



UNIVERZITET SINGIDUNUM
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE I MEĐUNARODNU
SARADNJU

Studijski program: Savremene informacione tehnologije

MASTER RAD

KOMPJUTERSKI KRIMINAL – NAPADI, OTKRIVANJE
I ZAŠTITA

Mentor:
Prof. dr Gojko Grubor

Student:
Maja Milovanović 410509/2012

Beograd, 2013. godine

Sadržaj:

1. Metodologija istraživačkog rada	6
1.1. Uvodne napomene i struktura rada	6
1.2. Predmet rada	6
1.3. Ciljevi rada	6
1.4. Hipotetički okvir	7
1.5. Metodi i tehnike istraživanja	7
2. Kompiuterski kriminal	8
2.1. Bezbednost	8
2.1.1. Bezbednost je proces	9
2.1.2. Bezbednosni ciljevi	9
2.1.3. Napadi i pretnje koje ugrožavaju bezbednost.....	10
2.1.4. Bezbednosne usluge	12
2.2. Razvoj kompiuterskog kriminala.....	13
2.3. Klasifikacija kompiuterskog kriminala.....	14
2.4. Oblici kompiuterskog kriminala.....	14
2.5. Osnovni elementi krivičnog dela.....	15
2.6. Tipovi kompiuterskog kriminala.....	15
2.7. Sektori koji koriste digitalnu forenzičku istragu u borbi protiv kriminala.....	16
2.7.1. Borba protiv kompiuterskog kriminala	16
2.7.2. Kompiuterski kriminal u Srpskom zakonodavstvu	17
3. Računar kao cilj napada (zlonamerni softveri).....	19
3.1. Vrste zlonamernih softvera	19
3.1.1. „Trojanski konji“ - trojanci	20
3.1.2. Logičke bombe	21
3.1.3. Crvi	21

3.1.4.	Virusi	22
3.1.4.1.	Virusi koji napadaju sisteme datoteka	22
3.1.4.2.	Makro virus i script virusi	23
3.1.5.	Špijunski programi (spyware)	23
3.2.	Zaštita od zlonamernog programa	24
3.2.1.	Specijalni programi	25
3.2.2.	Mrežne barijere	26
3.2.3.	Biometrijska zaštita	27
3.2.3.1.	Biometrija zasnovana na fizičkim karakteristikama	27
3.2.3.2.	Biometrija zasnovana na karakteristikama ponašanja	30
3.2.4.	Etičko hakerisanje	31
3.3.	Rootkit alati	33
3.3.1.	Razvoj rootkit alata	33
3.3.2.	Detekcija rootkit alata	33
3.3.3.	Vrste rootkit alata	34
3.3.3.1.	Linux rootkit alati	34
3.3.3.2.	Windows rootkit alati	35
4.	Zločini počinjeni uz pomoć računara	36
4.1.	Krađa identiteta na Internetu	36
4.2.	Internet prevara	37
4.3.	Cyberstalking (syber uhođenje)	38
4.4.	Dečija pornografija na Internetu	38
4.5.	Sajber terorizam	38
4.6.	Trgovina drogom	39
4.7.	Internet ubistva	39
5.	Istraga kompjuterskog kriminala	40
5.1.	Zvanična (javna) digitalna forenzička istraga	40

5.2.	Korporacijska digitalna forenzička istraga	41
5.2.1.	Uspostavljanje tima za upravljanje kompjuterskim incidentom	42
5.2.2.	Proces korporacijske istrage	43
6.	Model integrisanih procesa digitalne forenzičke analize	45
6.1.	Faze modela integrisanih procesa digitalne forenzičke analize	46
6.1.1.	Faza pripreme.....	47
6.1.2.	Faza razvoja	47
6.1.3.	Faza istrage fizičkog mesta krivičnog dela	47
6.1.4.	Faza istrage digitalnog mesta krivičnog dela.....	49
6.1.5.	Faza provere (kontrole).....	51
7.	Forenzički alati	52
7.1.	Tehnike i alati za akviziciju digitalnih podataka	52
7.2.	Ekstrakcija digitalnih podataka.....	54
7.3.	Rekonstrukcija osumnjičenog diska	55
7.4.	Softverski forenzički alati.....	55
7.5.	Hardverski forenzički alati	55
7.5.1.	Blokatori upisivanja.....	57
7.5.2.	Hard diskovi	57
7.5.2.1.	Konstrukcija hard diskova	58
7.5.2.2.	Smeštanje podataka na pločama hard diska.....	59
8.	Studija slučaja (Case study).....	61
8.1.	Scenario istrage kompjuterskog kriminala u organizaciji „XY“	61
8.2.	Korporacijska istraga	62
8.2.1.	Uzimanje imidza	62
8.2.2.	Analiza imidža.....	70
8.2.3.	Vraćanje obrisanih fajlova i foldera	72
8.2.4.	Postavljanje aplikacije za nadgledanje sistema.....	75

8.3. Javna istraga	77
9. Zaključak:.....	78
10. Literatura:	79

1. Metodologija istraživačkog rada

1.1. Uvodne napomene i struktura rada

Upotreba Interneta u početku je bila jako mala. Međutim, vremenom, Internet je omogućio povezivanje svih računara u jednu mrežu, globalnu mrežu. Uporedo sa njegovim razvojem počeli su da se pojavljuju sve češći i raznovrsniji napadi sa mreže. Internet je počeo da se koristi kako bi se izvršila i razna krivična dela. Tako je nastala nova oblast u kriminalu koja se naziva „kompjuterski kriminal“. Formirane su nove institucije koje imaju zadatak da se bave isključivo ovom vrstom kriminala.

Pod pojmom „kompjuterski kriminal“ se podrazumevaju sva krivična dela koja na neki način uključuju računar. Računar može da bude cilj napada, ali isto tako može i da se koristi i kao sredstvo za organizaciju raznih vrsta tradicionalnih krivičnih dela, i da olakša njihovo sprovođenje.

U ovom istraživačkom radu je opisan kompjuterski kriminal. Takođe govori se o njegovoj pojavi i razvoju. Akcenat je na metodama i tehnikama koje se koriste da bi se ovaj kriminal suzbio ili smanjio.

1.2. Predmet rada

Predmet ovog rada su metode i tehnike koje koriste iztražni organi u saradnji sa digitalnim forenzičarima, kako bi što bolje i sto brže došli do počinioca zločina. Takođe govori se i o tehnici koju digitalni forenzičari treba da poseduju, a takođe i o neophodnom znanju. Spomenuti su i prikazani i neki softveri koji uzimaju imidž, odnosno sliku računara sa kog je počinjen zločin, i uz koje kasnije sprovode istragu. Naravno u saradnji sa istražnim organima.

1.3. Ciljevi rada

Cilj rada je da prikaže celu sliku o kompjuterskom kriminalu i takođe da objasni na koj način može da se vrši istraga i koja tehnika je neophodna. Takođe, i da objasni na koji način digitalni forenzičari sarađuju sa istražnim organima, i na koj način oni mogu u najkraćem roku, zajedničkim snagama da reše zločin.

1.4. Hipotetički okvir

Opšta hipoteza

Izvršioци krivičnog dela su uglavnom hakeri koji na bilo koji način pokušavaju da zloupotrebe tuđe računare, mreže ili sisteme. Brojna tradicionalna krivična dela danas koriste računar, posebno kada je u pitanju organizovanje tog krivičnog dela, kao što su dečija pornografija, trgovina drogom, syber terorizam, krađa identiteta na Internetu i razne Internet prevare koje postaju sve češći oblik napada na pojedince. Kompjuterski kriminalci to rade uz pomoć raznih zlonamernih softvera koji se instaliraju na tuđem računaru i na taj način mogu da dođu do potrebnih informacija, mogu i da uspire rad tog sistema ili čak i da ga unište.

Radna hipoteza

Da bi korisnike u što većoj meri zaštitili od kompjuterskog kriminala, nacionalne države formiraju specijalna odeljenja koja se bave isključivo ovom vrstom kriminala, kao što su specijalna odeljenja MUP-a, sudstva i tužilaštva. Koriste se razni načini kako bi se ušlo u trag ovim prestupnicima. U borbi protiv kompjuterskog kriminala značajan doprinos daju i razne antivirusne kompanije koje prate maliciozne programe na Internetu, prave njihove karakteristične zapise (definicije) za svakodnevno ažuriranje svojih antivirusnih softvera.

1.5. Metodi i tehnike istraživanja

U pisanju ovog istraživačkog rada primenjen je analitički metod izučavanja brojnih definicija pojma kompjuterskog kriminala u svim njegovim pojavnim oblicima. Analizirane su vrste napada, koja je uloga računara u svim tim napadima i kako napadači koriste računar da bi sprovedi svako krivično delo.

Deo istraživačkog rada se bavi i metodama i tehnikama sprovođenja istrage. Objašnjene su obe vrste istaga, i na koji način se one integrišu i međusobno sarađuju kako bi u što kraćem vremenskom periodu rešili slučaj. Čitava istraga je prikazana na konkretnom primeru i uz pomoć određenog forenzičkog alata.

2. Kompjuterski kriminal

Digitalna ili kompjuterska forenzika se može definisati kao proces prikupljanja, očuvanja, analize i prezentovanja digitalnih dokaza. Forenzički alati omogućuju povraćaj i analizu obrisanih, skrivenih i privremenih fajlova kojima se ne može pristupiti na uobičajan način. Ceo izveštaj napravljen na osnovu digitalnih dokaza se koristi na sudu. Korišćenje ovih metoda za potrebe rekonstrukcije događaja okarakterisane su kao kompjuterski kriminal (engl. Cyber crime) [7].

Dakle, kompjuterski kriminal je oblik kriminalnog ponašanja, gde se krivično delo izvršava korišćenjem kompjuterske tehnologije i informacionih sistema ili tu spada svaki zločin koji uključuje računar ili računarsku mrežu tj. koristi ih kao sredstvo ili cilj izvršenja. Kompjuterska tehnologija se može zloupotребiti na razne načine. Svi oblici tradicionalnog kriminala se mogu izvesti uz pomoć računara ili mreže, kao što su krađe, utaje, pronevere itd. Informacije koje se dobijaju zloupotребom informacionih sistema na razne načine se mogu koristiti za sticanje protivpravne koristi. Dakle, u kompjuterski kriminal spada svako krivično delo koje je počinjeno uz pomoć računara ili mreže [5].

Uporedo sa ubrzanom informatizacijom društva i ulaskom Interneta u sve oblasti društvenog i privatnog života ljudi, kompjuterski kriminal postaje dominantan oblik zloupotreba, kršenja zakona i drugih normi ponašanja. Novi oblici napada na računare i računarske mreže javljaju se velikom brzinom, a novi tipovi kompjuterskog kriminala praktično zavise samo od mašte malicioznih napadača [2].

Dakle, sa razvojem ove vrste kriminala problem sigurnosti je postajao sve veći i veći i samim tim su počeli da se formiraju čitavi timovi za borbu protiv sajber kriminala odnosno za povećanje sigurnosti u sistemima.

2.1. Bezbednost

Bezbednost je proces održavanja prihvatljivog nivoa rizika. Ne može se kupiti kao proizvod ili usluga zato što to nije završno stanje, niti konačan proizvod. Bezbednost je proces u kome se koriste različiti proizvodi i usluge, procedure i pravila, ali se smatra da postoje i drugi bitni elementi kao što su edukacija, podizanje svesti i stalno praćenje stanja u ovoj oblasti [5].

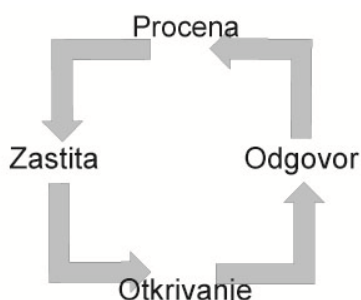
Postoji nekoliko principa koji važe kao osnovni postulati kada se govori o bezbednosti, a to su [5]:

- Bezbednost je proces.
- Ne postoji apsolutna bezbednost.
- Uz različite metode zaštite treba imati u vidu i ljudski faktor, sa svim slabostima.

2.1.1. Bezbednost je proces

Bezbednost kao proces se sastoji iz četiri osnovna koraka (slika 1). A to su [5]:

1. procena,
2. zaštita,
3. otkrivanje i
4. odgovor.



Slika 1 – Sigurnost kao proces

Procena je priprema za ostale tri komponente. Jako je bitna procena realnog stanja sistema jer greška u proceni može da naškodi svim operacijama koje slede. **Zaštita** je sprečavanje ili prevencija. Podrazumeva protiv meru kako bi se smanjila ugroženost sistema. Ukoliko ona zakaže primenjuje se sledeća mera, a to je otkrivanje. **Otkrivanje** predstavlja proces identifikacije upada ili incidenta koji se odnosi na bezbednost. I poslednji korak je odgovor. **Odgovor** ili reakcija predstavlja proces oporavka tj. lečenja posledica upada [5].

2.1.2. Bezbednosni ciljevi

Postoje tri osnovna cilja bezbednosti, a to su [5]:

1. poverljivost (engl. confidentiality),
2. celovitost (engl. integrity) i
3. raspoloživost (engl. availability).

Ova tri cilja čine takozvano „veliko trojstvo“ bezbednosti. Na engleskom jeziku skraćenica za ova tri termina je CIA, što znači Confidentiality, Integrity, Availability i poklapa se sa akronimom koji se koristi za najpoznatiju Američku obaveštajnu službu [5].

Poverljivost (engl. Confidentiality) obuhvata pokušaje da se spreči namerno ili nenamerno neovlašćeno otkrivanje sadržaja poruka. Poverljivost se može izgubiti na mnogo načina. **Integritet** (engl. integrity) obezbeđuje da podatke ne smeju menjati neovlašćena lica. Dakle, podaci moraju stići onako kako su poslani sa izvorišta na odredište. **Raspoloživost** (engl. availability) omogućava da korisnik može da pristupi svim potrebnim informacijama u svakom trenutku [5].

2.1.3. Napadi i pretnje koje ugrožavaju bezbednost

Postoje tri aspekta bezbednosti informacija [5]:

- **napad na bezbednost** – ovde spada bilo koja akcija koja ugrožava bezbednost informacija,
- **bezbednosni mehanizam** – mehanizam koji treba da detektuje i predupredi napad, ili da sistem oporavi od napada,
- **bezbednosna usluga** – usluga koja povećava bezbednost sistema za obradu i prenos podataka. Podrazumeva upotrebu jednog ili više bezbednosnih mehanizama.

Napadi su akcije koje su usmerene na ugrožavanje bezbednosti informacija, računarskih sistema i mreža. Postoje četiri vrste napada koje se dele u četiri kategorije [5]:

- presecanje (prekidanje),
- presretanje,
- izmena i
- fabrikovanje.

Na slici 2 se vidi normalan tok podataka:



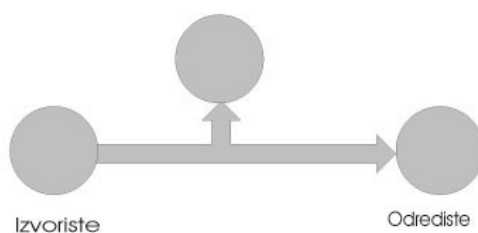
Slika 2 – Normalan tok podataka

Presecanje (slika 3) predstavlja napad na raspoloživost. Prekida se tok informacija i onemogućava se pružanje neke usluge ili funkcionisanje sistema. Spada u aktivan napad.



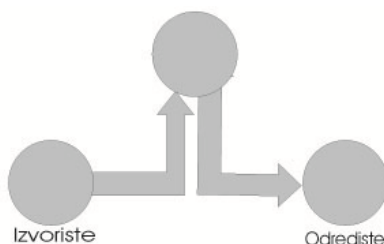
Slika 3 - Presecanje

Presretanje (slika 4) predstavlja napad na poverljivost. U praksi se naziva prisluškivanje saobraćaja, nadziranje njegovog intenziteta, uvod u osetljive informacije i drugo. Teško se otkriva zato što ne menja podatke i ne utiče na funkcionisanje sistema.



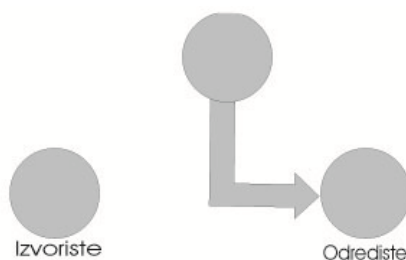
Slika 4 – Presretanje

Izmena (slika 5) predstavlja napad na integritet. Ovim napadom se menjaju podaci, pristupna prava, način funkcionisanja sistema i dr. Često ostaje neprimećen neko vreme.



Slika 5 – Izmena

Fabrikovanje (slika 6) predstavlja napad na autentičnost. Napadač generiše lažne podatke, lažni saobraćaj ili izdaje neovlašćene komande. Često se koristi za lažno predstavljanje korisnika.



Slika 6 – Fabrikovanje

2.1.4. Bezbednosne usluge

U bezbednosne usluge spadaju [5]:

- **poverljivost, privatnost** – predstavlja uslugu koja obezbeđuje pristup informacijama samo za one korisnike koji su ovlašćeni da pristupe tim informacijama,
- **provera identiteta** – ovo je usluga kojom se zahteva od svakog korisnika da se predstavi sistemu pre nego što nešto uradi, i da to i dokaže,
- **integritet** – to je usluga koja obezbeđuje celovitost podataka, tj. da napadač ne može da izmeni podatke a da to ostane neprimećeno,
- **neporicanje, priznavanje** – ova usluga obezbeđuje da korisnik ne može da pošalje poruku ili izmeni neki podatak a da posle tvrdi da to nije uradio,
- **kontrola pristupa** – ova usluga treba da predupredi zloupotrebu resursa. Pomoću ove usluge dozvoljava se objektu, sa proverenim identitetom i odgovarajućim ovlašćenjima, da koristi određene usluge ili operacije,
- **raspoloživost, upotrebljivost** – ovom uslugom se obezbeđuje dostupnost podacima i raspoloživost sistema koji pruža neke usluge.

2.2. Razvoj kompiuterskog kriminala

Već šezdesetih godina je bilo izveštaja o kompiuterskim manipulacijama, sabotazama, špijunažama i nelegalnim korišćenjem računarskih sistema. Sedamdesetih godina su se pojavili prvi ozbiljni zločini ove vrste. Zbog ograničenosti uloge računara u svakodnevnom životu ovi prekršaji su bili usmereni na krađe i prevare vezane za telekomunikacione usluge i prenos elektronskih sredstava. Kasnije sa povećanjem umreženih personalnih računara stvara se potreba za specifičnim zakonima vazanim za ovu vrstu kriminala [5].

U toku 1984. godine FBI je počeo razvoj laboratorije i programa za ispitivanje kompiuterskih dokaza koji je izrastao u jedinstveni CART tim (Computer Analysis and Response Team), kasnije formiran u mnogim organizacijama u SAD. Danas se forenzička analiza vrši u dobro opremljenim laboratorijama. U tom periodu je 70% osposobljenih zvaničnih agencija radilo ovaj posao bez razvijenih procedura za taj rad [2].

Sa pojavom digitalnog videa i audia uvodi se pojam digitalnih dokaza. Međunarodna organizacija za kompiuterske dokaze – IOCE (International Organization on Computer Evidence) je formirana 1997. godine. Tehnička radna grupa za kompiuterske dokaze, održala je svoj prvi sastanak u junu 1998. godine sa ciljem razvoja organizacionih procedura i relevantnih dokumenata za forenzičku istragu digitalnih dokaza. Kompiuterska forenzička analiza za manje od 20 godina pouzdano čuva digitalne podatke, oporavlja izbrisane podatke, rekonstruiše kompiuterske događaje, odvraća napadače, nudi dosta dobrih proizvoda i procedura za podršku [2].

Kompiuterska forenzička analiza se danas primenjuje u slučajevima: hakerskog upada, pronevere, pedofilskog kruga, imigracione prevare, trgovine drogom, falcifikovanja kreditnih kartica, piraterije softvera, falsifikata, ubistava, seksualnog uznemiravanja, krađe podataka, industrijske špijunaže, razvoda. [2]

Uputstvo za pretragu i privremeno oduzimanje računara objavilo je Ministarstvo pravde SAD 1994. godine [2].

Savremeni korisnici digitalne forenzike su: policija, vojska, pravosudni sistem (tužilaštvo i pravosuđe), firme koje se profesionalno bave oporavkom podataka iz računara, korporacije za upravljanje kompiuterskim incidentom [2].

Pojavom crva 1988. godine oboreno je 6000 računara. Iste godine je uhapšen Robert Moris i osuđen na novčanu kaznu i dobrotvoran rad. Kevin Mitnik je 1995. godine u SAD-u uhapšen i osuđen za falsifikovanje 20.000 brojeva kreditnih kartica. Sa povećanom upotrebom personalnih računara povećala se i potreba za zaštitom

od neovlašćenog pristupa računarskim podacima. Sve veća umreženost i prisutnost na Internetu izlaže računare novim opasnostima od spoljnih napada. Razvoj telekomunikacija i računarstva transformisao je mobilne uređaje u minijaturne umrežene računare sa velikim potencijalom za kriminal [5].

2.3. Klasifikacija kompjuterskog kriminala

Zbog širokog spektra ove vrste kriminala jako je teško izvršiti klasifikaciju. Glavne kategorije kompjuterskog kriminala mogu se grupisati na bazi uloge računara u izvršenju krivičnog dela, gde računar može biti [2]:

- **cilj napada** (upad u računar uz pomoć raznih zlonamernih softvera, krađa podataka),
- **sredstvo za napad** (prevare sa kreditnim karticama, slanje spama i slika),
- **povezan sa klasičnim kriminalom** (trgovina drogom i ljudima, dečija pornografija idr.) i
- **repozitorijum (skladište) digitalnih dokaza kompjuterskog kriminala.**

Konvencija o visokotehnološkom kriminalu Saveta Evrope pravi razliku između četiri vrste krivičnih dela [5]:

1. **dela protiv poverljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema** – njih čine nezakoniti pristup, presretanje i uplitanje u podatke ili sisteme,
2. **dela vezana za kompjutere** – falsifikovanje i krađe su glavni oblici ovih napada,
3. **dela vezana za sadržaje** – najčešći oblik je dečija pornografija,
4. **dela vezana za kršenje autorskih prava** – tu spada reprodukovanje i distribucija neautorizovanih primeraka.

2.4. Oblici kompjuterskog kriminala

Na osnovu konstatacije Ujedinjenih nacija, postoje dve subkategorije ovog kriminala [5]:

1. **sajber kriminal u užem smislu** – tu spada svako nezakonito ponašanje usmereno na elektronske operacije i na podatke koje se njima obrađuju (pravljenje i ubacivanje kompjuterskih virusa, haking, piraterija, kompjuterska sabotaza, špijunaža, prevara i krađa kompjuterskih usluga) i

2. **sajber kriminal u širem smislu** – tu spada svako nezakonito ponašanje vezano za kompiuterski sistem i mrežu (kompiuterski falcifikati, krađe, tehničke manipulacije uređajima ili elektronskim komponentama, zloupotrebe sistema plaćanja).

2.5. Osnovni elementi krivičnog dela

Osnovne elemente krivičnog dela kompiuterskog kriminala čine [2]:

- **dogadjaj**, odnosno šta se dogodilo u ispitivanom slučaju,
- **okolnosti**, ili kako se dogodilo i
- **mentalno stanje počinioca kriminala**, što je potrebno za klasifikaciju kriminala i profilisanje kompiuterskih kriminalaca.

2.6. Tipovi kompiuterskog kriminala

Tipovi kompiuterskog kriminala su brojni, a najčešći su [2]:

- krađa računarskih servisa,
- neovlašćeni pristup,
- piraterija softvera,
- otkrivanje, krađa i izmena računarskih podataka i informacija,
- iznuđivanje pomoću računara,
- neovlašćeni pristup bazama podataka,
- zloupotreba ukradene lozinke,
- prenos destruktivnih virusa,
- industrijska i politička špijunaža.

Zavisno od tipa počinjenih dela cyber kriminal može biti [5]:

- politički,
- ekonomski,
- proizvodnja i distribucija nedozvoljenih i štetnih sadržaja,
- manipulacija zabranjenim proizvodima, supstancama i robama,
- povreda sajber privatnosti.

2.7. Sektori koji koriste digitalnu forenzičku istragu u borbi protiv kriminala

Digitalnu forenzičku istragu koriste četiri društvena sektora [2]:

- zvanični organi istrage kompjuterskog kriminala (policija, tužilaštvo i sudstvo),
- organi odbrane (vojska, državna bezbednost),
- korporacije i veće organizacije za upravljanje kompjuterskim incidentom sopstvenim kapacitetima i
- profesionalne organizacije za oporavak podataka iz slučajno ili namerno oštećenih računarskih sistema.

Posledice kompjuterskog kriminala mogu biti [5]:

- **finansijske** – nastaju kada počinitelj vrši delo u cilju sticanja protivpravne imovinske koristi,
- **nematerijalne** – tu spada neovlašćeno otkrivanje tuđih tajni ili drugo „indiskretno - štetno postupanje“,
- **kombinovane** – povređuje se nečije moralno pravo i u isto vreme se nanosi i konkretna finansijska šteta.

2.7.1. Borba protiv kompjuterskog kriminala

Borba se zasniva na preventivnim i represivnim merama. One moraju biti usmerene na preduzimanje aktivnosti u cilju otklanjanja izvora, uslova, okolnosti ili propusta koji pogoduju zloupotrebi kompjutera. Njima treba obezbediti [5]:

- identifikaciju mogućih napada i njihovu klasifikaciju sa aspekta verovatnoće realizacije, objekta napada, načina i posledice realizacija,
- izbor i postavljanje odgovarajućeg sistema zaštite,
- održavanje, provera i unapređenje postavljenog sistema zaštite.

Najveći doprinos u ovoj borbi dala je „Grupa osam“ najrazvijenijih zemalja (G-8) koju čine: Francuska, Nemačka, Italija, Japan, Velika Britanija, Sjedinjene Države, Kanada i Rusija. To je osam vodećih industrijskih zemalja Sveta. Osnovni cilj je razmena mišljenja između država članica i usaglašavanje uglavnom spoljopolitičkih i ekonomskih pitanja [9].

2.7.2. Kompjuterski kriminal u Srpskom zakonodavstvu

Republika Srbija je 16. aprila 2005. godine u Helsinkiju potpisala kako Konvenciju o sajber kriminalu, tako i Dodatni protokol uz tu Konvenciju. Osnovni značaj ove konvencije je formiranje državnih organa koji su specijalizovani za borbu protiv sajber kriminala. Zakonodavstvo Republike Srbije je u periodu od aprila 2005. do marta 2009. godine usvojilo više propisa kojima se Konvencija sajber kriminala i Dodatni protokol implementiraju u naš pravni sistem. Narodna skupština Republike Srbije je ratifikovala Konvenciju o sajber kriminalu i Dodatni protokol tokom marta 2009. godine. Među njima su najvažniji [11]:

- zakon o organizaciji i nadležnosti državnih organa za borbu protiv sajber kriminala,
- krivični zakonik,
- zakon o odgovornosti pravnih lica za krivična dela,
- zakonik o krivičnom postupku,
- zakon o policiji,
- zakon o autorskim i srodnim pravima,
- zakon o telekomunikacijama,
- zakon o elektronskom potpisu,
- zakon o posebnim ovlašćenjima radi efikasne zaštite prava intelektualne svojine,
- pravilnik o uslovima za pružanje Internet usluga i sadržaju odobrenja.

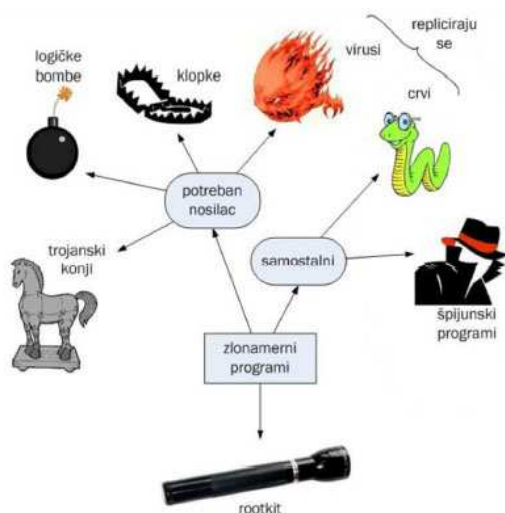
Konvencija je pokrenuta zbog sprečavanja zloupotreba podataka i sistema tako što će se pokrenuti kaznene mere za takvo delovanje kao što je opisano u konvenciji pri čemu će se primeniti kazne za efikasnu borbu protiv krivičnih dela i na taj način se pokušava da se obezbede uslovi za brzu i pouzdanu međunarodnu saradnju [11].

Konvencija o sajber kriminalu se sastoji iz četiri dela [11]:

- prvi deo čine objašnjenja osnovnih pojmova,
- drugi deo definiše mere koje treba da se preduzmu na nacionalnom nivou,
- treći deo definiše međunarodnu saradnju u okviru sprovođenja konvencije: opšta načela, izručenje, uzajamna pomoć, informacije, postupci, tajnost i ograničenja korišćenja, uzajamna pomoć itd,
- četvrti deo obuhvata završne odredbe, potpisivanje i stupanje na snagu.

Zbog nastanka sajber kriminala stvorila se potreba za angažovanjem posebno tehnički obučenih stručnjaka, ali i za drugačijom organizacijom državnih organa. Bilo je neophodno organizovanje posebnih državnih organa koji će se baviti ovom oblašću. Zato je organizovana posebna služba u MUP-u, zatim posebno tužilaštvo i posebno istražno i pretresno odeljenje Okružnog suda u Beogradu [11].

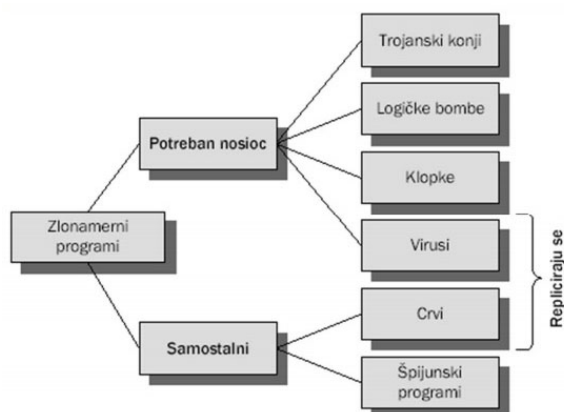
3. Računar kao cilj napada (zlonamerni softveri)



Slika 7 – Zlonamerni softveri [5]

Zlonamerni softveri su softveri koji se prave da bi na bilo koji način oštetili umrežen ili neumrežen računar i otežali ili onemogućili njegovo korišćenje. Neki softveri zahtevaju nosioce a neki su samostalni. Oni uglavnom rade u pozadini i to može da uspori rad računara ili čak da dovede do obaranja sistema.

3.1. Vrste zlonamernih softvera



Slika 8 – Vrste zlonamernih softvera [5]

Zlonamerni softveri se dele na softvere kojima je neophodan nosilac i na samostalne (slika 8). Samostalni su crvi i špijunski programi a programi kojima je potreban nosilac su trojanci i virusi.

Vrste zlonamernih softvera su:

- trojanci,
- logičke bombe,
- crvi,
- virusi,
- špijunski programi.

3.1.1. „Trojanski konji“ - trojanci

Trojanci se drugačije nazivaju „trojanski konji“. Trojanci su softveri koji se predstavljaju kao korisni programi i na taj način nateraju korisnike da ovaj program pokrenu. Najčešće se koriste za krađu poverljivih informacija. Za širenje trojanskih konja često se koristi crv kao nosioc [5].

Vrste trojanaca [5]:

- trojanac koji otvara zadnja vrata,
- nosioci zlonamernog softvera,
- kradljivci informacija, trojanski špijuni,
- proksi serveri i programi koji pozivaju telefonske brojeve.

Trojanac koji otvara zadnja vrata omogućava udaljenom korisniku da pristupi inficiranom računaru, i to najčešće tako da vlasnik računara nije ni svestan „posetioca“. Nakon inficiranja, napadač može da koristi resurse inficiranog računara u koje spadaju i poverljive informacije kao što su lozinke. Primer ovakvog trojanca je Back Orifice 2K (BO2K) koji omogućava praćenje pritisnutih tastera, prenosa datoteka, direktorijuma [5].

Nosioci zlonamernog softvera se nakon instalacije ponašaju kao magnet za drugi zlonamerni softver. Takvi su Downloader i Dropper [5].

Kradljivci informacija miruju na tuđem računaru dok ga pretražuju i traže poverljive podatke kao što su lozinke, privatni i javni ključevi, sertifikati ili podaci sa kreditnih kartica. Jedan od ovakvih trojanaca je PSW. PSW će poslati sve skupljene informacije e-poštom ili na neku drugu lokaciju. Slično se ponašaju i **trojanski špijuni** ili „**obaveštajci**“ koji omogućavaju da napadač prati rad korisnika, tako što prate i snimaju svaki njegov pokret [5].

Proksi serveri i programi koji pozivaju telefonske brojeve su trojanci koji pozivaju „egzotične“ telefonske brojeve da bi korisnici dobili ogromne telefonske račune [5].

Trojanski konji inficiraju računar ali ne i datoteke, pa ih je zato i lako otkriti i ukloniti. Često prave zapise u bazi Registry, kako bi omogućili svoje izvršenje prilikom svakog pokretanja sistema [5].

3.1.2. Logičke bombe

Posebna vrsta trojanaca su logičke bombe koje predstavljaju zlonameran kod koji je ubačen u neki koristan program i koji će se aktivirati kada određeni uslovi budu ispunjeni kao na primer u određeno vreme ili određenog datuma, ili ako se pojavi određeni korisnik. Sve zavisi od mašte pisca koda. Kada se aktivira obično se ponaša destruktivno a može i da ošteti sistem [5].

Virusi i crvi često sadrže logičke bombe koje će izvršiti neku akciju u unapred određeno vreme ili ako se ispune neki uslovi. Oni koriste ovu tehniku kako bi se neprimetno proširili na druge sisteme. Destruktivne akcije virusa i crva često se izvode uz pomoć logičkih bombi. Na primer da virus obriše određene datoteke nekog datuma. Primer ovakvog virusa je „Mikelandelo“, koji se aktivirao na njegov rođendan 6. marta [5].

3.1.3. Crvi

Crvi su samostalni programi koji se šire sa jednog računara na drugi. Najčešće metode prenošenja su upotreba elektronske pošte i Internet servisa (FTP, HTTP). Crv eksploatiše ranjivost žrtve ili koristi metode prevare i obmanjivanja, poznate kao društveni inženjering, kako bi naterao korisnika da ga pokrene [5].

U zavisnosti od toga kako se prenose postoje različite vrste crva [5]:

- e-mail crvi,
- instant poruka (IM crvi),
- Internet crvi,
- crvi deljenja podataka (file-sharing crvi),
- P2P crvi.

E-mail crvi se šire preko inficiranih poruka elektronske pošte i to kao priloge ili hiperveze (linka) ka inficiranim Web stranicama. Ukoliko se širi preko linka, korisniku se šalje „udica“ koja pokreće inficiranu web lokaciju, koja automatski instalira crva na žrtvu. Primeri ovog crva su: Netsky, MyDoom, Sasser idr. Tvorci ovih crva koriste metode društvenog inženjeringa, kako bi naterali korisnika da pokrene program u prilogu ili da ode na određeni link [5].

Instant poruka (IM crvi) su crvi koji se šire preko servisa za poruke kao što su MSN, Skype i dr. Oni šalju korisniku link ka inficiranoj Web lokaciji i kada korisnik pritisne vezu on preuzima i pokreće crva. Nakon što se crv instalira na računaru, on šalje sličnu poruku svim kontaktima. Primer ovog crva je: JS/CoolNow i Funner [5].

Internet Crvi su crvi koji na Internetu traže nezaštićene računare i kada ih pronadu sami se kopiraju i instaliraju. Dakle, dovoljno je da korisnik samo bude povezan na Internet [5].

Crvi deljenja podataka (file-sharing crvi) pokušavaju da se kopiraju na deljeni direktorijum i da prevare korisnika da ih pokrene [5].

P2P crvi se kopiraju ne neki P2P deljeni direktorijum i kada korisnici preuzmu određenu datoteku na taj način kopiraju i ove crve [5].

3.1.4. Virusi

Virusi su deo programskog koda koji je sposoban da se samokopira tako što dodaje svoj sadržaj u druge programe ili delove operativnog sistema. Na taj način inficira korisnika. Iz ovog se vidi da postoji velika sličnost između biloških i kompiuterskih virusa.

Virusi spadaju u najpodmuklije zlonamerne softvere. Često se dešava da usled infekcije virusima dolazi do brisanja različitih datoteka kao i do toga da se sistem dovede u stanje u kom ne može normalno da funkcioniše. Oni ne koriste mrežne resurse za širenje ali jako često se šire kao deo nekog crva.

Postoje dve vrste virusa. A to su:

- virusi koji napadaju sisteme datoteka i
- makro virusi i script virusi.

3.1.4.1. Virusi koji napadaju sisteme datoteka

Virusi ovog tipa za svoje širenje koriste jednu ili više vrsta sistema datoteka. Najveći broj ovih virusa inficira izvršne datoteke. Prema metodama inficiranja, virusi ovog tipa mogu se podeliti na [5]:

- prepisujuće viruse, tj. viruse koji prepisuju postojeći kôd (engl. overwriting),
- parazitske viruse (engl. parasitic),
- pridružujuće viruse (engl. companion),
- viruse startnog zapisa (engl. boot-sector).

Virusi koji prepisuju postojeći kod ili prepisujući inficiraju tako što u deo koda inficirane datoteke ubacuju svoj kod i na taj način ta datoteka postaje neupotrebljiva. Ovi virusi mogu da se detektuju ali jako teško se čiste jer antivirus ne zna da vrati prvobitni kod datoteke. Zato je poželjno povremeno iskopirati sve ove datoteke na neko drugo mesto i čuvati kopije zdravih izvršnih datoteka [5].

Parazitski virusi dodaju svoj kod u datoteku tako da datoteka ostane delimično ili potpuno funkcionalna. Svoj kod mogu upisati na početak datoteke, na kraj datoteke i unutar postojećeg koda. Virus koji dodaju na početak, pomeraju zdrav kod na kraju. Nakon pokretanja inficirane datoteke prvo se izvršava kod virusa. Većina virusa upisuje svoj kod na kraju datoteke a zatim modifikuje ulaznu taku u zaglavlju datoteke, kako bi osigurao da će se pre izvršenja samog programa izvršiti zlonamerni kod. Ovi virusi se lako otkrivaju i čiste na osnovu antivirusnih definicija. Treća kategorija su virusi koji svoj kod upisuju u šupljine između sekcija. Ukoliko se desi da je kod virusa loše napravljen, aplikacija neće funkcionisati i virus će brzo biti otkriven [5].

Pridružujući virusi ne menjaju sadržaj originalne datoteke, već samo njeno ime, i prave novu datoteku pod originalnim imenom koja sadrži virus. Umesto zdrave datoteke prvo se izvršava virus [5].

Virusi startnog zapisa svoj kod upisuju u glavni startni zapis čvrstog diska (master boot record) ili startni zapis aktivne particije na disku [5].

3.1.4.2. Makro virus i script virusi

Makro virusi su najčešće napisani i ugrađeni u dokumente koji se otvaraju aplikacijama iz paketa Microsoft Office. Ovi virusi za druge aplikacije su baš retki [5].

Skript virusi su podskup virusa koji napadaju sisteme datoteka, pisani na skript jezicima (JavaScript, PHP). Oni mogu da inficiraju i dokumenta u drugom formatu kao što je HTM, ukoliko datoteke tog formata omogućavaju i dozvoljavaju izvršavanje skriptova [5].

3.1.5. Špijunski programi (spyware)

Špijunski softver je softver instaliran bez znanja korisnika, koji služi da prati sve aktivnosti tog korisnika i da prikuplja informacije o njemu kao što su lozinke i finansijske informacije. Trojanski konji spadaju u špijunske programe.

Druga vrsta špijunskih programa su reklamni špijunski programi ili adware. On prikuplja informacije i šalje kompanijama koje se bave marketingom zasnovanim na

praćenju korisničkih navika pri pretraživanju Weba i na oglašavanju na iskaćućim prozorima i banerima ugrađenim u aplikativni softver [5].

Simptomi infekcije špijunskim programima su:

- neželjeni iskaćući (engl. Pop-up) prozori s reklamama koji se pojavljuju dok se pretražuje Internet,
- promene izgleda čitaća Weba – nova paleta alatki, promenjene ikonice ili baneri, promena podrazumevane stranice u čitaću,
- web zahtevi su preusmereni a veza sa Internetom je znatno sporija,
- računar radi sporije i nestabilno, operativni sistem se često blokira.

Neki od programa ove vrste su: Kazaa Media Desktop, e-Donkey, BearShare, DeamonTools kao i razni čuvari ekrana i teme za radnu površinu [5].

Detekcija ovih programa je jako teška i komplikovana. Nakon što se instaliraju ne mogu da se vide u sekciji „Add/Remove programs“. Najjednostavniji oblik špijunaže su špijunski kolačići. To su tekstualne datoteke koje razne marketinške kompanije koriste kako bi dobile informaciju kada je neki korisnik posetio neku Web stranicu. Ovakvi programi se jednostavno uklanjaju.

Postoje programi za zaštitu od ovog zlonamernog koda. Međutim, uvek treba paziti šta se instalira na računaru. Ne pritiskati mišem po iskaćućim prozorima i voditi računa sa elektronskom poštom. Nikad ne treba otvarati meilove od nepoznatog pošiljioca.

3.2. Zaštita od zlonamernog programa

Postoje različiti načini na koje se pojedinci i firme štite od nepoželjnih posetilaca ili softvera. Neki od tih načina su:

- specijalni programi,
- mrežne barijere,
- biometrijska zaštita,
- etičko hakerisanje.

3.2.1. Specijalni programi

Inficirani sistemi se čiste uz pomoć specijalnih programa za uklanjanje ovih softvera. Međutim, pošto postoji mnogo zlonamernih softvera koji su sakriveni u sistemu, ovi programi ne mogu uvek da ih pronađu. Zbog toga se ti softveri instaliraju ranije i na taj način oni čuvaju sistem da do zaraze ni ne dođe.

Postoje dve vrste softvera za zaštitu sistema:

- antivirusni softveri i
- softveri za zaštitu od špijunskog softvera.

Antivirusni softveri

Kao što je rečeno najlakši način da do zaraze dođe je instalacijom nekog softvera sumnjivog porekla i pritiskanjem miša po banerima i iskačućim prozorima. Zaštita od ovog je upravo izbegavanje instaliranja nesigurnih softvera i izbegavanje stranica sumnjivog sadržaja.

Drugi način zaštite su antivirusni programi. Neki su besplatni a za neke je potrebna licenca. Dve osnovne komponente kvalitetnog antivirusnog softvera su: klasičan skener i rezidentni skener. Klasičan skener proverava datoteke, MBR, bazu Registry, a rezidentni obezbeđuje proveru u realnom vremenu. Rezidentni skener proverava izvršne datoteke pri pokretanju, elektrošku poštu, Web stranice i P2P mrežu. Oba skenera koriste bazu opisa zlonamernih softvera, koja mora redovno da se obnavlja da bi detekcija bila uspešna. Ovaj softver mora da pronađe virus i da ga ukloni. U stvari to treba da uradi pre njegovog aktiviranja, u suprotnom postoji mogućnost da nakon što zarazi sistem ne može da se ukloni, jer neki virusi upisuju svoj kod i nakon toga antivirus ne ume da ovaj kod vrati u prvobitno stanje.

Najbolji besplatni antivirusni program je Avast i razvila ga je firma Alwil Software. Postoje i drugi besplatni programi kao što su: AVG, Antivir Personal Edition. Komercijalni softveri su Norton, Kaspersky, NOD32 i drugi.

Softveri za zaštitu od špijunskog softvera

Postoji i puno besplatnih i komercijalnih softvera ove vrste. Neki od tih softvera su: Spybot Search & Destroy, Spyware blaster.

Neki programi ove vrste spadaju u loše antišpijunske softvere, tzv. „rogue“ antišpijunske softvere. Oni prijavljuju da na sistemu postoji špijunski program iako ga nema i na taj način, uz pomoć društvenog inženjeringa teraju korisnike da kupe njihovu licencu.

3.2.2. Mrežne barijere

Direktna veza sa Internetom olakšava napadačima napad i zloupotrebu privatnih mreža. Tako da korisnici ne mogu da čuvaju svoje podatke. Da bi se zaštitili, administratori koriste mrežne barijere kako bi sačuvali svoje mreže.

Mrežne barijere se postavljaju kao kontrolne tačke između Interneta i privatne mreže. One ispituju pakete koji prolaze kroz mrežu i ako zadovoljavaju pravila koja su definisana u listama za kontrolu pristupa, ona će zabraniti ili dozvoliti prolaz tog paketa. Dakle, ona predstavlja filter između Interneta i lokalne mreže.

Funkcije mrežnih barijera [5]:

- filtriranje paketa,
- prevođenje mrežnih adresa i
- proksi servisi.

Filtriranje paketa. Proverava se zaglavlje paketa odnosno izvorišna i odredišna adresa kao i broj porta. Analizira se i upoređuje sa pravilima mrežne barijere. Ako paket zadovoljava pravila, dozvoljava mu se prolaz, u suprotnom se odbacuje [5].

Prevođenje mrežnih adresa. Prevodi adresu računara iz privatne mreže u jednu ili više javnih IP adresa i na taj način skriva identitet računara u lokalnoj mreži [5].

Proksi servisi. Proksi server je sloj između lokalne i spoljašnje mreže koji omogućava većem broju računara da dele jednu vezu ka Internetu i skladišti, tj. kešira podatke kako bi se ubrzao pristup tim podacima s lokalne mreže [5].

Mrežne barijere imaju i neke dodatne funkcije kao što su [5]:

- **Šifrovana provera identiteta** – dokazivanje identiteta korisnika na javnim mrežama,
- **virtuelno privatno umrežavanje** – uspostavljanje zaštićene veze između dve privatne mreže, preko nesigurnog medijuma kao što je Internet.

Postoje neki servisi koji su zasnovani na pretplati i oni su dostupni samo na nekim mrežnim barijerama. Oni mogu dubinski da analiziraju sadržaj paketa. Njihove funkcije su [5]:

- **traženje zlonamernog koda u paketima** – traži oznake virusa, crva i sl,
- **filtriranje na osnovu sadržaja** – blokira saobraćaj u zavisnosti od njegove sadržine.

3.2.3. Biometrijska zaštita

Reč biometrija potiče od grčke reči „bios“ i znači život, i „metron“ što znači mera i predstavlja skup metoda za identifikovanje pojedinaca na osnovu bioloških karakteristika ili karakteristika ponašanja. Najčešće se koristi za proveru identiteta ali je upotrebljiva i u drugim oblastima kao na primer prepoznavanje govora. Biometrijska provera identiteta obuhvata postupke prikupljanja i analize fizičkih karakteristika kao što su otisci prstiju i snimak rožnjače oka. Takođe i mnoge druge karakteristike koje se teško mogu oponašati, a takođe identifikuju čoveka, kao što je rukopis. Karakteristike se prikupljaju, odnosno „snimaju“ i pomoću specijalnih uređaja digitalizuju i obrađuju softverski [5].

Karakteristike kojima se opisuju biometrijske metode su [5]:

- **jedinstvenost** (opisuje koliko biometrijska karakteristika jednoznačno identifikuje pojedinca),
- **trajnost** (opisuje nepromenljivost karakteristike s vremenom, tj. koliko dugo osoba zadržava navedenu karakteristiku),
- **prikupljivost** (opisuje sa kojom se lakoćom dobija uzorak navedene karakteristike),
- **izvodljivost** (opisuje u kojoj je meri moguće u praksi implementovati navedene biometrijske metode),
- **prihvatljivost** (opisuje u kojoj je meri implementacija moguća a da se pri tome ne naruše ljudska prava).

Postoje dve vrste karakteristika na kojima se zasnivaju biometrijski metodi:

- biometrija zasnovana na fizičkim karakteristikama i
- biometrija zasnovana na karakteristikama ponašanja.

3.2.3.1. Biometrija zasnovana na fizičkim karakteristikama

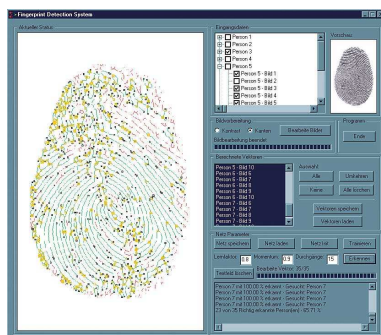
Otisak prsta (slika 9). Otisci prstiju su jedinstveni za svaki prst, svake osobe. Digitalno se predstavljaju sa 7–22 tačke čiji raspored jedinstveno identifikuje osobu. Ova je komercijalno najdostupnija metoda biometrijske tehnologije. Postoji puno jeftinih uređaja za prepoznavanje otisaka prstiju i za stane i za prenosne računare. Identifikacija osoba ovom metodom drugačije se naziva još i daktiloskopija. Karakteristike analize otiska prsta kao biometrijske metode su: osrednja prikupljivost i prihvatljivost i visoka jedinstvenost, trajnost i izvodljivost [5].



Slika 9 – Čitač otiska prsta [12]

Postoji i mogućnost da se prilikom startovanja računara ne koristi lozinka, nego da se pokrene uz pomoć usb čitača otisaka prstiju, koji vidimo na slici 9.

Na slici 10 se vidi program koji detektuje otiske prstiju.



Slika 10 – Fingerprint Detection System [14]

Rožnjača oka (slika 11). Skeniranje rožnjače oka obavlja se kamerom koja snima zapis o rožnjači. Dobijena slika se specijalnim programima predstavlja pomoću tačaka koje omogućavaju jednoznačno opisivanje uzoraka. Rožnjaču oka je moguće opisati sa 242 tačke. Ova tehnologija se često koristi za identifikaciju osoba koje ulaze u značajne prostorije, zato što spada u jednu od najsigurnijih biometrijskih metoda. Karakteristike ove metode su: visoka jedinstvenost i izvodljivost, osrednja trajnost i nizak nivo prikupljivosti i prihvatljivosti [5].



Slika 11 – Rožnjača oka [23]

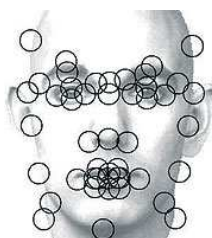
Geometrija šake. Ova provera identiteta je dostupna više od dvadeset godina. Biometrijski sistem meri fizičke karakteristike šake ili prstiju, kao što su dužina, širina, debljina prstiju i površina područja šake. Karakteristike ove metode su: visoka prikupljivost, osrednji nivo jedinstvenosti, trajnosti, izvodljivosti i prihvatljivosti [5].

Raspored vena dlana (slika 12). Za identifikaciju se koriste vene dlana. Informacije o venama dlana je teško duplirati jer su vene unutrašnji deo tela. Ova identifikacija nudi visok nivo preciznosti. Venski obrazac koji se koristi u ovoj tehnologiji oslanja se na sliku krvnih sudova u telu koja izgleda kao nasumična mreža na površini tela, kao na slici 12 [13].



Slika 12 – Krvni sudovi [10]

Prepoznavanje lica (slika 13). Tehnologija prepoznavanja lica radi tako što mapira strukturu kostiju lica, na primer, razmak između očiju, nosa, usta i ušiju. Mere se zatim digitalno kodiraju da bi se koristile u svrhu upoređivanja i potvrde. Uređaj za prepoznavanje lica gleda sliku ili video osobe i upoređuje ga sa onim koji je u bazi podataka. Na taj način upoređuje strukturu, oblik i proporcije lica, razmak između očiju, nosa, usta i vilice idr. Snima se nekoliko slika korisnika iz različitih uglova i sa različitim izrazima lica. Za vreme identifikacije, korisnik stoji ispred kamere nekoliko sekundi i onda se slike porede sa onim koje se nalaze u bazi [13].



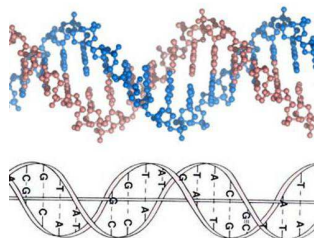
Slika 13 – Prepoznavanje lica [14]

Da bi se sprečilo da korisnik koristi sliku prilikom skeniranja, program je napravljen tako da može tražiti od korisnika da trepne, nasmeje se ili klimne glavom, ili korišćenjem termografije lica da bi se snimila toplota u licu [13].

Ova biometrijska metoda je jedna od jeftinijih jer nije neophodna skupa specijalna oprema. Prepoznavanje lica može se obaviti na svakom računaru sa kvalitetnijom video- kamerom, a za samo prepoznavanje zadužen je softver [5].

DNK (slika 14). Očitavanje i prepoznavanje jedinstvenog DNK osobe je relativno nova grana biometrije. U kombinaciji sa drugim biometrijskim tehnikama, analiza DNK obezbeđuje visoku tačnost prepoznavanja. Velika je verovatnoća da će se u budućnosti podaci o DNK čuvati u ličnim kartama. DNK se danas koristi u brojnim

sverama, kao što su dokazivanje očinstva ili rodbinskih veza i u kriminalistici. Karakteristike ove metode su: visok nivo jedinstvenosti, trajnosti i izvodljivosti i nizak nivo prikupljivosti i prihvatljivosti [5].



Slika 14 – DNK [15]

3.2.3.2. Biometrija zasnovana na karakteristikama ponašanja

Biometrija ponašanja opisuje fizičke karakteristike tela koje su delom jedinstvene za svaku osobu, kao što su kretanje u prostoru, glas, izgled idr. Dobijeni uzorci se predstavljaju krivama koje se koriste za opis ponašanja, a na osnovu njih je moguće raspoznavati ljude. One se uglavnom koriste zajedno sa još nekim tehnologijama [5].

Prepoznavanje glasa. Vrš se provera identiteta na osnovu jedinstvenih karakteristika glasa. Korisnik koji želi da se predstavi sistemu mora da izgovori tekst koji je prethodno izgovorio i koji je unešen u bazu podataka. Ovu metodu treba koristiti u kombinaciji sa drugim metodama jer postoji opasnost da neovlašćena osoba snimi ovlašćenog korisnika kako izgovara tu rečenicu i to kasnije reprodukuje. Ovo se uglavnom koristi u druge svrhe kao što je prepoznavanje govora, tj. prevođenje glasa u tekstualni zapis. Karakteristike ove metode su: nizak nivo jedinstvenosti, trajnosti i izvodljivosti, osrednji nivo prikupljivosti i visok nivo prihvatljivosti [5].

Prepoznavanje rukopisa ili potpisa. Ova metoda je zasnovana na analizi dinamike potpisa, tj. na merenju brzine, pritiska i ugla pri potpisivanju ili pisanju nekog teksta. Često se koristi u pravosuđu. Karakteristike su: nizak nivo jedinstvenosti, trajnosti i izvodljivosti, visok nivo prikupljivosti i prihvatljivosti.

Dinamika kucanja. Za ovu tehniku nisu potrebni dodatni uređaji za prikupljanje uzoraka. Glavna karakteristika na kojoj se zasniva ova tehnika su različiti vremenski razmaci koje korisnik pravi između pritiskanja dva tastera. Karakteristike su: nizak nivo jedinstvenosti, trajnosti i izvodljivosti, visok nivo prikupljivosti i prihvatljivosti [5].

Sa razvojem biometrijskih metoda, mnoge kompanije su počele da koriste ove metode za proveru identiteta. Međutim, postoje i negativni aspekti primene ovih metoda. Ove metode mogu da izazovu povređivanje korisnika. Ukoliko lopov želi da

ukrade tuđ auto koji koristi biometrijsku zaštitu, sem krađe on može i da povredi vlasnika da bi došao do željenog objekta. Takođe prikupljeni podaci mogu da se zloupotrebe tako što će se prodati nekom trećem licu koje će te podatke kasnije da zloupotrebi.

3.2.4. Etičko hakerisanje

Kada se sprovedu sve preporučene mere za zaštitu mreža i informacionih sistema od narušavanja sigurnosti, treba uraditi analizu i proveriti uspešnost zaštite. Osmišljeni su načini ispitivanja koji bi trebalo da pokažu koliko je zaštita pouzdana i efikasna. Međutim, oni koji napadaju mrežu stalno smišljaju nove načine i metode da ostvare svoje ciljeve. Da bi zaštitili mrežu, klijenti često angažuju hakere koji po dogovoru napadaju i proveravaju sigurnost, uz obavezu da svoja saznanja drže u tajnosti, da ih ne zloupotrebe i da ih prenesu samo organizaciji koja ih je angažovala i isključivo u svrhu unapređenja sigurnosti. Takvi hakeri se drugačije nazivaju i „etički hakeri“ ili „hakeri sa belim šeširom“. Oni uglavnom rade u raznim firmama koje se bave bezbednošću sistema [5].

Haker

Reč „haker“ prvenstveno se koristila da bi predstavila osobu koja uživa da proširuje svoje znanje o računarskim sistemima, za razliku od običnih korisnika, haker obožava da se bavi programiranjem i sticanjem novih znanja, i to se prvenstveno nazivalo „hakerisanje“. Zbog porasta popularnosti računara i njihove visoke cene pristup računarima je uglavnom bio ograničen. Najveća šteta u to vreme je bila krađa procesorskog vremena ili prostora na memorijskim medijumima. Nekada se dešavalo da preraste u bezopasne šale. Do oštećenja je moglo da dodje samo greškom tog korisnika, odnosno hakera. Ukoliko je dolazilo do nekih destruktivnih aktivnosti to bi objavile novinske agencije, koje umesto da koriste termin „kompjuterski kriminal“ koriste termin „haker“ da bi opisali osobu koja neovlašćeno ulazi u tuđ sistem zbog zabave, osвете ili zarade. I dalje se ova reč često koristi u negativnom smislu, a ređe u pozitivnom.

Etički haker

Etički haker se naziva još i „haker sa belim šeširom“. To je lice koje je protiv zloupotrebe informacionih sistema. Tako se nazivaju oni koji pokušavaju da prodru u tuđe sisteme i mreže kako bi pomogli vlasnicima tih sistema da sagledaju sigurnosne propuste. Mnogi od njih su zaposleni u kompanijama koje se bave bezbednošću. Sa druge strane postoje „hakeri sa crnim šeširima“ ili zlonamerni hakeri koji pokušavaju da upadnu u sistem i ukradu poverljive informacije ili da nanesu neku štetu. Obe vrste hakera koriste slične metode i alate ali s različitim ciljem.

Etički hakeri moraju pre svega da budu osobe od poverenja. Ispitujući bezbednost klijentovog sistema, etički haker može da otkrije informacije o klijentu koje bi trebalo da ostanu tajna. U velikim slučajevima gubitak tih informacija može da dovede do velikih gubitaka za firmu. Oni moraju da imaju veliko iskustvo u svim oblastima vezanim za računare.

Strpljivost je najbitnija osobina etičkih hakera. Oni moraju da se stave u poziciju zlonamernih hakera, koji su poznati po strpljivosti i spremnosti da nadgledaju sistem danima i nedeljama, čekajući priliku da upadnu u sistem [5].

Njihov posao je da pronađu odgovor na tri pitanja [5]:

- Šta može napadač da vidi na cilnom sistemu?
- Šta može napadač da uradi sa tim informacijama?
- Da li je neko primetio napadačev napad ili uspeh?

Na kraju piše izveštaj sa saznanjima koje je prikupio tokom procene i dostavlja je klijentima. Ako postoje ranjivosti na sistemu, izveštaj može da bude jako opasan ukoliko dospe u pogrešne ruke, tako da mora pažljivo da se dostavi direktno ovlašćenom licu.

Deset zapovesti računarske etike

Institut za računarsku etiku je neprofitna istraživačka organizacija koju čine Brookings Institute, IBM, The Washington Consulting Group i Wašington Theiological Group. Ova organizacija objavila je deset zapovesti računarske etike [5]:

1. Ne koristi računar da povrediš drugog.
2. Ne mešaj se nepozvan u tuđ rad na računaru.
3. Ne njuškaj po tuđim datotekama.
4. Ne koristi računar da bi lažno svedočio.
5. Ne koristi računar da bi krao.
6. Ne koristi komercijalni softver koji nisi platio.
7. Ne koristi tuđe računarske resurse bez odobrenja ili nadoknade.
8. Ne prisvajaj sebi zasluge za tuđu intelektualnu svojinu.
9. Razmisli o posledicama koje će program koji pišeš ili sistem koji projektuješ imati na društvo.
10. Koristi računar samo na način koji ne ugrožava druge.

3.3. Rootkit alati

Naziv „rootkit“ potiče od engleskih reči „root“, što znači koren i odnosi se na korisnika sa najvišim nivoom pristupa u UNIX i Linux okruženju, i reči „kit“ koja znači alat ili skup alata. Rootkit, dakle, možemo definisati kao skup alata, koji napadačima omogućuje najviši nivo pristupa i potpune kontrole kompromitovanog sistema. Da bi napadač mogao uspešno da završi napad, rootkit mora ostati „skriven“ u sistemu, tj. ne smeju ga videti administratori i programi za zaštitu od zlonamernog softvera. Dakle, rootkit predstavlja skup alata koji skriva prisustvo napadača i obazbeđuje mu potpunu kontrolu nad kompromitovanim sistemom [5].

3.3.1. Razvoj rootkit alata

U početku se termin rootkit odnosio na kolekciju alata koji su korišćeni za sticanje administratorskog pristupa na UNIX operativnim sistemima. Te kolekcije alata su često uključivale dobro poznate alate za nadzor sistema koji su bili modifikovani da prikriju akcije uljeza i hakera na sistemu [4].

Danas rootkit alati za Windows rade na drugačiji način i obično se koriste za skrivanje različitih vrsta malicioznog softvera od vlasnika sistema, pre svega od antivirusnog softvera. Rootkit sam po sebi nije zlonameran program, već neka vrsta neutralnog alata koja je u slučaju skrivanja virusa, crva, zadnjih vrata i spajvera iskorišćena u negativne svrhe. On ne čini nikakvu štetu, ali ako je kombinovan sa drugim štetnim programom, može da predstavlja pravi razlog za glavobolju, ukoliko uopšte korisnik uspe da sazna da ga ima na sistemu. Zbog toga je potencijal rootkit alata ogroman, a antivirusne kompanije priznaju da ovaj koncept još nije ni približno iskorišćen u onoj meri u kojoj bi mogao da bude. Na žalost, uvid u dešavanja jasno pokazuju da se tendencije kreću u tom smeru - čak i antivirusne kompanije priznaju da očekuju povećanje broja štetnog softvera koji će koristiti moć rootkit alata [4].

Najveća prašina oko ove vrste programa digla se pred kraj 2005. godine, kada je Sony uz neka svoja muzička CD izdanja isporučivao i skrivene rootkit programe. Kada bi se takav CD pokrenuo na računaru pod Windowsom, program bi se bez znanja korisnika računara instalirao i prosleđivao matičnoj kompaniji informacije o tom korisniku. Pored toga, taj rutkit je stvarao ozbiljne ranjivosti na računaru na kome je bio instaliran [4].

Prvenstveno, istorijski gledano, ovu tehnologiju su koristili samo hakeri. To se promenilo kada su FBI i razne druge obaveštajne službe otkrile korist ove tehnologije [4].

3.3.2. Detekcija rootkit alata

Šanse da se detektuje postojanje rootkita na sistemu leži u tome da se skeniraju procesi u radnoj memoriji, da se nadzire saobraćaj na mreži ili registruje instaliranje

programa bez znanja administratora. Međutim, veštine kreatora rootkit softvera napreduju, pa su tako najnovije verzije sposobne da presreću sistemske pozive upućene kernelu operativnog sistema, filtrirajući sopstvene. Rezultat je takav da jednostavno odsustvuju svi znakovi toga da se odvija proces koji pokreće rootkit, počev od imena izvršnog fajla pa do podešavanja u registry bazi. Posledica toga je da program postaje i ostaje potpuno nevidljiv [4].

3.3.3. Vrste rootkit alata

Postoje dve vrste rootkit alata, a to su [5]:

- rootkit alati za linux operativne sisteme i
- rootkit alati za windows operativne sisteme.

Mnogo je lakše bilo da se naprave alati za linux operativne sisteme zbog njihovog otvorenog koda sistema, dok je kod windowsa otežano ubacivanje ovog alata zbog skrivenog izvornog koda i zbog zaštite sistema koje onemogućava zamenu izvršnih fajlova.

3.3.3.1. Linux rootkit alati

Napad na sistem zasnovan na rootkit alatima izvodi se u četiri faze [5]:

- sakupljanje informacija o ciljnom sistemu,
- sticanje administratorskih prava,
- instaliranje rootkit alata i
- uspostavljanje kontrole nad ciljnim sistemom.

Rootkit alati se dele na dve grupe:

- korisnički (aplikacioni) rootkit alati i
- kernelski (na nivou jezgra) rootkit alati.

Korisnički rootkit presreće sistemske pozive na aplikacionom nivou. Kad god aplikacija napravi sistemski poziv, izvršenje tog sistemskog poziva je poznato pa ga zato rootkit vrlo lako može presresti. Jedna od najčešćih tehnika korisničkog rootkita je da modifikuje sistemske fajlove operativnog sistema. Dakle, rad ovih alata zasniva se na zameni legitimnih aplikacija zlonamernim datotekama. Napadač tom prilikom ostavlja “zadnja vrata” da bi i drugi put uspeo da uđe neprimećen i na lakši način [5].

Kernelski rootkit presreće ili modifikuje sistemske pozive na nivou kernela, odnosno na nivou jezgra, nivou kome obični, ili neautorizovani, korisnici nemaju pristupa. Presretanje sistemskih poziva na nivou kernela je idealno zato što se

kernel nalazi na najnižem nivou operativnog sistema i kao takav predstavlja najpouzdanije mesto sa koga se mogu izvršavati sistemski presretanja [4].

Zadnja vrata

Korišćenje zadnjih vrata za ponovne ulaske je popularna tehnika hakera, pošto se alati za postavljanje zadnjih vrata nalaze besplatno na hakerskim sajtovima. Napadači postavljaju zadnja vrata koristeći skriveni ID i password za logovanje koji proizvođači hardvera ili softvera legitimno postavljaju za svoje tehničare.

Zadnja vrata obezbeđuju tri glavne funkcije napadačima [1]:

- ući kasnije u sistem što je moguće skrivenije,
- ući kasnije čak i kada ga administrator obezbedi, npr. promeni šifru,
- ući kasnije u sistem u što kraćem vremenu.

Zaštita od rootkit alata

Za ove alate veži isto što i za viruse i crve – mnogo je lakše sprečiti instaliranje ovih programa nego ih kasnije ukloniti. Administrator treba redovno da proverava dnevničke datoteke i da u njima traži sumnjive ilegalne aktivnosti. Na taj način, brže može da pronađe rootkit ukoliko do instalacije dođe.

3.3.3.2. Windows rootkit alati

Kao što je rečeno, instalacija rootkit alata u windows sistemima je teža zbog zatvorenog izvornog koda.

Postoje tri osnovne metode implementacije aplikacionih rootkit alata [5]:

- upotreba postojećeg interfejsa za ubacivanje zlonamernog koda – ovaj sistem sadrži određene interfejse koji omogućavaju nadogradnju sistema sa alatima drugih proizvođača,
- deaktiviranje sistema zaštite datoteke,
- napadi DLL injection i API hooking – napadač ubacuje zlonamerni kod u neki proces i na taj način menja originalnu funkciju procesa.

4. Zločini počinjeni uz pomoć računara

Postoji puno kriminalnih dela koja ne nanose štetu direktno računaru već računar samo služi kao pomoć u organizovanju tog krivičnog dela. Sva tradicionalna krivična dela mogu da se ostvare uz pomoć računara, koji u velikoj meri olakšava njihovo sprovođenje.

Neka od ovih dela su:

- krađa identiteta na Internetu,
- Internet prevara,
- cyberstalking (syber uhođenje),
- dečija pornografija na Internetu,
- cyber terorizam,
- trgovina drogom,
- Internet ubistva.

4.1. Krađa identiteta na Internetu

Krađa identiteta je zločin kojim zločinci imitiraju druge ljude, obično za finansijsku dobit. Danas se često od pojedinaca traži da otkriju dosta ličnih informacija kao što su brojevi socijalnog osiguranja, potpis, ime, adresa, telefonski brojevi, pa čak i informacije o bankarskim i kreditnim karticama. Krađa identiteta može da ide dalje od novčanih posledica. Lopovi mogu da koriste tuđe informacije da dobiju neki lični dokument na kojem će biti njihova slika, ali tiđe ime i informacije [18].

Krađa identiteta na Internetu je vrsta prevare kojom se od korisnika računara putem lažne poruke, uz pomoć e-meila ili web sajta, saznaju lični i finansijski podaci. Internet pruža nove načine za lopove da ukradu tuđe lične informacije i da počinu prevaru. Jedan od načina je četovanjem i trojanskim konjem koji skupljaju sve informacije sa računara kao na primer šifre [18].

Ishod krađe identiteta je obično isti, bez obzira kako lopov dođe do informacija. Krađa identiteta na Internetu se razlikuje od obične krađe identiteta na nekoliko načina. Obična krađa identiteta se dešava nakon što je nekome nešto fizički ukradeno, kao na primer novčanik sa kreditnim karticama i vozačkom dozvolom. Krađa identiteta na Internetu može biti mnogo gora zato što može biti mnogo

razornija nego konvencijalne krađe, jer je većina žrtava potpuno nesvesna da joj je nešto ukradeno dok ne bude prekasno [18].

4.2. Internet prevara

Internet prevara predstavlja korišćenje Internet usluga ili softvera sa Internet pristupom sa ciljem pribavljanja imovinske koristi sebi ili drugom, ili nanošenjem štete. Ovo je najrašireniji oblik kompiuterskog kriminala. Broj oblika prevara i način njihove realizacije je preveliki. U praksi se javljaju kako primitivne i grube prevare tako i one prevare kod kojih učesnici ispoljavaju visok stepen veštine [19].

Neke od vrsta Internet prevara su [19]:

- pecanje (engl. phising),
- farming (engl. pharming),
- automobilske prevare na Internetu,
- online aukcijske prevare,
- maloprodajne šeme.

Pecanje su sistemi krađe poverljivih informacija, brojeva računa i pin kodova koristeći se lažnim web-sajtovima. Najčešće su to web – sajtovi finansijskog sadržaja, odnosno bankarski web – sajtovi, gde se očekuje da korisnik unese poverljive podatke, broj računa ili pin kod. Drugi način je preko e-meila, gde se korisniku pošalje e-mail u kome piše da će kartica biti isključena ako se ne javi na određeno mesto, i na taj način se očekuje da korisnik ode na određenu web – lokaciju, gde će mu uzeti sve podatke [19].

Farming je prefinjenija prevara iako podseća na „pecanje“, jer u ovom slučaju ne treba ni odgovarati na mail da bi Farmeri došli do podataka. Dovoljno je samo otvoriti mail i na računar se prikači malver (engl. malware) i ključ za generisanje (engl. key generator) koji će krasti informacije sa računara korisnika. Kad korisnik pokuša da se uloguje na sajt, virus će ga preusmeriti na lažan sajt banke, koji izgleda identično kao pravi, i kad unese svoje podatke prevaren je [19].

Automobilska prevara na Internetu. Prevarant postavlja nepostojeće vozilo na prodaju na web – sajt, najčešće luksuzan ili sportski auto, čija se cena nalazi dosta ispod tržišne vrednosti. Detalji o vozilu i slike se preuzmu sa sajtova koji se bave prodajom automobila preko Interneta. I na razne načine ubeđuje kupca da da bar deo para pre nego što shvati da je prevaren [19].

Online aukcijske i maloprodajne šeme. U online aukciji prevarant započinje aukciju na sajtovima sa veoma niskom cenom, pogotovu za skupe stvari kao što su satovi, kompjuteri ili vredni kolekcionarski predmeti. Prevarant prihvata uplatu, ali ne

isporučuje robu, ili isporuči nešto drugo u mnogo manjoj vrednosti od one koju je kupac tražio. Ista situacija je i sa maloprodajnim šemama [19].

4.3. Cyberstalking (syber uhođenje)

Cyberstalking je korišćenje Interneta za uhođenje ili uznemiravanje pojedinca, grupe pojedinaca ili organizacije. Takođe mogu da sadrže i netačne optužbe, nadgledanje, pretnje, sakupljanja podataka koji se koriste za uznemiravanje. Uznemiravanje možemo da definišemo kao mogućnost da jedna osoba koja poseduje određene podatke uznemirava neku drugu osobu tim podacima. Osoba koja se bavi syber uhođenjem može da bude nepoznata osoba sa Interneta ili osoba koju žrtva poznaje [21].

4.4. Dečija pornografija na Internetu

Dečija pornografija je jedan od oblika kriminala koji se najbrže širi na Internetu. U današnje vreme mnogo pornografskog sadržaja je dostupno na Internetu, koji omogućava brz i lak prenos tog sadržaja kao i njegovo umnožavanje [16].

Dečija pornografija se odnosi na materijale koji prikazuju dete ili osobu koja izgleda kao dete u eksplicitnim seksualnim scenama, ili u situacijama koje navode da se pomisli da je dete uključeno u eksplicitne seksualne scene. U dela dečije pornografije spadaju: proizvodnja dečije pornografije, distribucija, nuđenje, nabavljanje i posedovanje [16].

U Srbiji je 2010. godine počela da se sprovodi policijska akcija „Armagedon“. Ova akcija namenjena je sprečavanju distribucije dečije pornografije putem Interneta i ima međunarodni karakter. Srpska policija prilikom sprovođenja ove akcije sarađuje sa nekoliko država, pre svega Velikom Britanijom i Sjedinjenim Američkim Državama (SAD). Tokom 2010. godine uhapšeno je deset muškaraca, a njihov broj se u narednoj godini znatno povećao, što ukazuje na značaj ovog problema. Srbija je u ovoj akciji, koja se i dalje sprovodi, postigla jako dobre rezultate, a to su prepoznali i strani državni. Odeljenju za borbu protiv visokotehnološkog kriminala 2011. godine uručena je plaketa za zahvalnost, za rezultate akcije „Armagedon“. To je jedan od pokazatelja da u Srbiji postoji dosta razvijena svest o problemu dečije pornografije kao i inicijativa da se taj problem reši [16].

4.5. Sajber terorizam

Sajber terorizam, u širem smislu, predstavlja napade i pretnje usmerene protiv računara, računarskih mreža i informatičke opreme za skladištenje podataka, sa svrhom zastrašivanja i uticanja na vladajuće strukture i javnost u političkom i

socijalnom životu. Ovi napadi su uglavnom usmereni na personalne računare, a obavljaju se uglavnom pomoću virusa [17].

Kako još nije potpuno razjašnjeno šta je tačno sajber terorizam često dolazi do nesporazuma u tumačenju. Pod pojmom sajber terorizam često se pogrešno podrazumevaju slučajevi računarske ili Internet zloupotrebe, kao što su hakerske aktivnosti, širenje virusa i razni drugi on-line incidenati [17].

Neke od definicija kažu da je sajber terorizam „kriminalni akt izvršen kroz računare rezultujući u nasilju, smrti i/ili destruktiji, stvarajući teror radi ubeđivanja vlade da promeni svoju politiku“, zatim „nedozvoljeni napad ili pretnja uz pomoć računara, računarskih mreža ili sačuvanih podataka s ciljem da se zaplaši vlada ili njeni građani u cilju ostvarenja političkih ili drugih ciljeva“ itd [17].

4.6. Trgovina drogom

Trgovci drogom sve više koriste prednosti Interneta, tj. koriste e-meilove i druge Internet tehnologije da bi prodavale ilegalne supstance. Neki prodavci čak sklapaju dogovore u Internet kafeima, samim tim smanjuje se komunikacija licem u lice i omogućava im se veća sloboda [20].

4.7. Internet ubistva

Ovaj zločin se ostvaruje tako što ubica upoznaje žrtvu na Internetu. Naziv Internet ubica predstavlja osobu koja pronalazi žrtvu na Internetu ili snima i prikazuje ubistvo na Internetu. Prvo poznato ubistvo ove vrste desilo se 1996. godine [22].

U ovu oblast spada i Internet samoubistvo. Internet samoubistvo predstavlja pakt napravljen između pojedinaca koji se upoznaju na Internetu. Nekoliko samoubistava se desilo u Japanu ali u svakom slučaju ova samoubistva su jako retka [22].

Takođe, na Internetu se sreću i serijske ubice. Serijske ubice biraju troje ili više ljudi u određenom vremenskom razmaku između i to rade iz psihološkog zadovoljstva [22].

5. Istraga kompjuterskog kriminala

Digitalna forenzička analiza se deli u dve osnovne kategorije [2]:

- zvaničnu (javnu) i
- korporacijsku (privatnu) digitalnu forenzičku istragu.

5.1. Zvanična (javna) digitalna forenzička istraga

Ova istraga uključuje policijske organe istrage, specijalno tužilaštvo i specijalno sudstvo za borbu protiv visokotehnološkog (kompjuterskog) kriminala. Ovi organi rade u skladu sa raznim zakonima kao što su : Zakon o krivičnom postupku, Zakon o borbi protiv visokotehnološkog kriminala, Zakon o zaštiti informacija i informacionih sistema, Zakon o digitalnom dokazu, Zakon o elektronskom potpisu, Zakon o elektronskoj trgovini i razni drugi zakoni koji regulišu elektronsko poslovanje [2].

Zvanični organi istrage treba da rade prema strogo utvrđenim standardnim operativnim procedurama (SOP) za: pretragu, privremeno oduzimanje i ispitivanje računarskih sistema i drugih mrežnih uređaja, akviziciju digitalnih podataka/ dokaza sa različitih platformi i slika u cilju otkrivanja validnih digitalnih dokaza. Istražni organi moraju mnogo dobro da poznaju zakone i propise [2].

Prilikom utvrđivanja karaktera krivičnog dela, istražni organi traže odgovore na mnoga pitanja kao što su [2]:

1. Šta je bilo sredstvo izvršenja krivičnog dela?
2. Da li su računarski sistem i mreža poslužili kao jednostavan prolaz za izvršavanje krivičnog dela?
3. Da li je u pitanju kradja, provala ili vandalizam u sistemu?
4. Da li je napadač ugrozio nečiju privatnost i druga prava, ili uznemiravao?

Računarski sistem ili mreza se koriste kao sredstvo za izvršenje krivičnog dela, kao što je pištolj kod ubistva.

U izgradnji slučaja krivičnog dela mogu se razlikovati tri glavne faze [2]:

- postojanje slučaja izvršenja krivičnog dela,

- istraga krivičnog dela i
- suđenje.

Opšti proces zvanične istrage se sastoji iz četiri faze, i unutar svake faze se nalazi po nekoliko koraka. A to su: [2]:

- inicijalna istraga,
- ulazak u trag napadaču,
- otkrivanje identiteta napadača,
- hapšenje.

Zvanični proces istrage kreće od prijave krivičnog dela policiji. Nakon toga istražni organi prikupljaju dokaze za pokretanje tužbe. Zatim policija upoznaje tužioca koji obezbeđuje nalog za istragu od istražnog sudije i pokreće zvaničnu istragu. Sa sudskim nalogom organi istrage mogu legalno privremeno da oduzimaju osumnjičeni računarski sistem ili fizičku sliku čvrstog diska, radi forenzičke akvizicije i analize digitalnih dokaza [2].

Pre privremenog oduzimanja računarskog sistema, istražitelj dostavlja preliminarne dokaze o osnovanoj sumnji tužiocu za visokotehnološki kriminal i zahteva nalog za pretragu. Specijalni tužilac podnosi specijalnom sudu za visokotehnološki kriminal zahtev za nalog za pretres imovine osumnjičenog u kojem iznosi činjenice o predistražnom postupku i prilaže dokaze. Na osnovu ovog zahteva i dokaza o osnovanoj sumnji, specijalni sudija izdaje nalog za pretres stana i računarskog sistema osumnjičenog [2].

5.2. Korporacijska digitalna forenzička istraga

Javlja se sve veća potreba za zaštitom organizacija od različitih incidenata. Svaka od organizacija može da unajmi jednog od retkih stručnjaka u ovoj oblasti, ali je to i dalje jako skupo pa to predstavlja ograničavajući faktor za organizacije.

Dobra je praksa da korporacijski digitalni forenzičar timski radi sa administratorima sistema, mreže i zaštite i drugim specijalistima zaštite u cilju obezbeđivanja prihvatljivog nivoa zaštite računarskih sistema i bezbednog rada računarske mreže u Internet okruženju. Svi oni uglavnom rade samostalno ali u slučaju glavnog kompjuterskog incidenta, uvek rade zajedno. Ovakav rad obezbeđuje efikasno i efektivno trajno saniranje kompjuterskog incidenta u organizaciji i bez pozivanja spoljnih specijalista [2].

Ukoliko neka organizacija odluči da sama formira sopstveni tim za digitalnu forenzičku istragu, očekuje se da zvanični državni organi za borbu protiv kompjuterskog kriminala, obezbede [2]:

- pomoć timovima korporacija za otkrivanje uzroka incidenta i napadača u sistemima u kojima nemaju nadležnost,
- usaglašavanje korporacijske politike zaštite sa lokalnim zakonima i regulativama,
- preporuke i procedure za kontrolu sistema zaštite i
- informacije za obrazovanje u oblasti digitalne forenzike.

Formiranje korporacijskih kapaciteta može pozitivno da se odrazi u oblasti upravljanja ljudskim resursima. Korporacijska istraga može da obezbedi ključne informacije za različite aspekte upravljanja ljudskim resursima, kao što su: otpuštanje zaposlenih i ukidanje radnih mesta, upravljanje zaposlenima, disciplinske akcije, procena ekstremnih slučajeva (smrt, samoubistva i kidnapovanja). Takođe može da odigra značajnu ulogu za zaštitu intelektualne svojine, ugleda i brendova korporacija, ispitivanjem lažnih web sajtova, phishing napada i td [2].

5.2.1. Uspostavljanje tima za upravljanje kompjuterskim incidentom

Ovaj tim treba da bude centralizovan za sve delove korporacije. Može da bude sastavljen od zaposlenih u korporaciji koji ulaze u ovaj tim ukoliko dođe do incidenta. Članovi tima mogu biti i iznajmljeni ali u tom slučaju oni predstavljaju dodatnu ranjivost po sistem. Samo neke ogromne korporacije imaju posebno oformljen tim koji se bavi digitalnom forenzikom.

Tim za upravljanje bezbednosnim kompjuterskim incidentom treba da uključi sledeće uloge zaposlenih ili iznajmljenih specijalista [2]:

1. menadžer zaštite informacija,
2. administrator računarskog sistema/ mreže,
3. specijalista za upravljanje i kontrolu bezbednosnog rizika,
4. kontrolor sistema kvaliteta,
5. predstavnici drugih timova,
6. digitalni forenzičar,
7. pravnik organizacije,
8. menadžer za upravljanje ljudskim resursima.

Jako je bitno da korporacija generiše i implementira politiku digitalne forenzičke istrage sa saopštenjima koja omogućavaju ovlašćenim zvaničnim organima istrage da pristupe sistemu i izvrše akviziciju digitalnih podataka u fazu uključivanja zvaničnih organa istrage u korporacijsku forenzičku istragu. Saopštenja ove politike treba da sadrže najmanje sledeće zahteve za [2]:

- zaštitu osetljivih podataka,
- smanjenje rizika kod pristupa,
- definisano vreme zadržavanja informacija,
- usklađivanje sa legalnim zahtevima,
- forenzički oporavak i istragu incidenta,
- uspostavljanje forenzičkih resursa korporacije,
- obuka i osposobljavanje tima potrebnim znanjima i veštinama,
- oprema forenzičke laboratorije i terenskih forenzičkih alata i
- iznajmljivanje spoljnih partnera i eksperata u slučaju potrebe.

Uspeh formiranja ovog tima najviše zavisi od menadžmenta korporacije, jer je najteže njih ubediti da taj tim može da bude od velike koristi za korporaciju.

5.2.2. Proces korporacijske istrage

Korporacijska istraga se može smatrati predistražnim postupkom zvanične istrage kompiuterskog kriminala. Odvija se u tri glavne faze [2]:

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

Pokretanje istrage obuhvata obezbeđivanje mesta incidenta, pretragu, akviziciju dokaza izradu hipoteze o upadu i istraživanje alternativnih objašnjenja. **Određivanje karaktera incidenta** obuhvata analizu incidenta, analizu dokaza sakupljenih u prvoj fazi zajedno sa alternativnim objašnjenjima i određivanje karaktera incidenta – da li je bezbednosni incident krivično delo ili prirodan događaj. **Analiza digitalnih podataka** obuhvata analizu celokupnog digitalnog ili analognog dokaznog materijala, pripremu digitalnih dokaza za prezentaciju incidenta i drugih nalaza istrage vlasniku IKT sistema, ili zvaničnim organima, ako to vlasnik dozvoli.

Procedura korporacijske istrage kompjuterskog incidenta treba da obuhvata i sledeće postupke [2]:

- proveru evidencija, log fajlova kao i ostalih informacija o osumnjičenom,
- ispitivanje informanata,
- kontrolu svih faza,
- pripremu organa za pretragu (lociranje kompromitovanog računara),
- pretres resursa osumnjičenog i
- prikupljanje i analizu dokaza.

Da bi uspeh ove istrage bio potpun treba preći sedam sledećih koraka [2]:

- eliminisati očiglednost,
- postaviti hipotezu o napadu,
- rekonstruisati krivično delo,
- otkriti trag do osumnjičenog računara sa koga je napad izvršen,
- analizirati izvorni, ciljni i posredne računare,
- skupiti dokaze, uključujući ako je moguće i sam računar,
- predati nalaze i dokazni materijal korporacijskim ili zvaničnim organima istrage za dalji postupak.

Eliminisati očiglednost. Istraga počinje sa ovim korakom jer je najbitnije odrediti da li se incident stvarno dogodio, zato što računarski sistem može da padne iz više razloga. **Stvara se hipoteza o napadu** tako što prvo treba razumeti kako je napadač ušao u sistem. Teoretski se analizira napad. Treba testirati sve hipotetičke putanje svih korisnika koji imaju pravo pristupa da bi se utvrdilo da nisu možda oni napali sistem. Računar u ovoj fazi treba a ostane u onom stanju u kom je pronađen, jer uključivanje ili isključivanje računara može da izazove razne promene u računaru, posebno ako je u pitanju Microsoft OS. Treba utvrditi vreme i datum napada. Jedini način na koj bi računar mogao da se isključi je izvlačenjem kabla iz napajanja. U ovoj vrsti kriminala, za razliku od ostalih moguće je **rekonstruisati krivično delo**. Može da se sazna kako je napadač pristupio računaru, koju tehnologiju je koristio. **Rekonstrukcija traga do osumnjičenog računara.** Kompjuterski kriminalci su jako vešti i jako retko padaju u zamku ali se ipak po nekad desi, što je jako dobro za istražne organe. Zato se prvo traže logičke greške. Sam računar često ostavlja različite tragove pa forenzičar treba da zna šta i gde treba da traži. Iskusan napadač nikada ne napada sa svog računara. **Predavanje nalaza i dokaznog materijala** korporacijskim ili zvaničnim organima istrage za dalji postupak, forenzičar vrši isključivo po odobrenju vlasnika napadnutog sistema [2].

6. Model integrisanih procesa digitalne forenzičke analize

Ovaj model kreće sa pretpostavkom da je sam računar mesto krivičnog dela odnosno digitalno mesto krivičnog dela. Za otkrivanje fizičkih dokaza model primenjuje metode i tehnike istrage krivičnog mesta krivičnog dela i koristi iskustva iz istrage klasičnog kriminala. U istrazi digitalnog mesta krivičnog dela model koristi programski kod – binarne zapise za otkrivanje digitalnih dokaza [2].

U istrazi fizičkog mesta krivičnog dela, najpoznatija teorija je Lakardov zakon razmene materije: „Kada dva objekta dođu u kontakt, doći će do razmene materije između njih“. Na primer, dlake i vlakna sa tela zločinca se često zadrže na mestu krivičnog dela i slično se dešava i sa digitalnim mestom krivičnog dela. Privremeni fajlovi, sadržaj ram memorije koji je snimljen na čvrstom disku (swap fajl), izbrisani delovi fajlova mogu ostati u računarskom sistemu, tzv. fajl slack prostoru i nealociranom prostoru klastera na čvrstom disku. I to zahvaljujući raznim aplikacijama, pomoćnim alatima, operativnim sistemima koje je koristio napadač [2].

Forenzička istraga digitalnog mesta krivičnog dela se integriše sa istragom fizičkog mesta krivičnog dela, tako da se mogu sakupiti svi relevantni fizički i digitalni dokazi o aktivnostima napadača. U ovom modelu istrage kompjuterskog kriminala, digitalno mesto krivičnog dela može se smatrati sekundarnim mestom krivičnog dela, u odnosu na primarno fizičko mesto krivičnog dela koje čine sto i prostorija u kojoj se nalazi ispitivani računar [2].

Osnovni termini kada je u pitanju ova oblast su [2]:

- fizički dokaz,
- digitalni dokaz,
- fizičko mesto krivičnog dela,
- digitalno mesto krivičnog dela,
- revizija i analiza.

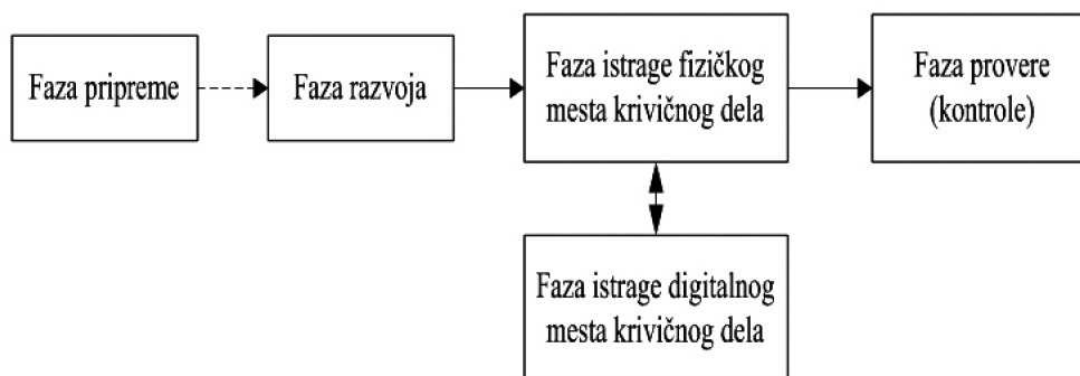
Fizički dokazi su objekti koji mogu potvrditi da se to krivično delo zaista i dogodilo ili ga povezuju sa zločincem. **Digitalni dokaz** predstavlja digitalni podatak koji potvrđuje da se zločin dogodio i koji može da dovede u vezu zločin i počinioca. **Fizičko mesto krivičnog dela** je okruženje gde postoje fizički dokazi o krivičnom delu. Okruženje gde se dogodi prvo krivično delo je primarno fizičko mesto krivičnog dela (npr. prostorija sa računarom iz koje je izvršen napad), a prostorija sa posrednim računarom preko kog je izvršen napad naziva se sekundarno fizičko

mesto krivičnog dela. **Digitalno mesto krivičnog dela** je virtuelno okruženje koje se sastoji od hardvera i softvera gde postoje potencijalni digitalni dokazi krivičnog dela kompjuterskog kriminala ili kompjuterskog incidenta. Postoje takođe primarno i sekundarno mesto krivičnog dela. **Revizija i analiza** označavaju da se neki objekat računarskog sistema ili računarske mreže, može procesirati na različite forenzičke načine, kako bi se iz njega prikupili, analizirali i kontrolisali podaci koji su relevantni za izgradnju čvrstih i neoborivih digitalnih dokaza [2].

6.1. Faze modela integrisanih procesa digitalne forenzičke analize

Ovaj model je primenljiv i na korporacijsku i na zvaničnu istragu, i ovaj model ima 17 faza koje su oraganizovane u pet grupa [2]:

1. faza pripreme,
2. faza razvoja,
3. faza istrage fizičkog mesta krivičnog dela,
4. faza istrage digitalnog mesta krivičnog dela,
5. faza provere (kontrole).



Slika 15 - Faze modela integrisanih procesa digitalne forenzičke analize [2]

6.1.1. Faza pripreme

Digitalni dokazi moraju da se sakupljaju skladište i čuvaju na forenzički ispravan način ili mogu biti izgubljeni. Ova faza ima zadatak da obezbedi potpunu operativnu i infrastrukturnu pripremu i podršku istrazi. Ona traje u kontinuitetu i nije vezana ni za jedno konkretno krivično delo. Operativna priprema obezbeđuje obuku za lica koja će biti uključena u incident. Infrastrukturna priprema obezbeđuje izvore iz kojih se generišu potrebni digitalni i drugi podaci da bi se izvršila potpuna i detaljna istraga koju je nemoguće izvršiti ukoliko ne postoje podaci. Primer ove faze su instalacije i raspoređivanje video nadzora i čitača kartica da bi se vremenski snimio pristup fizičkom prostoru [2].

6.1.2. Faza razvoja

Cilj ove faze je da obezbedi mehanizam za detekciju i za potvrdu incidenta. Zadaci u ovoj fazi se dosta razlikuju za korporacijsku i za javnu istragu [2].

Faza detekcije i izvršavanja

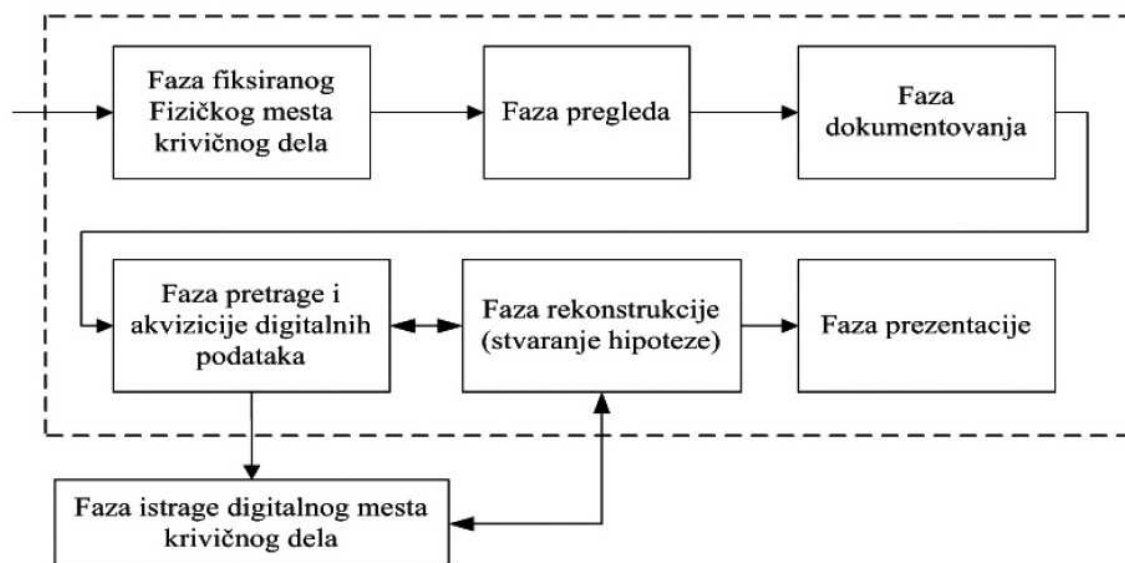
Ova faza detektuje incident i izveštava odgovorna lica. Može da se obavi pozivom 192 i ona definiše početak istrage [2].

Faza potvrde i autorizacije

Sada se istraga nastavlja u različitim smerovima. Ako je u pitanju javna istraga, traži se nalog za pretres ili neko drugo legalno odobrenje koje mora da bude potkrepljeno sa dovoljno inicijalnih dokaza. A kod korporacijske istrage nalozi za pretres nisu potrebni dok god se ne krše prava privatnosti [2].

6.1.3. Faza istrage fizičkog mesta krivičnog dela

Ova faza ima zadatak da prikupi i analizira fizičke dokaze i rekonstruiše akcije koje su dovele do incidenta. Najvažniji cilj istrage je da se identifikuju ljudi koji se doveli do ovog incidenta i za to su potrebni fizički dokazi. Ovaj deo istrage vrši istražitelj ekspert za istragu fizičkog mesta i interventni tim za reagovanje na kompiuterski incident ili tim za fizičko obezbeđivanje. Faze za istragu fizičkog mesta su prikazane na slici 16 [2].



Slika 16 - Faze i interakcija istrage fizičkog i digitalnog mesta krivičnog dela [2]

Faza obezbeđivanja (fiksiranja) fizičkog mesta krivičnog dela. Ona je ista za svaki tip krivičnog dela i aktivnosti koje se preduzimaju. I ona sadrži [2]:

- osiguranje izlaza,
- pomoć ranjenima,
- zadržavanje osumnjičenih,
- identifikovanje svedoka.

Faza revizije fizičkog mesta krivičnog dela. Organ istrage opservira fizičko mesto krivičnog dela i obično je prva osoba koja reaguje na incident. Cilj je da se identifikuje dokazni materijal i da se na osnovu toga razvije početna teorija [2].

Faza dokumentovanja fizičkog mesta krivičnog dela. Istražitelj treba da pravi fotografije, skice i video snimke mesta krivičnog dela i dokaza i da detaljno dokumentuje svaku aktivnost u procesu pretrage. Cilj je da se prikupi što više informacija i da se sačuvaju i zabeleže [2].

Faze pretrage i sakupljanja dokaza sa fizičkog mesta krivičnog dela. Ova faza obuhvata pretragu i detaljno prikupljanje dodatnih fizičkih dokaza iz dubine fizičkog mesta krivičnog dela. Pretraga može biti usmerena prema nestalim delovima fizičkih dokaza kao što je npr. oružje. Prikupljeni dokazi se šalju u forenzičku laboratoriju radi analize, a rezultati se koriste u sledećoj fazi rekonstrukcije incidenta. U ovoj fazi

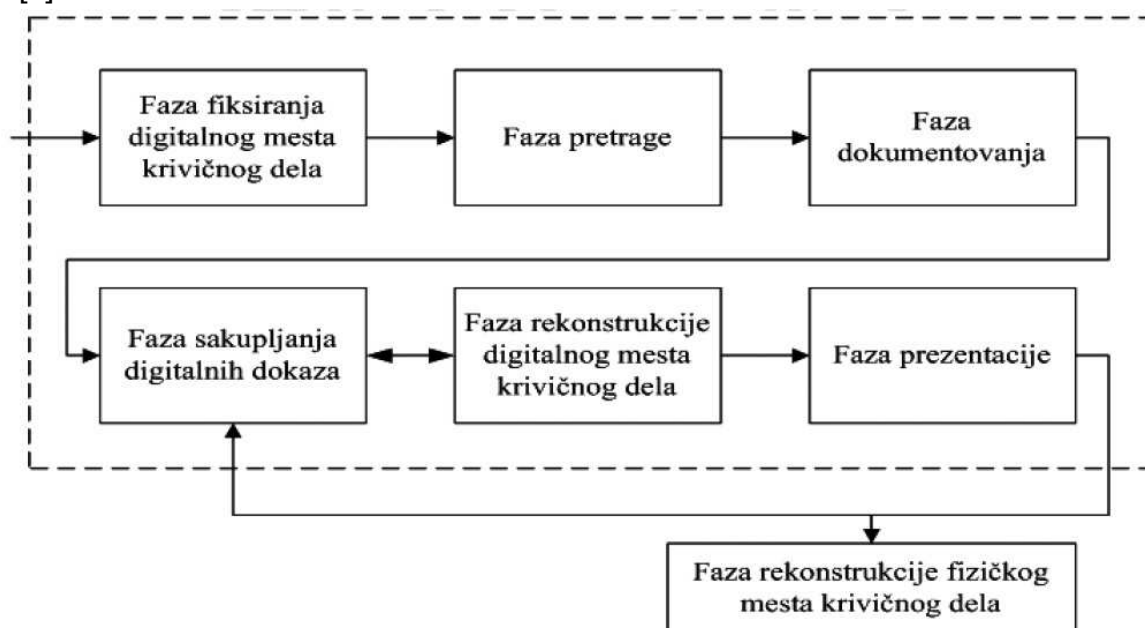
počinje forenzička istraga digitalnog mesta krivičnog dela. Računarski sistem se smatra fizičkim dokazom pa se i on oduzima kad god je to moguće [2].

Faza rekonstrukcije fizičkog mesta krivičnog dela. Ovde spada organizovanje rezultata analize prikupljenih fizičkih i digitalnih dokaza i korišćenje fotografija sa fizičkog mesta krivičnog dela da bi se razvila hipoteza o incidentu. Kod digitalnog incidenta, rezultati istrage digitalnog mesta krivičnog dela povezuju se sa fizičkim dokazima, da bi se povezala osoba sa digitalnim događajem [2].

Faza ekspertskog svedočenja/veštačenja fizičkog mesta krivičnog dela. U ovoj fazi forenzičar svedoči kao ekspert ili veštači fizičke i digitalne dokaze sudu ili upravi korporacije. On prezentuje dokaze i hipotezu koja je razvijena u fazi rekonstrukcije [2].

6.1.4. Faza istrage digitalnog mesta krivičnog dela

Ova faza počinje kada su fizički digitalni uređaji i drugi dokazni materijali prikupljeni kao fizički dokazi ili kada je sačuvan analizirani mrežni saobraćaj radi obezbeđivanja dokaza. Cilj ove faze je da se identifikuju digitalni podaci o događajima na sistemu i prezentuju istražnom organu. Ovde se svaki digitalni uređaj smatra posebnim fizičkim mestom krivičnog dela. Svi prikupljeni dokazi se šalju u fazu rekonstrukcije u kojoj će biti identifikovane veze između digitalnih uređaja. Digitalni forenzičar istražuje digitalno mesto krivičnog dela kroz sledeće faze koje su prikazane na slici 17 [2]:



Slika 17 - Faze forenzičke istrage digitalnog mesta krivičnog dela [2]

Faza fiksiranja digitalnog mesta krivičnog dela. Ova faza obezbeđuje ulaz ili izlaz ka ili od digitalnog mesta krivičnog dela i zaštitu integriteta digitalnih dokaza koji se lako mogu izmeniti. Ovo predstavlja izolaciju računarskog sistema od računarske mreže, sakupljanje nestabilnih i lako promenljivih podataka koji bi mogli biti izgubljeni kada se sistem isključi i identifikovanje bilo kakvih sumnjivih procesa koji su aktivni u sistemu. Treba registrovati i po mogućstvu ispitati sumnjive korisnike koji su ulogovani na sistem. Log fajlovi se mogu smatrati za očevidce digitalnog krivičnog dela i moraju biti obezbeđeni ukoliko postoji pretnja da mogu biti izbrisani pre nego što se sistem fizički iskopira [2].

Faza pretrage digitalnog mesta krivičnog dela. Ova faza se obavlja u forenzičkoj laboratoriji, na jednoj od forenzičkih replika (imidža) digitalnog mesta krivičnog dela. Ukoliko nije moguće privremeno oduzeti kompromitovani sistem, ova faza može da se izvrši i uživo u fizičkom okruženju sa tehnikama i alatima aktivne akvizice računara u radu, iako je poželjno laboratorijsko okruženje, zato što pruža kontrolisane uslove, a rezultati se mogu ponoviti sa drugom, referentnom replikom sistema, ako to zahtevaju sudski organi [2].

Faza dokumentovanja digitalnog mesta krivičnog dela. Ovde je potrebno pravilno dokumentovati digitalne dokaze koji su otkriveni u fazi akvizicije. Fizičke kopije sistema imaju istu ulogu kao i skice i video zapisi fizičkog mesta krivičnog dela. Svaki deo digitalnog dokaza koji se pronađe u toku forenzičke analize imidža sistema mora biti jasno dokumentovan. U ovoj fazi se dokumentuju pojedinačni delovi dokaza, ali se ne kreira finalni izveštaj o incidentu. Taj izveštaj se pravi u fazi prezentacije. Ova faza nije strogo odvojena, zato što se dokazi dokumentuju od trenutka otkrivanja i akvizicije do pripreme dokaza za prezentaciju (svedočenje/veštačenje) pred sudom [2].

Faza sakupljanja digitalnih dokaza sa digitalnog mesta krivičnog dela. Sastoji se od potpune digitalne forenzičke akvizicije relevantnih podataka iz računarskog sistema, radi izvlačenja digitalnih dokaza. Ova faza koristi rezultate iz faze pretrage da bi se usredsredila na dodatne indikatore koji upućuju na digitalne dokaze i odgovarajuće tipove analize. Najveći deo istrage se potroši u ovoj fazi [2].

Faza rekonstrukcije digitalnog mesta krivičnog dela. Ona se sastoji iz sastavljanja neoborivog, čvrstog digitalnog dokaza bez tzv. pukotina. Digitalni dokazi se mogu razvrstati na osnovu toga koliko su uverljivi i pouzdani. Podaci mogu da zahtevaju složene tehnike analize, kao što su analize izvršnih fajlova i dešifrovanje, a njihovi rezultati se koriste za izgradnju čvrstog dokaza [2].

Faza prezentacije digitalnog mesta krivičnog dela. Ona predstavlja prezentovanje otkrivenih digitalnih dokaza timu za istragu fizičkog mesta krivičnog dela i pripremu za ekspertska svedočenje ili veštačenje pred sudom [2].

6.1.5. Faza provere (kontrole)

Ovo je finalna faza koja se sastoji od revizije i kontrole integralnog procesa istrage, da bi se identifikovale oblasti koje se mogu poboljšati. Za digitalni kompiuterski incident, ovo obuhvata analizu kvaliteta rada organa istrage, i koliko dobro su izvršene fizička i digitalna istraga svaka za sebe, koliko dobro su urađene zajedno i da li postoji dovoljno fizičkih i digitalnih dokaza da bi se slučaj rešio [2].

7. Forenzički alati

Prvi forenzički alati su pomagali u ispitivanju privremeno oduzetih računara, i to na nivou heksadecimalnog zapisa. Tek 1990-e godine pojavljuju se specijalizovani forenzički alati [2].

Za opremanje digitalne forenzičke laboratorije za terenske i stacionarne uslove rada treba odrediti koji su alati najfleksibilniji, najpouzdaniji i najrentabilniji u obavljanju poslova forenzičke akvizicije i analize digitalnih dokaza. Održavanje ove laboratorije uključuje i formiranje softverke biblioteke – repozitorijuma, koja sadrži i sve starije verzije forenzičkih alata [2].

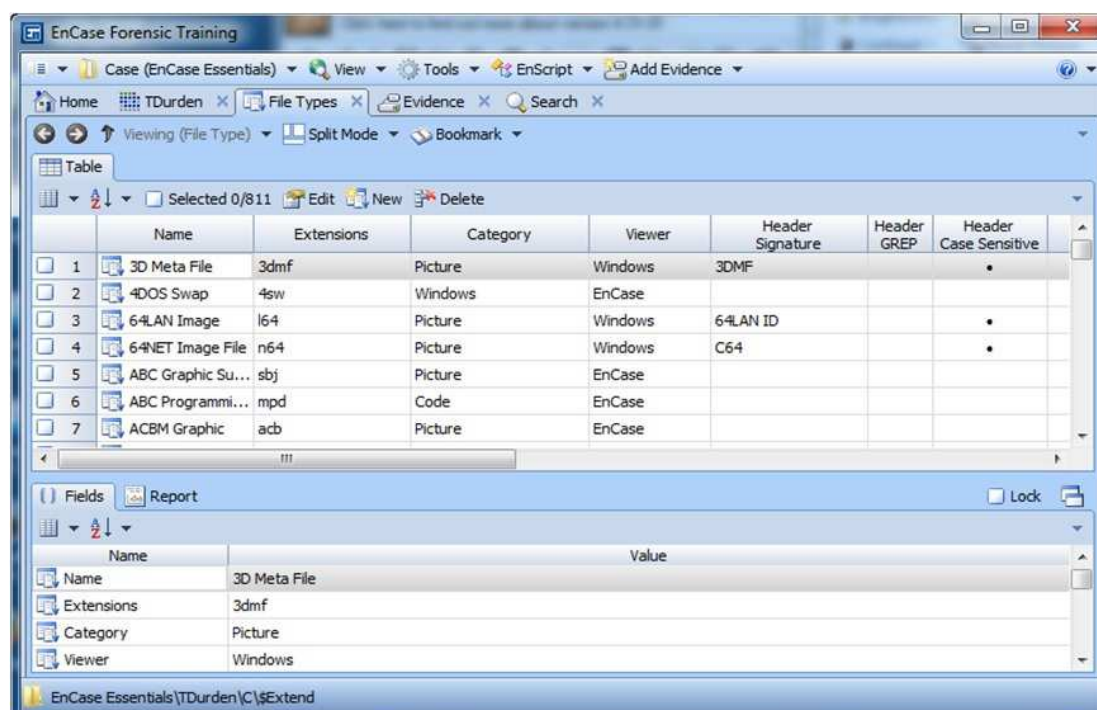
7.1. Tehnike i alati za akviziciju digitalnih podataka

Prvi zadatak u forenzičkoj istrazi računara je akvizicija digitalnih podataka i podrazumeva pravljenje fizičke kopije bit-po-bit originalnog (osumnjičenog/ ispitivanog) diska računara. Ova procedura sprečava korupciju i oštećenje digitalnih podataka na originalnom disku. Ovi alati za akviziciju vrše sledeće funkcije [2]:

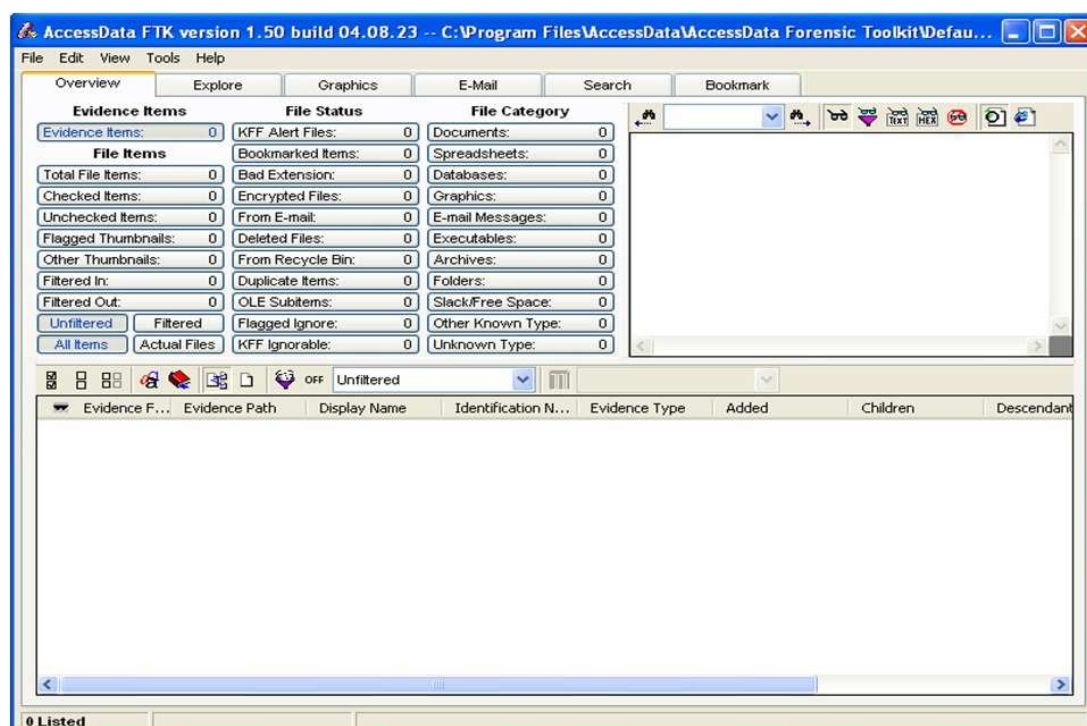
- kopiranje podataka sa fizičkog diska,
- kopiranje podataka sa logičkog diska/ particija,
- formatiranje akvizicijskih podataka,
- akvizicija komandnom linijom,
- akvizicija sa GUI alatima,
- udaljena akvizicija i
- verifikacija.

Za akviziciju podataka bit-po-bit sa originalnog na forenzički disk postoje hardverski i softverski alati. Primeri hardverskog alata za uzimanje fizičke slike računara su [2]:

- Image Masster Solo 2 Forensic (može samostalno da kopira podatke sa originalnog na forenzički disk),
- EnCase (slika 18)
- FTK (slika 19)



Slika18 - EnCase alat [6]



Slika 19 - FTK alat [6]

Postoje dve metode kopiranja u procesu akvizicije, i većina programa ima obe metode [2]:

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

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, to je jednostavna kopija bit-po-bit fajla podataka, particije diska ili celog diska. Može kopirati podatke sa jednog diska na drugi ili u jedan ili više segmentiranih fajlova podataka. Forenzičar može gledati sadržaj sirovih podataka imidža fajla sa heksadecimalnim editorom kao što su HexWorkshop ili WinHex [2].

Neki forenzički alati mogu izvršiti akviziciju podataka sa aktivnog računarskog sistema (u radu), udaljenim pristupom preko računarske mreže i transportovati ih u forenzički server zaštićenim kanalom [2].

Svi savremeni forenzički alati obezbeđuju metod za verifikaciju tačnosti procesa kopiranja podataka sa originalnog na forenzički disk [2].

7.2. Ekstrakcija digitalnih podataka

Ekstrakcija sa forenzičkim alatima ima zadatak oporavka podataka u forenzičkoj istrazi i zahtevniji je za upravljanje od svih ostalih funkcija alata. Ovaj proces obuhvata više koraka [2]:

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

Većina forenzičkih alata obezbeđuje funkciju **posmatranje podataka**, a od alata zavisi u kom se formatu vide. Npr. forenzički alat Drive Spy obezbeđuje gledanje logičke particije osumnjičenog diska i heksadecimalnog zapisa podataka u klasterima i sektorima diska. Alati kao što su FTK, EnCase, Smart iLook omogućuju nekoliko različitih načina pregleda. **Pretraživanje po ključnoj reči** je uobičajan zadatak ispitivanja računara i na ovaj način se oporavljaju ključni podaci. Ključne reči određuje forenzičar na bazi raspoloživih dokaza dobijenih u fazi predistražnog

postupka. FTK može dekompresovati arhivirane fajlove kao što je ZIP. **Rekonstrukcija podataka iz fragmenata izbrisanog fajla**, odnosno ekstrakcija podataka iz nealociranih prostora diska, postala je jako bitan zadatak. **Dešifrovanje šifrovanih fajlova podataka** je glavni izazov za forenzičara pored analize i oporavka podataka. Šifrovan može da bude ceo disk, samo particija ili samo neki fajl. Posle lociranja podataka vrši se **označavanje digitalnih dokaza** [2].

7.3. Rekonstrukcija osumnjičenog diska

Ova funkcija treba da regeneriše odnosno da rekonstruiše osumnjičeni disk, što se radi sa fizičkog duplikata osumnjičenog hard diska. Prvi razlog za rekonstrukciju događaja je da po zahtevu suda forenzičar može podići osumnjičeni računar i pokazati šta se dogodilo u toku krivičnog dela. Drugi razlog za dupliranje osumnjičenog diska je da se napravi identična kopija za potrebe drugih forenzičara odbrane, veštačenja. Ukoliko je imidž kopija uzeta sa prihvatljivim i pouzdanim forenzičkim alatom i prema propisanoj proceduri, ona se smatra originalom osumnjičenog diska [2].

7.4. Softverski forenzički alati

Softverski forenzički alati se grupišu u dve kategorije. A to su:

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

Aplikacije komandne linije su namenjene za izvršavanje samo jednog zadatka, kao što je SaveBack, alat na bazi DOS komandne linije. Za razliku od njih, **GUI aplikacije** su namenjene za obavljanje više forenzičkih funkcija, oni mogu obaviti većinu zadataka akvizicije. U ovu vrstu alata spadaju FTK i EnCase. Najbitnija funkcija ovih alata je ta što mogu u potpunosti da iskopiraju osumnjičeni disk [2].

7.5. Hardverski forenzički alati

Kako se brzo menjaju informaciono komunikacione tehnologije sistema, tako se zahteva i izbor novih forenzičkih alata za novi hardver. Kako se forenzički hardverski alati, radne stanice i serveri koriste intenzivno, zamenu treba planirati najmanje na dve godine. Snabdevači računarskih sistema nude širok asortiman forenzičkih

radnih stanica, koje korisnik treba da prilagodi svojim potrebama. Forenzičke radne stanice se mogu podeliti u tri kategorije [2]:

- **stacionarna radna stanica** (računarski sistem sa nekoliko kućišta za eksterne hard diskove i mnogo perifernih uređaja visokih performansi),
- **portabl radna stanica** (laptop računar sa ugrađenim LCD monitorom i skoro istim brojem kućišta i perifernih uređaja kao i stacionarna radna stanica),
- **prenosna radna stanica** (obično laptop ugrađen u transportnu torbu sa manjim brojem perifernih uređaja).

Digitalna forenzička laboratorija treba da ima što više različitih forenzičkih alata, softvera i hardvera da bi izvršila sve potencijalne zadatke istrage. Ako je moguće treba imati po nekoliko konfiguracija za istovremeni rad na različitim slučajevima. Problemi mogu nastati u podršci perifernim uređajima koji mogu doći u konflikt ili da ne rade. Forenzičar mora da zna koliko perifernih uređaja može da se poveže na sistem da bi on nesmetano radio. Prilikom odabira radne stanice treba birati onu koja može da omogući najveći broj proširenja. Treba uzeti što je moguće više memorije i što potpuniju kolekciju različitih veličina hard diskova. Primer kompletnog računarskog sistema je FRED ili DIBS Advance Forensic [2].

Digitalni dokazi se razlikuju od fizičkih i od drugih tipova dokaza po tome što se mogu kopirati do najsitnijih detalja - bitova. Forenzičar može napraviti tačnu fizičku kopiju čvrstog diska. Akvizicija digitalnih dokaza sa hardverskom tehnologijom uključuje [2]:

- blokatore upisivanja,
- razne adaptore,
- CD/DVD diskove za akviziciju,
- SCSI diskove i optičke kanale.

7.5.1. Blokatori upisivanja

To su hardversko- softverski uređaji za sprečavanje upisivanja podataka na ispitivani disk. Neki od primera se mogu videti na slici 20. Oni su obavezni u digitalnoj forenzici, jer sprečavaju forenzičare da slučajno upisuju podatke na ispitivani disk koji sadrži digitalne dokaze. Postoje i softverski i hardverski blokatori. Korišćenjem hardverskih blokatora upisivanja mogu se skinuti digitalni podaci sa brojnih tipova čvrstih diskova, a neki od njih su [2]:

- IDE čvrsti diskovi od 3,5 inča,
- SATA čvrsti diskovi,
- notebook čvrsti diskovi,
- toshiba čvrsti diskovi i dr.



Slika 20 - Hardverski blokatori [2]

7.5.2. Hard diskovi

Hard diskovi se koriste za čuvanje programa koje korisnik upotrebljava tokom rada na računaru, kao i za smeštaj podataka nastalih korišćenjem pomenutih programa. Pored ove dve namene hard disk se koristi i kao privremena memorija, kada mu za potrebe nekog posla zafali RAM memorija [3].

Hard diskovi koji su u upotrebi su IDE i SATA diskovi i mogu se videti na slici 21. IDE diskovi koriste trakasti kabal, a SATA diskovi koriste fleksibilne kablove slične telefonskom kablju [2].



Slika 21 - Primeri IDE i SATA diskova [2]

7.5.2.1. Konstrukcija hard diskova

Na slici 22 se može videti hard disk sa njegovim elementima:



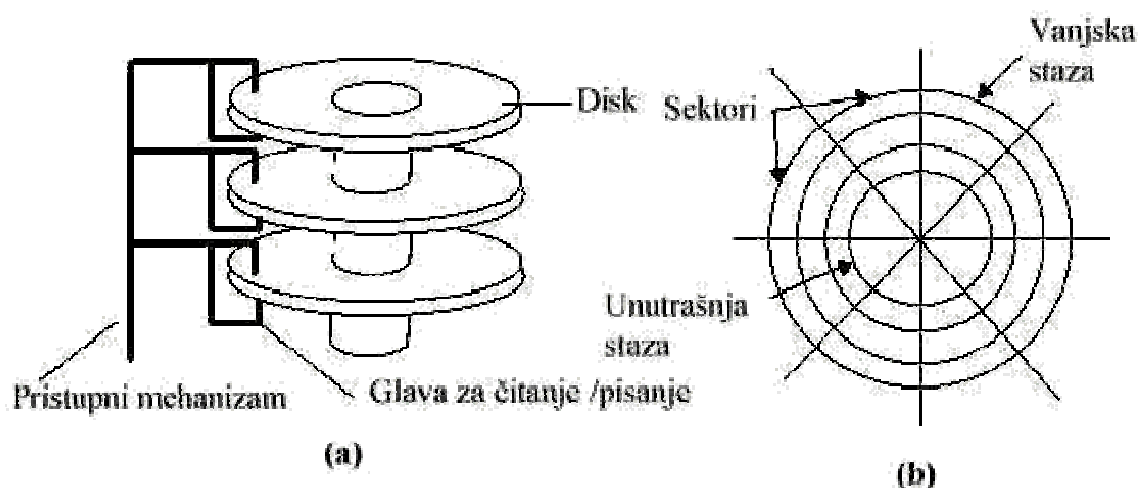
Slika 22 - Konstrukcija hard diska [24]

Glavni element hard diska su jedna ili više okruglih ploča od nemagnetnog materijala, koje su vezane zajedničkom osovinom. Ploče su sa obe svoje strane prevučene tankim slojem magnetnog materijala, na koji se upisuju podaci, i sa kojeg se kasnije očitavaju. Iznad obe strane svake ploče nalaze se glave za čitanje i upisivanje podataka. Glave su smeštene na specijalnim ručicama, koje se nalaze na zajedničkoj osovinu, tako da se istovremeno pokreću i menjaju svoj položaj od ivice ploča pa skoro do njihovog centra [3].

Svi elementi hard diska su hermetički zatvoreni u kućište kako bi se sprečila oštećenja osetljivih elemenata usled nečistoće prašine iz vazduha. Pomeranjem ručica sa glavama upravlja kontroler koji se nalazi na štampanoj ploči smeštenoj na donjoj strani kućišta hard diska. Kontroler ima i konektor preko koga se priključuje na računar. Takođe postoji i konektor za priključenje napona za napajanje. Uloga kontrolera je da obezbedi stabilnu brzinu obrtaja ploča sa magnetnim materijalom i da u zavisnosti od zahteva koji dobije od matične ploče obezbedi pomeranje ručica sa glavama za čitanje i pisanje na tačno određeno mesto [3].

7.5.2.2. Smeštanje podataka na pločama hard diska

Da bi se površina racionalno iskoristila, uvedena je posebna organizacija upisa koja je prikazana na slici 23.



Slika 23 - Upisivanje na hard disk [24]

Osnovni elementi su **staze**. One su raspoređene kao koncentrični krugovi na obe površine svih ploča, počevši od spoljne ivice prema unutrašnjosti ploče. Zavisno od vrste diska svaka staza može da sadrži veliki broj bitova. Zbog toga je staza podeljena u određeni broj **sektora** koji sadrži 512 bajtova podataka. Sledeći parametar hard diskova su **cilindri**. Cilindar čine staze na svim pločama koje se nalaze na istom poluprečniku. Sa ovom organizacijom se postiže racionalno iskorišćenje površine za smeštaj podataka i obezbeđuje se najbrži rad hard diskova [3].

Najmanja veličina prostora je sektor. Ako su podaci veći od jednog sektora, onda se prelazi u sledeći sektor u istoj stazi. Kad se popuni cela staza, prelazi se na stazu sa istim brojem, koja se nalazi na suprotnoj strani iste ploče. Nakon toga se popunjava

istoimena staza na susednoj ploči, tj. u okviru jednog istog cilindra. Tek kad se popuni ceo cilindar, ručice se pomeraju na sledeći. I tako je ostvareno minimalno mehaničko pomeranje ručica sa glavama, tako da se sa najmanjim pomeranjem ručica postiže najveća brzina upisivanja i očitavanja podataka [3].

Kod savremenih diskova broj sektora po stazama nije stalan, već se disk deli na veći broj **zona**. Broj sektora u stazama u jednoj zoni je stalan, ali u različitim zonama ima i različit broj sektora po stazama. Pošto su dužine staza koje se nalaze bliže spoljašnjoj ivici veće od dužina staza koje se nalaze bliže centru ploče, onda se u spoljašnjim stazama može smestiti više sektora, a to znači i veća količina podataka [3].

8. Studija slučaja (Case study)

8.1. Scenario istrage kompjuterskog kriminala u organizaciji „XY“

Organizacija „XY“ je firma koja se bavi proizvodnjom, prodajom, implementacijom energetskih postrojenja za elektrodistribuciju. Odnosno, prodaje i implementira visokotehnološke sklopke za ova postrojenja. Jedna od sklopki se može videti na slici br 24.



Slika 24 - Visokotehnološka sklopka [25]

Ova firma je najpoznatija u Srbiji u ovoj oblasti, a njoj konkurentska firma se nalazi i Republici Srpskoj. Njen pravi naziv se ne navodi jer želi da ostane anonimna.

Svaka firma poseduje informacije od značaja koje se ne iznose u javnost. Tako i firma „XY“ čuva određene informacije kojima ima prisup samo određeni broj zaposlenih u toj firmi. Ove informacije se čuvaju na posebnom računaru sa šifrom i koji nije povezan sa Internetom, kako bi se omogućila što veća bezbednost ovim informacijama. Na računaru se nalaze svi projekti i informacije koje se čuvaju od javnosti, odnosno od konkurentskih firmi.

Jedan od zaposlenih koji je bio jako dugo jedan od najboljih radnika, ima pravo pristupa. On se oženio, dobio dete i odlučio da traži povišicu jer je smatrao da svojim dugogodišnjim i napornim radom to i zaslužuje. Otišao je kod direktora na razgovor, međutim nije naišao na podršku koju je očekivao. Direktor nije želeo da mu da povišicu. To je njega jako razočaralo i kvalitet njegovog rada je počeo da se smanjuje velikom brzinom. On je taj postupak ponovio nekoliko puta, međutim odgovor je uvek bio isti. Vremenom je gubio motivaciju, kao i želju za radom i dokazivanjem i to se ispoljilo na njegovim rezultatima. Odjednom se potpuno promenio. Ponovo je počeo vredno da radi i rezultati su odjednom poboljšani i kupio je nova kola, iako nije dobio povišicu koju je tražio i više je nije ni spominjao.

Menadžeru je to postalo jako sumnjivo i porazgovarao je s njim. Zaposleni je odgovorio da ne radi nigde sem u toj firmi. Menadžer mu nije poverovao i odmah je sklonio računar u sef, na kom se čuvaju projekti, i krenuo da traži stručnjaka za digitalnu forenziku koji će mu rešiti neke sumnje.

Digitalni forenzičar je nakon dugog ispitivanja došao do zaključka da je neko od zaposlenih ukrao folder sa projektom sklopke, u kom su se nalazile sve informacije i nacrti tog projekta. Taj projekat je jedan od najbitnijih u organizaciji i zato te informacije spadaju u najpoveljivije. Nakon što je zaposleni iskopirao folder, on ga je i obrisao sa računara.

Forenzičar je uspeo da povрати taj folder, međutim, sad se javio još jedan veliki problem. Da li je to uradila osoba na koju menadžer sumnja? Šta je uradio sa podacima?

Nakon toga, menadžer se obratio istražnim organima, preneo im je sve poznate informacije i oni su sprovedi javnu istragu. Došli su do zaključka da je upravo zaposleni na kog je menadžer sumnjao to i uradio, i da je prodao te informacije konkurentskoj firmi koja se nalazi u Republici Srpskoj i tako firmi „XY“ naneo veliku štetu i gubitke.

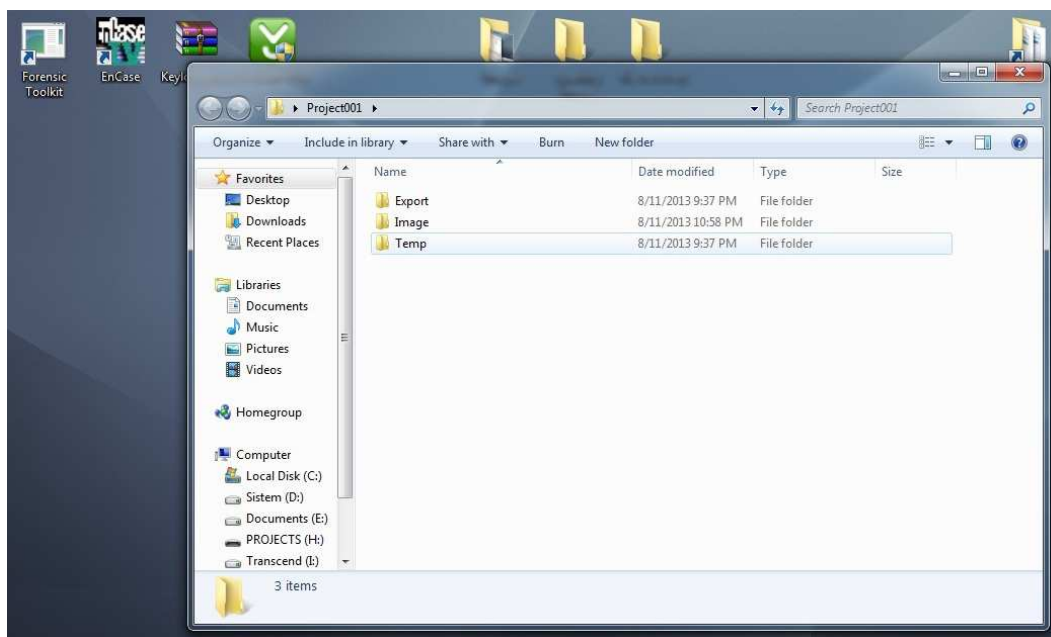
8.2. Korporacijska istraga

8.2.1. Uzimanje imidza

Nakon dolaska u organizaciju menadžer je forenzičaru predao računar na kom su se nalazili podaci sa svim projektima.

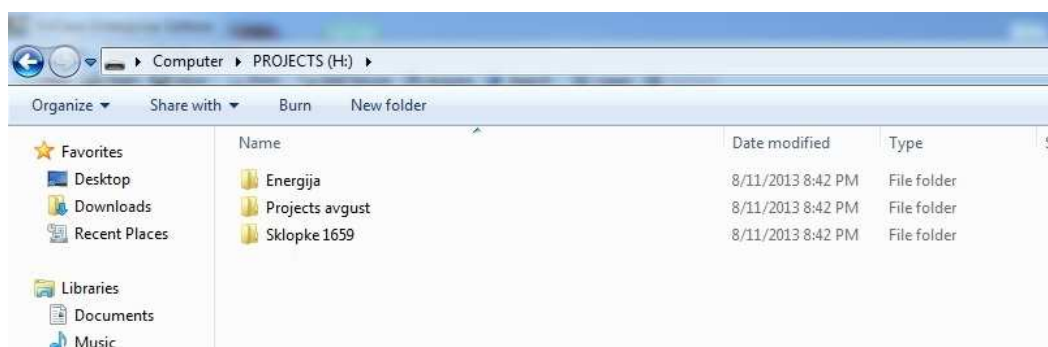
Na samom startu lokal disk se poveže sa blokatorom i na taj način je osigurano da digitalni forenzičar ne može ništa da izmeni, i samo tako su dokazi validni na sudu. Zatim se pokrene aplikacija koja se naziva EnCase i sa njom se uzima imidž tog računara.

Pre samog početka treba da se napravi folder u kom će se čuvati svi fajlovi koji se prave tokom rada. U tom folderu treba da budu tri nova foldera a to su: export, image i temp kao na slici 25.



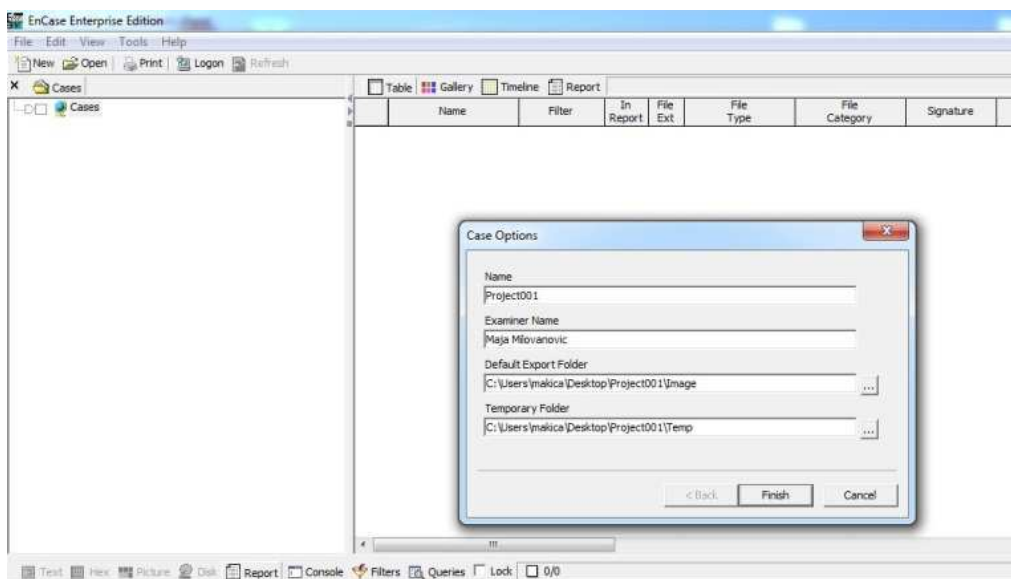
Slika 25

U folderu temp će se čuvati privremeni fajlovi, koje EnCase pravi tokom uzimanja imidža. U folderu image se čuva imidž tog diska i u export svi ostali fajlovi. Na sledećoj slici, broj 26, se može videti lokalni disk u kom se nalaze svi projekti ove organizacije.



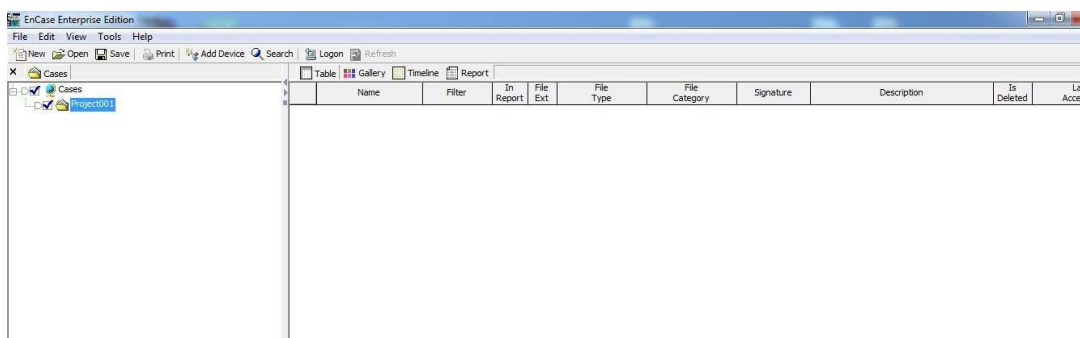
Slika 26

Nakon toga se pokreće program i treba da napravi novi slučaj kao na slici 27.



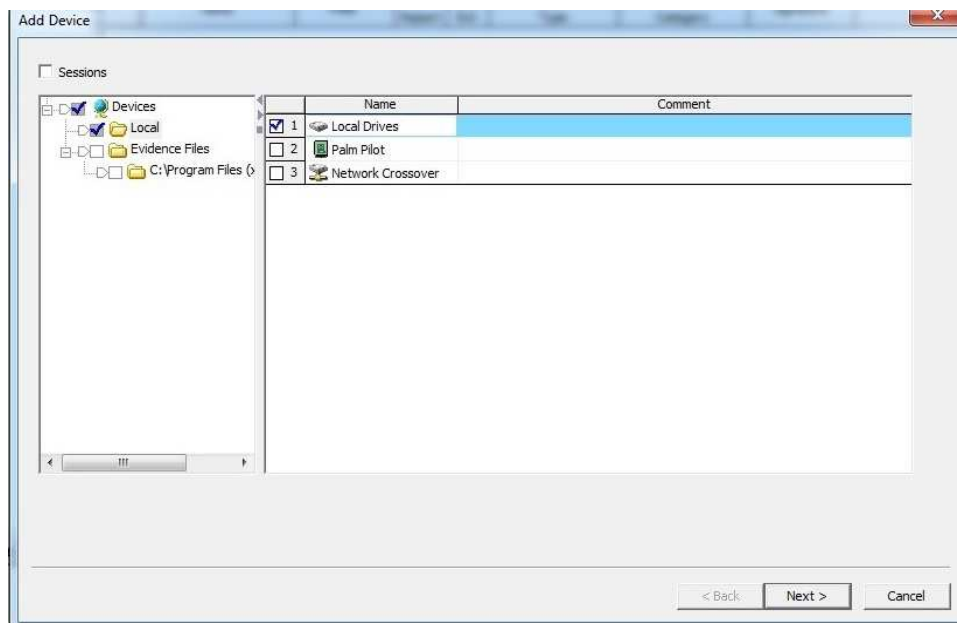
Slika 27

Prvo se unosi naziv projekta i ime forenzičara. Zatim putanja do export i temp foldera koji su prethodno napravljeni. Tako kreiran slučaj se vidi na sledećoj slici broj 28, u levom delu prozora.

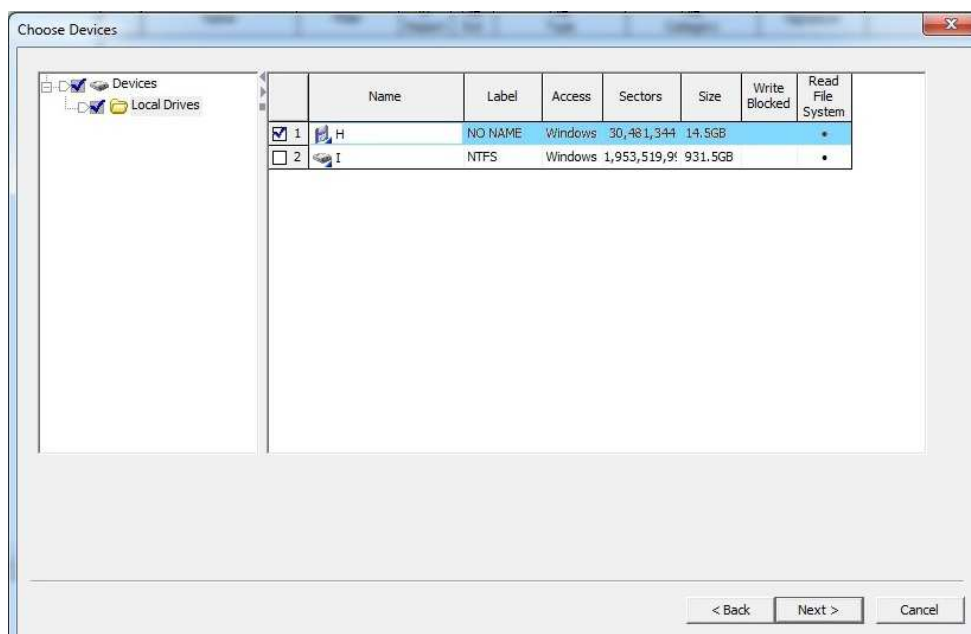


Slika 28

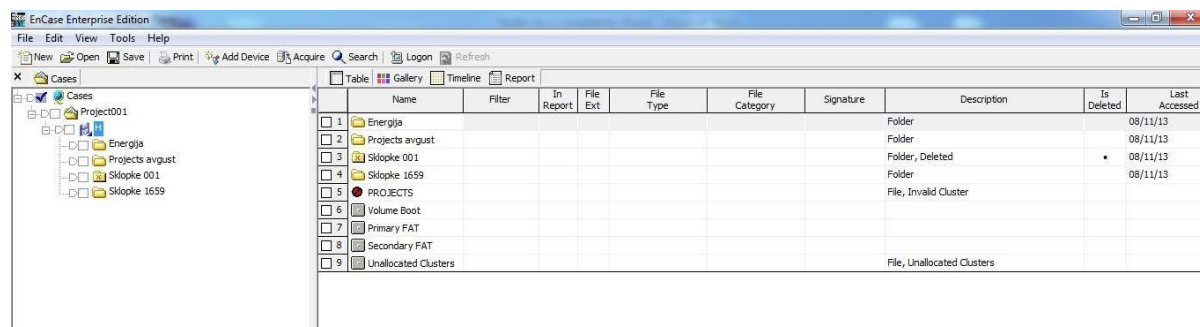
Zatim se dodaje uređaj, čiji se imidž kreira, tako što se odabere “add device” i pojavi se prozor kao na slici 29, gde se bira lokalni disk i nakon toga, kao na slici 30, se bira lokalni disk koji se analizira. U ovom slučaju je odabran H local disk. Onda se pojave svi fajlovi i folderi koji se nalaze u njemu, kao na slici 31.



Slika 29

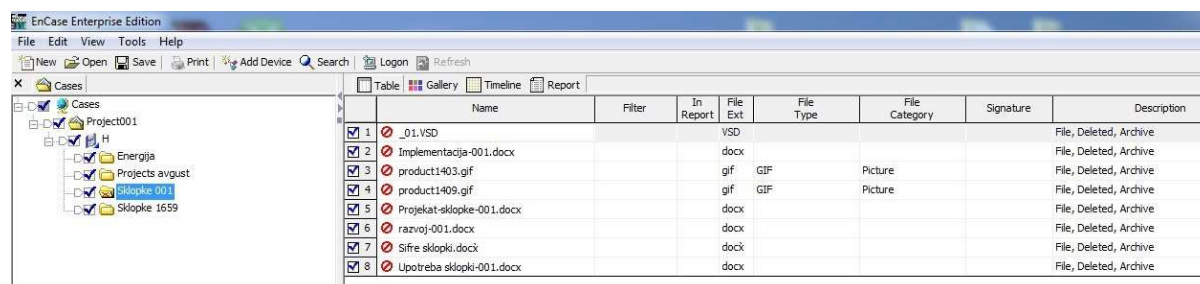


Slika 30

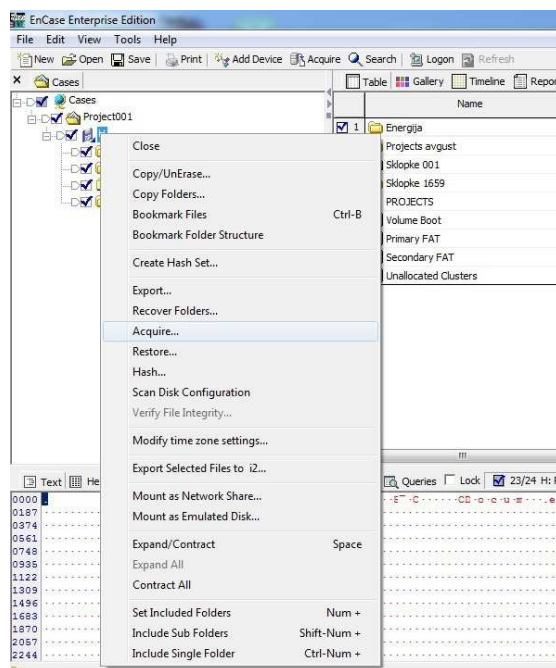


Slika 31

Sa leve strane prozora na slici 32 se vide folderi, a sa desne svi fajlovi koji se nalaze u njima. Na levoj strani se vidi jedan precrtani folder i naziva se “sklopke 001” To je znak da je taj folder obrisan kao i fajlovi koji se nalaze u njemu i koji se vide sa desne strane.

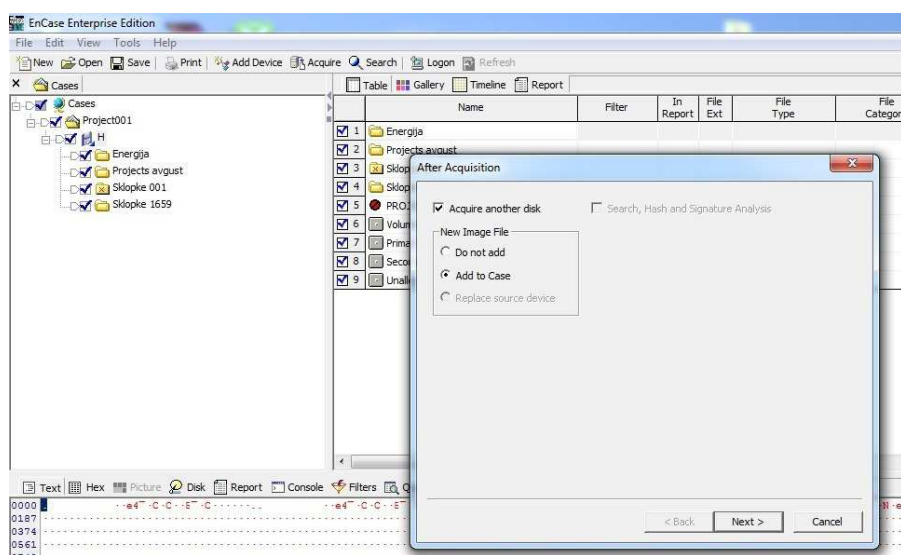


Slika 32

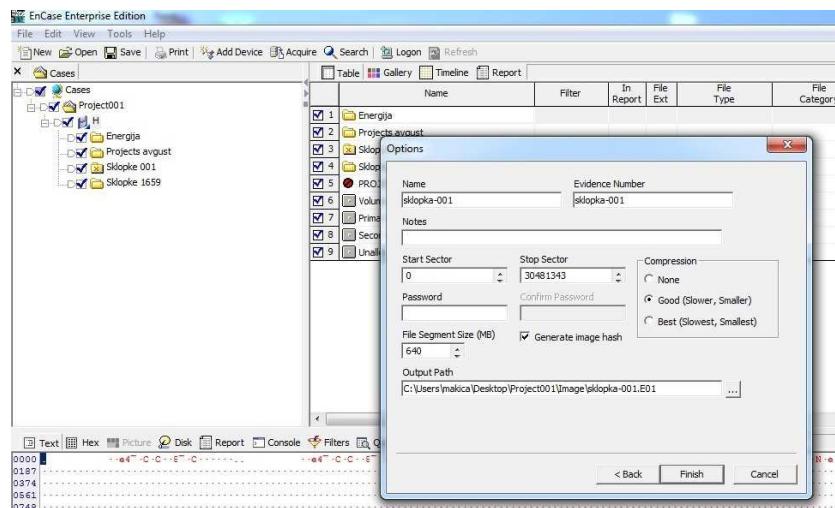


Slika 33

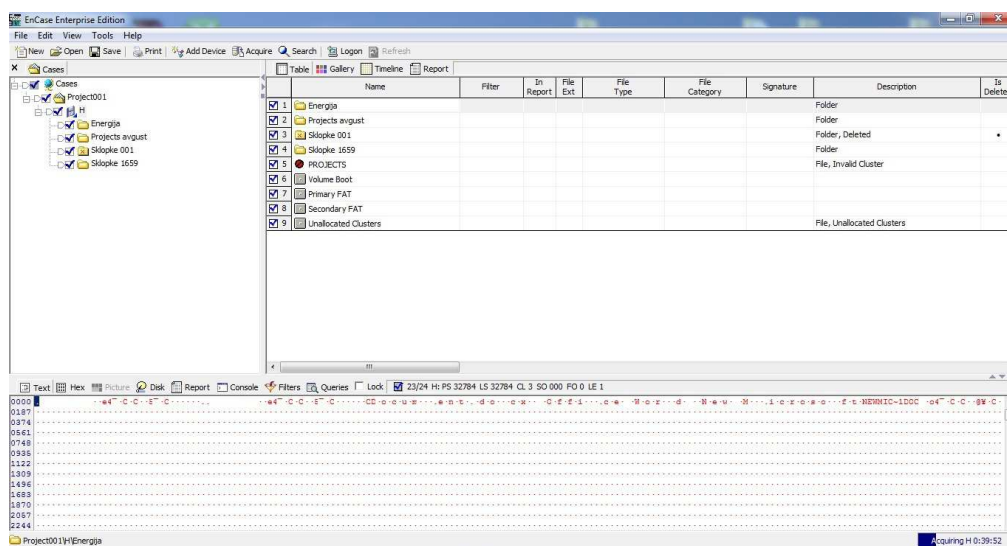
Sada treba forenzičar da uzme imidž tog diska, tako što bira desni klik tog local diska i onda bira “acquire” kao na slici 33. Zatim “add to case” (slika 34). Onda se doda naziv projekta i lokacija (slika 35) i na kraju bira “finish”. Nakon toga je potrebno neko vreme da se napravi imidž, a napredak se može pratiti u donjem desnom uglu kao na slici 36.



Slika 34

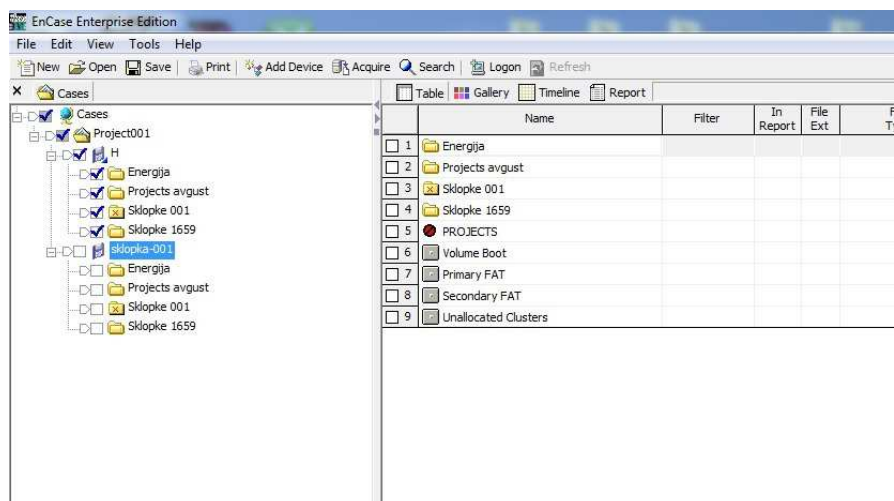


Slika 35

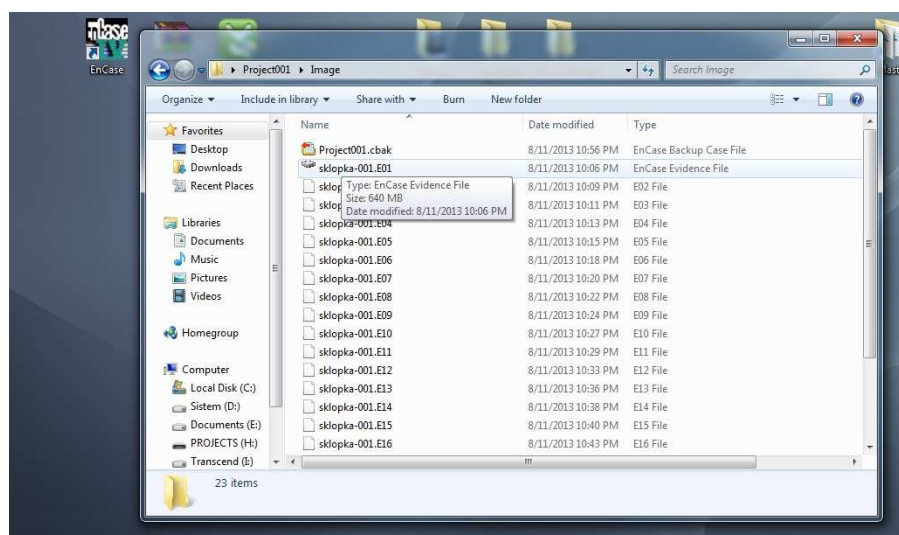


Slika 36

Nakon završetka se pojavljuje isti takav folder kao na sledećoj slici i to je imidž tog lokalnog diska. Sada se imidž nalazi u folderu image, koji je napravljen na početku i ima ekstenziju .EO1 kao na slici 38.



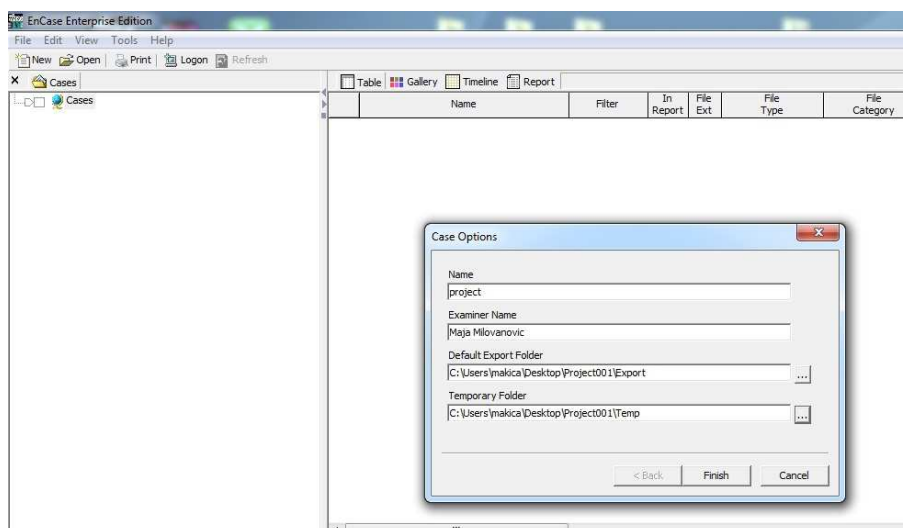
Slika 37



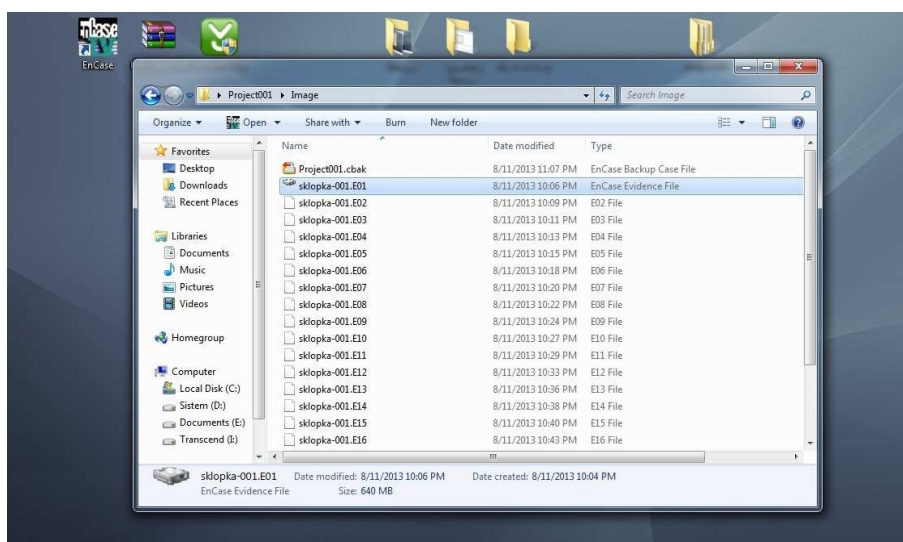
Slika 38

8.2.2. Analiza imidža

Nakon toga forenzičar pristupa analizi imidža. Prvo je potrebno da napravi slučaj isto kao i prilikom uzimanja imidža, kao na slici 39. Zatim odlazi u folder u koji je sačuvan imidž, i samo prevuče fajl sa ekstenzijom .EO1 koji se vidi na slici 40

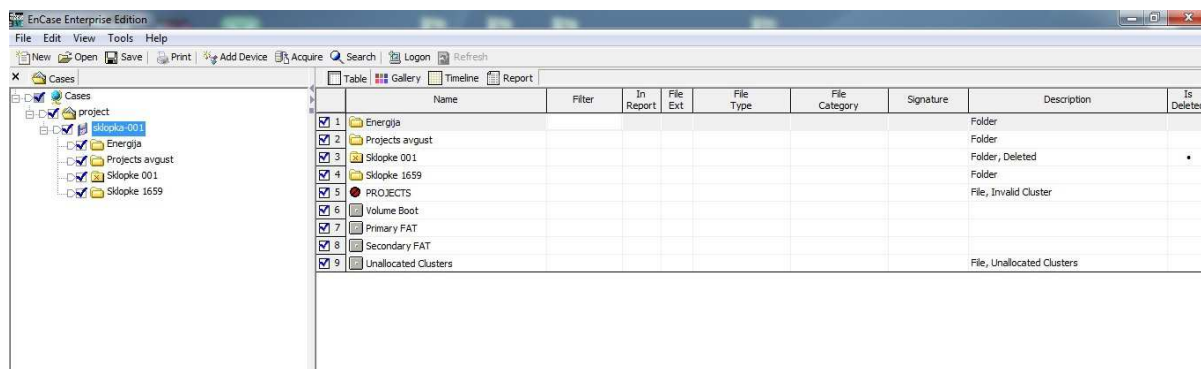


Slika 39



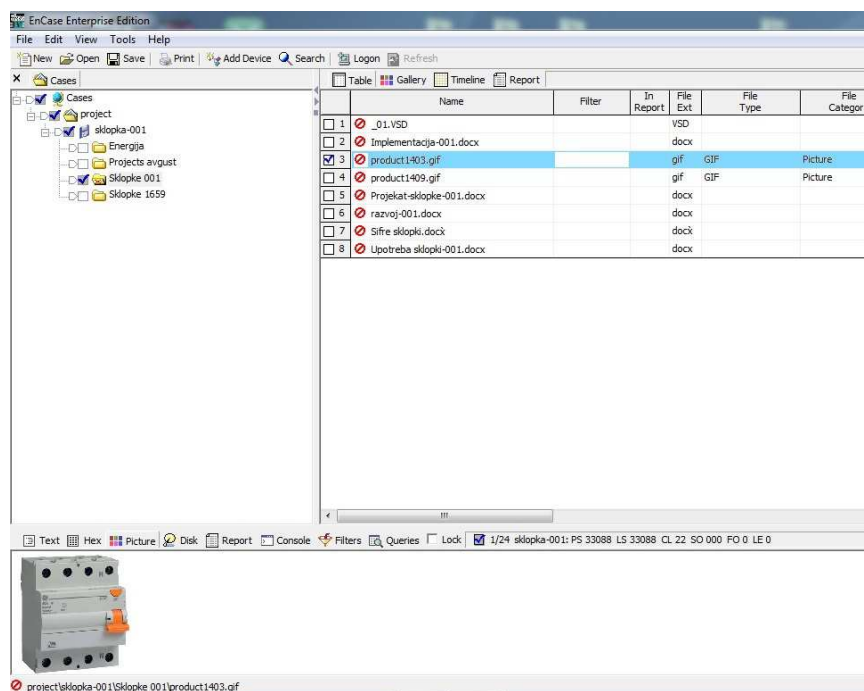
Slika 40

Nakon prevlačenja vidi se prozor kao na slici 41, i forenzičar sada može da vidi sve fajlove koji se tu nalaze kao i fajlovi koji su obrisani.

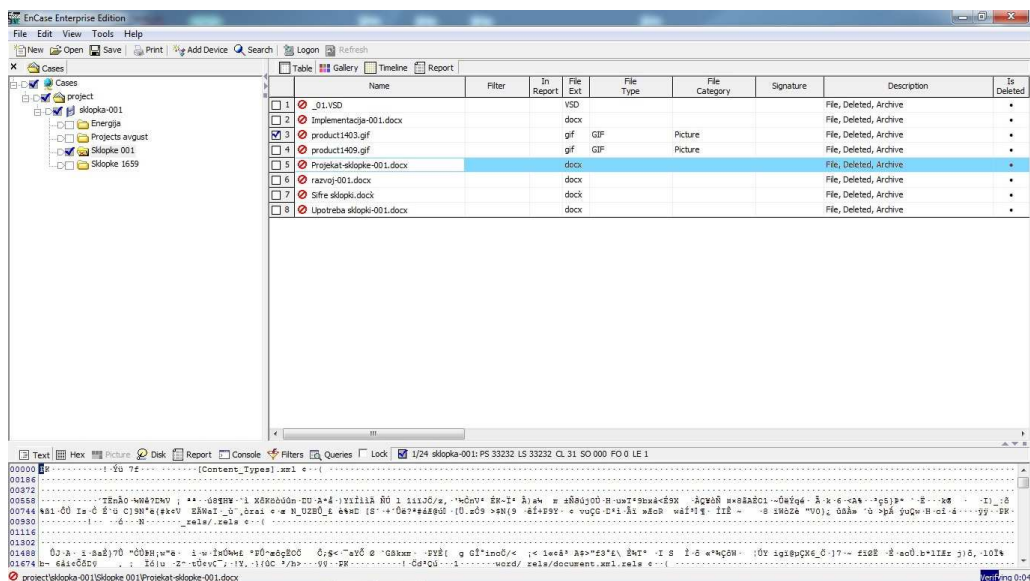


Slika 41

Na slici broj 42, klikom na neku sliku, u donjem delu mozemo videti sadrzaj. Klikom na tekstualni fajl, kao na slici 43 vidimo u donjem delu neka slova. Tek nakon oporavka ovog fajla moze se lepo videti njegova sadržina.



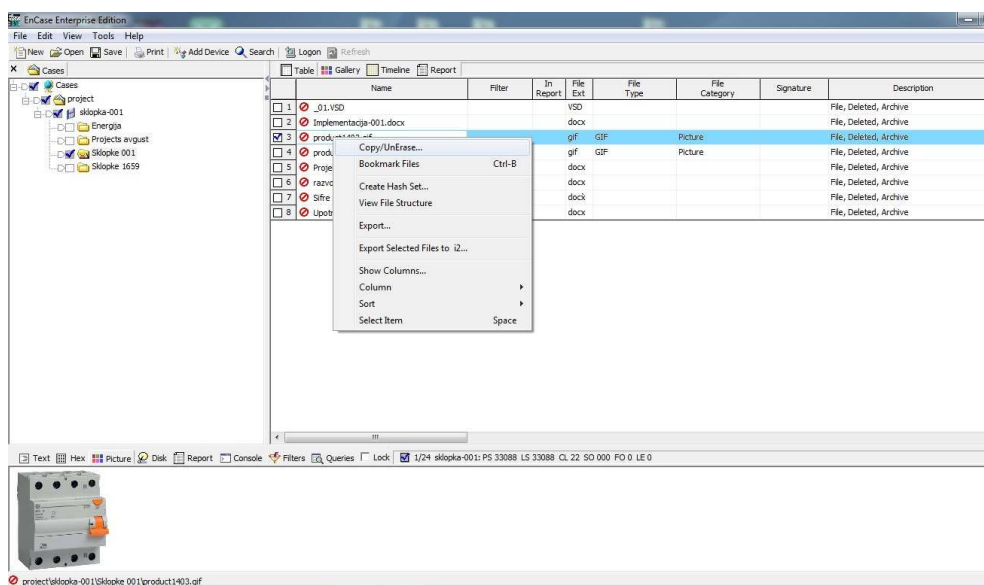
Slika 42



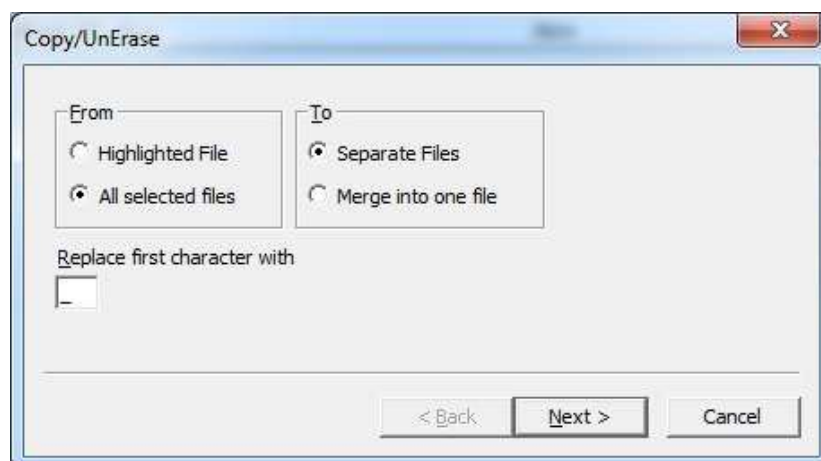
Slika 43

8.2.3. Vraćanje obrisanih fajlova i foldera

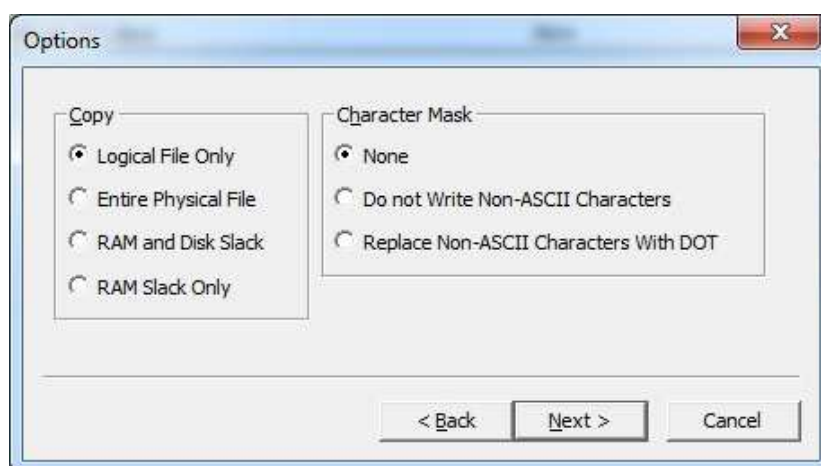
Obrisani fajl ili folder se oporavlja desnim klikom na fajl ili folder, zatim se bira opcija „copy/unrase“, što se vidi na slici 44. Zatim se podešava kao na slikama 45 i 46.



Slika 44

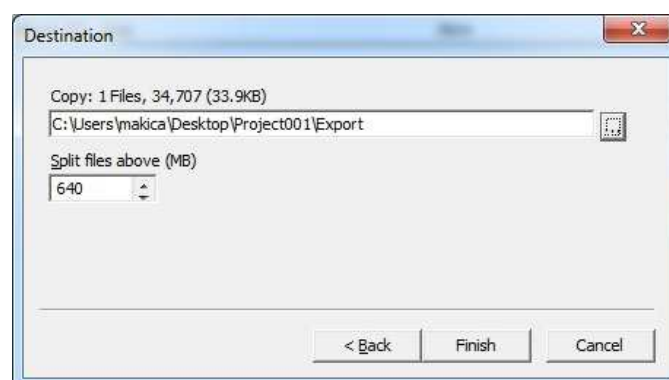


Slika 45

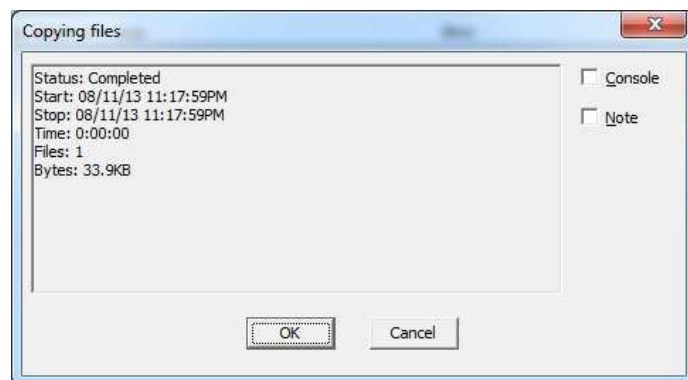


Slika 46

U prozoru koji se naziva Destination, slika 47, odabere se putanja do projekta gde će se čuvati ti fajlovi i odabere se finish. I na kraju aplikacija obaveštava o uspešno obavljenom kopiranju kao na slici 48.

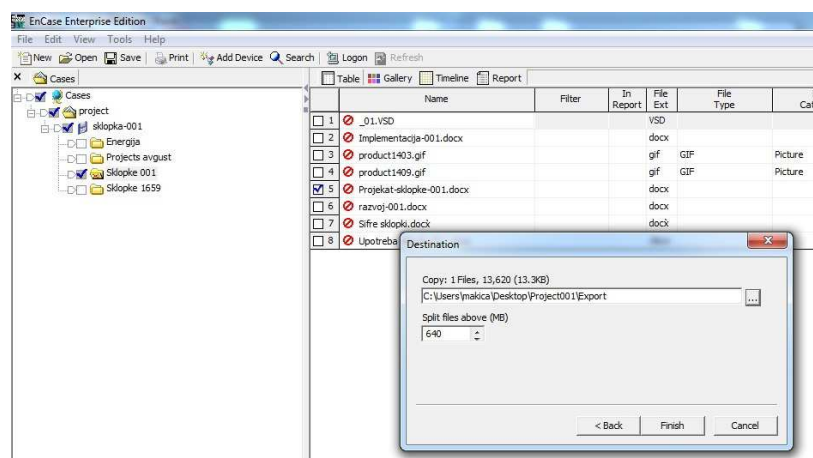


Slika 47

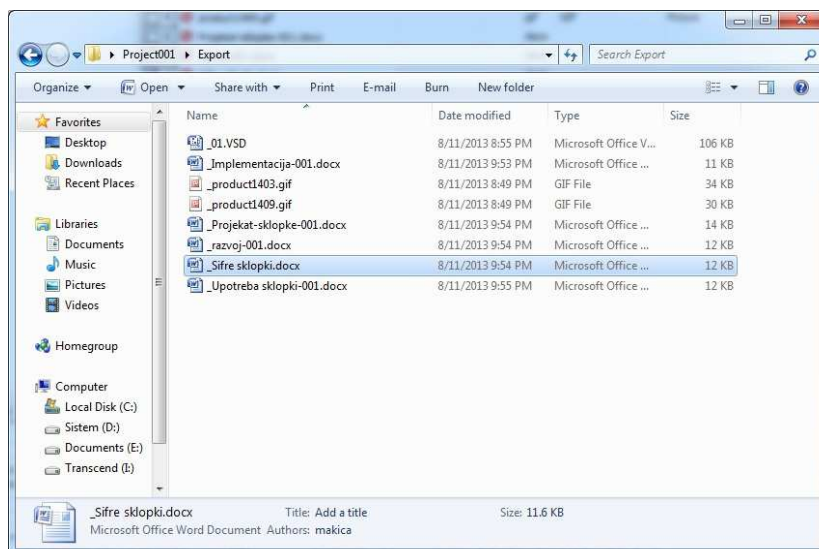


Slika 48

Tako je digitalni forenzičar otkrio šta se desilo, koj je fajl obrisao i na koj način je vraćen. Na slici 49 se vidi kako je odabrana destinacija i na kraju, na skici 50 se može videti ceo oporavljeni folder, koji je bio obrisao.



Slika 49



Slika 50

8.2.4. Postavljanje aplikacije za nadgledanje sistema

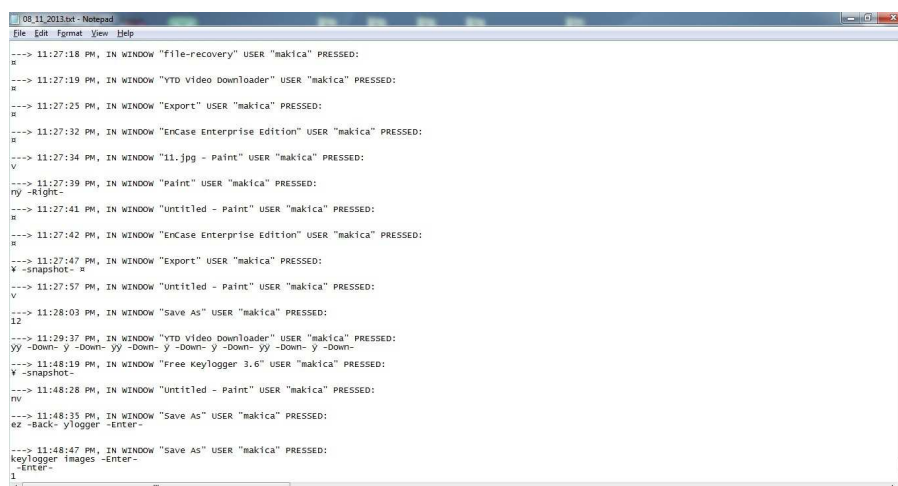
Nakon ovih dešavanja menadžer je želeo da se zaštiti na još neki način. U strahu da se to ne ponovi tražio je od forenzičara da mu bar na neko vreme, instalira neki program za stalno nadgledanje sistema kako bi pratio dešavanja.

Forenzičar mu je instalirao „keylogger“. Na slici 51 se vidi prozor u kom se podešavaju funkcije ovog programa. On je sakriven i sve vreme radi kao i antivirus. Sve njegove ikonice su sakrivene i tako nije moguće jednostavno ući mu u trag.

Jedini način za pokretanje je Ctrl+Shift+Alt+U. I nakon toga se otvara prozor kao na slici 51. Klikom na dugme „Keystrokes & Clipboard“ otvara se txt dokument, kao na slici 52, u kom pišu sva dešavanja koja su se desila na tom računaru i tog dana. Na kalendaru se bira dan koji korisnik želi da vidi.



Slika 51



Slika 52

8.3. Javna istraga

Digitalni forenzičar je otkrio šta se desilo sa projektom i povratio je taj folder. Sada je taj problem rešen ali ostaje drugi još veći problem. Ko je to uradio. Menadžer može samo da pretpostavlja ali ne može da bude siguran. Tako da su obaveštene vlasti i sada preuzimaju slučaj. Menadžer i digitalni forenzičar su preneli sve informacije koje su imali istražnim organima, koji su dalje nastavili sa radom. Krenuli su sa otiscima sa računara.

Nakon temeljno sprovedene istrage došli su do zaključka da je to uradio upravo onaj čovek na kog je menadžer i sumnjao.

9. Zaključak:

U ovom istraživačkom radu se vidi da je kompiuterski kriminal u stalnom porastu i da sadrži mnogo različitih oblika, i takođe je prikazan i način na koji se treba zaštititi. Zbog toga je bilo neophodno da se formiraju razne institucije koje će se baviti isključivo ovom vrstom kriminala. Postoje različite tehnike, metode i alati koje oni koriste u borbi. Istražni organi u velikoj meri sarađuju sa digitalnim forenzičarima tako što spajaju dokaze i na taj način mogu da naprave što tačniju rekonstrukciju događaja.

Ovaj rad ima zadatak da skrene pažnju na različitost ove vrste kriminala i da edukuje zaposlene u različitim firmama o opasnostima koje vrebaju sa Interneta. Na taj način bi oni stekli neko osnovno znanje i samim tim bi se kriminal koji koristi društveni inženjering smanjio.

10. Literatura:

[1]. „Digitalna forenzika računarskog sistema“ (2009) - Grubor Gojko, Milosavljević Milan - Univerzitet singidunum, Beograd

[2]. „Istraga kompjuterskog kriminala“ (2009) - Grubor Gojko, Milosavljević Milan - Univerzitet singidunum, Beograd

[3]. “Montaža i servisiranje računara” - Milosavljević M, Milić M. – Visoka škola elektrotehnike i računarstva, Beograd

[4]. „Rutkit tehnike“ (2011) - Jocić Đ. - Univerzitet Singidunum, Beograd

[5]. „Sigurnost računarskih sistema i mreža“ - Pleskonjić Dragan, Maček Nemanja, Đorđević Borislav, Carić Marko, Beograd

[6]. “Uvod u forenzičke alate” (prezentacija) - Grubor Gojko - Univerzitet singidunum, Beograd

Internet izvori:

[7]. http://sr.wikipedia.org/sr/Дигитална_форензика_и_алати (Pristupljeno: Januar 2013.)

[8]. http://sr.wikipedia.org/sr/Сајбер_криминал (Pristupljeno: Januar 2013.)

[9]. <http://sr.wikipedia.org/wiki/Г8> (Pristupljeno: Januar 2013.)

[10]. http://en.wikipedia.org/wiki/Computer_crime (Pristupljeno: Januar 2013.)

[11]. http://sr.wikipedia.org/wiki/Имплементација_Конвенције_о_сајбер_криминалу_у_српском_законодавству (Pristupljeno: Januar 2013.)

[12]. <http://idesh.net/tech-i-web/gadgeti-za-paranoicne/> (Pristupljeno: Januar 2013.)

[13]. http://www.zksoftware.co.rs/sta_je_to_biometrija.php (Pristupljeno: Januar 2013.)

[14]. <http://www.sk.rs/2005/03/skpr02.html> (Pristupljeno: Januar 2013.)

[15]. http://www.znanje.org/i/i2011/11iv04/11iv0425/struktura_dnk_osobine_i_funkci2.htm (Pristupljeno: Januar 2013.)

- [16]. http://sr.wikipedia.org/wiki/Dečja_pornografija_na_internetu (Pristupljeno: April 2013.)
- [17]. http://sr.wikipedia.org/wiki/Sajber_terorizam (Pristupljeno: april 2013.)
- [18]. http://sr.wikipedia.org/wiki/Крађа_идентитета_на_интернету (Pristupljeno: april 2013.)
- [19]. http://sr.wikipedia.org/wiki/Интернет_превапе (Pristupljeno: april 2013.)
- [20]. http://en.wikipedia.org/wiki/Computer_crime (Pristupljeno: april 2013.)
- [21]. <http://en.wikipedia.org/wiki/Cyberstalking> (Pristupljeno: april 2013.)
- [22]. http://en.wikipedia.org/wiki/Internet_homicide (Pristupljeno: april 2013.)
- [23]. <http://www.lensoptic.com/ocna-ordinacija/bolesti-oka/refrakcione-greske/astigmatizam/> (Pristupljeno: april 2013.)
- [24]. http://bs.wikipedia.org/wiki/Tvrđi_disk (Pristupljeno: jun 2013.)
- [25]. <http://www.minor.co.rs/index.php?id=fid-sklopke> (Pristupljeno: jun 2013.)