UNIVERZITET SINGIDUNUM



Milan Milosavljević
Gojko Grubor

DIGITALNA FORENZIKA RAČUNARSKOG SISTEMA

BEOGRAD, 2009.

UNIVERZITET SINGIDUNUM

DIGITALNA FORENZIKA RAČUNARSKOG SISTEMA

Udžbenik

Milosavljević Milan, Gojko Grubor

BEOGRAD 2009

DIGITALNA FORENZIKA

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

Tehnička obrada:
Časlav Maksić
Novak Njeguš

Dizajn korica:
Milan Nikolić

Godina izdanja:
2009.

Tiraž:
300 primeraka

Štampa:
ČUGURA print, Beograd
www.cugura.rs

ISBN: 978-86-7912--171-4

SADRŽAJ

SADRŽAJ i
SPISAK SLIKA 4
SPISAK TABELA 8
DIGITALNA FORENZIKA RAČUNARSKOG SISTEMA 9
UVOD 10
1 ISKLJUČIVANJE RAČUNARA 13
1.1 Kratak pregled istrage i akvizicije digitalnih podataka 2
1.2 Isključivanje računara sa Windows OS 16
REZIME 22
PITANJA ZA PONAVLJANJE 24
2 INTERPRETACIJA RAČUNARSKIH PODATAKA 25
2.1 Digitalni zapisi 25
2.2 Mali i veliki kraj prvi u redosledu bajta 29
REZIME 32
3 FIZIČKE KARAKTERISTIKE KOMPJUTERSKIH MEDIJA 34
3.1 Fizičke karakteristike disketa i čvrstih diskova računara 34
3.2 Proračun veličine čvrstog diska 41
3.3 BIOS i ograničenja proizvođača čvrstih diskova 41
REZIME 44
PITANJA ZA PONAVLJANJE 46
4 TEHNOLOGIJA CD, DVD I FLEŠ MEMORIJA 47
4.1 Tehnologija kompakt diskova 47
4.1.1 Fajl sistem kompakt diskova 49
4.2 DVD tehnologije 50
4.3 Fleš memorije 56
REZIME 61
PITANJA ZA PONAVLJANJE 64
5 HARDVERSKE KOMPONENTE RAČUNARA 65
REZIME 80
PITANJA ZA PONAVLJANJA 83
6 PROCES PODIZANJA OS RAČUNARA 84
6.1 BIOS sistem 84
6.2 POST funkcije 85
6.3 Funkcije komplementarnog metal-oksidnog poluprovodnika (CMOS) 85
6.4 Proces butovanja 86
6.4.1 Sekvenca butovanja Windows NT operativnog sistema 88
6.4.1.1 Koraci procesa butovanja 90
6.4.2 Sekvenca butovanja DOS sistema 92
REZIME 96
PITANJA ZA PONAVLJANJE 98
7 DIGITALNA FORENZIČKA ANALIZA RAČUNARA 99
7.1 Priprema za forenzičku analizu računara 99

REZIME 104
PITANJA ZA PONAVLJANJE 106
8 GEOMETRIJA DISKA 107
8.1 Deljenje diska na particije 107
8.1.1 Glavna particiona tabela (MPT) 110
8.1.2 Primeri analize MPT za različite particije diska 113
8.1.3 Nealocirani prostor diska 116
8.2 Formatiranje diska 117
8.2.1 Formatiranje diska sa FAT16 fajl sistemom 117
8.2.2 Formatiranje diska sa FAT32 fajl sistemom 119
8.2.3 Forenzičke implikacije formatiranja diska 121
8.2.4 Formatiranje logičke particije sa NTFS fajl sistemom 122
8.3 Označavanje diskova računara 123
8.3.1 Primeri označavanja diskova računara 126
8.3.2 Dugačka imena fajlova 131
REZIME 134
PITANJA ZA PONAVLJANJA 137
9 OPERATIVNI SISTEMI 140
9.1 Pregled UNIX/Linux operativnih sistema 146
9.2 Koncept korisnika i registri u operativnom sistemu 152
REZIME 164
PITANJA ZA PONAVLJANJE 168
10 FORENZIČKA ANALIZA FAJL SISTEMA 169
10.1 Struktura i tipovi FAT fajl sistema 169
10.1.1 Klasteri 171
10.1.1.1 Fragmentacija i defragmentacija klastera fajlova u FAT fajl sistemu 175
10.1.1.2 Analiza izbrisanih fajlova u FAT fajl sistemu 178
10.2 Analiza NTFS fajl sistema 182
10.2.1 Analiza MFT ulaza NTFS fajl sistema 188
10.2.2 Analiza MFT atributa NTFS fajl sistema 190
10.2.3 Analiza MFT *slack* prostora 193
10.3 Analiza kompresovanih podataka 194
10.4 Analiza šifrovanih informacija 195
10.5 Oporavak izbrisanog fajla u NTFS fajl sistemu 196
10.5.1 Konfigurisanje *Recycle Bin*-a 203
REZIME 205
PITANJA ZA PONAVLJANJE 210
11 PRIVREMENI I DRUGI FORENZIČKI RELVANTNI FAJLOVI 213
11.1 Privremeni fajlovi 213
11.2 Log fajlovi 215
11.3 Print Spooler fajlovi 216
11.4 Fajlovi linkova 217
11.5 Tipovi i potpisi fajlova 218
11.6 Potpisi fajlova 221
11.7 Forenzička analiza tragova korišćenja Interneta 224
11.7.1 Privremeni Internet fajlovi 225
11.7.2 Istorija aktivnosti na Internetu 227

11.8 Kolačići (*Cookies*) 229
11.9 Favorizovane lokacije 231
11.10 Direktno umrežavanje (*peer-to-peer*) 232
11.11 Ostali transferi fajlova 233
11.12 Tragovi E-mail poruka 234
11.13 Servisi za četovanje preko Interneta 237
11.13.1 Servis novinske grupe 238
11.13.2 AOL servis 238
11.14 Analiza izvršnih fajlova, *rutkitova*, *zadnjih vrata* i *snifera* 239
REZIME 246
PITANJA ZA PONAVLJANJE 250
12 DATUM I VREME U FORENZIČKOJ ANALIZI RAČUNARSKOG SISTEMA 252
12.1 Formati datuma i vremena u računarskim sistemima 252
12.2 Datum i vreme kao digitalni dokaz 254
12.2.1 Datum i vreme u Windows operativnom sistemu 255
12.2.2 Datum i vreme u Microsoft Internet Explorer (IE) 259
12.3 Kontrolna lista za dokaze o datumu/vremenu 259
12.4 Forenzički aspekt informacija o vremenu i datumu 260
REZIME 264
PITANJA ZA PONAVLJANJE 265
13 ANTI-FORENZIČKE AKTIVNOSTI I ALATI 266
REZIME 271
PITANJA ZA PONAVLJANJE 272
KLJUČNI TERMINI 273
LITERATURA 280
PRILOG I 283
PRILOG II 287
PRILOG III 289

SPISAK SLIKA

Slika 2.1 *Primer transformacije slova A iz ASCI kôda u binarni bajt* 25
Slika 2.2 *Deo ulaza MFT tabele za fajl memorisan u UNICODE-u* 26
Slika 2.3 *Pretvaranje binarnog koda u decimalni (ASCI slovo A)* 26
Slika 2.4 *Težinski faktori (a) i model (b) za pretvaranje binarnog zapisa u decimalni* 27
Slika 2.5 *Sve vrednosti hex zapisa* 27
Slika 2.6 *Primer konverzije binarnog u decimalni broj* 28
Slika 2.7 *Podela binarnog bajta na 2 nibla (a) i pondrisanje (b)* 28
Slika 2.8 *Podela bajta na 2 nibla (a) i pondrisanje (b)* 28
Slika 2.9 *Binarna reprezentacija decimalnog broja 83* 29
Slika 2.10 *Konverzija dva bajta u redosledu Mali kraj prvi (a) u decimalni broj (b)* 30
Slika 2.11 *Konverzija dva bajta u redosledu Veliki kraj prvi u decimalni broj* 30
Slika 3.1 *Flopi disk od 5 1/4 inča* 34
Slika 3.2 *Flopi disk od 3 1/4 inča* 35
Slika 3.3 *Dvostrano upisivanje na FD 1.44 MB* 36
Slika 3.4 *Fizičke karakteristike HD* 37
Slika 3.5 *HD sa dva diska i 4 glave za pisanje/brisanje* 37
Slika 3.6 *Upisivanje tragova (a), cilindri sa 3 traga (b), brojanje glava (c) i sektori (d) HD* 38
Slika 3.7 *Struktura sektora* 38
Slika 3.8 *Lokacija CHS 011- sektora 1, glave 1 cilindra 0* 39
Slika 3.9 *Primer oznake CHS na fizičkom HD* 39
Slika 3.10 *ZBR – Snimanje bita po zonama* 40
Slika 3.11 *Primer oznake CHS vrednosti od 8,2GB na HD od 82,3GB* 42
Slika 4.1 *Upisivanje podataka na CD* 47
Slika 4.2 *Presek strukture fabrički presovanih diskova* 48
Slika 4.3 *Kompakt disk za jednokratno -CD-R (a) i za višestruko snimanje (b)* 48
Slika 4.4 *Pod-formati DVD diskova* 50
Slika 4.5 *Pakovanje binarnih nosioca na CD i DVD disku* 51
Slika 4.6 *Struktura DVD diskova različitih kapaciteta* 51
Slika 4.7 *Tip informacija o CD dobijen softverskim alatom* 52
Slika 4.8 *Informacije o logičkoj particiji diska* 53
Slika 4.9 *Dijagnostičke informacije sa CD-R diska* 53
Slika 4.10 *Sadržaj fajla upisanog sa EasyCD Creator V.5 rezačem* 54
Slika 4.11 *Opcije vremena u rezaču EasyCD Creator* 54
Slika 4.12 *Različito očitavanje istog CD na različitim drajvovima* 55
Slika 4.13 *Struktura fajlova DVD* 55
Slika 4.14 *Tipovi kompakt fleš memorija* 57
Slika 4.15 *Iomega smart media i tipovi multi-media fleš memorija (a, b)* 57
Slika 4.16 *Bezbedna digitalna kartica (a) i xD-Picture kartica (b)* 58
Slika 4.17 *Tipovi memorijskih stikova* 58
Slika 4.18 *Sandisk T-fleš kartice (a) i DOM tipovi fleš memorije (b)* 59
Slika 4.19 *Tipovi Iomega Peerless USB fleš memorija (a) i tipovi PQI inteligentnih USB stikova (b)* 59

Slika 4.20 *Data play optički disk (a) i tpovi predmeta sa ugrađenom fleš memorijom (b)* 60
Slika 5.1 *PSU – jedinca za napajanje računara*.....65
Slika 5.2 *Antistatička oprema forenzičke laboratorije* 66
Slika 5.3. Tipična ATX glavna ploča 67
Slika 5.4 *Najčešći tipovi RAM memorija*.....68
Slika 5.5 *Tipovi CPU*.....69
Slika 5.6 *Grafička karta na glavnoj ploči (a) i PCI grafički adapter (b)* 70
Slika 5.7 *Neki tipovi tastatura: ergonomska, jednoručna standardna i holografska* 71
Slika 5.8 *Vrste portova (a) i tipovi standarda USB (b)* 72
Slika 5.9 *ULTRA ATA trakasti kabl (a) i SATA interfejs (b) i SCSI interfejs (c)* 75
Slika 5.10 *Mrežna kartica sa mrežnim konektorom RJ45*.....78
Slika 6.1 *BIOS ROM čip tipa* ***Amibios***.....84
Slika 6.2 *Primer CPU provere grafičke kartice u procesu butovanja* 87
Slika 6.3 *Ctrl-Alt-Del ekran dobrodošlice u Windows XP Home OS* 91
Slika 6.4 *Opcije setovanja MSN Messenger* 94
Slika 6.5 *Start-up meni za sve korisnike i jednog korisnika* 94
Slika 7.1 *Ilustracija promene heša sa promenom jednog bita informacije*.....103
Slika 8.1 *Dvo-dimenzionalni model fizičkog HD* 107
Slika 8.2 *MBR u hex zapisu tipičnog forenzičkog alata za analizu fajl sistema* 109
Slika 8.3 *Glavna particiona tabela (a) i interpretacija 16 bajtova prvog* ***entrija*** *MPT tabele (b)* 111
Slika 8.4 *MPT diska sa jednom particijom*.....113
Slika 8.5 *Informacije o MPT diska sa jednom particijom u* ***BIGDOS*** *DiskEditor alatu*.....113
Slika 8.6 *MPT u forenzičkom alatu* ***Nhorton Disk Editor***.....114
Slika 8.7 *MPT diska sa primarnom i proširenom particijom*.....114
Slika 8.8 *Položaj primarne i proširene particije sa tri logička diska (a)* 115
Slika 8.9 *Nekorišćeni prostor diska (a) i sumnjivo preoblikovanje particije diska (b)* 116
Slika 8.10 *Proces formatiranja za FAT16 i FAT32 fajl sisteme*.....117
Slika 8.11 *Formatiranje FAT 16 fajl sistema*.....118
Slika 8.12 *FAT tabela sa klasterima podataka u FAT 16 fajl sistemu* 119
Slika 8.13 *Formatiranje FAT 32 fajl sistema*.....120
Slika 8.14 *Razlike FAT 16 i FAT 32 fajl sistema*.....121
Slika 8.15 *Formatiranje NTFS fajl sistema*.....122
Slika 8.16 ***My Recent Document*** *u Windows OS*.....124
Slika 8.17 *Pravila označavanja particija na jednom HD* 126
Slika 8.18 Označavanje particija na jednom HD sa tri particije i dva fajl sistema.....127
Slika 8.19 Označavanje particija na jednom HD sa 3 particije i sa CD ROM i ZIP particijma 127
Slika 8.20 Označavanje particija na dva HD sa ZIP i CD ROM particijama 128
Slika 8.21 *Označavanje particija u slučaju skidanja i ponovnog dodavanja drugog diska* 129
Slika 8.22 *Prozor* ***Disk Management*** *za upravljanje particijama u Windows XP OS* 130
Slika 8.23 *Trag particije u ključu Regitra otkriven* ***Registry Editor****-om Win XP OS*.....130
Slika 8.24 *Trag imena particije u MBR* 131
Slika 9.1 *Grafički model funkcija operativnog sistema*.....140
Slika 9.2 Prozor DOS operativnog sistema 142
Slika 9.3 *Prozori Windows 3.1 i 3.11 OS*.....143
Slika 9.4 *Prozor* ***Program Manager*** *Windows NT 4 OS (a) i desktop Windows 95 OS (b)* 143
Slika 9.5 *Desktop otvorenog Windows ME OS (a) i Windows XP OS (b)*.....145

Slika 9.6 Istorija razvoja MS OS 146
Slika 9.7 *Manje poznate verzije Microsoft OS* 146
Slika 9.8 *Prozori Linux OS* 147
Slika 9.9 *Tipičan prozor Macintosh OS* 152
Slika 9.10 *Podešavanje korisničkog profila u Windows XP OS* 153
Slika 9.11 *Normalna konfiguracija profila novog korisnika u Windows XP OS (a) i prozor My Documments u Windows 9x OS (b)* 156
Slika 9.12 Prozor Registry Edit u Windows XP OS 158
Slika 9.13 *Informacije u Registry Editor-u o akcijama u Internet Explorer-u* 162
Slika 9.14 *Informacije u Registry Editor-u o akcijama u Media Player-u* 162
Slika 9.15 *Informacije o korisničkim imenima i pasvordima za web lokacije posećene u Internet Exploreru* 163
Slika 9.16 *Detalji o verziji Windows-a instaliranog na računaru* 163
Slika 10.1 Ulaz direktorijuma za tekst fajl od 600 bajta (forenzički alat X Way) 172
Slika 10.2 Prikaz tekst fajla od 600 bajta u OS 173
Slika 10.3 Slobodan prostor RAM (Ram Slack)-(a) i fajla (File Slack)-(b) 173
Slika 10.4 Kreiranje novog foldera u rut direktorijumu Windows (a) i DOS (b) OS 174
Slika 10.5 Ulaz novog foldera u rut direktorijumu u forenzičkom alatu 175
Slika 10.6 Fragmentirani i nefragmentirani klasteri 5 aktivnih fajlova na disku 176
Slika 10.7 Početak defragmentacije fajlova 1 i 2 od 5 fragmentisanih fajlova 178
Slika 10.8 Kraj defragmentacije 5 fajlova 178
Slika 10.9 FAT tabela sa 20 klastera i praznim direktorijumom sa 2 ulaza 179
Slika 10.10 Ažuriranje FAT tabele i ulaza direktorijuma za 2 memorisana fajla 180
Slika 10.11 Ažurirane promene u FAT tabeli i direktorijumu ulaza posle brisanja fajla 180
Slika 10.12 Metod oporavka klastera izbrisanog fajla 181
Slika 10.13 Ažuriranje ulaza oporavljenog izbrisanog fajla u direktorijumu ulaza 181
Slika 10.14 FAT tabela i direktorijum ulaza za dva izbrisana fajla 181
Slika 10.15 FAT tabela dva oporavljena fajla 182
Slika 10.16 Kašnjenje upisivanja podataka u RAM i trajnu memoriju 183
Slika 10.17 Optimizacija performansi USB u NTFS fajl sistema 184
Slika 10.18 Logovanje transakcija u **$Logfile** NTFS fajl sistema 185
Slika 10.19 Struktura MFT tabele u NTFS fajl sistemu 188
Slika 10.20 Identifikatori tipičnih atributa hedera u MFT NTFS fajl sistema 189
Slika 10.21 MFT heder i atributi u Windows XP OS 189
Slika 10.22 Atribut **$STANDARD_INFORMATION** u hex zapisu forenzičkog alata 190
Slika 10.23 Značenje kodiranih **flags** DOS atributa u hex zapisu 191
Slika 10.24 Atribut **$FILE_NAME** u hex zapisu forenzičkog alata 191
Slika 10.25 ASCI zapis imena fajla 192
Slika 10.26 Atribut **$DATA** u hex (a) i ASCII (b) zapisu 192
Slika 10.27 Veličine atributa prema veličini MFT ulaza u NTFS fajl sistemu 192
Slika 10.28 MFT atributi i MFT slack prostor 193
Slika 10.29 **Run** lista atributa za skladištenje lokacije i dužine podataka 194
Slika 10.30 Kompresija fajla u NTFS fajl sistemu 195
Slika 10.31 Fizički disk sa 4 logičke particije i 4 korpe za reciklažu u Windows XP OS 199
Slika 10.32 Korisnički SID za dva korisnika 200
Slika 10.33 Izgled **INFO2** fajla u forenzičkom alatu kada u Recycle Bin-u nema fajlova 201
Slika 10.34 Prenos 3 fajla drug&drop funkcijom u Recycle Bin 201

Slika 10.35 Izgled tri izbrisana fajla iz različitih logičkih particija u folderima RECYCLER 202
Slika 11.1 Interpretacija privremenih fajlova ~wrlxxxx.tmp u forenzičkom alatu 215
Slika 11.2 Instalacioni log fajl AOL klijenta 216
Slika 11.3 Primer **.LNK** fajla u forenzičkom alatu 218
Slika 11.4 Uobičajen potpis MS Office fajlova 222
Slika 11.5 Tačan Windows prikaz potpisa fajlova 222
Slika 11.6 Pogrešan Windows prikaz potpisa fajlova 223
Slika 11.7 Prikaz **.jpeg** slika sa **.doc** ekstenzijom u hex editoru 223
Slika 11.8 Korisničko podešavanje Internet keša na 0MB 226
Slika 11.9 Struktura Internet keš fajlova u **Content.IE5** folderu 227
Slika 11.10 Struktura foldera Internet History u Windows XP mašini 228
Slika 11.11 Struktura foldera Internet History u forenzičkom alatu 228
Slika 11.12 Opciju za korisničko podešavnje Internet History 229
Slika 11.13 Kolačići kao forenzički indikator Internet aktivnosti 230
Slika 11.14 Primer podataka koji se mogu nalaziti u kolačićima 231
Slika 11.15 Heder e-pošte 235
Slika 12.1 Datumi i vremena modifikacije u Windows Explorer-u 256
Slika 12.2 Pogled na sve glavne datume u Windows Explorer-u 256
Slika 12.3 Datum kreiranja foldera u prozoru **Properties** 257
Slika 12.4 Datumi kreiranja modifikovanja i pristupa u prozoru Properties 257
Slika 12.5 Prozor zbirne informacije o Word dokumentu u **Ilook** forenzičkom alatu 258
Slika 12.6 Prozori za podešavanje datuma, vremena i vremenske zone 261
Slika 12.7 Vremena kreiranja modifikacije i pristupa u prozoru Properties tekst fajla 262
Slika 12.8 Datumi i vremena fajla pomerenog drag&drop operacijom na istoj (a) i drugoj (b) particiji 262
Slika 12.9 Datumi i vremena fajla pomerenog copy/paste operacijom 263

SPISAK TABELA

Tabela 4.1 Različiti kapaciteti dva formata DVD diskova 56
Tabela 6.1 Faze, fajlovi i boot rutine Windows NT OS 88
Tabela 6.2 Ključni fajlovi i lokacije za butovanje 89
Tabela 6.3 Procesi i fajlovi DOS sekvence butovanja 92
Tabela 6.4 Uporedni prikaz različitih procesa butovanja 93
Tabela 8.1 Lista značajnijih kôdova tipova particija 112
Tabela 8.2 Uporedna tabela Windows OS i fajl sistema koje podržavaju 125
Tabela 8.3 Konverzija LFN/SFN imena fajla 133
Tabela 9.1 Komparativne prednosti i nedostaci Linux prema Windows OS 148
Tabela 9.2 Komparacija DOS i Linux komandi 148
Tabela 9.3 Uobičajena DOS/Windows i Linux imena fizičkih diskova 149
Tabela 9.4 Uobičajena imena fizičkih diskova u Linux OS 150
Tabela 9.5 Uobičajena imena Linux logičkih particija 150
Tabela 9.6 Podrazumevane lokacije za kreiranje profila za različite Windows OS 153
Tabela 10.1 Broj sektora po klasteru FAT 16 i FAT 32 fajl sistema 172
Tabela 10.2 Metadata sistemski fajlovi u NTFS fajl sistemu 186
Tabela 11.1 Uobičajeni tipovi fajlova i ekstenzija 219
Tabela 11.2 Uobičajeni tipovi grafičkih (a) i video (b) fajlova 220
Tabela 11.3 Ekstenzije uobičajenih šifrovanih fajlova 220
Tabela 11.4 Uobičajeni potpisi fajlova 224
Tabela 11.5 Zastavice (*flags*) koje se koriste u Unix/Linux komandnim linijama 241
Tabela 2.2 Trojan portovi 289
Tabela 2.3 Izvori za obuku iz digitalne forenzike 299
Tabela 2.4 Dodatna tehnička dokumentacija za obuku iz digitalne forenzike 299

DIGITALNA FORENZIKA RAČUNARSKOG SISTEMA

Cilj ovog udžbenika je da studenti nauče osnovne principe i zahteve digitalne forenzičke analize računarskog sistema. Razumevanjem prirode digitalnog zapisa, apstraktnih slojeva računara, funkcionalnosti hardvera i tehnologije primarnih i sekundarnih memorijskih medija računara, kao i forenzičkog značaja poznavanja registara, privremenih fajlova, datuma i vremena, zatim strukture fajl sistema i korisniku nepristupačnih mesta za skladištenje kompjuterski generisanih podataka (fajl slack i nealocirani prostor klastera), ali i problema primene antiforenzičkih aktivnosti i alata, studenti se osposobljavaju za samostalan oporavak skrivenih podataka u ispitivanom računaru primenom forenzičkih tehnika i alata.

UVOD

Ovaj udžbenik je namenjen studentima redovnih i master studija na studijskim programima sa težištem na zaštitu informacija i informaciono komunikacionih sistema. *Digitalna forenzička nauka* ili *digitalna forenzika,* relativno nova naučna disciplina (uspostavljena 1999. godine) obezbeđuje jedini pouzdani *alat* za istragu kompjuterskog kriminala, akviziciju i analizu digitalnih podataka i pripremu i prezentaciju digitalnih dokaza pred sudom. Metodološke i tehnološke osnove digitalne forenzike date su u uđžbeniku *Digitalna forenzička istraga kompjuterskog kriminala – metodološko tehnološke osnove*. U ovom udžbeniku težišno su opisane osnovne specifičnosti digitalne forenzičke analize računarskog sistema. Za potrebe vežbi, istraživanja i eksperimentalnih ispitivanja forenzičih alata, uz ovaj udžbenik je izrađen *Praktikum za digitalnu forenzičku analizu računarskog sistema*.

Digitalna forenzika uključuje otkrivanje (*pretraga, istraga*) i sakupljanje (*akviziciju*), čuvanje (*upravljanje*), dokazivanje (*analizu*) i ekspertsko svedočenje/veštačenje (*prezentaciju*) digitalnih dokaza pred sudom, u slučajevima zloupotrebe IKT sistema i upravljanja kompjuterskim incidentom, kompjuterskog kriminala, civilne parnice, ili administrativnih zahteva. Prate je brojni izazovi, uključujući brze promene računarskih i digitalnih uređaja, kao i sve sofistiraniji napadi na računarske sisteme i mreže i rapidni porast zloupotreba IKT sistema i kompjuterskog kriminala.

Najveći deo digitalne forenzike odnosi se na forenziku računarskih sistema, ili *kompjutersku forenziku*, bilo da su računari samostalni ili umreženi. Digitalna forenzika računarskog sistema obuhvata naučno ispitivanje i analizu podataka iz čvrstih diskova - HD (*Hard Drives*), fajl sistema i drugih medija i prostora za skladištenje podataka u računarskom sistemu, tako da se podaci mogu koristiti kao čvrsti i neoborivi dokazi pred sudom, [24], [25].

Digitalna forenzika računarske mreže, uključujući i Internet ili *kibernetička forenzik*a[1], otkriva i sakuplja informacije o tome kako je napadač, ili haker dobio pristup računarskoj mreži i računarskom sistemu. Analiziraju se log fajlovi da se odredi kada se korisnik ulogovao ili poslednji put koristio svoj

[1] *Cyber forensic*

lični identifikator (ID) za logovanje. *Forenzički analitičar digitalnih podataka* ili *digitalni forenzičar* nastoji da odredi kojim URL[2] je korisnik pristupio, kako se ulogovao na računarsku mrežu i sa koje lokacije.

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

Udžbenik je struktuiran modularno u 13 poglavlja sa rezimeom i pitanjima za ponavljanje polse svakog poglavlja. Rečnik ključnih termina i literatura dati su jedinstveno na kraju udžbenika za sva poglavlja.

U prvom poglavlju ukratko su opisani osnovni koraci digitalne forenzičke istrage i akvizicije digitalnih podataka sa fizičkog i digitalnog mesta krivičnog dela kopjuterskog kriminala, sa posebnim osvrtom na forenzički ispravan pristup isključivanju osumnjičenog računara za potrebe uzimanja fizičke slike čvrstog diska (imidža, miror kopije) ili privremenog oduzimanja.

U poglavljima 2. do 6. opisani su forenzički relevantni podaci o digitalnom zapisu i interpretaciji digitalnih podataka na apstraktnim slojevima računarskog sistema, zatim fizičke karakteristike kompjuterskih medija, optičkih diskova (CD, DVD, kompaktne fleš memorija) i hardverskih komponenti računara, kao i forenzički bezbedno podizanje (butovanje) računara sa različitim platformama i fajl sistemima.

U poglavljima 7. do 12. opisani su svi ključni aspekti digitalne forenzičke analize računarskog sistema: priprema za analizu, geometrija fizičkog HD, formatiranje i deljenje fizičkog diska u logičke particije, specifičnosti analize različitih operativnih (Windows, Linux/Unix, Macintosh i dr.) i fajl sistema (FAT 16, FAT 32, NTFS, Ext2/3, OX 2), analiza privremenih i drugih fajlova i datuma i vremena u računarskom sistemu.

[2] *Unified Resource Location*

U 13. poglavlju opisane su tipične antiforenzičke tehnike i alati za uništavanje potencijalnih dokaza o pristupu i aktivnostima u računaru, koje predstavljaju izvestan, ali ne i nerešiv, problem za forenzičare.

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

1 ISKLJUČIVANJE RAČUNARA

1.1 Kratak pregled istrage i akvizicije digitalnih podataka

Sa aspekta digitalne forenzike računarskog sistema, digitalna forenzička istraga može se podeliti u dve osnovne kategorije: *zvanična (javna)* i *korporacijska (privatna)* digitalna forenzička istraga. U svakom slučaju, računar ima glavnu ulogu u većini istraga krivičnih dela, pa je sposobnost analize računara i ekstrakcije relevantnih informacija, obaveštajnih podataka i dokaza od vitalnog značaja za istragu većine krivičnih dela kompjuterskog kriminala, gde računar može biti *kompromitovan* - računar „žrtva", ili *osumnjičen* – računar sa kojeg je napadač izvršion napad, ili *računar posrednik* – računar koji sadrži kompromitujući materijal bez znanja vlasnika ili služi za napad na drugi računarski sistem. Sa aspekta forenzičke analize kompromitovan, osumnjičen ili posredni računar - uvek je *ispitivani* računar. Zavisno od konteksta, osumnjičeni računar može obuhvatati izvorni, napadnuti ili posredni računar, jer je u praksi forenzičke istrage digitalnih dokaza često neophodno izvršiti forenzičku akviziciju i analizu računara sa kojeg je izvršen napad, napadnutog računara i nekog od posrednih računara, na primer, preko čijeg naloga je napadač ušao u sistem.

Dobra je praksa da digitalni forenzičar timski radi sa specijalistom zaštite da obezbede prihvatljivu zaštitu računarskih sistema i bezbedan rad računarske mreže u poslovnim sistemima. Funkcija digitalne forenzičke istrage, čini stabilnu celinu u ranjivom mrežnom okruženju sa implementiranim sistemom zaštite i uspostavljenim kapacitetima za upravljanje kompjuterskim incidentom. Iako sve tri grupe specijalista u velikim sistemima najčešće rade samostalno, u slučaju glavnog kompjuterskog incidenta sve tri grupe uvek rade zajedno. Ovakav *koraborativni* rad obezbeđuje saniranje kompjuterskog incidenta u organizaciji sa sopstvenim resursima i bez pozivanja spoljnih specijalista. Specijalisti za sisteme zaštite, analizu rizika i ranjivosti imaju iskustvo iz administracije sistema i poznaju neku metodologiju za analizu i ublažavanje rizika. Specijalisti za upravljanje kompjuterskim incidentom poznaju automatizovane detektore upada (IDS/IPS), monitorišu logove mrežnih barijera (*firewalls*), otkrivaju, prate, identifikuju i sprečavaju upade u

računarske mreže i u slučaju napada pomažu forenzičarima da rekonstruišu napad i identifikuju napadača. Digitalni forenzičari ispituju napadnute, kompromitovane ili osumnjičene sisteme koji sadrže potencijalne dokaze o kompjuterskom incidentu/kriminalu, dostavljaju nalaze o načinu napada članovima druga dva tima za efektivno fiksiranje otkrivenih ranjivosti sistema. Bliskom saradnjom ovih specijalista, efektivno se sprečava ponavljanje istog ili sličnog incidenta i podiže bezbednost sistema na viši nivo.

Uobičajeno ispitivanje računara i digitalna forenzička analiza počinju sa žalbom ili prijavom kompjuterskog incidenta, ili krivičnog dela, organima korporacijske istrage ili zvaničnim organima istrage. Prijava zvaničnim organima istrage može doći i posle izvršene korporacijske istrage, koja je potvrdila tip kompjuterskog incidenta i neophodnost angažovanja zvaničnih organa istrage. Bez obzira odakle dolazi zahtev za ispitivanje kompromitovanog/osumnjičenog računara (ISP, vlasnik korporacijskog IKT sistema, vlasnik računarskog sistema itd.), svaki podnosilac zahteva očekuje od organa istrage visok nivo znanja bilo da se radi o PDA uređaju, PC računaru, Laptop računaru, ili složenoj računarskoj mreži. U svakom slučaju, očekivanja od eksperata za digitalnu forenziku uvek su vrlo visoka, [24].

Prvi korak po prijemu zahteva i pre prihvatanja računara na ispitivanje i analizu podataka, treba razmotriti da li ima dovoljno informacija za razvoj strategije ispitivanja računara, kao što su identitet osumnjičenog, poznavanje pasvorda za računar ili bilo koji softver, poznavanje vlasnika računara i sl. U svakom slučaju, generalno se može očekivati globalni zahtev tipa „izvucite sve što je na računaru“, pošto većina podnosilaca zahteva, uključujući i policiju nije uvek svesna koliko infrmacija računar može da sadrži.

Po prihvatanju zahteva za forenzičku analizu računara, analitičar treba da razmotri obim zadatka i predvidi mogućnost angažovanja drugih eksperata, što je najčešće slučaj, ako su u pitanju platforme tipa *Linux, Unix, Macintosh* i sl., pošto većina digitalnih forenzičara specijalizuje svoja znanja na Windows platformama. U slučaju prijema više računara na ispitivanje treba razmotriti prioritet ispitivanja i proceniti sa kojeg računara se može izvući najviše dokaza, na primer fajl server gde osumnjičeni skladišti svoje podatke, *mail* server, ako istraga uključuje e-poštu, ili *proksi* server, ako se istraga odnosi na pristupe Internetu.

Sledeći korak je početak ispitivanja računara, ili pravljenje *imidža* na fornzičkom računaru za dalju analizu. Pri tome forenzičar stalno treba da ima

na umu da mora sudu predočiti dokaze o činjenicama koje su stvarno otkrivene u procesu analize. Svaki forenzičar treba da očekuje da bude pozvan da iznese ekspertsko mišljenje pred sudom, ili pak da veštači i razjašnjava određena pitanja u toku trajanja procesa.

Na kraju, digitalni forenzičar mora poznavati brojne forenzičke alate koji obezbeđuju pouzdanu akviziciju i analizu, ne menjaju stanje na originalnom ispitivanom računaru, ne menjaju digitalne podatke, čuvaju integritet podataka/dokaza u lancu istrage i koji obezbeđuju ponovljivost rezultata u slučaju zahteva suda.

Početak same analize računara podrazumeva da je ispred forenzičara privremeno oduzeti računarski sistem sa pratećom periferijom, medijumima i drugim potencijalnim dokazima, prikupljenim u procesu pretrage i privremenog oduzimanja računara, ili *imidž* HD-a osumnjičenog računara, ako nije moguće privremeno oduzeti računar. Forenzičar treba da razmotri brojna pitanja kao što su: koliko se brzo ispitivanje mora izvršiti, šta analiza obuhvata, koliko duboka anliza mora biti, šta analiza mora dokazati, da li je istraga reaktivna ili proaktivna i slično? Forenzičaru, takođe, mora biti jasno ko zvanično vodi istragu i usmerava rad forenzičara - tužilac, inspektor policije, ili menadžer organizacije.

U slučaju ispitivanja računara osumnjičenog forenzičar mora znati šta treba da traži u računaru: slike, dokumenta, šifrovane informacije, ključne reči ili druge informacije? Ove informacije forenzičar mora dobiti od zvaničnog organa koji vodi istragu.

U analizi računara, forenzičar često treba da planira istraživanje nepoznatog softvera koji se može naći na ispitivanom računaru, uključujući i maliciozni softver. Za uspešno ispitivanje računara od presudnog značaja su informacije o pasvordu, koje mogu znatno ubrzati proces analize.

Sledeći korak je bekapovanje radne kopije imidža za potrebe suda i obezbeđivanje zaštite integriteta i čuvanja podataka/dokaza u celom lancu istrage. Forenzičar istražuje digitalne podatke/dokaze na radnom *imidžu* u procesu koji može ličiti na „traženje igle u plastu sena“. Po završetku analize osumnjičenog računara, forenzičar izveštava o rezultatima istrage i priprema se za svedočenje pred sudom.

1.2 Isključivanje računara sa Windows OS

Isključivanje računara je veoma osetljivo pitanje u procesu forenzičke istrage. Metod isključivanja zavisi od operativnih okolnosti i situacije u kojoj se računar nalazi i nema jedinstvenog odgovora kako treba isključivati računar koji radi na određenoj platformi. Jedina sigurna stvar je da se *ni jedan računar u procesu pretrage i privremenog oduzimanja ne uključuje*, što bi bilo protiv svih principa čuvanja digitalnih dokaza. Uključen računar obavlja milione operacija u sekundi i izaziva brojne promene u sistemu, koje potencijalno mogu izazvati izmene dokaza koje je teško objasniti pred sudom. Ceo koncept forenzičke analize računara zasniva se na izgradnji i prezentaciji dokaza koji su pouzdani i činjenički.

Takođe, prvobitna praksa u razvoju digitalne forenzike (1990-tih) da se uvek isključi napajanje ispitivanog računara izvlačenjem kabla za napajanje iz računara, nije uvek najbolja u svetlu razvoja IK tehnologija, pa je potrebno znati kako postupati sa uključenim računarom i koje akcije treba preduzeti, a da su u skladu sa pravilima i uputstvima. U prvom redu treba znati na kojoj platformi računar radi.

Windows OS imaju tri moguća isključivanja sa različitim posledicama za digitalne podatke, [24]:

- normalno isključivanje (shutdown);
- korisnički definisano isključivanje i
- nasilno isključivanje napajanja.

Normalno isključivanje (*shutdown*) briše sve *bafere* (privremena skladišta) i privremene fajlove koje sistem koristi, zatvara sve tekuće procese i upisuje podatke u fajlove gde smatra potrebnim. Sistem u fazi isključivanja ima samo jedan cilj, da memoriše podatke koje korisnik želi da sačuva i one koje sam sistem treba, a ne brine o drugim podacima unutar sistema. Korisnik računara obično obraća pažnju samo na sopstvene podatke, dok forenzičar mora voditi računa o svim podacima u računaru, kao i o podacima koji mogu biti upisani u uključen računar sa udaljene lokacije tokom pretrage i pripreme za privremeno oduzimanje. Računar čuva zapise o vremenu i datumu za brojne procese i fajlove, pa je značajno da forenzičar ima u posedu ispitivani računar što je moguće ranije, da se eventualne promene koje unese forenzički alat/forenzičar, mogu što pre pokazati negde u sistemu. Cilj svakog forenzičara je da unese što manje promena u ispitivani sistem. U slučaju da je

računar koji se privremeno oduzama uključen, treba opservirati ekran, ustanoviti šta se može zajključiti iz tekućih procesa, fotografisati ekran i isključiti napajanje iz računara. Ovo obezbeđuje zaustavljanje računara i sprečava bilo koje neželjeno upisivanje na disk. U ovom slučaju gube se samo informacije iz RAM memorije, koje mogu uključivati tekući rad i informacije o setovanju koje bi kasnije bile upisane na disk i verovatno u registar. Često je za analizu značajno sačuvati podatke iz RAM memorije i ispitati ih. Za ovu operaciju postoje forenzički alati i tehnike žive (realne) forenzičke akvizicije. Međutim, ono što je u RAM memoriji još uvek može biti sačuvano na čvrstom disku u *swap fajlu*.

Windows *swap* fajlovi - fajlovi za brzu razmenu i *privremeni (keš) fajlovi Web pretraživača* kreiraju svi MS Windows OS. *Swap* fajlovi su potencijalni zlatni rudnik za forenzičare. Postoje dva tipa *swap* fajlova: *privremeni* i *permanentni*. Privremeni *swap* fajlovi nestaju kada se zatvara Windows. Permanentni *swap* fajlovi nastavljaju da postoje čak i posle isključivanja Windows OS. Fornzičar treba da ova dva tipa *swap* fajlova tretira na različite načine.

Prvo treba znati da se *swap* fajlovi konstantno menjaju. Ovo su fajlovi koje Windows OS koristi za svašta - od *scratch pads* (keša) do privremene memorije. Kada Windows OS izvršava više istovremenih zadataka on u stvari smešta deo neaktivnog programa u memoriju. Dakle, imamao utisak da nekoliko programa radi istovremeno, što u stvari nije slučaj. Oni se u stvari brzo premeštaju (razmenjuju) napred - nazad u/iz RAM memorije, tako brzo da nastavljaju da rade. U toku vremena kada stvarno ne rade, mali delovi programa nazvani *stub* (pikavci) i dalje ostaju u memoriji, držeći sve zajedno, sve dok se njegov program ponovo ne aktivira. Ako Windows OS nema dovoljno RAM memorijskog prostora za ovo premeštanje (*swapping*) on počinje premeštati fajlove na HD. Dakle, svašta može biti napisano u *swap* fajlu, samo to treba otkriti.

Swap fajlovi su ipak zagonetne. One se menjaju bez upozorenja i nema načina da se na to utiče. Windows OS radi najveći deo vremena ispod površine i izvan direktne kontrole korisnika. To znači on upisuje u *swap* fajl neprekidno, što naravno menja sadržaj tog fajla. Kada korisnik aktivira regularan proces isključivanja Windows OS, neki od procesa isključivanja se upisuje u *swap* fajl, prepisujući za forenzičara potencijalno korisne podatke. Što je još gore, proces startovanja Windows OS kreira i briše mnoge privremene fajlove, pa i neke *swap* fajlove.

Web pretraživač kao što je *Netscape* i *MS Internet Explorer*, kreiraju *keš fajlove* da poboljšaju performanse. Ovi fajlovi se teško vide, ali postoji besplatan korisnički alat *UNMOZIFY* koji dopušta da se vidi njihov sadržaj. Analiza keš fajlova web pretraživača primarni je cilj svakog digitalnog forenzičara u slučaju nepropisnog korišćenja i drugih zloupuptreba Web-a: posete porno sajtovima, dečije pornografije, istrage hakerskog napada, posete hakerskim sajtovima za skidanje alata za hakerisanje računara i sl.

Windows OS mora da koristi relativno malu i skupu RAM memoriju vrlo efikasno i efektivno, jer brzo postaje prepunjena. Zato je razvijen metod da se sadržaj pune RAM memoriju „prenese“ u skriveni *swap* fajl na čvrstom disku tako da sistem može ponovo koristiti RAM memoriju. Sistem po potrebi prenosi podatke iz *swap* fajla u RAM memoriju. *Swap* fajl je forma virtulne memorije. Ovu operaciju sistem izvršava „u letu“ i bez znanja korisnika. Koncept *swap* fajla zadržan je i u savremenim OS sa većom RAM memorijom i zauzima u Windows sistemima oko 1 i po puta memorije računara. U starijim Windows sistemima swap fajl se zvao *WINDOWS386.SWAP* , a u savremenijim OS zove se *PAGEFILE.SYS*, a normalno se nalazi u rutu C: praticije čvrstog diska. Veličinu i lokaciju ovog fajla i do izvesne mere način upravljanja može podešavati korisnik, iako u praksi većina korisnika ostavlja ovaj fajl u podrazumevanom (*default*) stanju podešavanja.

U *swap* fajlu praktično se mogu naći podaci svake vrste, od punog dokumenta, e-pošte, pasvorda, do potencijalno otvorenog teksta inače šifrovanih informacija, koji može omogućiti lakše probijanje šifre. Ovaj fajl može biti masivni repozitorij za informacije koje forenzičar ispituje.

U normalnom isključivanju OS isključuje napajanje sistema, pri čemu se mogu dogoditi brojne potencijalno loše stvari za forenzičara:

- *Swap* fajl može biti prepisan i dragocene informacije izgubljene;
- Mnoge aplikacije se čiste i brišu privremene fajlove koje OS kreira u pozadini;
- Mogu se izgubiti detalji o logovanju korisnika, jer se često podaci za registre upisuju u memoriju, a zatim pri isključivanju u fajl registar, što menja stanje registara;
- Oblasti nealociranog (*slack*) prostora na disku mogu biti prepisane sa poslednjim upisanim podacima, a time izgubljeni ranije upisani podaci koji su mogli biti potencijalni dokazi;

- U normalnom isključivanju sistem memoriše fajlove na čvrsti disk i priprema se za sledeće uključivanje, pa normalno isključivanje očigledno utiče na vreme i datum kreiranja, pristupa i modifikacije fajla, što treba objasniti pred sudom, jer je promena nastala dok je računar u posedu forenzičara.

Korisnički definisano isključivanje podrazumeva da sistem izvršava normalno isključivanje, ali na bazi neke predefinisane instrukcije vlasnika/korisnika izvršava neku operaciju nad podacima i fajlovima, pre nego što sistem izvrši normalno isključivanje. Primer softvera koji izvršava ovu operciju je MS Outlook, koji je podešen da čisti ili sažima pridružene podatke i pri tome prepisuje, ili briše potencijalne dokaze. Druge softverske aplikacije kao *TweakUI* (MS razvojni alat) izvršava operacije određenih čišćenja pre kompletiranja isključivanja. Vešt korisnik može programirati *batch* fajl za pokretanje slične aplikacije u toku normalnog isključivanja.

Za forenzičara najozbiljnije posledice ostavlja korišćenje tzv. antiforenzičkog alata tipa *Evidence Eliminator*, koji je dizajniran sa ciljem da briše sve tragove aktivnosti u računaru osim fajla kojeg korisnik želi da bude viđen: koji Internet sajt je posećen, koji fajl je otvaran i prepisan i oslobođen memorijski prostor na disku (*slack* i nealocirani). Alati koji imaju funkciju „vrućeg ključa“ još više mogu otežati isključivanje i rad forenzičara. Tipkanjem određenog znaka, ili sekvence na tastaturi može se pokrenuti operacija prepisivanja koje forenzičar uopšte nije svestan.

Nasilno isključivanje ostavlja bez promene sve što je bilo na čvrstom disku u vreme isključivanja. Nasilno isključivanje još uvek se smatra najboljim načinom isključivanja za digitalne forenzičare. Gube se podaci koji se nalaze u RAM memoriji u vreme isključivanja, ali postoji mogućnost da su neki, ili svi podaci iz RAM-a upisani u *swap* fajl pre nego što se isključivanje izvršilo. U ovom načinu isključivanja deševa se jedna značajna akcija koja utiče na to da sistem ništa ne menja kod novog uključivanja. U Windows OS 95/98 i ME i Windows NT sistemima (NT, 2000 i XP) sistem je obavešten markerom tzv. *„dirty bit*“ ili“*dirty flag“* da se dogodilo ispravno isključivanje. Ovaj bajt informacija postavlja se na sistemu kada se fajlu prvi put pristupi posle starta. U FAT fajl sistemu ovaj bajt je u alokacionoj tabeli fajlova (FAT), a u NT sistemima nalazi se u $Volume fajlu. Kada se sistem normalno isključuje i kada se sve aktivnosti sistema završe i svi fajlovi propisno isključe, sistem resetuje *dirty bit* pošto se isključi. Efekat ove akcije je da saopšti sistemu na sledećem startovanju da je izvršeno propisno isključivanje.

U slučaju nasilnog isključivanja računara ne dopuštamo sistemu da se očisti, ili isključi na normalan način, tako da *„dirty bit“* ostaje setovan, tako da OS računara pri sledećem startovanju ima informaciju da je došlo do nepropisnog isključivanja, kao u slučaju nestanka struje i sl. i da sistem treba da preduzme akcije za samoproveru. U Windows 9X ta akcija je pokretanje SCANDISK programa za proveru diska, a u NT platformama - CHKDSK programa. Sa aspekta forenzičke analize ne-brisanje tog jednog bita informacija iz sistemske oblasti, ili fajl sistema nema posledice za analizu, [24].

Stanje pripreme, hibernacije i spavanja su stanja računara na koje forenzičar može naići u radu. Ako je računar isključen rad forenzičara je jednostavan, pod uslovom da se računar ponovo ne uključuje. Problem je kada forenzičar naiđe na uključen računar, kada su moguće brojne situacije. Jedna mogućnost je da je računar u pripremnom (*standby*) stanju, ili hibernaciji. Neki korisnici to nazivaju spavanjem računara, mada praktično računar gotovo nikada ne spava. Pripremno stanje-*Standby* računara je kada su isključeni monitor i čvrsti disk, a računar troši manje energije. Kada korisnik ponovo pristupi računaru, operativno stanje računara se brzo uspostavlja, desktop se rekonstruiše iz memorije u koju se memoriše suspendovano stanje, onako kako je stavljen u pripremno stanje. Dakle, u *Standby* stanju računar ne memoriše stanje desktopa na disk, pa prekid napajanja, ili nasilno isključivanje može dovesti do gubitka nememorisanih podataka. Ovaj način suspenzije rada računara pogodan je za kraće odsustvovanje od računara i može se zaštititi pasvordom. U ovom stanju još postoji verovatnoća da su u toku neki procesi u računaru, što ukazuje indikatoreska svetlosna dioda na računaru, pošto sistem zahteva neku energiju za održavanje podataka u RAM memoriji. Digitalni forenzičari su podeljeni oko toga da li računar treba vraćati u operativno stanje pre propisnog isključivanja. Postupak treba da zavisi od slučaja i okolnosti. Ako postoji indicija da je korisnik radio nešto na računaru u inkriminisano vreme, ova se opcija može razmatrati, [24].

Stanje *Hibernacije* u Laptop računaru neznatno se razlikuje po preduzetim akcijama sistema. Računar se isključuje da štedi energiju, ali memoriše stanje na desktopu i sve iz RAM-a na čvrsti disk pre isključivanja. Stanje desktopa računar memoriše na čvrstom disku u HIBERFILE.SYS fajl. Kod novog uključivanja računara ovaj fajl rekonstruiše stanje desktopa kakvo je bilo pre uvođenja u hibernaciju. Ovaj način suspenzije rada računara pogodan je za duže udaljavanje korisnika i može se zaštititi pasvordom. Sa aspekta forenzičara u ovom stanju je nabolje naći računar, jer pokazuje u kojem

stanju je korisnik napustio računar i ostavlja sve fajlove koji postoje. HIBERFILE.SYS se može ispitati na forenzičkom računaru kao svaki drugi fajl i videti šta se tačno desilo pre postavljanja računara u ovo stanje.

Rad na aktivnom (živom) sistemu može obezbediti maksimum dokaza, pod uslovom da se unesu minimalne izmene u ispitivanom sistemu. Ako forenzičar pristupi računaru osumnjičenog koji još uvek radi, može otkriti otvoreni šifrovani tekst, ili *on-line* bazu podataka u koju korisnik skladišti svoje podatke, ili je u toku rad korisnika koji je relevantan dokaz za slučaj. Najbolje rešenje je da forenzičar izvuče maksimum podataka iz sistema u radu, ali da obezbedi integritet svih sakupljenih dokaza, uključujući fotografisanje ekrana i svih akcija, pre isključivanja i privremenog oduzimanja računara. Sve ovo mora se uraditi što je moguće pre, pošto je računar povezan na Internet, pa je moguć daljinski pristup i mogu nastupiti neželjene posledice za potencijalne dokaze. U svim navedenim slučajevima važno je kakva ovlašćenja ima forenzičar-istražitelj, [9].

REZIME

Digitalna forenzika, relativno nova naučna disciplina (od 1999), nalazi mesto u pravosudnom sistemu. Prate je brze promene računarskih i digitalnih uređaja, sve sofistiranijih napada na računarske sisteme i mreže i rapidni porast zloupotreba IKT sistema i kompjuterskog kriminala.

Računar ima glavnu ulogu u većini istraga krivičnih dela, pa je sposobnost analize računara i ekstrakcije relevantnih informacija i dokaza od vitalnog značaja za istragu većine krivičnih dela kompjuterskog kriminala. Može biti *kompromitovan, osumnjičen, izvorni, napadnuti (žrtva), posredni i ispitivani* računar.

Po prihvatanju zahteva za forenzičku analizu računara, sledeći korak je početak ispitivanja računara, ili pravljenje *imidža* na fornzičkom računaru za dalju analizu. Svaki forenzičar treba da očekuje da bude pozvan da iznese ekspertsko mišljenje pred sudom, ili pak da veštači i razjašnjava određena pitanja u toku trajanja procesa. Na kraju, digitalni forenzičar mora poznavati brojne forenzičke alate koji obezbeđuju pouzdanu akviziciju i analizu, ne menjaju stanje na originalnom ispitivanom računaru, ne menjaju digitalne podatke, čuvaju integritet podataka/dokaza u lancu istrage i obezbeđuju ponovljivost rezultata u slučaju zahteva suda.

Početak same analize računara podrazumeva da je ispred forenzičara privremeno oduzeti računarski sistem sa pratećom periferijom, medijima i drugim potencijalnim dokazima, prikupljenim u procesu pretrage i privremenog oduzimanja računara, ili *imidž* HD-a osumnjičenog računara, ako nije moguće privremeno oduzeti računar. U slučaju ispitivanja računara osumnjičenog forenzičar mora znati šta treba da traži u računaru: slike, dokumenta, šifrovane informacije, ključne reči ili druge informacije? Ove informacije mora dobiti od istražitelja.

Metod isključivanja računara je osetljivo pitanje i zavisi od operativnih okolnosti i situacije u kojoj se računar nalazi i nema jedinstvenog pravila. Sigurno je jedino da se *ni jedan računar u procesu pretrage i privremenog oduzimanja ne uključuje*. Uključen računar obavlja milione operacija u sekundi i izaziva brojne promene u sistemu, koje potencijalno mogu izazvati izmene dokaza koje je teško objasniti pred sudom.

Windows OS imaju tri moguća isključivanja - normalno (*shutdown*), korisnički definisano i nasilno isključivanje, sa različitim posledicama za digitalne podatke.

U normalnom isključivanju OS mogu se dogoditi brojne potencijalno loše stvari za forenzičara: *Swap* fajl može biti prepisan i dragocene informacije izgubljene; mnoge aplikacije brišu privremene fajlove; mogu se izgubiti detalji o logovanju korisnika; menja se stanje registara; *slack* prostor na disku može biti prepisan, a ranije upisani podaci izgubljeni; sistem memoriše fajlove na HD i priprema se za sledeće uključivanje, što utiče na vreme i datum kreiranja, pristupa i modifikacije.

Korisnički definisano isključivanje za forenzičara ostavlja najozbiljnije posledice korišćenjem tzv. antiforenzičkog alata tipa *Evidence Eliminator*, koji je dizajniran sa ciljem da briše sve tragove aktivnosti u računaru osim fajla kojeg korisnik želi da bude viđen.

Nasilno isključivanje ostavlja bez promene sve što je bilo na čvrstom disku u vreme isključivanja. Nasilno isključivanje još uvek se smatra najboljim načinom isključivanja za digitalne forenzičare, ne dopušta sistemu da se očisti, ili isključi na normalan način, tako da *„dirty bit“*, koji indicira normalno isključivanje kog Windows NT, 2000, XP OS, ostaje setovan tako da OS računara pri sledećem startovanju ima informaciju da je došlo do nepropisnog isključivanja, kao u slučaju nestanka struje i sl. i sistem preduzima akcije za samoproveru pokretanjem SCANDISK (Win 9x) ili CHKDSK (Win NT) aplikacija.

Forenzičar može naići na računar u stanju pripreme, hibernacije i spavanja. Sa aspekta forenzičara u stanju hibernacije je nabolje naći računar, jer pokazuje u kojem stanju je korisnik napustio računar i ostavlja sve fajlove koji postoje. Stanje desktopa računar memoriše se na HD u HIBERFILE.SYS fajl, koji se može ispitati na forenzičkom računaru kao svaki drugi fajl i videti šta se tačno desilo pre postavljanja računara u ovo stanje.

Rad na živom sistemu može obezbediti maksimum dokaza, pod uslovom da se unesu minimalne izmene u ispitivanom sistemu i da obezbedi integritet svih sakupljenih dokaza, uključujući fotografisanje ekrana i svih akcija, pre isključivanja i privremenog oduzimanja računara.

PITANJA ZA PONAVLJANJE

1. Šta je Windows SWAP fajl i kako radi?
2. Kakvi dokazi mogu da se nađu u SWAP fajlu?
3. Ukratko objasniti uticaj normalnog *shutdown*-a u Windows OS na podatke i stanje računara?
4. Kakvi se dokazi mogu izgubiti prilikom normalnog *shutdown-a*?
5. Kakve vrste aktivnosti obuhvataju korisnički definisan shutdown?
6. Gde se isključuje napajanje računara prilikom *hard shutdown*-a?
7. Kako treba forenzičar da se ponaša sa otvorenim *online storage* na sistemu osumnjičenog?
8. Kakvi mogu biti efekti kopiranja nekog od fajlova osumnjičenog na originalne podatke?
9. Ukratko objasniti ACPO principe vezane za kompjuterske dokaze?
10. Objasniti razliku između *Standby* i *Hibernate* stanja računara?
11. Šta "*dirty bit*" indicira u NTFS fajl sistemu?

2 INTERPRETACIJA RAČUNARSKIH PODATAKA

2.1 Digitalni zapisi

Sve što korisnik unosi u računar – tekst, slike, grafiku i brojke, na najnižem nivou računar vidi kao binarne podatke – 1 i 0. Binarni podatak ili *Bit* ima dva moguća stanja – 1 i 0. Kombinacija od 4 bita zajedno – *Nibl*, ima 16 mogućih stanja 1 i 0 od 0000 – 1111. Grupisanjem 8 bita zajedno dobije se *Bajt,* koji ima 256 mogućih kombinacija 1 i 0 od 0000 0000 – 1111 1111. Dva bajta zajedno, ili kombinacija od 16 bita formira *Reč.* Bajt i reč imaju veću funkcionalnost u memorisanju podataka, jer nose znatno više informacija od jednog bita.

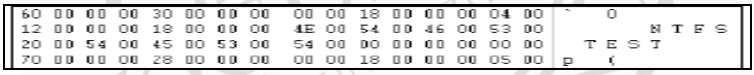
Da bi računar znao šta treba raditi sa nizom bita, treba da transformiše podatke u drugi oblik zapisa, kao na primeru na slici 2.1, gde je na tastaturi *word* procesora otkucano veliko slovo **A**, a niz bitova memoriše se na čvrstom disku kao **1** bajt, [24].



Slika 2.1 *Primer transformacije slova A iz ASCI kôda u binarni bajt*

Da bi računar znao da je uneto slovo A i kako da ga reprodukuje iz memorije, za ovu bazičnu operaciju koristi ASCII kôd prihvaćen kao standard u svetu računara. ASCII kôd se koristi da reprezentuje svaki od 26 karaktera engleskog alfabeta kao broj od 0-256 (256 mogućih varijacija), pri čemu ASCII koristi 1 bajt po karakteru. Brojevi 0-127 su standardni ASCI karakteri, a 128-256 je skup proširenih karaktera koji uključuje i slova glavnih svetskih jezika. Svaki put kada se na tastaturi otkuca neki ASCII karakter računar koristi ASCII tabelu da ga interpretira, konvertuje i memoriše u binarnoj formi.

Iako postoji godinama, ASCII kôd ima ograničenja, jer pokriva samo engleski jezik i nekoliko glavnih svetskih jezika. Zato je uveden *UNICODE* standard za uvođenje brojnih skupova jezičkih karaktera kojih ima u svetu. *UNICODE* koristi 2 bajta (16 bita ili reč) za skladištenje jednog karaktera, što je prihvatljivo za kapacitet savremenih čvrstih diskova od nekoliko 100 GB. *UNICODE* je razvijen kao format za „razmenu, procesiranje i prikazivanje pisanog teksta u različitim jezicima savremenog sveta“, a obezbeđuje jedinstveni broj za svaki karakter, bez obzira sa koje platforme dolazi, koji je program i koji jezik. Windows NT, 2000 i XP koriste *UNICODE* ekskluzivno na sistemskom nivou za manipulaciju karaktera i niza bitova. Može se predstaviti sa 8, 16, 32 – bita, a Windows sistem koristi 16-bitnu prezentaciju, što proizvodi maksimalno 65,536 mogućih varijacija karaktera. Međutim *UNICODE* može izazvati probleme forenzičarima kod pretraživanja teksta, jer koristi dva razmaka karaktera umesto jednog kod ASCII kôda. Ovo može otežati funkciju traženja reči zbog razmaka koji sistem ostavlja. Međutim, programeri forenzičkih alata su već rešili ovaj problem. U primeru na slici 2.2 prikazan je deo ulaza MFT tabele za neki fajl memorisan u *UNICODE*-u. Vidi se da za upisivanje slova **N** sistem koristi dva bajta: **4E 00**, dok za **T** koristi: **54 00**. ASCII reprezentacija u desnoj koloni pokazuje razmake slova.



Slika 2.2 *Deo ulaza MFT tabele za fajl memorisan u UNICODE-u*

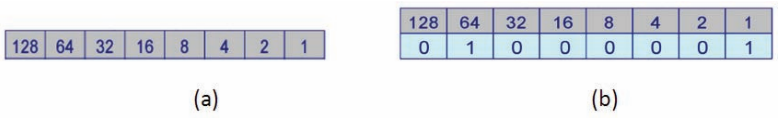
Deo procesa interpretacije binarnog niza u ASCII karaktere je pretvaranje binarnog kôda u decimalni broj. Svaki bajt, na primer slova **A** (slika 2.3), zapisuje sa desna na levo najmanje značajne bitove, slično kao decimalni broj: krajnje desno je jedinica, zatim desetice, pa stotine itd.



Slika 2.3 *Pretvaranje binarnog koda u decimalni (ASCI slovo A)*

U binarnom zapisu još uvek postoje jedinice, ali ne i desetice i stotine. Za formiranje težinskih faktora za pretvaranje binarnog koda u decimalni, počinje se od jedinice sa eksponentom 2 sa desna na levo, tako da je desna kolona još uvek 1, ali sledeća kolona ima težinski faktor 2 umeso 10 u decimalnom zapisu, zatim redom sa esponentom 2: 4, 8, 16, itd., (slika 2.4a).

Kombinovanjem težinskih faktora sa binarnim zapisom dobije se model za pretvaranje binarnog zapisa u decimalni, (slika 2.4b).



Slika 2.4 *Težinski faktori (a) i model (b) za pretvaranje binarnog zapisa u decimalni*

Za konverziju binarnog zapisa u decimalni, jednostavno se sabiraju proizvodi bita u binarnom zapisu (0 ili 1) sa težinskim faktorima tog bita, pa je u prikazanom primeru: **(1x64) + (1x1) = 65.** Tako na primer, binarni broj 0000 0000 ima decimalnu vrednost 0, a 1111 1111 ima vrednost 255, što daje ukupno 256 varijacija.

Kada se dobije 65 u prethodnom primeru, iz ASCII tabele za konverziju pronađe se konvertovana vrednost – slovo **A**. Za ovu operaciju računaru je potreban delić milisekunde.

Iako računar računa i skladišti uglavnom u binarnom zapisu, *heksadecimalni* (*heks*) zapis skraćuje zapis od **4** bita u jedan heksadecimalni broj, koji može imati 1 ili 2 cifre. Dakle, *heksa* zapis obezbeđuje efikasnije skladištenje podataka. Tako se binarni bajt može uskladištiti u dve *hex* cifre. *Hex* zapis je brojni sistem do vrednosti 16; koristi brojeve 0-9 i slova A-F koji zajedno daju 16 varijacija. Tako je moguće dobiti *hex* brojeve, na primer: 4C, D7, DE, koji se mogu lako identifikovati, ali i one koji liče na decimalne brojeve i teže ih je prepoznati, kao što su: 25, 65, 154 itd. Da bi se ova konfuzija izbegla uobičejeno je markiranje *hex* brojeva na jedan od tri načina:

- sa prefiksom „**h**“ (**h25**),
- sa sabskriptom „**16**“ (**25_{16}**), ili
- sa prefiksom „**0x**“ (**0x25**).

Sve vrednosti *hex* zapisa mogu se sumirati kao, (slika 2.5):

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

Slika 2.5 *Sve vrednosti hex zapisa*

Značaj *hex* zapisa može se ilustrovati sledećim primerom. Neka treba odgovoriti na pitanje koji je broj najveći od narednih brojeva u *hex*, binarnom ili decimalnom zapisu:

$$6AE9BC_{16}\ (\text{Hex})\ \text{ili}\ 11010101110100110111100_{2}\ (\text{Binary})\ \text{ili}\ 7{,}006{,}652_{10}\ (\text{Dec})$$

Kako su sva tri broja potpuno ista, jasno je koliko *hex* zapis zauzima manje prostora za skladištenje: *hex* zapis zauzima 6 cifara, decimalni 7, a binarni najviše. Pošto je memorijski prostor računara uvek kritičan, opravdan je razlog zašto se koristi *hex* brojni sistem. U sledećem primeru konverzije binarnog u decimalni broj dobije se, (slika 2.6):

128	64	32	16	8	4	2	1
0	1	0	1	0	0	1	1

(1x64)+(1x16)+(1x2)+(1x1)=83

Slika 2.6 *Primer konverzije binarnog u decimalni broj*

Konverzija binarnog broja u *hex* broj u mnogom je slična ovoj konverziji. Prvo se binarni bajt podeli u dva jednaka *nibla* od po 4 bita, (slika2.7a). Zatim se iznad svakog *nibla* ponovo upisuju isti težinski faktori kao za konverziju u decimalni broj, sa desna na levo i računaju po istom principu, (slika2.7b).



Slika 2.7 *Podela binarnog bajta na 2 nibla (a) i pondrisanje (b)*

Tako levi nibl ima: (1x4)+(1x1)=**5**, a desni: (1x2)+(1x2)=**3**. Kada se dve vrednosti napišu zajedno (prirodnim spajanjem kako su i razdvojeni) dobije se *hex* broj: **h53.**

Konverzija postaje kompleksnija kada *hex* broj dobija slova. Na primer, binarni broj 11001011 treba razdvojiti na dva jednaka nibla, (slika2.8a), a iznad svakog nibla upisati težinske faktore sa desna na levo, (slika2.8b)



Slika 2.8 *Podela bajta na 2 nibla (a) i pondrisanje (b)*

Levi *nibl* ima: (1x8)+(1x4)=**12**, a desni: (1x8)+(1x2)+(1x1)=**11**. Kako u konvrzionoj tabeli broj 12 ima *hex* ekvivalent **C**, a 11 ima **B**, u prethodnom primeru binarni broj 11001011 ima ekvivalentni *hex* broj **hCB**.

2.2 Mali i veliki kraj prvi u redosledu bajta

Poseban problem u računarskoj tehnici čini ne pridržavanje standardnih principa kod programiranja i skladištenja podataka, što dodatno otežava digitalnom forenzičaru razumevanje događaja u računaru. Jedna od značajnih stvari kod analize softvera je razumevanje redosleda bajta u kojem je više-bajtni broj uskladišten. Zavisno od OS postoje dva redosleda: *mali kraj prvi* (*Little Endian*) i *veliki kraj prvi* (*Bigg Endian*), prema analogiji razbijanja jajeta sa uže i šire strane.

Na početku razvoja računara različiti proizvođači (SPARC i IBM sa jedne i Intel sa druge strane) primenili su različite reprezentacije niza bitova. Jedni su skladištili bajt najnižeg red u nizu na najnižoj adresi, ili *mali kraj prvi*, dok su drugi skladištili bajt najnižeg reda na najvišoj adresi, ili *veliki kraj prvi*. Kada imamo samo jedan bajt infomacija sve je jasno – imamo 8 bitova i svaki ima svoj težinski faktor koji počinje sa najnižim redom sa desna na levo. U sledećem primeru neka je bajt predstavljen sa decimalnim brojem **83**,(slika2.9).

128	64	32	16	8	4	2	1
0	1	0	1	0	0	1	1

Slika 2.9 *Binarna reprezentacija decimalnog broja 83*

Ako imamo više od jednog bajta u nizu, važno je znati koji je metod skladištenja podataka korišćen, ili će rezultati forenzičke analize biti netačni. Neka si dva sledeća bajta uskladištena zajedno i neka predstavljaju broj veći od 256, (slika2.10).

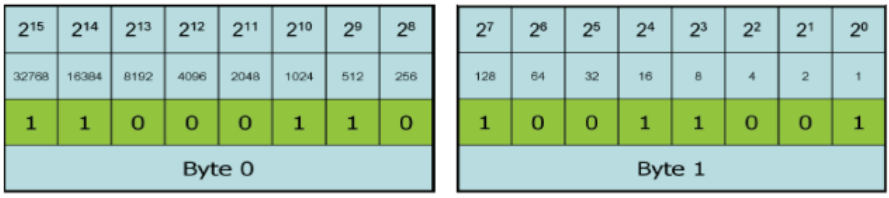


Slika 2.10 *Konverzija dva bajta u redosledu Mali kraj prvi (a) u decimalni broj (b)*

Ako su ova dva bajta uskladištena u redosledu *Mali kraj prvi,* bajt najnižeg reda uskladišten je na najnižoj adresi. Zbog toga jedinice ovog binarnog broja su sa desne strane u bajtu **0** i rastu prema levoj strani, zatim se broj nastavlja sa desne strane bajta **1**. U proračunu decimalne vrednosti ovog binarnog broja imamo sledeće:

Bajt 0=128+64+4+2=198, **Bajt 1**=32768+4096+2048+256=39168. Kada se ova dva broja saberu, dobije se: **198+39168=39366**.

Neka je isti binarni broj uskladišti u redosledu *Veliki kraj prvi,* imaće sledeću vrednost, (slika2.11):



Slika 2.11 *Konverzija dva bajta u redosledu Veliki kraj prvi u decimalni broj*

Bajt 0=32768+16384+1024+512=50698, **Bajt 1**=128+16+8+1=153. Kad se ove vrednosti saberu dobije se sasvim drugi decimalni broj: **50698+153**=**50841**.

Dakle, isti niz podataka isčitan na različite načine daje različite rezultate. Dodatni problem za forenzičare nastaje, što ponekad ne postoji način da se identifikuje kako su podaci uskladišteni i kako ih treba čitati. Verovatno najbolji primer koji ukazuje na značaj identifikacije načina skladištenja podataka je sistemsko skladištenje vremena i datuma. U 64-bitnom vremenskom zapisu u Windows OS, vremenski pečat je reprezentovan sa nizom karaktera koji u *hex* zapisu i redosledu *Mali kraj prvi* izgledaju kao: **10 B5 9D 9A 91 5D C5 01.** Dakle, pošto je datum zapisan u redosledu *Mali kraj*

prvi, da bi forenzičar ovaj zapis pročitao, treba ga prvo pretvoriti u redosled *Veliki kraj prvi*, zašto se prvo izvrši reverzija bajta: **01 C5 5D 91 9A 9D B5 10.** Sada se ovaj zapis pretvara u decimalni broj, pomoću tabela za konverziju, ili kao na slici 2.11. Dobije se sledeće vreme i datum: 23h:13min:59s od 20.05.2005.

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

REZIME

Sve unose u računar, na najnižem nivou računar vidi kao binarne podatke – **1** i **0**, koji se organizuju u 4 bita – *Nibl*, sa 16 mogućih stanja **1** i **0** od 0000 – 1111. Grupisanjem 8 bita dobije se *Bajt,* koji ima 256 mogućih kombinacija **1** i **0** od 0000 0000 – 1111 1111. Dva bajta zajedno, ili kombinacija od 16 bita formira *Reč.* Da bi računar znao šta treba raditi sa nizom bita, transformiše podatke u drugi oblik zapisa, koristeći ASCII kôd prihvaćen kao standard u svetu računara.

Zbog ograničenja ASCII kôda, jer pokriva samo engleski jezik i nekoliko glavnih svetskih jezika, uveden je *UNICODE* standard za brojne skupove jezičkih karaktera kojih ima u svetu. *UNICODE* koristi 2 bajta (16 bita ili reč) za skladištenje jednog karaktera, što je prihvatljivo za kapacitet savremenih čvrstih diskova od nekoliko 100 GB.

Iako računar računa i skladišti uglavnom u binarnom zapisu, *heksadecimalni* (*hex*) zapis skraćuje zapis od 4 bita u jedan heksadecimalni broj, koji može imati 1 ili 2 cifre. *Hex* zapis obezbeđuje efikasnije skladištenje podataka. Tako se binarni bajt može uskladištiti u dve *hex* cifre. *Hex* zapis je brojni sistem do vrednosti 16; koristi brojeve 0-9 i slova A-F koji zajedno daju 16 varijacija.

Poseban problem u računarskoj tehnici čini ne pridržavanje standardnih principa kod programiranja i skladištenja podataka, što dodatno otežava forenzičaru razumevanje događaja u računaru. Jedna od značajnih stvari kod analize softvera je razumevanje redosleda bajta u kojem je više-bajtni broj uskladišten. Zavisno od OS postoje dva redosleda: *mali kraj prvi* (*Little Endian*) i *veliki kraj prvi* (*Bigg Endian*), prema analogiji razbijanja jajeta sa uže i šire strane.

PITANJA ZA PONAVLJANJA

1. Koje tipove podataka računar prepoznaje?
2. Šta znači skraćenica BIT?
3. Koliko bajt ima bita?
4. Veličina Nibla?
5. Veličina reči?
6. Šta znači termin ASCII?
7. Koja je svrha ASCII tabele?
8. Koliko bajta zauzima jedan ASCII karakter?
9. Koliko bajta zauzima jedan UNICODE karakter u Windows sistemima?
10. Upisati sledeće vrednosti stepena sa osnovom 2:

    2^1 = 2^2 = 2^3 = 2^4 =

    2^5 = 2^6 = 2^7 = 2^8 =

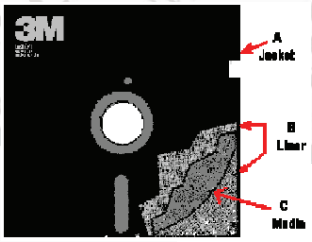
    2^9 = 2^{10} = 2^{16} =
11. Konvertovati binarni zapis 1001 1011 u decimalni.
12. Konvertovati binarni zapis 1001 1011 u heksadecimalni zapis
13. Šta je *Little Endian*?
14. Šta je *Big Endian*?

3 FIZIČKE KARAKTERISTIKE KOMPJUTERSKIH MEDIJA

3.1 Fizičke karakteristike disketa i čvrstih diskova računara

Forenzičar računara mora poznavati brojne elektronske i optičke medijume koji se koriste u računarskim sistemima za skladištenje podataka, njihove principe skladištenja digitalnih podataka i osnovne načine funkcionisanja, [24].

Fizičke karakteristike disketa-FD (*Flopy Discs*) su u upotrebi od 1971. godine (IBM). Inicijalno su korišćene za skladištenje OS koji pokreće računar. Tokom vremena razvijena su dva tipa FD u računaru – jedan za OS, a drugi za podatke sa oznakama **A** i **B**. Otuda savremni HD ima oznaku **C**. Postoje dve fizičke veličine FD 5 1/4 inča i 3 1/2 inča, pri čemu je prvi retko u upotrebi. Flopi disk od 5 1/4 inča je jedinstvena celina omota (A) koji fizički štiti medijum i disk u njemu (C), (slika 3.1).



Slika 3.1 *Flopi disk od 5 1/4 inča*

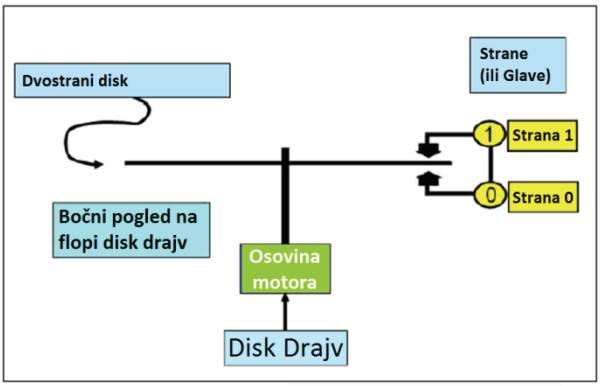
Sloj (B) namenjen je za čišćenje diska od prašine. Ovaj FD je osetljiv na prašinu i magnetni sloj se može oštetiti čak i upiisvanjem oznake na omotu. Sam disk je proizveo *Mylar*, koji je prekriven slojem metal oksida. Kroz ovalni otvor na donjem delu FD magnetne glave snimaju/čitaju podatke sa FD. Ovaj FD je sasvim fleksibilan i može biti težak za transport. FD se može zaštititi od upisivanja prekrivanjem proreza na desnoj ivici. Ovaj FD ima kapacitet od 720KB podataka koji se upisuju samo na jednu stranu diska.

Disketa 3 1/2 inča nalazi se u čvrstom plastičnom omotu. Takođe je proizvodi *Mylar* i sadrži sloj za čišćenje diska od prašine. FD se lakše transportuje, zbog veličine i čvrstog kućišta, (slika 3.2).



Slika 3.2 *Flopi disk od 3 1/4 inča*

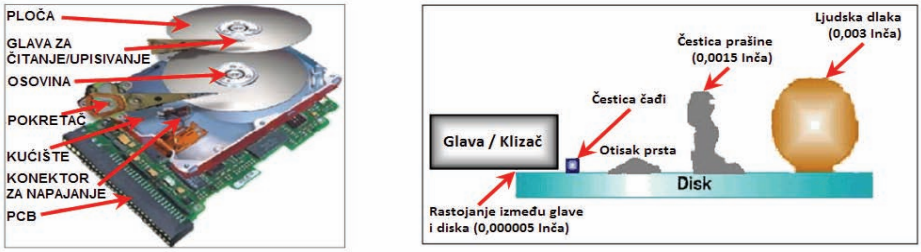
Pokretni zatvarač, koji se automatski otvara umetanjem FD u pogonsko kućište (drajv) računara, zatvara prorez za kontaktiranje magnetnih glava za snimanje/čitanje podataka i štiti disk od prašine. Ovaj FD ima klizač za zaštitu od snimanja, koji je na slici prikazan na donjem levom delu FD. Ako je prorez zatvoren (kao na slici) FD nije zaštićen od upisivanja podataka, a suprotno - jeste. Desni prorez na ovom FD je senzorski otvor na osnovu kojeg OS određuje koji tip FD koristi, pošto takav otvor nema FD tipa A. Ako se ovaj FD rastavi otvaranjem plastičnog omota, lako je ustanoviti da je sam disk izložen uticaju prašine koja ga oštećuje. Kapacitet ovog FD je 1.44MB. Raniji tipovi FD upisivali su podatka samo na jednu stranu, a savremeni FD ovog tipa snimaju podatke na obe strane diska sa dve pokretne magnetne glave. Glave za upisivanje/čitanje dodiruju medijum sa pokretnim vrhom (*pincer motion*). Kod ovog tipa FD magnetne glave se počinju brojati sa donje strane FD, koja je uvek prva strana, dok je gornja strana druga strana FD. Međutim, treba naglasiti da u računarskoj tehnici brojanje počinje sa 0, a ne sa 1 kako je logično u fizičkom svetu, (slika 3.3), [24].



Slika 3.3 *Dvostrano upisivanje na FD 1.44 MB*

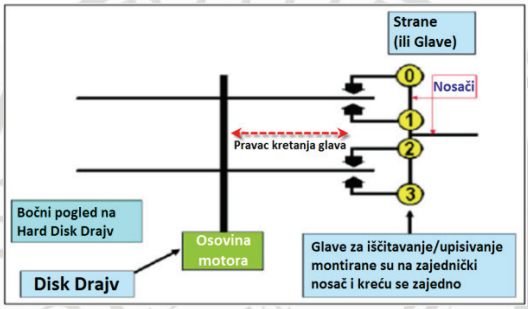
Fizičke karakteristike čvrstih diskova–HD imaju sličnosti sa FD samo u tome što se magnetni disk rotira oko pogonske osovine i podaci se čitaju pomoću glava za čitanje/upisivanje. HD obuhvata 1, ili više čvrstih diskova (ploča) jednake veličine smeštenih u metalnom kućištu jedan iznad drugog na pogonskoj osovini. Kućište HD se ne može otvoriti i diskovi su zaštićeni od prašine. Disk je presvučen tankim filmom magnetnog matrerijala. Što je magnetni film tanji, to se veća količina podataka može uskladištiti na film. Nosač glava za čitanje/upisivanje postavlja glave veoma blizu magnetnog filma, što dopušta upisivanje veće količine podataka, poznata kao prostorna gustoća.

Sterilnost HD postiže se u toku proizvodnje sklapanjem diska u sterilnim uslovima. Na slici 3.4, [24], vidi se u kojoj meri čestice prašine mogu uticati na funkcionisanje glava koje se kreću iznad magnetnog sloja diska na rastojanju od 0,00005 inča. Diskovi se obrću različitim brzinama, ali su uobićajene rotacione brzine 5400 o/min (obrtaja u minuti), 7200 o/min i 10000 o/min. Zato pri ovolikim rotacionim brzinama svaka čestica može izazvati oštećenje magnetne površine diska.



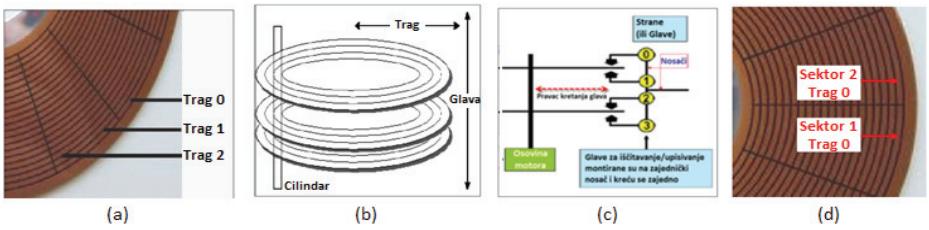
Slika 3.4 *Fizičke karakteristike HD*

Brojanje glava za čitanje/upisivanje, za razliku od FD, kod HD počinje sa gornje strane (0) prvog diska, (slika 3.5). Sve glave na nosaču glava kreću se zajedno bez obzira koja glava i na kojem disku je aktivna.



Slika 3.5 *HD sa dva diska i 4 glave za pisanje/brisanje*

Za lociranje podataka na HD tradicionalno se koristi sistem koordinacije sa metodom *CHS* (*cilindar, glava, sektor*) adresiranja. Glave za čitanje/upisivanje upisuju digitalne podatke (1 i 0) na površini ploča diska u obliku kružnih koncentričnih *tragova*, počevši upisivanje sa oboda diska prema središtu, (slika 3.6a). Brojanje tragova počinje od 0. Na jednom FDu može biti više hiljada tragova – na FD kapaciteta 720 MB i 1,44MB ima po 80 tragova na svakoj strani diska. Magnetni trag na disku je neznatno širi od glave za čitanje/upisivanje.



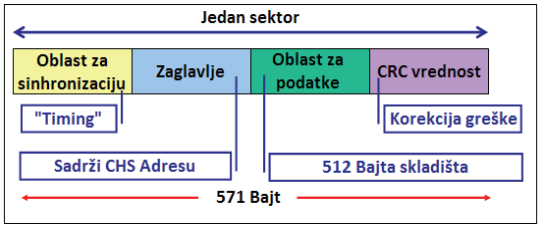
Slika 3.6 *Upisivanje tragova (a), cilindri sa 3 traga (b), brojanje glava (c) i sektori (d) HD*

Cilindar na HD je virtuelni, a čine ga tragovi istog broja, posmatrani iznad površine gornje ploče diska na dole do poslednje ploče diska, (slika 3.6b). Na FD cilindar sadrži dva traga istog broja na gornjoj i donjoj strani diska. Svi tragovi u jednom cilindru mogu se upisati/čitati istovremeno bez kretanja glava. Brojanje cilindera, kao i tragova počinje od 0 sa oboda prema centru.

Glava je fizički elemenat za upisivanje/čitanje podataka na/sa diska. Sa aspekta geometrije diska, glava je deo koordinacionog sistema za lociranje mesta na specifičnom sektoru podataka. Svaka strana svakog diska ima svoju glavu, (slika 3.6c).

Sektor je kontinualni, linearni niz magnetisanih bita koji zauzima zakrivljenu sekciju traga. Sektor je najmanja fizička jedinica za skladištenje na disku i normalno sadrži **512** bajta, (slika 3.6d). Brojanje sektora unutar CHS sistema adresiranja počinje sa **1**. Jedan trag sadrži veći broj sektora. Na FD od 720 KB ima 9 sektora po tragu, a FD od 1.44MB ima 18 sektora po tragu.

Šta se dešava u sektoru na disku, kada se upisuju podaci? Svaki sektor ima četiri glavne komponente: *zonu za sinhronizaciju, heder (zaglavlje), oblast podataka* i *CRC* (*Cycle Redundancy Value*) – vrednost za proveru redundantnosti ciklusa, (slika 3.7).

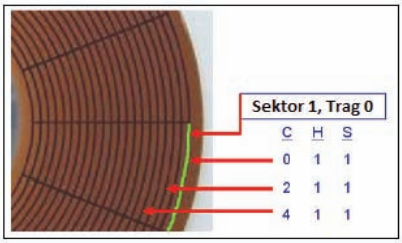


Slika 3.7 *Struktura sektora*

Zona za sinhronizaciju sinhronizuje aktivni sistem na odgovarajući sektor. Bez obzira na rotacionu brzinu diska asambl glava je uvek usklađen sa sektorom. Kada sektor dođe ispod glave, zona za sinhronizaciju podešava glavu i sektor za kompletiranje akcije čitanja, ili upisivanja na disk. *Heder* sektora sadrži vrednost CHS za određeni sektor, što je ponovo provera za pravi položaj sistema da očita/upiše podatke na mesto koje je za to predviđeno. *Oblast podataka* sadrži 512 bajta podataka korisnika. *CRC* vrednost je kontrolna suma za zaštitu integriteta podataka.

Kako sektor sadrži 512 bajta podataka, očigledno fizička veličina sektora mora biti veća. Aktuelna veličina sektora iznosi **571** bajt, ali korisnik, kao i forenzičar, mogu videti samo 512 bajta informacija, dok nedostajućih 59 bajta ostaje nevidljivo.

Za forenzičara važno je da razume kako cilindri, glave i sektori funkcionišu zajedno u fizikalnom smislu. Ako se posmatra gornja, ili druga strana (1) FD, oblast markirana zelenom bojom na slici 3.8., je sektor i to pretpostavimo sektor 1, koji pripada tragu 0, ili cilindru 0. Kako brojanje počinje sa sektorom 1, možemo označiti ovu lokaciju kao CHS 0,1,1, ili cilindar 0, glava 1, sektor 1, koji predstavlja tro-koordinatni sistem za lokaciju podataka na disku.



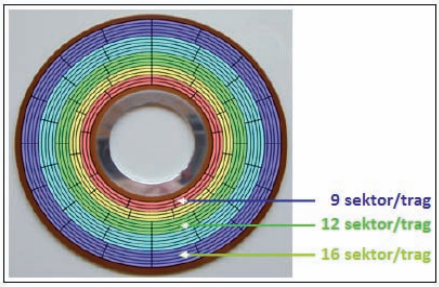
Slika 3.8 *Lokacija CHS 011- sektora 1, glave 1 cilindra 0*

Kod savremenog HD, na primer Laptop računara, koji je neznatno deblji od FD, oznaka ukazuje da HD ima 16 glava, odnosno 8 diskova, (slika 3.9). Međutim, treba postaviti pitanje da li se zaista u ovaj fizički obim može smestiti 8 diskova i da li se može verovati oznakama na HD?



Slika 3.9 *Primer oznake CHS na fizičkom HD*

Svakako da ne treba verovati oznakama proizvođača, ali forenzičar mora znati šta se zaista nalazi u kućištu HD. Kod prvih HD svaki disk je imao konstantan broj sektora po tragu – od spoljnog do unutrašnjeg traga, tako da su tragovi prema središtu diska imali veću gustinu pakovanja podataka. U nastojanju da što racionalnije iskoriste fizički prostor diska i uskladište što više podataka, proizvođači su razvili novu tehnologiju kojom se smanjuje gubljenje prostora za skladištenje i povećava gustina podataka. Da bi spoljni tragovi bili bolje iskorišćeni i imali veću gustinu pakovanja podataka, tragovi su deljeni u *zone* sa nejednakim broj sektora, tako da u spoljnoj zoni tragovi imaju veći broj sektora, s tim da se prema unutrašnjim zonama broj sektora po tragu sukcesivno smanjuje. Ova tehnologija proizvodnje HD nazvana je *Snimanje bita po zonama* – ZBR (*Zone Bit Recording*). Skladištenje podataka na HD kontroliše sofisticirana elektronika kartice *drajv* kontrolera, (slika 3.10), [24].



Slika 3.10 *ZBR – Snimanje bita po zonama*

Čvrsi disk se deli u zone sa određenim brojem koncentričnih tragova, tako da se broj sektora po tragu povećava u zonama koje su dalje od centra diska: 9, 12, 16 sektora po tragu na slici u primeru. Ovim je racionalizovana gustina pakovanja podataka na fizičkom disku, ali to znači i da ZBR lociranje podatka u sektoru ne može izvršiti sistem CHS adresiranja. Zato HD kontroler prevodi ZBR adresiranje u CHS, koje OS i BIOS prepoznaju. Sada postaje jasno zašto treba proveriti oznake na HD, posebno starije generacije, [24].

Međutim, u poslednje vreme pokazalo se da CHS adresiranje nije pogodno za diskove većeg kapaciteta. Treabalo je razviti novi, znatno jednostavniji sistem adresiranja koji HD posmatra u logičkim blokovima – LBA (*Logical Blocks Addressing*), koji počinju sa prvim sektorom i nastavljaju do poslednjeg sektora. LBA brojanje počinje od 0 i sektora 0, koji je prvi sektor na disku. U CHS adresiranju početak je bila adresa 0,0,1, u LBA adresiranju diska polazi se

od prvog sektora u prvom tragu diska, zatim ide dole kroz cilindar sve do kraja, a onda vrati opet gore na drugi sektor i nastavlja istim putem kroz cilindar na dole. Efektivno, CHS adresiranje koristi sistem kućnog broja, imena ulice i imena grada za adresiranje lokacije, dok LBA adresiranje prvo uzima broj kuće kao 0, a zatim daje svakoj kući novi broj sve dok ne dođe do kraja ulice.

3.2 Proračun veličine čvrstog diska

Sa aspekta forenzičara uvek je potrebno poznavati kapacitet analiziranog diska. Dok je kod ostalih medijuma (CD, USB, FD) uvek jasno iz oznake koliki kapacitet imaju, kod HD to nije slučaj. Forenzičar mora biti siguran koliko je podataka uskladišteno na disku, da su svi podaci preuzeti u procesu akvizicije i da je obuhvaćen ceo prostor diska. Veličina kapaciteta diska kod CHS adresiranja računa se množenjem broja, [24]:

C (cilindara) x **H** (glava) x **S** (sektora)/tragu x Bajta/sektoru = Ukupan broj bajta u HD

Na primer, neka HD ima oznaku: C=6304, H=16 i S=63, biće:

6304 x 16 x 63 x 512 = 3.253.469.184 ili oko 3,2 GB

Kod LBA adresiranja kapacitet diska se računa množenjem:

Ukupan broj sektora x 512 bajta = Ukupan broj bajta HD.

3.3 BIOS i ograničenja proizvođača čvrstih diskova

Stvarne informacije o kapacitetu HD smešetene su u BIOSu. Proizvođači u BIOSu koriste 24 bita za adresiranje HD: 10-za broj cilindera, 8-za broj glava i 6-za broj sektora. Ovoliko mali broj bita omogućava adresiranje samo ograničenog broja vrednosti u CHS sistemu. Ograničenje je postavljeno sa *interupt 13*h BIOS funkcijom, koja obezbeđuje komandni interfejs između kontrolera diska i svakog softvera koji zahteva pristup disku. Ograničenja proizvođača BIOSa mogu se izraziti na sledeći način, [24]:

Cilindri – 10 bita = 1 024 moguće vrednosti,

Glave – 8 bita = 256 mogućih vrednosti,

Sektori – 6 bita = 64 moguće vrednosti (efektivno samo 63 jer se sektor broji od 1).

Ako se uzmu maksimalne vrednosti, biće:
1024x256x63x512=8,455.716.864=8,4GB.

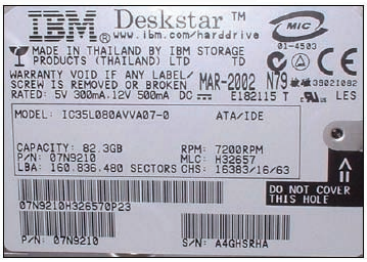
Dakle, korišćenjem CHS adresiranja može se adresirati samo HD do veličine od 8,4GB. Problem su prevazišli proizvođači diskova, koristeći drugačiji sistem vrednosti za CHS od proizvođača BIOS - isti broj bita (24 bita), ali ih deleći na drugačiji način:

Cilindri – 14 bita=16 383 moguće vrednosti (umesto 16 384 zbog ograničenja ATA-4),

Glave – 4 bita= 16 mogućih vrednosti,

Sektori – 6 bita = 64 moguće vrednosti (efektivno 63 jer brojanje počinje od 1).

Ako uzmemo maksimalne vrednosti i pomnožimo ih, dobije se ista vrednost, ili 8,4GB veličina diska. Kada su nastala ova ograničenja neki proizvođači HD nastavili su označavati svoje diskove znatno većeg kapaciteta oznakom maksimalnog kapaciteta CHS vrednosti - 8,4GB, na primer *Maxtor HD model 91728D8* pokazuje na oznaci CHS vrednosti od 16 383, 16 i 63, odnosno kapacitet od 8,4GB, dok se proverom na web sajtu firme otkriva vrednost istog HD od 17,2GB. Forenzički softverski alati mogu pokazati stvarnu vrednost HD, bez obzira na deklarisanu CHS vrednost proizvođača. Na slici 3.11 prikazan je primer *IBM Deskstar HD* koji stvarno ima kapacitet od **82,3GB**, dok CHS vrednost na istom disku ukazuje na vrednost 8,2GB.



Slika 3.11 *Primer oznake CHS vrednosti od 8,2GB na HD od 82,3GB*

Međutim, pronađen je novi način adresiranja za prevazilaženje ograničenja od 8,4GB, uvođenjem ekstenzije interupt 13*h*, gde se umesto 24 bita koriste 64 bita, što daje $9{,}4x10^{21}$ varijacija, ili omogućava adresiranje kapaciteta diska do oko 9,4 triliona GB.

Stariji računarski sistemi imali su samo jedan kanal kojim se HD povezuje sa glavnom pločom. Uvođenjem koncepta glavnog (*Master*) i potčinjenog (*Slave*) diska na istom kanalu, moguće je na istom kanalu koristiti dva HD, a koristeći spojnice (*jumpers*) na HD može se odrediti koji HD je glavni, a koji potčinjeni. Daljim razvojem računara, uvedena su dva kanala, od kojih svaku ima glavni i potčinjeni HD, što daje mogućnost vezanja četiri HD u računarskom sistemu. Takođe na ovim kanalima mogu se videti i drugi drajvovi, kao što su CD-ROM, ili DVD.

Takođe, moguće je imati mešovitu tehnologiju pogona diskova, a najpoznatiji primer je kombinovanje IDE i SCSI dikova koji koegzistiraju u istom računaru, koristeći SCSI kontroler, kao i SATA (serijski ATA) sa IDE drajvom

REZIME

Forenzičar mora poznavati brojne elektronske i optičke medije koji se koriste za skladištenje računarskih podataka, njihove principe skladištenja i osnovne načine funkcionisanja. Prvi mediji za skladištenje digitalnih podataka savremnih računara su diskete (FD): tipa A - veličine 5 1/4 inča i kapaciteta od 720KB i jednostranim upisivanjem/čitanjem podataka i tipa B – veličine 3 1/2 inča, kapaciteta 1,44MB i dvostranim upisivanjem u koncentrične tragove sa početkom od periferije diska prema centru.

Čvrsti diskovi (HD) su unapredili tehnologiju i kapacitet skladištenja do reda TB (1000GB). U kućištu HD može se nalaziti i do 16 ploča diska, na koje glave za upisivanje/čitanje upisuju podatke u koncentrične krugove (tragove). *Glava* je fizički elemenat za upisivanje/čitanje podataka na/sa diska. Glave se nalaze na ručki koje se kreću jednakom brzinom od periferije ka centru, pri obrtanju noseće osovine ploča HD od 5400-10000 o/minuti, zbog čega kućište HD zahteva visok stepen čistoće (sterilne uslove). *Cilindar* na HD je virtuelni, a čine ga tragovi istog broja, posmatrani iznad površine gornje ploče diska na dole do poslednje ploče diska. Svi tragovi u jednom cilindru mogu se upisati/čitati istovremeno bez kretanja glava. *Sektor* je kontinualni, linearni niz magnetisanih bita koji zauzima zakrivljenu sekciju traga i predstavlja najmanju fizičku jedinicu za skladištenje na disku od 512B. Svaki sektor ima *zonu za sinhronizaciju, heder, oblast podataka* i *CRC* - vrednost za proveru redundantnosti ciklusa.

Označavanje HD i adresiranje na bazi CHS podataka bilo je korektno do razvoja HD kapaciteta od 8,4GB, gde je ograničenje postavljeno sa *interupt13h* BIOS funkciojom, koja obezbeđuje komandni interfejs između kontrolera diska i svakog softvera koji zahteva pristup disku, zbog različitog korišćenja 24 bita za adresiranje HD, od strane proizvođača HD i BIOSa.

Za što racionalnije korišćenje fizičkog prostora HD i skladištenje što više podataka, proizvođači su razvili novu tehnologiju pakovanja podataka u tragovi podeljene u *zone* sa nejednakim brojem sektora, tako da u spoljnoj zoni tragovi imaju veći broj sektora, a u unutrašnjim se broj sektora po tragu sukcesivno smanjuje. Ova tehnologija se naziva *snimanje bita po zonama* – ZBR. Takođe je razvijen novi, znatno jednostavniji sistem adresiranja koji HD posmatra u logičkim blokovima – LBA. Dok CHS adresiranje počinje sa

adresom 0,0,1, LBA brojanje počinje od 0 i sektora 0, koji je prvi sektor na disku. Na bazi CHS ili LBA podataka na kućištu HD, forenzičar jednostavnim množenjem sa kapacitetom sektora (512B) može proveriti stvarni kapacitet diska, što je značajno za otkrivanje potencijalnih skrivenih particija.

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

PITANJA ZA PONAVLJANJE

1. Koje su to dve fizičke veličine FD koje susrećemo?
2. Koji od ovih je najčešći?
3. Koja strana FD je 0?
4. Koliki je kapacitet *high density* 3,5" FD izražen u CHS vrednosti?
5. Kako se računa kapacitet čvrstog diska (HD)?
6. Ukoliko oznaka na HD izražava CHS vrednost diska od 16.383, 16, 63 – kolika je njegova veličina?
7. Zašto je na HD rezervisan prostor od 8.4GB?
8. Kako je ovo prevaziđeno?
9. Kakva je uloga *Interupt13h* ekstenzije u ovom?
10. Šta je cilindar?
11. Šta sačinjava jedan sektor?
12. Šta u geometriji diska predstavlja glava?
13. Šta je trag?
14. Šta je LBA i čemu služi?
15. Objasnite kakve prednosti ZBR nudi i zašto?

4 TEHNOLOGIJA CD, DVD I FLEŠ MEMORIJA

4.1 Tehnologija kompakt diskova

Kompakt diskovi (CD) redovno se koriste za skladištenje podataka i forenzičari ih redovno nalaze u istrazi. CD se generalno mogu klasifikovati u dve glavne kategorije: *samo za čitanje* (*Read Only*), ili fabrički presovani i *za pisanje i čitanje* (*Recordable*). CD samo za čitanje dele se u dve glavne gkategorije, [17]:

1. *CD-DA* (*Digital Audio*) ili muzički CD i
2. *CD-ROM* ili CD za podatke.

CD za čitanje i pisanje takođe se proizvodi u dve glavne vrste:

1. *CD-R* (Recordable),
2. *CD-RW* (Rewritable).

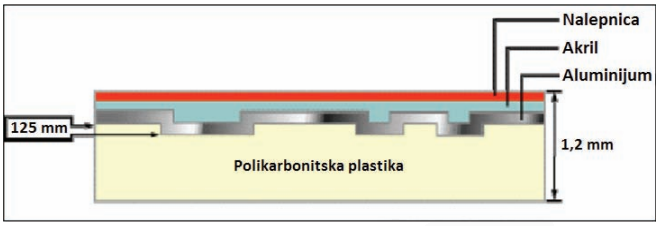
Ovi CD-ovi razlikuju se po fizičkoj kompoziciji, načinu skladištenja podataka i fizičkom izgledu. Zajednička im je samo veličina - debljina 1,2mm i prečnik 12cm. Standardna dimenzija CD odstupa u pogledu prečnika (manjeg) i oblika diska (veličine kreditne kartice). CD skladišti podatke po neprekidnoj spirali koja počinje od centra diska (slika 4.1). Širina spirale je 0,5 mikrona, a spirale su razmaknute 1,6 mikrona. Podaci se sa diska čitaju sa laserom usmerenim na disk, a meri se reflektovana svetlost.



Slika 4.1 *Upisivanje podataka na CD*

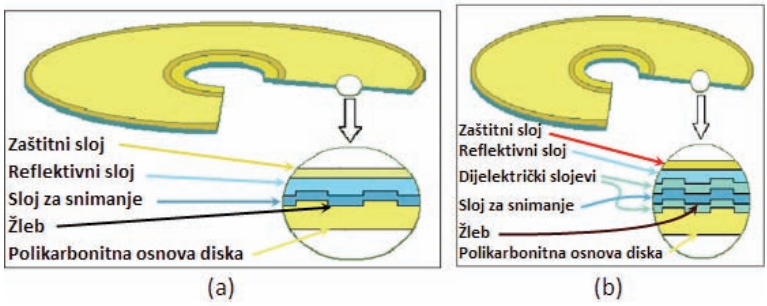
Fabrički presovani CD (samo za čitanje) skladište podatke kao mikroskopske ’čvoriće’ na aluminijumskom sloju koje pravi laser. Laser skenira disk i čita

sadržaj, detektujući čistu površinu aluminijumskog sloja kao **1**, a mesta gde su 'čvorići' kao **0,** (slika 4.2)**.**



Slika 4.2 *Presek strukture fabrički presovanih diskova*

Kompakt diskovi za snimanje (CD-R) imaju sloj od organske polimerske boje između polikarbonatnog i metalnog sloja, koji služe kao medijum za snimanje podataka. Laser u u toku snimanja u rekorederu *'spaljuje'* rupice u organskom sloju boje. *Spaljena* oblast slabije reflektuje lasersku svetlost od nezagrejane površine. Ovo omogućava upisivanje podataka na CD u sesijama, odnosno ne moraju se svi podaci upisati na CD-R odjednom, nego mogu u više vremenski nezavisnih sesija, što ima određene forenzičke posledice. CD-R sa upisivanjem podataka u jednoj sesiji, (slika 4.3a), može se čitati na skoro svakom plejeru ili drajvu, dok više-sesijski CD zahtevaju za čitanje više-sesijske čitače. CD-R medijumi su često zelene, žute ili plave boje, a mogu biti skoro u bilo kojoj boji.



Slika 4.3 *Kompakt disk za jednokratno -CD-R (a) i za višestruko snimanje (b)*

CD za višekratno snimanje podataka (CD-RW) umesto organske boje ima leguru. Laser menja stanje legure – zagrevanjem vrši kristalizaciju u dekristalizaciju i obrnuto. Ovaj proces, poznat kao tehnologija promene optičke faze (*Optical Phase Change Technology*), koristi različite vrste polimera u konstrukciji diska koji različito reaguju na temperaturu laserskog

zraka, što omogućava čitanje, pisanje i brisanje diska, (slika 5.3b). Za CD-RW zahteva se namenski drajv sa softverom za paketsko upisivanje.

Kapacitet kompakt diskova najčešći je 650 MB (74 minuta) i 800 MB (80 minuta). Veći kapacitet se jednostavno postiže zgušnjavanjem spirala na površini diska. Ako se koriste CD sa većim kapacitetom može doće do izvesne nekompatibilnosti sa starim CD diskovima. Sa tehnikom 'pregrevanja' (*overburning*) može se postići i veći kapacitet CD. Ovu mogućnost poseduje većina savremenih softvera za snimanje diskova (*Nero* itd.). Međutim, kako ovaj proces nije standardan, nema garancije da će se tako snimljeni diskovi moći čitati.

4.1.1 Fajl sistem kompakt diskova

Kao svaki sistem za skladištenja fajlova podataka, kompakt diskovi treba da koriste neki fajl sistem da bi se skladištili podaci na disk. Postoje tri glavna tipa fajl sistema CD, koji se razlikuju u pogledu podrške dužine imena fajla i kako se podaci stvarno skladište: *ISO 9660, Joliet* i *UDF* (*Universal Disk Format*) ili *ISO 13346,* [24].

Standard ISO 9660, uveo je suštinske restrikcije na originalnom fajl sistemu, razvijenom tokom vremena za kompakt diskove. Restrikcija se odnosi na konvenciju imenovanja fajla i strukturu direktorijuma koja to dopušta. Ime fajla može samo sadržavati velika slova, brojeve od 0-9 i donju crtu. Kada se piše ime direktorijuma, može se koristiti samo 8 karaktera, bez ekstenzije, a struktura direktorijuma je ograničena na 8 pod-direktorijuma po dubini. Mogućnost čitanja ovog tipa fajl sistema poseduju Unix i Apple Mac sistemi. Ovaj standard koristi logički fajl sistem, pa upisivanje paketa nije sasvim kompatibilno; standard mora tačno znati koji fajlovi će biti upisani i lokaciju njihovog izvora.

Standard JOLIET je ekstenzija standarda *ISO 9660* i dozvoljava dužinu imena fajla do 64 karaktera, uključujući razmak i koristi Unicode karaktere u imenu fajlova. Napisao ga je Microsoft i podržavaju ga Windows 95 i kasniji OS, osim Windows NT 4.0.

Univerzalni format diska (UDF) ili *ISO 13346* prevazilazi sve probleme standarda ISO 9660, omogućavajući inkrementalno dodavanje jednog po jednog fajla CD-Ru i CD-RWu, koristeći tehnologiju upisivanja paketa. Ovo stvara manje neiskorišćenog prostora na disku. UDF koristi *Virtuelnu*

alokacionu tabelu (VAT) za snimanje i opis lokacija svakog fajla na disku. VAT se kreira posle svake sesije snimanja. Svaka novo kreirana VAT uključuje podatke iz prethodne VAT, omogućavajući UDF da ima evidenciju i lokacije svakog fajla upisanog na disk, čak i kada je prepisan u nekoj fazi, što je značajno za forenzičara.

Sesije podataka upisuju se na disk korišćenjem softvra za upisivanje na CD - *rezača*, kao što su *Nero,* ili *Easy CD Creator*. Većina ovih aplikacija može koristiti navedene fajl sisteme. Da bi se obezbedila finkcija *drug&drop*, većina ovih aplikacija povezana je sa softverom za upisivanje paketa, kao što su *InCD* ili *DirectCD*. Računar treba da ima ugrađen CD drajv. Windows XP OS ima aplikaciju za upisivanje podataka na CD.

4.2 DVD tehnologije

Na neki način, DVD disk se može smatrati kao 'veliki' CD. Prvi DVD standardi uspostavljeni su 1995. godine. Razvijeno je više formata DVD, [17]:

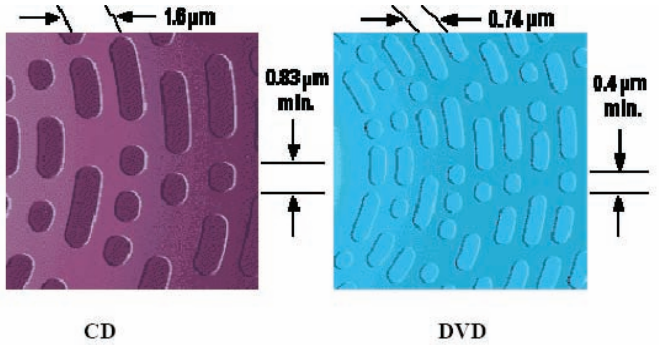
- DVD-ROM, medijum visokog kapaciteta za skladištenje podataka;
- DVD-Video, medijum za skladištenje video podataka;
- DVD-Audio, jedini digitalni audio format za skladištenje;
- DVD-R, obezbeđuje jednokratno upisivanje i višekratno čitanje format za skladištenje podataka;
- DVD-RAM, prvi DVD za pisanje-brisanje podataka;
- DVD-RW i DVD+RW, savremeni DVD za pisanje-brisanje podataka.

Savremeni DVD imaju iste fizičke dimenzije kao CD, ali postoje i manje dimenzije za digitalne video kamere. U odnosu na kapacitet skladištenja razlikuju se četiri sub-formata DVD, (slika 4.4).

Naziv	Kapacitet [GB]	Slojevi	Strane	Komentari
DVD-5	4,7	1	1	Jednostrani sloj
DVD-9	8,54	2	1	Dvoslojni
DVD-10	9,4	1	2	Dvostrani
DVD-18	17,08	2	2	Dvoslojni/Dvostrani

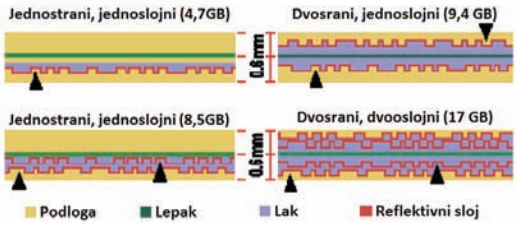
Slika 4.4 *Pod-formati DVD diskova*

Iako se DVD na prvi pogled lako može zameniti sa CD, znatno veći kapacitet DVD je očigledan. Veća gustina pakovanja nosilaca binarnog zapisa omogućava veći kapacitet DVD, što je prikazano na slici 4.5.



Slika 4.5 *Pakovanje binarnih nosioca na CD i DVD disku*

Tragovi za snimanje podataka postavljeni su bliže, što omogućava smeštanje znatno više imnogo manjih šupljina po tragu, tako da bi ispruženi spiralni trag DVD diska dostigao dužinu od 11km. Ovo je, ipak, lakši deo u povećanju kapaciteta DVD diska. Glavna tehnologija odnosi se na način rada lasera. Prečnik laserskog snopa kod DVD diskova smanjen je u odnosu na lasere za CD diskove sa 780nm na 680nm. Pored toga DVD tehnologija dopušta snimanje/čitanje na više slojeva, što se omogućava refokusiranjem lasera kroz površinski sloj na niži sloj. Zato su šupljine na donjem sloju nešto ređe (manje su kompaktne) nego na površinskom sloju, zbog čega nije isti kapcitet skladištenja na oba sloja. Ako DVD ima dva sloja, snimanje počinje na površinskom sloju po spiralnom tragu od centra prema periferiji, a zatim prelazi na donji sloj po tragu od periferije prema centru diska. Slična akcija odvija se i kod dvostranog DVD diska, (slika 4.6), [24].



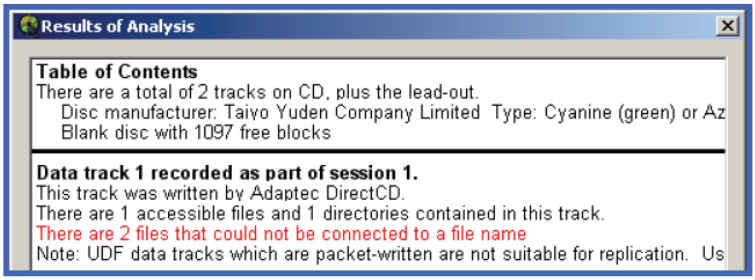
Slika 4.6 *Struktura DVD diskova različitih kapaciteta*

Svi tipovi DVD koriste UDF fajl sistem, ali podržavaju i ISO 9660 standard fajl sistema. Za čitanje DVD potrebno je imati DVD plejer, ili računar sa ugrađenim DVD-ROM drajvom, zajedno sa odgovarajućim softverom. Pri tome se mora voditi računa o kompatibilnosti. Neka osnovna pravila ove kompatibilnosti su:

1. DVD-RAM diskovi kompatibilni su samo sa DVD-RAM drajvovima.
2. Savremeni DVD-ROM drajvovi mogu čitati DVD-RW i DVD+RW diskove, pa zajednički fajl ne bi trebao da bude problem.
3. Moderni DVD–R drajvovi mogu čitati DVD-ROM, CD, CD-ROM, CD-R i CD-RW diskove, a većina može čitati podatke sa CD kao i DVD.
4. DVD+RW format drajv može generalno čitati DVD-RW disk, ali ne može upisivati u njega i obrnuto.
5. Najnoviji DVD plejeri mogu čitati RW i RW+ formate. Stariji plejeri bolje rade sa RW+, što nije uvek slučaj.

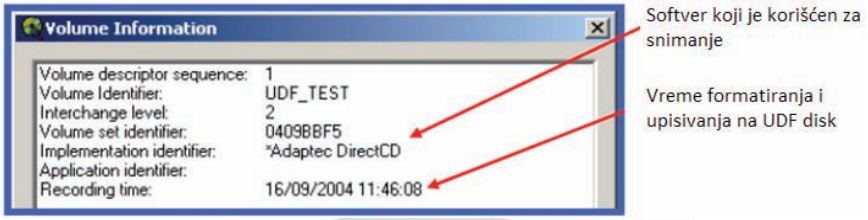
Sa forenzičkog aspekta važno je da forenzičar pouzdano identifikuje tip medijuma sa kojim radi. Jedna od mogućnosti je pažljivo ispitivanje nalepnice na disku, ali je teško razlikovati originalne i piratske diskove, zbog kvaliteta tehnologije za printovanje na disku. Na ovaj način može se identifikovati razlika između CD i DVD. Potrebno je razlikovati i CD i DVD diskove za jednokratno i višekratno upisivanje, što se može pročitati sa nalepnice blizu centra diska. Takođe, gledanjem diska prema svetlu moguće je videti da li je disk upisan, da li je jedno-sesijski, ili više-sesijski.

Postoji mnogo softverskih aplikacija koje pomažu u identifikaciji CD i DVD tipova diskova. Primer forenzički korisnih informacija koje se mogu dobiti sa CD korišćenjem ovih aplikacija prikazan je na slici 4.7.



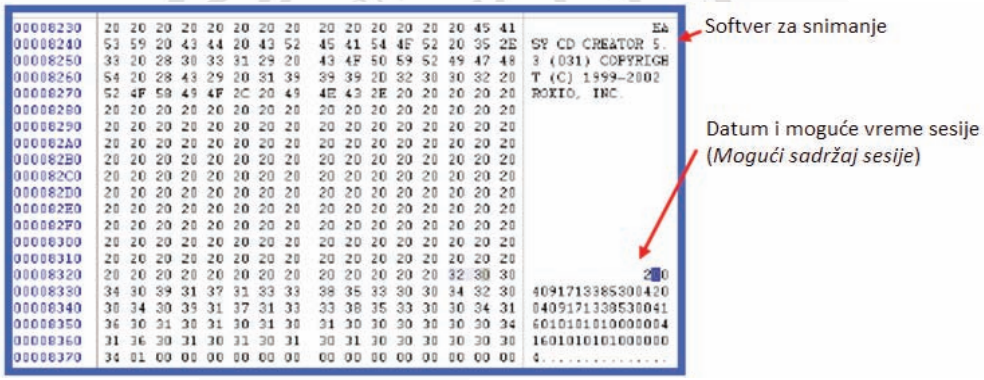
Slika 4.7 *Tip informacija o CD dobijen softverskim alatom*

Kada forenzičari rade sa ovakvim tipovima medijuma, korisno je najpre napraviti kopiju osumnjičenog diska i nikada pokušavati raditi sa originala. Ako ovo nije moguće, uvek treba koristiti CD-ROM drajv računara, radije nego neki čitač. Upotrebom istih alata mogu se naći informacije ilustrovane na slici 4.8.



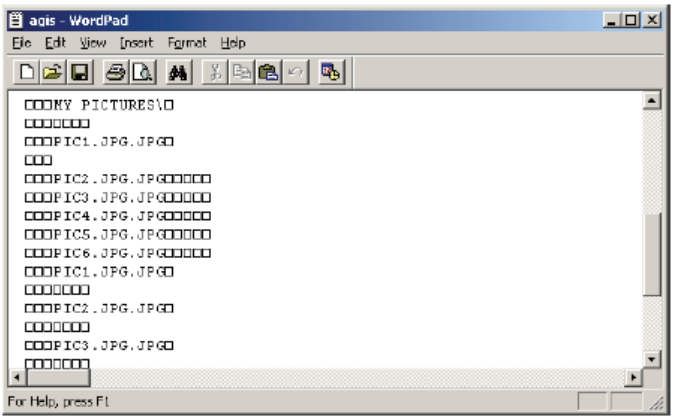
Slika 4.8 *Informacije o logičkoj particiji diska*

Izvlačenje ovog tipa podataka vrlo mnogo zavisi od toga koja je softverska aplikacija korišćena u procesu snimanja diska i procesu oporavka podataka. Na slici 4.9 prikazane su dijagnostičke informacije izvučene iz CD-R diska.



Slika 4.9 *Dijagnostičke informacije sa CD-R diska*

Većina CD/DVD aplikacija za snimanje ima log fajlove, koji mogu obezbediti neke korisne informacije o sadržaju podataka upisanih na disk. Na slici 4.10 prikazan je sadržaj 15 fajlova upisanih sa *EasyCD Creator V.5* rezačem.



Slika 4.10 *Sadržaj fajla upisanog sa EasyCD Creator V.5 rezačem*

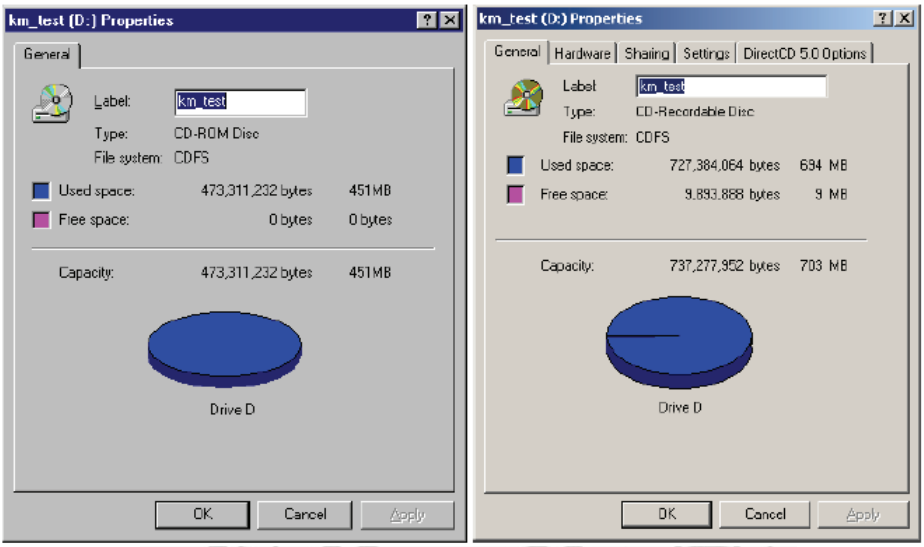
Kako neke aplikacije za snimanje treba da kreiraju sliku fajlova podataka pre upisivanja na disk, moguće je da slika fajlova postoji na HD. Druge aplikacije daju korisniku mogućnost da izabere ovu opciju. Treba pretražiti fajlove sa ekstenzijom .cif, .iso i .nrg.

Postoji, takođe, mogućnost oporavka informacija o vremenu i datumu. Ovo mogu biti informacije o sistemskom vremenu i datumu, ili vreme i datum koje je softver za snimanje dao nekoj sesiji. Neke softverske aplikacije daju korisniku izbor koje vreme i datum da koristi. Pri tome treba biti vrlo pažljiv i proveriti sistemski časovnik i kako aplikacija sinhronizuje vreme. Na slici 4.11 prikazana je opcija za korisnički izbor vremena i datuma u *EasyCD Creator* rezaču.



Slika 4.11 *Opcije vremena u rezaču EasyCD Creator*

Neki drajvovi ne pokazuju sve podatke koje CD ili DVD sadrži. U stvari, kako će neki disk biti očitan, zavisi od metoda snimanja i kompatibilnosti CD ROM čitača. Na slici 4.12 prikazan je isti CD očitan sa različitim drajvovima (čitačima), [24].



Slika 4.12 *Različito očitavanje istog CD na različitim drajvovima*

Posebno, ako se čita CD, a nije instaliran softver za upisivanje paketa, tada će se videti prazan disk. Druge mogućnosti uključuju više-sesijski disk, neki otvoreni UDF disk, ili neki disk koji je podvrgnut procesu 'pregrevanja' (*overburning)*.

Forenzičar, takođe, mora imati na umu da se struktura fajla kod DVD-Video diskova razlikuje od drugih formata, (slika 4.13).



Slika 4.13 *Struktura fajlova DVD*

Prvi direktorijum na disku mora biti VIDEO_TS direktorijum koji sadrži sve fajlove i koji ne sme biti veći od 1GB. VIDEO_TS i AUDIO_TS su obavezni direktorijumi. Fajlovi koji se ne zahtevaju za DVD-Video, ili DVD–Audio biće sadržani u drugim direktorijumima i koji će se koristiti kada se to zahteva.

Budućnost ovih medijuma leži u DVD tehnologijama, uz produženi 'rat formata' glavnih proizvođača diskova – *Blu-Ray* i *HD-DVD*. Postoje nagoveštaji da će *HD-DVD* verovatno preovladati zbog niže cene. Oba koriste

slične laserske tehnologije, ali različite po načinu upisivanja podataka, a kapacitet *Blu-Ray* formata je mnogo veći. Različiti kapaciteti ova dva formata prikazani su u tabeli 4.1.

Tabela 4.1 Različiti kapaciteti dva formata DVD diskova

KAPACITET	
BLU – RAY	**HD – DVD**
Jenoslojni ROM 25GB	Jenoslojni 15GB
Dvoslojni ROM 50GB	Dvoslojni 30GB
Jenoslojni RW 27GB	Neprimenjivo
Dvoslojni RW 54GB	Neprimenjivo
Najveći test 100GB	45GB
Teoretsko ograničenje 200GB	60GB

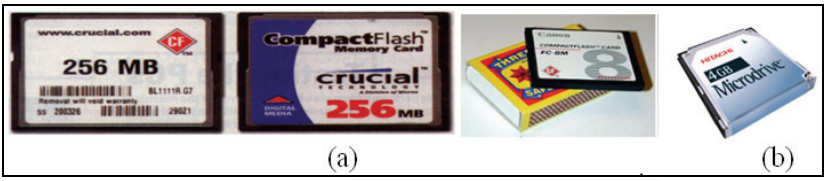
4.3 Fleš memorije

Termin '*fleš memorija*' koristi se da označi brzo i lako skladištenje podataka na različite digitalne, kompaktne uređaje bez pokretnih delova, koji mogu zadržati uskladištene podatke bez konstantnog napajanja. Može se koristiti kao pokretna memorija-kompakt fleš kartica, ili nepokretna memorija-mobilni telefon, MP3 plejer itd. Prednosti fleš memorije u odnosu na HD je što radi bešumno, nema pokretnih delova, omogućava brže čitanje/pisanje, lakši su, manje veličine i lakše se sakrivaju. Nedostaci su veća cena i ograničen kapacitet. Međutim, cene sve više padaju, a kapacitet se povećava. Ključni tehnički elementi koji obezbeđuju rad fleš memorije su: *plivajuća vrata, tranzistori, kvantno tunelovanje i vruće inektiranje elektrona*. U suštini, podaci se skladište u slojeve, izmenom broja elektrona koji se može uskladištiti u svaku pojedinačnu lokaciju. Postoje određena ograničenja u korišćenju ove tehnologije, a najviše se odnose na broj ciklusa brisanja, tipično između 10 000 i 1 000 000, koji se može izvršiti pre nego što medijum postane nestabilan.

Generalno, fleš memorija koristi *pseudo* FAT fajl sistem za skladištenje podataka, iako brojni fajl sistemi, uključujući i NTFS podržavaju fleš memorije, što znači da će se direktorijumi i struktura fajlova veoma razlikovati od onih u Windows sistemu.

1.1.1. Identifikovanje fleš memorija

Kompakt fleš u poređenju sa drugim tipovima fizički je veći, približno veličine kutije šibica. Postoje dva standarda kompakt fleš memorije: *tip 1CF* kapaciteta 2 GB, (slika 4.14a) i *tip 2CF* znatno su većeg kapaciteta do 8 GB, koji je malo deblji, (slika 4.14b), [24]**.**



Slika 4.14 *Tipovi kompakt fleš memorija*

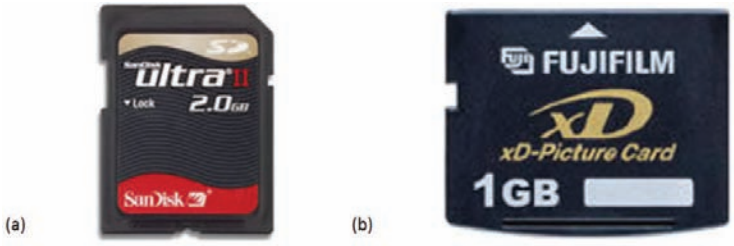
Smart media (*Toshiba),* poznat kao *čvrsti flopi disk – SSFD,* relativno je veći, ravan, fleksibilan i lomljiv, zbog primenjene tankoslojne tehnologije pakovanja. Vrlo su tanki i lako se sakrivaju. Tekući kapacitet je ograničen na 128 MB, (slika 4.15).



Slika 4.15 *Iomega smart media i tipovi multi-media fleš memorija (a, b)*

Multi-Media Card (*MMC*) proizvodi se u dve varijante: MMC kapaciteta do 128MB (slika 4.15a) i MMC+ do 1GB, (slika 4.15b). Obe su veličine poštanske marke, dugotrajne, čvrste i lako se sakrivaju.

Bezbedna digitalna kartica (*SD*) direktna je zamena MMC, slične veličine, ali neznatno deblja, kapaciteta do 2GB. Na raspolaganju je i mini SD. Obezbeđuje zaštitu autorksih prava i poseduje prekidač za sprečavanje upisivanja, (slika 4.16a).



Slika 4.16 *Bezbedna digitalna kartica (a) i xD-Picture kartica (b)*

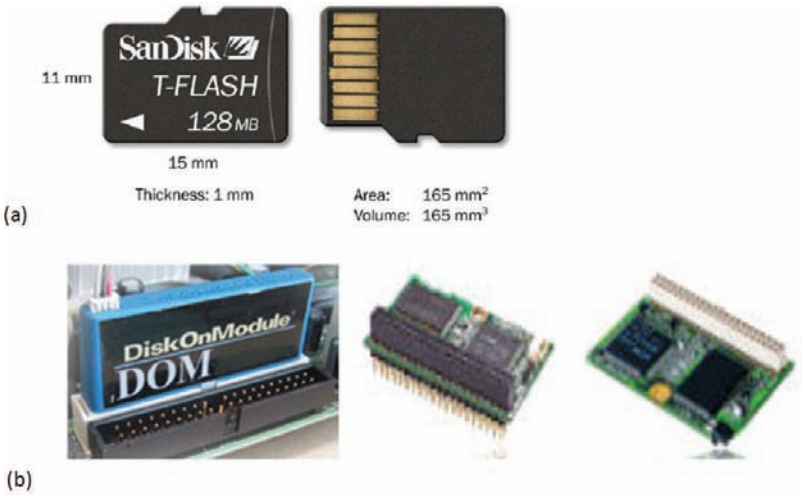
xD-Picture kartica originalno dizajnirana u *Fuji*-u, za njihove digitalne kamere, trenutno su najmanje od vodećih kartičnih formata. Dizajnirana sa prekidačem za zaštitu od upisivanja i sa kapacitetom od 2GB, a teoretski mogu uskladištiti do 8 GB, (slika 4.16b).

Memorijski stikovi originalno su razvijeni u *Sony* korporaciji. Proizvode se u dva glavna oblika. Standardni oblik je veličine pakovanja žvakaće gume, a manji je upola te veličine. Oba tipa se proizvode sa zaštitom od upisivanja i kapacitetom do 4GB. Profesionalna verzija ima brzinu prenosa podataka od 15Mb/s, što obezbeđuje skoro DVD kvalitet video signala u realnom vremenu. Proizvode ih brojne kompanije u svetu, ali su svi tipično sličnog oblika, (slika 4.17).



Slika 4.17 *Tipovi memorijskih stikova*

Trans-fleš (T-fleš) kartice relativno su novijeg datuma, ultra male veličine, dizajnirane kao polu-prenosne memorije za mobilne telefone i digitalne kamere. Nisu namenjene za česta pomeranja. Mogu ih koristiti skoro svi SD uređaji sa adapterom. Imaju kapacitet od 512MB do 1GB. Na slici 4.18a prikazane su *Sandisk T-fleš* kartice.



Slika 4.18 *Sandisk T-fleš kartice (a) i DOM tipovi fleš memorije (b)*

DiskOnModul(DOM), nedavno razvijen, 100% je kompatibilan sa IDE ATA interfejsom, radi potpuno jednako kao i čvrsti disk, ali bez ikakvih pokretnih delova, što veoma povećava brzinu i pouzdanost rada bez šuma i brzinu pristupa podacima. Imaju kapacitet do 2GB, (slika 4.18b).

Iomega Peerless bazirane na čvrstom disku *IBM TravelStar notebook*-a, koriste *fireware*/USB konektore i ne razmenjuju podatke sa memorijom (nemaju *swap* fajl). Proizvode se u jedinicama kapaciteta od 10GB i 20GB, (slika 4.19a).



Slika 4.19 *Tipovi Iomega Peerless USB fleš memorija (a) i tipovi PQI inteligentnih USB stikova (b)*

PQI Inteligentni stik je nova generacija fleš memorija, konstruisana sa ugrađenim USB adapterom. Visoko je adaptivan i radi gotovo sa svakim USB portom, bez obzira na OS. Imaju kapacitet do 1GB, (slika 4.19b).

Data Play za reprodukciju podatakau ekstremno je mali optički disk, dizajniran za skladištenje muzike. Može se koristiti za jednoktratno unošenje podataka, kao ROM i kao hibrid ova dva. Zahteva specijalni čitač. Proizvođači garantuju životni vek arhiviranih podataka do 100 godina. Imaju kapacitet od 350MB, (slika 4.20a). Na slici 4.20b prikazano je nekoliko tipova uređaja sa ugrađenom fleš memorijom, koje osumnjičeni mogu koristiti za skrivanje kompromitujućih sadržaja.

(a)



(b)



Slika 4.20 *Data play optički disk (a) i tpovi predmeta sa ugrađenom fleš memorijom (b)*

REZIME

Kompakt diskovi (CD) se redovno koriste za skladištenje podataka i forenzičari ih nalaze u istrazi. Generalno se mogu klasifikovati u dve glavne kategorije: *samo za čitanje* (*Read Only*) ili fabrički presovani: *CD-DA* ili muzički CD i *CD-ROM* ili CD za podatke i *za pisanje i čitanje* (*Recordable*): *CD-R* (*Recordable*), *CD-RW* (*Rewritable*). CD-ovi razlikuju se po fizičkoj kompoziciji, načinu skladištenja podataka i fizičkom izgledu. Zajednička im je veličina - debljina 1,2mm i prečnik 12cm. Standardna dimenzija CD odstupa u pogledu prečnika (manjeg) i oblika diska (veličine kreditne kartice). CD skladišti podatke po neprekidnoj spirali koja počinje od centra diska. Širina spirale je 0,5 mikrona, a spirale su razmaknute 1,6 mikrona. Podaci se sa diska čitaju sa laserom usmerenim na disk, a meri se reflektovana svetlost. Smanjenjem širine laserskog snopa za upisivanje/čitanje smanjuju se širina spirale i razmak između tragova spirale, što povećava kapacitet CD sa 650MB na 800MB.

CD za višekratno snimanje podataka (CD-RW) umesto organske boje ima leguru, a laser menja stanje legure – zagrevanjem vrši kristalizaciju u dekristalizaciju i obrnuto. Ovaj proces, poznat kao tehnologija promene optičke faze (*Optical Phase Change Technology*), koristi različite vrste polimera u konstrukciji diska koji različito reaguju na temperaturu laserskog zraka, što omogućava čitanje, pisanje i brisanje diska. Za CD-RW zahteva se namenski drajv sa softverom za paketsko upisivanje.

Postoje tri glavna tipa fajl sistema CD, koji se razlikuju u pogledu podrške dužine imena fajla i kako se podaci stvarno skladište: *ISO 9660, Joliet* i *UDF* (*Universal Disk Format*) ili *ISO 13346*, koji se najčešće koristi, jer prevazilazi sve probleme standarda ISO 9660, omogućavajući inkrementalno dodavanje jednog po jednog fajla CD-Ru i CD-RWu, koristeći tehnologiju upisivanja paketa.

Od 1995 razvijeno je više formata DVD: *DVD-ROM***,** visokog kapaciteta za skladištenje podataka; *DVD-Video***,** za skladištenje video podataka; *DVD-Audio*, jedini digitalni audio format za skladištenje; DVD-R, obezbeđuje jednokratno upisivanje i višekratno čitanje podataka; *DVD-RAM*, prvi DVD za pisanje-brisanje podataka; *DVD-RW i DVD+RW*, savremeni DVD za pisanje-brisanje podataka. Kapacitet DVD kreće se od 4,7 do 17,08GB.

Sa forenzičkog aspekta važno je da forenzičar pouzdano identifikuje tip medijuma sa kojim radi. Jedna od mogućnosti je pažljivo ispitivanje nalepnice na disku, ali je teško razlikovati originalne i piratske diskove, zbog kvaliteta tehnologije za printovanje na disku. Na ovaj način može se identifikovati razlika između CD i DVD. Potrebno je razlikovati i CD i DVD diskove za jednokratno i višekratno upisivanje, što se može pročitati sa nalepnice blizu centra diska. Takođe, gledanjem diska prema svetlu moguće je videti da li je disk upisan, da li je jedno-sesijski, ili više-sesijski.

Većina CD/DVD aplikacija za snimanje ima log fajlove, koji mogu obezbediti neke korisne informacije o sadržaju podataka upisanih na disk. Treba pretražiti fajlove sa ekstenzijom **.cif, .iso** i **.nrg**., a postoji, mogućnost oporavka informacija o vremenu i datumu, zavisno od primenjene aplikacije za snimanje.

Forenzičar, mora imati na umu da se struktura fajla kod DVD-Video diskova razlikuje od drugih formata i da obrati pažnju na diskove snimljene pregrevanjem za povećanje kapaciteta. Prvi direktorijum na disku mora biti **VIDEO_TS** direktorijum koji sadrži sve fajlove i koji ne sme biti veći od 1GB. **VIDEO_TS** i **AUDIO_TS** su obavezni direktorijumi. Fajlovi koji se ne zahtevaju za DVD-Video, ili DVD-Audio biće sadržani u drugim direktorijumima i koji će se koristiti kada se to zahteva.

Fleš memorija brzo i lako skladišti podataka na različite digitalne, kompaktne uređaje bez pokretnih delova, koji mogu zadržati uskladištene podatke bez konstantnog napajanja. Može se koristiti kao pokretna memorija-kompakt fleš kartica, ili nepokretna memorija-mobilni telefon, MP3 plejer itd., rade bešumno, nemaju pokretnih delova, omogućavaju brže čitanje/pisanje, lakši su, manje veličine i lakše se sakrivaju u poređenju sa HD. Nedostaci su veća cena i ograničen kapacitet. U suštini, podaci se skladište u slojeve, izmenom broja elektrona koji se može uskladištiti u svaku pojedinačnu lokaciju. Postoje određena ograničenja u korišćenju ove tehnologije, a najviše se odnose na broj ciklusa brisanja, tipično između 10 000 i 1 000 000. Kapaciteti fleš memorija sve su veći i kreću se i do nekoliko desetina GB i potencijalno mogu zameniti HD zbog svojih prednosti.

Generalno, fleš memorija koristi *pseudo* FAT fajl sistem za skladištenje podataka, iako brojni fajl sistemi, uključujući i NTFS podržavaju fleš memorije, što znači da će se direktorijumi i struktura fajlova veoma razlikovati od onih u Windows sistemu.

UNIVERZITET
PRIVATNI
AKREDITOVANI
UNIVERZITET
SINGIDUNUM

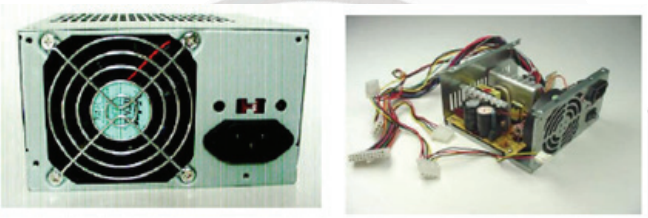
PITANJA ZA PONAVLJANJE

1. Koja se tri tipa fizičkih medijuma najčešće susreće u radu forenzičara?
2. Koja su tri najčešća fajl sistema na CD medijima?
3. Zašto je uveden UDF fajl sistem?
4. Koji se podaci mogu izvući iz CD medija?
5. Koja su dva fizička formata DVD?
6. Nabrojte 5 recordable formata?
7. Koja su dva DVD fajl sistema.
8. Nabrojte 6 procesa za uspešno butovanje NT sekvence?
9. Kojih je sedam fajlova uključeno u NT proces butovanja?
10. Koji su drugi procesi uključeni u NT sekvencu butovanja?
11. Koja dva fajla se koriste samo ako se zahtevaju?
12. Koja dva fajla NISU bitna za uspešno DOS butovanje?

5 HARDVERSKE KOMPONENTE RAČUNARA

Digitalni forenzičar treba da dobro poznaje terminologiju, tipove i osnovne funkcije uobičajenih hardverskih komponenti računarskog sistema.

Jedinica za napajanje (PSU[3]), snabdeva električnom energijom računar i njegove komponente, konvertujući naizmeničnu u jednosmernu struju potrebnu za rad komponenti računara, (slika 5.1).



Slika 5.1 *PSU – jedinca za napajanje računara*

Konektor PSU je standardizovan sa višebojnim žicama i teško ga je pogrešno spojiti. U toku razvoja računara nastalo je 6 različitih industrijskih standarda PSU. Tekući standard je ATX, dizajniran da odgovara svim ATX kućištima i ima električne karakteristike za korišćenje sa svim ATX glavnim pločama. Savremene PSU imaju snagu do 650W.

Kako se komponente računara oslanjaju na vrlo finu kontrolu nisko naponskog napajanja, u radu sa računarom značajno je obratiti pažnju na statički elektricitet, koji nastaje prirodnim pražnjenjem opterećenja vrlo visokog napona. Ljudski organizam je odličan provodnik pa u radu sa računarom digitalni forenzičar mora imati na umu efekte statičkog elektriciteta. Mnoge komponente računara sadrže mikroskopske električne komponente i prekidače, koji zahtevaju stabilan nivo napona napajanja. Kada forenzičar dodirne komponentu golom rukom uvek postoji statičko opterećenje koje se može isprazniti kroz osetljivu komponentu i uništiti je. Mere predostrožnosti od oštećenja komponenti računara statičkim ekektricitetom idu od koiršćenja antistatičke navlake za prst gde se kablom

[3] PSU- *Power Suply Unit*

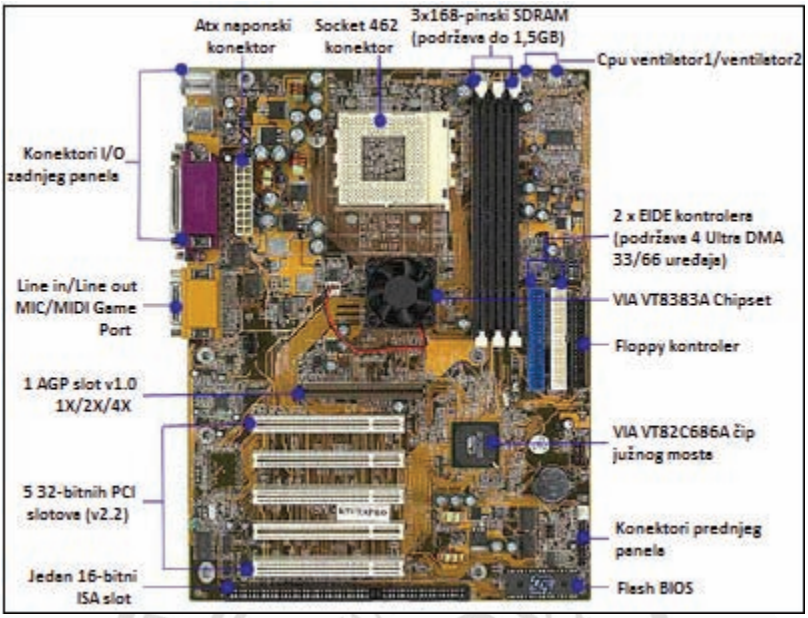
statički elektricitet odvodi u zemlju, do korišćenja antistatičkog seta: uzemljene podloge i radni stolovi sa antistatičkom navlakom za prst, (slika 5.2).



Slika 5.2 *Antistatička oprema forenzičke laboratorije*

Najbolje, ali i najskuplje rešenje je izgradnja kompletne antistatičke laboratorije za digitalnu forenzičku analizu, gde se antistatički elementi regularno testiraju.

Glavna ploča je glavna komponenta računara, koja omogućava napajanje i međusobnu komunikaciju svih delova računara. Sama za sebe glavna ploča ne znači ništa, njen glavni zadatak je da nosi glavni mikroprocesor i omogućava svim komponentama računara da se povežu na njega. Sve komponente računara u stvari su deo glavne ploče, ili su povezane na nju preko konektora. Na slici je tipična ATX glavna ploča, (slika 5.3), [33].



Slika 5.3. Tipična ATX glavna ploča

Tip glavne ploče određuje brojne faktore kao što su tip i veličinu RAMa, tip mikroprocesora i koliko perifernih komponenti se može povezati na računar. Ovo je odlučujući faktor koji omogućava korisniku da nadogradi i modernizuje računar. Forma glavne ploče – *oblik, veličina i raspored elemenata,* utiču na to gde se instaliraju komponente i na oblik kućišta računara. Najčešća forma glavne ploče je ATX i Mini ATX, između nekoliko poznatih tipova, [33].

BIOS (*Basic Input Output System*) – osnovni ulazno-izlazni sistem izgrađen je u softveru uskladištenom u čipu ROM (*Read Only Memory*) memorije, obično locirane na glavnoj ploči. BIOS određuje šta računar može raditi bez instalacije operativnog sistema, ili druge softverske aplikacije, dovodi računar iz isključenog stanja u položaj gde instalirani OS može nastaviti podizanje (*butovanje*) sistema i obezbeđuje da svi drugi čipovi, procesori, portovi i povezani uređaji komuniciraju jedni sa drugima i zajedno funkcionišu. BIOS obezbeđuje rutine na niskom nivou za povezivanje OS sa drugim hardverskim uređajima. Neke komponente računara, kao kontroleri diska i SCSI kartice imaju sopstveno BIOS setovanje. Kako je BIOS uskladišten u ROM čipu, podaci su uvek na raspolaganju i ne zavise od nestanka napajanja, ili kvara

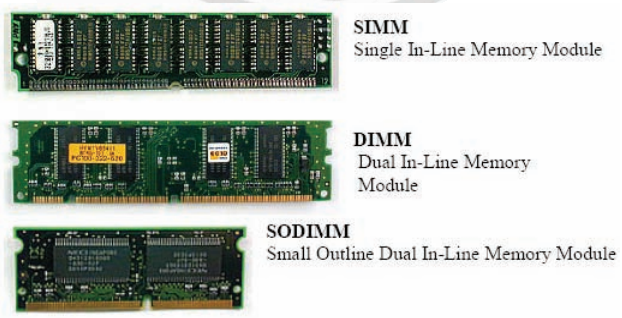
HD. Većina savremenih BIOSa uskladištena je na specijalnom tipu skalabilnog ROM čipa, tzv. čipa fleš memorije (*fleširanje* BIOSa).

CMOS (*Complimentary Metal Oxide Semiconductor*) je tip integrisanog kola koji koristi vrlo malu snagu, emituje malo toplote za razliku od drugih čipova i klasifikovan je kao osetljiva memorija. Da bi sačuvao podatke zahteva konstantno napajanje sa malom baterijom smeštenom na glavnoj ploči. CMOS sadrži i čuva sledeće podatke, [24]:

1. sistemski datum i vreme,
2. sekvencu butovanja,
3. specifilaciju drajva i
4. pasvord.

BIOS i CMOS rade zajedno na podizanju OS računara, ali su različite komponente. BIOS pokreće sistem, izvršava ključne funkcije startovanja sistema, kao što je samo-testiranje napajanja komponenti računara – POST (*Power On Self-Test*), testiranje integriteta sistema i upoređuje sve ovo sa podacima u CMOS čipu. CMOS jednostavno skladišti podatke koji se odnose na hardver računara.

RAM (*Random Access Memory*) je tip privremene memorije i koristi je OS da ubrza povezivanje između uređaja i aplikacija. Za funkcionisanje, RAM zahteva konstantno napajanje da bi zadržao uskladištene podatke. CPU – *centralna procesorska jedinica* ima direktan pristup RAM-u i oni uzajamno čitaju i upisuju podatke. Postoji više tipova formi RAM-a. Na slici 5.4 su tri najčešća tipa RAMa.

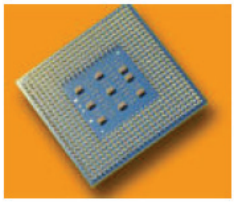


Slika 5.4 *Najčešći tipovi RAM memorija*

BUS (magistrala) je podsistem u arhitekturi računara koji prenosi podatke, ili napajanje između komponenti računara i može logički povezati nekoliko komponenti preko istog kola. Svaki ***bus*** definiše sopstveni skup konektora za fizičko priključivanje uređaja i komponenti na glavnu ploču. Postoje interni i eksterni *bus*, a uobičajeni su:

1. ISA (Industry Standard Architectures),
2. PCI (Peripheral Component Interconnect) i PCI Express,
3. MCA (MicroChannel),
4. VESA (Video Electronics Standards Association),
5. AGP (Accelerated Graphics Port),
6. ATA (Advanced Technology Attachment),
7. SCSI (Small Computer System Interface),
8. USB (Universal Serial Bus),
9. SATA (Serial Advanced Technology Attachment),
10. *Fireware* – IEEE 1394 standard.

Centralna procesrska jedinica - CPU ***(****Central Processing Unit****),*** ili mikroprocesor interpretira i procesira instrukcije i podatke sadržane u softverskim aplikacijama i drugim komponentama. Proizvodi se u jednom čipu od prvog mikroprocesora 1970. godine – *Intel 4004.* Do danas su povećane kapacitet, kompleksnost i konstrukcija, ali je osnovni dizajn ostao nepromenjen, (slika 5.5).



Intel Pentium 4



AMD Athlon 64

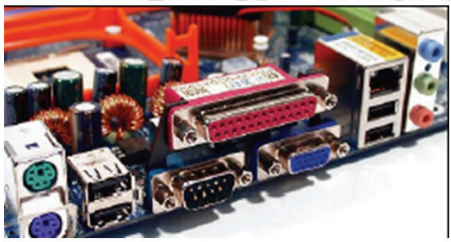
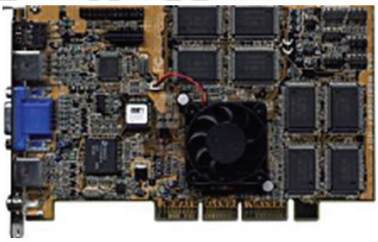
Slika 5.5 *Tipovi CPU*

CPU se spaja na glavnu ploču umetanjem u ugrađenu utičnicu (*socket*). Postoje dva glavna tipa utičnica:

- *ZIF Socket* (*Zero Insertion Force*) kod savremenih glavnih ploča, gde se CPU lako ubacuje i drži se feder-polugom, koja ga izbacuje kada se poluga podigne.
- *LIF utičnica* (*Low Insertion Force*), ili standardna utičnica koja zahteva neznatni pritisak za umetanje CPU, a zahteva specijalni alat za vađenje CPU.

Grafičke karte, ili grafički adapteri obezbeđuju vizuelni prikaz rezultata rada računara na ekranu monitora. Postoje tri tipa grafičkih adaptera:

Grafička karta na glavnoj ploči, koja koristi RAM kao skladište i pokazuje slabije performanse od nezavisnih adaptera, (slika 5.6a).

(a)  (b) 

Slika 5.6 *Grafička karta na glavnoj ploči (a) i PCI grafički adapter (b)*

PCI grafički adapter, povezuje se sa glavnom pločom preko slobodne PCI *slot*-utičnice, obično ima svoj RAM i mikroprocesor. Troši najveći deo procesorske snage CPU i memorije računara. Generalno je spor, jer ograničava brzinu transfera podataka, pa je zamenjen sa *PCI Express slotom*, koji obezbeđuje daleko brži transfer podataka i veće grafičke kapacitete i postaje standard savremene grafičke karte, (slika 5.6b).

AGP grafički adapter, povezuje se sa glavnom pločom preko namenskog SGP slota. Ima svoj RAM i procesor. Radi brže od PCI adaptera zbog načina

transfera podataka kroz namenski AGP slot. Postoji šest verzija AGP adaptera: *AGP1x, AGP2x, AGP4x, AGP8x, AGPPro i 64bitni AGP.*

Tehnologija monitora brzo je napredovala poslednjih 25 godina - od prvih monitora, crnih i zelenih displeja, preko savremenih sa velikim brojem boja, do grafičkih akceleratora koji mogu prikazati do 16,8 miliona različitih nijansi boja i imaju ekrane sa vrlo velikom rezolucijom.

DVI-Digitalni video interfejs je najnoviji proizvod u grafičkoj tehnologiji. Obezbeđuje komunikacije između monitora, grafičkih kartica, video i foto digitalnih kamera i prikazivanje aplikacija visoke rezolucije na ravnim ekranima, sa visokim propusnim opsegom i redukcijom interfejsa.

Tastature i miševi obezbeđuju korisniku unos podataka u računar, opštu interakciju sa računarom i kontrolu brojnih funkcija računara. Tastature se proizvode u brojnim oblicima i veličinama, ali sve rade na istim osnovnim principima – sastoje se od serije prekidača spojenih na mali mikroprocesor koji monitoriše stanje svakog prekidača, a zatim inicira specifični odgovor. Generalno, tastature se proizvode u dva tipa sa: *101 poboljšana ključa* i *104 Windows poboljšana ključa*. Ove tastature povezuju se na računar sa specijalnim konektorima, [34]:

1. 5-pinski DIN standarda,
2. 6-pinski PS/2 mini DIN standarda,
3. 4-pinski USB i
4. Laptop konektor za interno spajanje tastature.

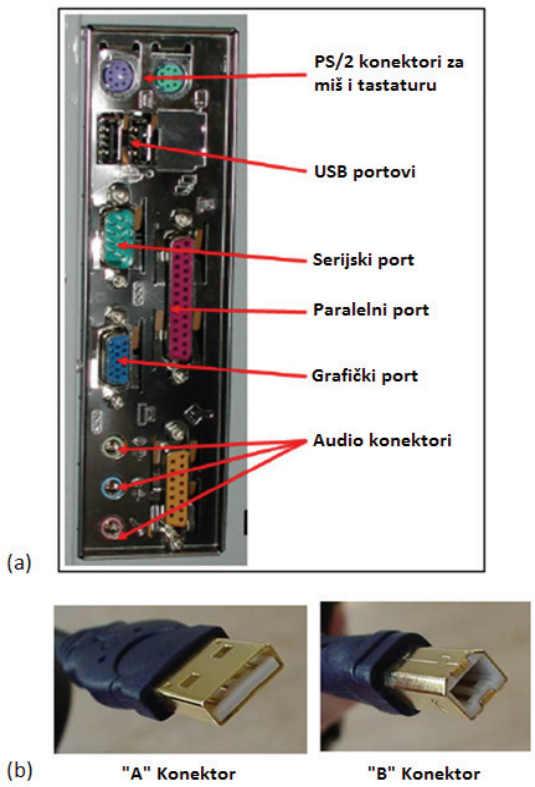
Poslednja verzija dizajna tastature je *holografska tastatura*, još u ranoj fazi razvoja, koja će potisnuti sve poznate tastature. Holografska slika projektuje se na površinu ispred korisnika. Akcije korisnika prekidaju se korišćenjem tehnologije detekcije kolizije, koja simulira kucanje na tastaturi, (slika 5.7), [24].



Slika 5.7 *Neki tipovi tastatura: ergonomska, jednoručna standardna i holografska*

Miš je hardverski uređaj koji obezbeđuje korisniku da kontroliše kursor za manipulaciju podataka bez upotrebe komplikovanih komandi. Tehnologija proizvodnje miševa počinje 1963. godine. U savremenoj formi, prvi miši je proizveden u kompaniji *Aple* za računar *Lisa* 1984. godine, a danas se proizvodi u tri tipa: *mehanički, optički i optičko-mehanički,* sa prednostima i nedostacima i mogućih pet načina spajanja na računar: *serijski port, PS/2 port, infracrveni, USB i Bluteooth*.

Ulazno-izlazni portovi obezbeđuju povezivanje perifernih uređaja na računar i nalaze se na zadnjoj strani računara. Mogu biti direktno povezani na glavnu ploću, ili na odvojenoj karti. Postoji više tipova portova, (slika 5.8a).



Slika 5.8 *Vrste portova (a) i tipovi standarda USB (b)*

Serijski portovi (COM) su bi-direkcionalni i prenose podatke bajt-po-bajt iz/u računar, koristeći za to različite pinove u konektoru. Prednost je što zahteva samo jednu žicu za prenos podataka. Nedostatak je spor prenos podataka u

poređenju sa paralelnim portom. Postoje dva tipa konektora – 9-pinski i 25-pinski. Serijski portovi se još uvek koriste za povezivanje većine modema, nekih printera, PDA i digitalnih kamera. Brzina prenosa podataka je do 115Kbps.

Paralelni portovi se često koriste za povezivanje printera, kamera i pokretnih drajvova na računar. Originalno su proizvedeni za povezivanje printera (*IBM, Centronics*), a koriste 25-pinski ženski konektor i 36-pinski muški konektor sa druge strane kabla. Računar na ovaj port šalje/prima podatke bajt-po-bajt, ali se podaci do drugog uređaja prenose paralelno preko 8 pinova, pa je prenos preko ovog porta 8 puta brži od serijskog porta. Postoje tri standarda paralelnog porta koje podržavaju savremeni računari, [24]:

1. **SPP** (*Stndard Parallel Port*) obezbeđuje dvosmernu komunikaciju i dupleksnu vezu koristeći sve raspoložive pinove.
2. **EPP** ***(****Enhanced Parallel Port),* proizveden 1991 za brži prenos podataka, tipično u opsegu 500Kbps-2Mbps, namenjen specifično za eksterne uređaje za skladištenje.
3. **ECP** *(Extended Capability Port),* proizveden 1992 za povećanu brzinu prenosa podataka za printere.

USB (*Universal Serial Bus*) *port* obezbeđuje serijsku konekciju do 127 različitih perifernih uređaja preko jednostrukog lako spojivog konektora na računaru ili habu. USB uređaj može se povezati i odspojiti u svakom trenutku. USB standard koristi dva tipa standarda konektora: **A** i **B**, (slika 5.8b).

Tip **A** USB konektora nalazi se na računaru, a **B** na digitalnom uređaju, što sprečava konfuziju. USB port dopušta najviše 5m dužine kabla, a do 30m preko haba. Tokom razvoja USB diferencirana su tri standarda:

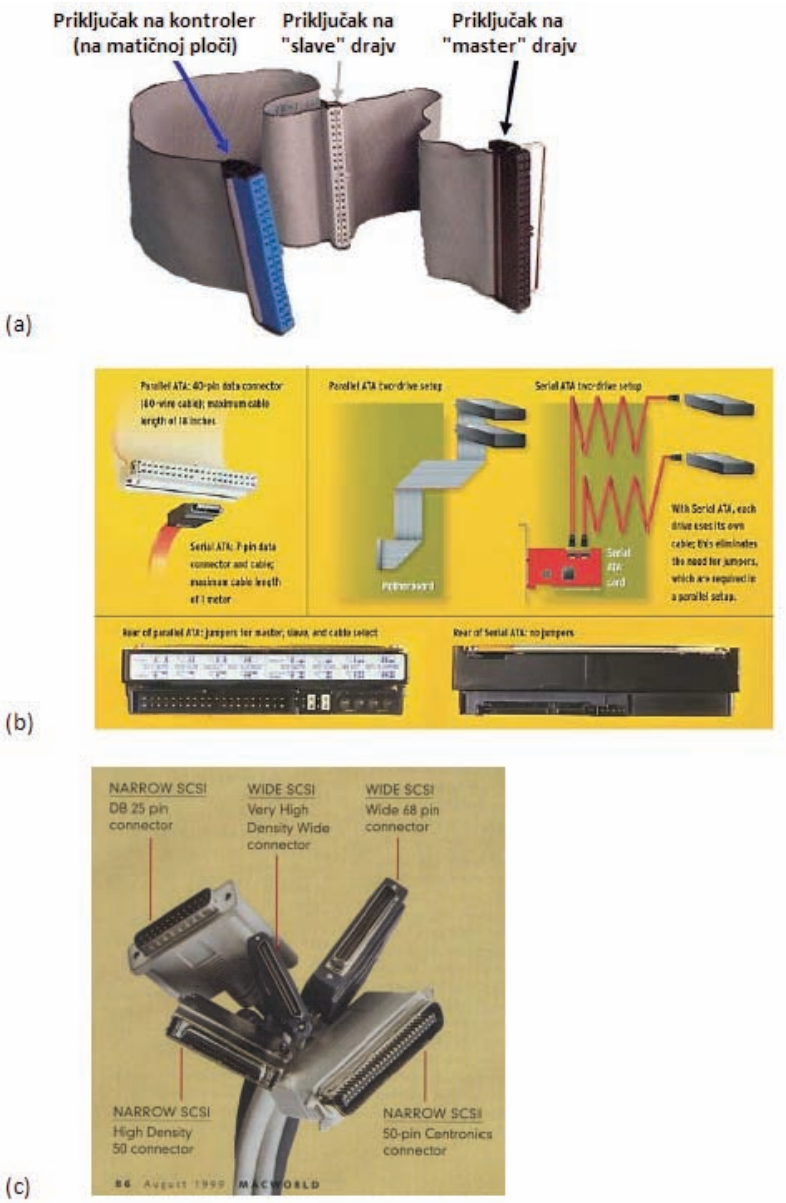
1. **USB1**, sa brzinom prenosa podataka od 1,5 Mbps,
2. **USB1.*1,*** sa brzinom prenosa podataka od 12Mbps,
3. **USB2,** sa brzinom prenosa 480Mbps.

Firewire (1995, *Appl*), standard IEEE 1394 (*High Performance Serial Bus*), vrlo sličan USB, obezbeđuje brzinu prenosa podataka između digitalnih uređaja do 800Mbps, sa potencijalnim povećanjem do 3,2Gbps, kada se prevaziđe problem kabliranja. Dopušta povezivanje do 63 uređaja na *bus* preko *Firewire 400* utičnice u toku rada.

IDE (*Integrated Drive Electronic***)** interfejs je standardni način povezivanja uređaja za skladištenje na računar. Interfejs je originalno deriviran iz IBM AT (*Attachment interface*) – ATA. Većina glavnih ploča opremljena je sa IDE interfejsom, koji je u stvari host adapter i obezbeđuje povezivanje nekog uređaja na računar. Stvarni kontroler je na električnom kolu u kućištu HD drajva. Originalno je razvijen za povezivanje HD drajvova, a zatim je razvijen za spajanje internih FD drajvova, CD-ROM/DVD drajvova i drajva za traku za bekapovanje. Retko se koristi za spajanje spoljnih uređaja. Razvijeno je nekoliko *ATA* standarda sa nasleđivanjem prethodnih kapaciteta:

1. **ATA *1***, originalni standard,
2. **ATA *2***, sa povećanom brzinom prenosa do 16,67Mbps i povećanom podrškom HD do 137,4GB. Često se naziva *Enhanced IDE*;
3. **ATA *3***, uvodi analizu samo-monitoringa i tehnologiju izveštavanja (SMART) i ima veću pouzdanost;
4. **ATA *4***, uvodi glavne dodatke standardu, u dva tipa *Ultra-DMA* i *Integrated AT Attachment Program Interface* (ATAPI) za CD-ROM drajvove itd. Povećava prenos do 33,33Mbps.

Svi IDE uređaji koriste trakasti kabl sa 40 ili 80 žica za spajanje na glavnu ploču. Generalno, nalazi se konektor na svakom kraju kabla i jedan na oko 2/3 dužine za spajanje na glavnu ploču. Kabl ne sme biti duži od 18 inča da bi se održao integritet signala. ULTRA ATA trakasti kabl za prenos podataka prikazan je na slici 5.9.



Slika 5.9 *ULTRA ATA trakasti kabl (a) i SATA interfejs (b) i SCSI interfejs (c)*

Obično, ali ne uvek konektori su kodirani bojom koja ukazuje na povezivanje sa specificiranim uređajem, a svi konektori imaju specifičan „mehanički ključ“ tako da se ne mogu zameniti i pogrešno staviti. Tipične boje su:

1. Plavi konektor, spaja se na glavnu ploču,
2. Crni konektor, spaja se na primarni drajv,
3. Sivi konektor, spaja se na podređeni (*slave*) drajv.

IDE utičnica na glavnoj ploči može podržati dva uređaja. Savremene glavne ploče imaju dualne IDE interfejse i mogu podržati do četiri uređaja. Ako se povezuju dva uređaja na glavnu ploče, jedan se mora proglasiti glavnim (*master*), a drugi podređenim (*slave*), postavljanjem spojki (*jumpers*) na uređajima. Generalno, prvi butabilni uređaj postavlja se za glavni (*master*).

SATA *(Serial ATA) interfejs* sličan USB 2.0 i *firewire* tehnologiji, obezbeđuje znatno veću brzinu prenosa podataka od postojećih ATA standarda. Prva generacija SATA interfejsa omogućava maksimalnu brzinu prenosa podataka do 160Mbps sa potencijalnim povećanjem do 600Mbps. Proizvedene su i glavne ploče sa SATA konektorima, ili se može koristiti dodatni adapter za PCI, ali je brzina ograničena na tekući PCI *bus*. SATA drajv se spaja sa 7-pinskim kablom koji ne može biti duži od 1m i može se povezivati u toku rada računara, (slika 5.10b).

SCSI (*Small Computer System Inerface*) interfejs obezbeđuje brzu komunikaciju između računara i uređaja sa brojnim prednostima: brzinom prenosa do 160Mbps, većom pouzdanosti, spajanje do 17 uređaja, rad sa većinom OS, (slika 5.10c). Problemi upotrebe SCSI interfejsa su:

1. mora se konfigurisati za specifični računar,
2. ima ograničenu BIOS podršku i obično zahteva poseban BIOS i kontroler karticu,
3. ima veliku varijaciju brzina i konektora (Narrow SCSI, High Density SCSI, Wide SCSI, Very High Density SCSI, Centronics Nerrow SCSI),
4. nema opšti softverski interfejs i
5. zaključivanje SCSI *busa* sa opterećenjem (*termination*), koje je glavni problem podešavanja SCSI, bez obzira na tip, jer ako se *bus* ostavi otvoren signal može ući u interferenciju sa komunikacijom između uređaja. Generalno, poslednji uređaj u seriji mora biti zaključen sa opterećenjem.

RAID diskovi (*Redundant Array of Independent Disks*) je sistem od više HD za deljenje, ili replikaciju podataka između drajvova. Ima više tipova, ali u osnovi svi rade na isti način. RAID kombinuje više fizičkih HD u jedan logički,

obezbeđuje jeftinije skladištenje podataka, veću pouzdanost i brzinu. Tipično se koriste na serverima i obično koriste diskove iste veličine. Neke glavne ploče već podržavaju RAID diskove. RAID se implementira i upravlja na jedan od dva načina: *hardverski, ili softverski RAID,* [24].

Hardverski RAID zahteva namenski RAID kontroler, koji može biti PCI proširena kartica, ili ugrađen na glavnoj ploči. Kontroler povezuje diskove i spaja ih na računar. Ovaj tip obezbeđuje bolje performanse i bolju podršku OS. Takođe, podržava spajanje u toku rada, ali u slučaju kvara kontrolera mogu se izgubiti svi podaci. Uobičajena su tri tipa RAID:

RAID 0: Deli podatke ravnomerno na dva i više diskova, bez redundantnosti informacija. Nije tolerantan na greške. Može se koristiti za kreiranje manjeg broja velikih virtulnih diskova od velikog broja malih fizičkih diskova.

RAID 1*:* Kreira fizičku kopiju podataka na dva ili više diskova. Ako jedan disk postane nestabilan, podaci se automatski očitavaju sa drugog. Obezbeđuje redundantnost i bekapovanje podataka.

RAID 5*:* Koristi paritet na nivou blokova na svim diskovima. Najpopularniji je tip RAID diskova i može se napraviti od diskova različite veličine, iako je dodatno skladištenje ograničeno na veličinu najmanjeg diska. Na primer, ako se disk od 120GB doda na dva diska od po 100GB, svaki će dobiti 100GB prostora za ukupnih 200GB, pošto se 100GB koristi za paritet, a 20 GB se ignoriše.

Postoje i drugi tipovi RAID diskova, od kojih se neki retko koriste, a neki su hibridni.

Softverski RAID je neznatno manje pouzdan, jer sa njim upravlja OS koristeći normalne kontrolere.

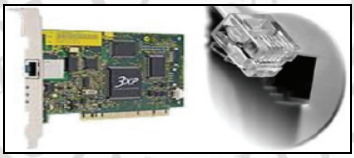
Komunikacija podataka između računarskih sitema moguća je na tri glavna načina:

1. **Bluetooth standard** koji omogućava međusobno bežično povezivanje bilo kojeg tipa elektronskih uređaja (računara, tastature, miša, mobilnog telefona i dr.) na ISM (*Industrial Scientific and Medical*) frekventnom opsegu između 2,40GHz i 2,48GHz. Problem od moguće interferencije između uređaja prevazilazi se korišćenjem niske predajne snage – do 1mW, što ograničava domet do 10m i korišćenjem *spred-spektrum* tehnike skakanja 79 slučajno izabranih

frekencija u ISM frekventnom opsegu koje se menjaju 1600 puta u sekundi. Omogućava prenos glasa i podataka sa brzinom do 1Mbps.

2. **Infracrveni primo-predajnik** u digitalnom modu koristi se za povezivanje računara sa nekim tipovima perifernih uređaja. Problem je što se zahteva optička vidljivost komunikacije. Prednost je prenos podataka samo između namenjenih uređaja.
3. **Mrežna konekcija** omogućava komunikaciju između dva i više računara. Može biti fiksana – povezana mrežnim kablovima, ili virtuelna – povezana modemima, ili bežičnim tehnologijama. Poznata su dva glavna tipa:
    a. ***LAN*** (*Lokal Area Network*) koji pokriva malu oblast kuće, kancelarije, ili zgrade.
    b. ***WAN*** (*Wide Area Network*) koja pokriva široku oblast i uključuje veliki broj računara, ili povezuje više LAN-ova. Internet je nabolji primer ove mreže.

Da bi se računar povezao na mrežu mora imati **NIC**-mrežnu karticu za povezivanje, koja može biti ugrađena na glavnoj ploči, ili na posebnoj kartici i ima specijalni konektor za povezivanje – **RJ45**, (slika 5.10).



Slika 5.10 *Mrežna kartica sa mrežnim konektorom RJ45*

Modemi se tipično koriste za prenos digitalnih podataka preko telefonske linije. Ima više tipova modema, ali svi izvršavaju glavni zadatak – proizvode noseći signal koji se lako moduliše ulaznim podacima, prenosi i demoduliše u originalni podatak. Postoje *radio* modemi za prenos više od 100 bita podataka u sekundi radio signalom, *optički* modemi za prenos optičkim kablovima više od milijardu bita u sekundi, ograničeni samo emisijom toplote u optičkom kablu. Glavni tip modema koji se danas koristi su uskopojasni 56Kbps modmi koji koriste telefonske parice za prenos podataka, malom brzinom i niskim kvalitetom, zbog kvaliteta telefonskih linija. **ADSL** (*Asymetric Digital Subscriber Line)* modemi koriste iznajmljene, namenske linije koje postoje u telefonskom kablu. Rade na dve brzine – od računara sa oko

1,5Mbps, a od računara sa maksimalno 8Mbps. Nema ograničenja opsega od strane ISP, ali ima u pogledu distance i signal se degradira sa povećanjem rastojanja od telefonske centrale.

Razvojem kablovske TV moguće je povezati se na Internet korišćenjem istog kabla iz kuće. Zahteva se poseban modem koji koristi ceo propusni opseg koaksijalnog kabla za prenos video signala. Brzina komunikacije teoretski je moguća sa 30-40 Mbps, ali je realno zbog deljenja kabla i drugih faktora mnogo manja.

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

REZIME

Digitalni forenzičar treba da dobro poznaje terminologiju, tipove i osnovne funkcije uobičajenih hardverskih komponenti računarskog sistema. *Jedinica za napajanje* (PSU) snabdeva električnom energijom računar i njegove komponente i igra značajnu ulogu u samotestiranju napajanja (POST) komponenti računara. *Glavna ploča* - glavna komponenta računara, omogućava napajanje i međusobnu komunikaciju svih delova računara, određuje tip i veličinu RAM-a, tip procesora i broj periferija koje se mogu povezati na računar.

BIOS, osnovni ulazno-izlazni softverski sistem uskladišten u ROM čipu, obično lociran na glavnoj ploči, određuje šta računar može raditi bez instalacije OS, ili druge softverske aplikacije, dovodi računar iz isključenog stanja u položaj gde OS može nastaviti *butovanje* sistema i obezbeđuje da svi drugi čipovi, procesori, portovi i povezani uređaji komuniciraju i zajedno funkcionišu. Većina savremenih BIOSa uskladištena je na specijalnom, skalabilnom ROM čipa, tzv. čipu fleš memorije (*fleširanje* BIOSa).

CMOS, integrisano kolo koje troši i emituje vrlo malu snagu, čuva sistemski datum i vreme, sekvencu butovanja, specifilaciju drajva i pasvord i zahteva konstantno napajanje sa malom baterijom smeštenom na glavnoj ploči. BIOS i CMOS su različite komponente, ali rade zajedno na podizanju OS računara. BIOS pokreće sistem, izvršava ključne funkcije startovanja sistema, kao što je samo-testiranje napajanja komponenti računara – POST, testira integritet sistema i upoređuje sve ovo sa podacima u CMOS čipu. CMOS jednostavno skladišti podatke koji se odnose na hardver računara.

RAM, primarnu privremenu memoriju, koristi OS da ubrza povezivanje između uređaja i aplikacija. RAM zahteva konstantno napajanje da bi zadržao uskladištene podatke. CPU, mikroprocesor koji interpretira i procesira instrukcije i podatke sadržane u softverskim aplikacijama i drugim komponentama, ima direktan pristup RAM-u i oni uzajamno čitaju i upisuju podatke. Postoje dve osnovne arhitekture CPU: CISC i RISC tipa sa dva glavna tipa priključnih utičnica na glavnu ploču: *ZIF Socket* i LIF utičnica.

BUS (magistrala), podsistem koji prenosi podatke, ili napajanje između komponenti računara, može logički povezati nekoliko komponenti preko

istog kola. Postoje interni i eksterni *bus*, a uobičajeni su: ISA, PCI i PCI Express, MCA, AGP, ATA, SCSI, USB, Fireware – IEEE 1394 standard itd.

Grafičke karte (grafički adapteri) obezbeđuju vizuelni prikaz rezultata rada računara na ekranu monitora. Postoje tri tipa grafičkih adaptera: *na glavnoj ploči*, koja koristi RAM kao skladište i pokazuje slabije performanse od nezavisnih adaptera; *PCI grafički adapter*, povezuje se sa glavnom pločom preko slobodne PCI *slot*-utičnice i obično ima svoj RAM i mikroprocesor, generalno je spor, jer ograničava brzinu transfera podataka, pa je zamenjen sa daleko bržim *PCI Express slotom* sa većim grafičkim kapacitetom, koji postaje standard savremene grafičke karte.

Monitori su od CRT tipa sa 256 nijansi boja u RGB standardu, razvijeni do savremenih TFT i LCD ravnih displeja, sa daleko manjom potrošnjom i disipacijom snage i brojem nijansi boja većim od 16 miliona. *Tastature i miševi*, ulazni uređaji, obezbeđuju korisniku unos podataka u računar, opštu interakciju sa računarom i kontrolu brojnih funkcija računara. *Tastature* se proizvode u brojnim oblicima i veličinama, ali sve rade na istim osnovnim principima – sastoje se od serije prekidača spojenih na mali mikroprocesor koji monitoriše stanje svakog prekidača, a zatim inicira specifični odgovor. *Miš* je hardverski uređaj koji obezbeđuje korisniku da kontroliše kursor za manipulaciju podataka bez upotrebe komplikovanih komandi. Prvi miši je proizveden u kompaniji *Aple* za računar *Lisa* 1984. godine, a danas se proizvodi u četiri tipa: *mehanički, optički i optičko-mehanički*, sa prednostima i nedostacima i mogućih pet načina spajanja na računar: *serijski port, PS/2 port, infracrveni, USB i Bluteooth*.

Ulazno-izlazni portovi obezbeđuju povezivanje perifernih uređaja na računar i nalaze se na zadnjoj strani računara, a mogu biti direktno povezani na glavnu ploću, ili na odvojenoj karti. Postoji više tipova portova: serijski; paralelni; USB, *Firewire,* infracrveni primo-predajnik*, Bluetooth standard* koji omogućava međusobno bežično povezivanje bilo kojeg tipa elektronskih uređaja: računara, tastature, miša, ili mobilnog telefona; *IDE* interfejs za standardni način povezivanja uređaja za skladištenje na računar, SCSI interfejs za brzu komunikaciju između računara i memorijskih uređaja.

Čvrsti diskovi (HD) i RAID diskovi – hardverski ili softverski sistem (tipa 0, 1 ili 5) od više HD za deljenje, ili replikaciju podataka između diskova, glavne su interne sekundarne memorije za masivno skladištenje podataka.

Modemi za prenos digitalnih podataka preko telefonske linije, proizvode noseći signal koji se lako moduliše ulaznim podacima, prenosi i demoduliše u originalni podatak, mogu biti: *radio* modemi za prenos više od 100 bita podataka u sekundi radio signalom; *optički* modemi za prenos optičkim kablovima više od milijardu bita u sekundi; uskopojasni 56Kbps modmi koji koriste telefonske parice za prenos podataka; *ADSL* koji koriste iznajmljene, namenske linije koje postoje u telefonskom kablu sa brzinom prenosa od 1,5Mbps do 8Mbps i video-kablovski sa brzinom komunikacije do 30-40 Mbps.

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

PITANJA ZA PONAVLJANJA

1. Ukratko opisati PSU funkcije?
2. Šta je statički elektricitet?
3. Zašto služi BIOS?
4. Zašto služi CMOS?
5. Navesti tri tipa RAM-a?
6. Navesti tri vrste magistrala (*bus*) u računaru?
7. Objasniti razliku između serijskog i paralelnog porta?
8. Zašto služi SCSI?
9. Kakve podatke čuva CMOS?
10. Zašto služi RAID?

6 PROCES PODIZANJA OS RAČUNARA

Sa aspekta digitalne forenzike, važno je znati šta se događa u računaru kada se uključi i kada se sistem podiže-*butuje* (*boot process*), jer ovo može ozbiljno uticati na forenzičke procese akvizicije i analize.

Kada je računar isključen, procesor ne funkcioniše, a RAM je prazan, ili sadrži izmešane podatke. Kada se pritisne taster za uključivanje računara, očekuje se da mašine dođe u poziciju iz koje se može koristiti za procesiranje podataka; da se aktiviraju OS i sve periferije – monitor, tastatura, miš; da ih sistem prepozna i da propisno rade. Za razumevanje akcija koje se događaju u računaru kada se uključi, potrebno je poznavati funkciju tri komponente računarskog sistema, koje učestvuju u procesu *butovanja*:

1. **BIOS** (Basic Input Output System)**,**
2. **POST** (Power On Self Test) i
3. **CMOS** (Complimentary Metal Oxide Semiconductor).

6.1 BIOS sistem

BIOS je ugrađeni softver uskladišten u ROM čipu, koji je obično lociran na glavnoj ploči. On određuje šta računar može uraditi bez podizanja OS, ili drugih aplikacija i dovodi računar u tačku u kojoj OS preuzima rad. BIOS obezbeđuje da sve komponente računarskog sistema – čipovi, procesori, portovi i priključeni periferni uređaji međusobno komuniciraju. Pošto je BIOS uskladišten u ROM čipu, podaci će uvek biti na raspolaganju i na njih ne utiče kvar čvrstog diska, ili pad napajanja. Većina savremenih BIOS-a je memorija fleš tipa, koja se po potrebi može ažurirati, (slika 6.1).



Slika 6.1 *BIOS ROM čip tipa* ***Amibios***

Kada se BIOS pokrene, njegova primarna funkcija je samotestiranje funkcionisanja svih komponenti sa priključenim napajanjem (POST) i aktiviranje drugih BIOS čipova na periferijskim uređajima, priključenim na glavnu ploču. Takođe, obezbeđuje OS sa osnovnim rutinama za interfejs sa drugim hardverskim komponentama. Pri tome treba imati na umu da neke komponente računara, posebno HD kontroler i SCSI kartice imaju svoja vlastita BIOS podešavanja.

6.2 POST funkcije

POST proces samotestiranja ispravnosti napajanja svih hardverskih komponenti računara, prva je aktivnost uključenog računara. Ovo je ugrađena dijagnostička aplikacija, koja proverava konfiguraciju i funkcionisanje hardverskih komponenti i proverava CMOS zapis. U savremenim računarima POST proces se izvršava veoma brzo. Ako računar naiđe na problem u toku POST procesa podizanja sistema-*butovanja*, čuje se *bip* zvuk koji upozorava da postoji neki problem. Različiti proizvođači koriste različite sekvence *bip* kôda za različite probleme. Ove informacije se mogu naći na *web* lokacijama proizvođača. Većina POST *bip* signala smatra se fatalnim, zato što POST proces testira vitalne komponente sistema. Fatalna greška trenutno zaustavlja proces *butovanja*, na primer ako nema modula sistemske memorije. *Bip* signal upozorava na problem u podizanju sistema, zato što do ove tačke na ekranu računara nema video signala, [24].

6.3 Funkcije komplementarnog metal-oksidnog poluprovodnika (CMOS)

CMOS je glavna klasa tipa integralnog kola. Zahteva vrlo malu snagu istosmernog napajanja za održavanje podataka i malo se zagreva za razliku od većine čipova. Za napajanje se obično koristi mala baterija. CMOS računara sadrži sledeće podatke:

1. sistemsko vreme i datum,
2. sekvence *butovanja*,
3. specifikaciju diska i

4. pasvorde za uključivanje sistema.

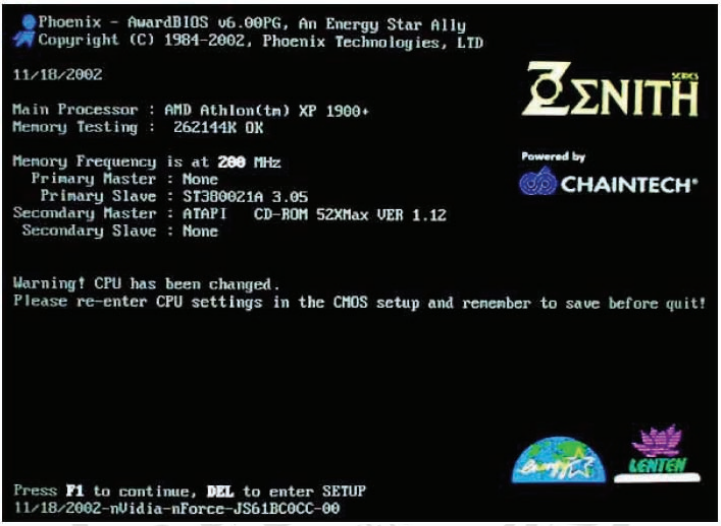
Očigledno je da su sistemsko vremena i datumi značajni podaci za forenzičara. Sekvence butovanja su značjne jer omogućavaju *butovanje* sa forenzičkog medijuma, umesto sa HD osumnjičenog računara. Specifikacija diska sadrži podatke o geometriji i kako je disk podeljen u particije. Pasvorde za uključivanje sistema ponekad proizvođači postavljaju podrazumevano, ali ih mogu podesiti i korisnici kao dodatnu zaštitu sistema. U slučaju da osumnjičeni računar ima ovaj pasvord, postoje brojni metodi za proboj, za koje postoje razlozi za i protiv, [24]:

1. *Ukloniti bateriju za napajanje CMOS-a***,** što će resetovati CMOS i svi prethodni podaci će biti izgubljeni, uključujući sistemsko vreme i datum,
2. *Uklanjanje diska,* što omogućava pristup disku, ali opet nema sistemskog vremena i datuma,
3. *Promena džampera na glavnoj ploči,* koja će ponovo resetovati CMOS, svi prethodni podaci će biti izgubljeni, uključujući sistemsko vreme i datum,
4. *Tajni pasvord,* kojeg mnogi proizvođači podrazumevano generišu za tehnički pristup,
5. *Društveni inženjering,* koji podrazumeva dolazak do pasvorda prevarom,
6. *Pitati osumnjičenog,* što nije uvek izvesno,
7. *Pogađanje pasvorda napadom rečnika,* što može dati dobar rezultat, ali zahteva određeno vreme i rad.

6.4 Proces butovanja

Kada računar završi prvi korak samotestiranja (POST), šalje signal prekidaču tajmera procesora (čipu) da je napajanje svih hardverskih komponenti računara *korektno*. Sada tajmerski čip prestaje da šalje signale za resetovanje i dopušta da se CPU inicijalizuje. Kada se CPU inicijalizuje, izvršava samotestiranje, pa ako je pozitivno, brišu se podaci iz memorije internog registra CPU, koji se resetuje i omogućava start programa iz BIOSa. BIOS je generalno lociran u RAM memoriji i počinje da se izvršava.

Treća faza butovanja sistema je kada BIOS poziva POST test. CPU šalje signale preko magistrale (*bus*) sistema da se uveri da sistem radi. Zatim CPU proverava svoj sistemski tajmer (ne sistemski časovnik!), da obezbedi da se sve operacije računara odvijaju sinhronizovano i po redosledu. Zatim se proverava grafička ploča (video adapter) i na ekranu se po prvi put nešto pojavi, (slika 6.2).



Slika 6.2 *Primer CPU provere grafičke kartice u procesu butovanja*

Sledeće se proverava sistem RAM memorije, što se ponekad vidi na ekranu, a POST zatim proverava tastaturu i da li je neki taster pritisnut, jer pritisak na bilo koji taster prekida proces butovanja sistema. Zatim se signal šalje preko specifične putanje na magistralu prema svakom drajvu diska koji je priključen, očekujući odgovor, a na ispitivanom drajvu obično svetluca LED. Konačno, rezultat POST testiranja upoređuje se sa podacima sadržanim u CMOSu. U CMOSu su ažurirane sve promene osnovnih sistemskih parametara. Takođe, rezultati POST testiranja mogu biti prikazani na ekranu, sa pitanjem korisniku za pristanak na neku promenu. U ovom slučaju CPU je promenjena, a promena je identifikovana sa podacima konfiguracije poslednjeg ispravnog butovanja iz CMOSa. Različiti proizvođači BIOSa omogućavaju prikazivanje različitih informacija na ekranu u ovoj fazi, a to su tipično:

- tip procesora,

- brzina kloka tajmera,
- drajvovi za FD,
- drajvovi za IDE/ATA diskove,
- osnovna memorija,
- proširena memorija,
- veličina keš memorije,
- portovi.

Konačno, kada se uspešno završe rutine POST procesa, BIOS tada traži namenjeni butabilni uređaj. Ako je HD namenjen za butovanje, sistem će tražiti **MBR**[4] na disku i počeće sekvencu butovanja.

Rezultat procesa butovanja na kraju omogućava korisniku da pristupi Windows desktopu i koristi računar. Proces butovanja za Windows NT mašine sasvim se razlikuje od onog u Windows 9x sistemima. Međutim, oba procesa treba da pristupe jednom te istom fajlu – MBR, da bi nastavili proces butovanja. Da bi se neki OS butovao, računar zahteva najmanje jednu aktivnu primarnu *butabilnu particiju* – particiju koja je *formatirana* i sadrži neki OS.

6.4.1 Sekvenca butovanja Windows NT operativnog sistema

Za uspešno butovanje NT sistema postoji 6 različitih faza u kojim sistem poziva brojne fajlove. U tabeli 6.1 navedene su ove faze (leva kolona) i fajlovi (desna kolona), ili rutine koje sistem poziva u svakoj fazi, [24].

Tabela 6.1 Faze, fajlovi i boot rutine Windows NT OS

Pre – Boot	POST Boot Record	MBR NTDLR
Boot **NTDLR calls:**	Boot.ini Ntdetect.com	Bootsect.dos Ntbootdd.sys
Kernel Load **NTLDR calls:**	Ntoskml.exe Hal.dll	

[4] *Master Boot Record*

Service Load	Smss.exe Winlogon.exe Lsass.exe Screg.exe
Logon	**CTR-ALT-DEL** Poziva poslednji dobro poznat set kontrola

Tabela 6.2 Ključni fajlovi i lokacije za butovanje

NTLDR *Učitavač operativnog sistema. Atributi: Sistemski; Skriveni; Samo za čitanje*	Koren aktivne particije
Boot.ini *Tekstualni fajl koji se koristi za kreiranje menija za odabir OS. Daje putanju na svaki dostupan OS. Atributi: Sistemski; Samo za čitanje*	Koren aktivne particije
Bootsect.dos [samo kod dualnog butovanja] *Sadrži boot sektor OS koji je učitan pre instalacije NT. Koristi ga NTDLR u multi-boot okruženju. Atributi: Sistemski; Skriveni*	Koren aktivne particije
Ntdetect.com *Aplikacija koja ipituje sve prisutne hardvere. Formira listu koju NTDLR koristi za kreiranje grane registra hardvera HKEY_LOCAL_MACHINE*	Koren aktivne particije
Nbootdd.sys [samo kod butovanja sa SCSI particije sa SCSI BIOS] *Drajver uređaja*	Koren aktivne particije
Ntoskrnl.exe *Jezgro samog operativnog sistema*	%SystemRoot%\System32\
Hal.dll *Apstrakcioni sloj hardvera*	%SystemRoot%\System32\
System	%SystemRoot%\System32\Config
Drajveri uređaja [Promenjiva]	%SystemRoot%\System32\Drivers
"Koren aktivne particije" = C:	**"%SystemRoot" = C:\winnt**

Od svih navedenih fajlova u tabeli 6.1, potrebni fajlovi za uspešno butovanje navedeni su u levoj koloni tabele 6.2 sa podrazumevanim lokacijama u desnoj koloni.

6.4.1.1Koraci procesa butovanja

Korak 1: **POST proces** izvršava svaki računar bez obzira na OS. Stabilna hardverska platforma je neophodna za uspešno butovanje. Posle uspešnog kompletiranja procesa POST testiranja, računar će locirati butabilni uređaj i učitati MBR u memoriju. But sektor iz aktivne particije učitava se u memoriju, a posle izvršavanja malog mašinskog kôda učitava se **NTLDR** u memoriju.

Korak 2: **NTLDR** je verovatno najkritičniji od svih fajlova korišćenih u procesu butovanja. Kada se **NTLDR** učita prebacuje se procesor iz realnog moda u 32-bitni mod prazne memorije. U realnom modu nije moguća translacija iz virtuelne u fizičku memoriju. U suštini ovo ograničava pristup fizičkoj memoriji samo prvim 640KB. U 32-bitnom modu prazne memorije, adresiraju se 32 bita memorije, sva fizička memorija se može čitati i uključuje se straničenje. Ovo je poznato i kao prelazak na *NT zaštićeni mod*, koji je podrazumevano stanje koje NT izvršavana za normelne operacije. Proces dalje startuje mini fajl sistem – drajvere koji podržavaju FAT i NTFS fajl sisteme, zatim čita **Boot.ini** fajl i prikazuje listu OS koji se mogu butovati. Ako se detektuje više od jednog OS, zahteva se intervencija korisnika da bi se proces nastavio. Ako se izabere neki drugi OS, pored onog koji podržava NTFS, **NTLDR** izvršava **Bootsec.dos** koji zatim podiže taj drugi OS. Ako se podiže OS koji podržava NTFS fajl sistem, **NTLDR** pokreće fajl **Ntdetect.com,** koji sakuplja informacije o konfiguraciji hardvera računara, poseblno:

1. ID računara,
2. tipove magistrale/adaptera,
3. SCSI adaptere,
4. video adaptere,
5. tastaturu,
6. COM portove,
7. paralelne portove,
8. Flopi diskove,
9. pokazivače (miš, ...),
10. ko-procesore za *floating-point*.

Kada **Ntdetect.com** sakupi i kompajlira listu ovih informacija, iste se koriste za popunu ključeva registra:

- **HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION**
- **HKEY_LOCAL_MACHINE\SYSTEM.**

NTLDR sada završava svoju ulogu u procesu *butovanja* i zatim prenosi kontrolu na **Ntoskrnl.exe** u srcu kernela Windows NT OS.

Korak 3: Učitavanje kernela (*kernel load***)** počinje kada **NTDLR** poziva fajlove **Ntoskrul.exe** i **Hal.dll** (*Hardware Abstraction Layer*) i učitava informacije iz registra sistema u memoriju da ih ova dva fajla mogu koristiti. Fajl **Ntoskrul.exe** koristi se za kontrolu hardvera i sistemskih parametara i obezbeđuje bezbedan pristup hardveru i procesima sistema. **NTDLR** zatim poziva fajl **Hall.dll** koji se pokreće, a zatim skriva i štiti kernel od previše poziva hardveru mašine od svake instalirane aplikacije koja se pokrene. Ovaj fajl takođe instalira set kontrola OS na niskom nivou i drajvere komponenti računara. U ovoj tački ekran je čist, a beli pravougaonik se progresivno širi u donjem delu ekrana. Ako sve nije u redu, tu počinje da se pojavljuje 'plavi ekran smrti' sistema.

Korak 4: Instalacija kernela (*Kernel instalation*) je sledeći korak. Kada se **Ntoskrnl.exe** instalira, kreira hardverski ključ u registru, od informacija sakupljenih ranije sa **Ntdetect.com**. Zatim, **Ntoskrnl.exe** inicijalizuje drajvere koji su ranije podignuti i skenira uređaje u registru sa startnom vrednosti **0x1**.

Korak 5: Učitavanje servisa (*services load*) počinje sa startom podsistema sesije menadžer- **Smss.exe** (*Session Manager Sub*-System*)*. Svi podsistemi su učitani. Ovaj fajl će aktivirati sve programe izlistirane u **Boot Execute** ključu registra. Zatim se učitava **Windows32k.sys** koji implementira **Windows32** grafički podsistem, startuje **Windowslogon.exe** koji, pak, startuje **Lsass.exe** (*Local Security Administration*), koji tada prikazuje prozor **Ctrl-Alt-Del**, ili prozor dobrodošlice u Windows XP OS, (slika 6.3).



Slika 6.3 *Ctrl-Alt-Del ekran dobrodošlice u Windows XP Home OS*

Kontroler servisa **Screg.exe** tada će proveriti registar za servise sa startnom vrednosti **0x2** i podiže ih. Servisi sa startnom vrednosti **0x3** startuju se manuelno, a oni sa startnom vrednosti **0x4** onemogućeni su u procesu podizanja sistema (*start-up*).

Kork 6: **Logon** je poslednji korak u procesu butovanja računara, koji se ne smatra uspešnim sve dok se korisnik ne uloguje na sistem. Proces prazni sve TSR (*Terminate and Stay Resident*) programe u memoriju i dopušta logovanje. Posle uspešnog logovanja kreira se i kopira kopija set kontrola u **LastKnownGood** kontrolni set za buduću upotrebu. Ovim se proces butovanja sistema uspešno završava.

6.4.2 Sekvenca butovanja DOS sistema

Sekvenca butovanja u DOS sistemu bitno se razlikuje od sekvence butovanja Windows NT OS. Procesi i fajlovi DOS sekvence butovanja prikazani su tabelama 6.3 i 6.4.

U tabeli 6.3 prikazane su sekvence butovanja i zahtevani fajlovi u DOS sistemima. Međutim, treba reći da, kao u NT sekvenci za butovanje, postoje fajlovi koji nisu potrebni, a ima i onih koje se koriste samo ako su tamo. Vidi se da postoje tri fajla koja uvek moraju biti prisutna za uspešno butovanje DOS sistema. DOS proces butovanja sistema je najprostiji i lako ga je kontrolisati. Sada postaje jasno zašto su potrebni blokatori upisivanja kada forenzičar dodaje osumnjičeni disk forenzičkoj mašini radi uzimanja fizičke slike. Ako je dopušteno butovanje na svaki način, veća je verovatnoća da će se uneti izmene u osumnjičeni disk, [24]. Različiti procesi butovanja za različite OS komparativno su prikazani u tabeli 6.4.

Tabela 6.3 Procesi i fajlovi DOS sekvence butovanja

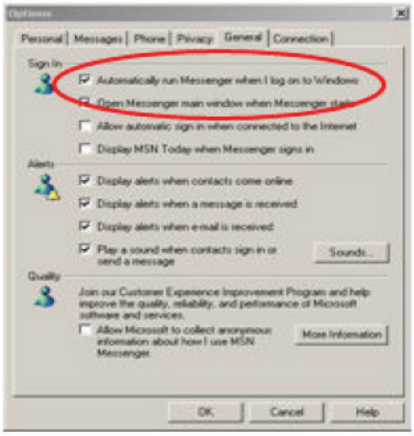
IO.SYS	Traži fajlove korišćenje sa kompresovanim drajvovima. Koristi Drvspace.bin; Drvspace.ini; dblespace.bin. Takođe. koristi neke proširene namene BIOS-a.
MSDOS.SYS	Tekstualni fajl koji sadrži konfiguracione podatke, start—up i boot opcije
CONFIG.SYS **Nije ključni za boot**	Koristi se za učitavanje drajvera uređaja i drugih korisničkih konfiguracija. Ovaj fajl može da izmeni korisnik. Ne zahteva se za boot proces.

COMMAND.COM	Sadrži interne DOS komande, kao što su COPY i DIR. Takođe, sadrži kôd za upravljanje I/O parametrima. Traži da li je prisutan AUTOEXEC.BAT fajl.
AUTOEXEC.BAT **Nije ključni za boot**	„Automatsko izvršavanje batch komandi“ Čuva listu korisnički konfigurisanih DOS komandi koje se automatski izvršavaju prilikom učitavanja DOS-a. Boot proces ga ne zahteva.

Tabela 6.4 Uporedni prikaz različitih procesa butovanja

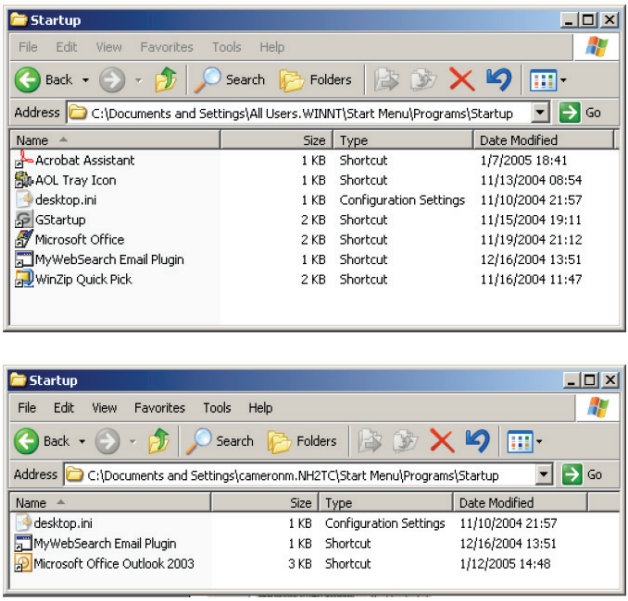
	MS-DOS	WIN9x	WIN NT/2K
1	IO.SYS	IO.SYS	NTLDR
2	MSDOS.SYS	MSDOS.SYS	BOOT.INI
3	CONFIG.SYS	DRVSPACE.BIN	BOOTSECT.DOS
4	COMMAND.COM	SYSTEM.DA	NTDETECT.COM
5	AUTOEXEC.BAT	USER.DAT	NTBOOTDD.SYS
6		CONFIG.SYS	NTOSKRNLEXE
7		AUTOEXEC.BAT	HAL.DLL
8		SYSEM.INI	SYSEM.KEYS
9		VMM32.VXD	DEVICE DRIVERS
10		WIN.COM	
11		KERNEL32.DLL	
12		GD132.EXE	
13		USER32.DLL	
14		WIN.INI	
15		Start Up Group	

Pored greške koja može nastati u nekom koraku procesa butovanja, koja dovodi do ’plavog ekrana’, postoje drugi spoljni uticaji na proces butovanja. Vešt korisnik može konfigurisati brojne vrednosti u registru i personalizovati proces butovanja. Postoje i brojne aplikacije koje omogućavaju korisnku da konfiguriše kako će se računar ponašati u toku procesa butovanja. Takođe, mnoge uobičajene aplikacije omogućavaju korisniku da ih pokrene u vreme butovanja računara. Primer je *MSN Messenger* koji se može podesiti da se pokreće kada se podigne Windows OS. (slika 6.4).



Slika 6.4 *Opcije setovanja MSN Messenger*

Postoje brojna podešavanja koja korisnik može izvršiti u samom Windows OS. Ovo diktira koje će se aplikacije podići i pokrenuti u toku procesa butovanja neposredno posle uspešnog logovanja. Na slici 6.5 prikazani su *start up* meni za sve korisnike, koji pokazuje šta se namerava pokrenutu i lični korisnički *start-up* meni.



Slika 6.5 *Start-up meni za sve korisnike i jednog korisnika*

Na dva ekrana na slici 6.5 prikazani su ***Windows Sweeper*** *i* ***TweakUI*** aplikacije i njihove sposobnosti da pokreću druge fajlove i aplikacije dok se sistem podiže. Očigledno, ovakve aktivnosti forenzičaru otežavaju posao, a sve ukazuje na to zašto forenzičar ne treba da radi na osumnjičenom računaru, sve dok zaista ne mora.

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

REZIME

Sa aspekta digitalne forenzike, važno je znati šta se događa u računaru kada se uključi i kada se sistem podiže (*butuje*), jer ovo može ozbiljno uticati na forenzičke procese akvizicije i analize. Kada je računar isključen, procesor ne funkcioniše, a RAM je prazan, ili sadrži izmešane podatke. Kada se pritisne taster za uključivanje računara, očekuje se da mašina dođe u poziciju iz koje se može koristiti za procesiranje podataka; da se aktiviraju OS i sve periferije; da ih sistem prepozna i da propisno rade. Za razumevanje akcija koje se događaju u računaru kada se uključi, potrebno je poznavati funkciju *BIOS, POST i CMOS*, koji učestvuju u procesu *butovanja*.

Kada se BIOS pokrene, njegova primarna funkcija je samotestiranje funkcionisanja svih komponenti sa priključenim napajanjem (POST) i aktiviranje drugih BIOS čipova na periferijskim uređajima, priključenim na glavnu ploču i obezbeđenje OS sa osnovnim rutinama za interfejs sa drugim hardverskim komponentama.

POST proces samotestiranja ispravnosti napajanja svih hardverskih komponenti računara, prva je aktivnost uključenog računara, dijagnostička aplikacija, koja proverava konfiguraciju i funkcionisanje hardverskih komponenti i proverava CMOS zapis. U savremenim računarima POST proces se izvršava veoma brzo, a ako računar naiđe na problem u toku POST procesa *butovanja*, čuje se alarmni *bip*.

CMOS sadrži sledeće sistemsko vreme i datum, sekvence *butovanja*, specifikaciju diska i pasvorde za uključivanje sistema. Sistemska vremena i datumi su značajni podaci za forenzičara. Sekvence butovanja su značjne jer omogućavaju *butovanje* sa forenzičkog medijuma, umesto sa HD osumnjičenog računara. Specifikacija diska sadrži podatke o geometriji i kako je disk podeljen u particije. Pasvorde za uključivanje sistema ponekad proizvođači postavljaju podrazumevano, ali ih mogu podesiti i korisnici kao dodatnu zaštitu sistema. U slučaju da osumnjičeni računar ima ovaj pasvord, postoje brojni metodi za proboj, koje forenzičar mora znati.

Proces butovanja sadrži više sukcesivnih faza. Kada računar završi prvi korak samotestiranja (POST), šalje signal prekidaču tajmera procesora (čipu) da je napajanje svih hardverskih komponenti računara *korektno*. Sada tajmerski čip prestaje da šalje signale za resetovanje i dopušta da se CPU inicijalizuje. U

drugoj fazi, kada se CPU inicijalizuje, izvršava samotestiranje, pa ako je pozitivno, brišu se podaci iz memorije internog registra CPU, koji se resetuje i omogućava start programa iz BIOSa, koji počinje da se izvršava. Treća faza butovanja sistema je kada BIOS poziva POST test. CPU šalje signale preko magistrale (*bus*) sistema da se uveri da sistem radi. Zatim CPU proverava svoj sistemski tajmer (ne sistemski časovnik!), da obezbedi da se sve operacije računara odvijaju sinhronizovano i po redosledu. Zatim se proverava grafička ploča (video adapter) i na ekranu se po prvi put nešto pojavi. Sledeće se proverava sistem RAM memorije, što se ponekad vidi na ekranu, a POST zatim proverava tastaturu i da li je neki taster pritisnut, jer pritisak na bilo koji taster prekida proces butovanja sistema. Zatim se signal šalje preko specifične putanje na magistralu prema svakom drajvu diska koji je priključen, očekujući odgovor, a na ispitivanom drajvu obično svetluca LED. Konačno, rezultat POST testiranja upoređuje se sa podacima sadržanim u CMOSu. Različiti proizvođači BIOSa omogućavaju prikazivanje različitih informacija na ekranu u ovoj fazi, a to su tipično: tip procesora, brzina kloka tajmera, drajvovi za FD, drajvovi za IDE/ATA diskove, osnovna memorija, proširena memorija, veličina keš memorije i portovi. Konačno, kada se uspešno završe rutine POST procesa, BIOS tada traži namenjeni butabilni uređaj. Ako je to HD, sistem će tražiti MBR na disku i počeće sekvencu butovanja. Rezultat procesa butovanja na kraju omogućava korisniku da pristupi Windows desktopu i koristi računar. Proces butovanja za Windows NT mašine sasvim se razlikuje od onog u Windows 9x sistemima. Međutim, oba procesa treba da pristupe jednom te istom fajlu – MBR, da bi nastavili proces butovanja. Da bi se neki OS butovao, računar zahteva najmanje jednu aktivnu primarnu *butabilnu particiju* – particiju koja je *formatirana* i sadrži neki OS.

Za uspešno butovanje NT sistema postoji 6 različitih faza u kojim sistem poziva brojne fajlove i zahteva se aktivna butabilna particija na HD, koja se podrazumevano nalazi u rutu *C:\ I %SystemRoot= C:\ winnt*.

Brojni alati (*Windows Sweeper i TweakUI*) omogućavaju da korisnici podešavaju koje se aplikacije podižu *startup* procesu, što može otežati posao forenzičaru i ukazuje da forenzičar ne treba da radi na osumnjičenom računaru, sve dok zaista ne mora.

PITANJA ZA PONAVLJANJE

1. Kojih šest procesa učestvuje u uspešnoj sekvenci NT butovanja?
2. Kojih sedam fajlova je uključeno u NT but proces?
3. Koji su drugi procesi uključeni u NT butovanje?
4. Koja dva fajla se koriste samo kada se zahteva?
5. Koja dva fajla nisu bitna za uspešno DOS butovanje?

7 DIGITALNA FORENZIČKA ANALIZA RAČUNARA

7.1 Priprema za forenzičku analizu računara

Osnovni zadatak svakog forenzičara je otkrivanje, izvlačenje iz računara, analiza i rad sa digitalnim podacima. Bez obzira na ulogu u slučaju kompjuterskog kriminala, digitalni forenzičar mora poznavati prirodu digitalnih podataka i kako rukovati sa njima. Digitalni podaci se mogu skladištiti u savremenim računarima u enormnim količinama. Čvrsti diskovi su dostigli kapacitet preko 700GB, a tu su i kapaciteti web servis provajdera na Internetu koji se još uvek ne koristi u dovoljnoj meri. Ogromnu većinu digitalnih podataka generišu korisnici.

Prvi forenzičari početkom 1990-tih počeli su razvoj alata za izvlačenje i oporavak podataka iz kompromitovanih računara koji obezbeđuju integritet ispitivanih podataka. Proces je poznat kao uzimanje *fizičke (miror slike, imidža*) ispitivanog računara. Forenzička analiza digitalnih podataka i računara došla je u fokus forenzičke nauke kao novi tip uzimanja dokaza, pored tradicionalnih vidova dokaza – otiska prsta, DNK, anlize krvi itd. Iako digitalna forenzika ima verifikovane metode i testove, uključujući široko prihvaćene hardverske i softverske alate, još je u ranoj fazi razvoja, [25].

Proces uzimanja *imidža* ispitivanog računara koristi jednostavan koncept kojeg izvršava alat dizajniran za tu namenu. Za prvo uzimanje *imidža* računara korišćen je *Northon Ghost* i drugi raspoloživi softverski alati. Razlozi za potrebu uzimanja *imidža* ispitivanog računara sasvim su opravdani. Zvanični organi istrage moraju na sudu dokazati da su digitalni podaci upravo onakvi kakvi su bili u računaru u trenutku pretrage i privremenog oduzimanja. Istraga kompjuterskog kriminala znatno je napredovala od kada sudija ne može da dovede u pitanje integritet digitalnog dokaza. Ako se dokazi ne mogu dovesti u pitanje, onda se može postaviti pitanje procesa korišćenog za dobijanje dokaza. Otuda potreba da se za izgradnju čvrstog digitalnog dokaza mora koristiti pouzdan metod.

Uzimanje bekapa digitalnih podataka u prvim danima razvoja digitalne forenzike, bilo je bolje od ničega, ali su u većini slučajeva bekapovani samo

fajlovi ispitivanog sistema, a ne i svi dokazi koji se mogu naći na aktivnom fizičkom disku ispitivanog računara. Upravo uzimanje *imidža* ispitivanog računara obezbeđuje uzimanje svih raspoloživih dokaza. NIST definiše ključne karakteristike forenzičkih alata za uzimanje *imidža* ispitivanog diska, koji treba da, [22]:

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

Preporučuje se uzimanje dve kopije *imidža* ispitivanog računara, jednu za analizu i drugu kao referentni original za potrebe suda. Sa pravosudnog aspekta, prvilo najboljeg dokaza zahteva da je dokaz original. Od trenutka uzimanja imidža originalnog, osumnjičenog računara, pa do eventualnog zahteva sudije za originalnim dokazom u toku suđenja, može proći dosta vremena, a može se desiti da je osumnjičeni računar već ponovo u upotrebi (na primer, poslovni server). Otuda je jasno da je najbolji dokaz i najbliži stvarnom originalu, upravo *imidž* kopija koja se čuva u lancu istrage kao referentna za potrebe suda, [27].

Digitalni forenzičar analizira drugu, *radnu imidž kopiju* sa raspoloživim forenzičkim alatima, pretražuje fajl sistem i ekstrahuje relevantne podatke za izgradnju čvrstih dokaza. *Imidž* originala obezbeđuje takođe i pravljenje više radnih kopija za eventualnu analizu na različitim mestima, ili u drugoj državi. Iz *imidža* se može i ponovo reprodukovati originalni disk, ako je potrebno za prikazivanje šta je osumnjičeni tačno imao na svom računaru, ili za detekciju virusa i trojanaca. Postoje brojni forenzički alati za akviziciju i analizu digitalnih podataka, a najviše se koriste ***En Case, Vogon, Safeback, iLook, FTK Imager i DD***. Formati i funkcionalnosti relevantnih forenzičkih alata mogu varirati, pa ih je potrebno testirati na NIST zahteve za forenzičke alate, [24].

Treba reći da *imidž* diska uzet bit-po-bit, predstavlja tačnu kopiju diska sa koga je uzet *imidž*, ali nije potpuno isti kao autorski (*proprietary*) *imidž*, format kojeg su razvili neki proizvođači da radi sa njihovim softverom. U

nekim slučajevima ovaj se *imidž* može smatrati sasvim dobrom kopijom originalnog diska, jer se razlika može objasniti, ako to sud zahteva.

Kod uzimanja *imidža* treba imati forenzički disk isti, ili veći od originalnog, ako kapacitet nije suviše velik. U slučaju uzimanja imidža diska od 700GB treba imati forenzički disk istog kapaciteta, ali je moguće i manji ukoliko forenzički alat za uzimanje *imidža* može vršiti i kompresiju signala, [9].

Bilo koji metod da se izabere za uzimanje *imidža* osumnjičenog računara, ili za izvlačenje i čuvanje dokaza, ili da je metod uzimanja imidža potpuno prihvatljiv, zahteva se da digitalni forenzičar može ponoviti i obezbediti iste rezultate u toku istrage.

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

Drugi potencijalni problem je uzimanje *imidža* čvrstog diska smeštenog na glavnoj ploči, kao kod Laptop računara, jer uklanjanjem diska sa ploče podaci više nisu čitljivi. Takođe, serveri mogu stvoriti probleme forenzičaru. U suštini, sa aspekta digitalne forenzike, server je samo računar i može biti potpuno isti kao ostali računari na lokaciji, ali i sasvim različit. Tako problem predstavljaju serveri ugrađeni u rekove sa RAID diskovima, jer forenzičar mora razumeti sve veze pre preduzimanja bilo koje akcije. Takođe, postojeći forenzički alati i oprema nisu dovoljni za akviziciju i analizu podataka sa *mainframe* servera, ukoliko se nađu na mestu krivičnog dela, [24].

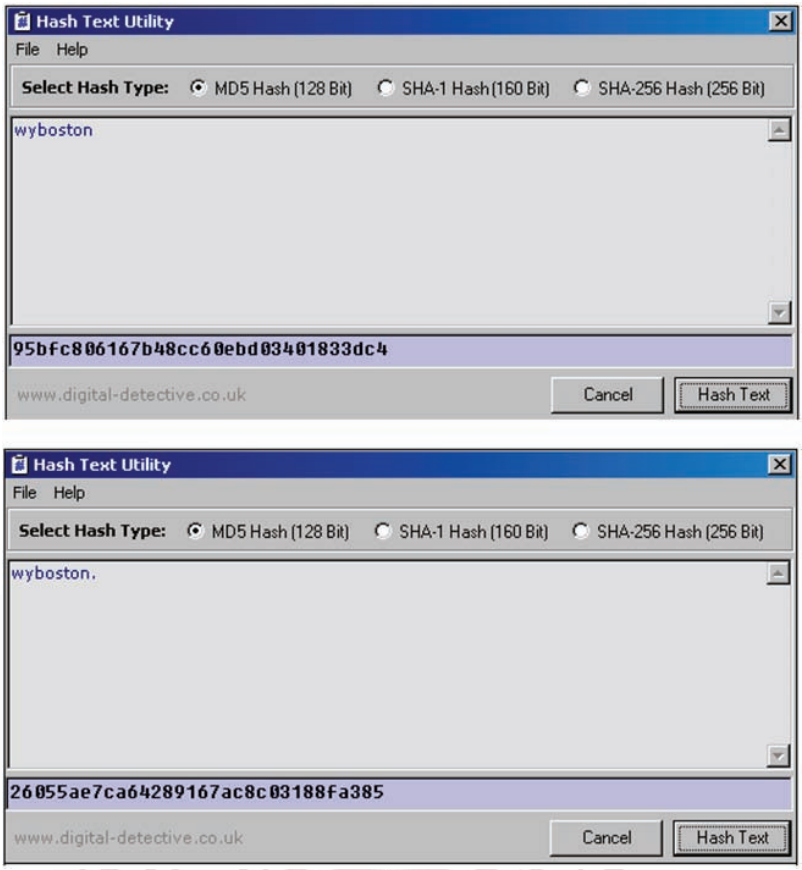
U svakom slučaju uzimanja imidža sa kompromitovanih servera od velikog značaja je obezbediti pomoć lokalnog administratora mreže, ukoliko nije sam osumjičen, o tome kako je sistem konfigurisan, ili za izvlačenje traženih podataka. Neki put moguće je doći do traženih podataka i bez uzimanja imidža sa poslovnih računara, a nekada forenzičar mora razmatrati pažljivo, da li obarati server poslovne organizacije, ili tražiti druge načina za sakupljanje podataka. Generalno RAID diskovi na računaru predstavljaju ozbiljan problem, jer su specifični proizvodi i forenzičar mora znati da li su konfigurisani kao fizički, ili logički diskovi u kom slučaju treba uzimati *imidž* svih diskova odjednom.

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

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

1.2. Zaštita integriteta podataka i verifikacija

Jedan od kriterijuma za forenzičke alate za uzimanje imidža diska je da može verifikovati integritet fajla imidža diska. Za zaštitu i verifikaciju integriteta fajla imidža diska koristi se jednosmerna matematička funkcija, ili algoritam - heš (*hash*) informacije. Ova se funkcija lako računa u jednom, ali vrlo teško, ili nikakao u drugom smeru. Ako se izračuna heš jednog fajla dobije se vrednost heša, koja je istovetna vrednosti dobijenoj kod verifikacije heša istim algoritmom, samo ako se fajl nije menjao. Svaka, pa i najmanja promena u sadržaju fajla, menja vrednost heša, što ukazije da je integritet narušen. U digitalnoj forenzičkoj akviziciji i analizi podataka, heširanje i verifikacija heša imidž fajla obavezno je da bi forenzičar mogao dokazati na sudu da originalni imidž nije menjan i da je integritet originalnih podataka sačuvan. Na taj način operacija heširanja obezbeđuje princip zaštite integriteta, akvizicijom sakupljenih digitalnih podataka sa osumnjičenog računara i postaje obavezna funkcija savremenih forenzičkih alata. Efektivno se najviše koriste dva algoritma za heširanje: ***MD5*** i ***SHA1,*** [29], [26]. Verovatnoća da dva fajla sa različitim sadržajem imaju isti MD5 heš je 2^{128}, što je veoma sigurna zaštita integriteta. Promena samo jednog bita informacije menja heš vrednost te informacije, što je ilustrovano na sici 7.1.



Slika 7.1 *Ilustracija promene heša sa promenom jednog bita informacije*

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

REZIME

Digitalni forenzičar mora poznavati prirodu digitalnih podataka i kako rukovati sa njima. Digitalni podaci se mogu skladištiti u savremenim računarima u enormnim količinama, na HD kapaciteta od preko 700GB, ili na HD kapacitetima web servis provajdera na Internetu koji se još uvek slabo koriste. Forenzička analiza digitalnih podataka i računara došla je u fokus forenzičke nauke kao novi tip uzimanja dokaza, pored tradicionalnih vidova dokaza – otiska prsta, DNK, anlize krvi itd., uzimanjem *fizičke (miror slike, imidža*) ispitivanog računara u procesu koji obezbeđuju integritet ispitivanih podataka. Iako digitalna forenzika ima verifikovane metode i testove, uključujući široko prihvaćene hardverske i softverske alate, još je u ranoj fazi razvoja. Proces uzimanja *imidža* ispitivanog računara koristi jednostavan koncept kojeg izvršava alat dizajniran za tu namenu.

Razlozi za potrebu uzimanja *imidža* ispitivanog računara uvek su legalni. Zvanični organi istrage moraju na sudu dokazati da su digitalni podaci upravo onakvi kakvi su bili u računaru u trenutku pretrage i privremenog oduzimanja. Istraga kompjuterskog kriminala znatno je napredovala od kada sudija ne može da dovede u pitanje integritet digitalnog dokaza. Ako se dokazi ne mogu dovesti u pitanje, onda se može postaviti pitanje procesa korišćenog za dobijanje dokaza. Otuda potreba da se za izgradnju čvrstog digitalnog dokaza mora koristiti pouzdan metod. Kako uzimanje *imidža* ispitivanog računara obezbeđuje uzimanje svih raspoloživih dokaza, definisane su ključne karakteristike forenzičkih alata za uzimanje *imidža* ispitivanog diska (NIST), koji treba da: generišu fizičku sliku ispitivanog diska bit-po-bit; ne menjaju originalni disk; mogu verifikovati integritet fajli imidža diska; imaju poznate ulazne i izlazne greške logovanja; imaju dokumentaciju; obezbeđuju tačne rezultate i ne menjaju digitalne podatke. Preporučuje se uzimanje dve kopije *imidža* ispitivanog računara, jednu za analizu i drugu kao referentni original za potrebe suda. Pri tome je najbolji dokaz i najbliži stvarnom originalu, upravo referentna *imidž* kopija koja se čuva u lancu istrage za potrebe suda. *Imidž* originala obezbeđuje takođe i pravljenje više radnih kopija za eventualnu analizu na različitim mestima, ili u drugoj državi. Iz *imidža* se može i ponovo reprodukovati originalni disk.

Kod uzimanja *imidža* treba imati forenzički disk isti, ili veći od originalnog, ako kapacitet nije suviše velik, ili koristiti forenzičke alate za uzimanje *imidža* koji vrše i kompresiju signala na forenzičke diskove manjeg kapaciteta. Kod uzimanja *imidža* DOS diskova, forenzičari nemaju veće probleme, jer DOS veoma dobro štiti integritet podataka, što nije slučaj sa Windows OS. Otkada je Windows OS postao standard, digitalni forenzičari u procesu uzimanja *imidža* moraju koristiti blokatore upisivanja, da bi sačuvali integritet podataka.

Forenzičari mogu imati probleme kod uzimanja *imidža* HD smeštenog na glavnoj ploči, kao kod Laptop računara, jer uklanjanjem diska sa ploče podaci više nisu čitljivi, ili kod uzimanja *imidža* RAID diskova, jer forenzičar mora razumeti sve veze pre preduzimanja bilo koje akcije. Takođe, postojeći forenzički alati i oprema nisu dovoljni za akviziciju i analizu podataka sa *mainframe* servera. Forenzičar uvek treba da razmatra mogućnost korišćenja usluga administratora ispitivanog računarskog sistema, kao i selektivnog uzimanja *imidža* sa određenih medija i delova HD, ako istražitelj raspolaže sa preciznim podacima o kakvom tipu dokaza se radi i gde se mogu nalaziti u računarskom sistemu.

Za akviziciju i analizu digitalnih podataka postoje brojni forenzički alati, a najviše se koriste *En Case, Vogon, Safeback, iLook, FTK Imager i DD*. Funkcionalnosti relevantnih forenzičkih alata mogu varirati, pa ih je potrebno testirati. Uvek je za forenzičara najbolje rešenje uzeti *imidž* celog računara i ostalih medija, ili ih privremeno oduzeti. Postoji i alternativa uzimanju *imidža* diska, kao što je *kloniranje diska* pomoću alata tipa *Image Master Solo i Logicube*, posebno u slučajevima gde se pretraga vrši tajno i gde je kritična brzina akvizicije podataka.

U digitalnoj forenzičkoj akviziciji i analizi podataka, heširanje i verifikacija heša *imidž* fajla obavezno je da bi forenzičar mogao dokazati na sudu da originalni *imidž* nije menjan i da je integritet originalnih podataka sačuvan. Efektivno se najviše koriste **MD5** i **SHA1** algoritmi za heširanje.

PITANJA ZA PONAVLJANJE

1. Šta možemo reći da je osnova celokupnog kompjutersko-forenzičkog posla?
2. Zašto uzimanje *imidža* mora biti neinvazivna aktivnost?
3. Koji deo diska ili medija treba *imidžovati*?
4. Koji je krajnji rezultat uzimanja *imidža* sa nekog diska ili medija?
5. Koje su prednosti *imidža* u odnosu na bekapovanu kopiju fajlova?
6. Nakon uzimanja imidža, šta možemo da radimo s njim?
7. Navesti 5 NIST principa uzimanja imidža diska?
8. Prilikom uzimanja imidža, na koji način možemo da sačuvamo prostor na prijemnom disku?
9. Navesti neke od problema koji su se javili prilikom *imidžovanja* računara ili medija?
10. Koje su dve najčešće metode hešovanja u forenzici?

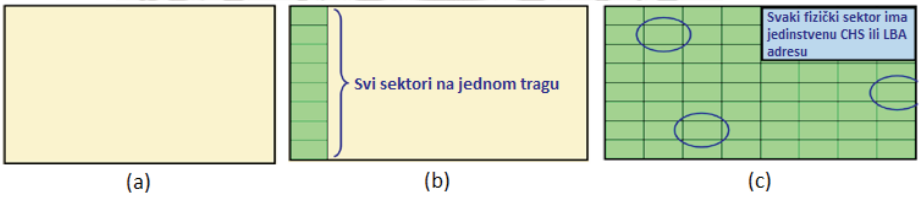
8 GEOMETRIJA DISKA

Da bi dobio podatke o tome kako je ispitivani disk organizovan i podeljen i gde su upisina fajlovi za analizu, forenzičar mora poznavati sledeća tri atributa, tzv. geometrije diska: *delenja diska na particije*, *formatiranje* i *označavanje diskova/particija,* [24].

8.1 Deljenje diska na particije

Poznavanje particija diska, značajno je da bi forenzičar mogao videti sve podatke na osumnjičenom disku, odnosno *imidžu* tog diska. Dobra praksa zaštite informacija sugeriše da se čvrsti disk u računaru obavezno podeli u najmanje dve particije - jedan za sistemske programe, a drugi za aplikacije i podatke, [13].

Prvi korak u podešvanju nekog diska za rad je deljenje diska na particije. Neka HD od 80 GB ima tri diska, ili 6 strana za upisivanje podataka. Za identifikovanje lokacije podataka koristi se tro-dimenzionalni sistem CHS adresiranja do veličine diska od 8,4GB, a za veće diskove LBA adresiranje. Ako se 80GB HD predstavi dvo-dimenzionalnim modelom, (slika 8.1), sektor LBA 0 biće u gorenjem levom uglu, a poslednji sektor u donjem desnom uglu.



Slika 8.1 *Dvo-dimenzionalni model fizičkog HD*

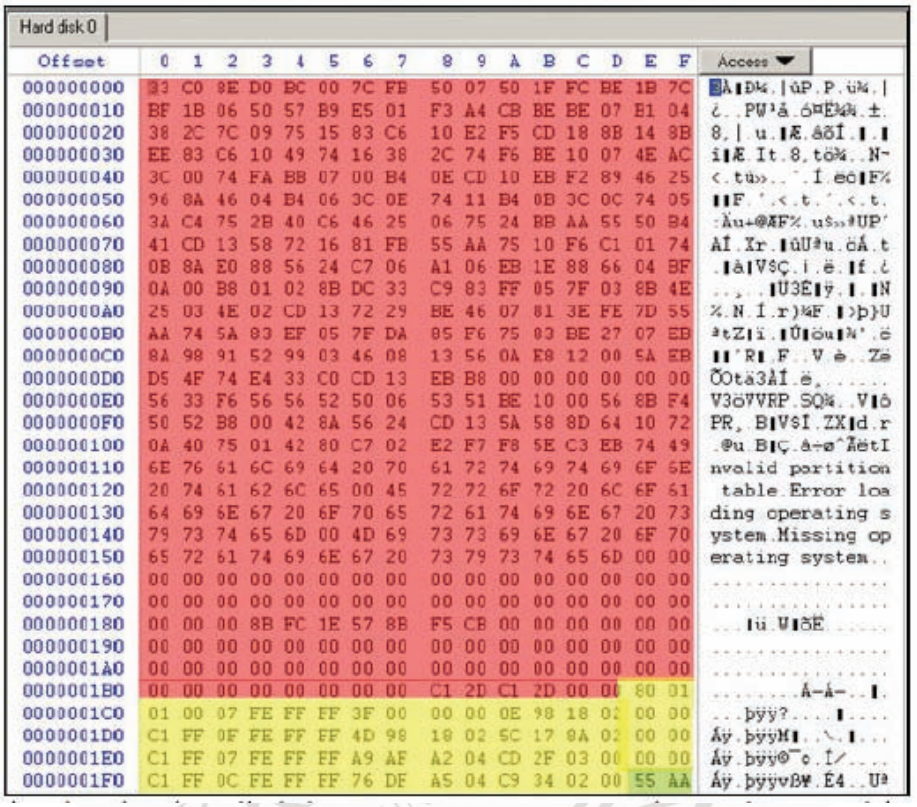
Dvo-dimenzionalni model fizičkog HD (a) dalje se segmentira u individualne, magnetski generisane oblasti za skladištenje podataka, koje se nazivaju **sektori**. Svi sektori u jednom tragu smešteni su u prvoj levoj koloni modela HD (b). Na fizičkom HD ovi su sektori smešteni na kružnom tragu i imaju trapezoidni oblik, a na 2-D modelu sektori se prikazuju jednakim pravougaonim segmentima (c). Ove sektore kreira proizvođač, koristeći

program za najniži nivo operacija. Uobičajena veličina sektora je **512 bajta**. Proces *formatiranja* HD na najnižem nivou polazi sa prvog gornjeg diska, cilindar po cilindar sa spoljne strane diska prema centru. Po završetku ovog procesa postavljeni su sektori na celom HD i svim njegovim površinama, a svaki sektor je jednozančno referenciran sa CHS, ili LBA vrednostima. U HD od 80GB ima oko 160.000.000 sektora.

Ovim je postavljanje bazične strukture HD izvršeno. Za prepoznavanje ove fizičke strukture računar koristi program za deljenje diska na particije tipa **FDISK** u DOS/Windows, **Partition Magic** i dr. Ovaj program obezbeđuje korisniku da izabere koji i koliki deo HD želi da koristi za svoje podatke i aplikacije. Ako korisnik na HD od 80GB želi imati samo jednu particiju, **FDISK** program za deljenje na particije prvo upisuje jedan sektor informacija u prvi sektor diska, lociran na CHS 0,0,1, ili LBA 0. Računar kasnije mora locirati ove informacije upravo tamo gde su upisane u predefinisanom postavljanju računara.

U sektoru 0 na fizičkom disku program za deljenje na particije upisuje informacije i taj sektor se naziva **MBR**-*Master Boot Record*. Na FD prvi sektor zove se *Boot Record* i FD se ne može deliti na particije. U MBR se upisuje neki kôd i **MPT** – *Master Partition Table,* koja sadrži informacije o organizaciji particija diska. U preostale sektore u prvom tragu u kojem je upisan MBR ne upisuje se ništa – samo nule. Međutim, neki specijalni softerski alati za šifrovanje diska, ili zaštitu pasvorda, mogu upisati podatke u ove sektore, [24], [25].

Digitalni forenzičar mora znati šta se tačno upisuje u MBR sektor koji je najznačajniji sektor na disku i bez njega je disk nekoristan. Na slici 8.2 koju generiše tipičan forenzički alat za analizu fajl sistema, MBR u heksa zapisu podeljen je u tri sekcije: crvenu, žutu i zelenu, [24].



Slika 8.2 *MBR u hex zapisu tipičnog forenzičkog alata za analizu fajl sistema*

Crvena sekcija predstavlja kôd (*Master Bootstrap Loader Code)* za upisivanje MBR. U Windows OS BIOS upisuje i izvršava ovaj kôd. U ASCII zapisu MBR sektora može se videti poruka o grešci koja se prikazuje ako MPT nije korektno konfigurisana.

Žuta sekcija MBR je **MPT** koja počinja od *ofseta* 446, računajući od početka MBR kôda i zauzima 66 bajta. MPT sadrži 4 ulaza (*entries*) od po 16 bajta. Maksimalan broj ulaza je 4, a minimalan - 1. Svaki ulaz sadrži važne informacije o nekoj particiji kao što su *tip, aktivnost, početak i kraj* particije. Nekorišćeni ulaz je popunjen sa nulama.

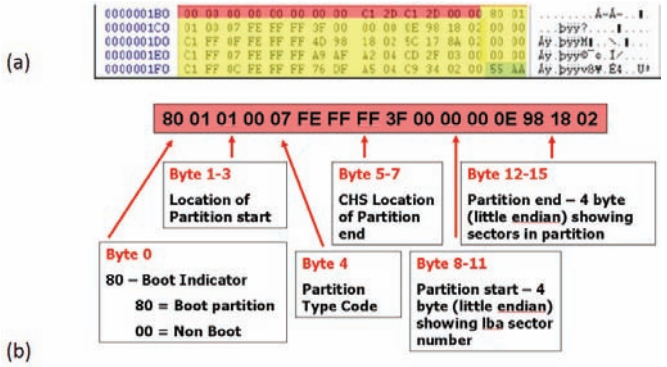
Zelena sekcija MBR sektora - 55 AA u heksa zapisu predstavlja potpis MBR sektora. Ovaj potpis koristi BIOS za proveru MBR podataka u toku butovanja. Ako potpis nije na mestu, dobije se greška poruke u ASCII zapisu.

U MPT tabeli mogu biti dva tipa particija: *primarna* i *proširena*. U svakoj MPT mogu biti do 4 primarne particije, ali samo 1 proširena particija. Primarna particija sadrži „logički disk“, koji je jednostavno deo HD kojeg OS tretira kao odvojenu jedinicu. Ako postoje dve primarne particije, svaka može da sadrži neki logički disk, a sistem će im normalno pripisati slova **C:** i **D:**. Logički disk u primarnoj particiji može se aktivirati nezavisno sa sopstvenim OS i fajl sistemom.

Proširena particija može biti samo jedna na fizičkom disku i definisana je svojom *particionom tabelom*, a ne sa MPT. Da bi se videlo kako je setovana proširena particija, potrebno je istu locirati u ulazu MPT, a zatim ići u lociranu particionu tabelu u aktuelnoj proširenoj particiji. Naravno sve ovo radi računar automatski. Particiona tabela je locirana u prvom sektoru proširene particije, pa je relativno lako pronaći. Particiona tabela može imati samo dva ulaza za - *logičku*, ili *proširenu* particiju. Ako se naprave dva logička diska u proširenoj particiji, oba se ne mogu definisati zajedno – svaki mora imati posebnu particionu tabelu. Ovo znači da u svakoj proširenoj particiji može biti određeni broj manjih proširenih particija, od kojih se svaka definiše sa drugom particionom tabelom. Teoretski nema ograničenja za proširene particije sve dok ima prostora na disku, ali ima ograničenja u broju slova koja se mogu dodeliti ovim particijama.

8.1.1 Glavna particiona tabela (MPT)

Glavna particiona tabela (MPT) počinje sa 446 ofsetom u MBR sektoru i zauzima 66 bajta sektora. Svaka linija sadrži 16 bajta. MPT počinje sa ulaznim bajtom „**80**“, a završava se potpisom MBR sektora – „**55 AA**“. Kako jdan ulaz koristi 16 bajta, sledeći ulaz počinje nakon 16 bajta i nalazi se tačno ispod ulaza „80“. Očigledno u ovoj MPT sva četiri entrija su korišćena – preostala tri počinju sa „**00**“ bajtom, (slika 8.3), [24].



Slika 8.3 *Glavna particiona tabela (a) i interpretacija 16 bajtova prvog* ***entrija*** *MPT tabele (b)*

Prvi *entri* (ulaz) od 16 bajta prikazan je na slici 8.4 (b) u jednoj liniji. Očigledno postoji značajna količina informacija u 16 bajta ovog *entrija*, koje su bitne za korektan rad drajva.

Bajt 0 je indikator aktivne particije – **80h** indicira da je particija aktivna, a **00h** - da nije aktivna. Aktivna particija sadrži sve informacije za proces butovanja.

Bajt 1-3 (brojanje počinje sa 0) pokazuje lokaciju starta particije drajva u CHS vrednostima, što je validno do 8.4 GB, a zatim nastupa LBA adresiranje.

Bajt 4 označava kod tipa particije, koji se pripisuje svakoj particiji na disku (drajvu). Ako OS u procesu butovanja prepozna ovaj ulazni bajt, pripisuje mu slovo za oznaku particije, a ako ne prepozna – ignoriše je. U tabeli 8.1 prikazana je lista značajnijih kôdova tipova particija, a sveobuhvatna lista se može skinuti sa Interneta. Iz tabele se, na primer, vidi da **07h** označava kôd HPFS/NTFS particije. Kôdovi tipa particije za sledeće tri particije (tačno ispod 07h) – **0Fh, 07h i 0C** ukazuju da je u pitanju proširena particija u Windows 95 OS, druga NTFS particija i particija FAT 32 fajl sistema, iako je ovaj primer uzet iz Windows XP OS.

Tabela 8.1 Lista značajnijih kôdova tipova particija

• 00 Empty	• 3C PartitionMagic recovery
• 01 DOS 12-bit FAT	• 43 Linux native (sharing disk with DRDOS)
• 04 DOS 16-bit FAT <32M	• 55 EZ-Drive (disk manager)
• 05 DOS Extended	• 64 Novell Netware 286
• 06 DOS 16-bit FAT >=32M	• 65 Novell Netware 386
• 07 HPFS / NTFS	• 70 DiskSecure Multi-Boot
• 0A OS/2 Boot Manager	• 82 Linux swap
• 0B Windows95 FAT32	• 83 Linux native(15)
• 0C Windows95 FAT32 (LBA)	• 84 OS/2 hidden C: drive
• 0E Windows95 FAT16 (LBA)	• 85 Linux extended
• 0F Windows95 Extended (LBA)	• 86 NTFS volume set
• 11 Hidden DOS FAT12	• 87 NTFS volume set
• 12 Compaq diagnostics	• F2 DOS 3.3+ secondary
• 14 Hidden DOS FAT16	
• 16 Hidden DOS FAT16 (big)	
• 17 Hidden HPFS/NTFS	

Bajt 5-7 u entriju MPT pokazuje CHS vrednost gde se particija završava.

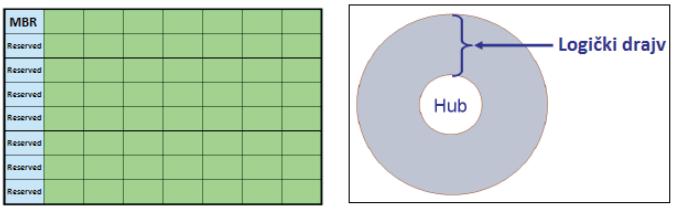
Bajtovi 8 -11 obezbeđuju LBA adresu početka particije zapisanu u *Little Endian*, što znači da je forenzičar mora invertovati da bi pročitao decimalni zapis iz hex zapisa.

Bajtovi 12 -15 pokazuju kraj LBA adrese particije.

Skrivene particije mogu se napraviti sa specijalnim kôdom za tip particije. Dobar primer skrivene particije je deo HD koje proizvođači odvoje za dijagnostiku softvera i alat za oporavak podataka. Ove particije mogu se videti sa specijalnim softverskim alatima koji menjaju tip kôda particije iz skrivenog u validno stanje, pa se ponovo skrivaju kada se problem fiksira. U MPT tabeli heksadecimalni bajtovi 14, 16 i 17 su svi validni kôdovi za skrivene particije, pa kada sistem otkrije ove kôdove normalno ignoriše ove particije i ne pripisuje im slova za oznaku diska. Za forenzičara problem nastaje ako u MPT naiđe na skrivenu particiju koja se razlikuje od prethodnih. Ove skrivene particije treba ispitati, jer mogu kriti kompromitovani materijal. Generalno, MPT i MBR sadrže mnogo informacija vitalnih za startovanje sistema i pozicioniranje podataka na disku.

8.1.2 Primeri analize MPT za različite particije diska

Primer 1*:* Neka je ceo HD ostavljen u jednoj particiji. MBR je smešten u sektoru 0, a ostatak prvog traga je rezervisan, (slika 8.4).



Slika 8.4 *MPT diska sa jednom particijom*

U MPT biće jedan ulaz, koji definiše ceo disk kao primarnu particiju. U reprezentaciji MPT sa **DiskEditor** alatom, **BIGDOS** ulaz pokazuje kôd tipa particije, *Boot marker* sa **Yes** označava aktivnu particiju, a startna i završna lokacija odgovarajuće ulazne bajtove iz 16-bitnih ulaza u MPT, relativni sektor je 63, a ukupan broj sektora particije iznosi 1024065 (slika 8.5).



Slika 8.5 *Informacije o MPT diska sa jednom particijom u* ***BIGDOS*** *DiskEditor alatu*

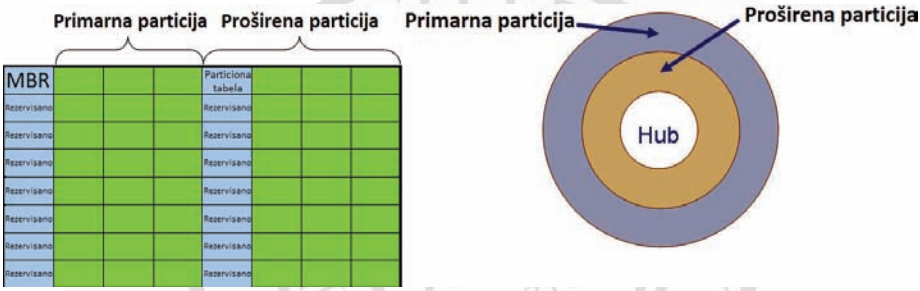
Ulaz (entry) relativnog sektore važan je za forenzičku analizu. Ulaz relativnog sektora je neki ofset od početka starta diska, posle prvog traga rezervisanih sektora u posle MBR zapisa. Particija počinje posle 63 sektora na disku što se vidi iz CHS vrednosti iz tabele, odnosno od 64 sektora u LBA adresiranju, gde brojanje počinje od 0. Kada se MBR upiše u prvom sektoru prvog traga (0), odnosno zauzme ceo prvi trag, sledeći podaci upisuju se u sledeći trag u prvom istom cilindru, a ne u trag 1, kako se može pomisliti. Zato se za bolje korišćenje CHS vrednosti za trag u MBR upisuje CHS vrednost 0,0,1, a zatim se inkrementalno menja vrednost H (glava), pa je CHS vrednost 0,1,1. Prva 53 sektora su sva na prvoj glavi, a 64 sektor je prvi sektor na drugoj glavi. Ovo može potvrditi primer iz tabele generisane sa **Nhorton Disk Editorom, (slika** 8.666).



Slika 8.6 *MPT u forenzičkom alatu* ***Nhorton Disk Editor***

Startna lokacija prikazana je kao Strana=*Side* 1 (kako alat zove glavu H), Cilindar 0, Sektor 1, tako da je CHS vrednost 0,1,1.

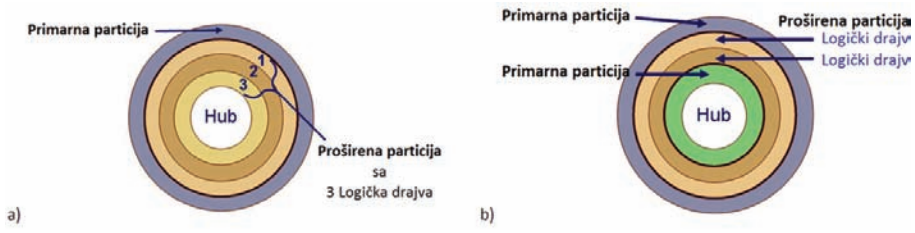
Primer 2: Neka disk ima primarnu i proširenu particiju, što znači da u MPT postoje dva ulaza, (slika 8.7).



Slika 8.7 *MPT diska sa primarnom i proširenom particijom*

U ovom slučaju prvi ulaz definiše primarnu particiju, a drugi proširenu particiju. Na preseku cilindera, vodi se kako su na disku smeštene primarna i proširena particija. Kako se iz MPT u **Disk Editor**-u na slici 8.7 vidi primarna particija završava u cilendru 79, glavi 254 i sektoru 63. Nova particija nikada, po konvenciji, ne počinje u sredini jednog cilindra, nego sa početka sledećeg cilindra, odnosno u ovom primeru-cilindra 80, glave 0 i sektora 1.

Primer 3: Neka HD ima jednu primarnu particiju i tri logička diska definisana u proširenoj particiji, (slika 8.8a).



Slika 8.8 *Položaj primarne i proširene particije sa tri logička diska (a)*

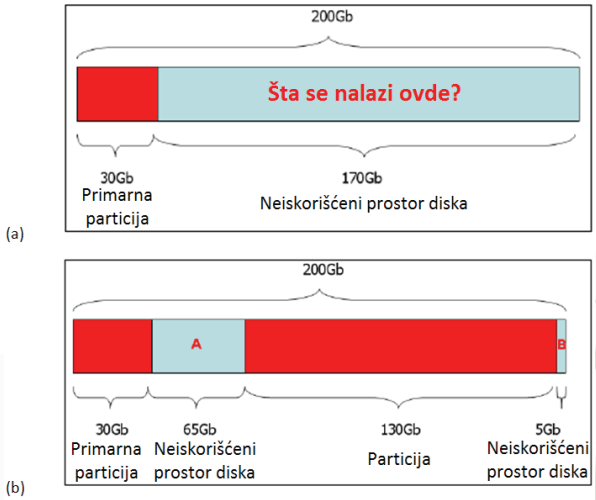
Na prvi pogled u MPT, ovaj HD treba da ima četiri ulaza, ali ih ima samo dva, zato što se u MPT mogu definisati četiri ulaza za primerne particije, ali samo jedan za proširenu particiju. Dakle, proširena particija mora uspostaviti svoj sistem administracije. Kako proširena particija mora imati svoje particione tabele, ovaj HD ima ukupno četiri particione tabele: MPT primarne particije, particiona tabela na početku proširene particije za logički disk 1, zatim particiona tabela za logički disk 2 i particiona tabela za logički disk 3. U primeru 4 jedan HD ima dve primarne particije i dva logička diska u proširenoj particiji, (slika 8.8b).

U MPT u ovom primeru postoje **tri** ulaza - za primarnua particiju u spoljnom delu diska, za celu proširenu partciju i za primrnu particiju u unutrašnjem delu diska. Takođe, ovaj HD ima ukupno tri particione tabele: MPT, particionu tabelu na početku proširene particije koja definiše prvu i drugu proširenu particiju i treću particionu tabelu koja definiše drugu unutrašnju primarnu particiju.

Forenzičar treba da zna kako je HD podeljen u particije da bi bio siguran da uzima *imidž* celog HD, vidi skrivene particije na disku i otkrije da li ima više OS na disku. Takođe, potrebno je razumeti koncept deljenja diska na particije, da bi se mogli razumeti računari sa *dualnim butovanjem* - sa dva i više različitih OS. Ako se striktno primene pravila uzimanja particija, onda uvek može postojati samo jedna primarna aktivna particija, koja će biti particija za butovanje. Ovo sprečava da jedan računar sa jedne primarne particije ima dualni sistem butovanja, koji omogućava korišćenje više OS. Da se obezbedi dualno butovanje, OS mora biti lociran na jednoj primarnoj particiji. Tako na jednom računaru može biti do četiri različita OS. *Računar se ne može butovati sa proširene particije*. Ne ulazeći u sve koncepte dualnog butovanja, dovoljno je reći da se proces butovanja mora prekinuti, kada računar traži aktivnu primarnu particiju i nudi opciju korisniku.

8.1.3 Nealocirani prostor diska

Neka računar ima HD od 200GB, a potrebno mu je samo 30GB prostora diska. Preostalih 170GB nekorišćenog prostora diska fizički postoji, ali nije adresiran u MPT, (slika 8.9), [24].



Slika 8.9 *Nekorišćeni prostor diska (a) i sumnjivo preoblikovanje particije diska (b)*

Ako je disk bio nov, a korisnik zauzeo samo 30GB, postoji mogućnost da u ostatak diska budu upisane sve same nule i taj se prostor naziva *nealocirani prostor* diska. Međutim, ako je ceo disk prethodno korišćen, a zatim particije preoblikovane, šta će biti preostlih 170GB diska? Pod uslovom da disk nije prepisan pre problikovanja particija, na tom delu diska još se uvek mogu naći podaci interesantni za forenzičara i mogu se otkriti odgovarajućim forenzičkim alatima. Neka sada korisnik sa softverom za particioniranje redefiniše particije na svom disku kao na slici 8.9b.

Forenzičara svakako interesuje kakve podatke može naći na ovako podeljenom disku u particijama **A** i **B**. Odgovor Nije izvesno, ali postoji verovatnoća da particija **A** od 65GB može sadržati skriveni kompromitujući materijal – dečiju pornografiju i slično.

8.2 Formatiranje diska

Posle deljenja diska na particije, potrebno je isti formatirati. Komanda računara za formatiranje inherentna je svim Microsft OS. Vremenom ova komanda je razvijena toliko da se može formatirati disk i inicijalizovati fajl sistem kojeg korisnik izabere, s tim da ga OS podržava. Da bi se razumeo proces formatiranja i fajl sistemi potrebno je analizirati osnovni fajl sistem – FAT[5] fajl sistem.

8.2.1 Formatiranje diska sa FAT16 fajl sistemom

U FAT fajl sistemu komanda za formatiranje kreira tri različite oblasti na logičkom disku i priprema disk za OS: *Boot record*, *Alakacione tabele fajl sistema* - FAT i *Root directory*. Ove oblasti se koriste da adresiraju i prate fajlove koji su uskladišteni na disku. Proces formatiranja različit je za FAT16 i FAT32 i moraju se razmatrati posebno. Ove razlike ilustrovane su u sledećoj tabeli koja prikazuje disk sa jednom primarnom i jednom proširenom particijom, (slika 8.10), [24].

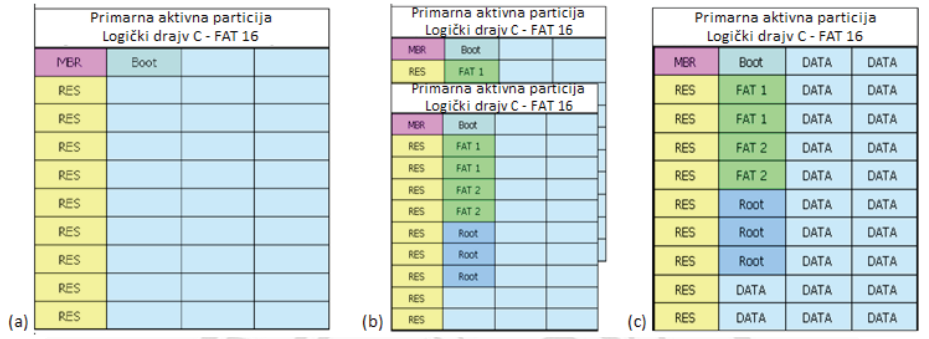
Primarna aktivna particija Logički drajv C - FAT 16				Proširena particija Logički drajv D - FAT 32			
MBR				PT			
RES				RES			
RES				RES			
RES				RES			
RES				RES			
RES				RES			
RES				RES			
RES				RES			
RES				RES			
RES				RES			

Slika 8.10 *Proces formatiranja za FAT16 i FAT32 fajl sisteme*

Levo je primarna particija formatirana sa FAT16 fajl sistemom. Na desnoj strani je logički disk u proširenoj particiji formatiran sa FAT32 fajl sistemom, da bi se ilustrovale razlike. U FAT16 formatu prvo se kreira *Boot record* (BR) za logički drajv lociran na prvom sektoru i zauzima jedan sektor. BR sadrži informacije o formatu logičkog drajva, uključujući informaciju proizvođača o

[5] *File Allocation System*

broju bajta po sektoru, broju sektora po klasteru, broju kopija FAT-a, maksimalnom broju ulaza u rut direktorijum, broju sektora po FAT, broju sektora po tragu, broju glava, oznaci o kapacitetu i opisu fajl sistema. Očigledno u BR svake particije ima značajan broj vitalnih informacija. Kada se sistem podiže, prvo ide u MBR da pronađe kako su particije podeljene na disku, a odatle ispituje BR svake particije da vidi kako su particije konfigurisane, (slika 8.11a).

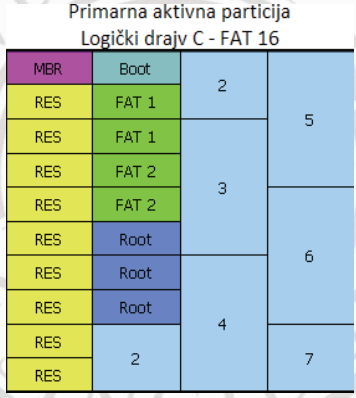


Slika 8.11 *Formatiranje FAT 16 fajl sistema*

Dalje format rezerviše prostor za prvu od dve fajl alokacione tabele (FAT). FAT je sistem pokazivača koji se koristi za praćenje tri traga: *fajlova na particiji, nealociranog prostora diska i defektnih oblasti logičkog diskova.* Broj sektora rezervisanih za FAT određen je veličinom particije. Posle prve FAT1 kreira se druga FAT2, kao bekap kopija FAT1. Kako se svaka FAT modifikuje, zadržavaju *sinhronizaciju*: FAT tabele moraju biti duplirane, ili će sistem pokazati grešku. Ovo je provera redundantnosti na sistemskom nivou. Posle kreiranja FAT tabela, kreira se *Rut direktorijum*, koji predstavlja listu fajlova na nivou ruta logičkog diska. Sadržaj rut direktorijuma u DOS OS nalazi se pod **C:**. U FAT16 sistemu kod starih OS (Windows 3.1) maksimalan broj ulaza koje rut direktorijum može imati je 512. Sa Windows 95A pojavio se koncept fajlova sa dugim imenom. To znači da svi fajlovi koriste najmanje dva ulaza direktorijuma – jedan fajlove sa kratkim imenom, drugi za fajlove sa dugim imenom, tako da se broj ulaza u Windows 95A najmanje prepolovio, (slika 8.11b).

Sve ovo do sada kreirano u FAT16 sistemu predstavlja sistemsku oblast – *But rekord, FAT tabele i rut direktorijum*. Ostatak oblasti particije koristi se za skladištenje podataka, (slika 8.11c).

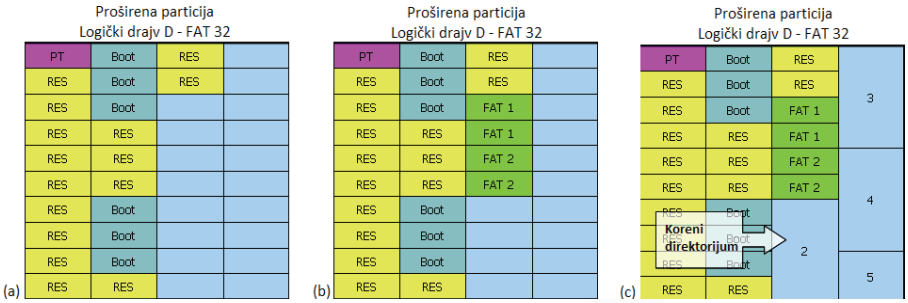
Dakle, formatiranje na najnižem nivou deli disk na upravljive segmente od po 512 bajta. U prvim diskovima malog kapaciteta sistem je mogao direktno upravljati sa sektorima tako da se ulaz u FAT tabeli direktno odnosio na sektor na logičkom disku. FAT16 ima ograničen broj alokacionih jedinica – sektora od $\mathbf{2^{16}}$ jedinica za skladištenje ili 65536 (0-65535) sektora, što daje *maksimalnu veličinu diska* od: 65536x512=33,554.432B, ili oko 33MB. Kada su diskovi prevazišli ovaj kapacitet, trebalo je pronaći novi metod adresiranja sektora na disku, što je dovelo do stvaranja koncepta ***klastera*** - grupe sektora, ili nove alokacione jedinice diska. Broj sektora korišćenih po klasteru određen je formatom i veličinom particije. Međutim, formatiranje može forsirati specifičan broj sektora po klasteru, ako to korisnik želi, a ako to fizički nije moguće, program za formatiranje to neće dozvoliti. Sada se ulazi u FAT tabeli odnose na klastere umesto na sektore. Brojanje klastera počinje sa 2, (slika 8.12).



Slika 8.12 *FAT tabela sa klasterima podataka u FAT 16 fajl sistemu*

8.2.2 Formatiranje diska sa FAT32 fajl sistemom

FAT32 fajl sistem sasvim je sličan sistemu FAT16. Neka je proširena particija formatirana kao FAT32. Formatiranje prvo kreira but rekord, ali dok je u FAT16 bio samo jedan, u FAT32 postoje dve kopije, svaka od po 3 sektora, za razliku od but rekorda FAT16 od jednog sektora. Ovi but rekordi su odvojeni sa 3 sektora rezervisanog prostora. Postoje dalje 23 rezervna sektora posle drugog but rekorda, što daje ukupno 32 sektora, (slika 8.13a).



Slika 8.13 *Formatiranje FAT 32 fajl sistema*

Posle but sektora u FAT32 formatiraju se dve sinhronizovane *fajl alokacione tabele*, zbog redundantnosti. Broj rezervisanih sektora za fajl alokacione tabele zavisi od veličine logičkog diska. U fajl sistemu FAT32 ovim je kompletirana sistemska oblast, (slika 8.13b).

U ovom fajl sistem *rut direktorijum* nije lociran u sistemskoj oblasti, nego u oblasti podataka, što omogućava da rut direktorijum, koji uvek počinje u klasteru 2, može rasti do bilo koje veličine, ograničene samo kapacitetom particije. Posle formiranja sistemske oblasti i rut direktorijuma, ostatak logičkog drajva formatiran je za korisničke podatke, (slika 8.13c).

Samo ime fajl sistema – FAT32 implicira da fajl sistem može alocirati $\mathbf{2^{32}}$ alokacionih jedinica - sektora, ili 4,294.967.296 sektora. Međutim u stvarnosti FAT32 koristi samo 28 bita, dok se najviša 4 bita ne koriste (zbog problema u *Scandisk* funkciji), što stvarno daje mogućnost adresiranja $\mathbf{2^{28}}$=268,435.456 alokacionih jedinica.

Razlike između FAT16 i FAT32 mogu se sumirati u sledećem, (slika 8.14):

1. FAT32 ima 2 kopije but rekorda, svaki dužine od po 3 sektora, a FAT16 jedan but rekord dužine 1 sektora;
2. FAT32 ima rut direktorijum lociran u oblasti podataka, ograničen samo veličinom particije, a FAT16 ima rut direktorijum u sistemskoj oblasti sa maksimalno 512 ulaza.
3. FAT16 koristi 16 bita za adresiranje klastera, a FAT32 koristi 28 bita i može adresirati više klastera.

FAT 16		FAT 32	
Logička veličina diska	Veličina klastera	Logička veličina diska	Veličina klastera
< 128 MB	4 Sektora (2KB)	< 512MB	Ne podržava
128MB – 255MB	8 Sektora (4KB)	512MB – 8GB	8 Sektora (4KB)
256MB – 511MB	16 Sektora (8KB)	8GB – 16GB	16 Sektora (8KB)
512MB – 1GB	32 Sektora (16KB)	16GB – 32GB	32 Sektora (16KB)
1GB – 2GB	64 Sektora (32KB)	32GB – 2TB	64 Sektora (32KB)

Slika 8.14 *Razlike FAT 16 i FAT 32 fajl sistema*

Neka je particija veličine 1,5MB. Ako je formatirna u FAT16 fajl sistemu podrazumevana veličina alokacionih jedinica biće 64 sektora. Ako je isti disk formatiran u FAT32 fajl sistemu, alokaciona jedinica biće 8 sektora. Kako se veličina alokacione jedinice odražava na skladištenje podataka? OS skladišti svaki fajl, veći ili manji, u svaku alokacionu jedinicu. Novi fajl popunjava sledeću praznu alokacionu jedinicu do kraja, a ako preostane neki fragment upisuje ga u sledeću alokacionu jedinicu, tako da i mali fragment velikog fajla može zauzeti celu alokacionu jedinicu bez obzira kolike je veličine. Na primer, neka je fajl 100B dužine. U FAT16 fajl sistemu alokaciona jedinica od 64 sektora je stvarne veličine od 32kB (oko 32,000B). Fajl od 100B upisuje se u alokacionu jedinicu, a ostaje nezauzetih 31.900B, koji se mogu koristiti za druge namene, ili ostati neiskorišćen prostor za korisnika. Ako se isti fajl upisuje u FAT 32 fajl sistem, alokaciona jedinica je samo 8 sektora veličine - ili 4kB, ili oko 4.000B. Ako se fajl upiše u ovu alokacionu jedinicu, ostaje 3900B neiskorišćenog prostora, što ovaj fajl sistem čini efikasnijim od FAT16 fajl sistema.

Dakle, sa aspekta forenzičke analize što je veća alokaciona jedinica to je ona bolja za forenzičara, jer može sadržavati potencijalno više digitalnih dokaza.

8.2.3 Forenzičke implikacije formatiranja diska

Svaki put kada se neki disk formatira, odvija se proces upisivanja but rekorda, ili prepisivanja, ako je već upisan. Zatim se FAT tabele prepisuju sa nulama, a brišu svi ulazi čime su sve alokacione jedinice na disku na raspolaganju sistemu. Rut direktorijum se takođe menja, ili se kreira na novom disku, ili prepisuje ako se formatira korišćeni disk. Međutim, *oblast podataka, koja je od osnovnog interesa za forenzičara, u standardnom formatiranju ostaje nedirnuta*. U FAT sistemu formatiranjem se gube svi pokazivači za podatke,

imena fajlova i svojstva koja su sadržana u ulazu direktorijuma, koji je upravo nuliran sa formatiranjem. Forenzički alati omogućuju pretraživanje podataka prema ključnoj reči, koja se obezbeđuje u odnosu na predmet i karakter slučaja kompjuterskog kriminala, pretraživanje grafičkih fajlova i oporavak fajlova iz informacija hedera. Isto je kod formtiranja FD, u većini slučajeva podaci će ostati. Izuzetak je korišćenje bezuslovne „**/u**“ komande u DOS OS za formatiranje FD, koja prepisuje sve podatke u oblasti podataka. Uobičajene komande koje se koriste za formatiranje su, [7]:

1. *Format* – standardni format koji aktivira *Scandisk* čekiranje integriteta celog diska;
2. *Format*/u – bezuslovni format u Windows9x OS;
3. *Format*/q – brzo formatiranje koje ne koristi *Scandisk*;
4. *Format*/s – standardni sistemski format koji postavlja sistemske fajlove na disku IO.SYS, MSDOS.SYS&COMMAND.COM.

8.2.4 Formatiranje logičke particije sa NTFS fajl sistemom

NTFS fajl sistem nema posebnu sistemsku oblast koja se koristi da održava tragove fajlova i obezbeđuje sistemske informacije. U ovom sistemu ***sve***, bukvalno ***sve*** se skladišti kao fajl. Fajlovi koji kontrolišu sistem označeni su znakom „**$**“ ispred fajla, radi lakše identifikacije, (slika 8.15).

MBR	DATA	DATA	DATA
RES	DATA	DATA	DATA
RES	DATA	DATA	DATA
RES	DATA	DATA	DATA
RES	DATA	DATA	DATA
RES	DATA	DATA	DATA
RES	DATA	DATA	DATA
RES	DATA	DATA	DATA
RES	DATA	DATA	DATA

Slika 8.15 *Formatiranje NTFS fajl sistema*

Interno, NTFS poznaje samo klastere, ili alokacine jedinice, dok uopšte nije svestan veličine sektora fizičkog diska. Sistem brojanja logičkih klastera sličan je LBA brojanju, ali umesto na fizičkom disku, klastere broji na logičkom disku. Zato se u NTFS fajl sistemu alokacija prostora na disku vrši sa ***run***

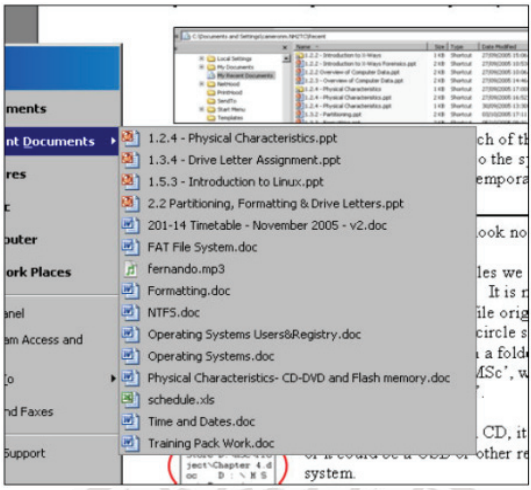
listom i pokazivačima. Unutar nekog fajla, NTFS se odnosi na podatke koji koriste *brojeve virtuelnih klastera*, a koji počinju sa prvim klasterom fajla. Dok je brojanje logičkih klastera neprekidno počevši od prvog klastera (klaster 0), brojanje virtuelnih klastera ne mora biti neprekidno i može se mapirati sa svakim brojanjem logičkih klastera na disku, [7], [24].

NTFS ima fajlove koji izvršavaju iste funkcije kao i sistemske oblasti u FAT sistemima. But rekord je zamenjen sa fajlom $BOOT, lociranim u prvom sektoru na logičkom drajvu kao i But rekord u FAT sistemima. Ovaj fajl sadrži važne informacije o konfigurisanju particije. FAT tabela je zamenjena sa fajlovima $BITMAP i $BADCLUSTER, koje mapiraju upotrebu diska. NTFS koristi 64 bita za brojanje klastera, ali kodira ih sa manje bajta po alokacionoj jedinici. Maksimalna veličina nekog fajla u NTFS sistemu je veličine 2^{64}= 16,446,744, 073,709,551,616B (bajta).

8.3 Označavanje diskova računara

Windows OS posle deljenja čvrstog diska na particije i formatiranja particija, označava particije diska pripisivanjem slova svakoj particiji diska da bi ih sistem mogao prepoznati. Slova **A** i **B** već su rezervisana za flopi diskove (FD). Sledeći istu logiku čvrsti disk (HD) dobio je za oznaku slovo **C**. Većina korisnika ima samo **C** disk u svom računaru – jedini fizički disk. Ako se u računar ugradi CD drajv, sistem mu automatski pripisuje slovo **D**. Ovo označavanje čini se jednostavno kod starijih sistema. Postoje pravila na osnovu kojih korisnik može videti kako su računar i diskovi konfigurisani. Novi OS Windows 2000 i XP otežavaju razumevanje pripisivanja slova i označavanja diskova u računaru, što može izazvati određene probleme za digitalne forenzičare, [24].

U normalnom računarskom sistemu može biti više referenci na oznaku drajva koji je izvor nekog dokumenta, ili fajla. Najbolji primer je **My Recent Document** meni (slika 8.16) do kojeg se dolazi otvaranjem prozora **Start**, a selektovanjem dobije se prozor sa 15 efektivnih prečica do dokumenta koje je korisnik nedavno otvarao na sistemu.



Slika 8.16 ***My Recent Document*** *u Windows OS*

Sistem pored poslednjih 15 dokumenata, čuva brojne prečice do drugih dokumenata, koje referencuiraju ime fajla i lokaciju. Ovo omogućava forenzičaru da identifikuje moguće priključivanje drugih medija na računar. Sistem koristi slova drajvova i ime fajla da bi mogao pratiti trag ove informacije i dovesti korisnika do korektnog dokumenta. Osim što su namenjeni za komforan rad korisnika, ukazuju forenzičaru kako je konfigurisan računar i gde mogu naći određeni dokument. Ne retko forenzičar naiđe na referentni sistem oznaka drajvova koji ne postoji na privremeno oduzetom osumnjičenom računaru. Ovo ukazuje da su drugi spoljni, pokretni mediji priključivani na sistem. U svakom slučaju forenzičar mora otkriti šta se dešavalo na sistemu. Cela oblast oznaka drajvova na računaru može biti komplikovana, pa računar uključen sa jednom konfiguracijom može biti sa savim drugom konfiguracijom kod sledećeg uključivanja, zbog dodavanja pokretnih medija i sposobnosti sistema da fiksira slova za oznake drajvova.

Kolaborativni rad OS i fajl sistema omogućava korisniku da upravlja podacima i obezbeđuju funkcinisanje sistema za pripisivanje slova drajvovima. Fajl sistem određuje kako su fajlovi uskladišteni i organizovani na particijama diska. OS je interfejs između računara i korisnika. Međutim, neki OS ne mogu prepoznati neke fajl sisteme i u tom slučaju pripisivanje slova za oznaku drajvova dovodi do konfuzije, što se može videti u tabeli 8.2.

Tabela 8.2 Uporedna tabela Windows OS i fajl sistema koje podržavaju

Operativni sistem	**Fajl sistem**
DOS 6.22	FAT12. FAT16
Windows 95a	FAT12. FAT16
Windows 95b	FAT12. FAT16, FAT32
Windows 68(SE)	FAT12. FAT16, FAT32
Windows ME	FAT12. FAT16, FAT32
Windows NT 4.0	FAT12. FAT16, NTFS
Windows 2000	FAT12. FAT16, FAT32, NTFS
Windows XP	FAT12. FAT16, FAT32, NTFS

Na primer, ako koristimo Windows 98 OS, ne možemo videti sadržaj logičkog diska koji je formatiran u NTFS fajl sistemu, zato što ovaj OS ne prepoznaje NTFS fajl sistem. Ako isti disk stavimo u računar sa Windows 2000 OS, particija će biti vidljiva.

DOS/Windows OS u procesu butovanja pripisuju slova drajvovima po standardnim pravilima. Ova se pravila mogu izmeniti kod nekih OS, kao što je Windows XP. Korisnik može očekivata da kada uključi računar sa dodatnim drajvom, da računar kod butovanja pokaže predefinisanu konfiguraciju, a zatim naknadno doda oznaku priključenog drajva. Ovo nije slučaj, jer postoje standardna pravila po kojima računar alocira i označava slova drajvova. Da bi se ova pravila primenila i razumeo proces pripisivanja slova drajvovima i konfigurisanja particija računara, forenzičar mora poznavati, [7], [24]:

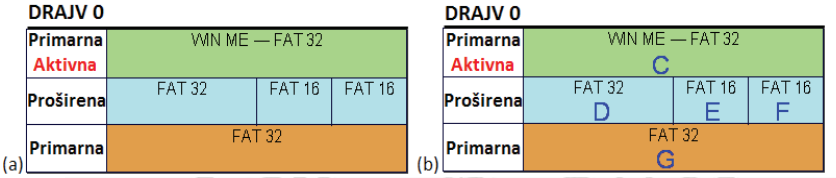
1. OS koji se koristi za podizanje (butovanje) sistema;
2. Strukturu particija diskova u sistemu;
3. Prvi sistem koji se nalazi na svakom logičkom disku;
4. Pravila po kojima računar alocira i označava slova diskova/particija:
   - ***Pravilo 1***: Prvoj primarnoj particiji na disku daje se uloga aktivne primarne particije i označava se prvim raspoloživim slovom (**C:**).
   - ***Pravilo 2***: Logički drajv u proširenoj particiji, prvi po redu fizičke lokacije od početka diska, označava se sledećim slovom.

- ***Pravilo 3***: Druga primarna particija, kako se nalazi u MBR označava se sledećim slovom.

5. Da se jedno pravilo mora primeniti na sve diskove (particije) u računaru, a zatim se prelazi na sledeće pravilo.

8.3.1 Primeri označavanja diskova računara

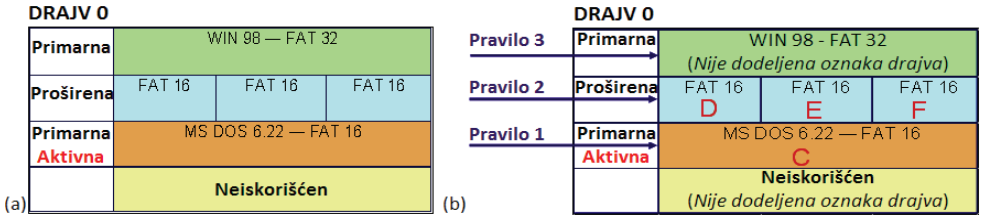
Primer 1: Neka računar sa Windows ME OS i FAT32 fajl sistemom ima samo jedan fizički HD podeljen na određeni broj primarnih i proširenih particija, (slika 8.17a).



Slika 8.17 *Pravila označavanja particija na jednom HD*

Primenjujući **Pravilo 1** prvo slovo – **C** pripisuje se *Aktivnoj primarnoj particiji*. Važno je znati koji je OS instaliran i koje fajl sisteme prepoznaje. Očigledno OS će prepoznati particiju sa koje se podiže i pripisaće joj slovo **C:**. Pošto postoji samo jedan fizički disk time je pravilo 1 kompletirano. Sada se primenjuje **Pravilo 2.** Traže se logički diskovi u proširenoj particiji i otkrivaju tri. Proverava se da li OS koji butira računar prepoznaje svaki od njih. Kako su svi sa FAT32 fajl sistemom, OS ih prepoznaje i po redu otkrivanja pripisuje sedeća slova **D:**, **E:** i **F:**. Time se prvilo 2 kompletira pošto postoji samo jedan fizički disk. Za **Pravilo 3**, tražimo bilo koju drugu primarnu particiju po redu u kojem se nalaze u MBR. U ovom slučaju nalazi se jedna primarna particija, formatirana u FAT32 kojeg OS prepoznaje. Ovoj particiji sistem pripisuje slovo **G:**, (slika 8.17b).

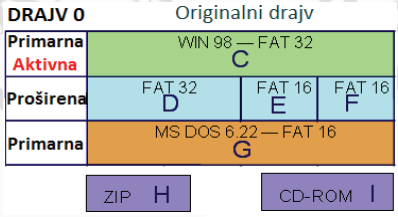
Primer 2: Neka se računar sa Windows 98 OS i FAT32 fajl sistemom, ima jedan HD na kojem ima MS DOS particiju formatiranu u FAT16 fajl sistemu, (slika 8.18a). Prema **Pravilu 1** sistem traži prvu a*ktivnu primarnu particiju* i pripisuje slovo **C:** MS DOS particiji sa koje se butuje. Kako postoji samo jedan HD, pravilo 1 je kompletirano.



Slika 8.18 Označavanje particija na jednom HD sa tri particije i dva fajl sistema

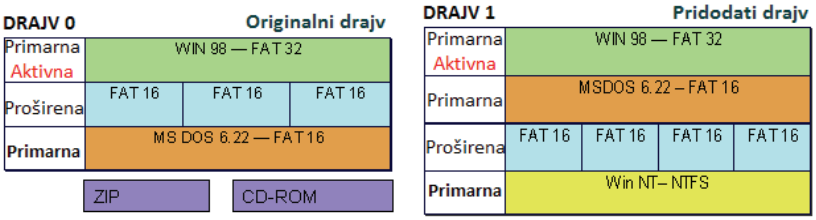
Prema **Pravilu 2** traže se logički drajvovi u proširenoj particiji. Nalaze se tri logička drajva formatirana u FAT16 fajl sistemu koje OS prepoznaje i označavaju sa **D:, E:** i **F**:. Ovim je Pravilo 2 kompletirano. Prema **Pravilu 3** traže se druge primarne particije po redu kako su upisane u MBR i označavaju dalje one čije fajl sisteme OS prepoznaje. U ovom slučaju OS je Windows 98 sa FAT32 fajl sistemom i zato particije neće biti označene, jer MS DOS ne prepoznaje FAT32 fajl sistem, (slika 8.18b). Dakle, na disku će biti jedna neadresirana oblast. U ovom primeru postoji samo jedna nekorišćena oblast, što znači da u MBR nema ulaza za ovu oblast. Ako sistem ne vidi određenu particiju neće je označiti slovom. Ali forenzičar ne može znati šta može biti na tom delu diska.

Primer 3: Neka računar sa jednim HD ima CD ROM i ZIP particije. Primena pravila za pripisivanje slova particijama su kao na slici, 8.19.



Slika 8.19 Označavanje particija na jednom HD sa 3 particije i sa CD ROM i ZIP particijma

Primer 4: Naka se računaru doda drugi čvrsti disk, koji može biti podešen sa HD koji je već u računaru, ili uzet sa drugog računara, (slika 8.20). Naravno, u slučaju forenzičke istrage ne treba nikada priključivati osumnjičeni disk sa originalnim dokazima u drugi računar, jer postoji verovatnoća da će se uneti neke izmene dokaza.

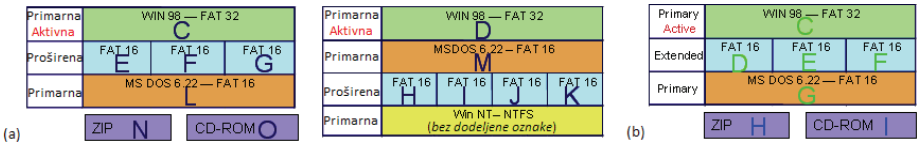


Slika 8.20 Označavanje particija na dva HD sa ZIP i CD ROM particijama

Levi HD je originalni, a desni naknadno dodat računaru. Pravila pripisivanja slova particijama primenjuju se jedno po jedno na svaku particiju u računaru čije formate OS prepoznaje. **Pravilo 1** se primeni na prvu primarnu particiju koja je aktivna. Računar se podiže sa originalnog HD, gde je primarna aktivna particija sa Windows 98 OS, formatirana u FAT32 fajl sistemu. Sada je OS kritičan faktor za ono što se može videti na oba diska. Tako se **C:** pripisuje originalnom HD, a zatim se **Pravilo 1** primenjuje na dodati HD, pa se slovo **D:** pripisuje FAT32 particiji aktivnoj na dodatnom disku, zato što ga OS za butovanje prepoznaje. Time je primena pravila 1 kompletirana.

Pravilo 2 se prvo primenjuje na originalni HD. Postoje logički diskovi u proširenoj particiji i svi su formatirani u FAT16 fajl sistemu, kojeg butabilni OS Windows 98 prepoznaje, pa ih označava sa **E:, F:** i **G:.** Dalje se Pravilo 2 primenjuje na dodati HD gde postoje 4 logička diska u proširenoj particiji formatirana u FAT 16, kojeg butabilni OS Windows 98 prepoznaje i pripisuje sledeća slova **H:, I:, J: i K**:. Ovim je Pravilo 2 kompletirano.

Pravilo 3 se prvo primenjuje na butabilni HD. Traže se druge primarne particije i postoji jedna formatirana u FAT16 fajl sistemu koju butabilni sistem prepoznaje i pripisuje slovo **L:**. Zatim se Pravilo 3 primenjuje na dodatni HD. Postoje dve primarne particije, jedna formatirana u FAT16, a druga u NTFS. Butabilni OS Windows 98 prepoznaje FAT16, ali ne i NTFS fajl sistem, zato pripisuje slovo **M:** prvoj particiji sa FAT16 fajl sistemom. Kada pripiše slova svim fiksnim drajvovima, sistem traži druge, počevši sa ZIP drajvom, zatim CD-ROM-om i pripisuje slova **N:** i **O:**. Konfiguracija sistema izgleda kao na slici 8.21a.

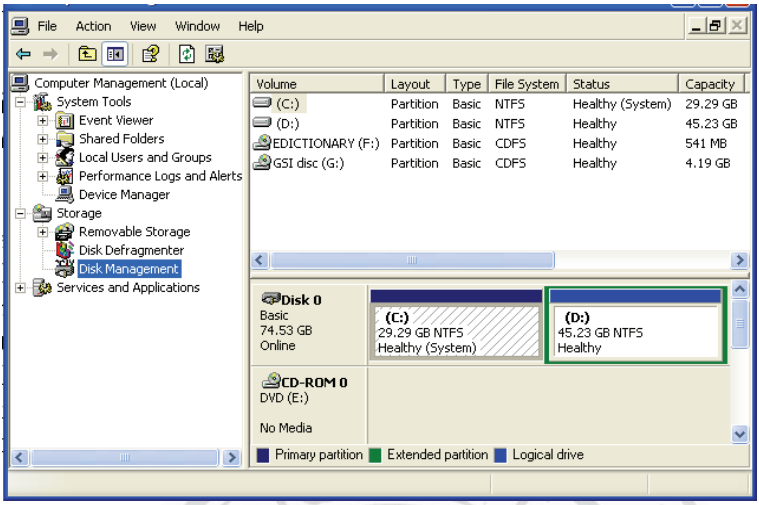


Slika 8.21 *Označavanje particija u slučaju skidanja i ponovnog dodavanja drugog diska*

Ako pogledamo kako je izgledala konfiguracija butabilnog HD pre dodavanja drugog HD i neka, na primer, postoji dokument na dodatnom HD uskladišten na particiji **J:**. Kada se dodatni HD ukloni. Dokument više nije priključen na sistem, ali može imati referencu na butabilnom HD. U drugom slučaju dokument može biti na butabilnom HD u particiji **D:,** pri čemu su sve ponovo označene, **(slika** 8.21b). Ako se računaru doda drugi HD, na primer forenzički, sada je particija **D**: na tom disku, što za forenzičara može predstavljati problem, ako ignoriše ova pravila.

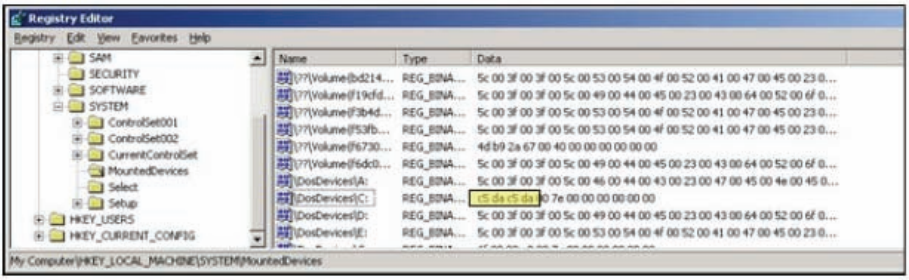
U određenim OS kao što su Windows 2000 i XP svako sa administrativnim pravima može pripisati različita slova particijama diska i učiniti ih polu-privremenim, što dodatno komplikuje rad forenzičara. Izuzetak je za sistemsku i butabilnu particiju koje zadržavaju svoja slova. Ova se slova mogu promeniti izmenom *Boot.ini* fajla.

Ovo se izvršava sa konzole za upravljanje računarom, koja se otvara desnim tasterom miša na *My Computer* i izborom *Mange*, a zatim *Disk Management*. Dobije se prozor *Computer Management*. Sve particije na računaru su prikazane i mogu se odavde upravljati, uključujući kreiranje, brisanje i formatiranje. Jedna opcija je izmena oznake particije i svako raspoloživo slovo može se pripisati logičkom disku (drajvu), što može izazvati problem forenzičaru. Svako proizvoljno pripisivanje slova logičkim particijama diska koje ne sledi pravila, otežavaju forenzičaru da razume kako je konfigurisan HD računara, (slika 8.22) .



Slika 8.22 *Prozor **Disk Management** za upravljanje particijama u Windows XP OS*

Svako dodavanje novog HD, ili priključivanje prenosnog diska ostavlja trag u računaru i omogućava forenzčaru da rekonstruiše šta se dešavalo na računaru. Ovi tragovi nalaze se u Regitru (*Registry*) u ključu HKEY_LOCAL_MACHINE/System/Mounted Devices, gde su registrovani svi priključivani drajvovi (logički, floppy, CD, DVD, FLASH USB) na sistem i koje su slovo za označavanje dobili, (slika 8.23).



Slika 8.23 *Trag particije u ključu Regitra otkriven **Registry Editor**-om Win XP OS*

Podaci u ključu Registra zapisuju se u heksadecimalnom kôdu. Iz sledeće tabele vidi se da **C:** disk na ovom računaru počinje sa **C5 DA 3F 00.** Iako ovo nije garantovan metod čini se da važi za većinu HD koji se priključuju na računar, gde se deo informacije koja se nalazi u MBR (neposredno ispred MPT tabele) unosi u ključ Registra, (slika 8.24), [24].



Slika 8.24 *Trag imena particije u MBR*

U MBR sigurno postoji samo jedan ulaz za svako slovo particije i odnosi se na poslednji uređaj koji je koristio to slovo. Na vrhu MBR vidi se da promenljivi diskovi **A** i **B** imaju ključeve koji počinje sa **5C DA 3F 00.** Eksperimenti pokazuju da je ovo potpis koji sistem upisuje u Registar za promenljive diskove kao što su FD i USB drajvovi. Međutim, eksterni USB priključen na XP sistem ostavlja isti trag kao normalni interni HD.

8.3.2 Dugačka imena fajlova

U starijim OS DOS i *Windows 3.1* postojala je striktna konvencija za imenovanje fajlova i dirktorijuma – **pravilo „8.3**“. Prefiks imena fajla mogao je imati najviše **8** karaktera, a ekstenzija najviše **3** karaktera, zatim sva slova morala su biti velika, neki karakteri su rezervisani za upotrebu i postojala je maksimalna dužina putanje/imena fajla od **78** karaktera. OS *Windows 95* je izmenio ova pravila. Slova nisu morala biti velika, manji broj karaktera je bio u rezervi, a broj karaktera putanje/imena fajla porastao na **258** karaktera, što je poznato kao **LFN** (*Long File name*)–dugačko ime fajla. Pored toga sistem je morao imati za svaki fajl kreirano ime za kratko ime fajlova–**SFN** (*Short File Name*), ukoliko LFN ne zadovoljava **„8.3“** pravilo. Ako sistem kreira *SFN* i *LFN*, sva svojstva fajla, kao što su veličina, početni klaster, atributi i informacije o datumu/vremenu, pripisuju se SFN radije nego LFN sistemu imenovanja fajlova.

Za kreiranje SFN imena fajla, sistem uklanja sve rezervisane karaktere, a zatim prevodi prefiks u 6 karaktera sa simbolom *tilda* (**~)**, a inkrementalno brojanje počinje sa 1. Zatim se dodaju tri karaktera ekstenzije, a sve konvertuje u velika slova. Važno je znati da SFN mora biti u kontinuitetu sa LFN u ulazu (*entriju*) direktorijuma, tako da se interpretiraju zajedno. U tabeli

8.3 na levoj strani dati su primeri formiranih LFN, a na desnoj – konvertovan LFN/SFN. Vidi se da fajl bez ekstenzije nema konvertovani par, fajl sa više tačaka gubi sve tačke osim poslednje, ime sa razmakom gubi razmak, a fajlovi koji će imati isto ime u istom direktorijumu kada se skrati ime počinju proces inkrementacije, [24].

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

Tabela 8.3 Konverzija LFN/SFN imena fajla

LFN	**LFN Alias/SFN**
LongFileName	LONGFI~1
File.Name.With.Dots	FILENA~.DOT
Name with sith space	NAMEWI~1
Name with sith space again!	NAMEWI~2
.Name beginning with dot	NAMEBE~1

Pošto kratko ime fajla ne može početi sa tačkom, ona se ispušta. Ako ima, na primer, 9 fajlova sa istim imenom, umesto prvih 6 karaktera, koristi se prvih 5, a dodaje simbol „**~**“ pre početka brojanja od 10 do 99. Više od 100 fajlova imaće samo 4 karaktera pre „**~**“ simbola, a ako postoji više fajlova od toga, nešto nije u redu sa maštom korisnika za imenovanje fajlova.

Za digitalnog forenzičara od velike dokazujuće vrednosti su duga imena fajlova (LFN), koji mogu biti vrlo deskriptivni i ukazivati na sadržaj.

REZIME

Da bi dobio podatke o tome kako je ispitivani disk organizovan i podeljen i gde su upisina fajlovi za analizu, forenzičar mora poznavati tzv. geometriju diska, tj. *delenje diska na particije*, *formatiranje* i *označavanje diskova/particija.* Iz particija diska forenzičar može videti sve podatke na *imidžu* osumnjičenog diska.

Proizvođač u procesu *formatiranja* HD na najnižem nivou, polazeći sa prvog gornjeg diska, cilindar po cilindar sa spoljne strane diska prema centru, formira bazičnu strukturu alokacione jedinice – sektore od 512 bajta na HD, koristeći program za najniži nivo operacija. Za prepoznavanje ove fizičke strukture računar koristi program za particioniranje (**FDISK**, **Partition Magic** i dr).

U sektoru 0 na fizičkom disku program za particioniranje upisuje **MBR**-*Master Boot Record*. Na FD prvi sektor zove se *Boot Record* i FD se ne može deliti na particije. U MBR se upisuje (*Master Bootstrap Loader Code)* kôd za upisivanje MBR, kojeg upisuje i izvršava BIOS i **MPT** – *Master Partition Table,* koja sadrži informacije o organizaciji particija diska, zauzima 66 bajta i sadrži 4 ulaza od po 16 bajta, sa informacijama o *tipu, aktivnosti, početku i kraju* particije. Nekorišćeni ulaz je popunjen sa nulama. U preostale sektore u prvom tragu u kojem je upisan MBR upisuju se samo nule, ali neki specijalni softerski alati za šifrovanje diska, ili zaštitu pasvorda, mogu upisati podatke u ove sektore. Digitalni forenzičar mora znati šta se tačno upisuje u MBR sektor koji je najznačajniji sektor na disku i bez njega je disk nekoristan.

Heks potpis MBR-55 AA koristi BIOS za proveru MBR podataka u toku butovanja. Ako potpis nije na mestu, dobije se greška poruke u ASCII zapisu. U MPT tabeli mogu biti do 4 *primarne* i samo 1 *proširena* particija. Primarna particija sadrži „logički disk"- deo HD kojeg OS tretira kao odvojenu jedinicu. Ako postoje dve primarne particije, svaka može da sadrži neki logički disk, a sistem će im normalno pripisati slova **C:** i **D:**. Logički disk u primarnoj particiji može se aktivirati nezavisno, sa sopstvenim OS i fajl sistemom. Proširena particija definisana je svojom *particionom tabelom*, a ne sa MPT. Particiona tabela je locirana u prvom sektoru proširene particije, pa je relativno lako pronaći, a može imati samo ulaze za *logičku*, ili *proširenu* particiju. U svakoj proširenoj particiji može biti određeni broj manjih proširenih particija, od

kojih se svaka definiše sa drugom particionom tabelom. Teoretski nema ograničenja za proširene particije sve dok ima prostora na disku, ali ima ograničenja u broju slova koja se mogu dodeliti ovim particijama.

Za uspešnu analizu, forenzičar mora znati značenje informacija koje nosi 16 bajta u heks zapisu u 4 ulaza glavne MPT tabele. Na primer, u MPT tabeli heksadecimalni bajtovi 14, 16 i 17 su validni kôdovi za *skrivene* particije. Kada sistem otkrije ove kôdove normalno ignoriše ove particije i ne pripisuje im slova za oznaku diska. Forenzičar treba ispitati ove skrivene particije, jer mogu kriti kompromitovani materijal, a MPT i MBR sadrže mnogo vitalnih informacija za startovanje sistema i pozicioniranje podataka na disku.

Da bi razumeo računar sa *dualnim butovanjem* - sa dva i više različitih OS, forenzičar mora razumeti koncept deljenja diska na particije. Da se obezbedi dualno butovanje, OS mora biti lociran na jednoj primarnoj particiji. Računar se ne može butovati sa proširene particije.

Za forenzičku analizu značajno je poznavati nealocirani prostor korišćenog diska, na kome su preoblikovane particije, a korisnik zauzeo manji deo diska. Pod uslovom da disk nije prepisan pre preoblikovanja particija, na tom delu diska još se uvek mogu naći podaci interesantni za forenzičara i mogu se otkriti odgovarajućim forenzičkim alatima.

Posle delenja diska na particije, potrebno je isti formatirati, komandama računara za formatiranje koje se nalaze u svim Microsft OS. Ova komanda formatira disk i inicijalizuje fajl sistem kojeg izabere korisnik i OS podržava. Da bi se razumeo proces formatiranja i fajl sistemi potrebno je analizirati osnovni fajl sistem – FAT fajl sistem. U FAT16 fajl sistemu komanda za formatiranje kreira sistemsku oblast: *Boot record*, *Alakacione tabele fajl sistema* - FAT i *Root directory* za adresiranje i praćenje fajlova uskladištenih na disku i priprema disk za OS. Broj sektora rezervisanih za FAT tabele, određen je veličinom particije. Posle prve FAT1 kreira se druga FAT2, kao bekap kopija FAT1. Kako se svaka FAT modifikuje, zadržavaju *sinhronizaciju*. FAT tabele moraju biti duplirane, ili će sistem pokazati grešku. Zatim se upisuje rut direktorijum u 3 sektora, a ostatak particije koristi se za upisivanje podataka. FAT16 ima ograničen broj alokacionih jedinica – sektora od $\mathbf{2^{16}}$ jedinica za skladištenje, ili 65536 (0-65535) sektora, što daje *maksimalnu veličinu diska* od oko 33MB.

FAT32 fajl sistem sasvim je sličan sistemu FAT16. Formatiranje prvo kreira dve kopije but rekorda, svaka od po 3 sektora (za razliku od but rekorda

FAT16 od jednog sektora), odvojene sa 3 sektora rezervisanog prostora. Posle drugog but rekorda postoje 23 rezervna sektora, što daje ukupno 32 sektora. Zatim se formatiraju dve sinhronizovane *fajl alokacione tabele*, zbog redundantnosti. Broj rezervisanih sektora za fajl alokacione tabele zavisi od veličine logičkog diska. Ovim je kompletirana sistemska oblast. *Rut direktorijum* nije lociran u sistemskoj oblasti, nego u oblasti podataka, što omogućava da rut direktorijum, koji uvek počinje u klasteru 2, može rasti do bilo koje veličine, ograničene samo kapacitetom particije. Posle formiranja sistemske oblasti i rut direktorijuma, ostatak logičkog drajva formatiran je za korisničke podatke. FAT32 fajl sistem može alocirati $\mathbf{2^{32}}$ sektora, ili 4,294.967.296 sektora.

Kada se disk formatira, upisuje se ili prepisuje but rekord, ako je već upisan, prepisuju se FAT tabele sa nulama, brišu svi ulazi, a sve alokacione jedinice na disku su na raspolaganju sistemu. Rut direktorijum se menja, kreira na novom disku ili prepisuje, ako se formatira korišćeni disk. Međutim, oblast podataka, koja je od osnovnog interesa za forenzičara, u standardnom formatiranju ostaje nedirnuta. Kod formtiranja FD, u većini slučajeva podaci će ostati, izuzetak je korišćenje bezuslovne „**/u**“ komande u DOS OS za formatiranje FD.

NTFS fajl sistem nema posebnu sistemsku oblast koja se koristi da održava tragove fajlova i obezbeđuje sistemske informacije, a ***sve*** se skladišti kao fajl. Fajlovi koji kontrolišu sistem označeni su znakom „**$**“ ispred fajla. Alokacija prostora na disku vrši sa *run listom* i pokazivačima.

Za označavanje particija diskova Windows OS koriste tri pravila, koja se po redu moraju izvršiti na sve particije u računaru. Svako dodavanje novog HD, ili priključivanje prenosnog diska ostavlja trag u računaru i omogućava forenzčaru da rekonstruiše šta se dešavalo na računaru. Ovi tragovi nalaze se u Regitru u ključu:

```
HKEY_LOCAL_MACHINE/System/Mounted Devices.
```

Za digitalnog forenzičara od velike dokazujuće vrednosti su duga imena fajlova (LFN), koji mogu biti vrlo deskriptivni i ukazivati na sadržaj

PITANJA ZA PONAVLJANJA

1. Šta je Unused Disk Space?
2. Šta je hidden particija?
3. Zašto bi neko želeo da ima skrivene particije na disku – dati jedan legitiman i jedan sumnjiv razlog?
4. Kako je nastala skrivena particija?
5. Koliko zapisa može da ima tabela particioniranja od početka proširene particije i šta su ti zapisi?
6. Šta je fajl sistem, i navesti nekoliko primera?
7. Šta je operativni sistem i navesti nekoliko primera?
8. Da bi se sistem butovao, šta je potrebno da računar poseduje?
9. Koji najniži nivo formata na disku kreira proizvođač?
10. Navesti dva primera programa koji omogućavaju particioniranje diska?
11. Šta program za particioniranje smešta u prvi sektor diska (CHS 0,0,1 ili LBA 0)?
12. Šta ovaj sektor sadrži što omogućava sistemu da razume način postavki diska?
13. Od kojeg ofseta kreće Master Partition Table (MPT)?
14. Šta odmah sledi iza MPT?
15. Koliko je velika MPT?
16. Koliko MPT ima zapisa?
17. Koliko je dugačak svaki zapis?
18. Koliko će MPT imati neiskorišćenih zapisa?
19. Objasniti šta govori svaki 16 bajtni zapis?
20. Koliko particija normalno može da se markiraju kao aktivne particije?

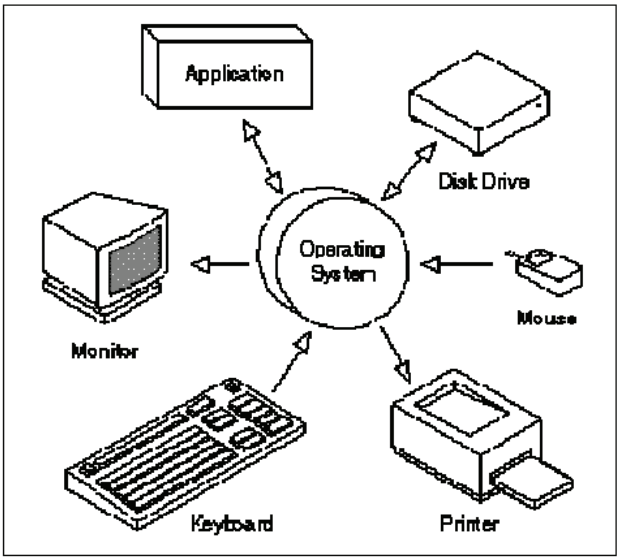
21. Šta je logički drajv?
22. Navedite tri oblasti u FAT16 fajl sistemu koje čine sistemsku oblast.
23. Koji tip informacija sadrži but rekord?
24. Koliko kopija FAT-a ima u but rekordu?
25. Koliko entrija može imati rut direktorijum FAT16?
26. Zašto fajlovi sa dugim imenom izazivaju problem u rut direktorijum FAT16?
27. Koliko alokacionih jedinica može obuhvatiti FAT16?
28. Šta je uvedeno da se prevaziđe ograničen broj alokacionih jedinica?
29. Kako počinje brojanje klastera u NTFS fajl sistemu?
30. Gde uvek možete naći But rekord u FAT16 particiji?
31. Koliko kopija But rekorda ima u FAT32 fajl sistemu?
32. Da li su kopije But rekorda u FAT32 fajl sistemu prostorno neprekinute?
33. Koliko je dug svaki But rekord u FAT32 fajl sistemu?
34. Od čega zavisi broj rezervisanih sektora u FAT tabeli?
35. Gde je uskladišten rut direktorijum u FAT32 fajl sistemu?
36. Zašto je tako uskladišten rut direktorijum u FAT32 fajl sistemu?
37. Koji je maksimalan broj sektora koji može biti alociran u jednom klasteru?
38. Šta klasteri znače za korisnika?
39. Šta klasteri znače za forenzičara?
40. Koliko alokacionih jedinica ima FAT32 fajl sistem?
41. Šta se događa sa oblasti podataka u FAT sistemima kod normalnog formatiranja?
42. Da li NTFS ima sistemsku oblast kada se drajv formatira?
43. Navedite tri oblasti u FAT16 fajl sistemu koje čine sistemsku oblast.
44. Koji tip informacija sadrži but rekord?

45. Koliko kopija FAT-a ima u but rekordu?
46. Koliko entrija može imati rut direktorijum FAT16?
47. Zašto fajlovi sa dugim imenom izazivaju problem u rut direktorijum FAT16?
48. Koliko alokacionih jedinica može obuhvatiti FAT16?
49. Šta je uvedeno da se prevaziđe ograničen broj alokacionih jedinica?
50. Kako počinje brojanje klastera u NTFS fajl sistemu?
51. Gde uvek možete naći But rekord u FAT16 particiji?
52. Koliko kopija But rekorda ima u FAT32 fajl sistemu?
53. Da li su kopije But rekorda u FAT32 fajl sistemu prostorno neprekinute?
54. Koliko je dug svaki But rekord u FAT32 fajl sistemu?
55. Od čega zavisi broj rezervisanih sektora u FAT tabeli?
56. Gde je uskladišten rut direktorijum u FAT32 fajl sistemu?
57. Zašto je tako uskladišten rut direktorijum u FAT32 fajl sistemu?
58. Koji je maksimalan broj sektora koji može biti alociran u jednom klasteru?
59. Šta klasteri znače za korisnika?
60. Šta klasteri znače za forenzičara?
61. Koliko alokacionih jedinica ima FAT32 fajl sistem?
62. Šta se događa sa oblasti podataka u FAT sistemima kod normalnog formatiranja?
63. Da li NTFS ima sistemsku oblast kada se drajv formatira?

9 OPERATIVNI SISTEMI

1.3. Pregled *Microsoft* operativnih sistema

Operativni sistemi danas su brojni i raznovrsni. Bez sumnje OS je najvažniji program koji radi na računarskom sistemu. Korisnici često uzimaju OS podrazumevano, a veću pažnju obraćaju na aplikacije sa kojima interaktivno rade, kao što su Word, Internet brauzer, grafički softver i dr. OS obezbeđuje rad svih komponenti sistema (slika 9.1), [7].



Slika 9.1 *Grafički model funkcija operativnog sistema*

Bez OS ni jedan od uređaja sa slike ne bi mogao raditi. OS pokreće druge programe, ili aplikacije koje moraju biti specifično napisane da rade sa tim OS. Na primer, mnogi programi napisani da rade sa Windows 98, neće uspešno raditi na Windows XP i obrnuto. OS pokreće i izvršava brojne bazične zadatke, bez kojih ne bi mogli raditi. OS prepoznaje ulaz sa tastature i miša, šalje izlaz na ekran monitora, čuva tragove direktorijuma i fajlova na HD i drugim medijumima i kontroliše periferne uređaje koji su priključeni na sistem: printere, skenere itd. OS se može uporediti sa saobraćajcem koji

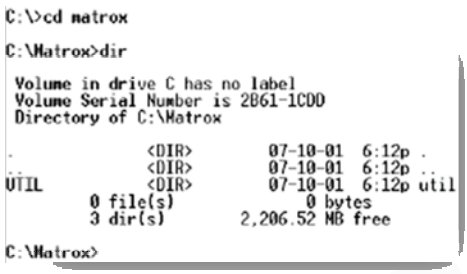
upravlja protokom informacija, upravlja korisnicima računarskog sistema i pokreće različite programe, sprečavajući međusobnu interferenciju. OS određuje pristup CPU i programu i vreme kada je pristup dopušten; upravlja internom memorijom u sistemu obezbeđujući pristup fajlovima za razmenu (*swap*) i upravlja prenosom podataka u te fajlove. OS šalje podatke o statusu, ili druge poruke kao što su greške kada ne može izvršiti operaciju. OS, odnosno, njegov podsistem zaštite - **NOSSS** (*Native OS Security Subsystem*) odgovoran je i za bezbednost sistema i sprečava pristup neovlašćenog korisnika sistemu. U savremenim OS zaštita je ključni funkcionalni elemenat, za razliku od starijih OS, gde to nije bio slučaj, [13].

Korisnici normalno interaktivno rade sa OS kroz **GUI** (*Grphical User Interface*) kao u slučaju Windows OS, ili kroz **komandu liniju** kod starijih OS (MS DOS). Generalno, OS se mogu klasifikovati kao:

- *Višekorisnički*, koji dopuštaju dva i više korisnika da aktiviraju i koriste programe u isto vreme (neki 100 pa i 1000 korisnika);
- *Višeprocesorski*, koji podržava pokretanje programa na više od jedne CPU;
- *Za više zadataka (multitascing)***,** koji omogućava konkurentan rad više od jednog programa i
- *'Multi threading'***,** za konkurentan rad više različitih delova jednog programa.

Forenzičar nikada ne sme pretpostaviti da korisnik ispitivanog računara radi sa najnovijom verzijom OS, ili da upotrebljava poslednje tipove medija.

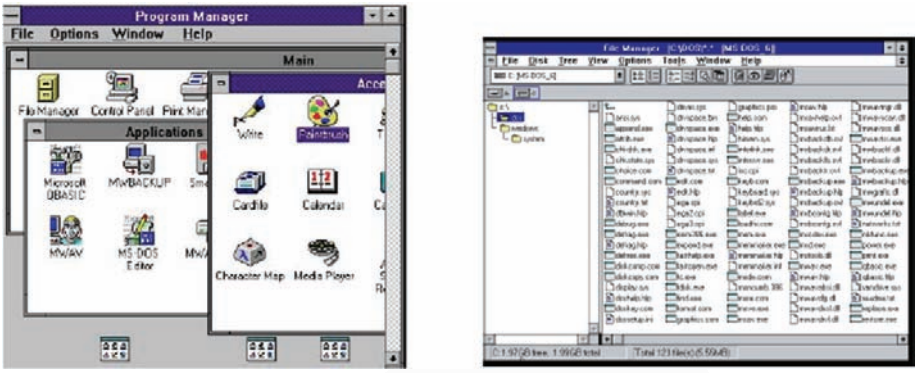
DOS (*Disk Operating System***) OS** razvio je Microsoft 1980-ih. Sledeći MS OS Windows 3x zahtevao je DOS, ali Windows 95 i kasniji nisu. Poslednje verzije Windows OS mogu još uvek (ponekad) pogoniti DOS programe. DOS je bio zasnovan na komandnoj liniji, bez miša. Postojale su bazične i kodirane komande, koje su često zahtevale više parametara i otkucanih karaktera za dobijanje željenog rezultata. Za verifikaciju DOS verzije, korisnik treba da otkuca komandu VER na komandnoj liniji. Na slici 9.2. prokazan je prozor u otvorenom DOS sistemu, [7].



Slika 9.2 Prozor DOS operativnog sistema

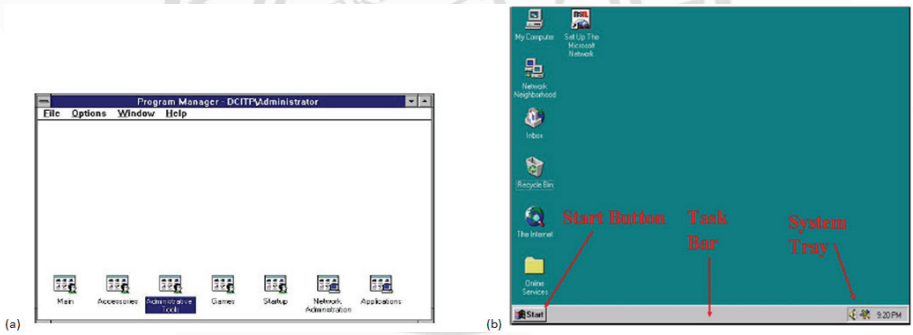
Sa tehnologijom forenzičke analize kompjuter sa DOS OS može „govoriti“, jer za sve akcije ostavlja tragove i ništa ne zaboravlja. Treba samo znati kako i sa čim otkriti te tragove. DOS OS održava prostor u memoriji za sve ulaze sa tastature. Ovaj privremeni memorijski prostor (*bafer* tastature) prazni se u HD kada je pun, ili kada korisnik sa njim završi. Sa tastature dolaze i lozinke, inkriminišuće fraze, maliciozni kodovi, ili druge fraze koje prekršioci žele sakriti, a digitalni forenzičari – otkriti, [24].

Windows 3.1 i 3.11 OS, objavljen aprila 1992 sa GUI interfejsom, dopušta korisniku upotrebu operacija koje nisu bile moguće u MS DOSu, kao što su korišćenje miša za navigaciju i manipulaciju sa računarom, pokretanje više aplikacija i obavljanje više zadataka u isto vreme. Ove funkcije su učinile znatno lakšim rad sa računarom i doprinele širokoj primeni računara, (slika 9.3).



Slika 9.3 *Prozori Windows 3.1 i 3.11 OS*

Windows NT 3.5.1 OS objavljen je 1994. i predstavlja prodor u NTFS fajl sistem i mnogo bezbediniji OS. Namenjen je za poslovne sisteme više nego personalnu primenu. Nasledio ga je mnogo popularniji Windows NT4 OS, (slika 9.4a).



Slika 9.4 *Prozor **Program Manager** Windows NT 4 OS (a) i desktop Windows 95 OS (b)*

Windows 95 OS predstavlja poboljšanu verziju Windows 3.11, sa sledećim novim funkcijama, (slika 9.4b):

1. *plug and play*, omogućava korisniku automatsku instalaciju komponenti i uređaja u računar sa odgovarajućim drajverima;
2. *32-bitni OS,* omogućava računaru brži i efikasniji rad;
3. *Registri,* kombinuje snagu INI fajlova za višekratno konfigurisanje i stavlja ih u dva fajla što dopušta lakšu lokaciju konfiguracije sistema;

4. *Memorija***,** poboljšana u odnosu na Windows 3.11 OS;
5. *Desni taster miša,* omogućava novi pristup i manipulaciju sa tekstom koristeći dva tastera umesto jednog;
6. *CD plejer,* poboljšan i sa auto plej funkcijom**.**

Windows 95 je kompletan OS koji ne zahteva DOS za pokretanje, omogućava imena fajlova do 255 karaktera dužine, priključivanje USB (Universal Serial Bus) i HD iznad 2 GB u kasnijim verzijama.

Windows NT4 OS izgleda kao Windows 95, ali je sasvim različit. Sadrži napredne bezbednosne karakteristike i naprednu mrežnu podršku, puni 32-bitni OS, administraciju korisnika i mnogo drugih funkcija. Ima slabiju podršku drajvera, drugih karakteristika i igara u poređenju sa Windows 95 i 98 OS, pa je više korišćen za poslovne potrebe. Objavljen je 1996. i namnjen za poslovne i profesionalne potrebe, sa sledećim bitnim karakteristikama:

1. mnogo brži i bezbedniji kada se korektno konfiguriše,
2. centralne administrativne funkcije,
3. bez *plug & play* mogućnosti i sa
4. komplikovanim podešavanjem i održavanjem.

Windows ME OS uveden je 2000. kao modernizacija Windows 95 i Windows 98 i dizajniran je za krajnje korisnike. Windows ME je kompatibilan sa Windows 98 aplikacijama i drajverima i uključuje, (slika 9.5a):

1. automatsko ažuriranje i preuzimanje apdejta;
2. poboljšanje mediuma i grafičkih kapaciteta;
3. restauracija sistema;
4. povratak (*rollback)* na prethodni dokument.

(a)  (b) 

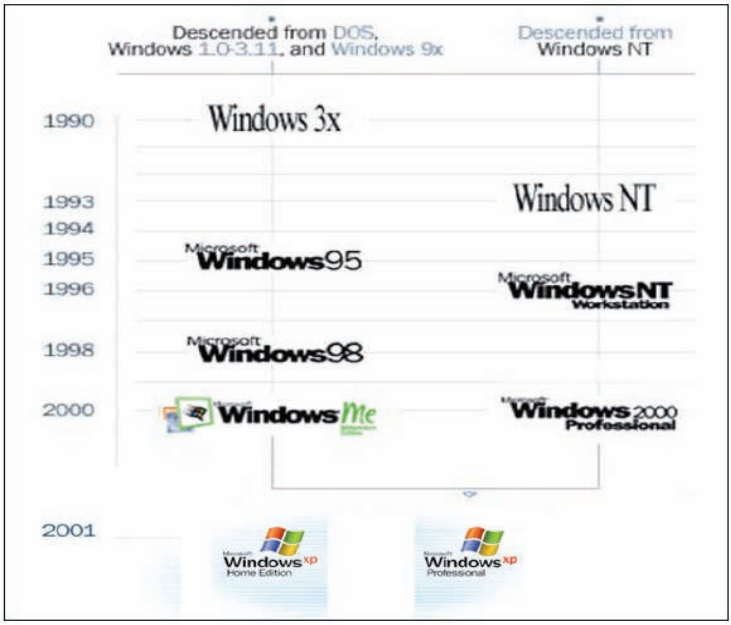
Slika 9.5 *Desktop otvorenog Windows ME OS (a) i Windows XP OS (b)*

Windows XP OS objavljen 2001. predstavlja konvergenciju dva glavna Microsoft OS u jedan. Raspoloživ je u sledećim verzijama: ***Home edition*** – *full/upgrade i* ***Professional*** – *full/upgrade*. Dizajniran je za korisnike koji slabije poznaju Windows operativne sisteme i sa nekim novim funkcijama, (slika 9.6b):

1. novi interfejs sa mogućnošću promene,
2. automatsko ažuriranje sa Interneta,
3. Internet Explorer 6,
4. višejezična podrška,
5. mogućnost šifrovanja fajla,
6. mogućnost pravljenja CD,
7. ugrađen *firewall* za zaštitu od napada sa Interneta,
8. udaljeni pristup i
9. anti-piratske karakteristike.

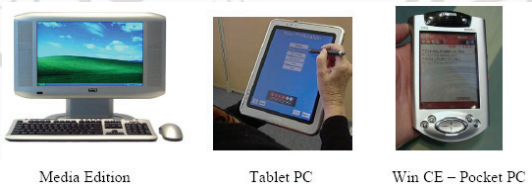
Zasnovan je na NT tehnologiji obezbeđuje veću bezbednost, ali omogućva korisnicima da formatiraju medija u FAT fajl sistemu. Profesionalna verzija dizajnirana je da radi u multiprocesorskom okruženju. *Service Pack 2* doneo je bolju bezbednost, ali i mnogo problema korisnicima.

Verifikacija OS u računaru vrši se pritiskom desnog tastera miša na **My Computer** ikonu, izborom **Properties,** ili pritiskom na **Start** taster i posmatranjem leve strane **Start** menija. Na slici 9.6 data je istorija razvoja MS OS.



Slika 9.6 Istorija razvoja MS OS

VISTA je poslednja verzija MS OS, objavljena 2007. godine. Druge verzije Windows proizvoda manje su popularne, (slika 9.7).



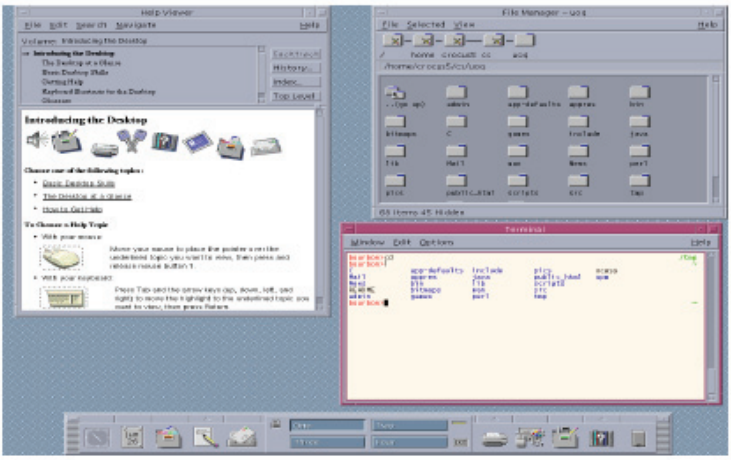
Slika 9.7 *Manje poznate verzije Microsoft OS*

9.1 Pregled UNIX/Linux operativnih sistema

UNIX OS, primarno namenjen za komercijalno, naučno i istraživačko okruženje, je višekorisnički, višeprocesorski i za više zadataka. Robustan je, pouzdan i skalabilan. Glavni proizvođači su *Sun, HP/Compaq i IBM.*

Linix OS zasnovan je na PC hardveru i obezbeđuje atraktivne cene i licence, uglavnom besplatno. Poznate su verzije *RedHat, Debian i SUSE.* Ranije verzije

nisu bile lake za obične korsnike, dok novije verzije vizuelno podsećaju na Windows OS i GUI, (slika 9.8).



Slika 9.8 *Prozori Linux OS*

Opeativni sistemi Linux postaju sve popuarniji kod običnih korisnika, a kod digitalnih forenzičara značajni su kao forenzički alati za analizu digitalnih podataka. Linux OS inicijalno je kreirao Linus Torvalds, Helsinški Univerzitet, 1991 godine, sa verzijom 1.0 objavljenom 1994. Iako je dizajniran da radi slično UNIX OS, razvijen je na INTEL-ovom CPU i bio besplatan, što je znatno uticalo na porast popularnosti ovog OS.

Kernel Linux OS, ili centralni modul OS, razvijen je i objavljen kao GNU *General Public Licence* (GPL) program, slobodno dostupan na web adresi www.gnu.org. Stotine organizacija i pojedinaca širom sveta objavilo je svoje verzije prizvoda na bazi Linux OS (tzv. *distribucije)*.

Pored toga što je besplatan, Linux je postao popularan po svojoj funcionalnosti, adaptivnosti i skalabilnosti u odnosu na UNIX i Microsoft OS-e. Mnoge velike kompanije obezbedile su podršku za Linux.

Inicijalno Linux OS korišćen je kao serverska platforma, specijalno sa adaptacijom za Internet. Hiljade web servera širom sveta radi na Linux platformi i *Apache* web-server softveru. Sve više se koristi u kućnim i poslovnim računarima, kao i mobilnim telefonima, web kamerama i PDA uređajima.

Sam Linux OS poboljšavan je godinama, a brojni aplikativni programi razvijeni su za rad na Linux OS, kao što su **GUI intefejs KDE** (*K Desktop Environment*) i **GNOME** (*Gnu Object Model Environment*), **OpenOffice** *word peocesor* i **Mozilla** web pretraživač. Neke Linux distribucije su komercijalizovane zbog „dodatnih vrednosti", kao što su **Red Hat, Mandrak i Mandriva i SUSE** (*Novell* proizvod). Komparativne prednosti i nedostaci Linux OS prema Windows OS date su u tabeli 9.1:

Tabela 9.1 Komparativne prednosti i nedostaci Linux prema Windows OS

Prednosti	Nedostaci
– Niska cena i visoka stabilnost. – Jeftiniji zahtevani hardver. – Imun na većinu virusa, Trojanaca i ranjivosti Windows-a. – Radi na velikom broju CPU-a. – Čita većinu fajl sistema i može se instalirati „samo za čitanje".	– Teži za korišćenje za prosečnog korisnika. – Manje raspoloživih aplikativnih programa. – Manje raspoloživih eksperata i programera. – Nema univerzalnu podršku glavnih snabdevača.

Kao i drugi OS, Linux ima veliki broj fajl sistema, drajvera, uslužnih alata, programa za upravljanje fajlovima i drugih aplikacija. Linux kao drugi OS koristi brojne podrazumevane lokacije za skladištenje svojih fajlova. Linux je takođe OS baziran na komandnoj liniji, sličnoj ranoj verziji Microsoft DOS-a. Razvijen je određeni broj GUI interfejsa za rad sa Linux OS, koji daju Windows tip prozora za rad. Ovi GUI su normalno bazirani na X-Windows aplikaciji razvijenoj da podržava GUI interfejs za UNIX, Linux i druge OS. Najpoznatiji Linux GUI je **KDE** i **GNOME**, ali ima i drugih.

Mnogo Linux distribucija dolazi sa prekonfigurisanim „*alias*" fajlovima koji prevode neke DOS komande u Linux komande tako kad se izvršavaju DOS komande, izvršiće se odgovarajuće Linux komande, (tabela 9.3), [7].

Tabela 9.2 Komparacija DOS i Linux komandi

DOS komanda	Linux komanda
DIR	is
CD	cd
MD	mkdir
COPY	cp

DEL	rm
REN	mv
ATTRIB	chmod

U nekim slučajevima forenzičar može odrediti ekspertizu osumnjičenog analizom njegovog izbora komandi. Ovo može posebno biti korisno u slučajevima upada u sistem. Ako osumnjičeni pokušava da koristi DOS komande, ili pokrene DOS, ili Windows hakerski program na Linux, ili UNIX OS, to obično ukazuje na ograničeno znanje napadača. Jedina standardna Linux komanda, koja nema stvarni DOS ekvivalent, je **DD** komanda. Dok je bazično specijalna komanda za kopiranje, DD komanda sa desnim specijalnim tasterom, argumentima, flegovima i kursorskim rečima prave forenzički kvalitetne kopije fizičkih diskova, logičkih diskova, fajlova i dr. Većina forenzičkih diskova za butovanje koriste DD kao bazu za forenzičke alate za uzimanje *imidža*.

Linux OS koristi različite konvencije za imenovanje uređaja za skladištenje, kao što su čvrsti disk i logičke particije. Važno je razumeti ovu konvenciju kada se koristi Linux za ispitivanje Windows ili DOS sistema, jer se neće videti poznato DOS/Windows označavanje slovima diskova i particija. Uobičajena DOS/Windows i Linux imena fizičkih diskova data su u tabeli 9.3, a imena fizičkih diskova u Linux OS data su u tabeli 9.4.

Tabela 9.3 Uobičajena DOS/Windows i Linux imena[6] fizičkih diskova

Uređaj	**DOS/Windows**	**Linux**
Floppy drajv	Drajv A ili B	/dev/fd0, /dev/fd1
IDE Master na primarnom kontroleru	Drive 0	/dev/had
IDE Slave na primarnom kontroleru	Drive 1	/dev/hdb
IDE Master na sekundarnom kontroleru	Drive 2	/dev/hdc
IDE Slave na sekundarnom kontroleru	Drive 3[7]	/dev/hdd
Prvi SCSI Disk (SCSI ID)	Drajv 0	/dev/sda
Drugi SCSI Disk,...	Drajv 1,...	/dev/sdb,...

[6] Ovo su najčešće korišćena imena. U realnosti, ali retko viđeno, imena uređaja mogu biti kakva god programer poželi.

[7] DOS fizički drajvovi se nabrajaju prema redosledu u BIOS-u i/ili onako kako su kablirani.

CD-ROM (IDE)	Drajv 0,...	/dev/cdrom
CD-ROM (SCSI)	Drajv 0,...	/dev/scd0,...

Tabela 9.4 Uobičajena imena fizičkih diskova u Linux OS

Uređaj	**Linux**
IDE Drajv 0, Prva particija	/dev/hda1
IDE Drajv 0, Druga particija	/dev/hda1
IDE Drajv 0, Treća particija	/dev/hda1
IDE Drajv 1, Prva particija	/dev/hdb1
IDE Drajv 2, Druga particija	/dev/hdb1,...
SCSI Drajv 0, Prva particija	/dev/sda1,...

Treba znati da su ovo uobičajena imena, dok u stvarnosti mogu biti bilo kakva, zavisno od inspiracije programera. U DOS OS fizički diskovi se broje onim redosledom kako ih pronađe BIOS i/ili kako su povezani. U Linux OS imena diskova/uređaja locirana su na **/dev** particiji, ili direktorijumu. Ovo je podrazumevana lokacija skladištenja za sve Linux specijalizovane fajlove i postoji mnogo prekonfigurisanih u brojnim distribucijama. U osnovi, ovi fajlovi se koriste kao *drajveri* hardverskih uređaja i sadrže drajvere za sve vrste flopi diskova (5.25”, 3.5”, niske i visoke gustine), USB uređaje, modeme, tastature, video kartice, monitore i druge uređaje. Linux koristi specijalne particije za virtuelnu memoriju sa sopstvenim virtuelnim fajl sistemom. Uobičajena imena Linux logičkih particija data su u tabeli 9.5.

Tabela 9.5 Uobičajena imena Linux logičkih particija

Particija	**Sadržaj**	**Fajl sistem**
/ (koren)	Drajveri uređaja, sistemski fajlovi, itd.	Ext2/3
/boot	Jezgro Linuksa (OS)	Ext2/3
/swap	Virtualna memorija	Swap[8]
/usr	Binarni izvršni fajlovi	Ext2/3

[8] *Linux koristi specialnu particiju za virtuelnu memoriju, sa sopstvenim fajl sistemom.*

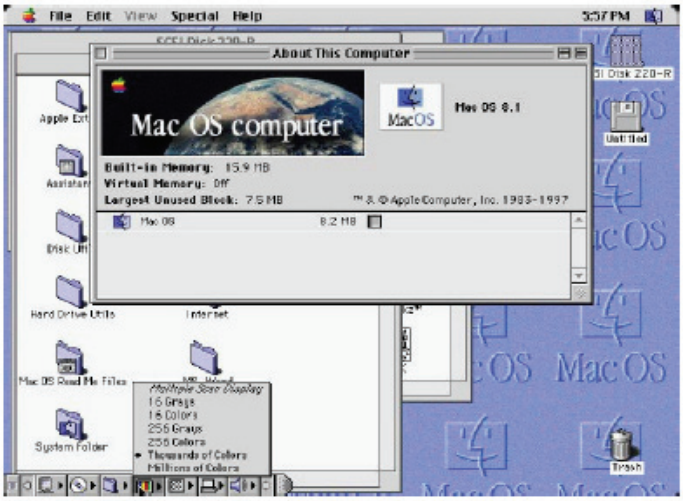
/var	Mail, printer spool fajlovi, log fajlovi	Ext2/3
/home	Korisnički direktorijumi	Ext2/3
/tmp	Privremeni fajlovi	Ext2/3

Na starijim Linux instalacijama ove particije su bile često raširene kroz dva, ili više fizičkih diskova i zbog relativno male veličine diskova u to vreme. Na primer, ako se e-*mail* fajl uskladišti u rut, ili but particije, a e-pošta prepuni ove particije, sistem će pasti.

Sa savremenim diskovima velikog kapaciteta većina Linux distribucija instalira ceo sistem na dve particije: obično **Ext3** za fajl sistem, a drugu kao ***swap*** particiju. Linux OS tipično koristi originaln fajl sistem **Ext2** ili **Ext3** (prošireni fajl sistem 2 ili 3), ali ima sposobnost čitanja skoro svakog fajl sistema i može instalirati fajl sistem u modu „samo čitanje“, ako se na odgovarajući način modifikuje kernel, ili dodaju drajveri. Sa forenzičkog aspekta ovo je velika prednost Linux fajl sistema.

Savremena Linux distribucija „**živi Linux na CD**“, objavljena na jednom CD-ROM disku i sposobna da butuje sistem sa CD, bez instalacije bilo kojeg softvera na host računaru, postala je značajan forenzički alat. Najpopularniji je **Knoppix,** [35]. Koristeći jednu od glavnih karakteristika Linux OS – sposobnost čitanja većine fajl sistema, ovaj CD može se koristiti za butovanje Microsoft Windows baziranih računara i analizu fajl sistema na Windows računaru, bez poznavanja bilo kojeg pasvorda za logovanje. Na ovaj način održva se i forenzički integritet ispitivanih podataka, što omogućava upotrebu butabilnog CD u brojnim aktivnostima digitalne forenzičke istrage.

Macintosh OS proizveden je 1980 (*Apple Computers*). Poslednja verzija OS **X** ugradila je **Unix** radi stabilnosti. Tipičan prozor *Macintosh* OS prikazan je na slici 9.9.



Slika 9.9 *Tipičan prozor Macintosh OS*

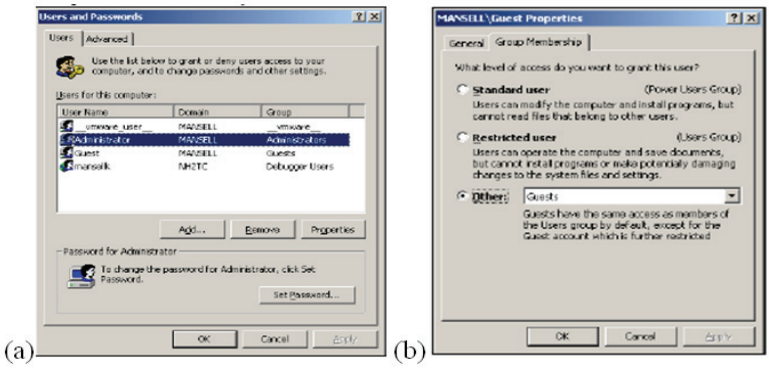
9.2 Koncept korisnika i registri u operativnom sistemu

Koncepti korisnika i *registara* u OS vrlo su važni za digitalnog forenzičara, jer pokazuju ko je odgovoran za neke aktivnosti na računaru. Podešeni profil korisnika i ulazi u *Registru* mogu dati neke podatke o tome šta se desilo i ko je odgovoran za akciju. Iako se u računarskom sistemu mogu proveriti vremena i datumi poslednjih akcija na računaru, ostaje pitanje ko je sedeo ispred računara i izvršio te akcije, što je regularan zahtev suda u procesu **rekonstrukcije slučaja** kompjuterskog kriminala. Odgovor uvek ne mora biti u računaru, pa je potrebna veština forenzičara i istražitelja, [25].

U starijim OS bezbednost nije bila prioritetna, dok je u poslovnim sistemima postala značajna *funkcionalna* komponenta. Windows NT, 2000 i XP OS zahtevaju logovanje korisnika sa nekim bezbednosnim podešavanjem i pasvordom. Međutim, često nalazimo računare na kojima su svi korisnici logovani kao podrazumevani korisnici, ili svi znaju pasvorde.

Windows 2000 ili XP OS omogućava pristup i korišćenje računara jednom ili više korisnika. Za to je potrebno kreirati određeni broj *korisničkih naloga*, ili *profila* sa definisanim ovlašćenjima za rad na objektima računarskog sistema. Uvek postoji administratorski nalog kreiran pod *generalni* korisnički nalog –

korisnik koji ima potpunu kontrolu nad računarom i konfigurisanjem računara. Korisnički profil kreira se u **Controle Panel** pod **User Accounts**. Na prozoru (slika 9.10a) vide se otvoreni korisnički nalozi, koji se dodaju sa tasterom *Add* i uklanjaju sa *Remove*.



Slika 9.10 *Podešavanje korisničkog profila u Windows XP OS*

Na sledećem prozoru (slika 9.10b) vide se prava profila korisnika MANSELL, koji je selektovan na prvom prozoru. Sa profilisanjem prava korisnika administrator sistema konfiguriše značajan deo mrežne zaštite, jer kontroliše u velikoj meri ponašanje korisnika na mreži. Generalno, konfigurisanje svih **NOSSS**[9] mehanizama zaštite u savremenom računarskom sistemu komplikuje rad forenzičara. Podrazumevane lokacije za kreiranje profila za različite Windows OS date su u tabeli 9.6, [24].

Tabela 9.6 Podrazumevane lokacije za kreiranje profila za različite Windows OS

Korisnici	**Windows XP/2000**	**Windows 9x/Me**
Određeni korisnici	C:\Documents and Settings\<korisnik>	C:\Windows\Profiles\<korisnik>
Svi korisnici	C:\Documents and Settings\	C:\Windows\
Podrazmevani korisnik	C:\Documents and Settings\Default User	nije primenjivo

Konfigurisanjem profila korisnika, ne kreira se korisnički fajl koji personalizuje korisnički rad na računaru. Ovaj fajl se kreira tek kada se korisnik prvi put

[9] NOSSS – *Native Operative System Security Subsystem*

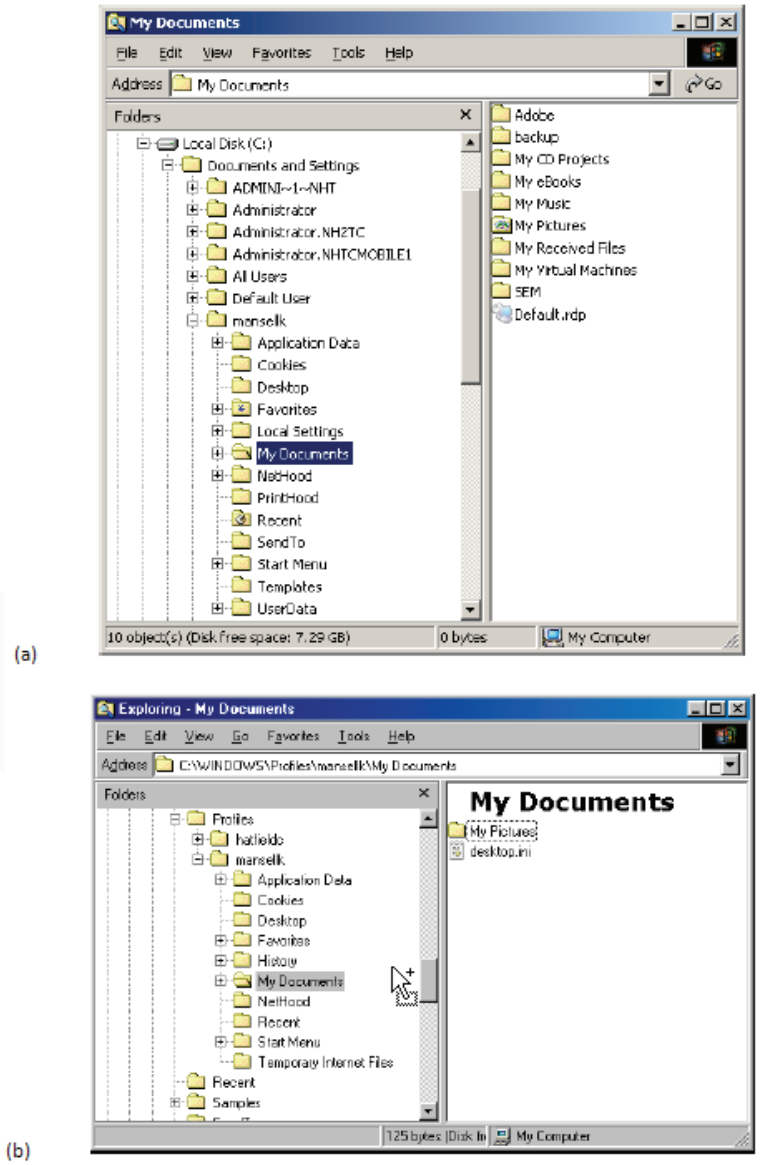
uloguje na sistem i memoriše u folder *C:/Documents and Settings* pod njegovim imenom, a predstavlja kopiju fajla koji se skladišti u *Default User* profilu. Svaki sledeći pristup tog korisnika registruje se i memoriše u isti fajl, a svaka promena koju taj korisnik izvrši u računaru reflektuje se na *Default User* profil. Administrator sistema može promeniti podešavanje za korisnike sistema po prvi put.

Fajl NTUSER.DAT je od velike važnosti za digitalnog forenzičara, jer sadrži elemente konfigurisanja za određenog korisnika i koristi se za popunu *Registra* kada se korisnik loguje, U toku podrazumevanog konfigurisanja profila u Windows XP OS kreiraju se i drugi folderi i lociraju u personalni profil, [24]:

1. *Application Data*, odnosi se na podatke koje koriste aplikativni programi koje korisnik može modifikovati, kada promeni konfiguraciju aplikacije;
2. *Cookies*, koji nastaju kao rezultat pretraživanja *web* lokacija;
3. *Desktop,* koji se odnosi na konfiguraciju desktopa: prečice, uobičajeno korišćene fajlove i aplikacije;
4. *Favorires***,** koji se odnosi na favorizovane web lokacije koje korisnik posećuje;
5. *Local Settings,* koji se odnosi na konfigurisanje uobičajenih aplikacija kao što su web lokacije posećene sa *Internet Explorer,* ili drugim pretraživačem sa imenima i sadržajem u forlderu *History*, pod-folderima koji sadrže privremene internet fajlove i profile Microsoft e-mail klijenata;
6. *My Documents,* za skladištenje dokumenata korisnika koji uključuje formiranje sub-foldera za *My Picture/My Music/My Video* (OS XP). Takođe i druuge aplikacije mogu smestiti ovde foldere za skladištenje i podrazumevano preuzimanje (*download*);
7. *NetHood,* u kojem su izlistirani mrežni serveri, ili zajednički (*shared*) mrežni folderi;
8. *PrintHood,* u kojem su izlistirani mrežni printeri;
9. *Recent,* u kojem su prikazane prečice prema nedavno otvaranim/korišćenim dokumentima i fajlovima;
10. *SendTo***,** koji sadrži prečice na mesta gde fajlovi mogu biti kopirani;

11. *Start Menu,* sadrži korisnički start meni i listu instaliranih aplikacija, ako se pojavljuju u listi start menija programa;
12. *Templates,* sadrži obrasce (templejte) aplikacija i
13. *User Data*, sadrži podatke korisnika*.*

Za Windows 9x OS konfigurisanje korisničkog profila neznatno se razlikuje. Profil *All Users* dopušta administratorima sistema da instaliraju zajedničke aplikacije i fajlove kojima svi korisnici sistema mogu imati pristup. Prečice ovim aplikacijama i fajlovima nalaze se u ovom folderu i svi korisnnici će imati pristup do njih. Aplikacije i fajlovi pojaviće se na desktopu svakog korisnika. Kako je pomenuto, administrator može promeniti podrazumevanu lokaciju za korisničke profile i njihovo ponašanje. Prozor na slici 9.11a pokazuje šta se vidi u normalnom konfigurisanju profila novog korisnika u Windows XP OS.



Slika 9.11 *Normalna konfiguracija profila novog korisnika u Windows XP OS (a) i prozor My Documments u Windows 9x OS (b)*

Treba znati da korisnički profil koji je kreiran bez ikakvih administrativnih prava ne može pristupiti folderima i drugim korisnicima u direktorijumu *Documents and Settings*, pošto nemaju potrebna ovlašćenja. Ovo forenzičar

treba da ima na umu kada se normalni korisnik optužuje za pristup i skladištenje potencijalnih dokaza na ona mesta na računaru kojima inače nema ovlašćenja.

Pomenute razlike između Windows XP i Windows 9x OS prikazane su u strukturi fajl sistema Windows 9x koji ima manje mehanizama zaštite, (slika 9.11b).

Razmatranje korisničkih profila na ispitivanom računaru značajno je zato što postojanje korisničkih profila ukazuje da više od jednog lica koristi računar, a forenzičar mora dokazati ko je autor kojeg fajla i akcije. U istrazi uvek treba očekivati da odbrana osumnjičenog tvrdi da je drugo lice izvršilo kompromitujuću akciju. Generalno, forenzičar treba naći odgovore na brojna piitanja, kao što su, da li je:

1. osumnjičeni počinilac aktuelni korisnik sistema,
2. neko drugi kompromitovao korisnički nalog/profil,
3. pasvord korisnika zaštićen,
4. moguće da neko drugi pristupi nalogu,
5. odgovoran neko sa pravima administratora,
6. moguća kompromitacija naloga i
7. da li se svi korisnici loguju na isti nalog, ili se računar uvek ostavlja isključen?

Ne treba očekivati da forenzičar dobije sve odgovore iz računara. Zato treba koristiti i druge izvore kao što su tehnike isleđivanja osumnjičenih i drugi izvori podataka (zabeleške, drugi medijumi i sl.).

Registri su srce Windows 2000 i XP OS i mogu se smatrati repozitorijumom informacija koje se odnose baš na sve što se radi sa računarom. Prvi put pojavili su se u Windows 3.1 OS kao jedan fajl – REG.DAT sa vrlo velikim ograničenjima u odnosu na tekuće registre Windows OS. Ove informacije sadrže podatke o OS, korisničke profile, lokacije fajlova, konfiguracije drajvera i hardvera. Kroz registre može se kontrolisati skoro sve o tome kako radi računar i OS.

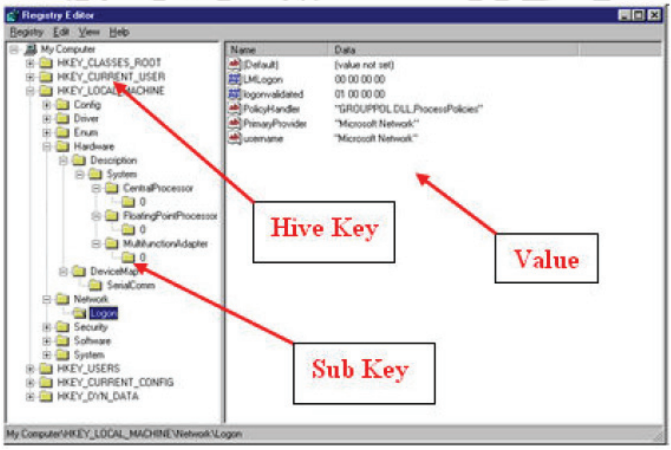
Registar savremenih Windows OS je centralna hijerarhijska baza slična stablu, kritična za rad sistema. Za razliku od uređivanja tekst dokumenta gde generalno postoji funkcija *undo* kojom se briše poslednja akcija i vraća u

prethodno stanje, svaka promena u registru je nepovratna. Zato registre mogu uređivati samo napredni korisnici, s tim da naprave bekap originalne konfiguracije registara pre svake promene.

Registri rade na isti način, sa neznatnim razlikama, u Windows 9x, ME i NT baziranim platformama. U registrima se mogu naći brojne informacije značajne za forenzičara:

1. Koje je web adrese (URL) korisnik otkucao u pretraživaču?
2. Koji je poslednji film osumnjičeni gledao na računaru?
3. Koje je ključne reči osumničeni koristio u *KaZaA* aplikaciji?
4. Koji su pasvordi korišćeni na računaru?
5. Tragovi prethodno instaliranih aplikacija koje je korisnik pokušao ukloniti itd.

Najlakši način za gledanje Registra je otvaranje **RUN** prozora iz **START** menija i kucanje **REGEDIT**, koji otvara prozor registara. Struktura registara veoma je slična strukturi foldera u *Windows Explorer*-u. Prvo se pokaže serija foldera poznatih kao *Hive Keys*. Svaki od *Hive Keys* sadrži seriju pod-foldera koji sadrže *sub-ključeve*. Svaki od ovih sub-ključeva sadrži svoje sub-ključeve koji sadrže *Vrednosti*. U nekom sub-ključu može biti mnogo vrednosti koje se odnose na sva podešavanja OS i računara, (slika 9.12), [24].



Slika 9.12 Prozor Registry Edit u Windows XP OS

Glavni *Hive Keys* podeljeni su u Sub-Keys, a na desnoj strani slike prikazana su Imena (*Name*) i Vrednosti (*Value*) koja koristi OS. Forenzičar treba da zna gde su uskladišteni fajlovi odakle Registar uzima informacije. Ako računar radi sa Windows 9x ili ME, fajlovi Registra su uskladišteni u Windows folderu. Fajlovi koji čine Registar u sistemu su:

- **C:\Windows\Classes.dat**
- **C: \Windows\System.dat**
- **C: \Windows\User.dat**

Ranije verzije Windows 95 i Windows 98 nemaju *Classes.dat* fajl. Svi ovi fajlovi su skriveni za regularnog korisnika sistema. Ako računar koristi Windows NT, uključujući Windows 2000 i XP, fajlovi Registra za mašinu uskladišteni su u sledećim glavnim folderima (i više drugih!):

- **C:\WINDOWSNT\System32\Config\software**
- **C:\WINDOWSNT\System32\Config\Security**
- **C:\WINDOWSNT\System32\Config\System**

Fajl Registra o korisnicima nalazi se u: *C:\Documents&Settings\<user>\ntuser.dat.* Svi su sakriveni i iz bezbednosnih razloga zaštićeni sistemski fajlovi. Za uspešnu forenzičku analizu potrebno je diskutovati glavni *Registry Hive Keys*:

HKEY_CLASSES_ROOT: Ovaj ključ sadrži informacije o podešavanju softvera fajl sistema. Sadrži prečice koje obezbeđuju da se podigne korektan program kada se otvori fajl u *Windows explorer*-u. Za svaki fajl postoji pridružen *Sub-Key* koji sadrži informacije o konfiguraciji. U stvari, ovaj ključ je pod-ključ od *HKEY_LOCAL_MACHINE* i uskladišten je u *HKEY_LOCAL_MACHINE\Software\ Classes*. Ako se promeni vrednost u bilo kojoj od ovih lokacija ta se promena reflektuje na druge.

HKEY_CURRENT_USER: Ovaj ključ sadrži sve informacije o konfigurisanju koje se odnose na tekuće korisnike ulogovane na sistem i, takođe, ima 7 glavnih pod-ključeva:

1. *AppEvents*: sadrži informacije o podešavanju zvuka (*bip*) kojeg sistem treba da reprodukuje za sistemski događaj.
2. *Control Panel*: ovde su uskladištene informacije o podešavanju kontrolnog panela.

3. *InstallLocation MRU*: sadrži informacije o putu skladištenja foldera i drajvova.
4. *Keyboard Layout*: specificira informacije o tekućem podešavanju i formi tastature.
5. *Network*: sadrži informacije o mrežnim konekcijama.
6. *RemoteAccess*: sadrži informacije o tekućim lokacijama za logovanje koje koriste modemske *Dial-up* konekcije.
7. *Software*: sadrži informacije o konfigurisanju softvera za tekuće logovane korisnike i kojim programima mogu pristupiti. Ovaj se ključ takođe može naći u HKEY_USER\Default, ili ako je formiran više od jednog profila u HKEY_USER\<profile name>. Svaka promena vrednosti u bilo kojoj od ovih lokacija, reflektovaće se na druge lokacije.

HKEY_LOCAL_MACHINE (Windows 9E&ME): sadrži informacije o podešavanju hardvera i softvera koje koriste svi korisnici računara. Ovaj ključ takođe ima 7 pod-ključeva:

1. *Config*: informacije o konfigurisanju, koje se mogu naći u ***HKEY_CURRENT_CONFIG.***
2. *Enum***:** informacije o hardveru.
3. *Hardware***:** informacije koje se prenose u Windows iz BIOS-a.
4. *Network***:** informacije o mrežama koje su povezane na mašinu.
5. *Security***:** informacije o podešavanju mehanizama mrežne zaštite.
6. *Software***:** specifične informacije i podešavanja softvera.
7. *System***:** informacije o *start-up*-u sistema i drajverima komponenti sistema i podešavanju OS.

HKEY_LOCAL_MACHINE (Windows NT): sadrži informacije o podešavanju hardvera i softvera koje koriste svi korisnici računara. Ima 5 glavnih pod-ključeva:

1. *Hardware***:** sadrži detaljne informacije o konfigurisanju hardvera sistema i lokalno priključenih uređaja.
2. *SAM***:** sadrži informacije za upravljanje bezbednosnim nalozima.

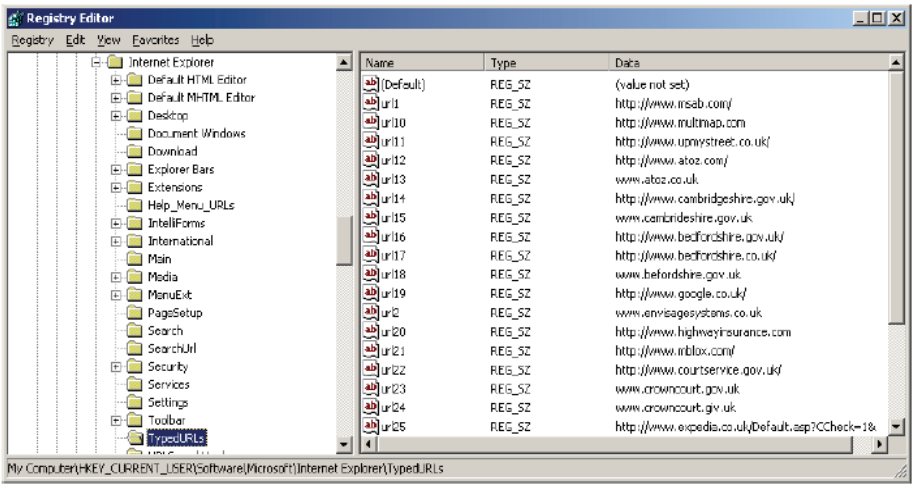
3. *Security***:** sadrži sve informacije o bezbednosti aplikacija.
4. *Software***:** sadrži kompletan opseg informacija o instaliranim aplikacijama.
5. *System***:** sadrži detaljne informacije o tekućoj kontrolnoj konfiguraciji sistema (*CurrentControlSet*) kao i sve prethodne kontrolne konfiguracije.

HKEY_USERS: sadrži informacije o svakom korisniku koji se može ulogovati na računar i njihove profile. Svaki korisnik ima pod-ključ sa jedinstvenim identifikatorom. Ako postoji samo jedan korisnik računara pod-ključ se naziva **.default**. Kada se korisnik uloguje, informacije u pod-ključu i **.default** pod-ključ biće preuzeti u HKEY_CURRENT_USER.

HKEY_CURRENT_CONFIG: sadrži informacije o tekućoj konfiguraciji hardvera kojeg lokalna mašina koristi u podizanju sistema (*start-up*). Usmerava na HKEY_LOCAL_MACHINE\Config.

HKEY_DYN_DATA (samo Windows 9x**):** sadrži dinamičke informacije o uređajima koje se samo ugrade i uključe (*plug in&play*). Ovde se podaci konstantno menjaju. Ceo ključ se prepisuje svaki put kada se računar podiže. Takođe, prisutan je u Windows NT Registru, gde je uključen u HKEY_LOCAL_MACHINE\Hardware.

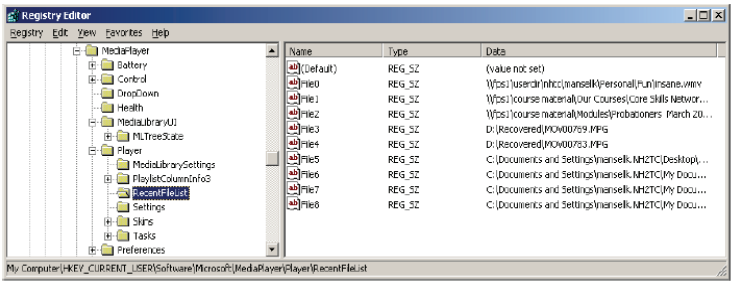
Na sledećim slikama prikazani su oblasti ključeva od interesa za forenzičara. Na slici 9.13 prikazani su detalji imena web lokacija koje je korisnik fizički otkucao u web pretraživaču, a ne samo onih koje je posetio. Neko je morao biti za tastaturom i kucati isti niz karaktera.



HKEY_CURRENT_USER\ Software\Microsoft\Internet Explorer\TypedURLs

Slika 9.13 *Informacije u Registry Editor-u o akcijama u Internet Explorer-u*

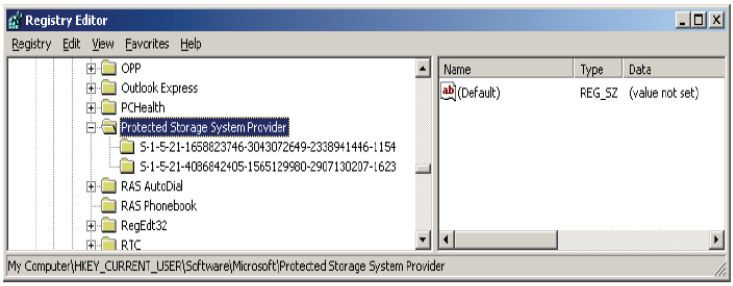
Na slici 9.15. pokazani su detalji o filmovima/klipovima koji je korisnik reprodukovao u *Media Player* aplikaciji.



HKEY_CURRENT_USER\ Software\Microsoft\Mediaplayer\Player\RecentFileList

Slika 9.14 *Informacije u Registry Editor-u o akcijama u Media Player-u*

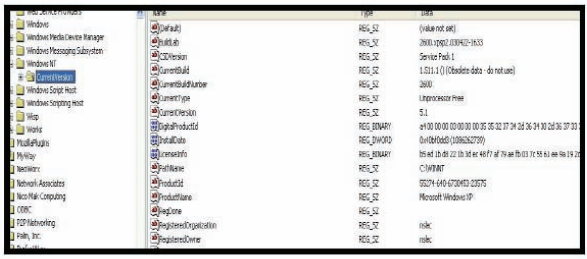
Na slici 9.15 prikazane su informacije o korisničkim imenima i pasvordima za web lokacije posećene u *Internet Explorer*-u. Za čitanje ovog sadržaja potreban je specijalni alat.



HKEY_CURRENT_USER\ Software \Microsoft\Protected Storage Provider

Slika 9.15 *Informacije o korisničkim imenima i pasvordima za web lokacije posećene u Internet Exploreru*

Na slici 9.16 ilustrovani su detalji o verziji Windows-a instaliranog na računaru.



HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\

Slika 9.16 *Detalji o verziji Windows-a instaliranog na računaru*

Očigledno, detalji koji se odnose na korisnike sistema mogu dati forenzičaru određene informacije o korišćenju računara i moguće ideje o tome ko je koristio računar. U ***Registru*** forenzičar može otkriti značajne informacije o sistemu i konfiguraciji sistema.

REZIME

Operativni sistem pokreće druge programe, ili specifično napisane aplikacije, pokreće i izvršava brojne bazične zadatke, prepoznaje ulaz sa tastature i miša, šalje izlaz na ekran monitora, čuva tragove direktorijuma i fajlova na HD i drugim medijumima i kontroliše periferne uređaje koji su priključeni na sistem: printere, skenere itd. OS se može uporediti sa saobraćajcem koji upravlja protokom informacija i korisnicima računarskog sistema i pokreće različite programe, sprečavajući međusobnu interferenciju; određuje pristup CPU i programu i vreme kada je pristup dopušten; upravlja internom memorijom u sistemu obezbeđujući pristup fajlovima za razmenu (*swap*) i upravlja prenosom podataka u te fajlove. OS šalje podatke o statusu, ili druge poruke kao što su greške kada ne može izvršiti operaciju. Podsistem zaštite - **NOSSS** (*Native OS Security Subsystem*) odgovoran je za bezbednost sistema i sprečava pristup neovlašćenog korisnika sistemu.

Korisnici interaktivno rade sa OS kroz **GUI** (npr., Windows OS), ili kroz *komandu liniju* (npr.,MS DOS). OS-i se mogu klasifikovati kao *višekorisnički*, *višeprocesorski*, *za više zadataka (multitascing)* i *'multi threading',* za konkurentan rad više različitih delova jednog programa.

Forenzičari u radu nailaze na Windows, Linux/Unix i Machintosh OS i potrebno je da poznaju osnovne funkcionalnosti ovih OS i njihove fajl sisteme, registre, upisivanje vremena i datuma itd.

Sa aspekta forenzičara Linux OS imaju određene prednosti u odnosu na Windows OS: niska cena i visoka stabilnost, jeftiniji je zahtevani hardver, imun je na većinu virusa, Trojanaca i ranjivosti Windows-a, radi na velikom broju CPU-a, čita većinu fajl sistema i može se instalirati „samo za čitanje". Nedostaci Linux OS su: teži su za korišćenje za prosečnog korisnika, manje je raspoloživih aplikativnih programa, eksperata i programera i nema univerzalnu podršku glavnih snabdevača. Linux OS je baziran na komandnoj liniji, sličnoj ranoj verziji Microsoft DOS-a. Razvijen je određeni broj GUI interfejsa za rad sa Linux OS, koji daju Windows tip prozora za rad. Ovi GUI su normalno bazirani na X-Windows aplikaciji razvijenoj da podržava GUI interfejs za UNIX, Linux i druge OS. Najpoznatiji Linux GUI je **KDE** i **GNOME**, ali ima i drugih. Mnogo Linux distribucija dolazi sa prekonfigurisanim „*alias*" fajlovima koji prevode neke DOS komande u Linux tako kad se izvršavaju DOS

komande, izvršiće se odgovarajuće Linux komande. U nekim slučajevima forenzičar može odrediti ekspertizu osumnjičenog analizom njegovog izbora komandi, posebno u slučaju upada u sistem. Ako osumnjičeni pokušava da koristi DOS komande, ili pokrene DOS, ili Windows hakerski program na Linux ili UNIX OS, to obično ukazuje na ograničeno znanje napadača. Jedina standardna Linux komanda, koja nema stvarni DOS ekvivalent, je **DD** komanda, bazično specijalna komanda za kopiranje, ali sa desnim tasterom, argumentima, flegovima i kursorskim rečima prave forenzički kvalitetne kopije fizičkih i logičkih diskova, fajlova i dr. Većina forenzičkih diskova za butovanje koriste DD kao bazu za forenzičke alate za uzimanje *imidža*. Važno je poznavati i Linux konvenciju za imenovanje uređaja za skladištenje, kada se koristi Linux za ispitivanje Windows ili DOS sistema. U Linux OS imena uređaja locirana su na **/dev** particiji, ili direktorijumu. Većina Linux distribucija instalira ceo sistem na dve particije: obično **Ext3** za fajl sistem, a drugu kao ***swap*** particiju. Linux OS tipično koristi originaln fajl sistem **Ext2** ili **Ext3** (prošireni fajl sistem 2 ili 3), ali ima sposobnost čitanja skoro svakog fajl sistema i može instalirati fajl sistem u modu „samo čitanje“, ako se na odgovarajući način modifikuje kernel, ili dodaju drajveri. Savremena Linux distribucija „**živi Linux na CD**“, objavljena na jednom CD-ROM disku i sposobna da butuje sistem sa CD, bez instalacije bilo kojeg softvera na host računaru, postala je značajan forenzički alat, a najpopularniji je **Knoppix**. Ovaj CD može se koristiti za butovanje Microsoft Windows baziranih računara i analizu fajl sistema na Windows računaru, bez poznavanja bilo kojeg pasvorda za logovanje. Na ovaj način održva se i forenzički integritet ispitivanih podataka, što omogućava upotrebu butabilnog CD u brojnim aktivnostima digitalne forenzičke istrage.

Koncepti korisnika i registara u OS vrlo su važni za digitalnog forenzičara, jer pokazuju ko je odgovoran za neke aktivnosti na računaru. Podešeni profil korisnika i ulazi u *Registru* mogu dati neke podatke o tome šta se desilo i ko je odgovoran za akciju u procesu *rekonstrukcije slučaja* kompjuterskog kriminala. Odgovor uvek ne mora biti u računaru, pa je potrebna veština forenzičara i istražitelja. U Windows 2000 ili XP OS korisnički profil kreira se u Controle Panel pod User Accounts, dodaju se sa tasterom *Add* i uklanjaju sa *Remove.* Korisnički fajl koji personalizuje korisnički rad na računaru kreira se tek kada se korisnik prvi put uloguje na sistem i memoriše u folder *C:/Documents and Settings* pod njegovim imenom, a predstavlja kopiju fajla koji se skladišti u *Default User* profilu. Fajl NTUSER.DAT je od velike važnosti za digitalnog forenzičara, jer sadrži elemente konfigurisanja za određenog

korisnika i koristi se za popunu *Registra* kada se korisnik loguje, a u Windows XP OS kreiraju se i drugi folderi i lociraju u personalni profil, kao: *Application Data*, *Cookies*, *Desktop, Favorires***,** *Local Settings, My Documents, My Picture/My Music/My Video* (OS XP) i dr.

Registri su srce Windows 2000 i XP OS i mogu se smatrati repozitorijumom informacija koje se odnose baš na sve što se radi sa računarom. Ove informacije uključuju podatke o OS, korisničke profile, lokacije fajlova, konfiguracije drajvera i hardvera. Kroz registre može se kontrolisati skoro sve o tome kako radi računar i OS. Registar savremenih Windows OS je centralna hijerarhijska baza slična stablu, kritična za rad sistema, nema funkcija *undo* kojom se briše poslednja akcija i vraća u prethodno stanje, pa je svaka promena u registru nepovratna.

U registrima se mogu naći brojne informacije značajne za forenzičara: web adrese (URL) koje je korisnik otkucao u pretraživaču, poslednji film koji je osumnjičeni gledao na računaru, ključne reči koje je osumničeni koristio u *KaZaA* aplikaciji, pasvordi koji su korišćeni na računaru, tragovi prethodno instaliranih aplikacija koje je korisnik pokušao ukloniti itd. Najlakši način za gledanje *Registra* je otvaranje RUN prozora iz START menija i kucanje REGEDIT, koji otvara prozor registara. Struktura registara veoma je slična strukturi foldera u *Windows Explorer*-u. Prvo se pokaže serija foldera poznatih kao *Hive Keys*. Svaki od *Hive Keys* sadrži seriju pod-foldera koji sadrže *sub-ključeve*. Svaki od ovih sub-ključeva sadrži svoje sub-ključeve koji sadrže *Vrednosti*. U nekom sub-ključu može biti mnogo vrednosti koje se odnose na sva podešavanja OS i računara.

Fajl Registra o korisnicima nalazi se u:
C:\Documents&Settings\<user>\ntuser.dat. Svi su sakriveni i iz bezbednosnih razloga zaštićeni sistemski fajlovi. Za uspešnu forenzičku analizu potrebno je diskutovati glavni *Registry Hive Keys*: HKEY_CLASSES_ROOT koji sadrži informacije o podešavanju softvera fajl sistema; HKEY_CURRENT_USER koji sadrži sve informacije o konfigurisanju koje se odnose na tekuće korisnike ulogovane na sistem i ima 7 glavnih pod-ključeva; HKEY_LOCAL_MACHINE (Windows 9E&ME), koji sadrži informacije o podešavanju hardvera i softvera koje koriste svi korisnici računara i ima 7 pod-ključeva; HKEY_LOCAL_MACHINE (Windows NT) koji sadrži informacije o podešavanju hardvera i softvera koje koriste svi korisnici računara i ima 5 glavnih pod-ključeva; HKEY_USERS koji sadrži informacije o svakom korisniku koji se može ulogovati na računar i njihove profile, a svaki korisnik ima pod-ključ sa

jedinstvenim identifikatorom; HKEY_CURRENT_CONFIG koji sadrži informacije o tekućoj konfiguraciji hardvera kojeg lokalna mašina koristi u podizanju sistema (*start-up*); HKEY_DYN_DATA **(**samo Windows 9x**)** koji sadrži dinamičke informacije o uređajima koje se samo ugrade i uključe (*plug in&play*).

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

PITANJA ZA PONAVLJANJE

1. Navedite neke osnovne funkcije operativnog sistema.
2. Kako se uobičajeno klasifikuju operativni sistemi?Koji interfejs koristi MS DOS operativni sistem?
3. Koja je najznačajnija nova funkcija u Windows NT 4.0 operativnom sistemu?
4. Da li Windows XP omogućava formatiranje medija u FAT fajl sistemu?
5. Zašto je primarno namenjen UNIX OS?
6. Kako se nazivaju verzije Linux OS?
7. Koje su ključne prednosti Linux OS u poređenju sa Windows OS?
8. Kako se zove jedina standardna komanda Linux-a koju nema DOS i za šta je može forenzičar koristiti?
9. Na kojoj particiji su locirana imena uređaja za skladištenje u Linux OS?
10. Koju sposobnost Linux OS najviše koriste forenzičari?
11. Kako se zove najpopularniji Linux forenzički alat?
12. Zašto može biti važno znati koji korisnici su bili ulogovani na osumnjičenom računaru?
13. Gde su podrazumevano [*default locations*] uskladišteni korisnički profili na disku Windows XP/2000, Windows 9x i Me sistema?
14. Šta može reći korisnički profil forenzičaru?
15. Šta je *Registry*?
16. Koje dokaze može naći forenzičar u *Registry*?
17. Koje su glavni fajlovi koji čine *Registry* i njihove podrazumevane lokacije u Windows XP/2000? Windows 9x i Me?

10 FORENZIČKA ANALIZA FAJL SISTEMA

10.1 Struktura i tipovi FAT fajl sistema

Poznavanje fajl sistema koji se koristi u OS, važno je razmatranje svakog forenzičara. Tip OS kojeg računar koristi sasvim je očigledan za korisnika sa ekrana uključenog računara, dok je tip korišćenog fajl sistema manje očigledan. Forenzičar treba da poznaje OS i njihove fajl sisteme, koji se razlikuju kod različitih OS. Fajl sistem određuje način na koji računar skladišti sve fajlove i foldere koji su potrebni korisniku, kao i to šta se dešava kada se oni premeste, ili izbrišu. Forenzičar mora poznavati kako svaki relevantni fajl sistem adresira i pronalazi fajlove na fizičkom/logičkom disku. Fajl sistem mora formatirati logički disk da bi radio. Relevantni fajl sistemi u savremenim OS su, [7], [24]:

- FAT 12 koji se koristi u FD (disketi);
- FAT 16, koristi se u DOS i Windows OS do Windows 95;
- FAT 32, verzija fajl sistema iz Windows 95B i Windows 9x serije;
- NTFS (*New Technology File System*), koristi se u OS Windows NT, 2000 i XP;
- HPSF (*High Performance File System*), u IBM OS/2;
- EXT, EXT2, EXT3&Reiser, fajl sistem u Linux OS;
- NSS&TFS (*Norton Storage & Traditional File System*).

Od većeg interesa je detaljno poznavanje Windows i Linux OS i njihovih fajl sistema. Poznati operativni sistemi su: *DOS, Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP i Linux* u više varijanti.

U ***FAT*** (*File Allocation Table*) ***16*** fajl sistemu tabela alokacija fajlova sadrži informcije o alociranim fajlovima, nekorišćenim lokacijama i neispravnim lokacijama. FAT tabela je model fizičkih sektora na fizičkm HD – svaka ćelija tabele predstavlja jedan zakrivljeni trapezoidni sektor. Fajlovi dolaze u svim oblicima i veličinama – od najmanjeg tekst fajla od samo nekoliko bajta do najvećih fajlova video filmova i baza podataka koji mogu biti reda MB i GB.

Poznato je da svaki fajl kada se skladišti može biti uskladišten samo u iznosu od 512 bajta, ili u jednom sektoru. Jedan fajl može biti veličine jednog sektora, a mogu biti milioni sektora. Bez obzira na veličinu fajla, OS mora slediti pravila FAT fajl sistema kojeg koristi, preko ulaza registrovanih u FAT tabeli koja reflektuje ta pravila.

Alokaciona tabela fajlova u FAT fajl sistemu ima samo 4 moguća ulaza označena sa:

1. **0** – znači da je alokaciona jedinica na raspolaganju za korišćenje,
2. **Broj ≥ 2** – znači da je sledeći deo fajla lociran u sektoru pod tim rednim brojem*,
3. **E** – indicira kraj fajla,
4. **B** – indicira loš sektor u koji se informacije ne mogu uskladištiti.

*Ulaz u FAT tabeli ukazuje na sledeću alokacionu jedinicu u kojoj postoji deo istog fajla Alokacione jedinice u FAT fajl sistemu počinju sa **2**. Moguć je slučaj da je alokaciona jedinica 2 rapoloživa za korišćenje, što je validan ulaz i ukazuje da ta jedinica formira deo fajla.

Druga kopija FAT tabele može se smatrati rezervnom kopijom (bekapom) i ove dve tabele treba da budu sinhrinizovane. Međutim, pošto su sinhronizovane, ako je oštećena prva FAT tabela, postoji verovatnoća da isto oštećenje ima i druga tabela.

U FAT fajl sistemu informacije o imenima fajlova, početku, završetku i veličini fajlova nalaze se u glavnoj listi – ***Imeniku ulaza*** (*Directory Entry*). Svi fajlovi u sistemu imaju ulaze u ***Imeniku ulaza***. Isti tip informacija o fajlovima sadrži i ***Root Directory***. ***Boot Record*** sadrži tehničke informacije o logičkim drajvovima. Sve tri ove oblasti u ***MBR*** - ***Boot Record, Root Directory i FAT tabela*** rade zajedno da omoguće korisnilu memorisanje, pronalaženje i korišćenje fajlova na računaru. Kako postoji više tipova FAT tabela, forenzičar mora znati kako ih može prepoznati.

FAT 12 je prvi *Microsoft* fajl sistem razvijen na FD, koji ga još uvek koristi. Znači da su svi kasniji MS OS podržavali FAT 12 fajl sistem, radi kompatibilnosti sa prethodnim sistemima. Ako savremeni računar (npr. Laptop) nema drajv za FD, to znači da ne podržava FAT 12 fajl sistem. Međutim, forenzičar mora poznavati ovaj fajl sistem zbog starijih računara koji su masovno u upotrebi.

FAT 12 znači da fajl sistem ima na raspolaganju za korišćenje ukupno **2^{12} = 4096** alokacionih jedinica. FD može imati 2 strane, sa po 18 sektora po strani i 80 tragova na svakoj strani, što daje ukupno 2880 sektora na disku – dovoljno da se adresira svaki individualni sektor korišćenjem FAT 12 fajl sistema, gde je svaka alokaciona jedinica po veličini jednaka jednom sektoru.

FAT 16 je sledeći *Microsoft* fajl sistem koji se pojavio na tržištu u Windows 3.0 i 3.11 pa čak i u Windows 95 OS. Ima na raspolaganju ukupno **2^{16}=65 536** alokacionih jedinica za korišćenje. Svaki sektor sadrži 512 bajta informacija, a koristeći isti metod za svaki alocirani sektor može se adresirati ukupno 33,554.432 bajta informacija, ili oko 33MB. Međutim, ovaj kapacitet su veoma brzo premašili proizvođači HD, pa se morao pronaći drugi način adresiranja i korišćenja celog raspoloživog prostora ovih diskova. Ovo je dovelo do razvoja koncepta ***klastera***, u kojem se koristi više sektora kao memorijska jedinica.

FAT 32 je poslednji sistem FAT tabela, uveden u *Microsoft* Windows 95(SE) OS, a podržavaju ga Windows 2000 i XP OS. FAT 32 daje 2^{32} odvojenih alokacionih jedinica, ali realno koristi samo 2^{28}=268,435.456 alokacionih jedinica.

10.1.1 Klasteri

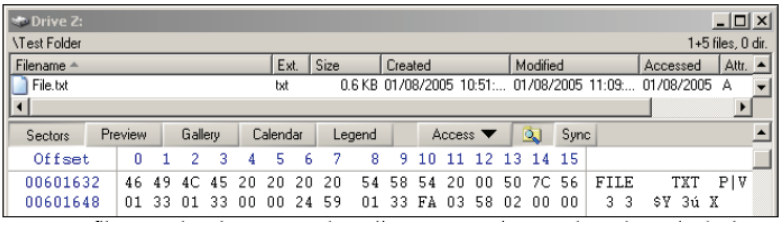
Klaster je grupisanje sektora koji se prostorno na disku nastavljaju jedan za drugim. Broj sektora u svakom klasteru je eksponent broja 2, a zavisi od korišćenog formata. Moguće je da korisnik upravlja i specificira broj sektora u klasteru. Međutim, informacija o broju sektora koji se koriste po klasteru data je u *But rekordu* rezervisanom za logičke diskove/particije. Najmanji broj sektora po klasteru je 4, što nije uvek slučaj. Veći logički diskovi imaće veći broj sektora po klasteru, maksimalno do 64, što je prikazano u tabeli 10.1.

Tabela 10.1 Broj sektora po klasteru FAT 16 i FAT 32 fajl sistema

FAT 16		FAT 32	
Logička veličina diska	Veličina klastera	Logička veličina diska	Veličina klastera
< 128 MB	4 Sectora (2KB)	< 512MB	Nije podržano
128MB – 255MB	8 Sectora (4KB)	512MB – 8GB	8 Sectora (4KB)
256MB – 511MB	16 Sectora (8KB)	8GB – 16GB	16 Sectora (8KB)
512MB – 1GB	32 Sectora (16KB)	16GB – 32GB	32 Sectora (16KB)
1GB – 2GB	64 Sectora (32KB)	32GB – 2TB	64 Sectora (32KB)

Način na koji se fajl ***memoriše*** u FAT fajl sistemu i šta se dešava u računaru u toku te operacije, forenzičar mora poznavati. Neka je kreiran fajl veličine od **600 bajta**. Dok se fajl formira nalazi se u memoriji i bez interakcije korisnika sa HD, ili medijumom. Postoji mogućnost da OS, ili neka aplikacija formira privremeni fajl koji je značajan izvor informacija za forenzičara.

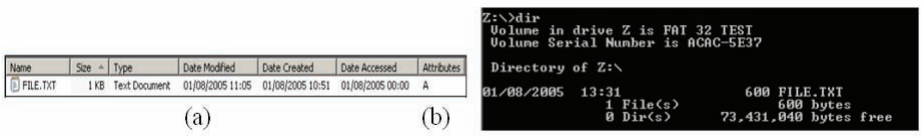
U procesu memorisanja i skladištenja fajla na disk, u prvom koraku fajl sistem traži prvu raspoloživu alokacionu jedinicu. Neka je klaster 2 raspoloživ za alokaciju na medijumu, koji je označen sa 0 u FAT tabeli. Klaster 2 ima 4 sektora (informaciju nalazimo u but rekordu) i može držati 2048 bajta podataka. Neka fajl od 600 bajta želimo memorisati u rut dorektorijum, tako da ulaz direktorijuma ide u rut direktorijum. Za svaki kreiran fajl formira se ulaz u direktorijumu (*direktory entry*) od najmanje 32 bajta, što je prikazano na slici 10.1, [24].



Slika 10.1 Ulaz direktorijuma za tekst fajl od 600 bajta (forenzički alat X Way)

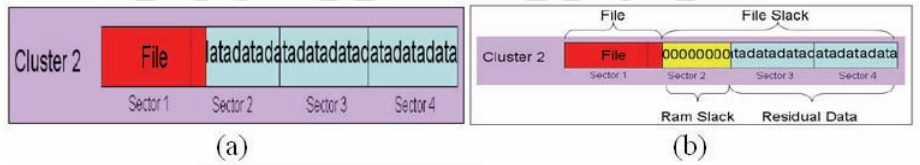
Ovaj ulaz sadrži informacije kao što su ime fajla, ekstenzija fajla, veličina fajla, datum i vreme kreiranja, datum i vreme modifikacije, datum pristupa (nema vremena ovde u FAT fajl sistemu), broj početnog klastera i atributi fajla. Ovaj

zapis omogućava da savremeni OS prikaže informacije kao na slici 10.2a, a stariji OS kao na slici 10.2b.



Slika 10.2 Prikaz tekst fajla od 600 bajta u OS

Kada napravi ulaz u rut direktorijumu, FAT sistem treba da se ažurira. Obe operacije izvršavaju se u stvari u isto vreme. Sistem zatim treba da upiše podatke u prvi raspoloživi klaster - klaster 2. Međutim, fajl ima svega 600 bajta, pa kapacitet klastera od 2048 bajta ostaje nepopunjen. Ostatak *nealociranog* prostora u zauzetom klasteru, dovodi do razvoja koncepta ***neiskorišćenog prostora fajla*** (*file slack*). Dakle, upisivanjem fajla od 600 bajta u alokacionu jedinicu - klaster 2 od 2048 bajta, fajl zauzima samo 600 bajta prostora, a ostatak alokacione jedinice je slobodan prostor. Kako klaster 2 ima 4 sektora od po 512 bajta, fajl od 600 bajta popuni prvi sektor klastera, a u drugi sektor upisuje se preostalih 88 bajta podataka fajla. U drugom sektoru ostaje nezauzeto 424 bajta. Preostali prostor drugog sektora koji nije popunjen upisanim fajlom naziva se ***slobodan prostor RAM***a (*Ram Slack*), (slika 10.3a). Prostor od kraja upisanih podataka fajla do kraja klastera naziva se ***slobodan prostor fajla*** (*File Slack*), (slika 10.3b), [24].



Slika 10.3 Slobodan prostor RAM (Ram Slack)-(a) i fajla (File Slack)-(b)

Termin *Ram Slack* dolazi od prvih fajl sistema koji su slučajno smeštali i uzimali podatke iz RAM memorije. Ovo znači da nije bilo načina da se kontroliše šta je stvarno poslato u tu lokaciju. Pojavom Windows 95 OS, ova praksa je promenjena i ostatak sektora sistem puni sa nulama, ali je naziv ostao u upotrebi. Preostala dva sektora ostaju nepromenjena i ovaj prostor se naziva ***preostali podaci*** (*Residual data*)**.** Ovaj prostor je od posebnog interesa za forenzičara. Ako se na nivou fajl sistema kojeg koristi OS otvori fajl **FILE**.**TXT**, videće se sadržaj fajla prikazan najverovatnije u *Notepad*-u sve

dok se podaci upisuju, ali se ne može videti oblast koja nije zauzeta podacima fajla. Međutim, forenzički alati rade sa podacima na nivou diska, tako da će se sav preostali prostor i podaci prethodnog fajla moći čitati i pretraživati. U gornjem primeru postoje dva sektora *preostalih podataka* koja treba analizirati. U slučaju većeg HD sa klasterom koji može imati i do 64 sektora, a sa upisanim istim fajlom od 600 bajta, preostaju 62 sektora ili 31744 bajta nezauzetog prostora sa *preostalim podacima*. Očigledno, iz podataka preostalih od prethodno izbrisanog fajla forenzičar može izvući mnogo korisnih informacija, kao što su e-mail adrese, lista dužnika, adrese klijenata i sl. Dakle, ako osumnjičeni korisnik ne upotrebljava neki anti-forenzički alat za brisanje svih tragova fajlova u računaru, ili alat za brisanje sa prepisivanjem, forenzičar ima velike šanse da otkrije koristan podatak za stvaranje digitalnog dokaza.

Slobodan prostor diska je termin koji se koristi da indicira da je FAT tabela označila alokacionu jedinicu kao raspoloživu za upotrebu. Fajl sistem ovo prepoznaje i može adresirati ovaj prostor i uskladištiti podatke. Slobodan prostor može takođe imati upisane podatke iz prethodno upisanog i izbrisanog fajla. Slobodan prostor je bio klaster 2 pre upisivanja fajla FILE.TXT od 600 bajta. Kada se jednom fajl upiše u klaster 2, ovaj klaster postaje alociran – dodeljen, ili rezervisan.

Forenzičar dalje mora znati šta se dešava u FAT fajl sistemu tokom ***kreiranja foldera.*** U rut direktorijumu kreira se istovremeno sa kreiranjem FILE.TXT fajla novi folder - NEW FOLDER. Ovaj folder u Windows sistemu izgleda kao na slici Sl 10.4a, a u DOS sistemu (b), ulaz foldera ide u *Rut direktorijum*, pošto je kreiran direktno u rutu **Z:** diska.

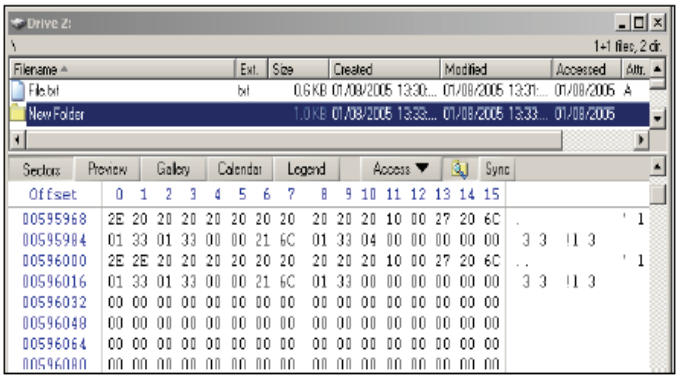


(a) (b)

Slika 10.4 Kreiranje novog foldera u rut direktorijumu Windows (a) i DOS (b) OS

Folder se skladišti na disku na isti način kao i fajl. Fajl sistem traži prvi raspoloživi klaster i memoriše ulaz foldera u njega. Ovaj ulaz je veličine od 32 bajta, što se vidi na slici 10.5 (ofset 00595968). Važne informacije su **'.'** i **'..'**

na početku ulaza foldera (desni prozor). Prva oznaka ukazuje na početak ulaza, a druga na pripadajući (*parent*) direktorijum. Ime NEW foldera nalazi se na nivou rut direktorijuma. Ovo je lokacija gde je sadržaj foldera uskladišten.



Slika 10.5 Ulaz novog foldera u rut direktorijumu u forenzičkom alatu

Na isti način kako smo u DOS sistemu morali otkucati '**CD**' da bi išli na jedan nivo više, tako su drugi FAT sistemi zadržali istu strukturu davanja imena. Dakle, kada smo sada u rut **Z:** direktorijuma i otkucamo CD NEW FOLDER, ili dva puta kliknemo na ulaz NEW FOLDER, fizički se premeštamo iz rut direktorijuma na disk, odnosno klaster gde je uskladišten NEW FOLDER. U ovo vreme direktorijum je prazan, ali kada ga počnemo popunjavati sa fajlovima, ili pod-folderima, pojaviće se ulazi ispod '**.**' i '**..**' (ofseti 00595984 i 00696016). Treba zapaziti da tamo gde se nalazi ***File slack*** u ulazu fajla, u direktorijumu nema ništa – ceo klaster je očišćen i ispisan nulama (ofset 00596032 i dalje).

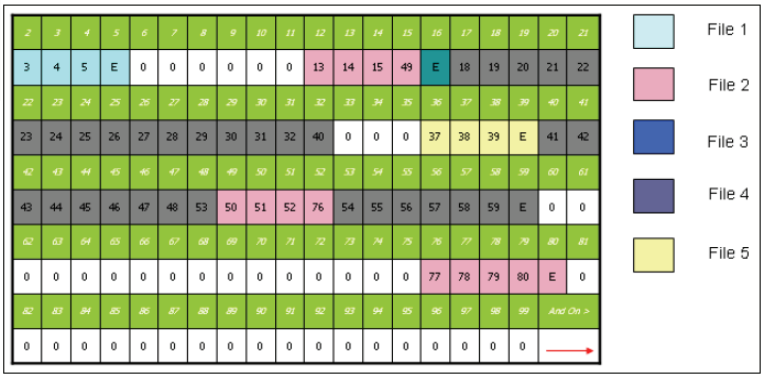
10.1.1.1 Fragmentacija i defragmentacija klastera fajlova u FAT fajl sistemu

Savremeni OS skladište fajlove za koje je potrebno više klastera u klastere koji se nalaze jedan do drugoga, odnosno *prostorno* povezane klastere bez prekida (*contiguos*). Tako računar zahteva manje vremena da pokrene glave i locira (čita/upisuje) delove fajla u povezanim klasterima, nego u nepovezanim, tzv. ***fragmentiranim*** klasterima. Računar uvek ne može uskladištiti svaki fajl u prostorno povezane klastere iz brojnih razloga. Neka

imamo word dokument od 20KB i počinjemo dodavati u ovaj dokument novi tekst kasnije. Postoje velike šanse da je u međuvremenu neki drugi fajl zauzeo klaster u kojem je smešten 20KB fajl. Računar sa FAT fajl sistemom traži sledeći raspoloživi klaster gde može uskladištiti podatke. Ovaj klaster može biti nepovezan sa originalnim, tj. fragmentiran i sasvim na drugom delu diska. Nivo fragmentacije nekog fajla može uticati na proces forenzičke analize. Sadržaj fajla koji je uskladišten u povezane klastere može se u celini oporaviti, dok nalaženje fragmentiranih delova fajla, bez dobre analize alokacione tabele fajlova može biti vrlo težak posao, [7], [24].

Alat za defragmentaciju klastera ugrađen je u sve savremene OS i korisnici se podstiču da regularno defragmentiraju svoj sistem i da ga učine efikasnijim. Ovaj proces uzima sve delove fragmentiranih fajlova i smešta ih zajedno u korektnom redosledu tako da ih računar može pronaći mnogo lakše.

Primer: Neka imamo 5 aktivnih uskladištenih, fragmentiranih i nefragmentiranih fajlova i neka su predstavljeni u FAT tabeli sa svojim ulazima. Neka je FAT tabela predstavljena slikom 10.6, koja pokazuje *klastere* 5 aktivnih fajlova, [24].



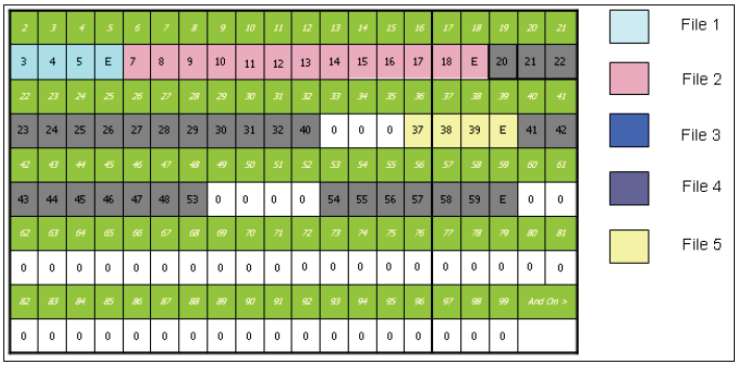
Slika 10.6 Fragmentirani i nefragmentirani klasteri 5 aktivnih fajlova na disku

Fajl 1 je očigledno potpuno povezan (neprekinut) – svi delovi nalaze se jedan iza drugog u povezanim klasterima i upisana je oznaka kraja fajla–**E** (EOF-*End of File*). Fajl 2 je fragmentiran u tri dela na različitim mestima, počevši od klastera 12-15, 49-52 i 76-80. Fajl 3 je u jednom klasteru – počinje i završava se u istom klasteru -16. Fajl 4 je takođe fragmentiran u tri dela u klasterima 17-32, 40-48 i 53-59, a fajl 5 zauzima 4 povezana klastera 36-39, što znači da

nije fragmentiran. Čak i ovakva fragmentacija na niskom nivou utiče na efikasnost računara.

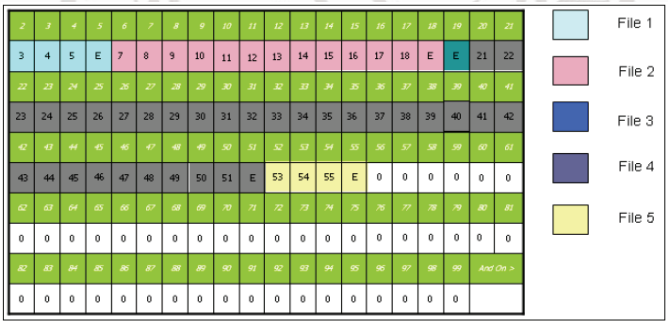
Aktiviranjem procesa defragmentacije računar nastoji da sve fragmentirane fajlove poveže u neprekinute celine. Proces ne utiče na Fajl 1 koji nije fragmentiran. Računar sada pokušava povezati Fajl 2 koji je fragmentiran. Na disku postoji nekoliko praznih alokacionih jedinica koje se mogu koristiti od 6 - 11 klastera. Ovi klasteri su prazni, što znači da se tamo mogu naći podaci iz izbrisanih fajlova. Zato, ako računar koristi ove klastere u procesu defragmentacije, ovi za forenzičara dragoceni podaci mogu biti prepisani i moguće trajno izgubljeni za potencijalne dokaze. U nastojanju da poveže sve fragmentirane fajlove u neprekinutu celinu, računar može pomeriti prva 4 klastera Fajla 2 u klastere 6 do 9. Zatim će pomeriti sledeću grupu od 4 klastera Fajla 2 iz klastera 49-52 na mesto klastera 10-13, tako da je sada povezano 8 klastera Fajla 2. Dalje je potrebno preneti preostale klastere Fajla 2 iz 76-80 klastera, ali za to više nema nezauzetog i neprekinitog prostora iza klastera 13. Zato računar mora prepisati Fajl 3 i deo Fajla 4 da bi u potpunosti defragmentisao Fajl 2, što nije prihvatljivo jer na taj način gubimo podatke. Dakle, računar mora uraditi nešto drugo, a to je da računar kopira podatke fajla 3 i fajla 4 i pomera ih na drugu nezauzetu lokaciju – slobodan prostor na disku, gde ih drži sve do trenutka kada ih vraća na poziciju defragmentisanih fajlova 3 i 4. Tako će u procesu potpune defragmentacije vrlo malo originalnih podataka ostati na originalnim lokacijama na disku. Kako sistem u procesu defragmentacije drži kopije fajlova u slobodnom prostoru diska, pa ako se isti fajl zatim izbriše posle defragmentacije, neki delovi fajla mogu se pronaći negde na disku. Zadatak forenzičara je da otkrije šta, kako i zašto se neki deo fajla nalazi bilo gde na disku, što nije nimalo lak posao.

Početak procesa defragmentacije u kojem je ceo Fajl 2 defragmentiran i povezan, a sadržaj fajla 3 i deo fajla 4 čuva se negde u slobodnom prostoru diska i čeka da se vrate natrag, prikazan je na slici 10.7.



Slika 10.7 Početak defragmentacije fajlova 1 i 2 od 5 fragmentisanih fajlova

Dakle, u procesu defragmentacije forenzičar može izgubiti neke podatke koji su možda trebali biti prepisani iz slobodnog prostora i *slack* prostora u neki fajl, ali može dobiti neke podatke koji su privremeno memorisani tokom procesa. Na kraju procesa defragmentacije u primeru fajl sistema sa 5 fajlova, defragmentisani fajlovi treba da izgledaju kao na slici 10.8, gde su svi fajlovi uskladišteni u povezane klastere.



Slika 10.8 Kraj defragmentacije 5 fajlova

Očigledna je efikasnost korišćenja prostora defragmentiranog diska u odnosu na fragmentirani disk.

10.1.1.2 Analiza izbrisanih fajlova u FAT fajl sistemu

Postoji više načina na koji korisnik može izbrisati neki fajl. Forenzičar mora znati šta se događa na disku kod svakog načina brisanja fajlova. Za

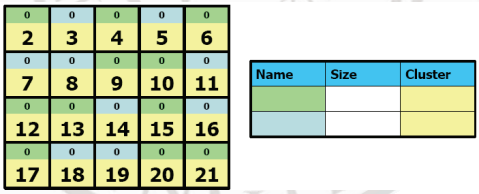
premeštanje fajla u korpu za otpatke (*Recicle bin*) postoje sledeći metodi, [24], [25]:

- desni taster miša i selekcija **Delete**,
- **drag&drop** u korpu za otpatke,
- taster **Delete** i
- potvrđeno brisanje (**Confirm Delete**).

Međutim postoje metodi za brisanje fajla iz fajl sistema koji ne idu kroz korpu za otpatke:

- Shift Delete,
- *Delete* u DOS-u,
- Empty Recicle bin.

Da bi se razumelo brisanje fajla u FAT fajl sistemu treba analizirati ***FAT tabelu*** i ***Direkrorijum ulaza*** (*Direktory Entriy*). Neka disk ima samo 20 klastera za skladištenje podataka i samo 2 ulaza u diretorijumu. Analizu treba početi sa praznom FAT tabelom (levo) i praznim direktorijumom ulaza (desno) na slici 10.9.



Slika 10.9 FAT tabela sa 20 klastera i praznim direktorijumom sa 2 ulaza

Neka se memorišu dva **Memo** fajla na disk, jedan po jedan. **Memo 1,** mali fajl od 11 klastera upisan je u klastere obojene zelenom bojom, da bi se lakše identifikovali i očigledno je fragmentiran na disku. Sada se FAT tabela mora ažurirati da bi prikazala gde su podaci **Memo 1** uskladišteni. Klaster 2 pokazuje da se sledeći deo podataka nalazi u klasteru 4, a klaster 4 ukazuje da se deo podataka nalazi u klasteru 6 i tako redom do kraja fajla **Memo 1** (**EOF**) u klasteru 21. Sada postoji validan skup ulaza koji pokazuju gde se svaki deo fajla **Memo 1** od 11 klastera može pronaći. Ulazi derektorijuma za **Memo 1** formirani su, a informcije o početnom klasteru i veličini nalaze se u ulazu direktorijuma. Neka se sada memoriše drugi fajl **Memo 2** na isti disk prikazan

sa ulazima obojenim u plavo. **Memo 2** počinje u klasteru 3, fragmentiran je i koristi klastere 5, 7, 8 itd. do klastera 19. Memo 2 zauzima 9 klastera ukupno i ima upisane ulaze u direktorijumu – veličinu i početni klaster, (slika 10.10).



Name	Size	Cluster
memo1	21,636	2
memo2	17,535	3

Slika 10.10 Ažuriranje FAT tabele i ulaza direktorijuma za 2 memorisana fajla

Neka se sada izbriše fajl **Memo 1** iz sistema i posmatraju promene koje nastaju, (slika 10.11). Prvo, u ulazima direktorijuma menja se prvi karakter imena fajla u grčki znak **σ** (sigma), ili što je korektnije koji se u *hex* zapisu identifikuje kao vrednost '**E5**'. Ovo je prvi bajt podataka u direktorijumu ulaza i prva tačka kontakta sa izbrisanim fajlom. Ako fajl sistem čita **E5** *hex* zapis tada zna da se ovaj ulaz ne koristi i da je na raspolaganju za prepisivanje sa novim ulazom.



Name	Size	Cluster
σemo1	21,636	2
memo2	17,535	3

Slika 10.11 Ažurirane promene u FAT tabeli i direktorijumu ulaza posle brisanja fajla

Sada treba identifikovati promene u FAT tabeli. Svi ulazi prethodno zauzeti sa **Memo 1** sada su prazni i spremni za novi fajl i resetovani na **0**, što za OS znači da može upisivati nove podatke. Međutim, izbrisani su samo ulazi, ali su podaci u klasterima ostali nepromenjeni i mogu se oporaviti, samo ako nisu prepisani sa novim fajlom. Podaci u direktorijumu ulaza još uvek su na raspolaganju za čitanje. Jedini gubitak podataka u ovoj oblasti je prvi bajt, ili prvo slovo imena fajla.

Fajl **Memo 1** sada je u celini izbrisana, pa ako želimo oporaviti izbrisani fajl moramo tražiti ostale raspoložive informacije u MFT tabeli, a to je najveći deo imena fajla, veličina fajla i početni klaster. Kao prvi korak, uzima se veličina fajla – **21,636** i izračuna koliko klastera zahteva ovaj fajl na disku. Na ovom disku veličina klastera je od 4 sektora ili 2048 bajta, što znači da je

potrebno: **21636/2948=10,56** ili **11** klastera za skladištenje tog fajla. Takođe, znamo da je početni klaster fajla klaster **2**. Ako se krene od početnog klastera **2** i crvenim okvirom i istakne početni i ostali koji slede sa ulazom **0**, dobije se diagram klastera izbrisanog fajla kao na slici 10.12.



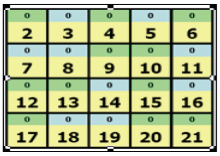
Slika 10.12 Metod oporavka klastera izbrisanog fajla

Dakle, na ovaj način svi zeleni ulazi izbrisanog fajla FAT tabele su selektovani. Ovaj metod precizno oporavlja izbrisani fajl. Da bi se fajl oporavio mogu se ponovo prepisati FAT ulazi kao ranije i klasteri ih počinju koristiti. Direktorijum ulaza takođe treba ažurirati, pošto **E5**h indicira izbrisane ulaze, tako da ga menjamo sa neuobičajenim karakterom, na primer donjom crtom '**_**'. Treba izbegavati stavljanje slova sa namerom pogađanja imena fajla, (slika 10.13).

Name	Size	Cluster
_emo1	21,636	2
memo2	17,535	3

Slika 10.13 Ažuriranje ulaza oporavljenog izbrisanog fajla u direktorijumu ulaza

Neka su sada izbrisana oba fajla **Memo 1** i **Memo 2**. U FAT tabeli izbrisani su svi FAT ulazi i nulirani, a oba ulaza u direktorijumu promenjena u izbrisane i označeni su sa **E5**h, (slika 10.14).

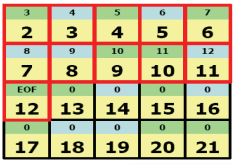


Name	Size	Cluster
σemo1	21,636	2
σemo2	17,535	3

Slika 10.14 FAT tabela i direktorijum ulaza za dva izbrisana fajla

Da bi se ovi fajlovi oporavili može se koristiti isti metod kao u prethodnom slučaju. Prvo se uzima izbrisani fajl od 21,636 bajta. Izračuna se koliko klastera veličine 2048 bajta zahteva za skladištenje na disk. Dobije se da je

potrebno 11 sektora. Zatim se istakne crvenim okvorom klaster 2, pa onda sledeći raspoloživi klasteri, koji je u ovom primeru očigledno klaster drugog fajla. Dakle, ako se pokuša oporavak **Memo 1** fajla i pretpostavi da je neprekinut (nije fragmentiran), a iz prethodnog primera je poznato da je fragmentiran, dobije se FAT tabela sa ulazima kao na slici Sl 10.15.



Slika 10.15 FAT tabela dva oporavljena fajla

Očigledno da **Memo 1** fajl nije lako uspešno oporaviti, jer je kombinovan sa drugim fajlom, može biti čitljiv, ali bez mnogo smisla. Za oporavak izbrisanih fajlova treba koristiti sve raspoložive informacije, jer fragmentacija u FAT sistemu može izazvati ozbiljne probleme u oporavku izbrisanog fajla.

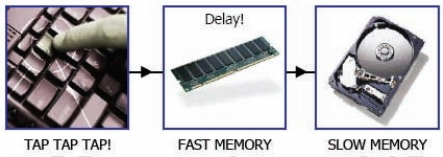
Iz ovog primera vidi se da ako je fajl neprekinut (nije fragmentiran) oporavak može biti prilično uspešan. Međutim, ako je fajl fragmentiran postoji ozbiljan problem za uspešan oporavak fajla. Takođe, fajl koji je upravo izbrisan može se uspešnije oporaviti nego fajl koji je izbrisan znatno ranije, jer je u međuvremenu sistem mogao prepisati i ponovo koristiti prostor izbrisanog fajla.

10.2 Analiza NTFS fajl sistema

Najveći broj savremenih računarskih sistema koristi *NTFS* fajl sistem. Za forenzičara značajno je razumeti dve ključne karakteristike ovog fajl sistema, koje ga razlikuju od FAT fajl sistema: *usporeno upisivanje/brisanje* i *logovanje transakcija,* [24].

Usporeno snimanje/brisanje (tzv. *Lazy Write*) je jedno od svojstava NTFS fajl sistema koje forenzičar mora razumeti. Sa aspekta digitalne forenzičke analize potrebno je podsetiti na tipove memorije u računarskom sistemu, njihovu namenu, prednosti i nedostatke. Čvrsti disk (HD) je mehanički uređaj sa pokretnim glavama i ansamblom ploča-diskova, koji može uskladištiti vrlo veliku količinu podataka za dugi period skladištenja. Zbog toga je brzina upisivanja/očitavanja podataka u/sa HD relativno spora u poređenju sa

drugim memorijskim komponentama. Računar ima i vrlo brze memorije za skladištenje privremenih fajlova. Primer je ***RAM*** (*Random Access Memory*) primarna memorija. Ova dva metoda skladištenja podataka, računar koristi da veštački poveća brzinu pristupa korisnika sistemu i podacima. Kada korisnik odluči da memoriše neke podatke u NTFS fajl sistemu, sistem ih upisuje na najbrži mogući način u RAM memoriju. Sistem pokazuje korisniku da su podaci memorisani, a oni su u stvari smešteni u RAM memoriju. Sistem neko vreme sačeka pa kada je spreman, unosi podatke iz RAM memorije na HD. Ovo kašnjenje između skladištenja u RAM i u permanentnu memoriju (HD) obično traje samo nekoliko sekundi, ali korisnik opravdano veruje da su podaci odmah memorisani i upisani na HD, (slika10.16).



Slika 10.16 Kašnjenje upisivanja podataka u RAM i trajnu memoriju

Ovo kašnjenje može se zapaziti kada se koriste prenosni medijumi, na primer USB. Za tu svrhu treba formatirati USB da podržava NTFS fajl sistem, pošto je ovo kašnjenje karakteristika NTFS sistema, na sledeći način:

1. desnim tasterom miša na **USB** uređaj u eksploreru,
2. otvoriti **Properties** opciju,
3. otvoriti **Hardware** opciju,
4. izabrati **USB drajv** sa liste,
5. otvoriti Properties,
6. otvoriti **Policies** opciju i
7. izabrati **Optimize for performance**, (slika10.17).

Upravo poslednja opcija (na slici) omogućava i onemogućava *Lazy Write* sistem.



Slika 10.17 Optimizacija performansi USB u NTFS fajl sistema

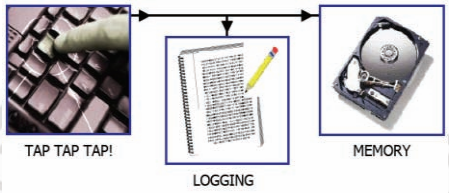
Kada je opcija **Optimize for performance** izabrana, važno je da se svaki prenosni medijum odspaja od računara korišćenjem sistemske ikone za bezbedno uklanjanje hardvera - ’ ’. Ako se USB uređaj ne ukloni na ovaj način, može se dogoditi da su podaci još uvek u RAM memoriji i da nisu kompletno upisani u USB memoriju. Razumevanje ove *Lazy Write* karakteristike NTFS fajl sistema značajno je za forenzičara, posebno u procesu pretrage i privremenog oduzimanja, pošto se može dogoditi da osumnjičeni USB sistem memoriše podatke iz RAMa u vreme privremenog oduzimanja. Drugim rečima, kada pristupi aktivnom osumnjičenom računaru, ili ako u vreme privremenog oduzimanja osumnjičeni briše podatke, npr., daljinski, forenzičar mora znati:

1. gde su podaci trenutno uskladišteni i
2. gde bi ovi podaci bili da se isključi napajanje iz sistema?

Pri tome treba znati da sistem prikazuje da **je proce**s memorisanja kompletiran, što ne mora biti slučaj – možda su u tom trenutku samo upisani podaci u RAM memoriju, ali ne i na HD. Ako se u tom trenutku isključi napajanje iz računara, svi podaci mogu ostati u RAM-u i biti trajno izgubljeni.

Isti proces upisivanja sa kašnjenjem (*Lazy Write*) primenjen je i za brisanje podataka. Kada korisnik sistema izvrši komande za brisanje podataka, čeka se neko vreme da sistem upiše izmene na HD.

Logovanje transakcija je druga funkcija ugrađena u NTFS sistem za poboljšavanje stabilnosti sistema. Metapodaci NTFS fajl sistema su bitni za rad sistema i moraju biti zaštićeni. Svaku promenu u nekom fajlu NTFS sistema, ažurira fajl *Metadata* NTFS fajl sistema. Da se obezbedi integritet promene u fajlu i spreči njeno oštećenje u NTFS fajl sistemu, postoji fajl metapodataka ***$Logfile*** koji upravo kontroliše proces logovanja transakcija, (slika 10.18).



Slika 10.18 Logovanje transakcija u **$Logfile** NTFS fajl sistema

Svaki put kada se izvrši neka izmena, u metadata fajlu dodaje se jedan ulaz (*entry*) u *$Logfile*. Ovaj ulaz je od 4KB dužine i sadrži sledeće inormacije:

1. *„LSN" (broj logičke sekvence)*: za praćenje redosleda dodavanja ulaza u Log fajl;
2. *„Redo Field":* gde se registruju informacije o transakcijama koje se upravo dešavaju;
3. *„Undo Field":* gde se registruju informacije koje omogućavaju povratak transakcije u originalno stanje, ako je potrebno;
4. ***„****Commit":* koja se upisuje kada je transakcija kompletirana.

Svakih 8 sekundi NTFS sistem proverava da li su sve transakcije kompletirane. Ovo vreme provere napredan korisnik može izmeniti u ***Registru***, što forenzičar mora imati u vidu. Šta se dešava sa transakcijom pre ove provere sistem ne mora znati. Ako postoji greška u transakciji, tada sistem treba da ispita *$Logfile* i da odredi šta je potrebno uraditi kroz sledeće akcije:

1. *„Search for first record"*: pretraživanje prvog registrovanog broja u ***LSN*** listi;

2. *„Analysis Pass“*: analiza uslova za prolazak transakcije, gde sistem određuje šta treba uraditi sa svakim ulazom (*entry*).
3. *„Redo Pass“:* gde se svi ulazi koji imaju *Commit* polje mogu ponoviti da obezbede uspešno kompletiranje transakcije.
4. *„Undo“:* svih ulaza koji nisu puni.
5. *„Commit“:* biće nekompletirani pre nego što zatim mogu ponoviti transakciju.

Logovanje transakcija obezbeđuje *povratak,* ili *oporavak* fajla. Struktura diska sa NTFS fajl sistemom razlikuje se od FAT baziranih sistema. NTFS fajl sistem nema sistemsku oblast za praćenje fajlova uskladištenih na disku kao kod FAT fajl sistema. U NTFS fajl sistemu sistemska oblast je zamenjena sa *sistemskim fajlovima,* koji obavljaju istu funkciju i mnogo više od toga kao i *sistemska oblast* u FAT fajl sistemu. Činjenica da ovo više nije restriktivna oblast diska, ukazuje na fleksibilnost NTFS sistema. Dakle, ***sve*** u NTFS sistemu je neki fajl. Sistemski fajlovi u NTFS fajl sistemu nazivaju se *Metadata fajlovi,* (tabela 10.2), [24].

Tabela 10.2 Metadata sistemski fajlovi u NTFS fajl sistemu

Zapis fajla	Naziv fajla	OS	Opis
0	$MFT		Indeks svakog fajla na logičkom disku
1	$MFTMirr		Backup prva 4 MFT zapisa
2	$Logfile		Transakcioni logging fajl
3	$Volume		Naziv, verzija i stanje logičkog diska
4	$AttrDef		Definicije atributa
5	.		Koreni direktorijum logičkog diska
6	$Bitmap		Iskorišćenost u odnosu na mapu slobodnih klastera
7	$Boot		Boot record
8	$BadClus		Oštećeni klasteri na logičkom disku
9/Bilo koji	$Quota	NT/2K	Quota informacije
9	$Secure	2K	Bezbednosni deskriptori logičkog diska
10	$UpCase		Tabela karaktera velikih slova

11	$Extend	2K	Direktorijuki sa dodatnim fajlovima metapodataka
12-15			Označeno kao korišćeno, ali je prazno
16-23			Označeno kao neiskorišćeno
Bilo koji	$ObjId	2K	Jedinstveni identifikatori dodeljeni fajlovima/direktorijumima
Bilo koji	$Reparse	2K	Reparse point informacije
Bilo koji	$UsnJrnl	2K	Dnevnik izmena
>24			Fajlovi i direktorijumi

Sa aspekta digitalne forenzičke analize, značajno je detaljnije razmotriti sledeće metadata fajlove NTFS sistema:

$MFT: MFT (*Master File Table*) je srce NTFS fajl sistema. Svaki fajl uskladišten u NTFS formatu mora imati najmanje jedan ulaz u MFT tabeli. MFT je sačinjena od određenog broja ulaza (*entries*), od kojih je svaki dugačak 1024 bajta. Svaki ulaz sadrži informacije koje se odnose na neki fajl na logičkom disku. Takođe, metapodaci su uskladišteni kao fajl, pa moraju imati ulaze u MFT, uključujući i ulaz za samu MFT.

$MFT mirr: Ovaj faj je kreiran za oporavak NTFS sistema i predstavlja tačnu kopiju najvažnijih oblasti MFT tabele – njen početak. Podrazumevano to je kopija prva 4 ulaza u MFT, ali može biti i više ulaza, ako se promeni veličina klastera. Ovaj fajl je obično lociran prema centru oblasti podataka.

$Logfile: Ovaj fajl se koristi za logovanje transakcija i sadrži ulaze od 4KB, koji registruju promene u svim fajlovima za potrebe oporavka u slučaju pada sistema.

$Volume: Ovaj fajl sadrži informacije o verziji NTFS koji se koristi u logičkom disku, ime i identifikator logičkog diska, kao i informacije o regularnom isključivanju (***shutdown***) kao što su marker *dirty flag*.

$AttrDef: Fajl sadrži informacije o atributima, vrednostima, imenima i veličinama.

.(dot): Sadrži ulaze uskladištene u rutu sistema. Ovo je efektivno folder ulaza za rut sistema.

$Bitmap: Ovo je mapa klastera na logičkom disku. Svaki bit u ovom fajlu predstavlja jedan klaster na disku. Klasteri mogu biti označeni kao da su u

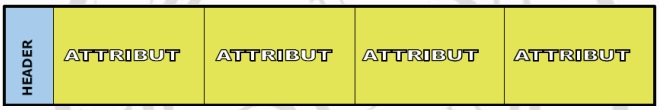
upotrebi, ili nisu u upotrebi, nasuprot FAT fajl sistemu u kojem FAT tabela sadrži 4 ulaza – ***0***, broj ***2*** ili veći, ***EOF*** marker ili ***Bad***.

$Boot: Fajl sadrži ***Boot sektor*** i ***Boot Code*** informacije. Uvek je locirana u Klasteru **0**. Skladišti lokacije *$MFT* i *$MFTMirr* koje su neophodne za podizanje (butovanje) sistema i povratak informacija korisnicima.

$BadClus: Ovaj fajl skladišti lokacije loših klastera na logičkom disku. Loš klaster biće označen kao u upotrebi u ***$Bitmap*** fajlu – a zatim se briše u ***$BadClus***.

10.2.1 Analiza MFT ulaza NTFS fajl sistema

Zapis u MFT sastoji se od *hedera* i seta *atributa,* (slika 10.19). Svaki ulaz u MFT je dužine 1024 bajta. Heder varira po veličini, zavisno od OS koji se koristi za kreiranje fajlova. Windows 2000 kreira hedere od 48 bajta, dok Windows XP ima hedere od 56 bajta.



Slika 10.19 Struktura MFT tabele u NTFS fajl sistemu

Heder uvek počinje sa ASCI nizom 'FILE'. Unutar hedera uskladišten je broj MFT ulaza za taj fajl. Bajtovi **22-23** čuvaju tekuće stanje MFT ulaza:

- 01 00 = Tekući fajl
- 00 00 = Izbrisani fajl
- 03 00 = Tekući folder
- 02 00 = Izbrisani folder

Posle hedera nalazi se neki broj ***atributa***. Svaki atribut skladišti različite delove informacija o fajlu, na primer:

- *„Standard Information"*: Skladišti podatke o datumu i vremenu,
- *„Filename"*: Skladišti informacije o imenu fajla,
- *„Object ID"*: Globalni jedinstveni identifikator fajla,
- ***„Data":*** Skladišti sadržaj fajla.

Svaki atribut je sačinjen od dve razdvojene oblasti: ***heder atributa*** i ***niz atributa***. Heder atributa sadrži: *identifikatore atributa, dužinu atributa, lokaciju niza atributa* i druge informacije. Niz atributa sadrži aktuelne podatke za te atribute.

Kada forenzičar zna tip informacija, traži ono što mu je potrebno da sazna kako da pronađe ove informacije i intepretira ih. Da bi se identifikovali atributi treba locirati identifikatore atributa. Lista tipičnih atributa na desnoj strani (slika 10.20) predstavljena je sa *identifikatorima* atributa od 32 bita uskladištena u ***Little Endian***-u na levoj strani.

10 00 00 00 = $STANDARD INFORMTION
30 00 00 00 = $FILE_NAME
40 00 00 00 = $OBJECT_ID
80 00 00 00 = $DATA

Slika 10.20 Identifikatori tipičnih atributa hedera u MFT NTFS fajl sistema

Posle identifikatora atributa dolazi dužina atributa, koja takođe ima vrednost od 32 bita, uskladištenu u ***Little Endian***-u. Sa ovim informacijama forenzičar može pregledati MFT ulaze i identifikovati individualne atribute. Prvo treba gledati MFT heder, koji u Windows XP OS predstavlja prvih 56 bajta. Posle MFT hedera dolazi prvi atribut. Atributi su uvek poredani prema numeričkom redosledu vrednosti identifikatora atributa, (slika 10.21). Identifikator atributa je 4 bajta, a sledeća 4 bajta su dužina atributa. Ovi se moraju računati u ***Little Endian***-u da bi se odredio ukupan broj bajta alociranih za ovaj atribut. *Važno je uočiti da se ukupan broj bajta računa od prvog bajta identifikatora do poslednjeg bajta niza atributa.*

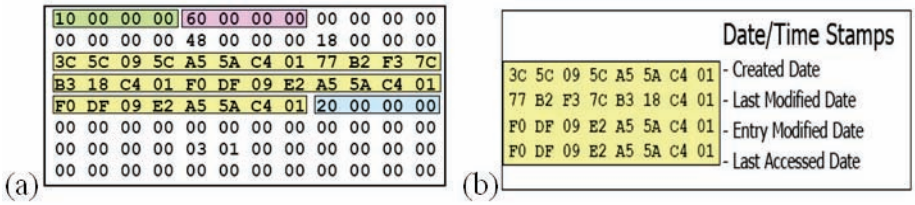


Slika 10.21 MFT heder i atributi u Windows XP OS

Atributi slede jedan za drugim neposredno bez praznog prostora između njih. Sa ovim jednostavnim proračunom mogu se kretati kroz MFT tabelu i identifikovati svi pojedinačni atributi. Kada se identifikuju svi individualni atributi dolazi heksadecimalna vrednost ***FF FF FF FF*** koja indicira kraj MFT ulaza.

10.2.2 Analiza MFT atributa NTFS fajl sistema

Kada forenzičar potpuno razume kako može locirati individualne atribute u NTFS fajl sistemu, onda može analizirati i izvlačiti podatke iz svakog atributa. Prvo treba pogledati u ***$STANDARD_INFORMATION*, (slika** 10.22), [7], [24].



Slika 10.22 Atribut **$STANDARD_INFORMATION** u hex zapisu forenzičkog alata

Ovo je prvi atribut iza MFT hedera, a počinje sa ulazom 10 00 00 00 u MFT zapisu (a). Prva 4 bajta ovog atributa (zelena) pokazuju identifikator atributa. Vrednost 10 00 00 00 indicira da je to ***$STANDARD_INFORMATION*** atribut koji sadrži informacije o *datumu i vremenu*. Sledeća 4 bajta (60 00 00 00) pokazuju dužinu atributa, a vrednost 60 00 00 00 u ***Little Endian***-u indicira vrednost od 96 bajta. Oblast istaknuta žutom bojom predstavlja informacije o datumu i vremenu koji su pridruženi ovom fajlu (b). Ovo formira deo niza atributa. Svaki fajl ima 4 ulaza za datum i vreme, jedan više nego što korisnik može videti. To je informacija o datumu i vremenu koju sistem koristi da ažurira datume i vremena za korisnike (*Entry modified date*).

Oblast naglašena sa plavom bojom sadrži 4 bajta DOS atributa za fajl: 20 00 00 00, što. u DOS atributima (*flags*) označava '***Archive***' (slika 10.23).

Code	Meaning
01 00 00 00	Read Only
02 00 00 00	Hidden
04 00 00 00	System
10 00 00 00	Directory
20 00 00 00	Archive
40 00 00 00	Device
80 00 00 00	Normal
00 01 00 00	Temporary
00 02 00 00	Sparse File
00 04 00 00	Reparse Point
00 08 00 00	Compressed
00 10 00 00	Offline
00 20 00 00	Not Content Indexed
00 40 00 00	Encrypted

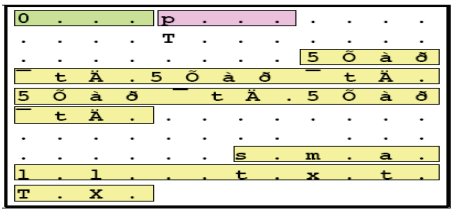
Slika 10.23 Značenje kodiranih **flags** DOS atributa u hex zapisu

Sada treba analizirati ***$FILE_NAME*** atribut. U ovom primeru isti je tip početka atributa – identifikator atributa od 4 bajta (30 00 00 00), iza kojeg slede 4 bajta o veličini atributa (70 00 00 00), (slika 10.24).

```
30 00 00 00 70 00 00 00 00 00 00 00
00 00 04 00 54 00 00 00 18 00 01 00
05 00 00 00 00 00 05 00 35 D5 E0 F0
AF 74 C4 01 35 D5 E0 F0 AF 74 C4 01
35 D5 E0 F0 AF 74 C4 01 35 D5 E0 F0
AF 74 C4 01 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 20 00 00 00
00 00 00 00 09 03 73 00 6D 00 61 00
6C 00 6C 00 2E 00 74 00 78 00 74 00
54 00 58 00
```

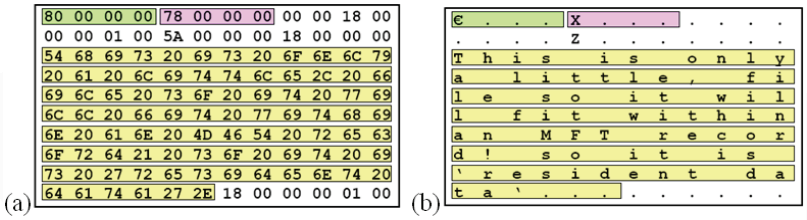
Slika 10.24 Atribut **$FILE_NAME** u hex zapisu forenzičkog alata

U ovom primeru postoje dve oblasti istaknute žutom bojom. Gornji boks u heksadecimalnom zapisu pokazuje NTFS zapise datuma i vremena u vrlo sličnom formatu kao u hederu ***$Standard_Information***. Ovi datumi i vremena su pridruženi atributu ***$File_name***. Iako je skoro sasvim identičan sa zapisom datuma i vremena u ***$Standard_ Information*** atributu, nije podešen da monitoriše fajl, nego samo ime fajla. Druga žuto istaknuta oblast je stvarno ime fajla za ovaj fajl. Ova informacija je uskladištena u UNICODE i nije čitljiva u gornjem boksu ako forenzičar dobro ne poznaje *hex* zapis. U donjem boksu, međutim, može se pročitati ime fajla – ***Small.txt***, (slika 10.25).



Slika 10.25 ASCI zapis imena fajla

Sledeći atribut koji forenzičar mora razumeti je ***$DATA*** atribut, koji sadrži stvarni sadržaj fajla. Ovaj atribut ima iste oblasti kao i drugi atributi fajla – heder atributa koji sadrži bajtove identifikatora atributa i veličine atributa, a zatim ostale pomoćne informacije. Ovaj atribut ima takođe svoj niz atributa. Sledeća dva dijagrama pokazuju ovaj atribut u *hex* (a) i ASCII (b) zapisu (slika 10.26).



Slika 10.26 Atribut **$DATA** u hex (a) i ASCII (b) zapisu

Dijagram (a) pokazuje sadržaj fajla ***Small.txt***. Kada je sadržaj fajla u celini unutar MFT ulaza, ovi se podaci nazivaju ***Rezidentni podaci***. Kako je MFT ulaz 1024 bajta dug, a svaki ulaz može sadržati neki broj atributa različite dužine. Ako je ukupna veličina ovih atributa manja od 1024 bajta svi se mogu uskladištiti u MFT ulaz. Ovo uključuje i podatke atributa. U sledećem dijagramu (slika 10.27) prikazne su veličine individualnih atributa prema ukupnoj veličini MFT ulaza.

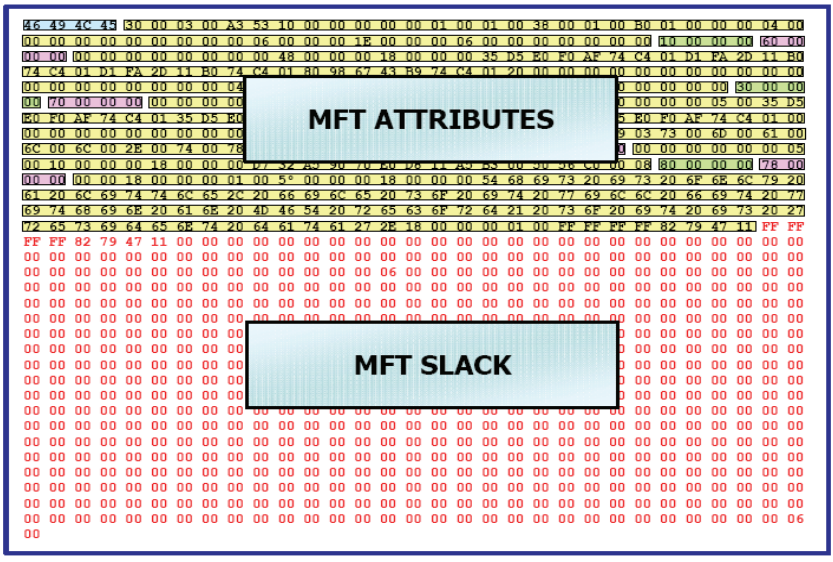
Attribute	Size
Header	56
Standard Information	96
Filename	112
Object ID	40
DATA	120
	424 Bytes / 1024 Bytes

Slika 10.27 Veličine atributa prema veličini MFT ulaza u NTFS fajl sistemu

MFT ulaz ne može biti manji od 1024 bajta. U gornjem primeru za ovaj ulaz iskorišćena su 424 bajta MFT, što ostavlja neiskorićenih 600 bajta ovog ulaza. Za označavanje kraja atributa unutar MFT ulaza koristi se vrednost **FF FF FF FF**. Svaki preostali prostor unutar MFT ulaza naziva se ***MFT slack***.

10.2.3 Analiza MFT *slack* prostora

Kod analize *MFT slack* (nezauzetog) prostora važno je razumeti kada *MFT slack* sadrži, a kada ne podatke. Kada se kreira novi fajl u MFT se upisuje 1024 bajta, što rezultira sa upisivanjem nula na kraju MFT ulaza. Kada se fajl modifikuje jedina promena se upisuje u MFT ulaz i ovaj može obezbediti podatke u *MFT slack* prostoru. Primer kada se ovo može dogoditi je promena imena fajla. Na primer, kada se kreira novi dokument, korišćenjem desnog tastera miša i metoda za kreiranje novog dokumenta, kreira se fajl '*New text document*'. Ovo se odmah upisuje u novi ulaz u MFT. Korisnik zatim promeni ime fajla u nešto kraće – '*small.txt*', što redukuje ukupan broj atributa potrebnih za ovaj fajl. Sada bi trebalo da postoje podaci u *MFT slack* prostoru. Na sledećem dijagramu (slika 10.28) ilustrovan je *MFT slack* (nezauzet) prostor.



Slika 10.28 MFT atributi i MFT slack prostor

Isto važi i za ***$DATA*** atribut, ako se rezidentni podaci izmene da budu kraći, originalni podaci uskladišteni u *MFT slack* prostoru mogu biti vidljivi.

Do sada smo posmatrali vrlo male fajlove tipa malih tekst fajlova, ili potencijalno GIF fajlova, koji mogu stati u MFT ulaz od 1024 bajta kao rezidentni podaci. Šta se dešava sa mnogo većim fajlom od 1024 ulaza? Svaki atribut ima dve glavne oblasti – *heder* i *niz atributa*. Heder atributa uvek mora biti smešten u MFT ulazu kao *rezidentni podatak*, dok niz atributa može biti uskladišten i izvan MFT ulaza, kao *nerezidentni podata*k. Kada podaci atributa postanu suviše veliki da se mogu uskladištiti kao rezidentni podaci, niz ***$DATA*** mora biti uskladišten kao nerezidentni podatak.

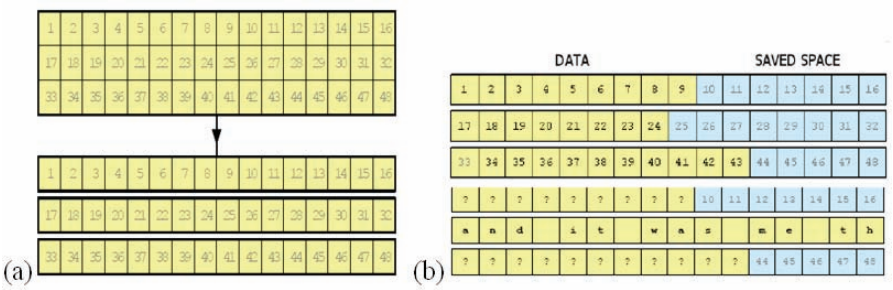
Dakle, neka su podaci sada uskladišteni u klasterima diska, MFT ulaz mora registrovati gde su ovi podaci locirani i koliko podataka je pridruženo ovom ulazu. Za praćenje traga skladištenja ovih podataka ***$DATA*** fajla, atribut sadrži ***Run listu*** – 31 17 05 98 01, (slika 10.29). *Run lista* skladišti lokaciju i dužinu podataka uskladištenih u klasterima na disku. Heder ***$DATA*** atributa prikazan na dijagramu još uvek ostaje unutar MFT ulaza. Kada se ova *Run lista* preračuna, ukazuje na lokaciju i dužinu ***$DATA*** atributa. Treba zapaziti da su ovi podaci, iako uskladišteni izvan MFT, još uvek neki atribut.



Slika 10.29 **Run** lista atributa za skladištenje lokacije i dužine podataka

10.3 Analiza kompresovanih podataka

Sposobnost kompresije savremenih OS ugrađena je i u NTFS fajl sistem, koji nema potrebe za dodatnim softverom za kompresiju. Kopresija se podešava sa ostalim atributima fajla i identifikuje se s ostalim atributima pomoću ***DOS flags***. Kada se aktivira proces kompresije, fajl koji je podvrgnut kompresiji deli se na kompresione jedinice od po 16 klastera, (slika 10.30a). Sistem zatim pokušava da komprimuje svaku kompresionu jedinicu individualno koristeći modifikovan ***LZ77*** algoritam koji zamenjuje ponavljajuće nizove nekim kôdom, (slika 10.30b), [24].



Slika 10.30 Kompresija fajla u NTFS fajl sistemu

U slučaju jednostavnog tekst fajla ovo mogu biti reči koje se ponavljaju. Kompresija može dramatično smanjiti zahtevani prostor za skladištenje fajla na disku. Međutim, nije uvek moguće kompresovati podatke. Ako sistem ne može memorisati barem jedan klaster u jednu jedinicu od 16 klastera, taj klaster će biti memorisan bez kompresije.

Kada ispituje disk koji može vršiti NTFS kompresiju, forenzičar treba da razmatri nekoliko pitanja. Pretraživanje diska prema ključnoj reči i rekonstrukcija diska možda neće funkcionisati, pošto reč koja se traži može biti kompresovana, odnosno da nije više upisana na disku u otvorenom tekstu. Takođe, treba znati da nema hedera, ili ekstenzije koja jasno indicira prisustvo kompresovanih fajlova - u Windows XP OS ovi se fajlovi prikazuju plavim slovima. Forenzički softver interpretira ove kompresovane fajlove koristeći njihov sistem identifikacije. Iako forenzički softver može oporaviti NTFS kompresiju, potrebno je proveriti da li je korišćeni alat ažuriran sa poslednjom verzijom i da li korektno oporavlja sve kompresovane informacije.

10.4 Analiza šifrovanih informacija

Šifrovanje u NTFS fajl sistemu uvedeno je sa Windows 2000 OS. Iako Windows 2000 i XP OS podržavaju šifrovanje, da bi ova funkcija bila aktivna disk mora biti formatiran za NTFS fajl sistem.

Kada se neki fajl šifruje, ne šifruje se ceo fajl nego samo *niz podataka*, dok je MFT ulaz za fajl i dalje u otvorenom tekstu. Šifrovanje se može podesiti za individualni fajl, ili za sve fajlove u izabranom direktorijumu. Za omogućavanje sistema da se butuje i radi normalno, postoje oblasti koje se

ne mogu šifrovati, kao što su metadata fajlovi i fajlovi u rutu sistema (Windows NT). Takođe, nije moguće šifrovati već kompresovane fajlove., [24], [25]

Šifarski sistem NTFS fajl sistema je veoma jak i nije ga lako probiti. Ipak, već postoje alati koji ga pod određenim uslovima mogu probiti.

Međutim, forenzičar mora imati na umu da se često u forenzičkom alati neki fajl pojavljuje kao nečitljiv ili možda šifrovan, što ne mora da znači. Treba proveriti da li se taj fajl može otvoriti nekom drugom aplikacijom, pre nego što se odluči da je nečitljiv.

10.5 Oporavak izbrisanog fajla u NTFS fajl sistemu

Od forenzičara se očekuje razumevanje procesa brisanja fajla u NTFS fajl sistemu i razlikovanje tog procesa od korišćenja *Recycla bin*-a. Postoje više načina na koji korisnik može brisati fajl, a sledeći metodi šalju izbrisani fajl u *Recycla bin,* [24]:

1. Desni taster miša i selektovanje *Delete*,
2. Drag&Drop u Recycla bin,
3. Taster *Delete*, potvrđeni *Delete*.

Sledeći metodi brišu fajl iz fajl sistema zaobilazeći *Recycla bin:*

1. Shift Delete,
2. *Delete* u DOS-u.

Brisanje fajla u NTFS fajl sistemu zahteva promene u metadata fajlovima. Kada se izvrše promene u metadata fajlovima, *$Logfile* treba da prati te promene za potrebe oporavka. Tako će brisanje fajla biti ažurirano u *$Logfile*.

Svaki fajl u NTFS ima jedan ulaz u MFT tabeli i zato, ako se fajl briše iz fajl sistema tada se on mora izmeniti u *$MFT* ulazu hedera, da bi odrazilo tekuće stanje ulaza.

U MFT ulazu hedera ažuriraju se bajtovi **22** ***i*** **23.** Moguća stanja koje možemo naći na ovim lokacijama su:

- **00 00** = Izbrisani (*Deleted*) fajl,

- **01 00** = Tekući fajl,
- **02 00** = Izbrisani direktorijum,
- **03 00** = Tekući direktorijum.

Ovde forenzičar mora znati da brisanje fajla ne uklanja, niti prepisuje MFT ulaz – on jednostavno ima samo ažuriran status koji pokazuje da je fajl „izbrisan". Dakle, jedine stvari koje se menjaju u MFT zapisu u vreme brisanja su ova dva bajta, a sve ostalo ostaje neizmenjeno.

Klasteri podataka koji su okupirani sa fajlovima više se ne zahtevaju, što se reflektuje u *$Bitmap* fajlu, koji se takođe ažurira. Svi klasteri označeni u *$Bitmap* fajlu kao da su u upotrebi nekog fajla, sada će biti označeni da nisu u upotrebi i zato će biti na raspolaganju sistemu za prepisivanje. Naravno, ovo se samo dešava kada se briše nerezidentni fajl, pošto rezidentni fajlovi ne koriste klastere i tako ne zahtevaju da *$Bitmap* fajl mapira njihovu oblast skladištenja.

Dakle, ovo nije promena aktuelnih podataka u klasterima, nego samo promena statusa klastera, a svi podaci u ovim klasterima ostaju posle brisanja. Posle brisanja nekog fajla NTFS fajl sistem ima sledeći status:

- ***$Logfile*** se ažurira da loguje promene u metapodacima, koristeći logovanje transakcija za oporavak u slučaju greške sistema.
- ***$MFT*** ulaz za izbrisani fajl se ažurira da indicira da je fajl sada izbrisan. Ovaj MFT ulaz sada je na raspolaganju sistemu za skladištenje novih fajlova i može biti prepisan. MFT ulazi se ispisuju sa vrha na dole, tako da će ulazi u MFT, bliži vrhu tabele biti prvi ispisani.
- ***$Bitmap,*** u klasterima prethodno okupiranim sa izbrisanim fajlovima i predstavljenim sa binarnim „1", sada menja u binarne „0", označavajući da klasteri nisu u upotrebi i da sistem u njih može skladištiti nove podatke i prepisati postojeće.
- ***Nerezidentni podaci*** u klasterima koji skladište podatke nisu izmenjeni i ostaju nedirnuti na disku u originalnim lokacijama.
- ***Rezidentni podaci*** ostaju netaknuti i neizmenjeni u MFT ulazu, jer MFT ulaz nije uklonjen.
- ***Ulazi direktorijuma*** se ažuriraju za izbrisane fajlove, indicirajući da su izbrisani.

Dakle, ako je fajl upravo izbrisan i još nije prepisan, postoji mnogo informacija na raspolaganji forenzičaru, koje se mogu lako identifikovati i oporaviti pomoću softverskih forenzički alata. Međutim, ovo nije uvek slučaj. Ako je fajl sistem izbrisao neki fajl, moguća su tri slučaja koji ovo menjaju:

Scenario 1: MFT ulaz je prepisan sa novim ulazom. Klasteri koji skladište originalne podatke nisu prepisani. MFT je sada kompletno prepisan, a svi pripadajući podaci prepisani. Podaci u klasterima ostaju nedirnuti i neizmenjeni i mogu se locirati i oporaviti forenzičkim alatima. Ovo su sada podaci u nealociranom prostoru bez dodatnih informacija. Zbog brisanja MFT ulaza, fragmentirani fajlovi se sada ne mogu oporaviti

Scenario 2: MFT ulaz nije prepisan sa novim ulazom. Klasteri koji skladište originalne podatke sada su prepisani sa sadržajem novog fajla. U MFT ovaj ulaz ostaje netaknut. Ako su podaci bili rezidentni, još uvek bi mogli biti ovde uskladišteni, a sve informacije još dostupne kao što su: imena fajlova, datum i vreme, podaci, *run* lista itd. Pitanje je šta sada pokazuje run lista? Podaci u klasterima sada su prepisani sa novim podacima i ne mogu se oporaviti. Forenzičar treba da ispita *File slack* i *MFT slack* prostore.

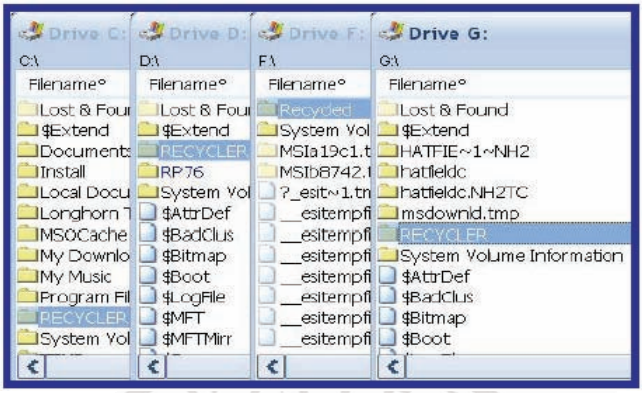
Scenario 3: MFT ulazi i klasteri za fajl prepisani su sa novim podacima. MFT je sada potpuno prepisana i svi pomoćni podaci su izbrisani i prepisani. Podaci u klasterima su prepisani sa novim podacima i više se ne mogu oporaviti.

Dakle, tek izbrisan fajl može se oporaviti sa svim podacima, imenima fajlova, atributima fajlova i vremenima i datumima, što daje dosta informacija forenzičaru. Što je duže vreme od kada je fajl izbrisan, to se smanjuje šansa za oporavak većine podataka i informacija, zbog ponovnog korišćenja MFT zapisa, ili oblasti podataka, što se ne može kontrolisati.

Korpa za reciklažu **(***Recycle Bin***)** u koju korisnici na više načina šalju izbrisani fajl ima značaj za forenzičara. Korpa za reciklažu prvo se pojavila u Windows 95 OS i od tada ostaje u desktop računarima na Windows platformama, bez izmene funkcije za korisnika.

Međutim, sa aspekta forenzičara korpa za reciklažu menjana je sa promenama OS i forenzičar mora razumeti te promene. Korpa za reciklažu je skriveni folder koji se nalazi u rutu svakog logičkog diska. Jedna od značajnih promena korpe za reciklažu je njeno ime pod kojim se skladišti na disk. U FAT formatiranom disku korpa za otpatke se naziva *Recicled,* a u NTFS disku *Recycler.* Kako je poznato na jednom fizičkom disku može biti više od jednog logičkog diska, od kojih svaki ima svoju korpu za reciklažu. Na slici 10.31

prikazan je jedan fizički disk podeljen na 4 logičke particije sa Windows XP OS instaliranim na C: particiji.



Slika 10.31 Fizički disk sa 4 logičke particije i 4 korpe za reciklažu u Windows XP OS

Na svakom logičkom disku, zavisno od OS postoji korpa za reciklažu sa različitim imenom, zavisno od OS. Korisnik sistema ima samo jednu korpu za reciklažu na ekranu, koja čita informacije iz korpi svih fajlova na svim logičkim diskovima i skuplja ih za korisnika u jednu korpu. Kada forenzičar traži dokaze iz korpe za reciklažu, forenzičar mora razmatrati iz koje korpe logičkog diska sistema su neki podaci i šta korpa predstavlja za korisnika. U tom smislu može poslužiti analogija sa *korpom za otpatke u kući*, *kesom za đubre* i *seckalicom dokumenata*.

Korpa za otpatke u kući–(*Recycle Bin*)***:*** Kada korisnik stavi sa stola neki papir u korpu za otpatke, još uvek ga može iz nje izvaditi, ako mu zatreba. Jedini način da se papir trajno ukloni je da se korpa isprazni.

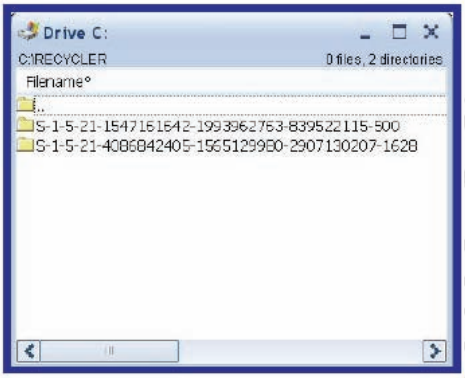
Kesa za đubre-Brisanje (*Deletion*)***:*** Kada se korpa za otpatke isprazni u kesu za đubre, gubi se kontrola o sadržaju, kesa se baca u kontejner, a gradska čistoća sakuplja i odnosi kese u vreme koje korisnik ne može kontrolisati. Ovaj korak korisnik preduzima da ukloni ono što mu ne treba.

Seckalica dokumenata-Brisanje softvera (*Shredder*): Ako je neki dokument poverljiv korisnik će upotrebiti seckalicu za trajno uništavanje.

Operativni sistem podrazumevano formira korpu za reciklažu u toku instaliranja svakog novog logičkog diska (particije) na fizičkom disku. Ovaj folder je prazan dok korisnik u njega ne počne slati izbrisane fajlove. U prvom trenutku brisnja nekog fajla, sistem kreira sledeće fajlove:

- *SID*[10] ime foldera za korisnika,
- *INFO2* fajl,
- Desktop.ini fajl i
- Placeholder(s) fajl.

SID ime foldera: Svakom korisniku u NTFS fajl sistemu alocira se jedinstveni korisnički ***ID***, poznat kao *korisnički* ***SID*** (bezbednosni identifikator). Na slici 10.32 prikazan je primer sa dva korisnika na sistemu i njihova dva jedinstvena SID-a. Kompletna lista SID identifikatora može se naći na web sajtu Microsoft-a.



Slika 10.32 Korisnički SID za dva korisnika

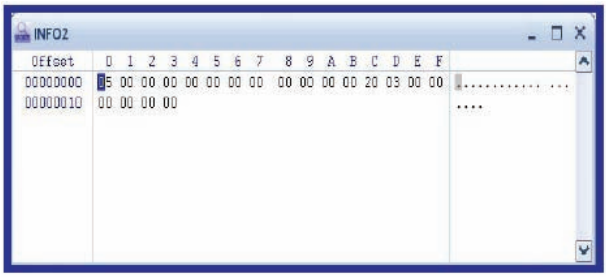
Ako na sistemu ima više korisnika, svaki korisnik će imati svoj folder u *Recycle Bin*-u. Kada korisnik izbriše fajl on se smešta u njegov SID folder u RECYCLER folderu.

Desctop.ini se modifikuje kada se *Recycle bin* isprazni, ili potpuno restaurira. Ovo je standardni sistemski fajl koji se koristi za podatke foldera. Podatak o modifikciji ovog fajla indicira kada je *Recycle Bin* poslednji put ispražnjen, ili potpuno restauriran.

INFO2 fajl sadrži detalje o fajlovima uskladištenim u *Recycle Bin-u* za taj određeni disk. Ovo je jedan fajl koji sadrži više ulaza. Kao i većina drugih fajlova, INFO2 ima heder od 29 bajta dužine. Posle hedera su smešteni ulazi za fajlove u *Recycle Bin-u*, svaki od po 800 bajta dužine. Ovi ulazi skladište

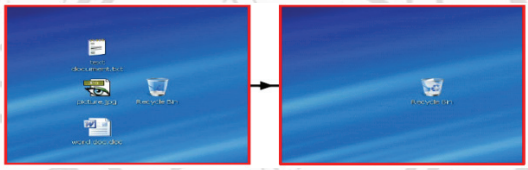
[10] *Windows Security Identifier*

relevantne informacije za restauraciju fajla u originalno stanje, ili za trajno brisnje fajla. Na slici 10.33 prikazan je INFO2 fajl kada nema fajlova u *Recycle Bin*-u, a sve što se može videti je INFO2 heder – 05.



Slika 10.33 Izgled **INFO2** fajla u forenzičkom alatu kada u Recycle Bin-u nema fajlova

Ako sada sa *drug&drop* prenesemo u *Recycle Bin* sa desktopa tri fajla: TEXT DOCUMENT.TXT, PICTURE.JPG i Word DOC:DOC oni će, nestati sa desktopa, (slika 10.34).



Slika 10.34 Prenos 3 fajla drug&drop funkcijom u Recycle Bin

Sada imamo fajlove u *Recycle Bin*-u i mora biti dodatnih fajlova u folderu RECYCLER. Ove fajlove u ovom slučaju sam sistem imenuje kao: *Dc5.doc, Dc6.txt, Dc7.jpg,* a nazivaju se *placeholders* i imaju jedinstvenu konvenciju imenovanja, po redosledu:

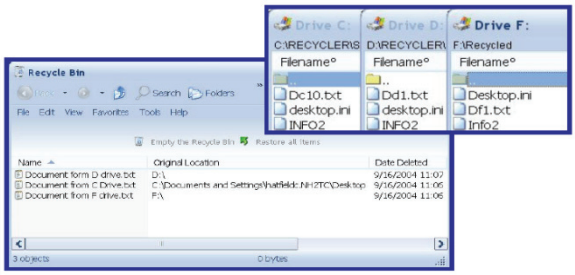
1. **D** – Deleted,
2. **c** – disk/particija izbrisanog fajla,
3. **#** – broj izbrisane sekvence,
4. **.doc** – originalna ekstenzija fajla.

U gornjem primeru svi fajlovi su izbrisani sa **C:** diska tako da će svi biti uskladišteni u RECYCLER folder na **C:** disku. Takođe, iz imena fajlova (#) vidi se da nisu prvi fajlovi poslati u *Recycle Bin* i da su tamo već bila 4 fajla (brojanje počinje sa 1). Pored kreiranja *placeholders,* INFO2 fajl se sada

ažurira za skladištenje informacija o ovim fajlovima. Svaki od ovih 800-bajtnih ulaza sadrži sledeće informacije:

1. originalna lokacija i ime fajla u *Unicode*,
2. originalna lokacija i ime fajla u *ASCII* kodu,
3. originalno slovo drajva (diska, particije),
4. broj sekvence *placeholders* i
5. datum/vreme brisanja.

Korisnici često brišu fajlove iz različitih logičkih particija, zato treba imati na umu da svaka logička particija ima svoj vlastiti RECYCLER. Tri fajla vidljiva u *Recycle Bin*-u na slici 10.35 izbrisana su iz različitih logičkih particija.



Slika 10.35 Izgled tri izbrisana fajla iz različitih logičkih particija u folderima RECYCLER

Oni su nevidljivi za korisnika sistema i samo se javljaju u jednom kontejneru - *Recycle Bin* na desktopu sistema. Manja slika pokazuje tri individualna diska i sadržaj RECYCLER foldera na ovim diskovima. Kada se fajl pošalje u *Recycle Bin* biće uskladišten u *RECYCLER* folderu onog diska sa kojeg je izbrisan. Kada se fajl šalje u *Recycle Bin* događaju se sledeće promene:

1. kreira se jedan ulaz u SID folderu za korisnika koji briše fajl,
2. ime fajla se zamenjuje sa *placeholders* imenom fajla,
3. INFO2 fajl se ažurira sa novim ulazom,
4. ažurira se vreme i datum poslednjeg pristupa i modifikacije ulaza.

Kada je fajl poslat u *Recycle Bin* stvarno se događaju sledeće stvari:

1. fajl nije izbrisan,

2. ništa nije izgubljeno, podaci su još uvek tekući i neizmenjeni, MTF je još uvek neizmenjena,
3. *Run* lista za podatke ostaje neizmenjena,
4. Fajl *$Bitmap* ostaje neizmenjen.

Kada restauriramo fajl iz *Recycle Bin*-a dgađaju se sledeće promene:

1. INFO2 fajl se ažurira, za relevantni ulaz,
2. ulaz u SID folderu se uklanja,
3. ulaz za originalni folder se kreira,
4. ime fajla u MFT se ažurira,
5. originalni fajl je restauriran.

Kada korisnik isprazni *Recycle Bin* tek onda su izbrisani fajl i podaci koje sadrži trajno izgubljeni. Generalno, forenzičar treba da razmatra nekoliko elemenata kada izvlači dokaze iz *Recycle Bin*-a:

- ***Da li je korisnik izbrisao fajl***?: Ako je logički disk formatiran u NTFS, tada će RECYCLER folder sadržavati sub-folder SID broja, koji indicira koji se korisnik logovao kada je fajl premešten u *Recycle Bin.* Disk formatiran u FAT fajl sistemu neće sadržavati SID folder, što znači da treba koristi drugi metod, na primer, traženje originalne lokacije i ko je imao pristup ovoj oblasti.
- ***Da li je kompjuter izbrisao fajl***?: Ovaj slučaj nije moguć, pošto program ne koristi *Recycle Bin.*
- ***Da li korisnik poznaje*** *Recycle Bin?*: Da li je korisnik ikada praznio ili restaurirao fajl iz *Recycle Bin-a*, ili menjao podešavanje *Recycle Bin*-a i da li je *Recycle Bin* prikazan na desktopu? Postoj brojni načini da se utvrdi znanje korisnika o računaru, komponentama i programima koji se pojave u analizi dokaza.

10.5.1 Konfigurisanje *Recycle Bin*-a

U većini slučajeva prenosni mediji nemaju *Recycle Bin.* Ovo zavisi od tipa medija koji se koristi. Generalno, mali prenosni USB-olovka neće imati *Recycle Bin.* Kada se izbriše fajl iz njega, ne može se izabrati premeštanje u *Recycle Bin* i sve će biti trajno izbrisano. Veći diskovi obično imaju *Recycle Bin*

i svaki izbrisani fajl biće premešten u RECYCLER folder tog diska. Korisnik može konfigurisati *Recycle Bin* tako da odgovara individualnim potrebama. *Recycle Bin* se može onemogućiti na svim logičkim diskovima, ili na individualnim logičkim particijama. Veličina diska alocirana za *Recycle Bin* takođe se može konfigurisati na svim ili individualnim logičkim diskovima. *Recycle Bin* radi po principu 'prvi unutra-prvi vani' (FIFO), tako kada se dostigne alocirani prostor *Recycle Bin*-a, sledeći fajlovi koji se upute u *Recycle Bin* trajno će izbrisate prve fajlove u tom *Recycle Bin*-u.

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

REZIME

Poznavanje fajl sistema koji se koristi u OS, važno je za svakog forenzičara. Fajl sistem određuje način na koji računar skladišti sve fajlove i foldere koji su potrebni korisniku i šta se dešava kada se oni premeste, ili izbrišu. Forenzičar mora poznavati kako svaki relevantni fajl sistem adresira i pronalazi fajlove na fizičkom/logičkom disku. Fajl sistem mora formatirati logički disk da bi radio. Relevantni fajl sistemi u savremenim OS su: FAT 12 koji se koristi u FD (disketi); FAT 16, koristi se u DOS i Windows OS do Windows 95; FAT 32 iz Windows 95B i Windows 9x serije; NTFS u OS Windows NT, 2000 i XP; HPSF u IBM OS/2; EXT, EXT2, EXT3&Reiser fajl sistemi u Linux OS i NSS&TFS. Od većeg interesa je detaljno poznavanje Windows i Linux OS i njihovih fajl sistema. Poznatiji operativni sistemi su: *DOS, Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP i Linux* u više varijanti.

U *FAT 16* fajl sistemu tabela alokacija fajlova sadrži informcije o alociranim fajlovima, nekorišćenim i neispravnim lokacijama. Tabela alokacija fajlova u FAT fajl sistemu ima 4 moguća ulaza. Oznaka **0** – znači da je alokaciona jedinica na raspolaganju za korišćenje; **Broj ≥ 2** – da je sledeći deo fajla lociran u sektoru pod tim rednim brojem; **E** – indicira kraj fajla i **B** – indicira loš sektor u koji se informacije ne mogu uskladištiti. FAT 12 je prvi *Microsoft* fajl sistem razvijen na FD, koji ga još uvek koristi i ima na raspolaganju za korišćenje ukupno 2^{12} = 4096 alokacionih jedinica veličine sektora. FAT 16 je sledeći *Microsoft* fajl sistem koji se pojavio na tržištu u Windows 3.0 i 3.11 i 95 OS. Ima na raspolaganju ukupno 2^{16}=65 536 alokacionih jedinica za korišćenje i može adresirati ukupno oko 33MB. Kako je ovaj kapacitet HD brzo prevaziđen, razvijen je koncept *klastera* u kojem se koristi više sektora kao memorijska jedinica. FAT 32 je poslednji sistem FAT tabela, uveden u *Microsoft* Windows 95(SE) OS, a podržavaju ga Windows 2000 i XP OS. FAT 32 daje 2^{32} odvojenih alokacionih jedinica, ali realno koristi samo 2^{28}=268,435.456 alokacionih jedinica. Informacija o broju sektora koji se koriste po klasteru data je u *But rekordu* rezervisanom za logičke diskove/particije. Najmanji broj sektora po klasteru je 4, što nije uvek slučaj. Veći logički diskovi imaće veći broj sektora po klasteru, maksimalno do 64.

Ako se u prvi slobodan klaster upiše fajl manji od veličine klastera, preostali *nealocirani* prostor može sadržavati ranije upisane potencijelne dokaze i naziva se fajl *slack.* Preostali prostor nepopunjenog sektora upisanim fajlom naziva se *Ram Slack.* Nepopunjeni sektori u kasteru sadrže rezidualne podatke, posebno značajne za forenzičara, ako osumnjičeni korisnik ne upotrebljava neki anti-forenzički alat za brisanje svih tragova fajlova u računaru. *Slobodan prostor* diska je termin koji se koristi da indicira da je FAT tabela označila alokacionu jedinicu kao raspoloživu za upotrebu. Folder u FAT fajl sistemu se skladišti na disku na isti način kao i fajl, što forenzičar mora znati. Važne informacije su **'.'** i **'..'** na početku ulaza od 32 bajta u FAT tabeli, gde prva oznaka ukazuje na početak ulaza foldera, a druga na pripadajući (*parent*) direktorijum.

Nivo fragmentacije nekog fajla može uticati na proces forenzičke analize. Sadržaj fajla koji je uskladišten u povezane klastere može se u celini oporaviti, dok nalaženje fragmentiranih delova fajla, bez dobre analize alokacione tabele fajlova može biti vrlo težak posao. Alat za defragmentaciju klastera ugrađen je u sve savremene OS i korisnici se podstiču da regularno defragmentiraju svoj sistem i da ga učine efikasnijim.

Postoji više načina na koji korisnik može izbrisati neki fajl. Forenzičar mora znati šta se događa na disku kod svakog načina brisanja fajlova. Za brisanje fajla kroz *Recicle bin* izbrisan fajl se lako oporavlja. Izbrisani fajl koji ne ide kroz *Recicle bin,* takođe se može oporaviti, jer su izbrisani samo ulazi, ali su podaci u klasterima ostali nepromenjeni i mogu se oporaviti, samo ako nisu prepisani sa novim fajlom. Podaci u direktorijumu ulaza još uvek su na raspolaganju za čitanje. Jedini gubitak podataka u ovoj oblasti je prvi bajt, ili prvo slovo imena fajla. Međutim, fragmentacija u FAT sistemu može izazvati ozbiljne probleme u oporavku izbrisanog fajla.

Najveći broj savremenih računarskih sistema koristi *NTFS* fajl sistem. Za forenzičara značajno je razumeti dve ključne karakteristike ovog fajl sistema, koje ga razlikuju od FAT fajl sistema: *usporeno upisivanje/brisanje* i *logovanje transakcija*. NTFS fajl sistemu upisuje podatke na najbrži mogući način u RAM memoriju, a korisniku pokazuje da su podaci memorisani, iako su u stvari smešteni u RAM memoriju. Sistem neko vreme sačeka pa kada je spreman, unosi podatke iz RAM memorije na HD. Ovo kašnjenje između skladištenja u RAM i u permanentnu memoriju (HD) obično traje samo nekoliko sekundi, ali korisnik opravdano veruje da su podaci odmah memorisani i upisani na HD. Razumevanje ove *Lazy Write* karakteristike NTFS fajl sistema značajno je za

forenzičara, posebno u procesu pretrage i privremenog oduzimanja, pošto se može dogoditi da osumnjičeni USB sistem memoriše podatke iz RAMa u vreme privremenog oduzimanja. Drugim rečima, kada pristupi aktivnom osumnjičenom računaru, ili ako u vreme privremenog oduzimanja osumnjičeni briše podatke, npr., daljinski, forenzičar mora znati gde su podaci trenutno uskladišteni i gde bi ovi podaci bili da se isključi napajanje iz sistema?

Logovanje transakcija je druga funkcija ugrađena u NTFS sistem za poboljšavanje stabilnosti sistema. Metapodaci NTFS fajl sistema su bitni za rad sistema i moraju biti zaštićeni. Svaku promenu u nekom fajlu NTFS sistema, ažurira fajl *Metadata* NTFS fajl sistema. Da se obezbedi integritet promene u fajlu i spreči njeno oštećenje u NTFS fajl sistemu, postoji metadata fajl *$Logfile* koji upravo kontroliše proces logovanja transakcija. Svakih 8 sekundi NTFS sistem proverava da li su sve transakcije kompletirane. Ovo vreme provere napredan korisnik može izmeniti u *Registru*, što forenzičar mora imati u vidu. Šta se dešava sa transakcijom pre ove provere sistem ne mora znati. Ako postoji greška u transakciji, tada sistem treba da ispita *$Logfile* i da odredi šta je potrebno uraditi. *Logovanje transakcija* obezbeđuje *povratak,* ili *oporavak* fajla.

Sa aspekta digitalne forenzičke analize, značajno je detaljnije razmotriti sledeće *metadata* fajlove NTFS sistema: *$MFT*, *$MFT mirr, $Logfile, $Volume, $AttrDef, .(dot), $Bitmap, $Boot i $BadClus.*

Zapis u MFT sastoji se od *hedera* i seta *atributa*. Svaki ulaz u MFT je dužine 1024 bajta. Heder varira po veličini, zavisno od OS koji se koristi za kreiranje fajlova. Windows 2000 kreira hedere od 48 bajta, dok Windows XP ima hedere od 56 bajta. *Heder* uvek počinje sa ASCI nizom 'FILE'. Unutar hedera uskladišten je broj MFT ulaza za taj fajl. Bajtovi 22-23 skladište tekuće stanje MFT ulaza. Posle hedera nalazi se neki broj *atributa*. Svaki atribut skladišti različite delove informacija o fajlu, npr., *Standard Information*-skladišti podatke o datumu i vremenu, *Filename* - skladišti informacije o imenu fajla, *Object IDs*-globalni jedinstveni identifikator fajla, *Data*-skladišti sadržaj fajla itd. Svaki atribut je sačinjen od dve razdvojene oblasti: *heder atributa* i *niz atributa*. Heder atributa sadrži: *identifikatore atributa, dužinu atributa, lokaciju niza atributa* i druge informacije, a *niz atributa* sadrži aktuelne podatke za te atribute.

Kada forenzičar potpuno razume kako može locirati individualne atribute u NTFS fajl sistemu, onda može analizirati i izvlačiti podatke iz svakog atributa.

Na primer, prvo treba pogledati u *$STANDARD_INFORMATION***,** prvi atribut iza MFT hedera, a počinje sa ulazom 10 00 00 00 u MFT zapisu. Prva 4 bajta ovog atributa pokazuju identifikator atributa. Vrednost 10 00 00 00 indicira da je to *$STANDARD_INFORMATION* atribut koji sadrži informacije o *datumu i vremenu*. Zatim treba nastaviti analizu redom sledeće 4 bajta itd.

Kod analize *MFT slack* prostora važno je razumeti kada sadrži, a kada ne podatke. Forenzičar, takođe, mora razumeti kompresiju fajlova koja je ugrađena i u NTFS fajl sistem, kao i šifrovanje fajlova da bi ih analizirao.

Brisanje fajla u NTFS fajl sistemu zahteva promene u metadata fajlovima. Kada se izvrše promene u metadata fajlovima, *$Logfile* treba da prati te promene za potrebe oporavka. Tako će brisanje fajla biti ažurirano u *$Logfile*. Svaki fajl u NTFS ima jedan ulaz u MFT tabeli i zato, ako se fajl briše iz fajl sistema tada se on mora izmeniti u *$MFT* ulazu hedera, da bi se odrazilo tekuće stanje ulaza. U MFT ulazu hedera ažuriraju se bajtovi 22 *i* 23*,* a izbrisani fajl ima oznaku 00 00 u MFT ulazu. Ovde forenzičar mora znati da brisanje fajla ne uklanja, niti prepisuje MFT ulaz – on jednostavno ima samo ažuriran status koji pokazuje da je fajl „izbrisan“. Svi klasteri označeni u *$Bitmap* fajlu kao da su u upotrebi nekog fajla, sada će biti označeni da nisu u upotrebi i zato će biti na raspolaganju sistemu za prepisivanje, a svi podaci u ovim klasterima ostaju posle brisanja. Dakle, ako je fajl upravo izbrisan i još nije prepisan, postoji mnogo informacija na raspolaganji forenzičaru. Pri tome forenzičar može naići na tri moguća scenarija: MFT ulaz je prepisan sa novim ulazom, MFT ulaz nije prepisan sa novim ulazom i MFT ulazi i klasteri za fajl prepisani su sa novim podacima, kada se podaci ne mogu više oporaviti.

Korpa za reciklažu **(***Recycle Bin***)** u koju korisnici na više načina šalju izbrisani fajl ima značaj za forenzičara. Na jednom fizičkom disku može biti više od jednog logičkog diska, od kojih svaki ima svoju korpu za reciklažu – u NTFS sistemu naziva se *Recycler*. Operativni sistem podrazumevano formira korpu za reciklažu u toku instaliranja svakog novog logičkog diska (particije) na fizičkom disku. U prvom trenutku brisnja nekog fajla, sistem kreira fajlove: *SID* ime foldera za korisnika, *INFO2*, *Desktop.ini* i *Placeholder*(s), koje forenzičar treba da detaljno anlizira. Forenzičar mora znati šta se dešava u fajl sistemu kada korisnik šalje fajl u *Recycler* folder i oporavlja fajl iz njega. U većini slučajeva prenosni mediji nemaju *Recycle Bin,* pa kada se izbriše fajl iz njih biće trajno izbrisan. *Recycle Bin* radi po principu ’prvi unutra-prvi vani’

(FIFO), pa kada se dostigne alocirani prostor sledeći fajlovi koji se upute u *Recycle Bin* trajno će izbrisate prve fajlove u tom *Recycle Bin*-u.

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

PITANJA ZA PONAVLJANJE

1. Koje su tri oblasti kreirane u FAT fajl sistemu poznate kao ‘Sistemska oblast’?
2. Koliko je velika svaka alokaciona jedinica?
3. Koja su četiri moguća entrija u FAT tabeli?
4. Ako memorišemo fajl od 1000 B, a alokacione jedinice sistema su od 4 sektora, šta se događa sa fajlom kada se memoriše i šta je preostalo što može biti od dokazne vrednosti?
5. Koja se tri termina upotrebljavaju za nekorišćene delove alokacionih jedinica kada je fajl memorisan?
6. Kada kreiramo direktorijum, šta se kreira na disku da to potvrdi?
7. Šta znače oznake ‘.’ i ‘..’?
8. Kada se kaže da je neki fajl fragmentisan?
9. Koji proces korisnik treba da primeni da sistem učini mnogo efikasnijim?
10. Kakav efekat može imati proces defragmentacije na forenzičko ispitivanje?
11. Opišite tri načina brisanja fajlova i unosa u *Recycle Bin*?
12. Navedite dva načina na koja se fajlovi brišu direktno bez unosa u Recycle Bin?
13. Koja se dva dela FAT fajl sistema menjaju kada se neki fajl obriše?
14. Kada je neki fajl obrisan, navedite šta se menja u direktorijumu entrija?
15. Kada je neki fajl obrisan šta se menja u FAT tabeli?
16. Ako je fajl u FAT fajl sistemu fragmentisan, koliko je verovatno da se delovi fajla mogu oporaviti?
17. Šta podrazumevate pod terminom *Lazy Write*?
18. Koje forenzičke implikacije *Lazy Write* može imati?

19. Šta podrazumevate pod terminom *Transaction Logging*?
20. Šta je namena *Transaction Logging*?
21. Šta je $MFT?
22. Šta možete očekivati da nađete u $MFTMirr?
23. Šta sadrži fajl $Volume?
24. Koja je namena $Bitmap i koji drugi fajl kooperira kod snimanja/praćenja korišćenja diska?
25. Koje dve stvari čine neki MFT *entry*?
26. Koje informacije možete naći u bajtovima 22 i 23 nekog MFT *entry*-a?
27. Identifikujte sledeće atribute iz njihovih identifikatora:
28. 10 00 00 00 30 00 00 00 80 00 00 00
29. Koje se informacije o atributu mogu naći neposredno iza identifikatora atributa i odakle se računaju?
30. Šta se može naći u *Standard Information* i koliko toga ima?
31. Šta sledi iza *Standard Information* što nam može reći nešto o fajlu?
32. Kako su uskladištene informacije u atributu *Filename*?
33. Koliko je velik svaki MFT *entry*?
34. Ako je sve u fajlu uključujući podatke manje od entrija, kako se nazivaju podaci u tom fajlu?
35. Ako je sve u fajlu znatno veće od entrija, šta se u atributu može naći umesto podataka?
36. Kako se zovu informacije uskladištene posle FF FF FF FF markera?
37. Kako radi kompresija fajla u NTFS fajl sistemu?
38. Koja forenzička razmatranja ima forenzičar o kompresiji?
39. Gde u NTFS zapisu možete naći informacije o statusu nekog fajla?
40. Koliko realno informacija može izvući forenzičar neposredno posle brisanja fajla u NTFS fajl sistemu?
41. Ako se fajl izbriše, a podaci su rezidentni, šta se može oporaviti ako MFT entry nije prepisan?

42. Ako pronađemo izbrisani entry za fajl sa nerezidentnim podacima, koliko se podataka može oporaviti i šta koristimo da ih nađemo?
43. Gde se mogu naći fajlovi oji se odnose na Recycle Bin?
44. Kako se naziva Recycle Bin folder u FAT fajl sistemu?
45. Kako se naziva Recycle Bin folder u NTFS fajl sistemu?
46. Šta se smešta u INFO2 fajl NTFS sistema što ukazuje na korisnika koji je izbrisao fajl?
47. INFO2 fajlovi su sačinjeni od hedera i entija za svaki fajl koji je poslat u *Recycl Bin*.
48. Koliko je veliki svaki od njih? Objasnite *Placeholder* 'Dd16.txt'?
49. Navedite detalje nekih informacija koje se mogu naći u entriju od 800 bajta INFO2 fajla?

11 PRIVREMENI I DRUGI FORENZIČKI RELVANTNI FAJLOVI

11.1 Privremeni fajlovi

U procesu forenzičke analize relevantne dokaze mogu sadržavati privremeni (*Temporary*) i drugi brojni fajlovi u fajl sistemu ispitivanog računara. Brojne aplikacije stvaraju privremene fajlove i ostavljaju ih u računaru kada aplikacija završi rad, ili ih brišu kada se aplikacija zatvori.

Microsoft definiše privremeni fajl kao „fajl koji je kreiran da privremeno skladišti informacije da bi se oslobodila memorija za druge namene, ili da radi kao sigurnosna mreža za sprečavanje gubitka podataka kada program izvršava neke funkcije“, [24].

Windows aplikacije, uključujući sam OS, često zahtevaju da privremeno uskladište podatke na čvrstom disku. Ovo je skoro uvek tačno kada se instalira softver, ali se može dogoditi i u drugo vreme. Mnoge aplikacije kreiraju privremene fajlove da pomognu svoje operacije. Ovi fajlovi se skladište u dizajnirani '*Temp*' folder. U nekim slučajevima (ne uvek) ovi fajlovi će imati **.TMP** ekstenziju, koja pretpostvlja da će ih Windows ili aplikacija koja ih je kreirala i izbrisati kada im više ne trebaju, što se međutim uvek ne događa. *Microsoft Office* kreira najviše privremenih fajlova. Aplikacija određuje automatski gde i kada treba da kreira privremeni fajl. Taj fajl treba da postoji samo dok traje sesija *MS Office* aplikacije. U procesu normalnog isključivanja (*shutdown*) privremeni fajl se prvo poveže sa otvorenim radnim fajlom, koji se zatim zatvara i memoriše, kada privremeni fajl treba da bude izbrisan. Međutim, nepropisno isključivanje aplikacije ne briše privremeni fajl i ostavlja ga za potencijalno forenzičko ispitivanje.

Word koristi privremene fajlove u normalnom radu na dva načina:

1. da oslobodi memoriju za drugi rad dok se aplikacija koristi, pomeranjem dela dokumenta na kome se ne radi u privremeni fajl na disku i omogućavajući najbolje korišćenje memorije za druge akcije na dokumentu – manipulaciju i uređivanje teksta itd.

2. da obezbedi neku vrstu zaštite integriteta podataka od grešaka u memorisanju fajlova, ili od pada napajanja dok je fajl otvoren.

MS Office tipično kreira sledeće privremene fajlove:

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

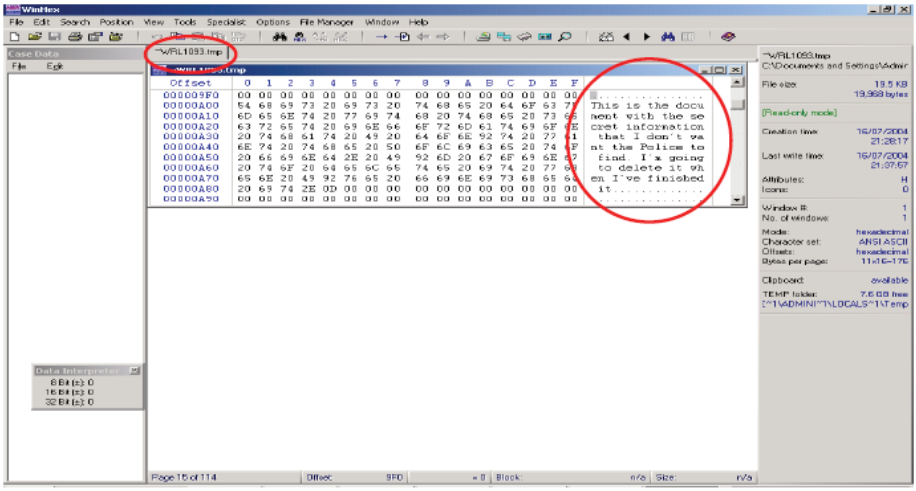
gde xxxx predstavlja broj sekvence.

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

```
C:\Documents and Settings\<username>\Local Settings\Temp

C:\Documents and Settings\<username>|Application Data\Microsoft\Word
```

Pretraživanjem sa *serch* funkcijom, koristeći **.TMP** ekstenziju kao ključnu reč, treba da se otkriju i druge lokacije. Na slici 11.1 je dat primer privremenih *clipboard* fajlova *~wrlxxxx.tmp* posmatran u forenzičkom alatu. Kako se može videti, zista sadrži potencijalne dokazujuće podatke.

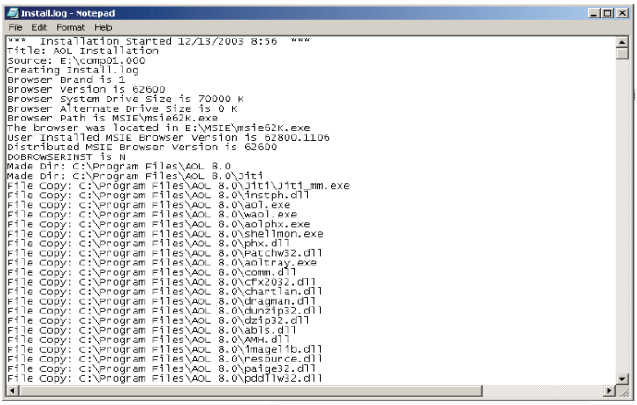


Slika 11.1 Interpretacija privremenih fajlova ~wrlxxxx.tmp u forenzičkom alatu

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

11.2 Log fajlovi

Log fajlovi mogu biti koristan izvor podataka o događajima na računaru. Brojne aplikacije kreiraju svoje log fajlove, bilo kao deo procesa instalacije, ili pri prvom aktiviranju. *Windows XP* pri instalaciji kreira negde oko 135 log fajlova, ili osnovnih tekst fajlova koji rade kao log fajlovi. Log fajlovi mogu sadržavati vrlo relevantne podatke, kao što su kada je aplikacija prvi put instalirana, kada je poslednji put pokrenuta, kako je podešena i koju je akciju imala u toku poslednjeg aktiviranja. Sami log fajlovi imaju svoj vremenski pečat, kao svaki drugi fajl kojeg OS procesira, [24].



Slika 11.2 Instalacioni log fajl AOL klijenta

Na slici 11.2. prikzan je instalacioni log fajl za nekog AOL (*America on Line*) klijenta. Kako se vidi fajl sadrži mnogo potecijalno korisnih informacija. Međutim, nije uvek jasno na koje se aplikacije, ili procese ovi log fajlovi odnose. Ponekad je potrebno da forenzičar pretražuje ceo logički disk, koristeći ***.log** izraz za pronalaženje svih relevantnih tipova fajlova, a zatim manuelno pretražuje svaki od njih, da odredi njegovu relevantnost. Lokacije svih log fajlova biće takođe registrovane u **Registru** i nekada treba razmotriti opciju pretraživanje celog **Registra**. Treba imati na umu da korisnik može promeniti lokaciju log datoteka izvan podrazumevane lokacije.

11.3 Print Spooler fajlovi

Primarna komponenta u *Windows* okruženju za printovanje (štampanje) je *print spooler* (Simultaneous Peripheral Operations On-Line), koji u privremenom fajlu čuva stranicu koju je neka aplikacija poslala na štampač za štampanje. Aplikacija i printer simultano mogu upisivati/čitati fajlove u *print spooler*-u, što ubrzava proces štampanja, omogućva formiranje redosleda za štampanje i povratak kontrole aplikacije pre završetka štampanja, [24].

Print spooler je u stvari jedan izvršni fajl koji upravlja celim procesom štampanja. *Print spooler* se podiže u toku podiznja (*start-up*) sistema i ostaje aktivan dok se sistem ne isključi. U Windows NT i XP *print spooler* kreira **.SPL** fajlove kada operacija štampanja počinje. U Windows 9x **.SPL** fajl daje ime kreiranom privremenom fajlu, gde se sadrži **EMF** (*Enhanced Metafile*). Podaci koji se odnose na štampanje sadržani su u **.SPL** fajlu. Generalno u Windows

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

11.4 Fajlovi linkova

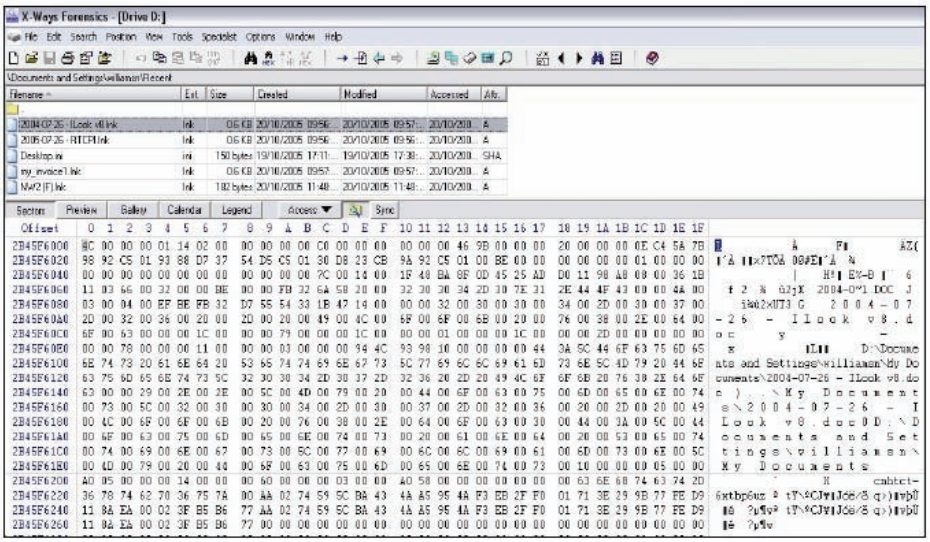
Fajlovi linkova ili prečica (*shortcuts*) mogu obezbediti takođe korisne informacije za forenzičko ispitivanje. Ovi fajlovi su jednostavno usmerivači, ili *poštanski signali* do ciljnih fajlova, aplikacija, direktorijuma i sistemskih objekata izvan fajl sistema, kao što su printeri i spoljni diskovi. Obezbeđuju korisnicima brzi pristup uobičajeno korišćenjim fajlovima i aplikacijama itd.

Uobičajena lokacija fajlova za linkovanje su Windows Desktop, Windows Recent, Windows Start Menu, Windows Sent to i Internet Explorer Favorites folderi. Ekstenzija za ove fajlove je **.LNK.**

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

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

U Windows 2000 i XP sistemima lokacija ovih fajlova je podrazumevana i nalazi se u **C:\Documents and Settings\<username>** i u nekom od sledećih sub-foldera: **\desktop, \Favourites, \My Recent Documents, \SendTo, \Start Menu**. Svaki od ovih foldera ima kreiran svoj vremenski pečat, a svaki fajl u njemu svoj puni *vreme&datum* pečat i punu putanju fajla na koga se link odnosi. Međutim, ovo nije toliko očigledno i zahteva dekodiranje, kada se idntifikuje relevantan ofset bajta. Na slici 11.3. je prikazn primer **.LNK** fajla, a relevantni ulazi podataka su naglašeni, [24].



Slika 11.3 Primer **.LNK** fajla u forenzičkom alatu

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

11.5 Tipovi i potpisi fajlova

Postoji više tipova fajlova u opticaju, a generalno se mogu identifikovati sa ekstenzijom. Tipično se ekstenzija izražava sa *tačkom* koju slede *2-4 karaktera*. Uzmimo za primer sledeća tri imena fajla, [7]:

1. proces

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

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

Uobičajeni tipovi fajlova i ekstenzija u *Microsoft* fajl sistemima i drugim platformama prikazni su u tabeli 11.1a. *Microsoft Office* set programa je verovatno najčešće upotrebljavan na ispitivanim računarima. Zbog toga forenzičari moraju poznavati dobro ove tipove dokumenata. U tabeli 11.1b. prikazani su neki drugi uobičajeni tipovi fajlova i ekstenzija, uključujući komprimovane fajlove, izvršne fajlove, sistemske i log fajlove i neke druge koji često mogu obezbediti dokazujuće podatke, [24].

Tabela 11.1 Uobičajeni tipovi fajlova i ekstenzija

a.

Common Microsoft Files	
File	File extension
MS Office Word	.doc .dot
MS Office Excel	.xls .xlt
MS Office PowerPoint	.ppt; .pps .pot
MS Office Access	.mdb; .adp; .mda .ade
MS Office Outlook	.pst .ost
MS Outlook Express	.dbx .wab
MS Internet Explorer	.htm .html

b.

Other Common File Types & Extensions	
File	File Extension
Compressed Files	.zip; .rar .Z; .gz
DOS executables	.com; .bat .exe
Initialisation files	.ini
System files	.sys
Log files	.log
Help files	.hlp
Text files	.txt; .wri; .rtf
Adobe files	.pdf; .pbd

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

Dobar deo rada forenzičara digitalnih podataka odnosi se na grafičke i druge multimedijalne fajlove, kao što su audio i video fajlovi koji se uobičajeno koriste u razmeni i posedovanju slika dečije pornografije. Ovi formati fajlova i ekstenzija prikazani su u tabeli 11.2.a i b.

Tabela 11.2 Uobičajeni tipovi grafičkih (a) i video (b) fajlova

a.

Common Graphics File Types	
File	File Extension
Joint photographic Experts Group	.jpg; .jif; .jpeg
Graphics Interchange Format	.gif, .giff
Windows Bitmap	.bmp
Portable Network Graphics	.png
Tagged Image File Format	.tif; .tiff

b.

Common Video & Audio File Types	
File	File Extension
Audio Video Interleaved	.avi
Apple QuickTime	.mov
Visual Image Directory	.vid
Moving picture Experts Group	.mpg .mpeg

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

Poslednja grupa fajlova je ona gde se koristi šifrovanje za skrivanje podataka od onih koji ne treba da ih vide, a među njima su najčešće upravo forenzički digitalni dokazi. Uobičajeni šifrovani fajlovi su prikazani u tabeli 11.3.

Tabela 11.3 Ekstenzije uobičajenih šifrovanih fajlova

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

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

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

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

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

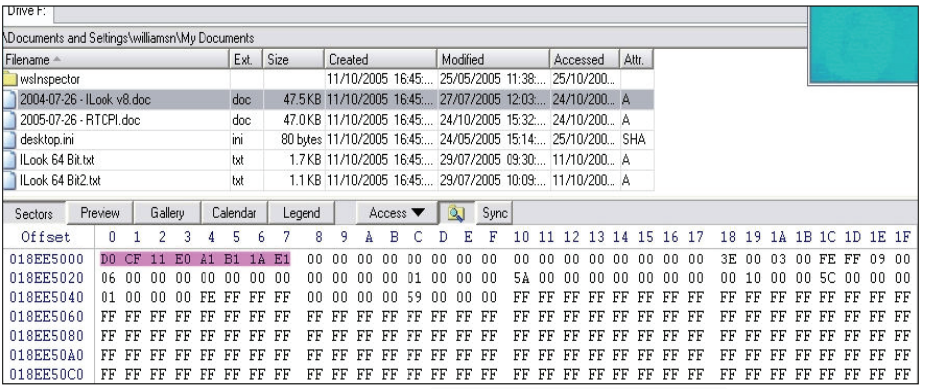
- identifikuju tip fajla,
- identifikuju putanju do pridružene asocijacije,
- vide ako postoji specijalne komande koje moraju biti prisutne da bi se fajl otvorio,
- traže informacije o rukovanju sa ugrađenim objektima,
- ispituju fajl za informaciju o ikoni i
- proveravaju da li se, ili ne može koristiti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

Sadržaji ovog registra su dinamički i menjaju se zavisno od broja instalirnih aplikacija.

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

11.6 Potpisi fajlova

U procesu ispitivanja fajl sistema forenzičar treba da razmatra i potpise fajlova. Pri tome ne treba mešati ekstenzije i potpise fajlova. U slučaju nekog tipa fajlova, svi fajlovi imaju jedan poznat i prepoznatljiv ***heder***, koji nije vidljiv u normalnom režimu rada i generalno za gledanje fajlova treba koristiti ***hex*** editor. Ovaj potpis fajlova je definitivan indikator tipa i sadržaja fajla. U slici 11.4 prikazan je uobičajen potpis fajlova za sve MS Office fajlove: D0 CF 11 E0 A1 B1 1A E1, [24].



Slika 11.4 Uobičajen potpis MS Office fajlova

Potpis fajla pojavljuje se na samom početku fajla, ali se ne vidi kod normalnog otvaranja *word* dokumenta. Poznavanje potpisa fajla je važno za forenzičara, jer maliciozni korisnik može izmenom ekstenzije fajla isti sakriti, a forenzičar preko potpisa fajla može otkriti pravi tip i sadržaj fajla. Tako u pred-ispitivanju forenzičar može otkriti samo **.doc** fajlove, među kojima se, međutim, mogu kriti brojni **.jpeg** fajlovi kompromitujućih slika. *Windows* kategorizuje fajlove prema njihovim ekstenzijama, pretpostavlja da su sve *word* dokumenti, daje im korektnu ikonu i pokušava otvoriti sa MS Word-om. U ovom slučaju svi **.jpeg** fajlovi neće se moći otvoriti. Takođe, ako se pretražuju fajlovi u potrazi za **.jpeg**, rezultat će biti negativan. Sledeća ilustracija u slici 11.5 pokazuje kako *Windows* radi u ovakvim situcijma i kako prikazuje rezultate takvih akcija. Prikazana su četiri uobičajena tipa fajlova koji se mogu naći na računaru. Windows je pripisao korektne ikone svakom tipu fajla i koristi korektne aplikacije da ih otvori. Otvaranje će biti uspešno jer su ekstenzije tačne.



Slika 11.5 Tačan Windows prikaz potpisa fajlova

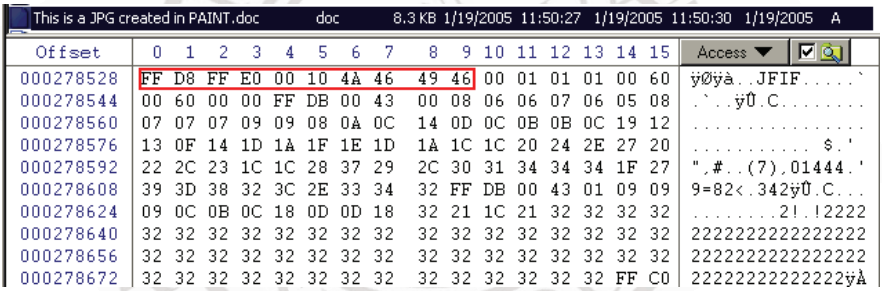
U sledećoj ilustraciji (slika 11.6) svi fajlovi su promenili ekstenzije u **.doc.** Ime, veličina i sadržaj fajla ostaju isti, a *Windows* pogrešno interpretira fajlove i pripisuje svakom ikonu word dokumenta i menja detalje tipa fajla, pošto ih tako vidi i pokušava ih otvarati sa *Word*-om.



Slika 11.6 Pogrešan Windows prikaz potpisa fajlova

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

U sledećoj ilustraciji na slici 11.7 prikazana je **.jpeg** slika sa **.doc** ekstenzijom. Međutim, potpis fajla govori nešto drugo: FF D8 FF E0 xx xx 4A 46 49 46 00 je jedinstven potpis za sve **.jpeg** fajlove.



Slika 11.7 Prikaz **.jpeg** slika sa **.doc** ekstenzijom u hex editoru

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

Uobičajeni potpisi fajlova dati su u tabeli 11.4, gde je prikazan jedan ekstrakt iz web resursa informacija hedera sadržanih u fajlovima.

Tabela 11.4 Uobičajeni potpisi fajlova

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

Postoje brojni izvori koji se mogu koristiti za istraživanje cele oblasti tipova, ekstenzija i potpisa fajlova[11].

11.7 Forenzička analiza tragova korišćenja Interneta

Istraživanje tragova pristupa Internetu na osumnjičenom računaru, samo je uvod u kompleksnu forenzičku analizu napada sa Inteneta. Konekcije računara i računarskih mreža na Internet stalno se usavršavaju, ali su u upotrebi i obični modemi preko telefonske linije, zatim ADSL i širokopojasni pristupi Internetu. Uređaji koji povezuju sisteme na Internet dramatično se menjaju – pored računara, to mogu biti i mobilni telefoni, televizori i brojni kućni aparati. Savremeni Internet u delovima sekunde može povezati digitalni svet preko brojnih i različitih medija kao što su servisi: (***World Wide Web***) web pretraživači, čet, *peer-to-peer* i novinske grupe. Praksa je pokazala

[11] http://www.garykessler.net/library/file_sigs.html
http://filext.com/
http://www.file-ext.com/
http://www.stack.com/file/extension/; http://www.fileinfo.net/

da u većini slučajeva kompjuterskog kriminala učestvuje u nekom obliku neki aspekt Interneta. Zato forenzičar mora razumeti kako radi Internet i kakve tragove ostavlja u računaru rad na Internetu, [25].

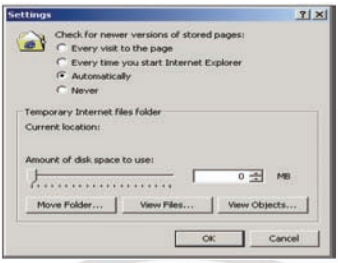
11.7.1 Privremeni Internet fajlovi

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

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

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

Ako forenzičar otkrije da je keš vrednost podešena na 0%, treba postaviti pitanje zašto je to tako (slika 11.8). Prvi rezon je da korisnik želi da računar ništa ne skladišti u keš prostor i da nešto želi sakriti. Promena vrednosti keša je jednostavna i direktna operacija.

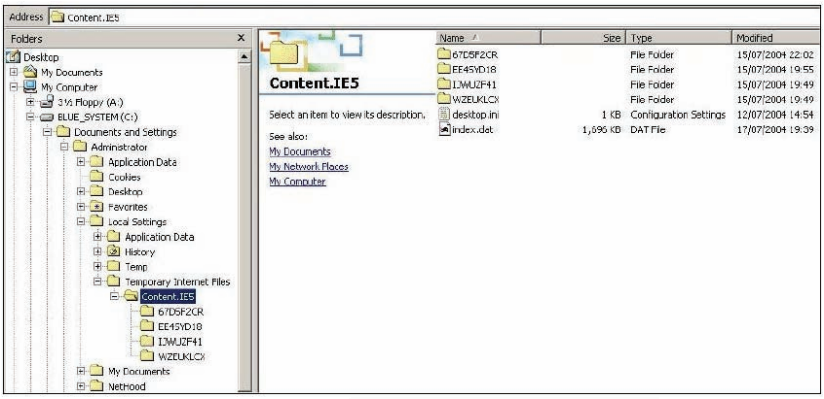


Slika 11.8 Korisničko podešavanje Internet keša na 0MB

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

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

Struktura ovih fajlova prikazana je u sledećem prozoru (slika 11.9). U folderu **Content.IE5** nalazi se neki broj slučajno imenovanih pod-folfdera sa imenima dužine 8 karaktera koje je sistem alocirao. Unutar ovog foldera je i fajl **INDEX.DAT,** koji kontroliše Internet keš i od vitalnog je značaja za forenzičare u istrazi aktivnosti korisnika na Intrnetu. Treba da imaju najmanje 4 ovakva foldera.



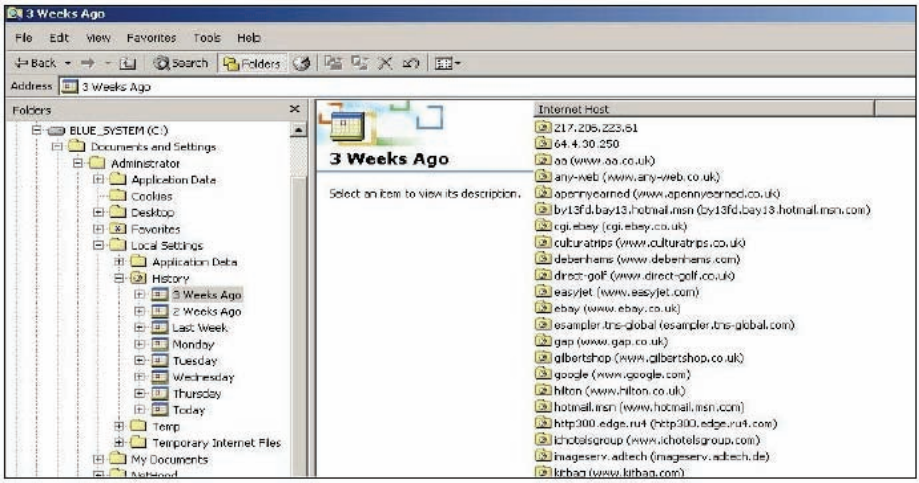
Slika 11.9 Struktura Internet keš fajlova u **Content.IE5** folderu

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

11.7.2 Istorija aktivnosti na Internetu

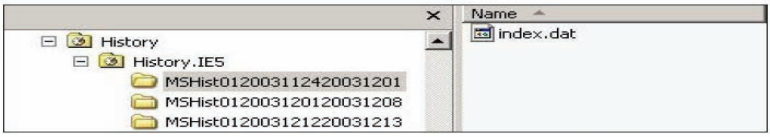
Istorija aktivnosti na Internetu (*Internet History*) obezbeđuje evidenciju lokacija koje je korsnik posetio sa svog računara u toku pretraživanja Interneta. Ova evidencija uključuje imena posećenih web lokcija, detalje o izvornim serverima, FTP sajtove, e-mail baziran na web-u i posećene novinske grupe,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

Istorija Interneta postoji da omogući korisniku da ide na prethodno posećene web lokacije sa liste koja se pojavljuje u pretraživaču. Kao kod privremenih Internet fajlova, postoji struktura foldera da čuva ove informacije. Ove lokacije podrazumevano su tačno na istom mestu kao za keš fajlove, ali ih korinik može pomeriti. U sledećem primeru prikazana je struktura foldera Internet History u Windows XP mašini, (slika 11.10), [24].



Slika 11.10 Struktura foldera Internet History u Windows XP mašini

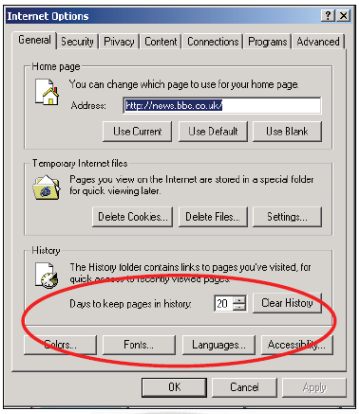
Vidi se da sistem deli foldere na dnevne i nedeljne istorije. Međutim, format ovih foldera kontroliše se sa **DESKTOP.INI** fajlom koji se nalazi u folderu. U stvari, forenzički alat vidi nešto drugačije ovu strukturu, (slika 11.11).



Slika 11.11 Struktura foldera Internet History u forenzičkom alatu

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

Internet History takođe ima opciju za korisničko podešavnje. Na sledećem panelu korisnik može lako promeniti broj dana koj istorija treba da čuva, (slika 11.12.).

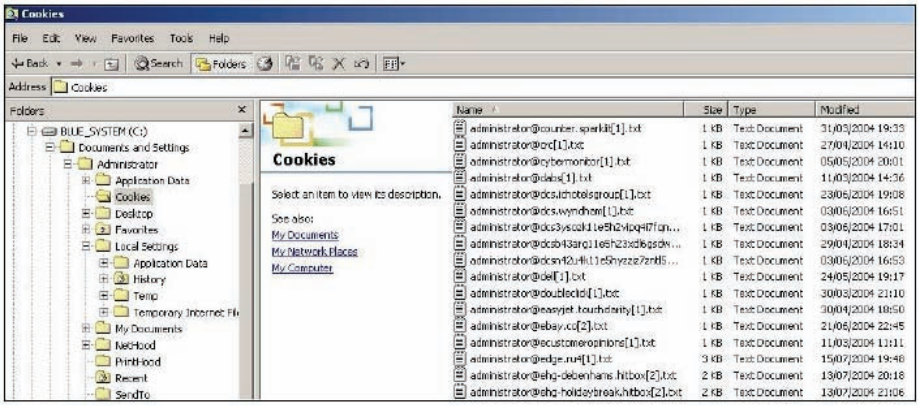


Slika 11.12 Opciju za korisničko podešavnje Internet History

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

11.8 Kolačići (*Cookies*)

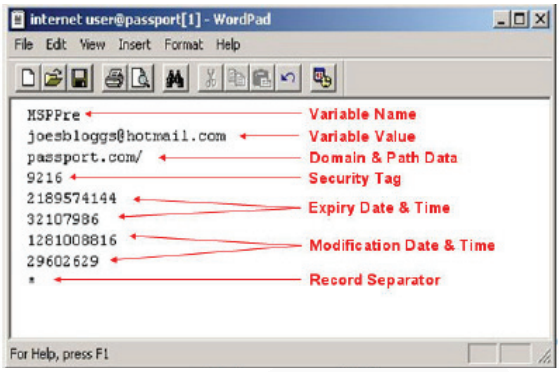
Kolačići su još jedan artefakt Internet aktivnosti koje korisnik malo, ili nikako kontroliše. Ovo su mali tekst fajlovi deponovani na čvrstom disku kao rezultat Internet aktivnosti i poseta web lokacijama. Kolačići se kreiraju kada pretraživač kontaktira web stranicu koja podržava funkcije kolačića, (slika 11.13).



Slika 11.13 Kolačići kao forenzički indikator Internet aktivnosti

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

Kolačići se mogu lako koristiti za čuvanje detalja o posećenoj lokaciji – imena, adresa i čak detalja o kreditinim karticama, za novu posetu toj lokaciji, (slika 11.14). Generalno, kolačići se koriste za identifikovanje korisnika koji je ranije posetio određenu lokaciju i može se koristiti za prikupljanje podataka o frekvenciji poseta, posmatranim informacijama i obezbeđenim materijalima. Sadržaj kolačića pojavljuje se na levoj strani prozora, a različiti delovi su dalje rasčlanjeni.



Slika 11.14 Primer podataka koji se mogu nalaziti u kolačićima

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

Osnovni forenzički alati mogu čitati sva tri tipa Internet fajlova na računaru, ali je najbolji poznati alat za analizu Internet istorije zove se ***NetAnalysis*** (*Crag Wilson*, www.digital-detective.co.uk). Ovaj alat sve tri oblasti prikazuje zajedno u tabelarnoj formi, omogućavajući analizu vremenske linije aktivnosti na Internetu i ima funkcije filtriranja i izveštavanja rezultata, [24].

11.9 Favorizovane lokacije

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

Listing favorizovanih lokacija može biti dobar izvor informacija za forenzičara: koje lokacije osumnjični regularno posećuje, vremena i datume koje fajlovi sadrže na čvrstom disku mogu biti indikatori aktivnosti i potencijalnih poseta.

Međutim, forenzičar mora znati da ulaze na *favorites* listu unosi i sistem, a ne samo korisnik, što mora uzeti u razmatranje. Iako se na ovu listu može staviti sve što korisnik želi, najvažnija informacija su URL koji indiciraju lokaciju na koju se favorizovana adresa odnosi.

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

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

11.10 Direktno umrežavanje (*peer-to-peer*)

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

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

(www.sandersonforensics.co.uk), koji je specijalno pisan za ispitivanje *FastTrack* protokola i koji obezbeđuje dešifravane termine za pretraživanje i druge podatke.

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

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

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

11.11 Ostali transferi fajlova

Forenzičar mora biti svestan da mnoge aplikacije za transfer fajlova imaju log fajlove koji omogućavaju da se otkrije kako je aplikacija korišćena. Verovatno najbolji primer su FTP klijenti koji se koriste za transfer web baziranog materijala na Iternet hostove za web lokacije.

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

11.12 Tragovi E-mail poruka

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

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

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

Outlook Express koristi **DBX** sistem fajlova. Postoji po jedan **DBX** fajl za svaki deo aplikacija - INBOX, OUTBOX, SENT ITEMS, DELETED ITEMS, DRAFTS itd. Pored toga, kada korisnik kreira sam novi folder, aplikacija kreira novi **DBX** fajl za skladištenje podataka sadržanih u folderu. **DBX** fajlovi nisu šifrovani, a sadržaj se može pretraživati na disku. Međutim, forenzičar mora znati da kod ovog tipa e-pošte, postoji mnogo podešavanja koja mogu uticati na dokaze, na primer, komprimovani fajlovi na izlazu aplikacija, [7], [24].

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

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

E-pošta bazirana na Internetu normalno se istražuje u privremenim Internet fajlovima, uz pomoć forenzičkog alata koji omogućava njihovu ekstrakciju, otvaranje i čitanje. Na osnovu ključne reči pronalazi se sadržaj e-poruka, bilo baziranih u aplikacijama, ili Internetu, a ostatak poruka leži u nealociranim prostorima diska. Format materijala treba da ukaže da se radi o porukama aplikacija za e-poštu, Veći deo strukture e-pošte, posebno informacija hedera, potpuno je jedinstven za e-poštu.

E-*mail heder* može biti neprocenjiv izvor informacija za forenzičara u otkrivanju izvora primljene poruke, ili dokazivanja da je neko odgovoran za neku akciju, ili aktivnost. Primer hedera poruke e-pošte na sledećoj ilustraciji pokazuje šta se sve može naći u njemu (slika 11.15).

```
Return-path: <paul_davis160@yahoo.co.uk>
Envelope-to: donjohnson160@zoom.co.uk
Delivery-date: Sun, 12 Sep 2004 21:53:46 +0100
Received: from web25207.mail.ukl.yahoo.com ([217.12.10.67])
        by store1.mail.uk.easynet.net with smtp (Exim 4.32)
        id 1C6bM2-0003TC-OF
        for donjohnson160@zoom.co.uk; Sun, 12 Sep 2004 21:53:46 +0100
Message-ID: <20040912205330.41893.qmail@web25207.mail.ukl.yahoo.com>
Received: from [217.40.25.5] by web25207.mail.ukl.yahoo.com via HTTP; Sun, 12 Sep 2004 21:53:30 BST
Date: Sun, 12 Sep 2004 21:53:30 +0100 (BST)
From: =?iso-8859-1?q?Paul=20Davis?= <paul_davis160@yahoo.co.uk>
Subject: Test Message 5
To: Don Johnson <donjohnson160@zoom.co.uk>
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="0-1845740439-1095022410=:39998"
Content-Transfer-Encoding: 8bit


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

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

Slika 11.15 Heder e-pošte

Hederi e-pošte najbolje se razumeju ako se čitaju odozdo na gore. Na dnu se vidi stvarna poruka koja je poslat–*test message*. Zatim se nalazi neka informacija o korišćenom sistemu kodiranja, koji se koristi u savremenim aplikacijama e-pošte da se usklade sa starijim sistemima i protokolima koji su još u upotrebi. Drugim rečima, poslata e-pošta može koristiti samo određeni opseg, ali je većina poruka veća od tog opsega, što se posebno odnosi na

priloge pošte (*attachments*). Zato se poruke moraju *kodiranjem* redukovati da bi bile poslate, a zatim na prijemnoj strani *dekodiranjem* vratiti u normalni format. Da bi se shvatio način na koji je heder struktuiran treba gledati u sledeće linije:

To: lice kome je poruka poslata,

Subject: efektivni izraz o čemu poruka govori,

From: *treba* da bude lice koje je poslalo poruku.

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

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

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

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

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

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

Forenzičar treba da objasni šta je IP adresa u hederu, što je moguće jasnije i kraće. IP adresa je jedinstven identitet nekoga ko je koristio Internet. Kada se korisnik poveže na Internet, ISP koji obezbeđuje tu vezu daje korisniku neku IP adresu za vreme rada na Internetu. Ta IP adresa je jedinstvena za tog korisnika za to vreme boravka na Internetu – slično telefonskom broju. IP adresa se piše u decimalnom zapisu sa tačkama, na primer: **123.45.230.16**.

Postoje različiti tipovi mreža, međutim bilo na Intranetu, ili na Internetu, korisnik mora imati IP adresu da bi bio prepoznat i povezan na mrežu. Trernutno se koristi IP verzija 4. Svaki segment IP adrese je neki bajt, drugim rečima IP adresa ima 256 mogućih vrednosti – 0 do 255. Dakle ne može se videti IP adresa sa brojem većim od 255. IP adrese se alociraju nekoj organizaciji koja generalno ima blok IP adresa koje konsekutivno mogu pripisati svojim klijentima. Tako u gornjem primeru, ISP je alocirao IP adrese u opsegu 123.45.230.0 do 123.45.230.255 – 256 mogućih adresa. Ako forenzičar želi da identifikuje ko je koristio IP adresu 123.45.230.16, mogu se koristiti brojni alati raspoloživi na Internetu (www.samspade.org ili www.centralops .net) da uzbace tu IP adresu i mogu dati informaciju o tome ko je administrirao tu IP adresu. Dalje treba kontaktirati tu organizaciju i tražiti koji korisnik je koristio tu IP adresuu u specifično vreme i datum. U ovoj tački, vreme, datum i vremenska zona dolaze u prvi plan, pa ako se pogrešno očitaju iz analiziranih podataka, IP adresa se može alocirati drugom licu i odvesti istragu u pogrešnom smeru.

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

11.13 Servisi za četovanje preko Interneta

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

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

drugi korisnik mogao logovati na mašinu osumnjičenog, ili je najčešće dato lažno ime.

11.13.1 Servis novinske grupe

Novinskoj grupi korisnik može pristupiti preko *Google*-a i sličnih pretraživača sa *Internet Explorerom* i drugim aplikacijama za pretraživanje. Dokazi o korišćenju ovog servisa nalazi se u privremenim Internet fajlovima (Internet kešu). Drugi način pristupa ovom servisu je korišćenjem neke od brojnih aplikacija za čitanje vesti, kao što je **Forte Agent** i **Outlook Express**. Svaka od ovih aplikacija rade na različit način, ali sve donose poruke grupa u aplikaciju, koje su sada lokalne za mašinu. Ovo olakšava analizu, ali podaci za analizu mogu biti preobimni, pošto neki korisnici mogu biti učesnici više novinskih grupa.

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

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

11.13.2 AOL servis

Iako je ovaj servis vezan pretežno za severnu Ameriku, sve se više širi u Engleskoj i šire. AOL v. 8.0 ili 9.0 korisnik treba da instalira aplikaciju – relevantne osnovne fajlove podešene za AOL i zatim izvrši zamenu relevantnih fajlova. Svaki AOL korisnik dobije ime glavnog ekrana (*master screen name)* koje mu omogućava da nameni daljih 6 imena ekrana, možda za članove familije i rođake. Svako ime ekrana dobija svoj skup fajlova. Na samom AOL forenzičar može oporaviti razne stvari koje se odnose na

korisnika – listu favorizovanih, listu najčešćih kontakata, imena ekrana, njihove knjige adresa, uskladištene i pročitane e-pošte, njihove menadžere daunlodovanja, otkucana URL istorija, klijentski logovi i njihove novinske grupe koje šalju poruke u AOL grupe.

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

11.14 Analiza izvršnih fajlova, *rutkitova*, *zadnjih vrata* i *snifera*

Izvršni fajlovi (*executable*) predstavljaju fajlove koji se mogu pokretati kao programi i obično se završavaju sa ekstenzijom **.exe**. Izvršni fajlovi predstavljaju specijalni slučaj digitalne forenzičke analize fajl sistema. U najvećem delu, izvršni fajlovi slede poznatu i dokumentovanu strukturu, zato što ih treba aktivirati na različitim verzijama Windows OS. Međutim, autori malicioznih programa otkrili su način da maskiraju strukturu da bi otežali, ili onemogućili analizu. Razumevanjem strukture i formata ovih fajlova i kako oni treba da izgledaju, forenzičari mogu razlikovati legitimne fajlove i izolovati sumnjive fajlove u Windows OS. Korišćenjem specifičnih tehnika i sa poznavanjem strukture i formata izvršnih fajlova, forenzičar može odrediti koji su fajlovi legitimni i koje artefakte treba pripisati određenom delu malicioznog koda, [9].

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

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

- sprečiti logovanje aktivnosti,
- uspostaviti zadnja vrata za ponovljeni ulaz,
- sakriti ili ukloniti dokaz o inicijalnom ulazu,

- sakriti specifične sadržaje fajlova,
- sakriti fajlove i direktorijume,
- sakupiti informacije, npr., korisnička imena i pasvorde.

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

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

Detekcija prisustva rutkitova: Ulazak napadača u računarski sistem može ostaviti dokazni trag u različitim porukama log fajla. Većina rutkitova uključuje uslužne alate za automatsko uklanjanje svake sumnjive ili inkriminišuće poruke iz log fajlova. Jedan od uobičajenih indikatora prisustva rutkita u sistemu je kada jedan ili više ključnih uslužnih alata koji su ranije radili bez otkaza, odjednom počne da se ponaša nekonzistentno zato što je napadač zamenio te alate sa verzijama rutkitova dizajniranim da sakriju svoje maliciozne aktivnosti, a koje se razlikuju od standardnih alata. Na primer, komandna linija prebaci na **netstat** ili **ps**, koji organizacija koristi bez problema svaki dan, može početi da vraća pogrešne poruke. Detekcija rutkitova je vitalna iako može biti najteži zadatak za sistem administratora. Rutkitovi spadaju u kategoriju malicioznih kodova tipa virusa, crva i trojanaca i detektuju se manje više na isti način. U stvari, većina rutkitova sadrži

komponentu zadnjih vrata trojanca za obezbeđivanje ulaza kasnije. Sofisticiran haker neće ostaviti nikakav trag koji se može otkriti forenzičkim alatima. Drugi mogu ostaviti tragove koje forenzičar može otkriti, ali samo ako je familijaran sa OS i mrežom. Sa povećanjem kapaciteta HD i kompleksnosti OS, traženje dokaza u hiljadama fajlova o prisustvu rutkitova može ličiti na traženje igle u plastu sena. Pored toga, instalacija rutkitova često falsifikuje vremenski pečat i informaciju o veličini fajla, tako da sprečava vizuelnu kontrolu integriteta od strane sistem administratora sa Unix/Linux **l**s komandom.

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

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

Zastavice (*flags*) koje se koristi u Unix/Linux komandama *stringova* dati su u tabeli 11.5.

Tabela 11.5 Zastavice (*flags*) koje se koriste u Unix/Linux komandnim linijama

Zastavica	Funkcije zastavice (*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

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

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

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

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

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

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

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

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

- **Fport.exe**: jedini Windows alat (*Foundstone Inc.*), koji izveštava o svim otvorenim TCP/IP i UDP portovima, ali ih i prati natrag da vlasnika aplikacije, aktivnih procesa sa ID, imenom i putanjom procesa *(www.foundstone.com*).
- **Superscan**: moćan skener TCP portova, uređaj za pingovanje i detektor imena hostova (*Foundstone Inc.*), ekstremno brz raznovrstan.

- **Nmap**: besplatan mrežni 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. (www.insecure.org/nmap).
- **Listdlls.exe**: windows besplatan pomoćni alat (autor *Mark Russinovich*) koji prikazuje punu putanju modula koji se učitava (www.sysinternals.com).

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

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

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

Detekcija i odbrana od mrežnih *snifera:* Skener (*snifer*) mrežnih paketa je uslužni alat koji monitoriše i loguje mrežne aktivnosti u fajl, praćenjem

saobraćaja, ali bez ikakve modifikacije mrežnih paketa. Ranije su to bili hardverski uređaji fizički spojeni na mrežu, a danas su softverski. Hakeri i krakeri ih koriste za hvatanje korisničkih imena i pasvorda koji se prenose kroz mrežu nezaštićeno, npr., u otvorenom tekstu ili čistom ASCII formatu gde se mogu čitati u *Notepad*-u. Takođe, gotovo svaki rutkit uključuje uslužni alat za praćenje mrežnog saobraćaja. Jedna uznemirujuće moćan aspekt *snifera* paketa je njihova sposobnost da postave host mašinu u *promiskuitetan mod* rada, u kojem mašina prima ne samo podatke usmerene na nju, nego i sav saobraćaj podataka u fizički spojenoj lokalnoj mreži, što sniferu daje ulogu špijunskog alata, pošto svaki interfejs u ovom modu sluša ceo mrežni saobraćaj.

Detekcija snifera je zahtevan, ali ne i nemoguć posao. Pod Unix i Linux OS, komanda **ifconfig** daje administratoru (superkorisniku) privilegiju da odredi koji uređaj radi u *promiskuitetnom* modu, što je indikator korišćenja snifera u mreži. Za proveru interfejsa pomoću ovog alata treba u RUN-u otkucati **ifconfig** i tražiti string PROMISC. Ako je ovaj string prisutan, interfejs je u *promiskuitetnom* modu. Za otkrivanje odgovornog procesa treba koristiti ugrađen alat kao što je **ps** pomoćni alat za identifikaciju procesa. Za Windows sisteme može se koristiti besplatan softverski alat komandne linije **PromiscDetect** za otkrivanje mrežnih adaptera u *promiskuitetnom* modu, koji se može daunlodovati sa www.ntsecurity.nu/toolbox/promiscdetect/, a radi sa Windows NT 4.0, 2000 i XP OS.

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

REZIME

U procesu forenzičke analize relevantne dokaze mogu sadržavati *Temporary* fajlovi u fajl sistemu ispitivanog računara, koje stvaraju brojne aplikacije, posebno kada se instalira softver. Ostaju u računaru kada aplikacija završi rad, ili se brišu kada se aplikacija zatvori. U nekim slučajevima (ne uvek) ovi fajlovi će imati **.TMP** ekstenziju, što znači da će ih Windows ili aplikacija koja ih je kreirala izbrisati kada im više ne trebaju. To se međutim uvek ne događa. *Microsoft Office* kreira najviše privremenih fajlova, sa tipičnom oznakom, npr., **~wrf0000.tmp-***Word* (podrazumevano). Postoje velike šanse da forenzičar ispita ove fajlove i oporavi vitalne dokazujuće podatke. Mogu biti uskladišteni u brojnim i različitim lokacijama, a najčešće u:

- **C:\Documents and Settings\<username>\Local Settings\Temp**
- **C:\Documents and Settings\<username>|Application Data\Microsoft\Word**

Log fajlovi mogu biti koristan izvor podataka o događajima na računaru, npr., kada je aplikacija prvi put instalirana, ili poslednji put pokrenuta, kako je podešena i koju je akciju imala u toku poslednjeg aktiviranja. Brojne aplikacije kreiraju svoje log fajlove, kao deo procesa instalacije, ili pri prvom aktiviranju. *Windows XP* pri instalaciji kreira negde oko 135 log fajlova, koji imaju svoj vremenski pečat. Kako nije uvek jasno na koje se aplikacije, ili procese ovi log fajlovi odnose, ponekad je potrebno da forenzičar pretražuje ceo logički disk, koristeći ****.log*** izraz za pronalaženje svih relevantnih tipova fajlova, a zatim manuelno pretražuje svaki od njih, da odredi njegovu relevantnost. Lokacije svih log fajlova je u **Registru.**

U Windows OS izvršni fajl *Print spooler* upravlja celim procesom štampanja, podiže se u *startup-u* sistema i ostaje aktivan dok se sistem ne isključi. U Windows NT i XP *print spooler* kreira **.SPL** fajlove kada operacija štampanja počinje. Generalno u Windows okruženju, tip podataka u formatu **EMF** predstavlja kompaktan ulaz podataka koji skladišti izlazni tekst, grafičke podatke i komande za štampanje i ne zavisi od uređaja, ili aplikacija; mogu biti kopirani, ili eksportovani i otvoreni sa specijalnim softverom, ili funkcijama za štampanje drugih aplikacija i dopušta ekstrakciju i gledanje drugih podataka, teksta ili slika. Većina forenzičkih alata može gledati **.SHD** fajlove i **EMF** podatke sadržane u njima. Zajedno sa **.SPL** fajlom nalazi se

kreiran **.SHD** fajl u „senci“, koji sadrži sve informacije, koje *spooler* treba za uspostavljanje štampanja u slučaju da se računar restartuje pre završetka operacije štampanja.

Fajlovi linkova (*shortcuts*) mogu obezbediti takođe korisne informacije za forenzičko ispitivanje, usmeravajući do ciljnih fajlova, aplikacija, direktorijuma i sistemskih objekata izvan fajl sistema, kao što su printeri i spoljni diskovi. Uobičajene lokacija u Windows 2000 i XP sistemima su *Desktop, Recent, Start Menu, Sent to i Internet Explorer Favorites* folderima u C:\Documents and Settings\<username>. Ekstenzija za ove fajlove je **.LNK.** Svaki fajl sadržiu puni *vreme&datum* pečat i punu putanju fajla na koga se link odnosi, što nije toliko očigledno i zahteva dekodiranje, kada se idntifikuje relevantan ofset bajta u forenzičkom alatu. U toku forenzičkog ispitivanja korisno je pretražiti ove fajlove u alociranim, nealociranim prostorima i *swap* fajlovima. Izbrisane prečice treba još uvek da imaju ulaz u MTF, a mogu se naći i u nealociranim oblastima klastera.

Postoji više tipova fajlova u opticaju, a generalno se mogu identifikovati sa ekstenzijom – *tačkom* koju slede *2-4 karaktera.* Ekstenziju prepoznaju korisnici i OS i pridružuju je određenoj aplikaciji, što uvek nije onako kako se vidi. Forenzičar mora dobro poznavati sve moguće tipove ekstenzija fajlova u ispitivanom računaru. Većinu ovih fajlova kreira sistem, ali su mnogi deo softverskih paketa, a mogu ih kreirati i korisnici. Forenzičar mora imati alate za otvaranje i čitanje ovih fajlova, ili izvlačenje dokazujućih podataka, posebno iz šifrovanih fajlova, gde su najčešće digitalni dokazi. U *Windows* OS ekstenzije fajlova su sadržane u ključu Registra - HKEY_CLASSES_ROOT, koji čuva tragove ekstenzija fajlova i njihovih asocijacija i tragove programa pridruženih tipovima fajlova koji su registrovani u sistemu, a predstavlja direktnu kopiju podataka sadržanih u ključu HKEY_LOCAL_MACHINE\Software\Classes.

U procesu ispitivanja fajl sistema forenzičar treba da razmatra i potpise fajlova i ne treba mešati ekstenzije i potpise fajlova. Svi fajlovi imaju prepoznatljiv *heder*, koji nije vidljiv u normalnom režimu rada i za gledanje fajlova treba koristiti *hex editor*. Ovaj potpis fajlova je definitivan indikator tipa i sadržaja fajla, a za sve MS Office fajlove uobičajeno je: D0 CF 11 E0 A1 B1 1A E1. Većina forenzičkih softverskih alata imaju aplikaciju koja vrši ’*analizu potpisa fajlova’*.

Istraživanje tragova pristupa Internetu na osumnjičenom računaru, samo je uvod u kompleksnu forenzičku analizu napada sa Inteneta. Značajni podaci

nalaze se u *privremenim Internet* fajlovima (*Internet Cache*) koji ostaju na računaru posle aktivnosti na nakoj web lokaciji. Korisnik može podesiti na minimum veličinu Internet keša na disku – 0MB, što efektivno znači kao da keša nema. Međutim, neki Internet keš uvek mora da postoji u računaru. Ako forenzičar otkrije da je keš vrednost 0%, treba postaviti pitanje zašto je to tako. U Windows 2000 i XP sistemima, keš fajlovi se nalaze u C:\Documents and Settings\{User Name}. Fajl INDEX.DAT kontroliše Internet keš i od vitalnog je značaja za forenzičare u istrazi aktivnosti korisnika na Intrnetu.

Značajno je ispitati *Internet History - master, nedeljni i dnevni,* kojima takođe, upravljaju INDEX.DAT fajlovi, kao i kolačiće i favorizovane lokacije. Forenzički je interesantan i *FastTrack* potokol P2P mreža, koji je verovatno najbogatiji sa dokaznim podacima. Postoje brojni alati, a *KaZAlyzer* je specijalno pisan za ispitivanje *FastTrack* protokola i obezbeđuje dešifravane termine za pretraživanje i druge podatke. Forenzičar mora znati i da deinstalacija *FastTrack* sistema ostavlja brojne važne tragove za ispitivanje, iako se Registar očisti, ostaje My Share Folder kao i DBB folder u korisničkom profilu.

Proizvodi kao što su *CuteFTP i WS-FTP* sadrže log fajlove svojih aktivnosti, koji obezbeđuju dragocene informacije o transferu fajlova sa vremenima i datumima distribucije. Aplikacije kao što su *Outlook, Outlook Express, Eudora i Pegasus* primeri su programa koji idu direktno u skladište e-pošte i izvlači svu dolazeću e-poštu. Za forenzičara je značajno da poznaje tipove fajlova koje može naći u ovim aplikacijama, npr., *Outlook* koristi seriju **.PSF**, ili .**OST** fajlova, a postoje priznate tehnike za ispitivanje ovih fajlova i softverski alati za njihovo dešifrovanje. Outlook Express koristi **DBX** sistem fajlova, za svaki deo aplikacija - INBOX, OUTBOX, SENT ITEMS, DELETED ITEMS, DRAFTS itd. Forenzičar treba da objasni šta je IP adresa u e-mail hederu, što je moguće jasnije i kraće.

Veće probleme forenzičar može imati u izvlačenju dokaza iz čet servisa tipa *Skype,* pošto podrazumevano svi čet klijenti imaju isključenu funkciju istorije, pa je analiza komunikacije tim teža. Veće šanse su kod servisa novinske grupe, gde aplikacije za čitanje vesti donose poruke grupa u lokalne mašine, što olakšava analizu. U ovim grupama može se naći najviše ilegalnih aktivnosti na hakovanju, fišingu, dečijoj pornografiji, terorizmu i drugim vidovima zloupotreba. Imaju strukture hedera slično e-pošti, pa postoji mogućnost identifikovanja lica koja su uputila poruku.

Rutkitovi su alati koje napadači koriste da sakriju svoje prisustvo u sistemu, a zadnja vrata, jedna od komponenti rutkita, koriste se za kasniji pristup

hakera sistemu. Često administrator ne može razlikovati rutkit od standardnog programa, pa su razvijene osnovne metodologije, alati i tehnike koje sistem administartori mogu koristiti za detekciju prisustva rutkitova, zadnjih vrata i mrežnih snifera.

Ključne tačke su uloga i značaj sistemskih procesa za detekciju skrivenih programa, način detekcije neobičnih i skrivenih fajlova koji su često znak kompromitacije sistema, zatim alata i tehnika za detekciju i uklanjanje rutkitova, zadnjih vrata i snifera mrežnih paketa.

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

PITANJA ZA PONAVLJANJE

1. Navedite četiri tipa informacija koje se mogu nalaziti u log fajlu.
2. Navedite dva tipa fajlova koji se koriste u Windows operaciji printovanja.
3. Navedite dva formata skladištenja podataka u *print spool* fajlove.
4. Kako se mogu kreirati link fajlovi?
5. Navedite podrazumevane lokacije za link fajlove u Windows *XP setup-u*?
6. Navedite četiri primera privremenih fajlova koje MS Office može kreirati?
7. Šta su metapodaci?
8. Zašto je potreban Internet keš?
9. Gde su podrazumevano uskladišteni privremeni Internet fajlovi na XP mašini?
10. Koliko možemo očekivati da nađemo keš foldera?
11. Koji fajl sakuplja zajedno sve informacije iz keš fajlova?
12. Šta je podrazumevano podešavanje za veličinu keša?
13. Može li korisnik imati veličinu keša od 0Mb?
14. Da li je veličina keš fajla zaista 0Mb?
15. Zašto je potrebna Internet istorija?
16. Koliki je podrazumevani broj dana skladištenja Internet istorije?
17. Kako možete opisati *cookies*?
18. Šta je namena *Internet favourites*?
19. Da li *favourite entries* uvek kreira korisnik odlaskom na izabrani?
20. Šta je *Peer to Peer* (P2P) umrežavanje?
21. Navedite dva P2P protokola koji se najčešće koriste?

22. Koji folder podrazumevano kreira KaZaA za skladištenje daunlodovanih fajlova?
23. Gde je taj folder podrazumevano lociran?
24. Kakvu moguću prednost daje forenzičaru otkrivanje log fajla od nekog FTP klijenta?
25. Koja su dva tipa e-mejlova koja efektivno postoje?
26. Koji tip fajlova koristi *Outlook*?
27. Koji tip fajlova koristi *Outlook Express*?
28. Gde se mogu naći dokazi koji se odnose na Internet bazirane hotmail naloge na mašini?
29. Gde se mogu naći informacije koje omogućavaju praćenje traga do izvora e-mejla?
30. Šta je IP adresa?
31. Da li ekstenzija fajla garantuje tip fajla kojeg forenzičar otkrije?
32. Kako Windows OS identifikuje i pokuša otvoriti fajl na zahtev korisnika?
33. Kako naš forenzički softver identifikuje da fajl možda nije ono što mu ime pokazuje?
34. Šta je rutkit (*Root Kit*)?
35. Šta je Trojanac?
36. Koliko delova čine Trojanca i koji se deo pojavljuje na kojoj mašini?
37. Koje su opšte mogućnosti Trojanaca?
38. Šta se može koristiti za detekciju prisustva Trojanaca na mašini?
39. Kako se naziva korišćenje velikog broja Trojanaca na mnogo računara za napad na web server i izvršavanje DDOS napada?
40. Navedite nekoliko koraka koji se mogu preduzeti za odbranu od Trojanaca?
41. Koju vrstu artefakata treba koristiti za odbranu od Trojanaca?

12 DATUM I VREME U FORENZIČKOJ ANALIZI RAČUNARSKOG SISTEMA

12.1 Formati datuma i vremena u računarskim sistemima

Dokazi o vremenima i datumima aktivnosti u računarskom sistemu i RM istovremeno su veoma značajni i veoma kompleksni. Dokazi o datumu i vremenu fundamentalni su deo većine digitalnih forenzičkih ispitivanja. Pravnici usmeravaju najćešće pažnju na vreme i datum kompromitacije RS, jer oni predstavljaju konkretnu vezu između realnog sveta i digitalnog okruženja. Generalno, što je forenzičar iskusniji to se manje oslanja na tačnost određenog vremena i datuma. Uvek je bolje tražiti *koraborativne* dokaze i posmatrati punu sliku događaja, [5].

Značaj i problematika otkrivanja vremena i datuma može se ilustrovati na primeru MS Windows OS i *Internet eksplorera*. Vreme i datum se računa jednostavnom funkciom časovnika u **CMOS** (*Complementary Metal Oxide Semiconductor*) kodenzatoru, koja računa tekuće vreme.

***32-bitni Windows/DOS format vremena*:** U Windows/DOS OS vreme se skladišti u binarnoj paketnoj formi. Datum i vreme uskladišteni su u sledećoj 32-bitnoj strukturi (4 bajta): *Sekunde zauzimaju 5 bitova od ofseta 0, minute zauzimaju 6 bitova od ofseta 5, a časovi 5 bitova od ofseta 11.* Ovih 5 bitova ne može uskladištiti 60 sekundi, tako da vreme mora biti inkrementalno popunjeno u 2 s (ravnim intervalima). Datum zauzima 5 bitova od ofseta 16, meseci zauzimaju 4 bita od ofseta 21, a godine zauzimaju 7 bitova od ofseta 25 (računajući od 1980).

Ovaj MS/DOS vreme/datum format koristi se u FAT fajl sistemu za snimanje vremena i datuma kreiranja, modifikacije i poslednjeg datuma pristupa.

64-bitni Windows FILETIME format vremena: Ovaj format uskladišten je kao 64-bitni broj (8 bajta) sa početkom od 100ns (1ns $=10^{-9}$ s) intervala od 00:00:00 na 1. januar 1601. Ovaj format se koristi u NTFS MFT za skladištenje MAC vremena - kreiranja, poslednje modifikacije, poslednjeg pristupa i poslednje modifikacije MFT snimka.

Unix vremenski format: Ovaj format je uskladišten kao 32 bitni broj koji počenje brojanje sekundi od 00:00:00 od 1. januara 1970. godine.

HFS and HFSD format vremena: Ovaj format datum/vremena ***Apple Mac*** fajl sistema uskladišten je kao 32 bitni broj sa početkom brojanja sekundi od 00:00:00 1. januara 1904. godine.

Prevođenje lokalnog i UTC vremena: Kada se radi u različitim vremenskim zonama, ili zbog promene vremena, važno je znati da li je vreme prevedeno u Koordinirano univerzalno vreme – **UTC** (*Coordinated Universal Time*), ili se koristi lokalno vreme. Univerzalno vreme - **UT** (*UniversalTime*), **UTC** i Srednje vreme po Griniču – **GMT** (*Greenwich Mean Time*) efektivno su ista vremena, ali IKT interesna zajednica u svetu najčešće loristi UTC vreme. Većina fajl sistema i aplikacija automatski računa razliku između lokalnog vremena i UTC i skladišti strukturu vreme/datum u UTC firmatu. Ovo daje prednost OS, ili aplikaciji, ali može zbuniti forenzičara. Kao jednostavan primer, pokušajte na NTFS particiji kreirati tekst fajl i zabeležiti vremena kreiranja i modifikacije fajla. Zatim promenite vremensku zonu i pogledajte ponovo vremena kreiranja i modifikacije istog fajla. Eksplorer je automatski preveo vreme iz uskladištenog UTC formata kao atributa u MFT i prikazao lokalno vreme prema novoj vremenskoj zoni.

Važno je uočiti da vremenska struktura sama ne snima UTC, ili lokalno vreme. Ova se odluka donosi kad se projektuje i programira fajl sistem, OS ili aplikacija. Postoje određene činjenice koje su obično istinite, kao na primer 64 bitni Windows *file time* se prevodi (ne uvek) iz lokalnog vremena u UTC i obrnuto. Ovo je rezultat pozivanja Windows API-a, a može se napisati program koji ignoriše ovaj protokol. Od pomenutih vremenskih struktura uobičajeno su kao lokalna vremena uskladištena samo 32-bitna Windows/DOS vremena i HFS (ali ne i HFSC) vremena, ali forenzičar uvek treba proveriti dokaz o vremenu/datumu.

Informacije o datumu i vremenu u registru: Vreme koje se zasniva na *Windows* platformama može se identifikovati kroz ispitivanje informacija sistemskih regisatara. Na živoj mašini ovo se može proceniti korišćenjem ne-forenzičkih tehnika kao što su *regedit* komanda iz *run* komandnog promta. U Windows ME/XP platformama vremenska zona je locirana u registru:

```
HKEY_Local_Machine/System/Current
ControlSet/Control/TimeZoneInformation/Bias
```

ActiveTimeBias je broj minuta (C ili _) za dodavanje UTC. Rezultati za korektno podešavanje za vremensku zonu Londona javlja se u formatu:

ActiveTimeBias REG_DWORD 0x00000000 StandardName REG_SZ GMT Standard Time.

Za pacifičko standardno vreme (GMTD480 min) podaci u registru prikazuju se na drugačiji način:

ActiveTimeBias REG_DWORD 0x000001e0, StandardName REG_SZ Pacific Standard Time.

Na sličan način u slučaju vremenske zone ispred GMT, na primer GMTD3, dodatak vremena bio bi negativan (_180 min) i predstvalja se sa:

ActiveTimeBias REG_DWORD 0xffffff4c, StandardName REG_SZ E.Africa Standard Time.

Ovo se može demonstrirati otvaranjem dva prozora u MS OS, jednog koji pokazuje *Regedit* i drugog *Time and Date Properties*. Jednostavno se izmeni vremenska zona u *Properties* prozoru i ispituju promene u prikazanim vremenima i u *Registru*. Ključ *'TimeZoneInformation'* u registru sadrži podatke važne za svako vreme dnevnog memorisanja, koji se odnose na vremensku zonu pod '*DaylightBias*, a period kada ovo treba primeniti definisano je korišćenjem '*DaylightStart*' i '*StandardStart*'. Jasno ovi se podaci moraju uračunati u vreme/datum informacije koje program za snimanje koristi u toku skladištenja.

12.2 Datum i vreme kao digitalni dokaz

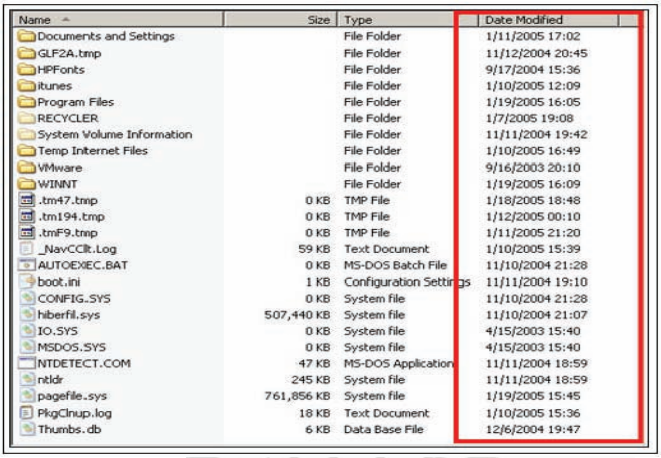
Vreme i datum u računaru oslanjaju se na sistemski časovnik i predstavljaju najproblematičniju oblast računarske forenzike. Generalno računar čuva snimke vremena i datuma (vremenski pečat) skoro za svaki tip akcije na računaru i to ne samo da ih kreira OS, nego i brojne aplikacije. Sa preciznom analizom vremena i datuma forenzičar može proizvesti dokazne podatke koji dokazuju kada su se određene akcije dogodile. Vreme i datum izvršavanja akcija može videti svaki korisnik u *properties* Windows Explorer-a za svaki fajl u Windows OS. Brojni vremenski pečati koje računar pravi, nisu toliko očigledni, na primer mnoge aplikacije vreme i datum akcija ugrađuje kao metapodatke u svoje fajlove. Ako se očigledni i skriveni vremenski pečati u dokaznom postupku slažu u svim uređajima na putu kompromitacije sistema,

akcija se može smatrati dokazanom, a ako ne potreban je dodatni napor da se ta razlika razume i objasni pred sudom. Forenzičar treba da ima na umu da vreme i datum napada na sistem najčešće mogu biti najvažniji dokaz koji mogu proizvesti. Vremenska linija napada pokazuje seriju događaja koji su se desili u toku napada i može povezati neku osobu sa aktivnostima na računaru u to vreme. Ako analiza otkrije pogrešno vreme i datum, to za dokazni postupak može biti fatalno i zbunjujuće za forenzičara i sud.

12.2.1 Datum i vreme u Windows operativnom sistemu

Windows OS-i bazično čuvaju tri vremena i datuma: ***kreiranja, modifikacije i posledenjeg pristupa***. U nekim starijim Windows OS, čuva se samo datum pristupa, ali ne i vreme. U računaru koji koristi NTFS fajl sistem u MFT tabeli nalazi se i datum modifikacije ulaza (*entry*). Forenzičar takođe, mora znati kako Windows računa ova vremena i datume. Generalno, datum se sadrži u atributima fajlova koj se odnose na svaki fajl, ili folder. OS-i koji koriste MS-DOS računaju svoje podatke precizno sa greškom do 2 sekunde od 1.01.1980. Na sistemima koji koriste NTFS i FAT32 datum i vreme se računaju sa tačnošću od 100 nsec od 1.01.1601 godine. Ovaj datum i vreme mogu se videti u MFT tabeli NTFS fajl sistema kao 64-bitni broj u **Litle Endian** zapisu, [24].

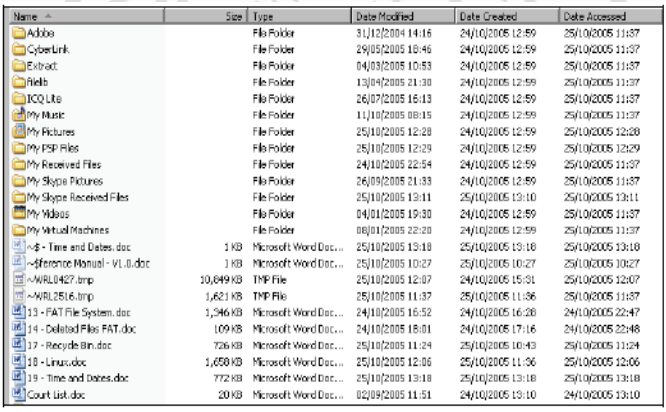
Uobičajena lokacija gde treba početi gledati datume i vremena u Windows OS je **My Computer,** ili **Windows Explorer**. Sledeći prozor pokazuje normalni pogled u Explorer-u, gde normalno nalazimo datume i vremena modifikacije (slika 12.1).



Name	Size	Type	Date Modified
Documents and Settings		File Folder	1/11/2005 17:02
GLF2A.tmp		File Folder	11/12/2004 20:45
HPFonts		File Folder	9/17/2004 15:36
itunes		File Folder	1/10/2005 12:09
Program Files		File Folder	1/19/2005 16:05
RECYCLER		File Folder	1/7/2005 19:08
System Volume Information		File Folder	11/11/2004 19:42
Temp Internet Files		File Folder	1/10/2005 16:49
VMware		File Folder	9/16/2003 20:10
WINNT		File Folder	1/19/2005 16:09
.tm47.tmp	0 KB	TMP File	1/18/2005 18:48
.tm194.tmp	0 KB	TMP File	1/12/2005 00:10
.tmF9.tmp	0 KB	TMP File	1/11/2005 21:20
_NavCClt.Log	59 KB	Text Document	1/10/2005 15:39
AUTOEXEC.BAT	0 KB	MS-DOS Batch File	11/10/2004 21:28
boot.ini	1 KB	Configuration Settings	11/11/2004 19:10
CONFIG.SYS	0 KB	System file	11/10/2004 21:28
hiberfil.sys	507,440 KB	System file	11/10/2004 21:07
IO.SYS	0 KB	System file	4/15/2003 15:40
MSDOS.SYS	0 KB	System file	4/15/2003 15:40
NTDETECT.COM	47 KB	MS-DOS Application	11/11/2004 18:59
ntldr	245 KB	System file	11/11/2004 18:59
pagefile.sys	761,856 KB	System file	1/19/2005 15:45
PkgClnup.log	18 KB	Text Document	1/10/2005 15:36
Thumbs.db	6 KB	Data Base File	12/6/2004 19:47

Slika 12.1 Datumi i vremena modifikacije u Windows Explorer-u

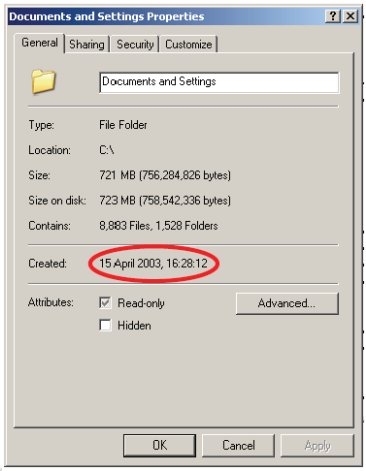
Izborom **View**, zatim **Details** opcije u Explorer-u, pogled se menja i izgleda kao u sledećem prozoru gde se vide svi glavni datumi.



Name	Size	Type	Date Modified	Date Created	Date Accessed
Adobe		File Folder	31/12/2004 14:16	24/10/2005 12:59	25/10/2005 11:37
CyberLink		File Folder	29/05/2005 18:46	24/10/2005 12:59	25/10/2005 11:37
Extract		File Folder	04/03/2005 10:53	24/10/2005 12:59	25/10/2005 11:37
Fileib		File Folder	13/04/2005 21:30	24/10/2005 12:59	25/10/2005 11:37
ICQ Lite		File Folder	26/07/2005 16:13	24/10/2005 12:59	25/10/2005 11:37
My Music		File Folder	11/10/2005 08:15	24/10/2005 12:59	25/10/2005 11:37
My Pictures		File Folder	25/10/2005 12:28	24/10/2005 12:59	25/10/2005 12:28
My PSP Files		File Folder	25/10/2005 12:29	24/10/2005 12:59	25/10/2005 12:29
My Received Files		File Folder	24/10/2005 22:54	24/10/2005 12:59	25/10/2005 11:37
My Skype Pictures		File Folder	26/09/2005 21:33	24/10/2005 12:59	25/10/2005 11:37
My Skype Received Files		File Folder	25/10/2005 13:11	25/10/2005 13:10	25/10/2005 13:11
My Videos		File Folder	04/01/2005 19:30	24/10/2005 12:59	25/10/2005 11:37
My Virtual Machines		File Folder	08/01/2005 22:20	24/10/2005 12:59	25/10/2005 11:37
~$ - Time and Dates.doc	1 KB	Microsoft Word Doc...	25/10/2005 13:18	25/10/2005 13:18	25/10/2005 13:18
~$ference Manual - V1.0.doc	1 KB	Microsoft Word Doc...	25/10/2005 10:27	25/10/2005 10:27	25/10/2005 10:27
~WRL0427.tmp	10,649 KB	TMP File	25/10/2005 12:07	24/10/2005 15:31	25/10/2005 12:07
~WRL2516.tmp	1,621 KB	TMP File	25/10/2005 11:37	25/10/2005 11:36	25/10/2005 11:37
13 - FAT File System.doc	1,946 KB	Microsoft Word Doc...	24/10/2005 16:52	24/10/2005 16:28	24/10/2005 22:47
14 - Deleted Files FAT.doc	109 KB	Microsoft Word Doc...	24/10/2005 18:01	24/10/2005 17:16	24/10/2005 22:48
17 - Recycle Bin.doc	726 KB	Microsoft Word Doc...	25/10/2005 11:24	25/10/2005 10:43	25/10/2005 11:24
18 - Linux.doc	1,658 KB	Microsoft Word Doc...	25/10/2005 12:06	25/10/2005 11:36	25/10/2005 12:06
19 - Time and Dates.doc	772 KB	Microsoft Word Doc...	25/10/2005 13:18	25/10/2005 13:18	25/10/2005 13:18
Court List.doc	20 KB	Microsoft Word Doc...	02/09/2005 11:51	24/10/2005 13:10	24/10/2005 13:10

Slika 12.2 Pogled na sve glavne datume u Windows Explorer-u

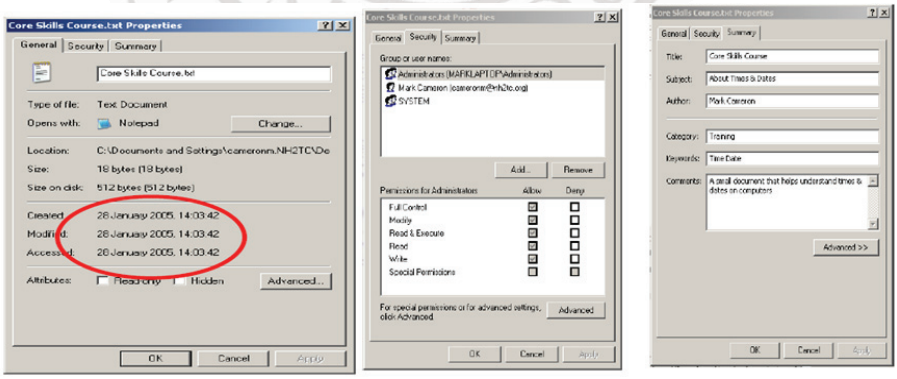
Na slici se vidi da svaki postojeći folder i fajl ima svoj vremenski pečat. Ako se detaljnije pogleda svaki fajl/folder može se pronaći više detalja o vremenima i datumima koji se odnose na fajlove/foldere. Na primer, na prozoru (slika 12.1) folder **Documents and Settings** je modifikovan 11.01.2005 u 17:02. Ako desnim tasterom miša na ovom folderu selektujemo **Properties**, može se naći više informacija. Datum kreiranja foldera je 15.04.2003 u 16:28:12, (slika 12.3).



Slika 12.3 Datum kreiranja foldera u prozoru **Properties**

Dobijanje informacija o vremenu i datumu kreiranja fajla/foldera u Windows fajl sistemu, kao deo procesa instalacije sistema, daje korisne informacije o samom procesu instalacije. Ako se gleda dublje u strukturu fajl sistema može se naći još više informacija o drugim sistemima i aplikacionim fajlovima, njihovoj instalaciji, korišćenju i interakciji.

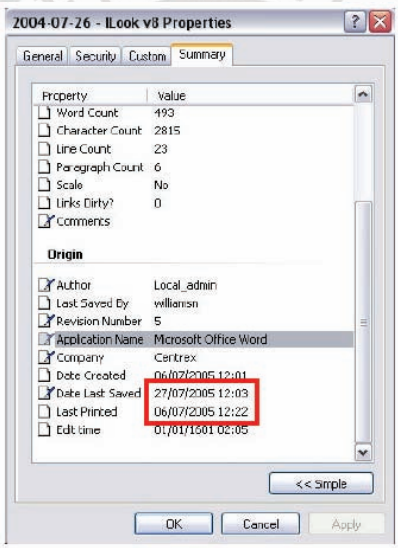
Ako se posmatra jednostavni tekst fajl, kao na slici 12.4, mogu se videti tri standardna datuma i vremena, koja su registrovana: ***kreirana, modifikovana, pristupljena***.



Slika 12.4 Datumi kreiranja modifikovanja i pristupa u prozoru Properties

Posmatranjem ovih podataka jasno se mogu videti relevantna vremena i datumi. Ovaj primer je sasvim jednostavan. Kreiran je prazan tekst fajl. Zatim je upisan mali tekst, što znači fajl je modifikovan i korisnik mu je pristupio. Vremenski pečati indiciraju da su se ovi događaji odvijali skoro simultano. Ako se otvori *advanced* opcija, može se dobiti više korisnih podataka. Ovi podaci takođe pokazuju ko je pristupio fajlu, njegova ovlašćenja i kratak sadržaj fajla. Kod određenih tipova fajlova mogu se dobiti dodatne informacije o vremenima i datumima.

U sledećoj ilustraciji vidi se sumarna informacija pridružena svakom word dokumentu, kada se gleda sa ***iLook*** forenzičkim alatom. Vide se dodatno vreme i datum kao što su **Datum poslednjeg memorisanja** i **Datum poslednjeg printovanja,** koji mogu biti od vitalnog značaja za istragu, (slika 12.5).



Slika 12.5 Prozor zbirne informacije o Word dokumentu u **Ilook** forenzičkom alatu

Mogu se videti i druge relevantne informacije, ali se forenzičar ne sme potpuno osloniti na vremena i datume fajlova, ako ne razume njihovu strukturu i ne razume uticaj određenih osnovnih operacija fajlova Windows OS na vremena i datume.

12.2.2 Datum i vreme u Microsoft Internet Explorer (IE)

*Microsoft Internet Explorer (***IE***)* kolačići (*cookies*) skladište se u folderu **'.\Cookies\'** zajedno sa pridruženom **index.dat** fajlom koji održava kolaćiće. Ovaj fajl ima sličan format **index.dat** fajlu istorije. Takođe, URL podaci imaju dva datuma od **0x8** i **0x10**. Prvi datum je UTC datum/vreme kada je kolaćić originalno preuzet na računaru. Drugi datum je datum/vreme kada je kolačiću poslednji put korisnik pristupio.

Studija slučaja: Računar u Londonu je radio na MS ME platformi, a vremenska zona podešena na ofset hex zapisu 0x00001e1 (C480 min), ili Pacifičko standardno vreme (PST). Uprkos korektnoj identifikaciji da je OS računara podešen na PST, ovo nije uneto u datum kojeg je u izveštaju prikazao forenzički alat *Encase V4* za interpretaciju datum/vreme informacija fajla i ekstrakciju podataka registra koji uključuju dodatak vremenske zone. Forenzički analitičar je dodatno koristio ***Net Analysis*** alat za analizu aktivnosti na Internetu. Ovo zahteva importovanje *index.dat* fajla i podešavanje dodatka vremenske zone. Nažalost forenzičar nije konfigurisao ***Net Analysis*** na pravi način pa je izveštaj prikazao vreme bez oduzimanja 8 časova. Na sreću, u daljem postupku, forenzičar je korigovao dokaz i ispravio ovu fundamentalnu grešku, čime je osumnjičeni optužen za "*korišćenje ID računara za pristup web sajtovima sa sadržajem* dečije *pornografije*" i dokazano da "*računar nije radio ni na koji način od trenutka privremenog oduzimanja*".

12.3 Kontrolna lista za dokaze o datumu/vremenu

Za kontrolnu listu za analizu datuma i vremena na računaru sugerisane su sledeće ključne aktivnosti:

1. Snimiti **CMOS** vreme na privremeno oduzetoj, ili ispitivanoj jedinici sistema u odnosu na aktuelno vreme, dobijeno korišćenjem časovnika preko radio/TV signala, ili pouzdanih vremenskih servera preko Interneta;
2. Uspostaviti tekuću vremensku zonu računara iz registra;
3. Ustanoviti da li prolećno/jesenje usklađivanje vremena (*daylight saving times*) ima neki efekat na vremena relevantna za istragu;

4. Identifikovati tipove struktura vremena koje koristi forenzički računar i utvrditi da li prikazuju lokalno, ili UTC vreme. Za ovo koristiti alate kao što su *Decode Date* od *Digital Detective Inc.* (www.digital-detective.co.uk)*;*
5. Tražiti *koraborativne* dokaze u formi dodatnog vremena, datuma i aktivnosti na tom računaru i drugim mrežnim uređajima, koji potvrđuju interpretaciju datuma i vremena kroz konzistentnu vremensku liniju;
6. Testirati rezultate koristeći isti OS i verziju aplikacije kao u ispitivanom računaru.

12.4 Forenzički aspekt informacija o vremenu i datumu

Najranije verzije *Windows OS*, koje su koristile DOS verzije, održavale su samo jednu vrednost datuma i vremena koji se odnose na fajl - **poslednji datum i vreme modifikacije** uskladišten sa 32 bita, da bi se mogao pratiti trag fajlova na medijima za skladištenje. Pojavom Windows OS sa FAT32 fajl sistemom registruju se sledeća vremena i datumi:

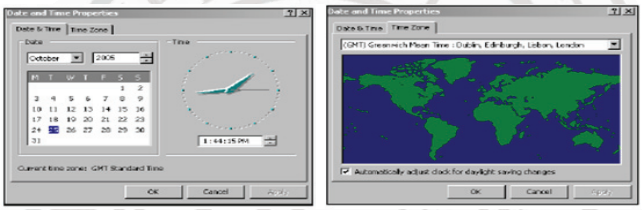
- Kreiranja: vreme kada je fajl kreiran u tekućem direktorijumu, kopiran u drugi direktorijum, upisana nova vrednost u fajl i kada je fajl premešten.
- Modifikacije: vreme kada je fajl poslednji put modifikovan i kopiran bilo gde.
- Pristupa: vreme kada je korisnik poslednji put pristupio fajlu. Ovu vrednost podešava aplikacija koja se koristi i ona menja ovu vrednost.

Kasnije verzije Windows OS koriste 64 bita za kreiranje i skladištenje informacija o vremenu i datumu i daju tačniju strukturu vremena i datuma. Iako sve ovo izgleda jednostavno, forenzičar mora biti spreman da objasni prisustvo određenog vremena i datuma u fajl sistemu. Do greške u vremenu i datumu može doći u sledećim situacijama:

- časovnik računara je isključen, ili netačan,
- fajl je kopiran na novu lokaciju na istom, ili drugom disku,

- fajl je premešten na novu lokaciju na istom, ili drugom disku,
- fajl je kopiran na drugi računar,
- pomeranje časovnika zbog prolećno/jesenjeg usklađivanja vremena,
- neusklađene vremenske zone,
- intervencija korisnika i
- intervencija softvera.

Nekoliko narednih primera ukazuje šta potencijalno može biti problem za forenzičara i kako ga treba prevazići. Treba početi sa časovnikom računara. Dvostrukim aktiviranjem tastera miša na ikonu časovnika u donjem desnom uglu ekrana otvara se prozor časovnik i vreme se po volji može izmeniti (slika 12.6).



Slika 12.6 Prozori za podešavanje datuma, vremena i vremenske zone

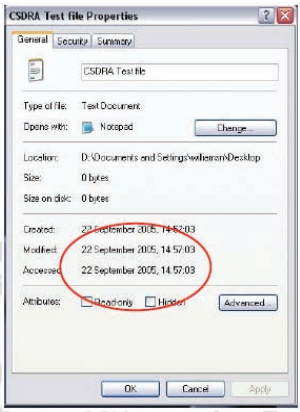
Jedna od prvih akcija forenzičara kod privremenog oduzimanja osumnjičenog računara je ispitivanje podešenosti časovnika računara, da bi se mogla utvrditi osnovna vremenska linija za ispitivanje kroz ceo slučaj. Nema ničega što govori da je neko/nešto u nekoj tački promenio/lo vreme na računaru, što je stalan problem za forenzičara. Ipak, ova praksa nije tako česta i može se prevazići sa intervjuom osumnjičenih i svedoka.

Drugi faktor je vremenska zona na koju je računar podešen. Za prosečnog korisnika vremenska zona koja je podešena na računaru, prilično je beznačajna, sve dok časovnik pokazuje prilično tačno lokalno vreme. Međutim, vremenske zone su značajne za forenzičara u istrazi *kibernetičkog kriminala*[12] sa Interneta i gde računar može biti *Laptop* koji se kreće kroz različite vremenske zone. Drugo pitanje je kada računar automatski menja vreme časovnika radi prolećno/jesenjeg usklađivanja vremena.

[12] *Cybercrime*

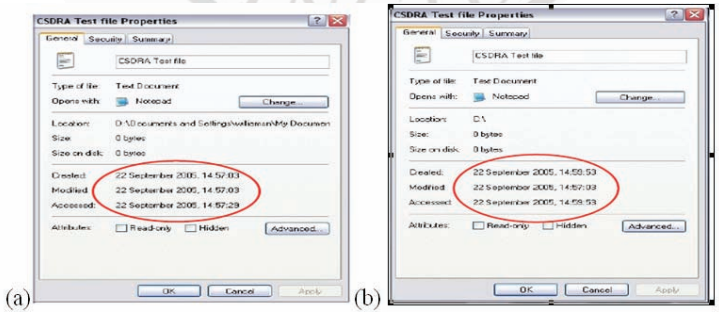
Uticaji različitih manipulacija sa fajlovima na promene u vremenima i datumima fajlova ilustrovani su kroz sledeća četiri scenarija.

1. Scenario: Kreiran je na desktopu prazan tekst fajl pod imenom *CSDRA Text file*. Sva vremena i datumi su konzistentni sa akcijom; vremena kreiranja, modifikacije i pristupa su očekivano ista, (slika 12.7).



Slika 12.7 Vremena kreiranja modifikacije i pristupa u prozoru Properties tekst fajla

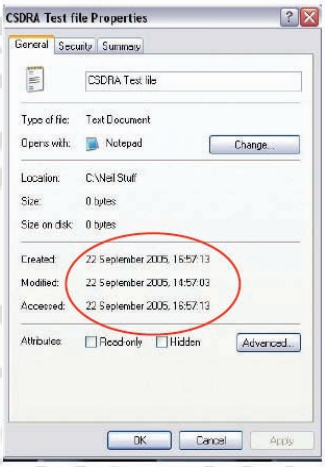
2. Scenario: Sada se isti fajl premesti *drag&drop* operacijom na drugu lokaciju na istom disku/particiji. Lokacija je promenjena pa se menja vreme i datum pristupa, a vremena kreiranja i modifikovanja ostaju ista. Međutim, činjenica je da stvarno nije bilo pristupa fajlu - jednostavno fajl je samo premešten, (slika 12.8a).



Slika 12.8 Datumi i vremena fajla pomerenog drag&drop operacijom na istoj (a) i drugoj (b) particiji

3. Scenario: Sada se fajl premesti ponovo sa *drag&drop* na drugi disk/particiju. Lokacija se promenila pa se menja vreme pristupa, ali i vreme kreiranja, pošto pomeranje fajla na drugi disk ima efekat kreiranja novog fajla. Međutim, datum modifikacije fajla ostaje isti pa imamo fajl koji je *kreiran posle poslednje modifikacije*. Naravno, ovakvo objašnjenje pred sudom može biti smešno, pošto nije logično da se neki fajl može modifikovati pre svog kreiranja, (slika 12.8b).

4. Scenario: Sada se fajl ponovo premesti sa funkcijom *copy/paste* u folder na istom disku/particiji. Lokacija se menja, pa se vremena i datumi kreiranja i pristupa ponovo menjaju, ali vreme modifikacije ostaje neizmenjeno, (slika 12.9).



Slika 12.9 Datumi i vremena fajla pomerenog copy/paste operacijom

Ovi primeri ilustruju koliko vremena i datumi u Windows operativnim sistemima mogu biti problematični. Iako Windows OS-i rade sa vremenom i datumom u osnovi na isti način, važno je znati da neke verzije to rade na neznatno drugačiji način. Potvrđeno je da prolećna i jesenja promena vremena mogu izazvati netačnost u prikazivanju vremena, što je *Microsoft* priznao i proizveo zakrpu za ovaj problem. Sličan je problem kod premeštanja fajla iz NTFS u FAT32 fajl sistem. Takođe, postoje brojne softverske aplikacije koje omogućavaju korisniku da kontroliše i definiše vremena i datume pripisane fajlovima.

REZIME

Dokazi o vremenima i datumima aktivnosti u računarskom sistemu i mreži su veoma značajni i kompleksni; fundamentalni su deo većine digitalnih forenzičkih ispitivanja, jer oni predstavljaju konkretnu vezu između realnog sveta i digitalnog okruženja. Iskusni forenzičar se malo oslanja na tačnost određenog vremena i datuma i uvek traži *koraborativne* dokaze događaja.

Značaj i problematika otkrivanja vremena i datuma može se ilustrovati na primeru MS Windows OS i *Internet eksplorera*. Vreme i datum se računa jednostavnom funkciom časovnika u **CMOS** (*Complementary Metal Oxide Semiconductor*) kodenzatoru, koja računa tekuće vreme. Forenzičar treba da poznaje formete vremena u različitim OS. Na primer, *64-bitni Windows FILETIME format vremena* koristi se u NTFS MFT za skladištenje MAC vremena - kreiranja, poslednje modifikacije, poslednjeg pristupa i poslednje modifikacije MFT snimka. Kada se radi u različitim vremenskim zonama, ili zbog promene vremena, važno je znati da li je vreme prevedeno u koordinirano univerzalno vreme – **UTC**, ili se koristi lokalno vreme. U Windows ME/XP platformama vremenska zona je locirana u registru: HKEY_Local_Machine/System/Current ControlSet/Control/TimeZone Information/Bias.

Vreme i datum u računaru oslanjaju se na sistemski časovnik i predstavljaju najproblematičniju oblast računarske forenzike. Sa preciznom analizom vremena i datuma forenzičar može proizvesti dokazne podatke koji dokazuju kada su se određene akcije dogodile. Vreme i datum izvršavanja akcija može videti i izmeniti svaki korisnik u *properties* Windows Explorer-a za svaki fajl u Windows OS. Zato forenzičar treba da obezbedi vremensku liniju napada iz više vremenskih pečata različitih uređaja i aplikacija, kao i da objasni nelogičnosti i izmene u nekom pečatu, na primer da je fajl *kreiran posle poslednje modifikacije*.

PITANJA ZA PONAVLJANJE

1. Koja tri vremena i datuma možemo videti za svaki fajl u računarskom sistemu?
2. U kojem starijem sistemu za svaki fajl postoji samo datum, a ne i vreme?
3. Gde je locirana vremenska zona u Windows ME/XP platformama?
4. Na koji uređaj se oslanjaju vreme i datum u računaru?
5. Navedite nekoliko faktora vremena i datuma koji mogu otežati rad forenzičara?
6. Objasnite kako je moguće da vremenski pečat pokazuje da je fajl *kreiran posle poslednje modifikacije*.
7. Kako korisnik može izmeniti vremenski pečat?
8. Koja se vremena registruju u FAT 32 fajl sistemu?
9. Navedite neke uzroke koji dovode do greške u vremenu i datumu.

13 ANTI-FORENZIČKE AKTIVNOSTI I ALATI

Relativno velika dostupnost forenzičkih alata i znanja može kontra-produktivno delovati na uspeh forenzičke analize. Sa jedne strane, forenzičari mogu lakše razrešiti problem na koji naiđu u radu, koristeći brojne baze znanja i informacija i alate različitih mogućnosti, sa druge strane istim alatima i znanjima mogu pristupiti razni maliciozni korisnici i vešti hakeri. Da bi se ilustrovale ove mogućnosti, između brojnih potencijalnih aktivnosti, dovoljno je detaljnije opisati primenu tehnike ***brisanja sa prepisivanjem*** (*wiping)* i primenu ***anti-forenzičkih alata*** (*counter-forensic*), [24].

Termin "*wiping*" pozajmljen je iz zajednice digitalnih forenzičara, da bi se moglo razlikovati kompletno uklanjanje podataka od običnog brisanja sa rutinskim komandama računara. Kao što je poznato, brisanje nekog fajla obično ne briše podatke tog fajla, nego samo menja deo imena fajla u direktorijumu, indicirajući OS, da su ti sektori i klasteri koje je fajl koristio sada na raspolaganju za neki novi fajl. Međutim, koristeći funkciju oporavka izbrisanog fajla, podaci iz tog fajla mogu se lako oporaviti. Čak ni formatiranje ne prepisuje većinu podataka na disku. Sa druge strane, *wiping* je proces koji prepisuje korišćeni prostor fajla koji se 'briše' sa beznačajnim podacima, najčešće nulama.

Većina forenzičkih alata za prepisivanje fajlova radi na nivou fizičkog ili logičkog diska, dok su brojni alati namenjeni za brisanje pojedinačnih fajlova, grupe fajlova, celog direktorijuma ili particije. Međutim, jedino pouzdan i forenzički prihvatljiv način prepisivanja diska je sa butabilnog flopi diska, ili CD-a.

Na raspolaganju su brojni alati za brisanje prepisivanjem podataka fajla, neki su besplatni, neki se dele, a drugi su komercijalno raspoloživi. Kao i drugi forenzički alati, treba ih testirati pre upotrebe, da bi im se moglo verovati. Većini forenzičkih alata baziranih na *Windows* platformama ne treba unapred verovati, zbog načina rada Windows OS-a i kontrole pristupa hardveru, ali mogu usmeriti pažnju forenzičara.

Podaci se sa diska mogu trajno ukloniti fizičkim uništavanjem diska, ili demagnetizacijom diska sa snažnim magnetnim poljima, što uvek nije

prihvatljiv način. Brisanje sa prepisivanjem podataka vrši se sa forenzičkim alatima i prepisivanjem podataka fajla sa nulama, jedinicama, ili slučajnim nulama i jedinicama, što efektivno uništava podatke.

Postoje brojni standardi za brisanje sa prepisivanjem koji su namenjeni mahom za klasifikovane i osetljive informacije. Ovi su standardi razvijeni, zato što je teoretski moguće oporaviti tako prepisane podatke sa upotrebom vrlo sofisticirane i skupe opreme. Naime, pošto se podaci na magnetskim medijima kreiraju pozicioniranjem magnetnih svojstava medijuma, ostatak pozicioniranja tih svojstava može preostati nakon prepisivanja i mogu se otkriti moćnim, izuzetno skupim, elektronskim mokroskopima. Međutim, sa praktičnog aspekta, jedno prepisivanje čine podatke nečitljivim, a višekratno prepisivanje potpuno uništava sve potencijalne forenzički relevantne podatke. Dalje, prepisivanje sa slučajnim nizom jedinica i nula još više otežava rad forenzičara. Ako, na primer, postoji rasprava o poreklu slučajnog niza, uopšte nije lako, ili je nemoguće dokazati njegovo poreklo, pa odbrana može lako iskoristiti tu situaciju.

Uobičajeno prihvatljiva forenzička praksa diktira da se W*iping* forenzički alati koriste za čišćenje medijuma namenjenih za skladištenje digitalnih dokaza, što otklanja sumnju da su na medijumu postojali neki podaci pre upisivanja dokaza sa ispitivanog slučaja.

Takođe, ova tehnika može se zahtevati za brisanje kompromitovanih medijuma sa ilegalnim sadržajem (npr., dečijom pornografijom), koji se posle presude vraća osumnjičenom, posebno u slučajevima kada su kombinovani sa legalnim podacima nad kojima osumnjičeni ima pravo vlasništva i kada se za to dobije sudski nalog.

Anti-forenzika je termin uveden poslednjih godina, a označava tehnike hakera i *kibernetičkih* kriminalaca namenjene za borbu protiv forenzičke istrage – otežavanje, ili onemogućavanje te istrage. Vešt haker može preduzeti brojne korake da izvrši ove zadatke.

Mnoge komponente i aplikacije Windows OS imaju mogućnost podešavanja konfiguracije tako da otežavaju forenzičku istragu. Neka se podešavanja mogu izvršiti različitim alatima **Controle Panel**-a na Windows OS, a druga se podrazumevano konfigurišu unutar određenih programa. Takvo podešavanje čisti *swap* fajl u toku isključivanja, čisti *run liste* u programima kao što su Windows **Media Player,** briše privremene Internet fajlove, ili Internet istoriju,

u toku zatvaranja pretraživača i prazni izbrisanu poštu iz **Outlook**-a po zatvaranju programa.

Alat za raspored rada (*scheduling tool*) u Windows OS može se koristiti da izvršava programe na regularnoj bazi. Neki od ovih programa, kao što je pomoćni alat za defragmentaciju, može prepisti potencijalne dokaze. Mogu se ispisati *batch* fajlovi sa ekstenzijom **.BAT** koji sadrže listu komandi, ili rutina programa koje će računar izvršiti u sekvenci, što će izbrisati, prepisati, ili drugačije maskirati potencijalni dokazi.

Pored standardnih Windows programa, dostupni su brojni, različiti specijalizovani softverski programi koji mogu uništiti dokaze. Neki su dizajnirani iz benignih razloga, a neki specijalno za uništavanje programa. Na primer, **Tweak UI** je *Microsoft*-ov besplatan i dostupan program na Internetu, namenjen za fino podešavanje interfejsa korisnika i donosi dodatne karakteristike MS operativnom sistemu, ali ima neka podešavanja koja omogućavaju skrivanje, ili brisanje potencijalnih dokaza, na primer, da briše dokumenta fajlova istorije, menja podrazumevanu lokaciju fajlova itd.

Direktnija pretnja za forenzičara su programi namenski pisani i dizajnirani da unište potencijalne dokaze, među kojima je najbolji ***Evidence Eliminator***^{TM} (*Robbin Hood Software Ltd.,* www.evidence-eliminator.com). Ovaj proizvod tvrdi se da uništava:

- Windows SWAP file,
- Windows Application logs,
- Windows Temporary Files,
- Windows Recycle Bin,
- Windows Registry Backups,
- Windows Clipboard Data,
- Start Menu Recent Documents history,
- Start Menu Run history,
- Start Menu Find Files History,
- Start Menu Find Computer History,
- Start Menu Order Data,
- Start Menu Click History,

- Microsoft Internet Explorer privremeno otkucane URLs, index fajlove, keš istoriju,
- Microsoft Internet Explorer AutoComplete memoriju poslednje lokacije i pasvorde,
- Microsoft Internet Explorer Cookies (Selectivno čuvanje cookie za verzije 5 i više),
- Microsoft Internet Explorer Internet components (selektivno čuvanje komponenti),
- Microsoft Internet Explorer Download Folder memoriju
- Microsoft Internet Explorer Favourites List,
- Microsoft Outlook Express v5+bazu podataka (Selectivno čivanje pošte i vesti),
- Windows Media Player History,
- Windows Media Player PlayLists in Media Library,
- America OnLine Instant Messenger contacts,
- Netscape Navigator privremeno otkucane URLs, index fajlove, keš i istoriju,
- Netscape Navigator Cookies (Selectivno čuvanje cookie za verzije 4 i više),
- Netscape Mail v4+ poslate i izbrisane e-mails,
- Netscape Mail hidden files,
- Kastomizovane liste fajlova i foldera, sa ili bez njihovog sadržaja,
- Kastomizovane liste skeniranja tipova fajlova u specifičnim folderima,
- Kastomizovane liste skeniranja tipova fajlova u svim diskovima/particijama,
- Izbrisana imena fajlova, veličine i atributi iz struktura direktorijuma,
- Slobodan prostor klastera ("File Slack") iz fajlova svih tipova,
- Magnetski ostaci prethodnih fajlova/foldera,
- Sav slobodan nealocirani prostor na svim čvrstim diskovima,

- Dokaze o aktivnostima u mnogim drugim programima, koji koriste Plug-In module,
- Slack prostor i izbrisane ulaze u Windows Registry-ju,
- Datume i vremena kreiranja i modifikovanja na svim fajlovima i folderima,
- Windows Registry nizove,
- Common Dialog lokacije preuzimanja/memorisanja istorije,
- Trenutno bezbedno brisanje podataka iz Windows Registry (NT4/2000/XP).

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

REZIME

Ako forenzičar pristupi računaru osumnjičenog koji još uvek radi, može otkriti otvoreni šifrovani tekst, ili *on-line* bazu podataka u koju korisnik skladišti svoje podatke, ili je u toku rad korisnika koji je relevantan dokaz za slučaj. Najbolje rešenje je da forenzičar izvuče maksimum podataka iz sistema u radu, ali da obezbedi integritet svih sakupljenih dokaza, uključujući fotografisanje ekrana i svih akcija, pre isključivanja i privremenog oduzimanja računara.

Relativno velika dostupnost forenzičkih alata i znanja može kontra-produktivno delovati na uspeh forenzičke analize, pošto istim alatima i znanjima mogu pristupiti razni maliciozni korisnici. Ovo dobro ilustruje primena tehnika *brisanja sa prepisivanjem* (*wiping)* i *anti-forenzičkih alata*. W*iping* je proces koji prepisuje korišćeni prostor fajla koji se 'briše' sa beznačajnim podacima, najčešće nulama, jedinicama ili njihovim slučajnim kombinacijam i to jedan ili više puta.

Uobičajeno prihvatljiva forenzička praksa diktira da se W*iping* forenzički alati koriste za čišćenje medijuma namenjenih za skladištenje digitalnih dokaza, što otklanja svaku sumnju da su na medijumu postojali neki podaci pre upisivanja dokaza sa ispitivanog slučaja.

Anti-forenzika je termin uveden poslednjih godina, a označava tehnike hakera i *kibernetičkih* kriminalaca namenjene za borbu protiv forenzičke istrage – otežavanje, ili onemogućavanje te istrage.

Pored standardnih Windows programa za brisanje nekih tragova fajlova, dostupni su brojni, različiti specijalizovani softverski programi koji mogu uništiti dokaze. Na primer, **Tweak UI** je *Microsoft*-ov besplatan i dostupan program na Internetu, može se podesiti da skriva, ili briše potencijalne dokaze, na primer, dokumenta fajlova istorije, menja podrazumevanu lokaciju fajlova itd. Međutim, najveća pretnja za forenzičara su programi namenski pisani i dizajnirani da unište potencijalne dokaze, među kojima je najbolji ***Evidence Eliminator*,** koji briše gotovo sve tragove rada korisnika u računaru i ostavlja vrlo malo prostora za izvlačenje dokaza.

U PRILOGU 5 dat je pregled značajnijih web adresa za obuku i obrazovanje u oblasti digitalne forenzike i za druge forenzičkih resurse.

PITANJA ZA PONAVLJANJE

1. Kakve posledice ostavlja prepisivanje medija na forenzičko ispitivanje?
2. Šta se normalno može videti na prepisanom disku?
3. Do kojeg nivoa treba prepisivati disk da se dobije najbolji rezultat?
4. Kakve razlike ima višekratno prepisivanje podataka u odnosu na jednokratno prepisivanje za forenzički analizu?
5. Zašto forenzičar treba da prepiše podatke na medijumu za skladištenje forenzičkih podataka?
6. Navedite dva alata koja mogu izazvati probleme forenzičaru uklanjanjem tragova potencijalnih podataka?
7. Navedite neki broj oblasti iz kojih alat kao *Evidence Eliminator* može ukloniti tragove sumnjivog korišćenja?

KLJUČNI TERMINI

Adresiranje logičkim blokovima (LBA): posmatra disk u logičkim blokovima, koji počinju sa prvim seltorom (0) i nastavljaju do poslednjeg sektora.

Alokaciona jedinica fajla: grupa prostorno povezanih sektora, poznata takođe kao klaster.

Anti-forenzika: tehnika za brisanje, sakrivanje, ili uništavanje podataka, tako da im drugi ne mogu pristupiti.

Aplikacija: softver koji izvršava sepecifične funkcije ili daje individualni pristup servisima Intwereta/mreža.

ASCII kod: standard interpretacije bnarnog zapisa u računaru; reprezentuje svaki od 26 karaktera engleskog alfabeta kao broj od 0-256 (256 mogućih varijacija), pri čemu ASCII koristi 1 bajt po karakteru; brojevi 0-127 su standardni ASCI karakteri, a 128-256 je skup proširenih karaktera koji uključuje i slova glavnih svetskih jezika.

Bezbedni heš algoritam (*Secure Hash Algorithm***):** digitalni 160-bitni sažetak sadržaja fajla (NIST) dobijen jednosmernom funkcijom koja se lako računa u jednom, a teško ili nikakou drugom smeru; forenzički alat ***FTK*** koristi 180-bitni heš SHA-1, a KFF biblioteka sadrži brojne heš funkcije poznatih fajlova.

Binarni zapis: zapis podataka na čvrstom disku u formi binarnih 1 i 0.

BIOS (*Basic Input Output System*): osnovni ulazno-izlazni sistem izgrađen je u softveru uskladištenom u čipu ROM (*Read Only Memory*) memorije, obično locirane na glavnoj ploči; određuje šta računar može raditi bez instalacije OS; dovodi računar iz isključenog stanja u položaj gde instalirani OS može nastaviti *butovanje* sistema i obezbeđuje da svi drugi čipovi, procesori, portovi i povezani uređaji zajedno komuniciraju i funkcionišu.

Blokator upisivanja: alat koji sprečava upisivanje ili modifikaciju podataka na račnaru od svih priključenih medijuma za skladištenje.

Brisanje prepisivanjem (*Wiping*)**:** prepisivanje medijuma ili dela medijuma sa slučajnim ili konstantnim vrednostima (1 i 0) da bi se prebrisali stari podaci i pripremio medijum za sakupljanje podataka.

BUS (magistrala): podsistem u arhitekturi računara koji prenosi podatke ili napajanje između komponenti računara i može logički povezati nekoliko komponenti preko istog kola.

Butovanje sistema: proces podizanja sistema po završetku POS procesa iz sekvence za butovanje zapisane u CMOS i BIOSu.

Cilinder: svi tragovi postavljeni jedan ispod drugog, posmatrano sa gornje površine prve ploče pa do donje površine poslednje ploče HD.

CMOS (*Complimentary Metal Oxide Semiconductor*): tip integrisanog kola koji koristi vrlo malu snagu, emituje malo toplote za razliku od drugih čipova i klasifikovan je kao osetljiva memorija; da bi sačuvao podatke zahteva konstantno napajanje sa malom baterijom smeštenom na glavnoj ploči; sadrži i čuva sistemski datum i vreme, sekvencu butovanja, specifilaciju diska/drajva i pasvord.

Centralna procesrska jedinica-CPU*:* mikroprocesor koji interpretira i procesira instrukcije i podatke sadržane u softverskim aplikacijama i drugim komponentama.

Četovanje preko Interneta (*Internet Relay Chat* -IRC): Internet servis koji omogućava pojedincima širom sveta sinhronizovanu živu diskusiju, razmenu fajlova i privatne razgovore.

Defragmentacija: proces u kojem računar nastoji da sve fragmentirane (prostorno nepovezane) fajlove poveže u prostorno neprekinute celine; forenzičar može izgubiti neke podatke koji su mogli biti prepisani iz slobodnog i *slack* prostora u neki fajl, ali može dobiti neke podatke koji su privremeno memorisani tokom procesa defragmentacije.

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.

Direktorijum: organizaciona struktura fajl sistema, koja se koristi za grupisanje fajlova.

E-mail: servis koji omogućava ljudima da šalju poruke jedni drugima elektronskim putem.

Eternet: IEEE 802.3 *Ethernet Standard* lokalne računarske mreže; koristi CSMA/CD tehnologiju za kontrolu pristupa fizičkim medijima (*Ethernet* kablovi).

Fajl sistem: metod za imenovanje, skladištenje, organizaciju i pristupanje fajlovima na logičkom disku.

Fajl: kolekcija informacija logički grupisanih u jedan entitet i nazvani jedinstvenim imenom, kao što je ime fajla.

Fleš memorija: označava brzo i lako skladištenje podataka na različite digitalne, kompaktne uređaje bez pokretnih delova; mogu zadržati uskladištene podatke bez konstantnog napajanja.

Forenzička analiza: treća faza forenzičkog procesa ispitivanja računarskog sistema i mreže, koja uključuje korišćenje legalnih metoda i tehnika za derivaciju korisnih informacija koje su bile predmet sakupljanja u fazi pretrage.

Forenzički čist 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.

Formatiranje: proces koji uspostavlja sistemsku strukturu sektora na HD na najnižem nivou, polazeći sa prvog gornjeg diska, cilindar po cilindar sa spoljne strane diska prema centru; po završetku ovog procesa postavljeni su sektori na celom HD i svim njegovim površinama, a svaki sektor je jednozanačno referenciran sa CHS, ili LBA adresnim vrednostima; *sistemske* oblasti se razlikuju kod FAT16, FAT32 i NTFS fajl sistema.

Fragmentacija: prostorno nepovezani klasteri koje zauzima jedan te isti fajl na disku, zato što računar uvek ne može uskladištiti svaki fajl u prostorno povezane klastere iz brojnih razloga.

Glava za čitanje/pisanje: fizički elemenat za upisivanje/čitanje podataka na/sa diska.

Glavna particiona tabela (MPT): počinja od *ofseta* 446, računajući od početka MBR kôda i zauzima 66 bajta; počinje sa ulaznim bajtom „**80**“, a završava se potpisom MBR sektora – „**55 AA**“; sadrži maksimalno 4 a minimalno 1 ulaz (*entry*) od po 16 bajta; svaki ulaz sadrži važne informacije o nekoj particiji kao što su *tip, aktivnost, početak i kraj* particije; nekorišćeni ulaz je popunjen sa nulama; može sadržavati dva tipa particija: do 4 *primarne* i samo 1 *proširenu.*

Grafička karta: grafički adapteri koji obezbeđuju vizuelni prikaz rezultata rada računara na ekranu monitora; postoje tri tipa grafičkih adaptera: na glavnoj ploči, PCI i AGP.

Heder fajla: podaci unutar fajla koji sadrže informacije za identifikaciju fajla i moguće metapodatke sa informacijama o sadržajima fajla.

Heksadecimalni (*heks*) **zapis:** brojni sistem do vrednosti 16 koji koristi brojeve 0-9 i slova A-F koji zajedno daju 16 varijacija; skraćuje zapis od **4** bita u jedan broj od 1 ili 2 cifre; obezbeđuje efikasnije skladištenje podataka.

Hibernacija: stanje u Laptop računaru gde se računar isključuje da štedi energiju, ali memoriše stanje na desktopu i sve iz RAM-a na čvrsti disk pre isključivanja.

Ime fajla: jedinstveno ime koje se koristi da referencira fajl.

Jedinica za napajanje (PSU): snabdeva električnom energijom računar i njegove komponente, konvertujući naizmeničnu u jednosmernu struju potrebnu za rad komponenti računara.

Klaster: blokovi fiksne dužine prostorno povezanih sektora koji skladište fajlove; OS pripisuje svakom klasteru jedinstven broj.

Kolačići (*Cookies***):** mali programi koji nastaju kao rezultat pretraživanja *web* lokacija, namenjeni za prikupljanje informacija o aktivnostima korisnika na web-u.

Kompakt disk (CD): optički medijum za skladištenje digitalnih podataka; generalno se mogu klasifikovati u dve glavne kategorije: *samo za čitanje* (*Read Only*), ili fabrički presovane *za pisanje i čitanje* (*Recordable*).

Korisnički profil: važan je za digitalnog forenzičara, jer pokazuje ko je odgovoran za neke aktivnosti na računaru; sadrži *korisnički nalog*, i pasvord za logovanje sa definisanim ovlašćenjima za rad na objektima računarskog sistema; kreira se u *Controle Panel* pod *User Accounts*.

Korisnički definisano isključivanje računara: podrazumeva da sistem izvršava normalno isključivanje, ali na bazi neke predefinisane instrukcije vlasnika/korisnika izvršava neku operaciju nad podacima i fajlovima, pre nego što sistem izvrši normalno isključivanje.

Logički bekap: kopija direktorijuma i fajlova logičkog diska.

Logički disk: particija ili kolekcija particija koje deluju kao jedinstven entitet kojeg je fajl sistem formatirao.

MAC vremena: vremena modifikacije, pristupa i kreiranja fajlova u operativnom sistemu.

Master Boot Record (*MBR***):** zapis u prvom sektoru (0) na fizičkom disku, gde se upisuje kôd (*Master Bootstrap Loader Code)* za upisivanje MBR i **MPT** (*Master Partition Table)* koja sadrži informacije o organizaciji particija diska.

Mali kraj prvi (*Little Endian*): skladištenje bajta najnižeg reda u nizu na najnižoj adresi.

Metapodaci: podaci o podacima; za fajl sisteme metapodaci su podaci koji obezbeđuju informacije o sadržajima fajlova.

Modemi: tipično vrše DA i AD konverziju i koriste se za prenos digitalnih podataka preko telefonske linije.

Nasilno isključivanje računara: ostavlja bez promene sve što je bilo na čvrstom disku u vreme isključivanja i još uvek se smatra najboljim načinom isključivanja za digitalne forenzičare.

Nealocirani prostor: svi klasteri na disku koji nisu pripisani tekućem fajlu; često se naziva slobodan prostor; neki od ovih klastera još uvek može sadržavati podatke iz izbrisanih fajlova, koji još nisu prepisani sa drugim fajlovima.

Novinska grupa (*Newsgroups*): *Online* ekvivalent javne oglasne table (*public bulletin boards*), koji omogućava asinhrone komunikacije često slične diskusiji.

Normalno isključivanje računara: briše sve *bafere* (privremena skladišta) i privremene fajlove koje sistem koristi, zatvara sve tekuće procese i upisuje podatke u fajlove gde smatra potrebnim.

Operativni sistem: program koji radi na računaru i obezbeđuje rad svih komponenti sistema i softversku platformu na kojoj mogu raditi drugi programi; mogu se klasifikovati kao *višekorisnički*, *višeprocesorski*, *za više zadataka (multitascing)* i *'multi threading'***,** za konkurentan rad više različitih delova jednog programa.

Particija: logički deo medijuma koji funkcioniše kao da je fizički odvojen od drugih logičkih delova medijuma.

Particioniranje: po završetku formatiranja – postavljanja bazične strukture HD, za prepoznavanje ove strukture računar koristi program za deljenje diska na particije, kojima fajl sistem pripisuje slovo oznake C, D, E, itd, da bi ih sistem mogao prepoznati.

***Peer-to-Peer* mreža (P2P)**: računarska mreža u kojoj su svi računari međusobno direktno povezani.

Port: broj na osnovu kojeg TCP/IP identifikuje Internet servise/aplikacije; npr., TCP/IP e-mail aplikacija koristi port 25 a *Usenet* aplikacije koriste port 119.

POST proces: prva aktivnost uključenog računara; samotestiranje ispravnosti napajanja svih hardverskih komponenti računara; ugrađena dijagnostička aplikacija, koja proverava konfiguraciju i funkcionisanje hardverskih komponenti i proverava CMOS zapis.

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.

RAM (*Random Access Memory***) primarna memorija:** tip privremene memorije koju OS koristi da ubrza vezu između uređaja i aplikacija; zahteva konstantno napajanje da bi zadržao uskladištene podatke; CPU ima direktan pristup RAM-u i oni uzajamno čitaju i upisuju podatke.

RAID diskovi (*Redundant Array of Independent Disks*): sistem od više HD za deljenje, ili replikaciju podataka između diskova; kombinuje više fizičkih HD, obično iste veličine, u jedan logički, obezbeđuje jeftinije skladištenje podataka, veću pouzdanost i brzinu; tipično se koriste na serverima i obično koriste diskove iste veličine.

Registar: srce Windows 2000 i XP OS i može se smatrati repozitorijumom informacija koje se odnose baš na sve što se radi sa računarom; vrlo značajan izvor za forenzičara.

Sakupljanje: prva faza forenzičkog procesa računarskog sistema i mreže, koja uključuje identifikaciju, označavanje, snimanje i akvizicija podataka iz mogućih izvora relevantnih podataka na forenzički čist disk, sledeći proceduru i uputstva za zaštitu integriteta podataka; često se naziva *akvizicija* po najznačajnijem koraku; mogu biti hardverski i softverski, koji je manje pouzdan.

Sažetak poruke (*Message Digest***):** heš vrednost koja jedinstveno identifikuje podatke; promena jednog bita u podacima daje kompletno različit sažetak.

Sektor: kontinualni, linearni niz magnetisanih bita koji zauzima zakrivljenu sekciju traga; najmanja fizička jedinica za skladištenje na disku normalne veličine **512** bajta; fizički sektori se odnose na ceo disk, a logički na particiju.

***Slack* prostor:** nekorišćen prostor u bloku alociranog fajla, koji može sadržavati rezidualne podatke.

Slobodan prostor: oblast na medijumu, ili u memoriji koja nije alocirana (zauzeta) nekim fajlom.

Subdirektorijum: direktorijum koji se sadrži u drugom direktorijumu; često se naziva folder.

Veliki kraj prvi: skladištenje bajta najnižeg reda na najvišoj adresi.

LITERATURA

1. Access Data, *Forensic Toolkit*, http://www.accessdata.com, 2005.
2. Access Data, User Guide Forensic toolKit, 2006.
3. Analyst's Notebook, http://www.i2.co.uk, 2006.
4. ASR, *Data Acquisition and Analysis: SMART*, http://www.asrdata.com./.
5. Boyd Ch., Forster P., *Time and date issues in forensic computingda case study*, www.elsevier.com, 2004.
6. Carrier B., Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers, International Journal of Digital Evidence, Winter 2003.
7. Carrier B.**,** *File System Forensic Analysis*, Addison Wesley Professional, carrier@atstake.com, 2005.
8. Carrier B., *Open Source Digital Forensics Tools:The Legal Argument*, carrier@atstake.com, 2002.
9. Carvey H., *Windows Forensic Analysis DVD toolkit,* Syngress Publishing Inc., www.syngress.com, 2007.
10. Casey E., Error, *Uncertainty, and Loss in Digital Evidence*, International Journal of Digital Evidence, Summer 2002.
11. Casey E., Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition, Academic Press © 2004.
12. Forensic Information Technology Working Group**,** *Guidelines for best practice in the forensic examination of digital technology*, www.fitwg.com, 2003.
13. Grubor G., *Osnove Kompjuterskog kriminala*, skripta, Univerziitet Singidunum, Fakultet za poslovnu informatiku, 2006, Beograd.
14. *Guidance Software: EnCase Forensic Edition*, http://www.encase.com./.

15. http://www.iacis.org.
16. http://www.ojp.usdoj.gov/nij/pubs.htm.
17. Infinadyne*, CD/DVD Inspector*, www.infinadyne.com, 2006.
18. IOCE, *IOCE Princips & Definitions*, IOCE 2. Conference, London, 7. 10. 1999.
19. Isobuster, *Smart Projects*, www.isobuster.com, 2006.
20. James S., Nordby J., Forensic Science: An Introduction to Scientific and Investigative Techniques, CRC Press, 2003.
21. Jusoft, *BadCopy*, www.jufsoft.com/badcopy.
22. Kent K., Chevalier S., Grance T., Dang H.**,** *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800-86 , August 2006.
23. Lee H., and all, *Henry Lee's Crime Scene Handbook,* Academic Press, 2001.
24. National Policing Improvement Agency, Core *Skills in Data Recovery & AnalysisCourse Reference Book V2.01*, Bradford, UK, maj 2007.
25. 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.
26. NIST, *Secure Hash Standard*, FIPS PUB 180, maj 1993.
27. Pettinari D., Cmdr., Handling Digital Evidence from Seizure to Court Presentation, IOCE conference, juni 2000.
28. RFC 3227, sekcija 2.1, *Guidelines for Evidence Collection and Archiving,* www.faqs.org/rfcs/rfc3227.html, 2002.
29. Rivest R., *The MD5 Message-Digest Algorithm*, Network Working Group RFC 1321, april 1992.
30. Tan J., *Forensic Readiness*, Technical report, www.@stake, 2001.
31. *The Sleuth Kit*, http://www.sleuthkit.org, 2006.
32. Wiebe J., *Survey of Hardware Data Acquisition Tools*, CEOWiebeTech, www.www.wiebetechwiebetech.com.com
33. www.motherboards.org.

34. www.wykpedia.com.
35. www.knoppix.com.

UNIVERZITET AKREDITOVANI PRIVATNI UNIVERZITET SINGIDUNUM

PRILOG I

Procedura ispitivanja čvrstih diskova

Asocijacija *IACIS* (*International Association of Computer Investigative Specialists)* preporučuje sledeću proceduru za forenzičko ispitivanje kompjuterskih čvrstih diskova (HD) i drugih fizičkih medija:

1. Uspostaviti forenzički sterilne uslove. Svi mediji koji se korite za ispitivanje moraju biti sveže pripremljeni, potpuno izbrisani od nebitnih podataka, skenirani na viruse i verifikovani pre upotrebe;
2. Svi korišćeni forenzički softverski alati moraju biti licencirani, a istražni organ (pojedinac, agencija) ovlašćen za njegovu upotrebu;
3. Orginalni (ispitivani) kompjuter se fizički analizira. Pravi se specifični opis hardvera i zapisuje sa komentarima, koji indiciraju sve neuobičajene nalaze u toku fizičke analize računara;
4. Preduzimaju se sve mere predostrožnosti u toku kopiranja ili pristupa orginalnim medijima, da bi se sprečio unos virusa, destruktivnih programa ili drugih nenamernih upisa na/sa orginalnih medija. Poznato je da zbog hardverskog i ograničenja OS ovo nije uvek moguće;
5. Proverava se i notira sadržaj CMOS i korektnost datuma i vremena internog kloka. Vreme i datum internog časovnika je vrlo važno za uspostavljanje sistema kreiranja fajlova i logovanja kompjuterskih događaja.
6. Orginalni mediji se normalno ne koriste za analizu. Treba napraviti kopiju zapisa bitova ili neku drugu sliku originalnih medija. Ove kopije se normalno koriste za stvarno ispitivanje (analizu). Notira se detaljan opis kopije podataka ili procesa uzimanja miror slike i identifikuju hardver, softver i mediji.
7. Kopija ili fizička slika orginalnog HD logički se ispituje i registruje se opis rezultata.

8. Ispituju se podaci fajlove za butiranje, korisnički definisanog sistema konfiguracije i fajlove operativnih komandi, kao što su CONFIG.SYS i AUTOEXEC.BAT, a rezultati se registruju.
9. Sve izbrisane fajlove koje se mogu oporaviti restauriraju se. Kada je to praktično i moguće, prvi karakter naziva restauriranih fajlova se menja u cilju kasnije identifikacije.
10. Normalno se pravi listing svih fajlova sa ispitivanih medija, bez obzira da li sadrže potencijalne dokaze ili ne.
11. Ako je prikladno, *nelocirani* prostor se ispituje na izgubljene/skrivene podatke.
12. Ako je prikladno, *slack* prostor se ispituje na izgubljene/skrivene podatke.
13. Ispituje se sadržaj svake fajlove korisničkih podataka u rut direktorijumu i svakom poddirektorijumu (ako postoji).
14. Zaštićene fajlove za čuvanje pasvorda otvaraju se i ispituju.
15. Štampani materijal, ili kopije prave se za sve očigledno dokazne podatke. Fajlova ili lokacija gde se dobije bilo koji dokazni podatak notira se na svakom štampanom materijalu. Svi štampani materijali označavaju se, sekvencijalno numerišu i propisno čuvaju i prenose.
16. Treba ispitati izvršne programe od specifičnog interesa. Fajlove korisničkih podataka do kojih se ne može pristupiti drugim sredstvima, ispituju se ovaj put korišćenjem postojećih (*native*) aplikacija u OS.
17. Propisno se dokumentuju svi komentari i nalazi forenzičara.

Procedura ispitivanja pokretnih medijuma

1. Uspostaviti forenzički sterilne uslove. Sve medije koji se koriste u procesu ispitivanja, potpuno izbrisati od podataka višestrukim prepisivanjem (*wiping*), skenirati na viruse i verifikovati pre upotrebe;
2. Svi korišćeni forenzički softverski alati moraju biti licencirani, a istražni organ (pojedinac, kompanija) ovlašćen za njegovu upotrebu;

3. Mediji se fizički ispituju, specifični opisi zapisuju i e markiraju radi identifikacije;
4. Preduzimaju se sve mere predostrožnosti u toku kopiranja ili pristupa orginalnim medijima da bi se sprečio unos virusa, destruktivnih programa ili drugih nenamernih upisa na/sa orginalnih pokretnih medija;
5. Testira se na forenzičkom računaru mogućnost zaštite pokretnog medija od upisivanja;
6. Pravi se fizički duplikat pokretnog medija, zaštićenog od snimanja na drugi pokretni (forenzički) medij, koji se koristi za aktuelno ispitivanje. Zapisuje se detaljan opis procesa;
7. Kopija ispitivanog medija logički se ispituje i zapisuje se opis nađenih rezultata, uključujući i sve što je neobično;
8. Podaci fajlove za butiranje, korisnički definisanog sistema konfiguracije i fajlove operativnih komandi (ako postoje), ispituju se, a rezultati se zapisuju.
9. Sve izbrisane fajlove koje se mogu oporaviti restauriraju se. Kada je to praktično ili moguće, prvi karakter restauriranih fajlova se menja u cilju kasnije identifikacije.
10. *Nelocirani* prostor ispituje se na izgubljene/skrivene podatke.
11. *Slack* prostor svake fajlove ispituje se na izgubljene/skrivene podatke.
12. Sadržaj svake fajlove korisničkih podataka u rut direktorijumu i svakom podirektorijumu (ako postoji) mora biti ispitan.
13. Zaštićene fajlove za čuvanje pasvorda otvaraju se i ispituju.
14. Ako pokretni medij sadrži očigledno dokazne podatke koji se mogu iskoristiti, pravi se listing za sve fajlove mediju, bez obzira da li sadrže očigledne dokazne podatke ili ne. Listing će indicirati koje fajlove su bile štampane, kopirane ili oporavljane.
15. Štampani materijal ili kopije prave se za sve očigledno dokazne podatke. Fajlova ili lokacija gde se dobije bilo koji očigledno dokazni podatak notira se na svakom štampanom materijalu. Svi štampani

materijali se označavaju, sekvencijalno numerišu i propisno čuvaju i prenose.

16. Treba ispitati izvršne programe od specifičnog interesa. Fajlove korisničkih podataka do kojih se ne može pristupiti drugim sredstvima, ispituju se ovaj put korišćenjem postojećih (*native*) aplikacija.
17. Propisno treba dokumentovati sve komentare i nalaze digitalnog forenzičara.

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

PRILOG II

Skraćena lista poznatijih Trojanaca za postavljanje zadnjih vrata

✓ **BackOrifice/BackOrifice 2000(BO2K).** Back Orifice (or BO2K) is probably the most advanced Trojan in circulation and requires a steep learning curve, making it the most difficult to put in place.

✓ **Back Construction.** This very rare backdoor lets the hacker have access to a system's hard disks. It always runs on port 5400, so it is advised that users simply block that port on their firewalls.

✓ **Barok.** This Trojan gathers dialup passwords and sends them to the hacker. The simple way to defend against the Barok: Don't select the option "Always remember my password" in password boxes.

✓ **Blade Runner.** This sophisticated Trojan is geared more toward the abilities of savvy system crackers as it contains components that are beyond the skills of average hackers.

✓ **Cyn.** This particular Trojan is similar in form and features to the SubSeven; however it includes an additional feature that allows a hacker to reset the system CMOS.

✓ **Deepthroat.** Deepthroat is a simple-to-use Trojan and has almost as many options as the SubSeven.

✓ **Girlfriend.** There isn't much to distinguish this Trojan, as it contains the standard features common to most Trojan backdoors. Most respectable firewalls can block Girlfriend.

✓ **Hack'a'Tack.** This easy-to-use and colorful remote-control Trojan is actually quite rare. Since this Trojan always runs on port 31787, it is relatively easy to defend against by just blocking access to port 31787 at the firewall.

✓ **SchoolBus.** This common Trojan is powerful despite its simplicity. It even boasts a builtin scanner and operates using port 54321 by default.

✓ **SubSeven (a.k.a. Backdoor-G).** With its small learning curve and numerous features, SubSeven is probably the most popular (from the hacker's standpoint) and powerful Trojan horse. The SubSeven Trojan can be configured to inform someone when the computer it has infected connects to the Internet. The hacker (who infected the system with the SubSeven) is then provided with information he or she may use against the system or organization.

UNIVERZITET PRIVATNI AKREDITOVANI UNIVERZITET SINGIDUNUM

PRILOG III

Najčešće napadani portovi

Sledeća tabela pokazuje primere najčešće napadanih portova korišćenih od stane hakera i Trojanaca. Ako zapazite da neko pokušava pingovati portove koji se normalno ne koriste, verovatno napadač pokušava da instalira Trojanca u mrežu. Treba znati da se neki Trojanci mogu konfigurisati da koriste bilo koji port, pa su ovde navedeni portovi koji se koriste po difoltu. Poznavanje ovih uobičajenih napada pomaže forenzičaru da lakše prati trag napadača i pomažu bolju zaštitu od sledećeg napada.

Tabela 13.1 Trojan portovi

Port #	Protokol	Opis
0	ICMP	Click attack
8	ICMP	Ping Attack
9	UDP	Chargen
19	UDP	Chargen
21	TCP	FTP service, Dolly Trojan
23	TCP	TELNET Service
25	TCP	SMTP, AntiGen
31	TCP	Agent 31, Hacker's Paradise
41	TCP	Deep Throat
53	TCP	DNS
58	TCP	DM Setup
79	TCP	Firehotcker
80	TCP	Executor
90	TCP	Hidden Port 2.o
110	TCP	ProMail Trojan
113	TCP	Kazimas

119	TCP	Happy99
121	TCP	Jammer Killah
129	TCP	Password Generator Protocol
135	TCP UDP	Netbios Remote procedure call
137	TCP UDP	Netbios name (DoS attacks)
138	TCP UDP	Netbios datagram
139	TCP UDP	Netbios session (DoS attacks)
146	TCP	Infector 1.3
421	TCP	Tcp Wrappers
456	TCP	Hacker's Paradise
531	TCP	Rasmin
555	TCP	Stealth Spy, Phaze
666	TCP	Attack FTP
777	TCP	AIM Spy Application
911	TCP	Dark Shadow
999	TCP	DeepThroat
9400	TCP	InCommand
9999	TCP	The prayer 1.2 -1.3
1000	TCP	Der Spaeher
1001	TCP	Silencer, WebEx
1011	TCP	Doly Trojan
1012	TCP	Doly Trojan
1015	TCP	Doly Trojan
1024	TCP	NetSpy
1025	UDP	Maverick's Matrix 1.2 - 2.0
1027	TCP	ICQ
1029	TCP	ICQ

1032	TCP	ICQ
1033	TCP	NetSpy
1042	TCP	Bla
1045	TCP	Rasmin
1080	TCP	Socks/Wingate
1090	TCP	Xtreme
1170	TCP	Voice Streaming Audio
1207	TCP	SoftWar
1214	TCP	KaZaa File Sharing (not a trojan)
1234	TCP	Ultors Trojan
1243	TCP	Sub Seven
1245	TCP	VooDoo Doll
1269	TCP	Maverick's Matrix
12631	TCP	WhackJob
1349	UDP	BackOrifice DLL Comm
1394	TCP	GoFriller, Backdoor G-1
1492	TCP	FTP99CMP
1505	TCPUDP	FunkProxy
1509	TCP	Psyber Streaming server
1600	TCP	Shivka-Burka
1604	TCP UDP	ICA Browser
1807	TCP	SpySender
1981	TCP	Shockrave
1999	TCP	BackDoor
2000	TCP	Remote Explorer
2001	TCP	Trojan Cow
2002	TCP	TransScout

2003	TCP	TransScout
2004	TCP	TransScout
2005	TCP	TransScout
2023	TCP	Ripper
2115	TCP	Bugs
2140	TCP	Deep Throat
2140	UDP	Deep Throat
2155	TCP	Illusion Mailer
2283	TCP	HLV Rat5
2565	TCP	Striker
2583	TCP	WinCrash
2716	TCP	The Prayer 1.2 -1.3
2721	TCP	Phase Zero
2801	TCP	Phineas Phucker
2989	UDP	Rat
3024	TCP	WinCrash
3028	TCP	Ring Zero
3129	TCP	Master's Paradise
3150	TCP	Deep Throat
3150	UDP	Deep Throat
3332	TCP	Q0 BackDoor
3459	TCP	Eclipse 2000
3700	TCP	Portal of Doom
3791	TCP	Eclypse
3801	UDP	Eclypse
4100	TCP	Watchguard Firebox admin DoS Expl
4092	TCP	WinCrash

4567	TCP	File Nail
4590	TCP	ICQ Trojan
5000	TCP	Sokets de Trois v1./Bubbel
5001	TCP	Sokets de Trois v1./Bubbel
5011	TCP	Ootlt
5031	TCP	Net Metropolitan 1.0
5032	TCP	Net Metropolitan 1.04
5321	TCP	Firehotcker
5400	TCP	Blade Runner
5401	TCP	Blade Runner
5402	TCP	Blade Runner
5521	TCP	Illusion Mailer
5550	TCP	Xtcp
5512	TCP	Xtcp
5555	TCP	ServeMe
5556	TCP	BO Facil
5557	TCP	BO Facil
5569	TCP	Robo-Hack
5637	TCP	PC Crasher
5638	TCP	PC Crasher
5714	TCP	WinCrash
5741	TCP	WinCrash
5742	TCP	WinCrash
6000	TCP	The Thing 1.6
6112	TCP UDP	Battle.net Game (not a trojan)
6346	TCP	Gnutella clone (not a trojan) see info
6400	TCP	The Thing

6667	TCP	Sub-7 Trojan (new icq notification)
6669	TCP	Vampyre
6670	TCP	Deep Throat
6671	TCP	Deep Throat
6711	TCP	Sub Seven
6712	TCP	Sub Seven
6713	TCP	Sub Seven
6723	TCP	Mstream attack-handler
6771	TCP	Deep Throat
6776	TCP	Sub Seven
6838	UDP	Mstream Agent-handler
6912	TCP	Sh*t Heap
6939	TCP	Indoctrination
6969	TCP	Gate Crasher, Priority
6970	TCP	Gate Crasher
7000	TCP	Remote Grab
7028	TCP	Unknown Trojan
7028	UDP	Unknown Trojan
7300	TCP	Net Monitor
7301	TCP	Net Monitor
7306	TCP	Net Monitor
7307	TCP	Net Monitor
7308	TCP	Net Monitor
7597	TCP	QaZ (Remote Access Trojan)
7789	TCP	ICKiller
7983	UDP	MStream handler-agent
8080	TCP	Ring Zero

8787	TCPUDP	BackOrifice 2000
8879	TCPUDP	BackOrifice 2000
9325	UDP	MStream Agent-handler
9872	TCP	Portal of Doom
9873	TCP	Portal of Doom
9874	TCP	Portal of Doom
9875	TCP	Portal of Doom
9876	TCP	Cyber Attacker
9878	TCP	Trans Scout
9989	TCP	iNi-Killer
10008	TCP	Cheese worm
10067	TCP	Portal of Doom
10067	UDP	Portal of Doom
10167	TCP	Portal of Doom
10167	UDP	Portal of Doom
10498	UDP	Mstream handler-agent
10520	TCP	Acid Shivers
10607	TCP	Coma
10666	TCP	Ambush
11000	TCP	Senna Spy
11050	TCP	Host Control
11223	TCP	Progenic Trojan
11831`	TCP	Latinus Server
12076	TCP	GJamer
12223	TCP	Hack'99, KeyLogger
12345	TCP	Netbus, Ultor's Trojan
12346	TCP	Netbus

12456	TCP	NetBus
12361	TCP	Whack-a-Mole
12362	TCP	Whack-a-Mole
12631	TCP	Whack Job
12701	TCP	Eclypse 2000
12754	TCP	Mstream attack-handler
13000	TCP	Senna Spy
13700	TCP	Kuang2 the Virus
15104	TCP	Mstream attack-handler
16484	TCP	Mosucker
16959	TCP	SubSeven DEFCON8 2.1 Backdoor
16969	TCP	Priority
17300	TCP	Kuang2 The Virus
18753	UDP	Shaft handler to Agent
20000	TCP	Millennium
20001	TCP	Millennium
20034	TCP	NetBus 2 Pro
20203	TCP	Logged!
20331	TCP	Bla Trojan
20432	TCP	Shaft Client to handlers
20433	TCP	Shaft Agent to handlers
21554	TCPUDP	GirlFriend
22222	TCP	Prosiak
23456	TCP	EvilFTP, UglyFTP
23476	TCP	Donald Dick
23477	TCP	Donald Dick
26274	TCP	Delta Source

26274	UDP	Delta Source
27374	UDP	Sub-7 2.1
27444	UDP	Trin00/TFN2K
27573	UDP	Sub-7 2.1
27573	TCP	Sub-7 2.1
27665	TCP	Trin00 DoS Attack
29559	TCP	Latinus Server
29891	TCP	The Unexplained
30029	TCP	AOL Trojan
30100	TCP	NetSphere
30101	TCP	NetSphere
30102	TCP	NetSphere
30133	TCP	NetSphere Final
30303	TCP	Sockets de Troie
30999	TCP	Kuang2
31335	UDP	Trin00 DoS Attack
31336	TCP	BO-Whack
31337	UDP	Backorifice (BO)
31337	TCP	Netpatch
31338	TCP	NetSpy DK
31338	UDP	Deep BO
31339	TCP	NetSpy DK
31666	TCP	BOWhack
31785	TCP	Hack'a'Tack
31787	UDP	Hack`a'Tack
31789	UDP	Hack'a'Tack
31790	UDP	Hack`a'Tack

31791	UDP	Hack'a'Tack
32418	TCP	Acid Battery
33270	TCP	Trinity Trojan
33333	TCP	Prosiak
33390	UDP	Unknown trojan
33911	TCP	Spirit 2001 a
34324	TCP	BigGluck, TN
37651	TCP	Yet Another Trojan
40421	TCP	Master's Paradise
40412	TCP	The Spy
40421	TCP	Agent, Master's of Paradise
40422	TCP	Master's Paradise
40423	TCP	Master's Paradise
40425	TCP	Master's Paradise
40426	TCP	Master's Paradise
43210	TCP	Master's Paradise
47252	TCP	Delta Source
47262	UDP	Delta Source
49301	UDP	OnLine keyLogger
50505	TCP	Sokets de Trois v2.
50776	TCP	Fore
53001	TCP	Remote Windows Shutdown
54320	TCP	Back Orifice 2000
54320	UDP	Back Orifice
54321	TCP	School Bus, Back Orifice
54321	UDP	Back Orifice 2000
57341	UDP	NetRaider Trojan

57341	TCP	NetRaider Trojan
60000	TCP	Deep Throat
61466	TCP	Telecommando
61348	TCP	Bunker-Hill Trojan
61603	TCP	Bunker-Hill Trojan
63485	TCP	Bunker-Hill Trojan
65000	TCP	Stacheldraht, Devil
65555	KP	Adore Worm/Linux

Tabela 13.2 Izvori za obuku iz digitalne forenzike

Naziv izvora za obuku	**URL**
CompuForensics	http://www.compuforensics.com/training.htm
Computer Forensic Services	http://www.computer-forensic.com/training.html
Computer Forensics Training Center Online	http://www.cftco.com/
Federal Law Enforcement Training Center (FLETC), Computer & Financial Investigations (CFI) Division	http://www.fletc.gov/cfi/index.htm
Foundstone	http://www.foundstone.com/
IACIS	http://www.iacis.info/iacisv2/pages/training.php
InfoSec Institute	http://www.infosecinstitute.com/courses/computer_forensics_training.html
MIS Training Institute (MISTI)	http://www.misti.com/
New Technologies Inc. (NTI)	http://www.forensics-intl.com/training.html
NW3C	http://www.nw3c.org/ocr/courses_desc.cfm
SANS Institute	http://www.sans.org/

Tabela 13.3 Dodatna tehnička dokumentacija za obuku iz digitalne forenzike

Naziv izvora	**URL**
Basic Steps in Forensic Analysis of Unix Systems, by Dave Dittrich	http://staff.washington.edu/dittrich/misc/forensics/

Naziv izvora	URL
Computer Forensics: Introduction to Incident Response and Investigation of Windows NT/2000, by Norman Haase	http://www.sans.org/rr/whitepapers/incident/647.php
Digital Investigation: The International Journal of Digital Forensics & Incident Response	http://www.compseconline.com/digitalinvestigation/
Electronic Crime Scene Investigation: A Guide for First Responders	http://www.ncjrs.gov/
Evidence Seizure Methodology for Computer Forensics, by Thomas Rude	http://www.crazytrain.com/seizure.html
Forensic Analysis of a Live Linux System, by Mariusz Burdach	http://www.securityfocus.com/infocus/1769 (part one), http://www.securityfocus.com/infocus/1773 (part two)
How to Bypass BIOS Passwords	http://labmice.techtarget.com/articles/BIOS_hack.htm
International Journal of Digital Evidence	http://www.utica.edu/academic/institutes/ecii/ijde/
NIST Interagency Report (IR) 7100, PDA Forensic Tools: An Overview and Analysis	http://csrc.nist.gov/publications/nistir/index.html
NIST IR 7250, Cell Phone Forensic Tools: An Overview and Analysis	http://csrc.nist.gov/publications/nistir/index.html
NIST SP 800-31, Intrusion Detection Systems	http://csrc.nist.gov/publications/nistpubs/index.html
NIST SP 800-44, Guidelines on Securing Public Web Servers	http://csrc.nist.gov/publications/nistpubs/index.html
NIST SP 800-45, Guidelines on Electronic Mail Security	http://csrc.nist.gov/publications/nistpubs/index.html
NIST SP 800-61, Computer Security Incident Handling Guide	http://csrc.nist.gov/publications/nistpubs/index.html
NIST SP 800-72, Guidelines on PDA Forensics	http://csrc.nist.gov/publications/nistpubs/index.html
NIST SP 800-83, Guide to Malware Incident Prevention and Handling	http://csrc.nist.gov/publications/nistpubs/index.html
An Overview of Steganography for the Computer Forensic Examiner, by Gary Kessler	http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm
RFC 3164: The BSD Syslog Protocol	http://www.ietf.org/rfc/rfc3164.txt
RFC 3227: Guidelines for Evidence Collection and Archiving	http://www.ietf.org/rfc/rfc3227.txt