

Digitalna forenzika

Andrej Brodnik

Andrej Brodnik: Digitalna forenzika

Računalnik

poglavlje 15

- pričakovano predznanje:
 - arhitektura računalnikov
 - osnove delovanja (BIOS)
 - operacijski sistem
 - sekundarni pomnilnik (disk) in njegova organizacija
 - datotečni sistemi

Andrej Brodnik: Digitalna forenzika

Zagon računalnika

- koraki ob zagonu računalnika
- ob zagonu se sproži BIOS (*Basic Input Output System*)
 - Open Firmware (Mac PowerPC), EFI (Mac Intel), Open Boot PROM (Sun), ...
- ta naredi POST (*Power On Self Test*)
- podatki o delovanju so shranjeni v xROM
- včasih geslo ščiti podatke – dobiti geslo od uporabnika

Andrej Brodnik: Digitalna forenzika

Zagon računalnika ...

- primer *Moussawi*:

Računalnik je bil zelo dolgo shranjen in se je spraznila baterija na matični plošči.
Dostop bil mogoč s pomočjo podatkov, ki jih so jih pridobili še pred tem, ko je zmanjkal napajanja.

- pomembno kako so podatki kodirani
 - ASCII, ...
 - tanki debeli konec
- kaj se zgodi, če odnesete disk na drug računalnik

Andrej Brodnik: Digitalna forenzika

Format datoteke

- datoteke imajo na začetku posebne podpise (www.garykessler.net/library/file_sigs.html)
- jpg: FF D8 FF E0, ali FF D8 FF E1
- gif: 47 49 46 38 37 61 ali 47, ali 49 46 38 39 61
- doc: DO CF 11 E0 A1 B1 1A E1

Andrej Brodnik: Digitalna forenzika

Format datoteke –primer

- jpeg zakodirana exif (Exchangeable image file format) datoteka

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	FF	D8	FF	E1	16	B1	45	78	69	66	00	00	4D	4D	00	2A
00000010	00	00	00	08	00	08	05	01	0F	00	02	00	00	16	00	00
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	03	00	00	00	01	00	01	00	00	01	1A	00	05	00	00
00000040	00	01	00	00	01	E4	01	1B	00	05	00	00	01	00	00	00
00000050	00	00	00	00	00	00	28	00	00	00	00	00	00	00	13	1
00000060	00	03	00	00	00	01	00	01	00	00	07	69	00	00	00	00
00000070	00	01	00	00	01	F4	00	00	09	34	00	00	00	00	00	00
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000120	41	4E	59	00	49	4F	41	41	48	24	44	58	34	33	33	30
00000130	00	44	49	47	49	54	41	4C	20	44	41	4D	45	52	41	30
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000200	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000210	00	05	00	00	01	00	00	03	E0	88	22	00	03	00	00	00
00000220	00	01	00	02	00	00	90	00	00	07	22	00	04	30	32	02
00000230	32	30	90	03	00	02	80	00	00	1A	00	00	03	EA	90	04

Andrej Brodnik: Digitalna forenzika

Format datoteke

- datoteka je lahko gnezdena v drugi datoteki
 - poiščemo datoteko
 - jo lahko označimo in prepišemo (*copy-paste*)
 - ali uporabimo orodje **dd**
- temu postopku rečemo obrezovanje / klesanje (*carving*)
- druga orodja:
 - scalpel (<http://www.digitalforensicssolutions.com/Scalpel/>), DataLifter (<http://www.datalifter.com/>)
 - EnCase (<http://www.guidancesoftware.com/forensic.htm>), FTK (Forensic Toolkit, <http://accessdata.com/products/computer-forensics/ftk>), X-Ways (<http://www.x-ways.net/>)

Andrej Brodnik: Digitalna forenzika

Izrezovanje

- na koncu dobimo samo vsebino in ne meta-podatkov iz imenika
- drugi problem je, da so lahko podatki razmetani po disku
 - Adroit (<http://digital-assembly.com/products/adroit-photo-forensics/>)

Andrej Brodnik: Digitalna forenzika

Format datoteke – izziv

- **Izziv:** vgnezdzite v eno datoteko drugo datoteko ter jo objavite na forumu. Nato naj drugi kolegi poiščejo vgnezdeno datoteko ter jo izluščijo. Pri tem uporabite orodje dd ali kakšno od orodij omenjenih na prejšnji strani.
- **Izziv:** sedaj pa razpršite datoteko v več kosov in vsakega vstavite v drugo datoteko ter vse objavite na forumu. Ponovno naj kolegi poiščejo vaše porazdeljene kose.

Andrej Brodnik: Digitalna forenzika

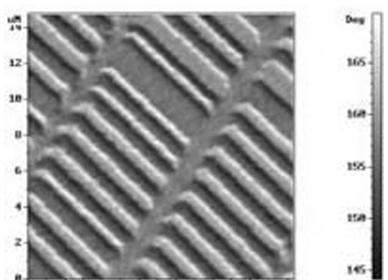
Shramba podatkov in skrivanje

- V/I enote so priključene na računalnik preko:
 - vodila (IDE, ATA, SATA; SCSI, firewire)
 - vmesnika (*controller*)
- vmesniki so lahko tudi pametni
 - SMART (*Self-Monitoring, Analysis, and Reporting Technology*)
 - hrani statistike dostopov in ostali podobni podatki
 - običajno niso pomembni za forenzično raziskavo

Andrej Brodnik: Digitalna forenzika

Shramba podatkov in skrivanje

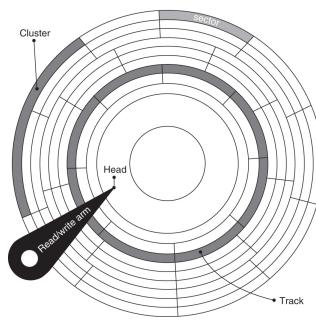
- podatke trajno običajno hranimo na disku
- kako izgleda trdi disk?



Andrej Brodnik: Digitalna forenzika

Shramba podatkov in skrivanje

- kako je organiziran disk?
 - plošče, sledi (cilindri), sektorji, gruče
- na prvi sledi, prvem sektorju so nadzorni podatki (MBR, *master boot record*)
 - velikost (geometrija), slabi bloki, particije, ...
- kako izgleda organizacija pri SSD?



Andrej Brodnik: Digitalna forenzika

Shramba podatkov in skrivanje

- Izviv: poiščite orodje anadisk in poglejte kaj zna in zmora početi.
- Izviv: kakšna je struktura MBR? Sestavite svoj MBR in ga objavite v forumu.

Andrej Brodnik: Digitalna forenzika

Shramba podatkov in skrivanje

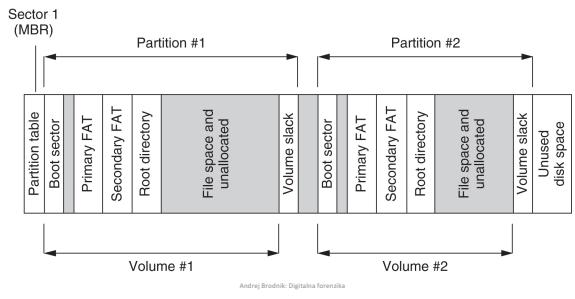
- pogled v boot sektor Windows95 stroja z orodjem Norton DiskUtils



Andrej Brodnik: Digitalna forenzika

Shramba podatkov in skrivanje

- poenostavljena organiziranost diska z datotečnim sistemom FAT



Andrej Brodnik: Digitalna forenzika

Shramba podatkov in skrivanje

- particija, volumen, snopič/del
- v njej datotečni sistem
- lahko tudi brez datotečnega sistema

Andraž Brodnik: Digitalna forenzika

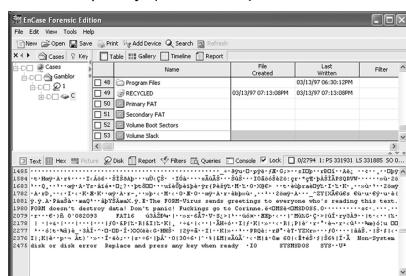
Shramba podatkov in skrivanje

- skrivanje podatkov zaradi notranje in zunanje fragmentacije:
 - skrivanje znotraj sektorja (bloka) – težko in neobičajno
 - skrivanje znotraj gruče
 - skrivanje znotraj particije (particije se običajno začnejo na začetku sledi)
 - skrivanje particije
- kriptiranje particije
- servisni podatki: DCO (*Drive/device configuration overlay*) in HPA (*Host/hidden protected area*) – http://www.forensicswiki.org/wiki/DCO_and_HPA

Andraž Brodnik: Digitalna forenzika

Shramba podatkov in skrivanje

- virus skrit v praznem koncu particije (*volume slack*)



The screenshot shows the EnCase Forensic Edition interface with a list of files in the 'Volume Slack' section. The list includes:

Name	File Created	Last Written
48 Program Files	03/13/97 06:30:19PM	
49 RECOVERY.PAT	03/13/97 07:13:08PM	
50 RECOVERY.PAT	03/13/97 07:13:08PM	
51 Secondary FAT		
52 Volume Boot Sectors		
53 Volume Slack		

Andraž Brodnik: Digitalna forenzika

Shramba podatkov in skrivanje

- ko je datoteka izbrisana, podatki ne izginejo
- tudi, ko formatiramo disk, podatki ne izginejo
 - poglejte orodje **fdisk**
- rezultat obeh operacij je pravilen datotečni sistem in kopica praznih blokov
- orodja: **sleuthkit** (<http://www.sleuthkit.org/>), Norton DiskEdit, ...

Andrej Brodnik: Digitalna forenzika

Shramba podatkov in skrivanje

- primer rekonstrukcije datotek na sveže formatiranem disku z orodjem EnCase

2	X readmeen.txt	01/04/04 11:19:02AM	
3	X readmefr.txt	01/04/04 11:18:56AM	
4	X src.zip	01/04/04 11:18:44AM	
5	X hxdef100.ini	12/31/03 10:17:36AM	
6	X hxdef100.2.ini	12/31/03 10:17:14AM	
7	Ø bdcli100.exe	12/31/03 10:16:02AM	
8	X rdbbs100.exe	12/31/03 10:15:50AM	
9	X hxdef100.exe	12/31/03 10:15:34AM	
10	Ø src.zip.Zone.Identifier		
11	Ø hxdef100.ini.Zone.Identifier		
12	Ø readmeen.txt.Zone.Identifier		
13	Ø hxdef100.exe.Zone.Identifier		
14	Ø readmeen.txt.Zone.Identifier		
15	Ø hxdef100.2.ini.Zone.Identifier		

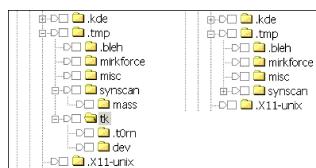
Shramba podatkov in skrivanje

- **Izziv:** poglejte kako izgleda MBR in boot sektor na vašem računalniku z ustreznim orodjem. Poročajte o tem na forumu.
- **Izziv:** preverite konfiguracijo vašega diska.

Andrej Brodnik: Digitalna forenzika

Skrivanje podatkov

- skrivanje particij
 - orodje Test Disk (<http://www.cgsecurity.org/>)
- na ravni datotek
 - skrivanje datotek: npr. MS Windows: *attrib +H* in *dir/AH*
 - parlament.jpg -> test.exe
 - sliko v predstavitev (ppt)
- najnovejša orodja



Andrej Brodnik: Digitalna forenzika

Gesla in kriptiranje

- orodja za razbijanje in iskanje gesel
 - Password Recovery Tool – PRTK in Distributed Network Attack – DNA (<http://accessdata.com/products/computer-forensics/decryption>)
 - John the Ripper (www.openwall.com/john/)
 - Cain and Abel (www.oxid.it/caim.html)
 - Advanced Archive Password Recovery (www.elcomsoft.com/azpr.html)

Andrej Brodnik: Digitalna forenzika

Gesla in kriptiranje

- več o kriptiranju in kriptografiji kasneje
- nekaj primerov
 - orodje caesar, rot13
 - podpora za PGP
 - orodje crypt

Andrej Brodnik: Digitalna forenzika

OS Windows

poglavlje 17

- datotečni sistemi
- reševanje podatkov
- zabeležke (*log files*)
- register
- komunikacijske sledi

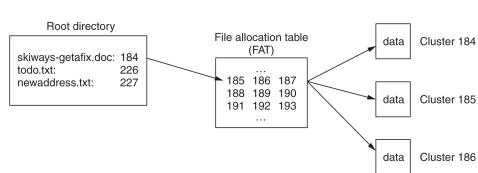
Andrej Brodnik: Digitalna forenzika

OS Windows – datotečni sistemi

- dva osnovna datotečna sistema FAT (*File Allocation Table*) in NTFS (*New Technology File System*)
- FAT
 - razvit najprej za gibke diske (diskete)
 - FAT12, FAT16, FAT32

Andrej Brodnik: Digitalna forenzika

Datotečni sistem FAT



- FATxx je povezan seznam indeksov gruč, v katerih je shranjena posamezna datoteka
- xx pomeni število bitov uporabljenih za indeks
- $12 = 2^{12} = 4096$, $16 = 2^{16} = 65.536$, $32 = 2^{28} = 268.435.456$

Andrej Brodnik: Digitalna forenzika

Datotečni sistem FAT

Name	Type	Size	Created	Modified	Accessed	Attr.	1st sector
(Root directory)		0.0 KB				18	
apid	do	0.5 KB	05/08/2003 14:41:44	05/08/2003 14:41:44	05/08/2003	188	
greenfield.do	do	19.5 KB	05/08/2003 14:43:00	05/08/2003 14:34:16	05/12/2003	A	306
contacts.xls	xls	16.5 KB	05/08/2003 14:43:15	02/18/2001 12:49:16	05/12/2003	RA	345
sklajways-gefax.doc	doc	21.0 KB	05/13/2003 12:32:00	05/13/2003 11:58:10	05/13/2003	A	215
todo.txt	txt	1.0 KB	05/13/2003 12:37:54	05/13/2003 12:40:48	05/13/2003	A	257
newaddress.txt	txt	1.2 KB	05/13/2003 12:42:17	05/13/2003 12:42:18	05/13/2003	A	258
Boot sector		0.5 KB				0	
FAT 1		4.5 KB				1	
FAT 2		4.5 KB				10	
Free space		1.4 MB					
Ide space							

- pogled korena datotečnega sistema na gibkem disku s pomočjo programa X-Ways
- hrani čas tvorjenja in zadnje spremembe a le datum zadnjega dostopa

Andraž Brodnik: Digitalna forenzika

FAT

Datotečni sistem FAT

- Izziv: sami poglejte kako izgleda FAT na vašem disku. Poglejte še posebej tiste gruče, ki so prazne – niso del nobenega datotečnega sistema.

Andraž Brodnik: Digitalna forenzika

Datotečni sistem NTFS

- sodobnejši datotečni sistem
 - vse je v datotekah
 - podatke o datotekah hrani v sistemskih datoteki \$MFT
 - imenjuje samo datoteka (B drevesna struktura)
 - je dneviški datotečni sistem (*journal*) in hrani transakcije nad datoteko v sistemski datoteki \$LogFile
- podpira več funkcionalnosti glede datotek
 - pravica dostopa (*ACL – Access Control List*)
- bolje varovan, saj hrani kopije podatkov o datotečnem sistemu na večih mestih (\$MFTMirr)

Andrej Brodnik: Digitalna forenzika

Datotečni sistem NTFS

File Record	Filename	Description
0	\$MFT	Master File Table
1	\$MFTMirr	A backup copy of the first 4 records of the MFT
2	\$LogFile	Log File for CHKDSK
3	\$Volume	Volume Name, Serial Number etc...
4	\$AttrDef	Definitions of every Attribute
5	(dot)	Root directory of the disk
6	\$Bitmap	Map of used and unused clusters
7	\$Boot	Boot record of the volume
8	\$BadClus	List of bad clusters on the partition
9	\$Secure	Security Descriptors for each file
10	\$UpCase	Table of uppercase characters used for conversion
11	\$Extend	Directory for the last four Metafiles.
12-23	UNUSED	Marked for use, or not in use, but empty.
Any	\$ObjId	Unique Object IDs given to every file
Any	\$Quota	Disk space usage quota information
Any	\$Reparse	Reparse point information
Any	\$UsnJrnl	NTFS USN Journal (for encryption)

Andrej Brodnik: Digitalna forenzika

Datotečni sistem NTFS

- **Izziv:** poiščite v svojem NTFS sistemu gruče, ki so prazne (neuporabljene) in nato poglejte njihovo vsebino.

Andrej Brodnik: Digitalna forenzika

NTFS – \$MFT

- primer enega zapisa v \$MFT
- zapis stoji iz prilastkov (attributes)
- zapis je velik 1kB
- če je datoteka majhna, se hrani kar v zapisu
- pri brisanju samo zastavica in potem se zapis ponovno uporabi

```
Pointed to by file: /raven.pdf
File type: data
MD5 of content: b030a08282c05f46ef7bd5a
SHA-1 of content: 292d0a2d3ba4a4c423978c813d8f73b
Details:
MFT Entry Header Values:
Byte Order Sequence: I
$LogFile Sequence Number: 16842551
Allocated File
Links: 1

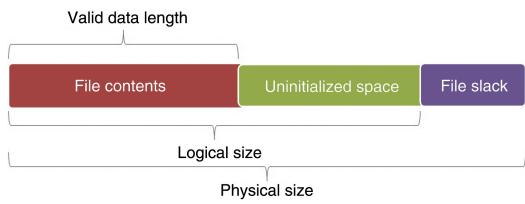
$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner SID: Security ID: 280
Created: Tue Mar 6 21:24:51 2007
File Modified: Wed Mar 7 19:16:13 2007
MFT Modified: Wed Mar 7 19:16:13 2007
Accessed: Wed Mar 7 19:16:13 2007
MFT Modified: Tue Mar 6 21:24:51 2007

$FILE_NAME Attribute Values:
Flags: Archive
Name: review.pdf
Parent File ID: 0x0000000000000005 Sequence: 5
Allocated Size: 0 Actual Size: 0
Created: Tue Mar 6 21:24:51 2007
File Modified: Tue Mar 6 21:24:51 2007
MFT Modified: Tue Mar 6 21:24:51 2007
Accessed: Wed Mar 7 19:16:13 2007
MFT Modified: Tue Mar 6 21:24:51 2007
```

Andrej Brodnik: Digitalna forenzika

NTFS – iskanje podatkov

- pri datoteki obstaja pojem fizične velikosti velikosti (gruče), logične velikosti (zapis v imeniku) in pojem konca datoteke (EOF)



Andrej Brodnik: Digitalna forenzika

NTFS – MFT zapis

```
* pogled na MFT
  zapis in razlika
  med obema
  velikostima

0C07F5010 46 49 4C 45 30 00 33 00 31 43 C0 8F 00 00 00 00 FILE0 1C I
0C07F5010 03 00 02 00 38 00 01 00 E0 01 00 00 00 04 00 00 8  a
0C07F5010 00 00 00 00 00 00 00 00 05 00 00 00 00 D4 1F 00 00 0 0
0C07F5010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0
0C07F5010 00 00 00 00 00 00 00 00 48 00 00 00 18 00 00 00 0 0
0C07F5010 48 08 C6 77 A0 C5 CA 01 48 08 C6 77 A0 C5 CA 01 H R w AE S R w AE
0C07F5010 48 08 C6 77 A0 C5 CA 01 48 08 C6 77 A0 C5 CA 01 H R w AE S R w AE
0C07F5010 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0
0C07F5010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0
0C07F5010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1
0C07F5010 00 00 00 00 00 00 00 00 30 00 00 00 70 00 00 00 0 P
0C07F5010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 R
0C07F5010 E6 24 00 00 00 00 01 00 48 08 C6 77 A0 C5 CA 01 #S H R w AE
0C07F5010 48 08 C6 77 A0 C5 CA 01 48 08 C6 77 A0 C5 CA 01 H R w AE S R w AE
0C07F5010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0
0C07F5010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0
0C07F5010 08 02 43 00 40 00 44 00 4C 00 41 00 42 00 7E 00 C M D I A B ~
0C07F5100 32 00 73 00 67 00 74 00 30 00 00 88 00 00 00 2 s e t o 1
0C07F5100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0
0C07F5100 E6 24 00 00 00 00 01 00 48 08 C6 77 A0 C5 CA 01 #S H R w AE
0C07F5100 48 08 C6 77 A0 C5 CA 01 48 08 C6 77 A0 C5 CA 01 H R w AE S R w AE
0C07F5100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0
0C07F5100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0
0C07F5100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0
0C07F5100 14 01 63 00 60 00 64 00 4C 00 61 00 62 00 73 00 c a d I a b s
0C07F5100 2D 00 73 00 67 00 74 00 76 00 61 00 62 00 69 00 s e t o s a l i
0C07F5100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0
0C07F5100 80 00 00 00 48 00 00 00 01 00 00 00 00 00 04 00 1 H
0C07F5100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0
0C07F5100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0
0C07F5100 00 04 LocalSize 00 00 00 E8 03 ValueDataLength 0 0 0
0C07F5100 31 01 CE AB 03 00 01 00 FF FF FF FF 82 79 47 11 1 I x yyyyyIG
```

Andrej Brodnik: Digitalna forenzika

NTFS – iskanje podatkov

- v imeniku lahko obstajajo datoteke z enakimi imeni

Andrej Brodnik: Digitalna forenzika

Datotečni sistem NTFS

- Izziv: katere gruče sestavljajo vašo datoteko?
- Izziv: poiščite zaseden a neuporabljen del vaše datoteke (na katerih gručah) in kaj v njem.
- Izziv: Kaj se zgodi, če naredimo 1000 datotek, jih nato 1000 pobrišemo in delamo naprej?

Andrej Brodnik: Digitalna forenzika

Kodiranje časa pri datotekah

- FAT: 1.1.1980 + LLLLLLMM MMMDDDDD hhmmmmm mmmsssss

Volume	File	Preview	Details	Gallery	Calendar	Legend	Sync	...
Offset	0 1 2 3 4 5 6 7 8 9 A B C D E F							
00002600	53 41 4C 45 53 20 20 20 20 20 28 00 00 00 00	SALES	(
00002610	00 00 00 00 00 94 7C 8D 20 00 00 00 00 00 00	B1 x . d o .	ñc					
00002620	42 69 00 79 00 2E 00 64 00 6F 00 0F 00 F1 63 00	ÿÿÿÿÿÿÿÿ	ÿÿÿ					
00002630	00 FF	ÿÿÿÿÿÿÿÿ	ÿÿÿ					
00002640	01 73 00 15 00 69 77 77 51 00 0B 00 00 00 00 00	à k . à a .	ñy					
00002650	73 00 2D 00 67 00 65 00 74 00 00 00 61 00 66 00	à e t a i						
00002660	S3 4B 49 57 41 59 7E 31 44 4F 43 20 00 0A 00 64	SKTINAY=1DOC	d					
00002670	AD 2E AD 2E 00 00 45 5F AD 2E B8 00 00 54 00 00	-.-. E-.-. T						
00002680	41 74 00 66 00 64 00 6F 00 20 00 0F 00 B3 74 00	At o d o .	't					
00002690	78 00 74 00 00 00 FF FF FF FF	x t ÿÿÿ	ÿÿÿ					
000026A0	51 4F 44 45 45 20 20 20 20 20 20 20 20 20 20	Data interpreter	Ø	TODO	TXT			
000026B0	54 58 55 55 55 55 55 55 55 55 55 55 55 55 55 55	DOS Date: 05/13/2003		à d				
000026C0	42 74 00 00 00 FF FF FF FF	11:58:10		à z				
000026D0	FF	Bt .	ÿÿÿÿÿÿ					
000026E0	01 6E 00 65 00 77 00 61 00 64 00 0F 00 8C 64 00	ÿÿÿÿÿÿÿÿÿÿ	ÿÿÿ					
000026F0	72 00 65 01 73 00 73 00 2E 00 00 00 74 00 78 00	n e w a d	id					
00002700	4E 45 57 41 44 44 7E 31 54 58 54 20 00 85 48 65	r e s s .	t x					
		HEWADD=1TXT	He					

Andrej Brodnik: Digitalna forenzika

Kodiranje časa pri datotekah

- FILETIME
 - 64 bitni zapis
 - vrednost = 1.1.1600 + število * 100ns



Andrej Brodnik: Digitalna forenzika

NTFS – sledi datotek

- različne operacije različno vplivajo na zabeležene čase v imeniku (tvorjenje – TV, zadnji dostop – ZD, zadnja sprememba – ZS, zapis spremenjen (NTFS) – VS):
 - premik datoteke v snopiču: ne vpliva na nič
 - premik datoteke v drugi snopič: TV, ZD, VS
 - kopiranje datoteke (ciljna datoteka): TV, ZD, VS
 - odreži&prilepi (cut&paste): ZD(*)
 - primi&potegni (drag&drop): ZD(*)
 - zbrisí: ZD, VS
- posebnosti:
 - datoteka na palčki, lahko preko scp/...: TV > ZS
 - pri brisanju imenika, se podatki o datotekah ne spreminjajo

Andrej Brodnik: Digitalna forenzika

NTFS – sledi datotek ...

- vsebina pisarniških datotek vsebuje metapodatke iz imenika
 - *Shrani kot:* če na isto datoteko, gre dejansko za prepis in ne za tvorjenje nove datoteke v imeniku, ne pa v datoteki
- tiskanje najprej prepriše datoteko v poseben imenik ter jo šelev nato natisne
 - C:\Windows\Spool\Printers, C:\WinNT\System32\Spool\Printers
 - tudi, ko tiskamo spletno vsebino ipd.

Andrej Brodnik: Digitalna forenzika

NTFS – sledi datotek ...

- Izviv: najdite datoteko, ki ima čas tvorjenja večji od časa zadnje spremembe.
- Izviv: Kaj lahko rečete, če ima nekdo takšno datoteko na sistemu in ima čas zadnjega dostopa enak času tvorjenja?
- Izviv: kaj je to EMF način tiskanja? Kaj se v tem primeru shrani v datoteki tiskalniške vrste (*spooler*)?

Andrej Brodnik: Digitalna forenzika

Reševanje podatkov

- reševanje izbrisanih datotek
 - različna orodja, ki jih lahko poganjamo na Windows OS

- orodje SleuthKit v kombinaciji z Autopsy Browser omogoča celo pregledovanje preko brskalnika (<http://www.sleuthkit.org/autopsy>)

Reševanje podatkov ...

- Izviv: namestite sleuthkit in Autopsy Browser in poiščite izgubljene datoteke.

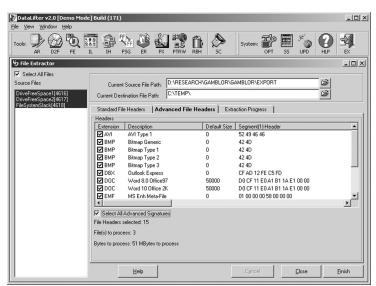
Andrej Brodnik: Digitalna forenzika

Reševanje podatkov ...

- iskanje izgubljenih datotek iz velike neoblikovane gmote
 - enako kot obrezovanju datotek

- orodje DataLifter:

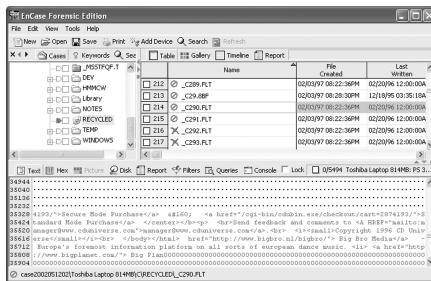
iščemo izgubljeno
datoteko iz dveh
gmot praznega
prostora in enega
preostanka
datotečnega
sistema



Reševanje podatkov ...

- če majhna datoteka prepriše veliko, lahko večino velike datotekе reconstruiramo

- enCase:
primer
nakupoval-
nega vozička
v CD
Universe, ki
se je znašel v
preostanku
datotečnega
prostora



Zabeležke (*log files*)

- operacijski sistem (odvisno od nastavitev) beleži marsikaj
 - dostopi do virov,
 - pojavlanje in brisanje virov,
 - napake itd.
- shranjene na %systemroot%\system32\config (c:\winnt\...)
- različne zabeležke v različnih datotekah: Appevent.evt, Secevent.evt, Sysevent.evt

Zabeležke

- *Izziv:* preverite format evt datoteke in poglejte, kdaj v njih, kdaj ste se prijavili v sistem.

Andrej Brodnik: Digitalna forenzika

Register

- v OS Windows so spremenljivke okolja procesa definirane v registru
- dejansko so podatki shranjeni v datotekah (*hives*) v sistemskem imeniku %systemroot%\system32\config
 - *nuser.dat* za vsakega uporabnika svoja datoteka
- datoteke lahko pregledujemo z Windows orodjem regedt32 (EnCase, FTK, ...)

Andrej Brodnik: Digitalna forenzika

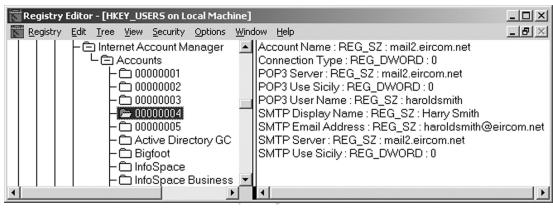
Register

- *Izziv:* preučite forenzično vrednost podatkov v registru.

Andrej Brodnik: Digitalna forenzika

Omrežne sledi

- nekaj tudi iz sistemskega okolja
 - ob vzpostaviti povezave, ...
- večina izvira neposredno iz aplikacij
 - brskalniki, poštni agenti, ...



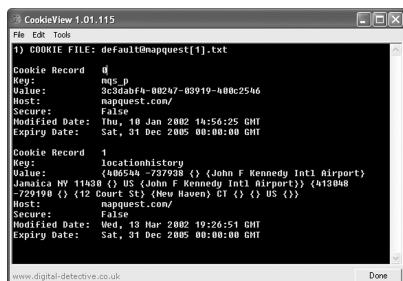
Omrežne sledi - brskalniki

- zgodovina:
 - firefox-3 je hrانil zgodovino v sqlite podatkovni bazi *Places.sqlite*
 - internet explorer hrани zgodovino v *index.dat*
 - orodja so na voljo za iskanje po teh bazah: www.odessa.sourceforge.net
- lokalni predpomnilnik
- piškotki

Andrej Brodnik: Digitalna forenzika

Brskalniki – piškotki

- primer pregleda piškotov z CookieView (www.digitaldetective.co.uk)



Brskalniki

- *Izziv:* poiščite kakšni ostanke v svojem predpomnilniku in jih preverite z zgodovino brskanja.
- *Izziv:* dobite od prijatelja datoteko z zgodovino njegovega brskalnika in jo razvozljajte.
- *Izziv:* preverite kakšne vse sledi pušča brskalnik IE, kakšne Mozilla in kakšne Opera.

Andrej Brodnik: Digitalna forenzika

E-pošta

- sledi so odvisne od poštnega agenta, ki ga uporabljamo
 - poslana in prejeta pošta
 - povzetki IMAP nabiralnikov
- vsebina, ki je zanimiva
 - samo besedilo pošte
 - pripombe(!) – MIME format

Andrej Brodnik: Digitalna forenzika

Drugi programi

- različni programi puščajo različne sledi
- omrežno programje
 - dostop do drugih sistemov
 - dostop drugih sistemov do našega sistema
- sistemski programi puščajo sledi v registru

Andrej Brodnik: Digitalna forenzika

Sledi omrežnega dostopa

- telnet dostop do acf2.nyu.edu

