



UNIVERZITET SINGIDUNUM
FAKULTET ZA INFORMATIKU I RAČUNARSTVO

Master rad

Digitalna forenzika Android operativnog sistema

Mentor:
Prof. Dr Gojko Grubor

Student:
Nikola Milenković
Br. indeksa: 410196/2012

Beograd, 2014.



FAKULTET ZA INFORMATIKU I RAČUNARSTVO

UNIVERZITET SINGIDUNUM

FAKULTET ZA INFORMATIKU I RAČUNARSTVO

Beograd, Danijelova 32

Kandidat: Nikola Milenković

Broj indeksa: 410196/2012

Smer: Savremene informacione tehnologije

Tema: Digitalna forenzička istraga Android operativnog sistema

Datum odobrenja rada:
Beograd, _____._____._____.

MENTOR

Prof. dr Gojko Grubor

DEKAN

Prof. dr

SADRŽAJ

Abstrakt	4
1 Metodologija istraživačkog rada	5
1.1 Uvodne napomene i obrazloženje rada.....	5
1.2 Predmet rada	5
1.3 Ciljevi rada.....	5
1.4 Hipotetički okvir	5
1.5 Metode i tehnike istraživanja	6
2 Digitalna forenzika Android operativnog sistema	7
2.1 Digitalna forenzika.....	7
2.2 Android operativni sistem.....	8
2.3 Digitalni dokaz.....	12
2.4 Kompromitovani računar	13
3 Forenzička akvizicija digitalnih podataka	14
3.1 Forenzička akvizicija rada na računaru	14
3.1.1 Lokardv princip razmene materije.....	15
3.1.2 Redosled sakupljanja nestabilnih podataka.....	16
3.1.3 Izbor i priprema alata	16
3.1.4 Metodologija akvizicije živog računara	17
3.2 Prednosti šive forenzičke analize	22
4 Digitalna forenzička analiza računara	23
4.1 Priprema za forenzičku analizu računara.....	23
4.2 Zaštita integriteta podataka i verifikacija	25
5 Privremeni i drugi forenzički fajlovi	27
5.1 Privremeni fajlovi.....	27
5.2 Log fajlovi	28
5.3 Print Spooler fajlovi	29
5.4 Fajlovi linkova	30
5.5 Tipovi i potpisi fajlova	31

5.6 Potpisi fajlova	33
5.7 Forenzička analiza tragova korišćenja interneta	35
5.7.1 Privremeni internet fajlovi	36
5.7.2 Istorija aktivnosit na internetu	37
5.8 Kolačići (Cookies).....	39
5.9 Favorizovane lokacije.....	40
5.10 Direktno umrežavanje (peer-to-peer)	41
5.11 Ostali transfer fajlova	41
5.12 Tragovi e-mail poruka	42
5.13 Servisi za četovanje preko interneta.....	44
5.13.1 Servis novinske grupe.....	44
5.13.2 AOL servis.....	45
5.14 Analiza izvršnih fajlova, rutkitova, zadnjih vrata i snifera.....	45
6 Digitalni dokaz.....	50
6.1 Digitalni kompjuterski dokaz.....	50
6.2 Pravosudni aspekt digitalnih kompjuterskih dokaza.....	51
6.3 Upravljanje digitalnim dokazima.....	52
6.4 Procedura sakupljanja posrednih kompjuterskih dokaza	53
6.5 Korisnici kompjuterskih digitalnih dokaza.....	55
6.6 Priprema digitalnih dokaza za veštačenje pred sudom.....	55
6.7 Preporuke IOCE za upravljanje digitalnim dokazima.....	55
7 Forenzička analiza digitalnih podataka	56
7.1 Forenzička analiza softvera	56
7.2 Forenzička analiza računara.....	57
7.3 Forenzička analiza kibernetičkog prostora	57
7.4 Slojevi apstrakcije	61
7.4.1 Greške u slojevima apstrakcije	62
7.4.2 Karakteristike slojeve apstrakcije	62
7.5 Zahtevi za alate za digitalnu forenzičku analizu.....	64
7.6 Apstrakcioni slojevi FAT fajl sistema.....	64

8 Forenzički alati.....	67
8.1 Opšte karakteristike	67
8.1.1 Tehnike i alati za akviziciju digitalnih podataka	67
8.1.2 Validacija i diskriminacija podataka	69
8.1.3 Ekstrakcija digitalnih podataka.....	70
8.1.4 Rekonstrukcija osumnjičenog diska	71
8.1.5 Izveštavanje o digitalnim dokazima	72
8.2 Hardverski forenzički alati	73
8.2.1 Blokatori upisivanja i drugi hardverski forenzički alati.....	74
8.3 Softverski forenzički alati.....	80
8.3.1 Forenzički alati komandne linije.....	80
8.3.2 Softverski forenzički alat „EnCase v4“ GUI tipa	81
8.3.3 SPADA forenzički alati na bazi Linux OS	92
8.4 Komparativni pregled funkcija ključnih forenzičkih alata	99
8.5 Validacija i testiranje forenzičkih alata	99
8.5.1 Razvoj procesa validacije forenzičkih alata.....	100
8.5.2 Proces testiranja softverskih forenzičkih alata	100
8.5.3 Procedura za validaciju forenzičkih alata.....	102
8.6 Značaj poznavanja izvornog koda forenzičkih alata	103
9 Digitalna forenzika mobilnih telefona i tablet računara	105
9.1 Mobilni telefoni.....	105
9.1.1 Digitalni dokazi na mobilnom telefonu.....	105
10 Studija slučaja kompjuterskog kriminala	108
Literatura.....	118

Abstrakt: Mobilni telefon predstavlja multifunkcionalni telekomunikacioni uređaj koji je, kao nijedan drugi, postao neodvojivi deo svakodnevnice. Mobilni telefoni su široko prihvaćeni i korisnici ih svuda nose sa sobom, poseduju čak po nekoliko uređaja ili korisničkih brojeva, a posebno je zanimljivo što, bez obzira na nivo tehničkog obrazovanja i aspiracija prema novim tehničkim dostignućima, svaki korisnik nastoji da ovlada sve većim brojem funkcija, ali i da poseduje uređaje sa novim ili naprednijim mogućnostima. S druge strane, mobilni telefoni danas mogu da čuvaju veliku količinu podataka vezanih za komunikacije (radi se već o hiljadama SMS poruka i poruka elektronske pošte), mogu se upotrebljavati i za bežični pristup Internetu (GPRS, EDGE, 3G, Wi-Fi), multifunkcionalnost telefona već dostiže mogućnosti personalnih računara, ali ide i korak dalje, jer integriše i uređaje kao što su fotoaparati, video kamere, snimači zvuka i uređaji za GPS navigaciju, i sve to mobilni telefon čini bogatim izvorom različitih podataka i informacija koje se ne mogu sagledati bez primene posebnih alata. Takve karakteristike mobilnih telefona i osobine njihovih korisnika naglašavaju značaj prikupljanja podataka koji se na njima nalaze za potrebe rada državnih bezbednosnih struktura, vođenja krivičnog postupka, ali i obezbeđivanja korporativne zaštite. U ovom radu je dat pregled mogućnosti mobilnih telefona kao izvora digitalnih dokaza i drugih informacija, kao i načina, alata i procedura prikupljanja podataka sa njih, i razmatraju se specifičnosti vezane za forenziku mobilnih telefona u krivičnom postupku, pre svega sa stanovišta digitalnog dokaza kao suštinskog rezultata forenzičkog rada, kao i osobenosti ove vrste digitalne forenzike u odnosu na forenziku računara koja je već u značajnoj meri standardizovana.

Ključne reči: Mobilni telefon, multifunkcionalnost, bezbednost, digitalni dokaz, krivični postupak.

Abstract: Mobile phone is a multifunctional telecommunications device which has, unlike any other device, become an inseparable part of everyday life. Mobile phones are widely used and users carry them everywhere. Some users even possess several devices and user numbers, but it is particularly interesting that, regardless of the level of technical education and aspirations towards new technical developments, each user tries to master an increasing number of functions and also to own devices with new or advanced functions. On the other hand, mobile phones can now store a large amount of data related to communications (like thousands of text messages and e-mails), they can be used for wireless Internet access (GPRS, EDGE, 3G, Wi-Fi). Mobile phone, with its multifunctional properties, already reaches the levels of functionality of personal computers, and it goes a step further because it integrates devices such as cameras, video cameras, sound recorders and GPS navigation units. All this makes a mobile phone a rich source of data and information which cannot be acquired without the use of special tools. Such characteristics of mobile phones and their users emphasize the importance of data collection for the needs of law enforcement agencies, criminal proceedings and corporate protection. This paper reviews the possibilities of mobile phones as a source of digital evidence and other information. It also reviews methods, tools and procedures of data collection stored on them. Specific circumstances related to mobile phone forensics in criminal proceedings are considered primarily from the standpoint of digital evidence being an essential result of forensic work. Peculiarities of this type of digital forensics in relation to the already greatly standardized computer forensics are also considered.

Keywords: Mobile phone, multifunctionality, security, digital evidence, criminal proceedings.

1. Metodologija istraživačkog rada

1.1 Uvodne napomene i obrazloženje rada

Mobilni telefon predstavlja multifunkcionalni telekomunikacioni uređaj koji je, kao nijedan drugi, postao neodvojivi deo svakodnevnice. Mobilni telefoni su široko prihvaćeni i korisnici ih svuda nose sa sobom, poseduju čak po nekoliko uređaja ili korisničkih brojeva, a posebno je zanimljivo što, bez obzira na nivo tehničkog obrazovanja i aspiracija prema novim tehničkim dostignućima, svaki korisnik nastoji da ovlada sve većim brojem funkcija, ali i da poseduje uređaje sa novim ili naprednijim mogućnostima. S druge strane, mobilni telefoni danas mogu da čuvaju veliku količinu podataka vezanih za komunikacije (radi se već o hiljadama SMS poruka i poruka elektronske pošte), mogu se upotrebljavati i za bežični pristup Internetu (GPRS, EDGE, 3G, Wi-Fi), multifunkcionalnost telefona već dostiže mogućnosti personalnih računara, ali ide i korak dalje, jer integriše i uređaje kao što su fotoaparati, video kamere, snimači zvuka i uređaji za GPS navigaciju, i sve to mobilni telefon čini bogatim izvorom različitih podataka i informacija koje se ne mogu sagledati bez primene posebnih alata. Takve karakteristike mobilnih telefona i osobine njihovih korisnika naglašavaju značaj prikupljanja podataka koji se na njima nalaze za potrebe rada državnih bezbednosnih struktura, vođenja krivičnog postupka, ali i obezbeđivanja korporativne zaštite. U ovom radu je dat pregled mogućnosti mobilnih telefona kao izvora digitalnih dokaza i drugih informacija, kao i načina, alata i procedura prikupljanja podataka sa njih, i razmatraju se specifičnosti vezane za forenziku mobilnih telefona u krivičnom postupku, pre svega sa stanovišta digitalnog dokaza kao suštinskog rezultata forenzičkog rada, kao i osobenosti ove vrste digitalne forenzike u odnosu na forenziku računara koja je već u značajnoj meri standardizovana.

1.2 Predmet rada

U ovom projektnom zadatku predmet istraživanja je osnova digitalne mobilne forenzike i najosnovniji alati. U prvom delu istraživačkog projekta izvršena je kratka revizija procesa digitalne forenzičke analize i osnovnih karakteristika i tipično zahtevanih funkcionalnosti softverskih forenzičkih alata.

1.3 Ciljevi rada

Cilj ovog istraživačkog rada je da se prikažu problemi sa kompjuterskim i mobilnim kriminalom sa fokusom na android operativni sistem, načini na koji oni mogu da se preduprede i reše u koliko dodje do kriminalnih aktivnosti.

1.4 Hipotetički okvir

Opšta hipoteza: Softverski digitalni forenzički alati se mogu podeliti na više načina, zavisno od kriterijuma klasifikacije. U odnosu na tip interfejsa softverski forenzički alati se dele na: digitalne forenzičke alate komandne linije i digitalne forenzičke alate sa GUI (Grafical User Interface) interfejsom. U odnosu na programski kod, softverski digitalni forenzički alati se dele na: digitalne forenzičke alate zatvorenog koda i digitalne forenzičke alate otvorenog koda. Pored velikog izbora digitalnih forenzičkih alata ne može se govoriti o najboljem digitalnom forenzičkom alatu. Specijalizovani forenzički alati koriste se za samo određenu vrstu fajlova ili obavljaju samo jedan zadatak digitalne forenzičke istrage. Ovi alati su namenski i pouzdaniji te mnogo efikasnije obavljaju zadatak nego neki univerzalni alati. Sa druge strane, sa adekvatnim skupom raznovrsnih digitalnih forenzičkih alata, forenzicar može brže i konformnije završiti više različitih zadataka digitalne forenzičke istrage. Najbolje je rešenje da digitalni forenzicar sam, na bazi predistražnih podataka i informacija o slučaju, izvrši izbor adekvatnih alata za konkretan slučaj, uključujući skup alata za izvršenje što više digitalnih forenzičkih zadataka na terenu kao i specijalizovane alate za detaljno i precizno izvršavanje karakterističnog forenzičkog zadatka.

Radna hipoteza: Generalno, digitalni forenzički alati zatvorenog koda pred sudom mogu biti priznati kao alati za akviziciju i analizu digitalnih podataka pod uslovom da su naučno potvrđeni, da im je poznat stepen greške koju unose i da mogu po zahtevu suda ponoviti proces izgradnje čvrstih digitalnih dokaza bez narušavanja integriteta akvizicijom prikupljenih digitalnih podataka. Forenzička prihvatljivost u praksi digitalne forenzičke istrage slučaja kompjuterskog incidenta/kriminala može se evaluirati verifikacijom deklariranih funkcionalnosti na istim i kontrolisanim slučajevima akvizicije i analize digitalnih podataka i komparacijom sa funkcionalnim ispitivanjem sličnog seta priznatih forenzičkih alata drugog tipa.

1.5 Metode i tehnike istraživanja

Osnovna metodologija prirodnih nauka je eksperimentalna metodologija. Treba je shvatiti kao istraživački proces kojeg čine dve celine: istraživanje i prezentacija rezultata istraživanja. U toku istraživanja potrebno je proći kroz četiri faze: postavljanje problema, formulisane hipoteze, proveravanje hipoteze i potvrđivanje (verifikacija) hipoteze.

U radu su napisane osnove digitalne forenzike mobilnih uređaja pomoću navedenih literatura u daljem radu biće uže napisano i objašnjeno o digitalnoj forenzici Android operativnog sistema i korišćenje određenih alata.

2 Digitalna forenzika Android operativnog sistema

2.1 Digitalna forenzika

Digitalna forenzika uključuje otkrivanje (pretraga, istraga) i sakupljanje (akviziciju), čuvanje (upravljanje), dokazivanje (analizu) i ekspertsko svedocenje/vestacenje (prezentaciju) digitalnih dokaza pred sudom, u slučajevima zloupotrebe IKT sistema i upravljanja kompjuterskim incidentom, kompjuterskog kriminala, civilne parnice, ili administrativnih zahteva. Prate je brojni izazovi, uključujući brze promene računarskih i digitalnih uređaja, kao i sve sofisticiraniji napadi na računarske sisteme i mreže i rapidni porast zloupotreba IKT sistema i kompjuterskog kriminala. 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 (Hard Drives), 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 računarske mreže, uključujući i Internet ili kibernetička forenzika, otkriva i sakuplja informacije o tome kako je napadač, ili haker dobio pristup računarskoj mrezi i računarskom sistemu. Analiziraju se log fajlovi da se odredi kada se korisnik ulogovao ili poslednji put koristio svoj lični identifikator (ID) za logovanje. Forenzički analitičar digitalnih podataka ili digitalni forenzičar nastoji da odredi kojim URL lokacijama je korisnik pristupio, kako se ulogovao na računarsku mrežu i sa koje lokacije.

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 (slika 1).

Forenzičar mora ispitivati HD i sve 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.

Postoje dve vrste forenzičke istrage u odnosu na organe koji je sprovode:

1. Zvanična istraga (policija, vlada)
2. Korporacijska istraga (privatni istražitelji)



Slika 1. Digitalni "otisak prsta"

2.2 Android operativni sistem

Android™ operativni sistem je trenutno najrasprostranjenij operativni sistem za mobilne telefone, zasnovan je na *Linux* kernelu i prilagođen je tako da se može koristiti na većini mobilnih uređaja, uključujući pored mobilnih telefona i tablet računare, laptop računare, netbook računare, smartbook računare, čitače elektronskih knjiga, pa čak i ručne satove. Iako je *Android Linux* distribucija, on po nekim stvarima odstupa od većine standardnih *Linux* distribucija, npr. *Android* nema standardni X Window System ili standardni skup GNU biblioteka pa tako nije u mogućnosti da pokreće aplikacije razvijene za druge standardne *Linux* sisteme.

Pokretanje samih aplikacija se, kod *Androida*, ne vrši direktno, već se aplikacije pokreću u okruženju odvojenom od ostatka sistema gde dobijaju samo određeni deo sistemskih resursa, pa tako nemaju pristup delovima sistema koji su im nepotrebni, što donekle poboljšava sigurnost i stabilnost sistema, takođe pri instalaciji aplikacija korisnik dobija listu svih dozvola koje jedna aplikacija zahteva da bi se instalirala, što korisniku daje mogućnost da uoči potencijalno štetne aplikacije i obustavi njihovu instalaciju pre nego što dođe do oštećenja.

Sa tehničke strane *Android* predstavlja *Linux* operativni sistem razvijen za ARM i x86 arhitekturu i sastoji se od modifikovanog monolitnog *Linux* kernela zaduženog za podršku hardvera i funkcija niskog nivoa, skupa biblioteka zaduženih za dodatne podrške kao što su iscrtavanje grafike, podrška za dekodovanje video snimaka, podrška za SSL enkripciju itd., u sklopu biblioteka se nalazi i odvojeni *Android Runtime* koji sadrži osnovne, bazne, biblioteke i *Dalvik* virtualna mašina zadužena za pokretanja aplikacija višeg nivoa napisanih u *Java* programskom jeziku. Na višem nivou od biblioteka su systemske aplikacije neophodne za upotrebu sistema od strane korisnika i tu se nalaze, window manager, menadžer resursa, menadžer instalacionih paketa, kao i aplikacije zadužene za obavljanje osnovnih funkcija vezanih za mobilne telefone ili uređaj na kom je instaliran *Android*, na najvišem nivou se nalaze krajnje korisničke aplikacije, odnosno aplikacije koje direktno koristi korisnik.

Ovakva arhitektura sistema nije iznenađujuća jer predstavlja standardnu arhitekturu *Linux* sistema gde su segmenti sistema razdvojeni po nivoima na kojim rade. Za crtanje 3D grafike *Android* koristi biblioteku zasnovanu na *OpenGL ES 2.0* specifikaciji, što ovom sistemu daje mnoge napredne grafičke sposobnosti. *Android* poseduje i ugrađenu podršku za multitasking.

Kroz svoju istoriju *Android* je imao nekoliko verzija od kojih je svaka donosila neku novinu i poboljšanje, tako je npr. verzija 1.0 bila prva zvanično dostupna verzija *Android* operativnog sistema, V1.5 Cupcake je bila njena nadogradnja zasnovana na *Linux* kernelu 2.6.27, V1.6 Donut je koristio 2.6.29 *Linux* kernel i imao još više dodatnih mogućnosti u odnosu na prvu 1.0 verziju. Sa pojavom verzija 2.0 i 2.1 pod nazivom Eclair ispravljene su mnoge postojeće greške u samom sistemu i dodate dodatne podrške za rad sa kamerom, kao i poboljšana virtualna tastatura. Verzija 2.2 Froyo je prešla na novi kernel 2.6.32, ubrzala je rad sa memorijom i poboljšala performanse samog sistema, V2.3 Gingerbread takođe prelazi na novi kernel 2.6.35 i dodatno poboljšava korisnički interfejs, takođe donosi sa sobom i podršku za veće displeje kao i za neke dodatne senzore. Verzija 3.0 poznata i kao Honeycomb bila je zasnovana na kernelu 2.6.36 i bila je prilagođena tablet računarima, dodati su joj interfejs elementi kao što su system bar i action bar koji su prilagođeni za tablet

računare, takođe pojednostavljena je i upotreba multitaskinga, redizajnirana je i virtualna tastatura tako da omogućiti lakše i brže kucanje a uklonjeni su i neki sigurnosni propusti.

Verzija 4.0 koja nosi naziv Ice Cream Sandwich je trenutno najnovija verzija Android operativnog sistema. Ova verzija donosi redizajnirani korisnički interfejs prilagođen za displeje visoke rezolucije i dizajniran je tako da omogućiti čist i jasan prikaz teksta i grafičkih elemenata na ovakvim displejima. System Bar, uveden još u verziji 3.0 osmišljen je tako da omogućiti brzu navigaciju i na njemu se nalaze tri virtualna tastera, od kojih su dva za navigaciju, i obavljaju ulogu tastera za povratak, back, i home tastera, dok je treći taster, Recent Apps, namenjen za prikaz aplikacija koje rade u pozadini. Uvođenjem Recent Apps tastera multitasking je postao dosta jednostavniji i brži za upotrebu.

Android 4.0 poseduje veoma razvijen interaktivni sistem obaveštenja, kod većine uređaja ova obaveštenja, vezana najčešće za dolazeće poruke ili trenutni rad neke aplikacije, su prikazana u System Bar-u, dok su kod uređaja sa manjim displejom obično prikazana u gornjem delu displeja (slika 2).



Slika 2. Android telefon „meni“

Organizacija radne površine je dosta pojednostavljena, instalirane aplikacije se mogu, radi lakše i brže upotrebe, razvrstati po folderima jednostavnim prevlačenjem ikonica aplikacija na željeni folder, u donjem delu radne površine je obezbeđen prostor za odabrane aplikacije gde korisnik može smestiti najčešće korišćene foldere i aplikacija i na taj način obezbediti veoma brz pristup istim.

Radnoj površini Androida 4.0 se, pored foldera, pomoću widget-a mogu dodati i izlazi pojedinih aplikacija i na taj način se na njoj mogu prikazati razni podaci kao što su trenutno stanje elektronske pošte ili kalendar. Veličina widget-a je promenljiva pa ćete tako biti u mogućnosti da jednostavno organizujete svoje widget-e na radnoj površini. Kako je, između ostalog, cilj nove verzije bilo i pojednostavljenje upotrebe, uvedene su i nove mogućnosti za lock screen koji sada pored svoje osnovne uloge može da posluži i u situacijama kada želite da proverite nove poruke, ili da na brzinu fotografirate neki zanimljiv događaj, takođe lock

screen pri slušanju muzike može da prikazuje naziv trenutne pesme i fotografiju albuma sa kog ta pesma potiče.

Pored standardnog načina za otključavanje telefona, dodata je i mogućnost otključavanja telefona prepoznavanjem lica. Za upotrebu ove mogućnosti se koristi prednja kamera. Još jedna zanimljivost vezana za jednostavniju i bržu upotrebu jeste i mogućnost brzog odgovaranja porukom na poziv, ovo je veoma korisno u situacijama kada niste u mogućnosti da odgovorite na poziv ali želite da obavestite drugu stranu o razlogu za to. Poruku koju želite da pošaljete na ovaj način možete odabrati sa liste poruka namenjenih za ovaj način slanja ili je možete sami naknadno napisati.

Treba naglasiti i da je samo ispisivanje poruka pojednostavljeno, tastatura je redizajnirana i poboljšana tako da je njen odziv znatno bolji, pored toga dodata je i poboljšana mogućnost provere ispravnosti ispisanog teksta, tako da sada tekst koji je pogrešno napisan biva podvučen crvenom linijom a klikom na njega dobijate tri ispravne ponuđene mogućnosti za zamenu pogrešnog teksta ispravnim, kao i mogućnost da uklonite odabranu reč ili da je dodate u rečnik kao ispravnu reč.

Dodatne rečnike namenjene za druge jezike moguće je naknadno preuzeti i instalirati. Android 4.0 Vam daje i mogućnost da tekst poruke diktirate, što je omogućeno posebnim softverom namenjenim za prepoznavanje glasa. Ovaj softver ne samo da Vam daje mogućnost skoro neograničeno dugog diktata, već Vam daje mogućnost i da diktirate tekst na bilo kom jeziku, kao i da diktirate interpunkcijske znake kako bi sročili ispravnu rečenicu. Ipak kako ni ovaj sistem nije u potpunosti precizan i bez greške, moguće greške u diktatu se obeležavaju kao i pri kucanju poruke i njihovo ispravljanje se izvodi na isti način. Pošto je upotreba interneta nezaobilazni detalj svakodnevice bilo je neophodno dodatno unaprediti mogućnosti komunikacije i deljenja sadržaja na globalnoj mreži (slika 3).



Slika 3. Android komunikacija sa internetom

People aplikacija je specijalno namenjena da zadovolji ove potrebe korisnika, ona predstavlja više od prostog adresara, pored toga što čuva podatke o korisnicima kao što su njihovi brojevi telefona, adrese, fotografije i statusi sa profila socijalnih mreža, ona takođe daje mogućnost direktnog pristupa kontaktima preko socijalnih mreža.

Pored ovoga Android Browser predstavlja još jednu bitnu stavku za korisnike interneta, on je dosta unapređen u odnosu na prethodne verzije pa je sada dosta brži i stabilniji, za šta je zaslužno uvođenje nove verzije WebKit jezgra i V8 Crankshaft interpretatora za JavaScript. Neke od zanimljivih i korisnih mogućnosti koje poseduje Android Browser su mogućnost da sa Google Chrome browsera preuzme sadržaj vezan za Vaše omiljene i najposećenije web stranice, kao i da stranice, koje želite da ostavite za kasnije čitanje, sačuva na vašem telefonu i na taj način Vam omogući pristup tim stranicama čak i u slučaju kada Vam internet nije dostupan.

Sačuvanim stranicama možete pristupiti jednostavnim odabirom sa liste sačuvanih stranica na kojoj je pored imena prikazan i izgled same stranice.

Još jedna bitna mogućnost koju Android Browser ima jeste i pun prikaz web stranice, odnosno mogućnost da prikaže stranicu onakvu kako bi ona izgledala da je gledate na računaru, ovu mogućnost je moguće uključiti i isključiti po želji.

Kako je slanje elektronske pošte u današnje vreme neizostavno, unapređena je i aplikacija za ovu namenu, sada ona ima pored standardnog automatskog ispravljanja unetog teksta, koje je prisutno i pri kucanju poruka, i mogućnost da automatski dovrši adresu željenog kontakta, takođe dodata je i mogućnost beleženja najčešće unošenih reči i njihovo automatsko dodavanje u elektronsku poštu, što dosta ubrzava proces sastavljanja pošte.

Za lakšu pretragu email naloga dodat je i integrisani meni sa podacima vezanim za naloge, radi lakšeg organizovanja email naloga i lakše razmene elektronske pošte Email aplikacija sada podržava i ugneždene foldere, od kojih svaki ima svoja pravila za sinhronizaciju. Ugrađena je i mogućnost za pretragu foldera na serveru, radi lakšeg pronalaženja željenih poruka.

Email aplikacija je jedna od aplikacija koje se mogu postaviti na radnu površinu u vidu widget-a i u tom slučaju ona daje pregled dolazećih poruka, kao i mogućnost odgovaranja na iste.

Pošto veliki broj aplikacija napisanih za Android zahteva vezu sa internetom, kontrola protoka podataka je postala neophodna, pa je ona sada ugrađena u vidu aplikacije koja grafički prikazuje količinu dolazećih i odlazećih podataka, kao i listu aplikacija koje su odgovorne za slanje i primanje podataka.

Ova aplikacija sem što prikazuje podatke vezane za protok podataka u mreži daje Vam i mogućnost da pojedinim aplikacijama ograničite količinu protoka ili u potpunosti ugasite pristup internetu, što može biti veoma korisno u slučaju kada ste ograničeni protokom od strane Vašeg provajdera.

Pored povezivanja Android uređaja na internet, omogućeno je i njihovo povezivanje sa drugim uređajima, bez potrebe za internetom, putem Wi-Fi mreže ili Bluetooth tehnologije, što daje mogućnost brže i direktne razmene sadržaja između Vašeg Android uređaja i uređaja na koji ste povezani.

Veliki broj Android telefona je više od običnog telefona, i zapravo prelazi u male multimedijalne uređaje, sa ovim na umu razvijen je i set aplikacija zaduženih za obradu fotografija i video snimaka i njihovo organizovanje.

Aplikacija pod nazivom Camera, kako joj i samo ime kaže, zadužena je za fotografisanje i snimanje sadržaja kamerom ugrađenom u telefon. Ova aplikacija pored svoje osnovne uloge daje i mogućnost proste obrade fotografije i deljenje iste putem elektronske pošte ili socijalnih mreža.

Tokom snimanja videa moguća je njegova obrada u realnom vremenu upotrebom Live Effects kolekcije efekata za obradu video snimaka. Ova kolekcija efekata pruža Vam mogućnosti da izmenite pozadinu video snimka ili da deformišete sliku na bilo koji način, pored toga što je Live Effects kolekcija dostupna u Camera aplikaciji ona je dostupna i u Google Talk aplikaciji gde je možete koristiti u toku video razgovora sa Vašim prijateljima. Pored osnovne podrške za kameru koju obezbeđuje, ova aplikacija je zadužena i za naprednije funkcije kao što su automatski fokus ili prepoznavanje lica.

Android dolazi i uz Gallery aplikaciju koja obavlja posao organizacije fotografija i video snimaka. Organizaciju fotografija možete izvršiti razvrstavanjem fotografija po albumima, vremenu fotografisanja, mestu fotografisanja ili po nekom parametru koji sami odaberete. Kao i aplikacija Camera i Gallery aplikacija ima neke napredne mogućnosti, i ona ujedno služi i za obradu fotografija, pa tako pomoću ove aplikacije možete ukloniti crvenilo u ocima, rotirati fotografije, promeniti im veličinu ili im dodati neke efekte. Kao i većina Android aplikacija i Gallery aplikacija ima ugrađenu mogućnost za deljenje sadržaja putem elektronske pošte, socijalnih mreža ili tekstualnih poruka.

Kako je pristupačnost sistema veoma bitna stavka, sa verzijom 4.0 Android je dobio poboljšanu podršku za slepe i slabovide osobe, tako da je sada moguće uvećati fontove na nivou sistema i uključiti zvučne signale koji se aktiviraju pri prvom pritisku na neki od interfejs elemenata, dok pri drugom pritisku na isti element dolazi do aktiviranja samog elementa. Sve standardne aplikacije su unapređene tako da slepim i slabovidim osobama omoguće jednostavnu upotrebu, takođe Android browser je opremljen skriptovanim čitačem sadržaja koji ima mogućnost da čita sadržaj sa sajtova i ujedno potpomaže u jednostavnoj navigaciji po sajtovima.

Iako Android sada predstavlja veoma zreo i pouzdan sistem iza koga stoji ogroman broj zadovoljnih korisnika, on to ne bi postao bez velike zajednice koja neprestano razvija aplikacije namenjene za ovu platformu i na taj način je čini upotrebljivom i živom, takođe ova zajednica sem što predstavlja životnu podršku za ovaj sistem ujedno predstavlja i glavnu pokretačku silu koja ovaj sistem, sa svakom novom verzijom, čini boljim i jednostavnijim za upotrebu. Pored velike podrške korisnika neizostavna je i podrška velikih firmi koje Android uvode za sastavni deo svojih uređaja i na taj način ga čine dominantnim sistemom za mobilne uređaje.

2.3 Digitalni dokaz

Digitalni dokaz je svaka informacija koja ima dokazujuću vrednost, a koja može biti uskladištena ili prenesena u digitalnom obliku. Pojam digitalnog dokaza, u digitalnoj forenzičkoj nauci, obuhvata kompjuterski uskladištene i generisane dokaze, digitalni audio i video signal, zapis sa mobilnog telefona, zapis sa digitalne fax mašine ili drugih digitalnih uređaja. Međunarodna organizacija za kompjutersku registraciju, International Organization of Computer Evidence (IOCE), propisala je opšte principe i procedure, koje se odnose na digitalne dokaze, za usaglašavanje metoda i praktičnih rešenja među nacijama i koje garantuju međunarodnu razmenu (transnacionalni menadžment) digitalnih dokaza. Nažalost, nigde u svetu još ne postoji verifikacija zvaničnih istražnih organa, forenzičkih analitičara i

pravosudnih organa, podjednako kvalifikovanih u svojim oblastima, da objektivno i tačno vode istragu, forenzičku akviziciju, analizu, dokazni postupak i prezentaciju digitalnih dokaza na sudu. Istraga incidentnog kompjuterskog događaja zahteva uvek timski rad. Za poslove akvizicije i forenzičke analize uvek treba angažovati kvalifikovanog eksperta za informacione tehnologije (IT), specijalistu za konkretni operativni sistem (OS), program, platformu, mrežu, itd.

Obuhvata kompjuterski uskladištene i generisane dokaze, digitalni audio i video signal, zapis sa mobilnog telefona, zapis sa digitalne fax mašine ili drugih digitalnih uređaja.

Digitalni dokazi po tipu mogu biti:

- *optužujući* (povezuju osumnjičenog sa krivičnim delom)
- *oslobađajući* (dokazuju da osumnjičeni nije umešan u konkretno krivično delo)
- *ukazuje* na određenu sumnju (da postoji veza između krivičnog dela i osumnjičenog).

U kompjuterskom incidentu postoje tri osnovne kategorije digitalnih podataka koji mogu činiti digitalni dokaz:

- Promenljivi podaci ili informacije koje se gube nakon isključivanja računara, kao što su podaci u radnoj memoriji (RAM), rezidentni memorijski programi itd.
- Osetljivi podaci ili podaci uskladišteni na čvrstom disku (HD) koji se lako mogu izmeniti, kao što je, npr. poslednje vreme pristupa log datoteci itd.
- Privremeno dostupni podaci, ili podaci uskladišteni na HD kojima se može pristupiti samo u određeno vreme (npr. šifrovani podaci).

2.4 Kompromitovani računar

Pojam kompromitovanog računara najčešće se odnosi na napadnuti računar („žrtvu”), ali, za potrebe forenzičke analize zavisno od konteksta, može obuhvatati i osumnjičeni izvorni, ili posredni računar, jer je u praksi istrage digitalnih dokaza često neophodno izvršiti forenzičku analizu računara sa kojeg je izvršen napad, napadnutog računara i nekog od posrednih računara, na primer preko čijeg naloga je napadač ušao u sistem.

U poslednje vreme pojavom smart mobilnih telefona i uređaja sa operativnim sistemima Android i Apple iOS sve više se pojavljuje kao kompromitovani računar i ovakva vrsta uređaja i kako stvari stoje sve više će se ovakve vrste uradjaja pojavljivati u digitalnoj forenzickoj istrazi.

3 FORENZIČKA AKVIZICIJA DIGITALNIH PODATAKA

3.1 Forenzička akvizicija računara u radu

Akvizicija digitalnih podataka, prva glavna faza digitalne forenzike analogna uzimanju otiska prsta, obuhvata procese otkrivanja, identifikacije i izvlačenja digitalnih podataka za potrebe forenzičke analize digitalnih dokaza. Generalno, potrebno je uzeti fizičku kopiju svakog medija (HD, CD, FD, memorija) i memorisati je na poverljiv, forenzički sterilan disk. Ako je moguće treba snimiti sve locirane i nelocirane podatke sa kompromitovanog računara.

U procesu akvizicije digitalnih podataka iz osumnjičenog računarskog sistema na fizičkom mestu krivičnog dela, forenzičar digitalnih podataka (*digitalni forenzičar*) uobičajeno preduzima sledeće korake:

1. *sprovodi* formalnu proceduru pretrage fizičkog i digitalnog mesta krivičnog dela,
2. *fiksira* fizičko i digitalno mesto krivičnog dela,
3. *dokumentuje* fizičko i digitalno mesto krivičnog dela,
4. *zaštićuje* osumnjičeni računar od izmene podataka i unošenja virusa/trojanca,
5. *isključuje* računarski sistem,
6. *označava i pakuje* sve komponente računarskog sistema,
7. *privremeno oduzima* računarski sistem, ili *imidž* HD i svih drugih medijuma (*radnu i referentnu* kopiju), ako to nije moguće i
8. *prenosi* privremeno oduzeti računarski sistem u forenzičku laboratoriju za forenzičku analizu.

Postoje brojna pitanja sa kojim se forenzičari suočavaju kada isključe osumnjičeni računarski sistem/e i sakupljaju *imidže* sa čvrstih diskova za ispitivanje, od kojih gubici zbog prekida e-transakcija savremenih poslovnih IKT sistema postaju sve značajniji, u uslovima porasta e-trgovine i e-poslovanja uopšte. Tome treba dodati da brojne organizacije na bazi SLA (*Service-Level Agreements*) ugovora imaju garanciju da će sistemi biti u radu 99,999% vremena (izuzev prozora za održavanje). Za uzimanje imidža savremenih čvrstih diskova velikog kapaciteta, na primer, 750GB u RAID aranžmanu sa 5 ili 8 ovakvih diskova, očigledno je potrebno više časova, što za organizaciju može biti neprihvatljivo, ako je za akviziciju diska od 80GB potrebno više od 4 sata. Pored toga često nije potrebno vršiti akviziciju svih podataka, ako je u fazi pretrage i predistražnom postupku otkriveno koji Brojni maliciozni programi za krađu personalnih informacija – pasvorda, ličnih fajlova i drugih ličnih podataka, nisu upisani na čvrsti disk nego postoje samo u memoriji, što znači kada se sistem isključi sve ove informacije nestaju.

U nekim slučajevima, pre ulaska u klasično forenzičko ispitivanje računara, forenzičar ima potrebu da sakupi neke informacije iz sistema koji je još u radu pre njegovog isključivanja i akvizicije bit-po-bit imidža čvrstog diska. Informacije za koje forenzičar može biti najviše zainteresovan su promenljive, nestabilne (*volatile*) i kratkotrajne informacije, koje prestaju da postoje kada se napajanje računara isključi. Ove nestabilne informacije obično postoje u fizičkoj memoriji - RAM-u i sastoje se od informacija o procesima, mrežnim vezama, sadržajima *clipboard*-a itd. Ove informacije opisuju stanje sistema u trenutku kada je forenzičar ispred njega. Forenzički istraživač može često biti u situaciji da izvrši brzo akviziciju podataka da bi odredio prirodu incidenta.

Na raspolaganju su alati i tehnike za sakupljanje nestabilnih informacija iz živog sistema, koje daju bolji uvid u stanje sistema i veći obim ukupnih informacija. Dakle, forenzičko ispitivanje računara u radu (*live response*) obuhvata procenu živog sistema u radu i sakupljanje nestabilnih, a u nekim slučajevima i drugih informacija. Sa ovim ne treba mešati pojam akvizicije podataka sa računara u radu (*live acquisition*) koja znači uzimanje imidža čvrstog diska sa računara u radu.

3.1.1 Lokardov princip razmene materije

U procesu forenzičkog ispitivanja računara u radu, forenzičari i članovi interventnog tima treba da imaju na umu važan princip – da će doći do promene u sistemu koji je u radu posle interakcije korisnika, ili forenzičara sa sistemom. U sistemu koji je u radu, promene će se dogoditi jednostavno zbog protoka vremena, rada procesora, skladištenja i brisanja podataka, uspostavljanja i ukidanja mrežnih konekcija itd. neke promene se dešavaju i kada je sistem samo uključen i nema nikakvih aktivnosti sa interfejsa. Promene se dešavaju i kada forenzičar pokrene forenzički alat za uzimanje imidža. Aktiviranje nekog programa izaziva upisivanje informacija u fizičku memoriju, a fizička memorija koju već zauzima neki proces u radu može isprazniti svoj sadržaj u *page* fajl. Kada forenzičar sakupi informacije i pošalje ih izvan sistema, kreira se nova mrežna konekcija. Sve ove promene mogu se zajedno objasniti *Lokardovim, principom razmene materije*: kada dva objekta dođu u kontakt između njih se razmenjuje ili prenosi materija. Primeri su, kada automobil udari u čoveka, a forenzičar ispituje žrtvu i locira materijal koji je dislociran sa mesta udesa. Isti se princip odnosi i na digitalno okruženje, na primer, kada dva računara komuniciraju u mreži, informacije se razmenjuju između njih. Informacija o jednom računaru pojaviće se u memoriji procesa i/ili log fajlovima u drugom računaru, ili kada se prenosni disk priključi na Windows računarski sistem, rezidenta informacija o uređaju ostaje u računaru. Kada forenzičar pristupi računaru u radu, dogodiće se promene u sistemu kako se izvršava forenzički program i podaci kopiraju sa sistema. Ove promene mogu biti prenosne – memorija procesa, mrežne konekcije, ili trajne – log fajlovi, ulazi Registra. Za demonstraciju Lokardovog principa razmene materije može se iskoristiti jednostavan alat kao što je **netcat** (*nc.exe* u Windows sistemu) za pisanje i čitanje informacija kroz mrežne konekcije. Programi koje forenzičar koristi za skupljanje informacija mogu imati druge efekte na živi system. Na primer, neki forenzički alat treba da čita nekoliko ključeva registra, a putanja do ovih ključeva biće očitana u memoriju. Windows XP OS izvršava *prefetching* aplikacija (pre aktiviranja uzima ih iz memorije i skladišti u registar), tako kada forenzičar aktivira program kojeg je korisnik već aktivirao na sistemu, biće modifikovano vreme poslednjeg pristupa *prefetch* fajlu, kao i sadržaj samog fajla. Ako program kojeg forenzičar pokrene nije ranije korišćen, biće kreiran novi *prefetch* fajl u *prefetch* direktorijumu, pod pretpostavkom da *prefetch* direktorijum nije dostigao svoj 128 .**pf** granični fajl. Forenzičari ne samo da moraju znati da se ove promene dešavaju, već ih moraju i dokumentovati i objasniti efekte svojih akcija na sistem u razumnom obimu. Na primer, forenzičar treba da odredi koji su .**pf** fajlovi u XP *prefetch* direktorijumu rezultat njegovih aktivnosti, a koji aktivnosti korisnika. Isto važi za vrednosti registra. Akcija forenzičara ažurira vreme poslednjeg upisa entrija u ključevima registra. Neke od ovih promena nisu rezultat akcije alata, nego ih pravi Windows Explorer, jednostavno zbog činjenice da je sistem živ i aktivan. Testiranjem i razumevanjem forenzičkih alata, forenzičar može dokumentovati i objasniti koji su artefakti na sistemu rezultat akcija forenzičara, a koji su rezultat akcija korisnika ili napadača.

Sve nestabilne informacije nemaju jednako vreme trajanja. Na primer, mrežne konekcije nestaju ponekad za nekoliko minuta, ako se ne koriste. Ovo se može videti gledanjem mrežnih konekcija u **netstat.exe** alatu. Međutim, sistemsko vreme se menja mnogo brže, dok će sadržaj *Clipboard* ostati sve dok se ne promeni, ili napajanje sistema ne isključi.

Pored toga neki procesi, kao što su servisi, rade dugo vremena, dok drugi procesi rade ekstremno kratko vreme, brzo izvršavajući svoje zadatke pre nestanka iz memorije. Ovo znači da forenzičar treba da sakupi neke informacije pre od drugih nestabilnih informacija. Generalno forenzičar može sa sistema u radu sakupiti značajne informacije, vodeći detaljne zabeleške o svakoj akciji, notirajući svaku razliku između UTC, lokalnog i sistemskog vremena i minimiziranjem promena datuma, za slučaj pravosudnih zahteva nekoliko godina kasnije.

3.1.2 Redosled sakupljanja nestabilnih podataka

Forenzičar prvo treba da sakupi informacije o statusu mrežnih konekcija, a najmanje promenljive informacije kao što je fizička konfiguracija sistema, treba sakupljati poslednje. U većini slučajeva kompjuterskog kriminala, civilne parnice, ili interne korporacijske istrage ne postoje predefinisani uslovi za primenu forenzičke istrage živog računara, popšto postoje brojni slučajevi gde se nestabilne informacije uopšte ne razmatraju. Razlozi za forenzičko ispitivanje živog računara zavise od specifičnosti (politike, regulativa i zakona) i prirode slučaja, a najčešće sam forenzičar treba da donese tu odluku. Na primer, administrator mreže zapazi neobičan saobraćaj u mreži, kojeg alarmira IDS sistem, a proverom log fajla *firewall*-a utvrđen sinhronizam i da je napad došao iz mreže, što potvrđuje i MAC adresa, ali je potrebno ovom saobraćaju pridružiti proces, ili korisnika. U tom slučaju forenzičar treba da izvrši ispitivanje živog sistema, da definitivno utvrdi izvor sumnjivog saobraćaja i koji ga proces generiše, da sakupi informacije o aktivnim procesima i mrežnim konekcijama, pre isključivanja sistema. Druge informacije sakupljene u ovom ispitivanju mogu pokazati da je neko logovan u sistem sa daljine preko mrežnog logovanja, ili kroz zadnja vrata, ili je aktivni proces pokrenut kao zadatak po rasporedu (*Scheduled Task*). Takođe, ovo ispitivanje je nezamenljivo u slučaju utvrđivanja da je u korumpiranom računaru aktivan Trojanac.

Generalno, sakupljanje informacija iz RAM memorije i njihova analiza su relativno nove oblasti digitalne forenzike (od 2005. godine). Iz RAM memorije mogu se izvući sledeće informacije:

- sistemsko vreme,
- logovani korisnici,
- otvoreni fajlovi,
- mrežne informacije,
- mrežne konekcije,
- informacije o aktivnim procesima,
- mapiranje procesa i portova,
- memorija procesa,
- status mreže,
- sadržaj *Clipboard*-a,
- informacije o servisu/drajveru,
- istorija komandi,
- mapirani drajvovi,
- deljeni fajlovi/direktorijumi.

3.1.3 Izbor i priprema alata

Za sve ove informacije mogu se izvlačiti odgovarajućim alatima tipa:

- Komandne linije (*CLI-Command Line Interface*) koji imaju manji “otisak u memoriji”, što znači da koriste manje memorije, oslanjaju se na manje DLL (*Dynamic Link Libraries*) i imaju manji uticaj na sistem. Ovi se alati lakše koriste, jednostavni su, izvršavaju specifične funkcije i lako se automatizuju kroz korišćenje batch ili skript fajlova, a izlaze šalje na komandnu liniju;

- Alati GUI tipa, tipično zahteva skladištenje izlaza u neki fajl. Kako je cilj forenzičkog ispitivanja živog računara da se ostvari što manji uticaj na ispitivani sistem, forenzičar treba da izbegava upotrebu GUI alata koji upisuje izlazne rezultate u fajl sistem, ali ne po svaku cenu. Ako forenzičar zna kako će podatke izvući iz fajl sistema i ako alat odgovara nameni, treba ga koristiti.

Osnovni korak u dokumentovanju forenzičkog alata čini *statičko* i *dinamičko* testiranje alata. *Statičko testiranje* uključuje dokumentovanje jedinstvenog identifikatora o alatu, kao što su:

- URL sa kojeg je dobijen softverski alat,
- veličina fajla,
- kriptografski heš za fajl, korišćenjem poznatog algoritma,
- izvlačenje informacija iz fajla, kao što su PE hederi, tip fajla, tabele *import/export* itd.

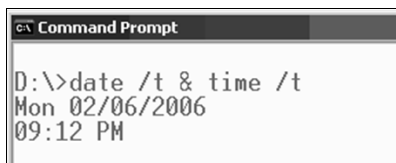
Ove se informacije lako izvlače korišćenjem alata komandne linije i programskih jezika, a ceo proces sakupljanja podataka može se automatizovati.

Dinamičko testiranje podrazumeva aktivan rad forenzičkog alata i korišćenje programa za monitorisanje promena koje alat izaziva u sistemu, tipa *RegMon* i *FileMon*. Aktivni procesi pristupaju ključevima i fajlovima Registra, ali isto i kreiranim i modifikovanim fajlovima. Alat tipa *Wireshark* može se koristiti za monitorisanje ulaznog i izlaznog saobraćaja u/iz sistema za testiranje forenzičkih alata, posebno ako statička analiza alata otkrije da alat uvozi mrežne funkcije iz drugih DLL.

Primer: Forenzičar može izvući sistemsko lokalno vreme i datum na bazi vremenske zone i usklađivanja vremena sa dnevnim svetlosti, korišćenjem jednostavnog Perl skripta, kao što je:

```
print localtime(time)."\n", ili za prikazivanje vremena u GMT foramatu sa:  
print gmtime(time)."\n";
```

Sistemsko vreme i datum iz *Command Prompt* u Windows XP OS prikazano je na slici 4.



Slika 4. Sistemsko vreme i datum u Windows XP OS

3.1.4 Metodologija akvizicije živog računara

Metodologija akvizicije živog računara zavisi od brojnih faktora. Najbolji pristup je imati potpuno razumevanje o tome šta je forenzičaru dostupno i šta može uključiti u set forenzičkih alata, a na bazi toga doneti odluku o tome kako raditi u konkretnom slučaju. Postoje dve bazične metodologije akvizicije živog računara na Windows platformi: *lokalna*, *udaljena* i *hibridna*, [4]

Metodologija lokalne akvizicije živog računara podrazumeva da forenzičar sedi za tastaturom sistema, unosi komande i skladišti informacije lokalno, direktno na čvrsti ili prenosni disk (USB - spojen spoljni disk), ili na zajednički mrežni lokalni resurs. Lokalno sakupljanje informacija sa nekoliko sistema može biti znatno brže nego lociranje mrežne konekcije ili bežični pristup mreži. Sa odgovarajućim kapacitetom spoljne memorije, svim potrebnim forenzičkim alatima na CD-i i sa pravim nivoom pristupa, forenzičar može brzo i

efikasno sakupiti potrebne informacije. Najjednostavniji način da se implementira lokalna metodologija je sa kreiranjem *bach* fajla i nekog skripta, na primer, Perl skripta koji se upiše samo jedanput i sa ovom komandom pokreće se automatski. Primer jednostavnog *bach* fajla koji se može koristiti u toku forenzičke akvizicije živog računara izgleda kao:

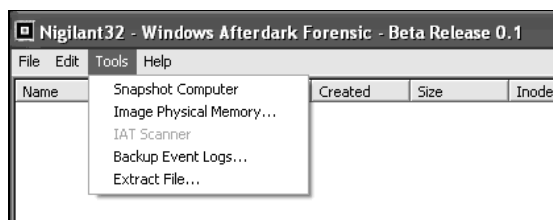
```
tlist.exe -c > %1\tlist-c.log
tlist.exe -t > %1\tlist-t.log
tlist.exe -s > %1\tlist-s.log
openports.exe -fport > %1\openports-fport.log
netstat.exe -ano > %1\netstat-ano.log
```

Ovde su data tri korisnička alata i pet komandi. Ovi fajlovi se memorišu kao **local.bat** i uključe se na CD sa alatima. Na CD treba dodati sigurne kopije komande procesora (**cmd.exe**) za svaki OS. Pre aktiviranja batch fajla, treba pogledati u sistem i videti koji su mrežni drajvovi raspoloživi, ili ubaciti USB memoriju u sistem i videti koje se slovo drajva dobija (npr., G:\), zatim aktivirati *bach* fajl (ako je CD-ROM na D particiji):

```
D:\>local.bat F:
```

Kada se *bach* fajl kompletira, na USB-u će biti pet fajlova. Zavisno od vrste podataka koje forenzičar želi izvući iz sistema, u batch fajl se mogu dodati različite komande. Postoji nekoliko raspoloživih alata dizajniranih za upotrebu u lokalnom sakupljanju podataka sa živog računara, kao što su *Incident Response Collection Report (IRCR)* v. 2.60 i *Windows Forensic Toolkit 61. (WFT)*. Iako se ovi alati razlikuju po implementaciji i izlazu, osnovne funkcionalnosti oba alata su u suštini jednaka: aktiviraju eksterne izvršne fajlove koje kontroliše Windows *batch* fajl i lokalno skladište izlazne rezultate. *WFT* alat skladišti sirove podatke i dopušta forenzičaru da pošalje izlaze komandi u HTML izveštaj.

Drugi pristup za razvoj metodologije lokalne forenzičke akvizicije računarskog sistema je da se enkapsulira što je moguće više funkcija u jednu aplikaciju koja koristi Windows API, kao što je **Nigilant32** (*Agile Risk Management LLC*). **Nigilant32** koristi isti Windows API poziv kojeg koriste spoljni alati za sakupljanje nestabilnih informacija sa sistema, (slika 5). Alat ima mogućnost da izvrši proveru fajl sistema i isprazni sadržaj fizičke memorije, (RAM).



Slika 5. GUI alat Nigilant (32)

Forenzički alati koji koriste *batch* fajl upotrebljavaju izvršne fajlove koji koriste iste, ili slične Windows API pozive kao i drugi alati tipa **Nigilant32**.

Metodologija daljinske akvizicije generalno se sastoji od serije komandi koje se izvršavaju na sistemu kroz mrežu. Ova metodologija je korisna za više sistema, pošto se proces logovanja u sistem i komande mogu lako automatizovati. Neki alati rade odlično u kombinaciji sa **psexec.exe** iz *SysInternals.com*, a dodatne informacije mogu se lako sakupiti korišćenjem **WMI** (*Window Management Instrumentation*). Bez obzira koji pristup forenzičar primeni treba da ima na umu da su mu potrebni lični podaci za logovanje u svaki

sistem i da svaki put kada se uloguje, treba da pokrene komande, sakuplja podatke i šalje ih u log fajl bezbednosno relevantnih događaja.

Ovo znači da se redosled sakupljanja nestabilnih podataka neznatno pomera i da treba prvo sakupljati podatke iz sadržaja log fajlova bezbednosno relevantnih događaja. Windows *batch* fajl se može koristiti kao baza za implementaciju ove metodologije. Uzimajući tri argumenta u komandnoj liniji – ime ili IP sistema i korisničko ime/pasvord informacije za logovanje, forenzičar može napraviti skript serije komandi za sakupljanje potrebnih informacija. Neke komande za izvršavanje trebaju fajl **psexec.exe**, koji kopira izvršni fajl na udaljeni sistem, pokreće ga i dopušta forenzičaru da sakuplja izlaze sa standardnog izlaza (STDOUT), ili preusmeri izlaz na fajl, kao kada se komande koriste lokalno. Druge komande će uzeti UNC putanju (\\) i informacije za logovanje kao argumente, pa nema potrebe za korišćenja fajla **psexec.exe**. Konačno, **WMI** se može implementirati preko *VBScripta* ili *Perl* za sakupljanje podataka. Microsoft obezbeđuje repozitorijum 63. skript sa brojnim primerima **WMI** kôda implementiranim u različitim jezicima za uključivanje *Perl*64. Implementacija *batch* fajla lokalne metodologije za metodologiju udaljenog pristupa prilično je trivijalna:

```
psexec.exe \\%1 -u %2 -p %3 -c tlist.exe -c > tlist-c.log
psexec.exe \\%1 -u %2 -p %3 -c tlist.exe -t > tlist-t.log
psexec.exe \\%1 -u %2 -p %3 -c tlist.exe -s > tlist-s.log
psexec.exe \\%1 -u %2 -p %3 -c openports.exe -fport > openports-fport.log
psexec.exe \\%1 -u %2 -p %3 c:\windows\system32\netstat.exe -ano >
%1\netstat-ano.log
```

Ovaj *batch* fajl (**remote.bat**) nalazi se u sistemu forenzičara i aktivira se na sledeći način:

```
C:\forensics\case007>remote.bat 192.168.0.7 Administrator password
```

Kada se jednom *batch* fajl kompletira, forenzičar ima na izlazu komande u 5 fajlova, spremne za analizu. Ako forenzičar nije vešt programer, a želi koristiti **WMI** za skupljanje informacija sa daljine, korisno je pogledati fajl **wmic.exe**. Ovaj fajl sadrži primere sakupljanja liste instaliranih pečeva sa udaljenog sistema. Cela klasa fajloga Win.32 može se ispitati sa **wmic.exe**. Na primer da se na ekranu udaljenog sistema prikaže aktivni proces na lokalnom računaru može se koristiti prilično jednostavna i direktna komanda:

```
C:\>wmic PROCESS GET ProcessId,Name,ExecutablePath
```

Uključivanjem nekoliko **wmic.exe** komandi u *batch* fajl, forenzičar može sakupiti širi opseg podataka sa udaljenog sistema, korišćenjem dodatnih svičeva kao što su

```
/Node:
```

```
/User:
```

```
/Password:
```

Forenzičar može preusmeriti izlaz u fajl različitog tipa CSV (za otvaranje u Excel-u ili parsiranje u Perlu) ili HTML tabele.

Sa druge strane administrator može koristiti ove komande za kompajliranje liste inventara hardvera i softvera i određivanje sistema koji zahtevaju ažuriranje sa novim pečevima i sl. **WMI** je moćan interfejs za upravljanje Windows sistemima, **wmic.exe** obezbeđuje laki pristup za automatizovane komande. Sa ispravni upravljanjem greškama, oporavkom sistema i logiovanjem u kodu, ovo može biti visoko efektivan i skalabilan metod za brzo sakupljanje informacija sa brojnih sistema, upravljanje i skladištenje sa jedne centralne lokacije: Ovu metodologiju implementira komercijalno raspoloživ alat **ProDiscover Incident Response (Technology Pathways)**. Sa centralne lokacije forenzičar može instalirati

jednog softverskog agenta, preko kojeg će tražiti korisne informacije, a zatim izbrisati agenta. Pomoću *ProScript API* ovog alata forenzičar može sa dodatnim programom (u *Perl* npr.) automatizovati ceo proces, što minimizira broj logovanja u *Security Event Log* i količinu softvera kojeg treba instalirati na udaljeni sistem. **ProDiscover IR**, takođe poseduje dodatne kapacitete za izvlačenje sadržaja iz fizičke memorije, kao i za izvršavanje *žive akvizicije* podataka sa računara u radu. Osnovno ograničenje ovog metoda žive akvizicije digitalnih podataka sa udaljene lokacije je što se forenzičar mora logovati na sistem kroz mrežu. Ako je na bilo koji način restriktivan sistem logovanja preko *NetBIOS* (Windows platforme), na primer *NetBIOS* nije instaliran, *firewalls/ruteri* blokiraju protokole i sl., ova se metodologije neće moći primeniti.

Hibridna metodologija žive akvizicije: Ovaj metod je kombinacija lokalne i daljinske metodologije žive akvizicije. Najčešće se primenjuje u situacijama kada se forenzičar ne može ulogovati u sisteme sa udaljene lokacije, a želi sakupiti sve informacije sa više sistema i uskladištiti podatke na centralnoj lokaciji. Forenzičar ili asistent tada odlaze do sistema sa forenzički sterilnim CD ili USB i blokatorom upisivanja, pristupa sistemu i aktivira alat za sakupljanje informacija. Kada se alati izvrše, svaki od njih šalje izlaz preko mreže na centralni *forenzički server*. Na ovaj način ne vrši se logovanje sa udaljene lokacije, poverljivi alati rade sa neizmenjenih izvora, a vrlo malo ima upisa na HD računara 'žrtve'. Sa dobrim planiranjem, smanjenjem grešaka, redukcijom ulaznih komandi, forenzičar može minimizirati interakcije sa sistemom. Najjednostavniji način primene hibridnog metoda žive akvizicije je sa upotrebom *bach* fajla.

Forenzičarima je na raspolaganju širok skup alata sa različitim funkcionalnostima i namenama. U procesu žive akvizicije treba koristiti alat koji obezbeđuje transport sakupljenih informacija sa udaljenog računarskog sistema do centralnog forenzičkog servera. Dobar alat za ovu svrhu je **Netcat**, tzv. „*TCP/IP švajcarski nož*“, zbog raznovrsnih mogućnosti. Pored brojnih funkcija, u ovom slučaju alat se koristi za transport informacija sa jednog sistema na drugi. Prvo se mora podesiti 'primalac' na forenzičkom serveru sa komandom:

```
D:\forensics>nc -L -p 80 > case007.txt
```

Ova komandna linija kaže alatu **Netcat** (*nc.exe*) da sluša na portu 80 (teško se ostvaruje držanje *nc.exe* otvorenog kada se konekcija zatvori) i sve što dođe na taj port pošalje (preusmeri) u fajl nazvan **case007.txt**. Sa ovim podešavanjem, lako se može modifikovati *batch* fajl umesto upisivanja izlaza komandi za fajlove, a zatim poslati kroz **netcat** do *primaoca* na forenzičkom serveru:

```
tlist.exe -c | nc %1 %2
tlist.exe -t | nc %1 %2
tlist.exe -s | nc %1 %2
openports.exe -fport | nc %1 %2
netstat.exe -ano | nc %1 %2
```

Ovaj fajl se uskladišti kao **hybrid.bat**, zatim se lansira iz komandne linije kao sa (**D:** je CD-ROM):

```
D:\>remote.bat 192.168.1.10 80
```

Kada se jednom pokrene ovaj *batch* fajl, svi podaci se bezbedno prenosi sa računara žrtve na forenzički server za bezbedno čuvanje i analizu.

Ovu metodologiju implementira nekoliko *freeware* alata, npr., **Forensic Server Project (FSP)**. **FSP** je alat otvorenog koda, pisan u *Perl* i besplatan. Ideja za **FSP** je nastala posle upotrebe **netcat**, gde forenzičar pokreće alat na sistemu žrtve sa CD-a, a zatim kanališe izlaze komandi kroz **netcat**, koji je odgovoran za slanje informacija na očekujući forenzički server. Ovo dobro radi u nekim situacijama, ali kada se broj komandi poveća i komande imaju širi opseg argumenata raste broj grešaka i metodologija postaje teška za primenu. Tako je nastao alat **Forensic Server Project**, koji automatizuje sakupljanje, skladištenje i upravljanje podacima žive akvizicije. **FSP** sadrži dve komponente: *server* i *klijent*. Serverska komponenta je poznata kao **FSP**. Forenzičar treba da kopira fajlove sa **FSP** na forenzičku radnu stanicu – forenzički Laptop i kada se aktivira - **FSP** će čekati za konekcije. **FSP** upravlja sa zadacima, logovanjem i skladištenjem u forenzičkom slučaju. Kada se primi konekcija od klijentske komponente, **FSP** reaguje u skladu sa različitim komandama koje dobija. Tekuća iteracija klijentske komponente - **FRU** (*First Responder Utility*), unosi se na računar žrtve sa CD ili USB. **FRU** je jednostavan uslužni alat koji se koristi za sakupljanje informacija sa računara žrtve. Kada **FRU** primi komandu, uzima izlaz komande i šalje ga na **FSP**, koji skladišti informacije i loguje aktivnosti. **FRU** može da sakuplja specifične vrednosti registra, ili vrednosti specifičnih ključeva registra.

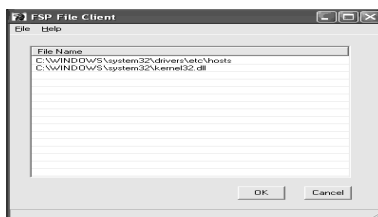
Kada su sve komande pokrenute i svi podaci sakupljeni, **FRU** saopštava **FSP** da može zatvoriti log fajl. **FRU** se kontroliše sa fajlom za inicijalizaciju **.ini** fajl (sličan **INI** fajlovima starog OS Windows 3.1) koji sadrži 4 sekcije:

1. [**Configuration**] – sa podrazumevanim podešavanjem da se **FRU** spaja sa **FSP** preko porta 80, koje se može promeniti sa komandne linije;
2. [**Commands**] – listira TTP alate za sakupljanje informacija, što može biti bilo koji Windows portabilni izvršni fajl (*PE-Portable Executable*) koji šalje svoj izlaz na konzolu forenzičkog servera. Format ove sekcije je različit i vrlo važan. Format svake linije izgleda:
 - a. **<index>=<command line>::<filename>**. Index je naredba koju forenzičar želi da se izvrši, npr., za određivanje redosleda izvršavanja komandi. Komandna linija sadrži komande kao u komandnom *promptu* na računaru;
3. [**Separators**] - prve dve sekcije su odvojene znakom jednakosti (=) iza kojeg sledi znak (::), a konačne sekcije jedne od ovih linija odvojene su sa (;), a kako nekoliko alata (*psloglist.exe* od *SysInternals.com*) imaju mogućnosti korišćenja ovog znaka, autor je morao izabrati drugi znak.
4. [**Names**] – ime fajla koji treba da se generiše, najčešće ime alata sa **.dat** ekstenzijom. Na ovaj način podaci se mogu sakupljati sa više sistema koristeći istu aktivnu instancu **FSP**.

Važno je znati da treba izmeniti ime TTP alata kojeg forenzičar koristi sa **FRU**, pošto alat reaguje sa sistemom žrtve. Dobra ideja je da su imena fajlova jedinstvena (npr. , kao **f_** ili **fru_**) da bi se artefakti na računaru žrtve razlikovali od standardnih artefakta Windows OS. Jedan primer uzet iz **FRU INI** fajla izgleda:

```
6=openports.exe -fport::openports.dat
```

Postoje i drugi klijenti dostupni za kopiranje fajlova i slanje sa računara žrtve. Na slici 6. prikazan je GUI klijenta za kopiranje fajla ili **FCLI**.



Slika 6. GUI klijenta za kopiranje fajla

Korišćenjem **FCLI** klijenta za kopiranje fajlova forenzičar jednostavno aktivira klijenta i selektuje **File** zatim **Config** da uđe u IP adresu i port **FSP** servera. Zatim selektuje **File** i **Open** i izabere fajlove koje želi kopirati. Kada su fajlovi za kopiranje selektovani forenzičar jednostavno klikne **OK** komandu. **FCLI** prvo sakuplja **MAC** vremena fajla i druge metapodatke, zatim računa heš vrednost fajla (MD5 i SHA-1). Ove se informacije šalju **FSP** serverskoj komponenti na forenzičkom računaru. Zatim **FCLI** kopira binarne sadržaje fajla na server. Kada se operacija kopiranja kompletira, **FSP** server računa heš vrednosti kopiranog fajla i verifikuje prema vrednostima heša dobijenim od **FCLI** pre operacije kopiranja. Sve ove aktivnosti se događaju automatski, bez ikakve interakcije forenzičara i sve ih **FSP** loguje.

Forenzički alat **Forensic Server Project** se isporučuje na DVD, na kome su uključeni filmovi koji ilustruju kako se podešava alat za upotrebu i daju instrukcije gde se može nabaviti potreban reproducer.

3.2 Prednosti žive forenzičke analize

U slučaju kompjuterskog incidenta organizacije, odnosno administratori često pribegavaju naizgled najjeftinijem rešenju tipa “*wipe-and-reload*”: formatiraju i izbrišu HD sa prepisivanjem, a zatim ponovo instaliraju OS sa čistog medija, ažuriraju sve zakrpe i hot fiksove, a reinstaliraju aplikacije i podatke sa bekapa. Međutim, ovaj pristup ne može, na prvom mestu, odrediti *kako* se incident dogodio. Korisnik može misliti da je izvedenom operacijom otklonio uzrok incidenta, što apsolutno ne mora biti slučaj. Svi incidenti se ne događaju zbog neinstaliranja zakrpa, ili *hotfix*-ova. Ponekad je uzrok incidenta slab pasvord, ili nepostojanje pasvorda na nalogu korisnika ili aplikaciji, kao što je *sa* pasvord na SQL Serveru, ili loše konfigurisani servis. Nikakav skup zakrpa ne može otkloniti da se ovi uzroci incidenta ne ponove. Ako korisnici/vlasnici sistema ne odrede kako se incident dogodio i ne otklone uzrok, velika je verovatnoća da će se incident ponovo dogoditi.

Pored toga, na računaru koji je aktivan forenzičar može otkriti veliku količinu značajnih informacija, kao što su podaci iz fizičke memorije, aktivni procesi, mrežne konekcije i sadržaji *clipboard* koji mogu imati značajan uticaj na forenzičku istragu.

4 Digitalna Forenzička analiza računara

4.1 Priprema za forenzičku analizu računara

Osnovni zadatak svakog forenzičara je otkrivanje, izvlačenje iz računara, analiza i rad sa digitalnim podacima. Bez obzira na ulogu uslužaju kompjuterskog kriminala, digitalni forenzičar mora poznavati prirodu digitalnih podataka i kako rukovati sa njima. Digitalni podaci se mogu skladištiti u savremenim računarima u enormnim količinama. Čvrsti diskovi su dostigli kapacitet preko 700GB, a tu su i kapaciteti web servis provajdera na Internetu koji se još uvek ne koristi u dovoljnoj meri. Ogromnu većinu digitalnih podataka generišu korisnici. Prvi forenzičari početkom 1990-tih počeli su razvoj alata za izvlačenje i oporavak podataka iz kompromitovanih računara koji obezbeđuju integritet ispitivanih podataka. Proces je poznat kao uzimanje fizičke (miror slike, imidža) ispitivanog računara. Forenzička analiza digitalnih podataka i računara došla je u fokus forenzičke nauke kao novi tip uzimanja dokaza, pored tradicionalnih vidova dokaza – otiska prsta, DNK, analize krvi itd. Iako digitalna forenzika ima verifikovane metode i testove, uključujući široko prihvaćene hardverske i softverske alate, još je u ranoj fazi razvoja. Proces uzimanja imidža ispitivanog računara koristi jednostavan koncept kojeg izvršava alat dizajniran za tu namenu. Za prvo uzimanje imidža računara korišćen je Northon Ghost i drugi raspoloživi softverski alati. Razlozi za potrebu uzimanja imidža ispitivanog računara sasvim su opravdani. Zvanični organi istrage moraju na sudu dokazati da su digitalni podaci upravo onakvi kakvi su bili u računaru u trenutku pretrage i privremenog oduzimanja. Istraga kompjuterskog kriminala znatno je napredovala od kada sudija ne može da dovede u pitanje integritet digitalnog dokaza. Ako se dokazi ne mogu dovesti u pitanje, onda se može postaviti pitanje procesa korišćenog za dobijanje dokaza. Otuda potreba da se za izgradnju čvrstog digitalnog dokaza mora koristiti pouzdan metod.

Uzimanje bekapa digitalnih podataka u prvim danima razvoja digitalne forenzike, bilo je bolje od ničega, ali su u većini slučajeva bekapovani samo fajlovi ispitivanog sistema, a ne i svi dokazi koji se mogu naći na aktivnom fizičkom disku ispitivanog računara. Upravo uzimanje imidža ispitivanog računara obezbeđuje uzimanje svih raspoloživih dokaza. NIST definiše ključne karakteristike forenzičkih alata za uzimanje imidža ispitivanog diska, koji treba da:

1. generišu duplikat bit-po-bit, ili fizičku sliku originalnog diska, ili particije;
2. ne menjaju originalni disk;
3. mogu verifikovati integritet fajli imidža diska;
4. imaju poznate ulazne i izlazne greške logovanja i da;
5. imaju dokumentaciju, obezbeđuju tačne rezultate i ne menjaju digitalne podatke.

Preporučuje se uzimanje dve kopije imidža ispitivanog računara, jednu za analizu i drugu kao referentni original za potrebe suda. Sa pravosudnog aspekta, pravilo najboljeg dokaza zahteva da je dokaz original. Od trenutka uzimanja imidža originalnog, osumnjičenog računara, pa do eventualnog zahteva sudije za originalnim dokazom u toku suđenja, može proći dosta vremena, a može se desiti da je osumnjičeni računar već ponovo u upotrebi (na primer, poslovni server). Otuda je jasno da je najbolji dokaz i najbliži stvarnom originalu, upravo imidž kopija koja se čuva u lancu istrage kao referentna za potrebe suda.

Digitalni forenzičar analizira drugu, radnu imidž kopiju sa raspoloživim forenzičkim alatima, pretražuje fajl sistem i ekstrahuje relevantne podatke za izgradnju čvrstih dokaza. Imidž originala obezbeđuje takođe i pravljenje više radnih kopija za eventualnu analizu na različitim mestima, ili u drugoj državi. Iz imidža se može i ponovo reprodukovati originalni disk, ako je potrebno za prikazivanje šta je osumnjičeni tačno imao na svom računaru, ili za detekciju virusa i trojanaca. Postoje brojni forenzički alati za akviziciju i analizu digitalnih podataka, a najviše se koriste En Case, Vogon, Safeback, iLook, FTK Imager i DD. Formati i funkcionalnosti relevantnih forenzičkih alata mogu varirati, pa ih je potrebno testirati na NIST zahteve za forenzičke alate.

Treba reći da imidž diska uzet bit-po-bit, predstavlja tačnu kopiju diska sa koga je uzet imidž, ali nije potpuno isti kao autorski (proprietary) imidž, format kojeg su razvili neki proizvođači da radi sa njihovim softverom. U nekim slučajevima ovaj se imidž može smatrati sasvim dobrom kopijom originalnog diska, jer se razlika može objasniti, ako to sud zahteva.

Kod uzimanja imidža treba imati forenzički disk isti, ili veći od originalnog, ako kapacitet nije suviše velik. U slučaju uzimanja imidža diska od 700GB treba imati forenzički disk istog kapaciteta, ali je moguće i manji ukoliko forenzički alat za uzimanje imidža može vršiti i kompresiju signala, [9]. Bilo koji metod da se izabere za uzimanje imidža osumnjičenog računara, ili za izvlačenje i čuvanje dokaza, ili da je metod uzimanja imidža potpuno prihvatljiv, zahteva se da digitalni forenzičar može ponoviti i obezbediti iste rezultate u toku istrage.

Iako je većina tehnika forenzičke analize dizajnirana za uzimanje imidža diskova različitih veličina, neki stariji uređaji mogu stvoriti probleme, jer nisu sasvim kompatibilni sa savremenim tehnologijama. Kod uzimanja imidža DOS diskova, forenzičari nemaju veće probleme, jer DOS veoma dobro štiti integritet podataka, što nije slučaj sa Windows OS. Otkada je Windows OS postao standard, digitalni forenzičari u procesu uzimanja imidža moraju koristiti blokatore upisivanja, da bi sačuvali integritet podataka.

Drugi potencijalni problem je uzimanje imidža čvrstog diska smeštenog na glavnoj ploči, kao kod Laptop računara, jer uklanjanjem diska sa ploče podaci više nisu čitljivi. Takođe, serveri mogu stvoriti probleme forenzičaru. U suštini, sa aspekta digitalne forenzike, server je samo računar i može biti potpuno isti kao ostali računari na lokaciji, ali i sasvim različit. Tako problem predstavljaju serveri ugrađeni u rekeve sa RAID diskovima, jer forenzičar mora razumeti sve veze pre preduzimanja bilo koje akcije. Takođe, postojeći forenzički alati i oprema nisu dovoljni za akviziciju i analizu podataka sa mainframe servera, ukoliko se nađu na mestu krivičnog dela.

U svakom slučaju uzimanja imidža sa kompromitovanih servera od velikog značaja je obezbediti pomoć lokalnog administratora mreže, ukoliko nije sam osumnjičen, o tome

kako je sistem konfigurisan, ili za izvlačenje traženih podataka. Neki put moguće je doći do traženih podataka i bez uzimanja imidža sa poslovnih računara, a nekada forenzičar mora razmatrati pažljivo, da li obarati server poslovne organizacije, ili tražiti druge načina za sakupljanje podataka. Generalno RAID diskovi na računaru predstavljaju ozbiljan problem, jer su specifični proizvodi i forenzičar mora znati da li su konfigurisani kao fizički, ili logički diskovi u kom slučaju treba uzimati imidž svih diskova odjednom.

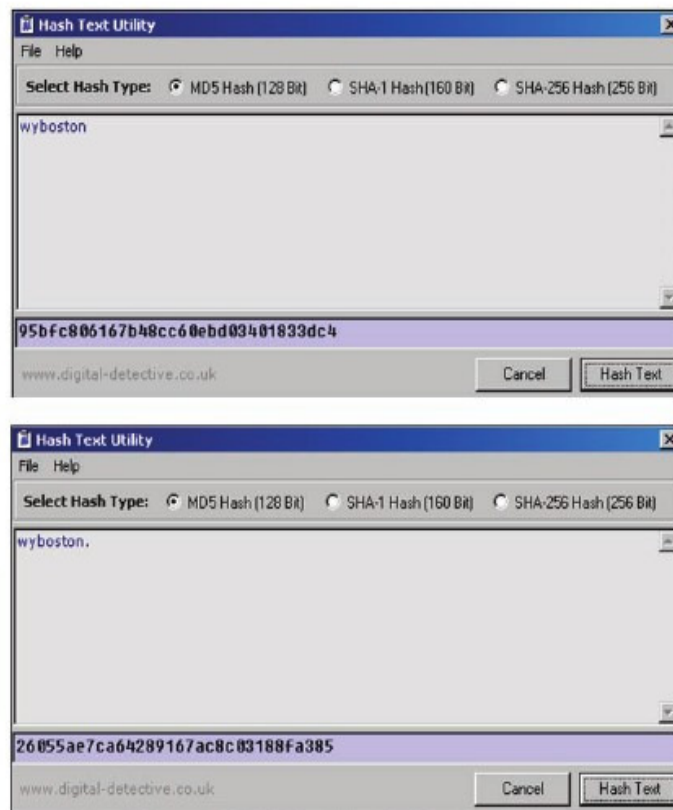
Forenzičar treba da razmatra mogućnost selektivnog uzimanja imidža sa određenih medija i delova HD, ako organ istrage raspolaže sa preciznim podacima o kakvom tipu dokaza se radi i gde se mogu nalaziti u računarskom sistemu, što najčešće nije slučaj. Uvek je za forenzičara najbolje rešenje uzeti imidž celog računara i ostalih medija, ili ih privremeno oduzeti za potrebe istrage. Postoji i alternativa uzimanju imidža diska, kao što je kloniranje diska pomoću alata tipa Image Master Solo i Logicube, posebno u slučajevima gde se pretraga vrši tajno i gde je kritična brzina akvizicije podataka.

Za svaki zadatak forenzičke analize, forenzičar treba da napravi plan analize na bazi raspoloživih informacija iz istrage i podataka i materijala dobijenih u procesu akvizicije. U PRILOGU 2 dati su ključni koraci procedure forenzičkog ispitivanja čvrstog diska i prenosnih medija.

4.2 Zaštita integriteta podataka i verifikacija

Jedan od kriterijuma za forenzičke alate za uzimanje imidža diska je da može verifikovati integritet fajla imidža diska. Za zaštitu i verifikaciju integriteta fajla imidža diska koristi se jednosmerna matematička funkcija, ili algoritam - heš (hash) informacije. Ova se funkcija lako računa u jednom, ali vrlo teško, ili nikakao u drugom smeru. Ako se izračuna heš jedno g fajla dobije se vrednost heša, koja je istovetna vrednosti dobijenoj kod verifikacije heša istim algoritmom, samo ako se fajl nije menjao. Svaka, pa i najmanja promena u sadržaju fajla, menja vrednost heša, što ukazuje da je integritet narušen.

U digitalnoj forenzičkoj akviziciji i analizi podataka, heširanje i verifikacija heša imidž fajla obavezno je da bi forenzičar mogao dokazati na sudu da originalni imidž nije menjan i da je integritet originalnih podataka sačuvan. Na taj način operacija heširanja obezbeđuje princip zaštite integriteta, akvizicijom sakupljenih digitalnih podataka sa osumnjičenog računara i postaje obavezna funkcija savremenih forenzičkih alata. Efektivno se najviše koriste dva algoritma za heširanje: MD5 i SHA1. Verovatnoća da dva fajla sa različitim sadržajem imaju isti MD5 heš je 2128, što je veoma sigurna zaštita integriteta. Promena samo jednog karaktera informacije menja heš vrednost te informacije, što je ilustrovano na sici 7.



Slika 7. Ilustracija promene heša sa promenom jednog karaktera

U tekstu na slici izmenjen je sadržaj fajla unošenjem samo jedne tačke i vrednost heša je izmenjena. Heš se skladišti zajedno sa uskladištenim fajlom, pa se u procesu verifikacije heša, vrednost heša ponovo računa sa istim algoritmom, a dobijena vrednost se upoređuje sa uskladištenom i ako su ove dve vrednosti jednake integritet uskladištenog fajla nije narušen.

5 Privremeni i drugi forenzički fajlovi

5.1 Privremeni fajlovi

U procesu forenzičke analize relevantne dokaze mogu sadržavati privremeni (Temporary) i drugi brojni fajlovi u fajl sistemu ispitivanog računara. Brojne aplikacije stvaraju privremene fajlove i ostavljaju ih u računaru kada aplikacija završi rad, ili ih brišu kada se aplikacija zatvori. Microsoft definiše privremeni fajl kao „fajl koji je kreiran da privremeno skladišti informacije da bi se oslobodila memorija za druge namene, ili da radi kao sigurnosna mreža za sprečavanje gubitka podataka kada program izvršava neke funkcije“. Windows aplikacije, uključujući sam OS, često zahtevaju da privremeno uskladište podatke na čvrstom disku. Ovo je skoro uvek tačno kada se instalira softver, ali se može dogoditi i u drugo vreme. Mnoge aplikacije kreiraju privremene fajlove da pomognu svoje operacije. Ovi fajlovi se skladište u dizajnirani 'Temp' folder. U nekim slučajevima (ne uvek) ovi fajlovi će imati. TMP ekstenziju, koja pretpostavlja da će ih Windows ili aplikacija koja ih je kreirala i izbrisati kada im više ne trebaju, što se međutim uvek ne događa. Microsoft Office kreira najviše privremenih fajlova. Aplikacija određuje automatski gde i kada treba da kreira privremeni fajl. Taj fajl treba da postoji samo dok traje sesija MS Office aplikacije. U procesu normalnog isključivanja (shutdown) privremeni fajl se prvo poveže sa otvorenim radnim fajlom, koji se zatim zatvara i memoriše, kada privremeni fajl treba da bude izbrisan. Međutim, nepropisno isključivanje aplikacije ne briše privremeni fajl i ostavlja ga za potencijalno forenzičko ispitivanje. Word koristi privremene fajlove u normalnom radu na dva načina:

1. da oslobodi memoriju za drugi rad dok se aplikacija koristi, pomeranjem dela dokumenta na kome se ne radi u privremeni fajl na disku i omogućavajući najbolje korišćenje memorije za druge akcije na dokumentu – manipulaciju i uređivanje teksta itd.
2. da obezbedi neku vrstu zaštite integriteta podataka od grešaka u memorisanju fajlov, ili od pada napajanja dok je fajl otvoren.

MS Office tipično kreira sledeće privremene fajlove:

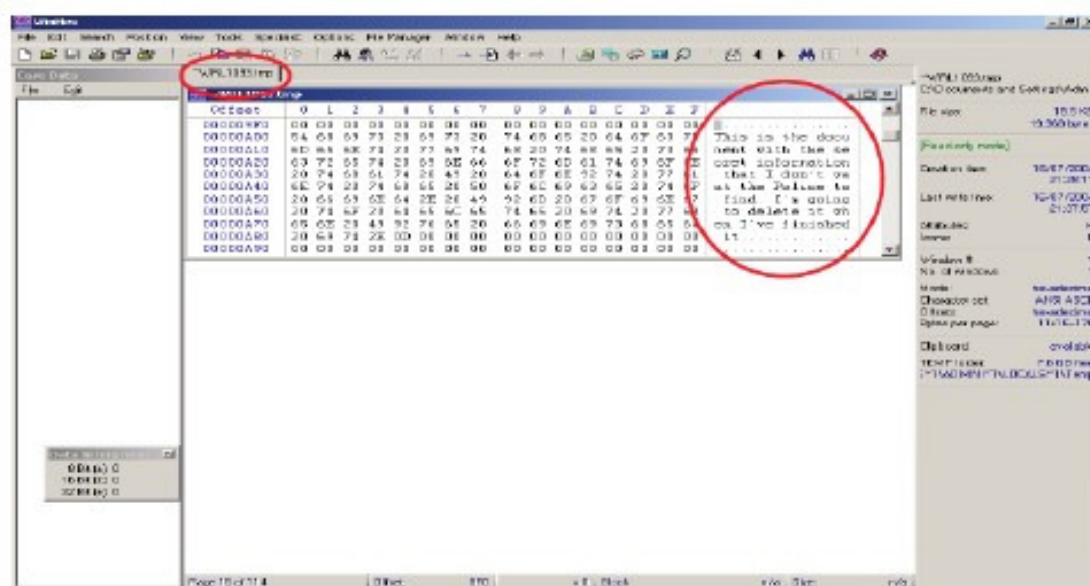
1. Word : ~wrf0000.tmp (podrazumevano)
 2. Word : ~mfxxxxx.tmp (podrazumevano)
 3. Word : ~dftxxxx.tmp (podrazumevano)
 4. Word : wrf0001.tmp (podrazumevano)
 5. Kopiranje drugog dokumenta: ~wrcxxxx.tmp
 6. Word dokument: ~wrxxxx.tmp,
 7. Fajl privremenog dokumenta: ~wrfxxxx.tmp,
 8. Rečnik: ~wrixxxx.tmp,
 9. Clipboard: ~wrlxxxx.tmp,
 10. Makroi: ~wrmxxxx.tmp,
 11. Word OLE dokument: ~wroxxxx.tmp,
 12. Scratch fajl: ~wrsxxxx.tmp,
 13. Konvertovani [foreign] dokument: ~wrvxxxx.tmp.
 14. PowerPoint: pptxxxx.tmp,
 15. Excel: ~dfxxxx.tmp.
- gde xxxx predstavlja broj sekvence.

Postoje velike šanse da forenzičar ispita ove fajlove i oporavi vitalne dokazujuće podatke. Ovi fajlovi mogu biti uskladišteni u brojnim i različitim lokacijama, u zavisnosti koja akcija fajla se dogodila. Dva najčešća mesta za inicijalnu pretragu privremenih fajlova su:

C:\Documents and Settings\\Local Settings\Temp

C:\Documents and Settings\\Application Data\Microsoft\Word

Pretraživanjem sa „search“ funkcijom, koristeći .TMP ekstenziju kao ključnu reč, treba da se otkriju i druge lokacije. Na slici 8 je dat primer privremenih clipboard fajlova ~wrlxxxx.tmp posmatran u forenzičkom alatu. Kako se može videti, zista sadrži potencijalne dokazujuće podatke.

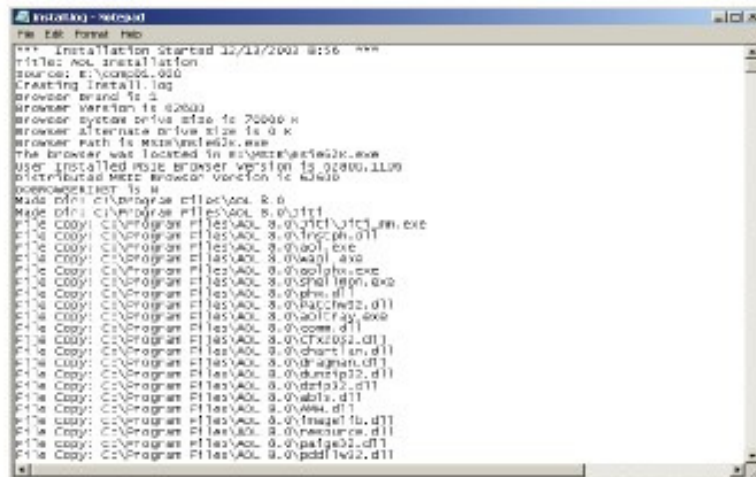


Slika 8. Interpretacija privremenih fajlova ~wrlxxxx.tmp u forenzičkom alatu

Za pretraživanje privremenih fajlova drugih aplikacija, potencijalno uskladištenih na različitim lokacijama i bogatim dokazujućim podacima, često je najbolje pogledati u folderpodataka aplikacije u Documents and Settings, ili u folderu aplikacija u C:\Programs.

5.2 Log fajlovi

Log fajlovi mogu biti koristan izvor podataka o događajima na računaru. Brojne aplikacije kreiraju svoje log fajlove, bilo kao deo procesa instalacije, ili pri prvom aktiviranju. Windows XP pri instalaciji kreira negde oko 135 log fajlova, ili osnovnih tekst fajlova koji rade kao log fajlovi. Log fajlovi mogu sadržavati vrlo relevantne podatke, kao što su kada je aplikacija prvi put instalirana, kada je poslednji put pokrenuta, kako je podešena i koju je akciju imala u toku poslednjeg aktiviranja. Sami log fajlovi imaju svoj vremenski pečat, kao svaki drugi fajl kojeg OS procesira.



Slika 9. Instalacioni log fajl AOL klijenta

Na slici 9. prikazan je instalacioni log fajl za nekog AOL (America on Line) klijenta. Kako se vidi fajl sadrži mnogo potencijalno korisnih informacija. Međutim, nije uvek jasno na koje se aplikacije, ili procese ovi log fajlovi odnose. Ponekad je potrebno da forenzičar pretražuje ceo logički disk, koristeći *.log izraz za pronalaženje svih relevantnih tipova fajlova, a zatim manuelno pretražuje svaki od njih, da odredi njegovu relevantnost. Lokacije svih log fajlova biće takođe registrovane u Registru i nekada treba razmotriti opciju pretraživanje celog Registra. Treba imati na umu da korisnik može promeniti lokaciju log datoteka izvan podrazumevane lokacije.

5.3 Print Spooler fajlovi

Primarna komponenta u Windows okruženju za printovanje (štampanje) je print spooler (Simultaneous Peripheral Operations On-Line), koji u privremenom fajlu čuva stranicu koju je neka aplikacija poslala na štampač za štampanje. Aplikacija i printer simultano mogu upisivati/čitati fajlove u print spooler-u, što ubrzava proces štampanja, omogućava formiranje redosleda za štampanje i povratak kontrole aplikacije pre završetka štampanja. Print spooler je u stvari jedan izvršni fajl koji upravlja celim procesom štampanja. Print spooler se podiže u toku podizanja (start-up) sistema i ostaje aktivan dok sesistem ne isključi. U Windows NT i XP print spooler kreira .SPL fajlove kada operacija štampanja počinje. U Windows 9x .SPL fajl daje ime kreiranom privremenom fajlu, gde se sadrži EMF (Enhanced Metafile). Podaci koji se odnose na štampanje sadržani su u .SPL fajlu. Generalno u Windows okruženju, tip podataka u formatu EMF,

iako su drugi tipovi zapisa podržani uključujući ASCII i sirove podatke, predstavlja kompaktan ulaz podataka koji skladišti izlazni tekst, grafičke podatke i komande za štampanje i ne zavisi od uređaja, ili aplikacija. To znači da može biti kopirana, ili eksportovana i otvorena sa specijalnim softverom, ili funkcijama za štampanje drugih aplikacija. Takođe, dopušta ekstrakciju i gledanje drugih podataka, teksta ili slika. Većina forenzičkih alata može gledati .SHD fajlove i EMF podatke sadržane u njima. Zajedno sa .SPL fajlom nalazi se kreiran .SHD fajl u „senci“, koji sadrži sve informacije, koje spooler treba za uspostavljanje štampanja u slučaju da se računar restartuje pre završetka operacije štampanja.

5.4 Fajlovi linkova

Fajlovi linkova ili prečica (shortcuts) mogu obezbediti takođe korisne informacije za forenzičko ispitivanje. Ovi fajlovi su jednostavno usmerivači, ili poštanski signali do ciljnih fajlova, aplikacija, direktorijuma i sistemskih objekata izvan fajl sistema, kao što su printeri i spoljni diskovi. Obezbeđuju korisnicima brzi pristup uobičajeno orišćenjim fajlovima i aplikacijama itd. Uobičajena lokacija fajlova za linkovanje su Windows Desktop, Windows Recent, Windows Start Menu, Windows Sent to i Internet Explorer Favorites folderi. Ekstenzija za ove fajlove je .LNK.

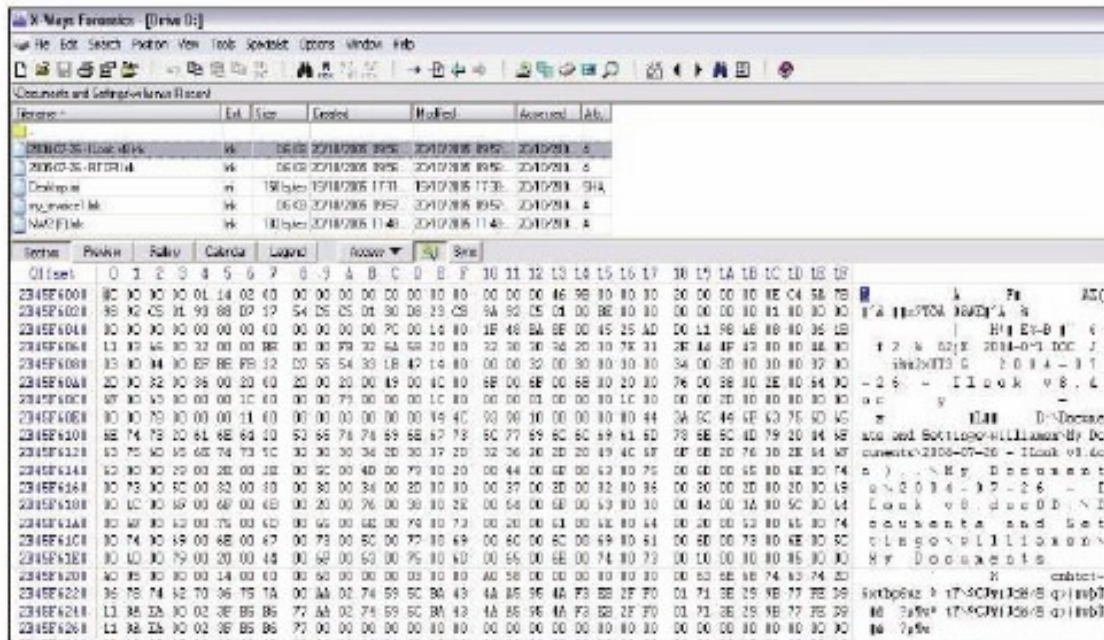
Detlnije ispitivanje ovih prečica može obezbediti dobar uvid u to kako je korisnik personalizovao svoj računar i pristupe aplikacijama i fajlovima. Ovi fajlovi se mogu kreirati na brojne načine:

- u toku instalacije operativnog sistema,
- u toku instalacije aplikacija,
- kreiranjem od strane korisnika.

U Windows 2000 i XP sistemima lokacija ovih fajlova je podrazumevana i nalazi se u C:\Documents and Settings\<username> i u nekom od sledećih sub-foldera:

\desktop, \Favourites, \My Recent Documents, \SendTo, \Start Menu.

Svaki od ovih foldera ima kreiran svoj vremenski pečat, a svaki fajl u njemu svoj puni vreme&datum pečat i punu putanju fajla na koga se link odnosi. Međutim, ovo nije toliko očigledno i zahteva dekodiranje, kada se identifikuje relevantan ofset bajta. Na slici 10. je prikazn primer .LNK fajla, a relevantni ulazi podataka su naglašeni.



Slika 10. Primer .LNK fajla u forenzičkom alatu

Na slici se može videti ime link fajla naglašen sivom bojom pri vrhu, a u donjem delu desno je datum izvršavanja link funkcije – lokacija fajla sa imenom diska i direktorijuma – u ASCII i Unicode zapisu. Bliže ispitivanje link fajla takođe obezbeđuje povezivanje fajla sa logičkim diskom na kojem je fajl smešten, a zatim na logički disk gde je smešten OS. Ovo potencijalno može indicirati da je korišćen prenosni (removable) disk. U toku forenzičkog ispitivanja uvek je korisno pretražiti ove fajlove i to u alociranim, nealociranim prostorima diska i swap fajlovima. Izbrisana prečica treba još uvek da ima ulaz u MTF. Klasteri u nealociranim oblastima mogu sadržavati fajlove prečica, mada ne mora biti ulaza da identifikuje u kojim klasterima. Pretraživanje sa linkom fajla treba da otkrije fajl i njegov sadržaj za ispitivanje.

5.5 Tipovi i potpisi fajlova

Posotji više tipova fajlova u opticaju, a generalno se mogu indentifikovati sa ekstenzijom. Tipično se ekstenzija izražava sa tačkom koju slede 2 - 4 karaktera. Uzmimo za primer 3 sledeća imena fajla:

1. proces
2. proces.doc
3. proces.jpg
4. proces.html

Za prvi fajl možemo reći da može biti bilo šta, dok je drugi word dokument o nekom procesu, treći je slika modela nekog procesa, a četvrti je *html* dokument za gledanje sa nekim *web* pretraživačem. Ekstenziju korisnici prepoznaju i pridružuju je određenoj aplikaciji. Upravo to čini i OS sa imenom fajla. Međutim, to uvek nije onako kako se vidi. Zašto je potrebna identifikacija tipa fajla? Forenzičar treba da zna da li će određeni tip fajla računari i OS kojeg koristi otvoriti i da li je potreban određeni softver za otvaranje i ispitivanje fajla. Većina fajlova koje forenzičari susreću u radu odnosi se na tekst, grafičke, audio, ili video fajlove. Takođe su česti komprimovani fajlovi – jednog, ili grupe fajlova povezanih u jedan 'arhivski' fajl. Kod komprimovanih fajlova može se dogoditi da postoji više različitih fajl ekstenzija u 'arhivu', što znači da je više od jedne aplikacije korišćeno za kompajliranje arhiva.

Uobičajeni tipovi fajlova i ekstenzija u *Microsoft* fajl sistemima i drugim platformama prikazni su u tabeli 1.a. *Microsoft Office* set programa je verovatno najčešće upotrebljavan na ispitivanim računarima. Zbog toga forenzičari moraju poznavati dobro ove tipove dokumenata. U tabeli 1.b. prikazani su neki drugi uobičajeni tipovi fajlova i ekstenzija, uključujući komprimovane fajlove, izvršne fajlove, sistemske i log fajlove i neke druge koji često mogu obezbediti dokazujuće podatke.

Tabela 1 Uobičajeni tipovi fajlova i ekstenzija

Common Microsoft Files		Other Common File Types & Extensions	
File	File extension	File	File Extension
MS Office Word	.doc .dot	Compressed Files	.zip, .rar .7z, .gz
MS Office Excel	.xls .xlb	DOS executables	.com, .bat .exe
MS Office PowerPoint	.ppt, .pps .pot	Initialisation files	.ini
MS Office Access	.mdb, .adp, .mda .ade	System files	.sys
MS Office Outlook	.pst .ost	Log files	.log
MS Outlook Express	.dbx .wab	Help files	.hlp
MS Internet Explorer	.htm .html	Text files	.txt, .web .rtf
		Adobe files	.pdf, .psd

a.

b.

Većinu ovih fajlova kreira sistem, ali su mnogi deo softverskih paketa, a mogu ih kreirati i korisnici. Kako raste iskustvo u radu sa računarom, sve se bolje prepoznaju značenja ekstenzija fajlova i šta one govore o određenom fajlu.

Dobar deo rada forenzičara digitalnih podataka odnosi se na grafičke i druge multimedijalne fajlove, kao što su audio i video fajlovi koji se uobičajeno koriste u razmeni i posedovanju slika dečije pornografije. Ovi formati fajlova i ekstenzija prikazani su u tabeli 2.a i b.

Tabela 2. Uobičajeni tipovi grafičkih (a) i video (b) fajlova

Common Graphics File Types		Common Video & Audio File Types	
File	File Extension	File	File Extension
Joint photographic Experts Group	.jpg, .jfi .jpeg	Audio Video Interleaved	.avi
Graphics Interchange Format	.gif, .giff	Apple QuickTime	.mov
Windows Bitmap	.bmp	Visual Image Directory	.vid
Portable Network Graphics	.png	Moving picture Experts Group	.mpg .mpeg
Tagged Image File Format	.tif, .tiff		

a.

b.

Forenzičar mora imati alate za otvaranje i čitanje ovih fajlova, ili izvlačenje dokazujućih podataka.

Poslednja grupa fajlova je ona gde se koristi šifrovanje za skrivanje podataka od onih koji ne treba da ih vide, a među njima su najčešće upravo forenzički digitalni dokazi. Uobičajeni šifrovani fajlovi su prikazani u tabeli 3.

Tabela 3. Ekstenzije uobičajenih šifrovanih fajlova

Common Encryption File Types	
File	File Extension
Pretty Good Privacy	.pgd .pgp
BestCrypt	.jbc

Ovim lista šifrovanih fajlova nije iscrpljena, a ekstenzije fajlova forenzičar mora verifikovati tokom analize.

Forenzičar, dalje mora razumeti kako *Windows* koristi ove ekstenzije fajlova. U *Windows* OS ekstenzije fajlova su sadržane u jednom od glavnih ključeva **Registra** - **HKEY_CLASSES_ROOT**, koji ima dva važna zadatka:

- da čuva tragove ekstenzija fajlova i njihovih asocijacija,
- čuva tragove programa pridruženih tipovima fajlova koji su registrovani u sistemu.

Striktno govoreći ovaj ključ registra je suvišan, jer je direktna kopija podataka koji su sadržani u ključu **HKEY_LOCAL_MACHINE\Software\Classes**. U stvari ova dva ključa su direktno povezana i sinhronizovana tako da se svaka promena u jednom, registruje u drugom ključu. Ovi ključevi se pune na dva glavna načina. Prvo kada se OS podiže, podrazumevano se podiže sveobuhvatna lista ekstenzija fajlova. Drugi način je kada se nova aplikacija, ili fajl podiže, relevantni tip podataka fajla popuniće ključeve. Kada korisnik otvori fajl, informacije u ovom ključu registra:

- identifikuju tip fajla,
- identifikuju putanju do pridružene asocijacije, vide ako postoji specijalne komande koje moraju biti prisutne da bi se fajl otvorio,
- traže informacije o rukovanju sa ugrađenim objektima,
- ispituju fajl za informaciju o ikoni i
- proveravaju da li se, ili ne može koristiti 'BrziPregled'.

Sadržaji ovog registra su dinamički i menjaju se zavisno od broja instaliranih aplikacija. Neki fajlovi nisu podrazumevano pridruženi određenim aplikacijama i mogu se otvoriti sa nekoliko različitih aplikacija. Ako *Windows* ne pridruži neki poseban fajl sa nekom aplikacijom, prikazaće dijalog boks s listom opcija aplikacija sa kojim bi se fajl trebao otvoriti. Postoji opcija za otvaranje svih fajlova sa izabranom aplikacijom.

5.6 Potpisi fajlova

U procesu ispitivanja fajl sistema forenzičar treba da razmatra i potpise fajlova. Pri tome ne treba mešati ekstenzije i potpise fajlova. U slučaju nekog tipa fajlova, svi fajlovi imaju jedan poznat i prepoznatljiv *heder*, koji nije vidljiv u normalnom režimu rada i generalno za gledanje fajlova treba koristiti *hex* editor. Ovaj potpis fajlova je definitivni indikator tipa i

sadržaja fajla. U slici 11 prikazan je uobičajen potpis fajlova za sve MS Office fajlove: **D0 CF 11 E0 A1 B1 1A E1**.

The screenshot shows a Windows Explorer window with a list of files in 'Documents and Settings\williamsn\My Documents'. Below the file list, the 'Preview' tab is active, displaying a hex dump of a file's signature. The hex dump shows the following sequence of bytes: D0 CF 11 E0 A1 B1 1A E1, which is the standard Microsoft Office file signature.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
018EE5000	D0	CF	11	E0	A1	B1	1A	E1	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
018EE5020	06	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
018EE5040	01	00	00	00	FE	FF	FF	FF	00	00	00	00	59	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
018EE5060	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
018EE5080	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
018EE50A0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
018EE50C0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF

Slika 11. Uobičajen potpis MS Office fajlova

Potpis fajla pojavljuje se na samom početku fajla, ali se ne vidi kod normalnog otvaranja *word* dokumenta. Poznavanje potpisa fajla je važno za forenzičara, jer maliciozni korisnik može izmenom ekstenzije fajla isti sakriti, a forenzičar preko potpisa fajla može otkriti pravi tip i sadržaj fajla. Tako u pred-ispitivanju forenzičar može otkriti samo **.doc** fajlove, među kojima se, međutim, mogu kriti brojni **.jpeg** fajlovi kompromitujućih slika. *Windows* kategorizuje fajlove prema njihovim ekstenzijama, pretpostavlja da su sve *word* dokumenti, daje im korektnu ikonu i pokušava otvoriti sa MS Word-om. U ovom slučaju svi **.jpeg** fajlovi neće se moći otvoriti. Takođe, ako se pretražuju fajlovi u potrazi za **.jpeg**, rezultat će biti negativan. Sledeća ilustracija u slici 12 pokazuje kako *Windows* radi u ovakvim situacijama i kako prikazuje rezultate takvih akcija. Prikazana su četiri uobičajena tipa fajlova koji se mogu naći na računaru. *Windows* je pripisao korektne ikone svakom tipu fajla i koristi korektne aplikacije da ih otvori. Otvaranje će biti uspešno jer su ekstenzije tačne.

The screenshot shows a Windows Explorer window with a list of four files. Each file has a correct icon and a correct application assigned to it. The files are: 'This is a JPG created in PAINT.jpg' (9 KB, JPEG Image, 1/19/2005 11:50), 'This is a notepad TEXT document.txt' (1 KB, Text Document, 1/19/2005 11:49), 'This is definitely a word document.doc' (20 KB, Microsoft Word Document, 1/19/2005 11:48), and 'This is a GIF from the Internet.gif' (11 KB, GIF Image, 7/24/2004 17:56).

This is a JPG created in PAINT.jpg	9 KB	JPEG Image	1/19/2005 11:50
This is a notepad TEXT document.txt	1 KB	Text Document	1/19/2005 11:49
This is definitely a word document.doc	20 KB	Microsoft Word Document	1/19/2005 11:48
This is a GIF from the Internet.gif	11 KB	GIF Image	7/24/2004 17:56

Slika 12 Tačan Windows prikaz potpisa fajlova

U sledećoj ilustraciji (slika 13) svi fajlovi su promenili ekstenzije u **.doc**. Ime, veličina i sadržaj fajla ostaju isti, a *Windows* pogrešno interpretira fajlove i pripisuje svakom ikonu word dokumenta i menja detalje tipa fajla, pošto ih tako vidi i pokušava ih otvarati sa *Word*-om.

The screenshot shows a Windows Explorer window with a list of four files, all with **.doc** extensions. Each file has a Microsoft Word Document icon and a Microsoft Word Document application assigned to it. The files are: 'This is a JPG created in PAINT.doc' (9 KB, Microsoft Word Document, 1/19/2005 11:50), 'This is a notepad TEXT document.doc' (1 KB, Microsoft Word Document, 1/19/2005 11:49), 'This is definitely a word document.doc' (20 KB, Microsoft Word Document, 1/19/2005 11:48), and 'This is a GIF from the Internet.doc' (11 KB, Microsoft Word Document, 7/24/2004 17:56).

This is a JPG created in PAINT.doc	9 KB	Microsoft Word Document	1/19/2005 11:50
This is a notepad TEXT document.doc	1 KB	Microsoft Word Document	1/19/2005 11:49
This is definitely a word document.doc	20 KB	Microsoft Word Document	1/19/2005 11:48
This is a GIF from the Internet.doc	11 KB	Microsoft Word Document	7/24/2004 17:56

Slika 13 Pogrešan Windows prikaz potpisa fajlova

Zadatak forenzičara je da razreši ovakav slučaj. U prvom redu može se svaki fajl eksportovati i gledati u **hex** editoru i manuelno ispitati sve potpise fajlova koje pronađemo prema njihovim ekstenzijama. To je svakako vrlo ekstenzivan posao. Na sreću, većina forenzičkih softverskih alata imaju aplikaciju koja vrši '*analizu potpisa fajlova*'. Ove aplikacije ispituju potpis svakog fajla i klasifikuju sadržaje fajlova, a zatim identifikuju sve nekonzistentnosti, koje forenzičar detaljnije ispituje da bi odlučio koji je stvarni tip i sadržaj svakog fajla.

U sledećoj ilustraciji na slici 14 prikazana je **.jpeg** slika sa **.doc** ekstenzijom. Međutim, potpis fajla govori nešto drugo: **FF D8 FF E0 xx xx 4A 46 49 46 00** je jedinstven potpis za sve **.jpeg** fajlove.

This is a JPG created in PAINT.doc																	doc		8.3 KB		1/19/2005 11:50:27		1/19/2005 11:50:30		1/19/2005		A	
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Access	☒										
000278528	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	60	ÿØÿà..JFIF.....											
000278544	00	60	00	00	FF	DB	00	43	00	08	06	06	07	06	05	08	...ÿÛ.C.....											
000278560	07	07	07	09	09	08	0A	0C	14	0D	0C	0B	0B	0C	19	12	\$.'											
000278576	13	0F	14	1D	1A	1F	1E	1D	1A	1C	1C	20	24	2E	27	20	(7).01444.'											
000278592	22	2C	23	1C	1C	28	37	29	2C	30	31	34	34	34	1F	27	9=82<.342ÿÛ.C...											
000278608	39	3D	38	32	3C	2E	33	34	32	FF	DB	00	43	01	09	09	21.12222											
000278624	09	0C	0B	0C	18	0D	0D	18	32	21	1C	21	32	32	32	32	2222222222222222											
000278640	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	2222222222222222											
000278656	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	2222222222222222											
000278672	32	32	32	32	32	32	32	32	32	32	32	32	32	32	FF	C0	22222222222222ÿÀ											

Slika 15. Prikaz **.jpeg** slika sa **.doc** ekstenzijom u hex editoru

Ako se otkriju ovakve nekonzistentnosti, to mora biti sumnjivo i forenžar treba da utvrdi zašto je to korisnik uradio.

Uobičajeni potpisi fajlova dati su u tabeli 4, gde je prikazan jedan ekstrakt iz web resursa informacija hedera sadržanih u fajlovima.

Tabela 4 Uobičajeni potpisi fajlova

Hex Signature	Ext	ASCII Translation	Description
47 49 46 38 37 61 47 49 46 38 39 61	GIF	GIF87a GIF89a	Graphics Interchange Format file Trailer: 00 3B (.)
D0 CF 11 E0 A1 B1 1A E1	DOC, DOT PPS, PPT XLA, XLS WIZ MSC MSI VSD DB	ÐÏ àj± á	Word Powerpoint Excel Wizard Microsoft Common Console Document Microsoft Installer package Visio file MSWorks database file
FF D8 FF E0 xx xx 4A 46 49 46 00	JFIF JPE JPEG JPG	ÿØÿà..JFIF.	JPEG/JFIF graphics file Trailer: FF D9 (.)

Postoje brojni izvori koji se mogu koristiti za istraživanje cele oblasti tipova, ekstenzija i potpisa fajlova.

5.7 Forenzička analiza tragova korišćenja interneta

Istraživanje tragova pristupa Internetu na osumnjičenom računaru, samo je uvod u kompleksnu forenzičku analizu napada sa Inteneta. Konekcije računara i računarskih mreža na Internet stalno se usavršavaju, ali su u upotrebi i obični modemi preko telefonske linije, zatim ADSL i širokopojasni pristupi Internetu. Uređaji koji povezuju sisteme na Internet dramatično se menjaju – pored računara, to mogu biti i mobilni telefoni, televizori i brojni kućni aparati. Savremeni Internet u delovima sekunde može povezati digitalni svet preko

brojnih i različitih medija kao što su servisi: (**World Wide Web**) web pretraživači, čet, *peer-to-peer* i novinske grupe. Praksa je pokazala da u većini slučajeva kompjuterskog kriminala učestvuje u nekom obliku neki aspekt Interneta. Zato forenzičar mora razumeti kako radi Internet i kakve tragove ostavlja u računar rad na Internetu.

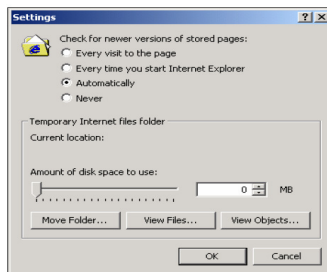
5.7.1 Privremeni internet fajlovi

Privremeni Internet fajlovi, ili tzv. **Internet Cache** (Internet keš) su fajlovi koji ostaju na računar posle aktivnosti na nekoj web lokaciji. U toku pretraživanja Interneta korisnik poseti milione web lokacija koje su smeštene na računarima širom sveta. Pre prikazivanja onog što želimo na ekranu, računar lokalno sakuplja informacije, odnosno preuzima (*downloads*) fajlove koji čine web stranicu sa izvornog računara i čuva ih u Internet kešu, a zatim ih prikazuje na ekranu monitora računara. Internet keš je samo neka oblast na čvrstom disku, pa kako se informacije upisuju na disk, sistem sve to registruje. HTML stranice sastoje se od teksta, grafičkih dokumenata, slika ili banera. Web stranica može biti jedan fajl, ili može sadržavati 10-20 ili više fajlova, što zavisi od dizajna web stranice.

Stavljanje informacija sa Interneta u Internet keš, pre prikazivanja na ekranu, osim što odražava posmatračke navike korisnika, posebno je važno i u slučaju spore Internet veze. Kada se stranica jednom prikaže na ekranu, korisnik se može premestiti na drugu stranicu na istoj, ili sasvim drugoj lokaciji. Na svakom pretraživaču postoji opcija **Back** za povratak na prethodnu stranicu. Ako se korisnik vrati na prethodnu stranicu pre nego što su preuzeti svi fajlovi sa lokacije, morao bi ponoviti preuzimanje web stranice sa te lokacije, da ne postoji Internet keš koji je već lokalno snimio celu *html* stranicu. Tako korisnik može mnogo brže sa lokalnog čvrstog diska prikazati preuzete *html* fajlove. Dakle Internet keš štedi vreme korisniku, a forenzičaru obezbeđuje odličan izvor informacija, obaveštenja i dokaza. Pošto su podaci sa nečije web stranice uskladišteni na disku, ako forenzičar poseduje disk može znati gde je korisnik bio na Internetu, šta je gledao i šta je uradio.

Korisnik može podesiti na minimum veličinu Internet keša na disku – **0MB**, što efektivno znači kao da keša nema. Međutim, *Microsoft* dokumentacija sugerise da neki Internet keš uvek mora da postoji u računar, pa makar da piše da je 0%, uvek je neki prostor alocirao za keš. Podrazumevana veličina keša kod novih mašina je 3% slobodnog prostora diska, što ukazuje koliko korisnih informacija ovde može biti uskladišteno.

Ako forenzičar otkrije da je keš vrednost podešena na 0%, treba postaviti pitanje zašto je to tako (slika 15). Prvi rezon je da korisnik želi da računar ništa ne skladišti u keš prostor i da nešto želi sakriti. Promena vrednosti keša je jednostavna i direktna operacija.

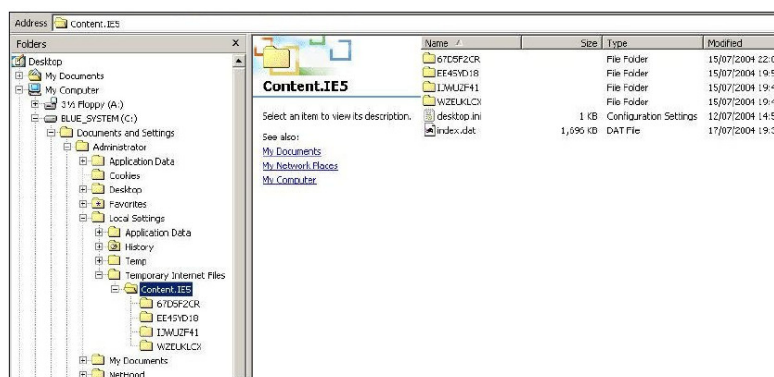


Slika 15. Korisničko podešavanje Internet keša na 0MB

U web pretraživaču treba otvoriti **Tools**, zatim **Internet Options** kao na gornjoj slici. Korisnik može ne samo izmeniti veličinu keša, nego i izbrisati fajlove koji formiraju deo keša. Ova vrednost se čuva kao ulaz u **Registru**.

Internet keš je serija foldera na čvrstom disku. U starijim Win 9x sistemima može se naći u **C:\Windows** folderu na mašini bez profila korisnika i u **C:\Windows\Profiles\ {Profile Name}** folderu na sistemu sa profilima korisnika. U Windows 2000 i XP sistemima, keš fajlovi se nalaze u **C:\Documents and Settings\{User Name}**. Treba znati da su ovo podrazumevane lokacije i da ih korisnik može smestiti bilo gde sa prepošavanjem.

Struktura ovih fajlova prikazana je u sledećem prozoru (slika 16). U folderu **Content.IE5** nalazi se neki broj slučajno imenovanih pod-foldera sa imenima dužine 8 karaktera koje je sistem alocirao. Unutar ovog foldera je i fajl **INDEX.DAT**, koji kontroliše Internet keš i od vitalnog je značaja za forenzičare u istrazi aktivnosti korisnika na Internetu. Treba da imaju najmanje 4 ovakva foldera.



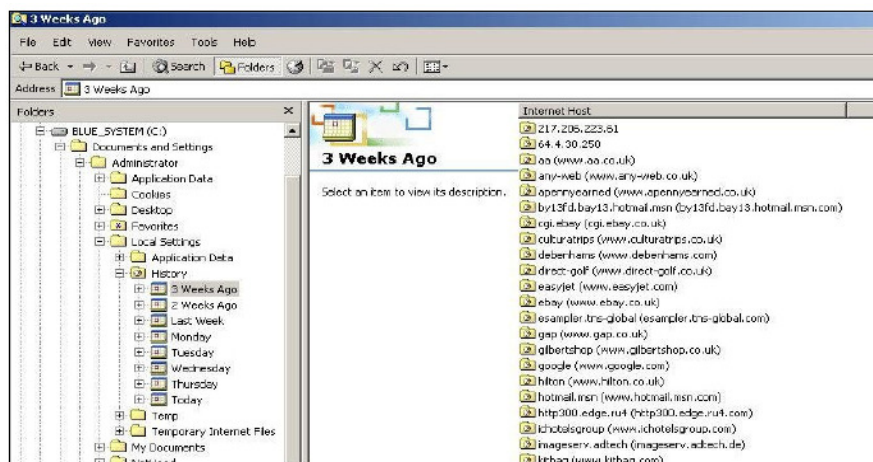
Slika 16 Struktura Internet keš fajlova u Content.IE5 folderu

Unutar svakog foldera su stvarni fajlovi preuzeti sa Interneta pre nego što su prikazani na ekranu računara korisnika. Njihovo alokiranje izvršio je sistem, a **INDEX.DAT** fajl registruje gde su oni i kako su zajedno uskladišteni. Fajlovi mogu biti **html** tipa, grafički, ili bilo šta, što je potrebno za propisno prikazivanje web stranice.

5.7.2 Istorija aktivnosti na internetu

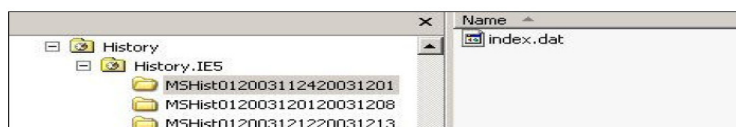
Istorija aktivnosti na Internetu (*Internet History*) obezbeđuje evidenciju lokacija koje je korisnik posetio sa svog računara u toku pretraživanja Interneta. Ova evidencija uključuje imena posećenih web lokacija, detalje o izvornim serverima, FTP sajtove, e-mail baziran na web-u i posećene novinske grupe, takođe bazirane na web-u. Istorija aktivnosti na Internetu i Internet keš, daju forenzičaru dobru sliku o tome kako je računar korišćen u toku pretraživanja Interneta.

Istorija Interneta postoji da omogući korisniku da ide na prethodno posećene web lokacije sa liste koja se pojavljuje u pretraživaču. Kao kod privremenih Internet fajlova, postoji struktura foldera da čuva ove informacije. Ove lokacije podrazumevano su tačno na istom mestu kao za keš fajlove, ali ih korisnik može pomeriti. U sledećem primeru prikazana je struktura foldera Internet History u Windows XP mašini, (slika 17).



Slika 17 Struktura foldera Internet History u Windows XP mašini

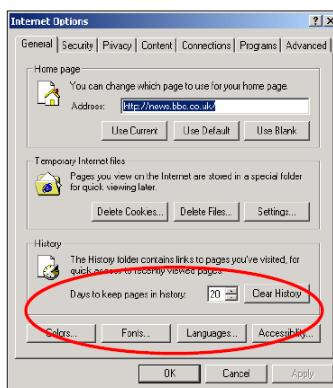
Vidi se da sistem deli foldere na dnevne i nedeljne istorije. Međutim, format ovih foldera kontroliše se sa **DESKTOP.INI** fajlom koji se nalazi u folderu. U stvari, forenzički alat vidi nešto drugačije ovu strukturu, (slika 18).



Slika 18. Struktura foldera Internet History u forenzičkom alatu

Forenzičar može otkriti tip foldera iz konvencije imenovanja koja se koristi u imenu foldera. Postoje tri tipa istorijskih fajlova: *master*, *nedeljni* i *dnevni*. Svim ovim fajlovima upravljaju **INDEX.DAT** fajlovi.

Internet History takođe ima opciju za korisničko podešavanje. Na sledećem panelu korisnik može lako promeniti broj dana koj istorija treba da čuva, (slika 19.).

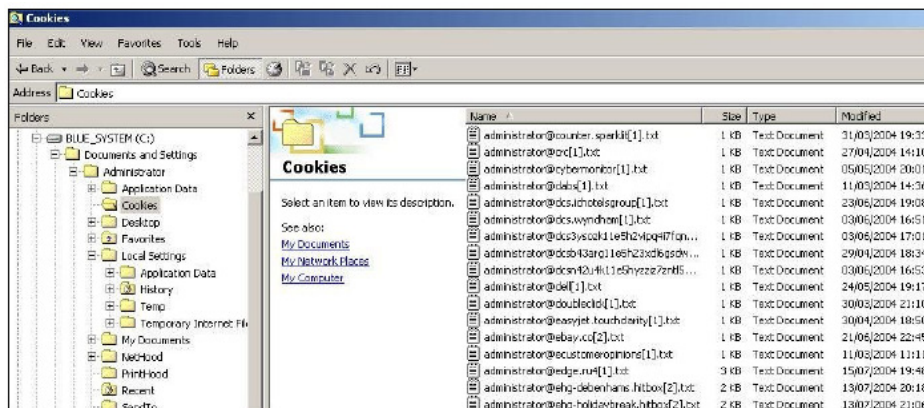


Slika 19. Opciju za korisničko podešavanje Internet History

Podrazumevano je podešeno 20 dana, pa ako forenzičar pronade znatno manje vreme, a **minimum je 0 dana, treba se pitati zašto je korisnik to promenio. Vrednost koja je pridružena ovom podešavanju nalazi se u Registru.**

5.8 Kolačići (Cookies)

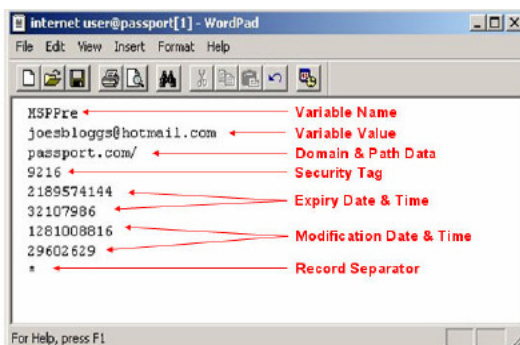
Kolačići su još jedan artefakt Internet aktivnosti koje korisnik malo, ili nikako kontroliše. Ovo su mali tekst fajlovi deponovani na čvrstom disku kao rezultat Internet aktivnosti i poseta web lokacijama. Kolačići se kreiraju kada pretraživač kontaktira web stranicu koja podržava funkcije kolačića, (slika 20).



Slika 20. Kolačići kao forenzički indikator Internet aktivnosti

Kolačići se podrazumevano skladište na istu lokaciju kao i prethodna dva Internet arhiva, ali korisnik može promeniti ovu lokaciju. U sledećem primeru, vide se URL koji su posećeni i koji su ostavili kolačiće na mašini. Kolačići sadrže znatne informacije o lokaciji i dalje informacije koje lokacija može koristiti za povratak posetioca na tu lokaciju. Svaki fajl kolačića ima vreme i datum registrovane na računaru, pa forenzičar može identifikovati neke detalje o tome kada se poseta dogodila.

Kolačići se mogu lako koristiti za čuvanje detalja o posećenoj lokaciji – imena, adresa i čak detalja o kreditnim karticama, za novu posetu toj lokaciji, (slika 20.1). Generalno, kolačići se koriste za identifikovanje korisnika koji je ranije posetio određenu lokaciju i može se koristiti za prikupljanje podataka o frekvenciji poseta, posmatranim informacijama i obezbeđenim materijalima. Sadržaj kolačića pojavljuje se na levoj strani prozora, a različiti delovi su dalje rasčlanjeni.



Slika 20.1. Primer podataka koji se mogu nalaziti u kolačićima

Ova oblast Internet artefakta uključuje vreme i datum koji se mogu videti forenzičkim alatima. Kolačići se generalno skladište na računaru bez znanja korisnika i od velike su dokazujuće vrednosti za forenzičara. Treba znati da neki kolačići mogu namerno biti postavljeni na mašinu da zavedu analitičara kao da je korisnik posetio tu lokaciju. U svakom slučaju, ako kolačići počinju sa imenima tipa *Lolita* i sl., treba računati da je korisnik posetio pornografske lokacije na Internetu.

Osnovni forenzički alati mogu čitati sva tri tipa Internet fajlova na računaru, ali je najbolji poznati alat za analizu Internet istorije zove se *NetAnalysis* (Crag Wilson, www.digital-detective.co.uk). Ovaj alat sve tri oblasti prikazuje zajedno u tabelarnoj formi, omogućavajući analizu vremenske linije aktivnosti na Internetu i ima funkcije filtriranja i izveštavanja rezultata.

5.9 Favorizovane lokacije

Funkcija favorizovanih lokacija omogućava upravljanje listom posećenih lokacija. Favorizovane lokacije mogu biti aranžirane u odvojene foldere, ili kategorije i postoje kao tekst koji sadrži URL-ove. Vrlo su slični LINK fajlovima koji nas upućuju na pojedinačna dokumenta na našim diskovima. Lokacija za ove fajlove je podrazumevano na istom mestu kao prethodni Internet artefakti, ali je korisnik može premestiti bilo gde.

Listing favorizovanih lokacija može biti dobar izvor informacija za forenzičara: koje lokacije osumnjični regularno posećuje, vremena i datume koje fajlovi sadrže na čvrstom disku mogu biti indikatori aktivnosti i potencijalnih poseta. Međutim, forenzičar mora znati da ulaze na *favorites* listu unosi i sistem, a ne samo korisnik, što mora uzeti u razmatranje. Iako se na ovu listu može staviti sve što korisnik želi, najvažnija informacija su URL koji indiciraju lokaciju na koju se favorizovana adresa odnosi.

Drugi artefakti *Internet Explorer* pretraživača je **Typed URLs**-lista onih ulaza koje je korisnik fizički napravio u prozoru pretraživača. Ova se lista čuva u ključevima Registra i lako se identifikuje. Takođe, ponekad je važno videti koja je startna stranica pretraživača, a ova informacija se čuva u ključevima Registra.

Prethodno razmatranje odnosi se na Windows Explorer kao najčešći u upotrebi. Brojni drugi pretraživači tipa *Mozilla*, *Firefox*, *Safari*, *Netscape*, *Opera*, *Avant* and *FlashPeak* rade na sličan način, ili imaju sopstveni sistem skladištenja Internet fajlova.

5.10 Direktno umrežavanje (peer-to-peer)

Sve češće informacije kruže Internetom kroz direktno umrežene mreže i računare (**P2P**), što je nelegalan način razmene ilegalnih informacija tipa muzičkih sadržaja, softvera i pornografije, a sve to vrlo jeftino, ili besplatno. Jedinu zahtev je da se računar poveže na Internet. Efektivno postoje dva glavna tipa P2P mreža – **FastTrack** klijent i **Gnutella** klijent. Oba tipa rade na različite načine, ali imaju isti cilj – povezati računar sa drugim računarom tako da dele fajlove. Poznatiji klijenti koji se koriste u P2P radu su **CuteMX**, **DC++**, **Kazaa**, **Kazaa Lite**, **Limewire**, **Morpheus**, **winMX** and **EDonkey2000**, ali je lista veoma duga.

Forenzički je interesantan FastTrack protokol, koji je verovatno najbogatiji sa dokaznim podacima. Samo postojanje ovog protokola na računaru indicira potencijalnu primenu, a na računaru ostaje mnogo artefakta posle korišćenja ovog protokola. Detaljniji uvid u oblasti skladištenja ovih fajlova na čvrstom disku obezbeđuje dalje dobre dokaze. Za pretraživanje materijala sa KaZaA, korisnik treba da unese ključnu reč koja se odnosi na traženi materijal. Podrazumevano FastTrack protokol skladišti korišćene termine za pretraživanje u Registar, ali u šifrovanom obliku. Iako su šifrovani, ovi termini se mogu otkriti korišćenjem naprednog alata za Registre, kao što je **Secret Explorer** (www.lastbit.com), ili **Registry Viewer** (*Access Data*) (www.accessdata.com), ili alternativno **KaZAlyzer** alat (www.sandersonforensics.co.uk), koji je specijalno pisan za ispitivanje *FastTrack* protokola i koji obezbeđuje dešifrovane termine za pretraživanje i druge podatke.

Druga oblast interesantna za forenzičku analizu je *Blocklists* koja sprečava pretraživanje i prikazivanje opscenih slika i materijala. Postojanje nekog *My Share Folder* na rutu C: diska je drugi indikator da je korišćen *FastTrack* P2P sistem, a sadržaj ovog foldera mogu biti daunlodovani fajlovi koji su kompletirani, ili **.DAT** fajlovi koji su delimično daunlodovani. Korisnik može izabrati gde će daunlodovati fajlove sa Interneta, ali se podrazumevano nalaze u rutu na **C:** particiji/disku. Pretraživač počinje preuzimanje fajlova iz izvora po uspostavljenoj vezi, ali ako se veza prekine, ili se sistem isključi usred transfera, **DAT** fajl je dovoljno inteligentan da traži isti, ili druge izvore za taj fajl i nastavi preuzimanje dok se ne kompletira.

Pored toga **DBB** fajlovi prate pozicije sistema i koriste se za popunjavanje delova aplikacija, kada se pokrenu. Oni skladište informacije o imenima fajlova, koji su daunlodovani i koji su fajlovi zatim podeljeni sa drugim korisnikom, što je važna analiza u distribuciji pornografskih sadržaja. Takođe, ovi fajlovi sadrže *heš* vrednost fajla koji je korišćen u procesu pretraživanja i deskriptore koji se koriste da identifikuju pretraživani fajl. **DBB** fajlovi su locirani u korisničkom profilu u **Application Data/DB** folderu.

Forenzičar mora znati i da deinstalacija *FastTrack* sistema ostavlja brojne važne tragove za ispitivanje, iako se Registar očisti, ostaje **My Share Folder** kao i **DBB** folder u korisničkom profilu.

5.11 Ostali transferi fajlova

Forenzičar mora biti svestan da mnoge aplikacije za transfer fajlova imaju log fajlove koji omogućavaju da se otkrije kako je aplikacija korišćena. Verovatno najbolji primer su FTP

kljenti koji se koriste za transfer web baziranog materijala na Internet hostove za web lokacije.

Proizvodi kao što su **CuteFTP** i **WS-FTP** sadrže log fajlove svojih aktivnosti, koji obezbeđuju dragocene informacije o transferu fajlova sa vremenima i datumima distribucije.

5.12 Tragovi e-mail poruka

U toku dana razmenjuju se milijarde *e-mail* poruka, što u internim mrežama, što preko Interneta. Mnoge od njih su samo nekorisna pošta - *spam*. Tragovi e-pošte u ispitivanom računaru mogu biti dobar izvor informacija za kompletiranje istrage. Efektivno mogu biti dva tipa e-pošte – *bazirani u aplikaciji računara* i *bazirani na Internetu*.

E-pošta bazirana na aplikaciji je pošta koju na računar donosi i skladišti program. Aplikacije kao što su **Outlook**, **Outlook Express**, **Eudora** i **Pegasus** primeri su ovih programa. Kada korisnik otvori aplikaciju ona ide direktno u skladište e-pošte i izvlači svu dolazeću e-poštu, ili će uraditi to na komandu korisnika. Pored toga, svaka pošta pripremljena za slanje napustiće aplikaciju i biti poslata na određene destinacije.

U ovim aplikacijama često se mogu naći dokazi o primljenim i poslatim e-mail porukama, a pošto se aplikacije nalaze na mašini osumnjičenog to predstavlja izvesni problem za pretragu. Postoje brojni forenzički alati koji analiziraju *e-mail* poruke bazirane na aplikaciji. Za forenzičara je značajno da poznaje tipove fajlova koje može naći u ovim aplikacijama. **Outlook** koristi seriju **.PSF** (*Personal Storage Fils*) fajlova, a može koristiti **.OST** (*Offline Storage Files*), gde korisnik ima lokalno uskladišten materijal na, recimo, laptop računaru, tako da napuštanjem mreže odnosi sa sobom *e-mail* poruke. Ovi fajlovi su podrazumevano šifrovani, pa je traženje ključne reči na disku vrlo teško. Međutim, postoje priznate tehnike za ispitivanje ovih fajlova i softverski alati za njihovo dešifrovanje.

Outlook Express koristi **DBX** sistem fajlova. Postoji po jedan **DBX** fajl za svaki deo aplikacija - INBOX, OUTBOX, SENT ITEMS, DELETED ITEMS, DRAFTS itd. Pored toga, kada korisnik kreira sam novi folder, aplikacija kreira novi **DBX** fajl za skladištenje podataka sadržanih u folderu. **DBX** fajlovi nisu šifrovani, a sadržaj se može pretraživati na disku. Međutim, forenzičar mora znati da kod ovog tipa e-pošte, postoji mnogo podešavanja koja mogu uticati na dokaze, na primer, komprimovani fajlovi na izlazu aplikacija.

Lokacija fajlova **Outlook** i **Outlook Express** normalno se nalazi unutar profila korisnika, ali forenzičar uvek mora imati na umu, da se ova lokacija može izmeniti i smestiti čak i na prenosni medijum, ili u mrežnu jedinicu za skladištenje. U tom smislu forenzičar mora poznavati koncept **Exchange Server**-a i namenskih mašina koje upravljaju e-poštom u organizaciji, što izlazi iz okvira ovog udžbenika.

E-pošta bazirana na Internetu neznatno se razlikuje po načinu na koji forenzičar može pristupiti i analizirati *e-mail* poruke. Iz samog imena vidi se da pošta verovatno nije na lokalnoj mašini koja se ispituje. Postoji izuzetak od ovog, neke se poruke mogu importovati u aplikacije kao što su **Outlook** i **Outlook Express**. U ovom slučaju dokazi će biti unutar podataka fajlova koje ove aplikacije koriste.

E-pošta bazirana na Internetu normalno se istražuje u privremenim Internet fajlovima, uz pomoć forenzičkog alata koji omogućava njihovu ekstrakciju, otvaranje i čitanje. Na osnovu

ključne reči pronalazi se sadržaj e-poruka, bilo baziranih u aplikacijama, ili Internetu, a ostatak poruka leži u nealociranim prostorima diska. Format materijala treba da ukaže da se radi o porukama aplikacija za e-poštu, Veći deo strukture e-pošte, posebno informacija hedera, potpuno je jedinstven za e-poštu.

E-mail *header* može biti neprocenjiv izvor informacija za forenzičara u otkrivanju izvora primljene poruke, ili dokazivanja da je neko odgovoran za neku akciju, ili aktivnost. Primer hedera poruke e-pošte na sledećoj ilustraciji pokazuje šta se sve može naći u njemu (slika 22).

```
Return-path: <paul_davis160@yahoo.co.uk>
Envelope-to: donjohnson160@zoom.co.uk
Delivery-date: Sun, 12 Sep 2004 21:53:46 +0100
Received: from web25207.mail.ukl.yahoo.com ([217.12.10.57])
    by store1.mail.ukl.easynet.net with smtp (Exim 4.32)
    id 1C6bM2-0003TC-CF
    for donjohnson160@zoom.co.uk; Sun, 12 Sep 2004 21:53:46 +0100
Message-ID: <20040912205330.41893.pmail@web25207.mail.ukl.yahoo.com>
Received: from [217.40.25.5] by web25207.mail.ukl.yahoo.com via HTTP; Sun, 12 Sep 2004 21:53:30 BST
Date: Sun, 12 Sep 2004 21:53:30 +0100 (BST)
From: =?iso-8859-1?Q?Paul=20Davis?= <paul_davis160@yahoo.co.uk>
Subject: Test Message 5
To: Don Johnson <donjohnson160@zoom.co.uk>
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="0-1845740439-1095022410=:39998"
Content-Transfer-Encoding: 8bit

--0-1845740439-1095022410=:39998
Content-Type: text/plain; charset=iso-8859-1
Content-Transfer-Encoding: 8bit

Test Message 5 Test Message 5 Test Message 5 Test Message 5 Test Message 5 Test Message 5 Test Message 5
```

Slika 22. Heder e-pošte

Hederi e-pošte najbolje se razumeju ako se čitaju odozdo na gore. Na dnu se vidi stvarna poruka koja je poslat *test message*. Zatim se nalazi neka informacija o korišćenom sistemu kodiranja, koji se koristi u savremenim aplikacijama e-pošte da se usklade sa starijim sistemima i protokolima koji su još u upotrebi. Drugim rečima, poslata e-pošta može koristiti samo određeni opseg, ali je većina poruka veća od tog opsega, što se posebno odnosi na priloge pošte (*attachments*). Zato se poruke moraju *kodiranjem* redukovati da bi bile poslate, a zatim na prijemnoj strani *dekodiranjem* vratiti u normalni format. Da bi se shvatio način na koji je heder struktuiran treba gledati u sledeće linije:

To: lice kome je poruka poslata,

Subject: efektivni izraz o čemu poruka govori,

From: treba da bude lice koje je poslalo poruku.

Date: vreme i datum mašine koja je poslala poruku, prema zapisu same mašine. Međutim, svi prethodni podaci lako se mogu promeniti i lažirati da se poruka i pošiljalac učine anonimnim i teško identifikuju. Ni na ovaj podatak forenzičar se ne može puno oslanjati, kao ni na druge podatke ispod ovog u hederu. Od ove tačke forenzičar može početi da veruje da više ništa pošiljalac poruke, ili mašina nisu dodatno upisivali u heder.

Received: (niža linija u hederu) IP adresa (videti u nastavku) mašine sa koje je poruka poslata i koju je u heder upisao prvi 'pouzdati' server primajući poštu kroz sistem e-pošte i Interneta. U ovom slučaju to je bio *Yahoo mail* server. Naravno forenzičar mora osnovano verovati da je ovaj server korektan i pouzdan. Vreme i datum upisan u hederu može se verifikovati sa vremenom i datumom na samom serveru i potvrditi korektnost rada servera. Pri tome treba voditi računa o vremenskoj zoni.

Message ID: jedinstveni identifikator kojeg u heder stavlja *Yahoo* server – broj je datum i vreme sa brojem milisekundi.

Received: (viša linija u hederu) *Easynet* server koji dodaje liniju u hederu posle prijema pošte od *Yahoo* servera sa svojim datumom i vremenom.

Delivery date: vreme i datum koje dodaje *Easynet* server kada je pošta stavljena u *inbox* primaoca - donjohnson160@zoom.co.uk, koji očekuje prijem pošte sa te lokacije.

Returne Path: lice kome poštu treba vratiti ako se selektuje **REPLY** opcija.

Forenzičar treba da objasni šta je IP adresa u hederu, što je moguće jasnije i kraće. IP adresa je jedinstven identitet nekoga ko je koristio Internet. Kada se korisnik poveže na Internet, ISP koji obezbeđuje tu vezu daje korisniku neku IP adresu za vreme rada na Internetu. Ta IP adresa je jedinstvena za tog korisnika za to vreme boravka na Internetu – slično telefonskom broju. IP adresa se piše u decimalnom zapisu sa tačkama, na primer: **123.45.230.16**. Postoje različiti tipovi mreža, međutim bilo na Intranetu, ili na Internetu, korisnik mora imati IP adresu da bi bio prepoznat i povezan na mrežu. Trenutno se koristi IP verzija 4. Svaki segment IP adrese je neki bajt, drugim rečima IP adresa ima 256 mogućih vrednosti – 0 do 255. Dakle ne može se videti IP adresa sa brojem većim od 255. IP adrese se alociraju nekoj organizaciji koja generalno ima blok IP adresa koje konsektivno mogu pripisati svojim klijentima. Tako u gornjem primeru, ISP je alocirao IP adrese u opsegu 123.45.230.0 do 123.45.230.255 – 256 mogućih adresa. Ako forenzičar želi da identifikuje ko je koristio IP adresu 123.45.230.16, mogu se koristiti brojni alati raspoloživi na Internetu (www.samspace.org ili www.centralops.net) da uzbace tu IP adresu i mogu dati informaciju o tome ko je administrirao tu IP adresu. Dalje treba kontaktirati tu organizaciju i tražiti koji korisnik je koristio tu IP adresu u specifično vreme i datum. U ovoj tački, vreme, datum i vremenska zona dolaze u prvi plan, pa ako se pogrešno očitaju iz analiziranih podataka, IP adresa se može alocirati drugom licu i odvesti istragu u pogrešnom smeru.

IP adrese mogu biti *statičke* – iste svo vreme, ili *dinamičke* – različite svaki put kada se korisnik poveže na Internet, birane iz skupa dodeljenih adresa. U poslednjem slučaju informacije o datumu i vremenu su zaista presudne za forenzički istragu.

5.13 Servisi za četovanje preko interneta

Čet klijenti, posebno najmlađa generacija, postaju sve popularnija zajednica na Internetu, gde su permanentne komunikacije održavaju na dnevnoj bazi. Nažalost, ovaj servis se često zloupotrebljava u brojnim slučajevima dečije pornografije. Savremeni čet servis može biti direktna komunikacija preko tastature, ili glasom –VOIP (*Vice over IP*) preko potpuno besplatnog programa kao što je **Skype**. Pored toga, većina čet klijenata nude razmenu informacija, tako da se šalju i primaju fajlovi. Lista mogućnosti koje čet klijent ima praktično je beskonačna. Nažalost, podrazumevano svi čet klijenti imaju isključenu funkciju istorije, pa je analiza komunikacije tim teža.

Uobičajeno čet klijente uključuju **Yahoo Messenger**, **MSN Messenger** (sa Windows XP OS), **MIRC**, **ICQ**, **AIM** (AOL Messenger) i **Trillian** – multičet program za konferencijsko četovanje više učesnika. Neki čet klijenti registruju činjenicu da je razgovor održan i vreme razgovora, što može biti dobra informacija za forenzičara da je kontakt održan, ali treba imati na umu da se drugi korisnik mogao logovati na mašinu osumnjičenog, ili je najčešće dato lažno ime.

5.13.1 Servis novinske grupe

Novinskoj grupi korisnik može pristupiti preko *Google*-a i sličnih pretraživača sa *Internet Explorerom* i drugim aplikacijama za pretraživanje. Dokazi o korišćenju ovog servisa nalazi se u privremenim Internet fajlovima (Internet kešu). Drugi način pristupa ovom servisu je

korišćenjem neke od brojnih aplikacija za čitanje vesti, kao što je **Forte Agent** i **Outlook Express**. Svaka od ovih aplikacija rade na različit način, ali sve donose poruke grupa u aplikaciju, koje su sada lokalne za mašinu. Ovo olakšava analizu, ali podaci za analizu mogu biti preobimni, pošto neki korisnici mogu biti učesnici više novinskih grupa.

Novinske grupe mogu postati dostupne kada se korisnik registruje, što u većini slučajeva ne zahteva nikakav novac. Ipak, ima izvora gde za određenu članarinu korisnik može pristupiti preko 100.000 novinskih grupa i ne začuđuje, da se baš u ovim grupama može naći najviše aktivnosti ilegalnih grupa - na hakovanju, fišingu, dečijoj pornografiji, terorizmu i drugim vidovima zloupotreba.

Novinske grupe su na sreću struktuirane slično e-pošti, u tome da poruke poslate u novinsku grupu imaju hedere koji su vrlo slični e-mail hederima. Tako postoji mogućnost identifikovanja lica koja su uputila poruku. Jedan od problema koji postoje u novinskim grupama je da informacije hedera koje forenzičar može relativno lako dobiti, ne moraju sadržavati podatke o, na primer, razmeni dečije pornografije, pri čemu slike mogu još uvek biti na serveru novinske grupe.

5.13.2 AOL servis

Iako je ovaj servis vezan pretežno za severnu Ameriku, sve se više širi u Engleskoj i šire. AOL v. 8.0 ili 9.0 korisnik treba da instalira aplikaciju – relevantne osnovne fajlove podešene za AOL i zatim izvrši zamenu relevantnih fajlova. Svaki AOL korisnik dobije ime glavnog ekrana (*master screen name*) koje mu omogućava da nameni daljih 6 imena ekrana, možda za članove familije i rođake. Svako ime ekrana dobija svoj skup fajlova. Na samom AOL forenzičar može oporaviti razne stvari koje se odnose na korisnika – listu favorizovanih, listu najčešćih kontakata, imena ekrana, njihove knjige adresa, uskladištene i pročitane e-pošte, njihove menadžere daunlodovanja, otkucana URL istorija, klijentski logovi i njihove novinske grupe koje šalju poruke u AOL grupe.

Kabinetu za skladištenje personalnih fajlova može se pristupiti ovim metodom zamene, koji daje pristup poslatoj, primljenoj i uskladištenoj pošti na PC mašini. Na ovaj način ne može se pristupiti e-pošti uskladištenoj na AOL on-line.

5.14 Analiza izvršnih fajlova, rutkitova, zadnjih vrata i snifera

Izvršni fajlovi (*executable*) predstavljaju fajlove koji se mogu pokretati kao programi i obično se završavaju sa ekstenzijom **.exe**. Izvršni fajlovi predstavljaju specijalni slučaj digitalne forenzičke analize fajl sistema. U najvećem delu, izvršni fajlovi slede poznatu i dokumentovanu strukturu, zato što ih treba aktivirati na različitim verzijama Windows OS. Međutim, autori malicioznih programa otkrili su način da maskiraju strukturu da bi otežali, ili onemogućili analizu. Razumevanjem strukture i formata ovih fajlova i kako oni treba da izgledaju, forenzičari mogu razlikovati legitimne fajlove i izolovati sumnjive fajlove u Windows OS. Korišćenjem specifičnih tehnika i sa poznavanjem strukture i formata izvršnih fajlova, forenzičar može odrediti koji su fajlovi legitimni i koje artefakte treba pripisati određenom delu malicioznog koda, [5].

Od posebnog značaja za forenzičara je lokacija i poznavanje *Rootkits*, alata koji se sve više koriste ne samo u kompjuterskom kriminalu, nego i u 'legitimnim' komercijalnim aplikacijama.

Rutkitovi i zadnja vrata (Backdoors): Da bi se haker koji počini kompjuterski kriminal uhapsio, potrebno je razumeti alate i tehnike koje hakeri koriste da savladaju korisničke sisteme. Jedan od najčešće korišćenih hakerskih alata za prodor u računarske sisteme su rutkitovi, koji se koriste za sledeće funkcije:

- sprečiti logovanje aktivnosti,
- uspostaviti zadnja vrata za ponovljeni ulaz,
- sakriti ili ukloniti dokaz o inicijalnom ulazu,
- sakriti specifične sadržaje fajlova,
- sakriti fajlove i direktorijume,
- sakupiti informacije, npr., korisnička imena i pasvorde.

Ime *rut kit* dolazi od alata koje sadrži za održavanje, ili držanje u rutu, a ne zato što sadrži alate za krekovanje ruta. U OS Unix i Linux rut je deo sistema sa najvišim privilegijama pristupa. Korisnici sa rut privilegijama imaju pristup svim aspektima OS, zato što pristup rutu implicira kompletnu kontrolu mašine.

Napadači koriste rutkitove za skrivanje i zaštitu svog prisustva u računarskom sistemu. Rutkitovi u Windows sistemima nisu toliko rasprostranjeni kao u Unix OS i obično se detektuju i odvrćaju antivirusnim softverima. U Unix i Linux OS, administratori mreže generalno veruju komandi **ps** za prikazivanje liste svih sistemskih procesa i **ls** komandi za listiranje svih fajlova lociranih na direktorijumu čvrstog disk. Rutkit generalno sadrži set hakerskih uslužnih alata, kao što su skriptovi za čišćenje log fajlova i sniferi mrežnih paketa. Pored toga, rutkitovi sadrže specijalizovane zamene ključnih Unix i Linux pomoćnih alata, kao što su *netstat*, *ifconfig*, *ps*, i *ls*. Iako hakeri moraju dobiti pristup sistemu žrtve pre nego što instaliraju rutkitove, lakoća njihove upotrebe, mogućnost širenja i količina destrukcije koju mogu izazvati, čine ih ozbiljnom pretnjom za administratore računarskih mreža. Neizbežno, u većinu računarskih sistema infiltriraju se napadači ili ih inficiraju neki tipovi malicioznih kodova. Prema javnom priznanju USDOJ, čak ni NASA sistemi nisu imuni na napade rutkitovima.

Detekcija prisustva rutkitova: Ulazak napadača u računarski sistem može ostaviti dokazni trag u različitim porukama log fajla. Većina rutkitova uključuje uslužne alate za automatsko uklanjanje svake sumnjive ili inkriminišuće poruke iz log fajlova. Jedan od uobičajenih indikatora prisustva rutkita u sistemu je kada jedan ili više ključnih uslužnih alata koji su ranije radili bez otkaza, odjednom počne da se ponaša nekonzistentno zato što je napadač zamenio te alate sa verzijama rutkitova dizajniranim da sakriju svoje maliciozne aktivnosti, a koje se razlikuju od standardnih alata. Na primer, komandna linija prebaci na **netstat** ili **ps**, koji organizacija koristi bez problema svaki dan, može početi da vraća pogrešne poruke. Detekcija rutkitova je vitalna iako može biti najteži zadatak za sistem administratora. Rutkitovi spadaju u kategoriju malicioznih kodova tipa virusa, crva i trojanaca i detektuju se manje više na isti način. U stvari, većina rutkitova sadrži komponentu zadnjih vrata trojanca za obezbeđivanje ulaza kasnije. Sofisticiran haker neće ostaviti nikakav trag koji se može otkriti forenzičkim alatima. Drugi mogu ostaviti tragove koje forenzičar može otkriti, ali samo ako je familijaran sa OS i mrežom. Sa povećanjem kapaciteta HD i kompleksnosti OS, traženje dokaza u hiljadama fajlova o prisustvu rutkitova može ličiti na traženje igle u plastu sena. Pored toga, instalacija rutkitova često falsifikuje vremenski pečat i informaciju o

veličini fajla, tako da sprečava vizuelnu kontrolu integriteta od strane sistem administratora sa Unix/Linux **ls** komandom.

Jedan način da se detektuju rutkitovi manuelnom inspekcijom, obično se izvodi korišćenjem *komandne stringova*. Pomoćni alati koji su standardni kod svih modernih Unix/Linux platformi, jedva da prikazuju čitljive delove binarnih fajlova. *Pomoćni string alati (strings utility)* traže *stringove* u regularnim fajlovima koji se mogu štampati i pišu ih na standardni printerski izlaz. *String* je svaka sekvenca od 4 ili više karaktera koji se mogu odštampati i koji se završava sa novom linijom ili sa karakterom **0**. Za iskusne sistem administratore komanda *stringova* može proizvesti čitljive podatke kao što su imena fajlova u kojima napadači drže pasvorde, verzija biblioteke sa kojom je kompajliran rutkit i druge informacije koje normalno nisu u korelaciji sa originalnim podacima u ispitivanom fajlu. Tačna sintaksa koju koriti *komanda stringova* varira u zavisnosti od verzije Unix/Linux OS koji se koristi. Generalno sintaksa za komande *stringova* je sledeća:

```
strings [-a] [-l] [-o] [-t (d) (o) (x)] [-n] [File name etc...]
```

Zastavice (*flags*) koje se koristi u Unix/Linux komandama *stringova* dati su u tabeli 5.

Tabela 5 Zastavice (*flags*) koje se koriste u Unix/Linux komandnim linijama

Zastavica	Funkcije zastavice (<i>flags</i>)
-a ili -l	Ova oznaka traži <i>stringove</i> koji se mogu štampati u celom fajlu (ne samo u sekciji podataka)
-n(broj)	Identična je -number oznaci.
-o	Identična je oznaci -t o i listira sve oktalne linije ofseta u fajlu.
-t(format)	Listira <i>offset</i> svake prethodne liniju komande od početka fajla.
d	Piše ofset u decimalnom formatu.
o	Piše <i>offset</i> u oktalnom formatu.
x	Piše <i>offset</i> heksadecimalnog formata. Napomena: kada su definisane -o i -t formati oznaka više od jedanput u komandnoj liniji, poslednja oznaka specificira ponašanje komandne linije.
-number	Specificira minimalnu dužinu stringa, različitu od podrazumevane vrednosti od 4 karaktera. Maksimalna vrednost dužine stringa je 4 096. Ova oznaka je identična -(number) oznaci
file	Identifikuje fajl kojeg treba pretraživati

Chkrootkit (www.chkrootkit.org) je kolekcija besplatnih alata za detekciju prisustva rutkitova na Linux sistemima. Može detektovati potpise velikog broja različitih, poznatih rutkitova upotrebom jedne aplikacije, ali i pokreće jedan generički test i može otkriti i potpis nepoznatog rutkita kojeg aplikacija ne podržava.

Intact (*Pedestal Software*) može detektovati prisustvo rutkitova kao i druge povrede sistema zaštite u Windows i Unix sistemima. Alat monitoriše promene u računarskim sistemima, uzimanjem *snapshot* objekata stabilnog sistema i poređenjem sa stanjem aktivnog sistema u realnom vremenu. Alat detektuje neovlašćene ulaze, efekte virusa, trojance, grube instalacione programe, korupciju fajlova, izmene bezbednosne konfiguracije i promene u podešavanju log fajlova za *auditing*.

Detekcija prisustva zadnjih vrata: Korišćenje zadnjih vrata za ponovljene ulaske u sistem je popularna tehnika hakera, pošto se alati za postavljanje zadnjih vrata nalaze besplatno na hakerskim sajtovima. Napadači postavljaju zadnja vrata za kasniji ulazak u sistem, koristeći skriveni ID i pasvord za logovanje koji proizvođači hardvera, ili softvera legitimno postavljaju u sistem za svoje tehničare za popravku i održavanje, ili trojance za uspostavljanje neovlašćenog ID i pasvorda za logovanje u sistem. Zadnja vrata za većinu napadača obezbeđuju tri glavne funkcije:

9. ući kasnije u sistem što je moguće skrivenije (da mašina ne ukazuje da ima nekog *online*),
10. ući kasnije u mašinu čak i kada je administrator obezbedi (npr., promenom svih pasvorda),
11. ući kasnije u sistem u što kraćem vremenu.

Veliki broj zadnjih vrata implementiran je primenom trojanaca. U stvari većina rutkitova sadrži „trojanizovanu“ verziju uobičajeno korišćenih programa i sistemskih pomoćnih alata. Dve popularne verzije aplikacija trojanaca, koje rade kao serverske komponente na napadnutom računaru su **BackOrifice** i **SubSeven**. Trojanci za postavljanje zadnjih vrata imaju brojne mogućnosti, uključujući:

- *upload* ili *download* fajlova,
- premeštanje, kopiranje ili brisanje fajlova,
- brisanje HD ili drugog diska podataka,
- izvršavanje programa,
- gledanje ekrana monitora kako ga korisnik vidi,
- aktiviranje log ključa (čak i unos skrivenog pasvorda),
- otvaranje, zatvaranje i premeštanje prozora,
- pomeranje kursora miša,
- gledanje svih otvorenih konekcija prema i od računara,
- zatvaranje mrežnih konekcija itd.

Postoje brojni trojanci koji cirkulišu Internetom. Većinu detektuju i otklanjaju antivirusni programi, ali je za forenzičara korisno poznavati ponešto o svakom od njih. Skraćena lista trojanaca za postavljanje zadnjih vrata data je u PRILOGU 3. U PRILOGU 4 data je lista portova koje rutkitovi i trojanci uobičajeno koriste za postavljanje zadnjih vrata.

Kako često standardni antivirusni programi ne prepoznaju potpise novih rutkitova i trojanaca, na raspolaganju su efektivniji besplatni alati za otkrivanje instalacije trojanaca ili zadnjih vrata u sistemu tipa:

- **Fport.exe**: jedini Windows alat (*Foundstone Inc.*), koji izveštava o svim otvorenim TCP/IP i UDP portovima, ali ih i prati natrag da vlasnika aplikacije, aktivnih procesa sa ID, imenom i putanjom procesa (www.foundstone.com).
- **Superscan**: moćan skener TCP portova, uređaj za pingovanje i detektor imena hostova (*Foundstone Inc.*), ekstremno brz raznovrstan.
- **Nmap**: besplatan mrežni mapper, alat otvorenog koda, koristan za ispitivanje mrežnih konekcija i *auditing* sistema mrežne zaštite, određuje koji su hostovi na raspolaganju u mreži i koje portove koriste. Radi na Unix i Linux OS, a ima verziju komandne konzole i GUI interfejsa. (www.insecure.org/nmap).
- **Listdlls.exe**: windows besplatan pomoćni alat (autor *Mark Russinovich*) koji prikazuje punu putanju modula koji se učitava (www.sysinternals.com).

Detekcija zadnjih vrata sa netstat komandom: Alat komandne linije **netstat**, koristan je za proveru mrežne konfiguracije i aktivnosti u mreži, a podržavaju ga Unix, Linux i Windows OS. Pokazuje koji su portovi na računaru otvoreni i listira sve otvorene konekcije prema i od računara. Za praćenje otvorene konekcije u Windows sistemu, može se koristiti besplatan alat **TCPView**, Windows program koji daje listu svih krajnjih tačaka TCP i UDP (npr., klijent, server itd.), uključujući lokalne i udaljene adrese i stanje TCP konekcija. U Windows NT, 2000 i XP, ovaj alat izveštava imena procesa koji su vlasnici krajnjih tačaka TCP. Alat se može daunlodovati sa www.sysinternals.com.

Uklanjanje rutkitova i trojanaca iz sistema: Za uklanjanje rutkitova i zadnjih vrata nije moguće generisati konzistentnu proceduru za uklanjanje, ali se može dati opšte uputstvo za preduzimanje neophodnih koraka, kao što su:

- Za uklanjanje trojanaca:
 1. Identifikovati fajl trojanca na HD računara.
 2. Otkriti kako je iniciran (npr., preko registra, Startup foldera itd.) i preduzeti akcije za sprečavanje restarta posle rebotovanja.
 3. Rebutovati mašinu i izbrisati trojanca.
- Za uklanjanje rutkitova:
 1. Izolovati napadnutu mašinu (odspojiti sa mreže/Interneta).
 2. Odrediti ozbiljnost kompromitacije.
 3. Početi čišćenje reinstalacijom OS i aplikacija sa poverljivog bekapa.
 - 4.

Detekcija i odbrana od mrežnih *snifera*: Skener (*snifer*) mrežnih paketa je uslužni alat koji monitoriše i loguje mrežne aktivnosti u fajl, praćenjem saobraćaja, ali bez ikakve modifikacije mrežnih paketa. Ranije su to bili hardverski uređaji fizički spojeni na mrežu, a danas su softverski. Hakeri i krakeri ih koriste za hvatanje korisničkih imena i pasvorda koji se prenose kroz mrežu nezaštićeno, npr., u otvorenom tekstu ili čistom ASCII formatu gde se mogu čitati u *Notepad*-u. Takođe, gotovo svaki rutkit uključuje uslužni alat za praćenje mrežnog saobraćaja. Jedna uznemirujuće moćan aspekt *snifera* paketa je njihova sposobnost da postave host mašinu u *promiskuitetan mod* rada, u kojem mašina prima ne samo podatke usmerene na nju, nego i sav saobraćaj podataka u fizički spojenoj lokalnoj mreži, što sniferu daje ulogu špijunskog alata, pošto svaki interfejs u ovom modu sluša ceo mrežni saobraćaj. Detekcija snifera je zahtevan, ali ne i nemoguć posao. Pod Unix i Linux OS, komanda **ifconfig** daje administratoru (superkorisniku) privilegiju da odredi koji uređaj radi u *promiskuitetnom* modu, što je indikator korišćenja snifera u mreži. Za proveru interfejsa pomoću ovog alata treba u RUN-u otkucati **ifconfig** i tražiti string PROMISC. Ako je ovaj string prisutan, interfejs je u *promiskuitetnom* modu. Za otkrivanje odgovornog procesa treba koristiti ugrađen alat kao što je **ps** pomoćni alat za identifikaciju procesa. Za Windows sisteme može se koristiti besplatan softverski alat komandne linije **PromiscDetect** za otkrivanje mrežnih adaptera u *promiskuitetnom* modu, koji se može daunlodovati sa www.ntsecurity.nu/toolbox/promiscdetect/, a radi sa Windows NT 4.0, 2000 i XP OS.

Koristeći činjenicu da promiskuitetni sniferi prate samo saobraćaj koji se deli između segmenata lokalne mreže, mogu se sprečiti postavljanjem mrežnih svičeva, koji „inteligentno“ šalju pakete samo na destinacioni računar, umesto standardnih habova koji šalju pakete na sve povezane računare.

6 Digitalni dokaz

6.1 Digitalni kompjuterski dokaz

Prema definiciji IOCE 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 orginalne digitalne informacije koje imaju dokazujuću vrednost i na koje se sud može osloniti, u kontekstu forenzičke akvizicije, analize i prezentacije.

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 (prepliću) i da nemaju tzv. pukotina za donošenje zaključaka, odnosno za utvrđivanje *čvrstog digitalnog dokaza*.

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. 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, sakupljati ključne dokaze i kritički vraćati na postavljenu hipotezu, tražeći odgovore na pitanja: zašto dokaz nije dobar, gde se izgubila neka važna činjenica, kako naći dokaz koji popunjava prazninu, šta uraditi ako se pronađe itd.? 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 dogodilo. 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 prepiše, ili izmeni. 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, što 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.

U kompjuterskom incidentu postoje tri osnovne kategorije digitalnih podataka koji mogu činiti digitalni dokaz:

- *Promenljivi podaci* ili informacije koje se gube nakon isključivanja računara, kao što su podaci u radnoj memoriji (RAM), rezidentni memorijski programi itd. 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 *log* datoteci itd.
- *Privremeno dostupni podaci*, ili podaci uskladišteni na HD kojima se može pristupiti samo u određeno vreme (npr. šifrovani podaci).

6.2 Pravosudni aspekt digitalnih kompjuterskih dokaza

Podsetimo se kako istražitelji, pravnici i sudije definišu dokazni materijal. Postoje formalna pravila sakupljanja dokaznog materijala, što treba da definiše normativni akt (pravilnik ili uputstvo). U anglosaksonskom sistemu postoji i zakon slučaja (*case law*) koji pokriva definicije i očekivane ishode bazirane na iskustvima i odlukama drugih sudova, a govori kako druge sudije i porote interpretiraju isti zakon.

Kompjuterski kriminal je uneo poseban problem u oblast sudskog veštačenja i svedočenja. Pravilo klasičnog svedočenja kaže da svedok može svedočiti samo ako je *očevidac*, odnosno samo o onome što je lično iskustio (čuo, video, zna), a ne iz druge ruke, što se smatra *posrednim* dokazom, poznat u žargonu kao “rekla – kazala”.

Međutim, kod računara imamo upravo slučaj da se, sve što se nalazi u njemu, može svesti pod kategoriju “rekla – kazala” dokaze. Naime, ništa direktno vezano za događaj se ne vidi u računaru, jer se *login* fajlova može naknadno izmeniti, promeniti datume fajlova, izbrisati ili izmeniti dokument, što praktično znači da samo osoba koja je izazvala kompjuterski incident (kompjuterski kriminalac) ima direktno saznanje o tome i jedini je *očevidac*, odnosno neposredan svedok. Dakle, kompjuterski podaci se mogu koristiti kao dokazi za svedočenje samo ako su veoma pažljivo preuzeti i ako zadovoljavaju neke specifične kriterijume u sudskom veštačenju (forenzičkoj akviziciji i analizi). Ovi su kriterijumi kritični u pogledu sposobnosti digitalnog forenzičara da sakupi što više posrednih dokaza pomoću kojih se dolazi do neoborivog dokaza. Praktično, posredni su svi dokazi u kompjuterskom krivičnom delu, koji se sakupe akvizicijom i analizom samog softvera, računara i/ili računarske mreže. Da bi posredni dokaz bio prihvatljiv za sud mora biti takav da potvrđuje hipotezu o čvrstom dokazu, ili da je pobija. Drugo, mora postojati dokaz da je *login* fajl, kao posredni dokaz, nastao u normalnom radnom procesu. Na primer u slučaju pada servera, potrebno je imati čvrste dokaze da je počinilac bio logovan kada je server pao. Ovo je dovoljno čvrst dokaz da nadležni istražitelj službeno zahteva prisluškivanje linije osumnjičenog i snimi vreme pristupa serveru. Ovo vreme se kasnije upoređuje sa *login* podacima u *log* fajlovima

računara i aktivnostima drugih mrežnih uređaja, što utvrđuje neoboriv dokaz pristupa serveru.

Kompjuterski dokaz mora biti autentičan. Sudski veštak za IKT (IKT veštak), mora potvrditi da je dokaz nepromenjen u odnosu na originalno stanje. Ovo je od kritičnog značaja za prihvatanje dokaza na sudu. Kako su dokazi pribavljeni, čuvani, prenošeni, zaštićeni od izmena i kako se sa njima manipuliralo, ključni su elementi da li će biti na sudu prihvaćeni ili odbačeni. Prethodno, originalno, stanje digitalnih dokaza moraju utvrditi sudski veštaci za IKT svojim svedočenjem, kao i forenzičari i organi istrage koji su te dokaze sakupili, čuvali, analizirali i rukovali njima.

Digitalni kompjuterski dokazi moraju zadovoljiti i sve ostale zahteve pravosudnih organa, koji se odnose na sudske dokaze i to:

- ako je potrebno koristiti kopiju, ona mora biti najbolja,
- ako je original na raspolaganju onda kopija ne važi,
- kopija može zadovoljiti sve zahteve za izvođenje dokaza (npr., printing *login* fajlova), ako postoji originalni fajl u kompjueteru za upoređenje,
- sudski veštak za IKT mora svedočiti kako je kopija (npr., printing *login* fajlova) napravljena, kao i druge detalje rukovanja sa fajlom i kopijom (printingom).

6.3 Upravljanje digitalnim dokazima

Upravljanje digitalnim dokazima koje obuhvata sakupljanje, prenos, analizu i čuvanje, zahteva posebnu diskusiju. Dokazi se čuvaju tokom čitavog lanca istrage, vođenja procesa, dokaznog postupka, suđenja i presude, što znači da je dokaz u posedu suda od trenutka akvizicije do završetka suđenja. Prikupljeni dokaz se mora čuvati od štetnih uticaja koji mogu dovesti do oštećenja: toplote, hladnoće, vode, elektromagnetnog dejstva itd. Svaki fajl sa dokazima treba bekapovati i uskladištiti zajedno sa digitalnim potpisom (DS), npr. CRCMD5, koji kreira siguran heš (*hash*). Sud može prihvatiti digitalno potpisan (heširan) dokaz kao originalan, jer svaka izmena fajlove uništava heš koji je digitalni pečat potpisa, što se lako utvrđuje poređenjem. Dobro je memorisati digitalni potpis u tekst podataka digitalnog dokaza, sve šifrovati i tako uskladištiti i čuvati.

U oblasti korporacijske i zvanične istrage kompjuterskog incidenta, moraju biti pouzdani ne samo svedoci i eksperti, nego i softverski i hardverski alati za forenzičku akviziciju i analizu digitalnih podataka. Načelno, softverski i hardverski forenzički alati, programi za praćenje saobraćaja i detekciju upada u radnu memoriju treba da budu namenski, komercijalno dostupni proizvodi sa sertifikatom o pouzdanosti za ovu vrstu poslova. Tako npr., dokazi sakupljeni sa nepouzdanim i ne-sertifikovanim forenzičkim alatima, mogu biti problematični, ili odbačeni od strane suda. Zato treba dokazati da stavljanje sinfera na mrežu nije namenjeno za prisluškivanje privatnih lica i ugrožavanje njihovih ljudskih prava, nego za dokazivanje upada neovlašćenog lica u IKT sistem.

Digitalni dokaz podrazumeva da postoji pravo vlasništva nad IKT sistemom, fajlovima i programima koji su oštećeni. Drugim rečima, ako se ne može dokazati da je nešto lično (privatno), onda se ne može ni optužiti neko da je to ukrao, oštetio i/ili izmenio. *Prava vlasništva* u IKT sistemima uspostavljaju se primenom, tajnih lozinki, mehanizama kriptozastite i drugih mehanizama za kontrolu pristupa, skrivenih fajlova, raznih upozorenja, koja sugerisu da je to vlasništvo i da bez eksplicitne dozvole vlasnika nema pristupa.

U dokazivanju kompjuterskog incidenta najbolje je doći do osumnjičenog računara, a kako to često nije moguće onda barem do fizičke (*mirror*) slike njegovog čvrstog diska (HD). Na osnovu te slike treba formirati ispitni HD na forenzičkom (ispitnom) računaru, koji mora biti tačan fizički duplikat HD računara osumnjičenog.

Ako inicijalna istraga unutar IKT sistema utvrdi da je napad došao izvan tog sistema i ako menadžer, ili vlasnik sistema donesu takvu odluku, onda se u toj tački moraju angažovati zvanični organi istrage, da bi se dobio nalog suda za pretres i privremeno oduzimanje osumnjičenog računara, radi akvizicije digitalnih dokaza. Ako je napad došao iz druge organizacije u istoj državi, treba doći do lokalnog administratora IKT sistema te organizacije i sa njim nastaviti istragu. Osumnjičeni računar obavezno treba zaštititi od kompromitacije, kad god se dođe do njega.

6.4 Procedura sakupljanja posrednih kompjuterskih dokaza

U procesu akvizicije koja obuhvata otkrivanje, identifikaciju, izvlačenje i sakupljanje digitalnih kompjuterskih dokaza, samo supljanje digitalnih dokaza zaokružuje se kroz više aktivnosti. Ozbiljnija procedura skupljanja digitalnih dokaza treba da obuhvati najmanje sledeće aktivnosti:

- Sakupljati sve podatke koji podržavaju osnovnu hipotezu o tome kako je došlo do kompjuterskog incidenta, odakle je napad potekao i šta je urađeno na napadnutom računaru.
- Sakupiti sve podatke koji su kontradiktorni postavljenoj hipotezi, da bi se podržalo dato objašnjenje, ili lakše suprotstavilo argumentima druge strane u sporu. U većini slučajeva, posebno u kriminalističkoj proceduri, treba imati na umu da obe strane žele da otkriju i podnesu *neoborive dokaze*.
- Sakupiti sve pokretne medije (diskete, CD-ROM,...) otkrivene na lokaciji osumnjičenog računara i analizirati ih. Ta analiza može se vršiti pomoću programa za analizu pokretnih medija (npr. *Sydex Anadisk* za diskete). Takođe se moraju sakupiti svi štampani materijali, rukopisi, zabeleške i dr., koji mogu ukazati na rasvetljavanje spornog događaja.
- Napraviti skice ili fotografisati osumnjičeni računar i sve periferne uređaje; označiti i sačuvati sve periferne uređaje i kablove radi ponovne montaže u forenzičkoj laboratoriji.
- Ako postoje matrični ili impakt printeri, ukloniti ribon i staviti novi; originalni ribon ispitati kao dokazni materijal; ako postoji displej na kompjuterskom ekranu, fotografisati ga.
- Isključivanje osumnjičenog računara je posebno osetljiva operacija. Zavisno od operativnog sistema (OS), postoje dve mogućnosti: ispitivani računar se može isključiti na klasičan način bez straha da će se izbrisati dokazi o upadu, ili se ne sme isključivati, jer bi se isključivanjem mogli uništiti dokazi o upadu. Na primer, ako se *Unix* mašine ne isključuje propisno može doći do oštećenja fajlova, ali ako se *Windows* mašina isključuje propisno, može doći do gubitka potencijalnih dokaza. Međutim, u ovim sistemima se lako kreiraju anti-forenzičke, tzv. *boby* zamke za uništavanje fajlova sa dokazima, ako se računar isključuje po propisu. Zato uvek postoji dilema da li računar isključiti propisno i sprečiti uništavanje nekih fajlova, ili ga isključiti nepropisno čime se omogućava aktiviranje *boby* zamke koja može da uništi dokaze. Kako će postupiti u konkretnom slučaju, to sam istražni organ mora proceniti. U ovom slučaju najbolje je koristiti pomoć sudskog veštaka, eksperta za

IKT, odnosno specijaliste za dati OS i platformu, kome se mora dobro objasniti legalni aspekt zahteva za zaštitu integriteta digitalnih dokaza.

- Ako je sigurno da postoji ugrađena zamka, najbolje je računar jednostavno isključiti iz mreže izvlačenjem kabla za napajanje sa zadnje strane računara, uz rizik da će biti uništeni neki podaci. Naravno, neki računari tako ne mogu da se isključe, npr., mainframe i mikrokompjuteri. Zato je potrebno angažovanje eksperta za IKT, koji treba da onesposobi svaku logičku bombu sakrivenu u napadnutom računaru.
- Za rebootiranje ispitivanog računara nikada ne treba koristiti njegov OS i komandnu liniju. Računar treba butirati sa butabilnog diska, koji je fizički zaštićen od upisivanja, čime se sprečava unošenje virusa, ili sa CD ROM-a koji je fizička slika OS.
- Kada se završi rebootiranje sistema, prvo se uzima fizička slika HD-a (alatom tipa *Drivespy*, *X-Way Forensic* i sl.), zatim se sakupljaju drugi dokazi i preliminarno ispituju. Najbolji način za skladištenje fizičke slike HD je optički disk (CD), jer je otporan na oštećenja usled elektromagnetnih zračenja iz okruženja, tj. ne može se brisati (osim ako je *rewritable* tipa), a može se lako kopirati.
- Privremeno oduzeti osumnjičeni računar sa svim pokretnim medijima, treba uskladištiti na bezbedno mesto, zaštićeno od uticaja okoline, posebno elektromagnetnih polja i obezbediti od neovlašćenog pristupa, jer se veštak mora zakleti na sudu da dokazni materijal nije bio dostupan neovlašćenim licima.
- Za razliku od pisanog dokaza, digitalni dokaz često može egzistirati u različitim formatima ranijih verzija, koje su još dostupne na HD. Poznavanjem lokacija njihovog postojanja i korišćenjem adekvatnih alata za forenzičku akviziciju sa različitih apstraktnih slojeva računarskog sistema, čak i izmenjeni formati istih podataka mogu se lako otkriti. Proces akvizicije najbolje poznaje iskusni forenzičar, koji najbrže otkriva moguće dokaze. Osim toga, u slučaju preliminarog ispitivanja i identifikacije digitalnih dokaza na licu mesta, kada se računar iz nekog razloga ne oduzima u cilju istrage, niti se pravi forenzička kopija HD, forenzičar najbrže identifikuje skrivena, nealocirana i izbrisana mesta koja treba gledati, znake koje treba tražiti i dodatne izvore informacija za relevantne dokaze, kao što su raniji formati podataka, npr., u *Memos*, *Spreadsheets*, .. koje postoje na HD, ili u bekap mediju, ili različito formatirane verzije podataka, npr. *.templates*, *.doc*, *.pdf* i sl., bilo da su tako namerno formirane ili su tretirane drugim aplikativnim programima, npr., *Word processing*, *spreadsheet*, *e-mail*, *timeline*, *scheduling*, *graphic*.
- Zaštita integriteta dokaza je kritična faza. Iskusan forenzičar mora obezbediti:
 - da ni jedan mogući dokaz ne bude oštećen, uništen ili kompromitovan na neki način sa procedurom forenzičke akvizicije i analize računara,
 - da se ni jedan mogući kompjuterski virus ne sme ubaciti u ispitivani računar u toku procesa akvizicije i analize,
 - da se sa potencijalno relevantnim dokazima propisno manipuliše i da se isti štite od eventualnih mehaničkih ili elektromagnetskih oštećenja,
 - da se uspostavi neprekidni lanac čuvanja i održavanja integriteta dokaza,
 - da funkcionalni aspekt ispitivanog sistema bude ugrožen što je moguće kraće vreme, ili nikako,
 - da se dobije bilo koja potrebna informacija u toku forenzičke akvizicije i analize, od saslušanih lica, ili advokata koji su prema etičkom kodeksu dužni pružiti sve neophodne informacije forenzičaru.

6.5 Korisnici kompjuterskih digitalnih dokaza

U procesu istrage kompjuterskog kriminala mnogi organi i institucije mogu zahtevati i koristiti kompjuterske digitalne dokaze, kao što su, [9]:

- tužilaštvo,
- pravosudni organi u privatnom parničkom postupku (pronevera, razvod, diskriminacija, uznemiravanje i sl.),
- osiguravajući zavodi, za moguću prevaru u slučajevima kompenzacije oštećenih lica i sl.,
- organizacije (vlasnici napadnutog informacionog sistema),
- zvanični istražni organi (MUP, BIA, VBA),
- pojedinci (vlasnici napadnutog sistema) i
- udruženja i samostalni IKT veštaci za potrebe veštačenja.

6.6 Priprema digitalnih dokaza za veštačenje pred sudom

Nezavisni ekspert za IKT koji pomaže istražnom organu u otkrivanju i akviziciji podataka treba da ima iskustvo iz široke oblasti informaciono komunikacionih tehnologija. Takav ekspert je uvek od velike koristi kada se vrši istraga konkretnog kompjuterskog incidenta. Međutim, iako je osnovni dizajn računara i aplikativnog softvera često sasvim sličan kod većine OS, pa se znanja iz jednog sistema lako prenose na drugi sistem, ipak za poslove akvizicije i forenzičke analize uvek treba angažovati kvalifikovanog eksperta za IKT, specijalistu za konkretni OS, program, platformu, mrežu itd., [10], [17].

Digitalne dokaze od trenutka otkrivanja do zaključno sa forenzičkom analizom, treba uvek tretirati kao da će biti prezentirani na sudu. Na sudu u parničkom ili krivičnom postupku, zavisno od težine kompjuterskog incidenta, digitalne dokaze prezentira-veštači zakleti sudski veštak za IKT, kvalifikovan za predmetni hardver i softver, krajnje objektivno, tačno, uverljivo i razumljivo. U najvećem broju slučajeva digitalne dokaze na sudu prezentira forenzičar koji je u toku istrage vršio akviziciju i forenzičku analizu digitalnih dokaza. Naravno, obe strane u sporu mogu zahtevati i druge, nezavisne veštace za IKT, što neminovno podrazumeva unakrsno ispitivanje i sučeljavanje mišljenja dva veštaka za IKT, podjednako istih znanja i iskustava. To je u praksi često faktor odvratanja, jer istaknuti eksperti za IKT odbijaju sudsko veštačenje i sučeljavanje mišljenja sa drugim podjednako dobrim sudskim ekspertom i radije prihvataju ulogu neutralnog stručnog konsultanta tužioca, ili samog sudije.

U pripremi za prezentaciju digitalnih dokaza na sudu veštaci za IKT moraju obaviti mnogobrojne konsultacije sa advokatom stranke koja ih angažuje (tužilaštva ili odbrane), za izbor metode prezentacije (korišćenje pomoćnih audio – vizuelnih sredstava, strategiju nastupa i sl.), a sami se psihički pripremaju za unakrsno ispitivanje i eventualno suočavanje sa svedočenjem drugog veštaka.

6.7 Preporuke IOCE za upravljanje digitalnim dokazima

Preporuke IOCE definišu postupke sa prikupljenim i obrađenim dokazima, [14]:

- Za čuvanje fizičke kopije digitalnih dokaza *nisu prihvatljivi* instant film paket, indžekt printeri, ink printeri, termalni voštano – papirni printeri, *dye* sublimacioni printeri, suvo srebrni printeri, laserski printeri i elektrostatički printeri.
- Za čuvanje originalne fizičke kopije digitalnih dokaza *prihvatljivi su*, zbog kvaliteta, trajnosti i pouzdanosti klasični filmovi na bazi srebro – oksida, CD ROM za jedno upisivanje (ne RW) i DVD.

- Za čuvanje originalne fizičke kopije digitalnih dokaza *moгу se koristiti*, uz kontrolu eventualnih gubitaka podataka posebno razvijan instant film, fotografski print, diskete, magnetne trake, HD, prenosni magnetni mediji, kompakt fleš memorija, PC kartice, smart kartice, prenosni magnetno–optički diskovi i magnetno–optički diskovi za jedno upisivanje.
- Za analizu treba koristiti *radnu fizičku kopiju*, a jednu *fizičku kopiju* sumnjičenog računara sačuvati kao referentni dokaz integriteta.
- *Dokumentacija* za analizu fizičke slike osumnjičenog računara mora biti precizna, detaljna, neporeciva i napravljena na poverljivom forenzičkom sistemu.
- *Verifikacija* referentne i analizirane radne kopije mora biti obavezna i da nepobitno potvrđuje da nije bilo povrede integriteta originalnih dokaza.
- *Čuvanje referentne fizičke kopije* u lancu *istrage* je stroga obaveza od pokretanja istrage i otkrivanja dokaza do svedočenja na sudu.

Procedura se mora administrativno propisati u svakom pravosudnom sistemu i mora postojati zakonska obaveza svakog pojedinca da čuva integritet dokaza.

7 FORENZIČKA ANALIZA DIGITALNIH PODATAKA

7.1 Forenzička analiza softvera

Pojam **kompromitovanog računara** najčešće se odnosi na **napadnuti** računar („žrtvu”), ali, za potrebe forenzičke analize zavisno od konteksta, može obuhvatati i **osumnjičeni izvorni, ili posredni** računar, jer je u praksi istrage digitalnih dokaza često neophodno izvršiti forenzičku analizu računara sa kojeg je izvršen napad, napadnutog računara i nekog od posrednih računara, na primer preko čijeg naloga je napadač ušao u sistem. Dakle, kompromitovani računar je i osumnjičeni računar koji sadrži i distribuira kompromitujuće materijale, na primer dečiju pornografiju i sl., [25].

Forenzička analiza digitalnih podataka, prema izvoru podataka, generalno se deli u tri glavne oblasti:

- forenzičku analizu softvera,
- forenzičku analizu računara i
- forenzičku analizu kibernetičkog prostora (računarskih mreža).

Analiza softvera, uglavnom visoko teoretski posao, najosetljiviji je deo digitalne forenzičke analize. Izrada softverskih alata za forenzičku analizu softvera je težak i složen posao, [5]. Ključ za identifikaciju autora malicioznog kôda je u selekciji odgovarajućeg korpusa kôda i identifikaciji odgovarajućih karaktersitika za upoređivanje [22].

Očigledan problem je što autori preduzimaju velike mere da sakriju svoj stil. Drugi manje vidljiv problem forenzičke analize softvera je što izvorni kôd analiziranog softvera nikada nije poznat. Ako se primeni inverzni inženjering sa izvornim kôdom kompajlera, može se rekonstruisati izvorni kôd programa. Međutim, na njega utiče kompajlerski kôd, koji u inverznoj rekonstrukciji vraća samo jedan programski kôd, koji ne mora obavezno biti pravi. Naime, isti kôd otkriven za vreme dekompajliranja može imati bilo koji od nekoliko različitih originalnih izvornih instrukcija.

Ipak postoje karakteristike u izvršnom kôdu koje mogu biti korisne za analitičara. Na primer, struktura podataka i algoritmi mogu biti jedinstveni za nekog programera i mogu sugerisati identitet, ako se posmatraju zajedno sa drugim faktorima istrage. Informacije o

korišćenom kompajleru i izvornom sistemu mogu biti umetnute u kompajlerski kôd. Programerske greške takođe mogu biti konzistentne i individualne su, pa ukazuju na identitet programera.

Raspoloživost originalnog izvornog kôda programa je od presudnog značaja i korisniji od kompajlerskog izvornog kôda. Neke od identifikacionih karakteristika su:

- selektovani jezik,
- metod formatiranja,
- stil komentara,
- imena varijabli,
- spelovanje i gramatika,
- korišćenje karakteristika jezika,
- izvršni putevi,
- bagovi i dr.

Obično kiber-pankeri dodaju pseudonime i druge komentare u svoj kôd, što profesionalci ne čine. Pisci virusa obično spadaju u kiber-pankere, dok pisci logičkih bombi i sopstvenih alata za upad nisu u toj kategoriji.

Druga oblast problema je kada deo kôda originalnog programera napadač izmeni, što forenzičara dovodi do programera, a ne do napadača. Kod analize malicioznog kôda korisno je suziti listu poznatih mogućnosti na prihvatljiv nivo i nastojati prikupiti što više uzoraka kôda napisanog od strane osumnjičenog, eliminišući eventualne tragove do programera.

7.2 Forenzička analiza računara

Forenzička analiza računara je aplikacija ispitivanja računara i tehnika analize u cilju određivanja potencijalno legalnih dokaza, generisanih, ili uskladištenih u računaru. Kompjuterski specijalisti mogu primeniti brojne metode za otkrivanje podataka koji se nalaze u računarskom sistemu, ili za oporavak slučajno izbrisanih, šifrovanih, ili oštećenih fajlova podataka, koje mogu pomoći kod izgradnje neoborivog digitalnog dokaza za pravosudni postupak. Međutim, za otkrivanje, izvlačenje i oporavak namerno izbrisanih, oštećenih ili sakrivenih podataka u računarskom sistemu, potrebna su dodatna znanja, veštine i forenzički alati i iskusni digitalni forenzičari.

Forenzička analiza računara je najobimniji deo digitalne forenzike, jer se u krajnjem slučaju brojni tragovi napada iz, ili izvan lokalne mreže, ili sa Interneta, uvek nalaze u nekom računarskom sistemu.

7.3 Forenzička analiza kibernetičkog prostora

Forenzičku analizu kibernetičkog prostora bez sumnje je najkompleksnija oblast digitalne forenzike i može biti veoma spor proces. Osnovni zahtev je uspostavljanje legalne saradnje država u borbi protiv kompjuterskog kriminala, uključujući usklađivanje standarda za kvalitet, akviziciju, analizu, prezentaciju i upravljanje digitalnim dokazima. Obično je potrebno da napadač bude na liniji, da bi bio uhvaćen. Neophodna je saradnja telefonskih kompanija i Internet servis provajdera (ISP), kao i zvaničnih istražnih organa.

U proceduri otkrivanja traga napadaču sa Interneta, treba sagledati IP adrese u *login* fajlu napadnutog računara i izvorne IP adrese koje su uhvatili mrežni *sniferi*, IDS/IPS i *Firewalls*, kao i informacije dobijene korišćenjem alata kao što su:

- ReverseFinger,
- Nslookup,
- TraceRoute itd.

Sve ovo za profesionalnog napadača može biti nedovoljno, ali je polazna tačka za napad i dobra osnova za početak forenzičke istrage kibernetičkog prostora.

Za hvatanje napadača sa Interneta i praćenje aktivnosti na napadnutom sistemu, veoma je važno obezbediti što više podataka o *online* logovanju. Nažalost, tih podataka nikada nema dovoljno u log fajlovima. Treba početi od toga da kompetentan napadač verovatno povremeno uskače u *web* lokacije i ostavlja zamke za upad (tipa trojanca ili *trap doors*), pre nego što preduzima sam napad u potpuno neodređeno vreme. U Log datoteci Unix platforme treba tražiti:

- Vreme logovanja i izlogovanja – npr., pomoću alata tipa *Lastlog*;
- Analizirati anomalije u *Lastlog* – korišćenjem alata za analizu log fajlova, kao što su npr., *Chklastlog*;
- Izvori IP adresa – korišćenjem *Syslog* ili drugih logova mogu se snimiti IP adrese. *Syslog* mora biti konfigurisan za ovaj tip informacija. On može proizvesti neku od nekoliko *Messages* fajlova. Drugi logovi mogu biti iz *TCP wrappers* instaliranog na kritičnim servisima. Slične informacije postoje u NT logovima. *Win 95* i *NetWare* nude malo, ili nimalo informacija o logovanju, dok log fajlovi *Win 2000/XP/2003* OS daju prihvatljiv nivo podataka;
- Kada se otkrije najbliža *web* lokacija sa koje se napadač ulogovao treba uspostaviti vezu sa administratorom te lokacije. Odatle treba ići na sledeću lokaciju i ako ima sreće dobiti IP adresu izvora, idući po tragu napada unazad. Ako je napadač *online* može se koristiti alat (tipa *Reverse Finger*, *Route Trace*) za otkrivanje lokacije napadača. Ako napadač koristi posredni računar, što je najčešće slučaj, ovaj alat nije od koristi i tu se istraga zaustavlja.
- Izvor napada sa Interneta često mogu biti administratorski serveri velikih ISP. Korišćenjem *TCP wrappera* u *Telnet* servisu može se identifikovati izvor napada. *Wrappers log* fajl registruje svaki pokušaj legalnog i ilegalnog logovanja, kao i odbijanja logovanja. *Login* fajlovi mogu da ne otkriju identitet stvarnog napadača. Zato treba biti zadovoljan ako se otkrije mašina sa koje je napad izvršen. Za uspešnu potragu za napadačem treba locirati izvornu mašinu, precizno vreme napada i IP adresu napadnutog računara (žrtve).
- Ako se napad ponavlja mogu se svi ovi podaci uhvatiti sa *sniferom* - skenerom za kontrolu mrežnog saobraćaja. IDS/IPS se mogu postaviti da reaguju na pakete koji sadrže sumnjive IP adrese: kada se aktiviraju alarmi, snimaju sve transakcije sa te adrese. Sofisticirani IDS/IPS mogu snimiti čitav scenario napada u detalje (npr., *Real Secure IPS*, *Internet Security Systems*). *Real Secure* softverski alat zavisi od profila napada i identifikuje pokušaje sumnjivih napada. Može preduzeti specifične akcije kao što je detaljno logovanje. Ovako detaljno dokumentovano logovanje veoma pomaže u forenzičkoj analizi napada i može biti čvrst dokaz ako se propisno sačuva. Neki IDS programi postižu iste rezultate, očitavanjem log fajlova u realnom vremenu i preduzimanjem skriptovanih akcija. Primer je alat: *ITA*, AXENT Technologies. Ovi su programi više usmereni na hostove pod napadom, dok su *sniferiski* tipovi programa fokusirani na aktivnosti u mreži. U traganju za napadačem koji ponavlja napad treba instalirati oba ova programa. Obično se nastoji prikupiti što više dokaza

da bi se moglo opravdano obratiti zvaničnom organima istrage kompjuterskog kriminala za dalji tok istrage.

- Prvi napad u IKT sistem najverovatnije dolazi preko telefonske veze. Postavljenje zamke za napadača i traganje za njim preko telefonskih veza podrazumeva uključivanje zvaničnih organa. Ako je napadač koristio telefonsku liniju, prva lokacija koju je napadač koristio posebno je značajna za istragu. Ako je koristio ISP vezu, obično postoji dobro registrovan pristup napadača u modemu koji je primio poziv. Većina ISP koriste skup modema sa terminalnim serverima koji pripisuju IP adrese slučajnim korisnicima koji biraju broj skupa modema. U datom vremenu napada log fajl registruje liniju sa koje je došao poziv. Odavde telefonska kompanija može odrediti odakle je poziv došao, što je za forenzičara vrlo korisno. Loše je što telefonski *frikeri* lako mogu hakerisati telefonske linije i sakriti stvarnu liniju sa koje pozivaju, što može biti kraj istrage korporacijskih organa i početak zvanične istrage.

Sistemske log fajlovi obezbeđuju dokaze o upadu u mrežu i host računar. Problem je što ovi fajlovi imaju svoja ograničenja, kao što su:

- Mora se dokazati da log fajl nije izmenjen, da bi imao *dokaznu* vrednost. Log fajlovi mogu biti modifikovani pre otkrivanja od strane digitalnog forenzičara. Ako je log fajl locirana na mašini žrtve, tj. može joj pristupiti administrator mreže, ili drugi supervizor, potrebno je objasniti da oni ili drugi sa istim ovlašćenjima nisu upali u log fajl i izmenili ga pre akcije forenzičara. Poznato je da dobar napadač obavezno očisti log fajlove i moguće tragove nekom od anti-forenzičkih tehnika. Jedina opcija u ovom slučaju je obezbediti validan dokaz koji pokazuje da fajl nije izmenjen. To može biti takav oblik log fajla koji ne može biti korumpiran, na primer: *ITA* od *AXENT* i *RealSecure* od *ISS* koji štite log fajl od modifikacije, ili direktan svedok koji potvrđuje da su se događaji prikazani u log datoteci stvarno desili. Log fajl se može obezbediti za rad na više načina. Najbolji metod je automatski skladištiti log fajl sa računara žrtve na log server mašinu namenjenu za arhiviranje logova (*log host*). Pristup *log host* mašini treba da bude ekstremno ograničen. Log fajl treba da bude bekapovan na pouzdan disk, ili drugi medijum, koje treba čuvati kao dokaze.
- Drugo ograničenje log fajlova je njihova kompletnost. Koristan log fajl za realizovan događaj treba minimalno da sadrži sledeće podatke: kada se događaj desio, izvor događaja i prirodu događaja. Najkompletniji logovi su uvek zahtevni, troše resurse sistema i smanjuju performanse. Dakle, veličina log fajlova mora biti kompromis između kompletnosti i funkcionalnosti.

Preporučuje se da log fajlovi pokazuju sledeće važne informacije:

- sve pristupe superkorisnika,
- sva logovanja i izlogovanja,
- pokušaje da se koristi bilo koji kontrolisani servis (npr. FTP, TELNET, R servise, itd.),
- pokušaje pristupa kritičnim resursima (fajlu lozinki, kernelu, *wrapper-u*, itd.) i
- detalje o e-mail porukama;

TCP wrapperi i drugi obično pišu svoje logove u sistemske log fajle u Unix sistemu. U NT Windows OS nema specijalizovanih programa kao *wrappers*, ali *security log* se može podešavati da sadrži više ili manje detalja. Često je zgodno na Unix mašinu žrtve instalirati *wrapper* i pustiti napadača da napada dovoljno dugo da se prikupe informacije o njemu i omogućiti izrada profila napadača. Da bi se dobile informacije koje se ne pojavljuju u log fajlu, bilo da logovanje nije kompletno, ili nema log fajla, može se koristiti kompjuterska forenzička tehnika. Cilj je sakupiti informacije koje su ostale na HD. Prva mogućnost je da je događaj logovan i log izbrisan pre nego što ga forenzičar pokupi. Ostaci log fajla na HD

mogu biti oštećeni, jer *login* program stalno prepisuje stare informacije (po principu FIFO-*first in-first out*). Moguće je analizom sektora HD i vremenskih fajlova rekonstruisati log fajl.

Analiza multiplikativnih logova ima za cilj da obezbedi kolaboraciju i da popuni praznine u istrazi. **Primer:** Neka imamo log fajl na Unix računaru žrtve koji nije kompletan. Sa alatom tipa *Chklastlog* možemo proveriti da li je log fajl menjan, ali alat ne garantuje da je log fajl kompletan. Kako postoje veoma efikasni hakerski alati koji mogu izmeniti log fajl, cilj multiplikativne analize log fajlova je da se pronađu razlike u onome što log fajlovi pokazuju i stvarnih događaja. Nažalost, ova analiza je vrlo osetljiva i dugotrajna, posebno za velike fajlove, jer je potrebno imati više log fajlova za isti događaj i uporediti istovetnost vremena za iste događaje. Ima više izvora ovih log fajlova: napadnuti računar, koji može imati TTPS program za višestruko, odvojeno logovanje, zatim bezbednosni log, sistemski i aplikativni logovi i potrebno je dobro poznavati predmetni OS. Korisno je napraviti analitičku radnu kartu za sistemske log fajlove u mreži kao u tabeli 6.

Tabela 6 Analitička vremenska radna karta sistemskih log podataka

	Sistemske log datoteke (isti događaj)		
	Log 1	Log2	Log 3
Vremena	15.12.2004 12:30	15.12.2004 12:35	15.12.2003 12:30

Korisno je analizirati SU (*Swich User*) log fajl, zato što napadač često ulazi u IKT sistem koristeći jedan nalog i prelazi na drugi nalog unutar kompromitovanog sistema. Kada se otkrije praznina u jednom log fajlu treba je popuniti vremenom za isti događaj u drugim log fajlovima. Nije neuobičajeno da hakeri dodaju informacije u log fajlove, da dovedu u zabludu forenzičara. Česte su promene ID u log datotaci. Zato log datoteci nikada ne treba verovati na prvi pogled. Ako forenzičar ne može naći još nešto da korelira kritičnom log ulazu, treba pretpostaviti da nešto nedostaje. U kompleksnom sistemu računara ništa se ne dešava bez povoda. Uvek postoji neka indikacija da se neki događaj dogodio. Na primer, treba rutinski porediti bezbednosni log fajl na računaru sa fajlom logovanja grešaka (pogrešnih ulaza i sl.) *urgent log* fajla, sačinjenim od ulaza deriviranih iz različitih izvora. Bezbednosni log je kombinacija bezbednosnih događaja logovanih sa *syslog* fajlovima i onih logovanih sa TTPs bezbednosnim programom. Log grešaka dolazi iz *syslog* fajlova, nakon što napravi *urgent* log fajl. Forenzičar dodaje *wrappers* log fajlove bezbednosnim log fajlovima u analitičkoj radnoj karti za svaki kritičan događaj i dobro ih analizira. Potrebno je više puta gledati i međusobno porediti log fajlove iz raznih mašina za iste (kritične) događaje. Najbolje rešenje je imati *log host* mašinu u koju treba smestiti sve log fajlove i tu ih kombinovati i analizirati. Sklapanje (rekonstrukcija) velikih log fajlova sa HD je veliki izazov, ali postoji više dobrih alata:

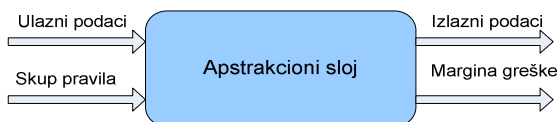
- *TEXTSEARCH* softverski alat: dobar za ASCII log fajlove; traži stringove vremena i teksta koji indiciraju događaje;
- *ASAX* (*freeware* paket) za Unix OS: dopušta kreiranje log *parsing* skripta, koji može tražiti različite stringove teksta;
- *ACL* (*Audit Command Language*): *ASAX* alat za DOS /Windows OS;
- *ASCII* (*CDL- Comma Delimited*): format u kojeg se eksportuje log fajl, a *CDL* dopušta čitanje i analizu u bazi podataka *spreadshit* dokumenata, kao što su *Excel* ili *Lotus 1-2-3* itd.

7.4 Slojevi apstrakcije

Slojevi apstrakcije računarskog sistema koriste se za analizu velike količine podataka u mnogo lakše upravljanoj formatu. Oni su nužne karakteristike dizajna savremenih digitalnih sistema, zato što su svi podaci, bez obzira na aplikacije, predstavljeni na disku, ili mreži u generičkom formatu *bita* – (1 i 0). Za korišćenje ovog generičkog formata skladištenja digitalnih podataka za uobičajene aplikacije, aplikacija prevodi bitove u strukturu koja zadovoljava njene potrebe. Uobičajeni format je sloj apstrakcije.

Primer bazičnog apstrakcionog sloja je ASCII kôd u kojem je svakom sloju engleskog alfabeta pripisan broj od 32-127. Kada se memoriše tekst fajl, slova se prevode u njihove numeričke reprezentacije i broježane vrednosti se memorišu na medijumu. Gledanjem sirovih podataka fajla prikazuje se serija 1 i 0. Primenjujući ASCII sloj apstrakcije, numeričke vrednosti se mapiraju prema odgovarajućim karakterima i fajl se prikazuje kroz seriju slova, brojeva i simbola. Tekst editor je primer rada na ovom sloju apstrakcije.

Svaki sloj apstrakcije može se opisati kao funkcija ulaznih i izlaznih veličina. Ulazne veličine u apstraktni sloj su kolekcija podataka i neki skup pravila za translaciju. Skup pravila opisuje kako treba procesirati ulazne podatke i u većini slučajeva je specifikacija dizajna objekta. Izlazne veličine svakog sloja apstrakcije su podaci derivirani iz ulaznih podataka sa marginom greške. U primeru ASCII sloja apstrakcije, ulazne veličine su binarni podaci i skup pravila za pretvaranje binarnih podataka u ASCII kôd. Izlazne veličine su alfanumeričke reprezentacije. Izlazni podaci sa sloja mogu biti ulazne veličine u drugi sloj apstrakcije, bilo kao aktuelni podaci koje treba prevesti, ili kao opisni meta-podaci koji se koriste za prevođenje drugih ulaznih podataka. Ulazi i izlazi apstrakcionog sloja ilustrovani su na slici 23.



Slika 23 Ulazni i izlazni podaci apstrakcionog sloja

U primeru ASCII koda, ako je izlaz prvog sloja apstrakcije bio tekst fajl u HTML dokumentu, karakteri bi bili ulazni podaci u HTML sloj apstrakcije, koji uzima ASCII podatke i HTML specifikaciju kao ulazne podatke i daje na izlazu formatirani HTML dokument. HTML pretraživač je tipičan primer alata koji prevodi prethodni ASCII sloj u HTML.

Primer opisnih meta podataka kao ulaznih veličina je blok pokazivača (*pointers*) i polja kucanja (*type fields*) u, na primer, *inode* strukturu UNIX fajl sistema. *Inode* struktura opisuje fajl i uključuje deskriptor koji indicira da li je *inode* za neki fajl, direktorijum ili neki drugi specijalni tip. Drugo *inode* polje je direktni blok pokazivač koji sadrži neku adresu na kojoj je sadržaj fajla memorisan. Obe vrednosti koriste se kao deskriptivni podaci kada se procesira sledeći sloj apstrakcije u fajl sistemu. Adresa se koristi za identifikaciju mesta na kojem treba čitati podatke u fajl sistemu, a vrednost otkucaja tastature (*type value*) koristi se za identifikaciju načina procesiranja podataka fajla, pošto se direktorijum procesira različito od fajla. U ovom slučaju, izlaz *inode* nije jedini ulaz u sledeći sloj, zato što ceo imidž fajl sistema treba da locira adresu bloka. Slojevi apstrakcije događaju se na mnogim nivoima. Sam fajl sistem je sloj apstrakcije za niz bajtova sa diska. Unutar fajl sistema se nalaze dodatni slojevi apstrakcije, a krajnji rezultat je manji niz bajtova u ulazu (*entry*) MFT koji predstavljaju fajl. Podaci fajla se zatim primenjuju na aplikativni sloj apstrakcije gde se dalje procesiraju.

7.4.1 Greške u slojevima apstrakcije

Svaki sloj apstrakcije može uneti greške i zbog toga je margina greške izlazna vrednost svakog sloja apstrakcije. Sveobuhvatna lista grešaka koje se mogu uneti u procesu forenzičke istrage, još uvek nije kompletirana. Definisane su greške koje unose forenzički alati za analizu i proces krišćenja slojeva apstrakcije. Nisu obuhvaćene greške nastale zbog prikrivanja traga napadača, greške alata za uzimanje imidža kompromitovanog HD, ili pogrešne interpretacije rezultata analize. Apstrakcioni slojevi mogu uneti dva tipa grešaka, [2]:

12. greška implementacije forenzičkog alata i
13. greška sloja apstrakcije.

Greška implementacije forenzičkog alata unosi se zbog programskih i dizajnerskih bagova forenzičkog alata, kao što su programerske greške, nekorektna specifikacija alata, ili korektna specifikacija alata, ali nekorektna specifikacija originalne aplikacije. Ovaj tip grešaka najteže je proračunati, jer zahteva brojna testiranja i revizije programskih kôdova. Kada se specifični bag forenzičkog alata jednom detektuje, isti se fiksira i izdaje se nova verzija alata. Redukciju grešaka digitalnih forenzičkih alata vrše malobrojni timovi u svetu (npr., NIST *Computer Forensics Tool Testing Group*). Da bi se smanjio rizik od ovog tipa greške, svaki alat mora imati marginu greške implementacije alata, proračunatu na bazi istorije bagova alata - broja bagova u poslednjim godinama i ozbiljnosti posledica. U proračunu ovog tipa greške teškoće nastaju kod zatvorenog izvornog kôda aplikacije, gde se bagovi ne objavljuju i fiksiraju se u tajnosti, pa te greške nije moguće uzeti u obzir.

Greška sloja apstrakcije unosi se zbog simplifikacije koja se koristi za generisanje sloja apstrakcije. Ovaj tip grešaka dešava se kada sloj apstrakcije nije deo originalnog dizajna. Na primer, *imidž* fajl sistema ima nekoliko slojeva apstrakcije u svom dizajnu. Kretanje sa jednog sloja apstrakcije na drugi unosi ovu grešku. Greška sloja apstrakcije postoji u IDS sistemu koji reducira višestruke mrežne pakete u specifični napad. Pošto IDS ne zna sa 100% sigurnosti da su paketi deo napada, proizvode neku marginu greške. Vrednost greške koju unosi IDS može biti različit za različite tipove napada, a vrednost greške može se smanjiti sa boljim tehnikama apstrakcije. Generalno problem grešaka koje unose slojevi apstrakcije rezultat je zbirnih grešaka koje unosi svaki sloj apstrakcije. Problem se rešava proračunom margine greške za svaki sloj i uračunavanjem ove greške u analizi rezultirajućih podataka. Da bi se ublažio rizik koji prati ovu grešku potrebno je imati pristup ulazima u sloj apstrakcije, skupu pravila i izlaznim vrednostima za verifikaciju translacije podataka.

7.4.2 Karakteristike slojeva apstrakcije

Slojevi apstrakcije i alati za njihovo procesiranje mogu se opisati kroz četiri osnovne karakteristike. Greška apstrakcije može se iskoristiti za opisivanje nekog sloja apstrakcije kao *sloj sa gubicima* i *sloj bez gubitaka*. Sloj sa gubicima je onaj sa marginom greške apstrakcije većom od nule, a sloj bez gubitaka ima nultu marginu greške apstrakcije. U ovu definiciju nije uključena greška implementacije alata, zato što je to specifična vrednost alata, a ne sloja apstrakcije. Primeri slojeva apstrakcije bez gubitaka su slojevi apstrakcije fajl sistema i ASCII kôda, dok su primeri slojeva apstrakcije sa gubicima IDS alarmi.

Sloj apstrakcije može se opisati sa svojim atributima mapiranja. *Jedan-prema-jedan* sloj ima jedinično mapiranje, tako da postoji korelacija jedan-prema-jedan između svakog ulaza i svakog izlaza. U ovu kategoriju spadaju mnogi slojevi fajl sistema i ASCII kôd. Ulazi ovih slojeva mogu se odrediti iz izlaza i skupa pravila. *Više-prema-jedan* sloj ima ne-jdinično

mapiranje, gde se neka izlana vrednost može generisati sa više ulaznih vrednosti. Primer je MD5 jednosmerna, heš funkcija. Dve ulazne vrednosti mogu generisati istu vrednost MD5 čeksume, iako je teško pronaći te vrednosti. Drugi primer više-prema-jedan sloja apstrakcije su IDS alarmi. Generalno niko ne može regenerisati pakete koji su generisali neki IDS alarmi, koristeći samo jedan alarm.

Mogu postojati slojevi apstrakcije unutar sloja apstrakcije na višem nivou apstrakcije. U slučaju čvrstog diska za skladištenje, postoje najmanje tri sloja apstrakcije na visokom nivou. Prvi je sloj medijuma koji prevodi jedinstveni format diska u generalni format sektora LBA i CHS adresiranja koje obezbeđuje hardverski interfejs. Drugi sloj je fajl sistem koji prevodi sadržaj sektora u fajlove. Treći sloj apstrakcije je aplikativni sloj koji prevodi sadržaj fajlova u zahtevani format aplikacije - tekst, slika, grafika.

Poslednji sloj u nivou apstrakcije zove se *granični sloj*. Izlaz iz ovog sloja ne koristi se kao ulaz u bilo koji drugi sloj na tom nivou. Na primer, sirovi sadržaj nekog fajla je granični sloj u fajl sistemu. Prevođenje u ASCII i HTML vrši se na sloju aplikativnog nivoa. Nivoi i slojevi apstrakcije HTML dokumenta prikazani su na slici 24.

Disk		Fajl sisem			Aplikacija
Glave	...	Boot sektor	FAT oblast	Oblast podataka	ASCII
LBA Sektori			...	...	HTML
		Fajl			

Slika 24. Slojevi apstrakcije HTML dokumenta

Digitalni forenzički alati za svaki sloj apstrakcije takođe se mogu svrstati u različite kategorije. *Translacioni alati* za prevođenje sa jednog sloja apstrakcije na drugi, koriste skup pravila translacije i ulazne podatke za generisanje izlaznih podataka. Namena ovih alata je da prevede podatke na sledeći sloj apstrakcije. *Prezentacioni alati* su oni koji uzimaju podatke sa izlaza translacionih alata i prikazuju ih na displeju na način koji je pogodan za forenzičara. Sa aspekta forenzičara, ova dva tipa alata ne treba razdvajati i u većini slučajeva nisu razdvojeni u savremenim alatima (*FTK*, *EnCase*, *iLook* itd.). Slojevi koji proizvode veliku količinu izlaznih podataka mogu ih razdvojiti radi efikasnosti. Na primer, neki translacioni alat može analizirati *imidž* nekog fajl sistema i prikazati fajlove i listinge direktorijuma po redosledu u kojem postoje u *imidžu*. Neki prezentacioni alat može uzeti te podatke i sortirati ih po direktorijumu da prikaže samo fajlove u datom direktorijumu. Drugi prezentacioni alat može sortirati MTF ulaze (*entries*) prema MAC vremenima - *Modifikacije*, *Pristupa* i *Izmene* svakog fajla u datom direktorijumu i prikazati vremensku liniju aktivnosti analiziranog fajla. Isti podaci postoje u svakom rezultatu, ali u formatu koji zadovoljava različite potrebe.

7.5 Zahtevi za alate za digitalnu forenzičku analizu

Na bazi navedenih definicija i ciljeva mogu se generisati sledeći zahtevi za digitalne forenzičke alate:

14. *Korisnost*: Za rešavanje problema kompleksnosti i težine analize podataka u najnižim formatima, alati moraju obezbediti podatke na sloju apstrakcije i u formatu koji pomažu forenzičaru. Minimalno forenzičar mora imati pristup graničnim slojevima apstrakcije.
15. *Sveobuhvatnost*: Da bi identifikovali optužujuće i oslobađajuće dokaze, forenzičari moraju imati pristup svim izlaznim podacima na datom sloju apstrakcije.
16. *Tačnost*: Za rešavanje problema greške koju slojevi apstrakcije unose u izlazni rezultat, alati moraju obezbediti tačnost izlaznih podataka, a da se margina greške može odrediti tako da se rezultati mogu na odgovarajući način interpretirati.
17. *Određenost*: Da bi se obezbedila tačnost alata, alat mora uvek proizvesti istu izlaznu vrednost kada se primene iste ulazna vrednost i skup pravila translacije.
18. *Proverljivost*: Da bi potvrdio tačnost alata, forenzičar treba da obezbedi verifikaciju dobijenih rezultata. Ova se verifikacija može izvršiti manuelno, ili koristeći drugi i nezavisan skup alata. Zbog toga forenzičar mora imati pristup ulaznim i izlaznim veličinama svakog sloja apstrakcije, tako da se izlaz može verifikovati.

Zaštita od upisivanja (read only): Iako nije neophodna karakteristika, ovaj atribut alata visoko se preporučuje, pošto priroda digitalnih medija dopušta lako uzimanje tačne kopije podataka, kopije se mogu napraviti pre upotrebe alata koji modifikuju original. Za verifikaciju integriteta rezultata, što sud može zahtevati, potrebno je obezbediti kopiju ulaznog originala podataka.

7.6 Apstrakcioni slojevi FAT fajl sistema

FAT 16 (*File Allocation Table*) fajl sistem, jedan od osnovnih fajl sistema, još uvek je u upotrebi u brojnim računarima. FAT fajl sistem je model realnog zapisivanja podataka na fizičkom čvrstom disku i sastoji se iz tri glavne oblasti:

19. *But sektor* koji sadrži adrese i veličine struktura u ovom specifičnom fajl sistemu, uključujući i lokaciju FAT (*File Allocation Table*) i oblasti podataka;
20. *FAT (File Allocation Table)* koja sadrži ulaze (*entries*) klastera i specificira koji je sledeći alocirani klaster, a koji je nealocirani klaster;
21. *Oblast podataka* koja je podeljena na konsekutivne sektore od po 512 bajta, svrstane u klaster od po 2, 4, 8, 16 sektora, zavisno od veličine logičkog diska. Klasteri skladište sadržaj fajla, ili direktorijuma. Svaki klaster ima svoj ulaz (*entry*) u FAT tabeli.

Fajlovi su opisani sa strukturom *entrija*, koja je uskladištena u klasterima alociranim u glavnom (*parent*) direktorijumu. Ova struktura sadrži ime fajla, vremena, veličinu i početni klaster. Preostali klasteri u fajlu, ako ih ima, nalaze se korišćenjem FAT tabele.

FAT 32 fajl sistem ima sedam slojeva apstrakcije.

1. *sloj apstrakcije* koristi kao ulazne podatke upravo sliku particija fizičkog diska, pretpostavljajući da je akvizicija sirove particije diska izvršena pomoću alata kao što je **UNIX DD** komandna linija. Ovaj sloj koristi definisanu strukturu *but* sektora iz kojeg ekstrahuje vrednosti veličine i lokacije. Primeri ekstrahovanih vrednosti uključuju, [1]:

22. startnu lokaciju FAT tabele,
23. veličinu svake FAT tabele,
24. broj FAT tabela,

25. broj sektora po klasteru,
26. lokaciju rut direktorijuma.

2. *sloj apstrakcije* uzima imidž i informaciju o FAT tabeli kao ulazne podatke i daje FAT i oblast podataka na izlazu. Izlazni podaci iz ovog sloja su sirovi podaci iz *imidža* i nisu strukturirani.

3. i 4. *sloj apstrakcije* daju strukturu FAT tabeli i oblasti podataka, koji su identifikovani u prethodnim slojevima apstrakcije. Jedan sloj uzima FAT oblast i veličinu ulaza FAT tabele kao ulazne podatke, a obezbeđuje *entrije* tabele kao izlazne podatke. Drugi sloj uzima oblast podataka i veličinu klastera kao ulazne podatke i obezbeđuju klastera kao izlazne podatke. Sadržaj fajlova i direktorijuma uskladišten je u klasterima u oblasti podataka.

5. *sloj apstrakcije* na nivou fajl sistema uzima klastera i vrednost tipa fajla kao ulazne podatke. Ako tip određuje neki fajl, onda je sirovi sadržaj klastera dat kao izlazni podatak. Ako se tip odnosi na direktorijum, onda je lista *entrija* direktorijuma izlazni podatak. Ako je dat sirov sadržaj, tada je to granični sloj, zato što ne postoji ništa drugo što se može procesirati slojevima apstrakcije fajl sistema. Podaci se prenose na aplikativni nivo. Ako su u prethodnom sloju dati *entriji* direktorijuma, to je parcijalni opis nekog fajla ili direktorijuma, pošto imamo samo prvi klaster u fajlu, a ne i ostale klastera.

6. *sloj* uzima startni klaster i FAT kao ulazne podatke i generiše punu listu alociranih klastera kao izlazne podatke.

7. *sloj* uzima klastera, *entrije* direktorijuma i punu listu klastera kao ulazne podatke, a generiše bilo ceo sadržaj fajlova, ili listing direktorijuma. Ovaj sloj koristi prethodno opisani peti sloj apstrakcije, pa je ovaj sloj granični, ako je dat sadržaj fajla. Ovi slojevi apstrakcije u FAT fajl sistemu prikazani su u tabeli 7.

Tabela 7 Slojevi apstrakcije FAT fajl sistemu

	Input	Output
1	File System Image	Boot Sector Values
2	FAT information from SB	FAT and Data Area
3	FAT Area, FAT Entry Size	FAT Entries
4	Data Area, Cluster Size	Clusters
5	Cluster, Type	Directory Entries or Raw Content
6	Starting Cluster, FAT Entries	List of Allocated Clusters
7	All file meta-data, Clusters	All Directory Entries or Raw Content

Alati za digitalnu forenzičku analizu, dizajnirani za FAT fajl sistem sa navedenim zahtevima, obezbeđuju forenzičaru ulazne i izlazne podatke za svaki od sedam slojeva apstrakcije i mogu predstaviti izlaz svakog sloja u jednom, ili više formata.

Alat za digitalnu forenzičku analizu, koji obezbeđuje listing sadržaja rut direktorijuma u **FAT 32** fajl sistemu, treba da na *imidžu* fajl sistema uradi sledeće:

1. procesira sloj apstrakcije 1 da identifikuje *but* sektor, uključujući lokaciju rut direktorijuma,
2. procesira sloj apstrakcije 2 da identifikuje FAT tabelu i oblast podataka,
3. procesira sloj apstrakcije 3 da dobije *entrije* u FAT tabeli,
4. procesira sloj apstrakcije 4 da dobije klastera za direktorijum,
5. koristi lokaciju rut direktorijuma da procesira sloj 6 za identifikaciju svih alociranih klastera i
6. procesira sloj apstrakcije 7 da dobije listing svih imena u direktorijumu. Alat za formatiranje u ovom slučaju može prikazati ili sve detalje o fajlu, ili samo imena fajlova.

Alat koji ima pristup izlazima u svakom od navedenih koraka, obezbeđuje laku verifikaciju rezultata.

Postojanje slojeva apstrakcije sa greškom povećava se sa povećanjem broja logova, mrežnih paketa i vremenskih linija aktivnosti fajla za analizu. Apstrakcioni slojevi se koriste za redukciju broja *entrija* logova za analizu, grupisanjem istih u događaje na višem nivou apstrakcije. Ovo unosi greške u konačni rezultat i zbog toga se mora potpuno razumeti i dokumentovati.

Sa aspekta apstrakcionih slojeva, *kompjuterska forenzika* je analiza ostataka kompjuterskog incidenta oštećenog, ili korumpiranog računara, pomoću skupa tehnika koje su analogne patološkom ispitivanju leša ubijenog, a vrši se za pravosudne potrebe radi otkrivanja dokaza u slučajevima krivičnog dela kompjuterskog kriminala, povrede korporacijske politike zaštite informacija i prikupljanja obaveštajnih podataka putem IKT sistema. Kompjuterska forenzika, sa aspekta apstrakcionih slojeva, obuhvata analizu sledećih glavnih apstrakcionih slojeva računarskog sistema:

Analiza fizičkih medija, sloja koji prevodi digitalne podatke za uobičajeno skladištenje u računaru, preko korisničkog interfejsa. Primeri su IDE, SCSI HD u kojima su *bajtovi* granični sloj, kompakt fleš memorija, memorijski čip. Analiza ovog sloja uključuje procesiranje standardnih slojeva računara i oporavak izbrisanih podataka.

Analiza menadžmenta medija, odnosi se na sloj apstrakcije koji organizuje medijume za skladištenje. Granični sloj je druga kolekcija bajtova sa medijuma. Primeri ovog sloja uključuju deljenje HD u particije, organizovanje multiplikativnih RAID diskova u logičke diskove i integrisanje multiplikativnih memorijskih čipova u memorijski prostor. Ovaj sloj možda ne postoji u svim tipovima medijuma, na primer, baza podataka može pristupiti celom HD bez kreiranja particija.

Analiza sistema fajlova, odnosi se na sloj apstrakcije koji prevodi bajtove i sektore iz particija HD u direktorijume i fajlove. Granični sloj je sadržaj fajlova. Analiza u ovom sloju uključuje posmatranje direktorijuma i sadržaja fajlova i oporavljenih izbrisanih fajlova.

Analiza aplikativnog sloja apstrakcije, koji prevodi podatke, tipično uzete iz sistema fajlova u korisnički iskoristive dokazne podatke (na primer, štampani materijal teksta, dijagrama i sl.).

8 Forenzički alati

8.1 Opšte karakteristike

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 sistema, [25].

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 konformnije 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 treba evaluirati karakteristike potencijalnih alata:

- 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.

8.1.1 Tehnike i alati za akviziciju digitalnih podataka

Akvizicija digitalnih podataka prvi je zadatak u forenzičkoj istrazi računara i podrazumeva pravljenje fizičke kopije bit-po-bit originalnog (osumnjičenog, ispitivanog) diska računara.

Ova procedura sprečava korupciju i oštećenje digitalnih podataka na originalnom disku. Akvizicija digitalnih podataka obuhvata sledeće funkcije:

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

Za akviziciju podataka bit-po-bit sa originalnog na forenzički disk postoje hardverski i softverski forenzički alati. Primeri hardverskih alata za uzimanje fizičke slike računara su: *Image MaSSter Solo 2 Forensic* komponenta sa *firmware* programom (*Intelligence Computer Solutions Inc.*) koji može samostalno kopirati podatke sa originalnog na forenzički disk. 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:

1. fizičko kopiranje celog fizičkog diska i
2. 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 proizvođače. 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 *HexWorkshop* ili *WinHex*. Heksadecimalni editori, poznatiji kao diskeditori, kao što je *Northon DiskEdit*, obezbeđuju čitanje podataka u heksadecimalnom zapisu i otvorenom tekstu. (slika 25)



Slika 25 Primer prozora heksadecimalnog zapisa u WinHex alatu Northon Commander

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

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

Neki savremeni forenzički alati mogu izvršiti akviziciju podataka na daljinu, preko računarske mreže. Svi savremeni forenzički alati obezbeđuju metod za verifikaciju tačnosti procesa kopiranja podataka sa originalnog na forenzički disk. Na primer, *EnCase* alat zahteva od forenzičara da uzme MD5 ili SHA1 heš vrednost podataka sakupljenih u procesu akvizicije, dok *SafeBack* uzima SHA 256 heš vrednost, a hardverski alat *Image MaSStar Solo* uzima CRC 32 vrednost.

8.1.2 Validacija i diskriminacija podataka

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

1. heširanje,
2. filtracija i
3. analiza hедера fajlova.

Proces validacije obezbeđuje integritet kopiranih podataka i omogućava njihovu diskriminaciju na dokazujuće i nedokazujuće podatke. Validacija podataka obezbeđuje se uzimanjem heš (sažetka) vrednosti nekim od raspoloživih algoritama, kao što su CRC 32, MD5, SHA 1, SHA 256, SHA 384 ili SHA 512. Ova funkcija uzimanja heš vrednosti kopiranih imidž podataka standardna je karakteristika gotovo svih savremenih forenzičkih alata. Preporučuje se uzimanje heš vrednosti celog diska, kao i svakog fajla na disku. Takve heš vrednosti su jedinstvene vrednosti podataka, kao otisak prsta za čoveka i obezbeđuju integritet podataka od prvog uzimanja heš vrednosti.

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

1. Nekoliko softverskih forenzičkih alata mogu integrisati skup heš vrednosti poznatih fajlova. Ovi alati upoređuju poznate fajlove sa istim na osumnjičenom disku i ako se ne poklapaju upozoravaju forenzičara da je fajl sumnjiv. Na ovaj način alat može značajno smanjiti količinu podataka za analizu i izvlačenje dokaza.

2. Drugi metod za diskriminaciju podataka je analiza i verifikacija informacija iz hедера svih tipova poznatih fajlova. Na primer oznaka JFIF ugrađena je ispred svih JPEG fajlova.
3. Treća grupa alata omogućava dodavanje jedinstvenih vrednosti podataka hедера u bazu podataka alata, što poboljšava funkciju diskriminacije u fazi analize. Pretraživanjem i upoređivanjem hедера alat može locirati fajlove koji mogu biti namerno izmenjeni. Ova funkcija može se koristiti za lociranje skrivenih fajlova.

8.1.3 Ekstrakcija digitalnih podataka

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

1. opservacija podataka,
2. pretraživanje sa ključnom reči,
3. dekompresija podataka iz fragmenata izbrisanog fajla,
4. dešifrovanje šifrovanih fajlova podataka i
5. označavanje (markiranje) digitalnih dokaza.

Opservacija podataka: Većina forenzičkih alata obezbeđuje funkciju posmatranja podataka, a kako se i u kojem formatu podaci vide, zavisi od alata. *Drive Spy (DII- Digital Intelligence Inc.)*, na primer, obezbeđuje gledanje logičke particije osumnjičenog diska i heksadecimalnog zapisa podataka u klasterima i sektorima diska. Alati kao što su *FTK*, *EnCase*, *Smart iLook*, *ProDiscover* i dr. nude nekoliko različitih načina posmatranja podataka, uključujući posmatranje logičke strukture fajlova i foldera (direktorijuma) na disku. Ovi alati, takođe, pokazuju alocirane (dodeljene) klastere sa podacima fajlova i nealocirane (nedodeljene) oblasti diska. Posmatranje podataka u njihovom normalnom (prirodnom) formatu, znatno olakšava analizu i donošenje zaključaka relevantnih za istragu. *Pretraživanje po ključnoj reči* uobičajeni je zadatak u ispitivanju računara. Ovim se oporavljaju ključni podaci. Ključnu reč u istrazi određuje forenzičar na bazi raspoloživih podataka o karakteru krivičnog dela kompjuterskog kriminala. Standardni pretraživači na bazi ključne reči obično generišu suviše informacija, pa je potrebno ispitati da li forenzički alat dopušta kombinaciju ključnih reči, što znatno skraćuje vreme pretraživanja. Takođe, treba ispitati da li su alati selektivni u izboru tipa pretraživanih podataka, na primer, samo za e-mail poruke. Neki forenzički alati vrše indeksiranje svih reči na disku. Ovo obezbeđuje *FTK* alat koristeći binarno indeksiranje (tzv. *b-stablo*) sa *dtSearch* funkcijom, koja obezbeđuje trenutno pronalaženje ključne reči i znatno ubrzava proces analize.

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

Rekonstrukcija fragmenata fajlova pobrisanih sa osumnjičenog diska (USA, *carving*; eng. *salvaging*) značajan je deo procesa forenzičke istrage. Ekstrakcija podataka iz nealociranih prostora diska postala je uobičajen zadatak za forenzičara. Lociranje informacija hедера fajla deo je ovog procesa. Većina alata analizira nealocirane prostore diska ili imidža diska, locirajući fragmente, ili cele strukture fajlova koje se mogu rekonstruisati i kopirati u novi fajl. *Drive Spy* alat može locirati podatke, ali zahteva mnogo manuelnog rada i metoda za

kopiranje klastera u novi fajl. Napredniji alati, kao što su *EnCase*, *FTK*, *ProDiscover*, *iLook* i drugi GUI tipa alati, imaju ugrađene funkcije koje automatski rekonstruišu fragmentirane podatke. *Data Lifter* i *Davory* alati specifično su dizajnirani da rekonstruišu fajlove poznatih podataka iz eksportovanog nealociranog prostora diska. *Data Lifter* ima interaktivne funkcije koje omogućavaju da forenzičar doda druge jedinstvene vrednosti podataka hedera u bazu alata.

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

Označavanje digitalnih dokaza vrši se posle lociranja podataka – glavnog zadatka u ispitivanju računara. Cilj označavanja podataka je da se forenzičar može po potrebi pozvati na označene podatke. Većina forenzičkih alata koriste funkciju označavanja digitalnih podataka za ubacivanje liste u generator za izveštavanje, koji proizvodi tehnički izveštaj o nalazima ispitivanja računara. Primer jednostavnog generatora za izveštavanje je log fajl kojeg kreira *Drive Spy* alat. Pošto je ovo alat komandne linije šel tipa, on može memorisati ključne reči za pretraživanje sa ekrana, ali ako se koristi Output komanda *Drive Spy* kopira izlaz ekrana generisan funkcijom traženja ključne reči u log fajl. Za posmatranje i analizu rezultata pretraživanja po ključnoj reči, treba ih izvući iz *Drive Spy* alata i otvoriti log fajl editorom teksta. Forenzički alati GUI tipa, kao što su *FTK*, *iLook*, *ProDiscover* ili *EnCase* imaju opciju označavanja digitalnih dokaza koje forenzičar identifikuje. Kada se podigne generator za izveštavanje u *FTK* ili *EnCase* alatu, identifikatori (oznake) digitalnih dokaza se unose u izveštaj. *FTK* i *iLook* generišu izveštaj u HTML formatu koji se može čitati u bilo kojem web pretraživaču. *EnCase* generiše izveštaj u RTF formatu dokumenta i može se čitati u većini *word* procesora.

8.1.4 Rekonstrukcija osumnjičenog diska

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

- kopiranje sa diska na disk,
- kopiranje sa fizičkog imidža na disk,

- kopiranje particije na particiju i
- kopiranje imidža particije na particiju.

Postoji nekoliko načina za rekonstrukciju forenzičke bit-po-bit kopije osumnjičenog diska. Pod idealnim uslovima najbolji metod forenzičkog dupliranja diska je obezbeđivanje HD istog modela i proizvođača kao što je originalni osumnjičeni HD. Ako je osumnjičeni HD novije generacije, nije teško pronaći isti tip, ali za starije proizvode to nije uvek moguće.

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

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

Hardverski duplikatori:

- Logicube Forensic SF-5000,
 - Logicube Forensic MD5,
 - Image MaSStar Solo 2 Forensic HD Duplicator.
- b. Softverski duplikatori:
- SafeBack,
 - SnapCopy.

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

- SafeBack,
- Snap Back i
- EnCase.

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

8.1.5 Izveštavanje o digitalnim dokazima

Da bi se proces forenzičke analize i ispitivanja diska kompletirao, potrebno je generisati izveštaj o ispitivanju. Pre pojave forenzičkih alata koji rade na Windows OS, ovaj izveštaj je zahtevao kopiranje podataka sa osumnjičenog diska i manuelnu ekstrakciju dokaza. Posle

ekstrakcije dokaza, forenzičar ih kopira u poseban program kao što je neki Word procesor, da bi se generisao izveštaj. Problem je bio sa ubacivanjem podataka koji se ne mogu čitati u Word procesoru, kao što su baze podataka, grafički prikazi i dr., što je forenzičar morao odštampati i prilagoditi uz izveštaj.

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

1. log izveštaj i
2. generator za izveštavanje.

Kao deo procesa validacije, potrebno je dokumentovati korake preduzete za dobijanje podataka sa osumnjičenog diska. Većina forenzičkih alata može generisati izveštaj o aktivnosti, poznat kao *log izveštaj*, koji se može dodati konačnom izveštaju forenzičara kao dodatni dokument o tome koji su koraci preduzeti u toku ispitivanja. Ovi podaci mogu biti korisni ako se zahteva ponavljanje ispitivanja. Za slučaj koji zahteva direktan uvid, log izveštaj potvrđuje koje aktivnosti su izvršene, a koji rezultati su dobijeni iz originalne analize i ispitivanja računara. Sledeći alati su samo neki od onih koji obezbeđuju log izveštaje: *FTK, iLook, X-Ways Forensic, Drve Spy*.

8.2 Hardverski forenzički alati

Tehnologije IK sistema brzo se menjaju, pa izbor hardvera utiče na izbor softverskih forenzičkih alata. Većinu komponenti savremenih računara proizvođači isporučuju sa srednjim vremenom otkaza od oko 18 meseci. Kako se forenzički hardverski alati, radne stanice i serveri koriste intenzivno, zamenu i znavljanje treba planirati najmanje svake 2 godine. Većina snabdevača računarskih sistema i komponenti nude širok asortiman forenzičkih radnih stanica, koje korisnik može prilagoditi svojim potrebama. Generalno, forenzičke radne stanice mogu se podeliti u sledeće tri kategorije:

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

Forenzičar treba znati da PC ima ograničenja u korišćenju broja perifernih jedinica. Što se dodaje više perifernih jedinica treba očekivati više problema, naročito kod starijih Windows 9x OS, pa je potrebno balansirati broj perifernih jedinica prema korišćenom OS. Digitalna forenzička laboratorija policijske agencije treba da ima što veći broj različitih forenzičkih alata, softvera i hardvera da bi izvršila sve potencijalne zadatke istrage kompjuterskog kriminala. Ako je moguće treba imati po nekoliko (2-3) konfiguracije PC za istovremeni rad na različitim slučajevima, zatim kompletirati repozitorijum softvera i hardvera sa svim prethodnim verzijama aktuelnih platformi.

Hardverska i softverska oprema u poslovnom okruženju namenjena za oporavak sistema i inicijalnu forenzičku istragu bezbednosnog kompjuterskog incidenta, može biti znatno skromnija i usklađena sa tipovima IKT sistema koji se koriste u poslovnom sistemu. Radnu stanicu za forenzičku akviziciju i analizu digitalnih podataka korisnici mogu izgraditi i u sopstvenom aranžmanu, s tim da treba postaviti granicu investicije za takav projekat.

Izgradnja forenzičke radne stanice nije toliko teška, koliko može brzo postati skupa, ako se dobro ne poznaju svi aspekti hardverskih i softverskih zahteva.

Problemi mogu nastati u podršci periferijskim uređajima, koji mogu doći u konflikt ili da ne rade i sl. Za sopstvenu gradnju forenzičke radne stanice treba obavezno obezbediti punu hardversku podršku. Zatim je potrebno identifikovati obim i tip podataka koje treba analizirati. Na primer, ako treba analizirati SPARC diskove iz računarske mreže poslovnog sistema, treba u radnu stanicu ugraditi SPARC diskove sa *blokatorom upisivanja*. U izgradnji sopstvene forenzičke radne stanice mogu se koristiti proizvodi specifičnih proizvođača od pojedinih komponenti do gotovih, kompletiranih radnih stanica, prema zahtevanoj konfiguraciji. Na primer, *F.R.E.D (DII)* kompletne radne stanice do jednostavne stanice za uzimanje imidža diskova tipa *FIRE IDE (DII)*.

Preporuke za nabavku/izgradnju forenzičke radne stanice korisno je razmotriti pre donošenja odluke. Odrediti gde će se vršiti akvizicija podataka, na primer, ako je to na terenu: obezbediti blokator upisivanja, preko Fire Wire i USB 2.0 - blokator tipa *Fire Chief (DII)* i Laptop računar. Za redukciju hardvera koji se nosi, može se koristiti *Wiebe Tech Forensic Drive Dock* sa regularnim *Drive Dock Fire Wire* mostom.

Kod izbora računara za stacionarnu ili prenosnu radnu stanicu, treba uzeti pun *tauer* koji omogućava proširenje, kao što su konvertori sa 2,5 inča na 3,5 inča za analizu Laptop HD na IDE HD zaštićene od upisivanja kontrolera. Treba uzeti što je moguće više memorije i što potpuniju kolekciju različitih veličina HD. Radnu stanicu treba opremiti sa 400W (ili većim) izvorom za napajanje sa UPS bekapom; kablom za podatke, SCSI drajv karticom, eksternim *Fire Wire* i USB portovima, ergonomičnom tastaturom i mišom, dobrom grafičkom kartom i najmanje 17-inčnim monitorom. Za profesionalno forenzičko ispitivanje preporučuje se video karta visokih performansi i veliki monitor.

Hardverski forenzički alati kreću se od jednostavnih jedno-namenskih komponenti do kompletnih forenzičkih računarskih sistema i servera. Jedno-namenske komponente mogu biti uređaji tipa *ACCARD AEC-7720WP Ultra Wide SCSI-to-IDE Bridge*, namenjen za sprečavanje upisivanja podataka na IDE HD, koji je kablom povezan na SCSI HD. Primer kompletnog računarskog sistema je *F.R.E.D* ili *DIBS Advance Forensic* radna stanica (*DII*). Brojni hardverski forenzički alati imaju implementiran odgovarajući program, tzv. *firmware*, programiran u samom alatu u EPROM memoriji i omogućavaju ažuriranje programa.

8.2.1 Blokatori upisivanja i drugi hardverski forenzički alati

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

Akvizicija digitalnih dokaza sa hardverskom tehnologijom uključuje, [38]:

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

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

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

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

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

Poznatiji proizvođači hardverskih i softverskih blokatora upisivanja su dostupni na brojnim web adresama.

Razlika između softverskih i hardverskih blokatora zapisivanja zavisi od definicije hardvera i softvera. Stvarno blokiranje upisivanja hardverom vrši se sa hardverskom komponentom, kako samo ime implicira, koja se ne može reprogramirati posle implementacije dizajna. Međutim, zbog kompleksnosti komunikacionih protokola (kao što su IEEE 1394-FireWire, USB2.9 itd.), često je nepraktično implementirati čiste hardverske blokatore upisivanja. Generalno, ono što se podrazumeva pod stvarnim hardverskim blokatorom zapisivanja, ustvari se vrši pomoću kombinacije jednog ili više mikroprocesora i hardverske logike u jednom kolu ili čipu. Ovi uređaji su programabilni i često reprogramabilni za proizvođača. Ovi programi nazivaju se *firmware*, relativno su mali i na njihovu funkciju ne utiče rad OS, pošto se standardni komunikacioni protokoli podešavaju nezavisno od bilo kojeg OS datog računara. Ovo je, sa aspekta forenzičara, osnovna prednost metoda hardverskih blokatora upisivanja u odnosu na softverske.

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

1. IDE čvrsti diskovi od 3,5 inča, klasični sa 40-pinskim IDE konektorom,
2. SATA čvrsti diskovi od 2,5 i 3,5 inča, koji postaje preovlađujući u svim desktop i većini *notebook* računarima,
3. *Notebook* čvrsti diskovi od 2,5 inča preovlađivali su u ovim računarima od početka proizvodnje do nedavno,

4. PCMCIA (PCCard) čvrsti diskovi, koji nisu šire prihvaćeni,
5. 1,8 inča *Toshiba* čvrsti diskovi, koji se često koriste u originalnom *iPod* uređaju,
6. 1,8 inča *Hitachi* čvrsti diskovi, koji se retko sreću u praksi,
7. Kompaktni fleš i mikrodiskovi, koji se preovlađujuće koriste u digitalnim kamerama i u nekim iPod uređajima,
8. SCSI čvrsti diskovi, koji se preovlađujuće koriste specijalno u starijim *Machintosh* i računarima sa visokim performansama,
9. Optički kanali (*Fiber Chanel*),
10. ZIF kablovski diskovi koji se koriste u video iPods i postaju preovlađujući u upotrebi.

Tipični hardverski blokatori izgledaju kao na slici 26.



Slika 26. Tipovi hardverskih blokatora

Poređenje IDE i SATA diskova prikazano je na slici 27. Dva SATA diska od 2,5 inča iznad jednog IDE diska od 3,5 inča. IDE diskovi koriste trakasti kabl, a SATA diskovi koriste fleksibilne kablove slične telefonskom kablju.



Slika 27. Primeri IDE i SATA diskova

Komplet blokatora upisivanja i adaptera za sakupljanje podataka sa klasičnih **3,5 inča IDE** diskova (slika 28) obuhvata forenzički **ComboDock** koji se priključuje na klasični 3,5 inča IDE čvrste diskove, ima **FireWire+USB** host pristup i paralelnu 40-pinsku IDE konekciju, a obezbeđuje blokirano upisivanje i brojne forenzičke karakteristike.



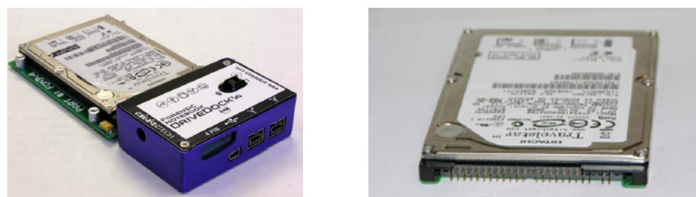
Slika 28 Sakupljanje podataka sa klasičnih 3,5 inča IDE diskova

Komplet blokatora upisivanja i adaptera za sakupljanje podatke sa **3,5 inča SATA** čvrstih diskova obuhvata (slika 29) forenzički **SATADock** koji se priključuje se na 3,5 inča SATA čvrsti disk, FireWire +USB pristup host računaru i SATA konektor i obezbeđuje blokirano upisivanje i brojne forenzičke karakteristike.



Slika 29 Sakupljanje podataka sa klasičnih 3,5 inča SATA diskova

Komplet blokatora upisivanja i adaptera za sakupljanje podataka sa 2,5 inča *notebook* čvrstih diskova obuhvata (slika 30) **Forensic Notebook DriveDock**, priključuje se na 2,5 inčna čvrste diskove i *FireWire* +USB pritupe host računaru, a obezbeđuje blokirano upisivanje i brojne forenzičke karakteristike.



Slika 30 Sakupljanje podataka sa notebook diskova od 2,5 inča

Komplet blokatora upisivanja i adapteri za sakupljanje podataka sa malih čvrstih diskova obuhvata, (slika 31a) PCCard (PCMCIA), kompakt fleš/mikrodiskove, 1,8 inča *Toshiba* diskove, SATA adaptere, 2,5 inča *notebook*, 1,8 inča ZIF Hitachi, a svi se spajaju na forenzički *ComboDock*.



Slika 31 Sakupljanje podataka sa malih čvrstih diskova

Komplet blokatora upisivanja i adaptera za 1,8 inča *Toshiba* koji se uobičajeno koriste u starijim *iPods*, spajaju se forenzičkim *ComboDock*-om, (slika 31b). Blokatori upisivanja sa 2,5 inča *Notebook* adapterom za 2,5 inča čvrste diskove koji se uobičajeno koriste u starijim *Notebook* računarima. Takođe rade sa paralelno spojenim 1,8 inča *Hitachi* diskovima. Spajaju se na forenzički *ComboDock*, (slika 31c). Blokatori upisivanja i 1-inčni adapter za akviziciju digitalnih podataka sa fleš memorija i mikrodiskova povezuju se paralelno na forenzički *ComboDock*, (slika 32a,b).



Slika 32 Sakupljanje podataka sa fleš memorije (a) mikrodiskova (b) i PCCard (PCMCIA) adapter(c)

PCCard (PCMCIA) adapter, relativno redak, povezuje se paralelno, polarizuje se kroz montažnu stranu šinskog slot. Nema polarizacije pinova na konektoru. Povezuje se na forenzički *ComboDock*, (slika 32c).

Blokatori upisivanja za akviziciju podataka sa SATA diskova koriste SATA adaptere koji se spajaju na bilo koji SATA čvrsti disk sa fizičkim ili logičkim particijama. Ima indikator pristupa i spaja se na forenzički *ComboDock*. (slika 33a).



Slika 33 SATA adapter za sakupljanje podataka sa SATA diskova (a) i SATA adapter priključen na SATA disk (b)

SATA adapter se priključuje na bilo koji SATA disk sa fizičkom ili logičkom particijom bilo koje veličine, (slika 33b).

Adapter 1,8 inča ZIF priključuje se na Hitachi ZIF diskove, ima ultra tanki kabl, debljine 0,2 ili 0,3 mm, koji se lako oštećuje. Preporučuje se obuka pre upotrebe. Uobičajeno se spaja na forenzički *ComboDock*, (slika 34.). 1,8 inča ZIF diskovi sa kablom su najvećeg kapaciteta za male *notebook* računare i većeg kapaciteta za iPod uređaje.



Slika 34 Adapter 1,8 inča ZIF za priključivanje Hitachi ZIF diskova

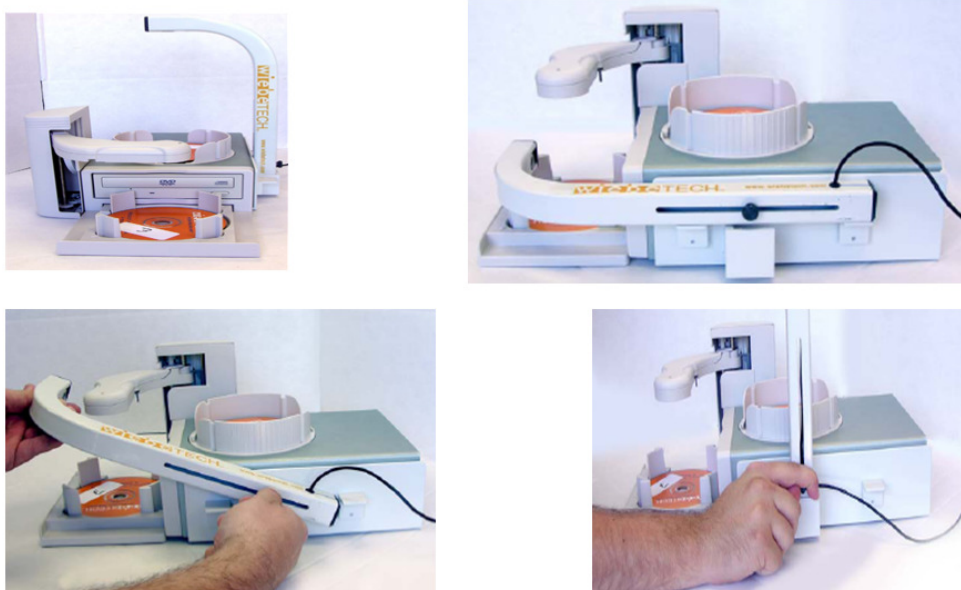
Akvizicija podataka sa CD/DVD diskova za razliku od čvrstih diskova može imati varijacije. Imidži kreirani sa optičkih diskova mogu neznatno varirati svaki put kada se imidž uzima, čak i kada se koriste isti disk i optički disk. Ovo je posledica brojnih faktora, kao što je prisustvo čestica prašine,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

1. izvrši akviziciju *imidža* fajlova sa diska koji se mogu čitati i analizirati softverskim forenzičkim alatima dizajniranim za tu namenu, tipa *FTK*, *Encase*, *iLook*, *xWay Forensic* itd;
2. obezbedi dokaz da originalni podaci na disku nisu izmenjeni u toku kopiranja, što se postiže korišćenjem forenzički poverljivog softvera za uzimanje *imidža* diska, što zadovoljava *CD/DVDImager*. Forenzički alati sa otvorenim izvornim kodom na bazi *Linux OS* za uzimanje *imidža* su *DD* i *CDRDAO*, koji su od velikog poverenja u forenzičkoj zajednici. Za neke diskove može biti potrebno da se Linux bazirani alati zamene. Forenzičar često mora da isproba nekoliko alata pre nego što uspešno napravi *imidž* neobičnog, ili problematičnog optičkog diska. *DD* i *CDRDAO* alati uspešni su za najveći broj optičkih diskova u upotrebi;

3. obezbedi dokaz da fajlovi sa *imidža* diska nisu izmenjeni posle inicijalnog kreiranja, što se obezbeđuje kreiranjem heš vrednosti uzetog imidža. Uzimanjem drugog heša imidža diska posle forenzičke analize, može se dokazati da imidž nije menjan u toku ispitivanja;
4. obezbedi upoređivanje *imidža* diska sa fizičkim dokazom. *CD/DVDImager* uzima sliku svakog diska i skladišti je sa *imidžom* diska. Heš vrednost fajla *imidža* takođe se generiše tako da forenzičar može kasnije potvrditi da slika nije bila izmenjena.

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

U bolje opremljenim forenzičkim laboratorijama koriste se roboti za akviziciju digitalnih podataka. *CD/DVD robot* sa USB konektorima za čitač i kameru ima ulazne i izlazne podizače, CD/DVD čitač, ručicu robota i kameru (slika 35).



Slika 35 CD/DVD robot

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

Uređaj *RP-PCIE-SCSI = Atto'sEPCI-5DRO-BR1 (a.k.a. EPCI-UL5D)* automatski blokira upisivanje svakog priključenog SCSI diska, za bezbedno izvlačenje podataka samo sa opcijom "čitanje". Koristi *Brzi Ultra SCSI* interfejs za podršku starijih SCSI proizvoda. Ima brzinu prenosa podataka do 320MB/sec po kanalu. Može da radi na dva nezavisna SCSI kanala. Posедуje *x4PCI Express* priključak na host računar. Koristi naprednu ADS (*Advanced Data Streaming*) tehnologiju i ima drajvere za podršku Windows i Linux OS. Podržava do 30 SCSI bus ID-s i može da radi preko kabla do 12 m dužine. Usaglašen je sa *RoHS*.

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

8.3 Softverski forenzički alati

Softverski forenzički alati grupišu se u dve osnovne kategorije:

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

Neki alati namenjeni su za izvršavanje jednog zadatka, kao što je *SafeBack* alat na bazi DOS komandne linije namenjen za akviziciju podataka sa diska. Primeri GUI tipa alata su *EnCase* i *FTK*, namenjeni za obavljanje više forenzičkih funkcija. Većina GUI alata tipično može izvršiti većinu zadataka akvizicije i analize digitalnih podataka u računarskom sistemu.

Značajan aspekt softverskih forenzičkih alata je sposobnost potpunog kopiranja, ili uzimanja fizičke slike bit-po-bit ili *imidža* (eng. *mirror; imaging*) osumnjičenog diska, ili drugog medijuma sa potencijalnim dokazima. Većina GUI alata mogu čitati i analizirati *imidž fajlove* i originalne diskove, kao što su najpoznatiji softverski forenzički alati *EnCase*, *FTK*, *X-Ways Forensic*, *iLook* i dr.

8.3.1 Forenzički alati komandne linije

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

Jedna od osnovnih prednosti alata komandne linije je što zahtevaju malo sistemskih resursa-većina zauzima jedan butabilni flopi disk i proizvodi izveštaj u tekst formatu.

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

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

- otvoriti Start, zatim Run i ukucati cmd za otvaranje šela komandne linije,
- ukucati cd\ koji vraća na rut direktorijum,
- ukucati dir/q>C:\Filowner.txt,

- koristiti bilo koji tekst editor za otvaranje C:\Filowner.txt i čitanje rezultata.

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

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

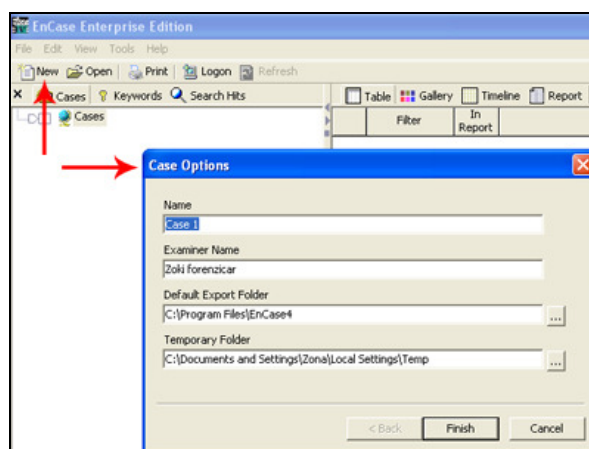
- zahtevaju velike računarske resurse (RAM memoriju),
- proizvode nekonzistenten rezultate zbog tipa korišćenog OS (npr., *Win XP Professional*, ili *Home Edition*),
- stvaraju zavisnost forenzičara od upotrebe samo jednog alata,
- u nekim situacijama ne rade pa se zahteva alat komandne linije u kompletu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

8.3.2 Softverski forenzički alat *EnCase v4* GUI tipa

EnCase je programski alat namanjen forenzičkoj istrazi digitalnih dokaza. Smatra se jednim od najboljih i najčešće korišćenih softverskih forenzičkih alata. *EnCase* program omogućava i olakšava forenzičaru istragu, akviziciju i analizu dokaznog materijala. *EnCase* ima kvalitetan GUI koji omogućava bolji i lakši pregled različitih fajlova kao što su izbrisani (*deleted*) fajlovi, *slack* i nealocirani prostori fajla. Ono što je svakako najvažnije za forenzičara, jeste da nema mogućnost izmene podataka sa *EnCase* alatom.

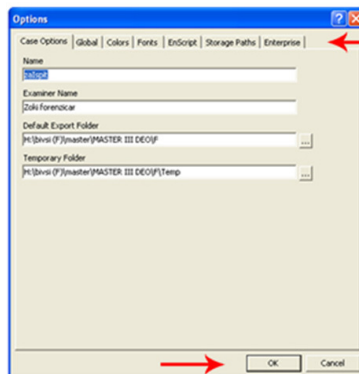
Interfejs: *EnCase v. 4* je mnogo urednija od svoje prethodne verzije 3, a najnovija verzija još je bolja. *EnCase* je organizovan po tabovima i postoji mogućnost prikazivanja većeg broja slučajeva, pri čemu je svaki slučaj organizovan u okviru svog foldera. Tabovi se mogu lako dodavati i uklanjati otvaranjem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

Navigacija: Aktiviranjem New u otvorenoj *EnCase* aplikaciji pojavljuje se dijalog za kreiranje novog slučaja (New Case). Unose se informacije kao što su ime slučaja, ime istraživača, folder za export i folder za privremene fajlove. Aktiviranjem opcije Finish kreiran je novi prazan slučaj (slika 36).



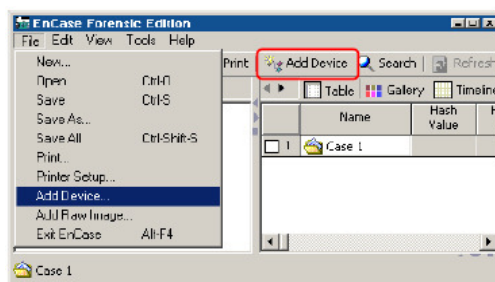
Slika 36 Otvaranje novog slučaja u *EnCase* alatu

Trebalo bi voditi računa o tzv. Case Management-u koji podrazumeva dodeljivanje imena slučajevima, ostavljanje prostora na disku za skladištenje dokaznog materijala, imenovanje foldera za privremene (*temporary*) fajlove i dr. Case Management je osnova forenzičke istrage dokaza. *EnCase* ima mogućnost otvaranja više slučajeva u isto vreme. Svaki će biti u zasebnom folderu sa jedinstvenim imenom i svaki će imati svoj Report View, Bookmark folder, Devices folder itd. Dijalog Options (slika 37) dobija se korišćenjem putanje Tools->Options sa linije menija. U okviru ovog dijaloga nalaze se opcije za podešavanje vremena, boje, fontova, *EnScript*-ova, *backup case* fajla *export* foldera, *temporary* foldera itd. Sve navedene opcije se jednom mogu podesiti i koristiti kao takve svaki sledeći put u radu sa *EnCase* alatom.



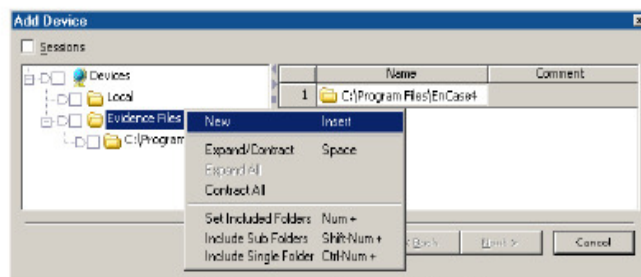
Slika 37 Otvaranje dijaloga Options u En Case alatu

Dodavanje dokaznog materijala novom slučaju vrši se na sledeći način: Selekcijom *Add Device* na fajl meniju ili otvaranjem opcije *Add Device* na top toolbar-u, (slika 38).



Slika 38 Dodavanje dokaznog materija novom slučaju u EnCase alatu

Otvaranjem opcije *Evidence Files* i selekovanjem *New* vrši se odabir fajlova sa određene lokacije. Pretraživanje lokacije se završava aktiviranjem *OK*, (slika 39).



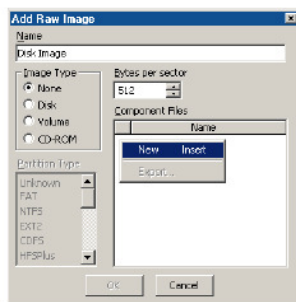
Slika 39 Odabir fajlova za pretraživanje

Novi folder se pojavljuje ispod foldera *Evidence Files*. Aktiviranjem prazne površine ispred fajlova u levom prozoru (koja postaje zelena) selektuju se svi fajlovi, a dostupni folderi i podfolderi se pojavljuju u desnom delu prozora. Selektovanjem (plava linija) željenog dokaznog materijala (*devices, volumes, floppy disk, removable media* itd.) sa desne strane vrši se odabir. Potrebno je nakon odabira aktivirati opciju *Next*. Neophodna je još jedna (finalna) potvrda za unos dokaznog materijala pre aktiviranja opcije *Finish*. Nakon što je izvršena potvrda, aktiviranjem *Finish* završava se proces dodavanja novog dokaznog materijala. Jedna od opcija koja se nalazi u okviru dijaloga *Add Devices* je opcija *Session*. Ona omogućava dodavanje dokaznog materijala koji je već pregledan, ili na bilo koji način izmenjen. *Verifikacija* započinje nakon što su fajlovi unešeni. *EnCase* verifikuje integritet fajlova. Zapocinjanje ovog procesa podrazumeva čitanje podataka i generisanje MD5 hash vrednosti, prikazivanje verifikacije i prikazivanje hash vrednosti u vidu izveštaja, (slika 40).



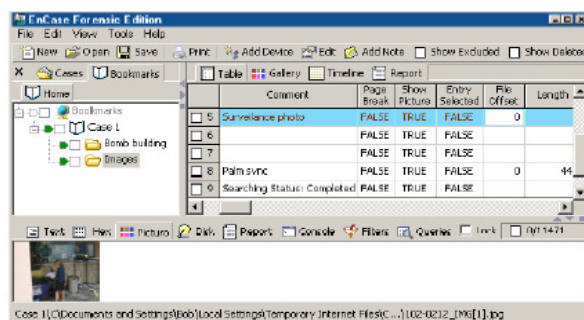
Slika 40 Verifikacija novog slučaja

Dodavanje sirovih imidž fajlova u EnCase vrši se korišćenjem putanje *File->Add Raw Image*. Pojavljuje se dijalog u koji se unose ime, dodatih fajlova, odabirom postojećih ili dodavanjem novih, ili takozvanih *chunk* fajlova koji se nalaze u *Components Files*, (slika 41).



Slika 41 Dodavanje sirovih imidž fajlova u EnCase alatu

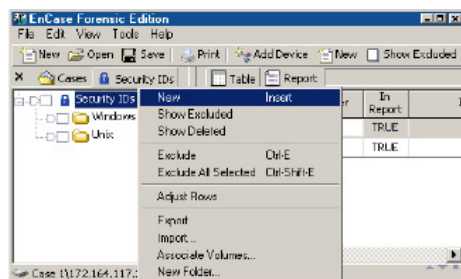
Sledeće što je neophodno uraditi jeste selektovati Image Type aktiviranjem odgovarajuće opcije između *None, Disk, Volume, CD-ROM*. Kada su Image Type ili Partition Type izabrani, aktiviranjem OK može se videti kompletan disk sa vidljivom strukturom fajlova. *Označavanje fajlova od interesa (bookmarks)* vrši se selektovanjem *Bookmarks* iz menija View. *Bookmarks* tab sadrži informacije koje su markirane kao fajlovi od interesa. Bookmarkovi mogu biti muzički fajlovi, slike, tekst i dr. Mogu se videti u Table, Gallery ili Timeline prikazu, (slika 42).



Slika 42 Indeksiranje fajlova u EnCase alatu

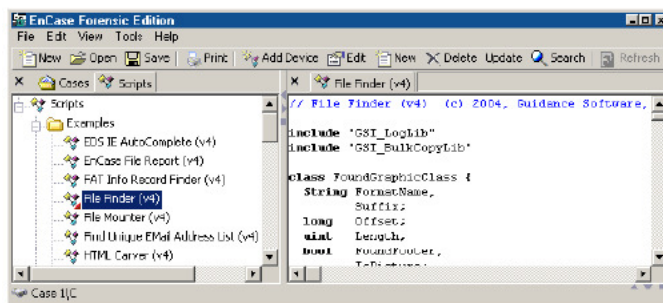
EnCase je program koji sadrži raznovrsne opcije za pretraživanje. Među pomenutim opcijama nalaze se i opcije za pretraživanje po tipu podataka, opcije za pretraživanje po ekstenzijama i upoređivanje istih radi dokazivanja da li je došlo do promene određenih ekstenzija ili nije, pretraživanje po ključnim rečima i mnoga druga.

Bezbednosni identifikator (SID) i određeni skup dozvola ima svaki fajl, ili folder u NTFS fajl sistemu. Iako se struktura fajlova razlikuje u NTFS 4 i NTFS 5 fajl sistemu, *EnCase* ekstrahuje pomenute informacije o fajlovima i folderima. *EnCase* radi sa Windows, Linux i Unix sistemima. Security IDs tab dozvoljava korisnicima da unesu „security ID“ za određeni dokazni matreijal. Do ovog taba dolazi se korišćenjem putanje View->Security Ids, (slika 43). U PRILOGU 1 dat je spisak poznatijih SID identifikatora u Windows operativnim sistemima.



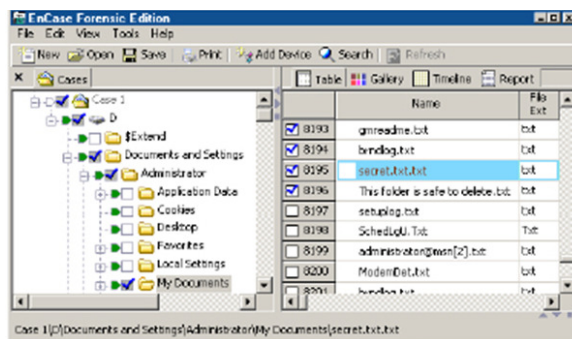
Slika 43 Određivanje bezbednosnog identifikatora dokaza

Skriptovi se aktiviraju opcijom Script do koje se dolazi korišćenjem putanje View->Scripts. Naime, skriptovi su mali programi, ili makroi koji su dizajnirani kako bi poboljšali automatizaciju forenzičke istrage i njenih procedura. Omogućena je manipulacija i pristup mnogim delovima *EnCase* interfejsa od pretrage bookmarkova do dodavanja informacija izveštajima, (slika 44).



Slika 44 Aktiviranje skriptova u EnCase alatu

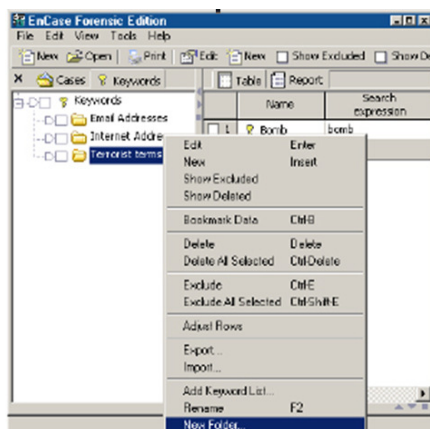
Kopiranje/oporavak izbrisanih fajlova, *EnCase* vrši „byte-po-byte“. Sve što treba uraditi jeste čekirati fajl i desnim tasterom miša izabrati opciju Copy/unErase. Pojaviće se dijalog kojim se vrši odabir između načina na koji će fajl biti vraćen, koji njegov deo (fizički, logički, RAM slack) i na kraju gde smestiti taj fajl, (slika 45).



Slika 45 Izbor fajlova i foldera za oporavak

Takođe, moguće je isto uraditi i sa *bookmark*-ovima. Proces je identičan opisanom bilo da se koristi jedan ili više *bookmark*-ova.

Pretraživanje po ključnoj reči identično je klasičnoj „find“ opciji u bilo kojoj aplikaciji. Unutar dijaloga za pretraživanje neophodno je uneti ključnu reč i na taj način izvršiti pretragu. Pored unošenja reči može se vršiti odabir po kome će biti izvršena pretraga. Tako se može tražiti *Unicode*, *Big-Endian Unicode*, *UTF-8* i dr. Keywords tab nudi više mogućnosti. Pored malopredašnjeg načina pretrage (što podrazumeva formiranje grupe) mogu se koristiti već formirane grupe za pretragu. Tako se, među njima, nalaze i pretrage e-mail adrese i web stranice, ili pretraga karaktera stranih jezika, (slika 46).



Slika 46 Pretraživanje po ključnoj reči u EnCase alatu

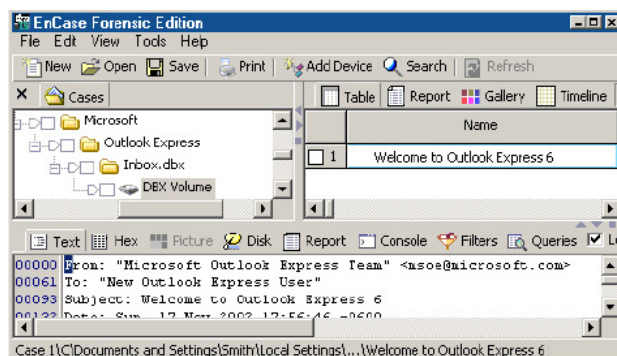
Pregled komponovanih fajlova pod kojim se podrazumevaju fajlovi sastavljeni od više slojeva kao što su OLE (*office* fajlovi), komprimovani fajlovi, *registry* fajlovi i *e-mail*. Da bi se videla struktura komponovanih fajlova neophodno je selektovati fajl i desnim tasterom miša izabrati opciju View File Structure.

EnCase v. 4 sadrži *EnScript* pod imenom *File Mounter* koji podržava rad sa komponovanim fajlovima, nudeći brz i lak dolazak do njihove strukture.

Registry fajlovi u Windows OS sadrži vredne informacije koje su vezane za računar osumnjičenog, a može im se pristupiti iz *EnCase* alata. U Win 95, 98 i ME OS nalaze se u *C:\Windows* pod nazivom *system.dat* i *user.dat*. U Win NT 4.0, 2000 ili XP OS ovi fajlovi se nalaze pod *C:\%SYSTEMROOT%\system32\config* i nose imena *security*, *software*, *SAM* i *system*.

Kompresovani fajlovi: *EnCase* podržava rad sa kompresovanim fajlovima kao što su WinZip(.zip), Gzip (.gz) i Unix .tar fajlovi. Da bi se otvorio kompresovani fajl neophodno je desnim tasterom miša na fajl izabrati opciju View File Structure.

Rad sa *Outlook Express e-mail .DBX* fajlovima, podržava *EnCase* alat. Ovi fajlovi su konvertovani u folder sa podgranom *DBX volume* ispod. Sa desne strane su izlistani mail-ovi, a ispod u okviru Text taba se nalazi njihov sadržaj, (slika 47).



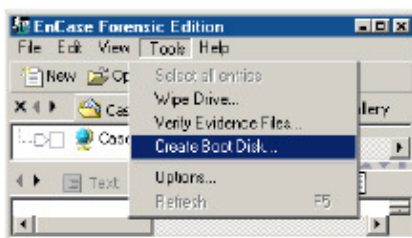
Slika 47 Čitanje Outlook Express .DBX fajlova u EnCase alatu

Obrisani e-mail i *attachment* mogu se povratiti sa nealociranog prostora klastera. Velika je verovatnoća da se ovi fajlovi nakon brisanja ne mogu povratiti, jer su delimično/potpuno prepisani, ali je zasigurno da se neki njegovi delovi mogu videti. *Base64* i *UUE Encoding attachment* će biti automatski prikazani u radu sa mail-ovima.

Rad sa MS Outlook e-mail-om identičan je radu sa Outlook Express-om. Kada *EnCase* izgradi Outlook .PSF fajl, on poruke konvertuje u RTF (*Rich Text File*) i ASCII tekst formatirani fajl (*message.rtf* i *message.txt*). Ovi fajlovi mogu biti otvoreni u Microsoft Word-u, ili Notepad-u.

Akvizicija EnCase alatom počinje sa kreiranjem *EnCase butabilne* diskete. EnCase Boot Diskette se koristi za butovanje korumpiranog računara. Butabilni disk se formira na sledeći način:

Sa Tools menija selekovati Create Boot Disk, (slika 48),



Slika 48 Kreiranje butabilne diskete u EnCase alatu

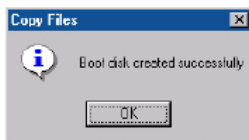
Postaviti disketu u *floppy* drive i aktivirati opciju Next.

Naredni dilajog nudi izbor između ažuriranja trenutnog diska, ili brisanja njegovih fajlova. Pojavljuje se Copy Files prozor koji nudi mogućnost kopiranja fajlova na disketu (*EnCase* DOS i EN:EXE).

Pretragom se dolazi do gore navedenih fajlova koji će biti na disketi.

Kada je putanja do *EnCase* fajla popunjena u okviru dijaloga i obojena plavom bojom tada je završen proces kreiranja i može se aktivirati Finish.

Na kraju se naznači da je butabilni disk uspešno kreiran i tada se može aktivirati OK, (slika 49).



Slika 49 Završetak kreiranja butabilne diskete u *EnCase* alatu

Izvaditi deisketu i pravilno je označiti.

Podizanje OS računara sa EnCase butabilnom disketom može biti rizično, pošto konfiguracija korumpiranog računara i njegovo stanje nisu poznati. Koraci ovog procesa su sledeći:

- potvrditi da je korumpirani računar isključen,
- otvoriti računar i ispitati postojanje nekih neuobičajenih konekcija,
- iščupati kablove sa svih rezidentnih hard drajvova,
- ubaciti *EnCase* butabilnu disketu i upaliti računar,
- pokrenuti CMOS (BIOS) *setup* da bi se podesilo butovanje sa diskete,
- izaći iz BIOS-a i sačuvati promene
- dozvoliti računaru butovanje sa diskete
- isključiti računar i priključiti Hard diskove,
- proveriti da li je disketa još uvek u drajvu, pokrenuti računar ponovo i dozvoliti mu butovanje sa diskete ponovo.

EnCase za *DOS* operativni sistem koristi se isključivo za akviziciju podataka. Izvršni fajl (EN.EXE) nalazi se u *EnCase* instalacionom folderu i kopiran je na *EnCase* butabilni disk tokom procesa njegovog kreiranja.

EnCase za *DOS* postavlja korumpirani računar u tzv. serverski režim rada i nudi još opcija kao što su zaključavanje i otključavanje hard drajvova (slika 50), akviziciju podataka, heširanje i mnoge dr.



Slika 50 Zaključavanje i otključavanje hard diskova

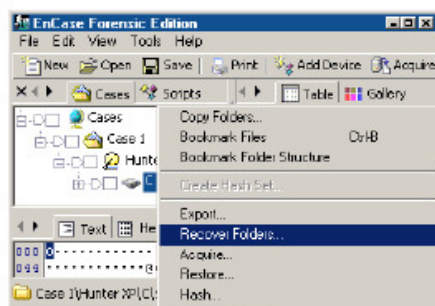
EnCase podržava rad sa *EnCase* Network Boot Disk-om uz korišćenje *parallel* i *crossover* kabla (poseban metod akvizicije računara korišćenjem mreže), takođe i *Drive-to-Drive* akviziciju, *FastBloc* (blokator između forenzičkog i korumpiranog računara) akviziciju,

RAID akviziciju, akviziciju Palm PDA uređaja, Zip/Jaz diskova kao što je Floppy, USB Flash, CD, DVD i mnogih drugih medija i rad sa više medija u isto vreme.

Podešavanje vremenske zone je ključna operacija u procesu analize digitalnih podataka. Različiti mediji u okviru jednog slučaja imaju različite vremenske zone, što dovodi do otežanog otkrivanja kada se događaj stvarno desio. *EnCase* daje mogućnost licima koja istražuju određeni slučaj da postave parametre vremenskih zona za svaki medij nezavisno od sistema i drugih medija u sistemu.

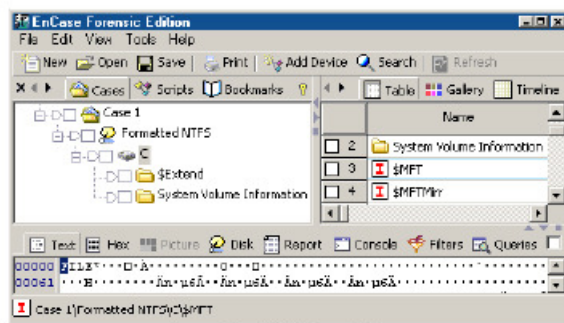
Oporavak foldera u FAT fajl sistemu: Prvi korak brisanja podataka je njihovo slanje u *Recycle Bin*. Smatra se da kada se *Recycle Bin* isprazni, da su podaci zapravo tada obrisani. Ipak, oni se i u tom trenutku nalaze na HDD i lako se mogu povratiti.

Nakon što je fajl ili folder dodat određenom slučaju kreiranom u *EnCase*-u, može se pokrenuti *Recover Folders* za sve FAT particije, koje se odabiraju tasterom desnog miša na fajl. Ovom komandom vrši se pretraga kroz sve nealocirane klustere konkretne FAT particije. Svaki folder FAT particije ima ulaz u obliku „..“ (*dot-double dot*). Ovi ulazi govore fajl sistemu gde se nalaze folderi. *EnCase* vrši pretragu kroz nealocirane klustere, traži ulaz („..“) i vrši povraćaj foldera koji su obrisani, ili sa njihovim ulazima koji su obrisani u glavnom direktorijumu. *EnCase* neće vratiti folder sa originalnim imenom (jer je ime obrisano u glavnom direktorijumu), ali će nastojati da povрати sve što se nalazi unutar tog foldera, uključujući i imena fajlova unutar foldera, (slika 51).



Slika 51 Oporavak izbrisanih foldera u *EnCase* alatu

Oporavak foldera u NTFS fajl sistemu: *EnCase* može da vrši povratak fajlova i foldera iz nealociranih klastera i rastavlja ih kroz Master File Table (\$MFT rekord) na fajlove bez glavnog direktorijuma. Ovo je posebno korisno, ako je disk reformatiran, a \$MFT fajl korumpiran. Oporavljeni fajlovi se smeštaju u sivi Lost Files virtuelni folder koji se nalazi na rut-u NTFS particije, (slika 52).



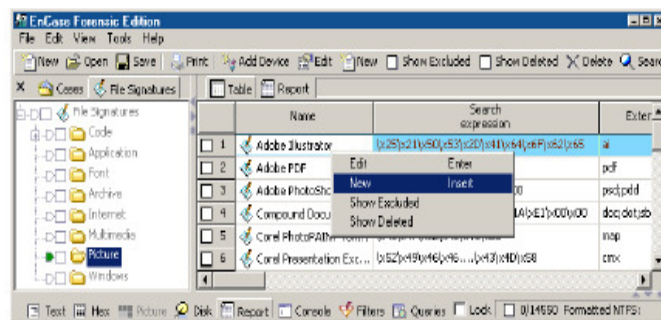
Slika 52 Formatirana NTFS particija

Oporavak obrisanih ili izgubljenih fajlova vrši se na sličan način kao kod FAT sistema aktiviranjem desnog tastera miša na određeni folder i odabirom Recover Folders.

Potpisi fajlova (File Signatures): Kada su tipovi fajlova standardizovani, *signature* ili *header* su delovi podataka koje program prepoznaje i prosleđuje određeni tip fajla konkretnom programu. *Header* ili *signature* fajla je povezan sa ekstenzijama fajlova.

Ekstenzije fajlova su delovi imena fajlova koji se nalaze odmah nakon tačke („.“). To usmerava sistem na otvaranje određenih programa namenjenih radu sa konkretnim fajlovima. Recimo, ako je ekstenzija fajla .TXT, očekuje se da je fajl tekstualnog oblika i računar će automatski otvarati neki od programa za obradu teksta. Međutim, u praksi se kriju razni tipovi fajlova iza tuđih ekstenzija. Kada se slika, originalno .JPEG ekstenzije, sakrije iza .TXT ekstenzije, ona će se nakon duplog klika levog tastera miša otvarati u nekom od programa za obradu teksta. Naravno, slika se neće videti, a računar će prijaviti grešku. Isti .TXT fajl se ne može otvoriti u nekom od programa za obradu fotografija. Zbog toga se forenzičari bave *header*-om ili *signature*-om u kome se nalaze tačne informacije o fajlu.

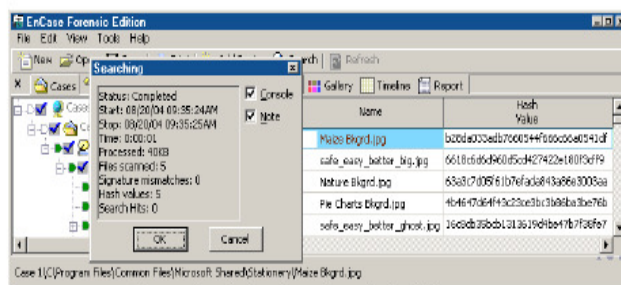
Signatures se mogu videti korišćenjem putanje View->File Signatures. *EnCase* pored velikog broja *signatures* ima i mogućnost dodavanja novih. Recimo .mp3 format nije u listi standardnih formata pa se u *EnCase*-u može dodati kao *signature* i podesiti da se po njegovom pronalaženju automatski otvara sa nekim od programa koji podražavaju njegov rad, (slika 53).



Slika 53 Dodavanje novih potpisa fajla u EnCase alatu

Sažetak fajla (Hash): *EnCase* omogućava dodeljivanje heš vrednosti koja predstavlja „digitalni otisak prsta“ svakog fajla. *EnCase* koristi 128 bitni MD5 kriptografski algoritam za generisanje heš vrednosti, koji spada u grupu heš algoritama, ili algoritama za sažimanje sadržaja fajla. Ovi algoritmi se još nazivaju i *digest*, ireverzibilni, ili algoritmi bez ključa. MD5 je veoma primenjivan u mnogim oblastima zaštite podataka. Danas se smatra ranjivim, tako da se ređe primenjuje u kriptografiji, ali je našao veoma čestu primenu u zaštiti integriteta većih fajlova zbog svoje brzine.

EnCase kreira takozvani Hash Set, ili kolekciju heš vrednosti. Ove vrednosti su od presudnog značaja za forenzičku analizu. Heš vrednostima se upoređuje, eliminiše, dokazuje, oslobađa i još mnogo toga, (slika 54).



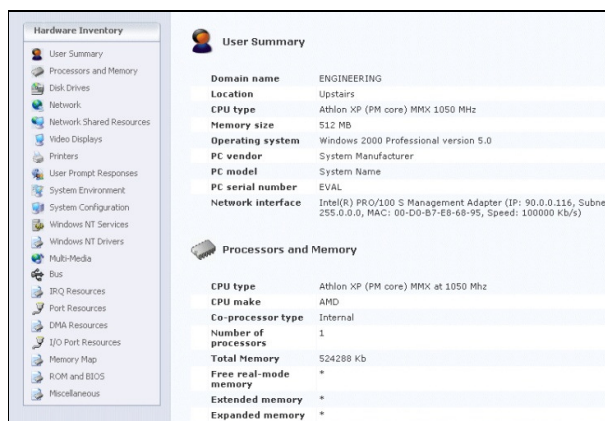
Slika 54 Generisanje heš vrednosti za izabrane fajlove

Proces oporavka podataka: Disk se uglavnom formatira, na neki od postojećih načina, radi brisanja podataka. Međutim, formatiranje, ili popularno *FDISK*-ovanje ne briše podatke u potpunosti, nego samo strukturu koja locira podatke i informacije o particioniranom disku. *EnCase* ima mogućnost oporavka podataka nakon formatiranja diska.

Ako prikupljeni dokazni materijal pokazuje logički deo diska, a ne pokazuje strukturu direktorijuma, znak je da je HD verovatno bio formatiran. Ako je u pitanju FAT sistem, *EnCase* ima mogućnost da u potpunosti izvrši povraćaj podataka sa diska. To se postiže aktiviranjem desnog tastera miša na svaki logički deo i odabirom *Recover Folders* opcije. Ovom opcijom vrši se pretraživanje foldera, subfoldera i fajlova i pronalaze sve informacije koje su i dalje na drajvu.

EnCase ima mogućnost davanja pregleda posećenih stranica - *Web History*, čija je evidencija o posećenosti već obrisana. Takođe, ima mogućnost povratka obrisanih *mail*-ova sa celokupnim tekstom i *attachment*-om.

Snimak trenutnog stanja sistema (System Snapshot) daje uvid u trenutno stanje računara i svih njegovih procesa koji su u toku. Naime, dobija se uvid u sve otvorene fajlove, procese i portove na lokalnom sistemu, efektivnim hvatanjem kratkotrajnih podataka koji se nalaze u RAM-u. Zbog toga što opstaju samo dok je računar upaljen, RAM predstavlja jedan od najvrednijih izvora podataka. Kod *EnCase Enterprise ver.4 snapshot* se vrši korišćenjem *EnScript*-ova, (slika 55).

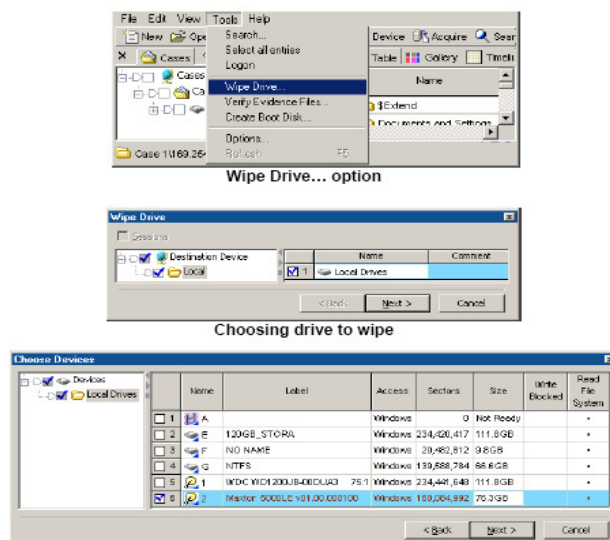


Slika 55 Snimak trenutnog stanja sistema

Arhiviranje dokaznog materijala smatra se dobrom forenzičkom praksom i preporučuje se odmah nakon njegove akvizicije. Na ovaj način se štiti materijal koji se lako može uništiti tokom istrage. Materijal se arhivira na CD-ROMu ili DVDu. Razlog je u tome što se podaci

tokom akvizicije pakuju u pakete veličine 640 MB što odgovara veličini CD-ROMa. Nakon što je materijal narezan na CD, neophodno je naznačiti disk sa imenom, datumom, .CASE fajlom i rednim brojem sekvence (grupa paketa veličine 640 MB).

Nakon što su svi koraci preduzeti, neophodno je očistiti sve tragove. Za to služi takozvana Wiping opcija. Wiping u potpunosti briše sve podatke prepisivanjem postojećih podataka sa jedinica (1), nulama (0), ili slučajnom kombinacijom 1 i 0. Potrebno je izabrati Wipe Drive... iz Tools opcija kako bi se obrisali svi podaci sa HD – a, (slika 56).

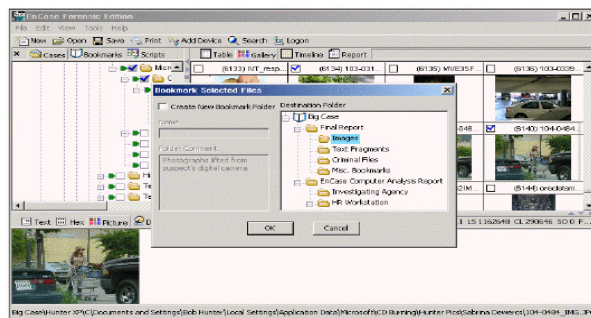


Slika 56 Izbor i selekcija diska za brisanje sa prepisivanjem u EnCase alatu

Prezentovanje dokaza i izveštavanje u pismenoj formi, pridržavajući se predviđenih pravila, finalana je faza forenzičke istrage. Izveštaj mora biti organizovan i prezentovan na razumljiv način. EnCase je dizajniran tako da predstavlja dokaze na organizovan način, što pomaže da se odmah nakon istrage može generisati odgovarajući izveštaj.

EnCase obezbeđuje nekoliko metoda za generisanje finalnog izveštaja. U praksi je čest primer „prelamanja“ izveštaja na nekoliko delova, sa sadržajem koji upućuje na sve njegove delove. Javlja se i potreba za izveštajima koji nisu u papirnoj formi (skladišteni na CD-ROMu), ali uz kratki sadržaj (*hyper linked summary*). EnCase je prilično fleksibilan kod formiranja finalnog izveštaja.

Izveštaj može biti standardnog tekstualnog formata (.rtf) koji se čita i iz MS Word – a, a može biti i HTML formata. Veliki broj slika u forenzičkoj istrazi otežava izveštavanje. Nakon indeksiranja slika, izveštaj se može generisati sa slikama u HTML formatu i skladištiti na disk sa svim neophodnim linkovima za dolaženje do određenog dela njegovog sadržaja. HTML format je prikladniji za ovu svrhu, posebno za prezentovanje dokaznog materijala sudu, kako zbog prostora („manje“ papira) i organizacije, tako iz zbog pregleda slika (*thumbnails*), (slika 57).



Slika 57 Simultano indeksiranje velikog broja slika relevantnih za istragu

Export izveštaja vrši se aktiviranjem desnog tastera miša na Export u desnom prozoru za eksportovanje u odgovarajućem formatu, kada je izveštaj sastavljen i prikazan. Kao što je već pomenuto, moguće je eksportovati izveštaj u dva formata: .RTF i HTML, (slika 58).



Slika 58 Eksportovanje izveštaja u EnCase alatu

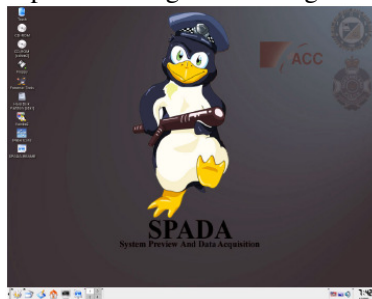
U zavisnosti od željenog formata, u narednom prozoru, treba izabrati odgovarajuću opciju. Ukoliko je izabran HTML format, u folderu će biti generisano sledeće:

- Full HTML format sa odgovarajućim imenom izveštaja,
- gallery.html sa thumbnail-ovima za simultan pregled slika,
- toc.html sa sadržajem i
- Frame View.html, koji kreira tzv. „frame view“ za prethodna tri fajla.

Duplim aktiviranjem levog tastera miša na Frame View.html, otvoriće se Explorer kao podrazumevani pretraživač sa imenima, datumima i ostalim informacijama koje su vezane za izveštaj.

8.3.3 SPADA forenzički alati na bazi Linux OS

Na slici 59 prikazan je desktop softverskog forenzičkog alata SPADA na bazi Linux OS.

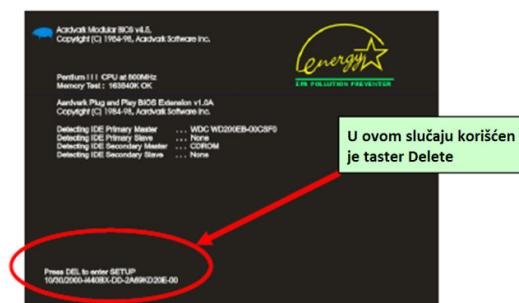


Slika 59 Desktop SPADA forenzičkog alata

Kada se instalira SPADA i pojavi desktop, na dnu ekrana vide se ikone *task bar*-a koji je deo KDE GUI interfejsa, kojeg SPADA koristi. Među tim ikonama su ikone za različite programe i pod-menije. Za primenu osnovnih funkcija SPADA alata, koje najčešće služe forenzičarima kao alat za *inicijalnu pretragu*, postoje četiri osnovna koraka:

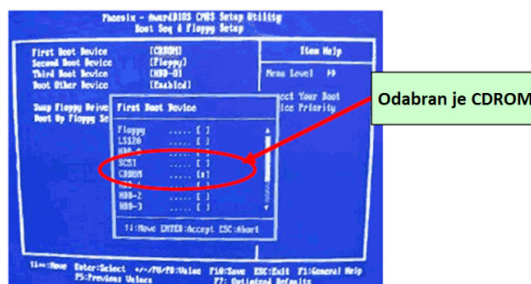
1. Korak: Forenzičar se prvo mora uveriti da računar ima instaliran CD-ROM drajv i da se računar butuje, kao prva opcija sa CD drajva. Zatim treba da proveriti podešavanje BIOS-a da se uveri da će se računar butovati sa CD-ROMa.

Mnogi računari pokazaće, tokom POST procesa, poruku koja indicira kako se ide u BIOS prozor za podešavanje (*Setup Screen*). Ako se ovo ne prikaže aktiviranjem nekoliko tipki tastature u toku procesa POST, često će se generisati POST greška i dopustiće pristup BIOS *Setup*-u, slika 60.



Slika 60 Aktiviranje POST procesa za pristup BIOS setup-u

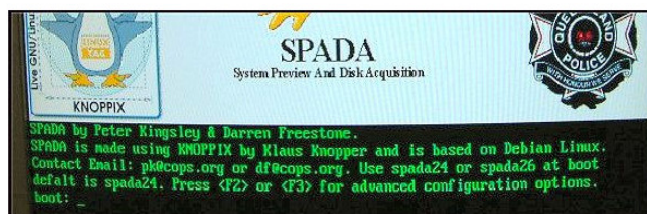
Tipičan ekran za podešavanje BIOS-a prikazan je na sledećoj slici, (slika 61).



Slika 61 Podešavanje BIOS-a u SPADA alatu

Ako računar nije konfigurisan da se butuje sa CD-ROMa, mora se podesiti na takav način i konfiguracija *setup*-a treba da se memoriše. Druga podešavanja ne treba menjati, a treba napraviti pisanu zabeležku o izvršenoj promeni.

2. Korak: Kada se PC konfigurira da se butuje sa CD-ROMa, treba ubaciti CD u drajv i restartovati i rebootovati sistem. Forenzičar mora posvetiti posebnu pažnju na aktivnosti na ekranu i treba da vidi SPADA meni za butovanje kao na slici 62.



Slika 62 SPADA meni za butovanje

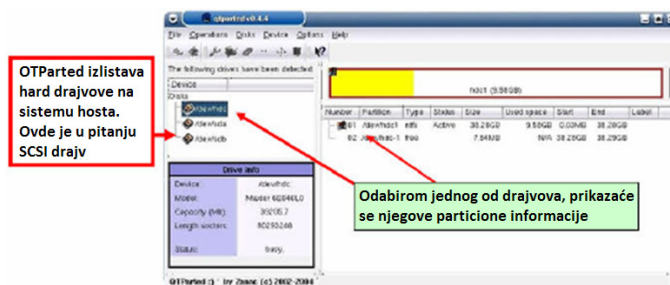
Postoje dve bazične predefinisane opcije za butovanje u Linux *kernelu* 2.4. Ovaj izbor treba da radi sa većinom sistema. Ako ne radi, treba eksperimentisati sa naprednim opcijama. Aktiviranjem Enter tipke tastature treba da podigne sistem. Proces treba posmatrati i biti spreman na reagovanje na svako upozorenje na neku grešku, ili anomaliju. Zatim se na zahtev sistema unosi geografski region i podešavaju lokalno vreme i datum.

3. Korak: SPADA program je podignut i proces inicijalnog pretraživanja sistema može se u celini izvršiti sa SPADA desktopa. Sa menija desktopa, treba aktivirati donju levu ikonu i otvoriti All Application meni, a odavde izabrati System, zatim QTParted opciju, (slika 63).



Slika 63 Aktiviranje procesa inicijalne pretrage sa SPADA alatom

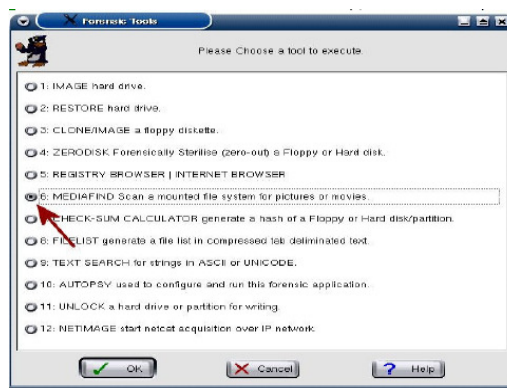
QTParted aplikacija se prva pokreće da se forenzičar upozna sa HD na host sistemu i kako je partitioniran. Forenzičar treba da pažljivo notira imena diskova prikazana u prozoru Device u *QTParted* aplikaciji, zato što ta informacija može trebati kasnije. Kada se ove informacije notiraju, aplikaciju treba zatvoriti, ili minimizirati, (slika 64).



Slika 64 Otvaranje *QTParted* aplikacije u SPADA alatu

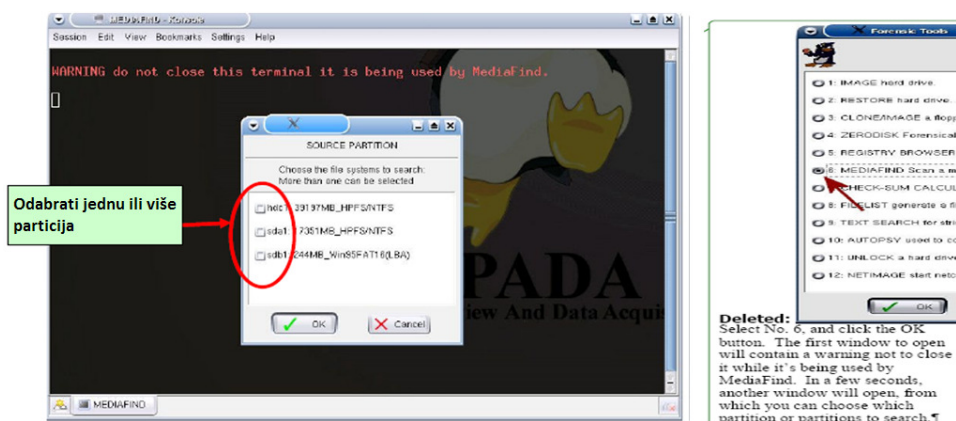
Treba zapaziti da SPADA „vidi“ Windows Dinamičke diskove, koje podržavaju Windows 2000 i XP OS-i i može ih instalirati kao normalne particije čvrstog diska. Ako se dinamički diskovi instaliraju na host sistem, linkovanjem u folder na drugoj particiji, SPADA ih neće videti u tom folderu.

4. Korak: Sada se *QTParted* aplikacija može zatvoriti, ili minimizirati i pošto je SPADA već instalirala diskove u modu „samo čitanje“, forenzičar može nastaviti četvrti korak - ispitivanje diskova na potencijalne dokaze. Postoji nekoliko načina pretraživanja diska, a najbolje je tehniku odrediti prema tipu informacija koje forenzičar traži. Kako se SPADA često koristi kao alat u inicijalnoj pretrazi slučajeva dečije pornografije, jedna od ključnih aplikacija je Mediafind. Za aktiviranje te aplikacije treba izabrati Forensic Tool ikonu na desktopu, koja će otvoriti sledeći prozor, (slika 65).



Slika 65 Aktiviranje Mediafind aplikacije u SPADA alatu

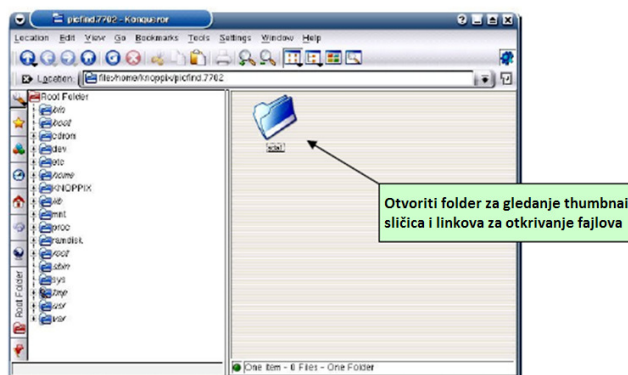
Treba izabrati N.6 i pritisnuti OK. Prvi otvoreni prozor sadrži upozorenje da se ne zatvara dok se koristi MediaFind aplikacija. Za nekoliko sekundi otvara se drugi prozor na kojem se može izabrati particija(e) za pretragu. MediaFind prozor prikazan je na slici 66.



Slika 66 MediaFind prozor u SPADA alatu

Kada se izabere željena particija, treba izabrati OK i program će tražiti da selektujete minimalnu veličinu fajla kojeg tražite. Ovo je zgodna funkcija koja eliminiše vrlo male grafičke fajlove, koji se obično nalaze u Windows sistemu. Takvih fajlova, vremenom akumuliranih, može biti na stotine, kao što su male ikone, delovi posećenih web lokacija itd. Ako forenzičar nije siguran u minimalnu veličinu fajla, treba ostaviti podrazumevanu poziciju.

Rezultati MediaFind aplikacije prikazani su na slici 67. Aplikacija automatski stavlja *thumbnail* (male slike) ikone i linkove do svakog fajla pronađenog u folderu, koji ima ime pretraživane particije, kako je gore prikazano. Otvaranjem ovog foldera pojavljuju se ikone fajlova koje sadrži. Ako postoji tip fajlova koji se može identifikovati po ekstenziji, kao što su .gif, .jpg, .bmp itd., ikona će biti veličine thumbnail reprezentacija fajla. Neki fajlovi se neće prikazati u *thumbnail* veličini, ali još uvek mogu biti vidljivi.



Slika 67 Rezultati MediaFind aplikacije

Za detaljno gledanje fajlova, treba samo otvoriti željeni fajl. SPADA je opremljena sa brojnim pretraživačima za otvaranje fajlova koji mogu prikazati ceo *imidž* diska. Kada se kursor miša postavi iznad ikone fajla, na dnu panela prikazaće se lokacija aktuelnog fajla u sistemu. U ovoj tački, forenzičar može kopirati fajl koji sadrži neki dokaz na drugi forenzički medijum.

Komandna linija SPADA/Linux programa potrebna je, jer se mogu se pojaviti slučajevi gde je poznavanje komandne linije korisno, iako je korišćenje Linux GUI-a veoma lako, na primer, neka nestandardna video karta može se neuspešno podizati sa GUI Windows XP sistemom. Kada se to dogodi, izlaz treba potražiti u komandnoj liniji. U tabeli 8. prikazane su korespondirajuće DOS i Linux komandne linije.

Tabela 8 Korespondirajuće DOS i Linux komandne linije

DOS Komanda	Linux Komanda
DIR	ls
CD	cd
MD	mkdir
COPY	cp
DEL	rm
REN	mv
ARIB	vhmod

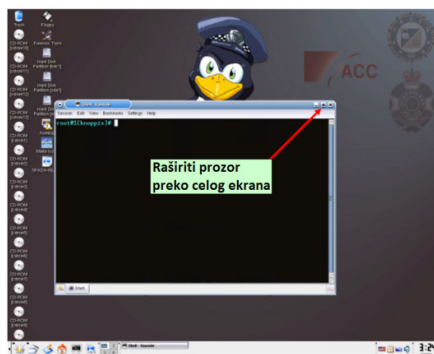
Takođe, treba znati da je Linux sistem osetljiv na veličinu slova, za razliku od DOS operativnog sistema. Ako se radi u Linux komandnoj liniji, imena fajlova, ili putanje sa mešovitom veličinom slova alfabeta, moraju se otkucati tačno onako kako se pokazuju. Druga osobina Linux-a je da ne prihvata prazan prostor u imenu fajla, što može izazvati problem kod korišćenja komandne linije. Da bi se ovaj problem prevazišao, treba razmak u nazivima Windows fajl sistema u Linuks komandnoj liniji zameniti sa znakom `?`. Na primer, Documents and Settings u Windows biće `cd:\Documents?and?Settings` u Linux komandnoj liniji.

Ekvivalent DOS, ili Windows prozora u Linux sistemu je Terminal Window. Ekvivalent butovanja DOS/Windows sistema u DOSu je butovanje Linux mašine u Terminal modu. Za otvaranje Terminal prozora u SPADA alatu, treba jednostavno selektovati ikonu Terminal Program u meniju na desktopu, (slika 68).



Slika 68 Otvaranje Terminal prozora u SPADA alatu [1]

Kao DOS prozor u Windows OS, ovaj boks se može proširiti na puni ekran, što se preporučuje, a izvršava pritiskom na srednju ikonu u gorenjem desnom uglu, (slika 69).



Slika 69 Proširivanje Terminal prozora u SPADA alatu na puni ekran [1]

Kao i DOS, Linux će se predstaviti sa promptom komandne linije `root@1[knoppix]#`, gde # simbol predstavlja heš potpis i indicira da je sistem u administratorskom modu i da forenzičar ima kompletnu kontrolu nad sistemom.

Osnovna navigacija u Linux Terminal Window: Verovatno najkorisnija Linux komanda je `ls` – komanda liste sadržaja direktorijuma. Kao `DIR` komanda u DOSu, ova komanda pokazuje listu fajlova u tekućem direktorijumu. Kao i u DOSu, postoji neki broj prekidača (*svičeva*) koji se mogu koristiti za definisanje načina rada `ls` komande. Korisna kombinacija podešavanja je: `ls-al`. Ova kombinacija će pokazati sve fajlove u tom direktorijumu, uključujući skrivene fajlove u nekom formatu sa dugim imenom. U tabeli 9. prikazani su različiti `ls` svičaevi.

Tabela 9 Svičevi za za definisanje načina rada ls komande [3]

-a	Shows you all files, even files that are hidden (these files begin with a dot.)
-A	List all files including the hidden files. However does not display the working directory (.) or the parent directory (..).
-b	Force printing of non-printable characters to be in octal \ddd notation.
-c	Use time of last modification of the i-node (file created, mode changed, and so forth) for sorting (-t) or printing (-l or -n).
-C	Multi-column output with entries sorted down the columns. Generally this is the default option.
-d	If an argument is a directory it only lists its name not its contents.
-f	Force each argument to be interpreted as a directory and list the name found in each slot. This option turns off -l, -t, -s, and -r, and turns on -a; the order is the order in which entries appear in the directory.
-F	Mark directories with a trailing slash (/), doors with a trailing greater-than sign (>), executable files with a trailing asterisk (*), FIFOs with a trailing vertical bar (), symbolic links with a trailing at-sign (@), and AF_UNIX address family sockets with a trailing equals sign (=).
-g	Same as -l except the owner is not printed.
-i	For each file, print the i-node number in the first column of the report.
-l	Shows you huge amounts of information (permissions, owners, size, and when last modified.)
-L	If an argument is a symbolic link, list the file or directory the link references rather than the link itself.
-m	Stream output format: files are listed across the page, separated by commas.
-n	The same as -l, except that the owner's UID and group's GID numbers are printed, rather than the associated character strings.
-o	The same as -l, except that the group is not printed.
-p	Displays a slash (/) in front of all directories.
-q	Force printing of non-printable characters in file names as the character question mark (?).
-r	Reverses the order of how the files are displayed.
-R	Includes the contents of subdirectories.
-s	Give size in blocks, including indirect blocks, for each entry.
-t	Shows you the files in modification time.
-u	Use time of last access instead of last modification for sorting (with the -t option) or printing (with the -l option).
-x	Displays files in columns.
-1	Print one entry per line of output.

Kada forenzičar otvori Terminal prozor, nalazi se podrazumevano u pod-direktorijumu nekoliko slojeva duboko u strukturi fajl sistema, što je prikazano putanjom:

```
//ramdisk/home/knoppix.
```

Za prelazak na rut direktorijum sistema treba koristiti komandu cd razmak-prednja kosa (cd /). Kao u DOS sistemu, ova komanda vodi na rut direktorijum bilo sa koje lokacije na logičkom disku. Ako se sada izvrši komanda ls, može se videti nekoliko izlistiranih fajlova i subdirektorijuma. Jedan od ovih, subdirektorijuma mnt sadrži fajlove koji su virtuelna tačka za instalaciju uređaja, uključujući čvrste diskove na host računarskom sistemu.

Za navigaciju diskova nabačenog host računara iz ruta (/) sistema, treba promeniti na mnt direktorijum (cd mnt). Ako je disk instaliran, ls će pokazati ime diska (hda1, sda1 itd.). Kada se pređe na izabranu particiju – cd hda1, na primer i otkuca ls, videće se poznato Windows okruženje. Odavde forenzičar može pretražiti logički disk i na forenzički ispravan način izvršiti inicijalno ispitivanje diska. Za ispitivanje diska u tipičnoj korisničkoj oblasti na Windows baziranom računaru, treba gledati fajlove u direktorijumu Documents and Settings, kucajući Documents?and?Settings u komandnoj liniji Linux-a.

Zavisno od slučaja, ovo inicijalno ispitivanje, može dati dovoljno podataka forenzičaru da isključi osumnjičeni računar i da ga privremeno ne oduzima za laboratorijsko forenzičko ispitivanje. Za dalje ispitivanje funkcionalnosti SPADA alata treba priključiti eksterne pokretne memorijske uređaje kao što su USB, fleš memorije, eksterni diskovi itd. i kopirati sumnjive fajlove na te uređaje za kasnije ispitivanje, ili prezentaciju pred sudom. SPADA, naravno, nije jedini butabilni Linux CD.

8.4 Komparativni pregled funkcija ključnih forenzičkih alata

Rezultati uporednog pregleda osnovnih funkcija relevantnih forenzičkih alata, dati u tabeli 73., mogu biti korisni i pomoći forenzičaru kod izbora forenzičkog alata koji najbolje odgovara potrebama.

Tabela 10 Uporedni pregled osnovnih funkcija relevantnih forenzičkih alata [3]

Funkcija forenzičkog alata	<i>Access Data Ultimate Kit (FTK)</i>	<i>Guidance Software EnCase</i>	<i>Digital Intelligence Drive Spy</i>
Akvizicija			
Fizičko kopiranje podataka	√	√	
Logičko kopiranje podataka	√	√	√
Formati akvizicije podataka	√	√	
Proces komandne linije		√	√
GUI proces	√	√	√
Udaljena akvizicija		√*	
Verifikacija	√	√	√
Validacija i diskriminacija			
Heširanje	√**	√**	√
Filtriranje	√	√	√
Analiza hедера fajlova	√	√	
Ekstrakcija			
Čitanje podataka	√***	√***	
Pretraživanje po ključnoj reči	√	√	√
Dekompresovanje	√	√	
Rekonstrukcija fragmentovanog fajla (<i>carving</i>)	√	√	
Dešifrovanje	√		
Označavanje dokaza	√	√	
Rekonstrukcija bezbednosnog događaja			
kopiranje diska na disk	√	√	√
Kopiranje imidža na disk	√	√	√
Kopiranje particije na particiju		√	√
Kopiranje imidža na particiju		√	√
Izveštavanje			
Log izveštaj	√	√	√
Generator izveštaja	√		
Legenda:			
* Zahteva se nabavka <i>Enterprise Edition</i>			
** Koristi MD5 i SHA1 algoritme za heširanje			
*** Varira format fajlova koje podržava			

8.5 Validacija i testiranje forenzičkih alata

Ekstrakcija i izgradnja čvrstih digitalnih dokaza koji optužuju, ili oslobađaju osumnjičenog i svedočenje pred sudom, krajnji su ciljevi digitalne forenzičke istrage, akvizicije i analize podataka. Da bi sud prihvatio digitalni dokaz, forenzičar mora biti spreman da, po zahtevu sudije, testira i vrednuje forenzički softverski alat sa kojim su dokazi procesirani u celom lancu istrage.

Na raspolaganju su određeni alati za validaciju forenzičkog softvera, koji omogućavaju da forenzičar razvije sopstvenu proceduru za validaciju i testiranje korišćenog forenzičkog alata.

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

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

8.5.1 Razvoj procesa validacije forenzičkih alata

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

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

8.5.2 Proces testiranja softverskih forenzičkih alata

Posle razvoja *specifikacije kategorije alata* i izbora alata, tim za testiranja izvršava sledeće aktivnosti u procesu testiranja alata:

- nabavlja alat za testiranje,
- revidira celu dokumentaciju,
- selektuje relevantne slučajeve za testiranje, zavisno od nominalnih karakteristika alata,
- razvija strategiju testiranja,
- testira alat,
- piše izveštaj o testiranju,
- supervizorsko telo pregleda izveštaj o testiranju,
- isporučioци/proizvođači alata pregledaju izveštaj o testiranju,
- isporučioци/proizvođači postavljaju alat na web stranicu,
- nadležni entitet postavlja izveštaj o testiranju na web lokaciju.

NIST je razvio opšti pristup za testiranje kompjuterskih forenzičkih alata, sa opštim kriterijumima za testiranje opisanim u, [29]. Generalno, nedostaju standardi, ili specifikacije koje opisuju što forenzički alati treba da rade i šta treba da imaju da bi prošli strogu proceduru pravosudnog procesa. NIST kriterijumi za validaciju i testiranje forenzičkih alata bazirani su na standardnim metodama testiranja *ISO 17025 - Kriterijumima za testiranje komponenti za koje ne postoje standardi*. Forenzička laboratorija mora zadovoljavati sledeće kriterijume i održavati preciznu evidenciju:

- *Uspostaviti kategorije kompjuterskog forenzičkog alata*: grupisati softverske alate prema ekspertski specifikovanim kategorijama, na primer, forenzički alati dizajnirani za izvlačenje podataka, alati za praćenje traga e-mail poruka itd.
- *Identifikovati zahteve za svaku kategoriju kompjuterskih forenzičkih alata*: za svaku grupu opisati tehničke karakteristike, ili funkcije koje forenzički alati moraju imati u toj kategoriji.

- *Razviti proceduru testiranja za verifikaciju alata*: na bazi zahteva razviti proceduru za testiranje kojom se dokazuje, ili opovrgava navedena mogućnost forenzičkog alata u odnosu na zahteve. Na primer, forenzički alat za oporavak podataka mora biti sposoban da izvuče podatke iz RAM *slack* prostora fajla.
- *Identifikovati slučaj za testiranje*: pronaći i razviti tipove slučajeva za ispitivanje sa forenzičkim alatom. Identifikovati informacije za izvlačenje iz uzorka diska, ili drugog medija. Na primer, koristiti *imidž* zatvorenog test fajla koji je generisan sa poverljivim forenzičkim alatom za testiranje novog forenzičkog alata u istoj kategoriji i videti da li su rezultati isti.
- *Uspostaviti i razviti metod testiranja*: razmatrajući namenu i dizajn alata, specificovati metod kako testirati forenzički alat i kakve instrukcije treba da ga prate.
- *Izveštaj o rezultatima testiranja*: opisati rezultate testa u izveštaju koji je u skladu sa ISO 17025 standardom, koji zahteva da izveštaj o testiranju mora biti tačan, jasan, nedvosmislen i objektivan.

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

NIST je razvio nekoliko alata za evaluaciju forenzičkih alata za uzimanje *imidža* diskova *FS-TST (Forensic Software Testing Support Tools)* koji ispituje kapacitet forenzičkog alata za uzimanje bit-po-bit kopije diska. CFTT tvrdi da sledeći programi za testiranje napisani u *Borland C++ 4.5* programskom jeziku mogu raditi sa *MS DOS 6.3 OS*:

- *DISKWIPE*: inicijalizuje disk za testiranje na predefinisane vrednosti za testiranje.
- *BADDISK*: simulira loše sektore na disku zamenom *Interrupt13*.
- *BADX13*: kreira loše sektore na proširenom BIOSu diska, sektori se listiraju u LBA formatu.
- *CORUPT*: korumpira jedan bit u specificovanom fajlu i proverava da li će ga forenzički alat detektovati.
- *ADJCMP*: upoređuje sektore prema sektoru sa dva diska različitih veličina, tj. prilagođava i upoređuje sektore za diskove koji imaju različite geometrije.
- *DISKCMP*: upoređuje dva diska i određuje da li su stvarno identični, kada su kopirani sa forenzičkim alatom za uzimanje bit-po-bit imidža.
- *PARTCMP*: proizvodi SHA1 heš za celu particiju.
- *DISKHASH*: proizvodi SHA1 heš za ceo disk.
- *SECHASH*: proizvodi SHA1 heš za specificovan sektor.
- *LOGCASE*: loguje informacije iz slučaja testiranja u fajl.
- *LOGSETUP*: obezbeđuje informacije za konfigurisanje izvršnog diska za testiranje.
- *PARTLAB*: štampa particionu MFT tabelu diska za testiranje.
- *DISKCHG*: menja podatke na disku i određuje da li se ta promena detektuje sa testiranim forenzičkim alatom.
- *SECCMP*: upoređuje sektore da bi se vrednovala kopija podataka.
- *SECCOPY*: dopušta forenzičaru da kopira specifičan sektor.

Drugi NIST-ovi program *NSRL* namenjen je za sakupljanje heš vrednosti fajlova svih komercijalno raspoloživih programskih aplikacija i sistemskih programa. U *NSRL* repozitorijumu primarno se koristi SHA-1 algoritam za generisanje skupa digitalnih potpisa, poznatog kao *referentni skupi podataka - RDS (Reference Data Set)*. SHA-1 algoritam za heširanje obezbeđuje viši stepen tačnosti od drugih metoda heširanja (*MD5* i *CRC-32*).

Ovim se smanjuje broj poznatih fajlova uključenih u ispitivanje diska i ostaju samo nepoznati fajlovi. RDS se može koristiti i za identifikaciju loših poznatih fajlova uključujući one sa ilegalnim sadržajem (dečija pornografija, virusi i sl.).

8.5.3 Procedura za validaciju forenzičkog alata

Izvlačenje i ispitivanje dokazujućih podataka sa jednim alatom.

Verifikacija dobijenih rezultata izvršavanjem istih zadataka sa sličnim softverskim forenzičkim alatom.

Za zadovoljenje kriterijuma za validaciju forenzičkog softverskog, ili hardverskog alata, potrebno je koristiti najmanje dva alata. Analitički alat za upoređivanje rezultata primene oba forenzička alata, mora biti dobro ispitan i verifikovan. Forenzičar mora dobro poznavati korišćeni forenzički alat i imati poverenje u njegove performanse, u slučaju zahteva sudije za neko obrazloženje.

Kao najjednostavniji metod za verifikaciju novog forenzičkog alata i upoređivanje rezultata je korišćenje disk editora, kao što je *Norton DiskEdit*, *HexWorkShop* ili *Win Hex*, koji omogućavaju čitanje podataka u sirovom formatu, tipično prikazuju fajlove, hedere fajlova, fajl *slack* prostor, RAM *slack* i druge podatke na fizičkom disku. Problemi mogu nastati kod ispitivanja kompresovanih fajlova (.ZIP ili .PST MS Outlook fajlova).

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

1. Izvršiti ispitivanje digitalnih dokaza sa nekim GUI forenzičkim alatom.
2. Izvršiti isto ispitivanje sa disk editorom (*Win Hex* ili *HexWorkShop*) i verifikovati da li GUI forenzički alat vidi iste podatke na istom mestu na testiranom, ili imidžu osumnjičenog diska.
3. Kada se fajl oporavi, odrediti heš vrednost u GUI alatu i u disk editoru, a zatim uporediti vrednosti i verifikovati integritet fajla.

U većini slučajeva *FTK* i *EnCase* forenzički alati služe kao referentni pouzdani alati za verifikaciju drugih forenzičkih alata, jer su široko priznati u pravosudnim sistemima brojnih država.

Postoje brojni forenzički alati koji mogu uspešno dopuniti kapacitete *FTK* i *EnCase* alata i treba ih koristiti.

Ažuriranje zakrpe (fiksiranje, pečovanje), ili nadogradnja postojećeg alata, potrebno je takođe verifikovati, da bi se sprečila korupcija digitalnih dokaza. Ako se utvrdi da novo fiksiranje, ili nadogradnja nisu pouzdani, taj se alat ne može koristiti za forenzičku akviziciju i analizu digitalnih podataka, dok se problem ne otkloni. Prva mogućnost je da se generiše izveštaj o grešci i dostavi proizvođaču, koji treba da dostavi novu fiksiranu zakrpu. Sledeći korak je nova runda testiranja validnosti pečovanog/nadograđenog alata.

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

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

8.6 Značaj poznavanja izvornog koda forenzičkih alata

Da bi neki digitalni dokaz bio prihvatljiv pred sudom, dokaz mora biti *relevantan* (ima dokazujuću/opovrgavajuću vrednost) i *pouzdan* (nepromenjen, verifikovano autentičan). Pouzdanost i validnost generisanog dokaza, kakav je izlaz iz digitalnog forenzičkog alata, određuje sudija u predistražnom postupku na bazi bazičnih principa za prihvatljivost naučno zasnovanih digitalnih dokaza (tzv. *Daubert* principi, SAD) pred sudom, koji obuhvataju četiri opšte kategorije:

- *Testiranje*: da je procedura primene forenzičkog alata testirana.
- *Stepen greške*: da je poznat stepen grešaka procedure primene forenzičkog alata.
- *Revizija*: da je procedura primene forenzičkog alata objavljena i višestruko revidirana.
- *Prihvatljivost*: da je procedura primene forenzičkog alata generalno prihvaćena u relevantnoj naučnoj zajednici.

Kako je većina poznatih alata za digitalnu forenzičku akviziciju/analizu razvijena sa komercijalnim interesom, malo je verovatno da će proizvođači objaviti ceo izvorni kôd. Imajući na umu definiciju prihvatljivosti digitalnih forenzičkih alata, alati sa zatvorenim izvornim kôdom mogu pružiti više praktičnih rešenja nego neki alati sa 100% poznatim izvornim kôdom. Softverski forenzički alati uslovno se dele u dve glavne kategorije alata, za: *ekstrakciju* i *prezentaciju* digitalnih dokaza. Alati za ekstrakciju procesiraju podatke i ekstrahuju relevantan podskup dokazujućih podataka. Na primer, neki alat za ekstrakciju može procesirati fajl sistem *imidža* osumnjičenog diska i na izlazu dati sadržaj fajla i opisne podatke, kao što su poslednji datum pristupa. Prezentacioni alati aranžiraju podatke iz ekstrakcionog alata u forenzički čitljiv i koristan format. Na primer, neki ekstrakcioni alat može analizirati *imidž* fajl sistema i na izlazu dati imena i vremena za svaki fajl, a prezentacioni alat može prikazati iste podatke, sortirane po direktorijumima, kako većina korisnika gleda fajl sistem. Drugi alat za prezentaciju može prikazati iste podatke, ali sortirane po vremenima modifikacije, pristupa i kreiranja (*MAC*) za kreiranje vremenske linije aktivnosti. Dakle, prikazivani su isti podaci, ali sa različitim pogledom primenjenog prezentacionog alata. Većina savremenih alat (*FTK*, *EnCase*, *iLook* i dr.) integriše i izvršava obe funkcije, ali postoje i jednofunkcionalni alati.

Ako su ekstrakcioni alati otvorenog izvornog kôda, a forenzičar ima pristup izlazu ovog apstrakcionog sloja, tada on može verifikovati izlaz prezentacionog alata. Zbog toga prezentacioni alat može ostati sa zatvorenim izvornim kôdom, ali sa objavljenim dizajnom i funkcionalnostima. Pored toga, mnogi savremeni forenzički alati za analizu bazirani su na prezentaciji rezultata. Na primer, gledanje heša u bazi podataka, rešenja konfiguracije preko mreže, poređenje tipova fajlova prema ekstenziji i pretraga po ključnoj reči, akcije su koje se događaju posle ekstrakcije podataka iz *imidža* fajl sistema. Zbog toga, kreiranje standardnih tehnika ekstrakcije podataka, neće ograničiti kompetentnost softverskih kompanija. Korisnički interfejs, karakteristike i podrška, faktori su koji razlikuju proizvođače/snabdevače alata. U stvari, ovo omogućava da se proizvođači usredsrede na inovativne prezentacione tehnike za analizu fajl sistema i poboljšanje alata za ekstrakciju i prezentaciju u manje zrelim oblastima primene, kao što su mrežna forenzika i redukcija podataka log fajlova.

Objavljivanjem izvornog kôda kroz ekstrakcione alate sa otvorenim izvornim kôdom, interesna zajednica digitalnih forenzičara može ispitati i vrednovati procedure koje se koriste za generisanje digitalnih dokaza. Ovaj model omogućava precizan proračun stepena greške, zato što se svi podaci koji se odnose na fiksiranje bagova alata za ekstrakciju mogu objaviti, a stabilan kôd se može kreirati prilično brzo, na bazi metodologije testiranja. Pored toga stepen greške takvog alata biće isti, zato što jedinu razliku unose bagovi u interfejsu i prezentaciji podataka. Zato će i proizvođači biti više zainteresovani da učestvuju u naporima za proračun stepena grešaka.

Koncept forenzičkih alata sa otvorenim izvornim kôdom bitno se razlikuje od koncepta drugih softvera sa otvorenim izvornim kôdom. Cilj većine softvera sa otvorenim izvornim kôdom je da se dobije veliki broj istraživača koji mogu pristupiti i ažurirati kôd. Cilj lansiranja forenzičkih alata sa otvorenim izvornim kôdom je da obezbedi lakši pristup za reviziju i testiranje alata, a ne za ažuriranje. Ograničena grupa istraživača ima ograničen pristup za razvoj i ažuriranje alata, a kôd se objavljuje sa digitalnim potpisom, za zaštitu integriteta.

Digitalni forenzički alati koriste se istovremeno kao radni alati zaposlenih forenzičara, osuđivanje kompjuterskih kriminalaca i demonstraciju nevinosti osumnjičenih. Sva ova pitanja su suviše ozbiljna da bi se softverski forenzički alati tretirali na isti način kao ostali softverski proizvodi. Drugim rečima, tržište forenzičkih alata ne treba da dominira, na bazi sakrivanja proceduralnih tehnika i izvornog kôda. Digitalna forenzička nauka sve više sazreva i zahteva neprekidno održavanje na visokim standardima. Korišćene procedure treba jasno objaviti, revidirati i diskutovati u interesnoj zajednici. Dostupnost alata za analizu široj populaciji korisnika, vrlo verovatno će povećati njihov kvalitet i iskoristivost. Sledeći stepen je da se poveća poverenje u softverske forenzičke alate kroz publikacije, revizije i formalna testiranja.

9 Digitalna forenzika mobilnih telefona i tablet računara

9.1 Mobilni telefoni

Mobilni telefon predstavlja multifunkcionalni telekomunikacioni uređaj koji je postao neodvojivi deo svakodnevnice svakog poslovnog čoveka. U poslednje 2 godine došlo je do velike popularizacije pametnih telefona (Smart Phone) a kao glavni predstavnik pojavio se prvo Apple sa svojim iPhone modelima a onda je u igru usao i Google sa svojim Android baziranim telefonima i uzeo potpuni primat na tržištu. Takođe među manje zastupljenima su Samsung sa svojim Bada operativnim sistemom i BlackBerry takodje sa svojih operativnim sistemom.

Mobilni telefoni danas mogu da čuvaju veliku količinu podataka vezanih za komunikacije (SMS i poruke elektronske pošte), mogu se upotrebljavati i za bežični pristup Internetu (GPRS, EDGE, 3G, Wi-Fi), multifunkcionalnost telefona već dostiže mogućnosti personalnih računara, ali ide i korak dalje, jer integriše i uređaje kao što su fotoaparati, video kamere, snimači zvuka i uređaji za GPS.

Mobilni telefoni mogu biti sredstvo za izvršenje krivičnog dela (na primer, snimanje dečije pornografije ili zlostavljanja), mogu biti objekat izvršenja (bilo da su ukradeni ili zaraženi zlonamernim softverom) i mogu sadržati dokaze vezane za određeno krivično delo. Zanimljivo je istaći da je u Americi 2006. godine, zabeleženo da je 80% sudskih slučajeva u to vreme imalo neku vrstu digitalnih dokaza povezanih sa mobilnim telefonima.

9.1.1 Digitalni dokazi na mobilnom telefonu

Digitalni dokazi sa mobilnog telefona mogu uz podatke dobijene od operatora mobilne telefonije, da ukažu na detalje kao što su: vreme kada se neki događaj desio, gde su se okrivljeni ili oštećeni nalazili i sa kim su komunicirali; sadržaji komunikacija SMS i MMS servisima, koji mogu da ukažu na to kako je krivično delo planirano ili izvršeno; imena ili nadimci pronađeni u imeniku mobilnog telefona, pretplatnički brojevi koji su im dodeljeni, kao i adrese elektronske pošte, a koji mogu da identifikuju lica, posebno kada se radi o organizovanoj grupi.

Prilikom postupka akvizicije mora se voditi računa o tome da ne sme doći do menjanja podataka sadržanih na mobilnom telefonu ili na mediju za skladištenje (memorijska kartica). Međutim da bi se podaci prikupili sa mobilnog telefona, on mora da bude aktivan, a uključivanje uređaja ili njegovo povezivanje sa računarom će najverovatnije promeniti određene podatke. Ukoliko je menjanje podataka neizbežno potrebno je to svesti na minimum i obavezno sve dokumentovati.

Bitno je istaći da pored interne fleš memorije, mobilni telefoni poseduju i druge vrste memorija, poput memorijskih i SIM kartica, čija forenzika se može vršiti nezavisno. Zbog toga, kada se govori o akviziciji podataka sa mobilnih telefona, pre svega se misli na prikupljanje podataka sa memorije samog uređaja.

Alati za forenziku mobilnih telefona



Slika 70 [4]

Neki od najpoznatiji forenzičkih alata za mobilne telefone su:

1. *Cellebrite Universal Forensics Extraction Device (UFED)*
2. *Oxygen Forensic Suite 2012*
3. *Paraben Device Seizure*
4. *MicroSystemation XRY*
5. *Logicube CellDEK*



Slika 71 [5]

Navedeni alati koriste iste protokole kao i neforenzički alati proizvođača, ali ne implementiraju komande koje eksplicitno modifikuju sadržaj memorije mobilnog telefona. Svi navedeni alati imaju mogućnost akvizicije podataka i sa GPS uređaja, ali i sa tablet računara poput iPad-a i Galaxy Tab-a, što je prirodno ako se uzme u obzir da ovi uređaji koriste operativne sisteme iOS i Android, koji se nalaze i na mobilnim telefonima.

Proizvođači neprestano prate razvoj novih modela i svoju bazu neprestano dopunjuju novim modelima koji se pojavljuju na tržištu.

I na kraju da zaključimo priču sa ovim, definitivno je da je i da će u budućnosti mobilni telefon biti veoma koristan izvor dokaza jer pojavom Cloud servisa i tablet računara koje možemo smatrati nekom vrstom naprednijeg mobilnog telefona jasno je da će sve veći deo komunikacije biti prebačen sa klasičnih računara na ove uređaje.

Takođe hoću da napomenem da postoji i forenzika koja se bazira na akviziciji putem određenih komunikacionih servisa i agenata kao što su AT Command Set, SyncML ili OBEX, koji su već zastareli, ili fabrički protokoli poput Nokia FBUS-a ali oni nisu deo ovog teksta i možda ću napisati poseban post o njima kao i o forenzici koja se bazira na direktnom pristupu memoriji i predstavlja nazahtevniji način akvizicije podataka i neophodna su određene hardverske intervencije kao što su skidanje čipa sa ploče, korišćenje porta za JTAG test (Joint Test Action Group) ili upotreba alata za flešovanje (flasher tools).

-Studija slučaja kompjuterskog kriminala- Nikola Milenković¹, Gojko Grubor²

Apstrakt

Digitalna forenzička istraga mobilnih digitalnih uređaja i smart telefona postaje novi izazov za forenzičare. Operativni sistemni, fajl sistemi i hardverska rešenja bitno zavise od proizvođača, a na raspolaganju je relativno mali broj dostupnih alata otvorenog koda. To je posebno problem za korporacijsku istragu, gde menadžment pokušava svojim resursima da reši tekući kompjuterski incident. U najvećem broju slučajeva kompjuterskog incidenta ili kriminala organizacije pokušavaju same rešiti problem, organizujući sopstvenu istragu pre donošenja odluke da li slučaj prijaviti zvaničnim organima istrage. Interna istraga koju treba da vodi kompetentan digitalni forenzičar u timu za upravljanje kompjuterskim incidentom treba da vodi istragu u skladu sa standardnim procedurama i principima digitalne forenzičke istrage, kao da će slučaj završiti na sudu. U ovom radu opisana je studija slučaja istrage Android smart telefona u organizaciji koja je uvela mobilni pristup lokalnoj bazi podataka za izvršne menadžere. U istrazi su korišćeni alati otvorenog koda i demo verzija specijalizovanog komercijalnog alata za forenzičku istragu Android platforme.

1. Slučaj interne forenzičke istrage

Mladi menadžer firme *Andropharm* koja se bavi kupovinom akcija i transakcijom novca svojih bogatih korisnika dobio je telefon nove generacije tzv. Smartfon, po odluci glavnog menadžera. Telefon je namenjen za mobilni pristup lokalnoj bazi podataka, ali ga je menadžer koristio i za lične potrebe. Često je skidao muzičke i druge sadržaje sa Interneta i pratio više društvenih mreža.

U organizaciji je svest o potrebi zaštite bila na veoma niskom nivou. Dinamika poslovanja i nekompetentnost glavnog menadžera najviše su doprinele takvom stanju. Kako je službena upotreba smart telefona u organizaciji bila na samom početku, tim za informatičku podršku nije adekvatno reagovao zbog nedostatka specijaliste za zaštitu. Zaštitu lokalne mreže obavljao je administrator zaštite. Tako izvršni menadžeri ni u jednom trenutku nisu upozoreni da je potrebna antivirusna zaštita mobilnih telefona kao i izbegavanje poseta sumnjivim veb sajtovima i intenzivnog praćenja društvenih mreža.

Menadžment firme je kroz nekoliko meseci primetio da im klijenti naprasno prelaze u konkurentsku firmu. U kratko vremenskom periodu firma je došla na rub bankrotstva. Sumnjajući da među njima postoji neko ko je prenesi poslovne tajne podatke konkurentskoj firmi, vlasnici su unajmili privatne istražitelje da provere kako je došlo do curenja osetljivih. Istraga je utvrdila da su udaljeni pristup serveru baze podataka imali samo vlasnik i dva izvršna menadžera. Oni su redovno preko smart telefona razmenjivala podatke o akcijama koje treba kupiti ili prodati za njihove klijente. Istražitelji su utvrdili da nije niko od radnika izdao firmu i odao tajne podatke, jer su bili previše vezani za firmu, a i pri tom su potpisali NDA (*Non Disclosure Agreement*) ugovor koji ih obavezuje da, u koliko otkriju osetljive informacije firme neovlašćenom licu, plate veliko obeštećenje firmi. Zbog svega ovoga istražitelji su zaključili da informacije nisu otkrili ljudi nego tehnologija. Oni su sugerisali vlasniku firme da iznajmi digitalnog forenzičara da otkrije uzrok oticanja osetljivih informacija iz firme.

¹ Nikola Milenković, master student, Singidunum University

² Gojko Grubor, PhD, Assistant professor, Singidunum University

1.1. Forenzička istraga

Vlasnik firme je sa skepticizmom prihvatio ovaj savet i iznajmio kao konsultanta digitalnog forenzičara koji je i ranije davao neke usluge firmi na zahtev administratora mreže. Digitalni forenzičar je uz pomoć tima za informatičku podršku detaljno ispitivao sve računare i mrežne uređaje koji se koriste u firmi. Kada je došao red i na mobilne telefone forenzičar je otkrio da se na smart telefonu jednog od izvršnih menadžera, nalazi trojanac keylogger prikriven rutkit tehnikom, koji je pristupnu lozinku za lokalnu bazu podataka poslao napadaču i omogućio mu pristup.

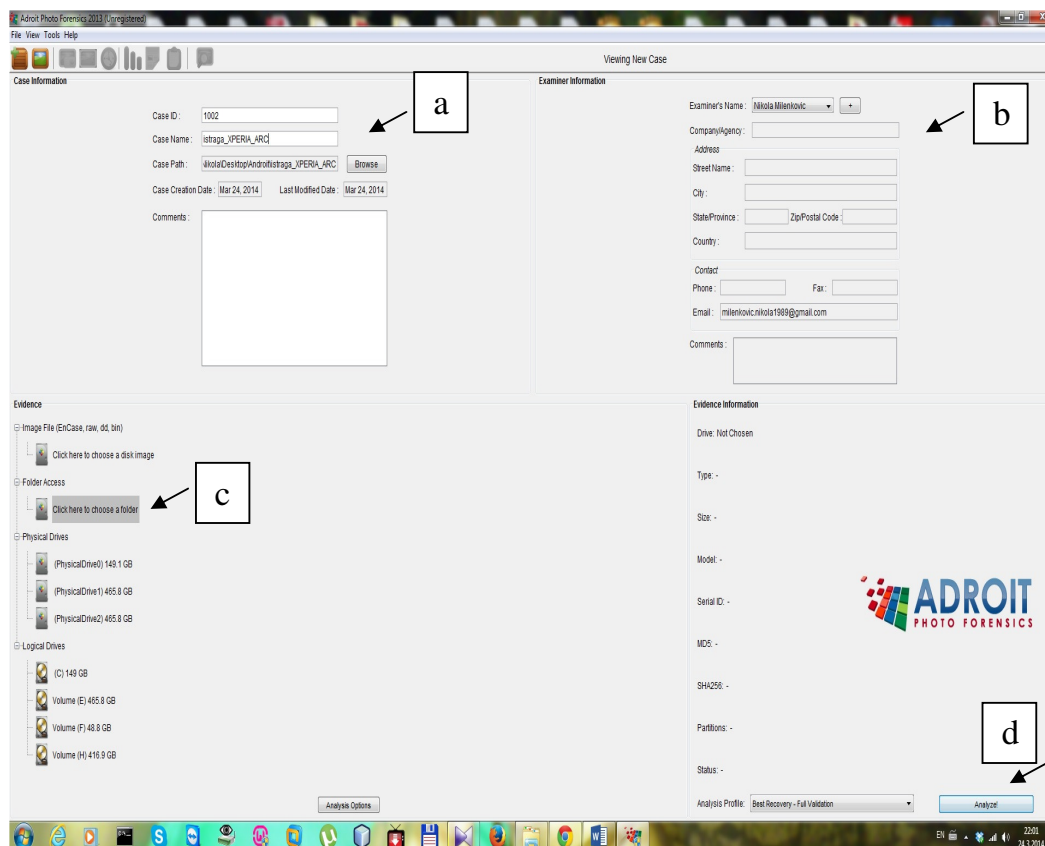
Za analizu telefona korišćen je program *“Belkasoft Evidence Center Ultimate”*. Program je instaliran na forenzičkom računaru na kome je izvršena forenzička akvizicija i analiza. Ispitivani Android telefon je priključen na USB port forenzičkog računara, preko softverskog blokatora upisivanja *“USB Write Blocker”* za sprečavanje upisivanja u ispitivani uređaj.



Slika 72: Softverski USB blokator upisivanja

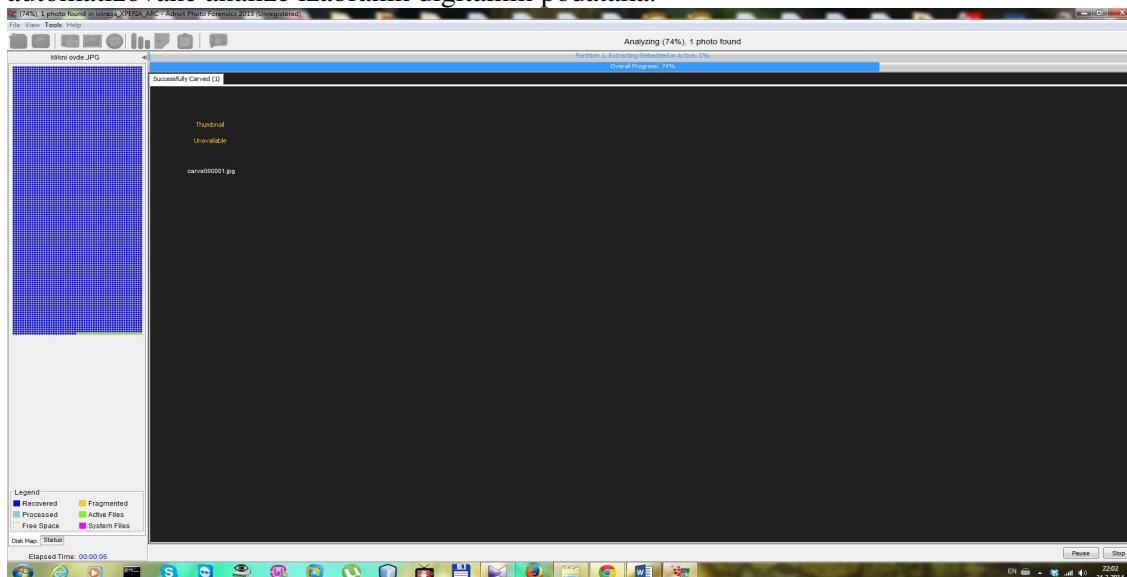
Forenzičar je za prvu aktivnost planirao da utvrdi na koji način je došlo do instalacije trojanca. Jedan od najpopularnijih i najlakših metoda upada trojanca u digitalni uređaj je preuzimanjem interesantnih slika i muzičkih sadržaja. Za ovu prvu proveru forenzičar je koristio demo verziju komercijalnog alata *„Adroit Photo Forensics 2013“* (USD 1.999).

Na slici 1. je prikazan početni prozor samog programa. Na vrhu strane u levom uglu nalaze se podaci, kao što su *„Case ID“*, *„Case Name“*, *„CaseID“* itd (a). koje popunjava forenzičar za evidentiranje slučaja. Sa desne strane nalaze se podaci analitičara koji se, takođe, moraju popuniti (b). Najbitniji deo se nalazi na levoj strani prozora, gde forenzičar podešava koji folder, sliku, ili partciju želi da istražuje. U ovom slučaju forenzičar je odabrao folder sa slikama koje su preuzete sa interneta (c), a u koje vlasnik telefona nije uopšte sumnjao.



Slika 73: Pripremanje programa za analizu

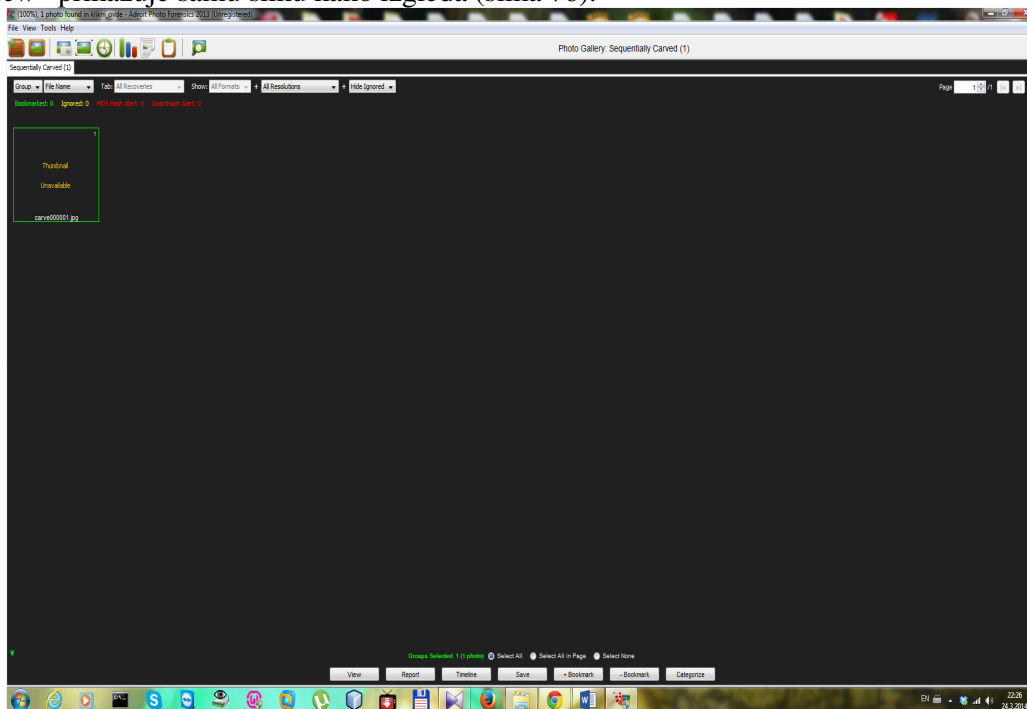
Nakon pripreme i podešavanja izvora za istragu potencijalnih digitalnih dokaza forenzičar na dugme iz donjeg desnog ugla „Analyze!“ (d). Na slici 74. je prikazan prozor automatizovane analize izabranih digitalnih podataka.



Slika 74: Process automatizovane analize digitalnih podataka

U ovom fazi program obavlja sav posao dok forenzičar samo nadgleda da se ne dogodi neki problem sa samim programom.

Na slici 75. Pokazan je kraj analize uređaja. Kako se na slici može i videti, pronađena je 1 skrivena (*hidden*) slika u ovom folderu! Na dnu ekrana u centralnom delu može se videti par komandi koje mogu biti veoma interesantne za ispitivanje posle programske analize. Dugme „View“ prikazuje samu sliku kako izgleda (slika 76).



Slika 75: Kraj automatizovane analize



Slika 76: Analizom otkrivena slika

Još jedna veoma interesantna opcija na prozoru (slika 75) je komanda „Report“, koja daje izveštaj o potpunom pregledu forenzičke analize (slika 77)

Case Information	Sequentially Carved Details	
Analysis Options	carve000001.jpg	
Examiner Information		
Evidence Information	File Name	carve000001.jpg (auto-generated)
Recovery Statistics	Category	Not Selected
Category Profile	Hash Alert	No
Sequentially Carved (1) Details	File Size	105472 bytes (103 KB)
Sequentially Carved File Information	File Type	JPEG/JPG
	Resolution	0 x 0
	Partition 1	NONAME
	Path	[NONE]
	Creation Date	Demo Version. Register to view.
	Modification Date	Demo Version. Register to view.
	Accessed Date	Demo Version. Register to view.
	File Status	Deleted
	Recovery Process	Sequential Carving
	Validity	Fully Recovered (File is in the correct format)
	MD5	Demo Version. Register to view.
	SHA256	Demo Version. Register to view.
	Cluster Ranges	Starting Cluster 0 Starting Sector Demo Version. Register to view. Cluster Count 206 (1 fragment) Sector Count Demo Version. Register to view. Cluster Ranges 0 - 205 Sector Ranges Demo Version. Register to view.
	EXIF info	
	Camera	
	Model	
	Software	
	Date/Time	
	Original	
	Digitized	
	Thumbnail	Please register to view thumbnail

Slika 77: Izveštaj o analizi

Ovaj izveštaj se može snimiti u pretraživaču (npr. Google Chrome.) i u njemu se nalaze sve informacije koje su pronađeno u folderu. U ovom slučaju to su informacije samo o jednoj slici koja je skrivala maliciozni program i napravila ogroman problem za firmu.

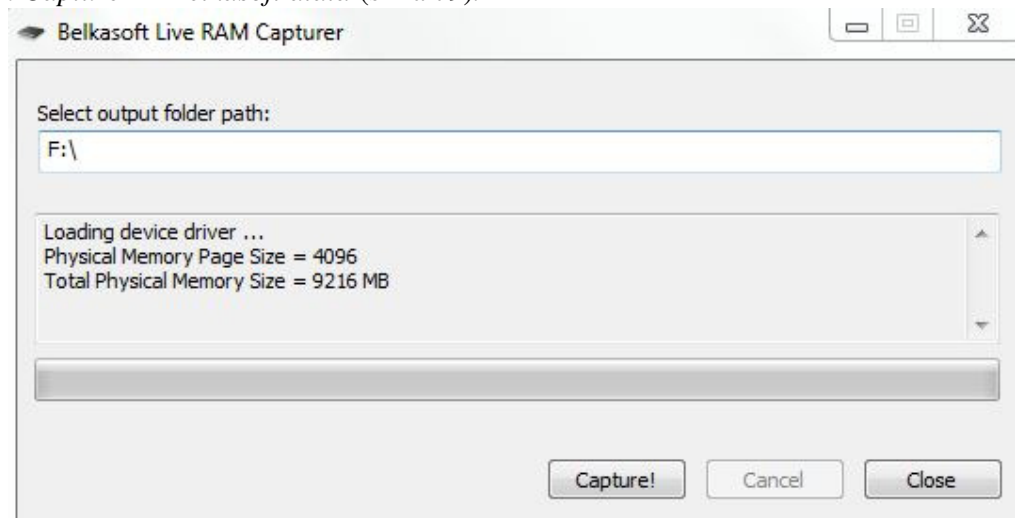
Na samom kraju treba napomenuti da rezultate analize program čuva u folderu koji sami postavite gde želite da bude sačuvan kao što je i pomenuto na početku pripreme za analizu. Ovaj izveštaj je generisan u .txt formatu, što znači da se može otvoriti iz, na primer, NOTEPAD programa. Izveštaj sadrži sve podatke koji su neophodni i osnovne informacije o samoj analizi, analitičaru, heš funkcijama (MD5, SHA 256) itd.

```
[ Monday, March 24, 2014 10:02:36 PM CET ] Case created-----Case ID: 1002Case Name: Case Information-----Case ID: 1002Case Name: istraga_XPERIA_ARCCase Path: C:\Users\Nikola\Desktop\Android\istraga_XPERIA_ARCCase Comments: Nikola MilenkovicCase Creation Date: Mar 24, 2014Case Last Accessed Date: Mar 24, 2014-----Evidence Drive: k1ikni ovde.JPGEvidence ID: Not AvailableEvidence MD5 Hash: Not CalculatedEvidence SHA256 Hash: Not AvailableEvidence Serial Evidence size: 125061 bytesPartition Count: 1-----Partition 1-----Volume Name: NONAMESize: 125061 bytesFree space: 125061 bytesFile system: unknownFile system: Case Initialize: FailCluster Size: 512 bytesFile system offset: 0 bytes-----Case Analysis using: Adroit Photo Forensics 3.2b-----[ Monday, March 24, 2014 10:03:00 PM CET ] Case options:-----Case Analysis options:-----Use file system to set offset, clusters and active files: trueRecover active photos from file system: trueValidate active photos found: trueIdentify active photos by header signature: trueCarve photos using file system logs (NTFS, FAT - Logcarving): trueCarve photos that are sequentially stored (Sequential carving): trueCarve photos that are fragmented (Smartcarving): trueLimit each Smartcarving cycle to: 1200Size Carve based on unallocated space (BMP, TIFF, RAW formats): trueDrive/Partition Format Detection (Offset & Cluster Size Analysis settings): Offset: 0 bytes, Cluster Size: 512 bytesIgnore photos smaller than 0 bytes: falseIgnore duplicate photos based on MD5 stored in the case: falseIgnore photos based on MD5 stored in the ignore DB: falseRecover embedded photos in active files: trueValidate embedded photos in active files: trueRecover embedded photos in carved files: trueValidate embedded photos in carved files: trueAnalyze all file types for embedded photos: trueEmbedded in unallocated space: Scan every byte in a sector for photoscreate preview thumbnails by scaling photo instead of embedded thumbnail: falseGenerate MD5 hash of each photo: trueGenerate SHA1 hash of each photo: falseGenerate SHA256 hash of each photo: falseGenerate MD5 hash of evidence: falseGenerate SHA1 hash of evidence: falseGenerate SHA256 hash of evidence: falseWrite detailed information of each photo to log: falseNo category profile was selected.[ Monday, March 24, 2014 10:03:00 PM CET ] Partition Analysis DetailsUsed Parameters: Partition 1-----Used Cluster count: 245Used Cluster size: 512 bytesUsed Drive size: 125061 bytesUsed offset: 0 bytes[ Monday, March 24, 2014 10:03:00 PM CET ] Case updated-----Case ID: 1002Case Name: Case Information-----Case ID: 1002Case Name: istraga_XPERIA_ARCCase Path: C:\Users\Nikola\Desktop\Android\istraga_XPERIA_ARCCase Comments: Nikola MilenkovicCase Creation Date: Mar 24, 2014Case Last Accessed Date: Mar 24, 2014-----Evidence Drive: k1ikni ovde.JPGEvidence ID: Not AvailableEvidence MD5 Hash: Not CalculatedEvidence SHA256 Hash: Not AvailableEvidence Serial Evidence size: 125061 bytesPartition Count: 1-----Partition 1-----Volume Name: NONAMESize: 125061 bytesFree space: 125061 bytesFile system: unknownFile system: Case Initialize: FailCluster Size: 512 bytesFile system offset: 0 bytes-----Case Analysis using: Adroit Photo Forensics 3.2b-----[ Monday, March 24, 2014 10:03:00 PM CET ] Analysis complete-----Time taken for analyzing case: 00:00:16
```

Slika 78: Izveštaj o analizi

1.2. Ispitivanje klona Android telefona

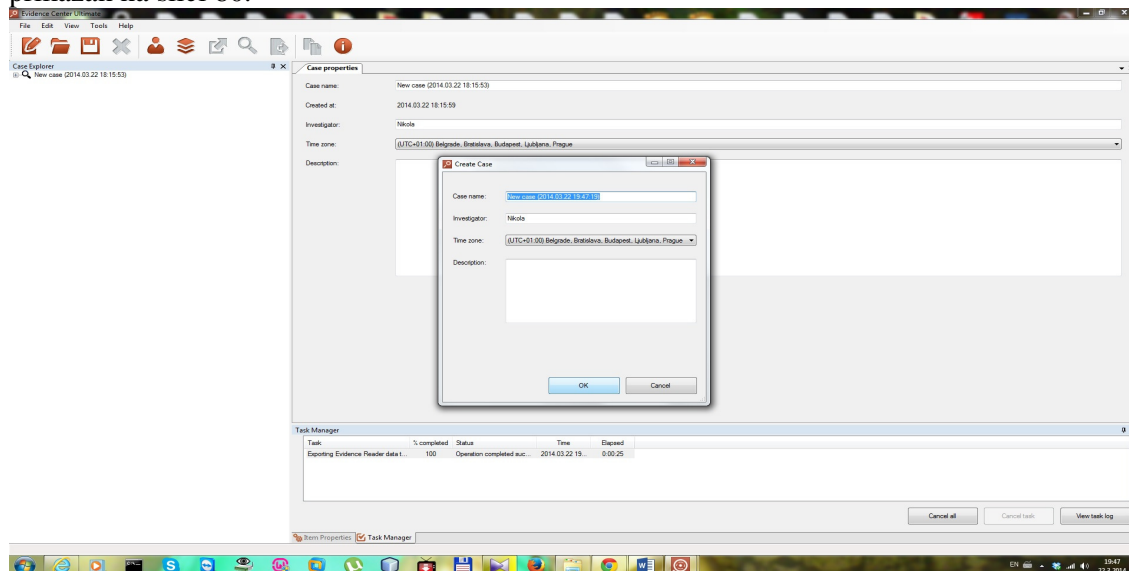
Posle ove analize forenzičar je nastavio dalje istraživanje telefona jer je očigledno da vlasnik ovog telefona nije obratio pažnju na bezbednost uređaja. U sledećoj fazi istrage forenzičar je napravio klon uređaja u cilju ispitivanja sadržaja RAM memorije telefona, programom *Ram Capturer* iz *Belkasoft alata* (slika 79).



Slika 79: (Ram capturer)

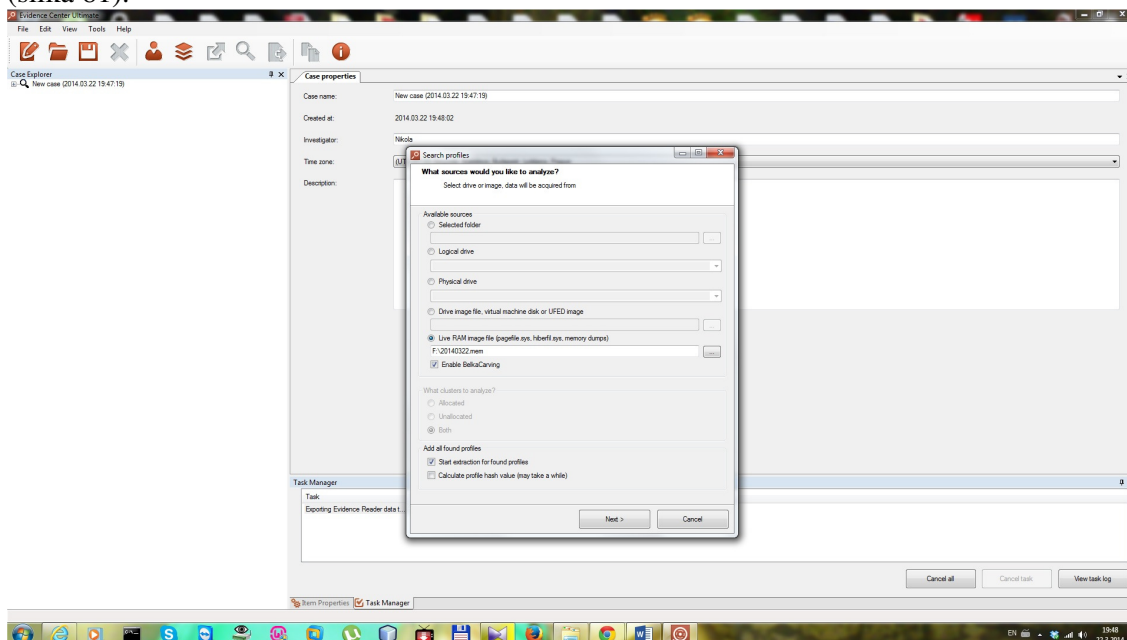
Prethodno je odredio lokaciju na forenzičkom čvrstom disku, na koju će biti sačuvan klon uređaja. Zatim je forenzičar pristupio analizi klona telefona programom "*Belkasoft Evidence Center Ultimate*" i otkrio malver program u fizičkoj memoriji uređaja koji je sakupljao sve podatke i slao na ciljnu mejl adresu hakera.

Klikom na ikonicu *New Case* koja se nalazi u gornjem levom uglu dobije se novi prozor prikazan na slici 80.



Slika 80: (Kreiranje analize)

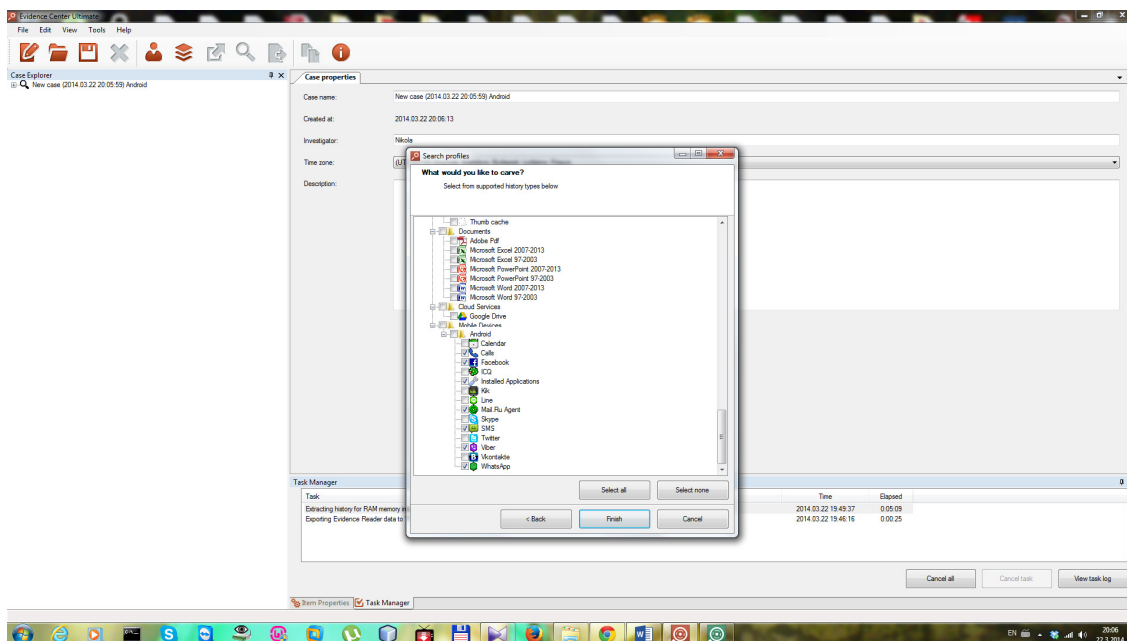
U ovoj fazi forenzičar upisuje ime istraživača i naziv istrage, a zatim bira šta želi istraživati (slika 81).



Slika 81: Dodavanje putanje klona koji se analizira

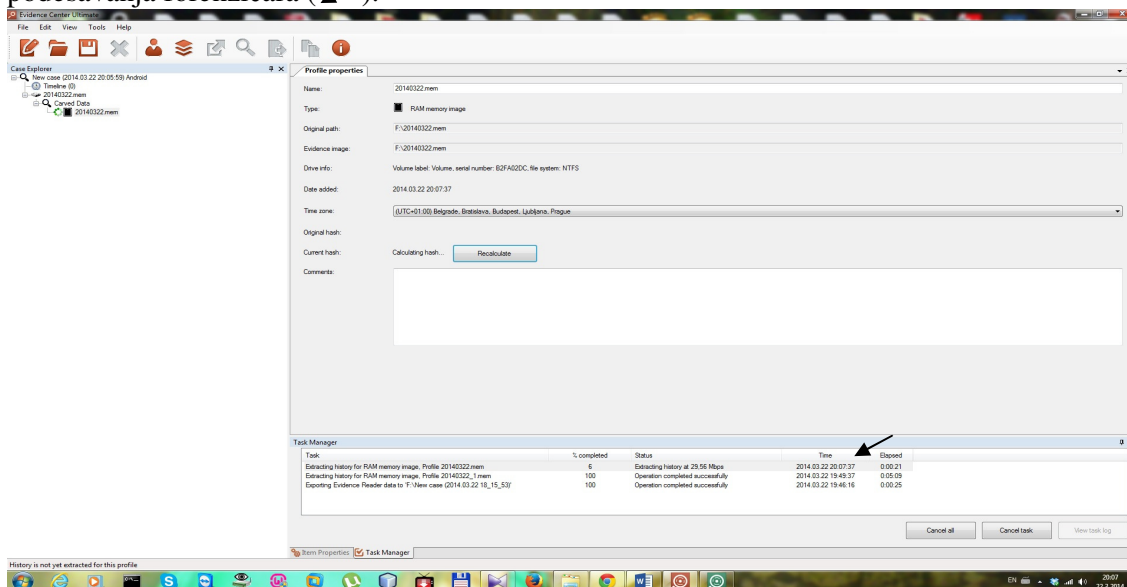
Kao što se može videti na slici 81 u ovoj fazi se može odabrati direktno skeniranje *Hard diska*. Međutim, za potrebe ove analize mora se odabrati klon samog uređaja koji je napravljen u prethodnom koraku.

Na slici 82 forenzičar je pristupio odabiru dela sadržaja koji želi da ispita iz celog klona uređaja.



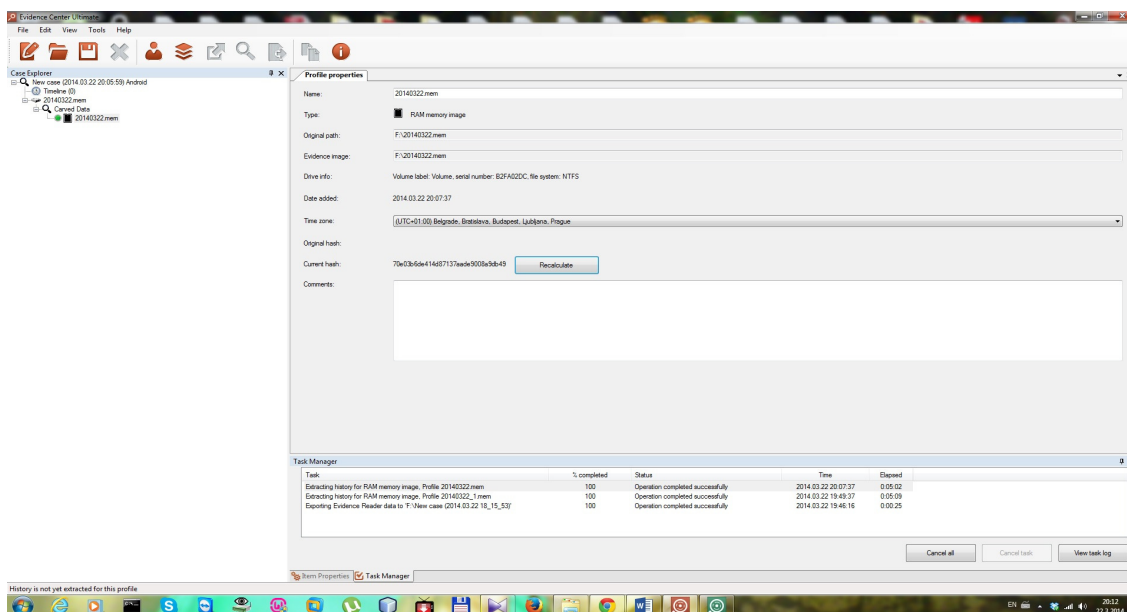
Slika 82: Izbor delova klona za analizu

Dakle, u ovoj fazi forenzičar je izabrao da se skenira samo interni deo operativnog sistema Android telefona, kao što su *pozivi*, *SMS poruke*, *instalirane aplikacije* u kojima je i pronađen malver program, *aplikacije za komunikaciju* popularnom metodom *Voice over IP*, kao što su *Viber* i *WhatsApp*. Na slici 83 je prikazan rad programa nakon svih ovih podešavanja forenzičara (▲).



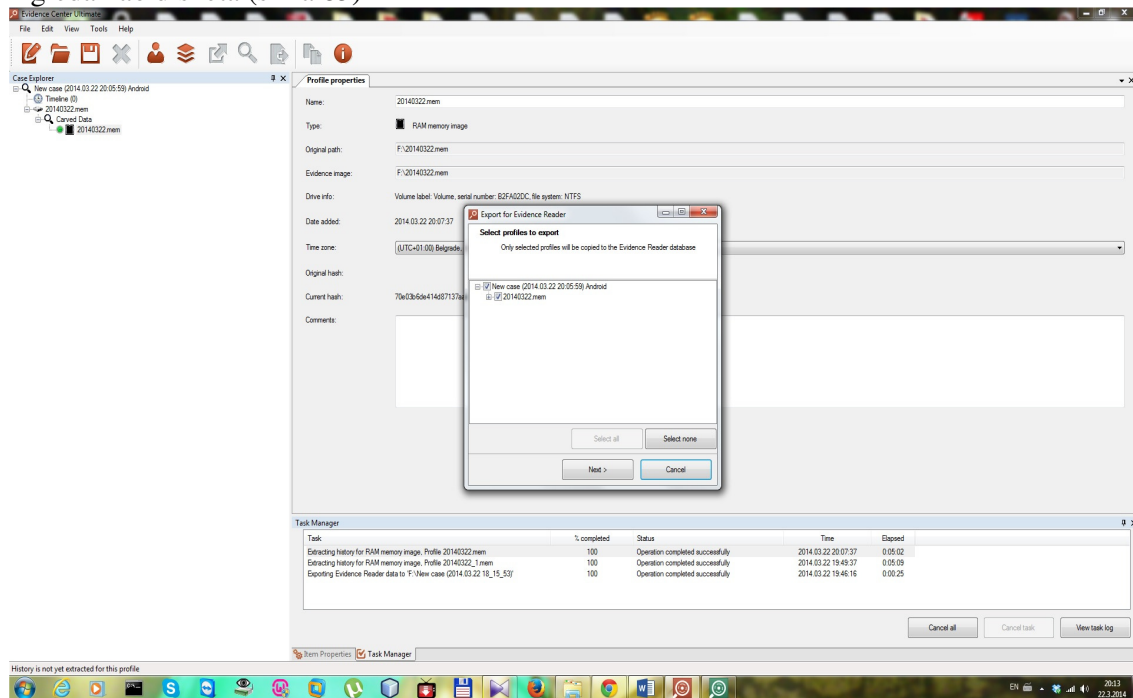
Slika 83: Analiza u toku

U samom podešavanju programa za analizu može se, takođe, postaviti jedna od najbitnijih opcija - da nakon izvršene forenzičke analize alat izračuna *hash* vrednost klona koja mora biti ista kao i heš vrednostna izračunata nakon kloniranja u početku istrage. Posle završetka analize, kao što se može videti na slici 84, ispisana je *hash* vrednost je ista kao i na početku analize, čime je verifikovan integritet ispitivanog sadržaja.



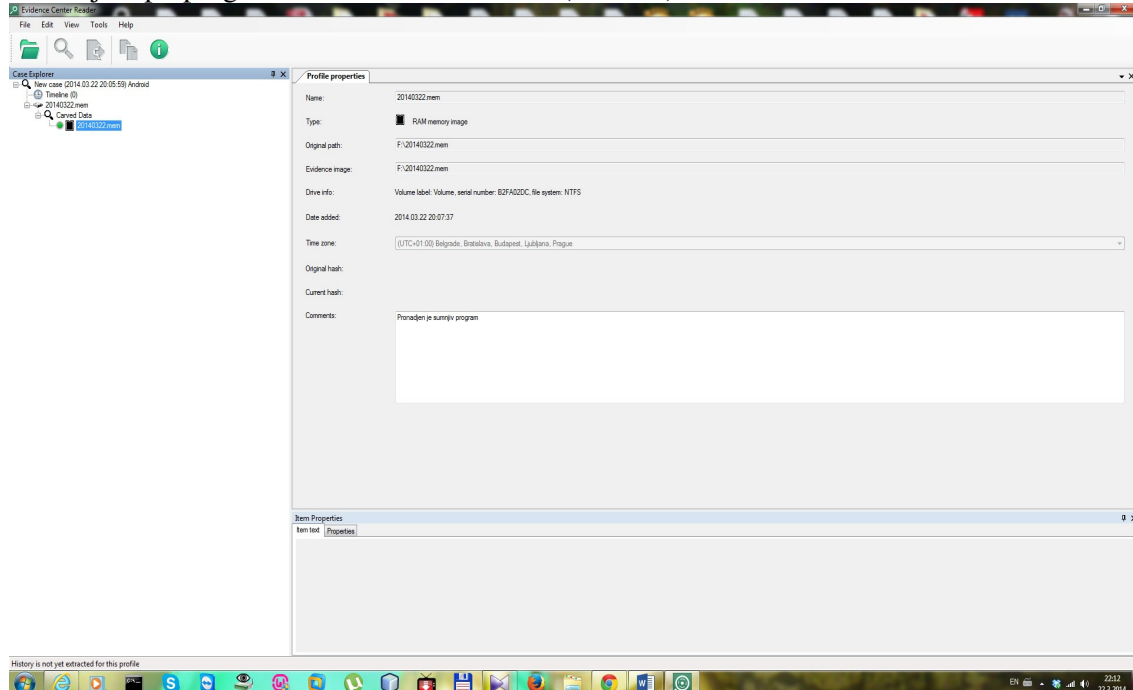
Slika 84: Verifikacija integriteta ispitivanog digitalnog sadržaja

Posle ovoga forenzičar je snimio svoje rezultate na željenu lokaciju klikom na ikonicu koja izgleda kao disketa (slika 85)



Slika 85: Izvoz rezultata analize

Ovim postupkom završena je analiza i prelazi se na postupak pregleda rezultata koji se odrađuje u potprogramu *Evidence ReaderNet* (slika 86).



Slika 86: Pregled rezultata

1.3. Rekonstrukcija slučaja

U izveštaju o forenzičkoj istrazi slučaja, digitalni forenzičar je naglasio da je sva analiza prikazana u radu izvršena pomoću besplatnih alata otvorenog koda i komercijalnog demo alata, a koji su prihvatljivi od strane pravosudnih sistema. Forenzičar je naveo da je napadač preko hakerskog programa (npr. *Faceniff*) pristupio nezaštićenom telefonu menadžera firme i instalirao trojanca *Text Tracker* koji potpuno nezapaženo radi u pozadini telefona, ne troši mnogo memorije i ne usporava uopšte rad telefona. Prilikom instalacije trojanc postavljen je cilj na *mail* na koji trojanac treba da šalje informacije o svim porukama i obavljenim pozivima sa tačnim vremenskim periodom. Forenzičar je, takođe, naveo u izveštaju da nije bilo moguće dokumentovati otkriveni malver zbog smanjene funkcionalnosti demo verzije *Androit* alata. Lokacija i naziv trojanca pojavili su se u alatu svega nekoliko sekundi i alat nije dozvolio dokumentovanje izveštaja analize.

2. Zaključak

U ovoj studiji slučaja opisan je uspešan pokušaj korporacijske forenzike zbog odbijanja menadžmenta firme da angažuje zvanične organe istrage. U prvom redu klasična istraga je utvrdila da nije bilo internog napada, a sam incident nije jasno definisan za otvaranje zvanične istrage. Slučaj je rešen angažovanjem konsultantskih usluga digitalnog forenzičara. Forenzička istraga je vođena sa poštovanjem svih principa i procedura digitalne forenzike sa pretpostavkom da će slučaj završiti na sudu. Rezultate forenzičke analize forenzičar je predao samo glavnom menadžeru (vlasniku) firme. Glavni menadžer je na sastanku kolektiva obavestio zaposlene da nije bilo namernog internog napada i da je u pitanju korupcija mobilnog telefona neopreznog menadžera. Nažalost, zbog nedostatka politike zaštite mobilnih telefona u firmi, neopreznog menadžer nije mogao biti sankcionisan, čak ni disciplinskom merom, bez obzira na učinjenu štetu. Glavni menadžer je zbog učinjene štete odobrio izradu politike zaštite i nabavku antivirusnih programa i obaveznu zaštitu svih digitalnih uređaja i smart telefona u firmi. Nakon ovoga svi članovi firme bili su zadovoljni što je konačno pronađeno kuda su procurele sve informacije i postali svesni potrebe zaštite informacija. Glavni menadžer je nalaz forenzičke analize prosledio dalje pravnoj službi za dalji postupak. Iako su nematerijalna šteta i ugled firme bili značajni vlasnik firme je odlučio da ne angažuje zvanične organe istrage.

Literatura

- [1] Milan Milosavljević, Gojko Grubor, *Digitalna forenzika računarskog sistema*, Univerzitet Singidunum, Singipedia, Beograd 2009.
- [2] Milan Milosavljević, Gojko Grubor, *Istraga kompjuterskog kriminala- metodološko tehnološke osnove*, Univerzitet Singidunum, Singipedia, Beograd 2010.
- [3] Igor Franc, *Digitalna forenzika*, <http://igorfranc.blogspot.com/2012/05/digitalna-forenzika.html>, Maj 2012.
- [4] Igor Franc, *Digitalna forenzika mobilnih telefona I tablet uređaja*, <http://igorfranc.blogspot.com/2012/11/digitalna-forenzika-mobilnih-telefona-i.html> Novembar, 2012.
- [5] Igor Vuković, *Digitalna forenzika mobilnih telefona za potrebe krivičnog postupka*, http://www.telekomunikacije.rs/aktuelni_broj/mr_igor_vukovic:_digitalna_forenzika_mobilnih_telefona_za_potrebe_krivicnog_postupka.377.html

Internet izvori

- [6] **Android operativni sistemi**, <http://www.itextreme.org/linux/129-sve-o-android-operativnom-sistemu#.UXe4WrWnxZF>
- [7] **Programi** (USB Write Block, Androit Photo forensic, Belkasoft Evidence), <http://dsicover.com/dsicover-software/usb-write-blocker/>, <http://digital-assembly.com/products/adroit-photo-forensics/>, http://forensic.belkasoft.com/en/bec/en/evidence_center.asp