

UNIVERZITET „SINGIDUNUM“

Departman za poslediplomske
MASTER STUDIJE

Studijski program:
Savremene informacione tehnologije

MASTER RAD

Istraga kompjuterskog kriminala u e-poslovanju

Mentor:
Doc. dr Gojko Grubor

Kandidat:
Bojan Milićević
Br.ind. 410324/2010

Beograd, decembar 2011.

Sažetak

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

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

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

Abstract

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

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

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

Sadržaj

1. Metodologija naučnog istraživanja.....	6
1.1 Uvodne napomene i obrazloženje rada.....	6
1.2 Predmet istraživanja.....	7
1.3 Ciljevi i zadaci istraživanja.....	8
1.4 Hipotetički okvir istraživačkog rada.....	9
1.5 Metodi, tehnike i tok istraživačkog procesa.....	9
2. Istraga kompjuterskog kriminala	11
2.1. Uvod.....	11
2.2. Proces korporacijske istrage.....	12
2.2.1. Sigurnosni standardi.....	12
2.2.2. Sigurnosna politika.....	14
2.3. Pravilnik o rešavanju sigurnosnih incidenata.....	16
2.3.1. Svrha.....	16
2.3.2. Prijava incidenta.....	16
2.3.3. Procedure i uputstva za rešavanje incidenata.....	17
2.3.4. Obuka.....	18
2.3.5. Sankcije.....	18
2.4. Tehnike i alati.....	19
2.4.1. Helix2008R1.....	20
2.5. Taksonomija kompjuterskog napada.....	24
2.6. Kompjuterska i mrežna forenzika.....	25
2.6.1. Pravila za sprovođenje kompjuterske i mrežne forenzike.....	26
2.6.2. Planiranje odgovora na kompjuterski incident.....	27
2.6.3. Procedure i uputstva za rešavanje incidenata.....	27
2.6.4. Obuka.....	29
2.6.5. Ubrzanje istrage.....	30
2.6.6. Sankcije.....	30
2.7. Zvanična istraga kompjuterskog kriminala	31

2.7.1 Uvod.....	31
2.7.2. Zvanična istraga incidenta.....	33
2.7.3. Metode i tehnike istrage.....	41
2.7.4. Alati.....	46
2.7.5. Helix2008R1.....	47
2.7.6. Digitalni kompjuterski dokazi.....	55
2.7.7. Rezultati istrage.....	58
2.8. Studija slučaja (<i>Case Study</i>).....	60
2.8.1. Scenario kompjuterskog incidenta firme.....	60
2.8.2. Uzimanje imidža USB uređaja	63
2.8.3. Predaja dokaza za zvaničnu istragu.....	66
2.8.4. Zvanična istraga	68
2.8.5. Prezentacija dokaza na sudu.....	72
3. Zaključak.....	73
4. Literatura.....	74

1. Metodologija istraživačkog projekta

1.1. Uvodne napomene i obrazloženje rada

Internet, globalna svetska kompjuterska mreža je za kratak vremenski period od desetak godina evoluirala u moćnu mrežu bez koje je nemoguće zamisliti život savremenog čoveka. Kada bi ova kompjuterska mreža prestala da funkcionise tek tad bi se shvatio njen značaj i u kojoj meri se protkala u sve pore savremenog društva. Broj korisnika Interneta iz godine u godinu beleži eksponencijalni rast broja korisnika i smatra se da ih trenutno ima oko 1,133,408,294 (17.2%) [1]. Uporedo sa razvojem i implementacijom kompjuterskih mreža u sistem globalne mreže - Intereneta, rastu i potencijalne opasnosti od različitih napada sa Interneta, uključujući brojne maliciozne kodove (programe) i napade ljudskog faktora – hakera, krakera, vandala i kompjuterskih terorista [2].

Razlozi za pojavu ovih napada su različiti. Najčešći razlog je sticanje finansijske dobiti, ali i drugi motivi, kao što su izazov, znatiželja, samopotvrđivanje, krađa informacija, špijunaža i drugi oblici kompjuterskog kriminala. "Pod kompjuterskim kriminalom u najširem smislu podrazumevaju se krivična dela prema krivičnom zakonu nacionalne države, u kojoj su na bilo koji način uključeni računarski sistemi i mreže [2].

Glavni cilj istrage kompjuterskog kriminala je, kao i u slučaju klasičnog kriminala, izgraditi za pravosudne organe neoporiv, ili čvrst dokaz, i/ili dokaz za oslobađanje osumnjičenog, i/ili pravedno sankcionisanje učinjenog dela¹. Da bi se obezbedio takav dokaz, u slučaju kompjuterskog kriminala, potrebno je, nizom posrednih dokaza, doći do informacija u digitalnom obliku koje imaju verodostojnu vrednost, a koja je uskladištena ili prenesena u takvom obliku. Ovakve informacije su digitalni dokazi.

¹ Milosavljević M., Grubor G., *Digitalna forenzika*, Univerzitet Singidunum, Beograd 2008, str. 12

U prvom delu rada dati su osnovni podaci o metodologija istraživanja projekta opisane su predmet istraživanja, ciljevi i zadaci istraživanja, hipotetički okvir istraživačkog rada, metodi, tehnike i tok istraživačkog procesa.

U drugom delu rada opisana je digitalna forenzička istraga kompjuterskog kriminala, forenzički alati koji se koriste, kao i dokazi koje treba prezentovati na sudu. Ovde su opisani procesi zvanične i korporacijske istrage. Za zvaničnu vrstu istrage nadležni su zvanični i pravosudni organi države, a korporacijska istraga je interna istraga organizacije (kompanije, firme institucije) koja se vrši sopstvenim snagama u cilju utvrđivanja prave prirode kompjuterskog incidenta. U ovom djelu je opisana i studija slučaja u kojoj jedna korporacijska istraga prelazi u zvaničnu istragu kompjuterskog kriminala.

U trećem delu rada su zaključkom potvrđeni postavljeni ciljevi i hipoteze o značaju i pomoći primene digitalne forenzičke istrage u upravljanju kompjuterskim incidentom i trajnom otklanjanju uzroka tog incidenta.

1.2. Predmet istraživanja

U ovom radu predmet istraživanja je kako otkriti, proučiti, predstaviti, pomoću kojih metoda i alata, pronaći i prezentovati digitalne dokaze protiv osumnjičenog, tako da ti dokazi imaju punu vrednost i prihvatljivost na sudu.

U prvom delu rada je objašnjena metodologija istraživanja naučnog rada predmet istraživanja, ciljevi i zadaci istraživanja, hipotetički okvir istraživačkog rada, metodi, tehnike i tok istraživačkog procesa.

U drugom delu rada je opisano kako treba da se sprovede jedna digitalna forenzička istraga u organizaciji, da bi se dobili validni digitalni dokazi za sudski postupak u slučaju velike štete od kompjuterskog incidenta, kao i alati i tehnike koje treba koristiti i standardne operativne procedure kojih se treba pridržavati.

Opisan je rad na živom (aktivnom) sistemu prema modelu statičke (*postmortem*) forenzičke istrage sa ili bez privremenog oduzimanja osumnjičenog računara. Uključen računar može da obezbedi najviše dokaza, ali pod uslovom da se unese što manje promjena, što obezbeđuju forenzički alati i tehnike.

Opisani su tokovi istrage, od dolazka na mjesto krivičnog djela do rekonstrukcije i istrage u kontrolisanim uslovima . U ovom delu je takođe opisan program Helix, koji važi za jedan od najboljih programa za forenzičku analizu nekog sistema ili medija .

1.3. Ciljevi i zadaci istraživanja

Glavni cilj ovog rada je da se demonstrira značaj korporacijske forenzičke istrage u odgovoru na kompjuterski incident koji nanosi evidentnu štetu organizaciji, sa posebnim osvrtom na nove tehnologije, alate i metode koje se koriste u istrazi.

Poseban cilj 1 je opisati kako treba da se izvrši jedna korporacijska istraga i da najmanja sitnica koja nije sprovedena u skladu sa standardnom procedurom (IOCE) uzimanja forenzičkog imidža ispitivanog računara, može ugroziti kompletnu istragu i odbaci taj digitalni dokaz od strane zvaničnih organa istrage koji preuzimaju slučaj za sudski postupak.

Poseban cilj 2 je da se pokaže kako se dolazi do relevantnih digitalnih dokaza i kako ih treba čuvati i prezentovati na sudu.

1.4. Hipotetički okvir istraživačkog rada

Opšta hipoteza:

Istraga kompjuterskog kriminala generalno sadrži sledeće faze:

- dolazak i fiksiranje mesta krivičnog djela,
- kopiranje podataka sa fizičkog i logičkog diska (uzimanje forenzičkog imodža),
- analiza podataka i pronalaženje dokaza pomoću odgovarajućih alata i metoda i
- predstavljanje dokaza na sudu.

Opšti problem prilikom forenzičke istrage bez privremenog oduzimanja računarske opreme je kad i na koji način se primenjuje i koja tehnika gašenja uključenog računara. Mada mnogi stručnjaci tvrde da je nasilno gašenje računara najefikasnije za slučaj forenzičke istrage, bez obzira koja platforma je u pitanju.

Radna hipoteza

Radna hipoteza je forenzička analiza za otkrivanje internog napada i zloupotrebe od strane zaposlenog sa privilegijama radi pribavljanja vlastite koristi i u kojoj mjeri je korporacijska istraga podpomogla zvaničnu istragu kompjuterskog kriminala.

1.5. Metodi, tehnike i tok istraživačkog procesa

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

- *sistematičnost* - dobra uređenost istraživanja i obezbeđivanje prirodnog i logičkog

sleda procesa,

- *kontrolisanost* - sprovođenje istraživanja u što moguće boljim i nadziranim uslovima, kako bi se isključila alternativna rešenja i
- *kritičnost* - sve važne tvrdnje o pojavama, procesima, odnosima i svojstvima moraju se ozbiljno, iskreno i strogo procenjivati, proveravati i obrazložiti.

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

U ovom istraživačkom radu korišćene su različite metode istraživanja i verifikacije procesa digitalne forenzičke istrage da bi se došlo do nekih saznanja, otkrili i izložili naučni principi, koja se primenjuje u digitalnoj forenzici.

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

2. Istraga kompjuterskog kriminala

2.1 Uvod

Krađa povjerljivih podataka je glavni uzrok korporacijske istrage. Ovi kompjuterski incidenti se sve češće događaju od strane zaposlenih u tim korporacijama. Shodno tome u korporacije se treba uvesti niz mera da bi se sprečila manipulacija tim podacima.

Prilikom korporacijske istrage kompjuterskog kriminala trebaju se poštovati ista pravila i standardi kao i kod zvanične istrage. Prilikom sprovođenja ove istraga treba da se uzme u obzir da u bilo kom trenutku ova istraga može da izađe iz okvira korporacije i bude predata nadležnom organu. Da bi smanjili stopu kompjuterskog kriminala u korporacijama treba da se uvede sigurnosna politika. To je jedan skup i dugotrajan proces kojem je potrebno prilagoditi sve djelove organizacije. Uvođenjem sigurnosne politike podiže se nivo sigurnosti informacionog sistema i korisnika.

Uvođenje sigurnosne politike može biti skup i dugotrajan proces u kojem je potrebno prilagoditi sve delove organizacije da rade sinhronizovano. Korporacijama i institucijama se preporučuje uvođenje sigurnosne politike radi podizanja nivoa sigurnosti kako informacionog sistema, tako i njihovih korisnika.

U ovom radu predmet istraživanja je pronalaženje digitalnih dokaza na mrežnim uređajima koji se koriste u korporacijama u cilju forenzičke akvizije na računarskim mrežama i izrada sigurnosne politike za korporaciju sa težištem na rešavanju kompjuterskih incidentata i digitalnu forenzičku istragu kompjuterskog kriminala.

2.2. Proces korporacijske istrage

Korporacijska istraga se može smatrati predistražnim postupkom zvanične istrage kompjuterskog kriminala.

Odvija se u tri faze:

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

Rekonstrukcija traga napada predstavlja čitanje log datoteka na celom putu napada, pri čemu se javljaju sledeći problemi:

- log datoteke su izmenjene, ne postoje ili su neadekvatne,
- isprekidana zaustavljanja između izvora napada i računara žrtve,
- uskraćena saradnja administratora posrednih računara,
- lažiranje IP adresa,
- izmenjeni log datoteka napadnutog računara ili primenjeni drugi trikovi za maskiranje neovlašćenog pristupa,
- samo jedan neovlašćeni pokušaj pristupa.

Prikupljanje dokaza i predavanje dokaznog materijala korporacijskim ili zvaničnim organima istrage, vrši se isključivo po odobrenju vlasnika napadnutog sistema i odluci korporacije.

2.2.1. Sigurnosni standardi

Standardi iz ISO/IEC 27000 serije korporacijama pružaju smernice za konstruisanje, primenu i proveru informacionih sistema čime se osigurava poverljivost, integritet i dostupnost informacionog sadržaja, sistema i procesa unutar organizacije. Za područje sigurnosti informacionih sistema najčešće se koriste dva standarda [13]:

- ISO/IEC 27001 i

- ISO/IEC 27002

ISO/IEC 27001² je službeni skup specifikacija na bazi kojih korporacije imaju pravo zatražiti postupak sertifikacije, ukoliko su primenile taj standard na sistem upravljanja sigurnošću informacija. Ovaj standard propisuje zahteve za uspostavljanje, sprovođenje, nadgledanje, ispitivanje, održavanje i poboljšanje sistema za upravljanje sigurnošću informacija.

Standard se sastoji od 5 delova:

1. Sistem za zaštitu informacija,
2. Odgovornost rukovodećih ljudi,
3. Unutrašnje provere sistema za zaštitu informacija,
4. Provera valjanosti sistema za zaštitu informacija i
5. Poboljšanja na sistemu za zaštitu informacija.

ISO/IEC 27001 standard definiše koje zahteve neki sistem za zaštitu informacija mora imati, pa za primerene provere navodi upotrebu ISO/IEC 27002 standarda. ISO/IEC 270023 je službeni standard, ali se tumači kao skup smernica koje je moguće upotrebiti [12].

Standard sadrži 39 ciljeva i sastoji se od 12 delova:

1. Procena rizika,
2. Sigurnosna politika,
3. Organizacija informacione sigurnosti,
4. Upravljanje imovinom,
5. Zaštita od zaposlenih,
6. Fizička zaštita i zaštita od okoline,
7. Upravljanje komunikacijama i operacijama,

² www.iso27001security.com/html/27001.html, nedelja 27.11.2011. god.

8. Provera pristupa,
9. Nabavka, razvoj i održavanje informacionih sistema,
10. Upravljanje incidentima u informacionom sistemu,
11. Upravljanje poslovnim kontinuitetom
12. Usklađivanje

2.2.2. Sigurnosna politika

Skup jasno definisanih pravila koja obuhvataju sva područja na kojima je moguće izvršiti neku vrstu napada naziva se sigurnosnom politikom (*Slika 1*). Sigurnosnom politikom jasno se određuju pravila ponašanja i odgovornosti vezane uz informacioni sistem kako bi se minimizovala šteta nastala namernim ili nenamernim delovanjem [4].

Sigurnosna politika korporacije ili institucije prilagođava se potrebama i nije jednaka za sve.

Standard je obavezni postupak ili pravilo koje je izrađeno kako bi učinilo politiku delotvornom, a mora uključivati jedan ili više tehničkih opisa za komponente računara, programe i njihovo rukovanje.

Smernice su uopštene izjave, preporuke ili administrativna uputstva koja daju okvirna uputstva za sprovođenje sigurnosne politike konstruisane kako bi se ostvarili ciljevi sigurnosne politike.

Uspostavom sigurnosne politike korisnicima su nametnuta obavezujuća pravila ponašanja koja ograničavaju slobodu pri pregledu poverljivih informacija, kao i pravila za ispravno korišćenje računarske opreme koja je korisniku data na korišćenje.

Sigurnosnom politikom osiguravaju se tri svojstva informacija koje sadrži neki sistem.

- poverljivost,

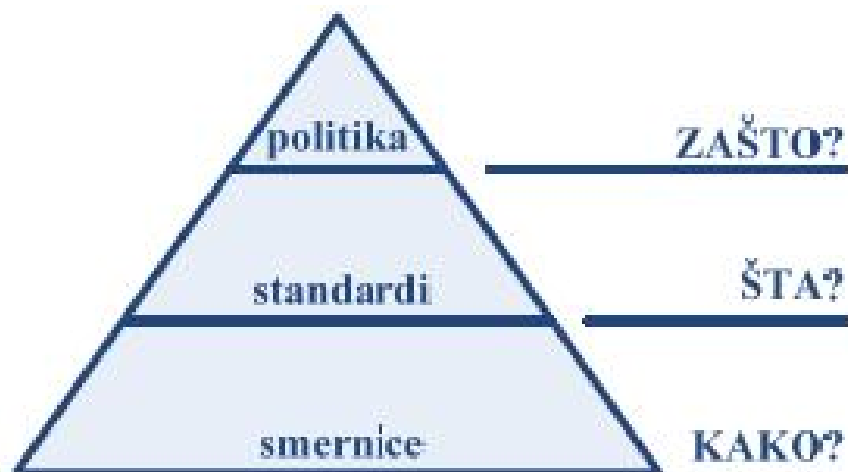
- integritet,
- dostupnost.

Mehanizmi zaštite i sprečavanja su podeljeni na tri osnovna nivoa:

- fizička sigurnost, pod kojom se smatra sigurnost računarske opreme i podataka,
- lična sigurnost je zaštita korisnika i poverljivih informacija o korisniku i
- sigurnost organizacije, koja zavisi od prva dva nivoa.

Da bi se zadovoljili propisani standardi sigurnosti informacioni sistemi se dele na tri glavna dela:

- računarsku opremu,
- programe i
- komunikacije.



Slika 1. Sigurnosna politika

2.3. Pravilnik o rešavanju sigurnosnih incidenata

2.3.1. Svrha

Svrha ovog dokumenta je da se ustanovi obaveza prijavljivanja problema prilikom rada sa računarskom opremom. Prosečan korisnik nemože znati da li je njegov računar žrtva sigurnosnih incidenata.

Svaki problem sa računarskom opremom treba biti prijavljen, a tehničko osoblje Odseka za informatiku, vrši opravku, podešavanje opreme i dr. U slučaju sumnje na sigurnosni incident prijavljuje timu za upravljanje kompjuterskim incidentima³.

Sigurnosne incidente rešava tim za upravljanje kompjuterskim incidentima sprovodeći tehnike kompjuterske i mrežne forenzike koje se koriste da otkriju digitalne dokaze u raznim kompjuterskim zločinima kao što su krađe poslovne tajne i uopšte zloupotreba računa i računarskih mreža u cilju zaštite intelektualne svojine.

2.3.2. Prijava incidenta

Svaki zaposleni, korisnik ili saradnik Korporacije dužan je prijaviti:

- usporeni rad računara,
- usporeni ili onemogućeni pristup mrežnom servisu,
- nemogućnost pristupa, gubitka ili neovlašćene izmene datoteke,
- pojave virusa ili nepoznatih ikonica na računaru,
- sumnju da se događa kompjuterski incident.

³ McClure S, Scambray J, Kurtz G., *Hakerske tajne: zaštita mrežnih sistema, prevod petog izdanja, Mikro knjiga, Beograd, 2006.*

Tim za upravljanje kompjuterskim incidentima izrađuje i ažurira listu kontakt osoba kojima se prijavljuju problemi u radu računara i servisa i obrazac za prijavu incidenta. Lista se deli svim zaposlenima i objavljuje se na internim web stranicama korporacije. Svaki incident se dokumentuje. Uz obrazac za prijavu incidenta, dokumentacija sadrži i obrazac sa opisom incidenta i preduzetih mera pri rešavanju problema.

2.3.3. Procedure i uputstva za rešavanje incidenata

Prilikom primena forenzičkih akcija tim za upravljanje kompjuterskim incidentima sprovodi sledeće procedure:

- informacioni sistem sačuvati u zatečenom stanju, odnosno ne činiti izmene koje bi otežale ili onemogućile dijagnostifikovanje,
- pravljenje dve kopije oštećenog hard diska, korišćenjem alata za kreiranje slike diska,
- dokumentovanje svake radnje, tako da se ponavljanjem zabeleženih akcija može rekonstruisati tok istrage,
- o istrazi se sačinjava izveštaj, kako bi u slučaju potrebe mogli poslužiti kao dokaz u eventualnim krivičnim ili sudskim procesima,
- izveštaji o oncidentu smatraju se poverljivim dokumentima i čuvaju se na taj način da im pristup imaju samo ovlašćene osobe.

Tim za upravljanje kompjuterskim incidentima ima ovlašćenja:

- praćenje svih korisničkih procesa na računaru i izlistavanja sadržaja korisničkog direktorijuma, ako sumnja da se računar koristi na nedozvoljen način
- pristupa svakoj datoteci u računarskom sistemu korporacije i
- pristupa sistemski uskladištenih podataka na serveru i rezervnih kopija podataka lokalnih korisnika,

bez dozvole zaposlenog kome je računarska oprema data na upotrebu, koji je kreirao datoteku ili napravio rezervnu kopiju podataka i ne smatraju se napadom na privatnost.

Podaci mogu biti upotrebljeni i na sudu.

Korporacija može objavljivati statističke podatke o sigurnosnim incidentima, bez otkrivanja poverljivih i personalnih informacija.

2.3.4. Obuka

Svi zaposleni se moraju obučiti za primenu procedura odgovora na kompjuterski incident.

Tim za upravljanje kompjuterskim incidentima planiraće simulaciju incidenta i testirati postupak u realnim situacijama.

Po završetku testa upoznati sve zaposlene sa iskustvima.

2.3.5. Sankcije

Svrha istrage je da se odredi uzrok nastanka problema i da se iz toga izvuku zaključci o tome kako sprečiti ponavljanje incidenta, ili se barem bolje pripremiti za slične situacije. Ako je uzrok sigurnosnom incidentu bila greška čoveka, protiv odgovornih se mogu preduzeti sankcije⁴.

Korporacija može osobama odgovornim za sigurnosni incident zabraniti fizički pristup prostorijama ili logički pristup podacima. Ukoliko je incident izazvao zaposleni spoljne firme, korporacija može zatražiti od nje da ga ukloni sa liste osoba ovlašćenih za obavljanje posla u korporaciji.

U slučaju teže povrede pravila sigurnosne politike korporacija može pokrenuti krivični postupak.

⁴ Pleskonić D., Maček N. Đorđević B. Carić M. *Sigurnost računarskih sistema i mreža, Mikro knjiga, Beograd, 2007.*

2.4. Tehnike i alati

Akvizicija digitalnih podataka prvi je zadatak u forenzičkoj istrazi računara i podrazumeva pravljenje fizičke kopije bit-po-bit originalnog (osumnjičenog, ispitivanog) diska računara. Ova procedura sprečava korupciju i oštećenje digitalnih podataka na originalnom disku. Akvizicija digitalnih podataka obuhvata sledeće funkcije [3]:

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

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

U procesu akvizicije podataka softverskim alatima postoje dva metoda kopiranja:

- fizičko kopiranje celog fizičkog diska i
- logičko kopiranje particija diska.
- Većina softverskih alata za akviziciju uključuje jednu ili obe ove funkcije. Formati koji su na raspolaganju za akviziciju diskova variraju od potpuno sirovih podataka u binarnom zapisu do kompresovanih podataka specifičnih za proizvode. Sirovi podaci su direktna kopija diska. Primer imidža sirovih podataka je izlaz UNIX i Linux šel **dd** komandne linije.
- Primer formata sirovih podataka je jednostavna bit-po-bit kopija fajla podataka, particije diska, ili celog diska. Alat za akviziciju sirovih podataka može kopirati podatke sa jednog diska na drugi disk, ili u jedan ili više segmentiranih fajlova podataka. Pošto je ovo zaista neizmenjena kopija, forenzičar može gledati sadržaj sirovih podataka imidža fajla sa heksadecimalnim editorom koji sadrže gotovo svi forenzički alati.

2.4.1. Helix2008R1

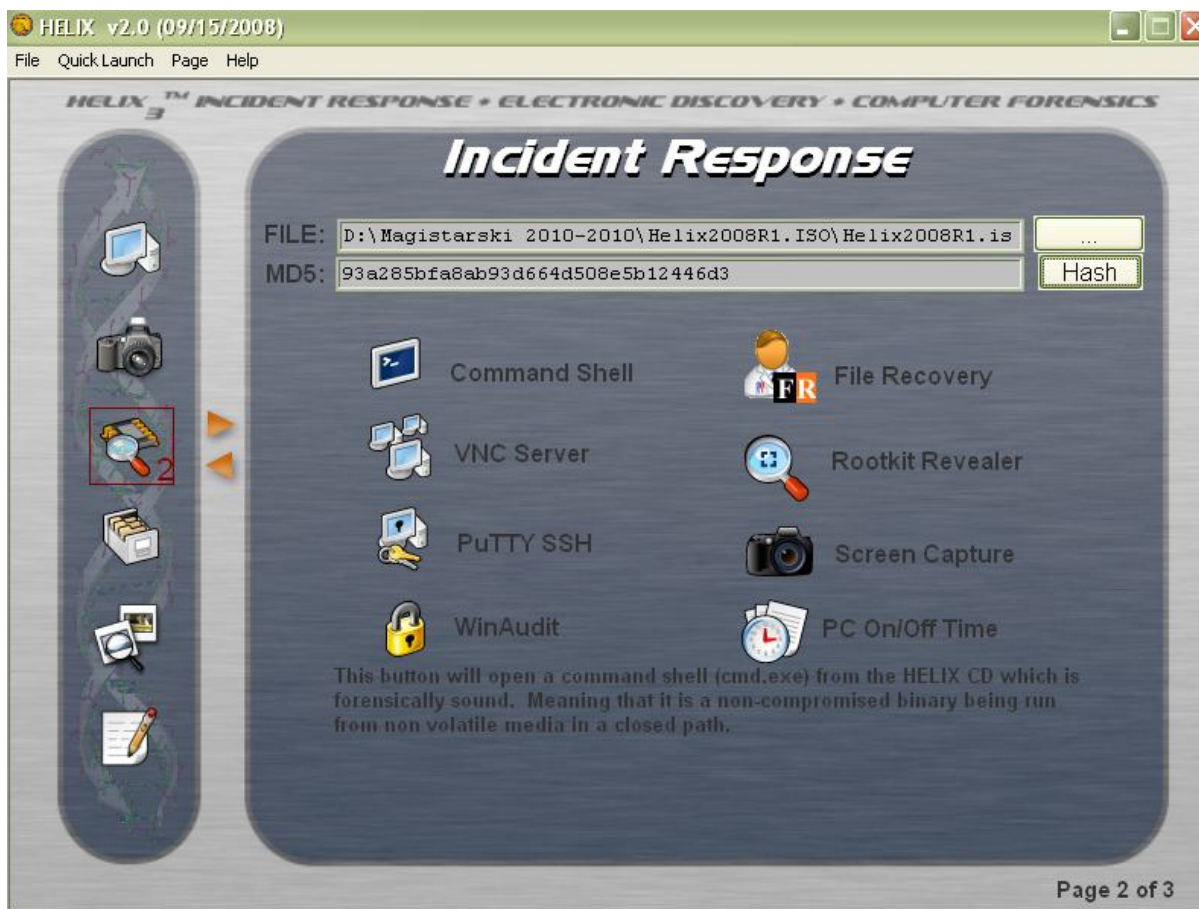
Heliks je veoma moćan alat. Ali sa velikom moći dolazi velika odgovornost, i kao potencijalni forenzika istraživači, naša je odgovornost da naučimo kako da pravilno koristimo ovaj alat.

Jednostavna greške i dobre namere mogu u potpunosti uništiti digitalne dokaze. Snažno se preporučuje da budući istražitelji praksu obavljaju na kontrolisanom sistemu, pre nego što pokušaju da pokupe dokaze iz realnog sistema. Ovaj alat može da radi na dve platforme , Windows i Lunix.



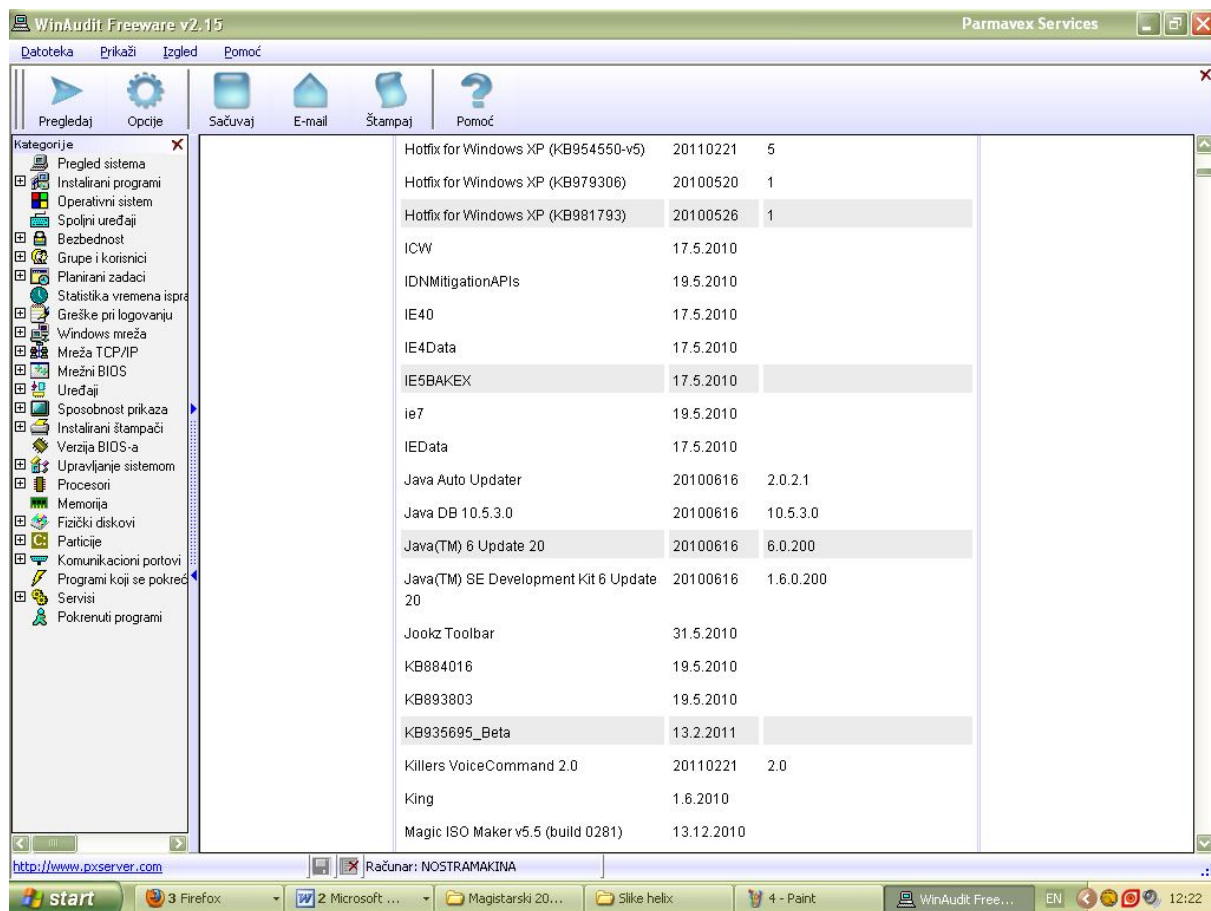
Slika 2. Početna stranica programske platforme Helix

Na *slici 2* vidimo početnu stranicu programske platforme Helix. Tu se nalazi određeni broj alata koji se koriste u istrazi. Nama je mnogo zanimljivija *slika 3*, jer na njoj vidimo heksadecimalni zapis jednog foldera. Ovaj zapis se uzima pre forenzičke istrage na tom folderu. Nakon obavljene istrage ponovo se uzima hash foldera na kome je sprovedena analiza. Ta dva zapisa treba da budu potpuno ista i to je dokaz da tokom digitalne forenzičke istrage ništa nije promjenjeno od strane forenzičara. Takodje na *slici 3* vidimo jos neke alate, kao sto je alat koji nam pokazuje kad je i koliko dugo racunar bio upaljen, program koji nam omogućava da povratimo fajlove koji su obrisani.



Slika 3. Heksadecimalni zapis jednog foldera

Na slici 4, na sledećoj stranici nalazi se screenshot jednog od alata sa ove platforme. Win Audit je program cijim pokretanjem aktivira se skeniranje računara na koji rade na windows platformi . Ona nam zatim ispisiuje kopletnu softversku i hardversku strukturu računara. Ispisiuje nam koji su programi pokrenuti , kad su instalirani koliko se često koriste, koji su uredjaji bili priključeni na računar. To se pokazalo izuzetno korisno jer on nam pokazuje ako je nekad na njega bio prikljucen neki eksterni memorijski medijum koji je predmet istrage. To nam omogućava da povezemo taj računar i taj medijum na osnovi digitalnog potpisa koji je taj medijum ostavio u računaru.



Slika 4. Screenshot Win Audit alata

U postojanju napora da se obezbede kompjuterski sistemi u sprečavanju incidenata, forenzičke tehnike su potrebne da se otkriju počinioci i da se omogući povratak imovine ili prihoda izgubljenih u incidentu.

Krajnji cilj računarske forenzike je da se obezbedi dovoljno dokaza da bi se otkriveni kompjuterski incident uspešno procesuirao.

2.5. Taksonomija kompjuterskog napada

Hakerski napadi dolaze od različitih izvora i od različitog nivoa umeća rada sa kompjuterima, od početnika do kompjuterskog eksperta. Najčešći koraci u izvođenju napada su:

- Upornost – predstavlja napadačevo prepoznavanje žrtve. U ovom koraku, napadač kreira profil organizacione strukture, mrežne mogućnosti, komponente mreža i sigurnosne mere. U trajanju ove faze napadač pronalazi svoje željene ciljeve i smišlja plan za zaobilazanje bezbednosnih mehanizama,
- Penetracija - je sledeći korak u napadu. Njom se obezbeđuje dovoljno podataka da bi se pristupilo meti i ciljanom sistemu. Na primer, ako sistem ima konfiguracionu grešku, i pristup FTP serveru preko protokla TFTP, do pristupa sistema, tada se napad razvija u pravcu korišćenja slabosti u protokolu TFTP,
- Sticanje ovlašćenja - cilj ovog koraka je da se iskoriste konfiguracione greške i propusti za sticanje dodatnih privilegija, kao što je pribavljanje administratorskog naloga,
- Delovanje - kada dobije dovoljan nivo ovlašćenja, napadač ispoljava cilj u vršenju nedozvoljenih radnji. Koristi ih za instalaciju trojanaca, zapisivanja lozinki, brisanja datoteka, ili bilo koje zlonamerno ponašanje koje ima na umu,
- Prikriivanje tragova - pre povlačenja, napadač pokušava da prikrije svoje tragove, brisanjem ili sakrivanjem datoteka koje je ostavio za sobom.

Ispitivanje ovih koraka daje vredne informacije u pronalaženju načina da se zaustavi napad. Oni takođe, pružaju uvid u stvari koje se mogu uraditi za poboljšanje sposobnosti hvatanje napadača koji je probio bezbednosni mehanizam.

2.6. Kompjuterska i mrežna forenzika

Srž delatnosti kompjuterske i mrežne forenzike je prikupljanje dokaza, koji se akumuliraju iz različitih komponenti sistema i služe za pronalaženje tragova o kompjuterskom incidentu. Informacija ne postaje dokaz dok incident nije potvrđen. Iz tog razloga, podaci se prikupljaju sa sistema kao potencijalni dokazi.

Postoji mnogo potencijalnih izvora dokaza u računarima i mrežnim komponentama. Datoteke su očigledan izvor potencijalnih dokaza. Aplikativna dokumenta word, excel, itd. su skoro uvek dragoceni potencijalni dokazi, kao i skrivene aplikacione datoteke koje sadrže informacije o istoriji, kešu, bekapu i *log* datoteka u kojima su upisane promene i događaji na računaru.

Pošto prikupljanje potencijalnih dokaza i pronalaženje aplikacionih datoteka na kompjuteru, nije lako, zahteva se angažovanje stručnjaka koji su posebno obučeni u neophodnim veštinama za uspešno obavljanje forenzičke istage. Forenzički stručnjak mora da ima istražiteljske veštine detektiva, pravne veštine advokata i kompjuterske veštine hakera. Čak i sa ovim veštinama, digitalna forenzika ne garantuje da će forenzički stručnjak naći dovoljno dokaza.

Međutim, iskusni forenzički stručnjaci mogu naći više potencijalnih dokaza nego što najbolji haker očekuje.

Za razliku od klasičnog forenzičkog ciklusa, gde forenzička aktivnost počinje posle učinjenog dela ili kasnije, pošto je delo otkriveno, u digitalnoj forenzici računarskih mreža, forenzičke aktivnosti prikupljanja potencijalnih dokaza počinju pre nego što je

kompjuterski incident učinjen. Po učinjenom incident digitalna forenzika se odnosi na analizu dokaza koji su već prikupljeni.

2.6.1. Pravila za sprovođenje kompjuterske i mrežne forenzike

U korporaciji vršiti sistematsko skladištenje i zadržavanje sadržaja aplikacija i korisničkih datoteka kao potencijalne dokaze, po sledećem:

- na serveru, za korisnike koji su priključeni na domensku računarsku mrežu, prilikom svakog odjavljivanja sa računarske mreže vršenjem sinhronizacije i
- na lokalnim računarima, koji nisu priključeni na računarsku mrežu, pravljenjem rezervnih kopija podataka, u skladu sa Pravilnikom o izradi kopija podataka.

Obrisane, skrivene i šifrovane datoteke, koje se nalaze na računarima su vlasništvo korporacije. Tim za upravljanje kompjuterskim incidentima ima prava pristupa svakoj datoteci u sistemu bez dozvole onoga koji je datoteku kreirao. Korisničke računare konfigurisati na taj način da se vrši praćenje i evidencija sistemskih, aplikacionih i mrežnih informacija, u vidu dnevnika (log) datoteka.

Mrežne uređaje konfigurisati tako da se log datoteke šalju na centralni log server⁵. Oni uređaji koji ne omogućavaju slanje log datoteka, periodično, preuzimati datoteke i skladištiti na centralni log server.

Sistemska vremena na mrežnim uređajima koja imaju tu mogućnost, podesiti po centralnom log server.

Pratiti sledeće mrežne aktivnosti:

- prijavljivanje i odjavljivanje računara sa domenske računarske mreže,

⁵ Pleskonić D., Maček N. Đorđević B. Carić M. *Sigurnost računarskih sistema i mreža, Mikro knjiga, Beograd, 2007.*

- pristup mrežnim servisima (daljinski Telnet, FTP sesija),
- internet servisi (e-mail i web pristup),
- za bežične korisnike, prijavljivanje na pristupnu tačku i dr.

Obezbediti pravljenje vremenske linije, prikupljanjem informacija na navedene načine i informacijama dobijenih od svedoka i fizičkih dokaza. Vršiti analizu TCP/IP paketa i njegovog zaglavlja koji sadrži informacije o izvoru i ciljnom računaru. IP adrese pružaju informacije o identitetu napadača i meti unutar računarske mreže korporacije, Prilikom konfigurisanja rutera i mrežnih barijera, sve odbačene pakete, koji nisu u skladu sa pravilima, preusmeriti na sigurno mesto i voditi evidenciju o njima. Konsultovati tehničku dokumentaciju, pisane instrukcije i priručnike o računarskoj opremi i specifičnim programima.

2.6.2. Planiranje odgovora na kompjuterski incident

Iako se politikom definišu pravila i uputstva za prikupljanje potencijalnih dokaza, usled oklevanja ili neuspeha u otkrivanju dokaza, može se izazvati veća šteta nego da se dogodio kompjuterski incident. Takođe, može se izgubiti prilika da se otkrije počinitelj i povratiti nastala šteta.

Digitalna forenzika zahteva efikasan *plan odgovora na napad*, da se odgovori, *ko, šta, kada i gde*.

2.6.3. Procedure i uputstva za rešavanje kompjuterskog incidenta

Prilikom primena forenzičkih akcija tim za upravljanje kompjuterskim incidentima sprovodi sledeće procedure:

- određivanje tačne prirode kompjuterskog incidenta ili zloupotrebe i dali je u toku ili je završen,
- informacioni sistem sačuvati u zatečenom stanju, odnosno ne činiti izmene koje bi otežale ili onemogućile dijagnostifikovanje,
- pravljenje **dve kopije** oštećenog hard diska, korišćenjem alata za kreiranje forenzičkog imidža diska,
- kopiranje kompjuterskih i mrežnih dnevnika,
- ograničavanje pristupa oštećenom sistemu,
- eliminisanje očiglednosti,
- postavljanje hipoteze o napadu:

Razumevanje kako je napadač izvršio incident, ušao u računarsku mrežu ili računar. Teoretski se analizira napad, mapiranjem svih mogućih vektora napada tj. pristupnih putanja računaru, testiranje hipotetičkih putanja i ACL (lista kontrole pristupa) svih korisnika i administratora koji imaju pristup računaru i mrežnim uređajima u cilju utvrđivanja da li su oni izvršioci napada. U ovom koraku se određuje vreme, datum i okolnosti napada,

- dokumentovanje svake radnje, tako da se ponavljanjem zabeleženih akcija može rekonstruisati tok istrage,
- rekonstruisanje krivičnog dela - vrši se testiranjem uspostavljene hipoteze napada gde se saznaje kojim putem je napadač pristupio sistemu. Upotrebljavaju se forenzički računari za simulaciju sa fizičkom slikom ili imidžom čvrstog diska - HD (bit-po-bit) napadnutog računara, po potrebi mrežni uređaji sa konfiguracionim podešavanjima koji su korišćeni u slučaju incidenta i drugo,
- otkrivanje traga do osumnjičenog računara - traženje logičkih grešaka napadača na log datotekama računara i mrežnih uređaja u cilju utvrđivanja identiteta napadača,
- analiza izvornog, ciljnog i posrednog računara,
- prikupljanje dokaza, markiranje, obeležavanje i pakovanje fizičkih dokaznih materijala,

- šifrovanje datoteka digitalnih dokaza PKI sistemom koji se koristi za zaštitu od izmena, primenom *hash* programa (SHA-256, SHA-512 i sl.)
- obezbeđenje dokaza o vremenskoj liniji incidenta,
- izrada izveštaja o istrazi, koji sadrži:
 - kratak sadržaj incidenta (opis incidenta),
 - metod istraživanja,
 - generalni zaključci po redosledu izvedenih dokaza,
 - opis navedenih zaključaka sa ukazivanjem na čvrste dokaze,
 - preporuka o sprečavanju ponavljanja incidenta,
 - predlog za dalji postupak.

Izveštaji o incidentu su poverljiva dokumenta i čuvaju se na taj način da im pristup imaju samo ovlašćene osobe.

Korporacija može objavljivati statističke podatke o sigurnosnim incidentima, bez otkrivanja poverljivih i personalnih informacija.

2.6.4. Obuka

Tim za upravljanje kompjuterskim incidentima treba biti uvežban za donošenje raznih odluka koje treba sprovoditi. Potrebno je pratiti i predviđati moguće kompjuterske incidente i davati rešenja za sprečavanje.

Timu treba izgraditi veštine da identifikuje da li se kompjuterski incident dogodio ili ne, a u slučaju da jeste, način na koji je učinjen, ko je izvršio incident i naći dokaze koje je ostavio.

Digitalnog forenzičara obučiti za:

- računarsku i mrežnu administraciju koja se koristi u korporaciji,

- generičke ranjivosti svih sistema koji su na upotrebi u korporaciji,
- hakerske tehnike udaljenog pristupa i
- legalno prikupljanje digitalnih dokaza, koji se koriste na sudu, čime se nesumnjivo potvrđuje da dokaz sadrži informaciju o učinjenom incidentu i da je legalno prikupljen.

2.6.5. Ubrzanje istrage

Forenzičku istragu zaključiti što je brže moguće. Istraga ometa korporacijske aktivnosti, naročito po pitanju korišćenja opreme koja neće biti dostupna za upotrebu. Pored toga, duga istraga, daje veće šanse da potencijalni dokazi budu uništeni ili ugroženi. Šteta učinjena incidentom treba da se ispravi što je pre moguće, omogućiti oporavak svega što je izgubljeno i spreči buduće napade.

Prilikom rada sa log datotekama, koje su uskladištene na centralnom log serveru, koristiti indeksiranje podataka i po potrebi vršiti upoređivanje sa originalnim informacijama.

Digitalne dokaze kao što su dnevničke (log) datoteke, IDPS (*Intrusion Detection and Prevention Systems*) izlazi, kao i indeksi podataka, treba:

- šifrovati i zaštititi sa jakom autentifikacijom
- imati jaku proveru identiteta i integriteta administrativnog pristupa mrežnim uređajima i
- periodično (na 10 dana) proveravati integritet prikupljenih podataka.

2.6.6. Sankcije

U glavom tekstu predloga sigurnosne politike, korisnicima je zabranjeno da instaliraju programe, bez odobrenja administratora računara, što uslovljava da se usled pojavljivanja drugih programa, zaposleni pozove na odgovornost.

Svrha istrage je da se odredi uzrok nastanka problema i da se iz toga izvuku zaključci o tome kako sprečiti ponavljanje incidenta, ili se barem bolje pripremiti za slične situacije.

Ako je uzrok sigurnosnom incidentu bila greška čoveka, protiv odgovornih se mogu preduzeti sankcije. Korporacija može osobama odgovornim za sigurnosni incident zabraniti fizički pristup prostorijama ili logički pristup podacima. Ukoliko je incident izazvao zaposleni spoljne firme, korporacija može zatražiti od nje da ga ukloni sa liste osoba ovlašćenih za obavljanje posla u korporaciji. U slučaju teže povrede pravila sigurnosne politike, korporacija može pokrenuti krivični postupak.

2.7 Zvanična istraga kompjuterskog kriminala

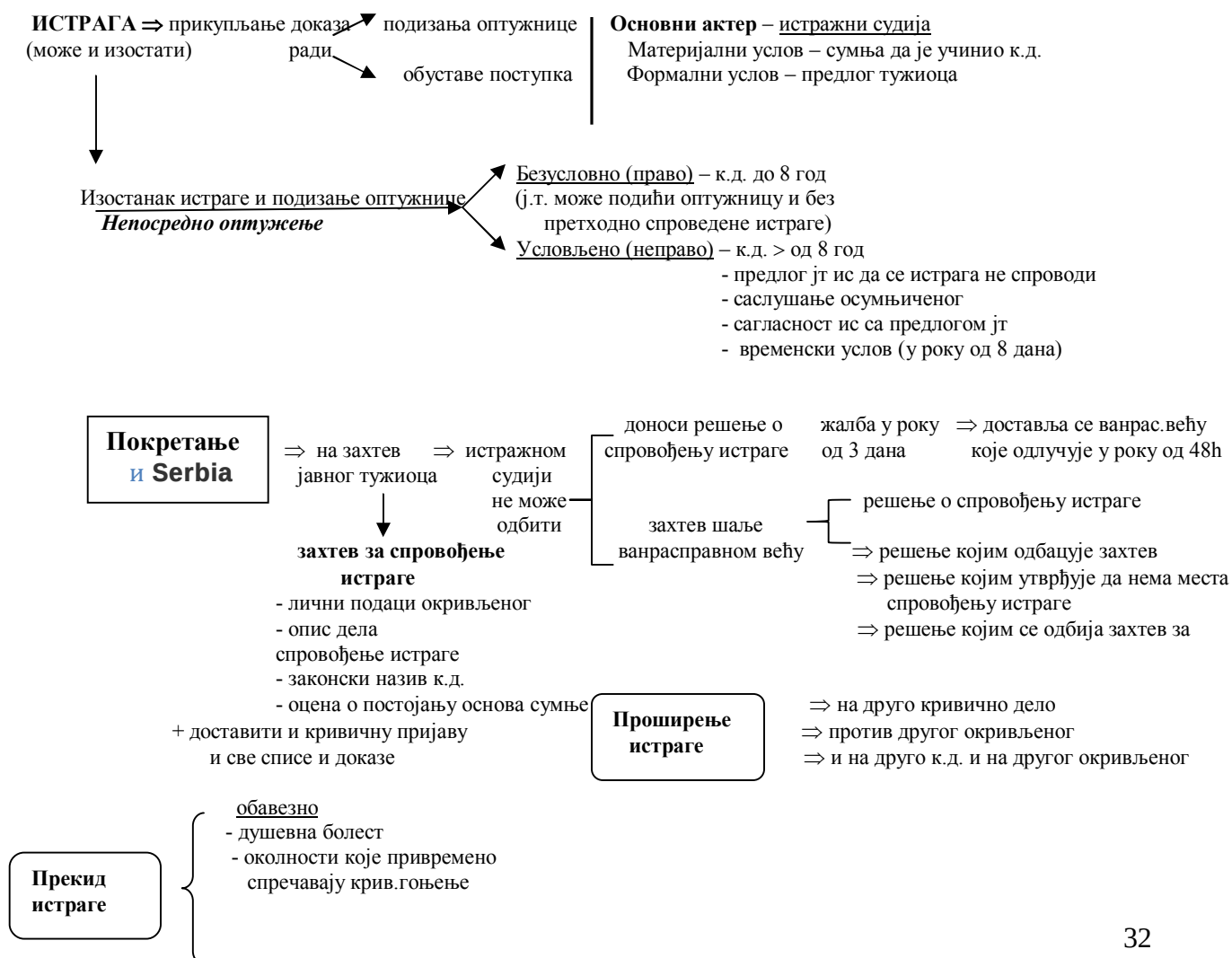
2.7.1. Uvod

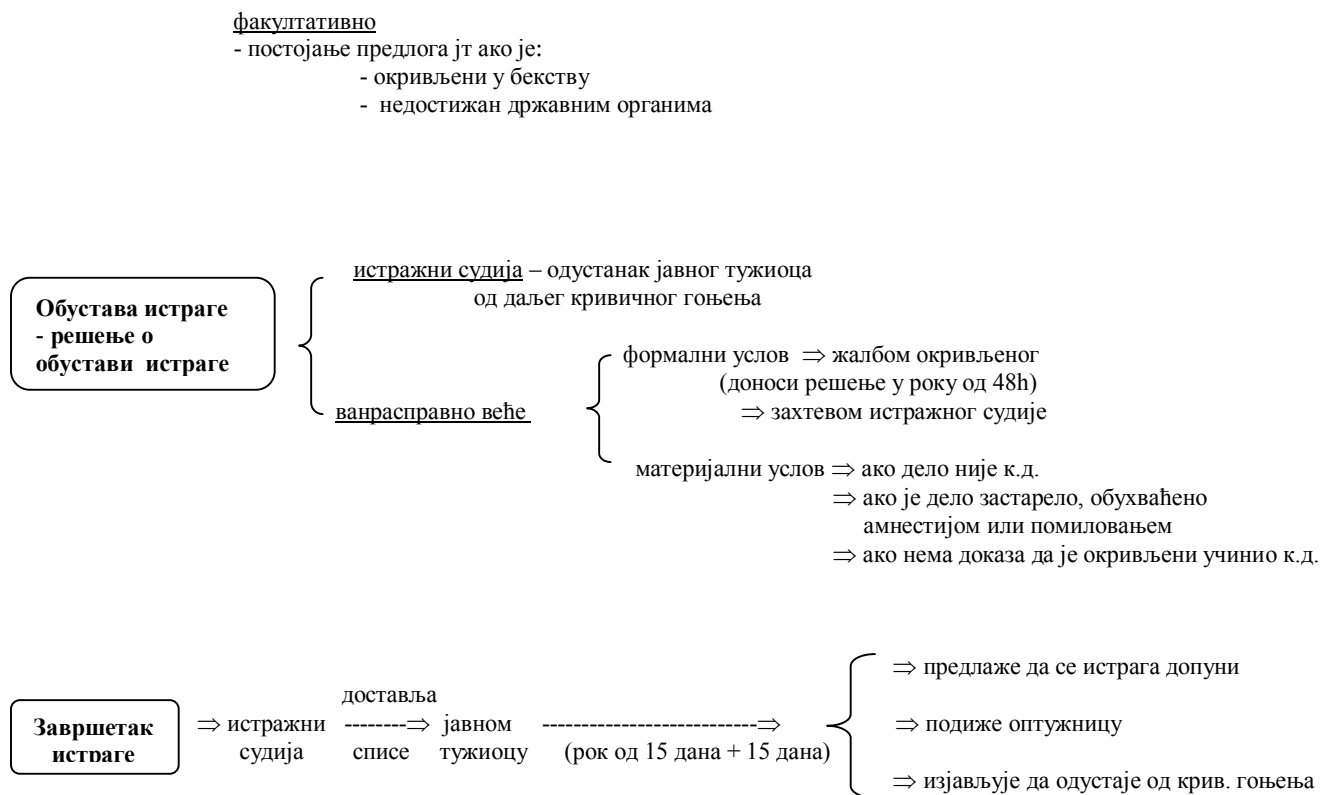
Najveći deo digitalne forenzike odnosi se na forenziku računarskih sistema, ili kompjutersku forenziku, bilo da su računari samostalni ili umreženi. Digitalna forenzika računarskog sistema obuhvata naučno ispitivanje i analizu podataka iz čvrstih diskova (HD), fajl sistema i drugih medija i prostora za skladištenje podataka u računarskom sistemu, tako da se podaci mogu koristiti kao čvrsti i neoborivi dokazi pred sudom.

Digitalna forenzika računarskog sistema razlikuje se od procesa oporavka podataka, slučajno izgubljenih ili izbrisanih. Digitalna forenzika oporavlja podatke, koje je korisnik namerno sakrio ili izbrisao, sa ciljem da obezbedi validnost oporavljenih podataka za dokaze pred sudom. Digitalni dokazi mogu biti optužujući, oslobađajući, ili da ukazuju na osnovanu sumnju. Forenzičar mora ispitivati čvrsti disk (HD) i sve druge sekundarne medije za skladištenje i iz obimnih digitalnih podataka izvući relevantne i održive dokaze. Takođe, procedure upravljanja i oporavka podataka posle destruktivnog vanrednog događaja treba da koriste tehnike i alate digitalne forenzike za izvlačenje izgubljenih podataka iz računara.

Funkcija digitalne forenzičke istrage, čini stabilnu celinu u ranjivom mrežnom okruženju sa implementiranim sistemom zaštite i uspostavljenim kapacitetima za upravljanje kompjuterskim incidentom. Iako sve tri grupe specijalista u velikim sistemima najčešće rade samostalno, u slučaju glavnog kompjuterskog incidenta sve tri grupe uvek rade zajedno. Ovakav koraborativni rad obezbeđuje saniranje kompjuterskog incidenta u organizaciji sa sopstvenim resursima i bez pozivanja spoljnih specijalista. Specijalisti za sisteme zaštite, analizu rizika i ranjivosti imaju iskustvo iz administracije sistema i poznaju neku metodologiju za analizu i ublažavanje rizika.

Na slici 5, prikazan je scenario jedne istrage koja treba da se sprovede po zakonu države Srbije.





Slika 5. Tok istrage

2.7.2. Zvanična istraga incidenta

Zvanična istraga uključuje policijske organe istrage, specijalno tužilaštvo i specijalno sudstvo za borbu protiv visokotehnološkog (kompjuterskog) kriminala. Ovi organi rade prema *Zakonu o krivičnom postupku*, *Zakonu o borbi protiv visokotehnološkog kriminala* i strogo utvrđenim procedurama za pretragu, privremeno oduzimanje i ispitivanje računarskih sistema i drugih mrežnih uređaja, u cilju otkrivanja validnih digitalnih dokaza. U slučaju zvanične istrage istražni organi moraju dobro poznavati i razumeti zakon i propise koji se odnose na kompjuterski kriminal, uključujući standardne lokalne procedure za pretragu i utvrđivanje slučaja kriminalnog dela.

U procesu utvrđivanja karaktera krivičnog dela kompjuterskog kriminala, istražni organ mora tražiti odgovore na brojna pitanja, kao što su:

- Šta je bilo sredstvo izvršavanja krivičnog dela?
- Da li su računarski sistem i mreža poslužili kao jednostavan prolaz za izvršavanje krivičnog dela?
- Da li je u pitanju krađa, provala ili vandalizam u sistemu?
- Da li je napadač ugrozio nečiju privatnost i druga prava, ili uznemiravao preko *Voice IP* ili *e-mail* servisa?

Računarski sistem i računarska mreža mogu biti sredstva za izvršavanje krivičnog dela i u tom smislu ne razlikuju se od pajsera provalnika za upad u tuđi stan, ili kalauza kradljivca kola. Računarski sistemi su kao sredstvo za izvršavanje krivičnog dela, ili predmet krivičnog dela, uključeni u brojne i ozbiljne zločine.

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

- postojanje slučaja izvršenja krivičnog dela,
- istraga krivičnog dela kompjuterskog kriminala i
- suđenje.
-

Opšti proces zvanične istrage kompjuterskog incidenta, sa pristupom istrazi po modelu “korak po korak”, gde svaki korak u okviru jedne faze istrage vodi u drugi i obezbeđuje kontrolnu listu aktivnosti u okviru svake od sledeće 4 faze, [4]:

1. inicijalna istraga,
2. ulazak u trag napadaču,
3. otkrivanje identiteta napadača i
4. hapšenje.

Iako policija svake države štiti javna dobra svojih građana, ne treba očekivati da svaki policajac bude IKT ekspert. U tom smislu uspostavljena su tri nivo potrebne stručnosti zvaničnih organa istrage, [3]:

1. Nivo: Osposobljenost za akviziciju digitalnih podataka i privremeno održavanje digitalnih dokaza.

2. Nivo: Osposobljenost za upravljanje procesom istrage visokotehnološkog kriminala. Organi istrage se osposobljavaju da postavljaju pitanja, razumeju IKT terminologiju i šta može, a šta ne može biti izvučeno iz digitalnih podataka.

3. Nivo: Specijalno obučeni policajci za izvlačenje, ispitivanje i analizu digitalnih dokaza, koje normalno izvršavaju specijalisti za digitalnu forenzičku analizu računara i računarskih mreža, ili istragu kompjuterskih i Internet prevara. Zvanični organi istrage osposobljeni na ovom nivou upravljaju slučajem krivičnog dela kompjuterskog kriminala, uspešno obezbeđuju reusurse za istragu, procenjuju obim istrage, delegiraju uloge i lica za sakupljanje i procesiranje informacija koje se odnose na osumnjičenog, kao i za akviziciju i analizu digitalnih podataka i izgradnju čvrstih dokaza.

Istražitelja kompjuterskog kriminala, pre privremenog oduzimanja računarskog sistema, dostavlja preliminarne dokaze o osnovanoj sumnji tužiocu za visokotehnološki kriminal i zahteva nalog za pretragu. Specijalni tužilac za visokotehnološki kriminal podnosi specijalnom sudiji za visokotehnološki kriminal zahtev za nalog za pretres imovine osumnjičenog u kojem iznosi poznate činjenice iz predistražnog postupka i prilaže raspoložive dokaze o počinjenom krivičnom delu. Na osnovu ovog zahteva i dokaza o osnovanoj sumnji, specijalni sudija za visokotehnološki kriminal izdaje nalog za pretres stana i računarskog sistema osumnjičenog.

Sa legalnog, tehničkog i etičkog aspekta ovo pitanje je veoma kompleksno. Napadači ostavljaju razne zamke koje se aktiviraju u neodređeno vreme. Da bi se analizirale mogućnosti i odredile procedure istrage aktivnog incidenta pretpostavlja se scenario u kome je napadač još na mreži, u mreži je aktiviran *ISS skener* i forenzički alat *SafeSuite* na web lokaciji provajdera.

Napadači na IKT sistem, odnosno računarsku mrežu ili pojedinačan računar, nakon prvog upada, najčešće ostavljaju razne zamke (zadnja vrata, trojance), a stvarnu štetu u napadnutom računaru nanose kasnije bez vidljivih tragova. Različite su aktivnosti u slučaju otkrivanja napada napadača, a primenjuju se odgovarajuće mrežne tehnike za postavljanje zamki za hvatanje napadača, ulazak u trag i praćenje traga napadača. U slučaju *on-line* napada moguće su situacije da je:

- napadač još uvek na mreži,
- u toku direktan napad preko modema i
- u toku *dial-up* napad preko telefonske mreže.

Za simulaciju reagovanja na slučaj napada na IKT sistem u kojem je napadač još uvek na mreži, aktivirani su *ISS skener*, programski alat *SafeSuite*, prema lokaciji Internet servis provajdera (ISP) koji prodaje prostor za postavljanje web stranica. Izvršeno je ispitivanje otpornosti sistema zaštite, aktiviranjem simulacije klasičnog hakerskog napada i napada struktuiranim simulatorom raznovrsnih napada.

Normalno je, da dobro zaštićena mreža ima *firewall* zaštitu od raznih napada sa Interneta. Ovaj tip zaštite ima odvojen DNS (*Domain Name Server*) sa ograničenim informacijama za posetioce izvan sistema. Namena servera je da onemogući napadaču izvan sistema da pronađe hostove (serve) koji su unutar sistema i da onemogući pokušaj postavljanja zadnjih vrata, koja bi im omogućila uspešno zaobilaženje *firewall*-a. Međutim, imena hostova su prisutna u drugim, skrivenim delovima razdvojnog DNS, pa je hakeru potrebno samo da zna kako da ih pronađe. Naravno, na mreži bez *firewall*

zaštite dostupan alat obezbeđuje kompletnu listu hostova i PC-a u mreži, internoj za kompaniju, ali eksternoj za javno korišćenje.

Sa ovom listom u posedu lako je njuškati po računarima u potrazi za lozinkom u nekom od njih. Ako se uspešno krekuje pasvord (lozinka), pogotovo onih računara koji su namenjeni da budu unutar mreže i koji imaju manje robustan sistem zaštite od onih za javni pristup, lako je videti konfiguraciju servera, što je otvoren poziv za napad. Ako napadač ne uspe krekovati pasvord, taj klijent je bezbedan za rad na web-u.

U simulacionom testu lako je unutar mreže otkriven PC sa Win 95 OS. PC je bio logovan na mrežu preko Telnet servisa, koji dopušta pristup sa pasvordom gost. Na prvi pokušaj pogađanja pasvorda sledilo je pitanje "Ko ste vi". Ono što je sledilo ilustruje primer hvatanja napadača u toku napada. Iako ovo nije jedini, pa čak ni najbolji primer, ipak, na odgovor da je u pitanju test i kontrola otpornosti sistema zaštite, vlasnik računara nije proverio da li je to tačno, što je bila velika greška. Drugim rečima, ako se uspostavi kontakt sa napadačem u toku napada i ako se ovaj predstavi, odmah treba preduzeti akciju za proveru njegovog identiteta.

Napadač na liniji predstavlja specijalni tip pretnje. On zna da je otkriven, ali i da je računar koji mu je dopustio pristup - ranjiv. Od tog trenutka vlasnik računara treba da preduzme hitne mere. Mora saznati kako je napadač ušao u sistem. Ako je u pitanju PC sa *Windows* OS, lako je utvrditi upad sa korišćenjem naloga gosta. Ako je u pitanju Unix platforma host računara, treba nekoliko neposrednih koraka da se otkrije šta se dešava. Napadi koji dolaze sa *dial-up* veze (telefona) mogu biti lakši za otkrivanje.

Postoje dva osnovna napada direktnim biranjem telefona:

- direktan napad na računar i
- napad na sistem centrale.

Interesantno je koliko slabo u praksi sistem administratori zaštićuju direktno vezane modeme na kritičnim hostovima.

U slučaju nezaštićenog modema na Unix mašini, moguće je setovati *com port* sa modemom za automatski odgovor. Iste mogućnosti imaju Windows OS. Postoji mnogo programa za udaljeni pristupa, kao što su: *PCAnywhere*, *LapLink*, *ReachOut* i stari *CarbonCopy*. Svi ovi programi imaju ograničenu zaštitu pasvordom. Kada je napadač jednom izabrao vaš broj i nalazi se na liniji i u računaru, jedina je mogućnost da mu se uđe u trag, angažovanje telefonske kompanije, što podrazumeva uključivanje zvaničnih organa istrage. Tu se mnoge organizacije prelome i prestanu tragati za napadačem. U tom trenutku treba pratiti aktivnosti napadača u internoj mreži. Omiljen trik napadača je postavljanje *snifera* i kupljenje pasvorda. Potrebno je odrediti koji nalog je napadač ukrao i upao u telefonski sistem. Zatim treba pratiti trag napadača u mreži i otkriti šta radi. Ovaj proces je uporno proveravanje više log fajlova u serverima mreže.

Neki tipovi softvera za daljinski pristup zahtevaju da host PC bude logovan na lokalnu mrežu (LAN) da bi dopustio legitimnim učesnicima pristup LANu. Kada već dobije pristup PCu, napadač može lutati po LANu kao legalni PC korisnik. Ovde log podaci mogu biti od slabe koristi, jer su podaci o legitimnim korisnicima pomešani sa maskiranim napadačima.

Ako je napadnuti računar imao aktiviran sistem logovanja, može se uz pomoć vlasnika računara odrediti kada se neovlašćeni napad dogodio i koristiti to kao početnu tačku traganja za akcijama napadača. Iako ova potraga liči na traženje igle u plastu sena, forenzički alati nude moguća rešenja. To su alati za otkrivanje podataka u skrivenim zonama HD (*slack* i nealocirani prostori klastera, *swap* fajlovi). Može se desiti da ime ili adresa napadača ostane zapisana u ovim zonama. Moguće je, takođe, da se cela *ekskurzija* napadača kroz mrežu pojavi na udaljenom računaru kroz kojeg je

napadač pristupio u mrežu (prvo birao telefonom). Ako se napravi mirror slika tog računara i analizira, tu je sve što je potrebno za otkrivanje traga napadača u mreži. Čak i kada napadač više nije na mreži, moguće mu je postaviti zamku u slučaju sledećeg napada.

U osnovi postoje tri mogućnosti kada se otkrije napadač na linji:

- zadržati ga dovoljno dugo za postavljanje zamke i praćenje traga,
- prekinuti vezu, u kom slučaju treba očekivati da se napadač vrati i
- učiniti nešto da se napadač uplaši i više nikada ne vrati natrag.

Ako se donese odluka za postavljanje zamke i praćenje traga napadača, kako će se to uraditi zavisi od toga kako je napadač priključen. Ako napadač dolazi sa Interneta ili spoljne RM, potrebna je saradnja sa administratorima duž puta kretanja napadača, a ako napadač dolazi preko telefonske linije, potrebna je saradnja sa telefonskom kompanijom.

U traganju za odgovor odakle dolazi napadač, treba početi gledanjem ko je na liniji sa akcijama koje odgovaraju korišćenoj platformi (Unix, Windows, Sun, ... OS), kojom se dobiju liste sa informacijama o izvoru napada (IP adrese ili puno ime domena lokacije napadača). Ne treba se previše uzбудiti jer to verovatno nije stvarno ime napadača, nego samo lokacija na kojoj je ukrao nalog. Taj podatak treba zapisati i zabeležiti sistemsko vreme na napadnutom računaru.

Sada je potrebno videti šta napadač radi. Posmatranjem tekućih procesa (u *Task manageru* kod Windows OS). Treba gledati sve procese koje nije moguće objasniti. Proces u kojem se sumnja da je napadač u toku treba notirati.

Posebno treba usmeriti pažnju na skenere (*snifere*), omiljeno sredstvo hakera za traženje pasvorda. Vešti hakeri obično preimenuju *snifer*, multipliciranjem instanci *daemon* ili servisa. Za mnogo više informacija o tome odakle dolazi napadač moraju se primeniti čisto hakerske tehnike sa puno veštine, brzine i pogađanja, zavisno od toga šta se vidi, kao u borbi dva iskusna hakera.

Zatim se može pokušati saznati nešto o sajtu sa koga je napad došao, ako ne o samom napadaču, ono o nalogu kojeg je ukrao. Odgovarajućim komandama (zavisno od platforme) saznaje se ko je izvorna lokacija, ime i broj telefona administratora lokacije. Može se saznati nešto o ukradenom nalogu sa te lokacije. Ne treba biti iznenađen ako pripada samom administratoru te web lokacije. Ako je administrator kooperativan i sa ovim informacijama može se početi traganje za napadačem unatrag.

Ako je moguće treba izvršiti svaki *online* zadatak sa drugog računara, da se izbegne skretanje pažnje na forenzičarske aktivnosti. Ceo ovaj postupak ne sme da traje više od par minuta. Sve akcije treba zabeležiti, vremena, adrese, korisnička imena i drugo. Međutim postoji čitav skup okolnosti vezanih za napad sa telefonske linije umesto preko Interneta. Za ove aktivnosti potrebno je saradnja i odobrenje nadležnih zvaničnih organa. Generalno svako postavljanje zamke napadaču podleže zakonu o prisluškivanju linija. Kako se *e-mail* smatra "tranzitom" podataka po žici, to i snifovanje e-pošte pripada tom zakonu.

Ako napadnuti IKT sistem ima sistem zaštite koji neprekidno skenira mrežni saobraćaj i skuplja informacije o normalnim aktivnostima, a posebno o neregularnostima, šanse za ulazak u trag napadaču su znatno veće. Ako se ignoriše otkriveni napadača na liniji, posledice mogu biti oštećenja sistema. Drugo, napadač može iskoristiti neki sistem za novi napad u ili izvan tog sistema, što može naneti i druge vrste štete. Uplašiti se i pobeći potpuno je amaterski. Iskusan napadač može otići, ako mu se administrator suprotstavi, ali se sigurno vraća. Ne preporučuje se ulazak u dijalog sa napadačem. To je gubljenje vremena i ništa se ne postiže.

Zamke (zadnja vrata, trojanci) su mehanizam koji hakeri ostavljaju na napadnutom računaru, a koja im omogućavaju kasniji povratak, bez ponavljanja kompromitacije računara. Ideja je da se postavi na nekoj ulaznoj tački u kompromitovani računar, tako da ne bude otkrivena i odstranjena od strane administratora. Ako administrator otkrije metod originalnog upada, može zatvoriti *rupu* i sprečiti upad napadača. Međutim, dobro skrivanje zamke je izbor napadača. Ovaj mehanizam omogućava napadaču da se bezbrižno vrati kasnije i završi napad, posebno kada je otkriven na liniji [3].

Potrebno je pratiti razvoj i upoznati se sa brojnim malicioznim metodama i tehnikama hakera za postavljanje zamki, kao i osposobiti administratore da razumeju kako da spreče napadače da se vrate u kompromitovani sistem.

Zamke za većinu napadača obezbeđuju:

- povratak u mašinu čak i kada administrator pokuša da je obezbedi, na primer promenom svih pasvorda,
- nevidljiv povratak, jer većina zamki izbegava logovanje, pa mnogo puta izgleda da nema nikoga na liniji čak i kada je napadač koristi i
- povratak u mašinu u najkraćem vremenu.

2.7.3. Metode i tehnike istrage

Sa aspekta teorije istrage, konsultovana je brojna literatura za fizičku istragu mesta krivičnog dela [2]. Faze fizičke istrage mesta krivičnog dela su:

- **Očuvanje, fiksiranje mesta krivičnog dela:** prvi korak je da se pomogne povređenima, zatim sledi potraga za osumnjičenima i hapšenje osumnjičenih i zadržavanje svih svedoka. Fizičko mesto krivičnog dela mora biti osigurano, a pristup omogućen samo ovlašćenim licima, istražnim organima, (kriminalistički inspektor, sudski istražitelj, forenzičar sudske medicine i.t.d.).

- **Pretraga mesta krivičnog dela:** organ istrage pažljivo pretražuje mesto krivičnog dela da bi identifikovao očigledne delove dokaza i kratkotrajne dokaze (krv, sluz, sperma, pljuvačka i.t.d.). Početna opažanja tipa *ko, šta, gde, kada, kako* dokumentuju se i kreira se početna teorija - *hipoteza slučaja*.
- **Dokumentovanje mesta krivičnog dela:** mesto krivičnog dela dokumentuje se fotografisanjem, skiciranjem i snimanjem digitalnog video snimka. Dokaze treba jednoznačno označiti, dokumentovati jasno, potpuno i sakupljati ih za analizu.
- **Istraga mesta krivičnog dela:** brojni obrasci istrage koriste se da bi se identifikovali dodatni dokazi koji nisu otkriveni u predistažnom postupku (pretrazi). Teorija razvijena u pretrazi koristi se za istragu specifičnih dokaza koji nedostaju (npr., oružje kojim je počinjeno ubistvo).
- **Rekonstrukcija krivičnog dela:** događaji koji su se dogodili na mestu krivičnog dela određuju se na osnovu izgleda mesta krivičnog dela, mesta i pozicije fizičkih dokaza, analiziranih rezultata iz forenzičke laboratorije i naučnih metoda primenjenih u istrazi i analizi dokaza.

Ovaj model omogućava kompletnu dokumentaciju mesta zločina i koristi iskustvo istražnog organa da bi se došlo do korisnih dokaza. Svi fizički predmeti ne mogu da se uzmu sa mesta krivičnog dela, tako da *Faza Istrage mesta krivičnog dela* mora biti potpuna da bi se sakupili potrebni dokazi, ali ne sme se preoptereti laboratorija sa predmetima koji nemaju veze sa slučajem.

U SAD “*Department of Justice*” objavio je model procesa istrage u “*Vodiču za istragu elektronske scene zločina*”. Vodič potpuno odgovara istrazi fizičkog mesta krivičnog dela, tako da je akcenat stavljen na zahteve istrage klasičnog kriminala, a malo pažnje se obraća na forenzičku analizu digitalnih sistema. Faze modela su sledeće [1]:

- **Priprema:** pripremiti opremu i alat potreban za istragu;

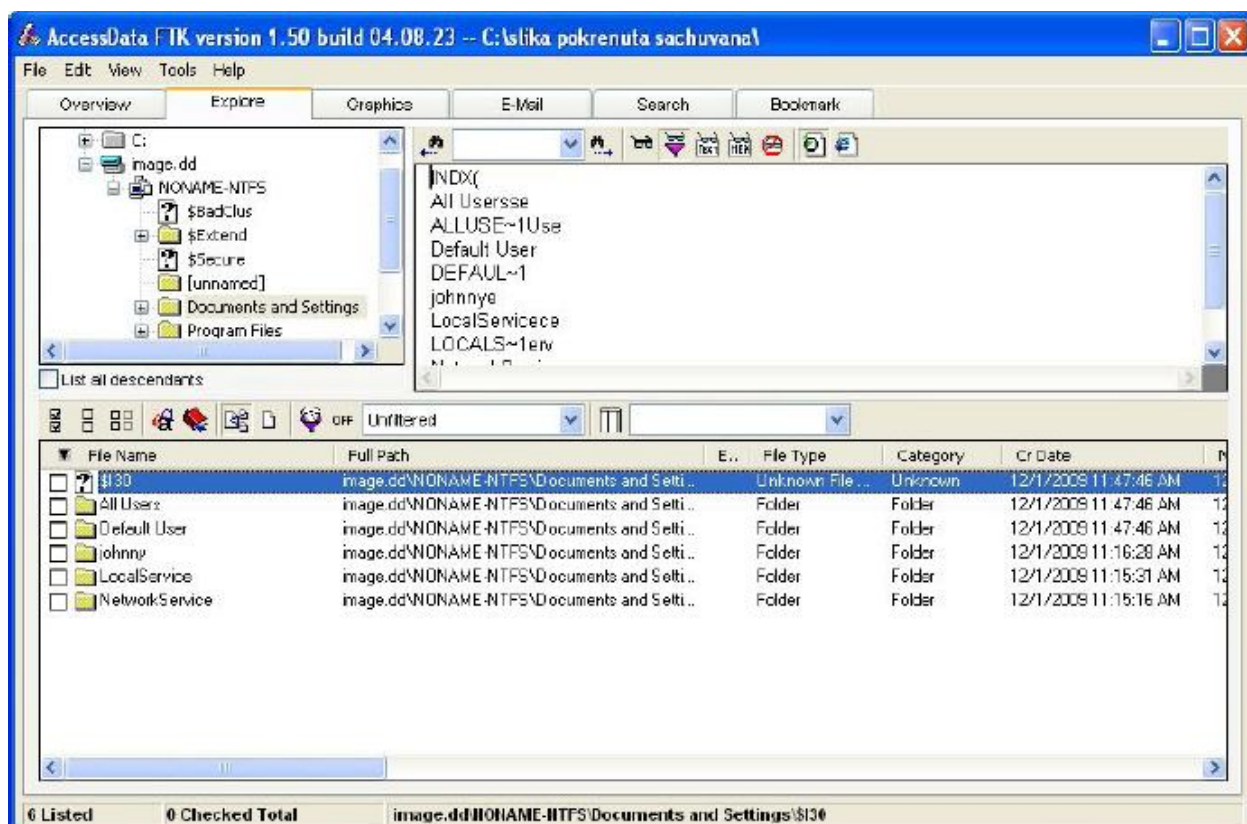
- **Sakupljanje:** naći i sakupiti elektronske (digitalne) dokaze;
- *Osigurati i proceniti mesto krivičnog dela:* obezbediti mesto krivičnog dela radi bezbednosti lica i integriteta podataka i identifikovati potencijalne dokaze;
- *Dokumentovati mesto krivičnog dela:* dokumentovati fizički opis mesta krivičnog dela uključujući fotografije računarskog sistema;
- *Sakupiti dokaze:* alatima za forenzičku akviziciju izvući podatke iz računara, privremeno oduzeti fizički računarski sistem, ili napraviti fizičku (*mirror*) kopiju podataka na forenzičkom računarskom sistemu;
- **Pregled/pretraga:** tehnički pregled i ispitivanje sistema radi nalaženja potencijalnih dokaza;
- **Analiza:** digitalna forenzička analiza hardverskim i/ili softverskim alatima računarskog sistema, digitalnih podataka, memorijskih medijuma; analiza rezultate tehničkog pregleda i drugog dokaznog materijala radi procene njihove važnosti za slučaj;
- **Izveštaj:** izveštaj se pravi posle svakog slučaja kompjuterskog (incidenta) kriminala.

Za opremanje digitalne forenzičke laboratorije treba odrediti koji su alati najfleksibilniji, najpouzdaniji i najrentabilniji za obavljanje posla. Tako softverski alati moraju biti kompatibilni najmanje sa sledećom generacijom OS. Na primer, uvođenjem NTFS fajl sistema u Windows NT OS, forenzičari su imali velike probleme. Proizvođači forenzičkih softverskih alata morali su revidirati svoje alate za analizu novog fajl sistema⁶.

Mnoštvo laboratorijskih alata je na raspolaganju forenzičaru, a koje će da upotrebi često zavisi od specifične prirode slučaja. Jedan od kompletnih alata za digitalnu forenzičku istragu je i *Forensic Toolkit*. Ova platforma nam omogućava kreiranje slika, analizu registra, dešifrovanje datoteka, razbijanje lozinki, identifikaciju steganografije i još mnogo drugih opcija. Između ostalog *FTK* nam omogućava da iz sačuvanih *dd* slika

⁶ Milosavljević M., Grubor G., *Digitalna forenzika računarskog sistema*, Univerzitet Singidunum, Beograd, 2009.

izvučemo dosta više informacija koje, čak i da sedimo ispred kompjutera koji ispituje, su sakrivene za regularnog korisnika.



Slika 6. Kopija čvrstog diska pokrenuta kao dokaz unutar FTK-a

Na slici 6. je prikazan tipčan izgled *FTK* programa, nakon što je digitalni otisak *image.dd* učitao kao dokaz. Značaj unikatne identifikacije digitalnog dokaza je u direktnoj vezi sa dokumentovanjem akcija nkoje je forezničar preduzeo pri prikupljanju digitalnog dokaza. Jedan od načina, *de facto* standard za identifikaciju datoteka je primena kriptografskog MD5 heš algoritma. Algoritam se zasniva na principu generisanja 128-bitne heš vrednosti izračunate na osnovu kompletnog sadržaja, i obično se prikazuje kao 32 heksadecimalna karaktera. Neki od drugih algoritama, koji služe istoj svrsi je i SHA-1 algoritam. Prednost ovih algoritama je osobina da se pri promeni i samo jednog bita programskog koda, MD5 heš vrednost te datoteke potpuno menja

Uspostavljanje i održavanje digitalne forenzičke laboratorije uključuje formiranje softverske biblioteke – repozitorijum, koji sadrži starije verzije forenzičkih alata, OS i drugih programa kao što su stare verzije Windows i Linux OS. Ako nova verzija forenzičkog softvera fiksira jedan bag, ali unese drugi, forenzičar može koristiti prethodnu fiksiranu verziju.

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

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

Za nabavku forenzičkog softvera potrebno je evaluirati karakteristike potencijalnih alata kao što su:

- OS na kojem forenzički alat radi,
- mogućnost rada verzije alata na jednom ili više OS i da li proizvode iste rezultate u višenamenskom radu,

- mogućnost analize više fajl sistema kao što su FAT, NTFS, Ex2fs,
- mogućnost korišćenja nekog programskog alata za automatizaciju funkcija i zadataka koji se u alatu ponavljaju,
- mogućnost automatizovanog obavljanja nekih funkcija, koje mogu smanjiti vreme analize podataka,
- Reputacija proizvođača alata i dr.

2.7.4. Alati

Akvizicija digitalnih podataka prvi je zadatak u forenzičkoj istrazi računara i podrazumeva pravljenje fizičke kopije bit-po-bit originalnog (osumnjičenog, ispitivanog) diska računara. Ova procedura sprečava korupciju i oštećenje digitalnih podataka na originalnom disku. Akvizicija digitalnih podataka obuhvata 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 forenzički alati. Primeri hardverskih alata za uzimanje fizičke slike računara su: **Image MaSster Solo 2 Forensic** komponenta sa *firmware* programom (*Intelligence Computer Solutions Inc.*) koji može samostalno kopirati podatke sa originalnog na forenzički disk. Druge aplikacije za akviziciju digitalnih podataka zahtevaju kombinaciju hardverskih i softverskih komponenti. Na primer, **EnCase** alat ima za akviziciju digitalnih podataka DOS program *En.exe* i jednu funkciju u svojoj GUI Windows aplikaciji. Za akviziciju podataka sa *En.exe* programom zahteva se da računar radi sa MS-DOS operativnim sistemom (OS), ima 12 V konektor za napajanje, IDE ili SCSI kabl za

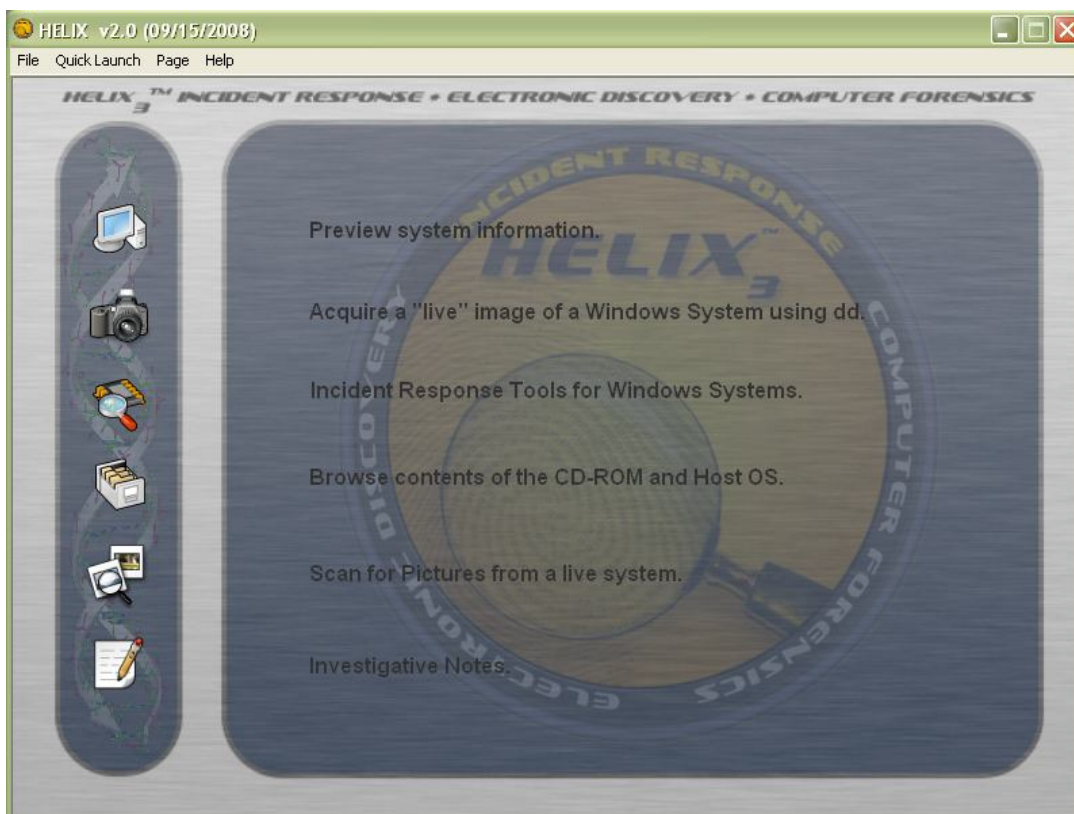
povezivanje. Windows aplikacija *EnCase* alata zahteva upotrebu blokatora upisivanja podataka na originalni disk, kao što je *FastBloc* za sprečavanje Windows OS da pristupi i korumpira originalni disk.

U procesu akvizicije podataka softverskim alatima postoje dva metoda kopiranja:

- fizičko kopiranje celog fizičkog diska i
- logičko kopiranje particija diska.
- Većina softverskih alata za akviziciju uključuje jednu ili obe ove funkcije. Formati koji su na raspolaganju za akviziciju diskova variraju od potpuno sirovih podataka u binarnom zapisu do kompresovanih podataka specifičnih za proizvode. Sirovi podaci su direktna kopija diska. Primer imidža sirovih podataka je izlaz UNIX i Linux šel **dd** komandne linije. Primer formata sirovih podataka je jednostavna bit-po-bit kopija fajla podataka, particije diska, ili celog diska. Alat za akviziciju sirovih podataka može kopirati podatke sa jednog diska na drugi disk, ili u jedan ili više segmentiranih fajlova podataka. Pošto je ovo zaista neizmenjena kopija, forenzičar može gledati sadržaj sirovih podataka imidža fajla sa heksadecimalnim editorom, kao što su *WinHex editor*, *X-Ways Forensic*, *I Look*, ***Helix***, *Katana* itd., a sadrže ga gotovo svi forenzički alati.

2.7.5. Helix2008R1

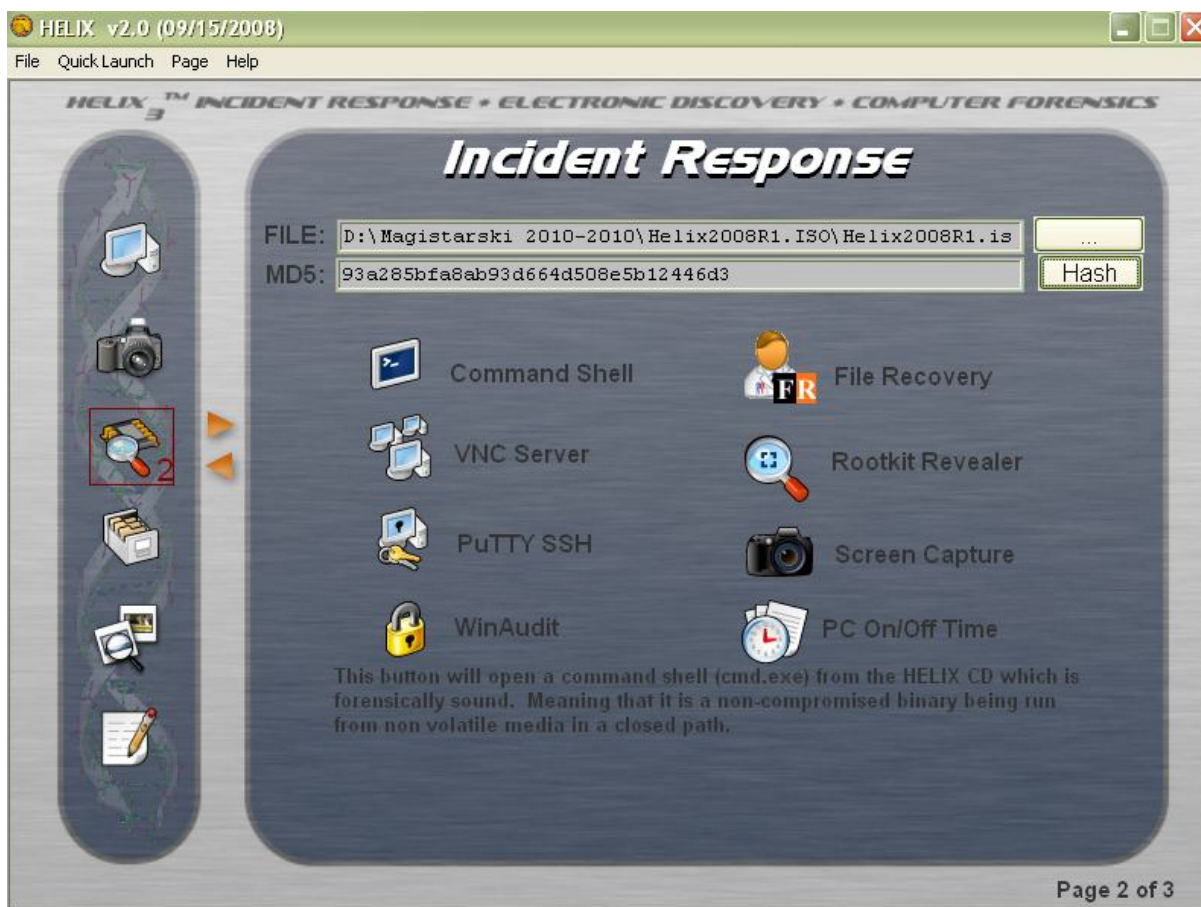
Heliks je veoma moćan alat. Ali sa velikom moći dolazi velika odgovornost, i kao potencijalni forenzika istraživači, naša je odgovornost da naučimo kako da pravilno koristimo ovaj alat. Jednostavna greške i dobre namere mogu u potpunosti uništiti digitalne dokaze. Snažno se preporučuje da budući istražitelji praksu obavljaju na kontrolisanom sistemu, pre nego što pokušaju da prikupe dokaze iz realnog sistema. Ovaj alat može da radi na dve platforme, Windows i Lunix.



Slika 7. Početna stranica Helix-a, sa svim alatima koji se koriste u istrazi

Na slici 7, vidi se početna stranica programske platforme Helix. Tu se nalazi određeni broj alata koji se koriste u istrazi. Nama je mnogo zanimljivija slika 8, jer se na njoj vidi heksadecimalni zapis jednog foldera – *hash* funkcije imidža nekog medijuma. Ovaj zapis se pravi u fazi uzimanja forenzičkog imidža ispitivanog medijuma, a pre forenzičke istrage na tom folderu imidža. Prema standardnoj proceduri IOCE za uzimanje forenzičkog imidža, obavezno se uzimaju dva imidža ispitivanog medijuma – *jedan radni i jedan referentni*. Na radnom imidžu se vrši ispitivanje, a referentni služi za dokazivanje da integritet originalnog imidža nije narušen tokom ispitivanja. Nakon obavljene istrage ponovo se uzima *hash* foldera imidža na kome je sprovedena analiza.

Taj zapis *hash*-a treba da bude potpuno isti kao i hash refrentnog imidža i to je dokaz da tokom digitalne forenzičke istrage ništa nije promjenjeno od strane forenzičara. Takođe na *slici 7* vidimo jos neke alate, kao što je alat koji pokazuje kad je i koliko dugo računar bio upaljen, program koji omogućava da se povrate fajlovi koji su obrisani.



Slika 8. Uzimanje heš vrednosti

Na *slici 8* na sledecoj stranici nalazi se *screenshot* jednog od alata sa ove platforme. *Win Audit* je program na *windows* platformi, čijim se pokretanjem aktivira skeniranje računara na kojem radi. Po završetku skeniranja, program ispisuje kopletnu softversku i hardversku strukturu računara, koji su programi pokrenuti, kad su instalirani

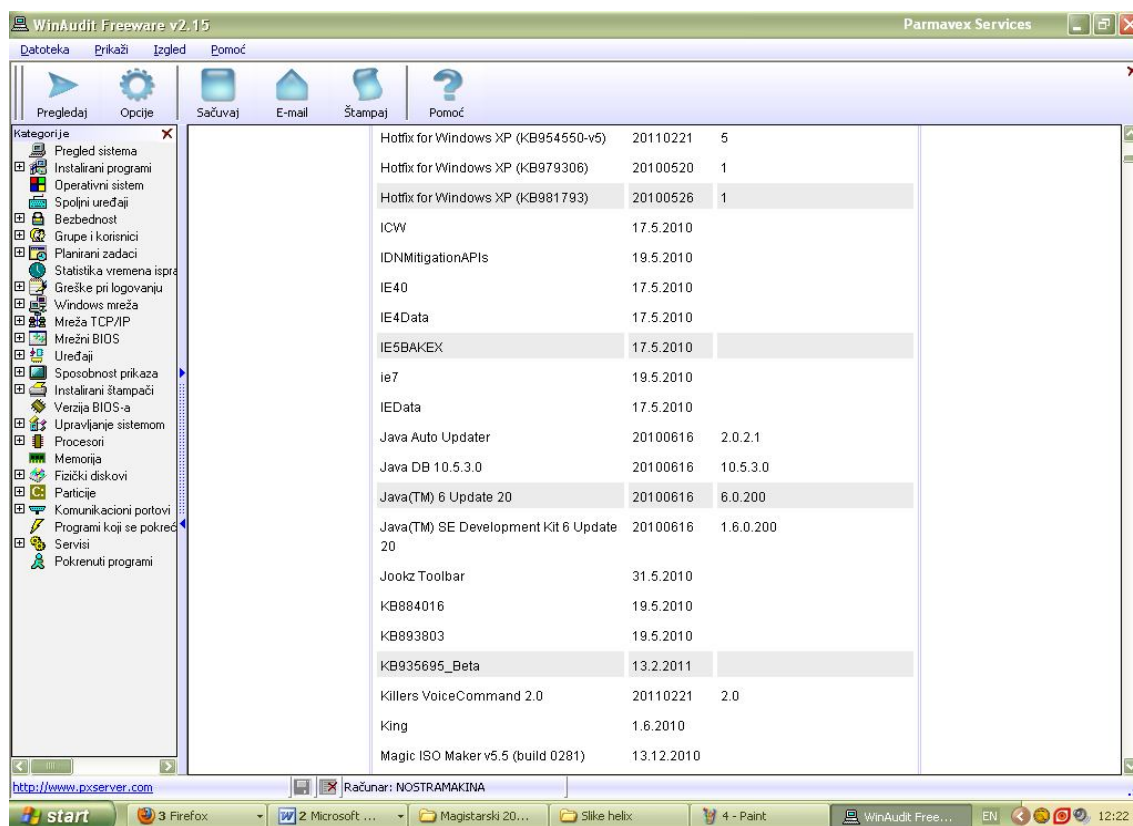
koliko se često koriste i koji su uređaji bili priključeni na računar. To se pokazalo izuzetno korisno jer on nam pokazuje ako je nekad na njega bio priključen neki eksterni memorijski medijum koji je predmet istrage.

To nam omogućava da povežemo taj računar i taj medijum na osnovu digitalnog potpisa koji je taj medijum ostavio u računaru.

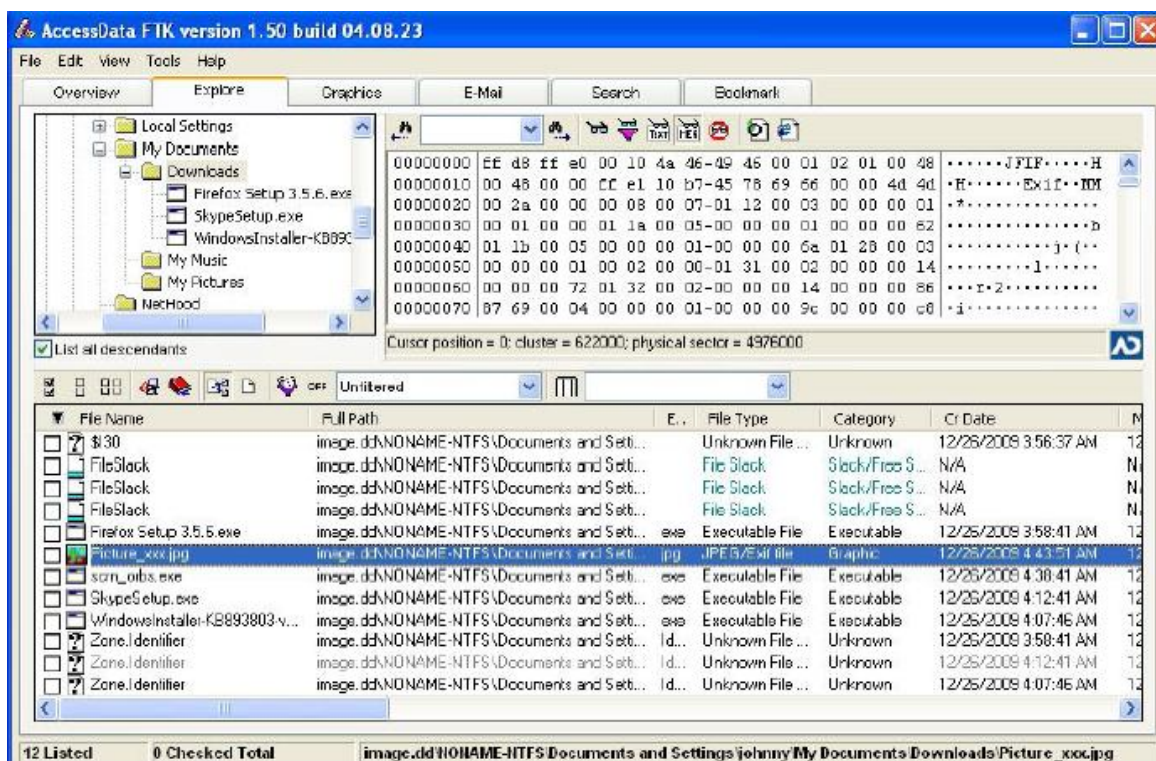
Na slici 9 se nalazi još jedna platforma sa alatima. Neki od ovih alata služe za probijanje šifri na nekim pretraživačima kao i pregled registara i sl.



Slika 9. Alati za probijanje šifri u pretraživačima i pregled registara



Slika 10. Skeniranje hardversko-soverske strukture računara



Slika 11. Pronalaženje ilegalne fotografije pomoću FTK-a

Pomoću programa FTK je prikazana na slici 11. Opsežna istraga treba biti sprovedena da bi se utvrdio način na koji je ova datoteka dospela na sistem. Pored Internet Explorera 6 i Firefox Internet browser-a, instalirani su i MSN Messenger i Skype programi za razmenu poruka, kao i Outlook Express 6 za rad sa elektronskom poštom.

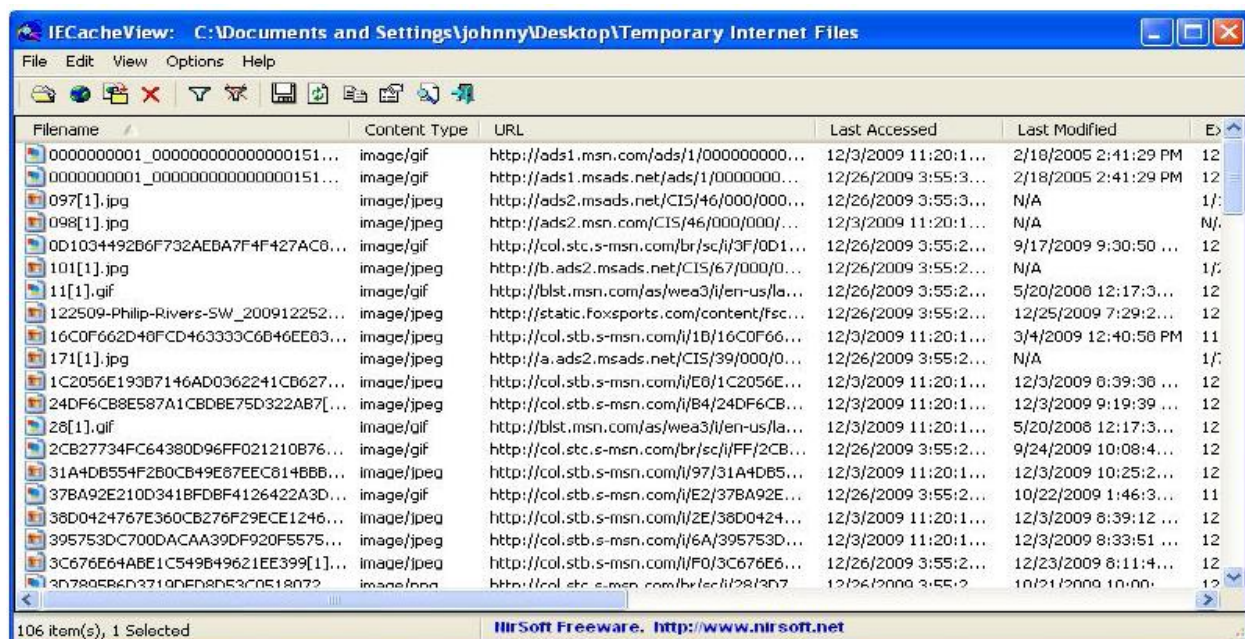
Programi za razmenu datoteka, bilo preko p2p ili torrent protokola, koji spadaju u sami vrh po mogućnosti da se pomoću njih preuzme ilegalni sadržaj, nisu pronađeni na sistemu. Svi ovi programi u nekom obliku skladište informacije o Internet lokacijama koje je korisnik posetio, o datotekama koje je preuzeo ili razgovorima koje je vodio.

Pomoću odgovarajućih alata, za svaki od ovih programa je moguće pregledati zapise o korišćenju. Iskustvo nam govori da ukoliko korisnici imaju instaliran neki napredniji Internet browser od Internet Explorer-a verzije 6, verovatno taj browser i koriste za rad na Internetu. Međutim, ne smemo zanemariti mogućnost da je maliciozni program preuzet sa Interneta pomoću Internet Explorer-a, naročito kada se u obzir uzmu svi sigurnosni propusti ovoga zastarelog programa, a koji se teško uklanja sa sistema.

Sadržaj Internet keša *Internet Explorer*-a, datoteka koje ubrzavaju rad na računaru, a forenzičarima često služe kao dokazni materijal, možemo da pronađemo u „C:\Documents And Settings\ johnny\Local Settings\Temporary Internet Files“ direktorijumu. Unutar svakog poddirektorijuma su stvarni fajlovi preuzeti sa Interneta pre nego što su prikazani na ekranu računara korisnika.

Datoteka *index.dat* služi za povezivanje svih ovih fajlova u smislenu celinu. Fajlovi mogu biti *html* tipa, grafički i slično, sve što je potrebno za ispravno prikazivanje Internet stranice. Još jedna, nezaobilazna lokacija je i „C:\Documents And Settings\johnny\Local Settings\History“, gde se u posebnim, vremenski organizovanim direktorijumima čuvaju podaci preuzeti sa Interneta, ukoliko nije drugačije podešeno, ili ukoliko oni nisu obrisani. Za lakši pregled informacija o datotekama preuzetim pomoću *Internet Explorera* može da se koristi alat *IECacheView* [23]. Pomoću *FTK*-a izdvajamo

direktorijum *Temporary Internet Files* pomoću opcije *Recursive Extract To...* i otvaramo ga u *IECacheView*-u. Samo nekoliko informacija se prikazuju na ekranu, kao što je i prikazano na slici 12, i njihovom analizom možemo da zaključimo da sporni materijal nije preuzet pomoću *Internet Explorer*-a.



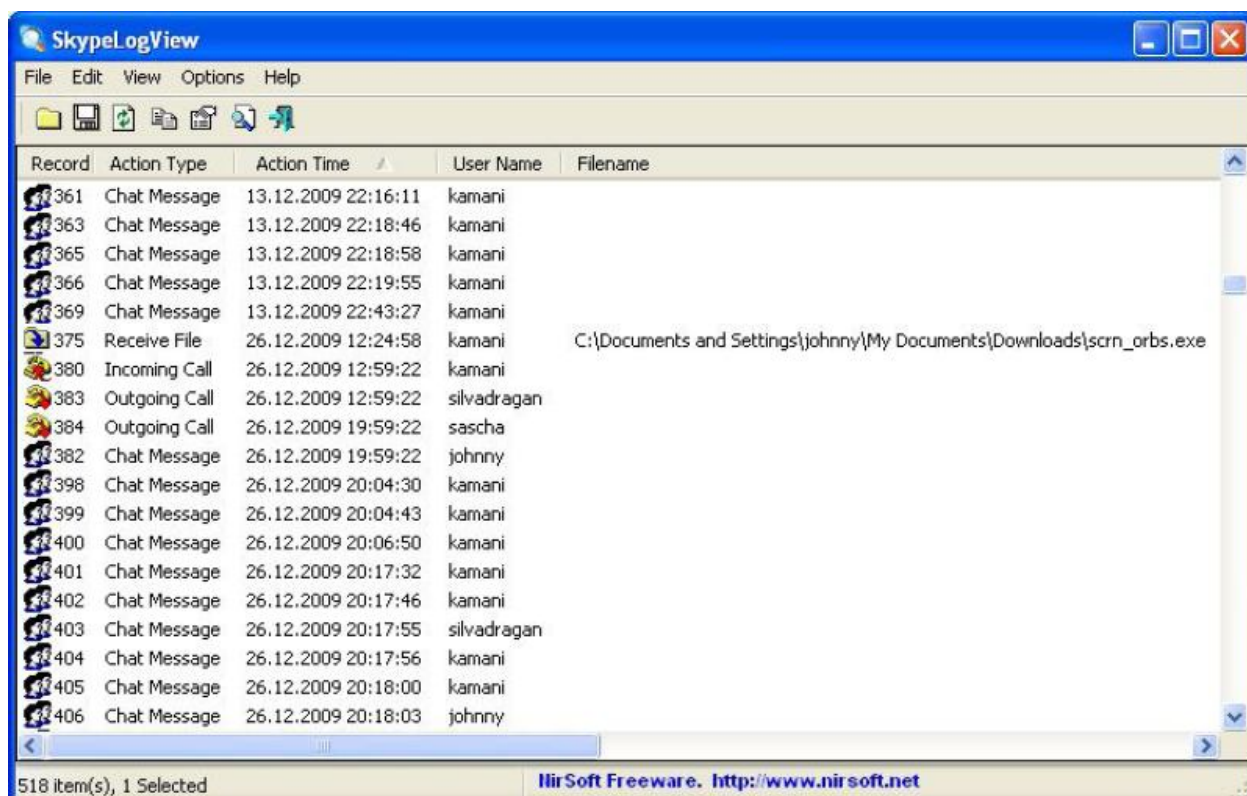
Slika 12. Pregled istorije korišćenja Interneta pomoću Internet Explorer-a

Na sličan način treba ispitati i zapise svih ostalih programa, kao i izvršiti ručnu pretragu za mogućim tragovima u vezi sa ilegalnim materijalom. Međutim, kako je dosadašnja istraga otkrila prisustvo zlonamernog programa pomoću koga je, što je i vrlo verovatno, neki udaljeni korisnik mogao da preuzme spornu datoteku, mi ćemo težište istrage da usmerimo na otkrivanje načina na koji je maliciozni program došao na sistem, a ne ilegalna fotografija.

Zapise programa koji imaju mogućnost preuzimanja datoteka sa Interneta smo već pregledali, ali ovaj put je pretraga usmerena na preuzete sumnjive programe.

Pregledom keša *Internet Explorer*-a, sem već pomenute lokacije sa koje je preuzet ilegalni materijal, pronađena je i referenca na lokaciju *Firefox* Internet pregledača iz čega zaključujemo da je korisnik verovatno kao podrazumevani *browser* koristio *Firefox*.

Za pregledanje keša *Firefox* browser-a, korišćen je program *MozillaCacheView*,... Obiman sačuvani keš ovog brauzera jasno ukazuje da je *Firefox* podrazumevani brauzer na sistemu, ali pretraga istorije za pojmovima „orbs“, „scrn_orbs“ i „notepad“ nije vratila nikakve rezultate. Slična pretraga log datoteka je urađena za programe *Outlook Express* i *MSN Messenger*, i rezultat je takođe bio negativan. Međutim, korišćenjem programa *SkypeLogView* otvoren je prethodno izdvojeni folder „C:\Documents and Settings\johnny\Application Data\Skype\johnny“.



Slika 13. Pregled zapisa pomoću SkypeLogView programa

U ovome direktorijumu se nalazi log datoteka Skype programa za razmenu poruka i Internet telefoniranje. Zapis istorije korišćenja Skype programa prikazan je na slici 13.

Analizom razgovora između korisnika johnny i kamani vođenog 26.12.2009. godine saznajemo da je korisnik kamani u 12:24 poslao datoteku scrn_orbs, koju je korisnik skull.cowboy i prihvatio. Posmatrajući intenzitet vođenih razgovora između ova dva korisnika, zaključujemo da johnny nije imao razloga da veruje da je u pitanju maliciozni program. Skype zapis takođe otkriva da je datoteka sačuvana u direktorijumu Downloads. I nakon što smo otkrili poreklo scrn_orbs datoteke, mi zapravo nemamo nikakve čvrste dokaze da su datoteke scrn_orbs, Orbs i notepad u vezi, sem što je antivirusni softver dve od tri datoteke označio kao istu vrstu trojanca. Ponovnim, ovaj put ručnim ispitivanjem Downloads lokacije pomoću FTK programa, ne pronalazimo nikakve tragove notepad datoteke. Verovatnoća da je korisnik, udaljeni korisnik ili maliciozni program obrisao ovu datoteku je jako velika.

2.7.6. Digitalni kompjuterski dokazi

Prema definiciji IOCE⁷ u oblasti digitalne forenzičke nauke, **digitalni dokaz** je svaka informacija u digitalnom obliku koja ima dokazujuću vrednost, a koja je ili uskladištena ili prenesena u takvom obliku. Pojam digitalnog dokaza uključuje kompjuterski uskladištene i kompjuterski generisane dokazne informacije, digitalizovane audio i video dokazne signale, signale sa digitalnog mobilnog telefona, informacije sa digitalnih faks mašina i signale drugih digitalnih uređaja. Znači, digitalni dokaz je bilo koja informacija generisana, obrađivana, uskladištena, ili prenesena u digitalnom obliku na koju se sud može osloniti kao validnu, tj. svaka binarna informacija, sastavljena od digitalnih **1** i **0**, uskladištena ili prenesena u digitalnoj formi, kao i druge moguće kopije originalne digitalne informacije koje imaju dokazujuću vrednost i na koje se sud može osloniti, u kontekstu forenzičke akvizicije, analize i prezentacije.

⁷ IOCE - International Organizatin for Computer Evidence

Digitalni kompjuterski dokaz formira se iz gomile posrednih stvarnih dokaza, od kojih se ni jedan ne sme isključiti iz bilo kog razloga. Dokazi moraju biti potpuni, da se međusobno dopunjuju (da su isprepleteni) i da nemaju tzv. pukotina za donošenje zaključaka, odnosno za utvrđivanje *čvrstog digitalnog dokaza* [2].

Generalni IOCE principi rada sa digitalnim dokazima harmonizuju metode i praksu između država, što garantuje uzajamnu prihvatljivost digitalnih dokaza. Sudska praksa prihvata kompjuterski generisane i kompjuterski memorisane digitalne dokaze pod odgovarajućim uslovima. Transformacija podataka iz serije kodiranih bita u sudski dokaz je apstraktan proces koji može navesti sudiju i porotu da dovedu u pitanje autentičnost i integritet kompjuterski generisanog dokaza. Treba da postoje procedure rukovanja i čuvanja, kao i procedure za akviziciju i analizu digitalnih dokaza sa čvrstog diska i drugih medija, odnosno, ne smiju se podaci izmeniti, manipulirati ili oštetiti ni u jednom koraku istrage [4].

Najteže je dobiti dokaze bez tzv. pukotina koji potpuno pokrivaju zaključke i objašnjenja. U izgradnji čvrstih (neoborivih) dokaza utvrđuje se: šta se stvarno desilo, šta je izgubljeno, koliki je iznos štete i da li se stvarno dogodilo krivično delo. Pri tome se mora zadržati potpuna objektivnost. Kada se rekonstruiše hipoteza o događaju, tada počinje prikupljanje dokaza. Dokaze treba prikupljati na mestu kompjuterskog krivičnog dela, jer to može biti jedini kontakt sa stvarnim dokazima. Treba raditi metodično, polako i sakupljati ključne stvari. Koristeći zaključke o događaju treba se vratiti na postavljenu hipotezu sa kritičkim pogledom, odnosno postaviti sebi pitanje kako bi lično prihvatio te dokaze ako bi se nalazio na suprotnoj strani. Treba misliti o svakom razlogu: zašto dokaz nije dobar, gde se izgubila neka važna činjenica, kako naći dokaz koji popunjava prazninu, šta uraditi ako se pronađe i.t.d. U ovoj fazi istrage jednako je važno dokazati kao i opovrgnuti dokaz.

Dakle, treba sakupljati sve posredne dokaze sa lica mesta, ne samo što digitalni forenzičar misli da treba, nego i sve ono što može potencijalno indicirati šta se stvarno desilo. U procesu akvizicije digitalnih dokaza, treba generalno snimiti listu fajlova i logova kao dokaze, čak i bez ikakve ideje šta se stvarno dogodilo. Treba imati u

dokaznom materijalu svaki fajl koji potencijalno može sadržavati dokaz, pre nego što se fajl prepíše, ili bude promenjen. Nakon inicijalne pretrage (bez privremenog oduzimanja računara), treba se okrenuti prvobitnoj hipotezi i dograditi je detaljnije sa prikupljenim dokazima.

Velika je verovatnoća da je propušten neki važan dokaz, što je dobar argument da se računar privremeno oduzme, dok traje istraga, ali nije uvek lako. Svaki posredni dokaz, koji zajedno čine dokazni materijal, treba tretirati kao da direktno vodi ka nepobitnom dokazivanju izvršenog krivičnog dela i kao da su svi jednako važni i kritični za konkretni slučaj.

Tek tada počinje proces izgradnje dokaza bez tzv. pukotina, odnosno, izgradnja neoborivog dokaza. Potrebno je, dakle, mnogo posrednog dokaznog materijala za jedan mali čvrsti dokaz.

Tri su osnovne kategorije digitalnih podataka koji mogu činiti digitalni dokaz u kompjuterskom incidentu:

- **Prelazni podaci** ili informacije koje se gube nakon isključivanja računara, kao što su veze sa otvorenom radnom memorijom, rezidentni memorijski programi i.t.d. Ovi podaci se mogu izgubiti u toku procesa isključivanja računara. Otuda je veoma važno do kraja precizno sprovoditi proceduru akvizicije. Pre isključivanja računara treba odmah ispitati, locirati i izvući osetljive i šifrovane podatke, jer se može desiti da se posle isključivanja ne može doći do njih (npr. vlasnik ključa ili smart kartice za pristup je nekooperativan ili mrtav, itd.).
- **Osetljivi podaci** ili podaci uskladišteni na čvrstom disku (HD) koji se lako mogu izmeniti, kao što je, npr. poslednje vreme pristupa *login* datoteci i.t.d.
- **Privremeno pristupačni podaci**, ili podaci uskladišteni na HD kojima se može pristupiti samo u određeno vreme (npr. šifrovani podaci).

2.7.7. Rezultati istrage

Generalno, istraga kompjuterskog kriminala i drugih slučajeva zloupotreba u IKT sistema često se može završiti bez rezultata, koji dovodi do hvatanja počinioca, suđenja i sankcionisanja, što se dešava iz više razloga:

- Gubljenja traga, jer je prošlo suviše vremena od incidenta i nema dokaza;
- Nekompletno logovanje, ili ga uopšte nema;
- Velik prostor skrivanja počinioca (Internet), a incident se dogodio samo jedanput, sa malo ili bez imalo dokaza;
- Incident nije sasvim određen, nije jasno da li je, ili nije bezbednosni incident;
- Ne može se nepobitno ukazati na počinioca;
- Nema dovoljno dokaza da se nepobitno dokaže slučaj;
- Postoji politički, ili drugi pritisak da se istraga zaustavi;
- Zataškavanje istrage i.t.d.
-

U slučaju da je istraga sprovedena u potpunosti, izveštaj se podnosi nadležnim zvaničnim organima za dalji pravosudni postupak. Dokument ***Izveštaj o istrazi*** treba da sadrži najmanje sledeće celine [3]:

Apstrakt istrage:

Opis događaja

Kratka metodologija istrage

Kratak opis skupljanja dokaza i metoda čuvanja istih

Zaključak sa kratkim uopštenim rezonima

Metodološki detalji

Istraga

Skupljanje i čuvanje dokaza

Nalaz 1 – Opis

Diskusija

Dokazi koji potvrđuju

.....

Nalaz N – Opis

Diskusija

Dokazi koji potvrđuju

Kratak sadržaj i zaključci

Dodatak

Lista ispitanih (intervjuisanih)

Lista dokaza

Sw i alati korišćeni u istrazi

IT eksperti i konsultanti

Kontakti na mestima koja su sarađivala (posrednici)

Drugi važni listinzi i informacije

U Izveštaju treba naglasiti da prikupljanje i čuvanje dokaza bilo u skladu sa zakonom o istražnom postupku i da li su informativni razgovori i saslušanja u toku istrage propisno vršeni primenom 7-stepenog metoda: *pripreme strategije saslušanja, vođenja razgovora, uspostavljanja kredibiliteta kod osumnjičenog, smanjenje otpora osumnjičenog, dobijanje (izvlačenje) priznanja, razvoj i eksploatacija priznanja i profesionalno zatvaranje saslušanja.*

2.8. Studija slučaja (*Case Study*)

Studija slučaja (*Case study*) već decenijama predstavlja bitan sastavni deo poslovne edukacije. Neke poslovne škole, kao što je *Harvard Business School*, svoje edukativne aktivnosti grade upravo na izradi i prezentaciji studija slučaja. Studije slučaja pomažu bolje razumevanje i upotrebu stečenog znanja tokom samog rada na pripremi studije.

Studije slučaja predstavljaju pisana dokumenta realnih poslovnih situacija, bazirana na konkretnim podacima i istraživanjima. Za vreme samog čitanja već pripremljenog case-a može se steći jasna slika o tome šta se dešavalo u kompaniji tokom određenog perioda vremena. Dešavanja koja se često opisuju u okviru case-a su promena organizacione strukture i proces donošenja strategijskih odluka u okviru preduzeća, kao i opis eksternih faktora koji su uticali na razvoj događaja. *Case study* predstavlja skraćeni i pojednostavljeni prikaz stvarnih situacija.

2.8.1. Scenario kompjuterskog incidenta firme

U firmi koja se bavi prometom roba i usluga posrestvom *Interneta*, podnešeno je više žalbi na osnovu povećanja cene prilikom naplate. Ova organizacija nije koristila ni jedan od proverenih sajtova za prenos novca poput *PayPal*-a (*slika 14*).



Slika 14. Sajt za prenos novca PayPal

Oni su koristili metod zasnovan na povjerenju svojih mušterija i lojalnosti svojih zaposlenih. Prilikom kupovine robe kod ove organizacije korisnik treba da ostavi svoje podatke sa kreditne kartice. Zabluda je da se mora kartica uvijek provući kroz uređaj da bi se sa nje skinuo novac. Da bi se novac skinuo sa vaše kartice dovoljno je da haker ima sledece elemente:

1. Podatke sa kartice (ime, prezime, broj kartice, datum isteka kartice)
2. Račun za robu ili usluge
3. I najbitnije CVV kod koji se nalazi na poledini kartice (slika 12).

Ovaj kod se ne nalazi ispisan na poleđeni svake kartice. Da bi omogućili ovaj način transakcije novca, prilikom otvaranja računa ste morali da zaokružite E trgovinu na vašoj kartici.



CVV: 3 or 4 digits that are used to Validate and Verify your card.

Slika 15. CVV kod na platnoj kartici⁸

Osumljiveni je radio u ovoj organizaciji i primao narudžbe od klijenata. Pošto je imao pristup velikom broju računa vidio je način kako da zaradi. On je otvorio firmu za pružanje intelektualnih usluga, jer mu je bio potreban račun da bi mogao da skine novac sa kartice. Sada je imao sve potrebne stvari da bi izvršio prevaru rešio je da sa svake transakcije skida po 5KM. Izabrao je baš ovu sumu, jer otprilike toliko iznosi tarifa kad uzimate novac sa bankomata od neke druge banke, kad plaćate na nekim

⁸ <https://secure.nebraskamed.com/images/cvv.jpg>

mestima. Tačnije izabrao je ovu sumu jer se ona najčešće pojavljuje na stanju, pa će prevarene mušterije pomisliti da je račun bio uvećan radi transakcije novca.

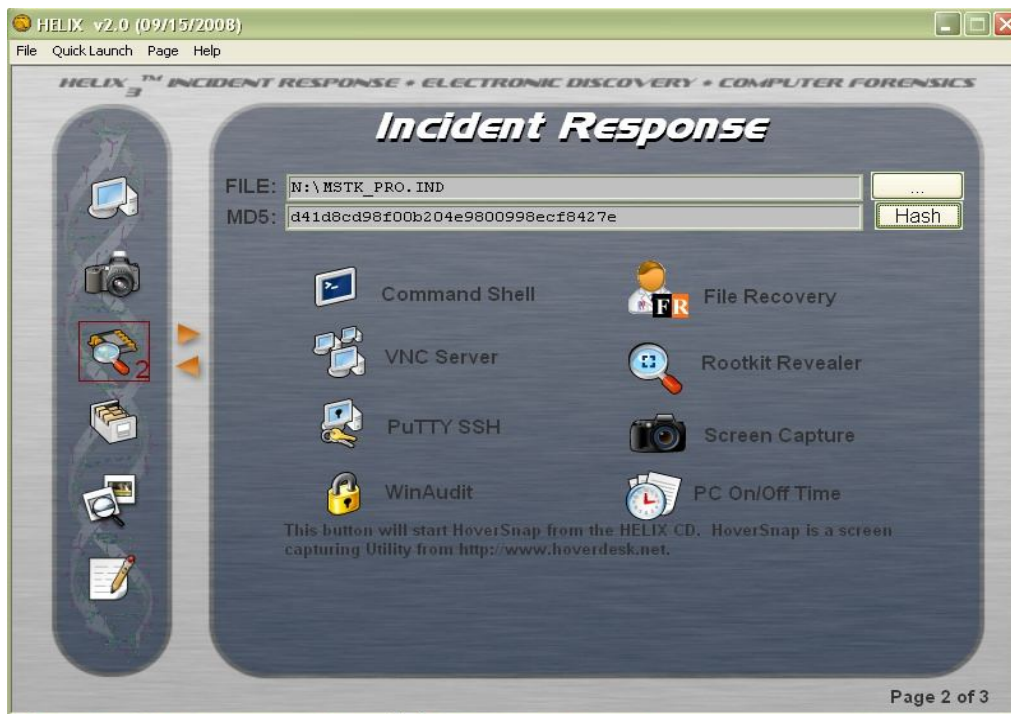
Osumnjičeni je sve podatke sa kartica snimao na USB uređaj i nosio ih kući čime je odmah izvršio prevaru i da nije zloupotrebio podatke. Onda je skidao sa računa klijenata na svoj račun novac. Na primer ako je klijent naručio robu u vrijednosti od 200KM, osumnjičeni bi skinuo 205KM. I onda sa svog računa naručio robu na njegovo ime i platio bi je 200KM. Jedino što je moglo da ga oda jeste što je ubrzo postao kupac broj jedan, a svaka firma želi da nagradi svog najboljeg kupca ili da mu da neki specijalni popust ili da pošalje kalendar za novu godinu. Tada su povezali da je njihov najbolji klijent takođe i njihov zaposleni pa su rešili da provjere.

2.8.2. Uzimanje imidža USB uređaja

Dok je osumnjičeni bio odsutan digitalni istražitelj iz tima za upravljanje kompjuterskim incidentom u kompaniji, uzeo je imidž njegovog USB uređaja. Ovaj digitalni istražitelj je specijalista za digitalnu forenziku, član tima za bezbednost informacija u kompaniji i član tima za upravljanje kompjuterskim incidentom. tako da je ovo korporacijska istraga kompjuterskog kriminala. U radu koristi CD set Helix alata verzije 2.0, kojim butuje računar sa priključenim osumnjičenim USB, a zatim uzima imidž (*Slika 16*) i njegovu *hash* vrednost (*Slika 17*).

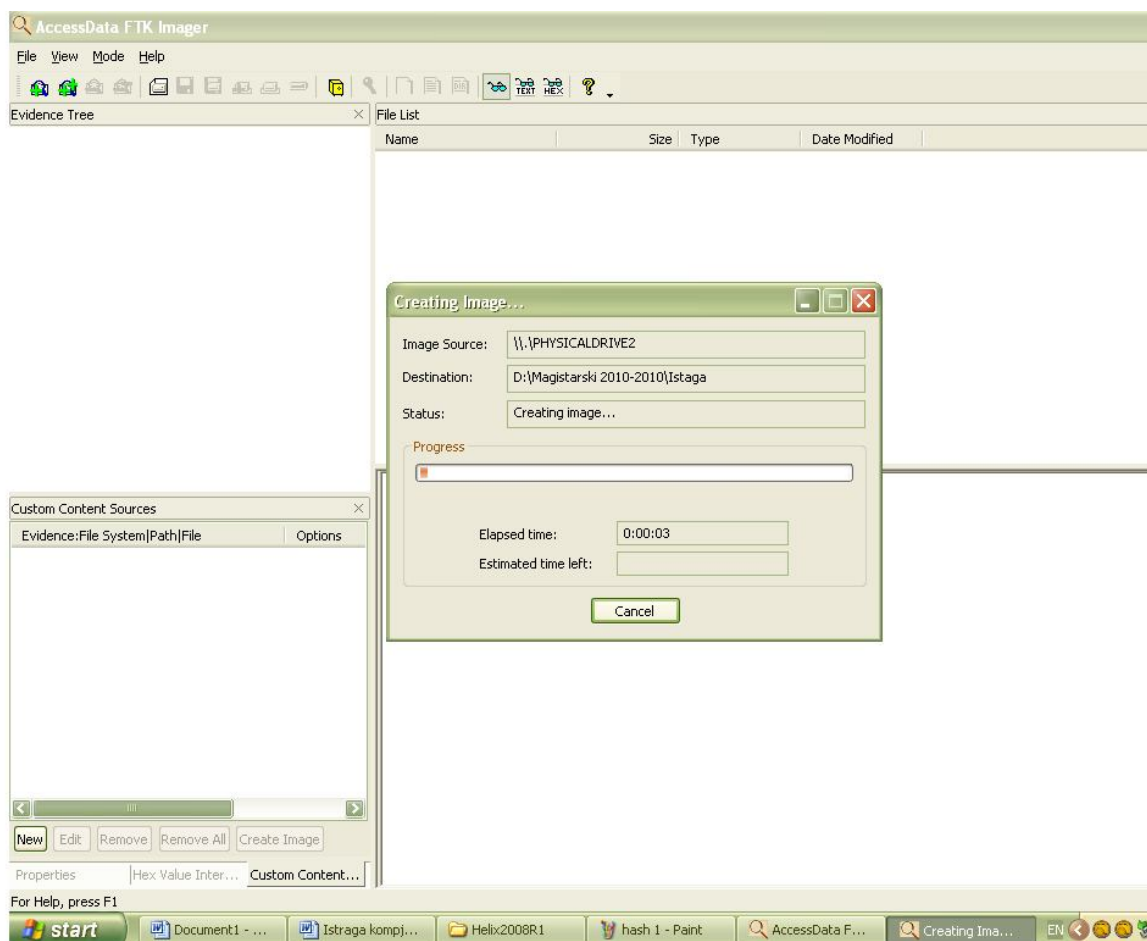


Slika 16. Uzimanje imidža USB uređaja



Slika 17. Heš vrednost USB uređaja

Pronađeni su podaci sa kreditnih kartica, a zatim je ponovo uzeta *haš* vrednost. Kompanija je odlučila da će sve predati na sud pošto su utvrdili nivo materijalne i nematerijalne štete načinjen njenoj imovini.

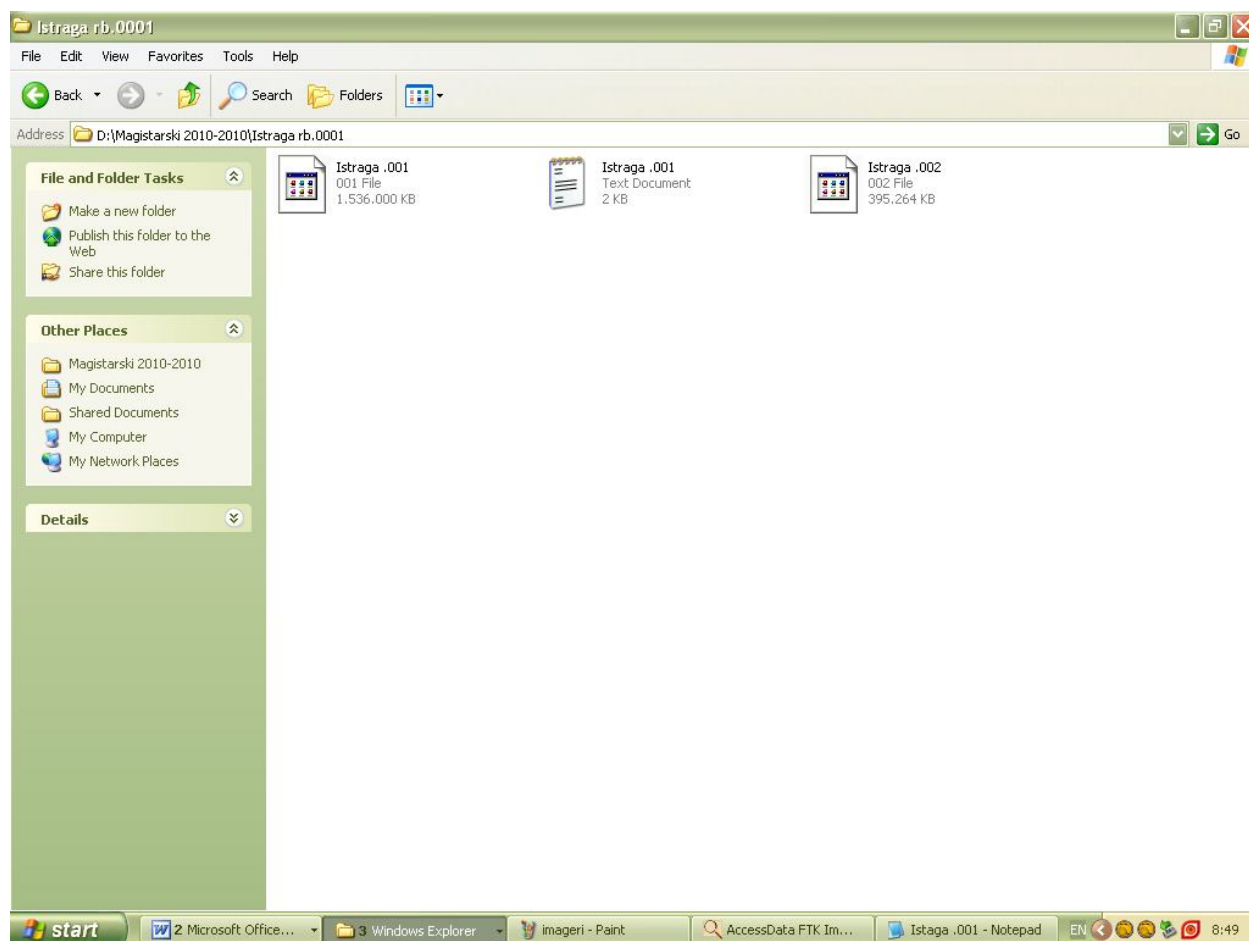


Slika 18. FTK imager i uzimanje imidža USB uređaja

Na slici 18 vidimo FTK imager koji je korišćen za uzimanje imidža USB uređaja. Uzimanje imidža snima mnogo više podataka i ne može se mjenjati, tačnije imidži se ne mogu mjenjati. Zato se koriste ovakvi specijalni alati, a ne alati za kopiranje (*copy/paste*). Pomoću ove palete programskih forenzičkih alata mogu se povratiti neki izbrisani podaci.

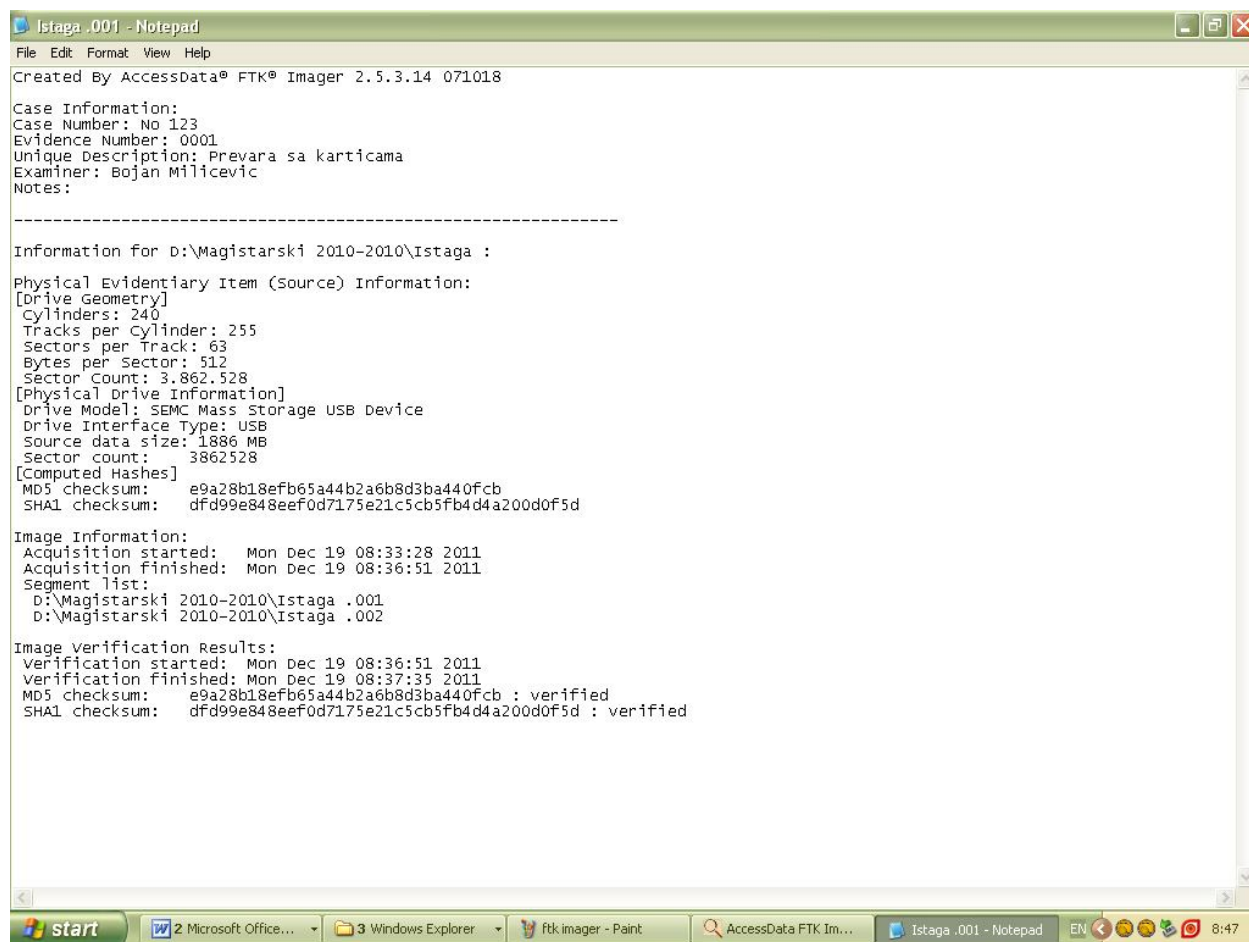
2.8.3. Predaja dokaza za zvaničnu istragu

Pošto ova istraga sad izlazi iz korporacijskih okvira. Digitalni forenzičari kompanije treba da predaju dokaze službenim organima. Da bi dokazi bili validni mi smo na početku uzeli dve haš vrednosti pre i posle rada na uređaju.



Slika 19. Zapisnik događaja i imidži za istražne organe

Na slici 19 se vidi folder u kome se nalaze imidži i zapisnik koji se predaje istražnim organima na dalju obradu, jer postoji osnovana sumnja da je to lice izvršilo prevaru.



```
Istaga .001 - Notepad
File Edit Format View Help
Created By AccessData® FTK® Imager 2.5.3.14 071018

Case Information:
Case Number: No 123
Evidence Number: 0001
Unique Description: Prevara sa karticama
Examiner: Bojan Milićević
Notes:

-----

Information for D:\Magistarski 2010-2010\Istaga :

Physical Evidentiary Item (Source) Information:
[Drive Geometry]
Cylinders: 240
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 3,862,528
[Physical Drive Information]
Drive Model: SEMC Mass Storage USB Device
Drive Interface Type: USB
Source data size: 1886 MB
Sector count: 3862528
[Computed Hashes]
MD5 checksum: e9a28b18efb65a44b2a6b8d3ba440fcb
SHA1 checksum: dfd99e848eef0d7175e21c5cb5fb4d4a200d0f5d

Image Information:
Acquisition started: Mon Dec 19 08:33:28 2011
Acquisition finished: Mon Dec 19 08:36:51 2011
Segment list:
D:\Magistarski 2010-2010\Istaga .001
D:\Magistarski 2010-2010\Istaga .002

Image Verification Results:
Verification started: Mon Dec 19 08:36:51 2011
Verification finished: Mon Dec 19 08:37:35 2011
MD5 checksum: e9a28b18efb65a44b2a6b8d3ba440fcb : verified
SHA1 checksum: dfd99e848eef0d7175e21c5cb5fb4d4a200d0f5d : verified
```

Slika 20. Izgled zapisnika istrage u notepad-u

Na slici 20 je zapisnik koji se predaje zajedno sa oba imidža. Tu se nalaze svi relevantni podaci i rezultati korporacijske forenzičke istrage koje treba dostaviti zvaničnom istražitelju da bi on mogao da provjeri tačnost ovih podataka i da dokaže da mi kao istražitelji nismo nista promjenili na ovome uređaju i da su podaci koji se na njemu nalaze kompromitujući za osumnjičenog.

2.8.4. Zvanična istraga

Sada je ova istraga koja je počela kao interna korporacijska istraga postala zvanična. U zvaničnoj istrazi imamo daleko veća ovlaštenja. Sledeći korak u istazi je da proverimo validnost dokaza i zaplena računara .

Credit Card Report

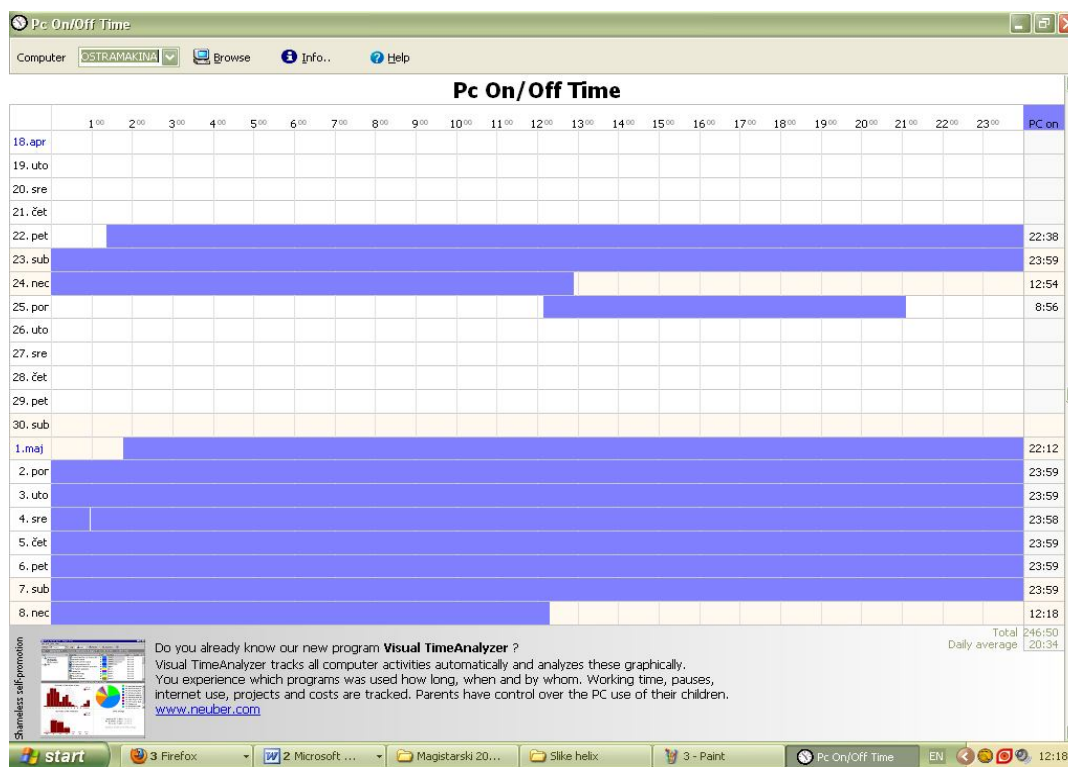
Customer ID: From: MIA To: MIA
 Credit Card From: CCB To: CCB
 Data From: 01/01/2008 12:00 AM To: 24/01/2008 12:00 AM

Date	Reference	Credit Card No.	Approval Code	Expiry Date	Payment	Charges	Sales	Discount	Tax
24/01/2008 10:38 AM	T01000007	123456	213	08/05/2009	250.00	0.00	250.00	0.00	0.00
24/01/2008 10:39 AM	T01000008	123456	3134	08/05/2009	5,600.00	0.00	1,600.00	0.00	0.00
24/01/2008 11:00 AM	T01000009	3139	3719	12/05/2008	38.00	0.00	38.00	0.00	0.00
24/01/2008 11:03 AM	T01000014	2280	331	12/05/2011	2,280.00	0.00	2,280.00	0.00	0.00
24/01/2008 11:06 AM	T01000015	830	838	12/05/2008	830.00	0.00	830.00	0.00	0.00
24/01/2008 11:09 AM	T01000016	29101	7381	11/03/2009	3,000.00	0.00	3,000.00	0.00	0.00
24/01/2008 11:10 AM	T01000019	3319	3830	20/05/2009	3,000.00	0.00	4,900.00	0.00	0.00
24/01/2008 11:11 AM	T01000020	2910	2930	02/10/2008	199.00	0.00	1,400.00	0.00	0.00
24/01/2008 11:13 AM	T01000025	3191	2801	20/10/2008	2,919.00	0.00	3,400.00	0.00	0.00
					14,126.00	0.00	16,000.00	0.00	0.00

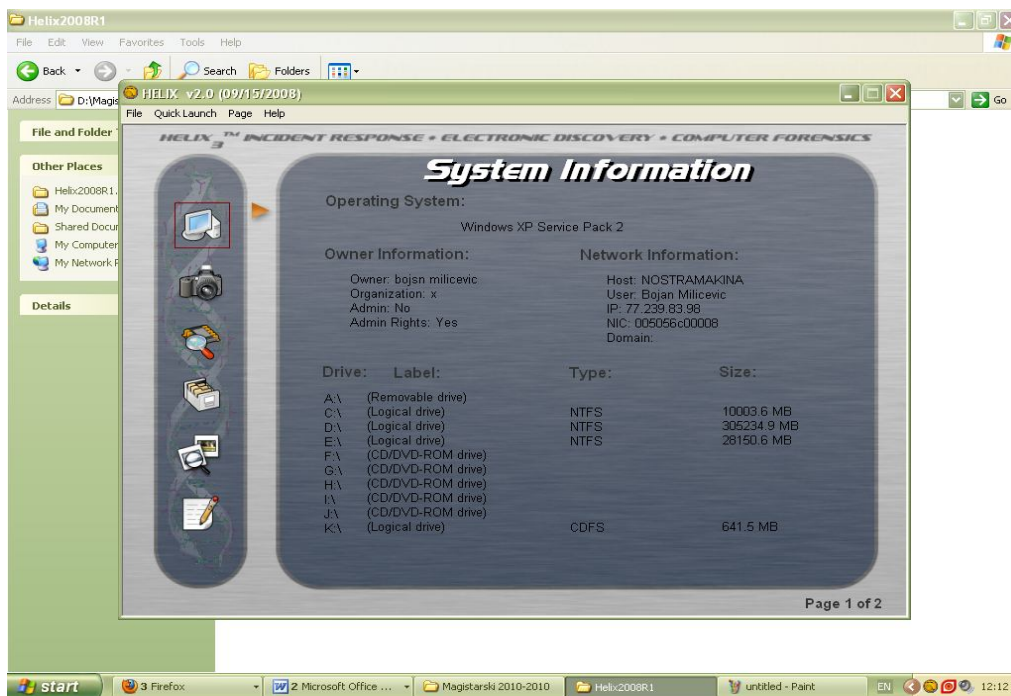
Current Page: No. 1 Total Page: No. 1 Zoom Factor: 100%

Slika 21. Izveštaj kreditne kartice

Na slici 21 je prikazano kako izgleda izveštaj kreditne kartice. Digitalni forenzičari počinju detaljni pregled računara jer postoji mogućnost da je se je isti bavio i drugim djelima. Pregleda se sve kao što vidimo na slikama ispod od sistema do vremena kad je računar bio upaljen (slika 22) IP adrese (slika 23), sajtovi koje je posećivao. Poslednjih godina je u praksi da se pregledaju slike na računarima iako njihovo djelo nije imalo nikakve veze sa takvim vrstama digitalnih zapisa. To se radi radi porasta pedofilije koja se širi putem interneta .



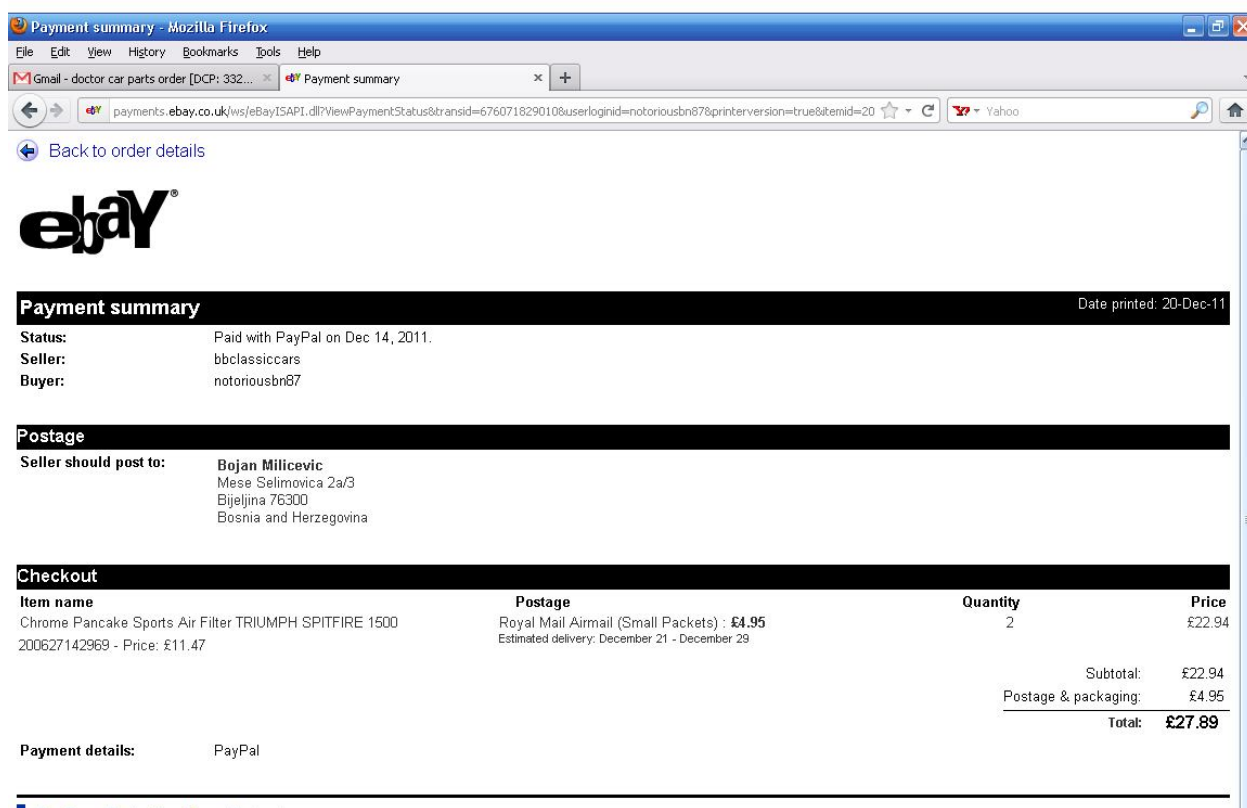
Slika 22. Prikaz vremenskog korištenja računara



Slika 23. Sistem informacije sa IP adresom

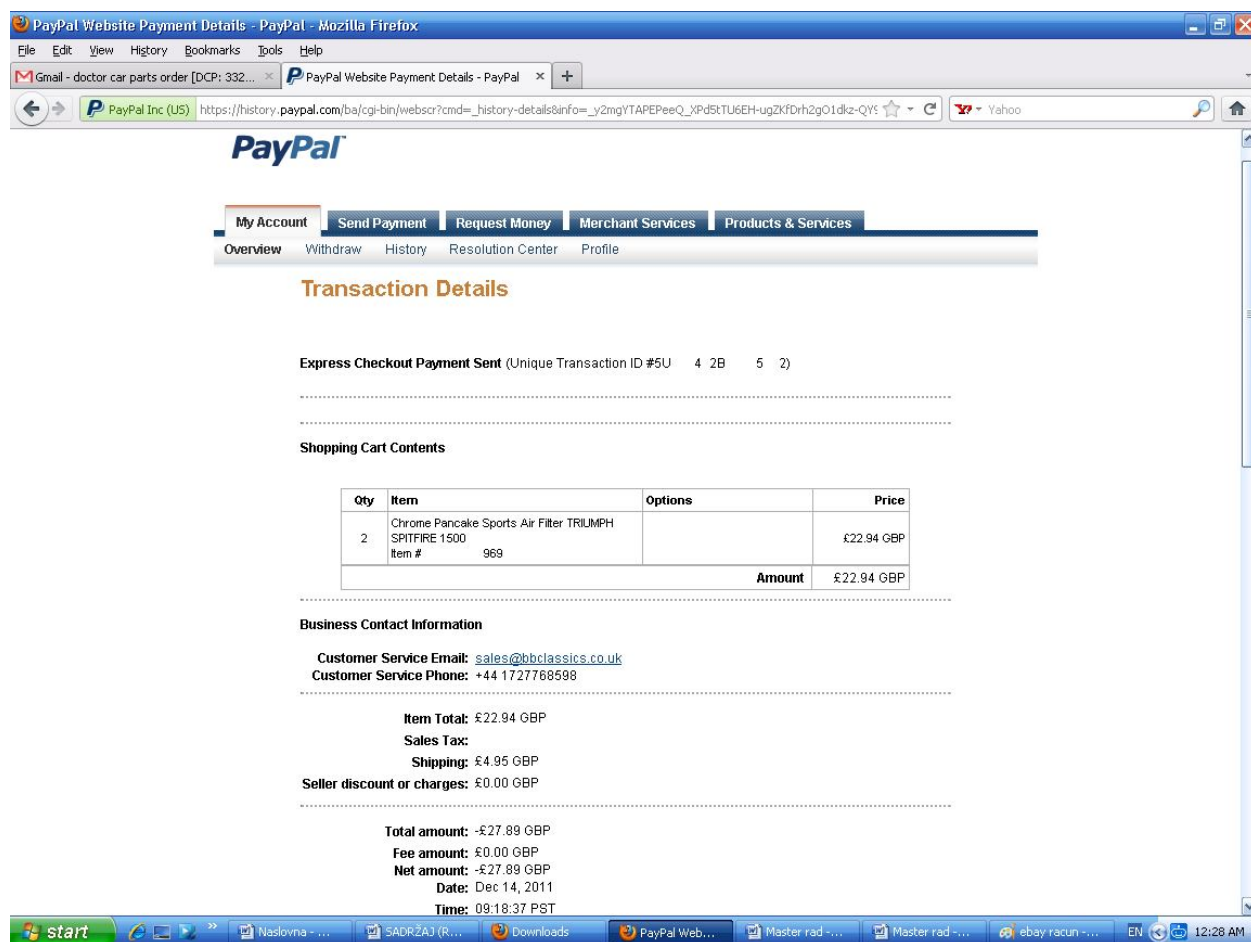
Digitalni forenzičari ispituju dokaze i oni odlaze na sud da ih prezentuju. Pošto je krivica osumnjičenog očigledna on nema drugog izbora nego da prizna krivicu.

Najteže kod ovakvih slučajeva nije dokazivanje krivice, nego otkrivanje prevare. I ovakvi slučajevi često prođu ne kažnjeni ili ne opaženi. Jer se radi o malim količinama novca na mnogo različitih računa. Tako da mnogi i ako primete da im nedostaje novac shvate to kao da je banka uzela proviziju.



Slika 24. eBay račun

Na slici 24 vidimo račun jednog od najboljih sajtova za kupovinu preko interneta. Ovaj sajt ima takozvanu zaštitu za kupce. Da bih kupovali na ovom sajtu treba vam samo kreditna kartica ili još je jednostavnije da otvorite račun na PayPal i onda možete da plaćate na skoro svim vodećim servisima za prodaju robe ili pružanje usluga.



Slika 25. PayPal račun

Na slici 25 vidimo račun za robu koju smo platili preko PayPal-a . Ova roba je kupljena na eBay-u ali je plaćena preko PayPal-a. Zahvaljući ovakvom načinu plaćanja podatci kreditne kartice koju smo koristili se nalaze u bazi paypal-a , a ne kod prodavca. Ovakav način plaćanja je izuzetno koristan ukoliko kupujemo mnogo robe preko interneta jer sa povećanjem broja različitih prodavaca sa kojima sarađujemo broj ljudi koji poznaju naše podatke ostaje isti.

2.8.5. Presentacija dokaza na sudu

Kada slučaj dobije sudski epilog, tada je primarni digitalni forenzičar onaj koga je angažovala kompanija dok je zvanični policijski istražitelj sekundarni. Digitalni forenzičar koga je angažovala kompanija treba da dokaže pred sudom da u toku istrage nije izmjenio nijedan podatak. On prezentuje heš vrednost koju je uzeo prije nego što je započeo bilo kakve radnje na uzetom imidžu . Zatim prezentuje dokaze koje je našao i koje je metode, načine, programe i procedure koristio u pronalaženju tih dokaza. Nakon iznošenja dokaza digitalni forenzičar iznosi heš vrednost koju je uzeo nakon izvršene istrage, kao i vreme i datum kada je ona uzeta. Heš vrednost koja je uzeta pre i Heš vrednost koja je uzeta posle moraju da budu potpuno iste da bi dokazi koje je digitalni forenzičar prezentovao bili validni na sudu. Uloga zvaničnog policijskog digitalnog forenzičara jeste da ukaže na anomalije ili greške tokom vršenja koproracijske istrage.

3. Zaključak

Iz ovog rada smo uvidili da su digitalni podatci, pogotovo oni koji se nalaze na internetu, podložni zloupotrebi od strane nekih drugih lica. Ta lica vrše krivična djela uglavnom da bi stekla neku finansijsku dobit, koriste najnovije metode i viruse da bi prikrili svoju prisutnost u nečijem računaru.

Forenzičari svakodnevno primenjuju nove alate i metode kao što smo videli u ovom radu da bi dosli do dokaza a da pri tome treba da ispoštuju sve u skladu sa zakonom da bi ti dokazi imali vrednost na sudu. Kroz ovaj rad potvrđena opšta i radna hipoteza, koja je postavljena na početku rada u metodologiji naučnog istraživanja.

Cilj eksperimentalnog istraživanja je prikaz gde i kako naći digitalne dokaze koji potvrđuju kompjuterski kriminal koji se može realno dogoditi u korporaciji.

Kao rezultat i zaključak eksperimentalnog istraživanja predložena je sigurnosna politika koja definiše digitalnu forenzičku istragu kompjuterskog incidenta i rešavanje sigurnosnih incidenata, skupom pravila, koja omogućavaju i olakšavaju oporavak sistema posle incidenta i time smanjuju uticaj i sprečavaju ponavljanje kompjuterskog incidenta.

Kompjuterska forenzika je mnogo šira od samog pružanja izvora potencijalnih dokaza. Ozbiljna korporacija uspostavlja tim za upravljanje kompjuterskim incidentima i planira obuku, zajedno sa sigurnosnim politikama i procedurama za forenzičku istragu.

Preventivne i reaktivne mere zaštite nisu više dovoljne održavanje računarskih sistema i mreža na prihvatljivom nivou rizika. Potrebno je pronaći način da se maliciozni napadi proaktivno spreče, uspešni napadi identifikuju. Kroz ovaj rad potvrđena opšta i radna hipoteza, koja je postavljena na početku rada u metodologiji naučnog istraživanja.

4. Literatura

- [1] McClure S, Scambray J, Kurtz G., *Hakerske tajne: zaštita mrežnih sistema, prevod petog izdanja*, Mikro knjiga, Beograd, 2006.
- [2] Milosavljević M., Grubor G. *Istraga kompjuterskog kriminala metodološko – tehnološke osnove*, Univerzitet Singidunum, Beograd, 2009.
- [3] Milosavljević M., Grubor G., *Digitalna forenzika računarskog sistema*, Univerzitet Singidunum, Beograd, 2009.
- [4] Pleskonić D., Maček N. Đorđević B. Carić M. *Sigurnost računarskih sistema i mreža*, Mikro knjiga, Beograd, 2007.
- [5] Ruth Andam, Zorayda E-Commerce and E-Business, Philippines, 2003

INTERNET IZVORI

- [6] <http://info.biz.hr>, petak 25.11.2011 god.
- [7] <http://sr.wikipedia.org> petak 25.11.2011 god.
- [8] <https://secure.nebraskamed.com/images/cvv.jpg>, petak, 25.11.2011 god.
- [9] <http://hr.wikipedia.org/wiki/E-poslovanje>, subota, 26.11.2011. god.
- [10] <http://www.net-security.org/dl/reviews/clarkch01.pdf>, subota, 26.11.2011. god.
- [11] <http://www.mmv.vic.gov.au/Assets/232/1/IntroductionToebusiness.pdf>, subota, 26.11.2011. god.
- [12] www.iso27001security.com/html/27001.html, nedelja 27.11.2011. god.
- [13] www.iso27001security.com/html/27002.html, nedelja 27.11.2011. god.