavku podataka sa istog. *Šta je zapravo to USB fleš?* USB fleš, ili kako mu je pravo ime, *USB Memory Drive* ili *Keydrive*, je mali prenosni uređaj za skladištenje podataka koji koristi flash memoriju (eng. *flash memory*) i USB konektor. Kao i čvrsti disk, USB fleš disk skladišti informacije, ali pomoću fleš diska možete lako preneti informacije sa jednog računara na drugi. USB fleš diskovi se razlikuju po veličini i obliku i mogu da sadrže gigabajte informacija. USB fleš diskovi zovu se i diskovi olovke, diskovi privesci za ključeve, diskovi ključevi i memorijski ključevi²⁵.

Priključuju se u normalan tip-A USB priključak, bilo na kompjuteru ili na USB hub-u. Uređaj se napaja preko USB priključka na PC-u i nije mu potrebno spoljno napajanje. Za razliku od ostalih prenosivih medija za skladištenje podataka, USB fleš koristi poluprovodničku tehnologiju (čipove) za čuvanje podataka. Ovo ih čini otpornim na fizička oštećenja i prašinu. Njihov kapacitet se menjao, od početnih 16MB do današnjih nekoliko gigabajtova. U 2003 većina USB fleš uređaja je radila na USB 1.0/1.1 standardu sa brzinom od 12 Mb/s. Od 2004 novi USB fleševi podržavaju USB 2.0 interfejs, sa maksimalnom brzinom čitanja od oko 100 Mb/s i nešto sporijom brzinom upisivanja podataka. U idealnim uslovima, ovako sačuvani podaci mogu opstati oko 10 godina, ali se ipak kao forenzički dokaz uzimaju podaci ne stariji od 6 meseci.

²⁵ <http://windows.microsoft.com/sr-Latn-CS/windows7/What-is-a-USB-flash-drive>, od petka 11.11.2011. god.

Fleš memorija je računarska memorija koja može da čuva podatke čak i kada nije pod naponom, a može se brisati i reprogramirati elektronskim putem. Ali čak i nakon brisanja podataka moguće ih je oporaviti uz pomoć nekih softversko-forenzičkih alata.

2.7.2 USB flash memorija

Svesni smo da mnogi ljudi danas sve svoje digitalne podatke čuvaju uz sebe, u svom džepu na popularnim flaševima. Samim tim digitalni forenzičari moraju se prilagoditi novonastalim uslovima i kao što su se nekad upoznavali sa mehanikom rada hard diskova, danas se moraju upoznati sa načinom rada fleš memorija.

Fleš memorija je postala dominantna na tržištu od kako se pojavio *USB flash drive*, koji se koristi za čuvanje i razmenu podataka između računara, i sve pohvale koja je fleš memorija pokupila krajem 20. veka pa sve do danas, dolaze upravo od *USB flash drive-a*.

USB flash drive je mobilan i moćan memorijski uređaj: mali, lagan, prenosiv, sa mogućnošću pisanja i brisanja podataka. Krajem 2000. godine počela je prodaja prve USB fleš memorije, koju danas popularnije zovemo *USB stick*, a prvi *USB stick* koji je proizveden imao je kapacitet od 8 MB. Od tada pa do danas kapacitet *USB stickova* rastao je iz godine u godinu tako da ih danas možemo pronaći sa kapacitetom od 128MB do 64GB. *USB stick* danas je jedan od najpopularnijih načina za prenos podataka jer je vrlo jednostavan za korišćenje. Danas, maksimalan kapacitet *USB flash drive-a* je zvanično 320GB, a pre samo godinu dana kapacitet od 8GB se smatrao luksuzom. Kapacitet je ograničen samo u zavisnosti od trenutne "gustine" fleš memorije [4].

Svaki USB fleš uređaj se sastoji od nekoliko osnovnih elemenata. To su u prvom redu NAND fleš memorijski čip i USB kontroler koji računaru ili nekom drugom uređaju omogućava pristup fleš memoriji. Ostatak čine generator takta, dodatni kontakti za programiranje i testiranje uređaja pri proizvodnji, led dioda za indikaciju rada i na kraju sama štampana pločica na koju su sve ove komponente integrisane.

Na štampanoj pločici je i fizički USB konektor kojim se uređaj priključuje na računar (*Slika 15*).



Slika 15. Spoljašnji izgled jednog USB fleša

USB fleš uređaj se sastoji od male printane ploče, na kojoj se nalazi fleš memorija, zatvorene u neko plastično ili metalno kućište.²⁶ *USB flash drive* ima velike prednosti u odnosu na ostale prenosive memorijske uređaje kao što su magnetne diskete i trake, ali i optičke memorije (CD, DVD). Kompaktniji su, generalno brži, mogu da nose veliku količinu podataka, i veoma su pouzdani (fizički pre svega). Moderni operativni sistemi tipa *Linux*, *Mac OS*, i *Windows*, imaju hardversku podršku za uređaje poput USB fleš memorija.

Poreklo i razvoj flash memorije

Prva kompanija koja je proizvela fleš memoriju i uvela je na tržište je bila *Intel*. U 1988. godini, ova grupacija je lansirala 256-bitni fleš čip - veliki kao kutija za cipele. *Intel* je prikazao prednosti "ugrađene memorije" koristeći jedan od starih magnetofona, koji bi lako mogao da napuni manji kofer. Intelov pronalazak je bio

²⁶ http://bs.wikipedia.org/wiki/USB_stick, od nedelje 18.09.2011. god.

takozvani NOR fleš, razvijen iz EPROM i EEPROM tehnologija za čipove i opremljen interfejsom za SRAM memoriju. NOR fleš je imao brzine upisivanja i brisanja koje bi se mogle smatrati sporim prema današnjim standardima i mogao je da izdrži samo mali broj ciklusa upisivanja (oko 100 000). On je bio primenjivan u oblastima gde su se stalno uskladišteni podaci samo povremeno i retko menjali.

Na primer, operativni sistemi digitalnih centrala ili mobilnih telefona su bili smeštani u jedinicama NOR fleš memorija. Za razliku od prethodnih tehnologija, fleš je omogućio da se brišu ili skladište podaci na više mesta u jednom koraku; to je predstavljalo ogromnu prednost u brzini. Ipak, čak i danas, trajna priroda ove memorije smatra se jednom od njenih najvećih prednosti. Druga vrsta fleš memorije je NAND fleš, projektovan 1989. godine u kompaniji Toshiba, i uspostavljen kao jeftinija i brža alternativa NOR flešu. Toshiba je takodje bila prva kompanija koja je koristila naziv fleš (*Flash*). U poredjenju sa NOR, NAND tehnologija je ponudila deset puta veći broj ciklusa upisivanja, i veće brzine i za skladištenje i za brisanje podataka. Memorijske ćelije u NAND memoriji su upola manje od onih u NOR memoriji. To za rezultat ima u najmanju ruku teorijsku manju cenu NAND memorije: manje dimenzije ćelije omogućavaju da se na datom prostoru ima veći kapacitet, što istovremeno znači i manju cenu za kupca i veću dobit za proizvođača. Prema proizvođaču fleša firmi *M-Systems*, NAND briše podatke za četiri milisekunde, dok NOR zahteva pet sekundi za isti proces. Razlog za ovo su veće dimenzije NOR blokova. – od 64 do 128 KB. Suprotno tome, NAND pristupa blokovima veličine između 8 i 32 KB. Zbog svoje bolje performanse, NAND se obično koristi u memorijskim karticama – kao što su *Compact-Flash*, *SmartMedia*, *SD*, *MMC*, *xD* i *PC kartice*, *USB flash*.

Princip rada flash memorije

Fleš memorija smešta informacije u redove FTG-a (*Floating Gate Transistor*) koji se nazivaju "ćelijama", i svaki od njih smešta po jedan bit informacije. Uređaji novijih generacija, koji koriste fleš memoriju, mogu da smeštaju više od jednog bita informacija po ćeliji, koristeći više od dva nivoa električnog punjenja, i svaka sledeća informacija je smeštena na "lebdećem" ulazu ćelije. Kod fleš-a, svaka ćelija izgleda slično kao i ćelija kod standardnog MOSFET-a (*Metal Oxide Semiconductor Field-*

Efect Transistor), osim što ima dva ulaza umesto jednog. Jedan ulaz (*gate*), kao i kod ostalih MOS tranzistora, je kontrolni ulaz (CG), a drugi ulaz je lebdeći ulaz (FG), izolovan jednim oksidnim slojem koji se nalazi svuda oko njega. Lebdeći ulaz se nalazi između kontrolnog ulaza i podloge. Pošto je lebdeći ulaz izolovan njegovim oksidnim slojem, bilo koji elektron koji se nađe na njemu ostaje zarobljen tu, i na taj način smešta informaciju. Kada se elektroni nalaze na lebdećem ulazu, oni modifikuju (delimično prekidaju) električno polje koje se javlja sa kontrolnog ulaza, što modifikuje naponski impuls (V_t) ćelije. Na taj način, kada je ćelija "očitanja" postavljanjem određenog naponskog impulsa na kontrolnom ulazu, trenutno električno stanje će ili pročitati ili neće pročitati, u zavisnosti od naponskog impulsa (V_t) ćelije, koji je kontrolisan od strane broja elektrona na lebdećem ulazu. Ovo prisustvo ili odsustvo trenutnog električnog stanja je detektovano i prevedeno u nule (0) i jedinice (1), reprodukujući tako smešteni podatak. U uređajima koji smeštaju više od jednog bita informacija po ćeliji (tzv. Multilevel cell device), količina trenutnog proticanja će biti detektovana, da bi se utvrdio broj elektrona smeštenih na lebdećem ulazu. Da bi memorijska ćelija bila programirana, fleš kontrola dovodi kratak naponski impuls. Ovo okida lavinski proboj u memorijskom tranzistoru koji puni lebdeći ulaz (tzv. *hot-electron injection*)²⁷. Na ovaj način, 1 Mbitni čip fleš memorije može biti programiran za dve sekunde, za razliku od normalnih EEPROM-ova, međutim, brisanje čipa se izvršava istovremeno [4].

Tokom brisanja, kontrola fleš memorije koristi trenutno prebacivanje brisanja za slanje impulsa brisanja u celo polje memorijske ćelije, pa se brišu sve memorijske ćelije. Vreme brisanja za celu fleš memoriju je oko jedne sekunde. To svakako predstavlja problem forenzičarima, jer praktično znači da se prepisivanjem, briše i ne može rekonstruisati prethodni sadržaj. Centralni deo fleš memorije je matrica memorijskih ćelija. Ćelije su adresirane baferom adrese, koji prima signale adrese i prenosi ih do sektora redova i kolona, naizmenično. Fleš memorije ne izvršavaju multipleksiranje adrese. Dekoderi redova i kolona selektuju jednu liniju reči i jedan, ili više parova bitskih linija, kao i u uobičajenom memorijskom čipu. Čitljivi podatak izlazi preko ulazno/izlaznog bafera podataka, ili se upisuje u adresiranu memorijsku ćeliju ovim baferom preko U/I ulaza. Procesi očitavanja, brisanja i programiranja se

²⁷ Lam Kenny, Lau Derek, Lui Dennis, „USB Thumb Drive - Designer Reference Manual“, Hong Kong, 2004.

kontroliraju dvobajtnim instrukcijama, koje eksterni mikroprocesor upisuje u registar instrukcija fleš kontrole. Za tipičnu fleš memoriju dostupne su sledeće instrukcije:

- Čitanje memorije (*Read Memory*): fleš memorija obezbeđuje podatke preko pinova podataka;
- Očitavanje identifikatora memorije (*Read Identifier Code*): fleš memorija obezbeđuje kôd na pinovima podataka, koji označavaju vrstu i verziju čipa;
- Podešavanje brisanja/brisanja (*Set-up Erase/Erase*): priprema fleš memoriju za proces brisanja i izvršava brisanje;
- Brisanje-potvrđivanje (*Erase-Verify*): briše sve memorijske ćelije i potvrđuje ovaj proces;
- Podešavanje programiranja / programiranje (*Set-up Program/Program*): priprema programiranje pojedinačnih memorijskih ćelija i izvršava ovaj proces;
- Programiranje – potvrđivanje (*Program-Verify*): izvršava programiranje i potvrđuje ovaj proces;
- Resetovanje (*Reset*): resetuje fleš memoriju u definisano početno stanje.

Fleš memorija ima karakteristiku da je *non-volatile* odnosno da ne gubi podatke koji su upisani na nju nakon što nestane napajanje, kao što je slučaj sa klasičnom radnom memorijom u računaru.

Posebna ograničenja

Ono što ograničava fleš memoriju je to što se mora brisati jedan po jedan "blok". Ovo generalno svim bitovima u ćeliji dodeljuje vrednost 1. Počevši od sveže obrisane blok, svaka lokacija unutar tog bloka može biti programirana. Ipak, čim se bitu jednom dodeli vrednost 0, samo brisanjem celog bloka, bitu se može promeniti vrednost ponovo na 1. Drugim rečima, fleš memorija nudi nasumičan pristup operacije čitanja i programiranja, ali ne može da ponudi bilo kakav nasumičan pristup ponovnom pisanju (*rewrite*) ili operaciji brisanja. U odnosu na hard disk, fleš memorija ima konačan broj ciklusa za brisanje i pisanje (*erase write cycles*) tako da se ovo mora malo ozbiljnije uzeti u obzir, pogotovo ako na nekom USB flash drive-u imamo instaliran neki operativni sistem. Ipak većina komercijalnih USB fleš memorijskih uređaja uglavnom garantuje 1 milion ciklisa.

Razvoj flash fajl sistema

Zbog posebnih karakteristika fleš memorije, njena upotreba je najefikasnija ako se koristi pod posebno dizajniranim fajl sistemima. Osnovni koncept "ispod haube" fajl sistema je: kada magacin fleša treba da se ažurira, fajl sistem će napisati novu kopiju promenjenih podataka na svež blok, postaviće nove pokazivače (*pointer-e*), i obrisće stari blok kada bude imao vremena. Jedan od starijih fleš fajl sistema bio je *Microsoft-ov* FFS2, koji je korišćen za rad pod MS-DOS-om. Oko 1994. *PCMCIA Industry Group*⁸ je odobrila FTL (*Flash Translation Layer*) specifikaciju, koja je dozvoljavala fleš uređaju da izgleda kao FAT disk. Drugi komercijalni sistemi, kao što je *FlashFX* kompanije *Datalight*, su bili tako kreirani da bi izbegli probleme sa patentima FTL-a. JFFS je bio prvi specifičarni fleš fajl sistem za *Linux*, koji je ubrzo zamenjen fajl sistemom JFFS2, a 2003. se pojavio YAFFS.²⁸ Ove fleš fajl sistem, u malom broju, uglavnom koriste digitalne kamere, foto aparati i sl. uređaji. Danas se u 76% slučajeva digitalni forenzičari susreću sa pseudo FAT fajl sistemom za skladištenje podataka na fleš memorijama, ali su sve brojniji i oni na kojima je NTFS fajl sistem i brojni drugi sistemi koji podržavaju fleš memorije. Istražiteljima to može predstavljati problem, jer se struktura fajlova često razlikuje od onih u *Windows* i *Linux* fajl sistemima [4].

Kapacitet flash memorije

Svaki čip fleš memorije doseže kapacitet od kilobit-a (128 *byte*-a) do nekoliko gigabita (1,073,741,824 bit-a). Čipovi su uglavnom sakupljeni zajedno kako bi se postigao što veći kapacitet memorije²⁹.

Brzina flash memorije

Uređaji koji koriste fleš memoriju su dostupni na različitim brzinama. Neki su optimizovani za brzinu od 2MB po sekundi, 12MB po sekundi itd. Ostale memorijske kartice su rangirane po 100x, 130x, 200x, itd. Za takve kartice, 1x znači da je brzina

²⁸ http://en.wikipedia.org/wiki/Flash_file_system, od utorka 15.11.2011. god.

²⁹ Lam Kenny, Lau Derek, Lui Dennis, „USB Thumb Drive - Designer Reference Manual“, Hong Kong, 2004.

prenosa podataka 150KB po sekundi, tj. brzina kojom su prvi napravljeni CD (eng. *Compact Disc*) uređaji mogli da prenose informacije.

Oštećenje podataka na flash memoriji

Najčešći razlog zbog kojeg dolazi do oštećenja podataka je taj što nekada ljudi uklone uređaj sa fleš memorijom (*USB flash drive* na primer) u toku pisanja podataka na nju. Situacija bi bila još gora ako uz to ne bi koristili i odgovarajući fajl sistem, ili ako bi usledila asinhronizacija (gde podatak i dalje čeka da bude napisan, a uređaj je već uklonjen) [4].

2.8 Korišćenje USB flash memorije u praksi

Danas se u velikom broju koriste *USB flash* memorijski uređaji, koji su postali neizbežni. Svojim rasprostranjivanjem sa tržišta polako izbacuju hard diskove i CD/DVD diskove. Količina podataka koja se na njima nalazi iz dana u dan je sve veća. Međutim ta rasprostranjenost može da izazove i neke negativne posledice. Svako ko želi da prokrijumčari ili ukrade podatke, a da pritom ne bude otkriven, može veoma lepo da iskoristi ove USB uređaje, iz jednostavnog razloga što može da se desi da ih uobičajene sprave za detektovanje uopšte ne registruju.

2.8.1. Prenos ličnih podataka

Danas se USB fleš ponajviše koristi da bi se sačuvali i nosili sa sobom lični podaci, kao što su dokumenti, slike, audio – video zapisi, itd. Osim toga oni preuzimaju prevlast u još nekim sferama. Jedan od primera jeste pojava takozvanih „Portabl aplikacija“ uz pomoć kojih se na fleš disku može naći i baza mail poruka, istorija posećenih stranica i sl.³⁰ Sve niža cena fleš memorija dovela je do toga da se neretko sreću veličine od 16GB. Ako uzmemo u obzir da prosečan *MS Word* dokument od deset stranica ima veličinu od oko 60kB, znači da potencijalno možete snimiti 280.000 dokumenata, ili 3 miliona stranica, na jednom disku. Takva priuštivost, prenosivost i kapacitet tih uređaja stavili su ih na među dva najveća rizika

³⁰ Lam Kenny, Lau Derek, Lui Dennis, „*USB Thumb Drive - Designer Reference Manual*“, Hong Kong, 2004.

za kompanije, ali i pojedince. Krađa fleš diska predstavlja krađu intelektualnog vlasništva vlasnika, ali često i trajni gubitak podataka. Kada jednom padnu u pogrešne ruke, ovi podaci mogu otići u konkurentske kompanije, u javnost, ili čak da posluže za krađu identiteta. Evropska agencija za sigurnost mreža i zaštitu podataka (*ENISA*³¹) procenila je nedavno da je šteta pri svakoj krađi informacija sa USB fleš uređaja oko 7.000 evra, kada je reč o pojedincima, ili čak 1,3 miliona kada su u pitanju kompanije ili državne institucije. U zaključaku tog istraživanja *ENISA*, je kao meru zaštite predložila, kompanijama i institucijama da uvedu pravilo da se zabrani korišćenje ličnih USB memorijskih uređaja na radnom mestu. Moderni forenzički alati mogu, u slučaju da se sumnja da je neko uz pomoć USB fleš memorije ukrao poverljive podatke otkriti kada je bio spojen na kompjuter, proizvođača, serijski broj, ali i što je najbitnije i podatke iako je korisnik pokušao da ih obriše.

2.8.2. Automatsko prikupljanje podataka

Bez nekog velikog iskustva prosečni Internet korisnik može lako doći do programa koji će njegov fleš disk pretvoriti u takozvanog USB lopova. Gotovih rešenja je na sve strane, a ne mora se biti veliki programer, a da se napravi autorun fajl, koji će pokrenuti softver koji će sa žrtvinog računara pokupiti sve šifre, chat istoriju, otvorene portove. Najveću popularnost imaju alati firme *NirSoft*, ali postoje i firme koje kao gotov proizvod prodaju USB kradljivce mnogo većih mogućnosti. Takvi programi mogu u rukama digitalnog forenzičara postati i dobar alat, ali su slučajevi takvog korišćenja još uvek retki, pre svega jer se tako prikupljeni podaci ne mogu smatrati valjanim dokazima.

2.8.3. Širenje zlonamernog softvera

Prema izveštaju firme *Sophos*, četvrti po redu način širenja računarskih virusa i crva u 2008. godini jeste uz pomoć prenosnih memorijskih uređaja. Možda najbizarniji primer ovakvog načina prenosa zloćudnih programa koji se dogodio tokom 2008. godine je onaj kada su astronauti iz NASA-e nepažnjom preneli crv *W32.Gammima.AG* putem USB memorije na internacionalnu svemirsku stanicu.

³¹ *ENISA – eng. European Network and Information Security Agency*

Antivirusni program je, srećom, detekovao zlonamerni program, ali su posledice mogle biti katastrofalne.

2.8.4. Forenzički alat

Do skora ne zamenjivi mediji prilikom digitalne forenzike Live CD i DVD diskovi polako gube primat, pred najezdom USB fleš memorija. USB disk može poslužiti za podizanje Live operativnog sistema, tj. sistema koji neće ugroziti podatke na postojećem čvrstom disku računara, ali se danas najčešće koristi za pravljenje duplikata digitalnog mesta krivičnog dela. Takođe u popravci računara i backupu podataka USB memorije postaju nezaobilazni alat. Često se na njima drži neki antivirus program kao i ostali programi za softversko održavanje sistema i sistemsku administraciju. Kompanija *SanDisk* predstavila je USB fleš koji automatski pravi backup podataka na mreži tako da, za slučaj da se on pokvari ili izgubi, datotekama se jednostavno može pristupiti putem Interneta.

2.8.5. Sigurnost podataka na fleš memorijama

Većina korisnika koji za prenos podataka koriste USB fleš ne razmišlja mnogo o sigurnosti podataka koji su snimljeni na njemu. Ipak ima onih kojima je sigurnost na prvom mestu³². U upotrebi je više različitih rešenja koja mehanički štite fleš diskove i memorijske kartice. Proizvođači u svojoj ponudi imaju rešenja i za one koji ne žele da podaci koji su snimljeni na USB flešu dođu u pogrešne ruke. Nekada se sve svodilo samo na prekidač kojim bi se zabranio upis, ali zbog njegove beskorisnosti prestalo sa proizvodnjom takvih rešenja. Najnovija rešenja pružaju 256 bitnu hardversku enkripciju podataka. Neretko je moguće čak i kreirati višestruka zaštićena područja koja su zaštićena posebnom lozinkom ili otiskom prsta na skupljim uređajima. Podaci se u ta područja mogu jednostavno kopirati i biće automatski kriptovani u „letu“. Kao dodatak, u mnoge, je ugrađena „File Shredder funkcija“ koja uklanja sve tragove obrisanih podataka. Na taj način nije ih više moguće rekonstruirati posebnim forenzičkim programima već su obrisani zauvek. Do sada su bili podržani isključivo *Windows* sistemi, a sada i *Mac* korisnici mogu

³² Lam Kenny, Lau Derek, Lui Dennis, „USB Thumb Drive - Designer Reference Manual“, Hong Kong, 2004.

iskoristiti mogućnosti koje nude drajvovi sa povišenim stepenom bezbednosti podataka. Osim hardverskih postoje i mnoga softverska rešenja kao što je *USB Lock AP* kompanije *Advanced Systems International* koji prebacivanjem samo 3 fajla na USB disk omogućava iste funkcionalnosti kao i hardverska zaštita. U slučaju da se želi potpuna zabrana rada sa USB memorijama malom izmenom u *Windows registry* bazi može se omogućiti neometan rad ostalih USB uređaja, koji se priključuju na PC, a zabraniti korišćenje fleš diskova³³.

2.9. Forenzika USB uređaja

Do prenosivih USB memorija, kod kompjuterskih kriminalaca, teško je doći, zbog njihove izuzetno male veličine. Tehnikama pronalaska se nećemo baviti u ovom radu, već samo metodama koje forenzičari trebaju da primene kada već imaju USB memorijski uređaj „u rukama“. Sa forenzičkog aspekta važno je da forenzičar pouzdano identifikuje tip USB uređaja sa kojim radi. Jedna od mogućnosti je pažljivo ispitivanje kućišta USB uređaja, ali i ovo nije sigurna metoda, jer može predstavljati zamku. Forenzičar ne sme da pretpostavlja koji je tip USB uređaja u upotrebi. Svakako uvek mora imati na umu da je osumnjičeni mogao da zameni kućište USB uređaja i da se unutra nalazi memorija drugog proizvođača. Osim standardnih metoda koje se primenjuju pri digitalnoj forenzici forenziku USB memorija treba obaviti u više faza.

2.9.1. Utvrđivanje relevantnih činjenica

Pre pristupanja pravljenja slike prenosive USB memorije kao digitalnog dokaza digitalni forenzičar treba da utvrdi i sve detalje neophodne za kompletan opis budućeg posla. Posebnu pažnju treba usmeriti na tip i oznaku memorije, specijalne oznake, vrste enkripcije ako postoje, vrstu fajl sistema, tipove potrebnih datoteka i sl.

³³ <http://www.pcchip.hr/sigurniji-rad-s-usb-memorijama/>, od srede 09.11.2011. god.

2.9.2. Izrada procene uspešnosti

U ovoj fazi forenzičar mora da utvrdi da li je osumnjičeno lice obrisalo tj. pokušalo da uništi digitalne dokaze, te ne osnovu ranije utvrđenih činjenica pravi procenu uspešnosti oporavka podataka u svrhu obezbeđivanja validnosti oporavljenih podataka kao dokaza pred sudom.

2.9.3. Kreiranje kopije podataka

Većina fleš memorijskih uređaja izgleda slično – memorijski čip prati odgovarajući kontroler. Ova dva elementa čine praktično ceo uređaj odnosno memoriju. Memorijski čip je u skoro svim vrstama memorijskih kartica, USB flash diskova kao i većini drugih digitalnih uređaja baziran na NAND tehnologiji i dolazi u klasičnom TSOP-48 kućištu. Svakako činjenica da se algoritam upisa/čitavanja podataka razlikuje od proizvođača do proizvođača, u znatnoj meri otežava proces spašavanja podataka. Iako veliki broj poznavaoaca računarske tehnologije smatra da je spašavanje podataka sa ovih memorija nemoguće, ta izjava je tačna samo u slučaju kada je memorijski čip uništen (slomljen ili pregoreo). Ovo se naravno odnosi na memorije nad kojima nije izvršeno namerno prepisivanje podataka ili memorije koje imaju izvesne hardverske ili softverske sisteme zaštite. Što se ostalih hardverskih problema tiče daleko je veća verovatnoća otkaz kontrolera, odnosno čipa koji je zadužen za upis podataka u memoriju kao i za čitanje podataka. U tom slučaju postoje velike šanse, da se u pomoć odgovarajućeg softversko-forenzičkog alata ostvari 100% uspeh spašavanja podataka.

2.10 Studija slučaja (Case Study)

U ovoj studiji slučaja (*eng. Case Study*) ćemo prikazati istragu kompjuterskog incidenta na korporacijskom nivou u jednoj banci, od strane nezadovoljnog radnika koji je osumnjičen za delo kompjuterskog kriminala.

U odnosu na zvaničnu digitalnu forenzičku istragu, istraga kompjuterskog incidenta na korporacijskom nivou, može se smatrati predistražnim postupkom, a odvija se u tri glavne faze:

- pokretanje istrage,
- određivanje karaktera kompjuterskog incidenta i
- analiza digitalnih podataka.

Pokretanje istrage obuhvata obezbeđenje mesta incidenta, pretragu, akviziciju dokaza, izradu hipoteze o upadu i istraživanje alternativnih objašnjenja. Određivanje karaktera incidenta obuhvata analizu incidenta, analizu dokaza skupljenih u prvoj fazi zajedno sa alternativnim objašnjenjima, da bi se odredilo da li je u pitanju bezbednosni incident sa krivičnim delom, ili prirodan događaj. Analiza digitalnih podataka obuhvata analizu celokupnog dokaznog materijala, pripremu digitalnih dokaza za prezentaciju incidenta i drugih nalaza istrage vlasniku IS, ili zvaničnim organima, ako to vlasnik odobri [2].

Procedura korporacijske istrage kompjuterskog incidenta, u opštem slučaju, obuhvata i sledeće postupke:

- Proveru evidencija, log fajlova, kao i ostalih informacija o osumnjičenom;
- Ispitivanje zaposlenih;
- Kontrolu svih faza istrage;
- Pripremu organa za pretragu (lociranje kompromitvanog računara);
- Pretres resursa osumnjičenog i
- Prikupljanje i analizu dokaza.

Glavno težište klasične istrage krivičnog dela uvek je na svedoke i osumnjičene. U korporacijskoj istrazi kompjuterskog incidenta najbolja kombinacija je zajednički timski rad iskusnog organa istrage i eksperata za IT. U istrazi kompjuterskog kriminala, generalno, ne postoji super policajac koji sam može rešiti čak i relativno jednostavniji slučaj kompjuterskog kriminala. Na isti način, timskim radom treba istraživati i kompjuterske incidente na korporacijskom nivou – najmanje administrator zaštite, administrator sistema i forenzičar. Svaki učesnik ima svoj zadatak u skladu sa svojom specijalizacijom i znanjem.

2.10.1. Scenario kompjuterskog incidenta na korporacijskom nivou

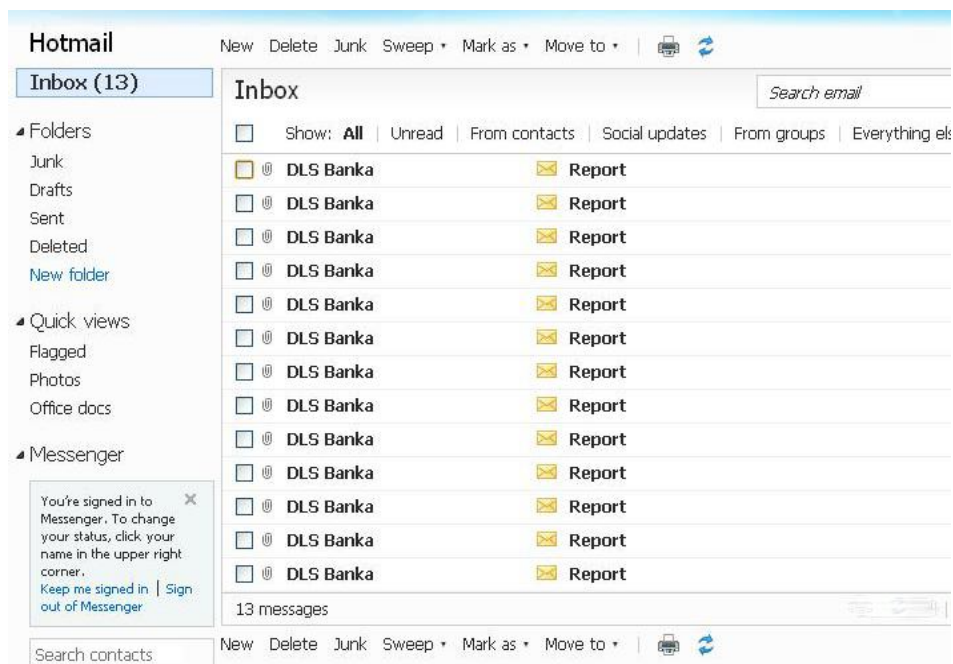
DLS banka je Nemačka banka koja ima svoju poslovnicu u RS, koja veoma uspešno posluje već duži niz godina. Svi zaposleni su radnici sa dugogodišnjim iskustvom iz oblasti finansija i bankarstva. U poslednjih godinu dana dešavale su se razne stvari polazeći od toga da se mesečni izveštaji ne poklapaju sa stvarnim novčanim stanjem u trezoru, pa su se morali ponovo obrađivati. Zatim, da se izveštaji sa berze izgube i da nije moguće utvrditi berzansko poslovanje, klijenti su se žalili da im na računima nedostaju neki manji novčani iznosi, koje je banka morala nadoknaditi. Sve ovo je bilo veoma dovoljno da se pokrene istraga kompjuterskog incidenta na korporacijskom nivou.

Poslovnica banke je angažovala interventni tim banke za istragu kompjuterskog incidenta. Direktor banke je odlučio da izvrši vlastitu inicijalnu istragu kompjuterskog incidenta na nivou banke, utvrdi karakter incidenta i tek onda, donese odluku o pozivanju zvaničnih organa istrage kompjuterskog kriminala. Uloga korporacijskih organa za istragu zloupotreba u IKT sistemu ograničena je zato što:

- većina organizacija nije opremljena odgovarajućim kapacitetima za istragu i forenzičku analizu i
- ovi organi istrage nemaju sva zakonska ovlašćenja za otkrivanje traga do napadača i zaplenu računarskih sistema napadača kao dokaznog materijala.

DLS banka je formirala svoj interventni (*CIRT*³⁴) tim za brzo reagovanje i istragu kompjuterskog incidenta, a prazninu u timu su popunili angažovanjem stručnog konsultanta za inicijalnu istragu, akviziciju i forenzičku analizu digitalnih dokaza. Za konsultanta su angažovali privatnu informatičku firmu sa znanjem i iskustvom u ovoj oblasti, kadrovski i materijalno opremljenu i osposobljenu za istragu i forenzičku analizu digitalnih dokaza. Sa firmom su potpisali ugovor u kome je navedena diskrecija i garancija da svi prikupljeni forenzički dokazi budu stroga tajna za koji niko ne sme znati, do trenutka utvrđivanja prirode incidenta i donošenja odluke vlasnika banke o (ne)uključivanju zvaničnih istražnih organa.

Nakon pokretanja istrage koja obuhvata obezbeđenje mesta incidenta, urađena je istraga i analiza svih računara koji se koriste i nalaze u banci, uz pomoć softversko-forenzičkog alata *EnCase*. Istraga se obavljala nakon završenog radnog vremena i bez prisustva ostalih radnika u strogoj tajnosti, tako da niko od zaposlenih ne posumnja da se radi o bilo kakvoj istrazi. Nakon nekoliko dana istraživanja na jednom računaru je pronađen instaliran *keylogger* koji je veoma vešto prikriven i koji je sve prikupljene podatke (brojeve računa klijenata, *password*-e, itd.) slao na *e-mail* osumnjičenom (*Slika 16*).



Slika 16. Izveštaji koje je keylogger slao na e-mail osumnjičenom

³⁴ *CIRT – eng. Computer Incident Response Team*

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR\Disk\Ven_TDKMedia&Prod_Trans-Ir_Drive&Rev_PM4P

07A6020855FA4FE80

07A6020855FA4FE80 ID Device (serial number)

Name	Type	Data
(Default)	REG_SZ	(value not set)
Capabilities	REG_DWORD	0x00000010 (16)
Class	REG_SZ	DiskDrive
ClassGUID	REG_SZ	{4d36e967-e325-11...
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USB
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{6080e081-ffad-58a...
DeviceDesc	REG_SZ	@disk.inf,%disk_de...
Driver	REG_SZ	{4d36e967-e325-11...
FriendlyName	REG_SZ	TDKMedia Trans-Ir...
HardwareID	REG_MULTI_SZ	USBSTOR\DiskTDK...
IdMfg	REG_SZ	@disk.inf,%genmar...
Service	REG_SZ	disk

68

2.10.2. Oporavak podataka sa USB flash uređaja

Pretresom celog objekta nije pronađen ni jedan USB uređaj koji odgovara *Registry* ključu iz *USBSTOR*-a. Sutradan su svi zaposleni radnici bili obavješteni da svi koji kod sebe imaju neke od USB uređaja predaju radniku obezbeđenja ili će biti pretreseni i kod koga se nadju takvi uređaji biće zaplenjeni. Nakon analize svih USB uređaja pronađen je uređaj koji se poklapa sa *Registry* ključem iz *USBSTOR*-a. Utvrđeno je ko je vlasnik USB uređaja i samim tim odmah se odredio i izdvojio potencijalni osumnjičeni, ali da bi se to dokazalo potrebno je izvršiti još neke digitalno-forenzičke analize i istraživanja.

Pronađeni USB uređaj je bio formatiran i na njemu nije bilo nikakvih podataka, moralo se pristupiti forenzičkoj istrazi, za te potrebe je korišten softversko-forenzički alat za digitalnu forenziku *EnCase* verzije 4. Većina ljudi misli da je potrebno formatirati USB uređaj, da bi se uništili tj. izbrisali podaci sa USB memorijskog uređaja. Donekle su u pravu, jer kada se posle formatiranja ponovo priključi USB uređaj videćemo da nema nista na njemu i da je prazan. *Da li je to zaista tako?* Uz pomoć *EnCase* softverskog alata za digitalnu forenzičku istragu, ti fajlovi se mogu pronaći i oporaviti, može se utvrditi vreme nastanka, upisa i poslednjeg pristupa padacima, kao i tip i veličina podataka. Američki stručnjaci iz FBI³⁵-a, koji se bave digitalnom forenzikom tvrde da se prepisani fajlovi mogu oporaviti i pronaći i posle 7 puta, dok Rusi tvrde da se i posle 26 puta brisanja i prepisivanja fajlovi mogu pronaći i oporaviti uz odgovarajuće hardversko-softverske alate za digitalnu forenziku.

Kada smo pronašli USB uređaj čiji se ključ poklapa sa *Registry* ključem iz *USBSTOR*-a i ustanovili da je USB fleš memorijski uređaj prazan, pokrećemo *EnCase* verzije 4, softverski alat/program za digitalnu forenziku. Kao što smo već rekli, *EnCase* je najpoznatiji i prvi prihvaćeni softverski alat zatvorenog programskog koda, namenjen forenzičkoj istrazi digitalnih dokaza, koji je proizvela firma *Guidance Software*³⁶.

³⁵ FBI – eng. Federal Bureau of Investigation

³⁶ <http://www.guidancesoftware.com/forensic.htm>, od utorka 20 .09.2011. god.

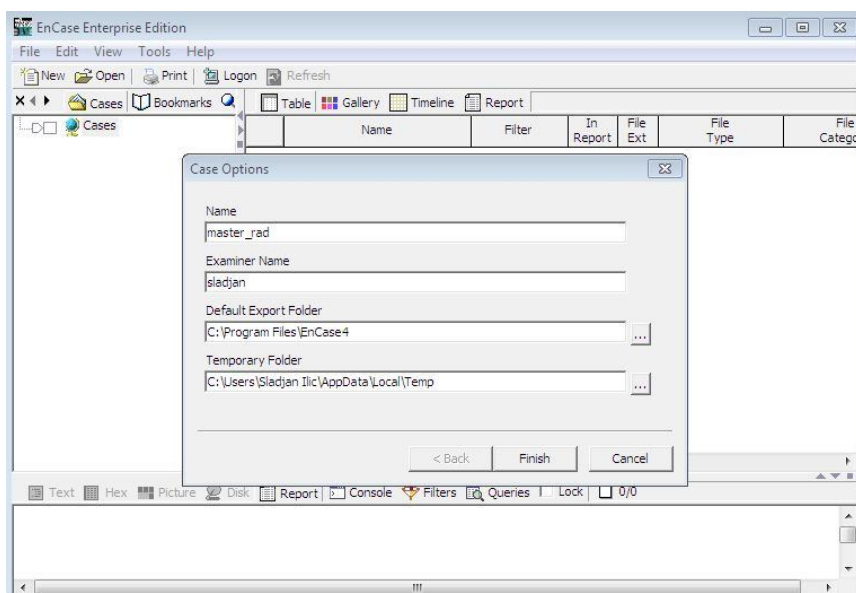
Smatra se jednim od najboljih i najčešće korišćenih softverskih forenzičkih alata. Na osnovu ovog softvera, kompanija *Guidance Software* je postala jedna od tri najveće svetske IT kompanije.

EnCase softversko-forenzički program omogućava i olakšava forenzičaru istragu, akviziciju i analizu dokaznog materijala. *EnCase* se danas koristi kao najnapredniji sigurnosti alat, a kao standard su ga prihvatile i neke vodeće kompanije i organizacije kao što su *Rolls Royce* i *NATO*. Isto tako, ovaj alat je rasprostranjen i koristi se pri primeni zakona u komercijalnim preduzećima za analizu i akviziciju podataka. Smatra se jednim od najboljih, i svakako je jedan od najčešće korištenih alata. *EnCase* kao alat omogućava i olakšava sudskim veštacima i stručnjacima iz IT okruženja istraživanje slučajeva, akviziciju i analizu dokaza i dokaznog materijala.

Dvoklikom na ikonicu *EnCase* softverskog alata (*Slika 18*), pokrećemo program, klikom na dugme *New* pojavljuje se dijalog za kreiranje novog slučaja (*New Case*). Unose se informacije kao što su ime slučaja, ime istraživača, *export* folder i folder za privremene (*temporary*) fajlove. Klikom na dugme *Finish* kreiran je novi prazan slučaj. (*Slika 19*).

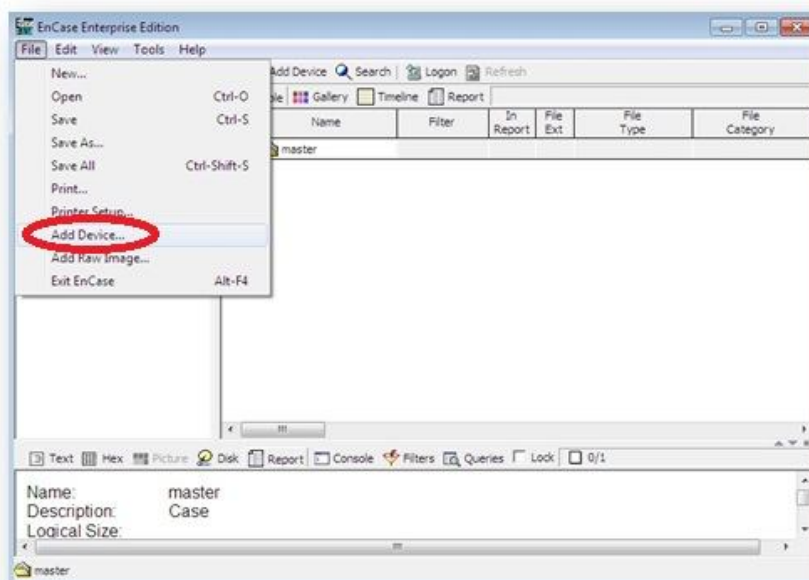


Slika 18. Ikonica EnCase alata za digitalnu forenziku

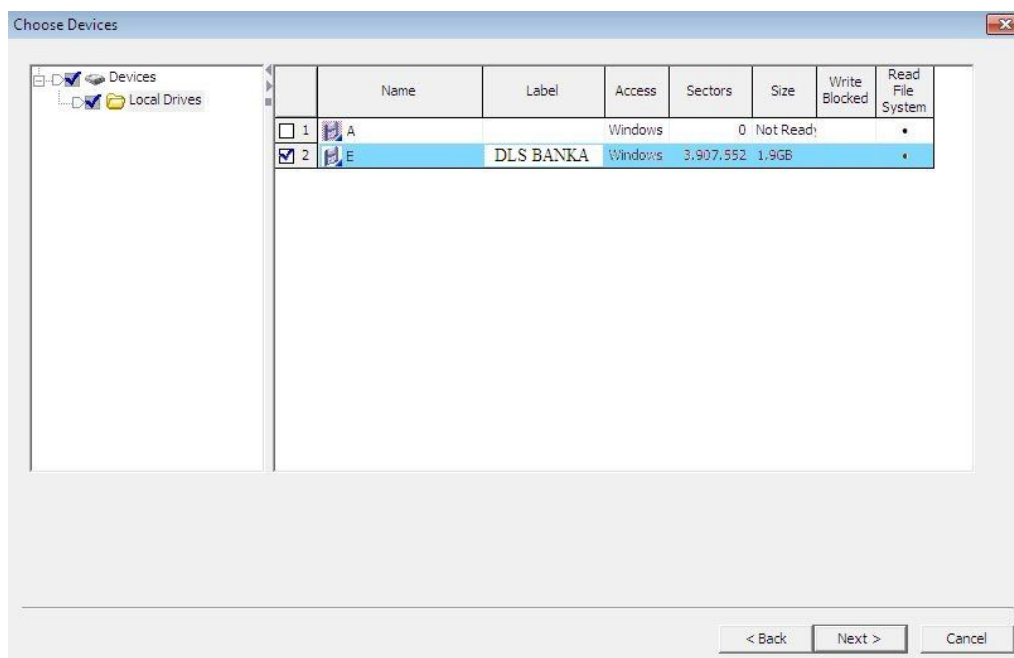


Slika 19. Pokretanje novog slučaja u EnCase alatu

Nakon pokretanja novog slučaja, idemo na opciju *Add Device*, iz Fajl menija i dodajemo dokazni materijal (Slika 20), tj. vršimo selekciju USB fleš memorijskog uređaja (Slika 21).



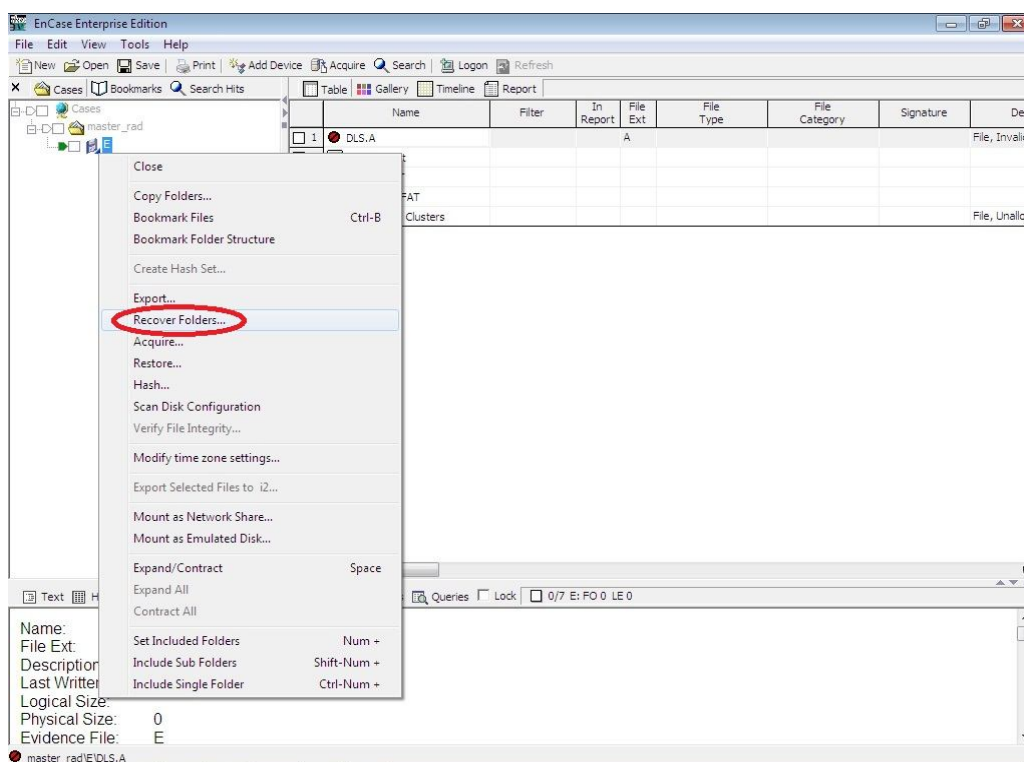
Slika 20. Dodavanje dokaznog materijala



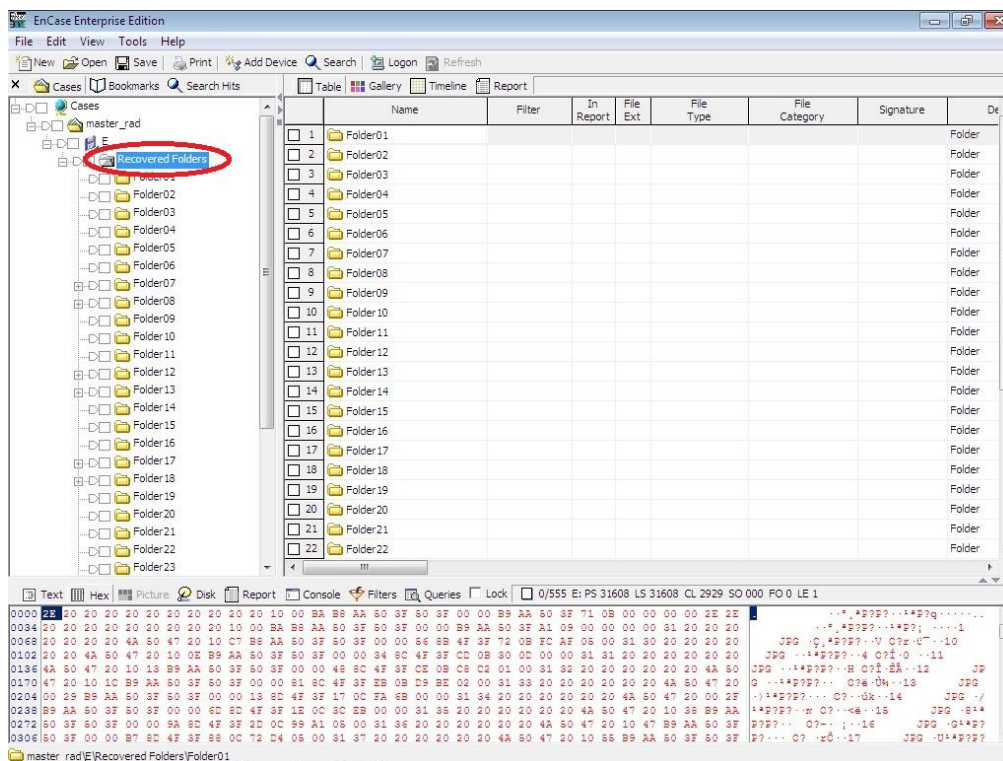
Slika 21. Selekcija USB memorijskog uređaja kao dokaznog materijala

Nakon što je USB uređaj dodat određenom slučaju kreiranom u *EnCase*-u, može se pokrenuti *Recover Folders* za FAT particije, koje se odabiraju desnim tasterom miša na fajl (Slika 22). Ovom komandom vrši se pretraga kroz sve nealocirane klastere konkretne FAT particije. Svaki folder FAT particije ima ulaz u obliku „. .“ (*dot, double-dot*). Ovi ulazi govore fajl sistemu gde se nalaze folderi. *EnCase* vrši pretragu kroz nealocirane klastere, traži ulaz („. .“) i vrši povraćaj foldera koji su obrisani, ili sa njihovim ulazima koji su obrisani u glavnom direktorijumu³⁷. *EnCase* neće vratiti folder sa originalnim imenom (jer je ime obrisano u glavnom direktorijumu), ali će nastojati da povrati sve što se nalazi unutar tog foldera, uključujući i imena fajlova unutar foldera, (Slika 23).

³⁷ Grubor G., Milosavljević M. (2007), „Digitalna forenzika“, Univerzitet Singidunum, Beograd, str. 77

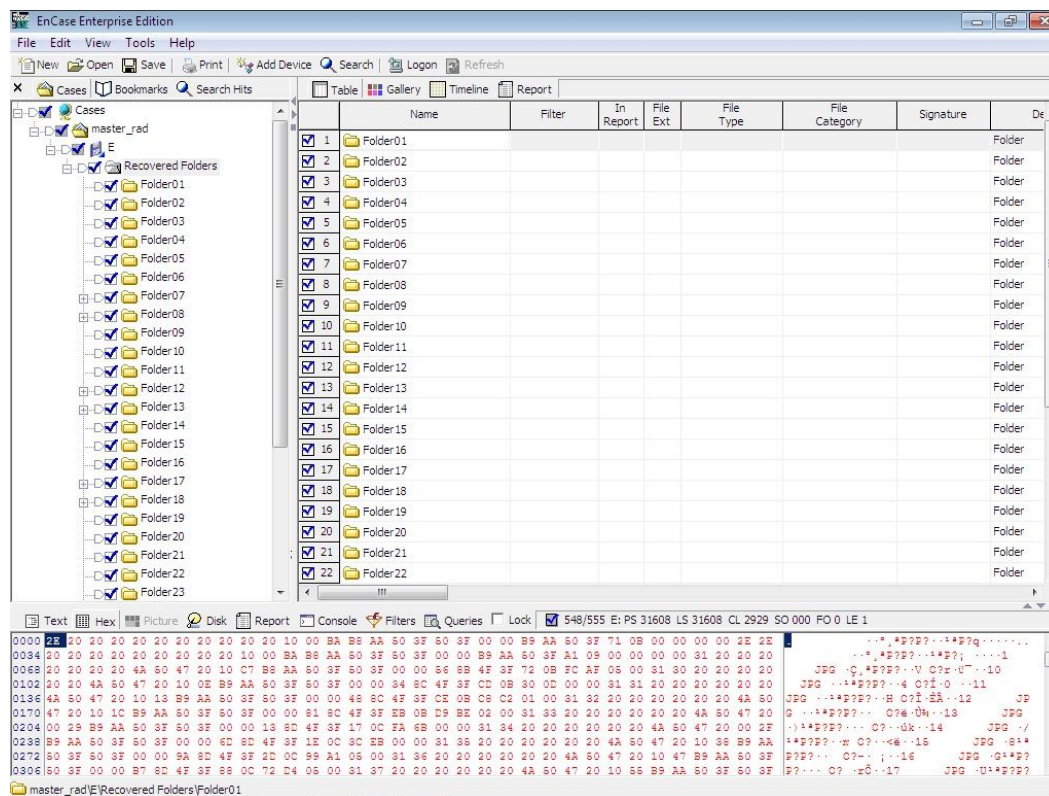


Slika 22. Oporavak foldera sa FAT fajl sistema opcijom Recover Folders



Slika 23. Oporavljeni folderi

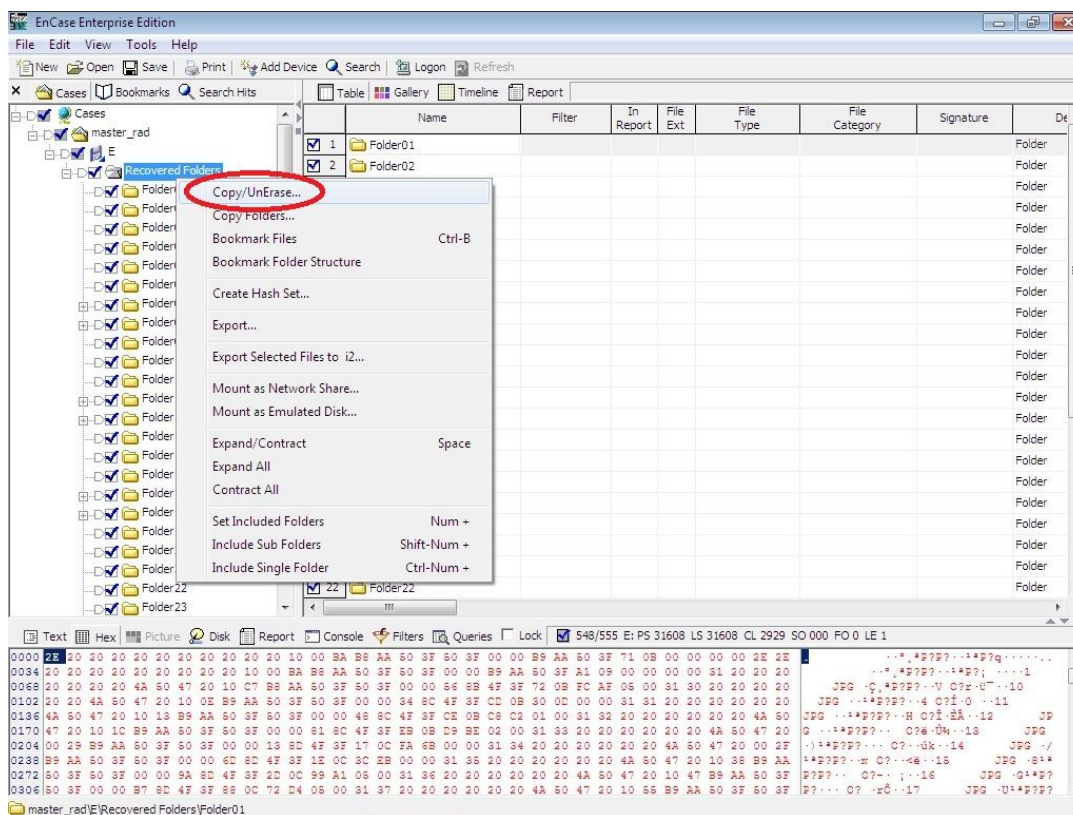
Nakon povratka foldera pristupamo direktnom pristupu i oporavku fajlova. Postoji mogućnost pojedinačnog biranja oporavka fajlova i foldera i oporavka svih foldera. Izabrali smo oporavak svih foldera (Slika 24).



Slika 24. Prikaz izabranih foldera za oporavak

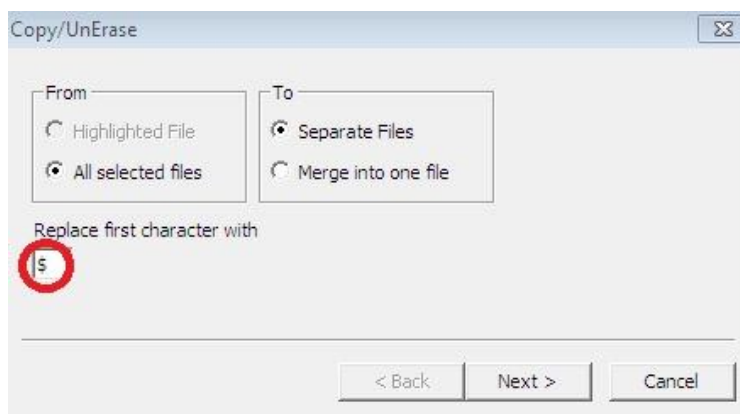
Kopiranje/oporavak izbrisanih fajlova EnCase vrši „byte-po-byte“³⁸. Sve što treba uraditi jeste čekirati fajl i desnim tasterom miša izabrati opciju *Copy/UnErase* (Slika 25). Pojaviće se dijalog kojim se vrši odabir između načina na koji će fajl biti vraćen, koji njegov deo (*fizički, logički, RAM slack*) i na kraju gde smestiti taj fajl.

³⁸ Grubor G., Milosavljević M. (2009), „Istraga kompjuterskog kriminala“, Univerzitet Singidunum, Beograd, str. 188



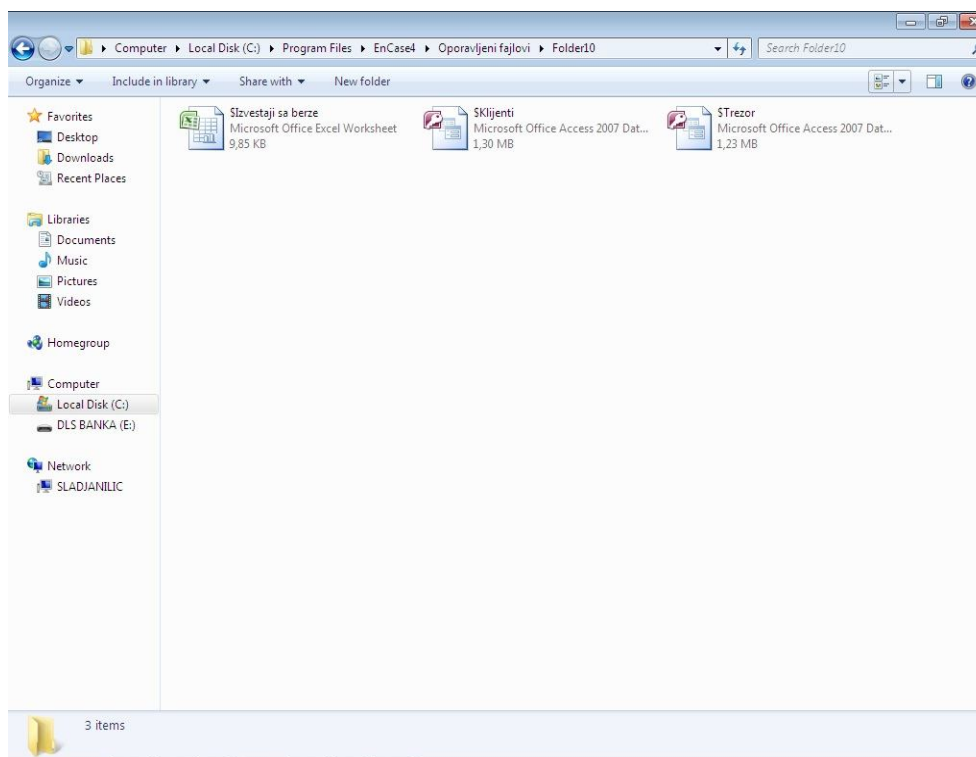
Slika 25. Kopiranje (oporavak) izbrisanih foldera

Prilikom samog kopiranja/oporavka fajlova u podešavanjima je postavljen znak dolara „\$“ koji će se nalaziti ispred samog naziva fajla i tako će se prepoznavati oporavljeni podaci (Slika 26).

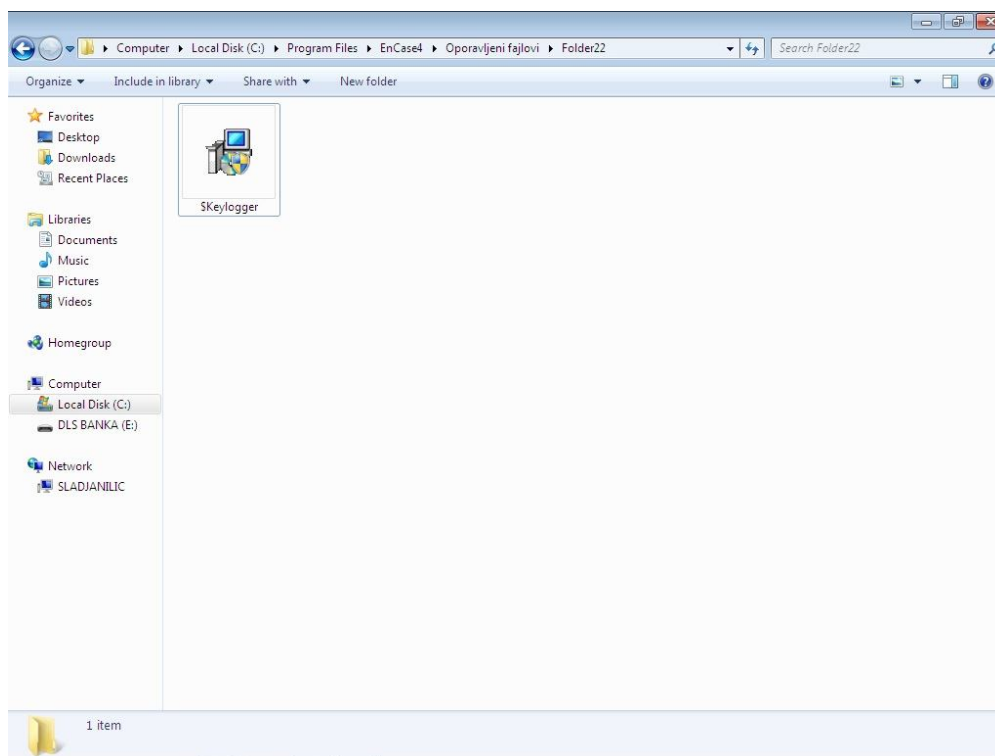


Slika 26. Oznaka „\$“ koja će se nalaziti kao prvo slovo naziva oporavljenog fajla

Nakon kopiranja tj. oporavka foldera na zadatu lokaciju, utvrđeno je da su folderi uspešno vraćeni/oporavljeni. Prvi znak u nazivu pronađenih fajlova jeste „\$“ kao što smo i označili prilikom samog procesa oporavka fajlova. Prilikom pregleda foldera pronađeni su ključni dokazi za ovu istragu, a to su baza podataka (*Microsoft Office Access Database 2007*), *Microsoft Office Excel* dokument, (*Slika 27*) i instalacija Keylogger-a, (*Slika 28*). Pronađena baza podataka koja je izrađena u *MS Office Access*-u je sadržala imena klijenata koji posluju sa bankom, u kojoj se nalaze njihovi lični podaci, brojevi telefona, adrese, brojevi žiro računa, novčani iznosi na računima, novčane transakcije, itd. Kao i baza podataka trezora banke u kojoj su se nalazili poverljivi podaci, dnevni i mesečni profit banke, novčano stanja trezora, itd. Takođe, pronađen je tabelarni prikaz berzanskog poslovanja banke, dnevni i mesečni izveštaji izraženi novčano i procentualno.



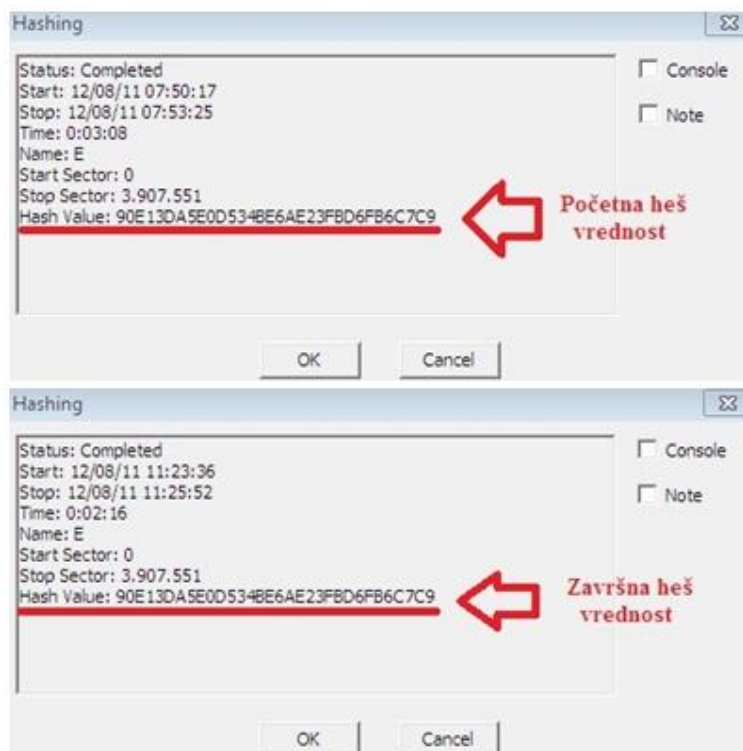
Slika 27. Prikaz uspešno oporavljenih fajlova



Slika 28. Prikaz Keylogger-a oporavljenog sa osumnjičenog USB uređaja

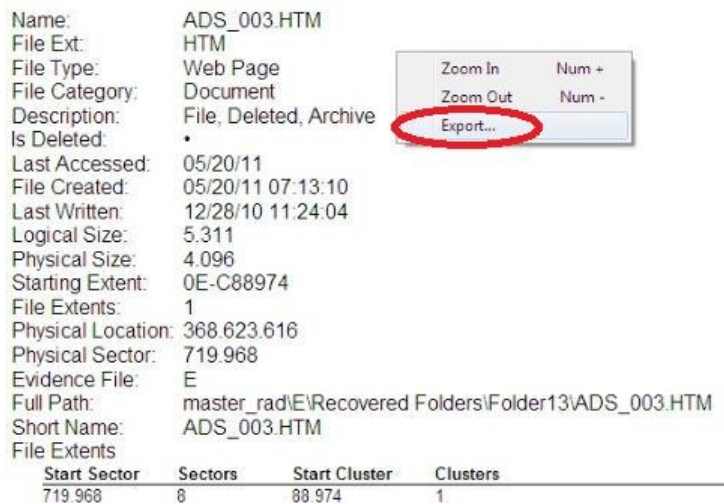
EnCase, takođe, omogućava dodeljivanje heš vrednosti koja predstavlja „digitalni otisak prsta“ svakog fajla. *EnCase* koristi MD5 algoritam za generisanje heš vrednosti. MD5³⁹ je kriptografski algoritam koji spada u grupu heš algoritama, ili algoritama za sažimanje sadržaja fajla. Ovi algoritmi se još nazivaju i *digest*, ireverzibilni, ili algoritmi bez ključa. MD5 je bio veoma primenjivan u mnogim oblastima zaštite podataka, mada se danas smatra podložan kriptografskim napadima, tako da se ređe primenjuje u kriptografiji, ali je našao veoma čestu primenu u zaštiti integriteta većih fajlova zbog svoje brzine. Dužina MD5 sažetka je 128 bita. Ove vrednosti su od presudnog značaja za forenzičku analizu. Heš vrednostima se upoređuje, eliminiše, dokazuje, oslobađa i još mnogo toga. U ovom slučaju smo dobili heš vrednosti urađene na početku i kraju forenzičke analize, i te vrednosti su iste, poklapaju se, a samim tim se dokazuje da u toku analize nije bilo nikakve izmene podataka (*Slika 29*).

³⁹ MD5 - eng. Message-Digest algorithm 5

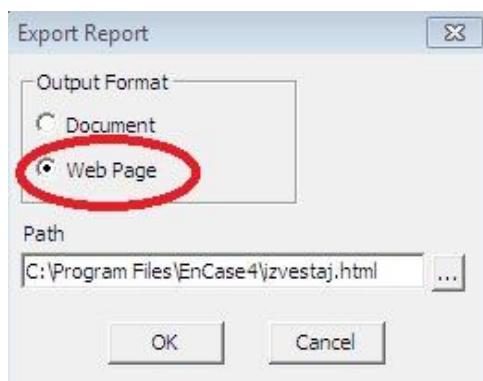


Slika 29. Početna i završna heš vrednost

Export izveštaja vrši se aktiviranjem desnog tastera miša na *Export* (Slika 30), u desnom prozoru za eksportovanje u odgovarajućem formatu, kada je izveštaj sastavljen i prikazan. Kao što je već pomenuto, moguće je eksportovati izveštaj u dva formata: .RTF i HTML (Slika 31).

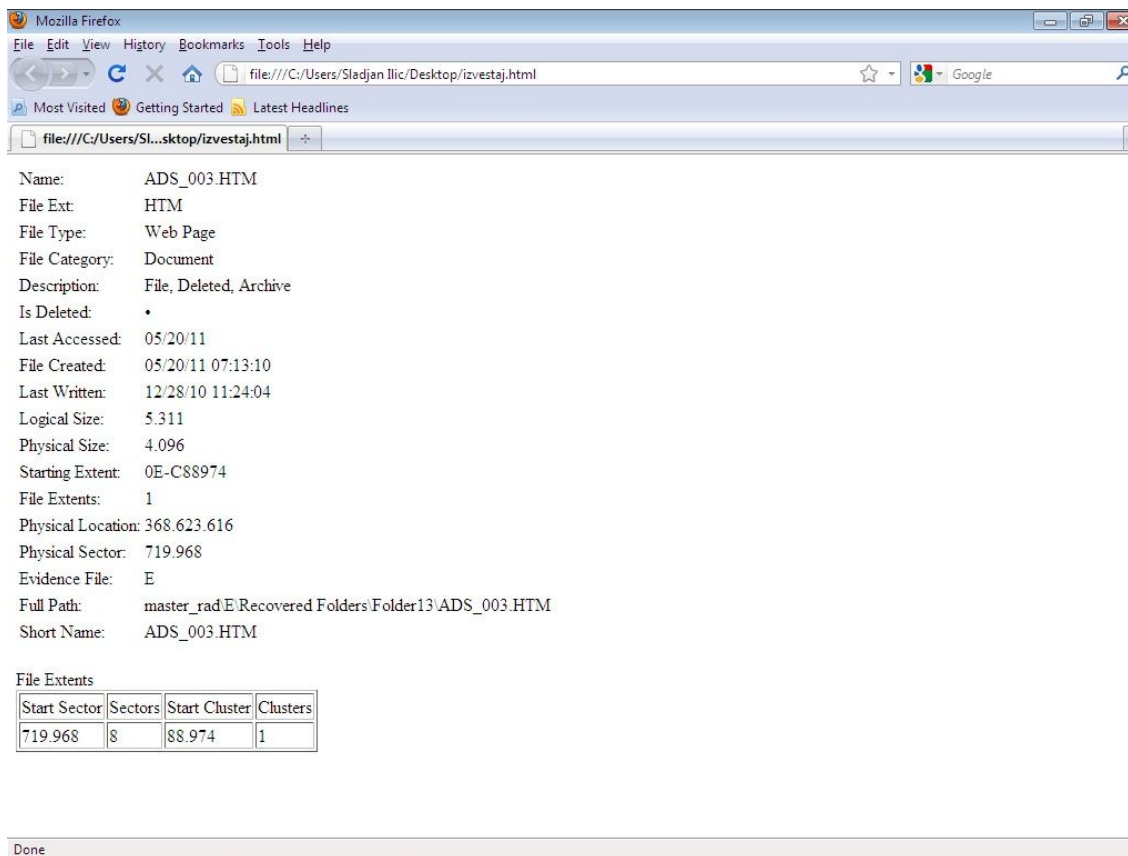


Slika 30. Export izveštaja



Slika 31. Export izveštaja u HTML formatu

Nakon exporta izveštaja i odabira da bude u HTML formatu, moguće je otvoriti i pregledati izveštaj u nekom od *Internet* pretraživača npr. *Mozilla Firefox*-u (Slika 32).



Slika 32. Prikaz HTML izveštaja otvorenog u pretraživaču Mozilla Firefox-u

Nakon obavljene forenzičke istrage pronađeni su optužujući dokazi koji upućuju na osumnjičenog u čijem se posedu našao USB uređaj. Izveštaj o izvršenoj istrazi kompjuterskog incidenta je dostavljen vlasniku sistema tj. banke i on dalje odlučuje o sudbini istrage, tj. da li će proslediti izvještaj zvaničnim organima za dalji pravosudni postupak ili će odlučiti da ova istraga ostane na korporacijskom nivou unutar organizacije i pronaći kompromis sa osumnjičenim. U slučaju da korporacijska istaga pređe u zvaničnu i da se pokrene dalji pravosudni postupak banka bi izgubila ugled i veliki broj klijenata i snosila bi ogromne finansijske gubitke.

3. ZAKLJUČAK

U ovom radu dat je prikaz nekoliko različitih alata za digitalnu forenziku, objašnjen je njihov način rada. Takođe, u ovom radu objašnjeno je šta je to USB *flash* memorija, poreklo i razvoj USB memorije, urađena je forenzika USB uređaja i oporavak izbrisanih podataka uz pomoć softversko-forenzičkog alata *EnCase*. Dat je prikaz i objašnjenje procesa oporavka podataka, objašnjen je način rada i funkcionalnost *EnCase* softverskog alata za digitalnu forenziku. U radu su date i spomenute definicije termina, kao što su digitalna (računarska) forenzika, kompjuterska istraga digitalnih dokaza, razvoj i vrste forenzičkih alata koji se najčešće upotrebljavaju u procesu prikupljanja dokaza, oporavak podataka, itd.

Digitalnu forenziku možemo posmatrati kao relativno novu naučnu disciplinu, koja nalazi svoje mesto u pravosudnom sistemu. Prate je brojni izazovi, što podrazumeva brze promene računarskih i digitalnih uređaja, kao i sve sofisticiranijih napada na računarske sisteme i mreže i rapidni porast zloupotreba IKT sistema i kompjuterskog kriminala.

Digitalna forenzička nauka obezbedila je forenzičke alate za relativno lagan i pouzdan pristup organa za digitalnu istragu osetljivim digitalnim podacima, ali tipično nedostaju metodi za verifikaciju korektnosti rada ovih alata, što je neophodno kada se digitalna forenzika posmatra sa naučnog aspekta.

Forenzički alati se neprestano razvijaju, modernizuju, popravljaju i reklamiraju. Neki od najpoznatijih i najčešće korišćenih programa današnjice su: *EnCase*, *FTK*, *CAINE*, *Helix*, *COFEE*, *Forensic Data Recovery*. Navedeni alati su kao što znamo prikazani i detaljnije objašnjeni u ovom radu, njihov princip rada i mogućnosti koje poseduju, a sve u svrhu što kvalitetnije forenzičke analize osumnjičenog računara.

Digitalni dokazi koji su potrebni za istragu, nalaze se analizom i evaluacijom svih podataka sakupljenih u fazi akvizicije digitalnih podataka, a mogu biti: optužujući, oslobađajući i da sadrži indikatore pokušaja sakrivanja podataka.

Proces digitalne forenzike obuhvata sledeće 4 glavne faze: *sakupljanje (akvizicija), ispitivanje, analizu, izveštavanje*. Akvizicija digitalnih podataka, je prva glavna faza digitalne forenzike, obuhvata procese otkrivanja, identifikacije i izvlačenja digitalnih podataka za potrebe forenzičke analize digitalnih dokaza.

Sprovedena istraživanja i primer oporavka izbrisanih podataka sa USB *flash* memorije su potvrdili postavljenu glavnu hipotezu o specijalizovanim forenzičkim alatima, kao što je *EnCase* softversko-forenzički alat, koji se tretira kao jedan od najpriznatijih svetskih softverskih alata, sa veoma velikom funkcionalnošću, a koji se koristi u svrhu digitalne forenzičke istrage. Takođe, da univerzalni forenzički alati sa adekvatnim skupom raznovrsnih digitalnih forenzičkih alata, omogućavaju forenzičaru brže i kvalitetnije izvršavanje više različitih zadataka digitalne forenzičke istrage. Ostalim objašnjenjima o poreklu i razvoju USB *flash* memorijskog uređaja i njegovoj upotrebi, koja je veoma mnogo zastupljena u današnje vreme, potvrđene su i ostale hipoteze.

4. LITERATURA

- [1] Casey Eoghan, „*Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*“, Second Edition, Great Britain, 2004.
- [2] Grubor G., Milosavljević M., „*Istraga kompjuterskog kriminala*“, Univerzitet Singidunum, Beograd, 2009. god.
- [3] Grubor G., Milosavljević M., „*Digitalna forenzika*“, Univerzitet Singidunum, Beograd, 2007. god.
- [4] Lam Kenny, Lau Derek, Lui Dennis, „*USB Thumb Drive - Designer Reference Manual*“, Hong Kong, 2004.
- [5] Sinchak Steve, „*Hacking Windows XP*“, United States of America, 2004.

Internet izvori:

- [1] <http://accessdata.com/>
- [2] http://bs.wikipedia.org/wiki/USB_stick
- [3] <http://digiex.net/downloads/download-center-2-0/applications/2812-cofee-microsoft-forensic-tool-download.html>,
- [4] <http://en.wikipedia.org/>
- [5] http://en.wikipedia.org/wiki/Flash_file_system
- [6] <http://hr.wikipedia.org/wiki/Helix>
- [7] <http://sigurnost.lss.hr/>
- [8] <http://sigurnost.lss.hr/documents/LinkedDocuments/NCERT-PUBDOC-2010-05-301.pdf>
- [9] <http://windows.microsoft.com/sr-Latn-CS/windows7/What-is-a-USB-flash-drive>
- [10] <http://www.caine-live.net/>
- [11] <http://www.digitalintelligence.com/>
- [12] http://www.ehow.com/about_6702877_forensic-data-recovery.html
- [13] <http://www.guidancesoftware.com/forensic.htm>
- [14] <http://www.microsoft.com/>
- [15] <http://www.pcchip.hr/sigurniji-rad-s-usb-memorijama/>