

Digitalna forenzika

Andrej Brodnik

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

Računalnik

*poglavje 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 zmanjkalo napajanja.

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

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

---

---

## Format datoteke

- datoteke imajo na začetku posebne podpise ([www.garykessler.net/library/file\\_sigs.htm](http://www.garykessler.net/library/file_sigs.htm))
- jpg: *FF D8 FF E0*, ali *FF D8 FF E3*
- gif: *47 49 46 38 37 61* ali *47*, ali *49 46 38 39 61*
- doc: *D0 CF 11 E0 A1 B1 1A E1*

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

---

---

## Format datoteke –primer

- jpeg zakodirana exif (*Exchangeable image file format*) datoteka

```

Hex  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 000a exif MM *
00000010  00 00 00 08 00 08 03 0F 00 02 00 00 00 16 00 00
00000020  01 02 01 10 00 02 00 00 00 1C 00 00 01 C0 01 12 000c
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 18 00 05 00 00 00 01 00 00
00000050  01 02 01 28 00 03 00 00 00 01 00 02 00 02 13 000e
00000060  00 03 00 00 00 01 00 01 00 00 07 69 00 04 00 00
00000070  00 01 00 00 01 F4 00 00 00 24 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  53 54 4D 41 4E 20 4B 4F 44 41 4B 20 44 58 34 33 33 30
000000D0  41 4E 59 00 4B 4F 44 41 4B 20 44 58 34 33 33 30
000000E0  20 44 49 47 49 54 41 4C 20 43 41 4D 45 52 41 00
000000F0  00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00
00000100  00 24 82 9A 00 05 00 00 00 01 00 00 03 DA 82 9D
00000110  00 05 00 00 01 00 00 00 00 00 00 00 00 00 00 00
00000120  00 01 00 02 00 00 00 00 00 07 00 00 04 30 32
00000130  32 30 90 03 00 02 00 00 00 14 00 00 02 EA 90 04 20
    
```

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

---

---

## Format datoteke

- datoteka je lahko gnezdena v drugi datoteki
  - poiščemo datoteko
  - jo lahko označimo in prepíšemo (*copy-paste*)
  - ali uporabimo orodje **dd**
- temu postopku rečemo obrezovanje / klesanje (*carving*)
- druga orodja:
  - scalpel (<http://www.digitalforensicsolutions.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:** vgnezdite v eno datoteko drugo datoteko ter jo objavite na forumu. Nato naj drugi kolegi poiščejo vgnezdjeno 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

---

---

---

---

---

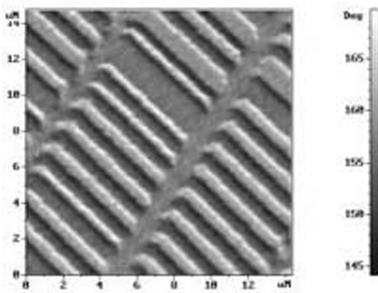
---

---

---

### Shramba podatkov in skrivanje

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



Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

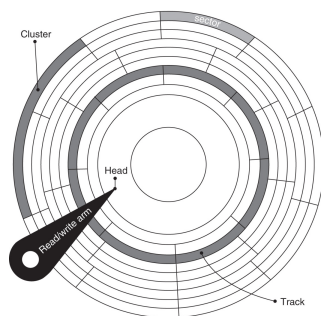
---

---

---

### 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

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

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

### Shramba podatkov in skrivanje

- pogled v bot sektor Windows95 stroja z orodjem Norton DiskUtils



Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

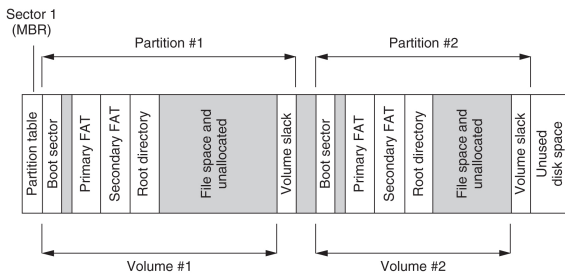
---

---

---

### Shramba podatkov in skrivanje

- poenostavljena organiziranost diska z datotečnim sistemom FAT



Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

### Shramba podatkov in skrievanje

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

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

### Shramba podatkov in skrievanje

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

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

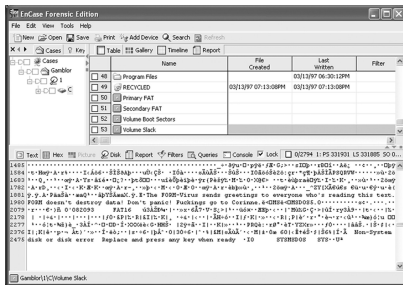
---

---

---

### Shramba podatkov in skrievanje

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



Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

## Shramba podatkov in skrivanje

- ko je datoteka izbrisana, podatki ne izginejo
- tudi, ko formatiramo disk, podatki ne izginejo
  - pogledajte orodje **Edisk**
- 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

<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	readneen.txt	01/04/04 11:19:02AM
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	readnefr.txt	01/04/04 11:18:56AM
<input type="checkbox"/>	4	<input checked="" type="checkbox"/>	src.zip	01/04/04 11:18:44AM
<input type="checkbox"/>	5	<input checked="" type="checkbox"/>	hxdmf100.ini	12/31/03 10:17:36AM
<input type="checkbox"/>	6	<input checked="" type="checkbox"/>	hxdmf100.2.ini	12/31/03 10:17:14AM
<input type="checkbox"/>	7	<input checked="" type="checkbox"/>	bdc1100.exe	12/31/03 10:16:02AM
<input type="checkbox"/>	8	<input checked="" type="checkbox"/>	rdrbs100.exe	12/31/03 10:15:50AM
<input type="checkbox"/>	9	<input checked="" type="checkbox"/>	hxdmf100.exe	12/31/03 10:15:34AM
<input type="checkbox"/>	10	<input checked="" type="checkbox"/>	src.zip:Zone.Identifier	
<input type="checkbox"/>	11	<input checked="" type="checkbox"/>	hxdmf100.ini:Zone.Identifier	
<input type="checkbox"/>	12	<input checked="" type="checkbox"/>	readmccz.txt:Zone.Identifier	
<input type="checkbox"/>	13	<input checked="" type="checkbox"/>	hxdmf100.exe:Zone.Identifier	
<input type="checkbox"/>	14	<input checked="" type="checkbox"/>	readneen.txt:Zone.Identifier	
<input type="checkbox"/>	15	<input checked="" type="checkbox"/>	hxdmf100.2.ini:Zone.Identifier	

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

## Shramba podatkov in skrivanje

- **Izziv:** pogledajte 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

---

---

---

---

---

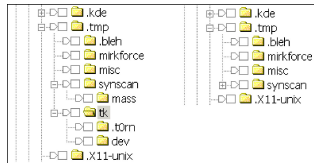
---

---

---

## Skrivanje podatkov

- skivanje partij
  - orodje Test Disk (<http://www.cgsecurity.org/>)
- na ravni datotek
  - skivanje datotek: npr. MS Windows: `attrib +H in dir/AH`
  - `parlament.jpg -> test.exe`
  - slika 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/](http://www.openwall.com/john/))
  - Cain and Abel ([www.oxid.it/cain.html](http://www.oxid.it/cain.html))
  - Advanced Archive Password Recovery ([www.elcomsoft.com/azpr.html](http://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

poglavje 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

---

---

---

---

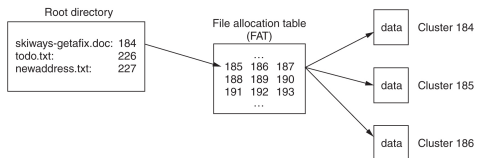
---

---

---

---

## 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 NTFS

- sodobnejši datotečni sistem
  - vse je v datotekah
  - podatke o datotekah hrani v sistemskih datoteki \$MFT
  - imenik je samo datoteka (B drevesna struktura)
- je dnevniški datotečni sistem (*Journal*) in hrani transakcije nad datoteko v sistemski datoteki \$LogFile
- podpira več funkcionalnosti glede datotek
  - pravica dostopa (*ACL – Access Control List*)
- boljše 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 in 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)

Table 3.1.1 – NTFS 3.0+ Metafiles

Andrej Brodnik, Digitalna forenzika

## Datotečni sistem NTFS

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

Andrej Brodnik, Digitalna forenzika



### NTFS – iskanje podatkov

- v imeniku lahko obstajajo datoteke z enakimi imeni

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

### Datotečni sistem NTFS

- **Izziv:** katere gručice 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 + LLLLLLLL MMMDDDDD hhhhhmmm mmmsssss

Volume	File	Preview	Datals	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	00	9A	7C	8D	2E	00	00	00	00	00	Bl x d o  c	
00002620		42	69	00	78	00	2E	00	64	00	6F	00	0F	00	F1	63	00	00
00002630		00	00	FF	FF	FF	FF	FF	FF	FF	00	00	FF	FF	FF	FF	00	00
00002640		01	73	00	6B	00	69	00	77	00	61	00	0F	00	F1	79	00	00
00002650		73	00	2D	00	67	00	65	00	74	00	00	61	00	66	00	00	00
00002660		53	4B	49	57	41	59	7E	31	44	4E	43	20	00	0A	00	64	00
00002670		AD	2E	AD	2E	00	00	45	5E	AD	2E	B9	00	00	54	00	00	00
00002680		41	74	00	6F	00	64	00	6F	00	2E	00	0F	00	B3	74	00	00
00002690		78	00	74	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	00	00
000026A0		54	4E	44	4E	20	20	20	20	54	58						x t yyy yyy	
000026B0		AD	2E	AD	2E	00	00	18	65	AD	2E						TUDO TXT >d	
000026C0		42	74	00	00	00	FF	FF	FF	FF	FF						- - - e - a z	
000026D0		FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	00	00	FF	FF	FF	FF	Bt yyyyyy  yy
000026E0		01	6E	00	65	00	77	00	61	00	64	00	0E	00	9C	64	00	00
000026F0		72	00	65	00	73	00	73	00	2E	00	00	00	74	00	78	00	00
00002700		4E	45	57	41	44	44	7E	31	54	58	54	20	00	85	48	65	00

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(\*)
  - zbrisi: 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
  - *Štrani kot*: če na isto datoteko, gre dejansko za prepis in ne za tvorjenje nove datoteke v imeniku, ne pa v datoteki
- tiskanje najprej prepíše datoteko v poseben imenik ter jo šele nato natisne
  - C:\Windows\Spool\Printers, C:\WinNT\System32\Spool\Printers
  - tudi, ko tiskamo spletno vsebino ipd.

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

---

---

### NTFS – sledi datotek ...

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

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

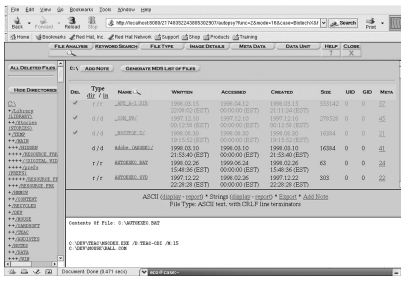
---

---

### Reševanje podatkov

- reševanje izbranih 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/>)



Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---

### Reševanje podatkov ...

- **Izziv:** namestite sleuthkit in Autopsy Browser in poiščite izgubljene datoteke.

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

---

---

---





## Zabeležke

- *Izziv:* preverite format evt datoteke in pogledajte, kdaj v njih, kdaj ste se prijaviili 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`
  - *ntuser.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

---

---

---

---

---

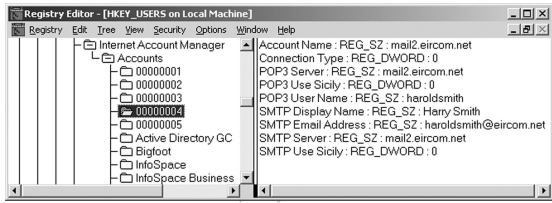
---

---

---

### Omrežne sledi

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




---

---

---

---

---

---

---

---

### Omrežne sledi - brskalniki

- zgodovina:
  - firefox-3 je hranil zgodovino v sqlite podatkovni bazi *Places.sqlite*
  - internet explorer hrani zgodovino v *index.dat*
  - orodja so na voljo za iskanje po teh bazah: [Odessa](http://www.odessa.sourceforge.net) ([www.odessa.sourceforge.net](http://www.odessa.sourceforge.net))
- lokalni predpomnilnik
- piškoti

Andrej Brodnik, Digitalna forenzika

---

---

---

---

---

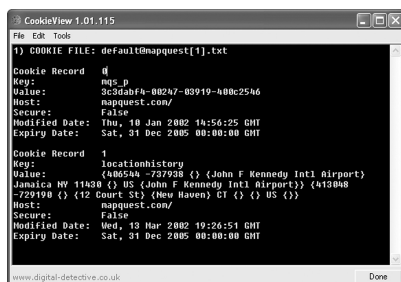
---

---

---

### Brskalniki – piškoti

- primer pregleda piškotov z CookieView ([www.digitaldetective.co.uk](http://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 njegvega brskalnika in jo razvozljajte.
- **Izziv:** preverite kakšne vse sledi pušča brskalniki IE, kakšne Mozilla in kakšne Opera.

Andrej Brodnik: Digitalna forenzika

---

---

---

---

---

---

---

---

## E-pošta

- sledi so odvisne od poštne agenta, ki ga uporabljamo
  - poslana in prejeta pošta
  - povzetki IMAP nabiralnikov
- vsebina, ki je zanimiva
  - samo besedilo pošte
  - priložnosti – 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

---

---

---

---

---

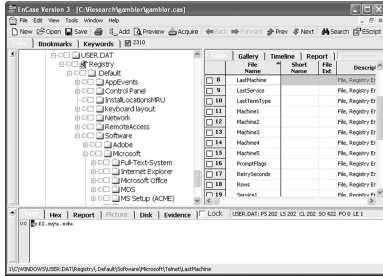
---

---

---

### Sledi omrežnega dostopa

- telnet dostop do acf2.nyu.edu



---

---

---

---

---

---

---

---