UNIVERZITET SINGIDUNUM

Milan Milosavljević
Gojko Grubor

ISTRAGA KOMPJUTERSKOG KRIMINALA



BEOGRAD, 2009.

UNIVERZITET SINGIDUNUM

Prof. dr Milan Milosavljević
Doc. dr Gojko Grubor

ISTRAGA KOMPJUTERSKOG KRIMINALA

METODOLOŠKO - TEHNOLOŠKE OSNOVE

Beograd, 2009

ISTRAGA KOMPJUTERSKOG KRIMINALA

METODOLOŠKO-TEHNOLOŠKE OSNOVE

Autori:
Prof. dr Milan Milosavljević
Doc. dr Gojko Grubor

Recenzenti:
Prof. dr Milovan Stanišić
Prof. dr Branko Kovačević

Izdavač:
UNIVERZITET SINGIDUNUM
Beograd, Danijelova 32
www.singidunum.ac.rs

Za izdavača:
Prof. dr Milovan Stanišić

Tehnička obrada:
Novak Njeguš

Dizajn korica:
Milan Nikolić

Godina izdanja:
2009.

Tiraž:
300 primeraka

Štampa:
ČUGURA print, Beograd
www.cugura.rs

ISBN: 978-86-7912-

SADRŽAJ

I. METODOLOŠKE OSNOVE ISTRAGE KOMPJUTERSKOG KRIMINALA

UVOD 3

1. RAZVOJ, ORGANIZACIJA I STANDARDI ISTRAGE KOMPJUTERSKOG KRIMINALA 6

1.1 KRATAK PREGLED RAZVOJA DIGITALNE FORENZIČKE ISTRAGE KOMPJUTERSKOG KRIMINALA I ANALIZE DIGITALNIH DOKAZA 8
1.2 STANDARDIZACIJA PROCEDURA DIGITALNE FORENZIČKE ISTRAGE
kompjuterskog kriminla 10
1.2.1 Definicije ključnih termina digitalne forenzičke istrage 10
1.2.2 Principi upravljanja digitalnim dokazima 11
1.2.3 Struktura standardne operativne procedure 12
1.2.4 Standardi i kriterijumi digitalne forenzičke istrage 13
1.2.4.1 Standardi i kriterijumi 1.1 13
1.2.4.2 Standardi i kriterijumi 1.2 13
1.2.4.3 Standardi i kriterijumi 1.3 13
1.2.4.4 Standardi i kriterijumi 1.4 14
1.2.4.5 Standardi i kriterijumi 1.5 14
1.2.4.6 Standardi i kriterijumi 1.6 14
1.2.4.7 Standardi i kriterijumi 1.7 15
1.2.4.8 Standard prihvatljivosti procedure 15
1.2.5 Standardizacija procedure privremenog oduzimanja računara kao dokaznog materijala 15
1.2.6 Procedura za obezbeđivanje kopija dokaza 17
1.2.7 Standardna procedura naučnog karaktera digitalnog dokaza 18
1.2.8 Standardna procedura testiranja forenzičkih alata 19
1.2.9 Legalni zahtevi za digitalne dokaze 21
1.2.10 Dostupnost standardnih procedura i alata 21
1.2.11 Tela za akreditaciju standarda digitalnih forenzičkih laboratorija 22
REZIME 23
PITANJA ZA PONAVLJANJE 24

2. ISTRAGA KOMPJUTERSKOG KRIMINALA

2.1 ZVANIČNA ISTRAGA KOMPJUTERSKOG KRIMINALA 25
2.2 KORPORACIJSKA DIGITALNA FORENZIČKA ISTRAGA 27
2.2.1 Uspostavljanje tima za upravljanje kompjuterskim incidentom 30
2.2.2 Procedura određivanja karaktera kompjuterskog incidenta 31
2.2.3 Model troškova korporacijske forenzičke istrage 33

2.3 PROCES KORPORACIJSKE ISTRAGE 37
2.4 ISTRAGA AKTIVNOG INCIDENTA – STUDIJA SLUČAJA 42
2.4.1 Scenario u kojem je napadač na mreži 42
2.4.1.1 Slučaj direktnog napada 43
2.4.1.2 Slučaj napada preko telefonske centrale 44
2.4.1.3 Mrežne tehnike za postavljanja zamke i praćenje traga napadača 44
2.5 TIM ZA ISTRAGU KOMPJUTERSKOG KRIMINALA 47
2.5.1 Interventni tim za korporacijsku istragu kompjuterskog incidenta 47
2.6 REZULTATI KORPORACIJSKE ISTRAGE KOMPJUTERSKOG INCIDENTNA 48
REZIME 50
PITANJA ZA PONAVLJANJE 51

3. FUNKCIONALNI MODELI DIGITALNE FORENZIČKE ISTRAGE 52

3.1 MODEL ISTRAGE FIZIČKOG MESTA KRIVIČNOG DELA 52
3.2 MODEL ZVANIČNE ISTRAGE DIGITALNOG MESTA KRIVIČNOG DELA 53
3.3 KORPORACIJSKI MODEL ISTRAGE KOMPJUTERSKOG INCIDENTA 53
3.4 MODEL INTEGRISANIH PROCESA DIGITALNE FORENZIČKE ISTRAGE 54
3.4.1 Faza pripreme 57
3.4.2 Faza razvoja 57
3.4.2.1 Faza detekcije i izveštavanja 58
3.4.2.2 Faza potvrde i autorizacije 58
3.4.3 Faza istrage fizičkog mesta krivičnog dela 58
3.4.3.1 Faza obezbeđivanja (fiksiranja) fizičkog mesta krivičnog dela 59
3.4.3.2 Faza revizije fizičkog mesta krivičnog dela 59
3.4.3.3 Faza dokumentovanja fizičkog mesta krivičnog dela 60
3.4.3.4 Faza pretrage i sakupljanja dokaza sa fizičkog mesta krivičnog dela 60
3.4.3.5 Faza rekonstrukcije fizičkog mesta krivičnog dela 61
3.4.3.6 Faza ekspertskog svedočenja/veštačenja fizičkog mesta krivičnog dela 61
3.4.4 Faza istrage digitalnog mesta krivičnog dela 62
3.4.4.1 Faza fiksiranja digitalnog mesta krivičnog dela 63
3.4.4.2 Faza pretrage digitalnog mesta krivičnog dela 63
3.4.4.3 Faza dokumentovanja digitalnog mesta krivičnog dela 64
3.4.4.4 Faza sakupljanja digitalnih dokaza sa digitalnog mesta krivičnog dela 65
3.4.4.5 Faza rekonstrukcije digitalnog mesta krivičnog dela 65
3.4.4.6 Faza prezentacije digitalnog mesta krivičnog dela 66
3.4.4.7 Faza provere 66
3.5 MODEL DOMENA SLUČAJA DIGITALNE FORENZIČKE ISTRAGE 67
REZIME 70
PITANJA ZA PONAVLJANJE 71

4. DIGITALNI DOKAZ **72**

4.1 DIGITALNI KOMPJUTERSKI DOKAZ 72
4.2 PRAVOSUDNI ASPEKT DIGITALNIH KOMPJUTERSKIH DOKAZA 73
4.3 UPRAVLJANJE DIGITALNIM DOKAZIMA 75
4.3.1 Procedura sakupljanja posrednih kompjuterskih dokaza 76
4.4 KORISNICI KOMPJUTERSKIH DIGITALNIH DOKAZA 78
4.5 PRIPREMA DIGITALNIH DOKAZA ZA VEŠTAČENJE PRED SUDOM 79
4.6 PREPORUKE IOCE ZA UPRAVLJANJE DIGITALNIM DOKAZIMA 79
REZIME 81
PITANJA ZA PONAVLJANJE 82
KLJUČNI TERMINI 83
LITERATURA 84

II. TEHNOLOŠKE OSNOVE DIGITALNE FORENZIČKE ISTRAGE

UVOD 89
1. DIGITALNA FORENZIČKA NAUKA **90**

REZIME 93
PITANJA ZA PONAVLJANJE 94

2. FORENZIČKA AKVIZICIJA DIGITALNIH PODATAKA **95**

2.1 FUNKCIONALNI MODEL FORENZIČKE AKVIZICIJE DIGITALNIH PODATAKA 95
2.1.1 Lokardov princip razmene materije 95
2.1.2 Redosled sakupljanja nestabilnih podataka 97
2.2 AKTIVNA FORENZIČKA AKVIZICIJA 98
2.2.1 Razvoj aktivne forenzičke akvizicije 99
2.2.2 Metodi aktivne digitalne forenzičke akvizicije 107
2.2.3 Izbor i priprema forenzičkih alata za aktivnu akviziciju 113
2.2.4 Prednosti i nedostaci aktivne forenzičke akvizicije 118
REZIME 124
PITANJA ZA PONAVLJANJE 126

3. FORENZIČKA ANALIZA DIGITALNIH PODATAKA **127**

3.1 DIGITALNA FORENZIČKA ANALIZA 127
3.1.1 Forenzička analiza softvera 127
3.1.2 Forenzička analiza računara 128
3.1.3 Forenzička analiza u virtuelnom okruženju 129
3.1.3.1 Studija slučaja digitalne forenzičke analize virtuelne mašine 131
3.1.4 Digitalna forenzička analizaračunarske mreže 132
3.1.5 Forenzička analiza kibernetičkog prostora 135

3.2 ZNAČAJ SLOJEVA APSTRAKCIJE ZA DIGITALNU FORENZIČKU ANALIZU 140
3.2.1 Greške u slojevima apstrakcije 141
3.2.2 Karakteristike slojeva apstrakcije 142
3.2.3 Apstrakcioni slojevi FAT fajl sistema 143
3.2.4 Zahtevi za alate za digitalnu forenzičku analizu 146
3.3 UTICAJ SKRIVANJA DIGITALNIH DOKAZA NA TEHNIKE FORENZIČKE ANALIZE 147
3.4 PROCES FORENZIČKE ANALIZE ČVRSTOG DISKA 149
3.4.1 Tok procesa digitalne forenzičke analize 149
3.4.2 IACS procedura kompletnog ispitivanja čvrstog diska 155
REZIME 157
PITANJA ZA PONAVLJANJE 159

4. FORENZIČKI ALATI 160

4.1 RAZVOJ FORENZIČKIH ALATA 160
4.2 OPŠTE KARAKTERISTIKE 161
4.2.1 Tehnike i alati za akviziciju digitalnih podataka 162
4.2.2 Validacija i diskriminacija podataka 164
4.2.3 Ekstrakcija digitalnih podataka 165
4.2.4 Rekonstrukcija osumnjičenog diska 167
4.2.4.1 Forenzički alati za oporavak fragmentiranog fajla 168
4.2.5 Izveštavanje o digitalnim dokazima 170
4.3 HARDVERSKI FORENZIČKI ALATI 170
4.3.1 Blokatori upisivanja i drugi hardverski forenzički alati 172
4.4 SOFTVERSKI FORENZIČKI ALATI 180
4.4.1 Forenzički alati komandne linije 180
4.4.2 Softverski forenzički alat zatvorenog koda EnCase v4 GUI tipa 181
4.4.3 Analiza Access Data FTK forenzičkog alata 199
4.4.4 Forenzički alati otvorenog izvornog koda 222
4.4.4.1 Značaj poznavanja izvornog koda forenzičkih alata 222
4.4.4.2 Forenzički alati otvorenog koda 224
4.4.4.3 SPADA forenzički alat na bazi Linux OS 227
4.4.4.4 Prdnosti i nedostaci Linux baziranih forenzičkih alata 236
4.4.5 Komparativni pregled funkcija ključnih forenzičkih alata 238
4.4.6 Validacija i testiranje forenzičkih alata 239
4.4.6.1 Razvoj procesa validacije forenzičkih alata 239
4.4.6.2 Proces testiranja softverskih forenzičkih alata 239
4.4.6.3 Procedura za validaciju forenzičkog alata 242
4.5 STUDIJA SLUČAJA: AKVIZICIJA IZVRŠNIH FAJLOVA, RUTKITOVA, ZADNJIH VRATA I SNIFERA 243
4.5.1 Rutkit alati 243
4.5.1.1 Podela rutkit alata 244
4.5.1.2 Napad rutkit alatima 245
4.5.2 Detekcija rutkitova, zadnjih vrata i mrežnih snifera 248

4.5.2.1 Detekcija prisustva rutkitova 248
4.5.2.2 Detekcija prisustva zadnjih vrata 251
4.5.2.3 Detekcija prisustva mrežnih snifera 254
REZIME 255
PITANJA ZA PONAVLJANJE 257
KLJUČNI TERMINI 258
LITERATURA 262

III. SVEDOČENJE I VEŠTAČENJE U INFORMACIONO KOMUNIKACIONIM TEHNOLOGIJAMA

1. ISKUSTVA SVEDOČENJA I VEŠTAČENJA IZ DRUGIH NAUČNO-TEHNIČKIH DISCIPLINA 267

1.1 SUDSKI VEŠTACI ZA SAOBRAĆAJ 267
1.2 EKSPERTI ZA FORENZIČKU ANALIZU UMETNIČKIH DELA 267
1.3 FORENZIČAR GEOLOG I EKSPERT ZA TAJNE GROBNICE 267
1.4 ISKUSTVA IZ SUDSKE MEDICINE 268
1.5 FORENZIČKI ENTOMOLOZI 268
REZIME 269
PITANJA ZA PONAVLJANJE 269

2. SPECIFIČNOSTI SVEDOČENJA I VEŠTAČENJA U KOMPJUTERSKOM KRIMINALU 270

2.1 PRIPREMA DOKAZA ZA SUDSKI PROCES 272
2.2 PRELIMINARNA PRIPREMA TUŽIOCA 272
2.3 KOMUNIKACIJE U PREDISTRAŽNOM POSTUPKU 272
2.4 DEFINISANJE USLOVA ZA IZNOŠENJE DIGITALNIH DOKAZA 273
2.5 PRIHVATLJIVOST KOMPJUTERSKI GENERISANIH DIGITALNIH DOKAZA NA SUDU 273
2.6 SVEDOČENJE I VEŠTAČENJE IKT EKSPERTA 274
2.6.1 Edukovanje pravosudnih organa 275
2.6.2 Veštačenje i naučne metode dokazivanja kompjuterskog kriminala 275
2.6.2.1 Rekonstrukcija događaja u sudskom postupku kompjuterskog kriminala 275
2.6.2.2 Instruisanje porote 276
REZIME 277
PITANJA ZA PONAVLJANJE 278
KLJUČNI TERMINI 279
LITERATURA 281
PRILOG I 282
PRILOG II 287

SPISAK SLIKA

Slika 1.1 Skladište čuvanja digitalnih dokaza 14
Slika 1.2 Daubert princip prihvatljivosti digitalnih dokaza na sudu 19
Slika 2.1 Hipotetička distribucija vrednosti i troškovi za otvaranje, standardizovane (levo) i zatvorene, autorske (desno) platforme 35
Slika 3.1 Fizičko mesto krivičnog dela kompjuterskog kriminala 52
Slika 3.2 Faze modela integrisanih procesa digitalne forenzičke istrage 56
Slika 3.3 Faze i interakcija istrage fizičkog i digitalnog mesta krivičnog dela 59
Slika 3.4 Faze forenzičke istrage digitalnog mesta krivičnog dela 62
Slika 1.1 Proces digitalne forenzike 91
Slika 2.1 Sadržaj šifrovanog fajla u AccessData FTK Imager alatu 101
Slika 2.2 Sadržaj dešifrovanog fajla u AccessData FTK Imager alatu 102
Slika 2.3 Particija E šifrovana sa BestCrypt alatom 102
Slika 2.4 Forenzička slika šifrovanog HD u AccessData FTK Imager alatu 103
Slika 2.5 Operacija čišćenja fajlova pomoću BestCrypt alata 104
Slika 2.6 Prozor uzimanja imidža u ProDiscover IR forenzičkom alatu 104
Slika 2.7 Dešifrovani dokument u RAM memoriji u ProDiscover IR alatu 105
Slika 2.8 Pogled na sadržaj fizičke memorije u ProDiscover IR alatu koji indicira da je BestCrypt proces aktivan 106
Slika 2.9 Dešifrovani sadržaj HD u toku aktivne akvizicije sa forenzičkim alatom ProDiscover IR 107
Slika 2.10 Helix forenzički alat za upravljanje incidentom, oporavak podataka i forenzičko podizanje ispitivanog sistema 108
Slika 2.11 Aktivna akvizicija pomoću forenzičkog alata Helix 109
Slika 2.12 GUI alat Nigilant (32) 110
Slika 2.13 Uspostavljanje veze pomoću Remote Admnistrator 114
Slika 2.14 Radmin Viewer 115
Slika 2.15 Sistemsko vreme i datum u Windows XP OS 115
Slika 2.16 GUI klijent za kopiranje fajla 118
Slika 2.17 Prikaz svih USB uređaja povezanih na računar u USBDeview alatu 119
Slika 2.18 Primer sistemskih informacija dobijenih aktivnom akvizicijom sa LiveWire alatom 120
Slika 2.19 Pogled na aktivne procese u LiveWire forenzičkom alatu 121
Slika 2.20 Otkrivanje šifre za rad keylogger-a u memoriji sa LiveWire alatom 121
Slika 2.21 Trag Hacker Defender-a u fizičkoj memoriji u LiveWire alatu 122
Slika 2.22 Drugi pogled na Hacker Defender u RAM memoriji u LiveWire alatu 122
Slika 3.1 Proces dualne analize podataka 131
Slika 3.2 Ulazni i izlazni podaci apstrakcionog sloja 140
Slika 3.3 Slojevi apstrakcije HTML dokumenta 143
Slika 3.4 Tok procesa digitalne forenzičke analize 152
Slika 4.1 Primer prozora u WinHex alatu Northon Commander-a 163

Slika 4.2 Prikaz thumbnalis slika u foremzičkom alatu File Hound 169
Slika 4.3 Tipovi hardverskih blokatora 174
Slika 4.4 Primeri IDEi SATA diskova 174
Slika 4.5 Sakupljanje podataka sa klasičnih 3,5 inča IDE diskova 175
Slika 4.6 Sakupljanje podataka sa klasičnih 3,5 inča SATA diskova 175
Slika 4.7 Sakupljanje podataka sa notebook diskova od 2,5 inča 176
Slika 4.8 Sakupljanje podataka sa malih čvrstih diskova 176
Slika 4.9 Sakupljanje podataka sa fleš memorije (a) mikrodiskova (b) i PCCard (PCMCIA) adapter (c) 176
Slika 4.10 SATA adapter za sakupljanje podataka sa SATA diskova (a) i SATA adapter priključen na SATA disk 177
Slika 4.11 Adapter 1,8 inča ZIF za priključivanje Hitachi ZIF diskova 177
Slika 4.12 CD/DVD robot 179
Slika 4.13 Otvaranje novog slučaja u EnCase alatu 182
Slika 4.14 Otvaranje dijaloga Options u En Case alatu 183
Slika 4.15 Dodavanje dokaznog materija novom slučaju u EnCase alatu 184
Slika 4.16 Odabir fajlova za pretraživanje 184
Slika 4.17 Verifikacija novog slučaja 185
Slika 4.18 Dodavanje sirovih imidž fajlova u EnCase alatu 185
Slika 4.19 Indeksiranje fajlova u EnCase alatu 186
Slika 4.20 Odrđivanje bezbedonosnog identifikatora dokaza 187
Slika 4.21 Aktiviranje skriptova u EnCase alatu 187
Slika 4.22 Izbor fajlova i foldera za oporavak 188
Slika 4.23 Pretraživanje po ključnoj reči u EnCase alatu 189
Slika 4.24 Čitanje Outlook Express .DBX fajlova u EnCase alatu 190
Slika 4.25 Kreiranje butabilne diskete u EnCase alatu 190
Slika 4.26 Završetak kreiranja butabilne diskete u EnCase alatu 191
Slika 4.27 Zaključavanje i otključavanje hard diskova 192
Slika 4.28 Oporavak izbrisanih foldera u EnCase alatu 193
Slika 4.29 Formatirana NTFS particija 193
Slika 4.30 Dodavanje novih potpisa fajla u EnCase alatu 194
Slika 4.31 Generisanje heš vrednosti za izabrane fajlove 195
Slika 4.32 Snimak trenutnog stanja sistema 196
Slika 4.33 Izbor i selekcija diska za brisanje sa prepisivanjem u EnCase alatu 197
Slika 4.34 Simultano indeksiranje velikog broja slika relevantnih za istragu 198
Slika 4.35 Eksportovanje izveštaja u EnCase alatu 198
Slika 4.36 Prikaz heš vrednosti u FTK alatu 199
Slika 4.37 Početni prozor FTK forenzičkog alata 200
Slika 4.38 Odabir tipa dokaza 201
Slika 4.39 Odabir tipa imidža 202
Slika 4.40 Kreiranje imidža 202
Slika 4.41 Verifikovanje rezultata imidžovanja nezaražene USB memorije 203
Slika 4.42 Verifikovanje rezultata imidžovanja zaražene USB memorije 203

Slika 4.43 TXT fajl generisan polse imidžovanja virusom nezaraženog (a) i zaraženog (b) USB 204
Slika 4.44 Generalije o slučaju i forenzičaru 204
Slika 4.45 Case Log opcije 205
Slika 4.46 Processes to Perform opcija 206
Slika 4.47 Refina Case 206
Slika 4.48 Refine index opcija 207
Slika 4.49 Add Evidence opcija 207
Slika 4.50 Dodavanje imidža dva USB memorijska uređaja kao dokaza 208
Slika 4.51 Napredne opcije Refine Evidence i refine Index 208
Slika 4.52 Obrada dokaza 209
Slika 4.53 Kartica Overview 209
Slika 4.54 Obeležen prepoznat maliciozni program na zaraženom USB 210
Slika 4.55 Pregled sadržaja kompresovanog fajla 210
Slika 4.56 Kartica Explore 211
Slika 4.57 Kartica Graphics 212
Slika 4.58 Kartica Search 212
Slika 4.59 Generalne informacije o svojstvima fajla 213
Slika 4.60 Informacije o sadržaju fajla 213
Slika 4.61 Pregled karakteristika malicioznog programa 214
Slika 4.62 Deo FTK log izveštaja 215
Slika 4.63 Podešavanje za prikaz Bookmark-ova 216
Slika 4.64 Odabir svojstava Bookmark-a i prikaz u izveštaju 216
Slika 4.65 Podešavanje prikaza grafičkih elemenata u izveštaju 217
Slika 4.66 Odabir putanje izveštaja i proizvoljnog grafičkog elementa 218
Slika 4.67 Početna strana izveštaja (index.htm) 218
Slika 4.68 Pregled fajlova u izveštaju 219
Slika 4.69 Pregled dokaza u izveštaju 219
Slika 4.70 Prikaz grafičkih elemenata u izveštaju 220
Slika 4.71 Desktop SPADA forenzičkog alata 227
Slika 4.72 Aktiviranje POST procesa za pristup BIOS setup-u 228
Slika 4.73 Podešavanje BIOS-a u SPADA alatu 228
Slika 4.74 SPADA meni za butovanje 229
Slika 4.75 Aktiviranje procesa inicijalne pretrage sa SPADA alatom 229
Slika 4.76 Otvaranje QTParted aplikacije u SPADA alatu 230
Slika 4.77 Aktiviranje Mediafind aplikacije u SPADA alatu 231
Slika 4.78 MediaFind prozor u SPADA alatu 231
Slika 4.79 Rezultati MediaFind aplikacije 232
Slika 4.80 Otvaranje Terminal prozora u SPADA alatu 233
Slika 4.81 Proširivanje Terminal prozora u SPADA alatu na puni ekran 234
Slika 4.82 ProDoscover forenzički alat 249
Slika 4.83 SuperScan forenzički alat 253

SPISAK TABELA

Tabela 1.1 Pomeranje vektora napada na IKT sisteme 10
Tabela 1.2 Primeri kategorija koncepta objekata za digitalnu forenzičku istragu 67
Tabela 1.3 Primeri provere međusobnih odnosa koncepata 68
Tabela 2.1 Karta konvencije bajta – B(Byte) 100
Tabela 3.1 Analitička vremenska radna karta sistemskih log podataka 138
Tabela 3.2 Slojevi apstrakcije FAT fajl sistemu 145
Tabela 3.3 Primeri dokumentovanja procesa digitalne forenzičke analize 153
Tabela 4.1 Pregled funkcija FTK forenzičkog alata 221
Tabela 4.2 Tabela 4.1 Korespondirajuće DOS i Linux komandne linije 233
Tabela 4.3 Svičevi za za definisanje načina rada ls komande 235
Tabela 4.4 Uporedni pregled osnovnih funkcija relevantnih forenzičkih alata 238
Tabela 4.5 Glavne oznake u Unix/linux string komandama3 251
Tabela P2.1 Poznatiji SID identifikatori 287

UNIVERZITET
PRIVATNI
AKREDITOVANI
UNIVERZITET
SINGIDUNUM

DEO

METODOLOŠKE OSNOVE ISTRAGE KOMPJUTERSKOG KRIMINALA

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

Cilj ove glave je da se definišu i opišu metodološke osnove istrage kompjuterskog kriminala koje obezbeđuju optimalni funkcionalni model za istragu kompjuterskog kriminala. Kada pročitaju ovu glavu, studenti će razumeti osnovne funkcionalne modele za zvaničnu i korporacijsku istragu kompjuterskog kriminala, specifičnosti istrage digitalnih dokaza, značaj digitalne forenzičke istrage za upravljanje kompjuterskim incidentom i prednosti procesa integrisane istrage fizičkog i digitalnog mesta krivičnog dela kompjuterskog kriminala.

UNIVERZITET
PRIVATNI
AKREDITOVANI
UNIVERZITET
SINGIDUNUM

UVOD

Uporedo sa razvojem i implementacijom računarskih mreža u sistem globalne mreže - Intereneta, rastu i potencijalne opasnosti od različitih napada sa Interneta, uključujući brojne maliciozne programe i napade ljudskog faktora - hakera, krakera, vandala i kompjuterskih kriminalaca i terorista. Računarske mreže Internet tipa nude brojne prednosti i omogućavaju izuzetno povećanje efikasnosti rada i smanjenje troškova, ali predstavljaju i kritičnu tačku bezbednosti, sa stanovišta rizika za *raspoloživost, integritet i poverljivost* informacija, servisa i aplikacija. U literaturi su objavljene brojne taksonomije pretnji i metode analize faktora rizika za računarske sisteme i mreža Internet tipa. Iako su ranijih godina napadi na računarske mreže Internet tipa bili pretežno eksterni, novije analize pokazuju da mnogo veće finansijske gubitke i drugu štetu nanosi širok spektar internih napada. Razlozi za to leže u samoj prirodi *intranet* mreža u kojima interni učesnici nisu samo zaposleni u datoj organizaciji i za koje postoji određeni stepen poverenja, već i poslovni partneri, zaposleni u firmama podružnicama, kooperanti, dostavljači i drugi učesnici iz *ekstranet* mreža, koji iz razloga jednostavnosti korišćenja i povećanja efikasnosti i produktivnosti rada imaju vrlo slična, ako ne i ista prava pristupa *intranet* mreži kao i zaposleni u datoj organizaciji. Pored finansijske dobiti registrovani su brojni motivi za razne vrste hakerskih i drugih napada na mreže državnih organa, uključujući: izazov i potrebu za samopotvrđivanjem, znatiželju za proboj visokotehnoloških sistema zaštite u ovim mrežama, maliciozne namere - krađu osetljivih informacija, špijunažu i namerna oštećenja informacija, aplikacija i sistema. U nekoliko poslednjih godina deluju organizacije profesionalnih hakera koji organizovano rade na principu sticaja profita od preduzimanja različitih oblika kompjuterskog kriminala. Ove organizacije hakera korumpiraju (*zombiraju*) brojne nezaštićene računare individualnih korisnika širom sveta, sa kojima ili posredstvom kojih napadaju ciljne web sajtove distribuiranim napadom odbijanja servisa (DDoS) i drugim tipovima napada. Vektor napada pomeren je sa korporacijskih servera koji se sve bolje štite na slabo zaštićene ili nezaštićene računare individualnih korisnika, koje korumpiraju preuzimaju kontrolu i koriste za kriminalne aktivnosti. Krajem 2007 godine u Rusiji je registrovana mreža (tzv. *botnet*) od 1,4 miliona *zombiranih* računara.

Pod kompjuterskim kriminalom u najširem smislu podrazumevaju se krivična dela prema krivičnom zakonu nacionalne države, u koja su na bilo koji način uključeni računarski sistemi i mreže. U kompjuterskom i kibernetičkom kriminalu (*cybercrime*) računari se koriste kao predmet napada i krađe, izmene ili uništavanja podataka, kao alat za izvršavanje tradicionalnih oblika kriminala i za skladištenje kompromitujućeg materijala.

Glavni cilj istrage kompjuterskog kriminala je, kao i slučaju klasičnog kriminala, izgraditi za pravosudne organe neoboriv ili čvrst dokaz krivice, i/ili dokaz za oslobađanje osumnjičenog, i/ili pravedno sankcionisanje učinjenog dela. Ključnu metodologiju istrage i dokazivanja kompjuterskog kriminala obezbeđuje metodologija istrage klasičnog kriminala, sa specifičnostima istrage osetljivih, lako promenljivih i po svojoj prirodi posrednih digitalnih dokaza. Digitalna forenzička nauka (1999) obezbeđuje primenu naučno derivirani i dokazanih metoda za: *čuvanje, sakupljanje, validaciju, identifikaciju, analizu, interpretaciju, dokumentovanje i prezentaciju* digitalnih dokaza iz različitih izvora digitalnih podataka sa ciljem rekonstrukcije događaja krivičnog dela kompjuterskog kriminala ili zloupotrebe računara. U oblasti digitalne forenzike prvo je definisana *Kompjuterska forenzika (FBI):* "Kompjuterska forenzika je aplikacija nauke i sistemskog inženjerstva na legalne probleme digitalnih dokaza". Definicije i kategorije digitalne forenzike su pokretna meta, koja prati promene u računarskim tehnologijama, elektronici i komunikacijama.

Za pravosudnu prihvatljivost digitalnih dokaza osnovne prepreke su osetljivost i promenljivost digitalnih podataka i inherentna posrednost digitalnih dokaza. Naime, u slučaju klasičnog kriminala neoboriv dokaz, na primer ubistva, je pištolj u ruci ubice. Takav *neposredan* dokaz u slučaju kompjuterskog kriminala gotovo je nemoguće obezbediti, ali je moguće izgraditi čvrst, neoboriv *digitalni dokaz* bez tzv. pukotina, od niza *posrednih* digitalnih dokaza, kakvi su po svojoj prirodi svi digitalni podaci uskladišteni ili generisani u računarskom sistemu.

Prema definiciji IOCE[1] u oblasti forenzičkih nauka, *digitalni dokaz* je svaka informacija u digitalnom obliku koja ima dokazujuću ili oslobađajuću vrednost, ili vrednost osnovane sumnje i koja je, ili uskladištena, ili prenesena u takvom obliku. U procesima zvanične istrage, prikupljanja, analize i prezentacije digitalnih dokaza potrebno je pridržavati se određenih *principa*, koji određuju proces upravljanja digitalnim dokazima. U svakom slučaju kompjuterskog kriminala, od trenutka otkrivanja do prezentacije digitalnih dokaza na sudu, prema iskustvima *najbolje digitalne forenzičke prakse*, optimalne rezultate daje timski rad od najmanje tri profesionalca: zvaničnog organa istrage, tužioca i eksperta u oblasti informaciono komunikacionih tehnologija (IKT).

Sudska praksa prihvata kompjuterski generisane i memorisane digitalne dokaze pod određenim uslovima. Transformacija digitalnih podataka u formi niza kodiranih bita u sudski dokaz, *apstraktan* je proces koji može navesti sudiju i porotu da dovedu u pitanje autentičnost i integritet kompjuterski generisanog dokaza. U tom smislu, moraju se na nacionalnom nivou, kroz zakon ili podzakonska akta, propisati odgovarajuće pro-

1 *International Organization of Computer Evidence* (http://www.ioce.org)

cedure, koje obuhvataju: proceduru rukovanja i čuvanja digitalnih dokaza i proceduru za forenzičku akviziciju/sakupljanje, analizu/dokazivanje i veštačenje/svedočenje digitalnih dokaza. Pojam *akvizicije* i *analize* je u ovom radu korišćen u smislu otkrivanja, sakupljanja, izvlačenja i dokazivanja digitalnih podataka u dokaznom postupku istrage kompjuterskog kriminala.

Kada sud ne poznaje pitanja o kojima se raspravlja, poziva ili svedoke eksperte, ili sudske veštake. Oblast kompjuterskog i kibernetičkog kriminala u koju su uključeni kompleksni IKT sistemi najbolji je primer sudske prakse gde se tipično zahteva ekspertsko svedočenje, ili veštačenje. Odluku o tome da li je neki IKT ekspert dovoljno kvalifikovan, pravosudni organi razrešavaju prihvatanjem sertifikata profesionalnog strukovnog udruženja, ili profesionalne interesne zajednice o osposobljenosti.

U svakoj nacionalnoj državi uspostavljaju se tela i institucije za akreditaciju i sertifikaciju iz predmetne naučne oblasti[2]. Sud treba da prihvati da je određeni IKT expert kvalifikovan, ako ima relevantni sertifikat ovih tela i institucija. Iako se reputacija tela i institucija koje daju sertifikate procenjuje u svakom konkretnom slučaju, sud obično ne sumnja u takve preporuke. Priroda naučne ekspertize je takva da je grupa, organizovana u strukovano udruženje, zainteresovana da zaštiti standarde u određenoj naučnoj oblasti. Nažalost, u IKT oblasti tipovi ekspertskh grupa i udruženja se razlikuju po formi i funkcijama od drugih naučnih i profesionalnih zajednica. Tako nekompetentan ekspert lako može ugroziti otkrivanje činjenica, ako ih sam pravi, ili izmišlja nepostojeće standarde u toku svedočenja.

Ozbiljan problem nastaje i kada, zbog moralnog stava, jedan IKT ekspert ne može suprotstaviti stav drugom, ili zauzeti suprotan stav u toku svedočenja/veštačenja, iako je suočen sa legalnim zahtevom da svedoči krajnje objektivno. Ta praksa je česta zbog profesionalne solidarnosti IKT eksperata, koji pri tome mogu pripadati istoj interesnoj zajednici IKT eksperata.

2 U Srbiji nadležno telo za akreditacije zove se **ATS**-Akreditaciono telo Srbije (ranije **YUAT**).

1. RAZVOJ, ORGANIZACIJA I STANDARDI ISTRAGE KOMPJUTERSKOG KRIMINALA

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

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

Glavne kategorije kompjuterskog kriminala mogu se grupisati na bazi uloge računara u izvršavanju krivičnog dela kompjuterskog kriminala, gde računar može biti:

- cilj napada (upad u računar, krađa podataka),
- sredstvo za napad (prevare sa kreditinim karticama, slanje spama i slika),
- povezan sa klasičnim kriminalom (trgovina drogom i ljudima, dečija pornografija i dr.) i
- repozitorijum (skladište) digitalnih dokaza kompjuterskog kriminala.

Takođe, u porastu je i klasičan kriminal povezan sa računarom, kao što su povreda intelektualne svojine (neovlašćeno kopiranje i krađa autorskih prava) i piraterija softvera.

Tipovi kompjuterskog kriminala su brojni, a najčešći su:

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

Generalno, *digitalnu forenzičku istragu* koriste četiri društvena sektora:

1. *Zvanični organi istrage kompjuterskog kriminala* (policija, tužilaštvo i sudstvo);
2. *Organi odbrane* (vojska, državna bezbednost);

3. *Korporacije i veće organizacije,* za upravljanje kompjuterskim incidentom sopstvenim kapacitetima, i
4. *Profesionalne organizacije za oporavak podataka* iz slučajno/namerno oštećenih računarskih sistema.

U kojoj meri zasbrinjava kompjuterski kriminal , govori i činjenica da su vlade više zemalja u svetu prepoznale rastući rizik kompjuterskog kriminala kao ključne faktore informaciong ratovanja u budućnosti. Posledice od uništavanja računarskih sistema i mreža, ometanja i špijunaže elektronskog poslovanja, e-trgovine, e-vlade, e-bankarstva, nuklearnih i elektrodistibutivih postrojenja, saobraćajnih mreža i drugih umreženih sistema, mogu biti potencijalno katastrofalne. Hakeri iz svih delova sveta udružuju se u veoma kompaktne organizacije, sposobne da za proboje u mreže i web servere preko Interneta angažuju računarsku moć i resurse koji su ravni moćnim super računarima (primer proboja DES kriptografskog algoritma sredinom 1990-tih).

U Estoniji, gde je informatizacija društva na zavidnom svetskom nivou (implementirane su e-Uprava, e-lične karte, e-pasoši, e-saobraćajna dozvola i e-socijalna/zdravstvena kartica). U proleće 2007. kompjuterski/kibernetički kriminalci (*cyber criminals*), navodno iz Rusije, napali su banke, vladine agencije i političke stranke u Estoniji. Cela zemlja je nakratko bila u potpunosti *offline* i postala tako prvo poprište informacionog ratovanja. Slični su napadi zabeleženi i na Gruziju 2008. godine, u vreme sukoba s Rusijom, kao i u Kirgistanu.

U toku 2007. nemačke obaveštajne službe su objavile kibernetičke napade iz Kine, na nekoliko nemačkih ministarstava i vladin web portal, s ciljem otkrivanja poverljivih informacija. Navodno su kineski hakeri postali tako uporni u svojim pokušajima industrijske špijunaže da je kancelarka Angela Merkel otvoreno zatražila od kineskih diplomata da se napadi prekinu. U periodu 2007/8. godine zabeleženi su masovni napadi na web sajtove vlade Republike Srbije i Srpske pravoslavne crkve.

Kompleksni, kompjuterski upravljani sistemi i kompjuterske mreže su najranjivije infrastrukture i zato bi mogle biti glavna meta terorista. Američki stručnjaci već godinama upozoravaju na mogući "elektronski Pearl Harbor", "digitalni 11. septembar" ili "*Cybergeddon*", a u svom izveštaju Kongresu navode kako upravo Kina "agresivno razvija svoje ratne *cyber* veštine i tehnologije" i kako bi "uskoro mogla biti u značajnoj prednosti" pred drugim nacijama. Mediji su već objavljivali vesti o kiber (*cyber)* ratovima među islamističkim grupama na Bliskom istoku. Svi ovi incidenti otvoraju brojna pitanja o tome da li se zaista radi o ratu, ili novom vidu kriminala - *kompjutrskom državnom terorizmu* i da li su opravdani adekvatni odgovori države.

Na sastancima NATO-a, takođe se vode burne rasprave o tome da li kiber napade treba tretirati kao oružane napade i da li treba razvijati sopstvene kadrove i tehnologiju za obranu od napada u kiber prostoru? Iako ove rasprave do sada nisu dale jasne odgovore, neke informacije ukazuju da neke države već posvećuju adekvatnu pažnju tom pitanju. Naime, Nemačka vlada je (početkom 2009.) odobrila nacrt zakona kojim bi se pojačala bezbednost informacija i komunikacijskih kanala u državnim IKT sistemima, a o kojem uskoro treba da raspravlja i Bundestag.

Kakve posledice ostavlja kompjuterski kriminal u svetu, najbolje ilustruju neke aktivnosti na nivou brojnih država u svetu. Početkom 2009. u gradu *Reinbachu* kraj Bonna, nemačka vojska je počela pripremu jedinice, sastavljene od 76 vojnika-hakera za novi tip ratovanja – *informaciono (digitalno) ratovanje*. Vojnici su obrazovani na *Bundeswehrovim* odeljenjima za IKT, a nove ratne metode uvežbavaju na svom glavnom oružju - računarima. Ovi *hakeri-ratnici*, treba da budu osposobljeni za obranu od kiber napada, ali i za - napade u kiber prostoru.

1.1 KRATAK PREGLED RAZVOJA DIGITALNE FORENZIČKE ISTRAGE KOMPJUTERSKOG KRIMINALA I ANALIZE DIGITALNIH DOKAZA

U toku 1984. FBI[3] je počeo razvoj laboratorije i programa za ispitivanje kompjuterskih dokaza koji je izrastao u jedinstveni CART (*Computer Analysis and Response Team*) tim, kasnije formiran u mnogim organizacijama u SAD. Danas je trend da se forenzička analiza računara vrši u dobro opremljenoj laboratoriji. Međutim, u tom periodu u SAD je oko 70% osposobljenih zvaničnih agencija radilo ovaj posao bez razvijenih procedura za taj rad. Takođe, je evoluirao naziv «Jedinice *za kompjutersku forenzičku analizu*» na «*Jedinicu za digitalne dokaze*».

Pojavom digitalnog videa i audia uvodi se pojam *digitalnih dokaza*. Međunarodna organizacija za kompjuterske dokaze - IOCE (*International Organization on Computer Evidence*) je formirana 1997. Tehnička radna grupa za kompjuterske dokaze - TWGDE (*Technical Working Group for Digital Evidence*) održala je prvi radni sastanak 17. juna 1998. sa ciljem razvoja organizacionih procedura i relevantnih dokumenata za forenzičku istragu digitalnih dokaza. Federalna kriminalistička laboratorija SAD je februara 1999. promenila ime TWGDE u SWGDE (*Scientific Working Group for Digital Evidence*). Ova se grupa sastaje najmanje jednom godišnje, a članovi mogu biti pred sudom zakleti (zvanični organi) i ne-zakleti eksperti i naučnici. U početku je koncept pronalaženja «latentnog-skrivenog dokaza u kompjuteru» nazvan *kompjuterskom forenzičkom analizom*. Kompjuterska forenzička analiza za manje od 20 godina pouzdano čuva digitalne podatke, oporavlja izbrisane podatke, rekonstruiše kompjuterske događaje, odvraća napadače, nudi dosta dobrih proizvoda i procedura za podršku. Kompjuterska forenzička analiza primenjuje se u slučajevima: hakerskog upada, pronevere, pedofilskog kruga, imigracione prevare, trgovine drogom, falsifikovanja kreditnih kartica, piraterije softvera, izbornog zakona, obscenih publikacija, falsifikata, ubistava, seksualnog uznemiravanja, krađe podataka-industrijske špijunaže, razvoda.

Uputstvo za pretragu i privremeno oduzimanje računara objavilo je Ministarstvo pravde SAD (DoJ), 1994:

3 FBI - Federal Bureau of Investigation, SAD

- hardver kao zabranjeno sredstvo ili pomoć za izvršavanje kriminala (klonirani mobilni telefon, ukraden mikrofiš);
- hardver kao instrument izvršavanja kriminala (značajna uloga u kriminalu - snifer paketa, čitač kreditnih kartica; distribucija dečije pornografije)
- hardver kao dokaz (svaki hardverski uređaj koji ima jedinstvenu karakteristiku da prikaže digitalni dokaz – sliku, podatak);
- informacija kao zabranjeno sredstvo ili pomoć za izvršavanje kriminala (u nekim zemljama korišćenje jake kriptozaštite je ilegalno, piratski softver, ukradene trgovačke tajne, liste lozinki, dečija pornografija);
- informacija kao instrument izvršavanja kriminala (automatizovani hakerski alati, *keyloger*-ski softver za snimanje otkucaja na tastaturi, krekeri lozinki);
- informacija kao dokaz (računar neprekidno ostavlja tragove bita, log fajlovi pristupa, e-mail poruke, upotreba kreditnih kartica, priznanice, telefonski pozivi .

FBI je 1999. sponzorisala razvoj SWGIT (*Scientific Working Group in Imaging Technologies*). «*Glavna misija SWGIT je da olakša integraciju tehnologije i sistema digitalne obrade slika u pravosudni sistem, obezbeđujući definicije i preporuke za akviziciju, skladištenje, procesiranje, analizu, prenos i izlazni format slika*».

Na bazi specifičnosti tehnika i alata i metoda istrage u forenzičkoj praksi su diferencirane sledeće glavne oblasti digitalne forenzike, [3]:

- forenzika računara (akvizicija i analiza HD i prenosivih medija);
- mrežna forenzika (upada u mrežu, zloupotreba itd.);
- forenzika softvera (ispitivanje malicioznih kodova, *malware* itd.)
- aktivna (živa) forenzika sistema (kompromitovanih hostova- servera, zloupotreba sistema itd.).

U početnoj fazi razvoja digitalnu forenziku koristili su primarno zvanični državni organi istrage kompjuterskog kriminala (policija, vojska i pravosuđe). Savremeni trend umrežavanja lokalnih mreža primenom Internet tehnologija (intranet i ekstranet mreže), razvojem bežičnih mreža, e-poslovanja i mobilnog poslovanja (m-poslovanja), zatim web servisa servisno orijentisanih aplikacija, značajno su povećani zahtevi za bezbednost informacija i e-transakcija na svim nivoima poslovnih IKT sistema. Savremeni sistemi zaštite postaju sve kompleksniji, kako se pomera težište osetljivosti poslovnih IKT sistema, javljaju novi tipovi rizika, menjaju metodi napada sa Interneta, a vektor napada pomera sa usamljenih hakera, sitnih prevaranata na web-u, poplave virusa i drugih malicioznih kodova i retkih napada na web servise, na napade organizovanih profesionalnih hakera, industrijskih kiber (*cyber*) špijuna i kompjuterskih kiber kriminalaca (tabela 1.1).

Tabela 1.1 Pomeranje vektora napada na IKT sisteme

1996	2007/2008
Hakeri iz hobija	Rentabilni profesionalni hakeri
Prevaranti na web sajtovima	Kriminalci
Virusi i drugi malicozni programi	Napadi odbijanja servisa (DoS, DDoS)
Retki napadi na web sajtove	Krađa identiteta
	Stalni napadi na web sajtove

Za upravljanje kompjuterskim incidentom u ovakvom okruženju zahtevaju se forenzička znanja i forenzičke tehnike i alati za otkrivanje i otklanjanje uzroka kompleksnih incidenata. Savremenih korisnici digitalne forenzike su:

- policija,
- vojska,
- pravosudni sistem (tužilaštvo i pravosuđe),
- firme koje se profesionalno bave oporavkom podataka iz računara,
- korporacije za upravljanje kompjuterskim incidentom.

Glavni indikatori razvoja digitalne forenzike u proteklom periodu ukazuju da hardver postaje sve osetljiviji na napade, zbog sve veće kompleksnosti, što znači da se mogu očekivati češće subverzije hardvera. Na primer, re-flešovanjem *firmware* čvrstog diska (HD), ili drugih sekundarnih periferijskih memorija mogu se sakriti podaci, ili učiniti HD/memorija nečitljivom. U tom smislu, forenzičar ne može verovati šta je na hardveru. Generalno, sistem zaštite može uticati na proces forenzičke akvizicije i analize. Na primer, forenzičar može naići na HD zaštićen lozinkom (lozinkom) sa kojeg nije moguće odrediti čak ni osnovne informacije, kao što su veličina diska i slika

Kratak istorijski pregled evolucije forenzičke analize digitalnih dokaza dat je u **Prilogu I,** [29].

1.2 STANDARDIZACIJA PROCEDURA DIGITALNE FORENZIČKE ISTRAGE KOMPJUTERSKOG KRIMINALA

1.2.1 Definicije ključnih termina digitalne forenzičke istrage

Evidentno je da informaciono komunikacione tehnologije najefikasnije globalizuju svet. Posledica je da se počinilac kompjuterskog kriminala javlja u jednom pravosudnom sistemu, a digitalni podaci koji dokazuju taj kriminal mogu se nalaziti u nekom drugom pravosudnom sistemu. Radna grupa SWGDE (SAD) je dala prvu definiciju digitalnih

dokaza - DE (*Digital Evidence*) i predlog *standarda* za razmenu DE između suverenih entiteta. Digitalizacijom audio i video signala i klasične fotografije došlo je do ubrzane konvergencije pomenutih tehnologija i integracije u računaru. Tako i termin *kompjuterski digitalni dokaz* (CDE) evoluira u digitalni dokaz (DE). Sa pravnog i tehničkog aspekta razmene DE, glavni zahtevi su postojanje jedinstvenih standarda, principa, kriterijuma i procedura digitalne forenzičke istrage kompjuterskog kriminala.

Dokument standarda je struktuiran kroz: *uvod*, *definicije i standarde* (principe i kriterijume) i *diskusiju* i usklađen sa zvaničnim Uputstvom - *American Society of Crime Laboratory Directors/Laboratory Accreditation Board Manual*, a sadrži definicije termina, standarda i principa kojih se treba pridržavati u radu sa digitalnim dokazima, [4], [22].

Digitalni dokaz: *DD je svaka informacija koja ima dokazujuću vrednost koja je ili uskladištena ili prenesena u binarnoj (digitalnoj) formi. DD uključuje kompjuterski dokaz, digitalni audio, digitalni video, mobilni telefon, digitalnu fax mašinu itd. Digitalni dokaz je informacija uskladištena ili prenesena u binarnoj formi na koju se sud može osloniti*.

Akvizicija digitalnih dokaza (ADE): *ADE počinje kada su informacije i/ili fizički predmeti skupljeni i uskladišteni za potrebe ispitivanja. Termin DE implicira da je skupljanje DE obavio neko koga sud prepoznaje, da je proces skupljanja DE legalan i u skladi sa zakonskom regulativom i da je skupljeni materijal sud prihvatio kao dokazni materijal. Objekti podataka i fizikalni objekti postaju dokazi samo kada ih takvim vide regularni zvanični organi istrage i pravosuđa.*

Objekti podataka: *Objekti ili informacije koje su pridružene fizičkim predmetima i koji imaju potencijalnu dokazujuću vrednost. Objekti podataka se mogu pojaviti u raznim formatima, ali se ne sme menjati originalna informacija.*

Fizički predmet: *Predmeti u kojima mogu biti uskladišteni objekti podataka ili informacije i/ili sa kojima su objekti podataka preneseni*.

Originalni digitalni dokaz: *Fizički predmeti i objekti podataka pridruženi tim predmetima u vreme akvizicije ili privremenog oduzimanja predmeta*.

Duplikat digitalnog dokaza: *Precizna digitalna reprodukcija svih objekata podataka koji se sadrže u originalnom fizičkom predmetu*.

Kopija digitalnog dokaza: *Precizna reprodukcija informacija koje su sadržane na originalnom fizičkom predmetu, nezavisno od originalnog fizičkog predmeta*.

1.2.2 Principi upravljanja digitalnim dokazima

U procesima zvanične istrage, prikupljanja, analize i prezentacije digitalnih dokaza potrebno je pridržavati se određenih *principa*, koji određuju proces upravljanja digitalnim dokazima. *IOCE principi* treba da, [14], [22]:

- budu konzistentni sa svim legalnim sistemima,
- dopuštaju korišćenje sa uobičajenim jezikom,
- budu trajni i međunarodno prihvatljivi,
- ulivaju poverenje i obezbeđuju integritet DE,
- budu primenjivi na sve vrste DE,
- budu primenljivi na svim nivoima, od pojedinca, preko zvaničnih agencije, do najvišeg nacionalnog nivoa.

Principi *nisu plan* implementacije. Oni treba da budu dizajnirani tako da dopuste svakom legalnom entitetu da kreira program koji odgovara situaciji. Primenom ovih *Principa* u skladu sa preporukama IOCE, upravljanje digitalnim dokazima (istraga, akvizicija, analiza, rukovanje i održavanje) postaje prihvatljivo i iskoristivo i izvan nacionalnih granica.

Glavni IOCE principi upravljanja digitalnim dokazima su:

U toku akvizicije DE, preduzete akcije ne treba da unose nikakvu izmenu tih DE.

1. Ako je potrebno da neko pristupi originalnom DE, mora biti kompetentan u oblasti digitalne forenzike.
2. Sve aktivnosti koje se odnose na akviziciju, pristup, skladištenje ili transfer DE moraju biti potpuno dokumentovane, sačuvane i raspoložive za reviziju.
3. Lice je odgovorno za sve aktivnosti preduzete prema DE dok su u njegovom posedu.
4. Svaka agencija/organizacija odgovorna za akviziciju, pristup, skladištenje ili prenos DE je odgovorna za usklađenost svoje prakse sa ovim principima.

Da bi se osigurala bezbedna *akvizicija* (otkrivanje, fiksiranje i izvlačenje), *upravljanje* (skupljanje, čuvanje i prenos) i *forenzička analiza* digitalnih dokaza i da bi se sačuvao integritet i pouzdanost dokaza, zvanični istražni i korporacijski organi za forenzičku istragu i analizu digitalnih dokaza, moraju uspostaviti i održavati efikasni sistem kontrole kvaliteta. Standardna radna procedura – SOP (*Standard Operation Procedure*) je dokumentovano uputstvo za kontrolu kvaliteta celokupnog postupka istrage, akvizicije, upravljanja i forenzičke analize digitalnih dokaza. SOP mora obuhvatiti propisno registrovanje svih aktivnosti istrage kompjuterskog incidenta/kriminala, kao i korišćenje drugih, u kriminalistici široko prihvaćenih procedura, opreme i materijala.

1.2.3 Struktura standardne operativne procedure

Kada se formulišu standardne radne procedure treba uključit sledeće elemente:

- **Naslov** – treba da sadrži ime procedure;
- **Namena** – zašto, kada i ko koristi proceduru;

- **Oprema/materijal/standardi/kontrole** - identifikuje koji se predmeti zahtevaju za izvršavanje procedure. Ovo može uključiti opremu za zaštitu, hardver, softver i načine konfigurisanja.
- **Opis procedure** – opis korak-po-korak kako se procedura izvodi. Ako je neophodno procedura treba da sadrži mere opreza koje treba preduzeti da se minimizira degradacija.
- **Kalibracija** – opisuje svaki korak koji se zahteva da se osigura tačnost i pouzdanost procedure. Gde je primenljivo, treba dokumentovati podešavanje instrumenata i proceduru kalibracije.
- **Kalkulacija** - opisuje bilo koju matematičku operaciju koja je primenjena u proceduri.
- **Ograničenja** – opisuju sve akcije, interpretacije, ili opremu koja nije odgovarajuća za proceduru.
- **Sigurnost** - identifikuje i adresira potencijalne hazarde kod korišćenja procedure.
- **Reference** - identifikuje interna i eksterna dokumenta koja agencija/ korporacija koristi za generisanje procedure i koja se odnose na proceduru i njene principe.

1.2.4 Standardi i kriterijumi digitalne forenzičke istrage

1.2.4.1. Standardi i kriterijumi 1.1

Sve agencije koje zaplenjuju i/ili ispituju digitalnu opremu moraju voditi i održavati odgovarajući SOP dokument, potpisan od strane nadležnog menadžera, koji sadrži jasno definisane sve elemente politike i procedura.

SOP mora biti obavezna za zvanične i korporacijske forenzičke organe zbog prihvatanja rezultata i zaključaka na sudu.

1.2.4.2 Standardi i kriterijumi 1.2

Menadžment agencije mora revidirati SOP jedanput godišnje da obezbede neprekidnost njihove efikasnosti i pogodnosti za primenu, zbog brzih tehnološki promena.

1.2.4.3 Standardi i kriterijumi 1.3

Korišćene procedure moraju biti generalno prihvaćene u oblasti forenzičke istrage, akvizicije i analize digitalnih dokaza i da ih u akviziciji, analizi i čuvanju podržavaju naučne metode. U izboru metoda evaluacije naučne vrednosti forenzičkih tehnika i procedura mora se biti fleksibilan. Validnost procedure treba uspostavljati demonstriranjem tačnosti i pouzdanosti specifične tehnike. U tom smislu korisna je javna naučna rasprava.

1.2.4.4 Standardi i kriterijumi 1.4

Agencija mora posedovati pisanu kopiju odgovarajućih tehničkih procedura koje koristi u radu. Potrebni hardverski i softverski elementi forenzičkih alata moraju biti navedeni u spisku uz opis propisanih koraka za upotrebu i jasno navedena sva ograničenja upotrebe tehnika i alata. Lica koja primenjuju procedure moraju biti dobro upoznata sa njima i dobro obučena za rad sa korišćenim alatima.

1.2.4.5 Standardi i kriterijumi 1.5

Agencija mora koristiti adekvatne hardverske i softverske forenzičke alate koji su efikasni za realizaciju procedura akvizicije i/ili analize digitalnih dokaza. Treba biti dovoljno fleksibilan u pogledu raznovrsnosti izbora metoda koje su najbolje za konkretni problem. Hardverski i softverski alati za akviziciju i/ili analizu digitalnih dokaza moraju biti testirani i da poseduju važeći sertifikat o verifikaciji funkcionalnog kvaliteta nadležne nacionalne institucije za akreditaciju i moraju biti u dobrom radnom stanju.

1.2.4.6 Standardi i kriterijumi 1.6

Sve aktivnosti koje se odnose na akviziciju (privremeno oduzimanje), skladištenje, ispitivanje/analizu, prenos digitalnih dokaza moraju biti registrovane u pisanoj formi i na raspolaganju za pregled i svedočenje/veštačenje. Generalno dokumentacija koja podržava zaključke forenzičke analize mora biti tako pripremljena da ih drugo kompetentno lice može izneti i u odsustvu originalnog autora. Mora se uspostaviti i održavati *lanac čuvanja dokaza* za sve digitalne dokaze, (slika 1.1).



Slika 1.1 Skladište čuvanja digitalnih dokaza

Stalno se moraju voditi pisane zabeleške i zapažanja o slučaju (mastilom ili dijagrami u kolor hemijskoj olovci) sa inicijalima autora kod svake korekcije (precrtane jednom crtom). Svaka zabeleška mora biti lično potpisana, sa inicijalima, digitalno potpisana ili sa drugom identifikacionom oznakom autora.

1.2.4.7 Standardi i kriterijumi 1.7

Bilo koja akcija koja ima potencijal da izmeni, ošteti ili uništi bilo koji aspekt originalnog dokaza mora se izvršavati od strane kvalifikovanog lica na forenzički ispravan način. Svaki metod izvršavanja forenzičke akcije mora biti dokumentovan, tačan, pouzdan, kontrolabilan i ponovljiv. Obučeno forenzičko osoblje mora koristiti kvalitetne forenzičke hardverske i softverske alate i odgovarajuću opremu.

1.2.4.8 Standard prihvatljivosti procedure

Za većinu softverskih forenzičkih alata nisu poznati programski izvorni kodovi, većina procedura nije objavljeno i nisu podvrgnute javnoj raspravi niti su opšte prihvaćene.

Forenzički alati sa zatvorenim kodom koji su testirani na naučno prihvatljivoj i ponovljivoj osnovi i čiji je broj i tip grešaka poznat i objavljen mogu se ravnopravno koristiti sa alatima sa otvorenim programskim kodom. Primer takvih alata je **EnCase 4.0** koji je testiran u NIST laboratoriji.

Forenzički alati sa otvorenim izvornim kodom imaju objavljene procedure, pa forenzičar može odlučiti da li da koristi alat ili ne [15].

1.2.5 Standardizacija procedure privremenog oduzimanja računara kao dokaznog materijala

Generalno u digitalnoj forenzici računarskog sistema, potencijalni izvori digitalnih dokaza mogu se naći u brojnim hardverskim i programskim komponentama sistema, [3]:

- HD, magnetna traka, eksterni/pokretni mediji za skladištenje podataka,
- log fajlovi mrežne infrastrukture (*firewall*, IDS/IPS, *proxy* server itd.),
- aplikacije i log fajlovi bezbednosno relevantnih događaja (tragova za *audit*),
- e-mail,
- sadržaj drugih servera (Windows zajednički fajlovi, web serveri, baze podataka itd.),
- uhvaćeni mrežni saobraćaj.

Osnovni problemi DF istrage su osetljivost digitalnih podataka - lako brisanje i izmena digitalnih podataka i kratkotrajnost u određenom stanju računarskog sistema. Na primer, startovanjem ažuriranja PC sa Windows XP platformom, menjaju se stotine podataka o datumu i vremenu (vremenskih pečata) i veliki broj fajlova. Priključivanje HD ili USB, takođe, menja vremenske pečate fajl sistema, a isključivanjem računara gube se podaci iz promenljive radne memorije (RAM-a). U određenim uslovima akvizicija (izvlačenje) digitalnih dokaza postaje veoma teška, na primer:

- mrežni saobraćaj postoji samo nekoliko milisekundi na žičnoj/kablovskoj mrežnoj infrastrukturi;

- upad i napad mogu biti izvedeni izuzetno sofisticiranim *rutkit* tehnikama za ubacivanje i skrivanje prisustva zadnjih vrata;
- aktivan rad napadnutog sistema (npr. servera) može onemogućiti akviziciju digitalnih dokaza, ako ga nije moguće isključiti ili privremeno oduzeti;
- antiforenzičke aktivnosti mogu sprečiti akviziciju digitalnih podataka.

Standardna procedura za otkrivanje i privremeno oduzimanje računara kao dokaznog materijala u slučaju kompjuterskog incidenta sadrži sledeće elemente (FBI, SAD), [2]:

1. Pretraga mesta krivičnog dela kompjuterskog kriminala:

- Snimiti na forenzički računar i logovati sve dokaze uzete na mestu krivčnog dela.
- Ako se računarski sistem ne može privremeno oduzeti iz nekog razloga, uzeti dve fizičke slike (imidža) HD osumnjičenog računara na forenzički sterilan HD.
- Ako se osumnjičeni računarski sistem može privremeno oduzeti, izvršiti demontažu sistema u skladu sa procedurom isključivanja (ako je računar uključen), označiti sve demontirane kablove i pripadajuće utičnice parovima jedinstvenih brojeva, označiti, takođe, sve odvojene elemente sistema (CPU kućište, tastaturu, miša, diskete, optičke diskove i druge medije) i spakovati za bezbedan transport do forenzičke laboratorije za ispitivanje.
- Registrovati detaljno sve informacije o vlasniku kompromitovanog računarskog sistema.
- Izraditi detaljan izveštaj sa opisom svih preduzetih akcija u toku pretrage mesta krivičnog dela i privremenog oduzimanja računarskog sistema.
- Sve aktivnosti pretrage na mestu krivičnog dela vršiti u skladu sa standardnom operativnom procedurom.

2. Integritet digitalnih podataka:

- Jedina sigurnost za integritet podataka je kredibilitet forenzičara/ istraživača, koji ima znanje i iskustvo za propisno procesiranje elektronskih dokaza.

3. Izveštaj o procesiranju i strukturi osumnjičenog HD:

- Spisak imena uključenog personala.
- Snimak vremena i mesta priključivanja.

4. Identifikacija ispitivanog materijala:

- Imena i serijski brojevi sve korišćene opreme i programa u osumnjičenom računarskom sistemu.
- Izveštaj o ostalim informacijama sakupljenim u predistražnom postupku.

5. Uspostavljanje lanca čuvanja digitalnih dokaza:

- Uspostaviti i održavati lanac čuvanja integriteta digitalnih i drugih tipova dokaza do završetka sudskog procesa u skladu sa principima i SOP.

6. Uslovi čuvanja digitalnih i drugih dokaza:

- Čuvati elektronske i druge dokaze u propisanim uslovima temperature, vlažnosti, prašine, magnetskih polja itd.

7. Procedura procesiranja dokaza sa HD:

- U zavisnosti od platforme osumnjičenog računara, primeniti SOP za isključivanje/podizanje (butovanje) računara i uzimanje forenzičkog imidža za analizu.
- Za forenzičku analizu obezbediti dve imidž kopije osumnjičenog HD.

8. Identifikaciono označavanje ostalih medija za skladištenje (osim HD):

- Sve medije za skladištenje podataka (trake, printerski kertridži, zip ili flopi diskovi, USB, CD ROM, DVD i druge prenosive dokaze), privremeno oduzete za ispitivanje, treba propisno označiti i dokumentovati prema sledećem:
  - sadržaj,
  - podaci sertifikovani/testirani/ispitani,
  - ime forenzičara-analitičara,
  - zaštita diska od upisivanja pre pregleda, kopiranja, analize kopije (ne originala), antivirusno skeniranje,
  - označiti svaku disketu, CD, DVD, USB sa a-1, a-2 itd.,
  - odštampati direktorijum sa svakog ispitivanog medija,
  - ako se u ovoj fazi otkriju informacije koje predstavljaju dokaz, odštampati sadržaj tog fajla i označiti štampani materijal sa istom alfanumeričkom oznakom.

1.2.6 Procedure za obezbeđivanje kopija dokaza

Procedure za obezbeđivanje kopija dokaza za javnog branioca, advokata odbrane, itd:

1. Pod istim uslovima napraviti radnu fizičku kopiju – forenzički imidž (kopiju bit-po-bit) originalnog osumnjičenog/ispitivanog HD sa potencijalnim dokazima i jedan forenzički imidž kao referentni za eventualne pravosudne potrebe.
2. Štampati za izveštaj sa radne forenzičke kopije, sve dok sadržaj ne postane suviše velik za potrebe istrage u celini. Ako takav izveštaj postaje preobiman, onda sažeti pisani izveštaj, a u prilogu podneti kopiju elektronskog dokaza.
3. Podaci sadržani u memorijskim uređajima i medijima *samo za čitanje*, ponekad se traže kao dokazi u formi štampane kopije.
4. Referentnu kopiju čuvati u celom lancu istrage za slučaj da sud ili druga strana sumnjaju i/ili zahtevaju da se dokaže integritet digitalnih dokaza, tj. da se dokaže da digitalni dokazi nisu izmenjeni pod uticajem forenzičkih alata u procesu analize i pripreme digitalnog dokaza za glavni pretres.

- Tehnička prezentacija pred sudom:
- Jednostavna i skoro oslobođena kompjuterske tehnologije;
- *PowerPoint* prezentacija koja jednostavno objašnjava kompleksni koncept;
- Poseban kompjuterski kriminal na Internetu;
- Kako radi Internet.

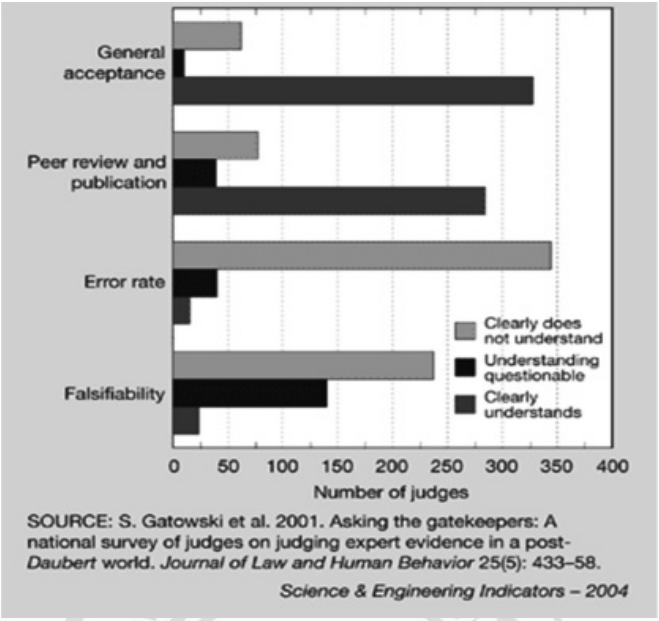
1.2.7 Standardna procedura naučnog karaktera digitalnog dokaza

Kako je digitalni podatak i potencijalni digitalni dokaz po svojoj prirodi veoma *osetljiv* na promene i uništavanje (brisanje) i u suštini uvek *posredan* dokaz za sud, može se lako dovesti u pitanje prihvatljivost digitalnog dokaza pred sudom, na zahtev druge strane ili samog suda. Kako je broj slučajeva kompjuterskog kriminala naglo rastao, bilo je potrebno obezbediti neoborive argumente za dokazivanje da se digitalni podatak može kopirati, čuvati i procesirati u računarskom sistemu, a da pri tome ne dođe do izmene digitalnih podataka koji čine čvrsti (neoborivi) digitalni dokaz, u odnosu na to kakvi su ti podaci bili u osumnjičenom računaru u trenutku akvizicije podataka i da, takođe, nisu izmenjeni u odnosu na stanje u osumnjičenom računaru pre same akvizicije i primene forenzičkog alata. Ovakve argumente, u principu, mogu obezbediti samo naučno dokazane i priznate tehnike, procesi i metodi akvizicije i analize digitalnih podataka, [39]. Ovakva procedura, koja se smatra bazičnom procedurom digitalne forenzike, poznata je kao *Daubert Gudlines*[4], ili *Daubert standardna procedura* uslova za prihvatljivost digitalnog dokaza pred sudom, koja mora biti takva da se:

- izvođenje dokaza može po zahtevu suda verifikovati;
- poznati stepen grešaka koje procedura unosi u digitalni dokaz može dokazati;
- objavi u vrhunskom, višestruko recenziranom naučnom časopisu, dok konferencijski radovi nisu prihvatljivi i
- da se prihvata u relevantnim naučnim krugovima.

Istraživanje (2004) u SAD je potvrdilo da razumevanje značaja *Daubert* principa za prihvatljivost digitalnog dokaza na sudu značajno varira, (slika 1.2).

4 Sudski slučaj *Daubert* vs. *Merrell Dow Pharmaceuticals* Vrhovni sud SAD je prihvatio kao referentni za prihvatljivost ekpertskog naučnog mišljenja za svedočenje/veštačenje u svim slučajevima federalnog suda.



Slika 1.2 Daubert princip prihvatljivosti digitalnih dokaza na sudu, [3]

Najveći stepen razumavanja je zahtev da je za forenzički alat poznat stepen greške koju unosi i da se to na zahtev suda može testom dokazati. *Standardna Daubert procedura* obuhvata uslove za forenzičku prihvatljivost softverskih alata i tehnika za primenu alata, procedura akvizicije, analize i čuvanja digitalnih dokaza, kao i ponovljivosti procedure za testiranje forenzičkih alata na zahtev suda. Do danas je nekoliko alata za digitalnu forenzičku analizu podvrgnuto ovoj standardnoj proceduri (npr. **EnCase**, **FTK** i dr.).

1.2.8 Standardna procedura testiranja forenzičkih alata

Iako još uvek ne postoji opšte prihvaćena i konzistentna standardna procedura za testiranje alata za forenzičku akviziciju i analizu digitalnih podataka u oblasti javne digitalne forenzike prihvata se sertifikacija radne grupe NIST-a specijalizovane za testiranje alata za forenziku računara - NIST CFTT (*NIST Computer Forensic Tool Testing*). U interesnoj zajednici digitalne forenzike preovlađuje mišljenje da forenzičke alate treba da testiraju i sertifikuju još i *vendori* (proizvođači i isporučioci) alata i sami korisnici – digitalni forenzičari, [6], [11].

Do sada[5] je NIST CFTT grupa razvila metodologiju samo za uzimanje fizičke (miror, slike ili imidža čvrstog diska). Procedura uzimanja fizičke slike diska sadrži samo izvođenje testova koji verifikuju očekivane funkcije softverskog alata, a ne podrazumeva kontrolu

5 do 2006, u toku je razvoj više procedura za testiranje drugih funkcija forenzičkih alata.

izvornog koda. U tom smislu, zbog mogućnosti kontrole koda, osnovne funkcije alata sa *otvorenim izvornim kodom* je lakše testirati i lakše je razviti efikasnije testove. Iako do sada nema objavljenog konzistentnog predloga metoda i procesa za proračun stepena grešaka hardversko/softverskih alata za digitalnu forenzičku analizu, dostupni su rezultati brojnih testova forenzičkih alata sa zatvorenim izvornim kodom. Cilj ovih testova je da se nedvosmisleno dokaže da neki forenzički alat unosi poznat tip i broj grešaka, što se može dokazati ponavljanjem procedure testa. Od velike pomoći je i činjenica da je zbog komercijalnih razloga u najboljem interesu *vendora* alata da je ova greška što je moguće manja, što opravdava i zahteve za sertifikaciju alata od strane vendora. Stepen grešaka forenzičkog alata treba da uključuje, pored funkcionalnih grešaka i greške u programiranju ili bagove. Aplikacije softverskih alata sa *zatvorenim izvornim kodom* mogu kriti skrivene bagove, koji nisu dokumentovani pa ostaju nepoznati i u sledećoj verziji proizvoda. Nasuprot, aplikacije forenzičkih alata sa otvorenim izvornim kodom omogućavaju poređenje dve verzije alata i otkrivanje eventualnih bagova koji su ostali skriveni u prethodnoj verziji.

Testiranje forenzičkih alata u NIST CFTT programu je, bez sumnje, kritično za digitalnu forenziku sa aspekta zahteva za prihvatljivost alata pred sudom. Međutim, postojeći zahtev za *vendorsko* ispitivanje alata, u principu ima drugačiji cilj. NIST Ispituje da li alat radi ono šta je pretpostavljeno da treba da radi da bi bio prihvatljiv za sud, dok *vendori* alata ispituju šta je pretpostavljeno da alat radi u različitim situacijama i ovo ispitivanje traje znatno duže i znatno je skuplje od testiranja NIST-a. Na primer, kompanija **ProDiscover** ima skup od 500 slučajeva testiranja svih forenzičkih platformi i alata koje ova razvija. Ipak, zbog sofisticirane prirode softvera i brojnih varijanti i permutacija sistemskih programa, nije realno zahtevati primenu nekog alata u svim forenzičkim situacijama i slučajevima. Drugim rečima, nije moguće potpuno simulirati i testiranjem obuhvatiti sve potencijalne kombinacije forenzičkog hardvera i softvera u vrlo različitim, realnim slučajevima kompjuterskog kriminala. U praksi, proizvođači forenzičkog softvera, za sada uspevaju samo da identifikuju većinu kritičnih bagova, ali nije neobično da se alati popravljaju u novim verzijama[6], na bazi povratnih informacija korisnika iz forenzičke zajednice. Tu je najveći problem što forenzičari ne mogu *vendorima* dostaviti fajlove sa dokazima o manifestaciji bagova zbog zahteva za zaštitom privatnosti i/ili tajnosti, a drugi razlog je što do sada forenzički alati generalno imaju slab sistem upravljanja greškama. Tako se javila potreba da forenzički alat treba da ima log fajl grešaka, čime bi korisnici mogli obavestiti *vendore* o problemima rada sa alatom bez ugrožavanja privatnosti i tajnosti predmetnog lica u analiziranom slučaju ili otkrivanja osetljivih informacija. Takođe, na ovaj način bi forenzičar registrovao problem, koji bi u suprotnom mogao ostati nezapažen.

Međutim, ostaje problem što se log fajl grešaka forenzičkog alata može u unakrsnom ispitivanju u sudskom procesu zloupotrebiti za prolongiranje istrage i samog procesa, ukazivanjem na nepouzdanost primenjenog alata, ili dovođenjem u sumnju integritet relevantnih digitalnih dokaza.

6 krpe („pečuju“) kao standardni softveri proizvedeni agilnim metodima.

Opšte je mišljenje u forenzičkoj interesnoj zajednici da je potrebno razviti standarde koji definišu očekivana ponašanja forenzičkih alata. Na primer, postoji potreba za standardnim formatom skladišta (baza podataka), formatom uvoza/izvoza (XML, CSV), za skupom zajedničkih indeksa i heš vrednosti i za definisanjem procesa i termina. Problem je dilema o tome ko treba da razvija takve standarde: korisnici, *vendori* ili konzorcijum za digitalnu forenziku. Očigledno je da bi standardizacija, na primer, formata za skladištenje digitalnih dokaza značajno povećala interoperabilnost i kompatibilnost forenzičkih alata. Sa aspekta prakse digitalne forenzičke akvizicije i analize, forenzičar zahteva da ima različite poglede na isti sadržaj sa različitim alatima. Na primer, *Access Data* (alat **FTK**) ima filozofiju da *„forenzički alat treba koristiti toliko dugo koliko daje očekivane informacije forenzičaru"*. Takođe, postoji potreba za većom automatizacijom rutinskih poslova i redosleda izvršavanja zadataka forenzičkih alata, kao i uvođenjem ekspertnih sistema u proces digitalne forenzičke akvizicije i analize.

1.2.9 Legalni zahtevi za digitalne dokaze

Oblast digitalne forenzičke nauke i forenzičke akvizicije i analize digitalnih dokaza još uvek je u razvoju. Nije poznato niti pouzdano utvrđeno da li se kao digitalni dokaz treba smatrati naučno potvrđen dokaz ili izlazni rezultat automatizovanog forenzičkog alata i primenjenih forenzičkih tehnika.

Bez obzira na ovakvo stanje, moraju biti zadovoljeni neki zahtevi da bi se ulazni digitalni podatak u pravosudni slučaj kompjuterskog kriminala smatrao prihvatljivim digitalnim dokazom. Međutim, naučno potvrđen digitalni dokaz mora biti istovremeno i relevantan i pouzdan (neoboriv) za konkretni slučaj. Pouzdanost naučnog dokaza se dokazuje primenom standarda koji zahteva da se procedura dokaznog postupka može testirati, verifikovati i da je metod testiranja naučno priznat. Relevantnost digitalnog dokaza određuje sud u kontekstu slučaja, a na bazi njegove vrednosti za optuživanje ili oslobađanje od krivične odgovornosti. Najčešće same digitalne dokaze treba podržati i sa drugim, fizičkim dokazima iz procesa istrage, uključujući i rezultate ispitivanja svedoka, otiske prsta, razne zabeleške i druge indikatore koji upućuju na identitet osumnjičenog. Višestruko podržani digitalni dokazi imaju veću prihvatljivost na sudu.

1.2.10 Dostupnost standardnih procedura i alata

Pojavom vrhunskih naučnih časopisa (*International Journal of Digital Evidence* i dr.) obajvljenji su i postali šire dostupni brojni radovi iz oblasti forenzičkih alata za akviziciju i analizu digitalnih dokaza sa višestrukom recenzijom. Takođe, objavljeni su brojni, dokumentovani podaci i detalji o tome kako rade i procesiraju različiti fajl sistemi ili kako se oporavljaju izbrisani fajlovi na HD i koliki stepen grešaka unose komercijalni forenzički alati. Pri tome neki fajl sistemi kao što je NFTS nisu čak ni javno dokumentovani – imaju

zatvoren izvorni programski kod. Kako fajl sistemi nisu dizajnirani da imaju neizbrisive fajlove, forenzičari za analizu digitalnih dokaza ne mogu znati koju proceduru koriste njihovi alati u izvršavanju ovih nedokumentovanih akcija.

Zato se za softverske forenzičke alate sa zatvorenim programskim kôdom (npr. **EnCase 4.0**) zahteva višestruko testiranje i objavljivanje rezultata testa sa stepenom greške koju alat unosi, što je prihvatljiva praksa za gotovo sve pravosudne sisteme u zapadnim zemljama. Sa druge strane, proizvođači alata sa otvorenim izvornim kodom uvek korektno objavljuju svoje procedure, pošto je izvorni kod na raspolaganju svakom korisniku koji ga može pročitati i proveri tačnost procedure.

1.2.11 Tela za akreditaciju standarda digitalnih forenzičkih laboratorija

Direkcija američkog udruženja kriminalističkih laboratorija (Bord laboratorija) za akreditaciju (ASCLD/LAB) je telo za akreditaciju koje propisuje kriterijume i standarde, koje specifične naučne i tehničke discipline moraju zadovoljiti i radu forenzičkih laboratorija za digitalne dokaze. Ovo telo izdaje *Priručnik za akreditaciju* koji sadrži: principe, standarde i kriterijume, kao i diskusije (pošto su standardi u razvoju). Priručnik je namenjen za rad menadžmenta forenzičkih laboratorija, radnog osoblja, kvalifikovanih lica-specijalista i laboratorijske opreme.

U SAD je na federalnom nivou osnovana *Asocijacija forenzičkih naučnika za analizu digitalnih dokaza* (AAFS). Članovi AAFS su najeminentniji naučnici koji se bave disciplinama u ovim oblastima, a od njih su mnogi i akademici. Asocijacija zahteva najmanje 50 članova za formiranje sekcije u nekoj državi. Novi članovi se prijavljuju generalnoj sekciji, iz koje se po potrebi mogu formirati odvojene specijalističke sekcije.

Jedan od brojnih problema u oblasti digitalne forenzičke istrage - haos u sertifikaciji *eksperata* za forenzičku analizu digitalnih dokaza, može se razrešiti samo ako se konzistentno primene usvojeni principi na sve oblasti digitalne forenzike za sudsku praksu. Sertifikacija profesija u oblasti digitalne forenzike treba da bude zajedničko pitanje i jedinstveno usklađena na međunarodnom nivou. Moraju postojati univerzalne mere za ocenu individualne kompetentnosti i ekspertskih znanja i veština. Tehnologija digitalne forenzičke istrage, akvizicije i analize zahteva razvoj standarda i protokola. Za praktičnu primenu u forenzičkoj praksi zahteva se obuka i edukacija koja se završava testiranjem stečenih znanja i veština u procesu sertifikacije. Nacionalni centri za sertifikaciju eksperata digitalne forenzike moraju raditi u bliskoj korelaciji sa međunarodnim telima za sertifikacije u ovoj oblasti, [6].

REZIME

Zašto je potreban zakonski i pravni okvir za digitalnu forenzičku istragu, sakupljanje (akviziciju), dokazivanje (analizu) i sankcionisanje (veštačenje/svedočenje i suđenje) slučajeva kompjuterskog kriminala? Nacionalni zakon o borbi protiv kompjuterskog kriminala je neophodan i neizbežan, zbog realnog trenda globalnog rasta kompjuterskog kriminala u svetu, kao formalni okvir za razvoj nacionalnih kapaciteta za istragu, dokazivanje i sankcionisanje krivičnih dela kompjuterskog kriminala. Pravni okvir se zahteva za potrebe nacionalnog pravosuđa i usaglašavanje prakse pavosudnih sistema na međunarodnom nivou, zbog globalnog, transnacionalnog karaktera kompjuterskog kriminala. Standardi i formalne operativne procedure istrage, akvizicije i analize digitalnih dokaza kompjuterskog kriminala neophodne su zbog kompleksnosti i delikatnosti zadataka i specifične prirode digitalnih dokaza.

Svaki slučaj istrage kompjuterskog kriminala zahteva razvoj biznis plana za uspostavljanje forenzičkih kapaciiteta (javnih/korporacijskih), detaljnog plana projekta forenzičke istrage, programa, vremenskog plana, budžeta i kadrova. Krajnji cilj digitalne forenzičke istrage je prikupiti dovoljno podataka i informacija da se krivično delo kompjuterskog kriminala dokaže pred sudom. Nažalost konzistentna tehnologija neophodna za rešenje svih slučajeva kompjuterskog kriminala još uvek ne postoji. Digitalni forenzičar treba znati da svaki upad u računarski i IKT sistem ostavlja brojne tragove, bez obzira koliko su teški za praćenje i otkrivanje. Svaki kompjuterski kriminal je rešiv uz veliko strpljenje i dovoljno znanja i upornosti.

Generalno, istraga kompjuterskog kriminala zahteva mnogo vremena, rada i novca, pa vešti eksperti mogue odužiti procedure u nedogled u cilju sticanja neopravdane koristi. Zato je potrebno uspostaviti i koristiti formalne, struktuirane, zakonski i pravno zasnovane, procedure istrage, akvizicije i analize digitalnih dokaza kompjuterskog kriminala. U najjednostavnijem slučaju zakonski okvir za istragu kompjuterskog kriminala mora obezbediti najmanje proceduru za vođenje istrage o slučaju kompjuterskog kriminala. Što su jasnije definisani proces, metodi i tehnologije istrage slučajeva kompjuterskog kriminala, to je veća verovatnoća za uspešan ishod istrage.

Najsigurniji istražni postupak u slučaju kompjuterskog kriminala je tipa striktnog sprovođenja propisane procedure i izvršavanje aktivnosti korak po korak. Prvo se mora doneti zaključak da je napad izvršen, a zatim proceniti karakter incidenta i doneti odluku o nivou korporacijske, odnosno, zvanične istrage.

Značajno je što se u cikličnom procesu upravljanja kompjuterskim incidentom, na osnovu rezultata digitalne forenzičke istrage, mogu otkloniti uzroci, a ne samo posledice svih bezbednosih ranjivosti računarskog sistema i mreža, koje se otkriju u sistemu zaštite i time poboljšati otpornost IKT sistema na nove napade.

PITANJA ZA PONAVLJANJE

1. Nabrojte osnovne elemente kompjuterskog kriminala.
2. Koje su glavne kategorije kompjuterskog kriminala sa aspekta uloge računara?
3. Navedite neke tipove kompjuterskog kriminala.
4. Ko su glavni korisnici digitalne forenzičke istrage?
5. Koje su glavne oblasti digitalne forenzike?
6. Definišite digitalni dokaz.
7. Koji su glavni IOEC principi upravljanja digitalnim dokazima?
8. Koje glavne elemente treba da sadrži standardna operativna procedura digitalne forenzičke istrage?
9. Navedite *Daubert* principe prihvatljivosti digitalnih dokaza pred sudom.
10. Objasnite pod kojim uslovima sud priznaje digitalne dokaze.

2. ISTRAGA KOMPJUTERSKOG KRIMINALA

2.1 ZVANIČNA ISTRAGA KOMPJUTERSKOG KRIMINALA

Generalno, digitalna forenzička istraga deli u dve osnovne kategorije, [3]:

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

Zvanična (javna) digitalna forenzička istraga uključuje policijske organe istrage, specijalno tužilaštvo i specijalno sudstvo za borbu protiv visokotehnološkog (kompjuterskog) kriminala. Ovi organi treba da rade u skladu sa brojnim zakonima kao što su: *Zakon o krivičnom postupku*, *Zakon o borbi protiv visokotehnološkog kriminala, Zakon o zaštiti informacija i informacionih sistema, Zakon o digitalnom dokazu, Zakon o elektronskom potpisu, Zakonu o elektronskoj trgovini* i dugi neophodni zakoni koji regulišu ukupno savremeno elektronsko poslovanje. Takođe, zvanični organi istrage kompjuterskog kriminala treba da rade prema strogo utvrđenim *standardnim operativnim procedurama* (SOP) za: pretragu, privremeno oduzimanje i ispitivanje računarskih sistema i drugih mrežnih uređaja, akviziciju digiotalnih podataka/dokaza sa različitih platvormi i slika, u cilju otkrivanja validnih digitalnih dokaza. U slučaju zvanične istrage istražni organi moraju dobro poznavati i razumeti sve zakone i propise koji se odnose na kompjuterski kriminal, uključujući standardne lokalne procedure za pretragu i utvrđivanje slučaja krivičnog dela kompjuterskog kriminala.

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

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

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

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

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

Opšti proces zvanične istrage kompjuterskog incidenta, sa pristupom istrazi po modelu "korak po korak", gde svaki korak u okviru jedne faze istrage vodi u drugi i obezbeđuje kontrolnu listu aktivnosti u okviru svake od sledeće 4 faze, [18], [20]:

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

U realnom slučaju krivičmog dela kompjuterskog kriminala tipičan proces istrage kreće od prijave kompjuterskog incidenta zvaničnim organima istrage (policiji). U fazi predistražnih radnji i pretrage istražni organi sakupljaju dovoljno dokaza za osnovanu sumnju i pokretanje tužbe protiv osumnjičenog počinioca (nekada može biti i nepoznat-NN počinila). O svojim nalazima policija upoznaje tužioca koji obezbeđuje nalog za istragu od istražnog sudije i pokreće zvaničnu istragu. Sa sudskim nalogo u gotovo svim pravosudnim sistemima organi istrage kompjuterskog kriminala mogu legalno privremeno oduzimati osumnjičeni računarski sistem ili uzimati fizičku sliku čvrstog diska, radi forenzičke akvizicije i analize digitalnih dokaza.

Iako policija svake države štiti javna dobra svojih građana, ne treba očekivati da svaki policajac bude IKT ekspert i da sve faze istrage kompjuterskog kriminala izvršavam samostalno. U tom smislu, preporučena su tri nivoa potrebnih stručnih znanja i veština zvaničnih organa istrage, [5]:

1. Nivo: Osposobljenost za akviziciju digitalnih podataka i privremeno čuvanje integriteta i propisno održavanje digitalnih dokaza. Ove poslove treba da obavljaju regularni kriminalistički tehničari (policajci) sa osnovnim informatičkim znanjima i osnovnim kursom digitalne forenzike;

2. Nivo: Osposobljenost za upravljanje procesom istrage visokotehnološkog kriminala. Organi istrage se osposobljavaju da postavljaju pitanja, ispituju informante (svedoke) razumeju IKT terminologiju i šta može, a šta ne može biti izvučeno iz digitalnih podataka. Ove poslove treba da obavljaju kriminalistički inspektori (policajci) sa završenim specijalističkim kursom za digitalnu forenzičku istragu kompjuterskog kriminala i oporavak digitalnih podataka, uključujući i osnove digitalne forenzike računarskih sistema.

3. Nivo: Specijalno osposobljeni policajci za izvlačenje, ispitivanje i analizu digitalnih dokaza, koje normalno izvršavaju specijalisti za digitalnu forenzičku analizu računara i računarskih mreža, ili kibernetičku (*cyber*) istragu kompjuterskih i Internet prevara. Zvanični organi istrage osposobljeni sa ovim znanjima i veštinama mogu kompetentno da upravljaju slučajem krivičnog dela kompjuterskog kriminala, uspešno obezbeđuju resurse za istragu, procenjuju obim istrage, delegiraju uloge i lica za sakupljanje i procesiranje informacija koje se odnose na osumnjičenog, kao i za akviziciju i analizu digitalnih podataka iz oštećenog, posrednih i osumnjičenog računara i izgradnju čvrstih dokaza. Posao istražitelja kompjuterskog kriminala završava se kada se pomoću propisane

procedure (SOP) i prihvatljive metodologije izvuku relevantni i čvrsti digitalni dokazi iz procesom akvizicije obezbeđenih i drugih izvora podataka.

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

2.2 KORPORACIJSKA DIGITALNA FORENZIČKA ISTRAGA

Savremeni novi mobilni telefoni, *Bluetooth* uređaji, kompaktne fleš memorijski uređaji i razni PDA mogu izvršiti gotovo sve zadatke kao laptop računari, uključujući i udaljeni pristup računarskoj mreži bez znanja organizacije. Ovo je samo deo sistema nove tehnologije koji zahteva zaštitu u IKT sistemu organizacije, ali predstavlja i izazov za primenu tehnika i alata korporacijske digitalne forenzike za rekonstrukciju kompjuterskog incidenta. U uslovima dinamički promenljivih kombinovanih pretnji koje mogu iskoristiti brojne slabosti web servisa i računarskih mreža organizacije, razumevanje uzroka i sprečavanje ponavljanja incidenta jednako je važno kao i sam sistem zaštite organizacije. Za otkrivanje uzroka i otklanjanje ranjivosti koje su dovele do incidenta, organizacija uvek može iznajmiti retke specijaliste za digitalnu forenziku, ali je za sada ta usluga najskuplji servis u sektoru zaštite informacija, što je najčešće ograničavajući faktor. Iako je korporacijska digitalna forenzika u ranoj fazi razvoja, izazovi i rizici koje donose nove, mobilne tehnologije nesumnjivo će uticati na sve veću primenu forenzičkih tehnika i alata u upravljanju kompjuterskim incidentom u organizaciji.

U kontekstu upravljanja kompjuterskim bezbednosnim incidentom u korporacijskom IKT sistemu, metodologija i tehnologija digitalne forenzičke istrage obezbeđuju stabilnu i kompletnu celinu u ranjivom mrežnom okruženju sa uspostavljenim politikama zaštite, implementiranim sistemom zaštite i uspostavljenim kapacitetima za upravljanje kompjuterskim incidentom. Dobra je praksa da *korporacijski digitalni forenzičar* timski radi sa administratorima sistema, mreže i zaštite i drugim specijalistima zaštite u cilju obezbeđivanja prihvatljivog nivoa zaštite računarskih sistema i bezbednog rada računarske mreže u Internet okruženju. Iako sve tri grupe specijalista u velikim sistemima najčešće rade samostalno, u slučaju glavnog kompjuterskog incidenta sve tri grupe uvek rade zajedno. Ovakav *koraborativni*[7] rad obezbeđuje efikasno i efektivno trajno saniranje kompjuterskog incidenta u organizaciji, sa sopstvenim resursima i bez

7 rad članova tima na različitim izvorima indikatora i dokaza istog kompjuterskog incidenta.

pozivanja spoljnih specijalista. Specijalisti za sisteme zaštite, analizu rizika i ranjivosti sistema i mreža imaju iskustvo iz administracije sistema i mreža i poznaju neku metodologiju za analizu i ublažavanje rizika. Specijalisti za upravljanje kompjuterskim incidentom poznaju automatizovane detektore upada (IDS/IPS tipa), monitorišu logove logičkih mrežnih barijera (*firewalls*), otkrivaju, prate, identifikuju i sprečavaju upade u računarske mreže i, u slučaju napada, pomažu forenzičarima da rekonstruišu napad, oporave podatke i identifikuju napadača. Digitalni forenzičari ispituju napadnute, kompromitovane ili osumnjičene računarske sisteme, uključujući i posredne računare, koji sadrže potencijalne dokaze o kompjuterskom incidentu/kriminalu i dostavljaju nalaze o načinu napada članovima druga dva tima za efektivno fiksiranje i trajno *otklanjanje* otkrivenih ranjivosti sistema. Bliskom saradnjom ovih specijalista, efektivno se sprečava ponavljanje istog ili sličnog incidenta i dugoročno podiže bezbednost sistema na viši nivo.

Potrebu za razvojem korporacijske digitalne forenzike mogu generisati različiti izvori, [3].

- interni zahtevi politike zaštite korporacije/organizacije za upravljanje kompjuterskim incidentom;
- spoljni faktori kao što su međunarodni zahtevi za standardizaciju i usklađivanje upravljanja zaštitom informacija, zadržavanja informacija itd.;
- razvoj sofisticiranih hakerskih alata i veština napada na računarske sisteme i mreže;
- nacionalni zakoni i regulative koji postoje u većini zemalja, mogu zahtevati uspostavljanje nekih oblika forenzičkih kapaciteta za borbu protiv kompjuterskog kriminala, kao što su zakoni o zadržavanju informacija (npr. Švajcarski zakon *ISP log retention*), regulative i standardi u industriji, zdravstvu, finansijskom sektoru itd.;
- standardi industrijske najbolje prakse u oblasti zaštite informacija, kao što su ISO/IEC 27001 (17799:2005) i drugi serije ISO/IEC 27k međunarodni standardi za zaštitu informacija, koji preporučuje procedure za skupljanje informacija i dokaza, analizu i procenu incidenata, zadržavanje e-mail poruka i slika, ili IAAC (*Information Assurance Advisory Council*) smernice, koje daju uputstva za obezbeđivanje korporacijskih forenzičkih kapaciteta;
- objavljivanje forenzičkih procedura i alata u višestruko recenziranim naučnim časopisima kao što su *Digital Investigation Journal*, *The International Journal of Digital Forensics & Incident Response* i drugim.

Ako neka korporacija/organizacija odluči da uspostavi sopstvene kapacitete za digitalnu forenzičku istragu na bazi internih potreba i zahteva politike zaštite za upravljanje kompjuterskim incidentom, očekuje se da zvanični državni organi za borbu protiv kompjuterskog kriminala u svakoj nacionalnoj državi obezbede:

- pomoć legalnim timovima korporacija/organizacija za upravljanje kompjut-

erskim incidentom kod otkrivanja uzroka incidenta i napadača, posebno iz drugog domena zaštite (drugog ISP), ili drugog pravosudnog sistema u kojima korporacijski organi istrage nemaju nikakvu nadležnost;

- usaglašavanje korporacijske politike/standarda zaštite sa lokalnim zakonima i regulativama, što može biti od velike koristi za razvoj forenzičkih kapaciteta;
- preporuke i procedure za kontrolu (*auditing*) sistema zaštite i
- informacije za obrazovanje u oblasti digitalne forenzike (npr. *International Journal of Digital Evidence* i slika).

Uspostavljanje korporacijskih kapaciteta za digitalnu forenziku može se pozitivno odraziti i u oblasti upravljanja ljudskim resursima. Proces korporacijske digitalne forenzičke istrage, forenzičke tehnike i alati mogu obezbediti ključne informacije za različite aspekte upravljanja ljudskim resursima, kao što su: otpuštanje zaposlenih i ukidanje radnih mesta, upravljanje zaposlenim, disciplinske akcije, procena ekstremnih slučajeva (smrti, samoubistava, kidnapovanja) i slika Od korporacijskih forenzičkih kapaciteta velike koristi mogu imati i različita stalna/privremena tela i timovi koji se formiraju u korporaciji, kao što su timovi za: istragu klasičnih prevara i kriminala, upravljanje kompjuterskim incidentom i vanrednim događajem, upravljanje rizikom, procenu rizika, kontrolu rizika od kompjuterskog kriminala, upravljanje kontinuitetom poslovanja itd. Sve ove uloge imaju potrebu da koriste usluge kompetentnog centralnog tima za zaštitu informacija sa digitalnim forenzičarom koji dobro poznaje forenzičke tehnike i alate.

Korporacijski kapaciteti za digitalnu forenziku mogu, takođe, odigrati značajnu ulogu za zaštitu intelektualne svojine, ugleda i brendova korporacije, ispitivanjem lažnih web sajtova, *phishing* napada itd.

U IKT sistemu korporacije, forenzički kapaciteti su od ključnog značaja za analizu tragova upada u sistem, ispitivanje povreda politika zaštite, utvrđivanje zloupotreba IKT infrastrukture, analizu prisustva logičkih bombi, rutkit tehnika, zadnjih vrata, trojanaca i drugih malicioznih kodova. Forenzičke alate i tehnike, korporacija može koristiti i za:

- verifikaciju procedura za saniranje korporacijskih diskova za skladištenje brisanjem sa prepisivanjem (*wiping*),
- verifikaciju implementacije šifarskih sistema na disku/u mreži,
- oporavak podataka sa pokvarenih HD i starih/zastarelih medija,
- oporavak lozinke na legitimne zahteve,
- utvrđivanje skrivenih grešaka i
- dizajn i arhitekturu IKT sistema koji obezbeđuju uspostavljanje forenzičkih kapaciteta korporacije.

Glavni problemi u procesu uspostavljanja forenzičkih funkcionalnosti u korporaciji su određivanje osnovnih potreba/zahteva za digitalnog forenzičara/tim forenzičara i nekih ključnih faktora za implementaciju uloge digitalnog forenzičara u organizaciji. Prirodno je da se uloga digitalnog forenzičara uspostavlja u korporacijskom timu za upravljanje kompjuterskim incidentom.

2.2.1 Uspostavljanje tima za upravljanje kompjuterskim incidentom

Sa aspekta efektivnosti sistema zaštite, korporacijski tim za upravljanje kompjuterskim incidentom u svim aspektima zaštite informacija, uključujući korporacijsku forenzičku istragu, treba da bude centralizovan za sve delove korporacije. Tim može biti uspostavljen od kompetentnih zaposlenih koji obavljaju redovne poslovne zadatke, a u timu rade po potrebi i u slučaju glavnog kompjuterskog incidenta. Neki ili svi članovi tima mogu biti iznajmljeni, što može predstavljati dodatnu ranjivost korporacije. Velike korporacije mogu imati poseban tim samo za digitalnu forenzičku istragu, akviziciju i analizu. Tipični tim za upravljanje bezbednosnim kompjuterskim incidentom treba da uključi sledeće uloge/profile zaposlenih ili iznajmljenih specijalista:

1. Menadžer zaštite informacija - CIO (*Chief Information Officer*);
2. Administrator računarskog sistema/mreže;
3. Specijalista za upravljanje i kontrolu bezbednosnog rizika;
4. Kontrolor sistema kvaliteta;
5. Predstavnici drugih timova (za vanredne događaje, usaglašenost standarda i slika)
6. Digitalni forenzičar;
7. Pravnik organizacije;
8. Menadžer za upravljanje ljudskim resursima.

Ključni nedostatak centralizovanog upravljanja kompjuterskim incidentom i sistemom zaštite u celini, može biti činjenica da se postepeno klasična paradigma savremenih organizovanih malicioznih, hakerskih napada sve više pomera na centralizovane entitete za upravljanje zaštitom informacija u korporaciji/ organizaciji.

Veoma je korisno da korporacija generiše i implementira *Politiku digitalne forenzičke istrage* sa saopštenjima koja omogućavaju ovlašćenim zvaničnim organima istrage da pristupe sistemu i izvrše akviziciju digitalnih podataka u fazi uključivanja zvaničnih organa istrage u korporacijsku forenzičku istragu. Saopštenja ove politike treba da sadrže najmanje sledeće zahteve za:

- zaštitu osetljivih podataka,
- smanjenje rizika kod pristupa (kontrolisati i logovati sve pristupe),
- definisano vreme zadržavanja informacija (e-mail poruka i dr.),
- usklađivanje sa legalnim i regulatornim zahtevima,
- odgovore na bezbednosne incidente,
- forenzički oporavak i istragu incidenta,
- uspostavljanje forenzičkih resursa (kapaciteta) korporacije,
- obuku i osposobljavanje forenzičara/tima potrebnim znanjima i veštinama,
- opremu forenzičke laboratorije i terenskih forenzičkih alata i
- iznajmljivanje spoljnih partnera i eksperata u slučaju potrebe.

Uspeh uspostavljanja korporacijskog tima za upravljanje kompjuterskim incidentom sa sopstvenim kapacitetima za korporacijsku digitalnu forenzičku istragu, u najvećoj meri zavisi od podrške menadžmenta korporacije. U prvom redu, potrebno je *ubediti* menadžment da je takav tim potreban korporaciji i da može doneti vidljive koristi. Pažnju treba usmeriti na razvoj opšte spremnosti korporacije da upravlja kompleksnim kompjuterskim incidentom, analogno pripremi za protiv požarnu zaštitu. Sve razloge treba ilustrovati sa najnovijim primerima štetnih posledica za brojne organizacije u svetu od raznih tipova zloupotreba računara i kompjuterskog kriminala. Praksa zaštite nesumnjivo potvrđuje da je spremnost korporacija/organizacija da razviju i implementiraju adekvatne sisteme zaštite informacija, proporcionalna količini akumuliranog straha menadžmenta od posledica koje su imale druge slične korporacije/organizacije[8]. Dobro je ilustrovati troškove jednog slučaja suđenja kompjuterskog kriminala i time opravdati troškove uspostavljanja forenzičkih kapaciteta korporacije. U ovom *markentiškom* procesu neophodno je razvijati svest o potrebi zaštite i kod drugih grupa zaposlenih, uključujući krajnje korisnike, i obezbediti opšte razumevanje i podršku cele organizacije. U prezentaciju treba uključiti tok procesa uspostavljanja kapaciteta korporacijske digitalne forenzičke istrage, potrebnu logističku i stručnu podršku i navesti postojeće kompetentne, nacionalne digitalne forenzičke centre.

Od posebnog značaja je uspostavljanje pouzdane, potpune i efikasne komunikacije između zaposlenih i interventnog tima i obrnuto. Korisno je odrediti odgovorna lica i navesti kontaktne informacije članova tima iz različitih delova IKT sistema i organizacije za potrebe sakupljanja digitalnih dokaza, kao i kontaktne informacije sa spoljnim saradnicima i konsultantima. Interventni tim treba da definiše i objavi sve komunikacione kanale, uključujući e-mail adresu, telefone, web lokaciju i dr.

Politika korporacijske digitalne forenzičke istrage treba da zahteva obaveznu obuku za sticanje različitih znanja i veština iz oblasti zaštite IKT sistema, upravljanja rizikom, upravljanja bezbednosnim incidentom i digitalne forenzičke istrage, akvizicije, oporavka podataka, analize i prezentacije digitalnih dokaza. Težište na obuci treba da bude na poznavanju metoda i procedura, razumevanju novih forenzičkih tehnika i alata. Cilj je da u korporacijskom timu za upravljanje kompjuterskim incidentom budu *sertifikovani* članovi iz relevantnih oblasti, kao što su **CISSP** (*Certified Information System Security Professionals*) za zaštitu IKT sistema ili na primer, **EnCE** (*EnCase Examiner*) – ovlašćeni forenzičar za ispitivanja sa **EnCAse** forenzičkim alatom i slika

2.2.2 Procedura određivanja karaktera kompjuterskog incidenta

Statistički gledano prosečan kompjuterski incident najčešće nije kriminalni akt. Međutim, u toku predistražnih i istražnih radnji treba verovati indikacijama istrage, a ne statističkim pokazateljima. Na bazi rezultata procesa određivanja karaktera kompjuterskog incidenta, čak i površnog i preliminarnog uvida u posledice incidenta, vlasnik

8 Istraživanje kompanije ORACLE u toku 2008. godine.

sistema donosi odluku da li će nastaviti istragu unutar organizacije sopstvenim kapacitetima, iznajmiti spoljne saradnike – eksperte, slučaj predati zvaničnim organima istrage, podići optužbu i slika

U svakom slučaju korporacijske, kombinovane ili zvanične istrage karaktera kompjuterskog incidenta, treba:

- Napraviti detaljan izveštaj o svim nalazima, dokumentovati izveštaj i nalaze i dati predlog/preporuku za dalji postupak;
- Dokazne materijale pažljivo markirati obojenom samolepljivom nalepnicom / trakom, sortirati u odvojene koverte sa detaljnim oznakama o sadržaju svake. Oznaka treba da ima mesta za potpis lica koje preuzima dokazni materijal u daljem postupku. Oznaku staviti preko strane koverte koja se lepi, tako da se pokaže da koverta nije otvarana;
- Kada se neki fajl memoriše kao digitalni dokaz, mora se zaštititi od izmene. Za zaštitu integriteta treba koristiti standardni *hash* program (SHA-256, SHA-512 i dr.) koji daje jedinstven sažetak fajla. Svaka i najmanja promena u fajlu menja *hash* vrednost fajla. Zatim se sažetak fajla zajedno sa fajlom digitalnog dokaza šifruje javnim ključem asimetričnog algoritma (raspoloživog na Internetu) i memoriše. Tako zaštićen dokaz se kada zatreba dešifruje privatnim ključem (matematičkim parom javnog ključa) i verifikuje se *hash* vrednost sa istim *hash* algoritmom. Ako je ova vrednost jednaka originalnoj vrednosti *hash-a* upravo dešifrovanog fajla sa digitalnim dokazom, onda nije bilo izmene i dokaz je prihvatljiv na sudu. Na sličan način, integritet fajla sa digitalnim dokazom može se bezbedno skladištiti i prenositi primenom digitalnog sertifikata i digitalnog potpisa u uspostavljenom PKI sistemu;
- Dobro je u izveštaju pomenuti svaki pojedinačni dokaz pod jedinstvenim brojem evidencije na koverti, što olakšava kasnije snalaženje;
- Izveštaj treba početi sa kratkim sadržajem incidenta (*Executive Summary*) u kojem se opisuje incident, metod istraživanja i generalne zaključke po redosledu izvedenih dokaza. U posebnom poglavlju detaljno opisati svaki navedeni zaključak posebno ukazujući na čvrste (neoborive) dokaze koji podržavaju ili osporavaju postavljenu hipotezu i zaključke;
- Vremenska evidencija je najbolji dokaz za zaključivanje o incidentu. Ako se obezbedi dokaz o *vremenskoj liniji* upada u sistem, u svim log fajlovima mrežnih uređaja i napadnutog računara, onda je to čvrst dokaz za slučaj. Treba imati na umu da se vreme i datum lako menjaju, pa je potrebno ovaj dokaz podupreti sa drugim dokazima iz napadnutog računara;
- Najniži rezultat istrage mora biti dovoljan za odluku na nivou organizacije - šta dalje uraditi sa istragom: obustaviti, nastaviti u organizaciji ili predati zvaničnim organima. Ta odluka najviše zavisi od prezentacije zaključaka i materijalnih dokaza za svaki zaključak;

- Izveštaj treba završiti sa preporukom kako sprečiti da se incident ne ponovi i šta dalje učiniti sa istražnim postupkom.

2.2.3 Model troškova korporacijske forenzičke istrage

Zahtevi za uspostavljanje digitalne forenzičke laboratorije i rad na terenu treba da sadrže specifikaciju kategorija (ne konkretnih proizvoda) neophodnih hardverskih i softverskih forenzičkih alata, kao što su forenzički računarski sistemi za akviziciju, analizu i testiranje, blokatori upisivanja, komercijalni alati zatvorenog izvornog koda, alati Linux/otvorenog koda i druga stacionarna/mobilna laboratorijska oprema (npr., stari mediji drajveri i tehnologija).

Na kraju korporacijska politika zaštite treba da preporuči referentne izvora za obuku iz oblasti digitalne forenzičke istrage kao što su: web lokacije[9], relevantni časopisi[10] i relevantni alati - komercijalni sa zatvorenim izvornim kodom (**EnCase**, **FTK** itd.) i sa otvorenim izvornim kodom (**Linux**, **Sleuthkit** itd.).

Kada se kompjuterski incident dogodi, kritičan faktor je brzina reakcije. U početnoj praksi forenzičke istrage kompjuterskog kriminala, pokazalo se da su podaci otkriveni u toku prvih *sedam* dana bili kritični za uspešan oporavak. Danas je to vreme znatno kraće i reda je nekoliko časova.

Za donošenje odluke o uključivanju internog, ili eksternog tima u digitalnu forenzičku istragu, organizacija treba da razmotri i izbalansira sledeće faktore, [27]: *troškove, vreme odgovora i osetljivost podataka*

Troškovi obuhvataju nabavku, ažuriranje i održavanje forenzičkog softvera, hardvera i opreme koja se koristi za skupljanje i ispitivanje podataka, a može uključivati i dodatnu fizičku zaštitu od njihove kompromitacije. Drugi značajni troškovi uključuju obuku osoblja i troškove rada, koji su posebno značajni za profesionalne forenzičare. Generalno, retko su troškovi angažovanja spoljnih forenzičara skuplji od troškova interne forenzičke istrage.

Jednostavan model troškova forenzičkog ispitivanja digitalnih uređaja pretpostavlja da postoji skup nekompatibilnih platformi, različitih tehnologija i očekivani broj uređaja za forenzičko ispitivanje i da razvoj metoda za forenzičku akviziciju i analizu ima neke fiksne troškove. Pretpostavlja se da su ovi troškovi isti za jednu tehnologiju, iako je u praksi skuplji reverzni inženjering autorskog formata digitalnih podataka, nego razvoj softvera za procesiranje otvorenog standarda. Međutim, u ovom modelu mere se troškovi porasta forenzičke akvizicije i analize zbog nekompatibilnosti platformi (hardvera i sistemskog softvera), odnosno formata (OS, fajl sistema, brauzera, e-mail sistema i slika). Model, takođe, pretpostavlja da je **F » MC**, pa su ukupni troškovi – **c(M)** za analizu digitalnih uređaja jednaki:

9 www.e-evidence.info; www.forensicswiki.org; www.forensicfocus.com i dr.

10 Elsevier's Digital Investigation Journal, International Journal of Digital Forensics & Incident Response, International Journal of Digital Evidence (IJDE) i dr.

$$c(M) = F * |M| + MC * \sum_{i=1}^{|M|} m_i$$

gde je:

M – broj nekompatibilnih platformi digitalnih uređaja,

i – broj različtih tehnologija digitalnih uređaja,

mi – očekivani broj uređaja digitalnih uređaja,

F – visoki fiksni troškovi ekstrakcije digitalnih podataka,

MC – marginalni troškovi ispitivanja (rada forenzičara na akviziciji i analizi).

U visoko distribuiranom zatvorenom okruženju (npr., u mreži ekstranet tipa) sa mnogo nekompatibilnih formata, |**M**| je velik, pa su i uključeni troškovi veliki. Ako su sistemi bazirani samo na nekoliko otvorenih standarda, tada su troškovi mnogo niži. Takođe, se uzima u obzir da dominira nekoliko popularnih tehnologija, distribuiranih u svetu, koje se u određenom okruženju mogu svesti na nekoliko relevantnih tehnologija, što je i slučaj sa mobilnim telefonima (*Simens, Motorola, Nokia, Sony Ericson, LG i Samsung*). Treba očekivati različitu distribuciju zavisno da li preovlađuje otvoreni ili zatvoreni (vlasnički) standard formata. Ova distribucija može imati veliki uticaj na stepen razvoja validne tehnike za ekstrakciju digitalnih podataka iz digitalnih uređaja. Pretpostavimo da su sve **i-te** platforme, potencijalno ciljne za forenzičko ispitivanje, poređane po zastupljenosti (popularnosti), tako da je, [3]:

m1 > m2 > : : : mi |M|

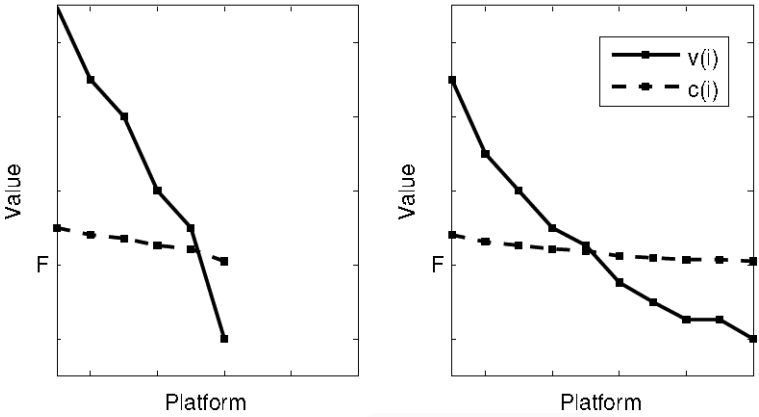
Sada se može definisati funkcija vrednosti:

v(i) = mi * fi * u,

gde je:

u – očekivana korisnost ekstrahovanih podataka (dokazujuća ili oslobađajuća vrednost digitalnog dokaza).

Na slici 2.1 prikazan je dijagram zavisnosti funkcija vrednosti **v(i)** prema troškovima **c(i),** gde je **c(i) = F + MC * fi* mi,** za dve različite vrednosti distribucija. Dijagram na levoj strani odgovara koncentrovanoj distribuciji na nekoliko standardnih platformi, dok se dijagram na desnoj strani odnosi na distribuciju u kojoj dominiraju zatvoreni formati. Treba zapaziti da se tačka u kojoj troškovi premašuju korist (vrednost) dostiže mnogo brže kada se koriste zatvoreni (vlasnički) sistemi. Tako da nisu samo ukupni troškovi ekstrakcije digitalnih podataka veći kod forenzike vlasničkih (zatvorenih) sistema, nego se uvećavaju dalje socijalni troškovi sa povećanjem broja takvih platformi koje ne garantuju razvoj odgovarajućih softverskih alata za oporavak podataka.



Slika 2.1 Hipotetička distribucije vrednosti i troškovi za otvorene, standardizovane (levo) i zatvorene, autorske (desno) platforme

Vreme odgovora na kompjuterski incident postaje sve kraće. Personal lociran na lokaciji incidenta može inicirati forenzičku istragu znatno brže od iznajmljenog tima. Takođe, za fizički distribuirane organizacije personal na lokaciji incidenta može brže reagovati nego tim iz centra organizacije.

Osetljivost podataka može uticati da organizacija odustane da angažuje spoljni forenzički tim, koji za analizu treba da uzme fizičku kopiju (imidž) čvrstog diska i pri tome ima pristup svim podacima, pošto na disku mogu biti važne privatne informacije, finansijski izveštaji, ili druge osetljive informacije. Međutim, ako postoje indicije da je član internog tima umešan u incident, onda je bolje angažovati spoljni forenzički tim.

Upravljanje bezbednosnim kompjuterskim incidentom može biti efikasnije i efektivnije, ako se forenzičke procedure ugrade u životni ciklus sistema IKT zaštite, kao na primer:

- regularno bekapovati sisteme i održavati prethodne bekape određeni vremenski period,
- omogućiti regularnu kontrolu (*audit*) radnih stanica, servera i mrežnih uređaja,
- prosleđivati rezultate kontrole u centralizovane log servere,
- konfigurisati log fajlove aplikacija kritičnih za misiju za kontrolu (*audit*), uključujući evidentiranje pokušaja ponovljenog autentifikovanja,
- održavati bazu sažetaka (*hash* funkcija) fajlova za uobičajene sistemske i aplikativne softvere i proveravati integritet softvera za važne sisteme,
- održavati evidenciju osnovne (*baseline*) konfiguracije mreže i sistema,
- u skladu sa pravosudnim zahtevima, uspostaviti politiku zadržavanja podataka za potrebe revizije istorije aktivnosti sistema i mreže u slučaju incidenta, kao i uništavanja nepotrebnih podataka, i

- razvijati forenzička uputstva i procedure konzistentno sa politikama organizacije i svim primenljivim zakonima, a u razvoj uputstava i procedura uključiti tehničke eksperte, pravne savetnike i menadžment.

Forenzičke tehnike i alati korisni su i za mnoge druge tipove zadataka, kao što su:

- *Otkrivanje grešaka*, pronalaženje virtuelne i fizičke lokacije hosta u nekorektno konfigurisasnoj mreži, rešavanje nekog funkcionalnog problema aplikacija, snimanje i revizija tekućeg OS i podešavanje konfiguracije aplikacije hosta.
- *Monitorisanje log datoteka*, kao što su analiza ulaza i koordinacija ulaza u log fajl iz više sistema, što može pomoći kod upravljanja kompjuterskim incidentom, identifikovanja povreda politika, kontrole (*auditing*) i drugih zadataka zaštite.
- *Oporavak podataka* izgubljenih u sistemu, uključujući podatke koji su slučajno, ili namerno izbrisani, ili na drugi način modifikovani. Količina podataka koji se mogu oporaviti zavisi od slučaja.
- *Akvizicija podataka* iz hosta koji se premešta, ili povlači iz primene. Na primer, kada korisnik napušta organizaciju, podaci sa njegove radne stanice mogu se skinuti forenzičkim alatom i uskladištiti za kasniju upotrebu, a mediji sanirati na forenzički način, da se uklone svi originalni podaci korisnika.
- *Obaveza po dužnosti/usklađenost sa regulativom*, u skladu sa zakonom, zahteva se da organizacije zaštite osetljive podatke i održavaju određene evidencije za potrebe kontrole (*auditing-a*). Takođe, zaštićene informacije su izložene i dostupne i drugim entitetima, pa se od organizacija zahteva da ih evidentiraju. Sve ove zadatke mogu obaviti forenzički alati.

Primarni korisnici forenzičkih alata i tehnika unutar neke organizacije, obično se dele u sledeće grupe:

- *Istražitelj* unutar organizacije najčešće dolaze iz redova kontrolnih organa/ inspekcije i kontrole kvaliteta, a odgovorni su za istragu navoda o zloupotrebama u IKT sistemu. Tipično koriste brojne forenzičke tehnike i alate. U istragu mogu biti uključeni i drugi organi, kao što su pravnici, predstavnik za ljudske resurse, zvanični organ istrage i drugi članovi izvan organizacije koji nisu deo internog tima za istragu.
- *IKT Profesionalci,* uključujući osoblje za tehničku podršku sistema i administratore sistema, mreže i zaštite. U toku rutinskog izvršavanja poslova, oni mogu koristiti relativno mali broj forenzičkih tehnika i alata, specifičnih za njihove oblasti rada, npr., za monitoring, detekciju grešaka i oporavak podataka.
- *Tim za upravljanje kompjuterskim incidentom* odgovara na različite bezbednosne kompjuterske incidente. Tipično koristi veliki broj različitih forenzičkih tehnika i alata u toku svoje istrage kompjuterskog incidenata.

2.3 PROCES KORPORACIJSKE ISTRAGE

U odnosu na zvaničnu digitalnu forenzičku istragu, istraga kompjuterskog incidenta na korporacijskom nivou, može se smatrati *predistražnim postupkom* zvanične istrage kompjuterskog incidenta/kriminala, a odvija se u tri glavne faze, [18], [21]:

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

Pokretanje istrage obuhvata obezbeđivanje mesta incidenta, pretragu, akviziciju dokaza, izradu hipoteze o upadu i istraživanje alternativnih objašnjenja.

Određivanje karaktera incidenta obuhvata analizu incidenta, analizu dokaza sakupljenih u prvoj fazi zajedno sa alternativnim objašnjenjima i određivanje karaktera incidenta – da li je bezbednosni incident krivično delo, ili prirodan događaj.

Analiza digitalnih podataka obuhvata analizu celokupnog digitalnog i analognog dokaznog materijala, pripremu digitalnih dokaza za prezentaciju incidenta i drugih nalaza istrage vlasniku IKT sistema, ili zvaničnim organima, ako to vlasnik odobri.

Procedura korporacijske istrage kompjuterskog incidenta, u opštem slučaju, treba da obuhvata i sledeće postupke, [18]:

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

Dok se težište klasične istrage krivičnog dela uvek usmerava na svedoke i osumnjičene, u korporacijskoj istrazi kompjuterskog incidenta najbolje rezultate daje timski rad iskusnih organa istrage i eksperata za IKT. U istrazi kompjuterskog kriminala, generalno, ne postoji *superpolicajac* koji sam može rešiti čak i relativno jednostavniji slučaj kompjuterskog kriminala. Na isti način, timskim radom treba istraživati i kompjuterske incidente na korporacijskom nivou, u kojem treba da učestvuju najmanje administrator zaštite, administrator sistema i forenzičar. Svaki učesnik ima svoj zadatak u skladu sa svojom specijalizacijom i znanjem.

Za istragu na korporacijskom nivou primenljiva su, gotovo uvek prve tri faze zvanične istrage (osim hapšenja), koje su primenljive za vlastitu istragu u okviru korporacije. Da bi uspeh korporacijske istrage kompjuterskog incidenta bio potpun, ove tri faze istrage treba izvršavati kroz sukcesivno izvršavanje 7 sledećih koraka (originalno 6 *Rosenblatt*-ovih), [38]:

- Eliministi očiglednosti;

- Postaviti hipotezu o napadu;
- Rekonstruisati krivično delo;
- Otkriti trag do osumnjičenog računara sa koga je napad izvršen;
- Analizirati izvorni, ciljni i posredne računare;
- Skupiti dokaze, uključujući, ako je moguće i sam računar i
- Predati nalaze i dokazni materijal korporacijskim, ili zvaničnim organima istrage za dalji postupak.

Eliminisanje očiglednosti: Istraga počinje sa eleminisanjem očigledno nemogućeg u slučaju incidenta u IKT sistemu. Najvažnije je odrediti da li se bezbednosni incident stvarno dogodio, jer računarski sistem može pasti iz mnogo razloga. Na primer, ako nema modema na napadnutom računaru, sigurno je da napad nije došao telefonskom linijom, nego iz lokalne mreže, ili samog napadnutog računara. Potrebno je vrlo pažljivo evaluirati putanje prema napadnutom računaru i analizirati mehanizme kontrole pristupa na mestu upada. U slučaju napada sa Interneta broj mogućih izvora praktično je neograničen. Ako se ne suzi polje vektora mogućih napada, ne postoji ni najmanja nada da će se napadač sa Interneta otkriti. Osim tehničkog aspekta, mora se analizirati i ljudski faktor. Na primer, od 4 administratora može se isključiti samo onaj koji je bio na planinarenju, bez struje i telefona.

Za vođenje preliminarnog informativnog razgovora sa očevidcima i svedocima treba:

- sakupiti informacije o pozadini i okruženju napadnutog računara,
- sakupiti detaljne informacije o incidentu sa aspekta žrtve napada,
- sakupiti dokaze o incidentu na napadnutom računaru (ne posrednim) i
- utvrditi tragove i dokumentovati procenjenu nastalu štetu u novčanim jedinicama.

Izrada hipoteze o napadu: Cilj procesa stvaranja hipoteze o napadu je razumeti kako je napadač ušao u sistem. Treba teoretski analizirati napad, mapiranjem svih mogućih vektora napada - pristupnih putanja računaru žrtve, kontrola pristupa računaru i log fajlovima računara žrtve, korišćenjem istog tipa forenzičkog računara i OS.

Drugi korak u izradi hipoteze napada je testiranje hipotetičkih putanja i ACL (kontrolnih lista pristupa) svih korisnika i superkorisnika koji imaju pravo pristupa računaru žrtve, da bi se utvrdilo da li su potencijalni napadači. Određuje se vreme, datum i okolnosti napada itd. U ovoj fazi važno je ne uključivati računar, ako već nije uključen, ili ne isključivati ga ako je uključen, jer ne treba praviti nikakve promene na napadnutom računaru, posebno ako je u pitanju neki *Microsoft* OS. Možda još postoje vredni dokazi na čvrstom disku računara, koji bi se mogli oštetiti ili uništiti nepropisnim radom na napadnutom računaru. Obavezno je isključiti računar iz mreže, raspojiti modem sa linije, a ako je neophodno isključiti napajanje računara izvlačenjem kabla za napajanje sa zadnje strane računara.

Rekonstrukcija krivičnog dela: Kompjuterski kriminal se, za razliku od ubistva ili pljačke, može rekonstruisati testiranjem uspostavljene hipoteze napada, gde se može saznati kojim putem je napadač pristupio računaru. Zatim, počinje rad u cilju prikupljanja informacija nephodnih da se opravda eventualno postavljanje zamke za napadača, za ulaženje u trag telefonskoj liniji koju je napadač koristio i informacija koje mogu suziti listu osumnjičenih, ili potvrditi da napadač nije iz redova zaposlenih.

U ovom koraku, forenzički računar za simulaciju napadnutog računara treba konfigurisati što je moguće bliže stvarnoj konfiguraciji računara žrtve - interna konfiguracija, logovanje, mrežne veze, kontrola pristupa. Ako je napadnuti računar PC, treba ga butirati sa pokretnog DOS butabilnog medija bez *Windows* OS i uzeti fizičku sliku HD (bit-po-bit) korišćenjem forenzičkog alata (npr., *FTK, EnCase*, *SafeBack, Sydex*). Zatim se fizička slika restaurira na forenzičkom računaru i dobije se tačan *miror* ili *imidž* slika napadnutog računara. Ako se dobije isti rezulatat kakav je dobio napadač počinje proces shvatanja *kako* je računar napadnut, što još uvek ne mora voditi do napadača, ali sigurno smanjuje listu osumnjičenih.

Rekonstrukcija traga do osumnjičenog računara: Većina kompjuterskih kriminalaca su veoma vešti, retko zabrljaju i padaju u zamku, ali se ipak dešava, što daje prednost istražnom organu. Zato je traženje logičkih grešaka prvi korak za ulazak u trag napadaču. Sam kompjuter ostavlja tragove u brojnim pristupačnim i skrivenim zonama na čvrstom disku (HD), pa forenzičar mora znati gde sve računar ostavlja tragove. Velika prednost istraživača kompjuterskog kriminala je u razumevanju funkcionisanja OS, fajl sistema, hardvera, interfejsa, komunikacija u i izvan računara, koji skrivaju zamke, čak i za najveštije hakere. Čak i kôd (virusa, na primer) kojeg programer napiše, može sadržavati indiciju o njegovom identitetu, koju vešt forenzičar može otkriti.

Računari su ekstremno konzistentni i predvidljivi u načinu procesiranja podataka. Ako se računar ne ponaša očekivano za to postoje samo dva razloga: ili forenzičar ne razume kako računar treba da se ponaša, ili je došlo do izmene u programu. To je od velike pomoći u istražnom postupku. Ako, je na primer, potpuno poznato kako neka aplikacija na svakom nivou procesira podatke, a u nekoj tački ih procesira nešto drugačije, to znači da treba pronaći logičke greške u indikacijama koje su nastale u toku istrage.

Ako postoji anomalija zbog koje dolazi do pada aplikacije, što samo po sebi nije neobično i ne sumnjajući na kriminal, treba analizirati log podatke za taj period. Log fajl indicira prekonfigurisane podatke, ali programske izmene mogu ostati nezapažene. Na primer, u jednom slučaju forenzičar nije uočio izmenu malog bloka kôda koja ukazuje da se programer logovao u inkriminisano vreme i programski izmenio vreme logovanja. Tako je bilo gotovo nemoguće dokazati ovu izmenu na sudu i slučaj je odbačen, a programer nije optužen. Međutim, to je bio prvi skriveni tok i logično, ako je log usmeravao na programera morao je postojati i drugi dokaz koji to podržava, ali ih nije bilo. Istraga kompjuterskog kriminala nije isključivo tehničke prirode, ali tehnički aspekt mora imati smisla. Ignorisanje bilo koje anomalije može dovesti do pogrešnog zaključka. Ovo je najteži deo istrage. Ako trag vodi izvan IKT sistema kojem pripada napadnuti računar, onda se trag mora rekonstruisati na Internetu.

Iskusni napadač nikada ne napada direktno sa svog računara nego koristi više korumpiranih, posrednih računara. Napadač uspostavlja **Trojanca**, **zamku** (*trap door*), ili **zadnja vrata** (*backdoor*) rutkit tehnikama na posredni računar i koristi lanac naloga ovog računara da dospe do ciljnog računara žrtve ili slabo zaštićenog računara u slučaju *phishing* napada (pecanja žrtve). Najčešće nema geografske korelacije između posrednih računara i napadača, a napadač često menja log fajlove da zametne trag. Na sti način i napadač - zaposleni iz mreže može napastiti sa udaljene lokacije.

Rekonstrukcija traga napada podrazumeva da se „otkriju znakovi pored svakog puta" kojim je napadač prošao, tj. logovi svakog ulaza u servere, rutere i telefonske centrale, pri čemu mogu nastati sledeći problemi:

- *ne postoje, neadekvatni su ili izmenjeni logovi za vremenski period napada,*
- *isprekidana zaustavljanja između izvora napada i računara žrtve,*
- *uskraćena saradnja administratora posrednih računara,*
- *lažiranje IP adresa (*spoofing *adresa),*
- *direktni konzolni pristup napadnutom računaru prikriven izmenom log fajla,*
- *izmena logova napadnutog računara, ili drugi trikovi za maskiranje neovlašćnog pristupa,*
- *postoji samo jedan pokušaj pristupa, bez daljih šansi za traganjem itd.*

Rekonstrukcija traga u računaru u velikoj meri zavisi od log fajlova. Ako je u napad uključeno više računara treba uporediti vremensku liniju log fajlova svih računara. Osnovni problem je namerna izmena log podataka nekog posrednog računara, što dovodi do pogrešnih zaključaka forenzičara. Log podatke mogu izmeniti i forenzičari i drugi subjekti, što predstavlja problem za pravosuđe. Zato, ako se izvlače log i drugi podaci, forenzičar obavezno treba da kopira dve fizičke kopije, jednu referentnu za dokazni postupak, a drugu za radnu kopiju.

Predavanje nalaza i dokaznog materijala korporacijskim, ili zvaničnim organima istrage za dalji postupak, forenzičar vrši isključivo po odobrenju vlasnika napadnutog sistema, koji odlučuje o daljem toku istrage. U ovoj tački istrage ispoljavaju se i osnovni problemi korporacijske istrage. Prvi problem je što organizacije, tipično, ne pripremaju svoje organe za istragu, a drugi što ova lica, koliko god da su osposobljena, ne mogu istraživati izvan svoje organizacije. Sledeći problem je što moraju voditi računa o objavljivanju podataka o upadu u IKT sistem organizacije, zbog klijenata, kupaca, potrošača, ugleda organizacije i brojnih drugih faktora.

Za korporacijsku digitalnu forenzičku istragu organizacija mora uspostaviti forenzičke kapacitete u okviru interventnog tima za upravljanje kompjuterskim incidentom. Ključne preporuke za uspostavljanje i organizaciju forenzičkih kapaciteta u organizaciju su, [25], [40]:

- Uspostaviti kapacitete za kompjutersku i mrežnu forenziku. Ako organizacija istragu kompjuterskog incidenta vrši na forenzički ispravan način, menadžer može brže i lakše doneti ispravnu odluku o daljim akcijama;

- Jasno odrediti koji deo forenzičkih poslova izvršava interni, a koji deo eksterni forenzički tim na bazi procene individualnih veština i sposobnosti, troškova, vremena za odgovor i osetljivosti podataka;
- Obezbediti robusne forenzičke kapacitete za interventni tim za upravljanje kompjuterskim incidentom, uključujući praktičnu obuku članova tima na aktuelnim forenzičkim kursevima za primenu novih forenzičkih tehnika i alata;
- U forenzičkim aktivnostima obezbediti učešće više uloga iz organizacije, uključujući specijalsiste zaštite, forenzičare, IKT profesionalce-informatičare, menadžere, pravnike, savetnike, personal za upravljanje ljudskim resursima, kontrolore i fizičko obezbeđenje, koji treba da shvate svoje uloge i odgovornosti u forenzičkoj istrazi, da se adekvatno obuče i upoznaju sa odnosnim politikama, uputstvima i procedurama;
- Forenzičke aktivnosti precizno obuhvatiti u politikama IKT zaštite, a organizacija može definisati i posebnu politiku za digitalnu forenzičku istragu, uspostaviti tim za forenzičku istragu i osposobiti druge zapolsene sa ulogama i odgovornostima za izvršavanje forenzičkih zadataka. Ova politika treba da uključi najmanje sledeće:
  - Saopštenje koje jasno definiše uloge i odgovornosti svih zaposlenih i spolja angažovanih učesnika u izvršavanju forenzičkih zadataka, jasno navodeći koga i pod kojim okolnostima treba kontaktirati u organizaciji;
  - Uputstva i procedure za forenzičke akcije koje pod normalnim i posebnim okolnostima treba, a koje ne treba primenjivati i da obuhvate upotrebu anti-forenzičkih alata i tehnika i način upravljanja osetljivim nenamerno izloženim informacijama;
  - Forenzičke aktivnosti ugraditi u životni ciklus IKT sistema, što omogućava efikasnije i efektivnije upravljanje brojnim incidentima. Primer su kontrola host računara i uspostavljanje politike zadržavanja podataka za reviziju istorije aktivnosti sistema i mreže.
  - Izraditi i održavati uputstva i procedure za izvršavanje forenzičkih zadataka. Uputstvo treba da uključi generalnu metodologiju za istragu bezbednosnog kompjuterskog incidenta koristeći forenzičke tehnike, a procedure treba da objasne kako se izvršavaju rutinski *zadaci i primenjuju forenzičke tehnike i alati.*

2.4 ISTRAGA AKTIVNOG INCIDENTA – STUDIJA SLUČAJA

Sa legalnog, tehničkog i etičkog aspekta ovo pitanje je veoma kompleksno. Napadači ostavljaju razne zamke i *vremenske bombe* koje se aktiviraju u neodređeno vreme u korumpiranom računaru. Da bi se analizirale mogućnosti i odredile procedure istrage ativnog incidenta pretpostavlja se scenario u kome je napadač još na mreži i neka je u mreži aktiviran *ISS skener* i neka se koristi forenzički alat *SafeSuite* na web lokaciji ISP (Internet servis provajdera).

Napadači na IKT sistem, odnosno računarsku mrežu ili pojedinačan računar, nakon prvog upada, najčešće ostavljaju razne zamke (zadnja vrata, trojance), a njihovo prisustvo vešto prikrivaju rutkit tehnikama. Stvarnu štetu/zloupotrebu ovi programi u napadnutom računaru nanose kasnije bez vidljivih tragova za korisnika. U slučaju otkrivanja napada, primenjuju se različite aktivnosti i odgovarajuće mrežne tehnike za postavljanje zamki za presretanje, ulazak u trag, praćenje traga i hvatanje napadača. U slučaju *on-line* napada moguće su situacije da je, [20]:

- napadač još uvek na mreži,
- u toku direktan napad preko modema (ADSL, kablovskog,…) ili je
- u toku dial-up napad preko telefonske mreže.

2.4.1 Scenario u kojem je napadač na mreži

Za simulaciju reagovanja na slučaj napada na IKT sistem u kojem je napadač još uvek na mreži, aktivirani su *ISS* skener, programski alat *SafeSuite*, prema lokaciji web servis provajdera. Izvršeno je ispitivanje otpornosti sistema zaštite, simulacijom klasičnog hakerskog napada i napada struktuiranim simulatorom kombinovanih napada.

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

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

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

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

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

2.4.1.1 Slučaj direktnog napada

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

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

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

Ako je napadnuti računar imao aktiviran sistem logovanja, može se uz pomoć vlasnika računara odrediti kada se neovlašćeni napad dogodio i koristiti to kao polaznu tačku istrage akcija napadača. Iako ova potraga liči na traženje igle u plastu sena, forenzički alati nude moguća rešenja. To su alati za otkrivanje podataka u skrivenim zonama HD

(*slack* i nealocirani prostori klastera, *swap* fajlovi i dr.). Može se desiti da ime ili adresa napadača ostane zapisana u ovim zonama. Moguće je, takođe, da se cela *ekskurzija* napadača kroz mrežu pojavi na udaljenom računaru kroz kojeg je napadač pristupio u mrežu (prvo birao telefonom). Ako se napravi miror slika tog računara i analizira, tu je sve što je potrebno za otkrivanje traga napadača u mreži. Čak i kada napadač više nije na mreži, moguće mu je postaviti zamku za sledeći napad. Kada se otkrije napadač na linji postoji mogućnost da se zadrži dovoljno dugo dok se ne postavi zamka za praćenje traga, prekine veza u kom slučaju treba očekivati da se napadač vrati, ili učini nešto da se napadač uplaši i više nikada ne vrati natrag.

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

2.4.1.2 Slučaj napada preko telefonske centrale

U slučaju napada na telefonsku centralu potreban je sudski nalog za postavljanje zamke za napadača (prisluškivanje linije) i praćenje traga napadača. Upoređivanjem vremena pristupa u log fajlu napadnutog računara sa vremenom pristupa u *pen* registru svih dolaznih poziva u telefonskoj centrali, može se otkriti trag napadača. Potpuni sistem zamke i praćenja traga prikuplja informacije koje prolaze telefonskom linijom, kao i izvore poziva.

Postavljanje zamke i praćenje traga u slučaju mrežnog pristupa znatno je teže. U većini slučajeva samo se može nagađati odakle napadač sa Interneta dolazi, pošto 'skače' iz sistema u sistem da bi izbegao detekciju (IDS/IPS). Važno je krenuti u akciju vrlo brzo i uz pomoć neposrednog sistem administratora može se otkriti trag napadača.

Pažljivi napadač uvek proverava da li je administrator mreže na liniji. Jedan od načina da se skrene pažnja sa administratora je uklanjanje svih referenci koje upućuju na administratora, a drugi davanje benignog naloga i maskiranje naloga administratora, kako rade i hakeri. Na primer, vešt napadač obično ulazi u sistem pomoću ukradenog naloga. Kada administrator listira korisnike na lniji (*on line*), napadač vidi samo poznate login podatke. Administrator uvek treba da izbegava logovanje sa konzole u rutu. Ako administrator trenutno izvrši zadatak može se dobro sakriti i posmatrati napadača bez podizanja alarma.

2.4.1.3 Mrežne tehnike za postavljanja zamke i praćenje traga napadača

U traganju za lokacijom napadača na liniji, treba početi sa otkrivanjem IP adrese, ili punog imena domena lokacije napadača. Ovim podacima ne treba previše verovati.

Ime napadača uglavnom nije stvarno, nego je to samo lokacija na kojoj je ukrao nalog. Podatak treba zapisati kao i sistemsko vreme na napadnutom računaru.

Dalje je potrebno videti šta napadač radi u sistemu, posmatranjem tekućih procesa (u *Task manageru* kod Windows OS). Treba uočiti sve procese koje nije moguće objasniti, a registrovati proces u kojem se sumnja da je napadač u toku.

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

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

Ako je moguće treba izvršiti svaki *online* zadatak sa drugog računara, da se izbegne skretanje pažnje na forenzičarske aktivnosti. Ceo ovaj postupak ne sme da traje više od par minuta. Sve akcije treba zabeležiti, vremena, adrese, korisnička imena i drugo. Međutim postoji čitav skup okolnosti vezanih za napad sa telefonske linije umesto preko Interneta. Za ove aktivnosti potrebno je saradnja i odobrenje nadležnih zvaničnih organa. Generalno svako postavljanje zamke napadaču podleže zakonu o prisluškivanju linija. Kako se e-*mail* smatra "tranzitom" podataka po žici, to i snifovanje e-pošte pripada tom zakonu. Ako napadnuti IKT sistem ima sistem zaštite koji neprekidno skenira mrežni saobraćaj i skuplja informacije o normalnim aktivnostima, a posebno o neregluarnostima, šanse za ulazak u trag napadaču su znatno veće. Ako se ignoriše otkriveni napadač na liniji, posledice mogu biti oštećenja sistema. Drugo, napadač može iskoristiti neki sistem za novi napad u ili izvan tog sistema, što može naneti i druge vrste štete. Uplašiti se i pobeći potpuno je amaterski. Iskusan napadač može otići, ako mu se administrator suprotstavi, ali se sigurno vraća. Ne preporučuje se ulazak u dijalog sa napadačem. To je gubljenje vremena i ništa se ne postiže.

Zamke (zadnja vrata, Trojanci) su mehanizmi koje hakeri ostavljaju na napadnutom računaru, a koji im omogućavaju kasniji povratak, bez nove kompromitacije računara. Ideja je da se zamka postavi na nekoj ulaznoj tački u kompromitovani računar, tako da je administrator ne otkrije i ukloni. Ako administrator otkrije metod originalnog upada, može zatvoriti *rupu* i sprečiti upad napadača. Međutim, dobro skrivanje zamke je izbor napadača. Ovaj mehanizam omogućava napadaču da se bezbrižno vrati kasnije i završi napad, posebno kada je otkriven na liniji, [18].

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

obezbeđuju nevidljiv povratak u mašinu u najkraćem vremenu, čak i kada administrator pokuša da je obezbedi, na primer promenom svih lozinki i u većini slučajeva izbegavanje logovanja.

U nekim slučajevima hakeri koriste ranjivosti (bagove) sistema kao jedine zamke. Tako ranjivost sistema ostaje jedina nedetektovana zamka u sistemu. Zavisno od tipa platforme napadnutog računara razvijen je veliki broj zamki koje se mogu svrstati u brojne, često promenljive kategirije: *za krekovanje lozinke, „Rhosts++", za čeksumu i timestamp, za login fajlovu, postavljene daljinski (telnet), za servise, Cronjob, za biblioteke, u kernelu, u fajl sistemu, na butabilnom bloku itd.*

Hakeri najčešće žele sakriti programe koje kasnije aktiviraju. To su najčešće krekeri lozinki ili sniferi. Postoji nekoliko metoda skrivanja zamki od kojih su najčešće:

- promena imena u ime drugog procesa,
- preimenovanje sniferskog programa u legitiman servis kao u syslog, koji se aktivira kad administrator kuca neku komandu, ili gleda koji procesi su aktivni, a pojavi se ime standardnog servisa,
- modifikovana biblioteka rutina tako da se na komandu ne pokazuju svi procesi,
- pečovana (zakrpljena) zamka u rutinu koju aktivira prekid rada, tako da se ona ne pojavljuju u tabeli aktivnih procesa i
- modifikovani kernel tako da se neki procesi ne vide.

Hakeri ne samo da žele sakriti svoj trag u mašini, nego ga žele što je moguće više sakriti i u mrežnom saobraćaju. Ove zamke za mrežni saobraćaj ponekad dopuštaju hakeru da dobije pristup kroz *firewall*. Postoj brojni programi zamki za mrežni saobraćaj koji omogućavaju hakeru da se postavi na određeni broj porta mašine i dobije pristup bez korišćenja normalnih servisa. Pošto mrežni saobraćaj ide preko nestandardnog mrežnog porta, administrator može prevideti hakera u saobraćaju. Ove zamke za mrežni saobraćaj tipično koriste TCP, UDP i ICMP, ali mogu koristiti razne vrste paketa, uključujući i šifrovanu zamku.

Haker može postaviti zamku za TCP *šel* na neki visok broj porta, po mogućnosti gde *firewall* ne blokira taj TCP port. Često su zadnja vrata zaštićena lozinkom, tako da kada se administrator konektuje na njega, pristup *šelu* se trenutno neće videti. Administrator može tražiti ove veze sa *Netstat* alatom da otkrije koji se portovi slušaju i gde i odakle idu tekuće veze. Ovaj tip zadnjih vrata često omogućava hakeru da probije TCP *Wrapper* tehnologiju. Ova zadnja vrata mogu biti aktivirana na SMTP portu, kroz koji mnogi *firewalls* dopuštaju saobraćaj za e-poštu.

Savremeni proaktivni sistemi za detekciju i sprečavanje upada u sistem (IPS-*Intrusion Protection Systems*) obezbeđuju inteligentnu tehniku za hvatanje napadača poznatu kao **ćup meda** (*honypot*). Ove tehnike omogućavaju 'zarobljavanje' hakera u napadnutom sistemu, kada se jednom otkrije. Generalna tehnika *honypot* obuhvata sledeće aktivnosti, [9]:

- Saznati koji nalog haker koristi za pristup sistemu. Ako je nalog ukraden, stvarnom vlasniku dati novi nalog, a ukradeni držati aktivnim. Promeniti prava ukradenog naloga da se ograniče njegove mogućnosti da kreira direktorijume koji sadrže vrlo velike i sumnjive fajlove;
- Ako haker dugo luta sistemom primetiće rekonfiguraciju i postati sumnjičav. Takođe verovatno nije sasvim poznato koja će informacija dovesti u iskušenje hakera da je preuzme (daunloduje);
- Cilj je smestiti hakera u bezopasnu zonu sistema (što je teško učiniti ako haker uđe u rut), dovesti ga u zabludu i navesti na vrlo obimno daunlodovanje. U toku dugog procesa daunlodovanja, izučavati napadača i pokušavati ući u trag izvora napada;
- Iako je vreme dugo, nema garancije da će haker ostati svo vreme u sistemu, može jednostavno preći na drugi kompromitovani računar i tražiti to tamo. Kada haker pronađe da je fajl lažan, učiniće virtuelni prekid gubi mu se svaki trag;
- Drugi problem je što haker može pobeći, alarmiran rekonfiguracijom sistema. Zato je honypot poslednje rešenje;
- Ako se želi sudsko gonjenje napadača u primenu ove tehnike treba uključiti zvanične organe istrage.

2.5 TIM ZA ISTRAGU KOMPJUTERSKOG KRIMINALA

Istragu kompjuterskog kriminala mogu efikasno vršiti samo visoko-specijalizovani stručni kadrovi u interventnim timovima nadležnih državnih organa sa odgovarajućim kapacitetima. Takav pristup jedino omogućava valjanu istragu i način da se sakupe, sačuvaju i na sudu veštače digitalni dokazi o izvršenom kompjuterskom kriminalu. Uspešan i efikasan rad interventnih timova može se obezbediti samo odgovarajućom specijalističkom obukom članova tima, [25].

2.5.1 Interventni tim za korporacijsku istragu kompjuterskog incidenta

Najčešća praksa je da organizacije izvrše vlastitu inicijalnu istragu kompjuterskog incidenta na nivou organizacije, utvrde karakter incidenta i tek onda, donesu odluku o pozivanju zvaničnih organa istrage kompjuterskog kriminala. Uloga korporacijskih organa za istragu zloupotreba u IKT sistemu ograničena je zato što većina organizacija nije opremljena odgovarajućim kapacitetima za forenzičku istragu i analizu i što ovi organi istrage nemaju sva zakonska ovlašćenja za otkrivanje traga do napadača i zaplenu računarskih sistema napadača kao dokaznog materijala.

Dobro rešenje je angažovanje stručnog konsultanta za inicijalnu istragu, akviziciju i forenzičku analizu digitalnih dokaza i voditi istragu vlastitim snagama, najmanje do

trenutka utvrđivanja prirode incidenta i donošenja odluke o (ne)uključivanju zvaničnih istražnih organa, što se na kraju najčešće učini. Organizacija, može formirati svoj interventni tim (*CIRT*) za brzo reagovanje i istragu kompjuterskog incidenta, a prazninu u stalnom timu popuniti pridruženim (pomoćnim) članovima - stručnim konsultantom, najčešće tehničkim ekspertom u oblasti zaštite IKT sistema, kontrole (*auditing*) sistema zaštite i digitalnim forenzičarom. Naravno, konsultant može biti i privatna informatička firma sa znanjem i iskustvom u ovoj oblasti, kadrovski i materijalno opremljena i osposobljena za istragu i forenzičku analizu digitalnih dokaza, [10].

2.6 REZULTATI KORPORACIJSKE ISTRAGE KOMPJUTERSKOG INCIDENTNA

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

- Gubljenja traga, kada prođe suviše vremena od incidenta i nema dokaza;
- Nekompletnog logovanja, ili uopšte nema logovanja;
- Cena istrage je veća nego gubici nastali usled incidenta i nije rentabilno nastaviti istragu;
- Velik prostor skrivanja počinioca (Internet), a incident se dogodio samo jedanput, sa malo ili bez imalo dokaza;
- Incident nije sasvim određen, nije jasno da li je, ili nije bezbednosni incident;
- Ne može se nepobitno ukazati na počinioca i nema dovoljno dokaza;
- Postoji politički, ili drugi pritisak da se istraga zaustavi;
- Zataškavanje istrage itd.

Ako se izvrši i kompletira istraga kompjuterskog incidenta obavezno je dostaviti *Izveštaj o istrazi.* U slučaju korporacijske istrage Izveštaj se dostavlja vlasniku sistema za dalje odlučivanje o sudbini istrage, ili nadležnim zvaničnim organima za dalji pravosudni postupak. Dokument *Izveštaj o istrazi* treba da sadrži najmanje sledeće celine [34]:

Apstrakt istrage
Opis događaja
Kratka metodologija istrage
    Kratak opis skupljanja dokaza i metoda čuvanja istih
    Zaključak sa kratkim uopštenim rezonima
Metodološki detalji
    Istraga
    Skupljanje i čuvanje dokaza
Nalaz 1 – Opis
    Diskusija
    Dokazi koji potvrđuju
.....
Nalaz N – Opis
Diskusija
    Dokazi koji potvrđuju
Kratak sadržaj i zaključci
Dodatak
Lista ispitanih (intervijuisanih)
Lista dokaza
Sw i alati korišćeni u istrazi
IT eksperti i konsultanti
Kontakti na mestima koja su sarađivala (posrednici)
Drugi važni listinzi i informacije

Važno je naglasiti da li je prikupljanje i čuvanje dokaza bilo/nije u skladu sa zakonom o istražnom postupku i da li su informativni razgovori i saslušanja u toku istrage propisno vršeni primenom 7-stepenog metoda:

1. pripreme strategije saslušanja,
2. vođenja razgovora,
3. uspostavljanja kredibiliteta kod osumnjičenog,
4. smanjenje otpora osumnjičenog,
5. dobijanje (izvlačenje) priznanja,
6. razvoj i eksploatacija priznanja i
7. profesionalno zatvaranje saslušanja.

REZIME

Proces digitalne forenzičke istrage nije jednostavan niti isti za sve tipove kriminala, ali postoje neke sličnosti - svi tipovi zahtevaju strukturu istražnog procesa, profesionalce koji razumeju predmetnu metodologiju i tehnologiju i profesionalce koji vode istražni postupak. Obe ove sposobnosti se retko mogu naći u jednoj osobi. Zatim, svi tipovi kompjuterskog kriminala zahtevaju odgovore na pitanja: ko, šta, gde, kada i zašto?

Najveći deo digitalne forenzike odnosi se na forenziku računarskih sistema, ili *kompjuersku forenzik*u. Digitalna forenzika računarske mreže, uključujući i Internet ili *kibernetička forenzik*a, otkriva i sakuplja informacije o tome kako je napadač dobio pristup računarskoj mreži. Generalno, digitalna forenzička istraga može se podeliti u dve osnovne kategorije: *zvanična (javna)* i *korporacijska (privatna)* digitalna forenzička istraga.

Opšti proces zvanične istrage bezbednosnog kompjuterskog incidenta, sa pristupom istrazi po modelu »korak po korak", obuhvata: inicijalnu istragu (pretragu), ulazak u trag napadaču, otkrivanje identiteta napadača i hapšenje.

Korporacijsku digitalnu forenzičku istragu, organizacija može izvršiti sopstvenim timom, iznajmljenim timom ili kombinovanim timom. Kada rezultati istrage ukažu na trag napadača izvan organizacije ili se zahteva hapšenje napadača, mora se angažovati zvanični organ istrage. Proces korporacijske istrage u većini slučajeva obuhvata tri ključne faze: pokretanje istrage, određivanje karaktera kompjuterskog incidenta i analizu prikupljenih digitalnih podataka.

Da bi uspeh korporacijske istrage kompjuterskog incidenta bio potpun, ove tri faze istrage treba izvršavati kroz sukcesivno izvršavanje 7 sledećih koraka: eliminisati očiglednosti, postaviti hipotezu o napadu, rekonstruisati krivično delo, otkriti trag do osumnjičenog računara sa koga je napad izvršen, analizirati izvorni, ciljni i posredne računare, skupiti dokaze, uključujući, ako je moguće i sam računarski sistem i predati nalaze i dokazni materijal korporacijskim, ili zvaničnim organima istrage za dalji postupak.

Istraga aktivnog kompjuterskog incidenta veoma je kompleksna sa legalnog, tehničkog i etičkog aspekta i najčešće zahteva angažovanje ISP i telefonskih provajdera izvan granica države napadnutog računara. Istraga aktivnog *on-line* napada može obuhvatiti slučaj: napadača na mreži, direktan napad preko modema i dial-up napad preko telefonkse mreže.

Brojni bezbednosni kompjuterski incidenti uključujući i kompjuterski kriminal mogli bi se upravljati efikasnije i efektivnije, ako se forenzičke procedure ugrade u životni ciklus sistema IKT zaštite. Veće organizacije tipično izgrađuju sopstvene kapacitete za upravljanje kompjuterskim incidentom, uključujući uspostavljanje interventnog tima. Ovaj tim pored tehnički kompetentnih lica treba da uključi i predstavnika izvršnih mendžera, pravnika i menadžera za upravljanje ljudskim resursima i korporacijskog digitalnog forenzičara. Korporacijski tim dostavlja izveštaj o rezultatima istrage vlasniku/menadžeru organizacije, koji donose odluku o daljem toku istrage.

PITANJA ZA PONAVLJANJE

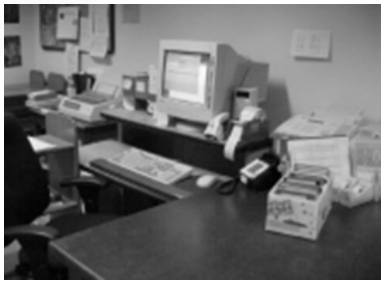
1. Navedite neka pitanja na koja zvanični organ istrage mora naći odgovore u utvrđivanju karaktera krivičnog dela kompjuterskog kriminala.
2. Nabrojte četiri osnovne faze procesa zvanične istrage kompjuterskog incidenta.
3. Nabrojte i obrazložite tri ključna faktora koji utiču na odluku organizacije o uključivanju internog, ili eksternog tima u digitalnu forenzičku istragu.
4. Nabrojte nekoliko tipova zadataka u kojima se mogu koristiti forenzičke tehnike i alati.
5. Navedite tri glavne grupe primarnih korisnika forenzičkih alata i tehnika unutar neke organizacije.
6. Koje su tri glavne faze procesa korporacijske istrage?
7. Navedite šest ključnih koraka istrage kompjuterskog incidenta u svakoj fazi istrage.
8. Opišite glavne probleme koji mogu nastati kod predavanja nalaza i dokaznog materijala korporacijskim, ili zvaničnim organima istrage.
9. Nabrojte pet osnovnih preporuka za uspostavljanje forenzičkih kapaciteta organizacije.
10. Koje su moguće situacije u slučaju aktivnog *online* napada u toku?
11. Navedite optimalni sastav interventnog tima za korporacijsku istragu kompjuterskog incidenta.

3. FUNKCIONALNI MODELI DIGITALNE FORENZIČKE ISTRAGE

3.1 MODEL ISTRAGE FIZIČKOG MESTA KRIVIČNOG DELA

Sa aspekta teorije istrage, konsultovana je brojna literatura za istragu fizičkog mesta krivičnog dela, [4], [8], [12]. Glavne faze istrage fizičkog mesta krivičnog dela su:

- ***Obezbeđivanje, fiksiranje mesta krivičnog dela*:** prvi korak je da se pomogne povređenima, zatim sledi potraga za osumnjičenima i hapšenje osumnjičenih i zadržavanje svih svedoka. Fizičko mesto krivičnog dela mora biti osigurano, a pristup omogućen samo ovlašćenim licima, istražnim organima, (kriminalistički inspektor, sudski istražitelj, forenzičar sudske medicine itd.).
- ***Pretraga mesta krivičnog dela:*** organ istrage pažljivo pretražuje mesto krivičnog dela, identifikuje očigledne delove dokaza i kratkotrajne dokaze (krv, sluz, sperma, pljuvačka itd.). Dokumentuju se početna opažanja tipa *ko, šta, gde, kada, kako* i kreira početna teorija - *hipoteza slučaja*.
- ***Dokumentovanje mesta krivičnog dela*:** mesto krivičnog dela dokumentuje se fotografisanjem, skiciranjem i snimanjem digitalnog video snimka. Dokaze treba jednoznačno označiti, potpuno dokumentovati i sakupiti za analizu.
- ***Istraga mesta krivičnog dela:*** brojni obrasci istrage koriste se da bi se identifikovali dodatni dokazi koji nisu otkriveni u predistražnom postupku (pretrazi). Teorija razvijena u pretrazi koristi se za istragu specifičnih dokaza koji nedostaju (npr., oružje kojim je počinjeno ubistvo).
- ***Rekonstrukcija krivičnog dela:*** događaji koji su se dogodili na mestu krivičnog dela određuju se na osnovu izgleda mesta krivičnog dela, mesta i pozicije fizičkih dokaza, analiziranih rezultata iz forenzičke laboratorije i naučnih metoda primenjenih u istrazi i analizi dokaza. Ovaj opšti model omogućava kompletnu dokumentaciju mesta zločina i koristi iskustvo istražnog organa da bi se došlo do korisnih dokaza. Svi fizički predmeti ne mogu da se uzmu sa mesta krivičnog dela, tako da *Faza Istrage mesta krivičnog dela* mora biti potpuna da bi se sakupili potrebni dokazi, ali ne sme se preoptereti laboratorija sa predmetima koji nemaju veze sa slučajem, (slika 3.1).



Slika 3.1 Fizičko mesto krivičnog dela kompjuterskog kriminala

3.2 MODEL ZVANIČNE ISTRAGE DIGITALNOG MESTA KRIVIČNOG DELA

U SAD "*Department of Justice*" objavio je model procesa istrage u "*Vodiču za istragu elektronske scene zločina*",[9]. Vodič potpuno odgovara istrazi fizičkog mesta krivičnog dela, tako da je akcenat stavljen na zahteve istrage klasičnog kriminala, a malo pažnje se obraća na forenzičku analizu izvora digitalnih podataka. Faze modela su sledeće:

- *Priprema*: pripremiti opremu i alat potreban za istragu**;**
- *Sakupljanje*: naći i sakupiti elektronske (digitalne) dokaze;
- *Osiguranje i procena mesta krivičnog dela*: obezbediti mesto krivičnog dela radi bezbednosti lica i integriteta podatka i identifikovati potencijalne dokaze;
- *Dokumentovanje mesta krivičnog dela:* dokumentovati fizički opis mesta krivičnog dela uključujući fotografije računarskog sistema;
- *Sakupljanje dokaza*: alatima za forenzičku akviziciju izvući podatke iz računara, privremeno oduzeti fizički računarski sistem, ili napraviti fizičku (*miror*) kopiju podataka na forenzičkom računarskom sistemu;
- *Pregled/pretraga:* tehnički pregled i ispitivanje sistema radi nalaženja potencijalnih dokaza;
- *Analiza*: digitalna forenzička analiza hardverskim i/ili softverskim alatima digitalnih podataka računarskog sistema i memorijskih medijuma; analiza rezultata tehničkog pregleda i drugog dokaznog materijala radi procene njihovog značaja za slučaj;
- *Izveštavanje:* izveštaj se pravi posle svakog slučaja kompjuterskog (incidenta) kriminala.

3.3 KORPORACIJSKI MODEL ISTRAGE KOMPJUTERSKOG INCIDENTA

Funkcionalni korporacijski model istrage bezbednosnog kompjuterskog incidenta obuhvata sledeće faze, [17], [25]:

- *Priprema za saniranje incidenta*: sa odgovarajućom obukom i infrastrukturom;
- *Detekcija incidenta*: identifikovati sumnjivi incident na bazi praćenja nagoveštaja i idnikatora;
- *Prva reakcija*: prepoznati i potvrditi da se incident dogodio, sakupiti preliminarne, nestabilne i posredne dokaze (koji se vremenom degradiraju i lako namerno menjaju);
- *Formulisanje strategije reakcije*: na bazi poznatih indikatora incidenta;
- *Dupliranje dokaza incidenta*: napraviti fizičku (*miror, imidž)* sliku kompromitovanog/ ispitivanog sistema;

- *Digitalna forenzička istraga:* akvizicija i analiza digitalnih podataka, ispitativanje sistema radi identifikacije *ko*, *šta* i *kako* je izvršio napad;
- *Implementacija mera zaštite*: izolovati kompromitovan sistem pre nego što se oporave podaci i sistem vrati u normalni režim rada;
- *Nadzor mreže:* posmatrati mrežu radi praćenja i identifikacije ponovljenih napada;
- *Oporavak sistema:* vratiti sistem u originalno stanje sa dodatnim, većim merama zaštite;
- *Izveštavanje:* dokumentovati sve aktivnosti reakcije na incident i dostaviti izveštaj;
- *Završna faza:* revidirati proces saniranja incidenta, izvući potrebna iskustva i eventualno poboljšati procese upravljanja bezbednosnim incidentom.

3.4 MODEL INTEGRISANIH PROCESA DIGITALNE FORENZIČKE ISTRAGE

Ovaj model istrage koristi većinu faza prethodnih modela istrage, ali problemu prilazi sa druge tačke gledišta. Model koristi pretpostavku da je računar sam po sebi mesto krivičnog dela, odnosno, *digitalno mesto krivičnog dela.* Za otkrivanje fizičkih dokaza kompjuterskog kriminala, model primenjuje metod i tehnike istrage fizičkog mesta krivičnog dela, koristi prirodne zakone o razmeni materije dva objekta u kontaktu[11] i bogata iskustva iz istrage klasičnog kriminala. U istrazi digitalnog mesta krivičnog dela model koristi programski kôd – binarne zapise za otkrivanje digitalnih dokaza, [6].

U istrazi fizičkog mesta krivičnog dela, najpoznatija primenjena teorija je *Lokardov zakon razmene materije,* [38]*:* "*Kada dva objekta dođu u kontakt, doći će do razmene materije između njih*". Na primer, dlake i vlakna sa tela zločinca često se zadržavaju na fizičkom mestu krivičnog dela. Sličan efekat se dešava u digitalnom mestu krivičnog dela. Privremeni fajlovi, sadržaj primarne (RAM) memorije koji je snimljen na čvrstom disku (tzv. *Swap* fajl), izbrisani delovi fajlova, mogu ostati u računarskom sistemu u tzv. *fajl slack* prostoru i *nealociranom* prostoru klastera na čvrstom disku, zbog delovanja softvera – aplikacija, pomoćnih alata, OS itd., koje je osumnjičeni koristio i izvršavao u toku napada. Podaci ulaze i ostaju u digitalnom mestu krivičnog dela, ostavljajući tragove digitalnog dokaza iza sebe na raznim mestima u memorijskim elementima računarskog sistema - hard disku, RAM memoriji, registrima, pokretnim memorijskim elementima (USB, CD-ROM, DVD) itd. Rad *digitalnog forenzičara* u potpunosti zavisi od rada operativnog sistema i aplikativnih programa, zato što oni nezavisno od korisnika kontrolišu koji dokaz je napisan i u kojem delu memorijskih lokacija.

11 *Lokardov* princip razmene materije.

Koristeći koncept da je kompjuter sam za sebe digitalno mesto krivičnog dela, može se *zrela* teorija istrage fizičkog mesta krivičnog dela u potpunosti primeniti na digitalnu forenzičku istragu. Pri tome se forenzička istraga digitalnog mesta krivičnog dela integriše sa istragom fizičkog mesta krivičnog dela, tako da se mogu sakupiti svi relevantni fizički i digitalni dokazi o aktivnostima napadača. U ovom modelu istrage kompjuterskog kriminala, digitalno mesto krivičnog dela može se smatrati *sekundarnim mestom krivičnog dela*, u odnosu na *primarno* fizičko mesto krivičnog dela – sto i prostorija u kojoj se nalazi ispitivani računar.

U ovoj oblasti, postoje brojne interpretacije i mišljenja oko terminologije i ključnih reči. Da bi se sprečila konfuzija, potreba je definisati osnovne termine procesa digitalne forenzičke istrage, tako da najtačnije odražavaju izabrani pristup problemu, [6], [8]:

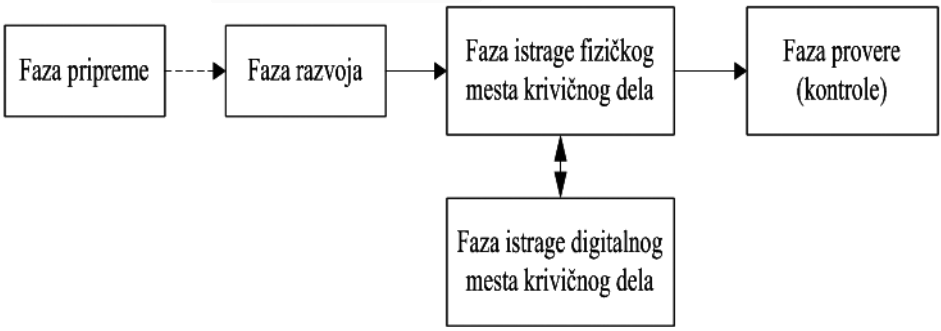
- *Fizički dokaz***:** fizički objekti koji mogu potvrditi da je krivično delo počinjeno i/ili koji povezuju zločinca i žrtvu, i/ili zločin i zločinca. Primeri fizičkog dokaza u kompjuterskom kriminalu su računar, čvrsti disk, PDA, CD-ROM itd. koji sadrže digitalne dokaze o izvršenom krivičnom delu kompjuterskog kriminala
- *Digitalni dokaz:* digitalni podatak koji može potvrditi da je kompjuterski kriminal počinjen i koji može da dovede u vezu krivično delo kompjuterskog kriminala i njegovog izvršioca. Primeri digitalnog dokaza su digitalni podatak u memoriji, na čvrstom disku, ili u mobilnom telefonu koji ukazuje na pristup i izvršenu akciju napadača u ispitivanom računaru.
- *Fizičko mesto krivičnog dela***:** fizičko okruženje gde postoje fizički dokazi krivičnog dela ili incidenta. Okruženje gde se prvo krivično delo dogodilo naziva se *primarno fizičko mesto krivičnog dela* (npr. prostorija sa računarom iz koje je osumnjičeni napadač izvršio napad)**,** a sledeće fizičko mesto je *sekundarno fizičko mesto krivičnog dela* (npr., prostorija sa posrednim računarom preko kojeg je napadač izvršio napad na računar – žrtvu).
- *Digitalno mesto krivičnog dela***:** virtuelno okruženje koje se sastoji od hardvera i softvera gde postoje potencijalni digitalni dokazi krivičnog dela kompjuterskog kriminala, ili kompjuterskog incidenta. Okruženje gde se prvi kriminalni akt dogodio je *primarno digitalno mesto krivičnog dela* (npr., računar osumnjičenog napadača)**,** a sledeća mesta nazivaju se *sekundarnim digitalnim mestima krivičnog dela* (npr., posredni, kompromitovani računar sa kojeg je napadač izvršio napad na računar – žrtvu). Često se praćenje traga napadača kreće od napadnutog računara, preko posrednih računara, pa do računara napadača, u kom slučaju je računar žrtva *primarno digitalno mesto krivičnog dela* kompjuterskog kriminala.
- *Revizija i analiza:* označava da se neki objekat računarskog sistema, ili računarske mreže, može procesirati na različite forenzički ispravne načine, da se iz njega mogu prikupiti, analizirati i kontrolisati podaci, relevantni za izgrdanju čvrstih, neoborivih digitalnih dokaza.

Model integrisanih procesa digitalne forenzičke istrage primenljiv je na korporacijsku i zvaničnu istragu. Zbog toga se izrazi "*mesto krivičnog dela*" i "*incident*" koriste u opštem smislu. Primeri fizičkog *mesta krivičnog dela* kompjuterskog kriminala su prostorija i sto na kome se nalazi računar osumnjičenog napadača, centar za obradu podataka u kojem je napadnuti server, soba za istragu dečije pornografije, ili kola u kojim je ubijen čovek, a na suvozačevom sedištu stoji otvoren laptop. *Bezbednosni incident* je bilo koja serija događaja koji se razlikuju od logovanih standardnih događaja u računarskom sistemu (*events*) i zahtevaju reagovanje interventnog tima za upravljanje kompjuterskim incidentom, ili forenzičkog tima za prikupljanje digitalnih dokaza. Ovo uključuje upad u server, izdavanje naloga za pretres kuće osumnjičenog i reagovanje specijalne jedinice MUP-a za borbu protiv visokotehnološkog (kompjuterskog) kriminala, na primer na hitni poziv 92 ili 911.

Pretpostavlja se da je veličina fizičkog mesta krivičnog dela inicijalno definisana prirodnim granicama neposrednog okruženja potencijalnih/poznatih digitalnih dokaza. Na primer, ukoliko je klasičan zločin ubistva počinjen u kući, onda kuća i imanje oko nje mogu biti inicijalno fizičko mesto krivičnog dela, a ova veličina se kasnije može povećavati ili smanjivati, zavisno od novih dokaza koji se otkriju u toku istrage. Za računarski sistem, inicijalno digitalno mesto krivičnog dela je tipično virtuelno okruženje kreirano lokalnim hardverom, periferijamai sistemskim i aplikativnim programima. Svaki pojedinačni računar, uključen u incident, najbolje je tretirati kao zasebno digitalno mesto krivičnog dela kompjuterskog kriminala.

Model integrisanih procesa istrage kompjuterskog kriminala ima 17 faza organizovanih u pet grupa (slika 3.2), [6]:

- Faza pripreme;
- Faza razvoja;
- Faza istrage fizičkog mesta krivičnog dela;
- Faza istrage digitalnog mesta krivičnog dela;
- Faza provere (kontrole).



Slika 3.2 Faze modela integrisanih procesa digitalne forenzičke istrage

Na slici 3.2. vidi se da se istrage fizičkog mesta izvodi uporedo sa istragom digitalnog mesta krivičnog dela kompjuterskog kriminala. U izgradnji čvrstih, neoborivih dokaza, rezultati istrage digitalnog mesta krivičnog dela integrišu se sa rezultatima istrage fizičkog mesta krivičnog dela kompjuterskg kriminala.

3.4.1 Faza pripreme

Cilj ove faze je da osigura potpunu *operativnu* i i*nfrastrukturnu* pripremu i podršku procesa digitalne forenzičke istrage. Digitalni i fizički dokazi mogu biti izgubljeni ukoliko nisu sakupljeni, skladišteni i zaštićeni (čuvani) na forenzički ispravan način. Ova faza traje u kontinuitetu i nije vezana za konkretno krivično delo kompjuterskog kriminala ili bezbednosnog incidenta, [6].

Operativna priprema obezbeđuje obuku i opremu za lica koja će biti uključena u istragu incidenta. Ovo uključuje obuku interventnog tima za kompjuterski incident, obuku laboratorijskih forenzičara i lica koja će primati inicijalne izveštaje o incidentu. Forenzička oprema sa kojom interventni tim pretražuje mesto krivičnog dela mora biti ispravna, potpuno sterilna i da predstavlja poslednja tehnološka rešenja. Oprema u laboratoriji za digitalnu forenzičku analizu i za terensku akviziciju digitalnih podataka/dokaza mora, takođe, da bude održavana na visokom nivou funkcionalnosti, pouzdanosti i spremna za analizu svih dospelih podataka o incidentu.

Infrastrukturna priprema obezbeđuje izvore iz kojih se generišu potrebni digitalni i drugi podaci da bi se izvršila potpuna i detaljna istraga, jer ukoliko ti podaci ne postoje nemoguće je izvršiti istragu. Ova faza odnosi se samo na lica koja održavaju infrastrukturu u fizičkom okruženju koje bi potencijalno moglo biti mesto kompjuterskog kriminala. Fizički primeri za ovu fazu su instalacije i raspoređivanje video nadzora i čitača kartica da bi se snimila vremena i datumi pristupa fizičkom prostoru za vreme krivičnog dela kompjuterskog kriminala. Digitalni primeri infrastrukturne pripreme su konfigurisanje log fajlova za skladištenje bezbednosno relevantnih događaja na serverima i drugim mrežnim uređajima i skupljanje log podataka na zaštićenom "log serveru", sinhronizacija internih satova na serverima i računarima sa protokolom za vremensku sinhronizaciju mrežnih uređaja - NTP (*Network Time Protocol*), projektovanje i implementacija sistema osnovne zaštite integriteta podataka sa heš algoritmom (MD5, SHA1, SHA256, SHA512 i dr.) i upravljanje zaštitom i promenama baze log podataka, [6].

3.4.2 Faza razvoja

Cilj ove faze je da obezbedi mehanizam za detekciju i potvrdu incidenta. Zadaci modela koji se izvode u ovoj fazi dosta se razlikuju za zvaničnu i korporacijsku istragu.

3.4.2.1 Faza detekcije i izveštavanja

Detektuje incident i izveštava odgovorna lica o incidentu. Ovo se može obaviti pozivom 92, preko alarma mrežnog detektora upada - IDS (*Intrussion Detection System*), ili *online* od agenta policije, koji istražuje ilegalne aktivnosti. Ova faza definiše početak procesa istrage.

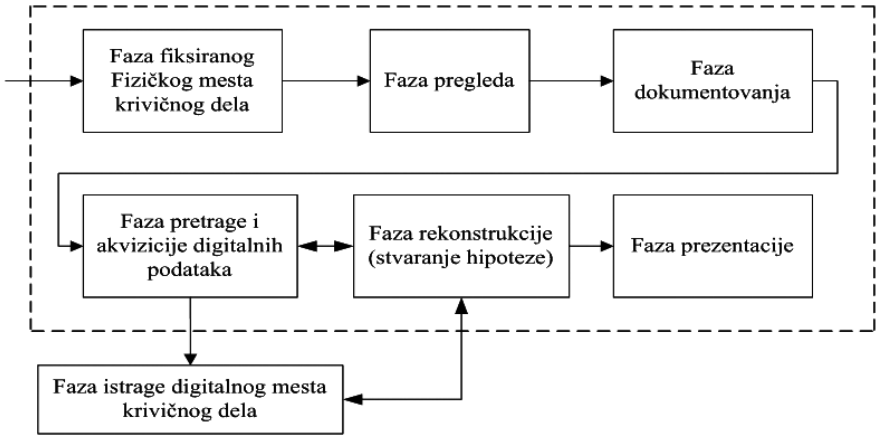
3.4.2.2 Faza potvrde i autorizacije

Nastavlja se u različitim smerovima, zavisno od situacije. Cilj ove faze je da se dobije ovlašćenje za istragu incidenta i mesta krivičnog dela. U slučaju zvanične istrage, ovaj korak podrazumeva obezbeđivanje naloga za pretres, ili drugo legalno odobrenje, koje mora biti potkrepljeno sa dovoljno inicijalnih dokaza, ili osnovanom sumnjom.

Za slučaj *korporacijske istrage incidenta*, nalozi za pretres nisu potrebni dok god se ne krše prava privatnosti, ili slučaj ne preraste kapacitete i sposobnosti korporacijskog tima za istragu, npr., međunarodni incident, zahtev za prisluškivanje telefona osumnjičenog, hapšenje i dr. U situaciji upada u server, ovaj korak uključuje interventni tim za odgovor na incidente koji proverava da li je sistem kompromitovan, tako što ispituju sumnjive aktivnosti na mreži, ili traže maliciozne programe (*rootkit*-ove) u sistemu. U toku ove analize uživo, važno je da se prema računarskom sistemu tim ophodi kao prema mestu krivičnog dela, da se primenjuje kompletna *standardana operativna procedura* pristupa kompromitovanom računaru i da se minimizira uticaj na ispitivani sistem. Posle potvrde da se incident zaista dogodio, neophodan je pristanak vlasnika sistema da bi se preduzele naredne akcije: uključili zvanični organi istrage, ili ne iz bilo kojeg razloga. Za servere čije je vreme aktivnog rada kritično za kompaniju, odobrenje mora da se traži na nivou izvršne vlasti, [12], [25].

3.4.3 Faza istrage fizičkog mesta krivičnog dela

Cilj ove faze je da prikupi i analizira fizičke dokaze i rekonstruiše akcije koje su dovele do incidenta. Jedan od najvažnijih ciljeva forenzičke digitalne istrage je da se identifikuju ljudi koji su odgovorni za incidente i zbog toga su potrebni fizički dokazi. U zvaničnom modelu istrage, istragu fizičkog mesta krivičnog dela vrše istražitelj-ekspert za istragu fizičkog mesta krivičnog dela i interventni tim za reagovanje na kompjuterski incident, ili tim za fizičko obezbeđenje. Faze za istragu fizičkog mesta krivičnog dela prikazane su na slici 3.3.



Slika 3.3 Faze i interakcija istrage fizičkog i digitalnog mesta krivičnog dela

3.4.3.1 Faza obezbeđivanja (fiksiranja) fizičkog mesta krivičnog dela

Ista je za svaki tip krivičnog dela. Osnovne aktivnosti koje se preduzimaju su:

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

U kompjuterskom incidentu, fizičko mesto krivičnog dela treba da se osigura koristeći iste procedure kao i kod fizičkog događaja koji nije digitalni. Na primer, u istrazi *upada u server*, ova faza uključuje identifikovanje lica koja su bila u centru za obradu podataka u vreme incidenta i sprečavanje ostalih lica da uđu u centar polse incidnta, pošto neko od zaposlenih može biti odgovoran za incident. Ova faza obezbeđuje mesto krivičnog dela od izmena, da bi se kasnije mogli sakupiti i identifikovati dokazi i ne čuva samo određene delove dokaznog materijala, već celokupno fizičko i digitalno mesto krivičnog dela kompjuterskog kriminala.

3.4.3.2 Faza revizije fizičkog mesta krivičnog dela

Organ istrage (zvanični, korporacijski) prolazi i opservira fizičko mesto krivičnog dela i obično je prva osoba koja reaguje na kompjuterski kriminal/incident. Cilj je da se identifikuju očigledni delovi dokaznog materijala, osetljivi delovi fizičkog dokaza i razvije početna teorija (hipoteza) o krivičnom delu. Na primer, u istrazi ubistva u stanu, u ovoj fazi se pregleda ceo stan i identifikuje kako je napadač ušao, na kom mestu se ubistvo dogodilo i šta se dogodilo sa žrtvom posle ubistva. Osetljivi digitalni dokazi moraju se

odmah dokumentovati i sakupiti da se ne bi oštetili. U digitalnom incidentu, primeri fizičkih dokaza koji su identifikovani u pretrazi uključuju broj i lokaciju računara, mrežne konekcije, ***PDAs*** (*Personal Digital Assistant*), broj i tip mobilnog telefona, zapisane lozinke na papiru, razne zabeleške o kantaktima, štampani materijali i CD-ROM-ovi ili neki drugi prenosivi mediji sa potencijalnim digitalnim dokazima. Pri završetku ove faze istražni organi imaju ideju kako da obrade fizičko mesto krivičnog dela i koje specijalne veštine su im potrebne za obradu. Ukoliko digitalni forenzičar nije na uviđaju u tom trenutku, treba ga pozvati da dođe i izvrši forenzičku akviziciju dokaza. Računar koji radi i koji je priključen na mrežu smatra se osetljivim dokazom, jer se digitalni dokazi koji se nalaze u njemu mogu izbrisati daljinski, komandom sa udaljenog računarskog sistema ili načinom isključivanja računara, ako je neophodno za privremeno oduzimanje ili uzimanje imidža. Zbog toga obavezno treba primenjivati standardne operativne procedure, kao što su: forenzički prihvatljivo isključivanje računara sa mreže, koje zavisi od vrste platforme (Windows, Linux/Unix,...); pretraga, demontaža, označavanje i pakovanje opreme računarskog sistema i mreže za privremeno oduzimanje i transport do forenzičke laboratorije za ispitivanje; akvizicija digitalnih podataka/dokaza na forenzički sterilne medijume itd.

3.4.3.3 Faza dokumentovanja fizičkog mesta krivičnog dela

Istražitelj treba da pravi fotografije, skice i video snimke mesta krivičnog dela i fizičkih dokaza i da detaljno dokumentuje svaku aktivnost u procesu pretrage. Cilj je da se prikupi što više informacija tako da se sačuvaju i zabeleže razmeštaj komponenti umreženog računarskog sistema i važni detalji sa fizičkog mesta krivičnog dela. Kod digitalnog incidenta važno je da se dokumentuju i fotografišu konekcije na računaru i stanje u kojem je računar zatečen (uključen, priključen na Internet i slika), broj i veličina čvrstih diskova i količina RAM memorije. U nekim slučajevima, treba sačuvati MAC[12] adrese mrežnih kartica da bi se DHCP[13] logovi mogli koristiti za identifikovanje sistemske aktivnosti. U ovoj fazi korisno je sačuvati serijske brojeve i "jednoznačne identifikacione oznake objekata računarskog sistema". Da bi se identifikovalo šta treba sačuvati, treba uzeti u obzir da forenzičke labaratorije za analizu ne mogu najčešće dobiti originalni fizički hardver, već samo fizičku kopiju (*imidž*) čvrstog diska. Treba dokumentovati sve što bi moglo biti od koristi za forenzičku laboratoriju za analizu, ili kasniju rekonstrukciju incidenta. Na kraju ove faze izrađuje se izveštaj o pretrazi i incidentu.

3.4.3.4 Faza pretrage i sakupljanja dokaza sa fizičkog mesta krivičnog dela

Obuhvata pretragu i detaljno prikupljanje dodatnih fizičkih dokaza iz dubine fizičkog mesta krivičnog dela. Pretraga može biti usmerena prema nestalim delovima fizičkih

12 Mashine Address Code

13 *Dynamic Host Configuration Protocol*

dokaza, kao što su oružje, ili može biti metodična i imati striktne obrasce (procedure) pretrage. Svaki tip dokaza treba da ima specifične standardne procedure, za prikupljanje (akviziciju) digitalnih i drugih dokaza. Za digitalni incident u ovoj fazi traže se dodatni mediji i digitalni uređaji sa mesta krivičnog dela, koji mogu biti izvor digitalnih dokaza. Ova faza, takođe, uključuje kontaktiranje administratora radi obezbeđivanja pristupnih logova (*access logs*) baze podataka, promenljivih logova za "*update*" servera, logova *firewoll*-ova, logova IDS/IPS sistema za detekciju i sprečavanje upada i logova udaljenog pristupa (*remote access logs*). Ovo je poslednja faza koja se vrši na realnom fizičkom mestu krivičnog dela kompjuterskog kriminala. Fizički dokazi koji su prikupljeni sa mesta krivičnog dela, šalju se u forenzičku laboratoriju radi analize, a rezultati se koriste u sledećoj fazi, rekonstrukcije incidenta.

Faza pretrage i prikupljanja dokaza sa fizičkog mesta krivičnog dela je faza u kojoj počinje forenzička istraga digitalnog mesta krivičnog dela. Računarski sistem se smatra fizičkim dokazom pa će se i on privremeno oduzeti kao dokazni materijal gde god je moguće. Procedura prikupljanja dokumentuje kako se prikupljaju važni podaci sa sistema koji je aktivan i kako se sistem isključuje.

3.4.3.5 Faza rekonstrukcije fizičkog mesta krivičnog dela

Uključuje organizovanje rezultata analize prikupljenih fizičkih i digitalnih dokaza i korišćenje fotografija sa fizičkog mesta krivičnog dela da bi se razvila hipoteza o incidentu. Za rad sa dokazima mora se koristiti naučni metod, da bi se mogle testirati hipoteze o incidentu. Kod *digitalnog incidenta*, rezultati istrage digitalnog mesta krivičnog dela povezuju se sa fizičkim dokazima, da bi se povezala osoba sa digitalnim događajem. Primeri u ovoj fazi su povezivanje logova sa servera u centru za obradu podataka sa *login*-ovima u radnoj stanici (napadnutom računaru) i drugim mrežnim uređajima, povezivanje *chat* aktivnosti otkrivenih u sistemu i povezivanje aktivnosti na kompromitovanom serveru sa aktivnostima na kućnom računarskom sistemu osumnjičenog i na serveru ISP-a. Da bi bila efektivna, u ovoj fazi treba uključiti i konsultovati digitalne forenzičare za pomoć oko povezivanja događaja sa više izvora digitalnih dokaza. Treba zapaziti da rekonstrukcija fizičkog mesta krivičnog dela nije isto što i "re-kreiranje fizičke scene", koje podrazumeva izradu fizičkog modela mesta krivičnog dela.

3.4.3.6 Faza ekspertskog svedočenja/veštačenja fizičkog mesta krivičnog dela

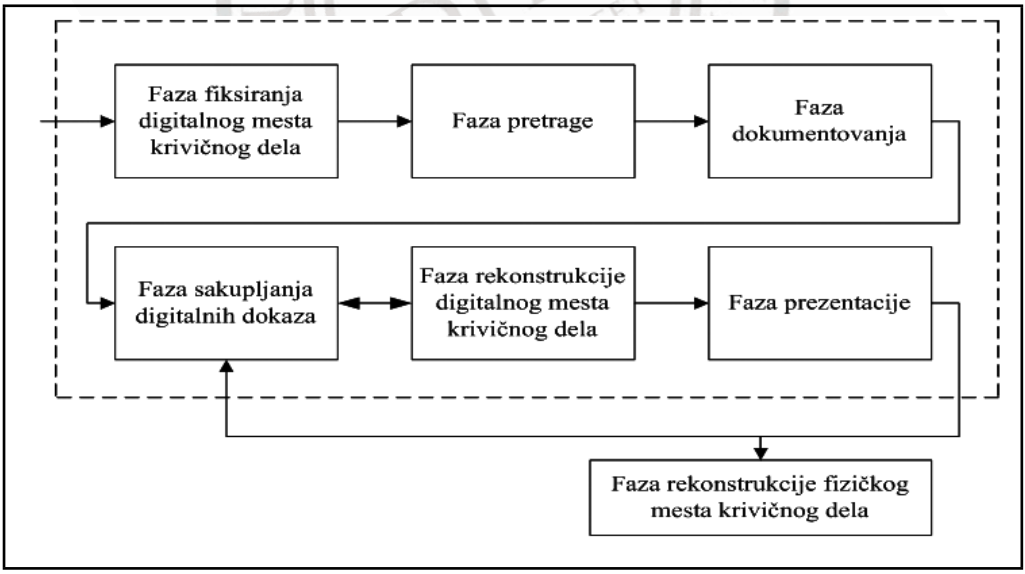
U ovoj fazi forenzičar treba da svedoči ka ekspert ili veštači fizičke i digitalne dokaze sudu ili upravi korporacije. Forenzičar prezentuje dokaze i hipotezu koja je razvijena u fazi rekonstrukcije fizičkog mesta krivičnog dela.

3.4.4 Faza istrage digitalnog mesta krivičnog dela

Faza istraga digitalnog mesta krivičnog dela počinje kada su fizički digitalni uređaji i drugi dokazni materijali prikupljeni kao fizički dokazi sa fizičko mesto krivičnog dela, ili kada je sačuvan analizirani mrežni saobraćaj radi obezbeđivanja dokaza. Ova faza prilazi računarskom sistemu kao fizičkom mestu krivičnog dela i pretražuje ga radi izvlačenja digitalnih dokaza. Cilj je da se identifikuju digitalni podaci o događajima na sistemu i prezentuju istražnom organu fizičkog mesta krivičnog dela.

U ovom modelu, svaki digitalni uređaj smatra se posebnim fizičkim mestom krivičnog dela. Konačni rezultati analize svakog digitalnog uređaja šalju se u *Fazu rekonstrukcije fizičkog mesta krivičnog dela,* u kojoj će biti identifikovane veze između digitalnih uređaja. Ovo omogućava da se analize različitih tipova uređaja izvrše na različitim mestima. Fizička mesta krivičnog dela kompjuterskog kriminala organizovana su u primarna i sekundarna mesta krivičnog dela, gde su primarna mesta ona gde se prvo krivično delo dogodilo, [3]. Digitalna mesta krivičnog dela mogu, takođe, da se organizuju u primarna i sekundarna mesta krivičnog dela. Na primer, server koji je kompromitovan bio bi primarno mesto krivičnog dela, a log server koji je kompromitovan kasnije zbog izmene log podataka koji su u vezi sa upadom, bio bi sekundarno digitalna mesto krivičnog dela.

Digitalni forenzičar istražuje digitalno mesto krivičnog dela kroz sledeće faze, (slika 3.4).



Slika 3.4 Faze forenzičke istrage digitalnog mesta krivičnog dela

3.4.4.1 Faza fiksiranja digitalnog mesta krivičnog dela

Ova faza obuhvata obezbeđivanje ulaza/izlaza ka/od digitalnog mesta krivičnog dela i zaštitu integriteta digitalnih dokaza koji se lako mogu izmeniti. U fizičkom svetu, ovome odgovara smanjenje broja otisaka stopala na fizičkom mestu krivičnog dela i sakupljanje fizičkih dokaza koji se mogu vremenom izgubiti. U digitalnom okruženju ovo bi značilo izolaciju računarskog sistema od računarske mreže, sakupljanje nestabilnih i lako promenljivih podataka koji bi mogli biti izgubljeni kada se sistem isključi (npr. iz RAM memorije) i identifikovanje bilo kakvih sumnjivih procesa, koji su aktivni u sistemu. Sumnjive korisnike, koji su ulogovani na sistem, treba registrovati i po mogućnosti ispitati. Log fajlovi se mogu smatrati za *očevidce digitalnog krivičnog dela* i moraju biti obezbeđeni ukoliko postoji pretnja da mogu biti izbrisani, pre nego što se sistem fizički iskopira. Treba zapaziti da drugi modeli koriste termin "čuvanje" u smislu očuvanje samih digitalnih dokaza u celokupnom lancu istrage od pretrage do završetka sudskog procesa. U ovom modelu "čuva se" celokupno digitalno okruženje. U stvari, nijedan digitalni dokaz nije još identifikovan, kada se ova faza izvršava. Jedna od prednosti digitalnog u odnosu na fizičko okruženje je u tome da se digitalno okruženje može lako kopirati. Zato, je uobičajeno u ovoj fazi da se napravi kompletna fizička (*miror*) slika *bit-po-bit*, ili *imidž* sistema na forenzičkom računaru, da bi se mogao kasnije analizirati u forenzičkoj laboratoriji. Preporučuje se uzimanje najmnje dva imidža osumnjičenog računara – jedan radni i jedan referentni kao dokaz da forenzičar i forenzički alat nisu uneli izmene digitalnih podataka primenom forenzičkih tehnika i alata u fazi forenzičke akvizicije i analize. Fizička kopija osumnjičenog računara – svih diskova/particija čuva celokupno digitalno mesto krivičnog dela, dok obične *backup* kopije sistema čuvaju samo dodeljene (alocirane) podatke u digitalnom mestu krivičnog dela. Kompromitovani kritični računarski sistemi mogu se sa forenzičke fizičke slike brzo oporaviti, priključiti na mrežu i vratiti u funkciju poslovnog sistema. Neki slučajevi zahtevaju da originalni čvrsti disk ostane fizički dokaz sve dok je slučaj u toku. Ako u ovoj fazi skeneri mrežnog saobraćaja snime ilegalni tok mrežnog saobraćaja, ovaj se snimak smatra referentnim (neizmenjenim) stanjem mreže i može se koristiti kao čvrst digitalni dokaz.

3.4.4.2 Faza pretrage digitalnog mesta krivičnog dela

Ova se faza tipično odvija u forenzičkoj laboratoriji na jednoj od forenzičkih replika (imidža) digitalnog mesta krivičnog dela. Međutim, u slučaju nemogućnosti privremenog oduzimanja ili isključivanje kompromitovanog sistema (npr. veliki korporacijski server kojeg nije moguće isključiti), ova se faza može izvršiti uživo u fizičkom okruženju sa tehnikama i alatima *aktivne akvizicije* računara u radu, iako je za digitalnu forenzičku akviziciju i analizu uvek poželjno laboratorijsko okruženje, zato što pruža kontrolisane uslove, a rezultati se mogu ponoviti sa drugom, referentnom replikom sistema, ako to

zahtevaju sudski organi. Iako se *Faza pretrage* izvodi na aktivnom (*živom*) sistemu[14], ipak treba napraviti forenzičku sliku sistema, tako da se svaki prikupljeni digitalni dokaz može verifikovati u kontrolisanom laboratorijskom okruženju. Ova faza se ponekad radi na terenu da bi se utvrdilo da li sistem treba privremeno oduzeti i nositi u laboratoriju na potpunu forenzičku analizu. Pretraga na terenu računarskog sistema koji se privremeno ne oduzima iz bilo kojeg razloga, treba da se izvodi na sistemu butovanom sa butabilnog CD/diskete i u forenzički sigurnom okruženju tako da digitalni podaci/dokazi ostanu nepromenjeni.

U *Fazi pretrage* pronalaze se očigledni delovi digitalnih dokaza za datu vrstu krivičnog dela kompjterskog kriminala. Na primer, u slučaju dečije pornografije istražitelj će prikupiti sve **.jpeg** i **.gif** i druge slike sa memorijskih medijuma sistema i identifikovati one koje bi mogli da se koriste kao dokazi. U slučaju upada u server, forenzički istražitelj traži očigledne znakove instalacije *rootkit* tehnika, analizira logove aplikacija i traži nove konfiguracione fajlove. U drugim slučajevima, mogu se analizirati Internet keš i Internet istorija na HTML pretraživaču. Kada se analizira mrežni saobraćaj o nekom incidentu, u ovoj fazi mogu se analizirati sav saobraćaj u vremenskom okviru incidenta i filtrirati određeni portovi i hostovi. U *Fazi pretrage* procenjuje se veština osumnjičenog i analiziraju tehnike i alati koje treba dokazati u istrazi. Istražitelj u ovoj tački može konsultovati eksperte u oblasti kriptologije, digitalne forenzičke analize, ili eksperte za oporavak podataka ukoliko su neki nestali, ili bili izbrisani.

3.4.4.3 Faza dokumentovanja digitalnog mesta krivičnog dela

U ovoj fazi pravilno se dokumentuju digitalni dokazi koji su sakupljeni i otkriveni u fazi akvizicije. Fizičke kopije sistema koje se uzimaju u *Fazi fiksiranja* digitalnog mesta krivičnog dela*,* imaju istu ulogu kao i skice i video zapisi fizičkog mesta krivičnog dela. Svaki deo digitalnog dokaza koji se pronađe u toku forenzičke analize *imidža* sistema mora biti jasno dokumentovan. Ova faza dokumentuje pojedinačne delove dokaza i ne kreira finalni izveštaj o incidentu. Finalni izveštaj forenzičke digitalne analize pravi se u *Fazi prezentacije.*

Digitalni dokazi mogu postojati u različitim apstraktnim slojevima računarskog sistema i moraju se dokumentovati pomoću specifičnih forenzičkih alata dizajniranih za izvlačenje podataka sa tih slojeva, [4]. Na primer, fajl se može dokumentovati sa punim imenom putanje, klastera i sektora na disku, koje koristi taj fajl sistem. Mrežni podaci se mogu dokumentovati sa izvornom i ciljnom adresom na raznim mrežnim nivoima. Kako su digitalni dokazi promenljivi i mogu ostaviti malo tragova, treba primeniti neku kriptografsku heš vrednost (MD5, SHA1 SHA256,...), na delove digitalnih dokaza u fazi skupljanja, da bi se po zahtevu suda mogao dokazati nepromenjen integritet dokaza. U ovoj fazi formira se lanac neprekidnog čuvanja integriteta i nadzora dokaza, da bi dokazi bili validni i prihvatljivi na sudu. U forenzičkoj praksi istrage digitalnih dokaza,

14 tzv. živa ili realna forenzička akvizicija

Faza dokumentovanja nije strogo odvojena, zato što se digitalni dokazi dokumentuju od neprekidno od trenutka otkrivanja i akvizicije do pripreme dokaza za prezentaciju (svedočenje/veštačenje) pred sudom.

3.4.4.4 Faza sakupljanja digitalnih dokaza sa digitalnog mesta krivičnog dela

Sastoji se od potpune digitalne forenzičke akvizicije relevantnih podataka iz računarskog sistema, radi izvlačenja digitalnih dokaza. Ova faza koristi rezultate iz *Faze pretrage* da bi se usredsredila na dodatne indikatore koji upućuju na digitalne dokaze i odgovarajuće tipove analize. Na primer, u ovoj fazi može se izvršiti pretraga po ključnoj reči za ispitivani slučaj, ukoliko su ključne reči identifikovane iz drugih dokaza. Nedodeljeni (nealocirani) prostori fajl sistema mogu se izvući i obraditi izbrisani fajlovi. Mogu se pratiti i analizirati aktivnosti korisnika nad fajlovima, kao i svi mrežni paketi sakupljeni softverom za monitoring mrežnog saobraćaja. U nekim slučajevima, prikladno je pregledati sadržaj svakog klastera (fizička pretraga), ili svakog fajla (logička pretraga). Kao što postoje različite tehnike istrage fizičkog mesta krivičnog dela, tako postoje i različite tehnike forenzičke akvizicije i analize digitalnog mesta krivičnog dela.

Najveći deo vremena digitalne forenzičke istrage potroši se u ovoj fazi. U digitalnom okruženju, dokazi su kopirani iz digitalnog mesta krivičnog dela, ali odatle nisu uklonjeni, što nije slučaj u realnom fizičkom svetu. Za neke tipove kompjuterskih incidenata, uobičajeno je da u ovoj fazi rade zajedno klasični i tehnički osposobljeni istražitelji, zbog ograničenog broja obučenih istražitelja za digitalnu forenzičku istragu. Na primer, tehnički osposobljen istražitelj će izvući sve slike iz sistema i poslati ih ne-tehničkim istražiteljima koji će analizirati svaku sliku i identifikovati one koje bi se mogle koristiti kao dokaz. Ova faza slična je *Fazi ispitivanja* u drugim modelima istrage.

3.4.4.5 Faza rekonstrukcije digitalnog mesta krivičnog dela

Ova se faza sastoji iz sastavljanja neoborivog, čvrstog digitalnog dokaza bez tzv. pukotina. Digitalni dokazi se mogu razvrstati i proceniti na osnovu toga koliko su uverljivi i pouzdani, [4]. Podaci koji zahtevaju složene tehnike analize, kao što su analize izvršnih fajlova ili dešifrovanje, izvode se u ovoj fazi, a njihovi rezultati se koriste za izgradnju čvrstog dokaza. Ova faza koristi stroge naučne metode da bi se dokazi mogli testirati i da bi se odbacile druge hipoteze, koje se potencijalno mogu zasnivati na digitalnom dokazu. U ovoj fazi se utvrđuje kako je digitalni dokaz dospeo tamo i šta njegovo postojanje znači. Kada digitalni dokaz nije dovoljan, uverljiv ili potpuno nedostaje, obnavlja se *Faza pretrage* da se otkriju i identifikuju dodatni, novi dokazi. Na primer, u slučaju upada u server, ova faza može dovesti u vezu eksplotaciju ranjivih servisa sa instalacijom *rootkit*-a i razvojem mrežnog *sniffer*-a. Izvorišna IP adresa mrežne konekcije može ukazati na potrebu analize sekundarnog digitalnog mesta krivičnog dela – posrednog računara. Ova faza je slična *Fazi analize* u drugim modelima.

3.4.4.6 Faza prezentacije digitalnog mesta krivičnog dela

Ova faza obuhvata prezentovanje otkrivenih digitalnih dokaza timu za istragu fizičkog mesta krivičnog dela i pripremu za ekspertsko svedočenje ili veštačenje pred sudom. Rezultate iz digitalne istrage, tim za istragu fizičkog mesta krivičnog dela koristi u *Fazi rekonstrukcije* krivičnog dela kompjuterskog kriminala. Istražtelj fizičkog mesta krivičnog dela integriše rezultate iz istrage svakog digitalnog mesta krivičnog dela. U ovoj fazi dokumentuju se i prezentuju otkrića u određenim mestima krivičnog dela, ostalim organima istrage. Korisno je i preporučuje se da tim za *fizičku* i *digitalnu* istragu bude jedinstven, jer je lakše ostvariti *potpunu komunikaciju* u kojoj se brže razmenjuju kvalitetnije informacije između članova istog tima.

3.4.4.7 Faza provere

Ovo je finalna faza i sastoji se od revizije i kontrole integralnog procesa istrage, da bi se identifikovale oblasti koje se mogu poboljšati. Za digitalni kompjuterski incident, ovo uključuje analizu kvaliteta rada organa istrage i koliko dobro su izvršene fizička i digitalna istraga svaka za sebe, koliko dobro su urađene fizička i digitalna istraga zajedno i da li postoji dovoljno fizičkih i digitalnih dokaza da bi se slučaj rešio. Rezultat ove faze mogu biti nove poboljšane procedure istrage, dodatna obuka, ili ništa ukoliko je sve ispalo kako je planirano.

U procesu digitalne forenzičke istrage kompromitovanog/osumnjičenog računarskog sistema na fizičkom mestu krivičnog dela, forenzički istražitelj digitalnih podataka (*digitalni forenzičar*) uobičajeno preduzima sledeće korake, [7], [20]:

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

3.5 MODEL DOMENA SLUČAJA DIGITALNE FORENZIČKE ISTRAGE

U funkcionalnom modelovanju procesa digitalne forenzičke istrage, od velike pomoći za forenzičare može biti korišćenje modela *domena slučaja* digitalne forenzičke istrage, [1].

Generalni pristup modelovanju domena slučaja digitalne forenzičke istrage je upotreba UML (*Unified Modelling Language*) alata za opisivanje ključnih, relativno nezavisnih *koncepata objekata*, njihovih *atributa* i *međusobnih veza* u oblasti forenzičke istrage slučaja. Model generiše *koncepte* objekata ekstrakcijom imenica i glagola iz dokumenata slučaja kao što su polazne činjenice i okolnosti, nalog za istragu, nalog za pretres stana, izveštaj o hapšenju, izveštaj o incidentu itd. Pri tome je važno zadržati koncepte dovoljno generičkim, tako da se mogu višekratno koristiti u domenu sličnih slučajeva, kao što je prikazano u tabeli 1.2.

Tabela 1.2 Primeri kategorija koncepata objekata za digitalnu forenzičku istragu

Kategorija koncepta objekata	Primer
Fizički ili opipljiv objekat	Mobilni telefon, HD, CD-R, DVD-RW disk i slika
Opis neke stvari	Marketinški izveštaj, Izveštaj o incidentu
Mesta (lokacije)	Kuća, ulica, automobil
Transakcije	Isplata, prodaja, deponovanje novca, e-mail transakcija
Uloge ljudi	Žrtva, osumnjičeni, svedok
Kontejner ispitivanih objekata	Baza podataka, HD-i
Objekti u kontejneru	Fajlovi, transakcije
Računar ili elektro-mehanički sistem	Repozitorijum podataka ili baza podataka na Internetu, sistem za autorizaciju kreditnih kartica
Koncepti apstraktnih imenica	Motiv, alibi, nevinost, siromaštvo
Organizacije	Mafija, odeljenje korporacije, državna organizacija
Događaj	Pljačka, sastanak, telefonski poziv, pristup fajlu
Pravila i politike	Zakon, procedure, politike zaštite korporacije
Finansijski, poslovni, ugovorni i pravni zapisi	Ugovor o zaposlenju, rentiranje, potvrda, nalog za pretres
Servisi	Letačko uputstvo, uputstvo za eksplozive i slika

tributi su karakteristike koje definišu koncepte objekata i predstavljaju informacije koje su bitne za digitalnu forenzičku istragu. Pre svega, lista atributa treba da bude dovoljno detaljna da obezbedi jedinstvenu diferencijaciju događaja u jednom konceptu objekta. Imena koncepata objekta i pripadajući atributi su najznačajnije informacije za potrebe planiranja procesa forenzičke istrage. Međutim, potrebne su dodatne informacije koje se odnose na koncepte objekata i druge informacije koje mogu pomoći organu istrage da razume pozadinu i okolnosti u ispitivanom slučaju. Takva lista u formi tabele (Tabela 1.3) može se koristiti kao kontrolna (*ček*) lista za identifikaciju potencijalnih odnosa između izabranih koncepata objekata u slučaju i biti od velike koristi istražitelju.

Tabela 1.3 Primeri provere međusobnih odnosa koncepata

Kategorije	Primeri
A je fizička particija B	DVD disk – radna stanica
A je logička particija B	Mapiranje mreže – Upad u mrežu
A je fizički sadržan u/na B	Korišćeni CD-R disk – CD slučaj
A je opis za B	*Readme* fajl – Izvršni program
A poseduje B	Osumnjičeni – nosilac (za lansiranje napada)
A je član B	Osumnjičeni – kriminalna banda
A je organizaciona jedinica B	IKT odeljenje – organizacija
A koristi ili upravlja sa B	Sistem administrator – RM kompanije
A je specijalizovana verzija uopštenog B	Sistem administrator – zaposleni organizacije
A komunicira sa B	Osumnjičeni – društvena grupa
A je poznat/registrovan/izvešten u B	Registar e-pošte – mrežni logovi

Praktična implementacija ovakvog pristupa kroz aplikaciju nekog forenzičkog alata za automatizaciju ovog modela još je u ranoj razvojnoj fazi. Dobra iskustva se mogu izvući iz oblasti IKT sistema u zdravstvu (medicini).

Forenzička praksa smatra da je „velika“ količina podataka od **20GB-2TB** (**1**terabajt=**1**TB≈10^{10}B). Objavljen je slučaj procesiranja podataka od 450TB sa magnetnih traka za bekapovanje sa zadatkom otkrivanja jedinstvenih fajlova preko ključnih reči. Ispostavilo se da je svega 6% materijala sadržavalo relevantne podatke. Za ovu forenzičku analizu angažovani su sledeći namenski uređaji i drugi resursi: 75 reproducera trake, 7 servera, 32 radne stanice, 7 forenzičara, rad od 24/7 u trajanju od 60 dana, sa ukupnim troškovima od 259.000 USD$.

Generalno, najveći problemi u procesu digitalne forenzičke istrage su brzina procesiranja po pravilu velike količine digitalnih podataka, skretanje pravca istrage slučaja, veliki i lozinkom zaštićeni čvrsti diskovi. Informacije iz predistražnog postupka, inicijalne pretrage i istrage fizičkog i digitalnog mesta krivičnog dela kompjuterskog kriminala/incidenta, kao što su dobra dokumentacija o tome šta se traži, šta su prioritetna pitanja i šta je očekivani izlaz digitalne forenzičke analize, mogu pomoći forenzičaru da se usredsredi na ispitivanje i analizu relevantnih podataka za izgradnju čvrstih digitalnih dokaza.

Ako se ispituju sistemi RAID diskova sa kapacitetom od više terabajta (TB), redukcija imidžovanja može se postići integracijom seta *hash* funkcija sa alatom za uzimanje imidža diskova. U mrežnoj forenzici za redukciju količine akvizicijom sakupljenih podataka mogu se koristiti tehnike uzorkovanja intercepcije mrežnog saobraćaja, kao i bolja klasifikacija relevantnih i nekorisnih podataka. Drugi pristup je da se primeni proaktivno inkrementalno uzimanje imidža iz korporacijskog visoko distribuiranog IKT okruženja. Posedovanje takvih imidža može u slučaju kompjuterskog incidenta/kriminala dati forenzičaru veliku prednost u procesiranju slučaja.

Ostale ideje za smanjenje problema velikog obima podataka za analizu je primena ekspertnih sistema (ES) i veštačke inteligencije (VI) u oblastima gde bi ova primena mogla biti zaista efektivna i efikasna. Takvo rešenje bi moglo biti primena procesiranja na bazi prirodnog jezika za automatizaciju kratkog sadržaja slučaja i pretraživanja tih sadržaja umesto klasičnog (*search*) pretraživanja na bazi ključne reči celokupnog obima podataka. Takođe, bi se primenom VI, ali i bez nje, mogle grupisati slike na bazi predefinisanog kriterijuma, na primer, „sve grupne fotografije ljudi“ u jedan fajl zajedno sa pripadajućim kriterijumom, što bi za forenzičara bila velika pomoć.

Definisanje forenzičkog cilja je metodološki veoma korisna faza digitalne forenzičke istrage, [6].

Definisanje forenzičkog cilja je tačka u kojoj forenzički analitičar formuliše proces pretraživanja digitalnih podataka, a rezultati pretraživanja su ciljni objekti. Za razliku od drugih faza procesa forenzičke analize, definisanje forenzičkog cilja zahteva intenzivniji rad forenzičara, ali može omogućiti automatizovanu podršku forenzičkih alata. Primer je alat koji posle pretraživanja fajlova sugeriše dalje pretraživanje ostalih objekata računarskog sistema, kao što su drugi fajlovi sa sličnim imenom, drugi fajlovi u istom direktorijumu ili fajlovi sa sličnim sadržajem, vremenski pečati ili tipovi aplkacija. Detekcija različitosti (*Outlier Detektion*) traži objekte koji su sakriveni ili se značajno razlikuju od njihovog neposrednog okruženja.

REZIME

Istragu događaja koji predstavljaju zloupotrebu u IKT sistemima i istragu kompjuterskog kriminala mogu efikasno vršiti samo visoko-specijalizovani stručni kadrovi u interventnim timovima sa odgovarajućim kapacitetima. Rezultati korporacijske istrage treba da se prikažu u izveštaju interventnog korporacijskog tima u standardnom formatu.

Integracijom zvaničnog modela istrage klasičnog kriminala i specifičnosti modela istrage bezbednosnog kompjuterskog incidenta, dobije se integrisani model istrage kompjuterskog kriminala koji celovito posmatra fizičko mesto krivičnog dela kao *primarno* i digitalno mesto krivičnog dela kao *sekundarno mesto* krivičnog dela kompjuterskog kriminala. Ovaj model omogućava kompletnu dokumentaciju mesta zločina i koristi iskustvo klasične istrage da bi se došlo do korisnih dokaza.

U funkcionalnom modelovanju procesa digitalne forenzičke istrage, od velike pomoći za forenzičare može biti korišćenje UML modela *domena slučaja* digitalne forenzičke istrage, koji generiše *koncepte* objekata ekstrakcijom imenica i glagola iz dokumenata slučaja kao što su polazne činjenice i okolnosti, nalog za istragu, nalog za pretres stana, izveštaj o hapšenju, izveštaj o incidentu itd. Atributi opisuju svojstva koncepata objekata i predstavljaju informacije bitne za digitalnu forenzičku istragu, a u kombinaciji sa dodatnim informacijama iz procesa istrage može se koristiti kao ček-lista za identifikaciju potencijalnih odnosa između izabranih koncepata objekata u slučaju, što može biti od velike koristi istražitelju.

U forenzičkoj praksi jedan od najznačajnijih problema je ispitivanje velike količine digitalnih podataka. Pored brojnih tehnika za smanjenje količine digitalnih podataka za imidžovanje i analizu, potencijalno se mogu koristiti ekspertni sistemi i veštačka inteligencija. Korisna faza digitalne forenzičke istrage je definisanje forenzičkog cilja pretraživanja digitalnih podataka, gde su rezultati pretraživanja ciljni objekti analize.

PITANJA ZA PONAVLJANJE

1. Navedite glavne faze istrage fizičkog mesta krivičnog dela klasičnog kriminala.
2. Navedite faze modela zvanične istrage digitalnog mesta krivičnog dela.
3. Navedite glavne faze korporacijskog modela istrage bezbednosnog kompjuterskog incidenta.
4. Šta predstavlja ispitivani računar u modelu integrisanih procesa digitalne forenzičke istrage?
5. Šta je ispitivani računar u slučaju kompjuterskog kriminala u odnosu na primarno fizičko mesto krivičnog dela?
6. Definišite digitalni dokaz.
7. Navedite pet osnovnih grupa organizovanja faza modela integrisanih procesa istrage kompjuterskog kriminala.
8. Navedite sve faze istrage digitalnog mesta krivičnog dela.
9. Opišite fazu dokumentovanja digitalnog mesta krivičnog dela.
10. Opišite fazu rekonstrukcije digitalnog mesta krivičnog dela.
11. Zašto je koristan model domena slučaja digitalne forenzičke istrage?

4. DIGITALNI DOKAZ

4.1 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 dokaza pred sudom.

Digitalni kompjuterski dokaz formira se iz gomile *posrednih* digitalnih podataka, od kojih se ni jedan ne sme isključiti iz bilo kog razloga. Digitalni podaci moraju biti potpuni, da se međusobno dopunjuju (preplićui) 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 u različitim pravosudnim sistemima. Sudska praksa prihvata kompjuterski generisane i kompjuterski memorisane digitalne dokaze pod odgovarajućim uslovima. Transformacija digitalnih 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. Zato treba da postoje procedure za rukovanje i čuvanje, kao i procedure za akviziciju i analizu digitalnih dokaza sa čvrstog diska i drugih medijuma, odnosno, ne smiju se podaci izmeniti, manipulisati ili oštetiti ni u jednom koraku istrage, [17], [22].

Najteže je dobiti digitalne dokaze bez tzv. pukotina, koji potpuno pokrivaju zaključke i objašnjenja. U izgradnji čvrstih (neoborivih) digitalnih dokaza utvrđuje se: šta se stvarno desilo, šta je izgubljeno, koliki je iznos štete i da li se stvarno dogodilo krivično delo kompjuterskog kriminala. Pri tome se mora zadržati potpuna objektivnost. Kada se rekonstruiše hipoteza o događaju, tada počinje prikupljanje dokaza. Dokaze treba prikupljati na mestu krivičnog dela kompjuterskog kriminala, jer to može biti jedini kontakt sa stvarnim dokazima. Treba raditi metodično, strpljivo sakupljati ključne dokaze i kritički se 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 dokaz 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. Sve posredne digitalne i druge fizičke dokaze, koji zajedno čine dokazni materijal, treba tretirati kao da direktno vode ka nepobitnom dokazivanju izvršenog krivičnog dela i kao da su svi jednako važni i kritični za konkretni slučaj. Tek tada počinje proces izgradnje čvrstog dokaza bez tzv. pukotina, odnosno, izgradnja neoborivog dokaza. Potrebno je, dakle, mnogo posrednog dokaznog materijala za samo jedan 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 regularnog 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):

4.2 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 iskusio (čuo, video, zna), a ne iz druge

ruke, što se smatra *posrednim* dokazom, poznat u žargonu kao "rekla – kazala", [11].

Međutim, kod računara imamo upravo slučaj da se, sve što se nalazi u njemu, može svesti pod kategoriju posrednih "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 specifične kriterijume u procesima forenzičke akvizicije, analize i sudskog veštačenja. Ovi su kriterijumi kritični u pogledu spsobnosti 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 podatak u *log* fajlu, 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 orginalno stanje. Ovo je od kritičnog značaja za prihvatanje dokaza na sudu[15]. Kako su dokazi pribavljeni, čuvani, prenošeni, zaštićeni od izmena i kako se sa njima manipulisalo, ključni su elementi da li će biti na sudu prihvaćeni ili odbačeni. Prethodno, originalno, stanje digitalnih dokaza moraju utvrditi svedoci eksperti ili sudski veštaci za IKT, 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 kompjuteru za poređenje,
- sudski veštak za IKT mora svedočiti kako je kopija napravljena (npr., štampana kopija login fajlova) kao i druge detalje rukovanja sa fajlom i štampanom kopijom.

15 *forensic evidence.*

4.3 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 (akvizicije i analize), glavnog pretresa (suđenja i presude), što znači da je dokaz u posedu suda od trenutka akvizicije do donošenja presude. Prikupljeni dokazi se moraju 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. algoritmom SHA256[16], koji kreira sigurnu heš (*hash*) funkciju (sažetak fajla). Sud može prihvatiti digitalno potpisan (heširan) dokaz kao orginalan, jer svaka izmena fajla menja vrednost heša 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, [7], [21], [24].

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 *snifera*[17] 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, informacijama 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* nad *informacionom imovinom*[18] – podacima i informacijama u IKT sistemima uspostavljaju se primenom, tajnih lozinki, mehanizama kriptozaštite i drugih mehanizama za kontrolu pristupa, skrivenih fajlova, kao i raznih upozorenja, koja sugerišu da je, na primer, neka informacija vlasništvo i da bez eksplicitne dozvole vlasnika nema pristupa, kopiranja ili otkrivanja.

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

Ako inicijalna korporacijska istraga unutar IKT sistema utvrdi da je napad došao izvan sistema korporacije i ako menadžer, ili vlasnik sistema donesu takvu odluku, onda se u

16 SHA256 –standardni 256-bitni heš algoritam iz serije SHA1, SHA128, SHA512,...

17 *Snife*r – skenerski uređaj za praćenje rada osumnjičenog u informacionom sistemu

18 Prema standardu ISO/IEC 27001 obuhvata: podatke, informacije, hardver, softver, mrežnu infrastrukturu i ljude

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.

4.3.1 Procedura sakupljanja posrednih kompjuterskih dokaza

Proces akvizicije koji obuhvata otkrivanje, identifikaciju, izvlačenje i sakupljanje digitalnih kompjuterskih podataka, uključujući potencijalne digitalne dokaze, izvršava se kroz više aktivnosti. Ozbiljnija procedura skupljanja digitalnih dokaza treba da obuhvati najmanje sledeće aktivnosti, [10], [9], [17], [19]:

- 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 osporavqaju postavljenu hipotezu, 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 (tužba i odbrana) žele da otkriju i podnesu neoborive dokaze;
- Sakupiti sve pokretne medijume (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 slučaja;
- Napraviti skice ili fotografisati osumnjičeni računar i sve periferne uređaje; označiti i sačuvati sve odvojene periferne uređaje i kablove računarskog sistema koji se privremeno oduzima, 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 zatečeno stanje;
- 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 regularnim putem, jer bi se isključivanjem mogli uništiti dokazi o upadu. Na primer, ako se Unix mašine ne isključe regularno može doći do oštećenja fajlova, ali ako se Windows mašina isključi regularnom (shatdown) metodom, može doći do gubitka potencijalnih dokaza;
- Pošto se u svim sistemima lako kreiraju anti-forenzičke zamke, ili se mogu koristiti antiforenzički softveri za brisanje regularnih tragova u računaru ,

forenzičari treba da obrate posebnu pažnju na tzv. boby zamke za uništavanje fajlova sa dokazima, ako se računar ne isključuje regularnim metodom. Zato uvek postoji dilema da li računar, na primer sa Windows OS, isključiti regularno i rizikovatii uništavanje nekih podataka, ili ga isključiti nepropisno čime se omogućava aktiviranje boby zamke koja može da uništi gotovo sve dokaze. Kako će postupiti u konkretnom slučaju, to mora proceniti sam istražitelj. U svakom slučaju najbolje je koristiti pomoć 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 najbolje angažovati eksperta za IKT, koji treba da onesposobi svaku logičku bombu sakrivenu u osumnjičenom/kompromitovanom računaru;
- Za rebutiranje ispitivanog, privremeno oduzetog računara nikada ne treba koristiti njegov OS i komandnu liniju. Računar treba butirati sa butabilnog diska/CD, koji je fizički zaštićen od upisivanja, čime se sprečava unošenje virusa, ili sa CD ROM–a koji je fizička slika OS;
- Kada se završi rebutiranje ispitivanog sistema, prvo se uzima fizička slika HD–a (alatom tipa Drivespay, X-Way Forensic i slika), 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 periferijama, 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 preliminarnog ispitivanja, otkrivanja 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, itd., koji postoje na HD, ili u bekap mediju, ili različito

formatirane verzije podataka, npr. .templets, .doc, .pdf i slika, bilo da su tako namerno formirane ili su tretirane drugim aplikativnim programima, npr., Word processing, spreadsheet, e-mail, timeline, sheduling, 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 ili uticajem forenzičkog alata,
- da se ni jedan mogući kompjuterski virus ne ubaci 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 funkcionalnost 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 saslušavanih lica, ili advokata koji su prema etičkom kodeksu dužni pružiti sve neophodne informacije forenzičaru.

4.4 KORISNICI KOMPJUTERSKIH DIGITALNIH DOKAZA

U procesu istrage kompjuterskog kriminala mnogi organi i institucije mogu zahtevati i koristiti kompjuterske digitalne dokaze, kao što su, [11], [14]:

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

4.5 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, a posebnu obuku i veštine iz specifične oblasti koju svedoči/veštači. 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., [12], [20].

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-svedoči IKT ekspert, ili 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 veštake 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 odvraćanja, pa vrhunski eksperti za IKT često odbijaju sudsko veštačenje i sučeljavanje mišljenja sa drugim podjednako dobrim forenzičkim ekspertom i radije prihvataju ulogu neutralnog stručnog konsultanta tužioca, ili samog sudije, nego odgovornog svedoka ili veštaka.

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

4.6 PREPORUKE IOCE ZA UPRAVLJANJE DIGITALNIM DOKAZIMA

Preporuke IOCE definišu postupke sa prikupljenim i obrađenim dokazma, [22]:

- Za skladištenje i čuvanje fizičke kopije digitalnih dokaza nisu prihvatljivi instant film polaroid tipa, indžekt printeri, ink printeri, termalni voštano – papirni printeri, dye sublimacioni printeri, suvo srebreni 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 jednokratno upisivanje (ne RW) i DVD-R za jednokratno snimanje.

- Za čuvanje originalne fizičke kopije digitalnih dokaza mogu 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 osumnjičenog računara sačuvati kao referentni dokaz integriteta.
- Dokumentacija za analizu fizičke slike osumnjičenog računara mora biti tačna, 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/veštačenja na sudu.

Procedura za upravljanje digitalnim dokazom mora se administartivno propisati u svakom pravosudnom sistemu i mora postojati zakonska obaveza svakog pojedinca da čuva integritet dokaza u lancu digitalne forenzičke istrage.

REZIME

Digitalni dokaz je svaka informacija uskladištena ili prenesena u digitalnoj formi, koja ima dokazujuću vrednost i na koju se sud može osloniti. Pojam digitalnog dokaza uključuje kompjuterski uskladištene i generisane dokaze, digitalni audio i video materijal, digitalni zapisi na mobilnom telefonu, digitalnoj fax mašini i drugim digitalnim uređajima.

Očekuje se da forenzička analiza digitalnih dokaza otkrije najviše potrebnih podataka za izgradnju čvrstog, neoborivog digitalnog dokaza, jer postoji velika razlika između kompjuterskog digitalnog dokaza u računaru (*computer evidence*) i čvrstih, neoborivih dokaza (*proof*) prihvatljivih na sudu. Neoborivi, čvrsti dokaz nepobitno uspostavlja činjenice, ali sadrži i subjektivnu interpretaciju kompjuterskog digitalnog dokaza koju izvodi forenzičar. Kompjuterski digitalni dokaz u računaru je *objektivan* digitalni podatak i može se koristiti u meri u kojoj se može dokazati da nije izmenjen.

Pri akviziciji kompjuterskih digitalnih dokaza treba uvek verovati u indikacije koje pokazuje istraga, sve dok se ne sastave svi delići posrednih digitalnih dokaza u čvrsti dokaz bez tzv. pukotina. Treba tražite nekonzistentnosti, ali prihvatiti i ono što se vidi, bez racionalizacije. Ako se u toku forenzičke akvizicije digitalnih dokaza dobiju konfliktni podaci, treba se vratiti korak unazad i pokušati otkriti šta se stvarno vidi. Možda konflikt uopšte i ne postoji. Ukoliko konflikt postoji, ne pokušavati njegovo rešavanje racionalizacijom.

Ni u kom slučaju ne menjati ništa u ispitivanim računarima, sa kojih se u procesu akvizicije digitalnih dokaza sakupljaju digitalni podaci i ne objavljivati nalaze forenzičke analize digitalnih dokaza u toku istrage. Treba uvek računati da će slučaj ići na sud, a napadač bi u međuvremenu mogao izmeniti svoj računar i izbrisati sve podatke i eventualne tragove napada, koji mogu biti potencijalni digitalni dokazi.

U periodu nepostojanja nacionalne zakonske regulative, preporuka, standarda, principa i procedura za istragu slučajeva kompjuterskog kriminala i zloupotreba IKT, akviziciju i analizu digitalnih dokaza i veštačenja pred sudom, treba u što je moguće većoj meri koristiti odgovarajuća, međunardodno priznata rešenja i najbolju praksu digitalne forenzike (IOCE).

PITANJA ZA PONAVLJANJE

1. Opišite kako se formira digitalni kompjuterski dokaz.
2. Koje su tri osnovne kategorije digitalnih podataka koje postoje u kompjuterskom incidentu postoje?
3. Navedite glavne pravosudne zahteve za prihvatljivost digitalnih dokaza.
4. Koja tehnika obezbeđuje zaštitu integriteta digitalnih dokaza u celokupnom lancu istrage?
5. Zašto je nedovoljna tehnika bekapovanja za skupljanje (akviziciju) digitalnih dokaza?
6. Kako se sve naziva proces uzimanja bit po bit slike ispitivanog računara?
7. Koji entiteti mogu biti korisnici digitalnih dokaza?
8. Navedite neki od problema i zahteve za pripremu digitalnih dokaza za veštačenje pred sudom.
9. Koji su sve mediji prihvatljivi za čuvanje originalne fizičke kopije digitalnih dokaza?
10. Zašto se preporučuje uzimanje dve fizičke kopije ispitivanog diska?

KLJUČNI TERMINI

Digitalna forenzika: Aplikacija nauke na identifikaciju, sakupljanje, ispitivanje i analizu podataka štiteći integritet informacija i održavajući striktno lanac čuvanja podataka.

Digitalni dokaz: Obuhvata svaki i sve digitalne podatke koji mogu nesumnjivo dokazati da je krivično delo kompjuterskog kriminala izvršeno ili može povezati delo i počinioca ili delo i žrtvu.

Fizički dokaz: Svaki fizički objekat koji može uspostaviti dokaz da je kriminalno delo učinjeno, ili povezati kriminal i žrtvu, ili kriminal i počinioca.

Forenzička nauke: Primena nauke na sudske zakonom obuhvaćene slučajeve.

Kibernetički kriminal (*Cybercrime*): Svako krivično delo gde način izvršenja, ili potpis uključuje upotrebu računarkih mreža na bilo koji način.

Kibernetički prostor (Cyberspace**)**: Odnosi se na konekcije i konceptualne lokacije kreirane korišćenjem računarskih mreža. U svakodnevnoj upotrebi postao je sinonim za Internet.

Kompjuterski kriminal: Uključuje krađu računarskih servisa, neovlašćeni pristup zaštićenim računarima, softversku pirateriju, izmenu ili krađu elektronski uskladištenih informacija, iznuđivanje izvršeno upotrebom računara, neovlašćen pristup bankama i krađa novca, saobraćaj sa ukradenim lozinkom i idntitetom i transmisija destruktivnih virusa ili komandi.

Mesto krivičnog dela (*Crime Scene*): Lokacija gde se dogodilo kriminalno delo.

Primarno mesto krivičnog dela: Lokacija na kojoj je osumnjičeni počinio najveći deo napada na žrtvu.

Rekonstrukcija kriminala: Određivanje akcija koje su dovele do izvršavanja krivičnog dela. Može se izvršiti na bazi izjava svedoka, priznanja osumnjičenog , izjave žive žrtve ili ispitivanja i interpretacije fizičkih i digitalnih dokaza. Neko ga definiše kao proces rekonstrukcije mesta krivičnog dela, što nije adekvatno, jer se mogu rekonstruisati samo aktivnosti koje su dovele do krivičnog dela.

Sekundarno mesto krivičnog dela: Svaka lokacija izvan primarnog mesta krivičnog dela na kojoj mogu biti dokazi o krivičnom delu. U kompjuterskom kriminalu to je osumnjičeni računar.

LITERATURA

1. Bogan C. & Dampier Dr David, *Preparing for Large-Scale Investigations with Case Domain Modeling",* CS 483, Washington State Universit, Spring 2009.
2. Brodsky S. L, *Testifying in Court: Guidelines and maxims for the Expert Witness*, Washington, DC, American Psychological Association, 1991.
3. Bruce J. Nikkel, *The Role of Digital Forensics within a Corporate Organization*, BSA Conference, Vienna, May 2006.
4. Carrier B., *Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers*, International Journal of Digital Evidence, Winter 2003.
5. Carrier B., Spafford H. E., *Getting Physical with the Digital Investigation Process,* International Journal of Digital Evidence, Vol. 2, Iss. 2, CERIAS, Purdue University, 2003.
6. Carrier B. &Spafford E., *Automated Digital target definition Using Oulier Analysis*, CS 483, Washington State Universit, Spring 2009.
7. Carvey H., *Windows Forensic Analysis DVD toolkit,* Syngress Publishing Inc., www.syngress.com, 2007.
8. Casey E., *Digital Evidence and Computer Crime*, Academic Press, 2000.
9. Farmer D., Wietse V., *Forensic Discovery*, http://www.fish2.com/forensics, 2006.
10. *Federal Rule of Digital Evidence*, http://www.house.gov./judiciary/ evid2001.pdf, USA gov., 2002.
11. Gary E. Fisher**,** *Computer forensics Guidance*, NIST, www.nist.com, 2001.
12. Grance T., Kent K., Kim B., *Computer Security Incident Handling Guide*, NIST Special Publication 800-61, January 2004.
13. Grimes R. A., *Honeypots for Windows*, www.amazon.com, 2006.
14. Grubor G., *Osnove Kompjuterskog kriminala*, skripta, Univerziitet Singidunum, Fakultet za poslovnu informatiku, 2006, Beograd.
15. http://www.atstake.com.
16. http://www.ensfi.org,
17. **http://www.iacis.org/**.
18. http://www.ncjrs.org, *Electronic Crime Scene Investigation: A Guide for First Responders*, 2001.
19. http://www.ojp.usdoj.gov/nij/pubs.htm
20. Icove D., Segar K., VonStorch W., *Computer Crime, A Crimefighter's Handbook,* O'Reilly & Associates, 2004.
21. Information Security Forum, *The standard of Good Pratctice for Digital Forensic*, www.isf.com, 2006.
22. IOCE, *IOCE Princips & Definitions*, IOCE 2. Conference, London, 7. 10. 1999.
23. ISF, *The standard of Good Pratctice for Information Security*, www.isf.com, 2006.
24. James S., Nordby J., *Forensic Science: An Introduction to Scientific and Investigative Techniques*, CRC Press, 2003.
25. Kent K., Chevalier S., Grance T., *Guide to Integrating Forensic Techniques into Incident Response*, NIST SP 800-86, 2006.
26. Lee H., and all, *Henry Lee's Crime Scene Handbook*, Academic Press, 2001.

27. Matson J.V., *Effective Expert Testimony,* 3rd edition Boca Raton, Press, p.71, 1999.
28. Milošević, M., *Stručna lica u krivičnom postupku*, Beograd: Policijska akademija, 1996.
29. Mocas Dr. Sarah, *Topics in Computer Science Introduction to Digital Forensi*cs, CS 483, Washington State Universit, Spring 2009National Policing Improvement Agency, *Core Skills in Data Recovery & AnalysisCourse Reference Book V2.01*, Bradford, UK, May 2007.
30. NIJ (National center for Forensic Science), *Digital Evidence in the Courtroom: A guide for Preparing Digital Evidence for courtroom Presentation*, mart 12, 2003.
31. Petrović R. S., *Kompjuterski kriminal II Izdanje,* MUP Republike Srbije, 2001.
32. Pettinari D., Cmdr., *Handling Digital Evidence from Seizure to Court Presentation*, IOCE conference, juni 2000.
33. Pollit M. Mark, *Report on Digital Evidence,* (FBI CART report, DC Washington, USA), Interpol Forensic Science Symposium, Lyon, France, 16 - 19. 10. 2001.
34. Republika Srbija, *Predlog krivičnog zakona, Glava 27-Krivična dela protiv bezbednosti računarskih podataka*, član 298-304, 2003.
35. Republika Srbija, *Zakon o borbi protiv visoko tehnološkog (kompjuterskog) kriminala,* 2005.
36. Rosenblatt, K. S., *High Technology Crime — Investigating Cases Involving Com*puters, KSK Publications, San Jose, CA, 1995.
37. Rosenblatt, K. S., *High Technology Crime — Investigating Cases Involving Computers*, KSK Publications, San Jose, CA, 1995.
38. Smith F. C., Gurley R. B., *A Guide to Forensic Testimony – The art and Practice of Presenting testimony as an Expert Technical Witness*, Addison – Wesley, Boston SAD, 2002.
39. Steel C., *Windows Forensic, The Field Guide for Corporate Computer Investigations*, John Wiley&Sons, 2006.
40. Whitcomb C M., *A Historical perspective of Digital Evidence*: *A Forensic Scientist's View,* International Journal of Digital Evidence, vol.1, issuue 1, 2002.
41. www.fbi.gov./hq/lab/fsc/backissu/oct2000/computer.html

UNIVERZITET
PRIVATNI
AKREDITOVANI
UNIVERZITET
SINGIDUNUM

II DEO

TEHNOLOŠKE OSNOVE DIGITALNE FORENZIČKE ISTRAGE

Cilj ove glave je da se definišu i opišu osnovne forenzičke tehnike i alati za istragu, akviziciju i analizu digitalnih dokaza. Razumevanjem potrebe za neprekidan razvoj funkcionalnosti forenzičkih alata za različite apstrakcione slojeve, kao i zahteva za razvoj alata za specifične forenzičke zadatke, ali i za integrisanje funkcija forenzičkih alata u set alata za terenski rad i laboratorijsku analizu, studenti se osposobljavaju za samostalan izbor optimalnih forenzičkih tehnika i alata za konkretni slučaj digitalne forenzičke istrage, akvizicije i analize.

UNIVERZITET
PRIVATNI
AKREDITOVANI
UNIVERZITET
SINGIDUNUM

UVOD

Ranih 90-tih razvijeni su prvi alati za istragu i ispitivanje digitalnih podataka. Asocijacija specijalista za istragu kompjuterskih podataka - IACIS (*Information Association of Computer Investigative Specialists*) organizuje obuku za digitalnu forenzičku istragu. Za uspešnu digitalnu forenzičku istragu potrebno je dobro poznavati različite platforme: DOS, MSDOS, Windows 9x/NT/2000/XP/Vista, UNIX/Linux, Machintosh i dr. Značajne resurse za digitalnu forenzičku istragu predstavlja mreža eksperata za digitalnu forenziku računarskih sistema i drugih profesionalaca i održavanje kontakata putem e-mail poruka sa specijalistima različitih disciplina, [21].

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

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

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

1. DIGITALNA FORENZIČKA NAUKA

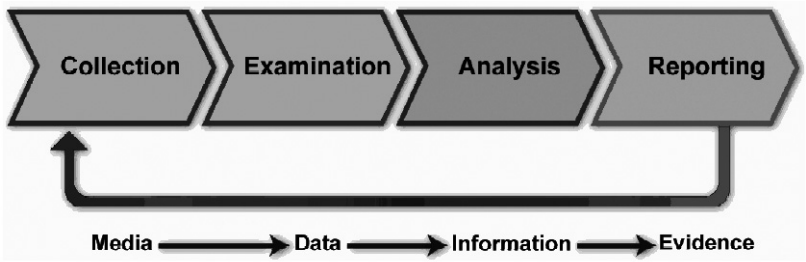
Digitalna forenzička nauka definiše se kao »*korišćenje naučno deriviranih i dokazanih metoda za sakupljanje, čuvanje, identifikaciju, analizu, interpretaciju, dokumentovanje i prezentaciju digitalnih dokaza deriviranih iz izvora digitalnih podataka, a namenjenih za lakšu rekonstrukciju događaja koji se smatraju krivičnim delom, ili neovlašćenim ometanjem planiranih operacija računarskih sistma i mreža*«, [28], [29].

Ova definicija pokriva široke aspekte digitalne forenzike od akvizicije podataka do legalnih akcija u pravosudnom postupku.

Proces digitalne forenzike na najvišem nivou apstrakcije uključuje *akviziciju* (sakupljanje) podataka iz nekog izvora - HD kompromitovanog računara, drugog medija, memorije i slika, *analizu* podataka i ekstrakciju dokaza, čuvanje dokaza u lancu istrage i *svedočenje* (veštačenje) dokaza pred sudom. U ovom poglavlju opisani su teorija i zahtevi za akviziciju i analizu digitalnih podataka i ekstrakciju dokaza iz prikupljenih podataka; opisana je priroda alata za digitalnu forenziku, date definicije i zahtevi. Postojeći digitalni forenzički alati daju rezultate koji se uspešno koriste pred sudom. Digitalna forenzička nauka obezbedila je forenzičke alate za relativno lagan i pouzdan pristup organa za digitalnu istragu osetljivim digitalnim podacima, ali tipično nedostaju metodi za verifikaciju korektnosti rada ovih alata, što je neophodno kada se digitalna forenzka posmatra sa naučnog aspekta.

Proces digitalne forenzike obuhvata sledeće 4 glavne faze (slika 1.1), [5], [22]:

- *Sakupljanje* (akvizicija): identifikacija, validacija, označavanje, snimanje i izvlačenje podataka iz mogućih izvora podataka, sledeći procedure koje štite integritet podataka.
- *Ispitivanje*: forenzičko procesiranje sakupljenih podataka korišćenjem kombinacije automatizovanih i manuelnih metoda i procena ekstrahovanih podataka od posebnog interesa, uz očuvanje integriteta podataka.
- *Analiza*: analiziranje rezultata ispitivanja, legalno opravdanim metodama i tehnikama, identifikovanje potencijalnih digitalnih dokaza, primenom naučno deriviranih i dokazanih metoda koje mogu koristiti za rekonstrukciju događaja u istrazi kompjuterskog kriminala.
- *Izveštavanje*: formiraju se čvrsti dokazi i priprema prezentacija dokaza pred sudom kroz ekspertsko svedočenje ili veštačenje. Izveštavanje rezultata analize, može uključiti opis primenjenih akcija, koji objašnjava kako su izabrani alati i procedure i određuje koje druge akcije treba da se izvrše, npr. forenzičko ispitivanje dodatnih izvora podataka, identifikovane ranjivosti, poboljšavanje postojećih kontrola zaštite, preporuke za poboljšavanje politika, procedura, alata i drugih aspekata procesa digitalne forenzike.



Slika 1.1 Proces digitalne forenzike

Generalno, digitalni dokazi koje istraga treba, nalaze se analizom i evaluacijom svih podataka sakupljenih u fazi akvizicije digitalnih podataka. Kao i u istrazi klasičnog kriminala, da bi otkrili istinu digitalni istražitelji moraju identifikovati podatke koji formiraju:

- *optužujuće dokaze*, verifikuju postojeće podatke i teorije (hipoteze),
- *oslobađajuće dokaze*, suprostavljaju se postojećim podacima i hipotezi, i
- indikatore pokušaja sakrivanja podataka.

Da bi se otkrili svi ovi tipovi dokaza, sakupljeni podaci moraju se analizirati i identifikovati potencijalni dokazi koji podržavaju postavljenu hipotezu, ili se suprostavljaju postavljenoj hipotezi, ili ukazuju na sakrivanje podataka.

U radu sa digitalnim podacima, u procesu akvizicije i analize, forenzičar se mora pridržavati *glavnih principa* za rad sa kompjuterskim digitalnim dokazima, koje su sa neznatnim varijacijama, propisale brojne međunarodne organizacije (IOCE, NIST, FBI), [24], [7], [27], [38]:

Princip 1: Ni jedna aktivnost agencije ili forenzičara ne sme izmeniti podatke koji se naleze u računaru ili medijumima za skladištenje i koji mogu biti potencijalni dokazi za sud.

Princip 2: U posebnim okolnostima kada organ istrage, forenzičar ili drugo lice mora pristupiti originalnim podacima, to lice mora biti kompetentno i mora dati dokaz koji objašnjava značaj i implikacije te aktivnost.

Princip 3: Treba kreirati i čuvati u celokupnom lancu istrage kontrolne tragove i druge zapise svih procesa izvršenih nad kompjuterskim elektronskim dokazima, da bi se obezbedila nezavisna forenzička analiza tih procesa sa istim rezultatima.

Princip 4: Lice nadležno za istragu slučaja kompjuterskog kriminala odgovorno je za obezbeđivanje sprovođenja svih aktivnosti forenzičke istrage, akvizicije, analize i prezentacije u skladu sa zakonskom regulativom i ovim proncipima.

Sa porastom kapaciteta sistema za skladištenje podataka, analiza svakog bita podataka praktično je „nemoguća misija“. Sakupljeni podaci su tipično serije *bajtova* podataka sa HD ili mrežnih uređaja. Ovakve sirove podatke teško je razumeti. U slučaju sistema sa više diskova, *RAID* ili *Volume Managament* tipa, sakupljeni podaci sa jednog diska ne mogu se analizirati sve dok se ne spoje sa podacima sa drugih diskova korišćenjem kompleksnih algoritama. *Problem kompleksnosti* u digitalnoj forenzici potiče i otuda što su sakupljeni podaci tipično u najnižem i najsirovijem formatu, koji je često težak za ljudsko razumevanje. Iako ih nije nemoguće interpretirati, zahtevaju visok stepen znanja i veština što se ne može tražiti od tipičnih istražitelja digitalnih podataka.

Problem kompleksnosti se rešava upotrebom alata za prevođenje podataka kroz jedan ili više slojeva apstrakcije sve dok ne budu razumljivi za ljudsku interpretaciju. Na primer, za gledanje sadržaja direktorijuma iz *imidža* (fizičke slike) fajl sistema, struktura fajl sistema mora biti procesirana tako da se na displeju prikaže odgovarajuća struktura podataka. Podaci koji predstavljaju sadržaj direktorijuma postoje u imidžu fajl sistema uzetom u fazi akvizicije podataka, ali u suviše niskom formati za identifikaciju. Direktorijum je sloj apstrakcije u fajl sistemu. Primeri drugih slojeva apstrakcije su:

- ASCII[19],
- HTML[20] fajl,
- Windows Registry,
- alarm IDS (Intrusion Detection System) i
- izvorni kôd.

Namena alata za digitalnu forenzičku analizu je da tačno predstavi sve podatke na sloju apstrakcije i u formatu koje forenzičar može efektivno koristiti za identifikaciju dokaza. Zahtevani sloj apstrakcije zavisi od veštine forenzičara i zahteva istrage. Na primer, u nekim slučajevima posmatranje sadržaja bloka sirovih podataka sa HD je adekvatno, dok se u drugim slučajevima zahteva procesiranje bloka sa HD kao strukture fajl sistema. Moraju postojati alati koji obezbeđuju obe opcije.

Glavne kategorije procesa digitalne forenzičke analize mogu se definisati i korišćenjem koncepta apstrakcionih slojeva, za razliku od ranijih definicija koje su zavisile od stručnosti i znanja forenzičara, [3]. Koncept apstrakcionih slojeva koristi se za definisanje zahteva za alate za digitalnu forenzičku analizu. U odnosu na slojeve apstrakcije računarskog sistema i pripadajuće digitalne podatake proizvedeni su alati za analizu tih podataka sa različitim stepenom definisanosti, slabije opisanim svojstvima i tipovima grešaka koje apstrakcioni slojevi proizvode kada se koriste sa forenzičkim alatima. Koncept digitalnih forenzičkih alata za apstrakcione slojeve računarskog sistema odgovara svim tipovima digitalne forenzičke analize, uključujući i podelu na analizu *medija, programskog kôda i računarske mreže*.

19 American Standard Code for Information Interchange

20 *Hipertext Markup Language*, jezik za izradui formatiranje HTTP stranice

REZIME

Digitalna forenzička nauka (*digitalna forenzika)* uključuje sakupljanje, čuvanje, dokazivanje i ekspertsko svedočenje/veštačenje digitalnih dokaza pred sudom, u slučajevima upravljanja kompjuterskim incidentom, kompjuterskog kriminala, civilne parnice, ili administrativnih zahteva. Digitalna forenzička nauka pokriva široke aspekte digitalne forenzike od akvizicije podataka do legalnih akcija u pravosudnom postupku. Najveći deo digitalne forenzike odnosi se na forenziku računarskih sistema, ili *kompjutersku forenziku*.

Za razliku od procesa *oporavka* slučajno izgubljenih ili izbrisanih *podataka,* digitalna forenzika računarskog sistema oporavlja podatke koje je korisnik namerno sakrio ili izbrisao, sa ciljem da obezbedi validnost podataka za dokaze pred sudom. Dobra je praksa da u slučaju bezbednosnog kompjuterskog incidenta digitalni forenzičar timski radi sa administratorom sistema/mreže, specijalistom za zaštitu i iskusnim istražiteljom klasičnog kriminala.

Kao i u istrazi klasičnog kriminala, da bi otkrili istinu organi istrage moraju identifikovati podatke koji formiraju *optužujuće dokaze, oslobađajuće dokaze* ili *indikatore pokušaja sakrivanja podataka*. Za upravljanje digitalnim dokazima u celom lancu istrage uspostavljena su 4 osnovna principa (FBI, NIST, IOCE) kojih se digitalni forenzičari i istražitelji moraju pridržavati.

Analiza prikupljenih podataka sa porastom kapaciteta HD i pojavom RAID diskova, postala je suviše kompleksna i praktično „nemoguća misija". Problem kompleksnosti u digitalnoj forenzici potiču i otuda što su sakupljeni podaci tipično u najnižem, sirovom formatu, teškom za razumevanje, pa zahtevaju upotrebu alata za prevođenje podataka kroz jedan ili više slojeva apstrakcije sve dok ne budu razumljivi za ljudsku interpretaciju.

Glavne kategorije digitalne forenzičke analize mogu se definisati i korišćenjem koncepta apstrakcionih slojeva, za razliku od ranijih definicija koje su zavisile samo od stručnosti i znanja forenzičara. Koncept apstrakcionih slojeva koristi se za definisanje zahteva za alate za digitalnu forenzičku analizu. Koncept digitalnih forenzičkih alata za apstrakcione slojeve računarskog sistema odgovara svim tipovima digitalne forenzičke analize, uključujući i podelu na analizu *medija, programskog kôda i računarske mreže*.

Digitalni forenzički alati sa otvorenim izvornim kodom (Linux tipa) postali su najčešće korišćeni softverski alat za akviziciju i forenzičku analizu digitalnih dokaza, zato što obezbeđuju analitičarima: veću kontrolu u radu sa digitalnim dokazima nego alati sa zatvorenim izvornim kodom; testiranje i verifikaciju onoga što sami alati rade; precizniji alat za forenzičku analizu digitalnih dokaza; lakše otkrivanje skrivenih podataka i bolji alat za dokazivanje pouzdanosti naučnog dokaza kvaliteta forenzičkih alata.

Međutim, forenzički alati sa zatvorenim programskim kodom postaju na isti način prihvatljivi u brojnim pravosudnim sistemima, ako su naučno potvrđeni i testirani, ako im je poznat nivo grešaka i ako se testovi mogu ponoviti i dati iste rezultate na zahtev suda.

PITANJA ZA PONAVLJANJE

1. Kada su razvijeni prvi alati za istragu i ispitivanje digitalnih podataka?
2. Koje su osnovne kategorije podele forenzičkih alata?
3. Kako se definiše digitalna forenzička nauka?
4. Koje su osnovne faze procesa digitalne forenzike?
5. Koje podatke moraju ortkriti digitalni istražitelji pred sudom?
6. Definišite glavne principe za rad sa kompjuterskim digitalnim dokazima.
7. Koja su dva glavna faktora kompleksnosti istrage digitalnih dokaza?
8. Koji se koncept koristi za definisanje glavnih kategorija procesa digitalne forenzike i alata za digitalnu forenzičku akviziciju i analizu?

2. FORENZIČKA AKVIZICIJA DIGITALNIH PODATAKA

2.1 FUNKCIONALNI MODEL FORENZIČKE AKVIZICIJE DIGITALNIH PODATAKA

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, u procesu klasične (*posmortem*) digitalne forenzičke akvizicije potrebno je uzeti fiziču kopiju (imidž) svakog ispitivanog medija (HD, CD, FD, fleš memorija) i imidž memorisati na poverljiv, forenzički sterilan disk. Ako je moguće treba snimiti sve locirane i nealocirane podatke sa kompromitovanog računara.

Funkcionalni model digitalne forenzičke akvizicije tipično koristi koncept sledećih apstrakcionih slojeva, [27]:

- određivanje slojeva ulaza i izlaza (I/O),
- pripisivanja operacija čitanja i upisivanja za pripadajuće forenzičke alate i
- vremensko pečaćenje operacija čitanja i upisivanja.

Korišćeni apstrakcioni slojevi u ovom modelu su: aplikacioni programi (I/O slojevi), fajl sistem, upravljanje medijima, fizički mediji i sloj umrežavnja. Operacije čitanja i upisivanja obuhvataju različite apstrakcione slojeve, a testiranje modela uključuje kompleksne forenzičke operacije sa primenom **DD** alata komandne linije za uzimanje fizičkog imidža diska, slanje izlaznog imidža preko mreže sa **Netcat** alatom na forenzički server, zatim izvlačenje imidža na drugi forenzički računar za analizu. Vremena upisivanja i čitanja mogu da se registruju na različitim mestima. Primena modela može biti korisna za ponovljivost procesa forenzičke istrage i dokazivanje čuvanja integriteta podataka.

2.1.1 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 bilo kog programa izaziva upisivanje informacija u fizičku memoriju, a fizička memorija koju već zauzima neki proces u radu može isprazniti svoj sadržaj u *page* ili *swap* fajl. Kada forenzičar sakupi informacije i pošalje ih izvan sistema kroz forenzički sigurne komunikacione kanale u fornzički server, kreira se nova mrežna konekcija.

Sve ove promene mogu se zajedno objasniti Lokardovim[21], principom razmene materije**:** *kada dva objekta dođu u kontakt između njih se razmenjuje ili prenosi materija,* [5]. Fizički primer Lokardovog principa je, 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, inforamacije se razmenjuju između njih. Informacija o jednom računarau pojaviće se u memoriji procesa i/ili log fajlovima, registrima itd., u drugom računaru, ili kada se prenosni USB disk priključi na Windows računarski sistem, rezidenta informacija o uređaju ostaje u računaru. Kada forenzičar pristupi računaru u radu, događaju se promene u sistemu kako se izvršava forenzički program i podaci kopiraju sa sistema. Ove promene mogu biti *prelezne* – memorija procesa, mrežne konekcije, ili *trajne* – log fajlovi, ulazi Registra, keš fajlovi (Internet istorija). Za demosntraciju Lokardovog principa razmene materije može se iskoristiti jednostavan mrežni 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 aktivni sistem. Na primer, neki forenzički alat treba da čita nekoliko ključeva registra u Windows XP OS. Putanja do ovih ključeva se upisuje u RAM memoriju. Kako Windows XP OS izvršava *prefetching* aplikaciju, uzimanje podataka iz memorije i skladištenje u registar procesora pre njihovog korišćenja, kada forenzičar aktivira program kojeg je korisnik već aktivirao na sistemu, biće modifikovano vreme poslednjeg pristupa korisnika *prefatch* fajlu, kao i sadržaj samog *prefatch* fajla. Ako program kojeg forenzičar pokrene nije ranije korišćen, biće kreiran novi *prefatch* fajl u *prefatch* direktorijumu, pod pretpostavkom da *prefatch* direktorijum nije dostigao svoj 128. po redu **.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, ako to sud zahteva. Na primer, forenzičar treba da utvrdi koji su **.pf** fajlovi u XP *prefeach* direktorijumu rezultat njegovih aktivnosti, a koji aktivnosti korisnika. Isto važi i za vrednosti upisane u Registre. Akcija forenzičara ažurira vreme poslednjeg upisa entrija (ulaza) u ključevima Registara. Neke od ovih promena nisu rezultat akcije forenzičkih alata, nego ih pravi Windows Explorer, jednostavno zbog činjenice da je sistem aktivan. Testiranjem i razumevanjem funkcionalnosti forenzičkih alata, forenzičar može dokumentovati i objasniti koji su artefakti na sistemu rezultat akcija forenzičara, a koji su rezultat akcija korisnika ili napadača, [6].

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 brisanja iz RAM memorije. Ovo znači da forenzičar treba da sakuplja neke nestabilne informacije pre drugih nestabilnih informacija. Generalno, forenzičar može sa sistema u radu

21 Dr. Edmond Locard, početkom 20. stoleća

sakupiti značajne informacije, vodeći detaljne zabeleške o svakoj akciji, svakoj razlici između UTC (*Universal Time Control*), lokalnog i sistemskog vremena i tako minimizirati uticaj promena datuma na konkretni slučaj i nekoliko godina kasnije, ako to zahtevaju pravosudni organi, [5].

2.1.2 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 aktivnog računara, pošto postoje brojni slučajevi gde se nestabilne informacije uopšte ne zahtevaju i ne razmatraju. Razlozi za forenzičko ispitivanje aktivnog računara više zavise od specifičnosti okruženja (politike, regulativa i zakona) i prirode smog slučaja, a najčešće sam forenzičar treba da donese tu odluku. Na primer, administrator mreže zapazi neobičan saobraćaj u mreži, kojeg alarmira IDS/IPS sistem, a proverom log fajla *firewall*-a utvrđen je vremenski sinhronizam koji dokazuje da je napad došao iz mreže, što potvrđuje i MAC[22] adresa, ali je potrebno ovom saobraćaju pridružiti proces, ili korisnika. U tom slučaju forenzičar treba da izvrši ispitivanje aktivnog sistema, da definitivno utvrdi izvor sumnjivog saobraćaja i koji ga proces generiše, da sakupi inforamcije o aktivnim procesima i mrežnim konekcijama, pre isključivanja sistema. Druge informacije sakupljene u ovom ispitivanju mogu pokazati da je neko logovan u sistem daljinskim pristupom preko više mrežnih logovanja, ili kroz zadnja vrata (*back door*), ili je aktivni proces pokrenut kao planirani zadatak (*Scheduled Task*). Takođe, ovo ispitivanje je nezamenljivo za utvrđivanje 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, [5]:

- sistemsko vreme,
- logovani korisnici,
- otvoreni fajlovi,
- mrežne informacije,
- mrežne konekcije,
- informacije o aktivnim procesima,
- mapiranje procesa i portova,
- memorija procesa,
- status mreže,

22 *Media Access Control* (MAC) – mašinska kontrolna adresa mrežnih uređaja

- sadržaj Clipboard-a,
- informacije o servisu/drajveru,
- istorija komandi,
- mapirani drajvovi,
- deljeni fajlovi/direktorijumi.

2.2 AKTIVNA FORENZIČKA AKVIZICIJA

Postoje brojna pitanja sa kojim se forenzičari suočavaju kada isključe osumnjičeni računarski sistem/e i sakupljaju *imidže* sa čvrstih diskova za ispitivanje, od kojih su najznačajniji gubici zbog prekida e-transakcija savremenih poslovnih IKT sistema, 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 vremenskog prozora za održavanje). Za uzimanje imidža savremenih čvrstih diskova velikog kapaciteta, na primer, 750GB u RAID[23] 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 tip dokaza treba tražiti. Takođe, brojni maliciozni programi za krađu personalnih informacija – lozinki, ličnih fajlova i drugih ličnih podataka, ne budu upisani na čvrsti disk nego ostaju samo u prmarnoj RAM memoriji, što znači kada se sistem isključi sve ove informacije nestaju, [5].

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

23 RAID - Redundant Area of Inexpensive Discs

2.2.1 Razvoj aktivne forenzičke akvizicije

Tehnologija je evoluirala na takav način da je aktivna digitalne forenzička akvizicija stvarno jedina opcija na raspolaganju pod određenim okolnostima. U prošlosti, računarske mreže su bile jednostavnije. Savremene računarske mreže su visoko distribuirane na više lokacija, što otežava posao administratorima sistema, mreža i zaštite IKT sistema. Mnoge organizacije imaju više računara na jednoj lokaciji, a nekoliko lokacija u gradu, zemlji ili na kontinentu. Takođe, upravljanje IKT resursima na web sajtu i web servisima može biti veoma težak zadatak. U klasičnoj digitalnoj forenzičkoj istrazi problem bi mogao nastati ako bi se isključivali računari sa mreže da bi se sprovela forenzička istraga svake sumnjive žalbe, bezbednosnog događaja ili kompromitovanog hosta, zbog uticaja na operacije računarskih resursa i web servise. Trijaža incidenata je veoma česta praksa kada se dijagnostifikuju problemi u mreži. To je prva reakcija, i ne pretpostavlja se odmah da je izvršen napad ili da je sistem ugrožen. U okruženju aktivne forenzičke akvizicije, korporacijski forenzičar bi mogao da se uloguje sa daljine, da vidi tekuće procese, sadržaj fizičke memorije i donese odluku da li da se uzima imidž[24] udaljenim pristupom ili da se računar fizički odstrani sa mreže radi daljeg forenzičkog ispitivanja. Metodologija aktivne forenzičke akvizicije omogućava održavanje-čuvanje operativne gotovosti svih mrežnih resursa.

Značajan razlog za razvoj aktivne forenzičke akvizicije je brzi razvoj sekundarnih (online) medijuma za skladištenja – HD. Na primer, neka je kompromitovan server intranet mreže organizacije, koji radi 24 časa, a ima HD kapaciteta 630 TB. (terabajta). Snimanje fizičke slike (imidža) ovog HD na forenzički HD manjeg kapaciteta , čak i sa kompresijom podataka trajalo bi veoma dugo i ne bi rešilo problem. Kompresija povećava vreme koje je potrebno za imidžovanje HD servera, jer algoritam kompresije zahteva vreme da ispita i ukloni suvišne detalje pre kompresije. Međutim, i dalje bi bilo nemoguće da se komprimuje veći HD na manji, recimo, USB eksterni disk. Ako bi se klasična akvizicija ovog HD vršila na forenzički HD iste veličine ostaje problem vremena potrebnog za akviziciju. Na primer, neka se koristi ICS Image MASSter Solo-3 IT alat za imidžovanje, koji može da duplira HD brzinom od 3 GB u minuti. Za uzimanje imidža HD od 630TB, očigledno bi bilo nepraktično, zbog potrebnog vremena:

630TB = 630 x 1TB=630x1,099,511,627,776 B = 6,926,923,254,988,880 B

Vreme potrebno za akviziciju – Ta je:

Ta= 630 TB/3GB= 6926923254988880B/3221225472B =
2150400 minuta=35840sati= 1493dana=preko 4 godine

24 *Image* (imidž) - fizička slika bit po bit

U gornjem primeru su primenjene tačne veličine konverzije bajta (B) u bite (b), gde je 1B=8b, prikazane u tabeli 2.1.

Tabela 2.1 Karta konverzije bajta – B (Byte)

Veličina drajva - Numerički prikaz
1 kB 1,024 b (bita)
1 MB 1,048,576 b
1 GB 1,073,741,824 b
1 TB 1,099,511,627,776 b
1 PB (petabajt)1,125,899,906,842,624 b
1 EB (exabyte) 1,152,921,504,606,840,000 b

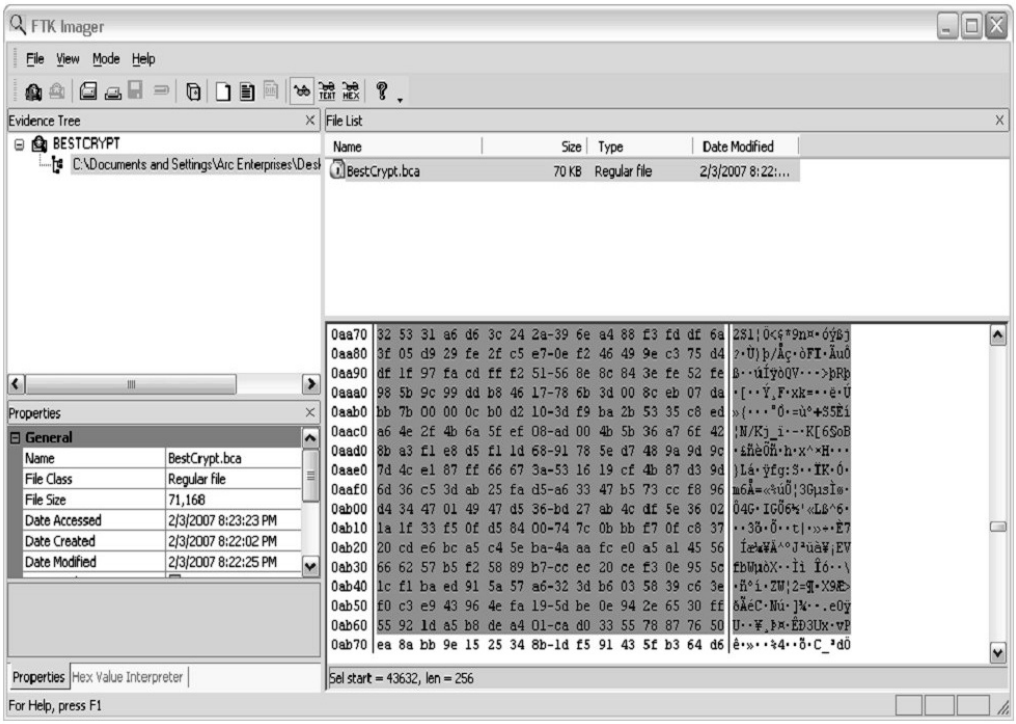
Kako se vidi iz prethodnog primera, imidžovanje celog HD ove i slične veličine jedan-na-jedan, apsolutno nije praktično. Čak i da se akvizicija izvrši dodatnim resursima, analiza ove količine digitalnih podataka bila bi preterano obimna i praktično neprihvatljiva. Razlika u sprovođenju analize tako velikog obima podataka, može se uporediti sa ispitivanjem svake osobe koja živi u gradu gde se desio kasičan zločin, umesto ispitivanja svake osobe u bloku gde se zločin desio.

Na kraju, isključivanje servera iz ovog primera, takođe, nije moguća opcija jer bi očigledna posledica bila velika ekonomska šteta za datu organizaciju. Mnogi IKT sistemi izvršavaju kritične poslovne zadatke, npr. zdravstveni IKT sistemi, sistemi za podršku transporta itd., i ne mogu biti isključeni bez štetnih posledica za poslovne procese.

Korišćenje šifrovanja fajlova je poraslo tokom poslednjih nekoliko godina. Kada se izvrši šifrovanje *objekta podataka*[25] sadržaj tog objekta je za forenzičara nečitljiv. Šifrovanje se primenjuje da sakrije, a nekada i komprimuje sadržaj objekta podataka. Šifrovanje se primenjuje na objekte podataka na jedan od sledećih načina:

1. Šifrovanje na nivou fajla, u kojem su šifrovani pojedinačni fajlovi. Na slici 2.1 je prikazan sadržaj šifrovanog fajla u forenzičkom alati **FTK,** [39].

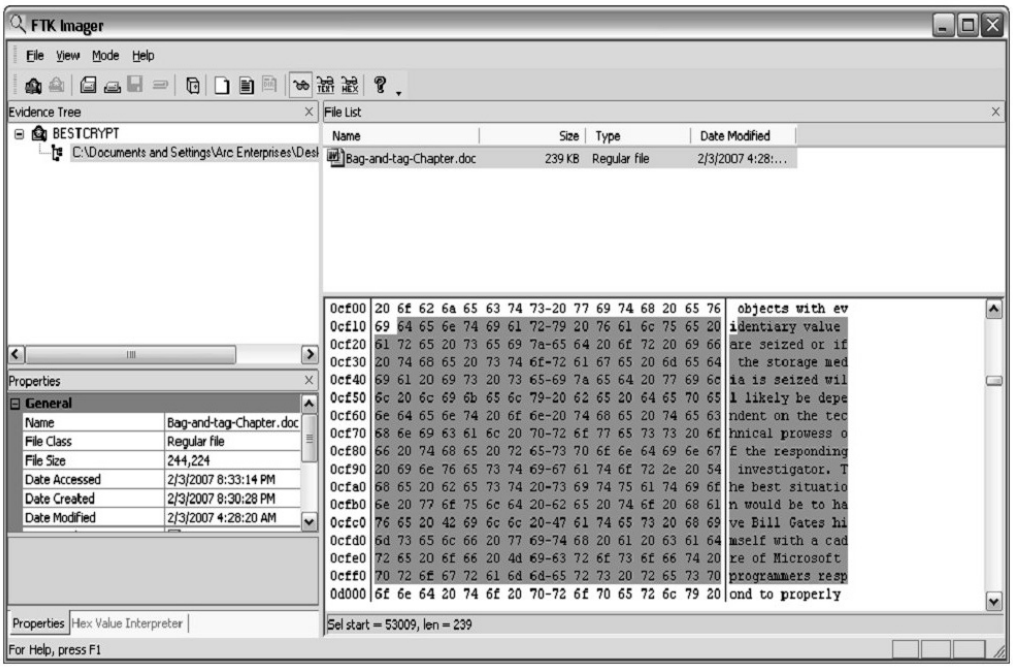
25 **Objekti podataka** - objekti ili informacije koje su pridružene fizičkim predmetima i koji imaju potencijalnu dokaznu vrednost. Objekti podataka se mogu pojaviti u raznim formatima, ali se ne sme menjati orginalna informacija.



Slika 2.1 Sadržaj šifrovanog fajla u AccessData FTK Imager alatu

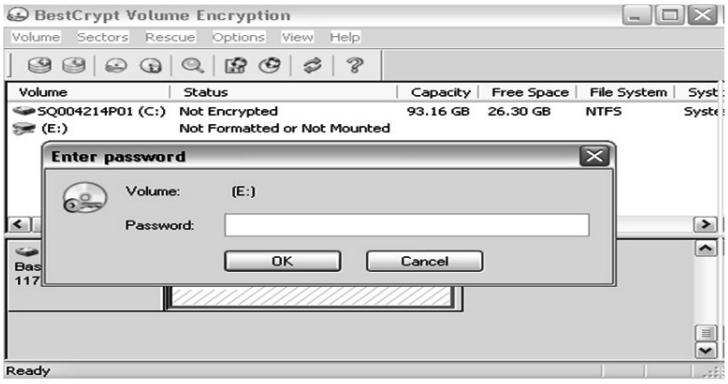
Da bi forenzički istražitelj sproveo klasičnu analizu (*postmortem analizu*[26]), on mora prvo dešifrovati fajl. Na slici 2.2 prikazan je dešifrovan fajl. Ako istražitelj nema pristup lozinki šifrovanog fajla, ovo bi moglo biti jako teško i vremenski zahtevno. U slučaju da se nema lozinke može se koristiti program za krekovanje. Ako je lozinka prevelika ili je fajl šifrovan jakim šifarskim algoritmom ovaj proces dešifrovanja bi mogao bit neuspešan, pa bi preostala samo neka od kriptoanalitičkih metoda (npr. brutalna sila).

26 Analiza isključenog računarskog sistema



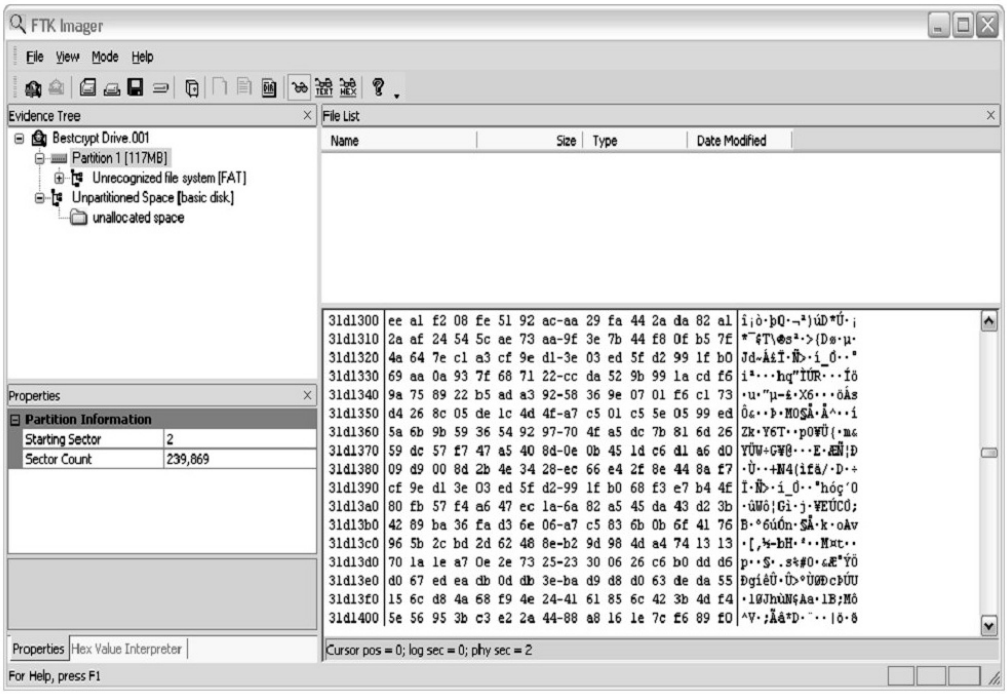
Slika 2.2 Sadržaj dešifrovanog fajla u AccessData FTK Imager alatu

2. Podaci se šifruju na nivou nosioca podataka (volumena, particije). U sledećem primeru (slika 2.3), nosilac podataka je šifrovan unutar čvrstog diska (HD).



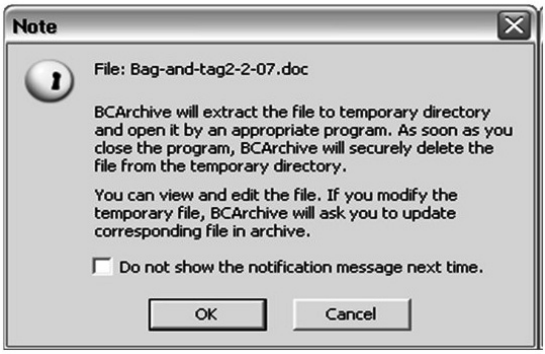
Slika 2.3 Particija E šifrovana sa BestCrypt alatom

3. Šifrovan je ceo HD. Na slici 2.4 prikazan je šifrovan ceo čvrsti disk u forenzičkom alatu **FTK**. Očigledno, ceo sadržaj diska je nečitak i ima malu vrednost za forenzičkog islednika.



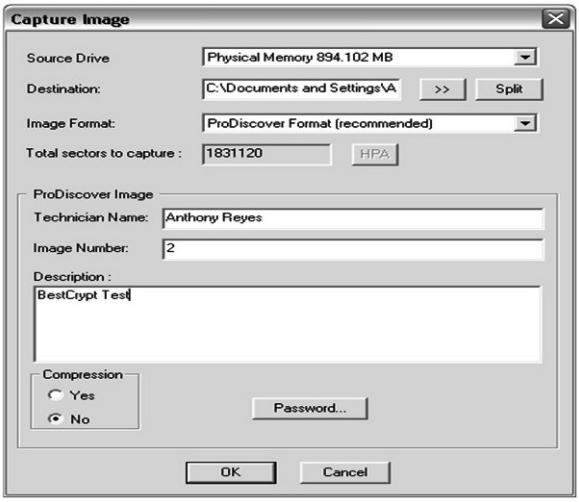
Slika 2.4 Forenzička slika šifrovanog HD u AccessData FTK Imager alatu

Kada sprovode klasičnu (*postmortem*) forenzičku akviziciju/analizu prema prve dve metode šifrovanja, forenzičari se često nadaju da će možda naći artefakte (ostatke) šifrovanih fajlova u otvorenom tekstu u nealociranom prostoru HD. Ove artefakte fajl sistem se nekada kreira nakon jednog otvaranja dokumenta, ili kada se isključi napajanje tokom prikazivanja fajla na ekranu monitora. Program *BestCrypt* omogućava otvaranje šifrovanog fajla u privremeni folder, a onda sigurno briše fajl kada se program zatvori (slika 2.5).



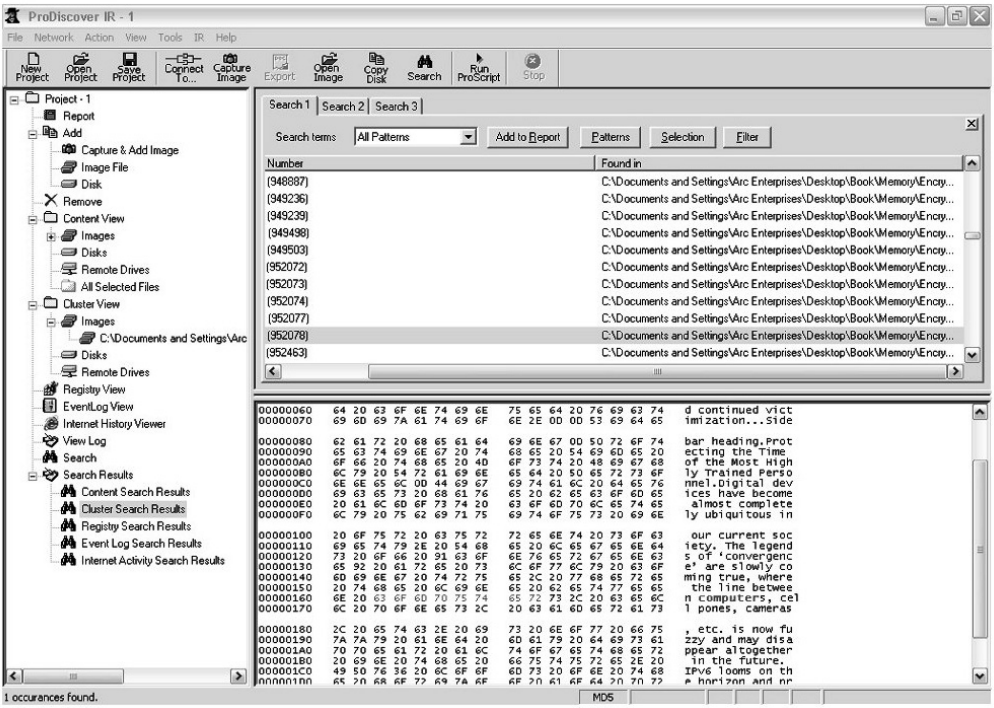
Slika 2.5 Operacija čišćenja fajlova pomoću BestCrypt alata

Kada se primenjuje aktivna forenzička akvizicija, šanse da se vidi sadržaj šifrovanog fajla su znatno veće. Kada je dokument u otvorenom tekstu otvoren i pripremljen za šifrovanje, biće učitan u fizičku primarnu memoriju (RAM). U aktivnom forenzičkom okruženju, islednik može uzeti imidž fizičke memorije računarskog sistema i skupiti korisne informacije (delove ili ceo otvoreni tekst) za dešifrovanje šifrovanog fajla. Sadržaj fizičke RAM memorije treba ispitati pre isključivanja napajanja. Slika 2.6 prikazuje jedan primer kako se može uzeti imidž fizičke memorije korišćenjem mrežnog forenzičkog alata **ProDiscover IR,** [42].



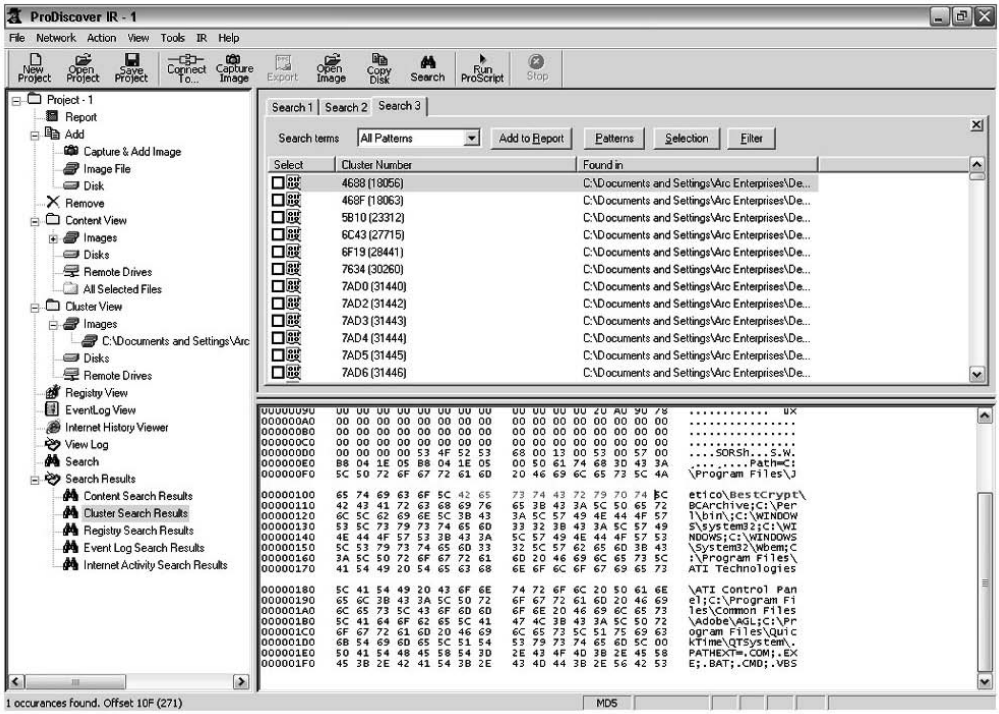
Slika 2.6 Prozor uzimanja imidža u ProDiscover IR forenzičkom alatu

Sa uzetog imidža RAM memorije, može se pregledati sadržaj. Na slici 2.7 se vidi otvoreni tekst sadržaja šifrovanog fajla, prikazan u heksadecimalnom i čitljivom ASCII formatu u forenzičkom alatu **ProDiscover IR**. Rekonstrukcija ove originalne informacije bila je moguća, jer je fajl dešifrovan od strane korisnika koji je trenutno (u toku akvizicije) radio na dokumentu.



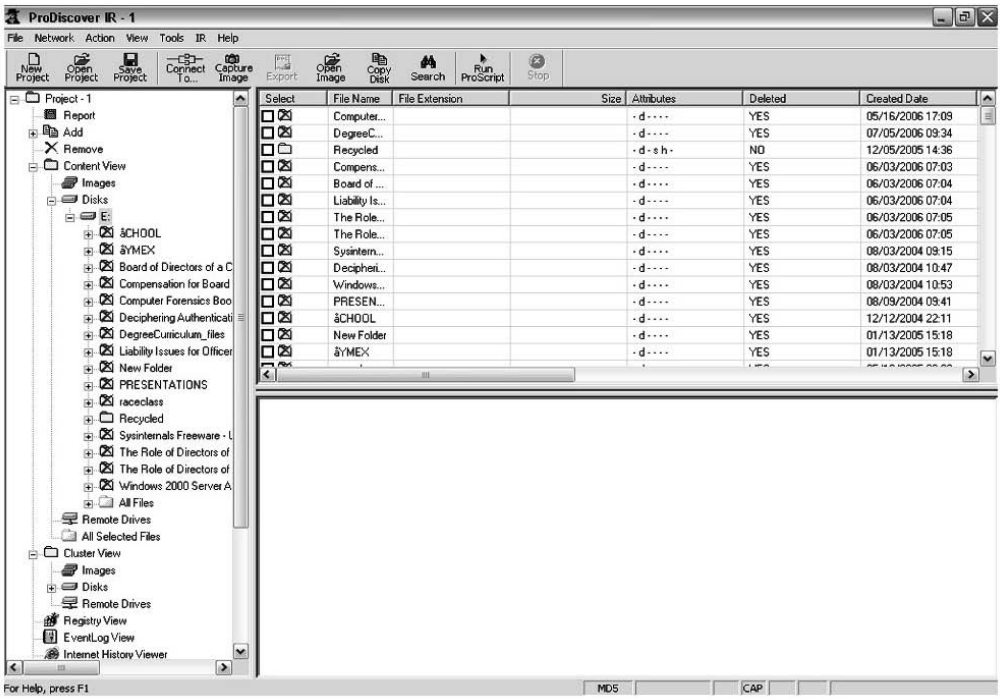
Slika 2.7 Dešifrovani dokument u RAM memoriji u ProDiscover IR alatu

Na slici 2.8 se može videti da je **BestCrypt p**rogram aktivan u fizičkoj memoriji. Vidi se na donjem desnom panelu.



Slika 2.8 Pogled na sadržaj fizičke memorije u ProDiscover IR alatu koji indicira da je BestCrypt proces aktivan

Takođe, u slučaju šifrovanja celog HD, forenzički istraživač bi mogao da vidi sadržaj diska koristeći tehnologiju za aktivnu forenzičku akviziciju. Naime, zbog toga što je HD trenutno korišćen (aktivan) u toku akvizicije, on je normalno dešifrovan. Na slici 2.9 prikazana je mogućnost da se u alatu **ProDiscover IR** vidi dešifrovan sadržaj ispitivanog HD.



Slika 2.9 Dešifrovani sadržaj HD u toku aktivne akvizicije sa forenzičkim alatom ProDiscover IR

Kao što se vidi iz prethodnih primera u digitalnoj forenzičkoj istrazi savremenih poslovnih IKT sistema, šifrovanje i drugi razlozi predstavljaju brojne problema za tradicionalnu forenzičku istragu. Svi ovi primeri ukazuju da je aktivna digitalna forenzička akvizicija neophodna opcija i da se sa tehnikama aktivne istrage mogu prevazići ovi problemi i prepreke.

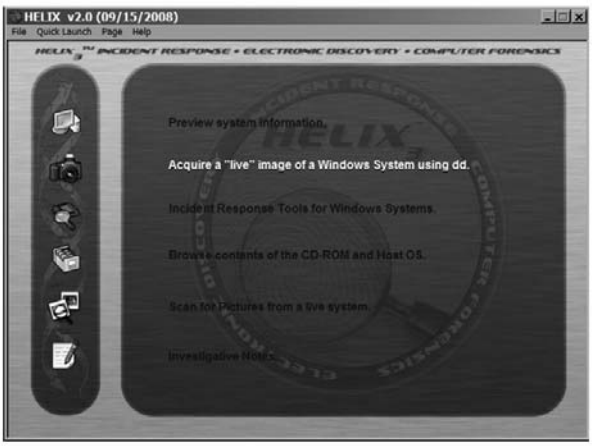
2.2.2 Metodi aktivne digitalne forenzičke akvizicije

Generalno, metodi aktivne digitalne forenzičke akvizicije mogu se klasifikovati u odnosu na različite kriterijume. Uobičajeni kriterijumi klasifikacije aktivne forenzičke akvizicije su u odnosu na:

- tehnike i alati za povezivanja forenzičkog računara na ispitivani računarski sistem i
- metode pristupa forenzičara ispitivanom računaru.

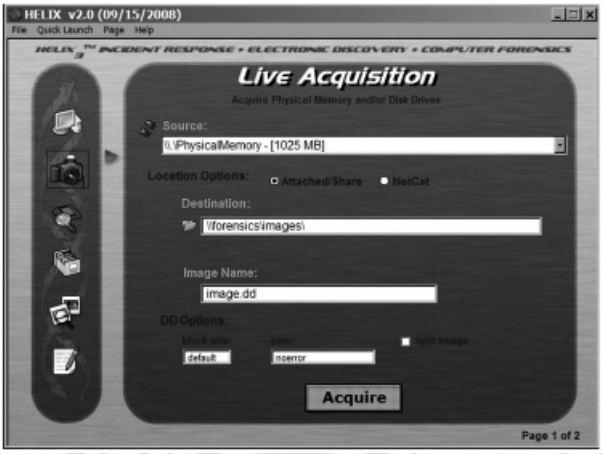
U odnosu na tehnike i alate za povezivanja forenzičkog računara na ispitivani računarski sistem, u svetu postoje brojne kompanija koje proizvode forenzičke softvere za odgovor na incidente, aktivnu mrežnu akviziciju i forenzičku istragu, od koji su poznatije: *Guidance Software, Technologies Pathways, Wetstone Technologies, ASR Data, E-fense i E-Trust by CA*. Na bazi ovih softvera proizvođači su razvili brojne modele tehnika i alata za povezivanje forenzičkog računara na ispitivani sistem u procesu aktivne forenzičke istrage, koji se generalno mogu grupisati u tri kategorije:

- *Pre-Deployed Agent model* je prvi primenjen metod, gde se specijalni softver instalira pre incidenta i potrebe za forenzičkim ispitivanjem, obično je sakriven od krajnjeg korisnika i aktivira se kada se uspostavi forenzički udaljeni pristup.
- *Direct Connect model,* koji se trenutno najviše koristi, je drugi metod gde je ciljni računar za aktivnu akviziciju direktno povezan sa udaljenom forenzičkom mašinom, a softver je ubačen u RAM memoriju. Veza ostaje aktivna sve dok se udaljena forenzička mašina ne isključi.
- *Treći metod* je *On Demand Connection model* gde se kompjuter povezuje sa ciljnom forenzičkom mašinom, a softver ubacuje u memoriju za specifični forenzički zadatak. Kada je zadatak akvizicije preko udaljene mašine završen, veza se trenutno raskida.
- Neki softveri koriste butabilni forenzički disk sa setom alata za akviziciju i analizu (npr. **Helix** firme *E-fense*). Tokom aktivne akvizicije, disk se učitava na aktivnu ispitivanu mašinu, a kompletom forenzičkih alata za ispitivanje inicira se virtuelna sesija za akviziciju podataka na forenzičku mašinu. Na slici 2.10 prikazan je butabilni CD-ROM disk sa setom **Helix** alata koji omogućava da se izvrši aktivna forenzika akvizicija i istraga.



Slika 2.10 Helix forenzički alat za upravljanje incidentom, oporavak podataka i forenzičko podizanje ispitivanog sistema

Na slici 2.11 prikazan je prozor za uzimanje imidža aktivnom forenzičkom akvizicijom pomoću seta forenzičkih alata **Helix**.



Slika 2.11 Aktivna akvizicija pomoću forenzičkog alata Helix

Klasifikacija u odnosu na *kriterijum pristupa* u forenzičkoj praksi aktivne akvizicije, zavisi od brojnih faktora. Naime, koji će od navedenih modela povezivanja na ispitivani računar forenzičar primeniti u forenzičkoj praksi, zavisi od više faktora, od kojih se neki ne mogu kontrolisati. Najbolji pristup je imati potpuno razumevanje o tome šta je forenzičaru dostupno u konkretnom slučaju i okruženju i šta može uključiti u set forenzičkih alata, pa na bazi toga doneti odluku o tome kako raditi. U odnosu na kriterijum *pristupa* ispitivanom računaru, razlikuju se tri bazična aplikativna metoda aktivne akvizicije računara sa Windows platformom, [5]:

- lokalna aktivna akvizicija,
- aktivna akvizicija udaljenim pristupom i
- hibridna aktivna akvizicija.

Metod lokalne akvizicije aktivnog računara podrazumeva da forenzičar sedi za tastaturom ispitivanog sistema u radu, unosi komande i skladišti informacije lokalno, direktno na forenzički čvrsti ili prenosni disk (unutrašnji/spoljni HD ili USB), ili ih šalje zaštićenim kanalima na zajednički mrežni lokalni forenzički server. 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 uskladištenim na optičkim diskovima (CD, DVD) i sa pravim nivoom pristupa, forenzičar može brzo i efikasno sakupiti potrebne informacije. Najjednostavniji način da se implementira metodologija lokalne aktivne akvizicije je sa krei-

ranjem *bach* fajla i nekog skripta, na primer, *Perl* skripta koji se upiše samo jedanput i sa ovom komandom pokreće se alat automatski. Primer jednostavnog *bach* fajla koji se može koristiti u toku forenzičke akvizicije aktivnog 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

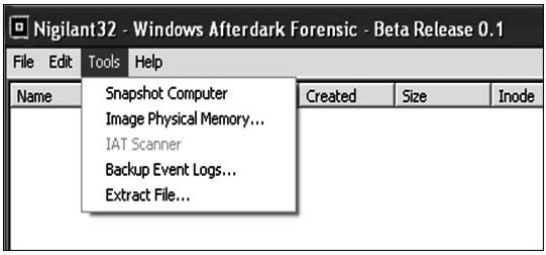
netstat.exe –ano > %1\netstat-ano.log

Ovde su data tri korisnička alata (**tlist, openports, netstat**) i pet skriptova komandi. Ovi fajlovi se memorišu kao **local.bat** i uključe se na CD/DVD sa forenzičkim alatima. Na CD/DVD treba dodati sigurne kopije komande procesora (**cmd.exe**) za svaki OS. Pre aktiviranja *batch* fajla, treba pogledati u sistem i videti koji su mrežni diskovi (drajvovi) raspoloživi, ili ubaciti USB memoriju u sistem i videti koje se slovo diska dobija (npr., G:\), zatim aktivirati *bach* fajl (ako je CD-ROM/DVD 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 nekiliko raspoloživih forenzičkih alata dizajniranih za aktivnu lokalnu akviziciju podataka sa računara u radu, 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 izlazima, osnovne funkcionalnosti oba alata su u suštini jednake: 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 format izveštaja.

Drugi pristup za razvoj metodologije aktivne lokalne forenzičke akvizicije računarskog sistema je da se enkapsulira što je moguće više funkcija u jednu aplikaciju koja koristi Windows API, kao što je alat **Nigilant32** (*Agile Risk Management LLC*). **Nigilant32** koristi isti Windows API poziv kojeg koriste spoljni alati za sakupljanje nestabilnih informacija sa sistema, (slika 2.12). Alat ima mogućnost da izvrši proveru fajl sistema i isprazni sadržaj fizičke memorije, (RAM).



Slika 2.12 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**.

Metod akvizicije udaljenim pristupom generalno se sastoji od serije komandi koje se izvršavaju na kompromitovanom sistemu slanjem instrukcija kroz mrežu. Ovaj metod je koristan za akviziciju podataka sa više računarskih sistema, pošto se proces logovanja u sistem i komande mogu lako automatizovati. Neki alati rade odlično u kombinaciji sa **psexec*.exe*** (*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 identifikacioni podaci za logovanje u svaki sistem i da svaki put kada se uloguje, aktivira komande, sakuplja podatke i šalje ih u forenzički računar, ostavlja tragove u log fajlu bezbednosno relevantnih događaja (*Security Event Log*) korumpiranog računara.

Ovo znači da se redosled sakupljanja nestabilnih podataka mora neznatno pomeriti 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 adresu sistema i korisničko ime/lozinka 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[27] 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 *Perl64*. 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 primer, 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 sakupljanje informacija udaljenim pristupom, korisno je pogledati fajl *wmic.exe*. Ovaj fajl sadrži primere sakupljanja liste instaliranih zakrpa sa udaljenog sistema, [40]. Cela kla-

27 Uniform Naming Convention

sa fajlova 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[28] (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 zakrpama i slika **WMI** je moćan interfejs za upravljanje Windows sistemima, *wmic.exe* obezbeđuje lagan pristup za automatizovane komande. Sa ispravnim upravljanjem greškama, oporavkom sistema i logiovanjem u hodu, ovo može biti visoko efektivan i skalabilan metod za brzo sakupljanje informacija sa brojnih računarskih sistema, upravljanje i skladištenje rezultata akvizicije sa jedne centralne lokacije. Ovakvu metodologiju implementira komercijalno raspoloživ alat **ProDiscover Incident Response** (*Technology Pathways*), [43]. Sa centralne lokacije forenzčar može instalirati jednog softverskog *inteligentnog agenta*, preko kojeg će tražiti korisne informacije, a zatim ga izbrisati. Pomoću *ProScript API* ovog alata forenzičar može sa dodatnim skriptom (u *Perl* npr.) u programu automatizovati ceo proces, što minimizira broj logovanja u log fajlu bezbednosno relevantnih događaja i količinu softvera kojeg treba instalirati na sistem za udaljeni pristup. **ProDiscover IR**, takođe poseduje dodatne kapacitete za izvlačenje sadržaja iz fizičke memorije, kao i za druge funkcije aktivne akvizicije podataka sa računara u radu.

Osnovno ograničenje metoda aktivne akvizicije digitalnih podataka sa udaljenim pristupom je što se forenzičar mora logovati na sistem kroz računarsku mrežu. Ako je na bilo koji način ograničen sistem logovanja preko *NetBIOS* (Windows platforme), na primer NetBIOS nije instaliran, *firewalls*/ruteri blokiraju protokole i slika, ovaj se metod neće moći primeniti.

Hibridni metod aktivne akvizicije je kombinacija lokalne i metodologije aktivne akvizicije sa udaljenim pristupom. 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 forenzički alat za akviziciju (sakupljanje) digitalnih podataka/dokaza. Kada se forenzički alati aktiviraju, svaki od njih šalje izlaz preko mreže na centralni *forenzički server*. Na ovaj način ne vrši se logovanje sa udaljenim pristupom, poverljivi

28 *Comma Separated Value* – ekstenzija fajla koji sadrži tabele (baze podataka)

forenzički alati vrše akviziciju sa neizmenjenih izvora podataka, a vrlo malo ima upisa na HD korumpiranog računara ('žrtve'). Dakle, sa dobrim planiranjem, smanjenjem grešaka koje alat unosi, redukcijom ulaznih komandi (npr., sa jednim skriptom izvršava se automatski pet komandi), forenzičar može minimizirati interakcije sa korumpiranim sistemom sa kojeg se vrši akvizicija podataka. Najjednostavniji način primene hibridnog metoda aktivne akvizicije je sa upotrebom *bach* fajla.

2.2.3 Izbor i priprema forenzičkih alata za aktivnu akviziciju

Sve informacije raspoložive u aktivnoj akviziciji mogu se izvlačiti odgovarajućim alatima i to:

- *Alatima komandne linije (CLI-Commande Line Interface)* koji imaju najmanji "otisak u memoriji", što znači da koriste manje memorije, oslanjaju se na manje DLL (*Dynamic Link Libraries*) računarskog sistema i samim tim imaju manji uticaj na promene u sistemu. Ovi se alati lakše koriste, jednostavni su, izvršavaju specifične funkcije i lako se automatizju kroz korišćenje batch ili skript fajlova, a izlaze šalje na interfejs komandne linije;
- *Alatima GUI tipa interfejsa*, gde se tipično zahteva skladištenje izlaza u neki fajl u fajl sistemu. Kako je cilj forenzičkog ispitivanja aktivnog 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, onda ga treba koristiti.

Osnovni koraci u dokumentovanju, verifikaciji i vrednovanju forenzičkog alata čine statičko i dinamičko testiranje alata, [33].

- *Statičko testiranje* uključuje dokumentovanje jedinstvenog identifikatora o alatu, kao što su:
- *URL sa kojeg je dobijen softverski forenzički alat,*
- *veličina fajla,*
- *kriptografski heš za fajl, dobijen korišćenjem poznatog heš algoritma,*
- *izvlačenje informacija iz fajla, kao što su PE (Portable Executable) hederi, tip fajla, import/export tabele 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 Registara i fajl 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 izvlačenja sistemskog vremena pomoću **Remote Administrator (Radmin)** programskog alata**.**

Radmin je multifunkcionalni program za daljinsku kontrolu, koji omogućava da se sa daljine posmatra ili radi na jednoj ili više mrežnih kompjutera sa radne stanice. Može se videti ekran udaljenog računara na sopstvenom monitoru preko prozora ili preko celog ekrana. Svako pokretanje miša ili signali sa tastature posmatranog računara, prenose se direktno ka udaljenom računaru. **Radmin** omogućava rad na svakom udaljenom računaru ukoliko je priključen na Internet ili LAN. Nije potrebna ni brza konekcija, modem 56K je dovoljno brz da obezbedi 5-10 slika u sekundi. U okviru LAN, 100-500 slika u sekundi je uobičajena brzina prenosa. U **Radmin** alatu brzina može biti podešavana.

Sistem **Radmin** alata uključuje dve aplikacije:

- *Radmin Server*, koji se instalira na udaljenom računaru i
- *Radmin Viewer* na lokalnom računaru koji prikazuje ekran udaljenog računara.

Mehanizam zaštite podataka u prenosu u **Radmin** programi je 256 bitna AES šifarski sistem. Za autentifikaciju koristi Kerberos protokol sa novim metodom autentifikacije zasnovanim na *Diffie-Hellman* razmeni ključa od 2048 bita. **Radmin** informacije o DNS i korisničkom imenu dodaju se u log fajl.

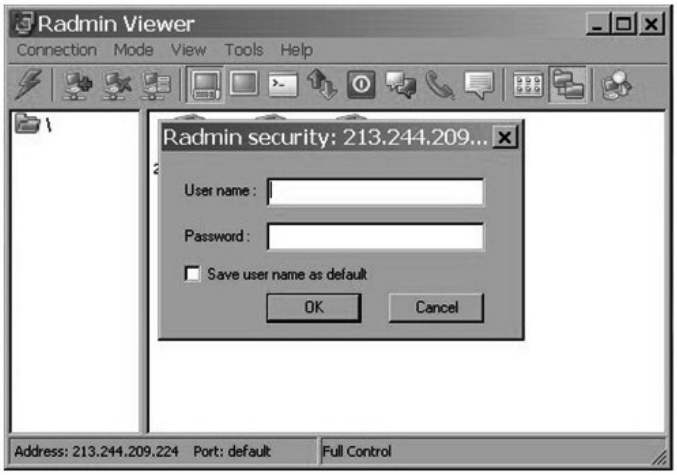
Radmin nema specijalne hardverske zahteve, dovoljan je računar koji može da radi na Windows 95 ili novijim operativnim sistemima**. Radmin Viewer** može funkcionisati čak i na 486 računarima sa 8 MB RAM i na Windows 9x/ME/NT/2000/XP/2003 Server/Vista 32-bit. **Radmin Server** može raditi na Windows 2000/XP/2003 Server/Vista 32-bit. Za sve operativne sisteme, računar bi trebao da ima instaliran TCP/IP protokol.

Kada se pokrene **Radmin Viewer** na lokalnom računar, klikne se „*Connect to*“ dugme, unese IP adresa ili DNS ime udaljenog računara, izabere „*Full Control*“ metod povezivanja i klikne **OK** dugme, (slika 2.13). Ovom metodom se preuzima potpuna kontrola nad udaljenim računarom.



Slika 2.13 Uspostavljanje veze pomoću Remote Administrator

Zatim se unese ID za logovanje i lozinka prema setovanju **Radmin Servera** ispitivanog računara, (slika 2.14).



Slika 2.14 Radmin Viewer

Desktop udaljenog računara će se pojaviti unutar prozora na udaljenom računaru.

Radmin takođe nudi i dodatne metode za rad sa udaljenim računarom: može se povezati preko *shell*-a sličnog *Telnet*-u, samo posmatrati udaljeni ekran, koristiti audio *chat* sa korisnikom udaljenog računara ili koristiti file transfer režim povezivanja.

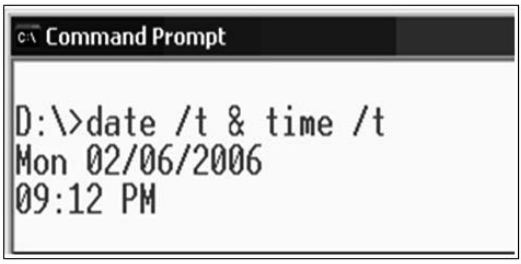
Na ovaj način, forenzičar može npr. izvući sistemsko lokalno vreme i datum na bazi vremenske zone i usklađivanja vremena sa dnevnom svetlosti, korišćenjem jednostavnog *Perl* skripta, kao što je:

print locatime (time).”\n”,

ili za prikazivanje vremena u GMT formatu sa skriptom:

print gmtime(time).”\n”.

Sistemsko vreme i datum iz Command Promt u Windows XP OS prikazano je na slici 2.15.



Slika 2.15 Sistemsko vreme i datum u Windows XP OS

U slučaju etičkog hakinga, kada forenzičar ne želi da osumnjičeni zna da je istraga u toku, može se umesto **Radmin** alata koristiti alat **ProDiscover Suite** koji podržava *stealth* mode[29].

Forenzičarima je na raspolaganju širok spektar alata sa različitim funkcionalnostima i namenama. U procesu aktivne akvizicije praktično je koristiti alat koji obezbeđuje transport sakupljenih informacija sa udaljenog računarskog sistema do centralnog forenzičkog servera. Dobar alat za ovu svrhu je **Netcat** [28], 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 (na kojem se teško ostvaruje zadržavanje *nc.exe* fajla otvorenim kada se konekcija zatvori) i da sve što dođe na taj port 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 sledećim instrukcijama:

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, na primer, sa D:\, gde se nalazi forenzički CD-ROM/DVD:

D:\>remote.bat 192.168.1.10 80

Kada se jednom pokrene ovaj *batch* fajl, svi podaci se bezbedno prenose sa ispitivanog (korumpiranog, osumnjičenog računara) na forenzički server za bezbedno čuvanje i forenzičku analizu.

Metodologiju aktivne akvizicije implementira nekoliko *freeware* forenzičkih alata, npr., **Forensic Server Project** (**FSP)** - alat otvorenog koda, pisan u *Perl-u* i besplatan. Ideja za **FSP** je nastala posle upotrebe **netcat**, gde forenzičar pokreće alat na kompromitovanom sistemu sa forenzičkog CD/DVD-a, a zatim kanališe izlaze komandi kroz **netcat**, koji je odgovoran za slanje informacija na centralni forenzički server. Ovaj metod dobro funkcioniše u nekim situacijama, ali kada se broj komandi poveća i komande imaju veći opseg argumenata, raste broj grešaka i proces metoda postaje težak za primenu. Tako je nastao alat **Forensic Server Project**, koji automatizuje sakupljanje, skladištenje i upravljanje podacima aktivne akvizicije. **FSP** alat sadrži dve komponente: *serversku* i *klijentsku*. 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 na mrežnu konekcije. **FSP** upravlja sa zadacima, logovanjem i skladištenjem u

29 skriven, pritajen metod

forenzičkom slučaju. Kada se ostvari 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 forenzičkog CD ili USB. **FRU** je jednostavan uslužni alat koji se koristi za sakupljanje informacija sa kompromitovanog računara. Kada **FRU** primi komandu, uzima izlaz komande i šalje ga na **FSP**, koji skladišti informacije i loguje aktivnosti na forenzičkom serveru. **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 3.11) koji sadrži 4 sekcije za: konfigurisanje (*Configurations),* komande (*Commands),* separaciju (*Separators) i* imenovanje (*Names).*

[Configuration] – sa podrazumevanim setovanjem da se **FRU** konektuje sa **FSP** preko porta 80, što se može promeniti sa komandne linije;

[Commands] – izlistira TTP alate za sakupljanje informacija, što može biti bilo koji Windows portabilni izvršni fajl (PE-*Portabile Executable*) koji šalje svoj izlaz na konzolu forenzičkog servera. Format ove sekcije je različit i vrlo važan. Format svake linije izgleda:

<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 *promtu* na računaru.

[**Separators**] - prve dve sekcije su odvojene znakom jednakosti **(=)** iza kojeg sledi znak **(::)**, a konačne sekcije jedne od ovih linija odvojene su sa **(;)**, a ako više alata *(npr.* **psloglist.exe** od *SysInternals.com)* imaju mogućnosti korišćenja ovog znaka, onda treba izabrati neki drugi znak.

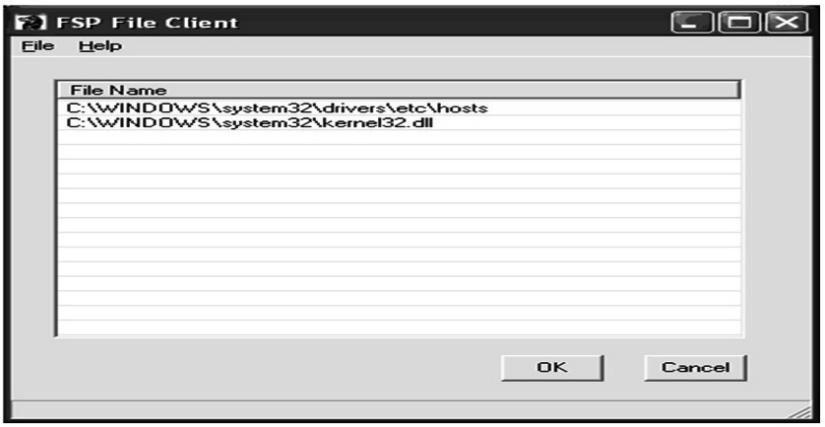
[Names] – ime fajla koji treba da se generiše, najčešće ime alata sa **.dat** ekstenzijom. Na ovaj način podaci se mogu sakupljati sa više sistema koristeći istu aktivnu instancu **FSP**.

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

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

Postoje i druge klijentske komponente dostupne za kopiranje fajlova i slanje digitalnih podataka sa kompromitovanog računara. 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 | 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, SHA-1,...). Ove se informacije šalju **FSP** serverskoj komponenti na forenzičkom računaru. Zatim **FCLI** kopira binarne sadržaje fajla na forenzički server. Kada se operacija kopiranja kompletira, FSP servera 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. Na slici 2.16. prikazan je GUI klijenta za kopiranje fajla ili FCLI komponente.



Slika 2.16 GUI klijent za kopiranje fajla

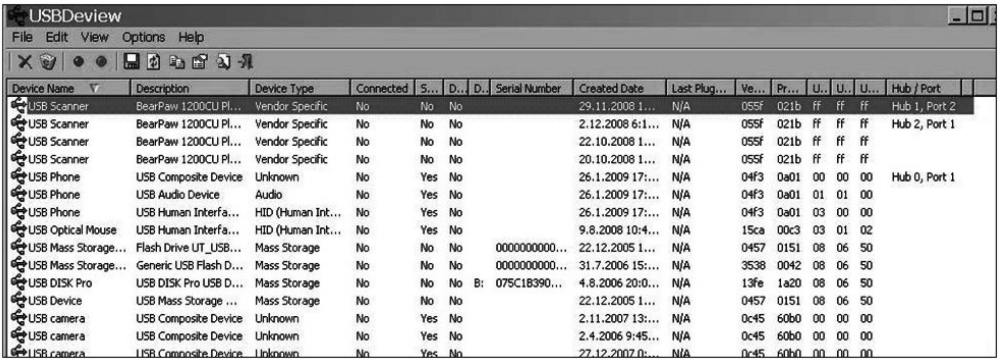
Forenzički alat **Forensic Server Project** se isporučuje na DVD-u, na kome su uključeni filmovi koji ilustruju kako se podešava alat za upotrebu i daju instrukcije gde se može nabaviti potreban uređaj za reprodukciju.

2.2.4 Prednosti i nedostaci aktivne forenzičke akvizicije

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 hotfiksove *(hotfix)*, a reinstaliraju aplikacije i podatke sa medijuma za bekapovanje. Međutim, ovakav pristup ne može, pre svega, odrediti *kako* se incident dogodio. Takođe, 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 hotfiksova. Ponekad uzrok incidenta mogu biti slaba lozinka, ili nepostojanje lozinke na nalogu korisnika ili aplikaciji, kao što je ***sa*** lozinka 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 utvrde kako se incident dogodio i ne otklone uzrok, velika je verovatnoća da će se incident ponovo dogoditi.

Aktivna forenzička istraga i akvizicija omogućavaju forenzičkim islednicima da otkriju značajne informaciju koje bi nestale pri klasičnoj (*postmortem*) istrazi isključenog računara. Ove informacije mogu imati značajan uticaj na forenzičku istragu, a mogu uključivati podatke iz fizičke memorije (RAM), aktivne procese, logove događaja, mrežne informacije, sadržaji *clipboard-a,* registrovane drajvere i servise.

Na primer, mali forenzički alat **USBDeview** pravi listu svih USB uređaja koji su prethodno bili korišćeni na ispitivanom računaru i svih USB uređaja koji su trenutno povezani sa ispitivanim računarom. **USBDeview** se može koristiti i na računaru kojem se pristupa daljinskim putem. Za svaki USB uređaj prikazuju se proširene informacije, kao što su: naziv uređaja/opis, tip uređaja, serijski broj uređaja za masovno skladištenje, datum/vreme kada je uređaj priključen, identifikacioni broj proizvođača, identifikacioni broj proizvoda itd., (slika 2.15). **USBDeview** takođe omogućava da se deinstaliraju USB uređaji koji su prethodno korišćeni i da se diskonektuju USB uređaji koji su trenutno povezani sa računarom.

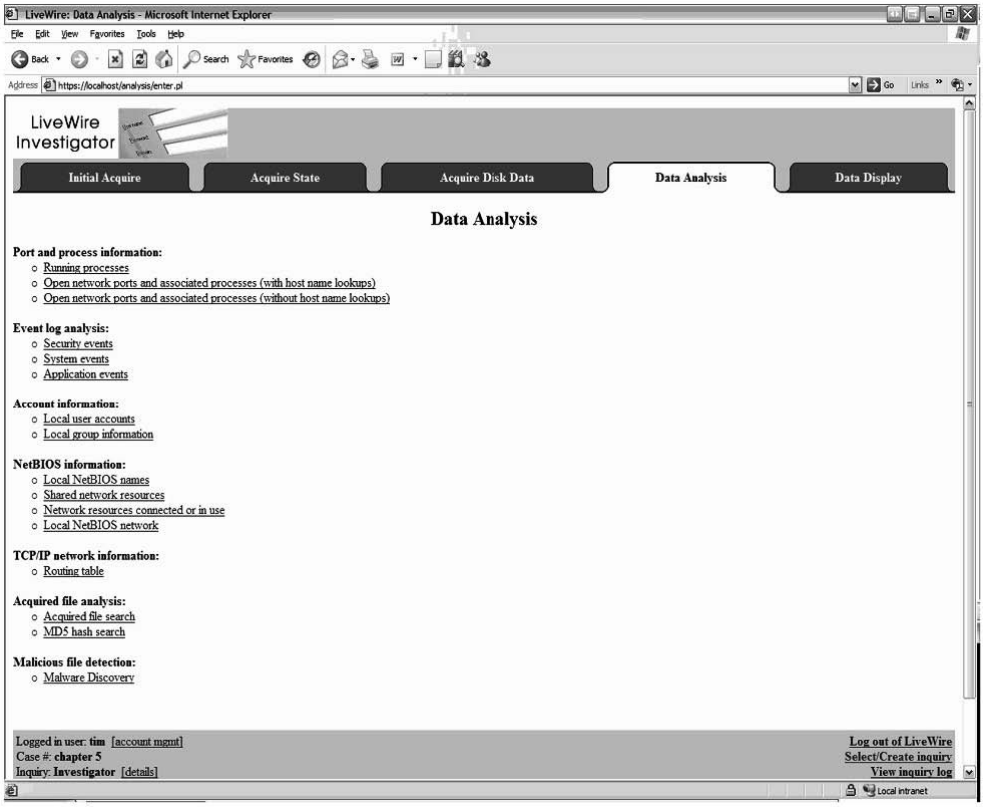


Slika 2.17 Prikaz svih USB uređaja povezanih na računar u USBDeview alatu

Aktivni servisi nam govore o tipovima servisa koji se mogu izvršavati na računaru. Ovi servisi se izvršavaju sa mnogo većim prioritetom nego procesi i mnogi korisnici nisu svesni da oni uopšte postoje. Zbog tipičnog nedostatka pažnje krajnjeg korisnika, oni postaju glavna meta napada za hakere. Tehnikama i alatima aktivne forenzičke istrage i akvizicije, mogu se videti stanja ovih servisa, koja bi mogla biti odlučujuća za dalji tok istrage. Na primer, haker bi mogao da isključi servis za *McShield* u *McAffee Antivirusnom* programu, a onda se kasnije vratiti i napasti mašinu malicioznim softverom.

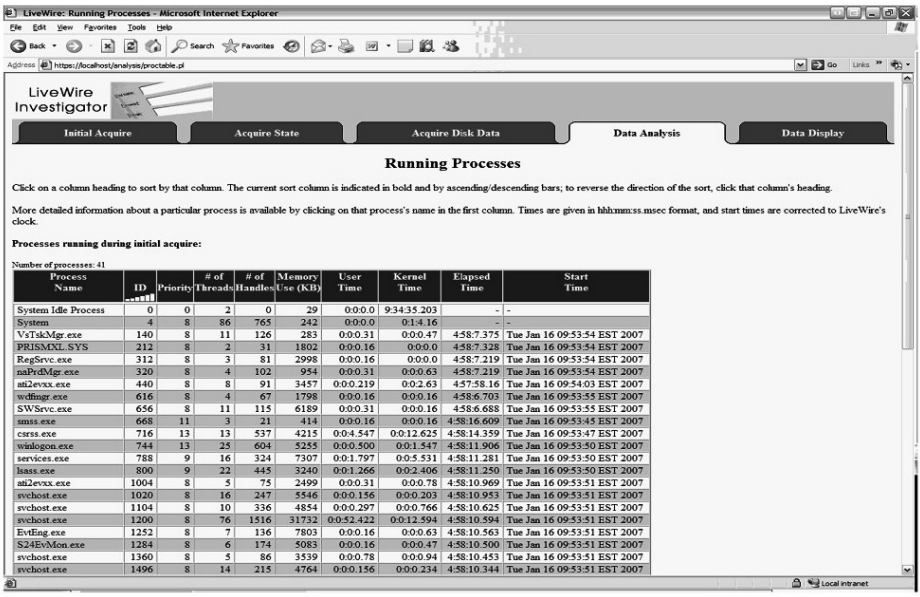
U slučajevima registrovanih drajvera, diskutabilno je da li se može dobiti lista drajvera u klasičnoj istrazi. Ako se na mestu krivičnog dela kompjuterskog kriminala i sprovodi aktivna istraga, mogao bi se videti drajver za, na primer, digitalnu kameru, koja bi mogla da se potraži u okruženju. Ali ako je lokacija napuštena, a drajver kamere se otkrije kasnije, forenzičar se može samo nadati da se kamera još uvek nalazi na

istom mestu. Uvid u registrovane drajvere daje forenzičkim islednicima informacije o perifernim uređajima sumnjive namene. Na slici 2.18 ilustrovane neke polazne sistemske informacije koje se mogu dobiti o stanju sistema aktivnom forenzičkom akvizicijom pomoću alata **LiveWire** forme *Wetstone*.



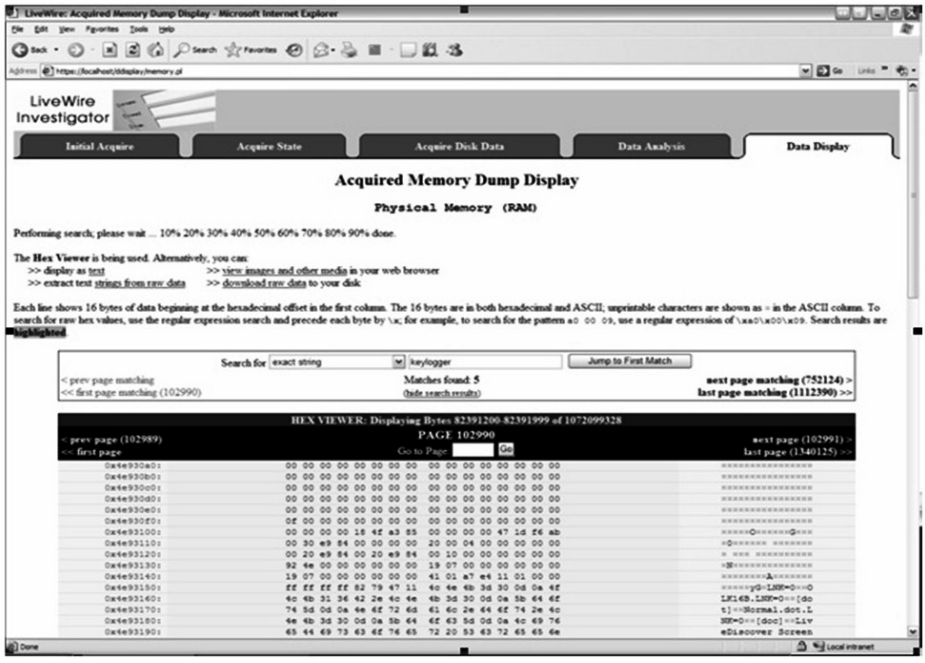
Slika 2.18 Primer sistemskih informacija dobijenih aktivnom akvizicijom sa LiveWire alatom

Uvid u aktivne procese sa povezanim otvorenim mrežnim portovima je jedan od najvažnijih zadataka analize stanja sistema. Uvid u sistem i tačna procena o tome koji je proces aktivan i koje portove oni koriste, kritična je faza za trijažu podataka za istragu. Na slici 2.19 dat je detaljni prikaz aktivnih procesa ciljne mašine pod istragom, gde se ne vide samo nazivi procesa već i prioritet, broj zadatka, broj obrade (*handl*-ova), utrošak memorije i vreme ispravnog rada. Sve to je važno znati ako forenzičar pokušava proceniti šta neko trenutno radi ili šta je radio u prošlosti. U klasičnoj digitalnoj forenzičkoj istrazi, sadržaj fizička memorije (RAM) je potencijalno najvažniji deo izgubljenih dokaza. U aktivnoj forenzičkoj akviziciji, ovaj odlučujući deo dokaza se lako prikuplja, bilo da se ceo sadržaj RAM-a uzima lokalno ili sa udaljenim pristupom.



Slika 2.19 Pogled na aktivne procese u LiveWire forenzičkom alatu

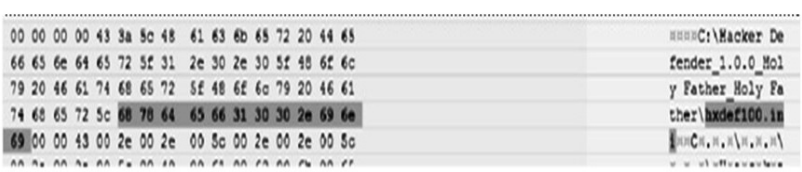
Na slici 2.20 može se u heksadecimalnom pretraživaču **LiveWire** forenzičkog alata videti sirovi binarni sadržaj imidža fizičke memorije sa otkrivenim *keylogger*-om.



Slika 2.20 Otkrivanje šifre za rad keylogger-a u memoriji sa LiveWire alatom

U klasičnoj istrazi i akviziciji sadržaj neobrađenih podataka koji obezbeđuje RAM memorija, gubi se ako se mašina isključi. Memorija sadrži brojne dokaze - od korisničkih naloga, lozinki, nesačuvanih sadržaja dokumenata i malicioznih programa.

Značajno je da se analizom podataka u imidžu RAM memorije, uzetom u procesu aktivne forenzičke akvizicije mogu otkriti maliciozni programi, Trojanci i rutkit alati, kao što je Hacker Defender program, popularan rutkit alat koji je sposoban da prikriva procese, fajlove i čak otvorene portove. Kada se ovaj program izvrši u napadnutom računaru, on krije svaki fajl koji sadrži prefix „hxdef". Kao rezultat, fajl „hxdef100.ini," koji je deo Hacker Defender programa se sakriva čim se Hacker Defender izvrši. Ovaj fajl je tada sakriven od svih korisnika i čak i od samog Windows Explorer-a. Međutim, fajl još uvek postoji u fizičkoj (RAM) memoriji. Primenom tehnika aktivne forenzičke akvizicije, može se uzeti imidž RAM memorije i identifikovati fajl "hxdef100.ini" u heksadecimalnom pretraživaču koji je smešten u RAM-u (slika 2.19). Isti metod se može koristiti da se otkrije bilo koji fajl ili proces koji Hacker Defender krije (slika 2.20). U toku procesa klasične forenzičke istrage i akvizicije, neki fajlovi ili procesi sakriveni Hacker Defender alatom mogu biti nedostupni forenzičkom istražitelju. Slike 2.21 i 2.22 pokazuju digitalni dokaz o prisustvu Hacker Defender rutkit programa u fizičkoj memoriji ispitivanog računara.



Slika 2.21 Trag **Hacker Defender**-a u fizičkoj memoriji u LiveWire alatu



Slika 2.22 Drugi pogled na **Hacker Defender** u RAM memoriji u LiveWire alatu

Dakle, istraživanje stanja kompjuterskog sistema je važan deo svake digitalne forenzičke istrage. Mogu se sakupiti dragocene informacije o slučaju, smanjiti rizik gubljenja podataka koji bi mogli biti ključni za istragu i sprečiti sporove sa drugom stranom u slučaju.

Naime, često se u aktivnoj istrazi previdi mrežno okruženje u kojem ciljni računar radi. Podaci koji su u upotrebi u mrežnim barijerama (*firewalls*), ruterima, detektorima upada u sistem (IDS/IPS) itd., podjednako su važni za forenzičara za rekonstrukciju

cele slike događaja. Tako, na primer, u slučaju otkrivanja **Hacker Defender** rutkit alata u ispitivanom računaru, advokat odbrane može tvrditi da je mašina njegovog klijenta bila kompromitovana i da njegov klijent nije mogao izvršiti krivično delo kompjuterskog kriminala. Provera logova mrežnih barijera može pokazati da je aktivnost **Hacker Defender** programa na ovom računaru bila blokirana. Forenzički istražitelj treba da u procesu aktivne akvizicije prikupi što više informacija o mrežnoj aktivnosti napadača. U tom smislu može se instalirati skener (*sniffer*) paketa sa odgovarajućom dozvolom za rad i izvršiti analiza paketa. Ovom tehnikom bi se moglo odrediti da li je neko bio priključen na osumnjičenu mašinu pre sprovođenja analize. Dakle, mogu se naći dodatni dokazi i izvan računara koji se ispituje.

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

REZIME

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. U procesu klasične (*posmortem*) digitalne forenzičke akvizicije potrebno je uzeti fiziču kopiju (*imidž*) svakog ispitivanog medija (HD, CD, FD, fleš memorija) i memorisati ga na poverljiv, forenzički sterilan disk.

Funkcionalni model digitalne forenzičke akvizicije tipično koristi koncept apstrakcionih slojeva: određivanja *ulaza i izlaza* (I/O), *pripisivanja operacija čitanja i upisivanja* za pripadajuće forenzičke alate i *vremensko pečaćenje operacija čitanja i upisivanja*.

U slučaju klasične forenzičke akvizicije, forenzičar izvlači podatke iz privremeno oduzetog osumnjičenog računara uzimanjem forenzičkog imidža (dve kopije), a zatim ispitivanje vrši na radnoj kopiji imidža na forenzičkom računaru.

U procesu aktivne forenzičke akvizicije 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. Kada forenzičar u procesu akvizicije pristupa računaru u radu, događaju se promene u sistemu (tzv. Lokardov princip razmene materije) kako se izvršava forenzički program i podaci imidžuju na forenzički sistem. Ove promene mogu biti *prelezne* – memorija procesa, mrežne konekcije, ili *trajne* – log fajlovi, ulazi Registra, keš fajlovi (Internet istorija).

Do razvoja metoda, tehnika i alata aktivne digitalne forenzičke akvizicije i istrage (aktivne digitalne forenzike) doveli su brojni faktori, od kojih su najznačajniji ubrzan razvoj kapaciteta memorijskih medija za skladištenje i ogromna količina podataka za akviziciju i analizu, pre svega HD (reda TB), zatim razvoj raznih antiforenzičkih tahnika i alata za skrivanje tragova i brisanje podataka i informacija koje mogu kompromitovati i dovesti u vezu napadača sa incidentom ili događajem kompjuterskog kriminala. Odgovore na ova pitanja nisu davale tehnike i alati klasične (*postmortem*) akvizicije isključenog računara.

U odnosu na tehnike i alate za povezivanja forenzičkog računara na ispitivani računarski sistem u procesu aktivne forenzičke akvizicije, mogu se grupisati tri kategorije modela tehnika i alata: *Pre-Deployed Agent model, Direct Connect model i On Demand Connection model.*

U odnosu na način pristupa ispitivanom računaru uradu, postoje tri osnovna metoda aktivne akvizicije sa: *lokalnim pristupom, udaljenim pristupom i hibridnim pristupom*. Poznavanje ovih metoda i posedovanje alata koji implementiraju njihove procese akvizicije, značajno povećavaju fleksibilnost i kapacitet forenzičara za sakupljanje digitalnih podataka i informacija, relevantnih za slučaj

kompjuterskog incidenta/kriminala. Koji će metod aktivne akvizicije forenzičar koristiti, zavisi od faktora kao što su postojeća infrastruktura mreže, mogućnosti forenzičara za implementaciju metoda, pa često i kultura rada i politička struktura organizacije.

U primeni svakog metoda forenzičar mora biti svestan činjenice da njegove akcije ostavljaju artefakte na kompromitovanom sistemu, kao što su upisivanja u Registar priključenog USB, izmena više fajlova, a izvršni *imidži* mogu biti smešteni u memoriju. Međutim, ove izmene mogu biti kvantifikovane, a sve akcije primene metoda aktivne akvizicije forenzičar treba da dokumentuje i da ih može objasniti na zahtev suda.

Iako nema čvrstog pravila kada forenzičar treba da primeni aktivnu akviziciju, treba imati na umu da brojni entiteti i regulatorna tela zahtevaju obaveznu primenu specifičnh kontrola (mehanizama i mera) zaštite računarskih sistema i mreža, uključujući i ograničenja prava pristupa osetljivim ličnim podacima i poverljivim informacijama, kao i činjenicu da aktivna akvizicija postaje sve značajnija u uslovima svremenog elektronskog poslovanja, gde je isključivanje računarskih sistema (npr. korporacijskih servera) za potrebe klasične akvizicije uzimanjem imidža HD kompromitovanog računara veoma teško ili neizvodljivo (npr., ne dozvoljava vlasnik sistema).

U slučaju da je na sistemu aktivirana tzv. *odbrana sa Trojancem*, aktivna akvizicija može pomoći da se utvrdi da li je Trojanac aktivan u trenutku sakupljanja informacija kao i da li je odgovoran za kompromitaciju ispitivanog računara, što može iskoristiti odbrana. Klijentska komponenta forenzičkog alata za aktivnu akviziciju sakuplja informacije o aktivnim procesima, servisima i drugim oblastima gde se mogu otkriti Trojanci ili artefakti za ubacivanje i skrivanje zadnjih vrata (*rutkitovi*), na osnovu kojih forenzičar može zaključiti da li su aktivni u trenutku akvizicije informacija.

PITANJA ZA PONAVLJANJE

1. Definišite digitalnu forenzičku nauku (digitalnu forenziku).
2. Navedite glavne faze procesa digitalne forenzike.
3. Koje podatke moraju otkriti organi istrage u procesu digitalne forenzičke istrage?
4. Navedite i definišite glavna četiri principa za rad sa kompjuterskim digitalnim dokazima.
5. Koje korake/aktivnosti tipično preduzima forenzičar u procesu akvizicije digitalnih podataka?
6. Koji je osnovni značaj aktivne (žive, realne) akvizicije računara u radu?
7. Objasnite Lokardov princip razmene materije primenjen na istragu kompjuterskog incidenta/kriminala.
8. Navedite redosled sakupljanja podataka u procesu žive akvizicije.
9. Nabrojte neke od informacija koje se mogu izvući iz RAM memorije računara u radu.
10. Navedite tri osnovna metoda aktivne akvizicije.
11. Koja tehnika obezbeđuje najjednostavniji način primene hibridnog metoda aktivne akvizicije?
12. Navedite ključne prednosti aktivne forenzičke akvizicije.

3. FORENZIČKA ANALIZA DIGITALNIH PODATAKA

3.1 DIGITALNA FORENZIČKA ANALIZA

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 materiajle, na primer dečiju pornografiju i slika, ali i korumpiran (*zombiran)* računar u kojem napadač drži skrivene ilegalne materijale, bez znanja vlasnika/korisnika računara [28].

Klasifikacije digitalne forenzičke analize mogu biti na bazi više kriterijuma. Uobičajena klasifikacija je na bazi izvor digitalnih podataka.

Forenzička analiza digitalnih podataka, prema izvoru digitalnih podataka, može se klasifikovati u tri glavne oblasti:

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

3.1.1 Digitalna forenzička analiza softvera

Digitalna forenzička analiza softvera, uglavnom visoko teoretski posao, najosetljiviji je deo digitalne forenzičke analize. Razzvoj tehnika i izrada softverskih alata za forenzičku analizu softvera je težak i složen posao, [6]. Ključ za identifikaciju autora malicioznog kôda je u selekciji odgovarajućeg korpusa elemenata kôda i identifikaciji unetih odgovarajućih ličnih karaktersitika autora za kasnije upoređivanje [25].

Očigledan problem je što autori malicioznih kôdova 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 orginalnih 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 orginalnog izvornog kôda programa je od presudnog značaja i korisniji od kompajlerskog izvornog kôda. Neke od identifikacionih karakteristika su, [25]:

- 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 orginalnog 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.

3.1.2 Forenzička analiza računara

Forenzička analiza računara je aplikacija ispitivanja računara i tehnika analize komponenti računara u cilju otkrivanja potencijalno legalno prihvatljivih dokaza, generisanih, ili uskladištenih u računaru. Kompjuterski specijalisti mogu primeniti brojne metode i tehnike 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, potrebana su dodatna znanja, veštine, forenzičke tehnike i 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 – krajnjem računaru, serveru, ruteru itd. Ova oblast digitalne forenzike detaljno je obrađena u *II Delu* udžbenika *Digitalna forenzika računarskog sistema.*

3.1.3 Forenzička analiza u virtuelnom okruženju

Virtuelizacija je stari koncept, prvi put uveden 1960-tih, sa pojavom *mainframe* računara. Ponovo je uvedena u personalnim računarima 1990-tih, a danas su na raspolaganju: *Microsoft Virtual PC (2007*), *VMWare* set softverskih alata (*VMWare*, 2007), softver otvorenog koda (besplatan) *QEMU* (Bellard, 2007) i nekoliko drugih. Virtuelna mašina (VM) je softverski proizvod koji omogućava korisniku da kreira jedno ili više okruženja (platformi) od kojih svako simulira svoj skup hardverskih komponenti (CPU, čvrsti disk, memoriju, mrežne kontrolere i druge hardverske komponente) i sopstveni softver. Idealno je kada se svaka virtuelna mašina radi i ponaša se kao potpuno nezavisan računar sa sopstvenim operativnim sistemom i hardverom. Korisnik može kontrolisati svako okruženje nezavisno i, ako je potrebno, umrežiti virtuelne računare zajedno ili ih spojiti na eksternu fizičku mrežu, [1].

Iskustva iz forenzičke prakse pokazala su ograničenja virtuelnog okruženja (*VMWare*, 2007) i da klasičan metod akvizicije i analize digitalnih podataka ne može biti automatski primenjen. Predložen je novi pristup u kojem se konvencionalno i virtuelno okruženje procesiraju nezavisno čime se skraćuje vreme analize i može se koristi manje kvalifikovano osoblje za forenzičku analizu.

Okruženje kreirano sa *VMWare* znatno se razlikuje od originalnog računarskog sistema, a osim toga mala je verovatnoća da sam *VMWare* može proizvesti sudski prihvatljive dokaze. U novom pristupu dva okruženja, konvencionalno virtuelno, koriste se konkurentno i nezavisno. Posle forenzički ispravne akvizicije imidža čvrstog diska prave se dve kopije. Jedna kopija se *hešuje*, čuva i procesira striktno prema proceduri čuvanja imidža u celom lancu istrage, a druga kopija imidža se daje tehničaru (ne forenzičaru) koji radi na njoj u mašini sa virtuelnim okruženjem ne obraćajući pažnju na striktne forenzičke procedure. Svaki nalaz se dokumentuje i predaje kvalifikovanom forenzičaru koji nalaze potvrđuje u skladu sa forenzičkim procedurama. Dodatna prednost je što virtuelno okruženje olakšava demonstraciju nalaza ne tehničkim licima

Proces klasične digitalne forenzičke istrage sadrži brojne korake, a može se generalno enkapsulirati u četiri ključne faze, [1]:

- pristup,
- akviziciju,
- analizu i
- prezentaciju (izveštavanje).

U fazi akvizicije forenzičar sakuplja što je moguće više promenljivih podataka sa aktivnog sistema, zatim isključuje računar i kreira forenzički (bit po bit) imidž svih medijuma za skladištenje. Pošto je **DD** imidž isti kao original, može se kopirati na disk istog ili većeg kapaciteta i butovati na drugi računarski sistem. Ovakav pristup je nepraktičan za re-kreiranje originalnog okruženja zbog brojnih mogućih hardverskih kombinacija.

Ako se forenzički imidž butuje na mašinu sa različitom konfiguracijom hardvera, operativni sistem će otkriti ove razlike i pokušati (u nekim slučajevima neuspešno) da instalira nedostajući drajver. Pored toga, neki instalirani servisi i softverski proizvodi mogu odbiti da startuju, ili se može desiti da se sistem uopšte ne butuje. Sličan problem postoji i u VM, koja simulira samo neke osnovne hardverske komponente, pošto nije kreirana da obezbedi punu podršku širokom opsegu hardverskih uređaja. Obezbeđeni DD imidž se neće moći neposredno instalirati na VM, pošto VM zahteva dodatne fajlove koji sadrže informacije o okruženju u kojem se butuje. Ovaj problem mogu rešiti različiti softverski proizvodi koji kreiraju ove dodatne fajlove sa parametrima zahtevanim za VM. Neki od ovih uslužnih alata su:

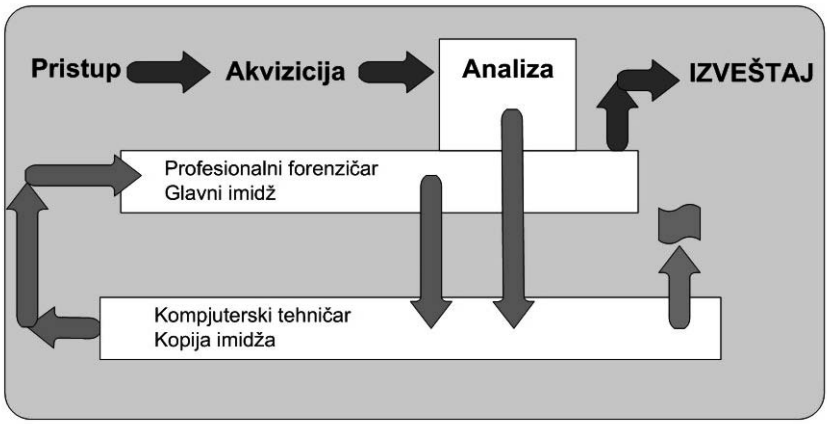
- **EnCase Physical Disk Emulator** (PDE), komercijalni proizvod (*EnCase Forensic Modules*, 2007),
- **ProDiscover** familija komercijalnih i besplatnih alata (*Technology Pathways*), **LLC** (*ProDiscover*, 2007),
- **Live View**, besplatan alat (*Gnu Public License* – GPL, 2007)

Iako su postojale sumnje u vrednost **VMWare** alata za virtuelno butovanje u procesu forenzičke istrage (Fogie, 2004), pošto se zahtevaju brojne izmene originalnog okruženja, ako se želi imidž butovati na VM. Takođe, kada se sistem butuje na VM novi podaci se upisuju na originalni imidž i menjaju ih, što forenzički nije prihvatljivo. Zlatno pravilo da se forenzička analiza vrši na imidžu - bit po bit fizičkoj slici originalnog ispitivanog diska, u virtuelnom okruženju je nesumnjivo narušeno.

Australijski institut za kriminologiju je izdao smernice (McKemmish, 1999) sa preporukom da proces analize digitalnih dokaza treba da bude usaglašen sa sledećim osnovnim principima:

- Minimalno rukovanje i rad sa originalnim računarskim sistemom i čvrstim diskom;
- Nalog za bilo kakvu izmenu i dokumentovanje izmene;
- Usaglašenost sa pravilima rukovanja sa digitalnim dokazima;
- Ne raditi ništa izvan opsega sopstvenog znanja i veštine forenzičke analize.

Tačnost procesa analize može se značajno povećati, a vreme analize podataka skratiti ako se proces proširi uključivanjem dve paralelne linije istrage, kao na slici 3.1.



Slika 3.1 Proces dualne analize podataka

U modelu se koristi personala sa dva nivoa forenzičkih kompetencija:

- manje iskusnih kompjuterskih tehničara i
- iskusnih forenzičara.

Manje iskusni forenzički/kompjuterski tehničar radi po zadatku, ne mora da striktno sledi pravila metoda forenzičke istrage i nikada ne unosi rezultate istrage direktno u formalni proces izveštavanja. Uloga tehničara je da u kopiji materijala proveri sve što je od potencijalnog interesa i zatim podnese izveštaj profesionalnom forenzičaru istraživaču. Zadatak kompjuterskog tehničara je da dobijeni imidž butuje na virtuelnoj mašini, tretira je kao normalan *živi* računarski sistem i pretražuje sve detalje relevantne za istragu. Metod kojeg koristi kompjuterski tehničar na vrši validaciju integriteta dobijenog imiđža što nema posledica za istragu. Sve nalaze predaje iskusnom forenzičaru na verifikaciju i dalju istragu. Da bi instalirao imidž na VM mašinu tehničar treba da instalira dodatne drajvere (npr. **LiveView**) koji definitivno kontaminiraju imidž i prema tome rezultati ovog ispitivanja nebi bili prihvatljivi na sudu

Osposobljeni i iskusni profesionalni forenzički istraživači rade striktno prema metodama digitalne forenzičke istrage računarskog sistema. Forenzičar koristi standardne forenzičke tehnike i procedure da potvrdi rezultate analize tehničara i u izveštaj unosi samo rezultate koji su forenzički potvrđeni.

3.1.3.1 Studija slučaja digitalne forenzičke analize virtuelne mašine

U forenzičkom slučaju primene ovog modela sa **VMWare** alatom, kompjuterski tehničar je otkrio dva interesantna fajla - *DriveHQ* i *Simple File Shredder*. Prvi fajl je predstavljao web adresu skladišta podataka na web serveru. Tehničar je otkrio da je

pristup skladištu podataka zaštićen lozinkom i posle primene nekoliko alata za oporavak (krekovanje) lozinke uspeo dešifrovati lozinku alatom *Aqua Deskperience*. Drugi fajl je anti-forenzički program za eliminisanje digitalnih podataka iz računara. Tehničar je sve nalaze i rezultate istrage dostavio forenzičaru. Digitalni forenzičar je zaključio da je prvi fajl iznajmljeni repozitorijum što je ukazivalo da su potencijalni dokazi verovatno odlagani u tom skladištu. Na osnovu drugog fajla, forenzičar je zaključio da osumnjičeni koristi anti-forenzički alat za brisanje dokaza, što je značilo da je verovatno malo dokaza ostalo na ispitivanom računaru i da je potrebna dalja istraga na referentnom, forenzički zaštićenom imidžu u pokušaju otkrivanja novih dokaza sa forenzičkim tehnikama i alatima, kao i istraga odloženih podataka u web serveru.

Za bolju procenu digitalne forenzičke analize virtuelnih mašina potrebno je jasnije definisati zadatke tehničara i ispitati druge softvere za virtuelizaciju sa svim prednostima i nedostacima.

3.1.4 Digitalna forenzička analiza računarske mreže

Digitalni forenzičar računarske mreže mora da poznaje brojne metode raznih vrsta mrežnih napada da bi mogao odrediti forenzički metod i tehniku za sprečavanje ponavljanja i otklanjanje uzroka napada, [43].

Karakteristični i najčešći tipovi napada na računarske mreže i primarni načini odbrane su:

1. **DoS/DDoS napad** može da se izvrši na:
   - *mrežnom sloju* slanjem malicioznog datagrama koji sprečava mrežne konekcije ili
   - *aplikativnom sloju* gde neka maliciozno programirana aplikacija daje komandu sistemskom programu, koja izaziva ekstremno korišćenje procesora ili zaustavlja rad računara. Tipičan primer je bombardovanje nekorisnom e-poštom – *spamom* i obaranje e-mail servera.

   Odbrana: višeslojnim sistemom mrežne zaštite (*firewalls*, DMZ[30]) sprečiti sumnjivi mrežni saobraćaj da stigne do hosta (servera) i sumnjive komande programa, čime se može minimizirati rizik DoS/DDoS napada.
2. ***Spoofing***:
   - lažno predstavljanje gde host ili aplikacija napadača imitira akcije drugog hosta ili aplikacije.
   - **Primer** je ranjivost *BSD rlogin* servisa koji imitira TCP konekciju sa drugog hosta, pogađanjem brojeva TCP sekvence i sledeći IP adrese iz mrežnih paketa.

30 DMZ – demilitarizovana zona u kojoj se nalaze uređaji dostupni sa Interneta – autentifikacioni server, proxy server, web server, *exchange* server (e-pošte) itd.

Odbrana:

- verifikacija autentičnosti datagrama i komandi;
- sprečiti rutiranje datagrama sa neispravnim IP adresama izvora i
- uvesti nepredvidljivost u mehanizme kontrole konekcije, kao što su brojevi TCP sekvence i alokacija dinamičke IP adrese portova.

3. **Prisluškivanje:**
   - Najjednostavniji tip napada, gde se host konfiguriše da prisluškuje i hvata mrežni saobraćaj koji mu ne pripada. Pažljivo napisan program za prisluškivanje mrežnog saobraćaja može pokupiti lozinke iz log fajla mrežnih konekcija korisnika;
   - Posebno je ranjiv emisioni (*broadcast*) tip mreža kao što je *Ethernet*.

   Odbrana:
   - izbegavati *broadcast* mrežne tehnologije i nametati korišćenje sistema kriptozaštite informacija na komunikacionim linijama,
   - filtriranje IP sa *firewalls* je korisno, za sprečavanje neovlašćenog pristupa kao i DoS napada na mrežnom sloju i IP *spoofing* tehnika, ali nije efikasno za sprečavanje iskorišćenja ranjivosti mrežnih servisa ili programa i prisluškivanja.

Mrežna zaštita počinje sa autentifikacijom korisnika u autentifikacionom i autorizacionom serveru (A&AS) u DMZ, najčešće korisničkog imena i lozinki. Autentifikovanim korisnicima, *firewall* konfigurisan na bazi implementacije politike zaštite, A&AS omogućava pristup servisima za koje su autorizovani. Iako se efektivni za sprečavanje neovlašćenog pristupa ove kontrole mrežne zaštite ne sprečavaju transmisiju kroz mrežu malicioznih programa i potencijalno štetnih sadržaja.

Honeypots tehnike su u suštini resursi - mamci dostupni sa Interneta. Mogu se razmestiti u mreži sa skenerima za monitoring mrežnog saobraćaja i IDS/IPS sistemima za rano upozorenje upada u računarsku mrežu. Napadači koriste različite tehnike u nastojanju da kompromituju dostupni resurs-mamac. Za to vreme, administratori zaštite mogu izučavati tehnike napada u toku samog napada, a posebno posle napada. Rezultati analize mogu se koristiti za dalje jačanje sistema zaštite aktuelne računarske mreže.

Generalno, bazični alati za mrežnu zaštitu su:

- Logičke barijere (*Firewalls*) za saobraćaj u/iz mreže;
- Antivirusni programi (AVP);
- Programi za zaštitu od napada sa Interneta;
- Jaka autentifikacija (PKI infrastruktura, jednokratna lozinka, smart kartice sa digitalnim sertifikatom);
- Mrežni skener (*Netwark Analyzer*) za kontrolu mrežnog saobraćaja;
- IDS/IPS sistem za detekciju upada u računarsku mrežu.

Digitalna forenzika računarske mreže ili *mrežna forenzika* je proces sakupljanja informacija koje se kreću kroz mrežu i koji pokušava da poveže na neki način raspoložive forenzičke kapacitete za digitalnu forenzičku istragu, akviziciju i analizu mrežnih digitalnih podataka. Mrežni forenzički alati su hardversko – softverski uređaji koji automatizuju ovaj proces. Forenzika bežične mreže je proces sakupljanja informacija koje se kreću kroz bežičnu mrežu i koji pokušava da poveže na neki način raspoložive forenzičke kapacitete za digitalnu forenzičku istragu, akviziciju i analizu digitalnih podataka iz bežične mrežne.

Poznatiji mrežni forenzički alati sa otvorenim izvornim kodom su**: Wireshark; Kismet; Snort; OSSEC; NetworkMiner,** koji je na raspolaganju na *SourceForge i Xplico* **i NFAT,** Internet/IP dekoder saobraćaja kojeg podržavaju sledeće protokoli: HTTP, SIP, FTP, IMAP, POP, SMTP, TCP, UDP, IPv4, IPv6.

NetworkMiner je mrežni forenzički alat za analizu mrežnih podataka, a **NFAT (***Network Forensic Analysis Tool***)** je mrežni forenzički alat za **Windows** platforme**.** Alat se može koristiti kao pasivni mrežni skener (*sniffer*) koji hvata mrežne pakete da bi detektovao OS, sesije, imena hostova, otvorene portove itd. bez propuštanja bilo kojeg saobraćaja u mrežu. Namena alata je da sakupi podatke, kao što su potencijalni digitalni dokazi upada u mrežu (incidenta/kriminala), iz mrežnih hostova i drugih mrežnih uređaja, a manje podatke o mrežnom saobraćaju. Glavni pogled je host centrični, tj. informacije su grupisane po hostovima, a ređe se prikazuju kao lista paketa/frejmova.

Relevantni mrežni, digitalni forenzički alati za dubinsku analizu zasnovani na *data mining* tehnikama su:

- **E-Detective,**
- **ManTech International Corporation,**
- **Network Instruments,**
- **NetDetector**, **(***NIKSUN)*
- **PacketMotion,**
- **NetIntercept**, **(***Sandstorm)*
- **NetBeholder (***Mera Systems***),**
- **Traffic Monitor (***InfoWatch***)**

Relevantni sistemi/alati zasnovani na protoku saobraćaja (*Flow-Based Systems*) su:

- **Arbor Networks**
- **GraniteEdge Networks**
- **Lancope (**http://www.lancope.com**)**
- **Mazu Networks (**http://www.mazunetworks.com**)**

Hibridni sistemi za mrežnu forenziku kombinuju analizu protoka saobraćaja, dubinsku analizu, monitorisanje bezbednosnih događaja i izveštavanje incidenata. Tipično rešenje je **Q1 Labs (**http://www.q1labs.com).

Težinu problema digitalne forenzičke istrage, akvizicije i analize računarske mreže usložava kompleksnost tipova mreža koje moraju biti obuhvaćene:

- *računarske i komunikacione mreže,*
- *telekomunikacione mreže (*žične, bežične, optičke),
- *transportne mreže* (putne, železničke, avionske, pomorske),
- *humane mreže* (terorističke mreže, mreže trgovine drogom, mreže međuljudskih odnosa - *Facebook* i slika).

U ovom kontekstu digitalna forenzička istraga računarske mreže tipično prati sledeći osnovni proces:

- Istragu početi od napadnute mašine**;**
- Pratiti trag do drugih posrednih mašina, sve do izvora napada, koristeći tesnu saradnju sa ISP i telekomunikacionim provajderima u odnosnim regionima/državama,
- Koristiti tehnike vizuelizacije traga napada u pogođenoj, kompromitovanoj/posrednoj mašini i interakcije svih uključenih mreža i uređaja.

3.1.5 Forenzička analiza kibernetičkog prostora

Forenzičku analizu kibernetičkog prostora bez sumnje je najkompleksnija oblast digitalne forenzike i može biti veoma spor i naporan proces. Osnovni zahtev je uspostavljanje legalne saradnje država u borbi protiv kompjuterskog kriminala, uključujući usklađivanje standarda za kvalitet digitalne forenzičke istrage – pretragu, akviziciju, analizu, prezentaciju i upravljanje digitalnim dokazima. Obično je potrebno da napadač bude na liniji, da bi relativno brzo bio uhvaćen. Neophodna je saradnja telefonskih kompanija i Internet servis provajdera (ISP), kao i zvaničnih istražnih organa specijalne policije, [22].

U generičkoj proceduri otkrivanja traga napadaču sa Interneta, treba sagledati IP adrese u *login* fajlu napadnutog računara i izvorne IP adrese koje su uhvatili mrežni uređaji zaštite – skeneri saobraćaja (*sniferi*), IDS/IPS sistemi i *Firewals*, kao i druge informacije dobijene korišćenjem alata tipa:

- ***ReverseFinger,***
- ***Nslookup,***
- ***TraceRoute*** itd.

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

Za hvatanje napadača sa Interneta i praćenje aktivnosti na napadnutom sistemu, veoma je važno obezbediti što više podataka o *online* ima u posrednim računarima. Nažalost, tih podataka nikada nema dovoljno u log fajlovama. Treba poći od toga da

kompetentan napadač verovatno povremeno uskače u *web* lokacije i ostavlja zamke za upad (tipa trojanca ili *trap doors*) primenom *rutkit* tehnika koje istovremeno prikrivaju njihovo prisustvo, pre nego što kasnije sam preduzme napad u potpuno neodređeno vreme.

U *log* datoteci računara sa Unix platformom treba tražiti, [6]:

Vreme logovanja i izlogovanja, npr., pomoću alata tipa ***Lastlog****;*

- Analizirati anomalije u Lastlog, korišćenjem alata za analizu log fajlova, kao što su npr., Chklastlog;
- Izvorne IP adresa, koje se analizom Syslog ili drugih logova mogu otkriti. Syslog mora biti prethodno konfigurisan za ovaj tip informacija. On može proizvesti neku od nekoliko Messages fajlova. Drugi logovi mogu biti iz TCP wrapers 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 log 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 još uvek 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 wrapera u Telnet servisu može se identifikovati izvor napada. Wrapers 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, međutim, napad ponavlja mogu se svi ovi podaci uhvatiti skenerom za kontrolu mrežnog saobraćaja (sniferom). IDS/IPS se mogu konfigurisati da reaguju alarmom na pakete koji sadrže sumnjive IP adrese; kada se aktiviraju alarmi, snimaju se sve transakcije sa te adrese. Sofisticirani IDS/IPS mogu detaljno snimiti čitav scenario napada (npr., Real Secure IPS, Internet Security Systems). Real Secure softverski alat zavisi od profila napada i identifikuje pokušaje sumnjivih napada; može preduzeti i 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 integritet podataka. 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 napadnute hostove, 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 osnovano obratiti zvaničnom organima istrage kompjuterskog kriminala za dalji tok istrage.

- Za napad u IKT sistem preko telefonske modemske veze, postavljenje zamke za napadača i traganje za njim podrazumeva uključivanje zvaničnih organa istrage. 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 neki brojiz 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 policijske istrage.

Dakle, sistemski log fajlovi obezbeđuju brojne dokaze o upadu u mrežu i host računare. Problem je, međutim, što ovi fajlovi imaju svoja ograničenja, kao što su:

- Mora se na sudu dokazati da log fajl nije izmenjen, da bi imao dokaznu vrednost. Poznato je da log fajlovi mogu biti modifikovani pre otkrivanja od strane digitalnog forenzičara. Ako je log fajl locirana na napadnutoj mašini, tj. može joj pristupiti administrator mreže, ili drugi supervizor, potrebno je dokazati da oni ili drugi superkorisnici sa istim ovlačćenjima nisu upali u log fajl i izmenili ga pre akcije forenzičara. Poznato je, takođe, 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. Takav dokaz može biti pre-konfigurisan log fajl 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. Bezbedan rad log fajla se može osigurati 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 i strogo kontrolisan. Log fajl treba da bude bekapovan na pouzdan disk, ili drugi medijum, koje treba čuvati kao referentne dokaze.
- Drugo ograničenje log fajlova je njihova kompletnost. Koristan log fajl za analizu realizovanih događaja napada treba minimalno da sadrži sledeće podatke: vreme kada se događaj desio, IP adresu izvora događaja i prirodu događaja (bezbednosni događaj - incident, regularan event). Najkompletniji logovi su uvek zahtevni, troše resurse i smanjuju performanse računarskog sistema. Dakle, veličina log fajlova mora biti kompromis između zahteva forenzičke kompletnosti i funkcionalnosti.

Najbolja forenzička praksa preporučuje da log fajlovi registruju sledeće važne informacije:

- sve pristupe superkorisnika,
- sva logovanja pristupa i napuštanja sistema (login i logout),
- pokušaje korišćenja bilo kojeg kontrolisanog servisa (npr. FTP, TELNET, R-servisa itd.),
- pokušaje pristupa kritičnim resursima (fajlu lozinki, kernelu, wrapper-u itd.) i
- detalje o e-mail porukama.

TCP wraperi i drugi programi obično pišu svoje logove u sistemski log fajl u Unix sistemu. U NT Windows OS nema specijalizovanih programa kao **wrappers**, ali *security log* se može konfigurisati tako 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 omogući izrada profila napadača. Da bi se dobile informacije koje se ne pojavljuju u log fajlu, bilo da logovanje nije kompletno, ili uopšte 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 je forenzičar pokupio. Zatim, da ostaci log fajla na HD mogu biti oštećeni, jer *login* program stalno prepisuje stare informacije novim, po principu FIFO (*First in-First out*). Međutim, analizom sektora HD i vremenskih fajlova moguće je potpuno rekonstruisati log fajl.

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[31] log fajlova je da se pronađu razlike u onome što log fajlovi pokazuju i stvarnih događaja. Nažalost, ova analiza je vrlo delikatna i dugotrajna, posebno za velike fajlove, jer je potrebno imati više log fajlova za isti događaj i uporediti istovetnost vremena za iste događaje. Dobro je što obično ima više izvora ovih log fajlova: napadnuti računar koji može imati TTPS program za višestruko, odvojeno logovanje, zatim bezbednosni log, sistemski i aplikativni logovi. Pored toga, potrebno je dobro poznavati predmetni OS. Korisno je napraviti analitičku radnu kartu za sistemske log fajlove u mreži kao u tabeli T. 3.1.

Tabela 3.1 Analitička vremenska radna karta sistemskih log podataka

	Sistemske log datoteke (isti događaj)		
	Log 1	**Log2**	**Log3**
Vremena	15.12.2004 12:30	**15.12.2004 12:35**	15.12.2003 12:30

31 analize podataka iz log fajlova više mrežnih uređaja.

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 standardog logovanja grešaka - pogrešnih ulaza (*entries*) i slika i *urgent log* fajlom, sačinjenim od ulaza deriviranih iz različitih izvora. Bezbednosni log je često kombinacija bezebdnosnih događaja logovanih sa *syslog* fajlovima i onih logovanih sa TTPs[32] bezbednosnim programom. Log grešaka dolazi iz sistemskih *syslog* fajlova, nakon što naprave *urgent* log fajlove. Forenzičar dodaje *wrappers* log fajlove bezbednosnim log fajlovama 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 isti (kritični) događaj. Najbolje rešenje je imati *log host* mašinu u koju treba smestiti sve log fajlove i tu ih kombinovati i analiztirati. Sklapanje (rekonstrukcija) velikih log fajlova sa HD je veliki izazov, ali postoji više dobrih alata, [29]:

- 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.
- Zeitline: forenzički editor vremenske linije događaja, koji se fokusira na korelaciju i rekonstrukciju datuma/vremena događaja nekog incidenta iz različitih izvora u računarskoj mreži. Uvoz i normalizacija podataka o vremenskim pečatima u ovom alatu vrši se pomoću filtera. Filteri se učitavaju dinamički tako da korsinik može sam razviti novi filter, bez potrebe da rekompajlira program. Ovaj alat može pretraživati događaje na bazi ključne reči i/ili zadatog vremenskog opsega događaja. Alat događaje organizuje u hijerarhijsku strukturu, [2].

Kompleksna oblast digitalne forenzike kibernetičkog prostora zahteva detaljniju obradu, što prevazilazi obim ovog udžbenika.

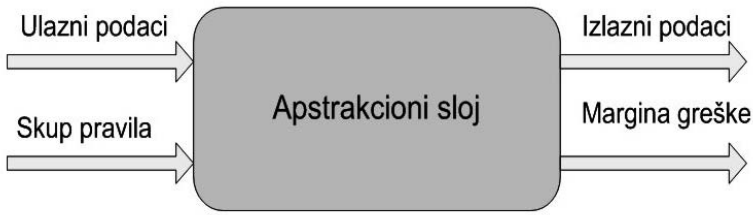
32 *Trusted Third Party* – treća strana od poverenja

3.2 ZNAČAJ SLOJEVA APSTRAKCIJE ZA DIGITALNU FORENZIČKU ANALIZU

Slojevi apstrakcije računarskog sistema koriste se za analizu velike količine podataka u mnogo lakše upravljanom 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, [3].

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 brojčane 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 metapodaci koji se koriste za prevođenje drugih ulaznih podataka. Ulazi i izlazi apstrakcionog sloja ilustrovani su na slici 3.2.



Slika 3.2 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 otkucaja na tastaturi (*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[33] koji predstavljaju fajl. Podaci fajla se zatim primenjuju na aplikativni sloj apstrakcije gde se dalje procesiraju.

Primeri alata za oporavak fragmentiranog fajla (*carving*) na apstrakcionom sloju – *fajla* u fajl sistemu, najbolje prikazuju sve prednosti korišćenja koncepta apstrakcionih slojeva računarskog sistema i mreže za definisanje forenzičkih alata.

3.2.1 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]:

- greška implementacije forenzičkog alata i
- 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 Frensics 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.

33 *Master File Table*

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.

3.2.3 Karakteristike slojeva apstrakcije

Slojevi apstrakcije i alati za njihovo procesiranja mogu se opisati kroz četiri osnovne karakteristike. Greška apstrakcije može se iskoristititi 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. J*edan-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. Teoretski 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[34] i CHS[35] 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.

34 *Logical Block Addressing* binarnih zapisa na HD

35 *Cilinder Heads Sectors* adresiranje binarnih zapisa na HD

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 3.3, [3].

<table>
<tr><th colspan="2">Disk</th><th colspan="3">File system</th><th>Application</th></tr>
<tr><td>Heads</td><td>...</td><td>Boot Sector</td><td>FAT Area</td><td>Data Area</td><td rowspan="2">ASCII</td></tr>
<tr><td colspan="2">LBA Sectors</td><td></td><td>...</td><td>...</td><td rowspan="2">HTML</td></tr>
<tr><td colspan="2"></td><td colspan="3">File</td></tr>
</table>

Slika 3.3 Slojevi apstrakcije HTML dokumenta

Digitalni forenzički alati za svaki sloj apstrakcije takođe se mogu svrstati u različite kategorije. Tipična podela alata je na:

- translacione i
- prezentacione alate.

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 (*entrys*) prema MAC[36] 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.

3.2.4 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, [3], [28]:

36 *Modification Access Change vremena*

But sektor koji sadrži adrese i veličine struktura u ovom specifičnom fajl sistemu, uključujući i lokaciju FAT (*File Allocation Table*) i oblasti podataka;

FAT (File Allocation Table) koja sadrži ulaze (*entrys)* klastera i specificira koji je sledeći alocirani klaster, a koji je nealocirani klaster;

Oblast podataka koja je podeljena na konsekutivne sektore od po 512 bajta, svrstane u klastere od po 2, 4, 8, 16 sektora, zavisno od veličine logičkog diska. Klasteri skladište sadržaj fajla, ili direktorijuma. Svaki klaster ima svoj ulaz (*entry*) kojim se adresira 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 logičkih 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]:
   - startnu lokaciju FAT tabele,
   - veličinu svake FAT tabele,
   - broj FAT tabela,
   - broj sektora po klasteru,
   - lokaciju rut direktorijuma.
2. *sloj apstrakcije* uzima imidž i informaciju o FAT tabeli kao ulazne podatke i daje FAT i oblast pdataka na izlazu. Izlazni podaci iz ovog sloja su sirovi podaci iz *imidža* i nisu struktuirani.
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 klastere kao izlazne podatke. Sadržaj fajlova i direktorijuma uskladišten je u klasterima u oblasti podataka.
5. *sloj apstrakcije* na nivou fajl sistema uzima klastere 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 klastere.

6. *sloj* uzima startni klaster i FAT kao ulazne podatke i generiše punu listu alociranih klastera kao izlazne podatke.
7. *sloj* uzima klastere, entrije direktorijuma i punu listu klastera kao ulazne podatke, a generiše bilo ceo sadržaj fajlova, ili listing dirktorijuma. 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 3.2, [3].

Tabela 3.2 Slojevi apstrakcije FAT fajl sistemu

	Input	**output**
1	File System Image	Booz 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 of Raw Content
6	Starting Cluster, FAT Entries	List of Allocated Clusters
7	All file meta-data, Clusters	All Directory Entries of 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:

- procesira sloj apstrakcije 1 da identifikuje *but* sektor, uključujući lokaciju rut direktorijuma,
- procesira sloj apstrakcije 2 da identifikuje FAT tabelu i oblast podataka,
- procesira sloj apstrakcije 3 da dobije *entrije* u FAT tabeli,
- procesira sloj apstrakcije 4 da dobije klastere za direktorijum,
- koristi lokaciju rut direktorijuma da procesira sloj 6 za identifikaciju svih alociranih klastera i
- 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, optički disk. Analiza ovog sloja uključuje procesiranje standarnih 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 delenje 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 slika).

3.2.5 Zahtevi za alate za digitalnu forenzičku analizu

Na bazi navedenih definicija i ciljeva mogu se generisati sledeći zahtevi za digitalne forenzičke alate, [28]:

- *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.
- *Sveobuhvatnost:* Da bi identifikovali optužujuće i oslobađajuće dokaze, forenzičari moraju imati pristup svim izlaznim podacima na datom sloju apstrakcije.
- *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.

- *Određenost:* Da bi se obezbedila tačnost alata, alat mora uvek proizvesti istu izlaznu vrednost kada se primene iste ulazna vrednost i skup pravila translacije.
- *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 analize, što sud može zahtevati, potrebno je obezbediti refrentnu kopiju ulaznog originala podataka (drugi *imidž* osumnjičenog računara).

3.3 UTICAJ SAKRIVANJA DIGITALNIH DOKAZA NA TEHNIKE FORENZIČKE ANALIZE

Istraživanje je pokazalo da forenzičari najčešće susreću pet sledećih tehnika za sakrivanje podataka, [24]:

- preimenovanje fajla (21%),
- šifrovanje (19%),
- steganografija (12%),
- rutkitovi (9%),
- fajl sistem (5%),
- prenosni medij (5%).

Pored toga svaki anti-forenzički alat kreira različit operativni otisak na fajl sistemu. Ovaj otisak uključuje način na koji alat preimenuje fajlove koji se brišu i log fajlove koje alat generiše. Zato je moguće dizajnirati forenzički uslužni alat koji automatski skenira ove potpise fajlova u sistemu i otkriva da li je alat za preimenovanje fajlova korišćen. U toku je razvoj ovakvog alata.

Potreba za alatom koji automatski otkriva potpise anti-forenzičkih programa otvara pitanja detekcije Trojanaca i tzv. „odbrane trojancima“ pred sudom. Naime, ako je osumnjičeni (ispitivani) računar napadnut Trojancem, onda osumnjičeni može osnovano tvrditi da je njegov računar korumpiran i da ilegalne aktivnosti nisu njegovo delo, nego anonimnog napadača. Tako ostaje dilema da li tužilac treba da dokaže da Trojanac nije uključen u slučaj, ili odbrana – da jeste uključen.

Za ovakve slučajeve mogu biti korisni neki alati koji vrše komparativnu analizu sadržaja. Jedan primer je prezentacija različitih atributa blokova (klastera) diska u bojama da se vidi da li se javlja neki vizuelni obrazac koji upućuje na maliciozni kod. Forenzički alat **Lazarus** u **Coroner Toolkit**-u radi ovo u izvesnom stepenu, ali je kategorizacija podataka prilično uopštena. Takođe se može koristiti forenzički alat **Starlight**[37] za modelovanje i vizuelizaciju podataka fajl sistema. Drugi primer je da se generiše alat za komparaciju sa generičkom specifikacijom, kao što je, na primer, JPEG specifikacija, kojim se može otkriti povreda specifikacije i na primer sakrivena pornografska slika pod imenom word dokumenta (sa ekstenzijom .docx). Ovaj pristup obuhvata promenu *sintakse*, tj. povrede protokola za ugrađivanje informacije korupcijom FCT (*File Control Table*) tabele u slici, nasuprot steganografske semantike, nečeg ugrađenog u sadržaj gde, na primer, neka slika čuva jedan znak sa kodiranom informacijom na sebi.

Istraživanja pokazuju da u procesu forenzičke analize postoje faktori koji utiču da se analiza digitalnih dokaza najčešće vrši duže od očekivanih rokova postavljenih od strane tužioca/odbrane. Glavnih sedam faktora, koji čine proces forenzičke analize vremenski zahtevnim, su, [24]:

1. Veličina podataka (25%);
2. Loše planiranje procesa analize (10%);
3. Nedovoljna automatizacija (7%);
4. Ulazno/izlazni protok podataka (7%);
5. Ograničeni ljudski i tehnički resursi (7%);
6. Dugo vreme uzimanja imidža diska (5%);
7. Ograničenje forenzičkih alata (5%).

Ista istraživanja su potvrdila da su sledeći faktori najveći nedostatak forenzičkih (alata) kapaciteta za analizu podataka:

1. Brzina procesiranja (14%);
2. Automatizacija procesiranja (12%);
3. Redukcija podataka za analizu (4%);
4. Šifrovanje (4%);
5. Veliki kapacitet diskova/particija (4%);
6. Osposobljenost za analizu (4%).

Perspektivna forenzička tehnika za povećanje ukupne efektivnosti i efikasnosti forenzičke istrage je *transparentna metodologija za selektivnu akviziciju*, koja omogućava ukupno smanjenje vremena potrebnog za akviziciju i analizu podataka, pomeranjem procesa filtracije sa procesa analize na sakupljanje (akviziciju) podataka. Ovo filtriranje je već delimično izvršeno u fizičkoj forenzičkoj istrazi i otkrivanju e-dokaza upada u sistem. Ovaj način sakupljanja podataka će značajno promeniti tekuće forenzičke tehnike, kada vreme i troškovi forenzičkih resursa postanu preveliki za upravljanje.

37 http://starlight.pnl.gov

Bitan razlog za pomeranje fokusa metodologije akvizicije podataka je i činjenica da uzimanje fizičke slike (imidža) diskova sve više postaje legalni i finansijski rizik. Cilj tekućih istraživanja je da se formalizuje jedna apstraktna metodologija koju može koristiti celokupna forenzička zajednica u svetu. Ova bi metodologija uključivala identifikaciju dokaza na mestu krivičnog dela kompjuterskog kriminala i selektivnu ekstrakciju iz aktivnih („živih“) i statičkih (isključenih) računarskih sistema, dok je proces uzimanje imidža i analiza potskupa informacija rezervisan samo za specifične situacije. Moguć je legalni problem u ovoj metodologiji gde odbrana može tvrditi da su propušteni potencijalno oslobađajući (*exculpatory)* dokazi. Nova metodologija može koristiti analogiju modela e-otkrivanja koristeći rentabilan okvir i koncept „sličnosti“ heš vrednosti poznatih fajlova sistemskih i aplikativnih programa sa ispitivanim fajlovima.

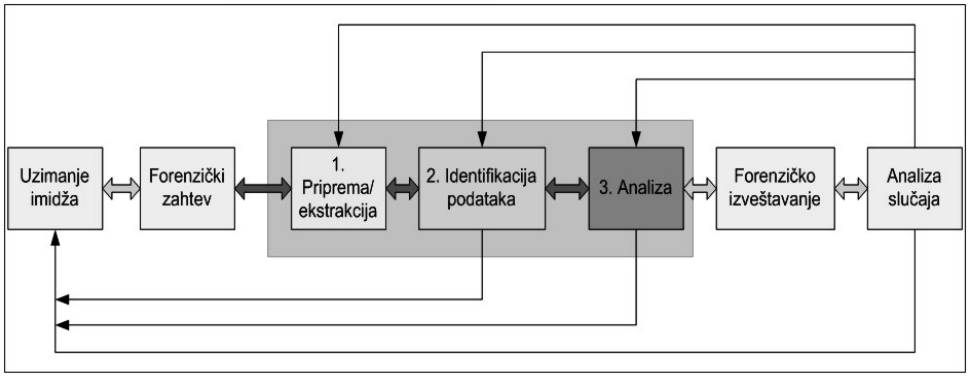
3.4 PROCES FORENZIČKE ANALIZE ČVRSTOG DISKA

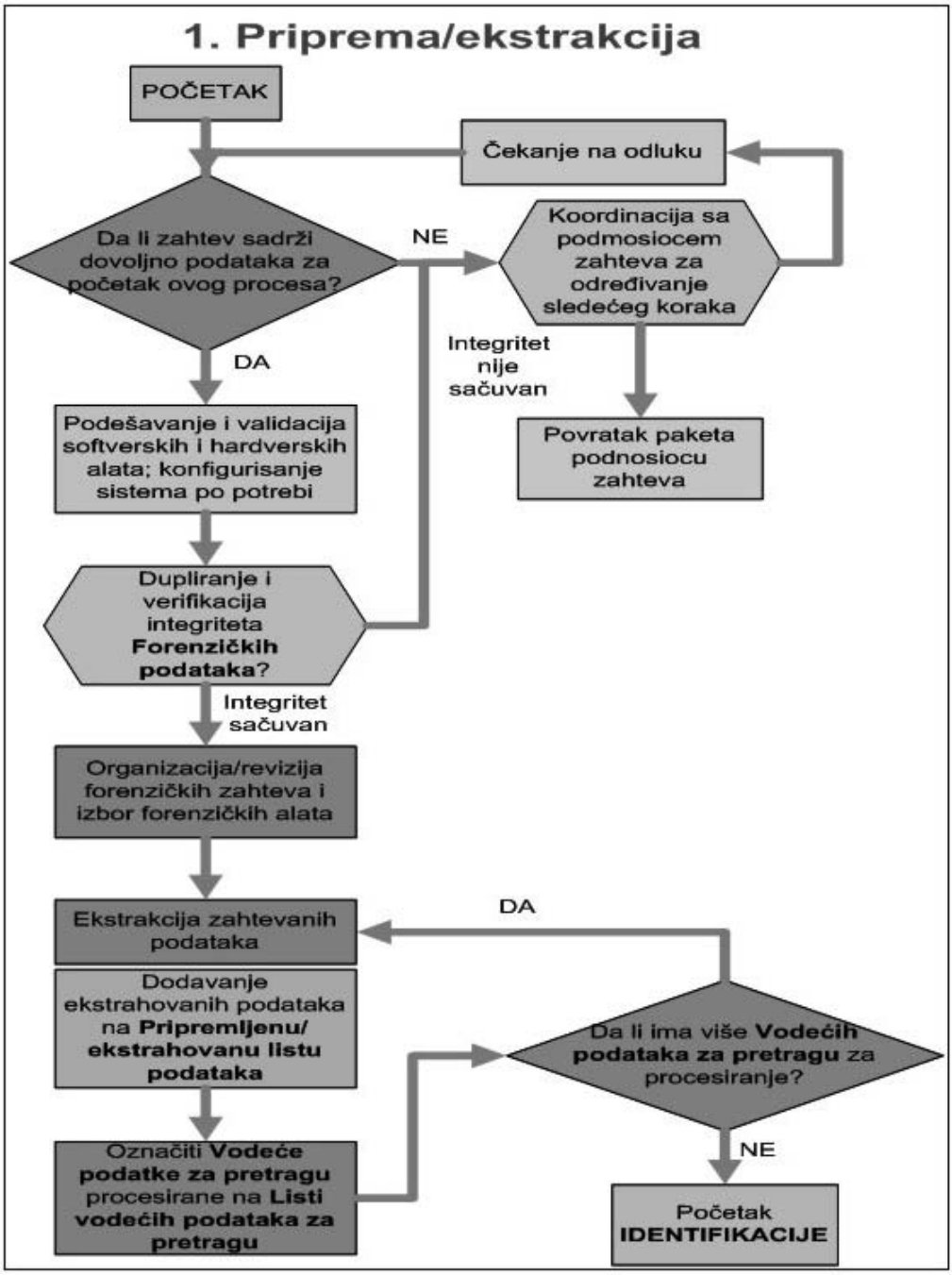
Poznato je da su gotovo sva forenzička ispitivanja računarskih medija međusobno različita i da se svaki ne može voditi na isti način zbog brojnih razloga. Ovu proceduru forenzičkog ispitivanja čvrstog diska preporučuje međunarodna asocijacija specijalista za istragu kompjuterskih dokaza – IACIS (*International Association of Computer Investigation Specialist*) sa ciljem da promoviše i standardizuje proces forenzičke akvizicije i analize (ispitivanje) kompjuterskih digitalnih dokaza.

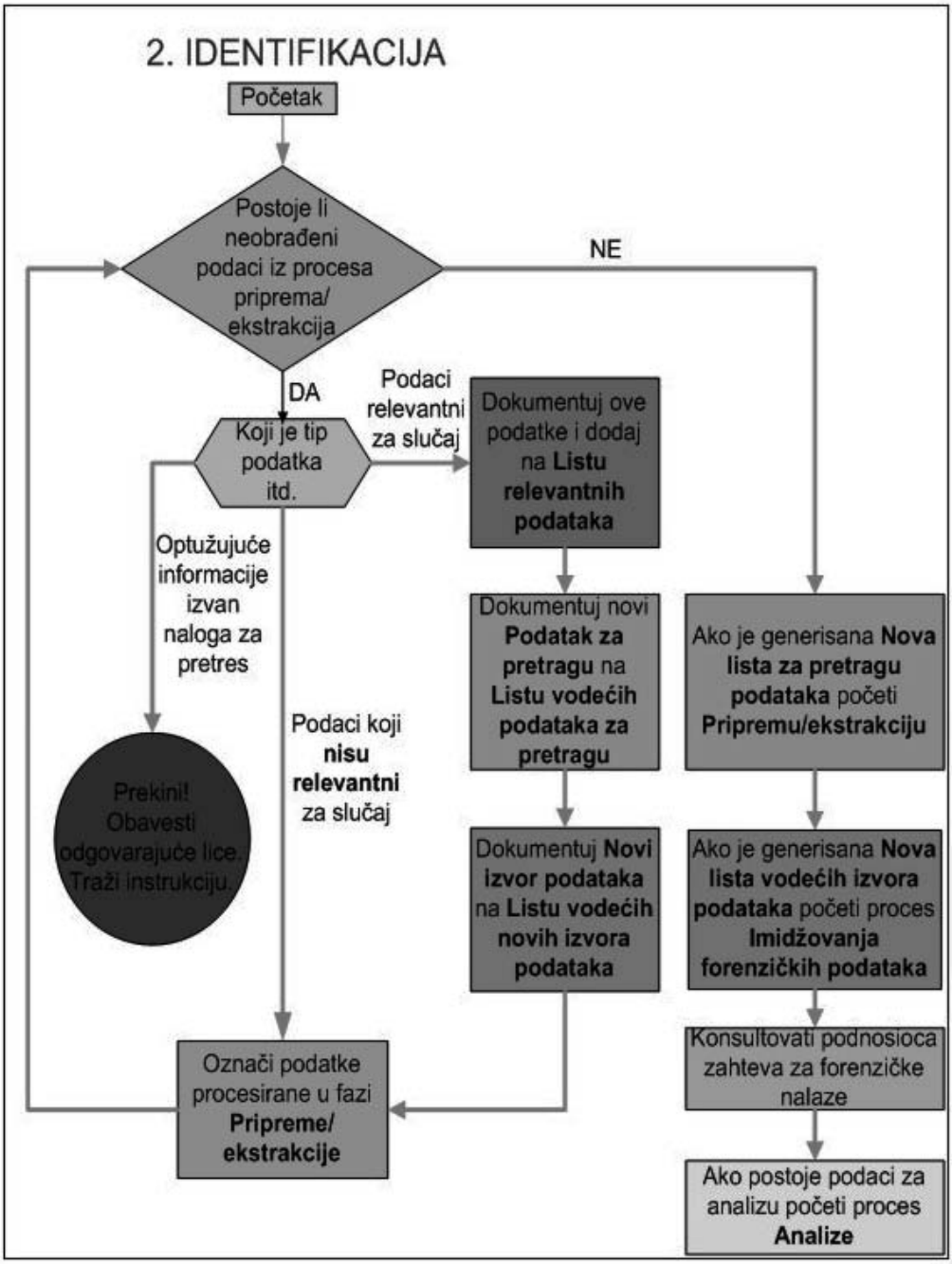
- Glavni zahtevi za digitalnu forenzičku akviziciju i analizu:
- *Moraju* se koristiti forenzički sterilni mediji za ispitivanje.
- Ispitivanje *mora* sačuvati integritet originalnih medija.
- Štampani materijal, kopije podataka i drugi artefakti koji su rezultat ispitivanja *moraju* biti propisno označeni, kontrolisani i prenošeni.

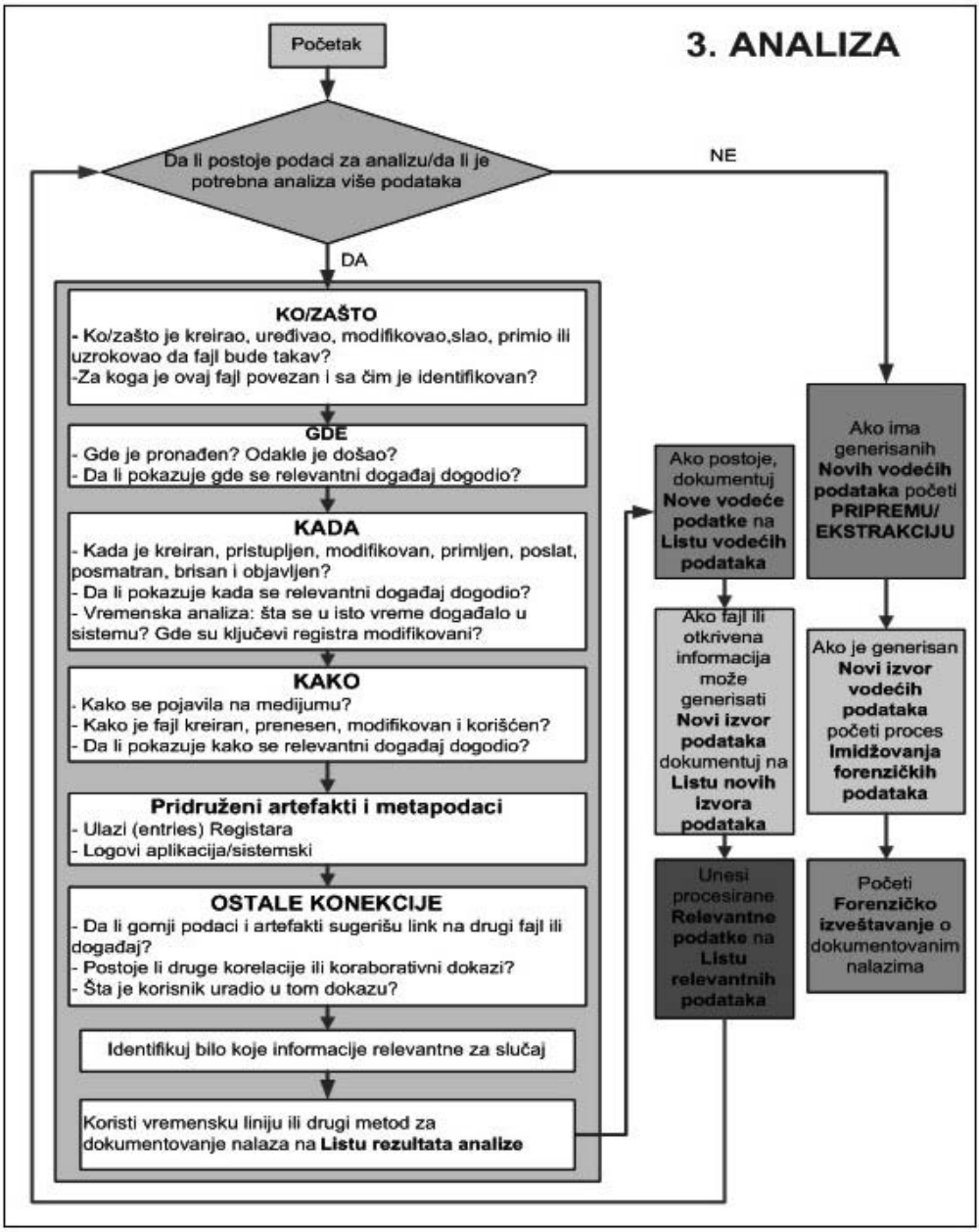
3.4.1 Tok procesa digitalne forenzičke analize

Dijagrami toka procesa digitalne forenzičke analize prikazani su na slici 3.4.




1. Priprema/ekstrakcija
POČETAK
Čekanje na odluku
Da li zahtev sadrži dovoljno podataka za početak ovog procesa?
NE
Koordinacija sa podmosiocem zahteva za određivanje sledećeg koraka
Integritet nije sačuvan
Povratak paketa podnosiocu zahteva
DA
Podešavanje i validacija softverskih i hardverskih alata; konfigurisanje sistema po potrebi
Dupliranje i verifikacija integriteta **Forenzičkih podataka**?
Integritet sačuvan
Organizacija/revizija forenzičkih zahteva i izbor forenzičkih alata
Ekstrakcija zahtevanih podataka
DA
Dodavanje ekstrahovanih podataka na **Pripremljenu/ ekstrahovanu listu podataka**
Da li ima više **Vodećih podataka za pretragu** za procesiranje?
Označiti **Vodeće podatke za pretragu** procesirane na **Listi vodećih podataka za pretragu**
NE
Početak **IDENTIFIKACIJE**


2. IDENTIFIKACIJA
Početak
Postoje li neobrađeni podaci iz procesa priprema/ ekstrakcija
NE
DA
Podaci relevantni za slučaj
Koji je tip podatka itd.
Dokumentuj ove podatke i dodaj na **Listu relevantnih podataka**
Optužujuće informacije izvan naloga za pretres
Podaci koji **nisu relevantni** za slučaj
Prekini! Obavesti odgovarajuće lice. Traži instrukciju.
Dokumentuj novi **Podatak za pretragu** na **Listu vodećih podataka za pretragu**
Ako je generisana **Nova lista za pretragu podataka** početi **Pripremu/ekstrakciju**
Dokumentuj **Novi izvor podataka** na **Listu vodećih novih izvora podataka**
Ako je generisana **Nova lista vodećih izvora podataka** početi proces **Imidžovanja forenzičkih podataka**
Označi podatke procesirane u fazi **Pripreme/ ekstrakcije**
Konsultovati podnosioca zahteva za forenzičke nalaze
Ako postoje podaci za analizu početi proces **Analize**



Slika 3.4 Tok procesa digitalne forenzičke analize

Dokumentacija procesa digitalne forenzička analize vodi se u listama prikazanim u tabeli 3.3.

Tabela 3.3 Primeri dokumentovanja procesa digitalne forenzičke analize

Lista vodećih podataka za istragu	
Vodeći podaci za istragu	**Primedbe/zabeleške/poruke**
Generalno ovo uključuje otvaranje fajla slučaja u izabranom alatu i unos forenzičkog imidža u fajl. Ovo može takođe uključiti re-kreiranje mrežnog okruženja ili baze podataka za simulaciju originalnog okruženja. Primeri vodećih podataka za istragu: • Identifikacija i ekstrakcija svih e-mail poruka i izbrisanih fajlova • Pretraga medija za dokaze dečije pornografije • Konfigurisanje i učitavanje imidža baze podataka za *data minig* • Oporavak svih izbrisanih fajlova i indeksa diskova/particija za reviziju od strane forenzičara na slučaju	Ova se sekcija koristi po potrebi: Primer zabeleške: • Obavezno notirati ime forenzičara na slučaju klada se istraga/ispitivanje završi

Lista ekstrahovanih podataka	
Pripremljeni/ekstrahovani podaci	**Primedbe/zabeleške/poruke**
Lista pripremljenih/ekstrahovanih podataka je lista stavki koje su pripremljene ili ekstrahovane za identifikaciju dokazujućih podataka za forenzički slučaj/zahtev. Primeri pripremljenih/ekstrahovanih podataka: • Imidž HD procesiran pomoću FTK ili EnCase forenzičkog alata za trijažu podataka od strane forenzičara istrage • Eksportovani fajlovi registara i instaliran alat *Registry viewer* za forenzičku analizu registara • Učitani fajlovi imidža baze podataka na DB server i spremni za istraživanje podataka (*data minig)* • Oporavak svih izbrisanih fajlova i indeksa diskova/particija za reviziju od strane forenzičara na slučaju	Ova se sekcija koristi po potrebi: Primer zabeleške: • Brojni fajlovi locirani u c:\movies direktorijumu imaju .avi ekstenziju, a u stvari su Excel tabele.

Lista relevantnih podataka	
Relevantni podaci	**Primedbe/zabeleške/poruke**
relevantnih podataka je lista podataka koji su relevantni za forenzički slučaj/zahtev. Primer relevantnih podataka: • Ako forenzički slučaj otkriva podatke o falsifikovanju i prevari sa kreditnim karticama, svi podaci koji se odnose na brojeve kreditnih kartica, slike, e-mail diskusije o izradi kreditnih kartica, vreme i datum pretrage za programima za izradu brojeva kreditnih kartica, relevantni su podaci za slučaj	Ova se sekcija koristi po potrebi: Primer zabeleške: • Prilog u Outlook .pst>poruka5 ima virus u sebi. Proverite sa AVP pre slanja ili otvaranja poruke • Identifikovano i oporavljeno 12 e-mail poruka koje detaljno opisuju plan izvršenja krivičnog dela kompjuterskog kriminala

Lista novih izvora vodećih podataka	
Novi izvori vodećih podataka	**Primedbe/zabeleške/poruke**
Lista novih izvora vodećih podataka je lista podataka koje treba izvući za koraborativnu potvrdu postojećih dokaza ili dalju istragu. Primeri novih izvora vodećih podataka: • E-mail adresa: jdole@gmail.com • Log fajlovi sa FTP servera • Pretplatnička informacija za neku IP adresu • Log informacije za transakciju iz servera	Ova se sekcija koristi po potrebi: Primer zabeleške: • U toku forenzičke analize HD subjekta J. Đorđa osumnjičenog za prevare sa kreditnim karticama, otkrivena je e-mail poruka da je J. Đorđe tražio od B. J. da se isplata izvrši sa mašine za štampanje kreditnih kartica.

Analiza rezultata	
Analiza rezultata	**Komentari/zabeleške/poruke**
Lista značajnih podataka koji daju odgovore na forenzička pitanja: *ko, šta, kada, gde i kako*? Primer rezultata analize: • 1. *Windows\$NtUninstallKB887472$\10dat \data\sendbox.dbx\message5.eml \Special Tools\stegano.exe • 3. 1/**04**/09 1/**05**/09 - modifikovana i poslata slika licu X.Y.	Ova se sekcija koristi po potrebi Primer zabeleške: 1. *10.data, 5 e-mail poruka i stegano.exe* pokazuju da osumnjičeni koristi steganografski alat da sakrije 10$ sliku u 10.dat u 11.03h, 1/04/09 i da je poslao licu … u 11.10h 1/05/09

3.4.2 IACIS procedura kompletnog ispitivanja čvrstog diska

1. Uspostaviti forenzički sterilne uslove. Sveže pripremiti sve korišćene medijume u toku procesa ispitivanja, potpuno izbrisati m(prepisivanjem) sve nebitne podatke, skenirati na viruse i verifikovati pre svake upotrebe.
2. Koristiti samo licencirane softvere ili autorizovane za upotrebu od strane ovlašćenog forenzičara ili zvanične državne agencije.
3. Fizički ispitati originalni računar, napraviti specifične zabeleške i opisati hardver. U komentarima navesti sve ono što je otkriveno neuobičajeno u fizičkom ispitivanju računara.
4. Preduzeti sve hardversko/softverske mere predostrožnosti u toku svakog pristupa ili kopiranja originalnih medija, da se spreči prenošenje virusa, destruktivnih programa ili drugih nepotrebnih zapisa na/sa originalnih medija. Poznato je da zbog ograničenja hardvera i operativnog sistema ovo uvek neće biti moguće.
5. Proveriti sadržaj CMOS, kao i internog takta i registrovati korektnost datuma i vremena. Vreme i datum internog takta je često vrlo značajno za utvrđivanje vremena i datuma kreiranja i modifikacije ispitivanog fajla.
6. Napraviti bit-po-bit (fizičku, miror, imidž) kopiju originalnog diska, pošto se originalni mediji obično ne koriste za stvarno ispitivanje. Detaljno dokumentovati i opisati proces kopiranja i identifikacije hardvera, softvera i medija.
7. Ispitati logičke particije kopije (klona ili imidža) originalnog čvrstog diska, dokumentovati i opisati šta je otkriveno.
8. Ispitati i dokumentovati podatke iz but rekorda, korisnički definisane konfiguracije sistema i fajlova operativnih komandi kao što su CONFIG.SYS i AUTOEXEC.BAT u FAT faj sistemima.
9. Restaurirati sve izbrisane fajlove koji se mogu oporaviti. Gde je praktično i moguće sve prve karaktere restauriranih fajlova promeniti sa HEX E5 u, na primer, „-„ ili neko jedinstven karakter, za identifikacione potrebe.
10. Napraviti spisak (listing) svih fajlova, koje sadrži ispitivani medijum, bez obzira da li sadrži potencijalne dokaze ili ne.
11. Ako je pogodno (nije prevelika količina materijala, nema vremenskih i drugih ograničenja) ispitati *fajl slack* prostore svakog fajla na izgubljene ili skrivene podatke.
12. Ako je pogodno (nije prevelika količina materijala, nema vremenskih i drugih ograničenja) ispitati sve *nealocirane* prostore svakog fajla na prisustvo izgubljenih ili skrivene podatke.
13. Ispitati sadržaje svakog fajla korisničkih podataka u rut direktorijumu i svakom folderu (ako postoji).

14. Otvoriti i ispitati sve fajlove zaštićene lozinkom.
15. Za sve odgovarajuće dokazujuće digitalne podatke obezbediti elektronsku ili štampanu kopiju. Na svakom materijalu (štampanom, elektronskom) označiti fajl u kome se nalaze dokazujući podaci. Označiti sve materijalne dokaze, sekvencijalno numerisati i propisno obezbediti i prenositi.
16. Ispitati sve izvršne programe (*executables*) od specifičnog interesa. Fajlovi korisničkih podataka kojima se ne može pristupiti na drugi način treba ispitati ovaj put koristeći prirodne aplikacije ispitivanog računara.
17. Propisno dokumentovati sve komentare i nalaze.

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

REZIME

Forenzička analiza digitalnih podataka, prema izvoru podataka, generalno se deli na forenzičku analizu *softvera*, *računara* i *kibernetičkog prostora* i *računarske mreže*.

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

Forenzička *analiza računara,* najobimniji deo digitalne forenzike, je aplikacija ispitivanja računara i tehnika analize u cilju određivanja potencijalno legalnih dokaza, generisanih, ili uskladištenih u računaru. U slučaju virtuelnih mašina na osumnjičenom računaru, iskustva iz forenzičke prakse pokazala su ograničenja virtuelnog okruženja (*VMWare*, 2007), kao i da se klasičan metod akvizicije i analize digitalnih podataka ne može automatski primeniti. Predložen je novi pristup u kojem se konvencionalno i virtuelno okruženje procesiraju nezavisno čime se skraćuje vreme analize i može se koristi manje kvalifikovano osoblje za forenzičku analizu.

Forenzička analizu kibernetičkog prostora je najkompleksnija oblast digitalne forenzike i može biti veoma spor proces. Osnovni zahtevi su uspostavljanje legalne saradnje država i usklađivanje standarda kvaliteta – pretrage, akvizicije, analize, prezentacije i upravljanja digitalnim dokazima. Za hvatanje napadača sa Interneta i praćenje aktivnosti na napadnutom sistemu, važno je obezbediti što više podataka o *online* logovanju. Ako se napad ponavlja mogu se svi ovi podaci uhvatiti sa mrežnim skenerom (*sniferom*). Kako postoje efikasni hakerski alati za izmenu log fajla, preduzima se tehnika multiplikativne analize log fajlova iz više mrežnih uređaja u cilju otkrivanja razlika u vremenskoj liniji zapisa u log fajlovima i stvarnih događaja.

Slojevi apstrakcije računarskog sistema koriste se za analizu velike količine podataka u mnogo lakše upravljanom formatu i za izradu forenzičkih alata za apstrakcioni sloj, na primer ASCII. Svaki sloj apstrakcije može uneti grešku implementacije forenzičkog alata i grešku sloja apstrakcije. Margina greške je izlazna vrednost svakog sloja apstrakcije. Generalno, greške koje unose slojevi apstrakcije rezultat su zbirnih grešaka koje unosi svaki sloj apstrakcije. Problem se rešava proračunom margine greške za svaki sloj i uračunavanjem ove greške u analizi rezultirajućih podataka. Digitalni forenzički alati za svaki sloj apstrakcije mogu se svrstati u kategoriju *translacionih alata,* za prevođenje sa jednog sloja apstrakcije na drugi, ili *prezentacionih alata*, za prikazivanje podataka na pogodan način za forenzičara. Ova dva tipa alata ne treba razdvajati i u većini slučajeva nisu razdvojeni u savremenim alatima (**FTK, EnCase, iLook** itd.). Osnovni zahtevi za alate za digitalnu forenzičku analizu su *korisnost, sveobuhvatnost, određenost, poverljivost i zaštitu od upisivanja*.

Sa aspekta apstrakcionih slojeva, *kompjuterska forenzika* obuhvata analizu *fizičkih medija, menadžmenta medija, sistema fajlova* ***i*** *aplikativnog sloja apstrakcije* računarskog sistema; predstavlja analizu ostataka kompjuterskog incidenta korumpiranog računara, pomoću skupa tehnika analognih 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. Digitalni forenzički alati za svaki sloj apstrakcije mogu se svrstati u kategoriju *translacionih alata,* za prevođenje sa jednog sloja apstrakcije na drugi, ili *prezentacionih alata*, za prikazivanje podataka na pogodan način za forenzičara. Ova dva tipa alata ne treba razdvajati i u većini slučajeva nisu razdvojeni u savremenim alatima (**FTK, EnCase, iLook** itd.). Osnovni zahtevi za alate za digitalnu forenzičku analizu su *korisnost, sveobuhvatnost, određenost, poverljivost i zaštitu od upisivanja*.

Na proces digitalne forenzičke analize mogu uticati razne antiforenzičke aktivnosti, od kojih se najčešće susreću: preimenovanje fajla (21%), šifrovanje (19%), steganografija (12%), rutkitovi (9%), fajl sistem (5%), prenosni medij (5%). Za čestu odbranu osumnjičenog pred sudom da mu je računar kompromitovan i da on nije počinio krivično delo (tzv. „odbrana Trojancem“), mogu se koristiti forenzički alati koji vrše komparativnu analizu sadržaja.

Proces digitalne forenzičke analize obuhvata tri ključne faze: pripremu i ekstrakciju podataka, identifikaciju relevantnih podataka i analizu i izgradnju čvrstog digitalnog dokaza. Sve aktivnosti analize dokumentuju se za potrebe forenzičkog izveštavanja i prezentacije dokaza.

PITANJA ZA PONAVLJANJE

1. Definišite pojam kompromitovanog računara.
2. Koje su tri glavne oblasti forenzičke analize digitalnih podataka?
3. Zašto je forenzička analiza softvera najzahtevniji i najkompleksniji zadatak?
4. Navedite neka ključna pitanja koja forenzičar mora razmatrati u proceduri otkrivanja traga napadaču sa Interneta.
5. Navedite dva osnovna tipa grešaka koje mogu uneti slojevi apstrakcije.
6. U koje dve osnovne kategorije mogu da se svrstaju digitalni forenzički alati za svaki sloj apstrakcije?
7. Navedite šest osnovnih zahteva za alate za digitalnu forenzičku analizu.
8. Koliko slojeva apstrakcije ima FAT fajl sistem?
9. Šta predstavlja četvrti sloj apstrakcije FAT fajl sistema?
10. Kako se može definisati kompjuterska forenzika sa aspekta apstrakcionih slojeva?
11. Koja četiri glavna apstrakciona sloja računarskog sistema obuhvata kompjuterska forenzička analiza?

4.FORENZIČKI ALATI

4.1 RAZVOJ FORENZIČKIH ALATA

Evolucija alata za digitalnu forenzičku istragu - akviziciju i analizu, [27]:

- Prvi alati su malo pomagali u ispitivanju privremeno oduzetih računara i to na nivou heksadecimalnog zapisa;
- U 1990-tim na raspolaganju su specijalizovani forenzički alati:
  - **DD** (Unix) za kopiranje i konverziju sirovih digitalnih podataka na niskom nivou;
  - **Safeback** za uzimanje imidža diska, razvijen za **IRS;**
  - **EnCase,** set forenzičkih alata sa GUI i interfejsom komandne linije;
  - **Sleuthkit** kolekcija alata baziranih na Unix i Windows platformama
- Mrežni alati, ali ne specifično za digitalnu forenziku u periodu od 2002-2003:
  - **Carnivore**[38] (FBI) korisnički prilagodljiv snifer paketa koji može monitorisati sav Internet saobraćaj ciljnog korisnika);
  - **Carnivore** i nova verzija DCS-1000, nisu korišćeni u FBI. FBI je koristio nepoznati komercijalni proizvod za nadgledanje Interneta 30 puta u istragama u tom periodu.
- Glavni problemi sa forenzičkim alatima su:
  - bagovi u softveru,
  - promene u OS i hardveru računara,
  - kompleksnost,
  - nedostatak standarda i razvoj standarda,
  - alati sa otvorenim izvornim kodom,
  - počelo testiranje forenzičkih alata.
- Istraživanje i iskustva iz prakse potvrdila su da su najveći nedostaci savremenih forenzičkih alata:
  - bagovi (15%),
  - nedostatak standarda (10%),
  - interoperabilnost (8%),
  - automatizacija (6%) i
  - formalno testiranje (4%).

38 *Carnivore software,* http://www.securityfocus.com/news/10307).

4.2 OPŠTE KARAKTERISTIKE

Za opremanje digitalne forenzičke laboratorije za terenske i stacionarne uslove rada, treba odrediti koji su alati najfleksibilniji, najpouzdaniji i najrentabilniji za obavljanje poslova forenzičke akvizcije i analize digitalnih dokaza. Jedan od zahteva je da softverski forenzički alati moraju biti kompatibilni najmanje sa sledećom generacijom OS. Na primer, uvođenjem NTFS faj sistema u Windows NT OS, forenzičari su imali velike probleme zbog slabog poznavanja strukture i funkcionalnosti NTFS fajl sistema. Proizvođači forenzičkih softverskih alata morali su revidirati svoje alate za analizu novog fajl sistema, [28].

Uspostavljanje i održavanje digitalne forenzičke laboratorije ukjlučuje i formiranje sofverske biblioteke – repozitorijuma, koji sadrži sve starije verzije forenzičkih alata, OS i drugih programa, kao što su stare verzije Windows i Linux OS. Ako nova verzija forenzičkog sofverskog alata fiksira jedan bag, ali unese drugi, forenzičar može koristiti prethodnu stabilni (fiksiranu) verziju istog alata.

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 koristitit alate sa komandnom linijom, ili GUI interfejsom.

Primer kolekcije forenzičkih alata može se naći na **The@tstake Sleuth Kit** (**TASK**), gde je na raspolaganju besplatan alat **IBM Public Licence Version 1.0**, baziran na starom alatu **The Coroners Toolkit (TCT**), prvom setu alata na raspolaganju forenzičarima. Ovaj set alata se delimično sastoji od komandne linije Unix komandi, kao što je fajl koji pokušava da odredi vrstu fajla na bazi inicijalnog dela fajla (hedera), [7].

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, pre nego neki univerzalni alat koji između ostalog analizira i ove podatke, zato što su strogo namenski alati pouzdaniji za tu konkretnu funkciju. Sa druge strane, forenzičar koji poseduje višenamenski skup alata, na primer tipa **FTK**, koji omogućava obavljanje više različitih zadataka forenzičke istrage, može brže i konfornije sa jednim alatom završiti sve raznovrsne zadatke. Razumno rešenje je da forenzičar za terenski rad obezbedi rentabilan skup alata koji izvršava što veći broj tipičnih forenzičkih zadataka, sa određenim specijalizovanim alatima koji brže i tačnije izvršavaju datu funkciju. Pre nabavke forenzičkog softvera i donošenja odluke, treba evaluirati najmanje sledeće karakteristike potencijalnih alata, [6]:

- 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,
- reputaciju proizvođača alata i dr.

4.2.1 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 podatataka na originalnom disku. Generalno, alati za akvizicija digitalnih podataka, vrše sledeće funkcije, [5], [28]:

- kopiranje podataka sa fizičkog diska,
- kopiranje podataka sa logičkog diska/particija,
- formatiranje akvizicijskih podataka,
- akvizija 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), da ima 12 V konektor za napajanje i IDE ili SCSI kabl za povezivanje. Windows aplikacija **EnCase** alata zahteva upotrebu hardverskog *blokatora upisivanja* podataka na originalni disk, kao što je **FastBloc** za sprečavanje Windows OS da pristupi i korumpira originalni disk u procesu akvizicije.

U procesu akvizicije podataka softverskim alatima postoje dva metoda kopiranja:

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

Većina softverskih alata za akviziciju uključuje jednu ili obe ove funkcije. Formati koji su na raspolaganju za akviziciju diskova variraju od potpuno sirovih podataka u binarnom zapisu do kompresovanih podataka specifičnih za proizvode. Sirovi podaci

su direktna kopija diska. Primer imidža sirovih podataka je izlaz UNIX i Linux šel **DD** komandne linije. Primer formata sirovih podataka je jednostavna bit-po-bit kopija fajla podataka, particije diska, ili celog diska. Alat za akviziciju sirovih podataka može kopirati podatke sa jednog diska na drugi disk, ili u jedan ili više segmentiranih fajlova podataka. Pošto je ovo zaista neizmenjena kopija, forenzičar može gledati sadržaj sirovih podataka imidža fajla sa *heksadecimalnim editorom* kao što su **HexWorkshop** ili **WinHex**. Heksadecimalni editori, poznatiji kao *diskeditori*, kao što je **Northon DiskEdit,** obezbeđuju čitanje podataka u heksadecimalnom zapisu i otvorenom tekstu, (slika 4.1)



Slika 4.1 Primer prozora u WinHex alatu Northon Commander-a

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 smanji ukupan obim i da se forenzički relevantni 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 alati za uzimanje imidža diska tipa **FRED** (*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 protreban 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 sa aktivnog računarskog sistema (u radu), udaljenim pristupom preko računarske mreže i transportovati ih u forenzički server zaštićenim kanalom.

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 za zaštitu integriteta imidžovanih podataka.

4.2.2 Validacija i diskriminacija podataka

Validacija i diskriminacija podataka elementarni su procesi u radu sa digitalnim podacima. Osnovne funkcije procesa validacije i diskriminacije podataka su, [29]:

- heširanje,
- filtracija i
- analiza hedera fajlova.

Proces validacije obezbeđuje integritet kopiranih podataka i omogućava njihovu diskriminaciju na *dokazujuće* i *nedokazujuće* podatke. Validacija podataka obezbeđuje se uzimanjem heš vrednosti (sažetka) sa 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 čvrstih digitalnih dokaza. Namenjen je za filtriranje - uklanjanje standardnih *dobrih* podataka od sumnjivih podataka. U *dobre* podatke spadaju poznati fajlovi kao što su sistemski (OS) i uobičajenih aplikativnih programa (*MS Word, Adobe* i slika). Većina forenzičkih alata obezbeđuje tri metoda diskriminacije podataka:

- Nekoliko softverskih forenzičkih alata mogu integrisati skup heš vrednosti poznatih fajlova. Ovi alati upoređuju poznate fajlove sa istim na osumnjičenom disku i ako se ne poklapaju upozoravaju forenzičara da je fajl sumnjiv. Na ovaj način alat može značajno smanjiti količinu podataka za analizu i izvlačenje dokaza. Izmenjeni fajl sa velikom veovatnoćom sadrži skriveni ilegalni podatak (sliku) ili maliciozni kod.
- Drugi metod za diskriminaciju podataka je analiza i verifikacija informacija iz hedera svih tipova poznatih fajlova. Na primer oznaka JFIF ugrađena je ispred svih JPEG fajlova.
- Treća grupa alata omogućava dodavanje jedinstvenih heš vrednosti podataka hedera u bazu podataka alata, što poboljšava funkciju diskriminacije u fazi

analize. Pretraživanjem i upoređivanjem heš vrednosti hedera alata mogu se locirati fajlovi koji su namerno izmenjeni ili zaraženi malicioznim programima. Ova funkcija može se koristiti i za lociranje skrivenih fajlova na disku/particiji.

4.2.3 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 digitalnih podataka*. Proces ekstrakcije digitalnih podataka obuhvata više koraka, [29]:

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

Pregled i opservacija podataka: Većina forenzičkih alata obezbeđuje funkciju posmatranja podataka, a kako se i u kojem formatu podaci vide, zavisi od alata. Forenzički alat **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 pregleda i 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, dobijenih u fazo predistražnog postupka. 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, kao na primer, **FTK** alat koji koristi binarno indeksiranje (pravi tzv. *b-stablo*) sa *dtSearch* funkcijom. Ova funkcija obezbeđuje trenutno pronalaženje ključne reči i znatno ubrzava proces analize.

Dekompresija podataka: **FTK** alat takođe može dekompresovati arhivirane 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. I ovaj alat kreira fajl *b-stabla* indeksa koji se može gledati po kompletiranju pretraživanja sa ključnom reči.

Rekonstrukcija fragmenata fajlova izbrisanih 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 hedera 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 referentnu 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 Service*) provajdra proizvoda zaštite – *PGP* ili *GnuPG*. Sa aspekta forenzičara, šifrovani fajlovi i sistemi su problem. Mnogi forenzički alati tipa **FTK** za oporavak lozinke mogu generisati potencijalnu listu za *napad rečnikom* na lozinku. Postoji izvesna šansa da je lozinka upisana u privremeni (*temporary*) fajl, ili sistemski fajl na osumnjičenom disku, kao što je *Pagefile.sys*. **FTK** alat generiše listu lozinki i šalje je u *AD Password Recovery Toolkit* (PRTK) rečnik. PRTK prvo otvara listu rečnika lozinki za šifrovane fajlove. Ako ovaj napad ne uspe ostaje kriptoanalitički napad brutalnom silom, koji zahteva veliku računarsku moć i višeprocesorske mašine.

Označavanje (indeksiranje) 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 indeksiranih podataka 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.

4.2.4 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, [29]:

- 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. Međutim, 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** alat komandne linije. Ovaj dinamični alat ima, međutim, veliki nedostatak pri kreiranju radnog duplikata sa originalnog diska: *forenzički disk mora biti identičan originalnom disku po CHS (cilindri, sektori, tragovi) podacima*. Ako nije na raspolaganju identičan HD, forenzička radna stanica mora omogućiti da se iz BIOS-a manipuliše sa CHS podacima da bi se uparili sa originalnim vrednostima. Pri tome 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 svaremenih softverskih forenzičkih alata forenzički disk mora biti najmanje jednak, ili većeg kapaciteta od imidžovanog osumnjičenog diska.

Za kopiranje sa diska na disk brži su hardverski nego softverski alati za dupliranje diska. Sledeći hardverski i softverski alati prilagođavaju geometriju CHS forenzičkog diska prema geometriji CHS originalnog, imidžovanog diska, [29], [44]:

*a. 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 **Shadow Drive (***Voom Technology***)**, 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 **Shadow Drive** 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.

4.2.4.1 Forenzički alati za oporavak fragmentiranog fajla

Forenzički alat **Scalpel**[39] napisan na bazi alata **Foremost 0.69**, namenjen je za forenzičko procesiranje i oporavak fajlova (*carving*) sa forenzičkog imidža na bazi analize hedera i futera. Alat brzo otkriva fajlove proizvoljne veličine na mašini sa skromnim resursima. Eksperimenti su pokazali da je ovaj alat znatno brži od drugih, na primer od **Foremost** alata i nešto brži od **WinHex** i **FTK** alata. **Scalpel** postiže ovako visoke performanse inicijalnim skeniranjem podataka koje treba slagati (*carve*) i kreiranjem indeksa lokacija hedera i futera. Zatim alat pravi redosled rada i vrši drugo skeniranje podataka koje treba slagati u fajlove u skladu sa opcijama u konfiguracionom fajlu. Konfiguracioni fajl **Scalpel v. 1.53** je kompatibilan sa istim fajlom **Foremost** alatom, ali se razlikuju opcije komandnih linija:

39 Autori su *Golden Richard* & *Roussev Vassil*

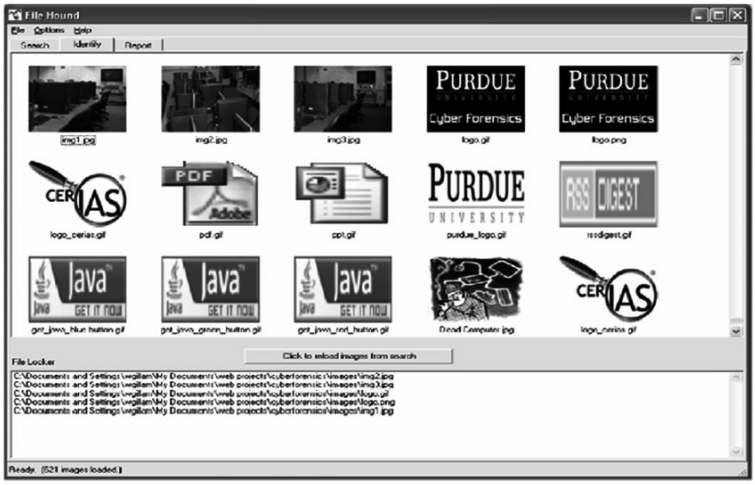
```
Usage: scalpel [-b] [-h|V] [-v] [-s num] [-i <file>] [-o <outputdir>]
       [-n] [-c <config file>] <imgfile> [<imgfile>] ...

-b  Carve files even if defined footers aren't discovered within
    maximum carve size for file type [foremost 0.69 compat mode]
-c  Choose configuration file
-h  Print this help message and exit
-i  Read names of files to dig from a file
-o  Set output directory for carved files
-n  Don't add extensions to extracted files
-r  Find only first of overlapping headers/footers [foremost 0.69 compat mode]
-s  Skip n bytes in each disk image before carving
-V  Print copyright information and exit
```

```
    maximum carve size for file type [foremost 0.69 compat mode]
-c  Choose configuration file
-h  Print this help message and exit
-i  Read names of files to dig from a file
-o  Set output directory for carved files
-n  Don't add extensions to extracted files
-r  Find only first of overlapping headers/footers [foremost 0.69 compat mode]
-s  Skip n bytes in each disk image before carving
-V  Print copyright information and exit
-v  Verbose mode
```

Značaj komparativne analize alata za oporavak fajlova (*carving*) iz imidža je činjenica da različiti alati daju znatno različite izlaze, što ukazuje na potrebu da se uvede više konzistentnosti u metode oporavka fajlova.

Specifičan forenzički alat **File Hound** (*Gillam Blair, Rogers Marc*) nude besplatan, korisnički pogodan alat za zvanične organe istrage koji omogućava istražitelju da pretraži i otkrije na HD hedere uobičajenih grafičkih fajlova: PNG, GIF, JPG, WMF, BMP. Kada se pretraživanje završi forenzičar može koristiti **File Hound** za pregled *thumbnails* slika i izabere slike za dalju analizu/reviziju (slika 4.2) koristeći komparaciju i algoritam za analizu boje kože.



Slika 4.2 Prikaz thumbnails slika u forenzičkom alatu **File Hound**

IDEAL Technology Corporation za automatizaciju osnovnih forenzičkih alata razvila je koristan forenzički alat **STRIKE (***Real Time Exstraction of Actionable Intelligence***)** koji brzo određuje da li ispitivani računarski sistem sadrži tražene informacije, vršeći brzu trijažu na nekoliko računara između stotine pa i hiljadu računara.

4.2.5 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. Da bi se generisao izveštaj posle ekstrakcije dokaza, forenzičar mora da ih kopira u poseban program kao što je neki Word procesor. 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 štampati na papiru i prilagati uz izveštaj, [29].

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

- log izveštaj i
- generator za izveštavanje.

Kao deo procesa validacije, potrebno je dokumentovati korake preduzete za dobijanje podataka sa osumnjičenog diska. Većina forenzičkih alata može generisati izveštaj o aktivnosti, poznat kao *log izveštaj,* koji se može dodati konačnom izveštaju forenzičara kao dodatni dokument o tome koji su koraci preduzeti u toku ispitivanja digitalnih podataka. 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***.

4.3 HARDVERSKI FORENZIČKI ALATI

Kako se brzo menjaju informaciono komunikacione tehnologije IKT sistema, tako se zahteva i izbor izbor softverksih forenzičkih alata za novi hardver. Većinu hardverskih komponenti savremenih računara proizvođači isporučuju sa srednjim vremenom otkaza (MTBF[40]) od oko 18 meseci. Kako se forenzički hardverski alati, radne stanice i serveri koriste intenzivno, zamenu i zanavljanje 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, [29]:

40 *Mean Time Between Failure* – vreme između dva otkaza

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

Forenzičar treba znati da PC ima ograničenja u korišćenju broja periferijskih jedinica. Što se dodaje više periferijskih 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 korporacijsku 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 zahteva za hardversom i softverom.

Problemi mogu nastati u podršci periferijskim uređajima, koji mogu doći u konflikt ili da ne rade i slika 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, **FRED** (*DII*[41]) 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, [29].

Odrediti gde će se vršiti akvizicija podataka, pa ako je to, na primer, na terenu treba obezbediti:

- blokator upisivanja, preko Fire Wire i USB 2.0 - blokator tipa **Fire Chief** (*DII*) i
- forenzički Laptop računar.

41 **F**orensic **R**ecovery **E**vidence **D**evices, Digital Inteligence Incorporation, SAD

Za redukciju hardvera koji se nosi, može se koristiti **Forensic Drive Dock** *(Wiebe Tech)* sa regularnim **Drive Dock** *Fire Wire* mostom.

Kod izbora računara za stacionarnu ili prenosnu radnu stanicu, treba uzeti pun *tauer* tipa računar koji omogućava najveći broj 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[42] bekapom; kablom za podatke, SCSI drajv karticom, eksternim *Fire Wire* i USB portovima, ergonomičnom tastaturom i mišom, grafičkom kartom velike memorije 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 **AEC-7720WP Ultra Wide SCSI-to-IDE Bridge (***ACCARD***)**, namenjen za sprečavanje upisivanja podataka na IDE HD, koji je kablom povezan na SCSI HD. Primer kompletnog računarskog sistema je **FRED** ili **DIBS Advance Forensic,** (*DII*) radna stanica. Brojni hardverski forenzički alati imaju implementiran odgovarajući program, tzv. *firmware*, programiran u samom alatu u EPROM memoriji i omogućavaju ažuriranje programa, [44].

4.3.1 Blokatori upisivanja i drugi hardverski forenzički alati

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

Akvizicija digitalnih dokaza sa hardverskom tehnologijom uključuje, [44]:

- blokatore upisivanja,
- razne adaptere,
- CD/DVD diskove 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.

42 *Uninterupable Power Suply*, uređaj

Softverski blokatori upisivanja uobičajeno se koriste kada nisu na raspolaganju hardverski blokatori i predstavljaju racionalnu alternativu. Softverski blokatori upisivanja, kao što su **PDBlock** (*Dll*), tipično radi u šel modu kao što je DOS. Kada se koristi **PDBlock,** potrebno je znati da se menja *Interupt 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.

Hardverskim blokatorom upisivanja povezuju 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, na primer, Windows aplikacije ili Windows Explorer da otvaraju fajlove, ili Word procesor da ih čita. Ako se kopira Word Windows podatak na blokirani disk, na prozoru forenzičke radne stanice se prikazuje da je kopiranje uspešno izvršeno. Međutim, blokator upisivanja u stvari prepiše i nulira sve te podatke. Kada se na radnoj stanici potraži kopirani fajl na blokiranom disku, tamo ga neće biti.

Postoje hardverski blokatori upisivanja koji se povezuju na računar kroz *FireWire*, USB 2.0 i SCSI kontroler. Većina ovih blokatora upisivanja omogućava forenzičaru da ukloni i ponovo spoji disk bez regularnog isključivanja (*shut down*) forenzičke radne stanice, što skraćuje vreme procesiranja ispitivanog diska, [44].

Poznatiji proizvođači hardverskih i softverskih blokatora upisivanja su dostupni na brojnim web adresama[43].

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 reprogamirati 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. Programi se nazivaju *firmware*, relativno su mali i na njihovu funkciju ne utiče rad OS, pošto se standardni komunikacioni protokoli automatski podešavaju nezavisno od bilo kojeg OS datog računara. Ovo je, sa aspekta forenzičara, osnovna prednost metoda hardverskih blokatora upisivanja u odnosu na softverske.

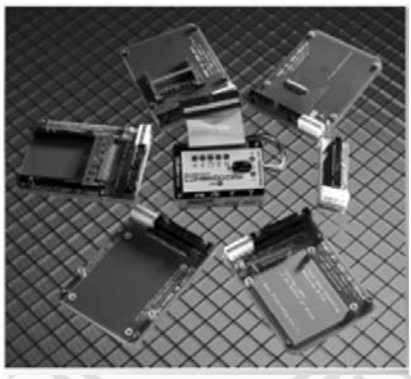
Korišćenjem hardverskih blokatora upisivanja mogu se skinuti digitalni podaci sa brojnih tipova čvrstih diskova, kao što su [44]:

- IDE čvrsti diskovi od 3,5 inča, klasični sa 40-pinskim IDE konektorom,
- SATA čvrsti diskovi od 2,5 i 3,5 inča, koji postaje preovlađujući u svim desktop i većini *notebook* računarima,

43 www.digitalintelligence.com; www.forensicpc.com
www.guidancesoftware.com/products/access-prosuites.shtm; www.voomtech.com
www.mykeytech.com; www.wiebeteach.com; www.paraben-forensic.com/ lockdown.hatml

- *Notebook* čvrsti diskovi od 2,5 inča preovlađivali su u ovim računarima od početka proizvodnje do nedavno,
- PCMCIA (PCCard) čvrsti diskovi, koji nisu šire prihvaćeni,
- 1,8 inča *Toshiba* čvrsti diskovi, koji se često koriste u originalnom *iPod* uređaju,
- 1,8 inča Hitachi čvrsti diskovi, koji se retko sreću u praksi,
- Kompaktni fleš i mikrodiskovi, koji se preovlađujuće koriste u digitalnim kamerama i u nekim iPod uređajima,
- SCSI čvrsti diskovi, koji se preovlađujuće koriste specijalno u starijim Machintosh i računarima sa visokim performansama,
- Optički kanali (*Fiber Chanels*),
- ZIF kablovski diskovi koji se koriste u video iPods i postaju preovlađujući u upotrebi.

Tipični hardverski blokatori izgledaju kao na slici 4.3.



Slika 4.3 Tipovi hardverskih blokatora

Poređenje IDE i SATA diskova prikazano je na slici 4.4. 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 kablu.



Slika 4.4 Primeri IDE i SATA diskova

Komplet blokatora upisivanja i adaptera za sakupljanje podataka sa klasičnih ***3,5 inča IDE*** diskova (slika 4.5) 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.



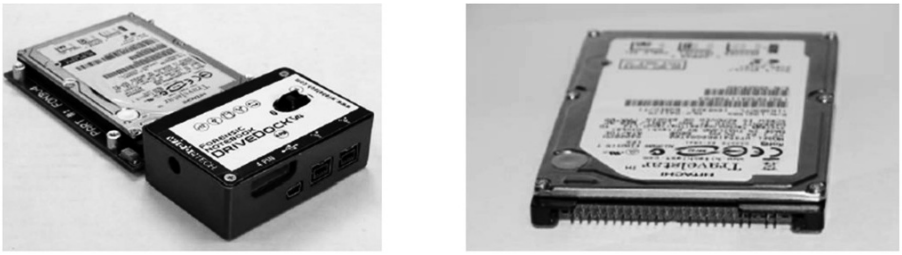
Slika 4.5 Sakupljanje podataka sa klasičnih 3,5 inča IDE diskova

Komplet blokatora upisivanja i adaptera za sakupljanje podatke sa ***3,5 inča SATA*** čvrstih diskova obuhvata (slika 4.6) 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.



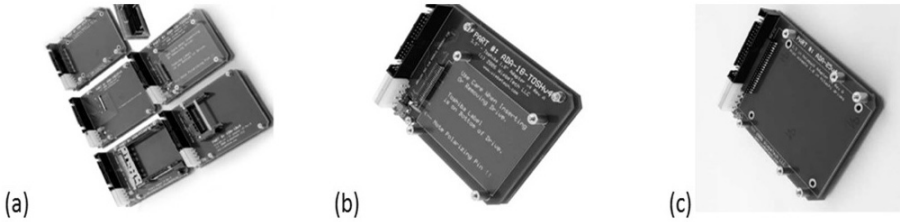
Slika 4.6 Sakupljanje podataka sa klasičnih 3,5 inča SATA diskova

Komplet blokatora upisivanja i adaptera za sakupljanje podataka sa 2,5 inča *notebook* čvrstih diskova obuhvata (slika 4.7) **Forensic Notebook DriveDock**, koji se priključuje na 2,5 inčna čvrste diskove i *FireWire* + USB pristupe host računaru, a obezbeđuje blokiranje upisivanja i brojne forenzičke karakteristike.



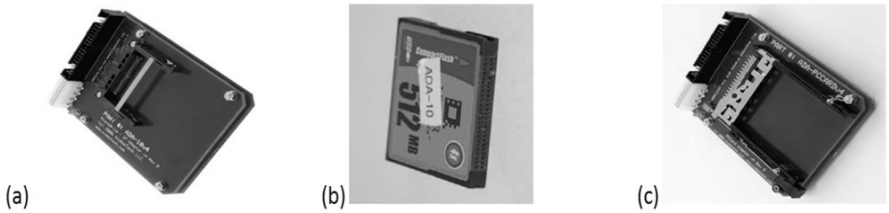
Slika 4.7 Sakupljanje podataka sa notebook diskova od 2,5 inča

Komplet blokatora upisivanja i adapteri za sakupljanje podataka sa malih čvrstih diskova obuhvata, (slika 4.8a) 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 4.8 Sakupljanje podataka sa malih čvrstih diskova

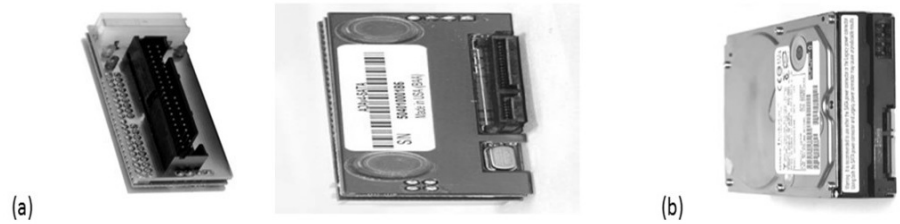
Komplet blokatora upisivanja i adaptera za 1,8 inča *Toshiba* koji se uobičajeno koriste u starijim *iPod*s, spajaju se forenzičkim **ComboDock-**om, (slika 4.8b). Blokatori upisivanja sa 2,5 inča *Notebook* adapterom za 2,5 inča čvrste diskove koji se uobičajeno koriste u starijim *Notebook* računarima. Takođe rade sa paralelno spojenim 1,8 inča *Hitachi* diskovima. Spajaju se na forenzički **ComboDock**, (slika 4.8c). Blokatori upisivanja i 1-inčni adapter za akviziciju digitalnih podataka sa fleš memorija i mikrodiskova povezuju se paralelno na forenzički **ComboDock**, (slika 4.9a,b).



Slika 4.9 Sakupljanje podataka sa fleš memorije (a) mikrodiskova (b) i PCCard (PCMCIA) adapter (c)

PCCard (PCMCIA) adapter, relativno redak, povezuje se paralelno i polarizuje kroz montažnu stranu šinskog slota. Nema polarizacije pinova na konektoru. Povezuje se na forenzički **ComboDock**, (slika 4.9c).

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 4.10a).



Slika 4.10 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 4.10b).

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 4.11). ZIF diskovi od *1,8 inča* sa kablom su najvećeg kapaciteta za male *notebook* računare i većeg kapaciteta za iPod urađaje.



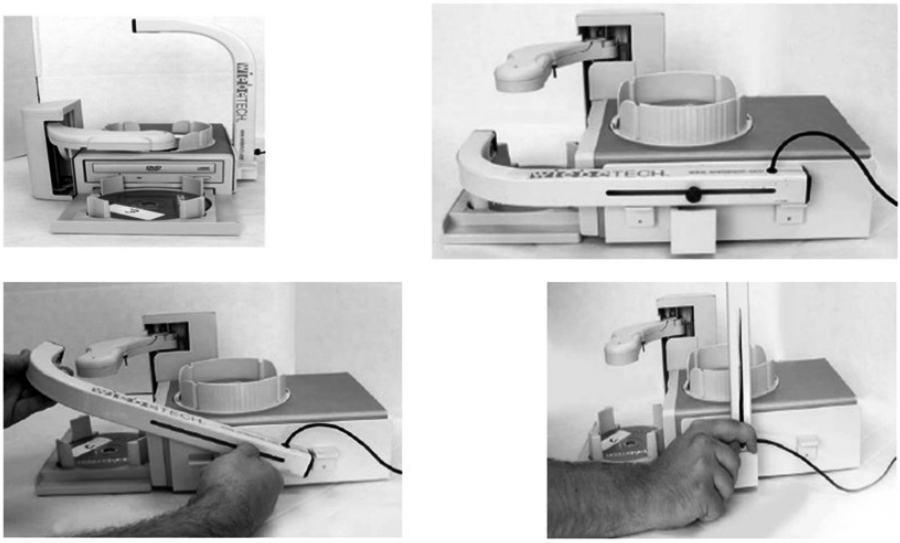
Slika 4.11 Adapter 1,8 inča ZIFza priključivanje Hitachi ZIF diskova

Akvizicija podataka sa optičkih 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, podložnijih greškama od onih koje koriste kontroleri čvrstih diskova. Razmatrajući ove faktore svaka forenzička istraga koja uključuje dokaze na optičkim medijima treba da ima četiri sledeća cilja i to:

- Izvršiti akviziciju *imidža* fajlova sa diska koji se mogu čitati i analizirati softverskim forenzičkim alatima dizajniranim za tu namenu, tipa **FTK, EnCese, iLook, xWay Forensic i**td;
- Obezbediti 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 Linix 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;
- Obezbediti 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;
- 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 štampa 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 opremnljenim 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 robora i kameru (Slika 4.12).



Slika 4.12 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 svkog 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. Poseduje *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*[44].

RP-PCIE-FC=Atto'sCTFC-42RO-BR1 (a.k.a. Celerity FC-42ES) automatski blokira upisivanje u svaki prključeni *FiberChanel* uređaj, za bezbedno izvlačenje podataka samo sa opcijom "čitanje". Sadrži 4GB-tni dvo-kanalni *FiberChanel*-host računar adapter sa brzinom prenosa podataka do 800 MB/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* prozvodima. Uključuje dva 4Gb LC SFPa. Usklađen je sa *RoHSC*, [3].

44 *Restriction of Hazardous Substances Directive* – Direktiva EU iz 2003 godine, efektivna od 1.07.2006.

4.4 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**[45] alat na bazi DOS komandne linije namenjen za akviziciju podataka sa diska. Primeri GUI tipa alata su **EnCase**[46] i **FTK**[47], 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. *miror; 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.

4.4.1 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 (fajl *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:

45 NTI-National Technology Inc.
46 Guidance Software
47 Access Data

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

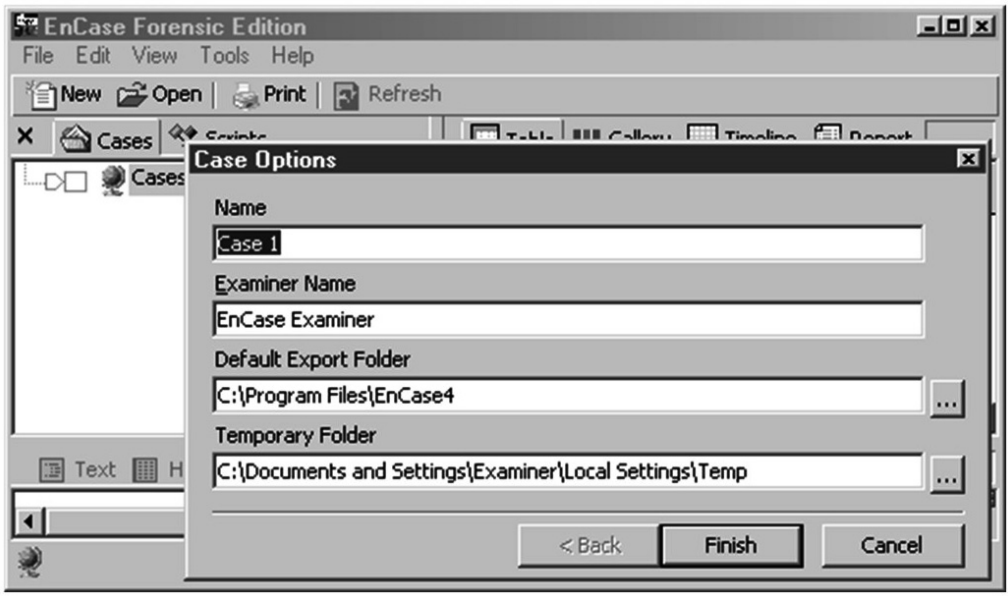
4.4.2 Softverski forenzički alat zatvorenog kôda EnCase v4 GUI tipa

EnCase je najpoznatiji i prvi prihvaćeni softverski alat zatvorenog programskog koda, 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, fajl *slack* i nealocirani prostori fajla. Ono što je svakako najvažnije za forenzičara, jeste da nema mogućnost izmene podataka sa **EnCase** alatom, [8].

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

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 4.13).

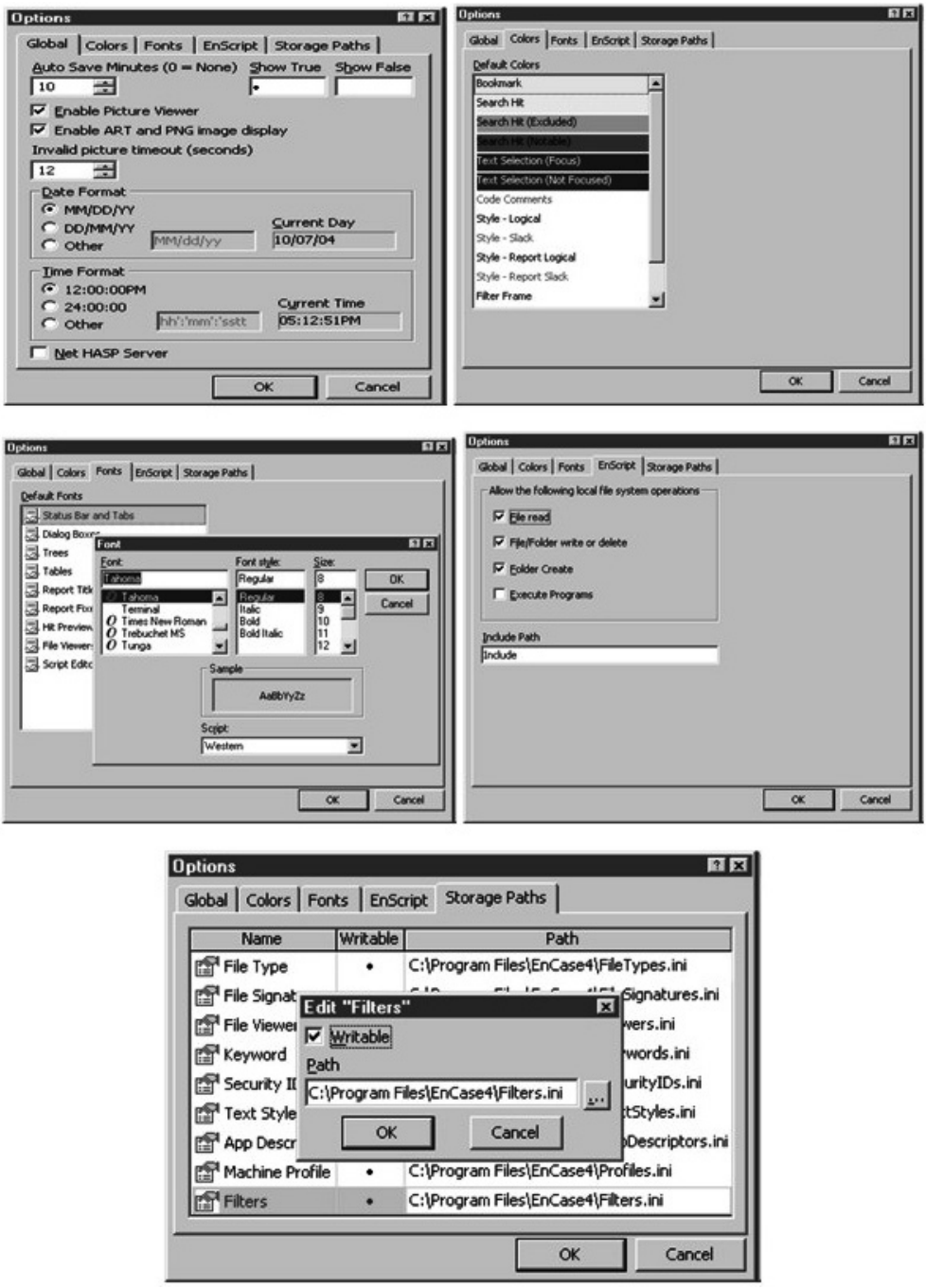


Slika 4.13 Otvaranje novog slučaja u EnCase alatu

Trebalo bi voditi računa o tzv. *Case Menagement*-u koji podrazumeva dodeljivanje imena slučajevima, ostavljanje prostora na disku za skladištenje dokaznog materijala, imenovanje foldera za privremene (*temporary)* fajlove i dr. *Case Menagement* 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.

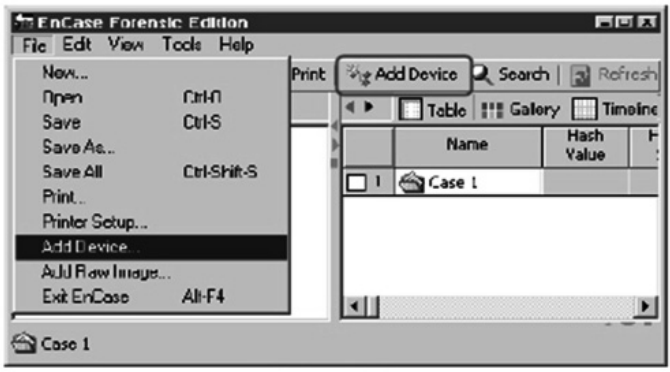
Dijalog *Options* (slika 4.14) dobija se korišćenjem putanje *Tools->Options* sa linije menija. U okviru ovog dijaloga nalaze se opcije za podešavanje vremena, boje, fontova, *EnScript*-ova, *backup case* fajla *export* foldera, *temporary* foldera itd. Sve navedene opcije se jednom mogu podesiti i koristiti kao takve svaki sledeći put u radu sa **EnCase** alatom.



Slika 4.14 Otvaranje dijaloga Options u **En Case** alatu

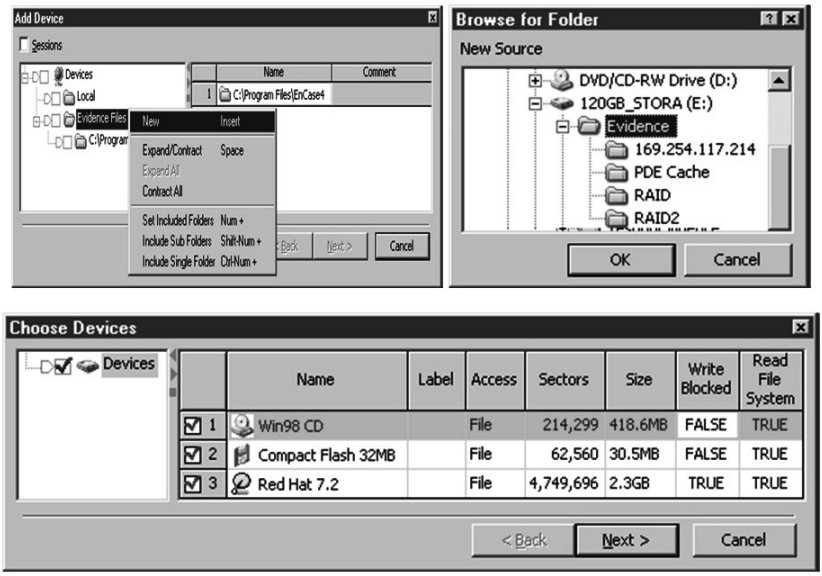
Dodavanje dokaznog materijala novom slučaju vrši se na sledeći način:

- selekcijom *Add Device* na fajl meniju ili
- otvaranjem opcije *Add Device* na top *toolbar*-u, (slika 4.15).



Slika 4.15 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 4.16).



Slika 4.16 Odabir fajlova za pretraživanje

Novi folder se pojavljuje ispod foldera *Evidence Files*. Aktiviranjema 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.

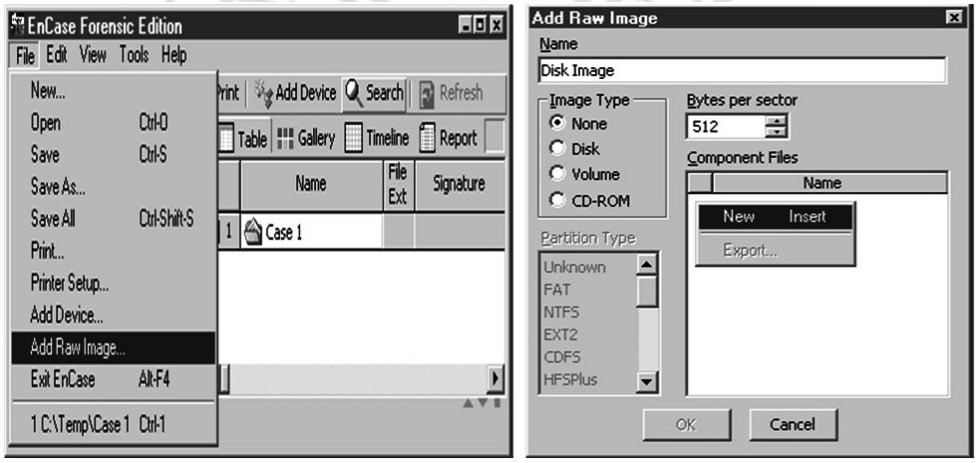
Jedna od opcija koja se nalazi u okviru dijaloga *Add Devices* je opcija *Session*. Ona omogućava dodavanje dokaznog materijala koji je već pregledan, ili na bilo koji način izmenjen.

Verifikacija započinje nakon što su fajlovi unešeni. **EnCase** verifkuje integritet fajlova. Započinjanje ovog procesa podrazumeva čitanje podataka i generisanje MD5 *hash* vrednosti, prikazivanje verifikacije i prikazivanje *hash* vrednosti u vidu izveštaja, (slika 4.17).



Slika 4.17 Verifikacija novog slučaja

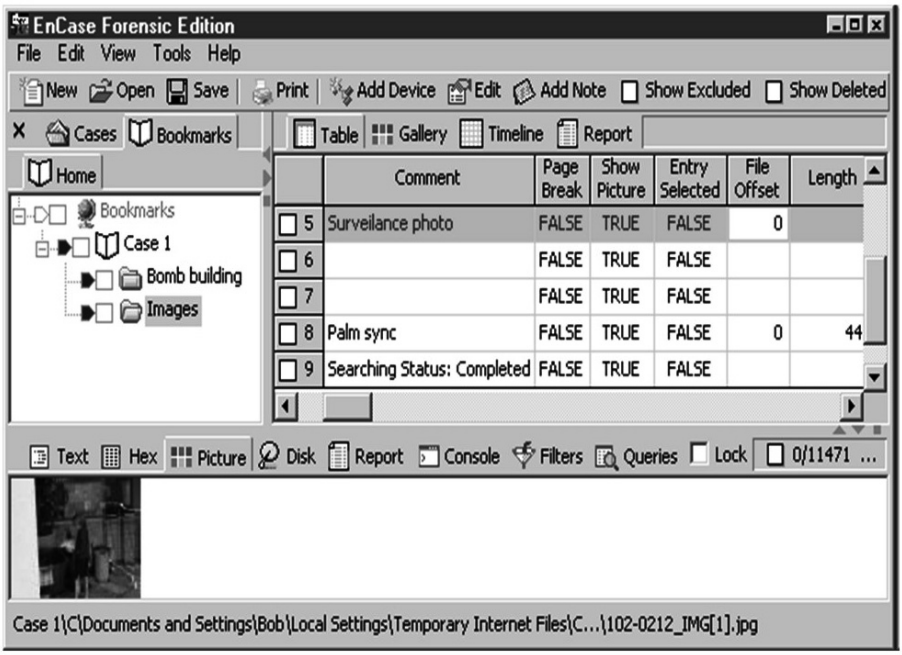
Dodavanje sirovih imidž fajlova u **EnCase** vrši se korišćenjem putanje *File->Add Raw Image*. Pojavljuje se dijalog u koji se unose ime, dodatih fajlova, odabirom postojećih ili dodavanjem novih, ili takozvanih *chunk* fajlova koji se nalaze u *Components Files***, (**slika 4.18).



Slika 4.18 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.

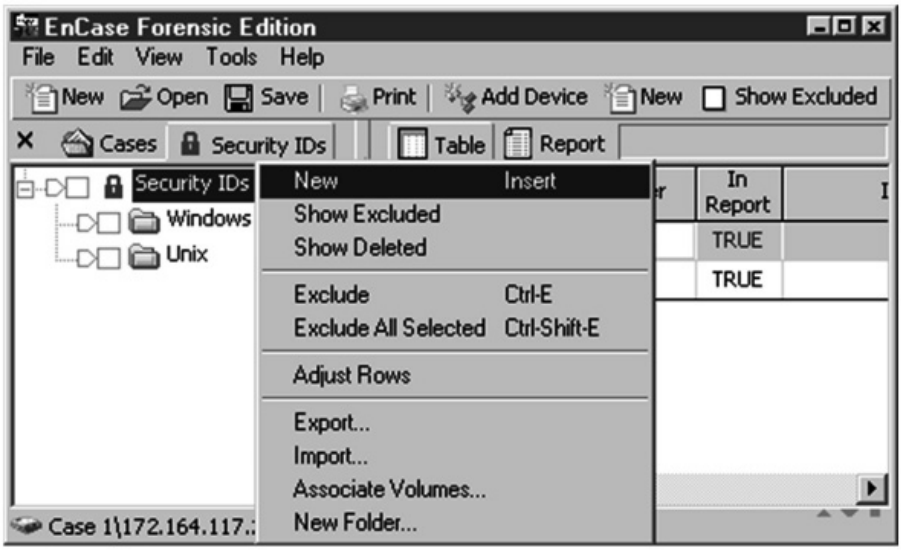
Označavanje ili indeksiranje fajlova od interesa (*bookmarks*) vrši se selektovanjem *Bookmarks* iz menija *View*. *Bookmarks* tab sadrži informacije koje su markirane kao fajlovi od interesa. Indeksirani mogu biti muzički fajlovi, slike, tekst i dr. Mogu se videti u *Table*, *Gallery* ili *Timeline* prikazu, (slika 4.19).



Slika 4.19 Indeksiranje fajlova u EnCase alatu

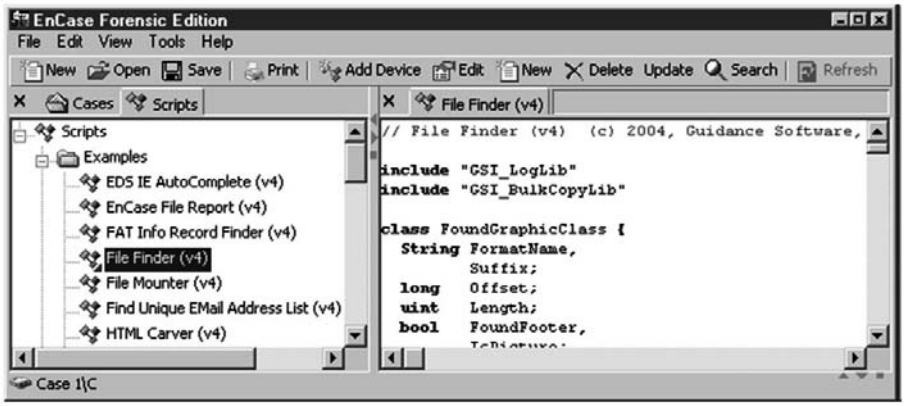
EnCase je program koji sadrži raznovrsne opcije za pretraživanje. Među pomenutim opcijama nalaze se i opcije za pretraživanje po tipu podataka, opcije za pretraživanje po ekstenzijama i upoređivanje istih radi dokazivanja da li je došlo do promene određenih ekstenzija ili nije, pretraživanje po ključnim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

Bezbednosni identifikator (SID) i određeni skup dozvola ima svaki fajl, ili folder u NTFS fajl sistemu. Iako se struktura fajlova razlikje 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 materijal. Do ovog taba dolazi se korišćenjem putanje *View->Security Ids*, (slika 4.20). U PRILOGU 1 dat je spisak poznatijih SID identifikatora u Windows operativnim sistemima.



Slika 4.20 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 indeksa do dodavanja informacija izveštajima, (slika 4.21).



Slika 4.21 Aktiviranje skriptova u EnCase alatu

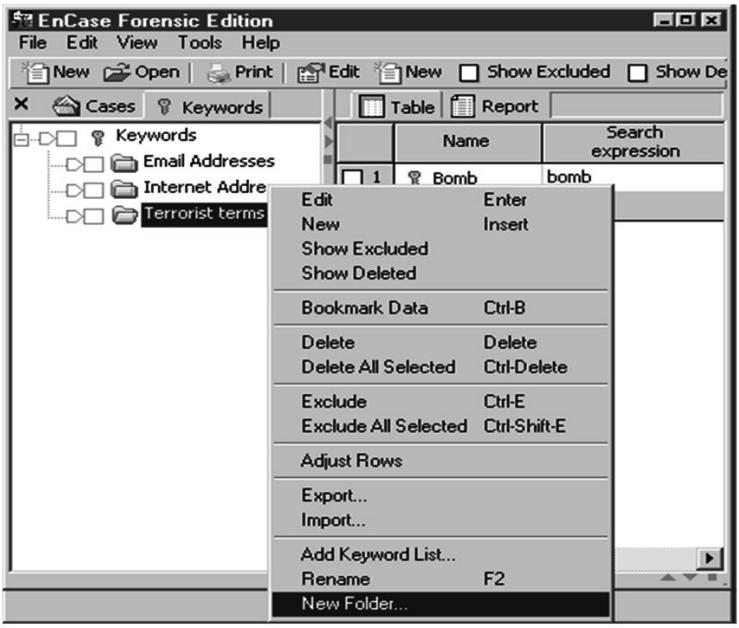
Kopiranje/oporavak izbrisanih fajlova, **EnCase** vrši „*byte-po-byte*“. Sve što treba uraditi jeste čekirati fajl i desnim tasterom miša izabrati opciju *Copy/unErase*. Pojaviće se dijalog kojim se vrši odabir između načina na koji će fajl biti vraćen, koji njegov deo (fizički, logički, RAM *slack*) i na kraju gde smestiti taj fajl, (slika 4.22).



Slika 4.22 Izbor fajlova i foldera za oporavak

Takođe, moguće je isto uraditi i sa indeksima. Proces je identičan opisanom bilo da se koristi jedan ili više indeksa (*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 malopređašnjeg 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 4.23).



Slika 4.23 Pretraživanje po ključnoj reči u EnCase alatu

Pregled komponovanih fajlova pod kojim se podrazumevaju fajlovi sastavljeni od više slojeva kao što su OLE[48] (*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*.

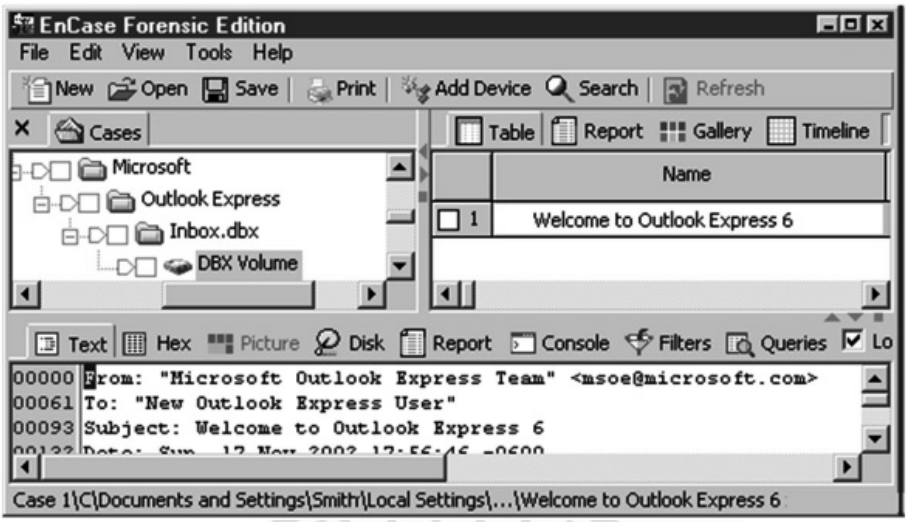
EnCase v. 4 sadrži *EnScript* pod imenom *File Mounter* koji podržava rad sa komponovanim fajlovima, nudeći brz i lak dolazak do njihove strukture.

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 *secutity*, *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*.

EnCase alat podržava rad sa *Outlook Express e-mail .DBX* fajlovima. 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 4.24).

48 *Object Linked Embedded*, MS tehnologija na kojoj je baziran Microsoft Office paket; podrazumevaju npr. da se Excel tabele mogu naći u okviru Word dokumenta.



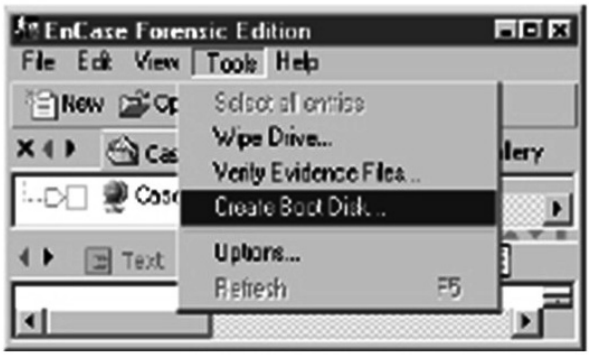
Slika 4.24 Čitanje Outlook Express .DBX fajlova u EnCase alatu

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 Expres*-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 4.25),



Slika 4.25 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 4.26).



Slika 4.26 Završetak kreiranja butabilne diskete u EnCase alatu

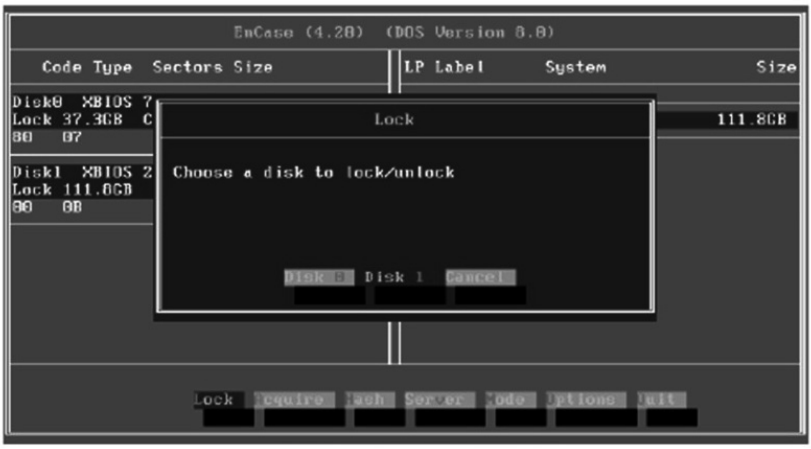
- Izvaditi deisketu i pravilno je označiti.

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 čvrstih diskova,
- 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,
- isključitie računar i priključiti čvrste 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 čvrstih diskova (slika 4.27), akviziciju podataka, heširanje i mnoge dr.



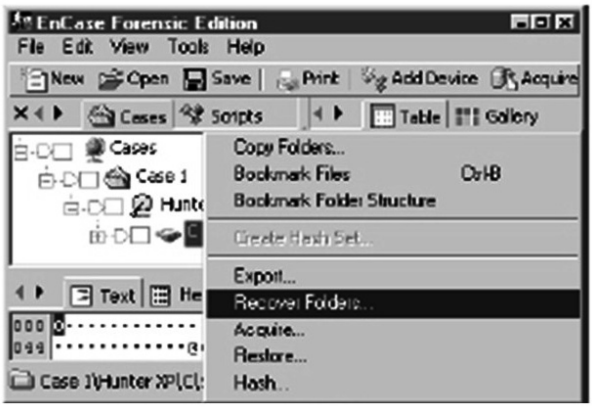
Slika 4.27 Zaključavanje i otključavanje hard diskova

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/J*az 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.

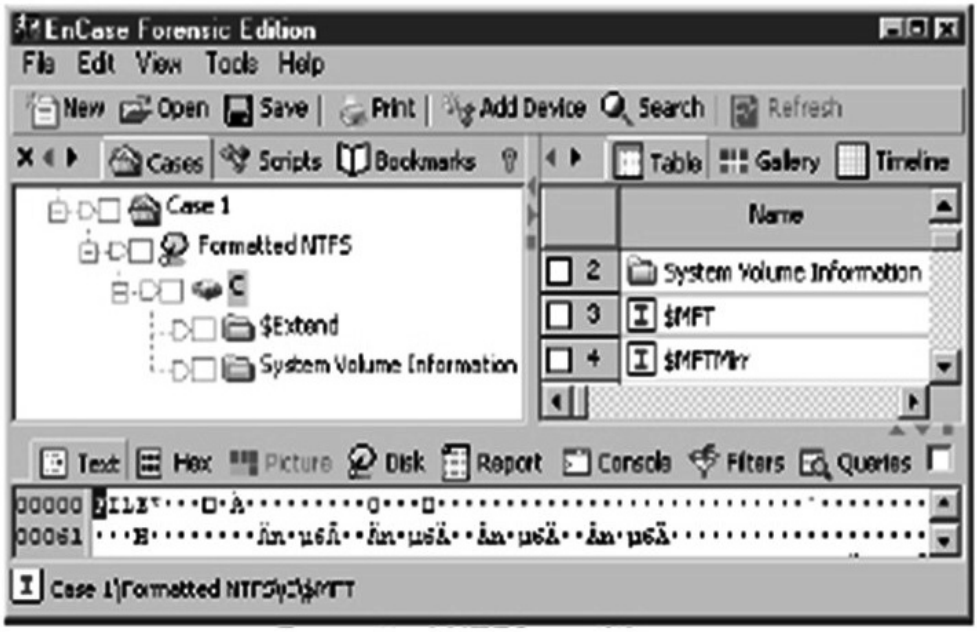
Oporavak foldera u FAT fajl sistemu: Prvi korak brisanja podataka je njihovo slanje u *Recycle Bin.* Smatra se da kada se *Recycle Bin* isprazni, da su podaci zapravo tada obrisani. Ipak, oni se i u tom trenutku nalaze na HDD i lako se mogu povratiti.

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 klastere konkretne FAT particije. Svaki folder FAT particije ima ulaz u obliku **„. ..“** (*dot-double dot)*. Ovi ulazi govore fajl sistemu gde se nalaze folderi. **EnCase** vrši pretragu kroz nealocirane klastere, traži ulaz (**„. ..“**) i vrši povraćaj foldera koji su obrisani, ili sa njihovim ulazima koji su obrisani u glavnom direktorijumu. **EnCase** neće vratiti folder sa originalnim imenom (jer je ime obrisano u glavnom direktorijumu), ali će nastojati da povrati sve što se nalazi unutar tog foldera, uključujući i imena fajlova unutar foldera, (slika 4.28).



Slika 4.28 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 rutu NTFS particije, (slika 4.29).



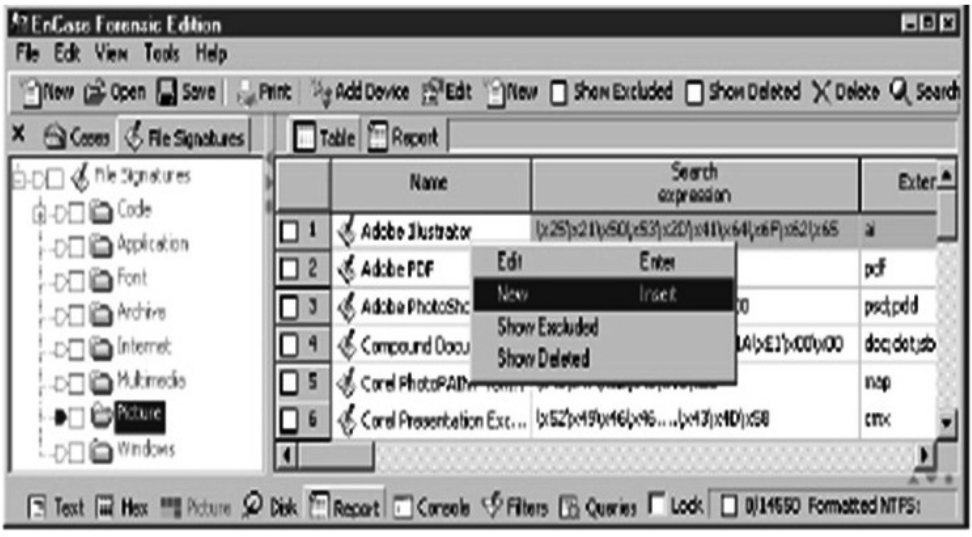
Slika 4.29 Formatirana NTFS particija

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.

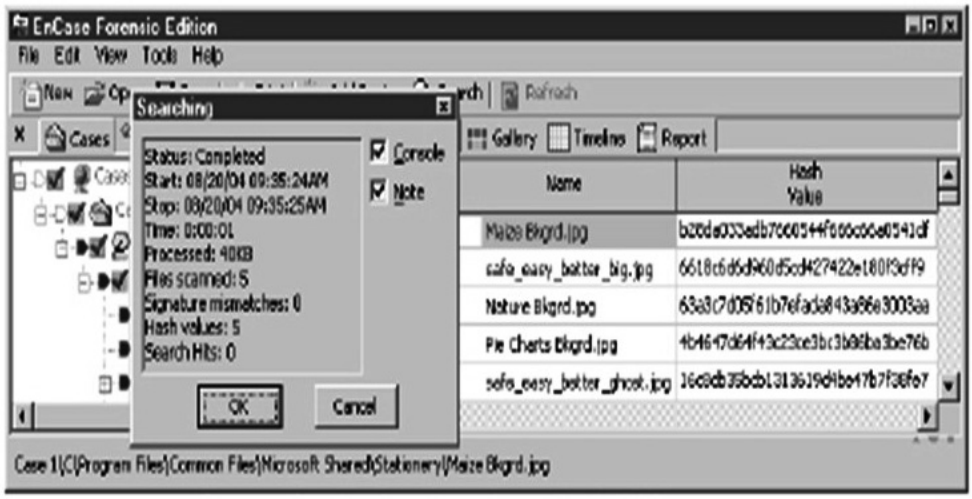
Signatures se mogu videti korišćenjem putanje *View->File Signatures*. **EnCase** pored velikog broja *signatures* ima i mogućnost dodavanja novih. Recimo .mp3 format nije u listi standardnih formata pa se u **EnCase**-u može dodati kao *signature* i podesiti da se po njegovom pronalaženju automatski otvara sa nekim od programa koji podražavaju njegov rad, (slika 4.30).



Slika 4.30 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[49] 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*, ireverizibilni, 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 4.31).



Slika 4.31 Generisanje heš vredn.osti za izabrane fajlove

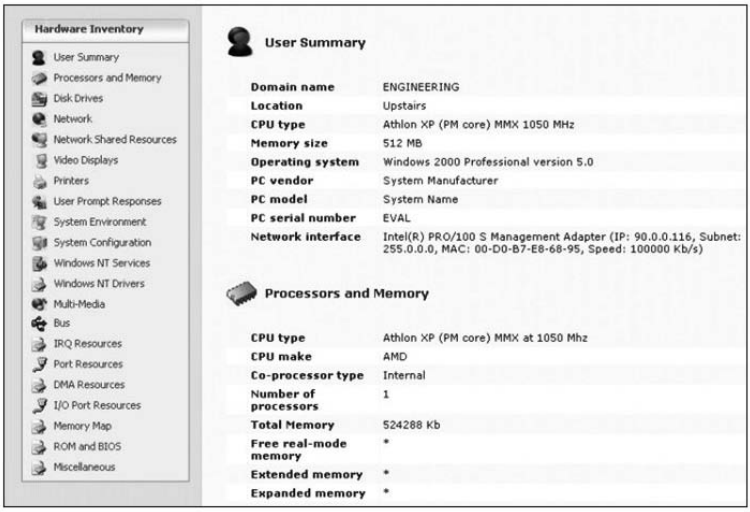
Proces oporavka podataka: Disk se uglavnom formatira, na neki od postojećih načina, radi brisanja podataka. Međutim, formatiranje, ili popularno *FDISK*-ovanje ne briše podatke u potpunosti, nego samo strukturu koja locira podatke i informacije o particioniranom disku. **EnCase** ima mogućnost oporavka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

49 Message-Digest algorithm 5

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 predstavljaja jedan od najvrednijih izvora podatatka. Kod **EnCase Enterprise ver.4** *snapshot* se vrši korišćenjem *EnScript*-ova, (slika 4.32).



Slika 4.32 Snimak trenutnog stanja sistema

Arhiviranje dokaznog materijala smatra se dobrom forenzičkom praksom i preporučije 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 označiti 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 jedinicama (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 4.33).

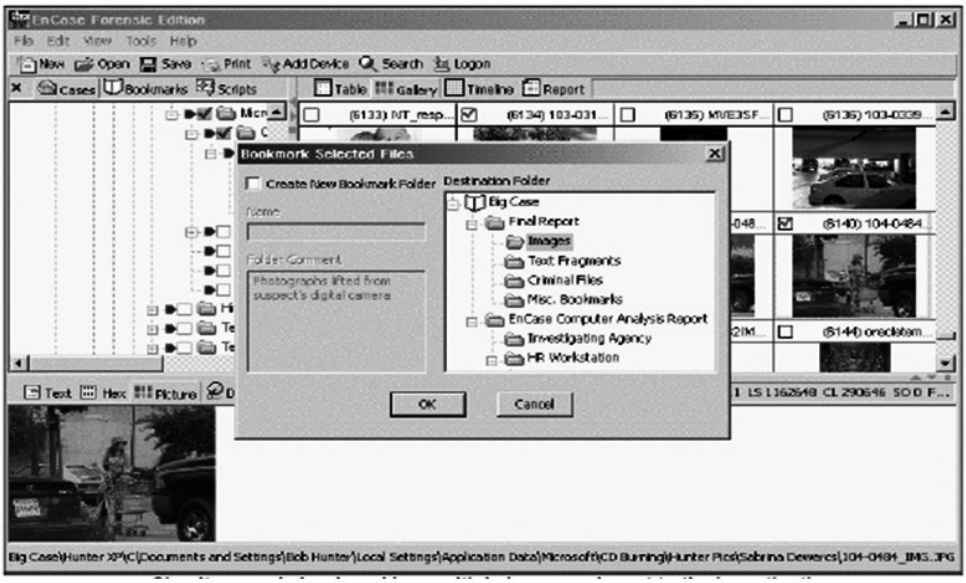


Slika 4.33 Izbor i selekcija diska za brisanje sa prepisivanjem u EnCase alatu

Prezentovanje dokaza i izveštavanje u pisanoj 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.

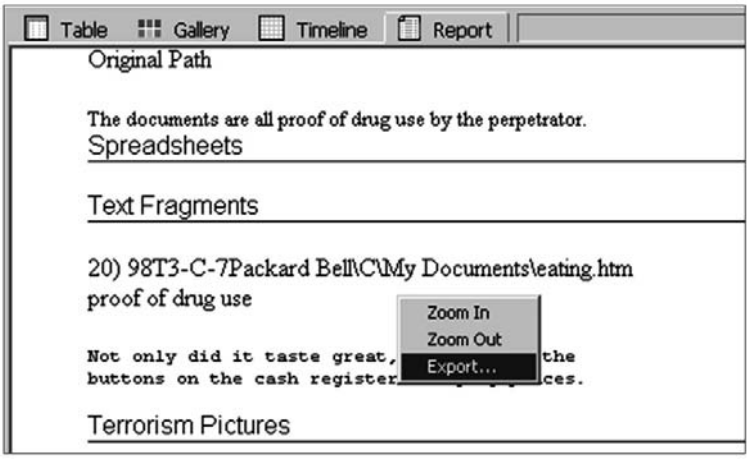
EnCase obezbeđuje nekoliko metoda za generisanje finalnog izveštaja. U praksi je čest primer „prelamanja" izveštaja na nekoliko delova, sa sadržajem koji upućuje na sve njegove delove. Javlja se i potreba za izveštajima koji nisu u papirnoj formi (skladišteni na CD-ROMu), ali uz kratki sadržaj (*hyper 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 4.34).



Slika 4.34 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 4.35).



Slika 4.35 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 genesisano sledeće:

- Ful 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 inforamcijama koje su vezane za izveštaj.

4.4.3 Analiza Access Data FTK forenzičkog alata

Pregled opštih karakteristika. Forenzički alat FTK (Forensic Toolkit)[50] predstavlja skup forenzičkih alata koji može da izvrši više zadataka digitalne forenzičke istrage. Prvi među njima je alat za akviziciju FTK Imager koji obezbeđuje bit-po-bit kreiranje imidža korumpiranog diska. Kopija je apsolutno identična originalu, čak i sa stanovišta nealociranog prostora. Ovo je veoma bitna činjenica imajući u vidu da će digitalni dokaz biti priznat na sudu samo ako je relevantan i pouzdan, a u toku forenzičke istrage se koristi upravo kreirana kopija. Za analizu podataka, FTK forenzički alata koristi više načina: heširanje, korišćenje baze heš vrednosti poznatih programa i pretraživanje.

Heširanje predstavlja generisanje jedinstvene vrednosti za fajl ili ceo disk u zavisnosti od njegovog sadržaja. Heš vrednosti se koriste da bi se obezbedio integritet podataka. FTK koristi dve funkcije heširanja MD5 (Message Digest 5) i SHA-1 (Secure Hahs Algorithm), (slika 4.36).

```
MD5 checksum:    5f57ff1a9223e13faeff909b6c0940e1
SHA1 checksum:   ab255666da5a447f8bdef5819747bf8a80f81cf8
```

Slika 4.36. Prikaz heš vrednosti u FTK alatu

Po podrazumevanom podešavanju **FTK** kreira MD5 heš vrednost. MD5 heš vrednosti koristi **KFF** (*Known File Filter*) biblioteka za identifikovanje fajlova. SHA-1 je novija funkcija heširanja. KFF može sadržati SHA-1 heš vrednosti fajlova, ali ih najčešće ne sadrži. Heš vrednosti se mogu kreirati **FTK** alatom, ali i **FTK** Imager-om.

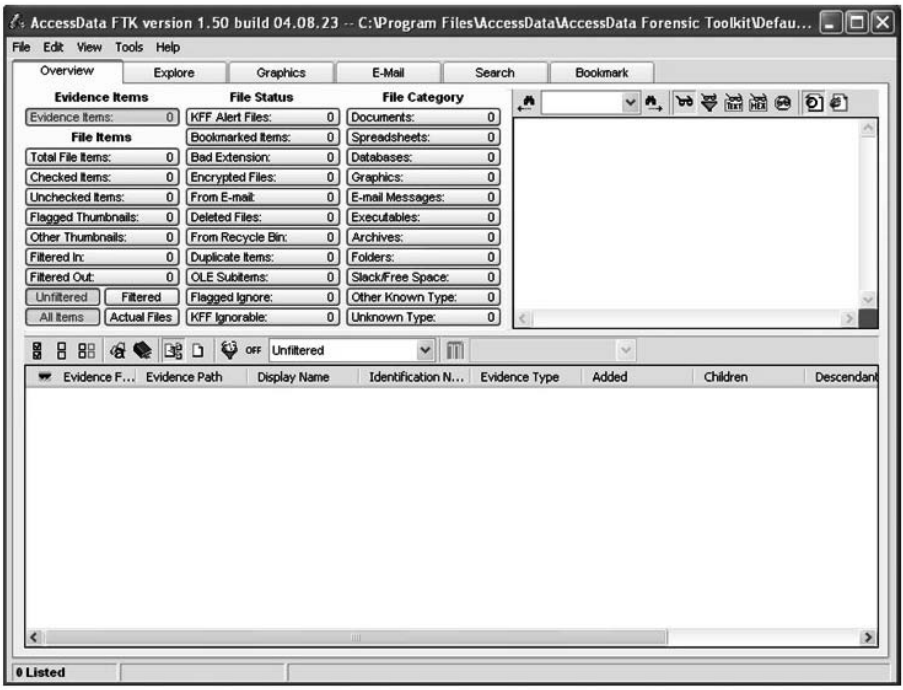
Kao što je već napomenuto **KFF** biblioteka sadrži informacije o poznatim sistemskim i programskim fajlovima. Prilikom analize podataka kada se kreiraju heš vrednosti fajlova, oni se upoređuju sa vrednostima u KFF i ako se naiđe na identičnu vrednost, taj fajl se smatra poznatim i ignoriše se u daljoj istrazi. Na ovaj način se skraćuje vreme potrebno za analizu podataka. KFF sadrži **HashKeeper**[51] bazu podataka gde se čuvaju heš vrednosti poznatih fajlova. Ovu bazu podataka je potrebno periodično ažurirati.

50 *AccessData Corporation*, FTK Manual
51 http://www.accessdata.com/downloads.htm

Pretraživanje **FTK** forenzičkim alatom može biti indeksirano ili ne. Indeksirana pretraga koristi indeks fajl za pronalaženje određenog termina. Indeks fajl sadrži termine i iz alociranog i iz nealociranog dela dokaza. Neindeksirana pretraga može da se vrši redom po svim terminima, a u ovoj pretrazi mogu da se koriste i regularni izrazi. **FTK** forenzički alat koristi mašinu za indeksirano pretraživanje *dtSearch* koja veoma brzo pretraži gigabajte teksta. Mašina za pretraživanje *dtSearch* je trenutno jedna od vodećih alata za ovaj deo digitalne forenzičke istrage.

FTK forenzički alat ima mogućnost generisanja log fajla u toku istrage, ali i završnog izveštaja istrage. **FTK** automatski kreira log fajl pod nazivom *ftk.log*. Ovaj fajl može da bude od velike koristi u toku analize podataka kao trag koji ukazuje na to šta se sve dešavalo u toku istrage. Log fajl može biti pridružen završnom izveštaju kao dodatak. FTK koristi Report Wizard za generisanje izveštaja u HTML formatu. Tako generisani izveštaji su prihvatljivi i predstavljaju validni dokument o rezultatima istrage. U izveštaju mogu biti uključene informacije obeležene tokom istrage (bookmarks), grafički elementi, liste fajlova i drugi dodaci.

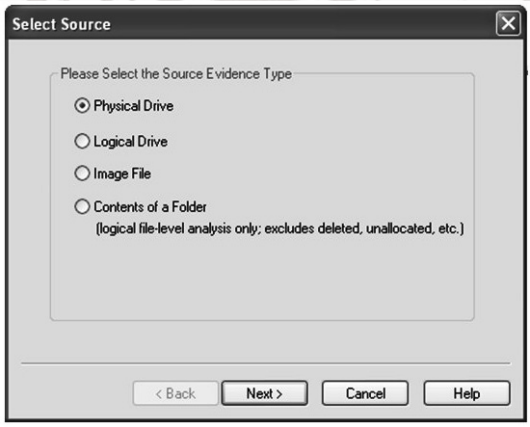
Interfejs FTK forenzičkog alata veoma liči na bilo koji Windows prozor. FTK forenzički alat je GUI tipa, pa samim tim nije komplikovan za korišćenje, (slika 4.37).



Slika 4.37 Početni prozor FTK forenzičkog alata

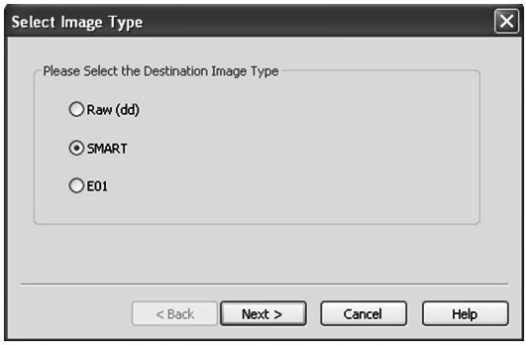
Početni prozor FTK forenzičkog alata sadrži šest kartica: *Overwiev, Explorer, Graphics, E-mail, Search i Bookmark*. Overwiev kartica prikazuje generalne informacije o slučaju kao i listu analiziranih dokaza. Explorer kartica prikazuje strukturu direktorijuma svakog dokaza, sadržaj selektovanog fajla i njegove karakteristike kao što su tip fajla, putanja i druge. *Graphics* kartica omogućava prikazivanje svakog grafičkog fajla. Ova kartica pruža mogućnost odabira onih grafičkih elemenata koje želimo da prikažemo u izveštaju. E-mail kartica prikazuje e-mail sandučiće sa porukama i fajlovima koji su pridruženi porukama. Prikaz je u HTML formatu. U kartici *Search* je moguće vršiti indeksiranu ili običnu pretragu po ključnoj reči. Indeksirana pretraga je mnogo brža. Prilikom pretrage rezultat se prikazuje u listi rezultata. U toku istrage moguće je obeležiti neke informacije kao bitne za slučaj, a njihov pregled moguće je uraditi u kartici *Bookmark*. Njih je moguće dodati u izveštaj, a uz njih postoji mogućnost dodavanja komentara.

FTK Imager je alat za kreiranje imidža fizičkog diska, logičkog diska, fajla ili sadržaja foldera. Dakle, FTK Imager nudi mogućnost odabira tipa dokaza čiji imidž se kreira, (slika 4.38).



Slika 4.38 Odabir tipa dokaza

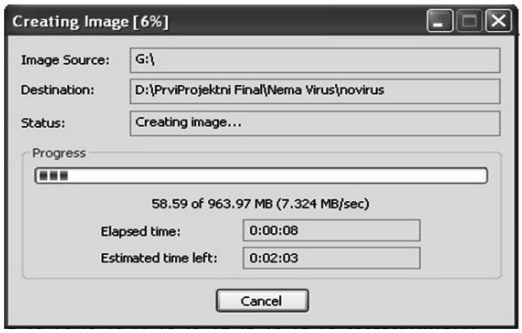
Kada se odabere opcija kreiranja disk imidža i odluči se za tip dokaza, bira se tip imidža (slika 4.39). Od tipa imidža zavisi koji forenzički alati će moći da ga koriste a koji neće. Ukoliko je potrebno uraditi analizu sa više forenzičkih alata, ovo je izuzetno bitan momenat jer od odabira tipa imidža zavisi tok čitave dalje forenzičke istrage.



Slika 4.39 Odabir tipa imidža

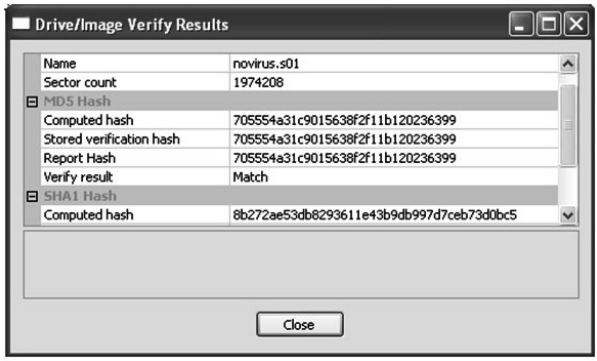
U slučaju FTK forenzičkog alata, u ponudi su tri opcije tipa imidža *Raw(dd), SMART* i *EO1*. *Raw(dd*) tip imidža kreira nekompresovani imidž i ukoliko se odluči za ovaj tip potrebno je obezbediti dovoljno prostora za kreiranje ovakvog imidža. *SMART* i *EO1* tipovi imidža kompresuju imidž i omogućavaju bržu forenzičku akviziciju. Kako su današnji hard diskovi sve veći, ova činjenica nije za zanemarivanje, jer je cilj što brže kreirati imidže i njihove kopije i izvršiti analizu. Sa alatom koji omogućava kompresiju imidža, navedeni zahtevi su zadovoljeni.

Nakon popune generalija kao što su broj slučaja, broj dokaza i opis dokaza, kreira se imidž i odredi lokacija za čuvanje imidža, kao i naziv imidža (slika 4.40). Postoji mogućnost verifikacije imidža po njegovom kreiranju. Takođe, može se uključiti opcija prekalkulacije statistike.

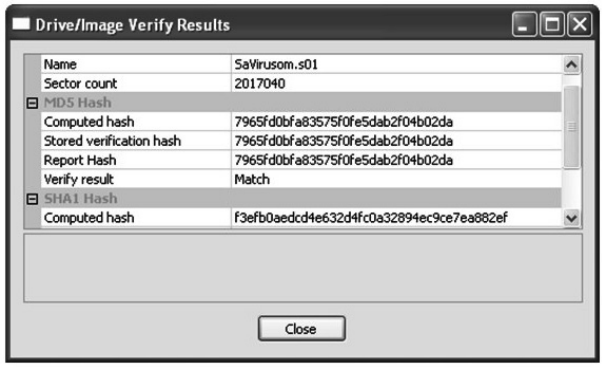


Slika 4.40 Kreiranje imidža

Verifikacija heš vrednosti imidža USB diska nezaraženog virusima prikazana je na slici 4.41, a zaraženog USB sa virusom na slici 4.42. Razlike heš vrednosti ukazuju da je integritet USB diska narušen.

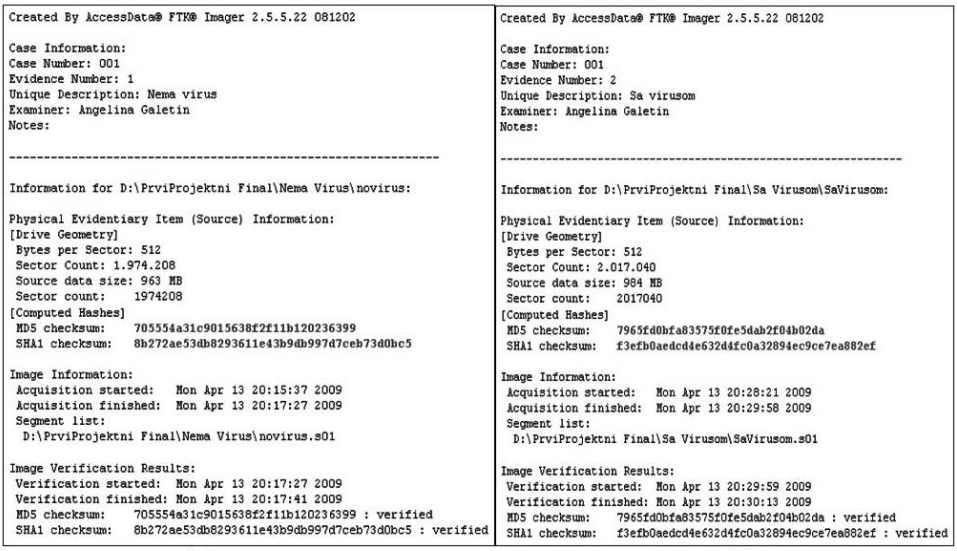


Slika 4.41. Verifikovanje rezultata imidžovanja nezaražene USB memorije



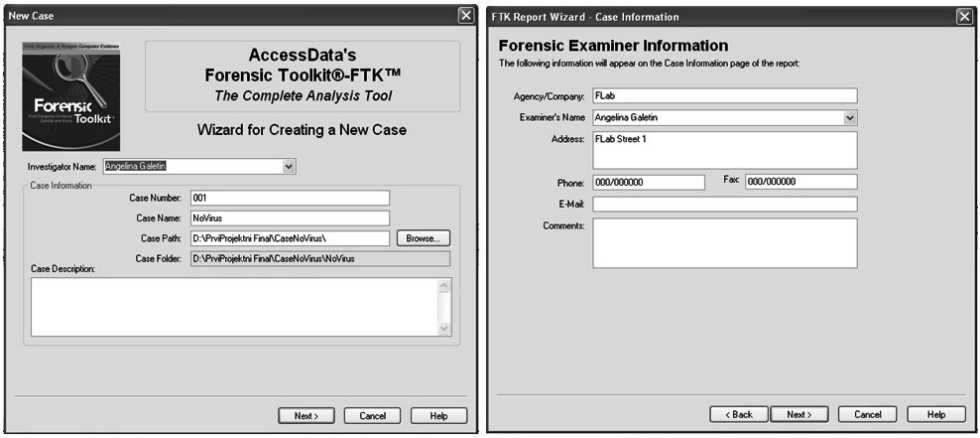
Slika 4.42. Verifikovanje rezultata imidžovanja zaražene USB memorije

Nakon kreiranja imidža generisani su TXT i CSV fajlovi sa kompletnim pregledom svih fajlova na USB memorijskom uređaju (slika 4.43). Jasno su uočljive različite heš vrednosti dobijene prilikom imidžovanja.



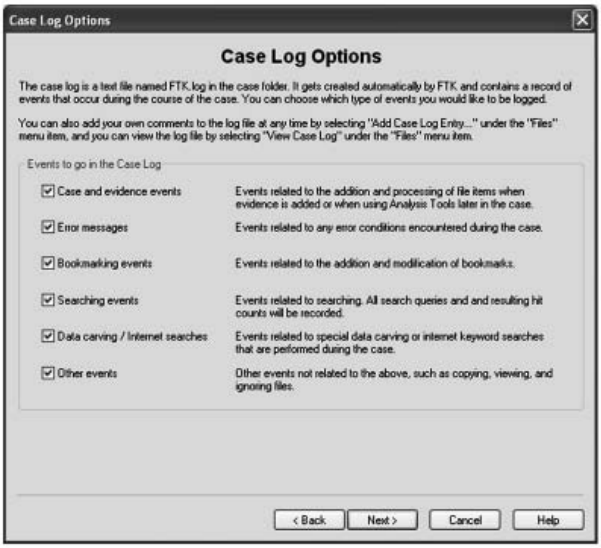
Slika 4.43 TXT fajl generisan posle imidžovanja virusom nezaraženog (a) i zaraženog (b) USB

Kada su uzeti imidži ispitivanog diska, u ovom slučaju *USB* memorije, može se započeti novi slučaj. Najpre je potrebno uneti genaralije o samom slučaju i forenzičaru koji vrši ispitivanje (slika 4.44).



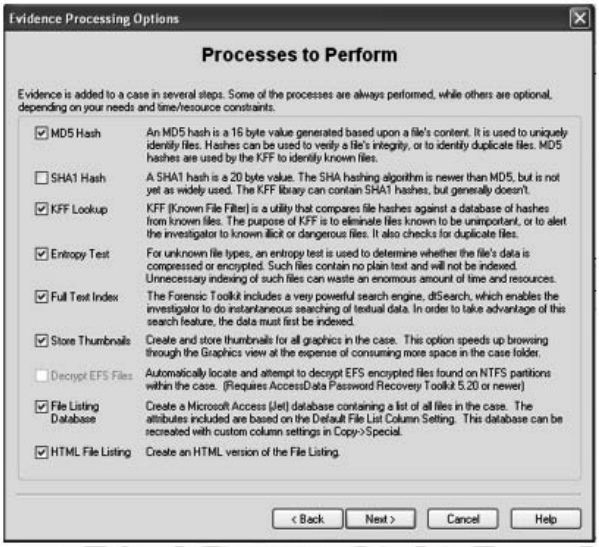
Slika 4.44 Generalije o slučaju i forenzičaru

U sledećem koraku, *Case Log Options*, donosi se odluka koji će događaji tokom analize biti uključeni u log fajl. Tekstualni fajl *FTKlog,* FTK forenzički alat kreira automatski. Na slici 4.45 prikazan je slučaj uključivanja svih opcija.



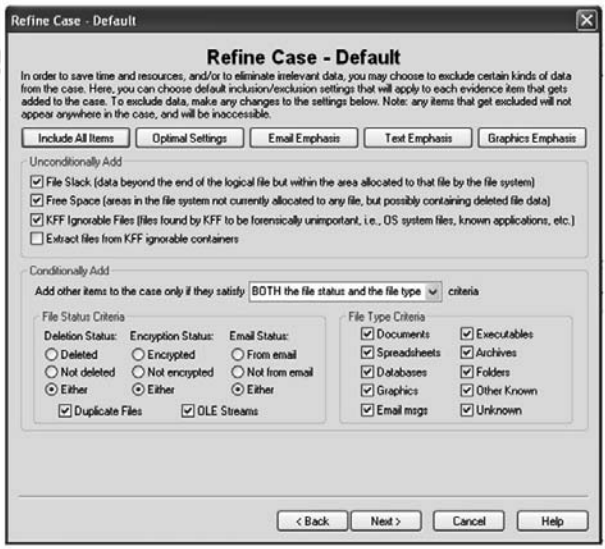
Slika 4.45 Case Log opcije

Processes to Perform je naredni korak analize i u njemu se odabiraju procesi koji treba da se izvrše nad trenutnim dokazom. Uvek treba imati u vidu koji procesi odgovaraju trenutnom dokazu. Ovo je veoma bitno da bi se skratilo vreme potrebno za analizu. U ovom koraku mora se voditi računa o tome da *SHA*-1 heširanje i dešifrovanje *EFS* fajla nisu podrazumevano uključeni, pa se moraju po potrebi naknadno uključiti (slika 4.46).



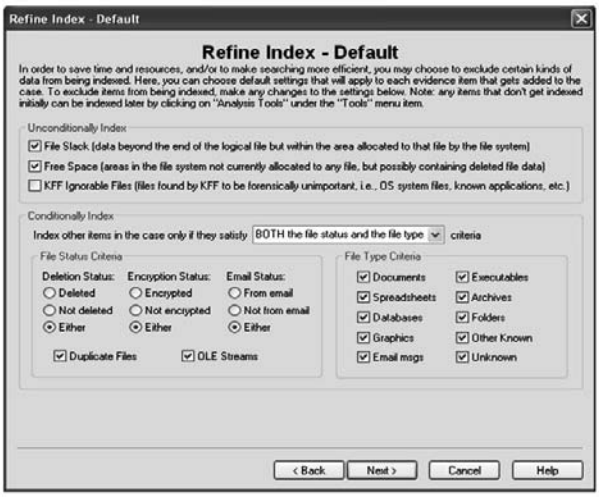
Slika 4.46 Processes to Perform opcija

Refine Case opcija omogućava da se iz slučaja izuzmu određeni tipovi podataka. Preporučuje se da se uključe svi tipovi podataka kada se dodaje novi dokaz u slučaj, pošto naknadno dodavanje nije moguće. Ukoliko se neki tip podataka isključi, on neće biti razmatran ni u jednom dokazu koji se naknadno dodaje u slučaj (slika 4.47).



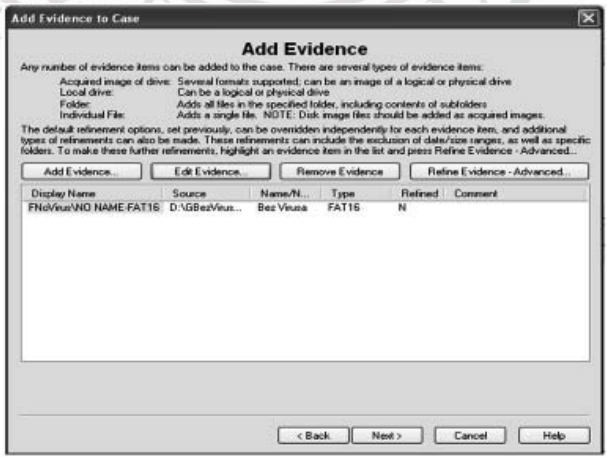
Slika 4.47 Refine Case

Indeksiranje podataka je veoma dobra opcija koju FTK forenzički alat omogućava. Indeksiranje omogućava brže pretraživanje, ali sa druge strane zahteva više vremena u procesu analize. Naravno, *Refine Index* omogućava da se neki tipovi podataka isključe iz indeksiranja, čime se vreme analize skraćuje. Preporučuje se da se prihvate podrazumevana podešavanja za indeksiranje podataka (slika 4.48).



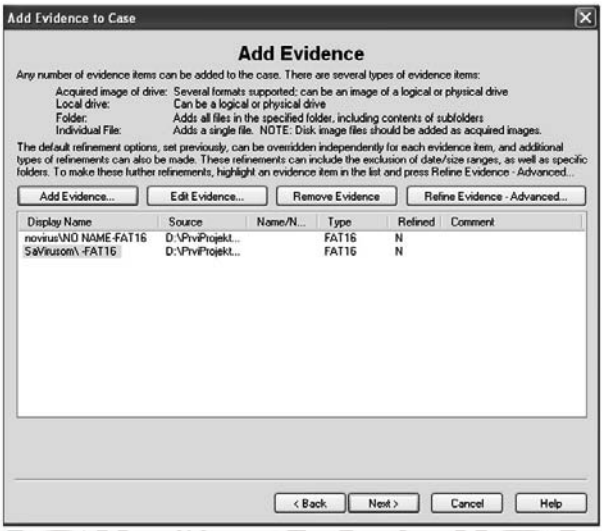
Slika 4.48. Refine Index opcija

Konačno, posle svih podešavanja, može se dodati dokaz ili više njih (slika 4.49).



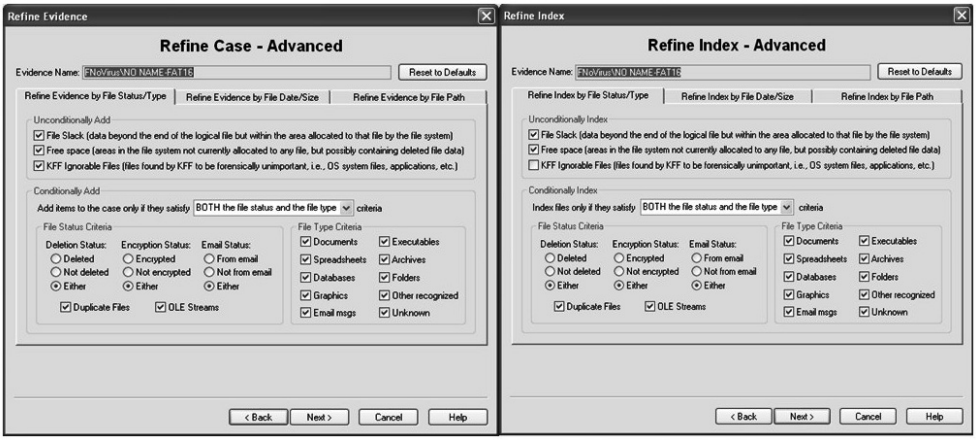
Slika 4.49 Add Evidence opcija

Kao dokaz mogu se uneti imidž, lokalni disk, sadržaj foldera ili pojedinačni fajl. Da bi se sačuvao integritet dokaza, oni se dodaju sa atributom *Read Only*. Svaki uneti dokaz može se menjati, a takođe može se i ukloniti sa liste dokaza. Na slici 4.50 prikazan je primer dodavanja novog dokaza - imidža virusom zaraženog i nezaraženog USB memorijskog uređaja.



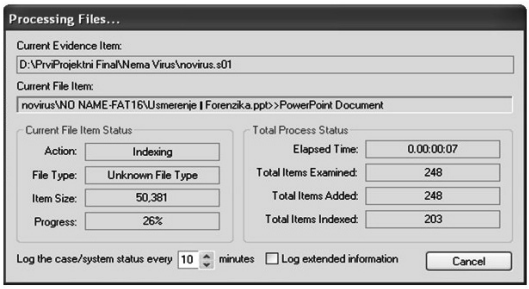
Slika 4.50 Dodavanje imidža dva USB memorijska uređaja kao dokaza

Pod opcijom *Refine Evidence – Advaced* mogu se ukloniti određeni tipovi, datumski ograničeni fajlovi ili fajlovi sa određene putanje iz svakog pojedinačnog dokaza. U ovom delu moguće je na isti način predefinisati indeksiranje za svaki dokaz opcijom *Refine Index – Advaced* (slika 4.51).



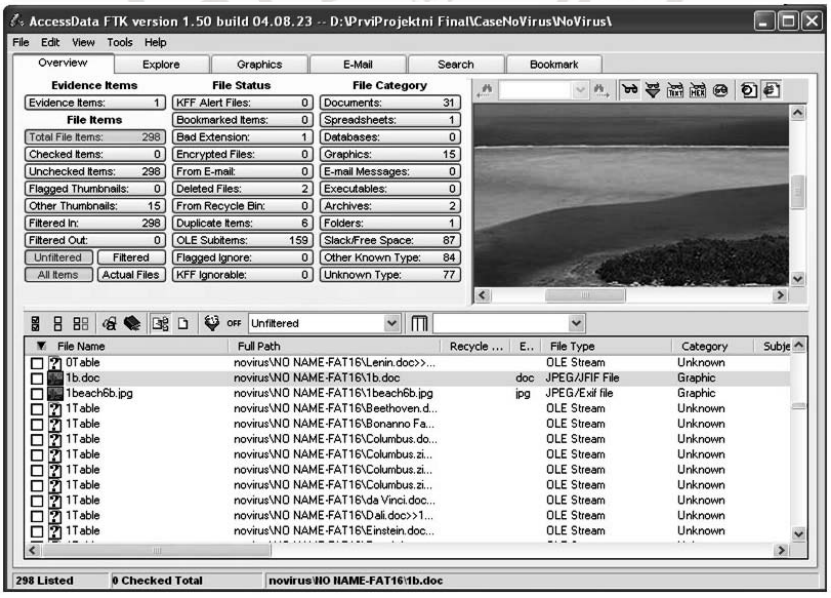
Slika 4.51 Napredne opcije Refine Evidence i Refine Index

Na samom kraju, na prozoru *Case Summary*, pregledno se može proveriti sve ono što je uključeno u slučaj sa svim dokazima i procesima nad njima. U ovom koraku moguće je vratiti se na bilo koji prethodni i izvršiti neku korekciju. Ukoliko su sva podešavanja dobra i svi dokazi obuhvaćeni može se pristupiti obradi dokaza. U narednom koraku može se odrediti vremenski interval upisa u log fajl (slika 4.52).

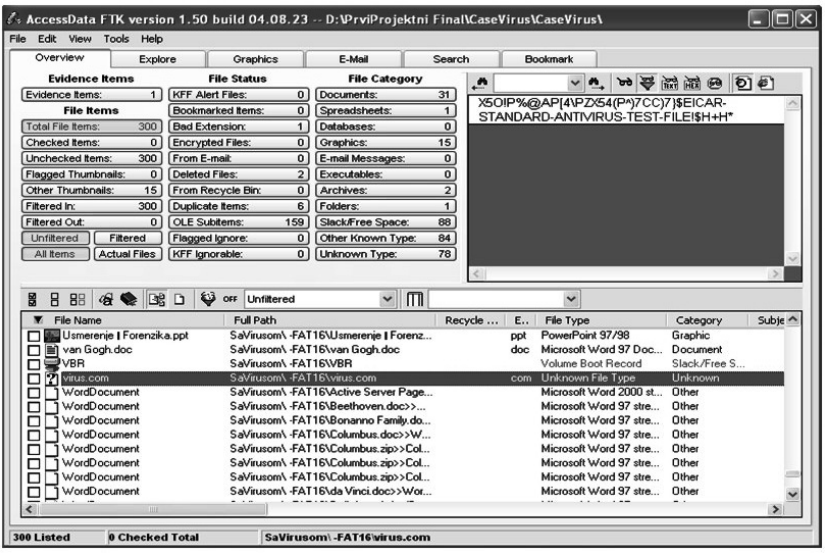


Slika 4.52 Obrada dokaza

Pregled dobijenih rezultata. Kada se otvori postojeći slučaj, odabirom raznih opcija sa početnog prozora, mogu se pregledati fajlovi sa svim svojim karakteristikama kao što su putanja ili tip fajla. Moguće je pregledati strukturu direktorijuma svakog fajla. Postoji mogućnost pregleda grafičkih fajlova sa opcijom odabira onih koje želimo da prikažemo u izveštaju (slika 4.53). Takođe, postoji mogućnost pretraživanja po ključnoj reči, kao i obeležavanje bitnih informacija uz dodavanje komentara (slika 4.54) .

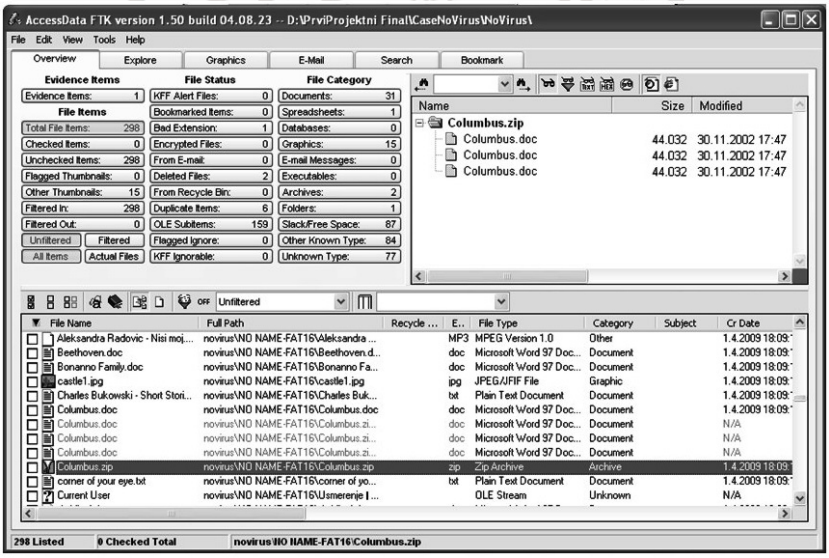


Slika 4.53 Kartica Overview

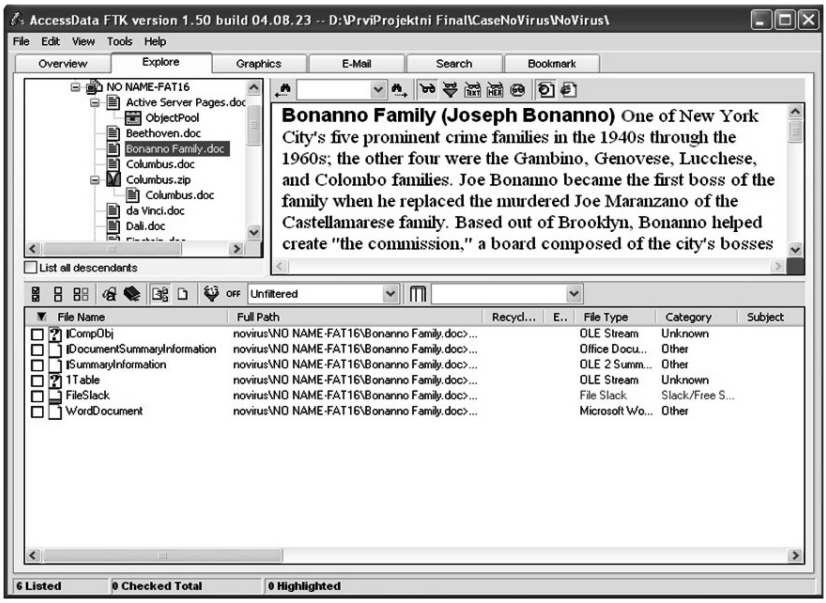


Slika 4.54 Obeležen prepoznati maliciozni program na zaraženom USB

Posebno bi trebalo naglasiti da FTK forenzički alat omogućava pregled sadržaja kompresovanih fajlova kao što su ZIP, RAR i drugih. Osim prikaza, FTK forenzički alat vrši i dekompresiju ovih fajlova (Slika 4.55).



Slika 4.55 Pregled sadržaja kompresovanog fajla



Slika 4.56 Kartica Explore

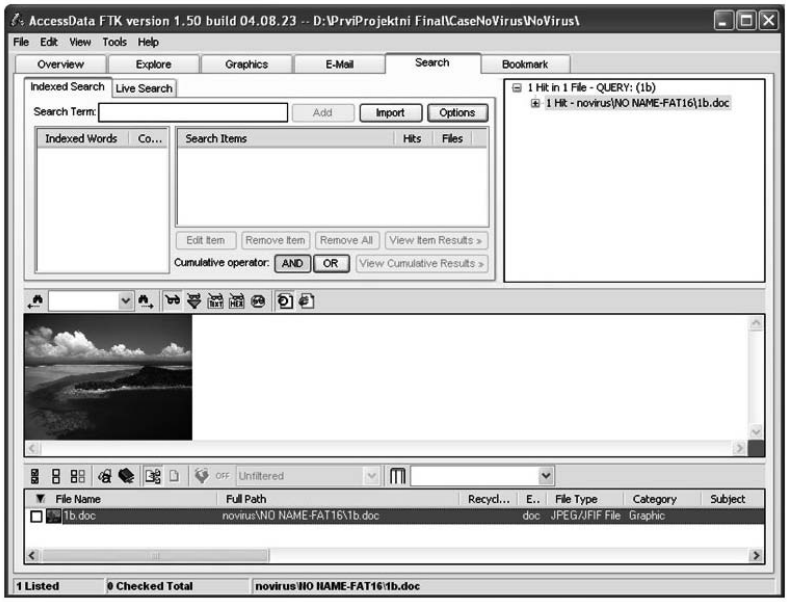
Kartica *Explore* omogućava pregled direktorijuma i foldera ispitivanog imidža sa mogućnošću unosa komentara forenzičara (slika 4.56).

Kartica *Graphics* omogućava pregled slika (*tumbnails*) imidža (slika 4.57). Obeležena slika (*1b.doc*) ima ekstenziju .doc. Kako je česta praksa promena ekstenzije korumpiranog fajla, ako se fajlu slike promeni ekstenzija u *.doc* fajl, ovaj fajl postaje neupotrebljiv za Word aplikaciju. Slika *1b.jpg* je preimenovana u *1b.doc* i Microsoft Office Word, kao aplikacija koja otvara *.doc* fajlove ne može da otvori preimenovani fajl. Međutim, kartica *Graphics* prikazuje pravu sliku i prepoznaje tip fajla JPEG. Bez obzira na promenu ekstenzije fajla navedene slike, FTK forenzički alat je uspešno prepoznao sliku u JPEG formatu.



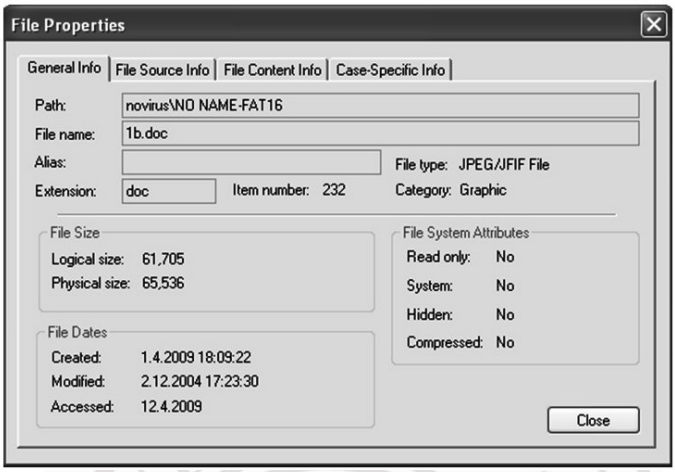
Slika 4.57 Kartica Graphics

Kartice E-*mail* i *Search* omogućavaju ispitivanje zaglavlja e.mail poruka i pretraživanje fajlova ispitivanog imidža po ključnoj reči. Na raspolaganju je i pretraživanje fajlova imidža po indeksima (kartica *Bookmark*), (slika 4.58)



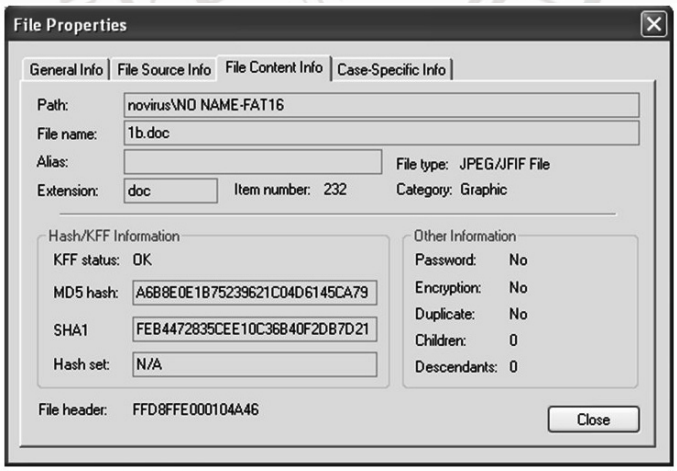
Slika 4.58. Kartica Search

Kada je potrebno pregledati svojstva fajlova, FTK forenzički alat ima i tu mogućnost. Biranjem opcije *File Properties* iz komande glavnog menija *Tools* dobijaju se sva svojstva selektovanog fajla (slika 4.59).



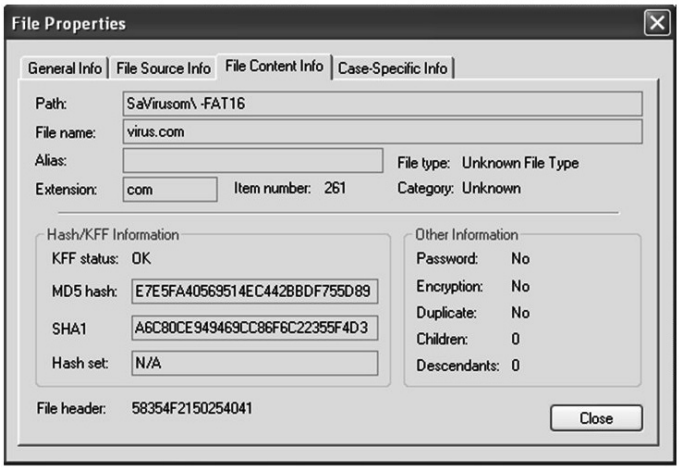
Slika 4.59 Generalne informacije o svojstvima fajla

Posebno je značajna kartica *File Content Info* gde može da se, pored putanje, naziva i ekstenzije fajla pročitaju heš vrednosti fajla, heder fajla, te KFF status i još dodatne informacije poput lozinke, duplikata ili šifrovanja fajla (Slika 4.60).



Slika 4.60 Informacije o sadržaju fajla

Na isti način mogu se ispitati svojstva nepoznatog fajla sa virusom (Slika 4.61).



Slika 4.61 Pregled karakteristika malicioznog programa

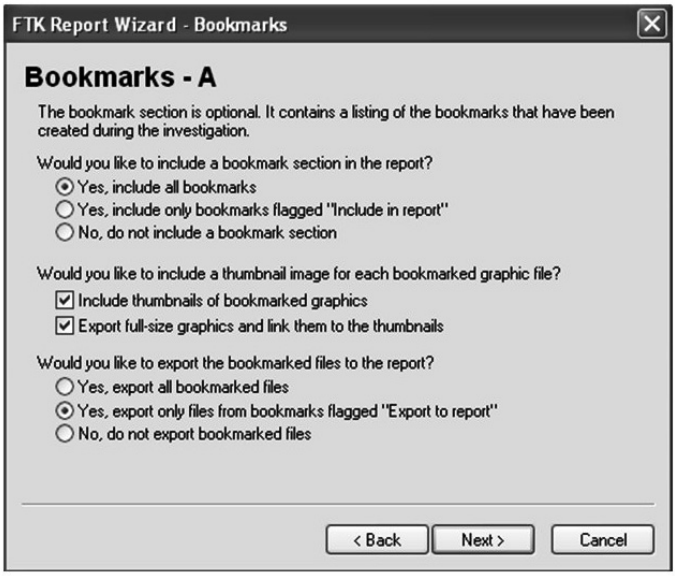
Pored ovoga, u postojeći slučaj je moguće dodati novi dokaz. Novi dokaz se dodaje na identičan način kao kada u novom slučaju po prvi put dodajemo nove dokaze. Dodavanje novog dokaza je moguće samo ukoliko slučaj nije otvoren u *Case Agent Mode*, koji ima atribut *Read Only* i ne dozvoljava dodavanje novih dokaza.

Kreiranje izveštaja. Izveštaj u formi tekstualnog log fajla, FTK forenzički alat automatski generiše (slika 4.62).



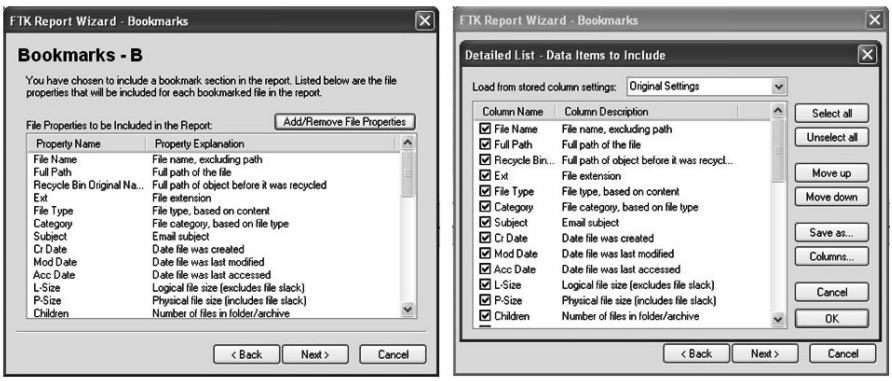
Slika 4.62 Deo FTK log izveštaja

Log izveštaj može biti uključen u generatoru izveštaja koji kreira izveštaj u HTML formatu. Generator izveštaja omogućava podešavanje prikaza određenih podataka u izveštaju. Pored osnovnih informacija o forenzičaru i slučaju, generator izveštaja opciono nudi i informacije o podešavanju mnogih drugih parametara, na primer indeksa (*bookmarks*), koje treba po zahtevu/potrebi uključiti u log izveštaj (Slika 4.63).



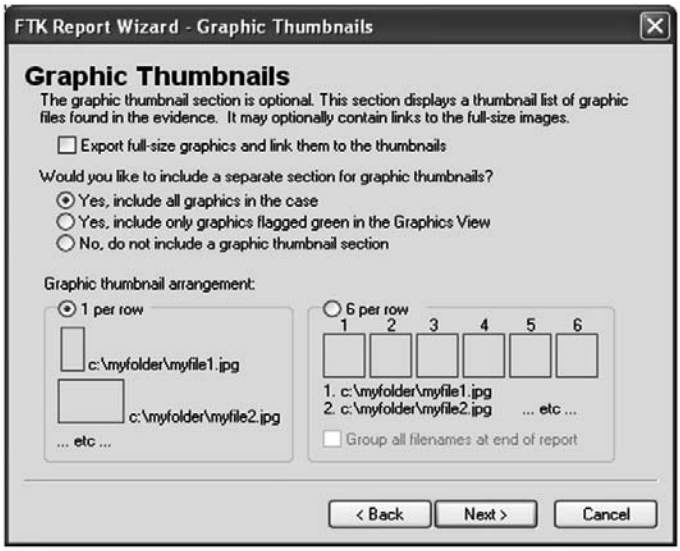
Slika 4.63 Podešavanje za prikaz Bookmark-ova

Kreirani *Bookmark*-ovi mogu biti uključeni u izveštaju, a ne moraju. Mogu biti uključeni svi, a mogu se odabrati samo oni koji su obeleženi kao *''Include in report''*. Takođe, postoji mogućnost odabira svojstva svakog *Bookmark*-a koja će biti prikazana u izveštaju (Slika 4.64).



Slika 4.64 Odabir svojstva Bookmark-a i prikaz u izveštaju

Prikaz grafičkih elementa u izveštaju je veoma bitno. U izveštaju mogu biti prikazani svi grafički elementi, samo oni koji su obeleženi ili ne moraju uopšte biti prikazani (Slika 4.65).

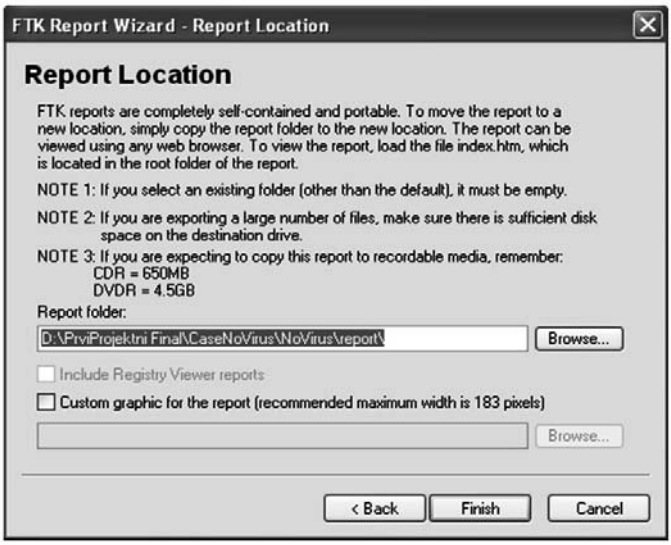


Slika 4.65 Podešavanje prikaza grafičkih elemenata u izveštaju

Prilikom kreiranja izveštaja postoji još niz podešavanja kao što su putanja fajlova u odabranoj kategoriji, lista svojstava i odluka koja od njih da se prikazuje, lista fajlova u odabranoj kategoriji, uključivanje *MS Access* baze podataka u izveštaj itd.

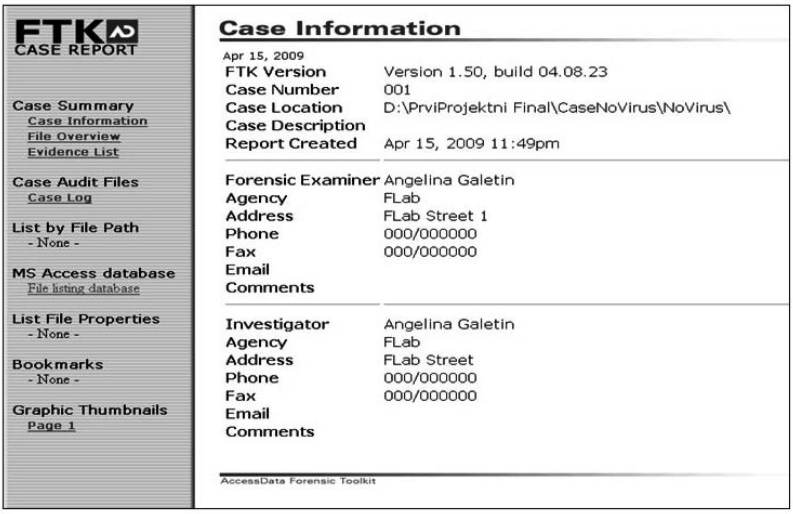
Ono što je posebno bitna odlika FTK forenzičkog alata je mogućnost uključivanja drugih fajlova kao što su lista heš vrednosti, rezultati pretrage ili log fajl. Po podrazumevanom podešavanje log fajl se priključuje izveštaju.

Kada se odabere putanja izveštaja, moguće je dodati i proizvoljni grafički element (Slika 4.66).

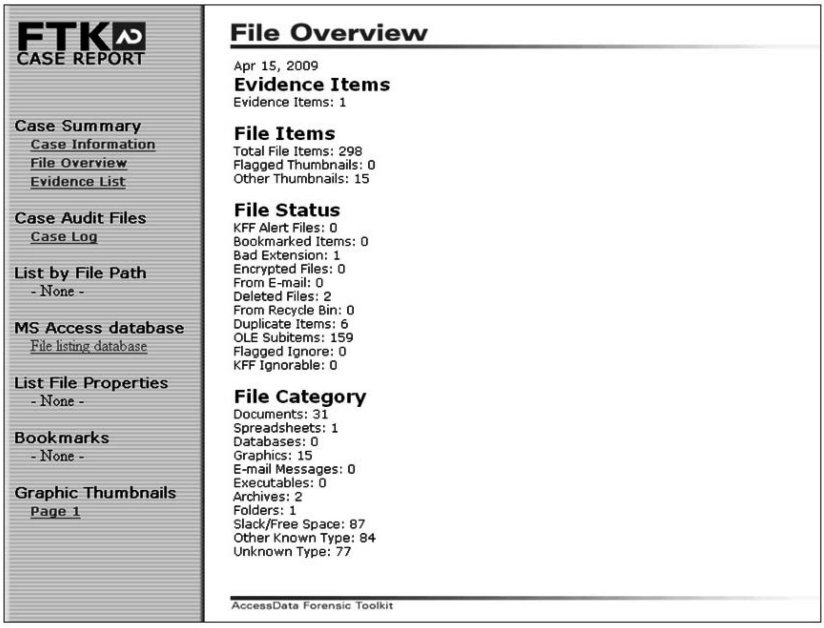


Slika 4.66 Odabir putanje izveštaja i proizvoljnog grafičkog elementa

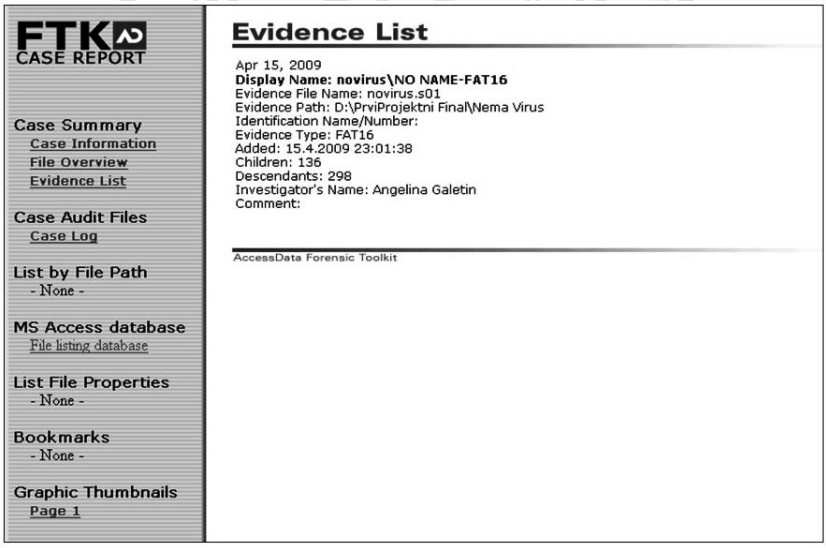
Kada je izveštaj kreiran, on se nalazi u HTML formatu i može ga prikazati Internet Explorer ili bilo koji drugi pretraživač ili program koji prikazuje HTML format (slika 4.67-69).



Slika 4.67 Početna strana izveštaja (index.htm)

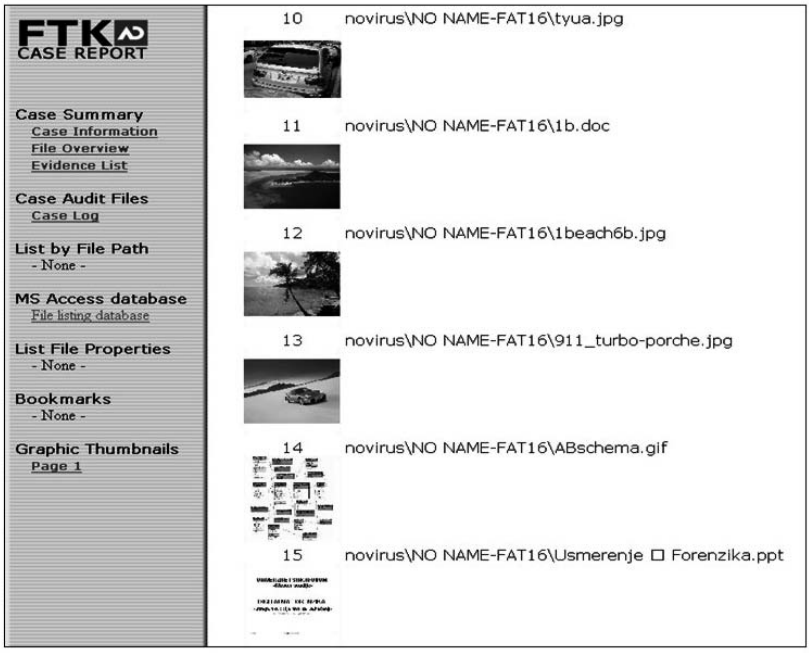


Slika 4.68 Pregled fajlova u izveštaju



Slika 4.69 Pregled dokaza u izveštaju

U meniju sa leve strane FTK izveštaja nalaze se svi oni elementi koji su unapred bili odabrani za prikaz prilikom kreiranja izveštaja. Jednostavnim klikom na neki od njih u središnjem delu se prikazuje odabrani sadržaj (slika 4.70).



Slika 4.70 Prikaz grafičkih elemenata u izveštaju

FTK forenzički alata nudi opciju ažuriranja izveštaja. Kada je izveštaj kreiran, moguće je izvršiti ažuriranje u smislu izmene prikaza podataka. Ukoliko želimo da dodamo novu sekciju u izveštaj potrebno je izvršiti modifikaciju izveštaja.

U tabeli , predstavljene su tabelarno funkcije FTK forenzičkog alata po koracima digitalne forenzičke istrage.

Tabela 4.1 Pregled funkcija FTK forenzičkog alata

AKVIZICIJA
U procesu akvizicije FTK forenzičkim alatom može se izvršiti fizičko kopiranje podataka, te logičko kopiranje podataka. Posebna je prednost odabir formata akvizicije podataka gde svaki tip ima kako svoje prednosti tako i svoje nedostatke. Akvizicija FTK forenzičkim alatom je u potpunosti GUI proces, a proces komandne linije nije omogućen. FTK forenzički alat u procesu akvizicije vrši i verifikaciju, što je u svakom slučaju pozitivna karakteristika. Ono što se može navesti kao nedostatak FTK forenzičkog alata u procesu akvizicije jeste nemogućnost vršenja udaljene akvizicije.
VALIDACIJA I DISKRIMINACIJA
FTK forenzički alat se u procesu validacije i diskriminacije odlikuje dobrim karakteristikama. Što se tiče heširanja, FTK forenzički alat vrši 128 bitno MD5 heširanje i SH1 160 bitno heširanje. FTK forenzički alata vrši filtriranje fajlova. Takođe, vrši se i analiza hedera fajlova.
EKSTRAKCIJA
U zavisnosti od formata fajlova koje podržava, FTK forenzički alat omogućava čitanje podataka. U procesu ekstrakcije omogućeno je pretraživanje po ključnoj reči. Dobra karakteristika FTK forenzičkog alata je dekompresovanje fajlova, te rekonstrukcija fragmentovanog fajla (*Data Carving*). Pored navedenih osobina, FTK forenzički alata kao pozitivnu karakteristiku ima i dešifrovanje fajlova. FTK forenzički alata u procesu ekstrakcije omogućava označavanje dokaza.
REKONSRUKCIJA BEZBEDNOSNOG DOGAĐAJA
Ono što u ovom radu nije urađeno, ali predstavlja karakteristiku FTK forenzičkog alata u procesu rekonstrukcije bezbednosnog događaja svakako treba navesti. FTK forenzički alat u procesu rekonstrukcije bezbednosnog događaja omogućava kopiranje diska na disk i kopiranje imidža na disk. Ne postoji mogućnost kopiranja particije na particiju, kao ni kopiranje imidža na particiju.
IZVEŠTAVANJE
FTK forenzički alat se pokazao kao dobar alat za generisanje izveštaja. Prilikom analize FTK forenzičkim alatom se generiše log izveštaj koji beleži dešavanje u toku analize. Pored toga, FTK forenzički alat poseduje i generator izveštaja sa mnogobrojnim podešavanjima, što je dobra karakteristika. Između ostalog u izveštaj generisan FTK forenzičkim alatom može se uključiti i log izveštaj.

4.4.4 Forenzički alati otvorenog izvornog koda

4.4.4.1 Značaj poznavanja izvornog kôda 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, [4]:

- ***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 porizvođače/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 zaineresovani da učestvuju u naporima za proračun stepena grešaka.

Koncept forenzičkih alata sa otvorernim 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 integrieteta.

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.

Neki od značajnijih forenzičkih alata mogu se naći na sledećim web adresama:

- **Ultimate Toolkit (UTK),** *(AccessData)* http://www.accessdata.com.
- **EnCase** *(Guidance Software Forensics)***,** http://www.guidancesoftware.com.
- **Maresware Computer Forensics software**, http://www.dmares.com**.**
- **Paraben,** http://www.paraben.com.
- **ProDiscover** *(Technology Pathways),* http://www.prodiscover.com.
- **SMART** *(ASR Data)***,** http://www.asrdata.com.
- **X-Ways Forensics,** www.x-ways.net.
- Više forenzičkih alata može se naći na web adresi http://www.forensics.nl/toolkits.

4.4.4.2 Forenzički alati otvorenog kôda

U *forenzičke alate otvorenog kôda* - OSS ubrajaju se alati na bazi *Unix* i *Linux* OS. Brojni alati iz spektra Unix programskih uslužnih alata kao što je **[*shell, tee,*» I « & ><]** omogućavaju forenzičaru usmeravanje (*piping*), preusmeravanje, pravljenje skriptova i automatizaciju, [32].

Najpoznatije *Linux* distribucije su: *Knopix, Ubuntu Redhat, Novell/SuSe* i dr. Najpopularnije distribucije su *KDE* i *Gnome* koje obezbeđuju desktop GUI slične Unix-u, MS Windows, Machintosh i NeXT OS. Ovi alati generišu napredno *shell* okruženje, *web* i GUI ulazno/izlazne interfejse. Najpoznatiji alati su **KDE, Gnome, Windowmaker, bash, zsh, emacs i mc**. Linux okruženje omogućava kreiranje forenzičkog butabilnog CD ili DVD, koji obezbeđuje butovanje ispitivanog računara bez podizanja procesa butovanja ispitivane mašine. Linux platforma, takođe, obezbeđuje na bazi **Knoppix**-a obiman skup pre-instaliranih forenzičkih alata, uključujući: **FCCU, GNU/Linux Forensic Boot CD** (koristi ga Federalna policija za kompjuterski kriminal Belgije), **Helix** (*US e-fense Inc*.). Za punu instalaciju treba napisati skript:

-> Ubuntu, doing forensics -> Debian,

koji automatizuje servise butovanja. Linux alati uzimaju imidž i vrše akviziciju podataka sa brojnih medijuma, kao što su: ATA, SATA, SCSI i USB čvrstih diskova, *Firewire*, CD, DVD, USB stikova, traka, disketa itd. Alati praktično uzimaju bezbedno podatke sa svih medijuma na kojim su podaci uskladišteni u sektore. Takođe, skidaju slike bez instalacije drajvera, ne zahtevaju hardverske blokatore upisivanja, upravljaju greškama i lošim (*bad*) sektorima. Najpoznatiji alati su: [**dd, dcfldd, dd_rescue, sdd, AIR, sleuthkit, adepto, grab.**

Alati kao što su **gzip, openssl, dcfldd, gnupgp, split, md5** vrše kompresiju imidžovanih podataka, klasifikaciju po tipu fajla, preusmeravanje i omogućavaju šifrovanje, digitalno potpisivanje i hešovanje podataka imidža. Linux bazirani set alata[**pilot-link, gnupod, gnokii, opensc,** omogućavaju pristup brojnim priručnim i ugrađenim računarima kao što su PDA, iPod, digitalna kamera, mobilni telefon i smart kartice.

Za izvlačenje i formatiranje podataka iz fajl sistema standardno se koristi **dd** alat za uzimanje sirovog imidža fajl sistema. Napredni forenzički alat -**AFF** (*Advances Forensic Format*) **dd** i **afflib** su alati otvorenog koda, ekvivalentni formatu fajla *EnCase.E0** **EnCase** alata.

Za zaštitu integriteta digitalnih podataka i dokaza Linuks bazirani forenzički alati **md5sum, openssl, dcfldd, gnupg, openTSA**, omogućavaju kriptografski heš (MD5, SHA1), digitalni potpis forenzičara (**PGP/GPG, SMIME**), vremenski pečat (**TSA, RFC 3161**).

Za pakovanje imidžovanih podataka Linux alati **tar, zip, gzip, bzip, openssl, gnupg** arhiviraju sa kompresijom i opciono šifrovanjem, više fajlova/direktorijuma u formatima koji ne zavise od tipa proizvoda i proizvođača. Za skladištenje podataka na različite medijume za skladištenje (CD, DVD, traku) i bekapovanje koriste se alati tipa*:* **dump,**

tar, amanda, cdrecord, a za interni transfer digitalnih dokaza sa šifrovanjem i jakom autentifikacijom koriste se alati kao što su: **scp, apache-ssl, smime, pgp**.

Alati za detekciju izbrisanih particija i restauraciju su: **gpart, disktype, testdisk, hexedit –sector**. Za oporavak izbrisanih fajlova iz većine fajl sistema, oporavak podataka iz *fajl slack* prostora i sastavljanje izbrisanih fajlova iz fragmentisanih klastera mogu se koristiti alati tipa: **gpart, sleuthkit, formost, fatback, e2salvage, formost, disktype, testdisk, scrounge-ntfs, scapel, magicrescue**.

Za šifrovane i steganografski sakrivene podatke, oporavak lozinke i detekciju steganografije mogu se koristiti alati kao što su: **fcrackzip, crack, lcrack, nasty, john the ripper, stegdetect, stegbreak, cmospwd, pwl, madussa**.

U procesu digitalne forenzičke analize za pretraživanje i filtriranje podataka relevantnih za digitalni dokaz koristi se baza heš vrednosti poznatih sistemskih fajlova, poznatih aplikacija i antivirusnih i anti rutkit programa kao što su: **clamAV, F-PROT, chkrootkit, grep, autopsy, find, swish-e, glimpse, ftimes, md5deep, hashdig.**

Za utvrđivanje vremenske linije napada, korelaciju i sortiranje mogu se koristiti odlični **Sleutkit** proizvodi, kao što su: **pyflag, autopsy, zeitline, sleuthkit.**

Alati tipa **ghex, khex, hexedit, openssl, uuencode, mimedecode, hexdump, od, strings, antiword** predstavljaju širok spektar konvertora, heks editora, analizatora e-*mail* priloga, alata za analizu podataka i log fajlova (*cookies* fajlova, keša *browsers, Internet istorije itd*.).

Za gledanje tekućih i starih dokumenata/Slika i multimedijalnih sadržaja može se koristiti veliki broj alata za upravljanje *thumbnail-s* (male slike za istovremeni pregled) sa skriptom, manipulaciju Slika, konfigurisanje reprodukcije video snimka različitih formata, kao što su: **openoffice, gv, xv, imagemagic, mplayer, vlc.** Za podizanje i pretraživanje sumnjivih Slika na *read only* način u različitim fajl sistemima (Apple, Microsoft, različiti Unix) mogu se koristiti **mount, losetup**. Za virtuelno butovanje slike na Linux PC, MacOS9 i OSX Slika, Windows Slika i drugih Linux Slika (X86 OS) koriste se alati **pearpc i VMWare**.

Alati **dosemu, wine, VMWare, pose, x48, linux-abi** su simulatori za aktiviranje programa koji rade na DOS/Windows, Mac, HP48 i različitim Unix operativnim sistemima. Brojni alati se koriste za analizu zastarelih sistema i to:

- **xzx, fuse, x81** za PC iz 80- i 90-tih kao što su Sinclair ZX Spectrum, ZX81;
- **xgs, prodosemu, vMac, basiliskII** za Apple IIGS, prvi Machintosh PC;
- **vice, frodo** za Commodore C64, C128, VIC20, PET i CBM-II;
- **uae, hatari, e-uae** za Amigu;
- **stonx, atari800** za *AtartiST, Atari 800* ;
- **hercules** za mainframes i mini računare IBM System/370, ESA/390;
- **sim, klh10** za Dec PDP-seriju, Nova i IBM 1401;
- **doscmd, dosbox, dosemu** za MS-DOS;
- **cpmemu** za CPM.

Upravljanje forenzičkim slučajem, indeksiranje (*bookmarking*) i izveštavanje automatski generisanim izveštajem u .pdf formatu moguće je u izvesnoj meri. Integrisani sistem indeksiranja je teško ostvariti i zahteva suviše mnogo posebnih alata, kao i integrisano izveštavanje, ako se koristi više alata. Često je upravljanje forenzičkim slučajem rudimentarno i zasniva se na bazi upravljanja fajlovima/direktorijumima. Za upravljanje, indeskiranje i izveštavanje u forenzičkom slučaju mogu se koristiti alati: **pyFlag, autopsy, sleuthkit, Latex, pdf tools**.

Za *Microsoft* sisteme – analizu regisatra, log datoteke događaja, *INFO2* i *Recycle bin, .cab* fajlova i OLE svojstava mogu se koristiti sledeći alati: **ntreg, kregedit, regviewer, grokevt, rifiuti, orange, fccudocprop**.

Za analizu *Outlook* i *IE* pretraživača, konverziju MS *Outlook* **.pst** fajlova u otvoren tekst, analizu keš fajlova i kolačića (*cookies*) koriste se alati: **libpst, readpst, pasco, galleta**.

Prikupljanje paketa u mrežnoj forenzici može se izvršiti sa alatima kao što su: **tcpdump, etherreal, tcpflow, ssldump, tcptrace, ngrep, driftnet**, bazični alati za digitalnu forenzičku istragu na Internetu su: **nslookup, dig, whois, traceroute**.

Za aktivnu digitalnu forenzičku akviziciju (*Live Digital Forensic Aquisitions*), ispitivanje memorija, stanja sistema i konfiguracije, log fajlova i host baziranih IDS sistema mogu se koristiti alati kao što su: **ps, netstat, ifconfig, lsof, memdump, tripwire**.

Digitalna forenzika softvera - emulatora/simulatora, debagera, *dissassemblers* i reverzni inženjering vrše se alatima kao što su: **gdb, strace, coreography, fenris, truss i dtrace (Solaris)**.

Za digitalnu forenzičku istragu često se korisni i brojni ne-forenzički alati za otkrivanje grešaka u hardveru i softveru i otklanjanje bagova (*debugging tools*), konverziju i migraciju podataka, popravljanje podataka, procesiranje log fajlova, alati za statističke proračune i proračun trenda i dr.

Poznatiji izvori za Linux alate su sledeće web lokacije: e-evidence.info, opensource-forensics.org, Linux-forensics.com, freshmeat.net i sourceforge.net.

4.4.4.3 SPADA forenzički alat na bazi Linux OS

Na slici Slika 4.71 prikazan je desktop softverskog forenzičkog alata SPADA na bazi Linux OS, [28].



Slika 4.71 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 proveri podešavanje BIOS-a da se uveri da će se računar butovati sa CD-ROMa.

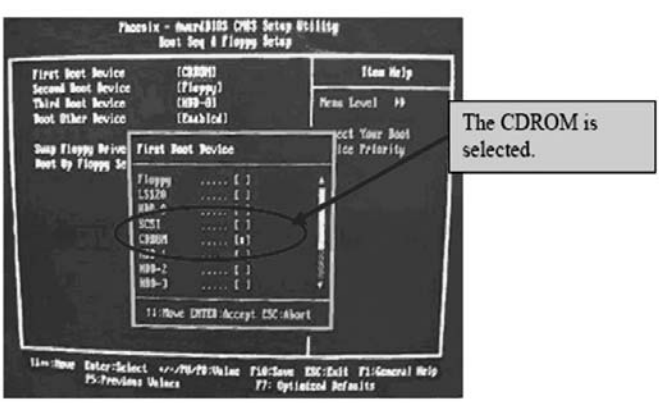
Mnogi računari pokazaće, tokom POST[52] procesa, poruku koja indicira kako se ide u BIOS prozor za podešavanje (*Setup Screen)*. Ako se ovo ne prikaže aktiviranjem nekoliko tipki tastature u toku procesa POST, često će se generisati POST greška i dopustiće pristup BIOS *Setup*-u, slika 4.72.

52 Power On Self Test



Slika 4.72 Aktiviranje POST procesa za pristup BIOS setup-u

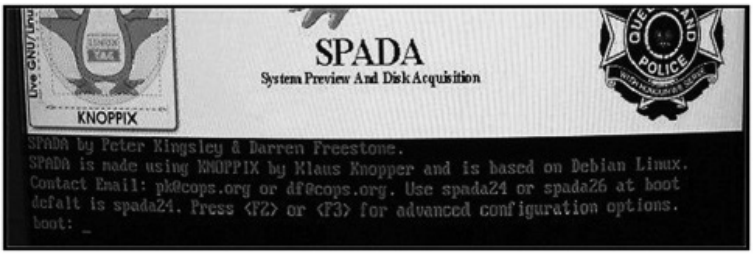
Tipičan ekran za podešavanje BIOS-a prikazan je na sledećoj slici, (slika 4.73).



Slika 4.73 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 podšavanja ne treba menjati, a treba napraviti pisanu zabelešku o izvršenoj promeni.

2. Korak: Kada se PC konfiguriše da se butuje sa CD-ROMa, treba ubaciti CD u drajv i restartovati i rebutovati sistem. Forenzičar mora posvetiti posebnu pažnju na aktivnosti na ekranu i treba da vidi SPADA meni za butovanje kao na slici slici 4.74.



Slika 4.74 SPADA meni za butovanje

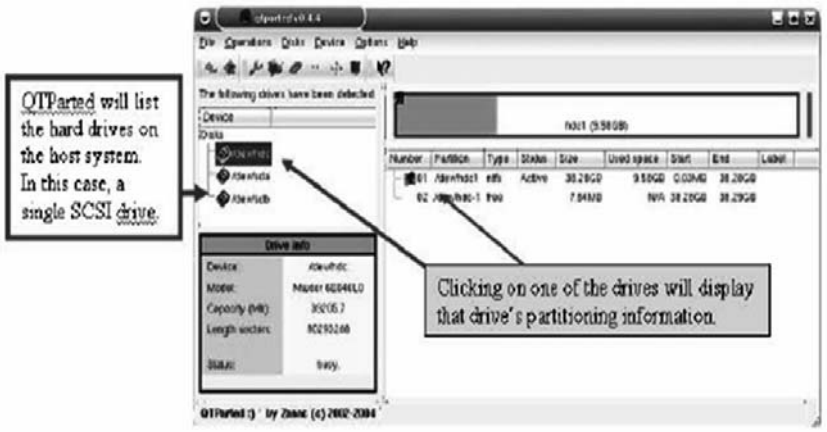
Postoje dve bazične predefinisane opcije za butovanje u Linux *kernelu 2.4*. Ovaj izbor treba da radi sa većinom sistema. Ako ne radi, treba eksperimentisati sa naprednim opcijama. Aktiviranjem *Enter* tipke tastature treba da podigne sistem. Proces treba posmatrati i biti spreman na reagovanje na svako 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 4.75).



Slika 4.75 Aktiviranje procesa inicijalne pretrage sa SPADA alatom

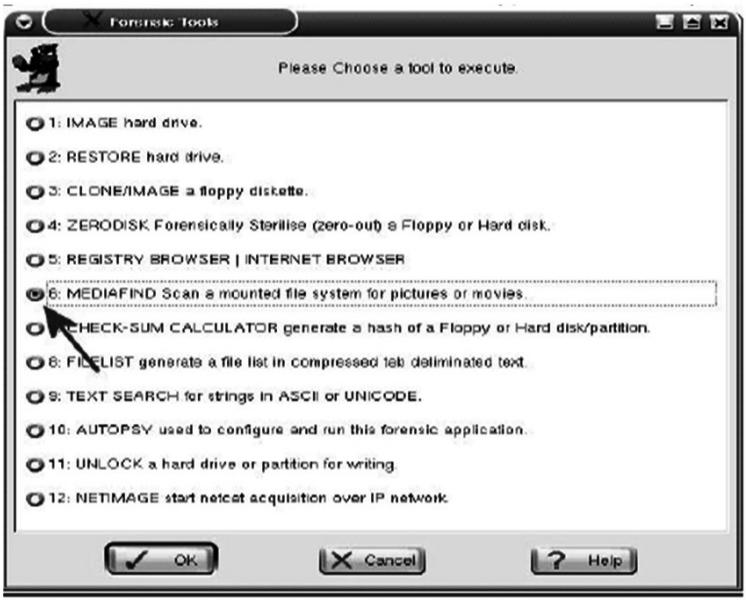
QTParted aplikacija se prva pokreće da se forenzičar upozna sa HD na host sistemu i kako je particioniran. Forenzičar treba da pažljivo notira imena diskova prikazana u prozoru *Device* u *QTParted* aplikaciji, zato što ta informacija može trebati kasnije. Kada se ove informacije notiraju, aplikaciju treba zatvoriti, ili minimizirati, (slika 4.76).



Slika 4.76 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 4.77).



Slika 4.77 Aktiviranje Mediafind aplikacije u SPADA alatu

Treba izabrati No.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 slici 4.78.



Slika 4.78 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 Slika4.79. 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 4.79 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.

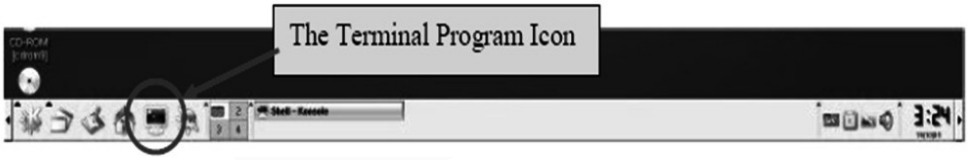
Komandna linija SPADA/Linux programa potrebna je, jer se mogu pojaviti slučajevi gde je poznavanje komandne linije korisno, iako je korišćenje Linux GUI-a veoma lako, na primer, neka nestandardna video karta može se neuspešno podizati sa GUI *Windows* XP sistemom. Kada se to dogodi, izlaz treba potražiti u komandnoj liniji. U tabeli 4.1. prikazane su korespondirajuće DOS i Linux komandne linije.

Tabela 4.2 Korespondirajuće DOS i Linux komandne linije

DOS Command	Linux Command
DIR	ls
CD	cd
MD	mkdir
COPY	CP
DEL	rm
REN	mv
ATTRIB	chmod

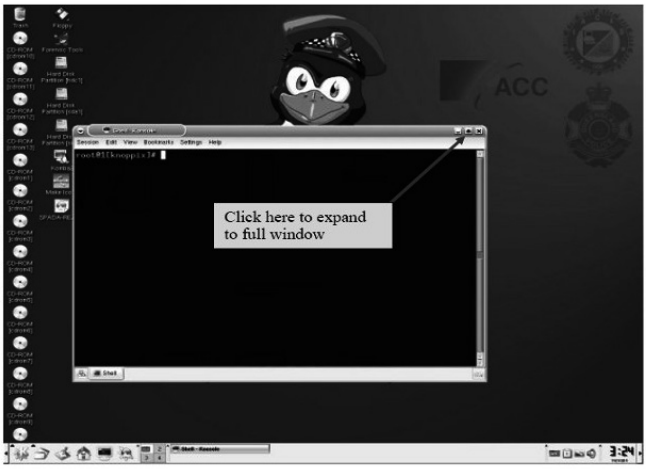
Takođe, treba znati da je Linux sistem osetljiv na veličinu slova, za razliku od DOS operativnog sistema. Ako se radi u Linux komandnoj liniji, imena fajlova, ili putanje sa mešovitom veličinom slova alfabeta, moraju se otkucati tačno onako kako se pokazuju. Druga osobina Linux-a je da ne prihvata prazan 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 Sett*ings u Windows biće *cd:\Documents?and?Settings* u Linix komandnoj liniji.

Ekvivalent DOS, ili Windows prozora u Linix 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, (Sslika 4.80).



Slika 4.80 Otvaranje Terminal prozora u SPADA alatu

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 4.81).



Slika 4.81 Proširivanje Terminal prozora u SPADA alatu na puni ekran

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 4.3. prikazani su različiti *ls* svičevi, [28].

Tabela 4.3 Svičevi za za definisanje načina rada ls komande

-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-direkroriju-mu 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.

4.4.4.4 Prednosti i nedostaci Linux baziranih forenzičkih alata

Prednosti i nedostatke Linux/Unix forenzičkih alata treba razmatrati u odnosu na primenu na terenu i u forenzičkoj laboratoriji.

Raspoloživost Linux forenzičkih alata je veoma visoka. Softver je besplatan i dostupan na Internetu, a izvorni kôd je obezbeđen. Alate je moguće dovesti do izvanredne tačnosti i *efikasnosti* primene, pošto dopuštaju veći stepen automatizacije i unošenja programskih kôdova (skriptova). Ova svojstva su korisna za analizu više slučajeva u isto vreme i veći obim laboratorijske forenzičke analize. Kako se izvorni kôd može slobodno menjati ovi alati su korisnički prilagodljivi i mogu se učiniti optimalnim u datom okruženju.

Podrška ovim alatima je brza i efektivna, uključujući help desk, brzu implementaciju zakrpa i novih rešenja, što je idealno za akademske forenzičke laboratorije. Koristeći otvoren izvorni kôd nezavisno od proizvođača, Linux usmerava na zajednički rad konkurentskih grupa, zasnovan na prethodnim iskustvima i obezbeđuje vremensku kompatibilnost tehnologija.

Osnovi nedostaci *Linux* alata u forenzičkoj laboratoriji su:

- obično zahtevaju dodatnu obuku forenzičara, vreme i rad za učenje,
- komandna linija nije toliko intuitivna kao GUI interfejs,
- nema formalne organizacije za podršku, iako je neformalna podrška interesne zajednice nekada superiornija,
- kvalitet podrške veoma varira,
- otežana je interoperabilnost sa drugim tehnologijama u vlasništvu (*Microsft*, npr.),
- u nekim slučajevima slaba je dokumentacija, gde izvorni kôd može biti jedina dokumentacija.

Pored problema velike količine digitalnih podataka za akviziciju i analizu, jedan od značajnijih problema digitalne forenzičke istrage je potreba da se u većini praktičnih slučajeva zahteva primena velikog broja različitih alata za akviziciju i analizu digitalnih podataka. Ovde nije problem primena velikog broja specijalizovanih alata koji izvršavaju najbolje određene forenzičke funkcije, nego potreba da se precizno razume kako ovi alati rade, što postaje sve složenije, kako se dodaju novi alati u nekom procesu. Na primer, većina forenzičara sugeriše da se koristi **Knoppix boot CD** za forenzičko butovanje ispitivanog računara sa Windows platformom, imidžovanje i ispitivanje čvrstog diska i uverava da je to forenzički ispravna praksa. Međutim, sve dok se ovaj alat dobro ne upozna, ne može se znati da **Knoppix** podrazumevano upisuje u *swap* fajl na čvrstom disku čim se poveže na računar, što može prepisati korisne podatke i uništiti forenzičku istragu. Naravno ova se akcija može onemogućiti u toku procesa butovanja, ali to treba znati i uraditi. Zato je odgovor na pitanje da li koristiti ovaj alat, pre „možda", nego „da".

Ako forenzičar zna šta traži, gde da to nađe i ako nađe relevantne podatke, za digitalni dokaz kompromitacije ispitivanog računara, to još uvek ne znači da zna šta se dogodilo i kako je došlo do incidenta. Na primer, u slučaju u kojem je osumnjičeni zaposleni optužen da je namerno izvršio defragmentaciju diska kada je saznao da forenzički tim dolazi da privremeno oduzme disk radi ispitivanja. Forenzičar je pregledom *prefetch* direktorijuma u NTFS fajl sistemi Windows XP OS otkrio da je defragmentacija izvršena neposredno pre oduzimanja, što je zaposleni negirao. Međutim, forenzičar nije znao *prefetch* funkciju i da Windows OS stavlja listu često korišćenih aplikacija u folder koji se zove *prefetch*, a koji se nalazi u Windows direktorijumu, ima ekstenziju **.pf** i tipično ima alfa numeričku sekvencu posle imena fajla**.** *Prefetch* je poboljšana karakteristika Windows OS. Forenzičar je pregledom *prefetch* direktorijuma video dva fajla: DEFRAG. EXE-23434DEF.pf i DFRGNTFS-2223rrdesfc.pf. Posmatranjem ova dva fajla i njihovih vremena modifikacije, izgledalo je da je zaposleni aktivirao defragmentaciju diska neposredno pre oduzimanja diska. Međutim, to nije bilo tačno. Forenzičar nije znao da Windows XP pokreće defragmentaciju diska automatski i u pozadini kada je sistem neaktivan (*idle*) neko specifično vreme, tipično 5 minuta. Da je to forenzičar to znao mogao je manuelno pokrenuti defragmentaciju diska, videti koji se fajlovi javljaju u *prefetch* direktorijumu i uporediti ih sa onima koje je prethodno otkrio. Da je ovo uradio forenzičar bi video da se fajlovi ne slažu. Dalje bi mogao proveriti na web-u (Google) ili nekom drugom mestu da ove fajlove u *prefetch* direktorijumu pravi Windows OS, vršeći optimizaciju performansi diska i da nisu rezultat akcije krajnjeg korisnika.

Ovaj i slični primeri ukazuju da forenzičar mora precizno i odlučno izneti svoje svedočenje/veštačenje pred sudom. Digitalni dokaz nije opipljiv, a druga strana uvek može imati sličnog ili boljeg forenzičara koji može naći pukotinu u dokazu.

4.4.5 Komparativni pregled funkcija ključnih forenzičkih alata

Rezultati uporednog pregleda osnovnih funkcija relevantnih forenzičkih alata, dati u tabeli 4.4, mogu biti korisni i pomoći forenzičaru kod izbora forenzičkog alata koji najbolje odgovara potrebama, [29].

Tabela 4.4 Uporedni pregled osnovnih funkcija relevantnih forenzičkih alata

Funkcija forenzičkog alata	***Access Data Ultimate Kit* (FTK)**	***Guidance Software EnCase***	***Digital Intelligence Drive Spy***
Akvizicija			
Fizičko kopiranje podataka	√	√	
Logičko kopiranje podataka	√	√	√
Formati akvizicije podataka	√	√	
Proces komandne linije		√	√
GUI proces	√	√	√
Udaljena akvizicija		√*	
Verifikacija	√	√	√
Validacija i diskriminacija			
Heširanje	√**	√**	√
Filtriranje	√	√	√
Analiza hedera fajlova	√	√	
Ekstrakcija			
Čitanje podataka	√***	√***	
Pretraživanje po ključnoj reči	√	√	√
Dekompresovanje	√	√	
Rekonstrukcija fragmentovanog fajla (*carving*)	√	√	
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 *Enterprise Edition*
** Koristi MD5 i SHA1 algoritme za heširanje
*** Varira format fajlova koje podržava

4.4.6Validacija 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 za ispitivanje forenzičkih alata razvio je NIST. Razvoj metodologije pokretali su zahtevi za funkcionalnosti forenzičke istrage i analizu digitalnih podataka. Aktivnost forenzičke istrage se deli u diskretne funkcije, 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 planirana 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**, [33], [34].

4.4.6.1Razvoj 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.

4.4.6.2Proces 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,
- isporučioci/proizvođači alata pregledaju izveštaj o testiranju,
- isporučioci/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 literaturi [34]. 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, specifikovati metod kako testirati forenzički alat i kakve instrukcije treba da ga prate.
- Izveštaj o rezultatima testiranja: opisati rezultate testa u izveštaju koji je u skladu sa ISO 17025 standardom, koji zahteva da izveštaj o testiranju mora biti tačan, jasan, nedvosmislen i objektivan.

Drugi standard, *ISO 5725*, zahteva tačnost za sve aspekte procesa testiranja alata, što znači da rezultati testiranja moraju biti *ponovljivi* i *reproduktivni*. *Ponovljivost rezultata* znači da ako forenzičar radi sa jednim alatom u istoj laboratoriji i na istoj mašini, alat mora generisati jednak rezultat. *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[53] 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 Interupt13.

BADX13: kreira loše sektore na proširenom BIOSu diska, sektori se listiraju u LBA formatu.

CORUPT: korumpira jedan bit u specifikovanom 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 specifikovan 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**[54] namenjen je za sakupljanje heš vrednosti fajlova svih komercijalno raspoloživih programskih aplikacija i sistemskih programa. U **NSRL** repozitorujumu primarno se koristi SHA-1 algoritam za generisanje skupa digitalnih potpisa, poznatog kao *referentni skupi podataka* - RDS (*Rference 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 slika).

53 NIST Computer Forensic Tool Testing program
54 National Software Reference Library

4.4.6.3 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 bobro 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:
- Izvršiti ispitivanje digitalnih dokaza sa neknim GUI forenzičkim alatom.
- Izvršiti isto ispitivanje sa disk editorom (*Win Hex* ili *HexWorkShop*) i verifikovati da li GUI forenzički alat vidi iste podatke na istom mestu na testiranom, ili imidžu osumnjičenog diska.
- Kada se fajl oporavi, odrediti heš vrednost u GUI alatu i u disk editoru, a zatim uporediti vrednosti i verifikovati integritet fajla.
- U većini slučajeva *FTK* i *EnCase* forenzički alati služe kao referentni pouzdani alati za verifikaciju drugih forenzičkih alata, jer su široko priznati u pravosudnim sistemima brojnih država.
- Postoje brojni forenzički alati koji mogu uspešno dopuniti kapacitete *FTK* i *EnCase* alata i treba ih koristiti.
- Ažuriranje zakrpe (fiksiranje, pečovanje), ili nadogradnja postojećeg alata, potrebno je takođe verifikovati, da bi se sprečila korupcija digitalnih dokaza. Ako se utvrdi da novo fiksiranje, ili nadigradnja 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 zakrpama i nadograđivati novim verzijama. Pri tome treba primenjivati navedenu proceduru za ispitivanje validnosti nove verzije softverskog ili hardverskog alata.

4.5 STUDIJA SLUČAJA: AKVIZICIJA 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 akvizicije 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 su otkrili 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 poznavanjem strukture i formata izvršnih fajlova, forenzičar može odrediti koji su fajlovi legitimni i koje artefakte treba pripisati određenom delu malicioznog koda.

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

4.5.1 *Rutkit* alati

Rutkit je tehnologija - alat koji se sastoji od malih i korisnih programa koji dozvoljavaju napadaču da sačuva pristup rutu i prikrije prisustvo na računaru. Rutkit program je kreiran da sakrije kôd i podatke na sistemu. Obično je namenjen za daljinski pristup i prisluškivanje. Rutkit tehnike nisu uvek „loše" i ne koriste ih samo zlonamerni napadači.

U Linux i Unix OS, rut je deo sistema sa najvišim privilegijama pristupa. Korisnička prava pristupa sa rut privilegijama omogućavaju kompletnu kontrolu mašine. Naziv *rutkit* nastao je od alata koji sadrži programe za održavanje, ili zadržavanje u rutu. Rutkitovi su jedan od najčešće korišćenih hakerskih alata za prodor u računarske sisteme. Hakeri ih koriste za sledeće funkcije:

- sprečiti logovanje aktivnosti,
- uspostaviti zadnja vrata (*backdoor*) za ponovljeni ulaz,

- sakriti ili ukloniti dokaz o inicijalnom ulazu,
- sakriti specifične sadržaje fajlova,
- sakriti fajlove i direktorijume,
- sakupiti informacije, npr., korisnička imena i lozinke.

Da bi se haker koji počini kompjuterski kriminal uhapsio, potrebno je razumeti alate i tehnike koje hakeri koriste da savladaju korisničke sisteme.

Primer neetičke primene *rutkit* alata je slučaj DRM softvera Somy kompanije za zaštitu muzičkih CD od kopiranja. Naime, stručnjak za operativne sisteme Windows, *Mark Russinovich*, je otkrio slučaj sada već čuvenog rootkit alata podmetnutog u DRM softver koji je Sony isporučivao sa svojim audio diskovima. Kompanija Sony BMG (trenutno druga najveća izdavačka kuća na svetu) pokušala je da problem piraterije reši uvođenjem novog DRM softvera (tkz.„*XCP*" tehnologije), koju je Sony licencirao od britanske kompanije *First 4 Internet*. *XCP* (*eXtended Copy Protection*) tehnologija radi samo na Windows operativnim sistemima; dozvoljava reprodukciju muzike na računaru samo iz pratećeg plejera i sprečava korisnike da naprave više od par kopija originalnog diska.

4.5.1.1 Podela rutkit alata

Rootkit alati se mogu podeliti u dve osnovne grupe, [6]:

1. *aplikacioni rutkit alati*, koji kao i sve ostale aplikacije rade u neprivilegovanom korisničkom režimu (*user mode*) i
2. *rootkit alati na nivou jezgra*, koji se integrišu u samo jezgro i rade na nivou jezgra (*kernel mode*).

Ove dve vrste alata razlikuju se po mestu u sistemu na kome su smešteni i načinu na koji skrivaju svoje prisustvo u sistemu.

Aplikacioni rutkit alati zasnivaju svoj rad na zameni legitimnih aplikacija zlonamernim fajlovima. Ubačeni fajlovi omogućavaju napadaču da prikrije svoje prisustvo i da obavi željene aktivnosti na sistemu (npr., alat može da obezbedi zadnja vrata, koja napadač može da iskoristi).

U grupu programa koje napadač menja kako bi sakrio svoje prisustvo na sistemu spadaju programi koji:

- skrivaju zlonamerne fajlove i direktorijume koje je napadač podmetnu (*ls,*
- *find, du*),
- skrivaju procese koje je napadač pokrenuo (npr., *ps*),
- sprečavaju ubijanje procesa koje je pokrenuo napadač (*kill, killall*),
- prikrivaju aktivnosti napadača na mreži – otvorene portove, mrežne
- konekcije (*netstat, ifconfig*),
- skrivaju unos u fajl *crontab,*

- skrivaju zapise u log datoteci o vezama koje napadač ostvaruje sa
- udaljenim sistemom (*syslogd*)

Rutkit alati na nivou jezgra zasnovani su na činjenici da je jezgro Linux sistema modularno - korisnik sa rut privilegijama može u jezgro učitati neki modul - LKM (Loadable Kernel Module) i na taj način proširiti funkcionalnost operativnog sistema. Ovi rutkit alati se otkrivaju teže od aplikacionih, jer se integrišu u samo jezgro operativnog sistema, što znači da ih može zaobići provera integriteta sistema obavljena u neprivilegovanom režimu rada.

4.5.1.2 Napad rutkit alatima

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 odvraćaju antivirusnim softverima. U Unix i Linux OS, administratori mreže obično 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.

Napad na Linux sistem, zasnovan na rutkit alatima, izvodi se u četiri faze:

- sakupljanje informacija o ciljnom sistemu (koji je operativni sistem u pitanju, koja verzija jezgra, koji korisnički nalozi postoje itd.),
- sticanje administratorskih prava, tj, prava koja ima korisnik ruta i koja su najčešće neophodna za instalaciju,
- instaliranje rutkit alata i
- uspostavljanje kontrole nad ciljnim sistemom.

Napad na Windows OS može se izvesti rutkit alatima upotrebom više različitih tehnika.

A. Upotreba postojećeg interfejsa za ubacivanje zlonamernog koda

Operativni sistem Windows sadrži određene interfejsne komponente koje omogućavaju nadogradnju sistema alatima drugih proizvođača.

Izmena procesa prijavljivanja: Proces prijavljivanja na sistem (*user logon process*) može se proširiti novim programima i/ili bibliotekama. Standardna procedura prijavljivanja na Windows sistem počinje zadavanjem kombinacije tastera *Ctrl+Alt+Delete*. Nakon toga, proces *winlogon,* koji nastaje pokretanjem datoteke *winlogon.exe*, poziva standardnu Windows biblioteku *msgina.dll*-GINA (*Graphical Identification and Authentication*) koja proverava identitet korisnika na osnovu unetog korisničkog imena i lozinke. Korišćenjem tehnike ubacivanja trojanca, unosi se **FakeGINA** rutkit alat, može da se izmeni proces prijavljivanja.

Deaktiviranje sistema zaštite datoteka: Napadači često moraju da promene neki sistemski fajl koji nije predviđen da se menja. Da bi u tome uspeli, potrebno je da nadvladaju Windowsov sistem zaštite fajla - WFP (*Windows File Protection*). Prilikom instalacije operativnog sistema generiše se spisak značajnih sistemskih fajlova. Njihova zamena drugom verzijom moguća je jedino ukoliko administrator instalira neku zvaničnu zakrpu (*hotfix*) ili novi *Service Pack*.

Napadi sa DLL injection i API hooking: Ove dve tehnike napada usmerene su na procese – napadač ubacuje zlonameran kod u neki proces i na taj način menja originalnu funkciju procesa. Tehnika ubrizgavanja DLL biblioteke (*DLL injection*), tj. ubacivanja zlonamerne DLL biblioteke u memorijski prostor aktivnog procesa, izvodi se u nekoliko faza. Tehnika *API hooking* nadovezuje se na *DLL injection* i predviđa ubacivanje zlonamernih rutkit funkcija u legitimne DLL datoteke. **AFX Windows Rootkit** je jedan od alata koji kombinuje tehnike *DLL Injection* i *API hooking*. Ova aplikacija prikriva aktivne procese u sistemu, direktorijume, fajlove, zapise u bazi Registry, TCP i UDP portove itd. Ovaj alat ne formira zadnja vrata, pa se zato se najpre formira „ulaz" u sistem pomoću nekog drugog alata čije se prisustvo krije koristeći **AFX Windows Rootkit**.

B. Upotreba različitih tehnika skeniranja

Postoje različite tehnike skeniranja konekcija koje su na raspolaganju forenzičaru za etički haking i udaljeni pristup ispitivanom računaru. Na raspolaganju su brojne tehnike skeniranja koje se mogu koristiti za ovu namenu. Jedan od pionira primene različitih tehnika skeniranja konekcija je *Fyodor*[55]. Veći deo navedenih tehnika skeniranja razradio je upravo *Fyodor*, [5]:

- **Skeniranjem preko TCP konekcije** (*TCP connect scan*) udaljeni računar se povezuje sa ciljnim i sprovodi se potpuno trostepeno usaglašavanje (SYN, SYN/ACK i ACK), što ciljni sistem lako otkriva.
- **Skeniranje tipa TCP SYN** ili *poluotvoreno skeniranje* (*half-open scanning*), pošto se ne ostvaruje potpuna TCP veza. Skener ciljnom priključku šalje paket SYN, a ako od priključka primi paket SYN/ACK, može da zaključi da prisluškuje konekciju (da je u stanju LISTENING). Ako se primi paket RST/ACK, to obično znači da ciljna konekcija nije aktivna. Zatim skener šalje paket RST/ACK tako

55 *Fyodor* je mnoge tehnike skeniranja ugradio u svoj alat **Nmap**.

da se potpuna veza nikada ne ostvaruje. Ova tehnika je diskretnija od ostvarivanja potpune TCP veze i ciljni sistem je možda neće zabeležiti.

- **Skeniranje tipa TCP FIN** ciljnom priključku šalje paket FIN. Prema dokumentu RFC 793, ciljni sistem treba da uzvrati paketom RST za sve priključke koji su zatvoreni. Tehnika obično radi samo sa UNIX-ovim TCP/IP stekovima.
- **TCP skeniranje tipa „božićne jelke" (***Xmas Tree***)** ciljnom priključku šalje pakete FIN, URG i PUSH. Prema dokumentu RFC 793, ciljni sistem treba da uzvrati paketom RST za sve zatvorene priključke.
- **Nulto TCP skeniranje** (*Null*) isključuje (resetuje) sve indikatore. Prema dokumentu 793, ciljni sistem treba da uzvrati paketom RST za svaki zatvoren priključak.
- **Skeniranjem tipa TCP ACK** otkrivaju se pravila zaštitne barijere (*firewall*). Ovim se može utvrditi da li je zaštitna barijera samo filtar za pakete koji dozvoljava prolaz jedino za uspostavljene veze (veze sa uključenim bitom ACK) ili je reč o barijeri koja čuva informacije o sesiji, sa složenim mehanizmom propuštanja paketa.
- **Skeniranjem TCP prozora** otkrivaju se otvorene kao i filtrirane/nefiltrirane konekcije na nekim sistemima (na primer, na sistemima *AIX* i *FreeBSD*), a prema odstupanju koje se javlja u izveštaju o veličini TCP prozora.
- **Skeniranje tipa TCP RPC** je tehnika, specifična za sisteme UNIX, koja se koristi za otkrivanje i identifikovanje konekcija za daljinsko pozivanje procedura - RPC (*Remote Procedure Call*) programa koji su s njima povezani i verzija tih programa.
- **Skeniranjem tipa UDP** ciljnoj konekciji se šalje paket UDP protokolom. Ako ciljni priključak odgovori porukom *„ICMP port unreachable*", to znači da je priključak zatvoren. Ukoliko skener ne primi takvu poruku, može se zaključiti da je priključak otvoren. Pošto je UDP poznat kao protokol kome ne treba povezivanje, preciznost ove tehnike veoma zavisi od opterećenja mreže i sistemskih resursa. UDP skeniranje postaje veoma sporo ukoliko njime skeniramo uređaj koji detaljno filtrira pakete. Ukoliko se UDP skeniranje primenjuje putem Interneta, rezultati su nepouzdani.

Izvesne realizacije protokola IP imaju neugodnu osobinu da uzvraćaju paketom RST za svaki skeniran priključak, bilo da se on prisluškuje ili ne. Zbog toga rezultati koje se dobijaju takvim skeniranjem mogu da variraju. Međutim, skeniranje tipa TCP SYN i skeniranje preko TCP konekcije rade u svim slučajevima.

4.5.2 Detekcija rutkitova, zadnjih vrata i mrežnih snifera

4.5.2.1 Detekcija prisustva rutkitova

Ulazak napadača u računarski sistem može ostaviti dokazni trag u različitim podacima log fajla. Većina rutkitova uključuje uslužne alate za automatsko uklanjanje svakog sumnjivog ili inkriminišućeg podatka 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 počnu da se ponašaju 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. Tehnike i alati rutkitova spadaju u kategoriju malicioznih programa tipa virusa, crva i trojanaca i detektuju se manje više na isti način. U stvari, većina rutkitova sadrži komponentu zadnjih vrata trojanca za obezbeđivanje kasnijeg ulaza. 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 **l**s komandom.

ProDiscover Suite kombinuje sve alate iz grupe **ProDiscover**. To je moćan kompjuterski forenzički alat koji omogućava korporativnim profesionalcima zaštite da reaguju na incident sa unutrašnjeg i spoljašnjeg izvora. **ProDiscover Suite** omogućava forenzičaru daljinsko ispitivanje sadržaja diska ispitivanog sistema preko mreže – proveru da li postoje Trojanci ili neki drugi maliciozni programi koji su možda kompromitovali sistem, ili da bi istražio ilegalne aktivnosti narušavanja politike zaštite korporacije ili incident kompjuterskog kriminala. Pomoću **ProDiscover Suite**, mogu se skupiti dokazi za potencijalne pravosudne procedure. Primena ovog seta alata obezbeđuje brojne pogodnosti forenzičaru:

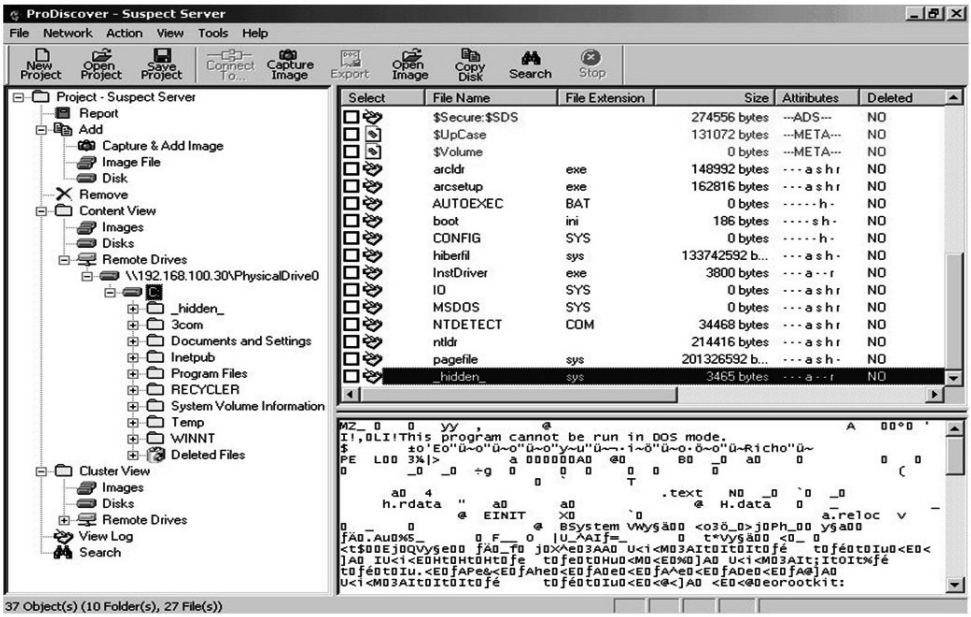
- Ubrzava istragu i štedi putne troškove pomoću udaljenog pristupa i aktivne forenzike akvizicije ispitivanog sistema preko mreže;
- Brzo otkrivanje Trojanaca i rutkitova, čak i *kernel mode* Trojance koji se prikrivaju u sistemima;
- Svi sakupljeni podaci koji se šalju preko mreže mogu biti zaštićeni 256 bitnim *Twofish* šifarskim sistemom;
- Automatsko kreiranje i snimanje MD5 ili SHA1 heš vrednosti fajlova sa digitalnim dokazima za zaštitu integriteta dokaza;

- Kreiranje imidža celog osumnjičenog diska, uključujući i sakrivene delove, da bi se sačuvali originalni dokazi;
- Pregledanje FAT12, FAT16, FAT 32 i sve NTFS fajl sisteme uključujući *Dynamic Disk* i *Software RAID*;
- Pregledanje *Sun Solaris UFS* i *Linux Ext. 2/3* fajl sisteme.

ProDiscover Suite je ključni alat za efektivnu digitalnu forenzičku istragu i odgovor na kompjuterski incident. Od ovog alata nije moguće sakriti podatke, jer čita HD na nivou sektora i na taj način „nadmudruje" standardne fajl sisteme. Ovo omogućava da se povrate obrisani fajlovi, pretražuju podaci u fajl *slack* prostoru i nealociranom prostoru diska kao i pregled Windows *Alternate Data Streams*. Ovaj jedinstveni pristup takođe omogućava da se pregledaju fajlovi bez promene bilo kojih dragocenih dokaza na disku.

ProDiscover Suite omogućava daljinsku aktivnu pretragu sistema u okviru mreže dok su još uvek povezani i izvršavaju svoje uobičajene zadatke. Nije potrebno ni rebutovati sistem da bi se izvršilo forenzičko ispitivanje. Za osetljivije pretrage **ProDiscover Suite** podržava *stealth* mode (skrivenjen metod).

ProDiscover Suite vrši pretragu fajlova i procesa koji su zamaskirani Trojancima ili rutkitovima. Može se kreirati referentni skup heš potpisa za sve fajlove na sistemu i kasnije koristiti te potpise da bi se uporedili sa kompromitovanim sistemom tj. da bi se videlo da li su neki fajlovi izmenjeni. Moguća je i pretraga diska, uključujući i *slack* prostore, po zadatoj reči i izrazu, (slika 4.82).



Slika 4.82 ProDiscover forenzički alat

Sistemski zahtevi za instalaciju **ProDiscover** alata:

- Windows 2000/2003/2008/XP/Vista OS,
- 800 MHz ili više *Pentium-compatible* CPU,
- 256 MB RAM (512 MB i više preporučeno),
- 25 MB slobodnog prostora na HD;
- CD-ROM ili DVD-ROM diskove;
- VGA ili monitor veće rezolucije i
- Tastatura i Miš.

Poznatiji alati za otkrivanje rutkitova su:

- **RootkitRevealer**[56] je zakonom zaštićen alat za rutkit detekciju za Microsoft Windows OS. Jedan od tragova koji rutkit alati ostavljaju za sobom je razlika u „slici" sistema, tj. u rezultatima skeniranja sistema na najvišem nivou (Windows API) i rezultatima skeniranja na najnižem nivou („sirov" sadržaj fajl sistema ili baze Registry na disku). Zato se rutkit alati (aplikacioni ili alati jezgra), koji manipulišu API-jem da bi se sakrili, mogu otkriti na osnovu razlike izmenu informacija pribavljenih od API-ja i informacija dobijenih pri skeniranju strukture fajl sistema. Ovaj alat je prvi detektovao *XCP rootkit* koji je kompanija *Sony* neetički koristila u komericjalne svrhe;
- **Rkscan** je skener rutkit alata na nivou jezgra.
- **Rkdet** je detektor rutkit alata na Linux operativnim sistemima.
- **Chkrootkit**[57] 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*)[58] 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*.

Manuelna inspekcija, jedan od načina da se detektuju rutkitovi, obično se izvodi korišćenjem *komande 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

56 *Mark Russinovich*, www.sysinternals.com
57 *www.chkrootkit.org*
58 *www.pedestalsoftware.com*

sistem administratore komanda stringova može proizvesti čitljive podatke kao što su imena fajlova u kojima napadači drže lozinke, verzija biblioteke sa kojom je kompajliran rutkit i druge informacije koje normalno nisu u korelaciji sa originalnim podacima u ispitivanom fajlu. Tačna sintaksa koju koristi *komanda stringova* varira u zavisnosti od verzije *Unix/Linux* OS koji se koristi. Generalno, sintaksa za komande stringova je sledeća:

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

Oznake (*flags*) koje se koristi u Unix/Linux *string* komandama dati su u tabeli 4.5.

Tabela 4.5 Glavne oznake u Unix/linux *string* komandama

Oznaka	Funkcije oznaka (*flags*)
-a ili **-**	Ova oznaka traži stringove 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 *offset* svake prethodne liniju komande od početka fajla.
d	Piše ofset u decimalnom formatu.
o	Piše *offset* u oktalnom formatu.
x	Piše *offset* 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

4.5.2.2 Detekcija prisustva zadnjih vrata

Korišćenje zadnjih vrata *(backdoors)* za ponovljene ulaske u sistem je popularna tehnika hakera, pošto se alati za postavljanje zadnjih vrata nalaze besplatno na haker-

skim sajtovima. Napadači postavljaju zadnja vrata za kasniji ulazak u sistem, koristeći skriveni ID i lozinku 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 lozinke za logovanje u sistem. Zadnja vrata za većinu napadača obezbeđuju tri glavne funkcije:

- ući kasnije u sistem što je moguće skrivenije (da mašina ne ukazuje da ima nekog *online*),
- ući kasnije u mašinu čak i kada je administrator obezbedi (npr., promenom svih lozinki),
- 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:

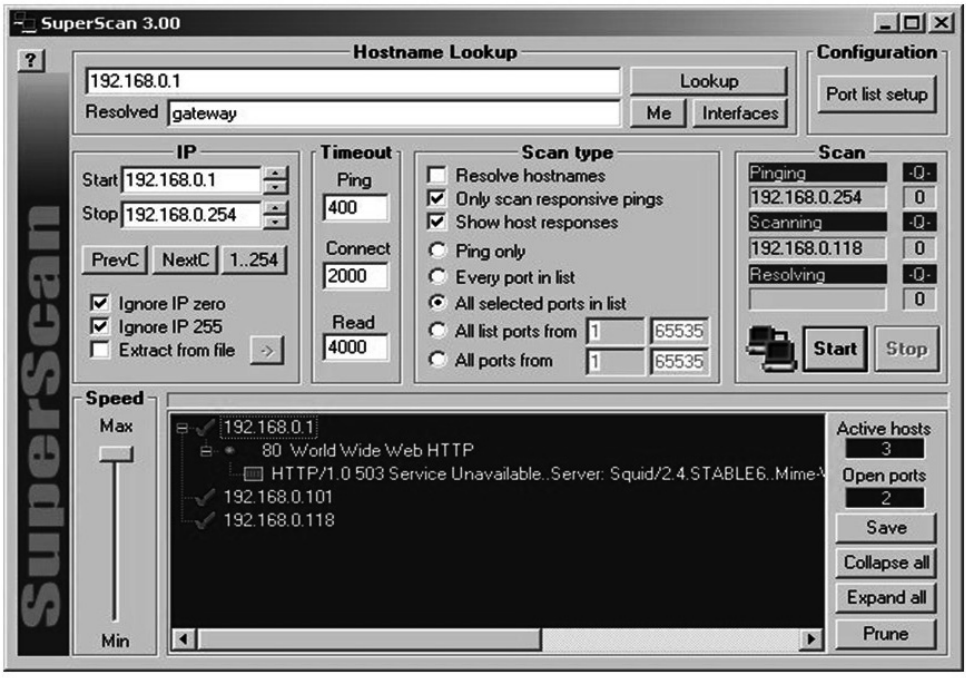
- *upload* ili *download* fajlova,
- premeštanje, kopiranje ili brisanje fajlova,
- brisanje HD ili drugog diska podataka,
- izvršavanje programa,
- gledanje ekrana monitora kako ga korisnik vidi,
- aktiviranje log ključa (čak i unos skrivene lozinke),
- otvaranje, zatvaranje i premeštanje prozora,
- 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 da znaju ponešto o svakom od njih. 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**[59] je 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.
- **Nmap**[60] je besplatan mrežni maper, 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.

59 *www.foundstone.com*
60 www.insecure.org/nmap

- **Listdlls.exe**[61] je Windows besplatan pomoćni alat (autor *Mark Russinovich*) koji prikazuje punu putanju modula koji se učitava.
- **SuperScan** je moćan skener TCP portova, uređaj za pingovanje i detektor imena hostova (*Foundstone Inc.*), ekstremno brz i raznovrstan (slika 4.83).



Slika 4.83 SuperScan forenzički alat

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**[62]**,** 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.

61 www.sysinternals.com
62 *www.sysinternals.com*

4.5.2.3 Detekcija prisustva mrežnih snifera

Skener (*sniffer*) 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 lozinki koja se prenose kroz mrežu nezaštićeno, npr., u otvorenom tekstu ili čistom ASCII formatu gde se mogu čitati u *Notepad*-u. Gotovo svaki rutkit uključuje uslužni alat za praćenje mrežnog saobraćaja. Jedan uznemirujuće moćan aspekt *sniffer* paketa je njihova sposobnost da postave host mašinu u *promiskuitetan režim* rada, u kojem mašina prima ne samo podatke usmerene na nju, nego i sav saobraćaj podataka u fizički spojenoj lokalnoj mreži. To sniferu daje ulogu špijunskog alata, pošto svaki interfejs u ovom modu sluša ceo mrežni saobraćaj.

Za Windows sisteme može se koristiti besplatan softverski alat komandne linije **PromiscDetect**[63] za otkrivanje mrežnih adaptera u *promiskuitetnom* modu, koji radi sa Windows NT 4.0, 2000 i XP OS.

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.

63 www.ntsecurity.nu/toolbox/promiscdetect/

REZIME

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

Ranih 90-tih razvijeni su prvi alati za istragu i ispitivanje digitalnih podataka. Brojni savremeni forenzički alati koriste se istovremeno i za akviziciju i analizu digitalnih podataka. Dele se u dve glavne kategorije: hardverski i sofverski alati. Kriterijumi za izbor adekvatnog specijalizovanog alata, ili seta alata, značajnija su pitanja za svakog forenzičara, nego preporuke pojedinačnih forenzičkih alata. Forenzički alati se neprestano razvijaju, modernizuju, popravljaju i reklamiraju. Kod nabavke forenzičkog alata uvek treba imati na umu vrste fajlova i podataka, koje alat treba da analizira. Preporučuje se namenski alat specijalizovan za određenu vrstu podataka, (npr., za *MS Access* bazu ili e-mail poruke), pre nego neki univerzalni alat koji između ostalog analizira i ove podatke. Strogo namenski alati su pouzdaniji za tu konkretnu funkciju. Sa druge strane, forenzičar koji koristi višenamenski set alata, (npr., **FTK)**, koji omogućava obavljanje više različitih forenzičkih zadataka, može brže i konfornije sa jednim alatom završiti sve 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.

Hardverski forenzički alati obuhvataju stacionarne, portabl i prenosne radne stanice, različite tipove blokatora upisivanja, uređaja za dupliranje čvrstog diska, adaptera, specijalnih kablova, CD/DVD diskova za akviziciju, SCSI diskova itd. Generalno, hardverski forenzički alati su pouzdaniji, ali i skuplji i vremenski zahtevniji za rad.

Sa aspekta funkcionalnosti, 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, a prezentacioni alati aranžiraju podatke iz ekstrakcionog alata u forenzički čitljiv i koristan format. Većina savremenih alat (*FTK, EnCase, iLook* i dr.) integriše i izvršava obe funkcije, ali postoje i jednofunkcionalni alati.

Sa apekta poverenja u funkcionalnost, softverski alati se dele na alate sa zatvorenim i otvorenim izvornim kôdom. 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. Generalno, 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. Ovo omogućava da se proizvođači alata 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 za forenzičku akviziciju i analizu. Koncept forenzičkih alata sa otvorernim izvornim kôdom bitno se razlikuje od koncepta drugih softverskih proizvoda sa otvorenim izvornim kôdom, jer je cilj obezbedi lakši pristup za reviziju i testiranje alata, a ne za njihovo ažuriranje. U *forenzičke alate otvorenog kôda* - OSS ubrajaju se alati na bazi *Unix* i *Linux* OS. Glavne prednosti Linux/Unix forenzičkih alata, u odnosu na primenu na terenu i u forenzičkoj laboratoriji, su visoka raspoloživost, dobra podrška, a nedostaci su: obično zahtevaju dodatnu obuku forenzičara, vreme i rad za učenje,komandna linija nije toliko intuitivna kao GUI interfejs, nema formalne organizacije za podršku, kvalitet podrške veoma varira, otežana je interoperabilnost sa drugim tehnologijama u vlasništvu (*Microsft*, npr.), u nekim slučajevima slaba je dokumentacija, gde izvorni kôd može biti jedina dokumentacija.

Sa aspekta interfejsa, softverski forenzički alati grupišu se u dve osnovne kategorije: *aplikacije komandne linije* i *GUI aplikacije*. Značajan aspekt softverskih forenzičkih alata je sposobnost potpunog kopiranja, ili uzimanja fizičke slike bit-po-bit ili *imidža* osumnjičenog diska, ili drugog medijuma sa potencijalnim dokazima.

Savremeni softverski forenzički alati mogu generisati elektronski izveštaj u različitim formatima - Word dokument, HTML, RTF ili PDF. Osnovne komponente procesa izveštavanja su: log izveštaj i generator za izveštavanje.

Da bi se obezbedio neophodni integritet digitalnih podataka, kao i poznavanje stepena greške koju alat unosi, potrebno je poznavati pouzdanu metodu testiranja validnosti forenzičkog alata. Na raspolaganju su određeni alati za validaciju forenzičkog softvera, koji omogućavaju da forenzičar razvije sopstvenu proceduru za validaciju i testiranje korišćenog forenzičkog alata. Metodologiju za ispitivanje forenzičkih alata razvio je NIST.

Pouzdanost i validnost generisanog dokaza, kao izlaza iz digitalnog forenzičkog alata, određuje sudija u predistražnom postupku na bazi bazičnih principa za prihvatljivost naučno zasnovanih digitalnih dokaza pred sudom, da je procedura primene forenzičkog alata: testirana, poznat stepen grešaka, objavljena i višestruko naučno revidirana i generalno prihvaćena u relevantnoj naučnoj zajednici.

U procesu digitalne forenzičke analize ispitivanog računara, od posebnog značaja za forenzičara je lokacija i poznavanje *rutkit* alata, tehnika prikrivanja zadnjih vrata, detekcije i uklanjanja *rutkitova,* koji se sve više koriste ne samo u kompjuterskom kriminalu kao antiforenzičke tehnike, nego i u 'legitimnim' komercijalnim aplikacijama.

PITANJA ZA PONAVLJANJE

1. Navedite osnovne karakteristike alata koje je potrebno evaluirati za nabavku forenzičkog softverskog alata?
2. Koje osnovne funkcije obuhvata proces akvizicije digitalnih podataka?
3. Navedite dva metoda akvizicije podataka softverskim alatima.
4. Koje su tri osnovne funkcije validacije i diskriminacije podataka?
5. Koje su osnovne funkcije u procesu rekonstrukcije ispitivanog diska?
6. Navedite nekoliko alata koji prilagođavaju geometriju CHS forenzičkog diska prema geometriji CHS originalnog/ispitivanog diska.
7. Navedite neki alat koji vrše kopiranje sa imidža na disk.
8. Nabrojte nekoliko softverskih alata koji obezbeđuju log izveštaje.
9. Nabrojte glavne kategorije hardverskih forenzičkih alata.
10. Koje su dve osnovne kategorije softverskih forenzičkih alata sa aspekta interfejsa.
11. Navedite nekoliko prednosti alata komandne linije.
12. Navedite nekoliko nedostataka GUI forenzičkih alata
13. Kako se vrši akvizicija podataka EnCase alatom?
14. Kojom putanjom se mogu videti potpisi fajlova u EnCase alatu?
15. Koji heš algoritam koristi EnCase v.4 forenzički alat?
16. Navedite ime najpoznatijeg forenzičkog alata na bazi Linux-a.
17. Navedite osnovne elemente procedure za validaciju forenzičkih softverskih alata.
18. Zašto je značajno poznavanje izvornog koda forenzičkog alata?

KLJUČNI TERMINI

Adapter za akviziciju podataka: hardverski uređaj koji ima funkciju fizičkog prilagođavanja različitih memorijskih medija u procesu akvizicije podataka sa osumnjičenog na forenzički sterilan medijum.

Akvizicija podataka: glavna faza digitalne forenzike analogna uzimanju otiska prsta, koja obuhvata procese otkrivanja, identifikovanja i sakupljanja potencijalnih dokaza na bazi rezultata istrage u predistražnom postupku za potrebe forenzičke analize digitalnih dokaza; klasična akvizicija obuhvata najčešće uzimanje fizičke slike (*imidža*) HD i drugih medija ispitivanog računara, a živa akvizicija podrazumeva skupljanje podataka sa računara u radu.

Bezbedni heš algoritam (*Secure Hash Algorithm*): digitalni 160-bitni sažetak sadržaja fajla (NIST) dobijen jednosmernom funkcijom koja se lako računau jednom, a teško ili nikakou drugom smeru. FTK koristi 180-bitni heš SHA-1. KFF biblioteka sadrži brojne heš funkcije poznatih fajlova.

Blokator upisivanja: hardversko-softverski alat koji sprečava upisivanje ili modifikaciju podataka na ispitivanom disku računara, od svih priključenih medijuma za skladištenje.

Butabilna disketa/CD: disketa/CD za nezavisno butovanje OS iz DOS komandne linije.

Digitalna forenzička nauka*:* Korišćenje naučno deriviranih i dokazanih metoda za identifikaciju, skupljanje, vrednovanje, analizu, interpretaciju, dokumentaciju, veštačenje, čuvanje i rukovanje digitalnim dokazima sa ciljem olakšavanja, ili unapređivanja rekonstrukcije događaja prepoznatog kao krivično delo, ili pomoći za prepoznavanje neovlašćenih akcija koje ometaju planirane operacije.

Dinamičko testiranje alata: podrazumeva aktivan rad forenzičkog alata i korišćenje programa za monitorisanje promena koje alat izaziva u sistemu.

Ekstenzija fajla: oznaka tipa fajla koju operativni sistem prepoznaje i pokušava otvoriti sa odgovarajućom aplikacijom.

Fizička Slika diska: (*imidž, mirror*) fizička kopija bit-po-bit diska ispitivanog računara na forenzički sterilan disk.

Forenzička analiza kibernetičkog prostora: najkompleksnija oblast digitalne forenzike i može biti veoma spor proces koji zahteva uspostavljanje legalne saradnje država u borbi protiv kompjuterskog kriminala, uključujući usklađivanje standarda za kvalitet, akviziciju, analizu, prezentaciju i upravljanje digitalnim dokazima.

Forenzička analiza računara: aplikacija ispitivanja računara i tehnika analize u cilju određivanja potencijalno legalnih dokaza, generisanih, ili uskladištenih u računaru.

Forenzička analiza softvera: visoko teoretski, najosetljiviji deo digitalne forenzičke analize, zahteva složene forenzičke alate; identifikacija autora malicioznog kôdazasniva se na selekciji odgovarajućeg korpusa kôda i identifikaciji odgovarajućih karaktersitika za upoređivanje.

Forenzička analiza: Treća faza forenzičkog procesa računarskog sistema i mreže, koja uključuje korišćenje legalno opravdanih metoda i tehnika za derivaciju korisnih informacija koje su bile predmet sakupljanja u fazi pretrage.

Forenzički alati GUI tipa: pojednostavljuju forenzičku akviziciju i analizu, ali neki ne mogu otkriti svaki dokaz; većina dolazi u setu alata za više zadataka (***EnCase, FTK***); imaju nekoliko prednosti- jednostavna upotreba, mogućnost obavljanja više zadataka i ne zahtevaju učenje starijih OS.

Forenzički alati komandne linije*:* prvi alati za analizu i ekstrakciju podataka sa flopi i čvrstog diska (MS DOS za IBM PC fajl sisteme); mogu izvući podatke iz *slack* i nealociarnih prostora fajl sistema, izbrisanih fajlova, pretraživati po ključnoj reči/karakteru, računati heš vrednost, oporaviti izbrisani fajl, izvršiti analizu fizičkog i logičkog diska i dr.

Forenzički čist disk/medijum: digitalni medijum koji je kompletno prepisan (*wiped*) i očišćen od svih podataka, uključujući nebitne i rezidualne podatke, skeniran na maliciozne programe i verifikovan pre upotrebe.

Granični sloj nivoa apstrakcije: poslednji sloj u nivou apstrakcije čiji se ne koristi kao ulaz u bilo koji drugi sloj na tom nivou; npr., sirovi sadržaj nekog fajla u fajl sistemu.

Greška implementacije: 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.

Greška sloja apstrakcije: unosi se zbog simplifikacije koja se koristi za generisanje sloja apstrakcije, a dešava se kada sloj apstrakcije nije deo originalnog dizajna.

Hardver: Fizičke komponente računara.

Hešovanje (*Hashing*): generisanje alfanumeričkih vrednosti određene, fiksne dužine na bazi sadržaja fajla i primene algoritma jednosmerne matematičke funkcije, koja se lako računa u jednom, a izuzetno teško ili nikako u drugom smeru; koristi se za dokaivanje da kopija fajla imidža ispitivanog diska nije izmenjena u procesu forenzičke akvizicije i analize; statistički je nemoguće da izmenjeni fajl generiše isti broj heša.

Imidž diska: fizička kopija bit-po-bit ispitivanog fizičkog/logičkog diska.

Indeksiranje fajlova (*bookmarks*): vrši se posle lociranja podataka – glavnog zadatka u ispitivanju računara, sa ciljem da se forenzičar može po potrebi pozvati na označene podatke; većina forenzičkih alata koristi ovu funkciju za ubacivanje liste u generator za izveštavanje, koji proizvodi tehnički izveštaj o nalazima ispitivanja računara.

Ispitivanje: druga faza forenzičkog procesa računarskog sistema i mreže, koja uključuje forenzičko procesiranje velike količine sakupljenih podataka koristeći kombinaciju automatizovanih i manuelnih metoda za ekstrakciju podataka od posebnog interesa, štiteći integritet informacija i održavajući striktno lanac čuvanja podataka.

Izveštavanje: konačna faza forenzičkog ispitivanja računara i mreže, koja uključuje izveštavanje rezultata analize - opis korišćenih akcija, objašnjenje selekcije alata i procedura, određivanje drugih akcija koje treba izvršiti (tj. forenzičko ispitivanje dodatnih izvora podataka, fiksiranje identifikovanih ranjivosti, poboljšavanje postojećih kontrola zaštite) i obezbeđenje preporuke za poboljšavanje politika, uputstava, procedura, alata i drugih aspekata forenzičkog procesa; formalnost procesa izveštavanja veoma zavisi od situacije.

Kompromitovani računar: u kontekstu digitalne forenzike - ispitivani računar koji može biti napadnuti (žrtva), posredni, ili osumnjičeni računar sa kojeg je izvršen napad; u kontekstu upravljanja kompjuterskim incidentom - korumpirani (*zombirani*) računar iskorišćen za ilegalne aktivnosti bez znanja vlasnika računara.

Kopiranje sa diska na disk: forenzičko dupliranje ili kopiranje sadržaja diska/medijuma osumnjičenog računara direktno na drugi forenzički sterilan disk/medijum istog ili većeg kapaciteta; na raspolaganju je više alata koji to omogućavaju, a besplatan je *Linux dd Shel command*, a brži su hardverski nego softverski alati.

Kopiranje sa diska na fajl: forenzičko kopiranje sadržaja diska/medijuma na logički *imidž* fajl.

Log izveštaja: izveštaj o aktivnosti kojeg generiše većina forenzičkih alata (*FTK, iLook, X-Ways Forensic, Drve Spy*) i može se dodati konačnom izveštaju forenzičara kao dodatni dokument o tome koji su koraci preduzeti u toku ispitivanja; potvrđuje koje aktivnosti su izvršene, a koji rezultati dobijeni iz originalne analize i ispitivanja računara.

Lokardov princip razmene: kada dva objekta dođu u kontakt između njih se razmenjuje ili prenosi materija; teorija da svako/svašta, ko/što uđe na mesto krivičnog dela uzima deo materije sa lokacije i ostavlja deo materije kad napusti lokaciju.

MAC adresa (*Media Access Control Address***)**: jedinstveni broj pripisan mrežnoj kartici (NIC) koji se koristi za adresiranje podataka na sloju veze podataka računarske mreže.

Metodologija lokalne akvizicije živog računara: podrazumeva da forenzičar sedi za tastaturom sistema u radu, unosi komande i skladišti informacije lokalno, direktno na HD, ili USB, ili na zajednički forenzički, mrežni lokalni resurs.

Nepromenljivi podaci (*Non-Volatile Data*): podaci koji ostaju neizmenjeni čak i posle isključivanja računara.

Opservacija podataka: funkcija posmatranja podataka, koju obezbeđuje većina forenzičkih alata, a kako se i u kojem formatu podaci vide, zavisi od alata.

Optužujući dokaz: digitalni dokaz koji obezbeđuje nepobitne okrivljujuće činjenice.

Oslobađajući dokaz: digitalni dokaz koji obezbeđuje nepobitne oslobađajuće činjenice.

Podaci: odvojeni delovi digitalnih informacija koji su formatirani na specifičan način i mogu se nalaziti na različitim slojevima apstrakcije računarskog sistema.

Pretraživanje po ključnoj reči: funkcija softverskih forenzičkih alata za traženje forenzički interesantnog podataka.

Prezentacioni alati: forenzički alati koji prezentuju digitalne dokaze u formi pogodnoj za čitanje i interpretaciju podataka.

Program za pretraživanje (*Search Engine*): baza podataka Internet resursa koja se može istraživati korišćenjem ključne reči i fraza; rezultat pretrage obezbeđuje direktan link do informacije.

Promenljivi podaci: podaci na živom sistemu koji se gube kada se isključi napajanje računara. **Brisanje prepisivanjem (***Wiping***)**: prepisivanje medijuma ili dela medijuma sa slučajnim ili konstantnim vrednostima da bi se prebrisali stari podaci i pripremio medijum za sakupljanje podataka.

Protokol za rešavanje adresa (ARP**)**: TCP/IP set koji se koristi dinamički za pridruživanje mrežnog sloja IP adresa sa slojem veze podataka MAC adresa.

Rekonstrukcija fragmenata fajla (***carving***): postala je uobičajen zadatak za forenzičara; sakuplja fragmente pobrisanih delova fajla sa osumnjičenog diska; značajan je deo procesa forenzičke istrage; izvlači podatke iz nealociranih prostora diska; locira informacija hedera fajla; fragmente, ili cele strukture fajlova rekonstruiše i kopira u novi fajl.

Sakupljanje: prva faza forenzičkog procesa računarskog sistema i mreže, koja uključuje identifikaciju, označavanje, snimanje i akvizicija podataka iz mogućih izvora relevantnih podataka, sledeći proceduru i uputstva za zaštitu integriteta podataka; često se naziva akvizicija po najznačajnijem koraku.

Sažetak poruke (*Message Digest*): heš vrednost koja jedinstveno identifikuje podatke. Promena jednog bita u podacima daje kompletno različit sažetak. Primeri MD5, SHA1**Statičko testiranje alata**: 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.

Translacioni alati: forenzički alati koji vrše translaciju podataka sa jednog na drugi sloj apstrakcije računarskog sistema.

LITERATURA

1. Bem D., Huebner E., *Computer Forensic Analysis in a Virtual Environment,* University of Western Sydney, Australya, 2008
2. *Buchholz F., i Falk C., Timeline, a Forensic Timeline Editor*", *2005*
3. Carrier B., *Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers*, International Journal of Digital Evidence, 2003.
4. Carrier B., *The Legal Argument*, carrier@cerias.purdue.edu, 2005.
5. Carvey H., *Windows Forensic Analysis DVD Toolkit,* Syngress Publishing Inc., www.syngress.com, 2007.
6. Fisher E. G.**,** *Computer Forensics Guidance*, NIST, www.nist.com, 2001.
7. Grunwald L*., Searching for Evidence Digital Forensic Analysis*, CTO Januar 26, 2004.
8. Guidance Software*, EnCase Forensic Edition*, http://www.encase.com, 2006.
9. http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html.
10. http://msdn.microsoft.com/library/default.asp?url=/library/enus/sysinfo/base/file_times.asp.
11. http://msdn.microsoft.com/library/default.asp?url=/library/enus/wmisdk/wmi/win32_process.asp.
12. http://support.microsoft.com/?id=837243.
13. http://support.microsoft.com/default.aspx?scid=kb;en-us;236995.
14. http://support.microsoft.com/default.aspx?scid=kb;en-us;250320
15. http://support.microsoft.com/default.aspx?scid=kb;en-us;314056.
16. http://support.microsoft.com/kb/119495/EN-US/.
17. http://support.microsoft.com/kb/137984/ .
18. http://support.microsoft.com/kb/222193/EN-US/.
19. http://support.microsoft.com/kb/q163409/.
20. http://vil.nai.com/vil/content/v_100559.htm.
21. http://www.iacis.org/.
22. Icove D., Segar K., VonStorch W., *Computer Crime, A Crimefighter's Handbook,* O'Reilly & Associates, 2006.
23. IOCE, *IOCE Princips & Definitions*, IOCE 2. Conference, London, 1999.
24. Kenneally E., Brown Ch., *Risk sensitive digital evidence collection*, CS 483, Washington State Universit, Spring 2009.

25. Krsul I., Spafford E. H., *Authorship Analysis: Identifying the Author of a Program,* Department of Computer Sciences, Purdue University, CSD – TR – 96 - 052, 1996.
26. Len P., Lynn B., *Reproducibility od digital Evidence in Forensic Invstigation*, CS 483, Washington State Universit, Spring 2009.
27. Mocas Dr. Sarah, *Topics in Computer Science Introduction to Digital Forensic*s, CS 483, Washington State Universit, Spring 2009.
28. National Policing Improvement Agency, *Core Skills in Data Recovery & AnalysisCourse Reference Book V2.01*, Bradford, UK, 2007.
29. Nelson B., Phillips A., Enfinger F., Christopher S., *Guide To Computer Forensics And Investigations*, Second Edition, Published by Course Technology, 25 Thompson Learning, lnc., Printed in Canada, 2006.
30. NetBIOS, http://en.wikipedia.org/wiki/NetBIOS.
31. Netcat, www.vulnwatch.org/netcat/.
32. Nikkel B, *Digital Forensics using Linux and open source tools*, PPP septembar 26, 2005.
33. NIST - CFTT, *Computer Forensic Tool Testing*, www.cftt.nist.gov, 2001.
34. NIST – CFTT, *General Test Methodology for Computer Forensic Tools*, *v. 1.9*", www.cftt.nist.gov/testdocs.html], 2001.
35. Pollit M. Mark, *Report on Digital Evidence,* (FBI CART report, DC Washington, USA), Interpol Forensic Science Symposium, Lyon, France, 2001.
36. psfile.exe, www.microsoft.com/technet/sysinternals/utilities/psfile.mspx .
37. psloggedon, www.microsoft.com/technet/sysinternals/SystemInformation/PsLoggedOn.mspx .
38. RFC 3227, *Guidelines for Evidence Collection and Archiving,* www.faqs.org/rfcs/rfc 3227.html, 2002.
39. Scouts E., *WMI Tutorial*, 66, 2005.
40. strings**.**exe, www.microsoft.com/technet/sysinternals/Miscellaneous/Strings.mspx.
41. SubSeven, www.symantec.com/avcenter/venc/data/backdoor.subseven.html.
42. Technology Pathways, *Pro Discover DFT*, http://wwww.techpathways.com, 2006.
43. Thuraisingham Dr. B., *Digital Forensics: Network Forensics – II*, The University of Texas at Dallas, October 29, 2008.
44. Wiebe J., *Survey of Hardware Data Acquisition Tools*, CEOWiebeTech LL-Cjames@wiebetech.com, www.www.wiebetechwiebetech.com.com.
45. www.cftt.nist.gov.

46. www.diamondcs.com.au/index.php?page=consolecmdline.
47. www.microsoft.com/resources/documentation/windows/.xp/all/proddocs/en-us/tasklist.mspx.
48. www.microsoft.com/resources/documentation/windows/xp/all/proddocs/enus/openfiles.mspx.
49. www.microsoft.com/technet/sysinternals/Security/LogonSessions.mspx .
50. www.microsoft.com/whdc/devtools/debugging/default.mspx.
51. www.ntsecurity.nu/toolbox/pmdump/.
52. www.sysinternals.com/Utilities/Handle.html.
53. www.sysinternals.com/Utilities/ListDlls.html.
54. www.sysinternals.com/Utilities/PsList.html

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

III DEO

SVEDOČENJE I VEŠTAČENJE U INFORMACIONO KOMUNIKACIONIM TEHNOLOGIJAMA

Cilj ove glave udžbenika je da studentima približi specifičnosti ekspertskog svedočenja i sudskog veštačenja pred sudom u slučajevima visokotehnološkog, posebno kompjuterskog kriminala. Razumevanjem specifičnih aspekata IKT veštačenja u odnosu na brojne tradicionalne forenzičke discipline (sudsku medicinu, veštačenje u saobraćaju itd.), forenzičari se osposobljavaju za timski rad sa specijalnim istražiteljem digitalnih podataka, tužiocem i istražnim sudijom na izgradnji čvrstih digitalnih dokaza, kao i da se naviknu na atmosferu i uslove koji vladaju u sudnici na glavnom pretresu, posebno u uslovima unakrsnih ispitivanja, koji se za tehničke eksperte često čine neprirodnim.

UNIVERZITET
PRIVATNI
AKREDITOVANI
UNIVERZITET
SINGIDUNUM

1. ISKUSTVA SVEDOČENJA I VEŠTAČENJA IZ DRUGIH NAUČNO-TEHNIČKIH DISCIPLINA

1.1 SUDSKI VEŠTACI ZA SAOBRAĆAJ

Iskustva veštačenja iz drugih disciplina dragocena su za oblast IKT veštačenja. Primeri su brojni i ta iskustva treba koristiti. Korisno iskustvo iz prakse je slučaj procenitelja štete u saobraćajnim udesima, [9]. Klasičan je primer iz pravosudne prakse SAD neuspelog svedočenja dva poštena i kvalifikovana tehnička eksperta, koji iznesu svoja svedočenja, ali ne uspevaju da adekvatno razreše slučaj. Onda forenzički analitičar presuđuje slučaj, utvrđujući identičnost hemijskog sastava guma optuženog sa tragovima guma na mestu zločina [10]. Poznato je da agresivna spremnost advokata da po svaku cenu odbrane svoju stranku, u velikoj meri odvraća tehničke eksperte da svedoče pred sudom, jer dolaze u neprijatne situacije unakrsnog ispitivanja advokata.

Iskustva iz ove oblasti veštačenja ukazuju da konstruktivno unakrsno ispitivanja eksperta druge strane može potvrditi tačnost osnovnih činjenica, principa ili ograničenja datih u svedočenju eksperta, kao i da je najčešći razlog za napad u unakrsnom ispitivanju ispoljena pristrasnost, predrasuda ili neobjektivnost IKT eksperta. Tu spadaju i pitanja da li je neki ekspert plaćen da svedoči i koliko, ili nije i zašto svedoči ako nije plaćen.

1.2 EKSPERTI ZA FORENZIČKU ANALIZU UMETNIČKIH DELA

Eksperti za forenzičku analizu umetničkih dela imaju velike sličnosti i nude dobra iskustva ekspertima za forenzički analizu digitalnih dokaza. Kao u proceni falsifikata velikih umetničkih dela, IKT ekspert u civilnim parnicama ili krivičnim delima kompjuterskog kriminala mora izvršiti rekonstrukciju digitalnih dokaza, ponašanja računarske mreže u slučaju napada, rekonstrukciju traga napada, identifikaciju i autentifikaciju digitalnih dokaza i njihovih autora ili korisnika, [7].

1.3 FORENZIČAR GEOLOG I EKSPERT ZA TAJNE GROBNICE

Forenzičar geolog i ekspert za tajne grobnice nude veoma dragocena iskustva za razumevanje IKT ekspertize - kako na jednostavan i razumljiv način izneti naučna saznanja zvaničnim pravosudnim i istražnim organima, koji nemaju ta znanja i iskustava. Ovi eksperti potpisuju i u praksi sprovode etičke i druge kodekse ponašanja, moraju poštovati mnoge procedure i standarde, potpuno ih dokumentovati, a rezultate i zaključke bazirati na podacima, informacijama i znanjima koja pripadaju polju njihove ekspertize. Oni

moraju održati svoju akademsku i profesionalnu reputaciju na najvišem nivou, jer suprotna strana uvek pokušavati dovesti u pitanje neki deo reputacije eksperta. Ekspert - veštak mora biti spreman profesionalno i lično da uvek pruži najbolju predstavu svoje karijere, iako bez činjenica nema garancije da ispravna teorija, metode i adekvatna veština prezentacije dokaza, mogu uspešno razrešiti neki forenzički problem, [3].

1.4 ISKUSTVA IZ SUDSKE MEDICINE

U sudskoj medicini**,** uspostavljeni standardi su podvrgnuti proveri naučne javnosti, dok u oblasti IKT, mnogi aspekti IKT veštačenja samo su objavljeni kao uspešni ili neuspešni hakerski napadi bez izlaganja široj naučnoj javnosti i uspostavljanja pouzdanih standarda u većini zemalja u svetu. Uspostavljanjem standarda iz oblasti IKT ekspertskog svedočenja i IKT veštačenja, olakšaće se rad IKT profesionalaca, njihovih organizacija i udruženja, kao i pravosudnog sistema i društva u celini.

Kao i forenzičar sudske medicine, ekspert koji u kriminalnom slučaju skuplja uzorke tela za analizu, tako i IKT forenzički ekspert – IKT veštak, treba da uzme tačnu fizičku kopiju slike podataka sa medija računarskog sistema i drugih uređaja za skladištenje podataka za kasniju forenzičku analizu i ispitivanje. Sudnica je sama po sebi strana i negostoljubiva sredina za IKT eksperta – naučnika. Nedostatak regulative o sudskom veštačenju u oblasti IKT može biti noćna mora za advokate i sudije koji nemaju načina da procene kvalifikaciju, stručne sposobnosti IKT eksperta, kao ni kvalitet i pouzdanost prezentiranih digitalnih dokaza, [8].

1.5 FORENZIČKI ENTOMOLOZI

Forenzički entomolozi (nauka o insektima) pomažu u utvrđivanju vremena ubistva i lokaciji tela, nađenih u prirodnoj sredini, u trenutku ubistva, analizom dokaza iz okruženja koji se odnose na insekte. Digitalni forenzičar za rekonstrukciju događaja mora da dokaže vreme događaja prateći vremensku liniju kroz brojne uređaje, potencijalno široko distribuirane na Internetu. U kompjuterskom okruženju čak je za softversku grešku preuzeta i reč **bag** (*bug*), koja označava seriju problema u računarskim programima, nastalih zbog grešaka podataka, [5].

REZIME

Porastom zloupotreba IKT i kompjuterskog kriminala, ukazala se potreba za detaljnijom zakonskom regulativom istrage, dokazivanja i sankcionisanja zloupotreba i slučajeva kompjuterskog kriminala, kao i za normativnim regulisanjem uslova, načina i postupka organizovanja stručnih lica–veštaka u oblasti IKT i odgovarajućih stručnih, etičkih i legalnih profila koje bi morali ispunjavati, radi otkrivanja, dokazivanja i razrešavanja odlučujućih činjenica u građanskoj i krivično pravnoj zaštiti oštećenih.

Veštačenje digitalnih dokaza, kao najmlađa oblast sudskog veštačenja, nasledila je bogata iskustva iz tradicionalnih oblika veštačenja, pre svega: saobraćaja, umetničkih dela, sudske medicine, geologije, entomologije i dr. Brojne specifičnosti ekspertskog svedočenja i veštačenja u IKT, zahtevaju da se ova oblast posebno istraži.

PITANJA ZA PONAVLJANJE

1. Iz kojih disciplina su važna iskustva za oblast IKT veštačenja?
2. Na koji način su važna iskustva eksperata za forenzičku analizu umetničkih dela?
3. Koje su sličnosti veštačenja digitalnog forenzičara sa veštakom sudske medicine?
4. Zašto su značajna iskustva iz veštačenja umetničkih dela?
5. Kako se mogu iskoristiti iskustva forenzičkih entomologa?

2. SPECIFIČNOSTI SVEDOČENJA I VEŠTAČENJA U KOMPJUTERSKOM KRIMINALU

Eksperti IKT iz naučnih krugova, bez obzira da li su angažovani u akademskim profesijama ili nisu, uvek su iznenađeni sa fenomenom ispitivanja u parničkom procesu. Za njih su neprihvatljiva pravila rivaliteta u legalnom pravosudnom sistemu, nasuprot principa kolegijalnosti, koji je se podrazumeva i barem je teoretski prisutan u svetu nauke i akademske profesije. Posebno je to slučaj u unakrsnom ispitivanju agresivnih advokata suprotnih strana. Takođe, eksperti se moraju navići i na uobičajenu ležernu atmosferu u sudnici pre ulaska sudije i porote i krajnje napetu atmosferu posle njihovog ulaska, kada se sve drastično menja, [10].

Generalno, specifične veštine koje digitalni forenzičar za ekspertsko svedočenje i/ili veštačenje treba da poseduje mogu se grupisati u sledeće kategorije**:**

- Identifikovati relevantne elektronske dokaze za povredu specifičnog zakona;
- Identifikovati i objasniti verovatni uzrok u meri koja je dovoljna za dobijanje
- naloga za pretres i razumeti ograničenja naloga;
- Locirati i oporaviti relevantne elektronske dokaze iz računara primenom različitih forenzičkih alata;
- Razumeti i održavati sve zahteva u lancu istrage;
- Slediti dokumentovan proces digitalne forenzičke istrage (standardne operativne procedure).

Posebno digitalni forenzičar mora posedovati specifične veštine i poznavati sledeće izvore digitalnih dokaza:

1. *Izvore korisnički kreiranih elektronskih dokaza:*
    - address book (adresar)
    - fajlovi e-pošte,
    - audio/video fajlovi,
    - fajlovi slika/grafike,
    - kalendari,
    - Internet indeksi (*bookmark*) za omiljene lokacije (*favorites*),
    - fajlovi baza podataka,
    - fajlovi tabela (*spreadsheet*),
    - dokumenta ili tekstualni fajlovi
2. *Izvore kompjuterski generisanih digitalnih dokaza*:
    - fajlovi za bekapovanje,
    - log fajlovi,
    - konfiguracioni fajlovi,

- printerski *spool* fajlovi,
- kolačići (*cookies*),
- *swap* fajlovi,
- skriveni fajlovi,
- sistemski fajlovi
- fajlovi istorije rada aplikacija,
- privremeni fajlovi.

3. *Mesta za pretraživanje i identifikaciju digitalnih dokaza*:
   - loši klasteri,
   - računarski podaci o datumu, vremenu i lozinki,
   - izbrisani fajlovi,
   - slobodan prostor diska (neupisani klasteri),
   - sakrivene particije,
   - izgubljeni klasteri,
   - metapodaci u fajl sistemu,
   - druge particije,
   - rezervisane oblasti u logičkim particijama fajl sistema,
   - fajl *slack* prostor,
   - informacije o registraciji softvera,
   - sistemske oblasti u fajl sistemu (FAT 16, FAT 32) i oblast podataka u NTFS fajl sistemu,
   - nealocirani prostor diska (ostaci podataka izbrisanih fajlova).
4. *Izvore dokaza o aktivnostima na Internetu:*
   - kolačići (*cookies*): lokacija, sadržaj, alati kolačića,
   - keš pretraživača (Internet keš): lokacija, alati.

Svi izneseni primeri tehničke ekspertize i zahtevi za specifičnim veštinama u oblasti digitalne forenzike, ukazuju na značaj formiranja na nivou države, pored zvaničnih organa digitalne forenzičke istrage, šire interesne zajednice digitalnih forenzičara i drugih eksperata za istragu kompjuterskog kriminala (na primer, instituta ili strukovnih udruženja IKT veštaka u različitim oblastima kompjuterskog kriminala). Ova zajednica treba da obezbedi standardizaciju i sertifikaciju: principa, metodologije i tehnologije digitalne forenzičke istrage, akvizicije, analize i ekspertskog svedočenja/ veštačenja pred sudom, kao i profesionalnih profila samih IKT eksperata.

2.1 PRIPREMA DOKAZA ZA SUDSKI PROCES

Najznačajnija pitanja za tužioce u toku istrage, dokazivanja i pripreme za veštačenje pred sudom je da obezbede osnovna znanja o tehničkim aspektima digitalnih dokaza i dovoljno vremena za rukovanje raspoloživim digitalnim dokazima, [8].

Kako efikasne pripreme za glavni pretres počinju već nakon završetka istražnog postupka, potreba za kompetentnim tehničkim znanjima održava se kroz ceo tok slučaja. U predistražnom postupku, u procesu pripreme treba obratiti pažnju na pripremu tužioca na obim istrage, efikasnu komunikaciju između tužioca, organa istrage i forenzičkog analitičara i na rukovanje sa digitalnim dokazima.

2.2 PRELIMINARNA PRIPREMA TUŽIOCA

Idealno, slučaj sa digitalnim dokazima treba da razvija i priprema tim koji se sastoji od najmanje tri lica: tužioca, kriminalističkog inspektora i forenzičara (IKT veštaka). Često slučaj sa digitalnim dokazima predstavlja posebno proceduralno i materijalno pitanje. Jedan od prvih zadataka tužioca naimenovanog za vođenje slučaja, je uvid u obim istrage, što uključuje nekoliko ključnih pitanja i razmatranja, [10]:

- priprema razumljive prezentacije slučaja za glavni pretres (otkrivanje činjenica),
- razjašnjavanje prirode tehnoloških pitanja (tehnika i alata),
- identifkacija i objašnjenje izvora i prirode digitalnih dokaza,
- identifikovanje potencijalnih izvora materijalnih digitalnih dokaza (npr., bekap datoteke, log datoteke itd.).
- razmatranje svih odgovarajućih sankcija.

2.3 KOMUNIKACIJE U PREDISTRAŽNOM POSTUPKU

Sva tri člana istražnog tima treba da se sastaju više puta pre glavnog pretresa radi planiranja veštačenja nalaza i razmene mišljenja o konkretnom slučaju, uključujući: razjašnjavanje i analizu rezultata istrage, zakonske osnove slučaja, elemenata krivičnog dela i prihvatljivih elemenata odbrane; razmatranje najverovatnijeg obima i pravca glavnog pretresa, saslušanja svedoka i unakrsnih ispitivanja; određivanje tipa digitalnih dokaza i razmatranje propisa o rukovanju sa digitalnim dokazima, [4], [6].

2.4 DEFINISANJE USLOVA ZA IZNOŠENJE DIGITALNIH DOKAZA

Uslovi koje treba razmatrati pre iznošenja digitalnih dokaza pred sudom obuhvataju, [5], [9]:

- Diskreciono pravo sudija o prihvatljivosti digitalnih dokaza;
- Relevantnost digitalnog dokaza za dokazivanje, ili pobijanje osnovane sumnje, gde je relevantan "dokaz koji ima tendenciju da izgrađuje nepobitnu činjenicu", a posebno se razmatraju štetnost i prigovor da je dokaz "dokaz drugog zločina, greške ili dela";
- Autentifikacija digitalnog dokaz u toku svedočenja sa nekom razumnom verovatnoćom;
- Posrednost svedočenja zbog posredne prirode digitalnih podataka i dokaza.
- Razlikovanje čvrstog digitalnog dokaza prethodno uskladištenog u računaru, od ilustrativnih (pomoćnih) kompjuterskih dokaza koji samo ilustruje tvrdnju (svedočenje), ali ništa sam po sebi ne dokazuje;
- Autentifikacija kompjuterski uskladištenih čvrstih dokaza čime tužilac mora pokazati da je dokaz uskladišten u računaru, upravo ono što tvrdi da jeste;
- Prihvatljivost papirne kopije kompjuterski uskladištenih čvrstih dokaza, prema pravilu najboljeg dokaza.

Čak i ako se kompjuterski uskladišten dokument može sa tehničkog aspekta smatrati ne-originalnim dokumentom, naročito ako se uzme u obzir da su originalni podaci u računaru samo nizovi bitova (1 i 0), pravilo "najboljeg dokaza" ne pravi problem o prihvatanju odštampanog kompjuterskog dokaza kao originalnog dokaza, ako on tačno predstavlja uskladištene podatke. Ovaj princip primenjuje se čak i ako duplikat/kopija digitalnih dokaza nema isti izgled (ima različite fontove, margine i slika). Tako je moguće obimne fakture i kompleksne dokaze u slučaju finansijske prevare izneti na sudu kao relevantne dokaze.

2.5 PRIHVATLJIVOST KOMPJUTERSKI GENERISANIH DIGITALNIH DOKAZA NA SUDU

Prihvatljivost kompjuterski generisanih digitalnih dokaza na sudu određuju sledeći parametri, [1], [2]:

- Relevantnost digitalnih dokaza;
- Način integracije digitalnih dokaza kroz iskaz IKT veštaka u sudski proces;
- Autentifikacija i druga osnovna pitanja zaštite integriteta digitalnih dokaza;
- Posrednost kompjuterski generisanog dokaza, sa mogućnošću provere integriteta dokaza od uzimanja imidža u procesu akvizicije do veštačenja pred sudom, ako to sud zahteva.

2.6 SVEDOČENJE I VEŠTAČENJE IKT EKSPERTA

U međunarodnoj praksi razvijeno je više preporuka za ispitivanje mišljenja - svedočenja ili veštačenja IKT eksperta (*expert opinion testimony*) i prihvatanje istih kao dokaza na sudu, [10]. U praksi IKT veštačenja najčešće se prihvataju dokazi utvrđeni na naučnim principima. Po ovim principima sudija prihvata digitalni dokaz na osnovu njegove relevantnosti, pouzdanosti i proverljivosti predloženih naučnih metoda, tehnika akvizicije i analize i prezentacije digitalnih dokaza na sudu, za svaki konkretan slučaj. Sud odlučuje da li je svedočenje IKT veštaka bilo od pomoći za utvrđivanje odlučujućih činjenica i istine.

Generalno, sud može prihvatiti ekspertsko svedočenje, gde IKT ekspert na poziv suda, iznosi svoje stručno mišljenje o digitalnim dokazima koji optužuju ili oslobađaju, ali ne iznosi mišljenje o utvrđenim činjenicama, koje su relevantne za slučaj. Tehničko ekspertsko mišljenje treba da bude prihvatljivo za sud i kada ekspert/ forenzičar uvodi nove softverske alate ili nove verzije starijih softverskih alata za akviziciju i analizu digitalnih medija, ali primenjuje naučne principe digitalne forenzike i to na zahtev suda može potvrditi. Takođe, tehnike za primenu alata za akviziciju i analizu digitalnih dokaza, na osnovu kojih forenzičar izvlači zaključke, moraju biti za sud relevantne, pouzdane, proverljive i u skladu sa usvojenim principima i da se na zahtev suda mogu testitrati i verifikovati. IKT veštačenje podrazumeva da o digitalnim dokazima svedoči zakleti IKT ekspert – ovlašćeni sudski veštak, koji iznosi stručno mišljenje o digitalnim dokazima, ali i o utvrđenim relevantnim činjenicama koje se odnose na slučaj, [10].

Suđenja koja uključuju digitalne dokaze razlikuju se od svih drugih suđenja sa dva glavna aspekta:

- često se pokreće pitanje legalnosti prihvatanja digitalnih dokaza i
- ovaj proces uključuje kompleksan skup nepoznatih pojmova i termina.

Zato je pažljiva priprema digitalnih dokaza i planiranje prezentacije i korišćenja dokaza u sudskom procesu od posebnog značaja. Dobar metod prezentacije kompleksnih digitalnih dokaza, uključuje, [10]:

Korišćenje vrlo jednostavnih analogija za objašnjenje generalnog koncepta (npr. slanje e-maila je kao slanje poštanske karte);

- Definisanje tehničkih reči pojmovima koje pravosudni organi i porota mogu razumeti;
- Korišćenje Slika, crteža ili grafikona za demonstraciju kompleksnih sistema;
- Izgradnju svedočenja početi kroz uvodnu reč sa jednostavnim konceptima, a zatim preći na kompleksnija pitanja koja objasniti u detalje;
- Povezivanje tehnologije u slučaju sa tehnologijama koje su prisutni pravosudni organi i drugi u sudnici već upoznali ili koristili, gde je moguće.

2.6.1 Edukovanje pravosudnih organa

Ako je slučaj kompleksan, potrebno je edukovati sve prisutne u sudnici (sudiju i porotu) u svakoj fazi suđenja (parnice). Edukacija treba da obuhvati: proveru usklađenosti sa naučnim principima; proveru zakonske prihvatljivosti digitalnih dokaza i saslušanja IKT veštaka pre glavnog pretresa; primenu principa uviđaja; uvodnu izjavu; svedočenje/veštačenje IKT eksperta; unakrsno ispitivanje i završnu reč (izjavu) i zatvaranje svedočenja/veštačenja, [10].

Iako je važno za sudiju i porotu održavati na minimalnom nivou razumevanja, nije cilj da se od njih stvaraju eksperti za samu po sebi kompleksnu problematiku IKT veštačenja, nego da shvate suštinu ekspertskog svedočenja ili veštačenja.

Svaki slučaj zahteva da tužilac pažljivo razmotri šta treba da bude dokazano/opovrgnuto i ispita sve elemente optužnice, da bi obezbedio prezentaciju ubedljivih dokaza za svaki elemenat optužnice. Često postoji konflikt između praktičnih ograničenja na to šta se može dokazati ili opovrći (pobiti) i šta od alternativnih objašnjenja advokat odbrane može iskoristiti da unese razumnu sumnju u dokazni postupak ili dokaze.

Šta jedan tužilac treba da opovrgava, zavisi od samog pitanja i snage preostalih dokaza u slučaju. Na primer, u slučaju dečije pornografije, kada je bitan elemenat poznat, može opovrći tvrdnju odbrane da su slike uskladištene u računar osumnjičenog bez njegovog znanja, jer nije razumno prihvatiti alternativu, tj. da su se u njegovom računaru slike pojavile same po sebi, osim ako odbrana ne dokaže da je računar kompromitovan (*zombiran*) trojancem i rutkit tehnikom, [4].

Važno pitanje je kada izabrati trenutak pobijanja tvrdnji odbrane. Na primer, ako je znanje osumnjičenog o sadržaju računara značajno, ponekad je mudro dopustiti da osumnjičeni pokrene pitanje i da sami dokazi (bilo kroz unakrsno ispitivanje, ili u ponovljenom procesu) pobiju ovu tvrdnju, pre nego da se opovrgavanje dokaza izvrši u glavnom pretresu.

2.6.2 Veštačenje i naučne metode dokazivanja kompjuterskog kriminala

2.6.2.1 Rekonstrukcija događaja u sudskom postupku kompjuterskog kriminala

Dok je svaki slučaj veštačenja koji uključuje digitalne dokaze međusobno različit, postoje neki zajednički elementi koje se javljaju u odnosu na osnovne elemente optužnice i prirodu računara i mreža, a to su, [10]:

Identitet osumnjičenog*: Iako digitalni dokaz može dokazati da je kriminalni akt izvršen sa kompjutera osumnjičenog, potrebno je direktno povezivanje osumnjičenog sa računarom sa kojeg je izvršen napad, na bazi ličnog priznanja ili izjave, posrednog zaključivanja, bitne informacije u računaru koje mogu postojati jedino sa znanjem osumnjičenog, analize sadržaja, gramatike i stila koji ukazuju na osumnjičenog i slika*

Znanje*: U nekim slučajevima potrebno je pokazati da osumnjičeni ima adekvatno znanje i poznaje digitalne dokaze na računaru.*

Hronologija događaja*: Vreme i datum kreiranja fajlova mogu biti moćan dokaz koji povezuje osumnjičenog sa računarom i kompjuterskim incidentom, uključujući sva ograničenja koja se odnose na laku izmenu vremena i datuma u računaru.*

2.6.2.2 Instruisanje porote

Ne postoji obrazac instrukcije porote za slučajeve kompjuterskog kriminala prihvatljiv za većinu pravosudnih sistema. Takođe, teško je i prilagoditi neki potvrđen sistem instrukcija porote za slučajeve kompjuterskog kriminala iz drugog pravosudnog sistema u konkretan pravosudni sistem. Mogu se koristiti instrukcije za porotu uzete iz oblasti veštačenja fizičkih dokaza, a zasnovane na elementima sličnosti krivičnog dela. Na primer, instrukcije za provalu i prevaru mogu poslužiti kao model za prevaru u kompjuteru.

Treba pažljivo razmotriti sastav porote i ne birati samo tehničke eksperte da budu članovi porote, nego pronaći nekoliko lica koja imaju dovoljno iskustva iz korišćenja računara, da bi bili sposobni da prate tehničko veštačenje u toku procesa. Idealno je da jedan do dva člana porote budu sposobni da shvate digitalne dokaze i da mogu to objasniti ostalim članovima, kada porota donosi odluku posle pretresa, [10].

Treba razmišljati o problemu uključivanja IKT eksperta u porotu, na isti način kao o uključivanju lekara u porotu za slučaj u kojem je relevantna praksa sudske medicine. Kako doktor medicine može objasniti komplikovan medicinski koncept ostalim članovima porote, tako i IKT ekspert može razjasniti komplikovana i kompleksna pitanja razumevanja digitalnih dokaza.

REZIME

Eksperti IKT, koji uglavnom dolaze iz naučnih krugova, uvek su iznenađeni sa fenomenom ispitivanja u sudskom/parničkom procesu, posebno u slučaju unakrsnog ispitivanja agresivnih advokata suprotne strane. Za njih su neprihvatljiva pravila rivaliteta u legalnom pravosudnom sistemu, nasuprot principa kolegijalnosti, koji se podrazumeva u svetu nauke i akademske profesije.

Specifične veštine koje digitalni forenzičar za ekspertsko svedočenje i/ili veštačenje treba da poseduje mogu se grupisati u sledeće kategorije**:** identifikovati relevantne elektronske dokaze za povredu specifičnog zakona; identifikovati i objasniti verovatni uzrok u meri koja je dovoljna za dobijanje naloga za pretres i razumeti ograničenja naloga; locirati i oporaviti relevantne elektronske dokaze iz računara primenom različitih forenzičkih alata; razumeti i održavati sve zahteva u lancu istrage; slediti dokumentovan proces digitalne forenzičke istrage (standardne operativne procedure) i razviti veštinu koncizne, razumljive i terminološki pojednostavljene prezentacije digitalnih dokaza i svedočenja/veštačenja pred sudom.

Timski rad tužioca/istražnog sudije, kriminalističkog inspektora (rukovodioca istrage) i forenzičkog analitičara digitalnih dokaza (IKT veštaka) osnovni je zahtev u istrazi, dokazivanju, pripremi i prezentaciji digitalnih dokaza pred sudom.

U pripremi za glavni pretres slučaja koji sadrži digitalne dokaze, tužilac mora razmatrati niz važnih pitanja, kao što su: iskustva iz drugih naučno-tehničkih oblasti ekspertskog veštačenja; autentifikacija i priprema čvrstih digitalnih dokaza za prezentaciju, i priprema IKT veštaka za svedočenje pred sudom.

Očekuje se da forenzička analiza digitalnih dokaza otkrije najviše potrebnih podataka za izgradnju čvrstog, neoborivog digitalnog dokaza bez tzv. pukotina. Postoji velika razlika između kompjuterskog digitalnog dokaza u računaru (*computer evidence*) i čvrstih, neoborivih dokaza (*proof*) prihvatljivih na sudu. Neoborivi, čvrsti dokaz nepobitno uspostavlja činjenice, ali je to i subjektivna interpretacija kompjuterskog digitalnog dokaza koji izvodi veštak za informacione tehnologije. Kompjuterski digitalni dokaz u računaru je objektivan digitalni podatak i može se koristiti u meri u kojoj se može dokazati da nije izmenjen, na primer, ulazna log datoteka je uvek ulazna log datoteka.

U procesu pripreme digitalnih dokaza tužilac mora razjasniti relevantana pitanja kao što su: dokazna vrednost, posrednost i prihvatljivost; štetnost i značaj za slučaj; čvrsti kompjuterski uskladišteni i kompjuterski generisani dokazi i ilustrativni (pomoćni) kompjuterski dokazi za slučaj.

U procesu pripreme IKT veštaka za svedočenje (veštačenje) pred sudom, tužilac mora pripremiti veštaka za: dokazivanje naučnog karaktera digitalnih dokaza, jednostavnu i uverljivu rekonstrukciju kompjuterskog incidenta (identiteta i znanja osumnjičenog, i hronologije incidenta) pred sudom, neophodnu edukaciju svih prisutnih u sudnici o najnužnijim znanjima o primenjenim IKT u slučaju i za instruisanje porote.

PITANJA ZA PONAVLJANJE

1. Navedite glavne specifičnosti veštačenja digitalnih dokaza.
2. Kad počinje priprema dokaza za sudski postupak?
3. Navedite ključna pitanja za preliminarnu pripremu tužioca.
4. Zašto je značajna dobra komunikacija u predistražnom postupku?
5. Koje uslove treba razmatrati pre iznošenja digitalnih dokaza pred sudom?
6. Koji ključni parametri određuju prihvatljivost kompjuterski generisanih digitalnih dokaza na sudu?
7. Na osnovu čega sudija prihvata digitalni dokaz?
8. Koje elemente uključuje dobar metod za prezentaciju kompleksnih digitalnih dokaza?
9. Zašto je potrebno edukovanje sudskih organa?
10. Koji su zajednički elementi u rekonstrukciji tipičnog događaja kompjuterskog kriminala?

KLJUČNI TERMINI

Digitalni dokaz: «digitalni dokaz je svaka informacija koja ima dokazujuću vrednost, koja je ili uskladištena ili prenesena u binarnoj (digitalnoj) formi»; uključuje kompjuterski generisan i uskladišten dokaz, digitalni audio, digitalni video, mobilni telefon, digitalnu fax mašinu, itd; digitalni dokaz je informacija uskladištena ili prenesena u binarnoj formi na koju se sud može osloniti.

Diskretno sudijsko pravo: pravo sudije da prihvati dokaz na bazi procene relevantnosti, štetnosti ili prigovora da je „dokaz drugog zločina ili dela", pouzdanosti i naučne proverljivosti tehnika i alata za prikupljanje, analizu i izgradnju čvrstih dokaza.

Duplikat digitalnog dokaza: precizna digitalna reprodukcija svih objekata podataka koji se sadrže u originalnom fizičkom predmetu.

Ekspertsko IKT svedočenje: objektivno svedočenje IKT eksperta koji iznosi samo naučno utvrđene činjenice, ali ne i svoje mišljenje.

Entomologija: grana zoologije koja se bavi izučavanjem insekata.

Fizički predmet: Predmeti u kojima mogu biti uskladišteni objekti podataka ili informacije i/ili sa kojima su objekti podataka preneseni.

Glavni pretres: sudski proces na kome se pretresaju sve činjenice i dokazi prikupljeni u istražnom postupku od strane tužilaštva i odbrane.

IKT ekspert: stručnjak iz oblasti IKT koji ima adekvatno regularno obrazovanje, ali i sertifikovanu obuku i stečene veštine iz neke uže IKT oblasti.

IKT veštačenje: objektivno svedočenje IKT eksperta koji iznosi naučno utvrđene činjenice, ali i svoje mišljenje o događaju.

Kompjuterski kriminalci*:* rade sa ili bez računara – kradu tuđe industrijske i nacionalne tajne, kradu novac, uništavaju datoteke, OS ili menjaju podatke Web stranica ili baza podataka.

Kopija digitalnog dokaza: precizna reprodukcija informacija koje su sadržane na originalnom fizičkom disku/medijumu, nezavisno od originalnog fizičkog diska/medijuma

Orginalni digitalni dokaz: fizički predmeti/objekti koji sadrže podatke u vreme akvizicije ili privremenog oduzimanja predmeta/objekata.

Posrednost digitalnih dokaza: inherentna priroda računarski generisanih podataka, koja odražava činjenicu da direktan digitalni dokaz može obezbediti samo počinilac krivičnog dela kompjuterskog kriminala.

Rekonstrukcija digitalnog dokaza: izgradnja čvrstog, neoborivog digitalnog dokaza iz ogromne količine digitalnih i drugih podataka sakupljenih u procesu akvizicije.

Rekonstrukcija traga napadača: praćenje traga napadača od napadnutog računara, preko posrednih računara (ISP ili korumpiranih računara), kao i provajdera telefonskih usluga do izvornog računara sa kojeg je napad izvršen; ne uključuje povezivanje identiteta napadača sa malicioznim aktivnostima na izvornom računaru sa ispitivanim događajem, što je i najteži deo u rekonstrukciji krivičnog dela.

Relevantnost digitalnih dokaza: određuje sudija, koristeći diskreciono pravo, na bazi procene značaja dokaza za slučaj, eventualne štetnosti i procene da li je „dokaz za drugo krivično delo".

Rukovanje digitalnim dokazima: čuvanje i zaštita integriteta digitalnih dokaza u celom lancu istrage – od otkrivanja i akvizicije dokaza do svedočenja/veštačenja pred sudom.

Sudski veštak: stručno lice koje ima formalno, stručno i specijalističko obrazovanje iz neke tehničke oblasti, sa zakletvom pred sudom da će svoje stručno mišljenje bazirati na strogim naučnim principima i iznositi objektivno i nepristrasno u cilju dokazivanja ili oslobađanja osumnjičenog.

Unakrsno ispitivanje: ispitivanje svedoka/veštaka na glavnom pretresu od strane advokata tužilaštva i odbrane.

LITERATURA

1. Anthony F. Desante, *Evidentary Consideration for Collecting and Examining Hard-Drive*, Media 28.11. 2001, Forensic Sciences 262, The George Washinton University.
2. Carrier B., *Open Source Software in Digital Forensics*, carrier&atstake.com).
3. *COAST project PERDU University*, http://www.cs.perdue.edu/coast-library.html. *http://www.iacis.org/*.
4. Icove, D., Segar, K., and VonStorch, W., *Computer Crime, A Crimefighter's Handbook,* O'Reilly & Associates.
5. IOCE, *IOCE Principles and Definitions*, 2. sastanak, 7.10.1999, Marriott Hotel, London.
6. Krsul I. & Spafford E. H., *Authorship Analysis: Identifying the Author of a Program,* Department of Computer Sciences, Purdue University, CSD-TR-96-052, 1996.
7. Pettinari Cmdr. D., *Handling Digital Evidence from Seizure to Court Presentation,* juni 2000.
8. Pollit M. M., *Report on Digital Evidence (Izveštaj FBI CART, DC Washington, USA),* Interpol Forensic Science Symposium, Lyon, France, 16-19.10.2001.
9. Robbins J., *PC software forensic, Expert witness, An Explanation of Computer Forensics,* 2003.
10. Rosenblatt, K. S., *High Technology Crime — Investigating Cases Involving Computers,* KSK Publications, San Jose, CA, 1995.
11. Spafford E. H. & S. A., *Software Forensics: Tracking Code to Its Authors*, Weeber, *Computers & Security,* 12(6), pp. 585–595, Dec. 1993.
12. Whitcomb C. M., *A Historical perspective of Digital Evidence: A Forensic Scientist s View,* International Journal of Digital Evidence, vol.1, issuue 1, proleće 2002.

PRILOG I

ISTORIJSKI RAZVOJ DIGITALNE FORENZIČKE

- **1980-tih**: prva razmena informacija o napadima na računare i mreže između agenata tajnih službi (*Geeks with Gins*), SAD (Maryland, Baltimore).
- **1980-1990**:
  - slaba podrška menadžera, nerazumevanje razlike između kompjuterskog kriminala i digitalne forenzika (diferencijacija tek 1990-tih);
  - rana tehnologija digitalne forenzike (8 inča disketa, IBM PC, telekomunikacioni sistemi) za sprečavanje gubitaka, prevara I zaštitu;
  - rani oblici pedofilije preko Interneta;
  - rani oblici hakerskih napada preko Interneta;
  - napad *Morris* crvom;
  - nema opšte svesti i priznanja da su ovi napadi veliki problem.
- **Rane 1990-te**:
  - počelo formiranje organizacija za istragu komopjuterskog kriminala u državama SAD;
  - prva organizacija u policiji Portlanda.
- **Sredninom 1990-tih**:
  - projekat *Nevine slike*, 1993. policijski detektivi u Maryland, SAD (pedofilija http://www.fbi.gov/publications/innocent.htm), rutinsku otkrili razmenu pornografskih slika zloupotrebu dece u periodu od preko 25 godina;
  - još nije bilo slučajeva suđenja, ali se kriminal događa;
  - FBI osniva jedinicu za digitalnu forenziku;
  - većina državnih agencija nema potrebne resurse za digitalnu forenziku;
  - počinje razvoj politika i procedura sa ciljem obezbeđivanja prihvatljivosti u sudskom procesu;
  - **1993**: prva eksplozija bombe u WTC (Svetskom trgovinskom centru), osumnjičeni imao računar kod kuće i na poslu; oba računara sa HD od 20MB privremeno oduzeti; za istragu ceo sadržaj sa HD odštampan; otkriveni fragmenti pisma *NY Times*-u u kojem se prihvata odgovornost za eksploziju;
  - **1995**: eksplozija u *Oklahoma City* , još uvek mali kapacitet digitalnih medija i slična istraga.
- **Kasne 1990-te**:
  - počelo bekapovanje dokaza (kompjuterska forenzika kritična u većini slučajeva);

- uspostavljaju se nacionalne i međunarodne organizacije za digitalnu forenziku;
- kompjuterska forenzika priznata kao naučna disciplina(1999) od relevantnih naučnika i istraživača.

- **2000-te**:
  - velika količina digitalnih podataka na raspolaganju („digitalno zagušenje“) prati sve aktivnosti pojedinaca – brojni potencijalni digitalni dokazi;
  - klasični kriminal proizvodi veliku količinu digitalnih dokaza;
  - kompjuterski kriminal – ogromna količina kompleksnih digitalnih dokaza;
  - zvanični organi istrage nespremni za ispitivanje tolike količine digitalnih podataka;
  - dolaze do eksplozivnog razvoja kompjuterske forenzičke nauke; obuka, oprema i praktična znanja ne prate ovaj rast; nedostaju prave definicije i standardi;
  - digitalni dokazi priznati na sudu i stavljeni u ravan DNK dokaza (*American Society of Crime Lab Directors Accreditation Board,* dao jedno od najbržih odobrenja);
  - većina slučajeva predstavlja sve tipove kriminala;
  - 2001: rušenje WTC, posle jedne sedmice istrage prikupljeno 175GB relevantnih digitalnih podataka; do decembra 2001 – 125 terabajta (TB) u traženju odgovora „sta znamo o osumnjičenim“?
- **Srednje 2000-te do danas:**
  - ni jedan digitalni forenzičar ne može biti dovoljno iskusan da radi sa svim tehnologijama i slučajevima kompjuterskog kriminala; potrebno je uspostaviti nove uloge/odgovornosti za kompleksnu problematiku digitalne forenzike;
  - problem akvizicije i analize ogromne količine digitalnih podataka;
  - sporo uspostavljanje legalnih standarda za prihvatljivost digitalnih dokaza i veštačenje pred sudom;
  - razvoj standarda za forenzičke laboratorije i digitalne forenzičare;
  - standardi najbolje prakse i validacije forenzičkih tehnika i alata;
  - definisanje slojeva apstrakcije i željenih svojstava forenzičkih alata: *integritet podataka, autentifikacija autora forenzičke akvizicije/ analize, ponovljivost procesa, ne unošenje kontaminacije podataka, minimizacija količine podataka za analizu;*
  - definisanje svojstava digitalnih dokaza koja se mogu prikazati u određenom alatu/tehnici;
  - napuštanje prakse da jedno lice radi sve poslove digitalne forenzike i specijalizacija poslova; pokazalo se korisnim za razvoj standarda, procedura i obuke u digitalnoj forenzici;

- diferenciranje poslova u oblasti digitalne forenzike: *kriminalistički tehničar za digitalnu forenziku* (pretraga mesta krivičnog dela kompjuterskog kriminala i sakupljanje dokaza), *digitalni forenzičar-ispitivač* (proces, analiza, validacija digitalnih podataka/dokaza) i *digitalni forenzičar –istražitelj* (analiza i interpretacija digitalnih dokaza).

Razvoj forenzičke nauke analize DD [12] :

- 13. Interpolov simpozijum *forensic science.*
- 3. izveštaj o digitalnim dokazima (prvi 1995).
- Već je formirana međunarodna interesna zajednica naučih digitalnih forenzičara (IOCE-*International Organization on Computer Evidence*), sa svojim profesionalnim naučnim telima i laboratorijama. (za izveštaj 70 agencija dalo svoje priloge)
- *Forensic Computing Group*, UK: mađu najstarijim organizovanim; ima nekoliko agencija za istragu i forenzičku analizu; sadrži ASPO (*Association of Chief Police. Oficers*) – prvo uputstvo za otkrivanje i zaplenu računara, CCWG (*Computer Crime Working Grou*p).
- *Europian Network of Forensic Science Institutes - Forensic Information Technology Working Group* (FIT-WG): formirana 1998, prvo uputstvo za standarde i procedure, domaćin sastanka IOCE 2000.; septembra 2001 domaćin obuke u Norveškoj, Oslo (istraga i forenzika IT: **http://www.ensfi.org.**
- *National Institute of Justic*e, USA: od 1997 radi na dokumentaciji- prvi odgovor na kompjuterski kriminal sa digitalnim dokazima, razvoj DE laboratorije (podaci sa: **http://www.ojp.usdoj.gov/nij/pubs.htm**).
- SWGDE, formirana 1997: TWGDE formirana od FBI kadrova u SAD, prerasta u SWGDE sa DE forenzičarima iz Kanade - izdali *Predlog standarda za razmenu digitalnih dokaza* (rukovanje DE) 1999.
- IOCE (*International Oganaisation on Computer Evidence*), formirana 1997.
- SWGDE (*Scientific Working Group on Digital Evidence*), februara 1999.
- U 1999. CART (FBI u SAD ima više od 50 kancelarija) obezbeđuje terenski rad u potrazi i zapleni osumnjičenih računara, kao i forenzičku analizu u laboratoriji sa više od 2.400 analiza kompjuterskih dokaza.
- *Forensic Science Laboratory*, MUP Slovenije, Stefanova 2, 1501 Ljubljana, Slovenija, 2002.
- *Udruženje sudskih veštaka za informacione tehnologije „IT Veštak",* Danijelova 32, 11000 Beograd, 2002.
- Uzimanje miror slike diska/kopiranje strima bitova 1980-ih, prvi proizvod.
- Naknadna analiza, pravljenje izveštaja o rezultatima analize.
- Pojava alata za forenzičku analizu, integracija alata za akviziciju i analizu.
- Alati: **DIBS, Safeback, Mresware, NTI Authentec, EnCase, AccessData FTK, ILOOK.**

- Većina proizvoda za PC i Win OS osim: **TCT Coroner Toolkit** (Dan Farmer i Wietse Venema), TASK-&Stake **Sleuth Kit.**
- Preko 93 % svih snimljenih materijala u svetu 1999. bilo je u digitalnom formatu. Mnogo je urađeno na formatima fajlova.
- IJDE *(International Journal of Digital Evidence.*
- Analiziraju se podaci-dokazi sa: velikih sistema HD, FD, CD,..; udaljenih sajtova, računarskih mreža, kao i dokazi dobijeni prisluškivanjem podataka u toku transmisije.
- Za analizu diskova formirani su najviši standardi analize.
- SAD pristup novim naučnim dokazima: sudija deluje kao čuvar kapije-dokaz nije prihvatljiv sve dok generalno nije naučno prihvaćen, dok se ne da testirati, da se metoda dokazivanja može proveriti, da dokazi lako prezentiraju na sudu.
- Legalni dokaz je ono što se demonstrira pred sudom.
- Digitalni dokaz mora biti: *prihvatljiv, autentičan, tačan, kompletan, ubedljiv za sud.*
  - **Prihvatljiv**: u skladu sa uobičajenom pravosudnom praksom, otporan na unakrsna ispitivanja, sa dokaznim dokumentima, kopijama, usklađen sa nacionalnim zakonom.
  - **Autentičan**: može eksplicitno povezati fajlove, podatke sa specifičnim licem i događajem (kroz AC, logovanje, kontrolu log fajlova, kriptozaštićenu autentifikaciju.
  - **Tačan**: pouzdani kompjuterski procesi za sadržaj podataka, da možemo objasniti kako se dogodio incident, šta su ulazi u incidentu, šta su interni procesi, šta su kontrole.
  - **Kompletan**: ispričati sa svojim rečima celu priču o posebnim okolnostima.
  - **Ubedljiv za pravosudne organe**: da ima dokaznu vrednost, objektivan, praktičan test prezentacije.
- **Kompjuterski dokaz**: razlikuje od drugih sudskih dokaza, može se promeniti svakog trenutka u kompjuteru i na prenosnom putu i to bez traga, može se promeniti u toku skupljanja dokaza, neposredni kompjuterski dokaz ne može čovek direktno čitati niti koristiti, mnogi dokazi za prikaz su odštampani primarni elektronski dokazi, kompjuter stvara i registruje dokaze, stopa promene tehnologije, kompjuter stvara mnoge prilike, ali i pretnje-mnogoviše komercijalnih transakcija registruje, mnogo je lakše pratiti istoriju aktivnosti lica, pomaže u metodama istrage.
- **Istorija kompjuterskog dokaza**: *mainframes, PC, LAN, Inte*rnet.
- **Mainframes**: kontrolabilni printinzi, rani problem prihvatljivosti, kako testirati pouzdanost dokaza.

- **PC**: može li biti zaplenjen za analizu, disk se može «imidžoivatii», a zatim analizirati kao «stvaran» dokaz; možemo li verovati «imidžu» diska, kakav je kvalitet interfejsa?
- **LAN**: suviše kompleksan za zaplenu i laboratorijsku analizu; kako obezbeđujemo kompletnost, kako obezbeđujemo pouzdanost?
- **Internet**: možemo zapleniti individualni PC, možemo se osloniti na dokaz sa udaljenog računara, sa forenzičkog raćunara istražitelja i dobijen intercepcijom podataka na prenosnom putu.

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

PRILOG II

POZNATIJI BEZBEDNOSNI IDENTIFIKATORI (SID) U WINDOWS OPERATIVNIM SISTEMIMA

Bezbednosni identifikator (SID) je jedinstvena vrednost promenljive dužine koja se koristi da identifikuje bezbednosnog principala ili grupe u Windows operativnim sistemima. Poznatiji SID su grupa SID identifikatora koji identifikuju generičke korisnike ili grupe. Njihova vrednost ostaje konstantna kroz ceo operativni sistem. Ova informacija je korisna za forenzičara koji ispituje bezbednosni događaj. Takođe je koristan za potencijalno prikazivanje problema koji se mogu videti u AQCL editoru. Neki SID se može prikazati u ACL editoru umesto u imenu korisnika ili grupe.

Tabela P2.1 Poznatiji SID identifikatori

SID	IME	OPIS
S-1-0	Null Authority	An identifier authority
S-1-0-0	Nobody	No security principal
S-1-1	World Authority	An identifier authority
S-1-1-0	Everyone	A group that includes all users, even anonymous users and guests. Membership is controlled by the operating system.
S-1-2	Local Authority	Note By default, the Everyone group no longer includes anonymous users on a computer that is running Windows XP Service Pack 2 (SP2).
S-1-3	Creator Authority	An identifier authority
S-1-3-0	Creator Owner	An identifier authority.
S-1-3-1	Creator Group	A placeholder in an inheritable access control entry (ACE). When the ACE is inherited, the system replaces this SID with the SID for the object's creator.
S-1-3-2	Creator Owner Server	A placeholder in an inheritable ACE. When the ACE is inherited, the system replaces this SID with the SID for the primary group of the object's creator. The primary group is used only by the POSIX subsystem.
S-1-3-3	Creator Group Server	This SID is not used in Windows 2000.
S-1-4	Non-unique Authority	This SID is not used in Windows 2000.
S-1-5	NT Authority	An identifier authority.
S-1-5-1	Dialup	An identifier authority.

SID	IME	OPIS
S-1-5-2	Network	A group that includes all users who have logged on through a dial-up connection. Membership is controlled by the operating system.
S-1-5-3	Batch	A group that includes all users that have logged on through a network connection. Membership is controlled by the operating system.
S-1-5-4	Interactive	A group that includes all users that have logged on through a batch queue facility. Membership is controlled by the operating system.
S-1-5-5-X-Y	Logon Session	A group that includes all users that have logged on interactively. Membership is controlled by the operating system.
S-1-5-6	Service	A logon session. The X and Y values for these SIDs are different for each session.
S-1-5-7	Anonymous	A group that includes all security principals that have logged on as a service. Membership is controlled by the operating system.
S-1-5-8	Proxy	Description: A group that includes all users that have logged on anonymously. Membership is controlled by the operating system.
S-1-5-9	Enterprise Domain Controllers	This SID is not used in Windows 2000.
S-1-5-10	Principal Self	A group that includes all domain controllers in a forest that uses an Active Directory directory service. Membership is controlled by the operating system.
S-1-5-11	Authenticated Users	A placeholder in an inheritable ACE on an account object or group object in Active Directory. When the ACE is inherited, the system replaces this SID with the SID for the security principal who holds the account.
S-1-5-12	Restricted Code	A group that includes all users whose identities were authenticated when they logged on. Membership is controlled by the operating system.
S-1-5-13	Terminal Server Users	This SID is reserved for future use.
S-1-5-18	Local System	A group that includes all users that have logged on to a Terminal Services
S-1-5-19	NT Authority	A service account that is used by the operating system
S-1-5-20	NT Authority	Local Service
S - 1 - 5 - d o - main-500	Administrator	Network Service
: S-1-5-do-main-501	Guest	A user account for the system administrator. By default, it is the only user account that is given full control over the syste

SID	IME	OPIS
S-1-5-domain-502	KRBTGT	A user account for people who do not have individual accounts. This user account does not require a password. By default, the Guest account is disabled.
S-1-5-domain-512	Domain Admins	A service account that is used by the Key Distribution Center (KDC) service.
S-1-5-domain-513	Domain Users	A global group whose members are authorized to administer the domain. By default, the Domain Admins group is a member of the Administrators group on all computers that have joined a domain, including the domain controllers. Domain Admins is the default owner of any object that is created by any member of the group.
S-1-5-domain-514	Domain Guests	A global group that, by default, includes all user accounts in a domain. When you create a user account in a domain, it is added to this group by default.
S-1-5-domain-515	Domain Computers	A global group that, by default, has only one member, the domain's built-in Guest account.
S-1-5-domain- 516	Domain Controllers	A global group that includes all clients and servers that have joined the domain.
S-1-5-domain-517	Cert Publishers	A global group that includes all domain controllers in the domain. New domain controllers are added to this group by default.
S-1-5-root domain-518	Schema Admins	A global group that includes all computers that are running an enterprise certification authority. Cert Publishers are authorized to publish certificates for User objects in Active Directory.
S-1-5-root domain-519	Enterprise Admins	A universal group in a native-mode domain; a global group in a mixed-mode domain. The group is authorized to make schema changes in Active Directory. By default, the only member of the group is the Administrator account for the forest root domain.
S-1-5-domain-520	Group Policy Creator Owners	A universal group in a native-mode domain; a global group in a mixed-mode domain. The group is authorized to make forest-wide changes in Active Directory, such as adding child domains. By default, the only member of the group is the Administrator account for the forest root domain.
S-1-5-domain-533	RAS and IAS Servers	A global group that is authorized to create new Group Policy objects in Active Directory. By default, the only member of the group is Administrator.
S-1-5-32-544	Administrators	A domain local group. By default, this group has no members. Servers in this group have Read Account Restrictions and Read Logon Information access to User objects in the Active Directory domain local group. By default, this group has no members. Servers in this group have Read Account Restrictions and Read Logon Information access to User objects in Active Directory.

SID	IME	OPIS
S-1-5-32-545	Users	A built-in group. After the initial installation of the operating system, the only member of the group is the Administrator account. When a computer joins a domain, the Domain Admins group is added to the Administrators group. When a server becomes a domain controller, the Enterprise Admins group also is added to the Administrators group.
S-1-5-32-546	Guests	A built-in group. After the initial installation of the operating system, the only member is the Authenticated Users group. When a computer joins a domain, the Domain Users group is added to the Users group on the computer.
S-1-5-32-547	Power Users	A built-in group. By default, the only member is the Guest account. The Guests group allows occasional or one-time users to log on with limited privileges to a computer's built-in Guest account.
S-1-5-32-548	Account Operators	A built-in group. By default, the group has no members. Power users can create local users and groups; modify and delete accounts that they have created; and remove users from the Power Users, Users, and Guests groups. Power users also can install programs; create, manage, and delete local printers; and create and delete file shares.
S-1-5-32-549	Server Operators	A built-in group that exists only on domain controllers. By default, the group has no members. By default, Account Operators have permission to create, modify, and delete accounts for users, groups, and computers in all containers and organizational units of Active Directory except the Builtin container and the Domain Controllers OU. Account Operators do not have permission to modify the Administrators and Domain Admins groups, nor do they have permission to modify the accounts for members of those groups.
S-1-5-32-550	Print Operators	A built-in group that exists only on domain controllers. By default, the group has no members. Server Operators can log on to a server interactively; create and delete network shares; start and stop services; back up and restore files; format the hard disk of the computer; and shut down the computer.
S-1-5-32-551	Backup Operators	A built-in group that exists only on domain controllers. By default, the only member is the Domain Users group. Print Operators can manage printers and document queues.
S-1-5-32-552	Replicators	A built-in group. By default, the group has no members. Backup Operators can back up and restore all files on a computer, regardless of the permissions that protect those files. Backup Operators also can log on to the computer and shut it down.
The following groups will show as SIDs until a Windows Server 2003 domain controller is made the primary domain controller (PDC) operations master role holder. (The "operations master" is also known as flexible single master operations or FSMO.) Additional new built-in groups that are created when a Windows Server 2003 domain controller is added to the domain are		

SID	IME	OPIS
S-1-5-32-554	BUILTIN\Pre-Windows 2000 Compatible Access	An alias added by Windows 2000. A backward compatibility group which allows read access on all users and groups in the domain.
S-1-5-32-555	BUILTIN\Remote Desktop Users	An alias. Members in this group are granted the right to logon remotely.
S-1-5-32-556	BUILTIN\Network Configuration Operators	An alias. Members in this group can have some administrative privileges to manage configuration of networking features.
S-1-5-32-557	BUILTIN\Incoming Forest Trust Builders	An alias. Members of this group can create incoming, one-way trusts to this forest.
S-1-5-32-557	BUILTIN\Incoming Forest Trust Builders	An alias. Members of this group can create incoming, one-way trusts to this forest.
S-1-5-32-558	BUILTIN\Performance Monitor Users	An alias. Members of this group have remote access to monitor this computer.
S-1-5-32-559	BUILTIN\Performance Log Users	An alias. Members of this group have remote access to schedule logging of performance counters on this computer.
S-1-5-32-560	BUILTIN\Windows Authorization Access Group	An alias. Members of this group have access to the computed tokenGroupsGlobalAndUniversal attribute on User objects.
S-1-5-32-561	BUILTIN\Terminal Server License Servers	An alias. A group for Terminal Server License Servers. When Windows Server 2003 Service Pack 1 is installed, a new local group is created.
S-1-5-32-562	BUILTIN\Distributed COM Users	Description: An alias. A group for COM to provide computerwide access controls that govern access to all call, activation, or launch requests on the computer.

Primenjivo za:

- Microsoft Windows Server 2003, Standard Edition (32-bit x86)
- Microsoft Windows Server 2003, Enterprise Edition (32-bit x86)
- Microsoft Windows Server 2003, Datacenter Edition (32-bit x86)
- Microsoft Windows XP Professional
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows 2000 Professional Edition

Odlukom Senata Univerziteta "Singidunum", Beograd, broj 636/08 od 12.06.2008, ovaj udžbenik je odobren kao osnovno nastavno sredstvo na studijskim programima koji se realizuju na integrisanim studijama Univerziteta "Singidunum".

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд