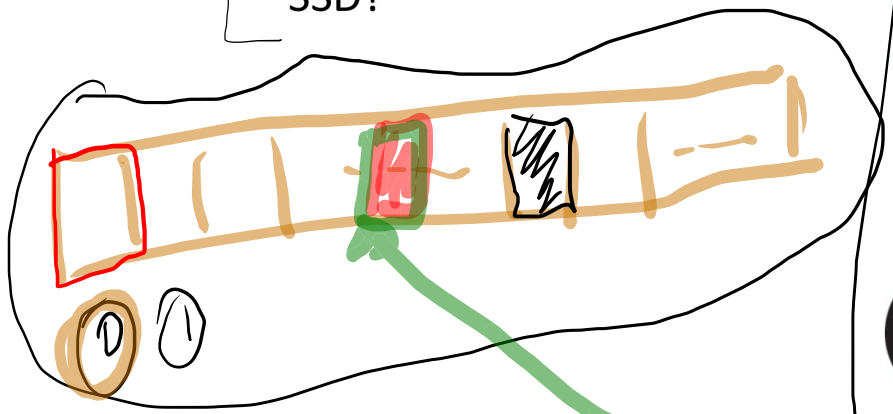
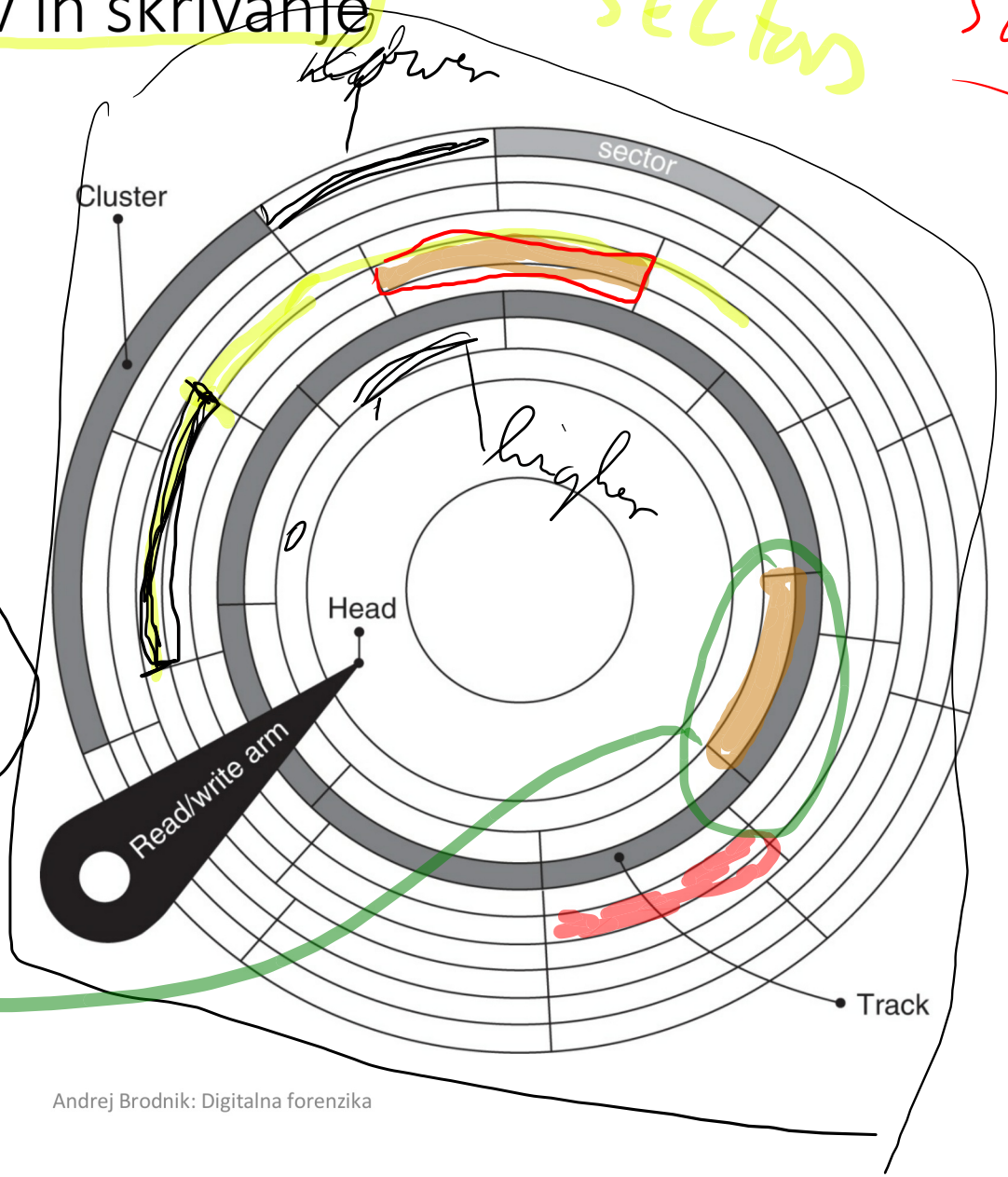
# Digitalna forenzika

Andrej Brodnik

# 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?





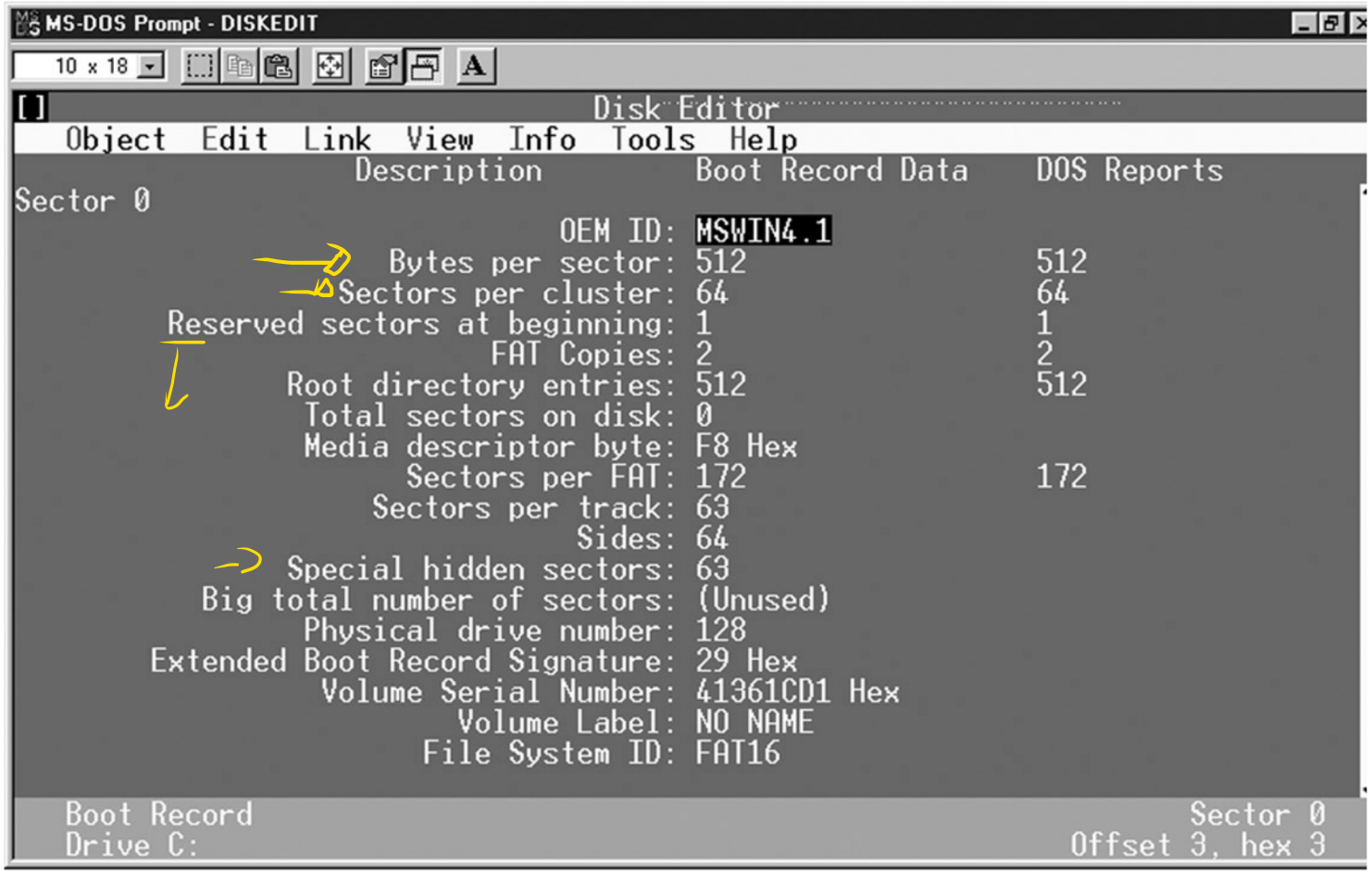
# Shramba podatkov in skrivanje

- *Izziv:* poiščite orodje anadisk in poglejte kaj zna in zmore početi.

- *Izziv:* kakšna je struktura MBR? Sestavite svoj MBR in ga objavite v forumu.

# Shramba podatkov in skrivanje

- pogled v bot sektor Windows95 stroja z orodjem Norton DiskUtils



```
root:~ # diskinfo -v /dev/ada0
/dev/ada0
        512             # sectorsize
        1000204886016   # mediasize in bytes (932G)
        1953525168      # mediasize in sectors
        0               # stripesize
        0               # stripeoffset
        1938021         # Cylinders according to firmware.
        16              # Heads according to firmware.
        63              # Sectors according to firmware.
        TOSHIBA MG03ACA100      # Disk descr.
        Y4U9K5A9F       # Disk ident.
        No              # TRIM/UNMAP support
        7200            # Rotation rate in RPM
        Not_Zoned       # Zone Mode
```

```
root:~ # diskinfo -v /dev/ada1
/dev/ada1
        512             # sectorsize
        5000981078016   # mediasize in bytes (4.5T)
        9767541168      # mediasize in sectors
        4096            # stripesize
        0               # stripeoffset
        9690021         # Cylinders according to firmware.
        16              # Heads according to firmware.
        63              # Sectors according to firmware.
        TOSHIBA MG04ACA500E     # Disk descr.
        16NAK05LFJJA    # Disk ident.
        No              # TRIM/UNMAP support
        7200            # Rotation rate in RPM
        Not_Zoned       # Zone Mode
```

| Volume Name | Free | Capacity | Mount Point | File System | BSD Name |
|---|---|---|---|---|---|
| Macintosh HD | 199,63 GB | 499,96 GB | / | APFS | disk1s5s1 |
| Macintosh HD - Data | 199,63 GB | 499,96 GB | /System/Volumes/Data | APFS | disk1s1 |

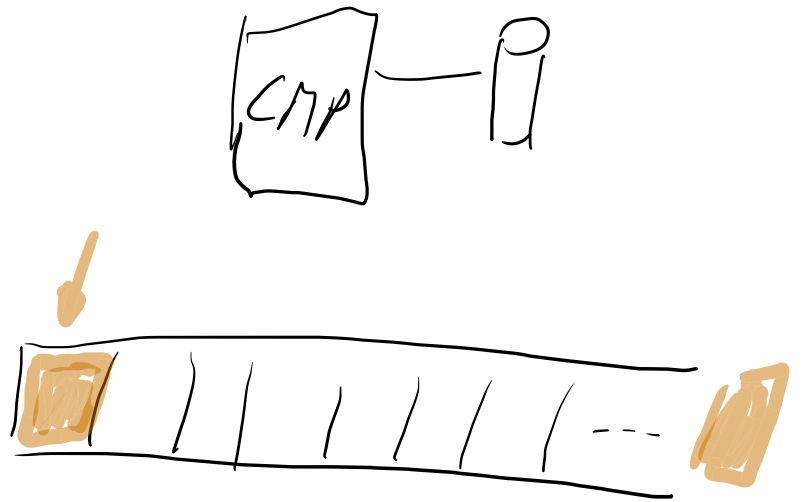
**Macintosh HD - Data:**

Free: 199,63 GB (199.627.882.496 bytes)
Capacity: 499,96 GB (499.963.174.912 bytes)
Mount Point: /System/Volumes/Data
File System: APFS
Writable: Yes
Ignore Ownership: No
BSD Name: disk1s1
Volume UUID: A519D5B2-9B02-4B38-A8C8-DEA7C1496C6B
Physical Drive:
    Device Name: APPLE SSD AP0512J
    Media Name: AppleAPFSMedia
    Medium Type: SSD
    Protocol: PCI-Express
    Internal: Yes
    Partition Map Type: Unknown
    S.M.A.R.T. Status: Verified

| Volume Name | Free | Capacity | Mount Point | File System | BSD Name |
|---|---|---|---|---|---|
| Macintosh HD | 199,63 GB | 499,96 GB | / | APFS | disk1s5s1 |
| Macintosh HD - Data | 199,63 GB | 499,96 GB | /System/Volumes/Data | APFS | disk1s1 |

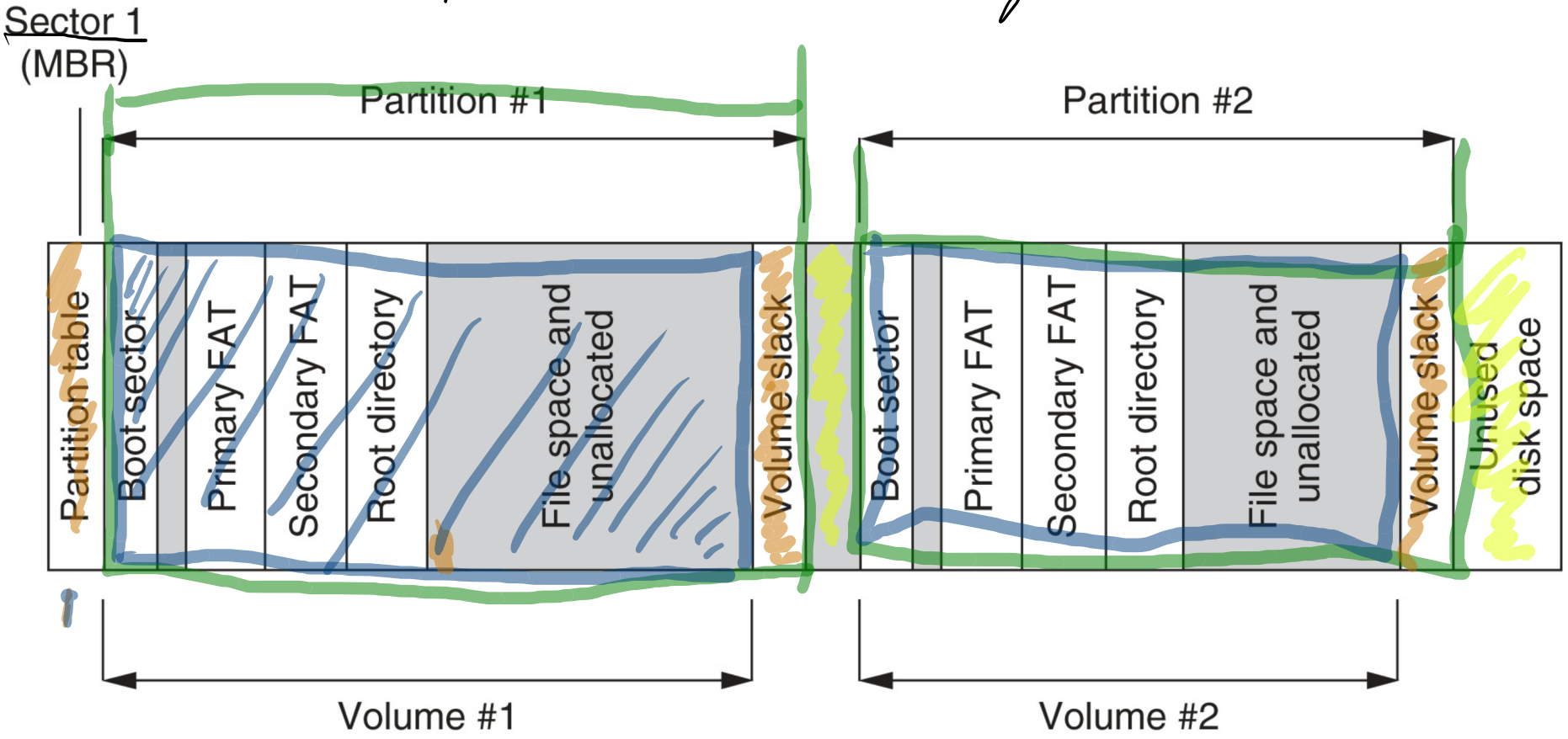
**Macintosh HD:**

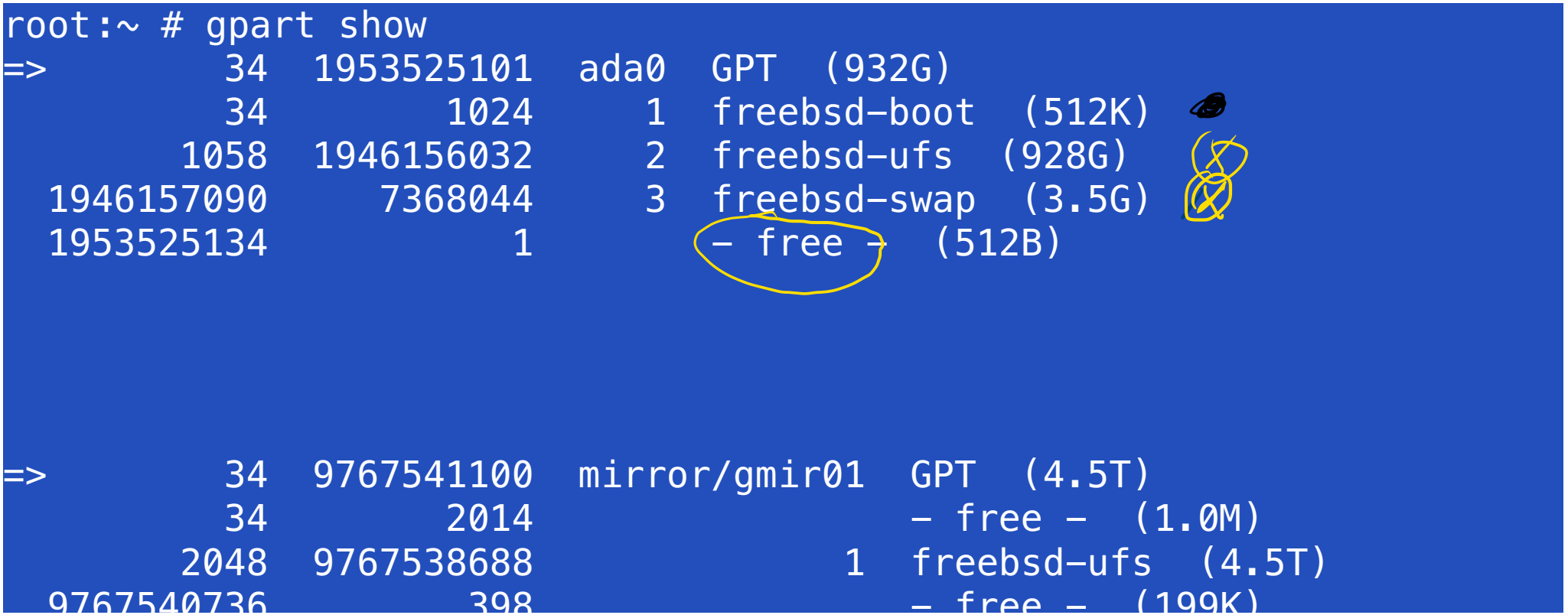
| | |
|---|---|
| Free: | 199,63 GB (199.627.882.496 bytes) |
| Capacity: | 499,96 GB (499.963.174.912 bytes) |
| Mount Point: | / |
| File System: | APFS |
| Writable: | No |
| Ignore Ownership: | No |
| BSD Name: | disk1s5s1 |
| Volume UUID: | B74BEC77-8176-43EB-858C-AF912CBE921E |
| Physical Drive: | |
| Device Name: | APPLE SSD AP0512J |
| Media Name: | AppleAPFSMedia |
| Medium Type: | SSD |
| Protocol: | PCI-Express |
| Internal: | Yes |
| Partition Map Type: | Unknown |
| S.M.A.R.T. Status: | Verified |



# Shramba podatkov in skrivanje

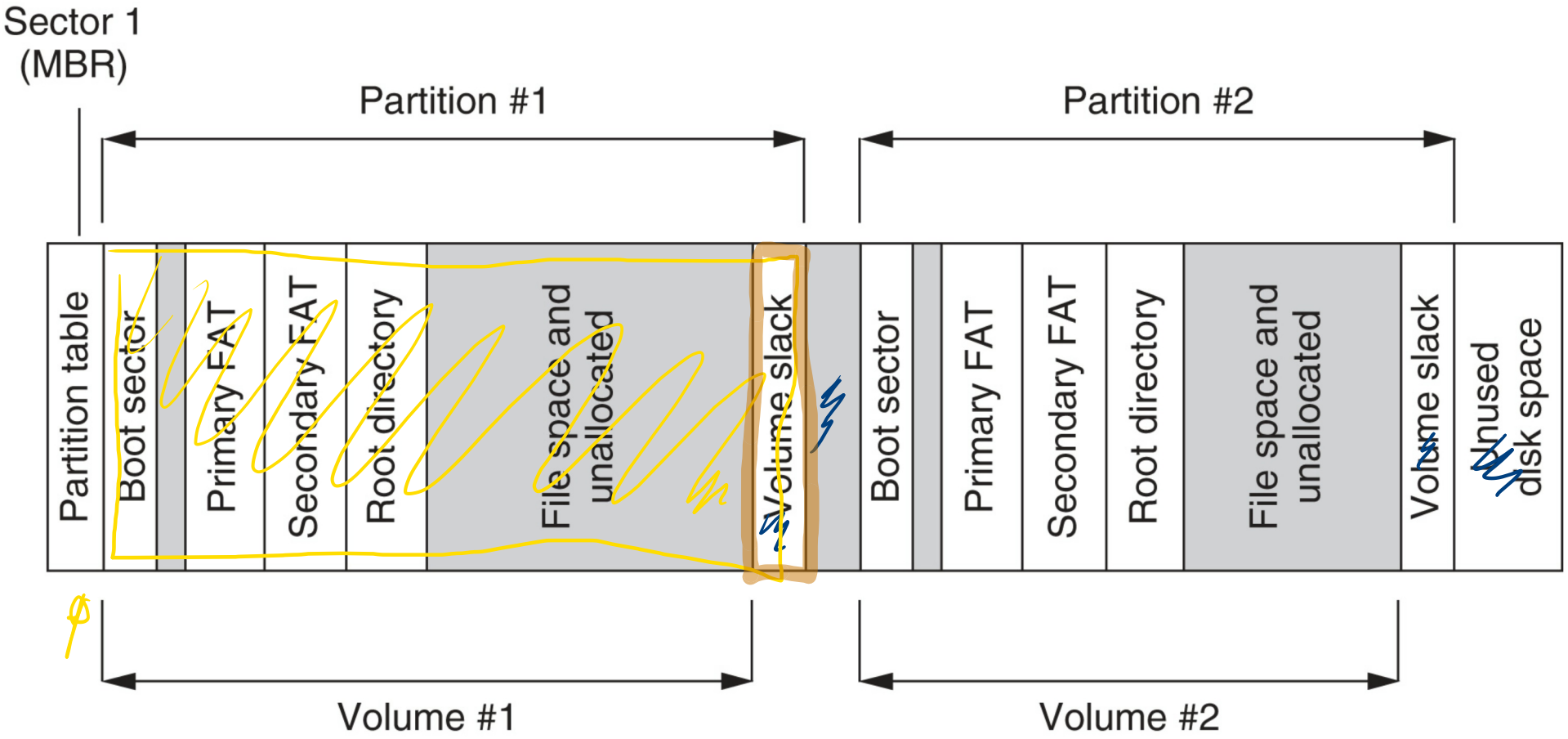
- poenostavljena organiziranost diska z datotečnim sistemom FAT




root:~ # gpart show
=> 34 1953525101 ada0 GPT (932G)
34 1024 1 freebsd-boot (512K)
1058 1946156032 2 freebsd-ufs (928G)
1946157090 7368044 3 freebsd-swap (3.5G)
1953525134 1 - free - (512B)
=> 34 9767541100 mirror/gmir01 GPT (4.5T)
34 2014 - free - (1.0M)
2048 9767538688 1 freebsd-ufs (4.5T)
9767540736 398 - free - (199K)

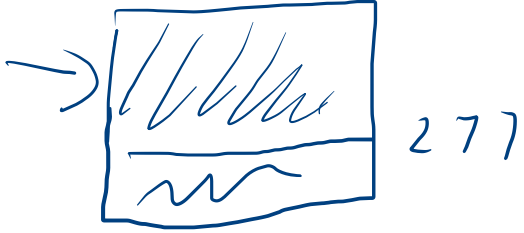
# Shramba podatkov in skrivanje

- poenostavljena organiziranost diska z datotečnim sistemom FAT



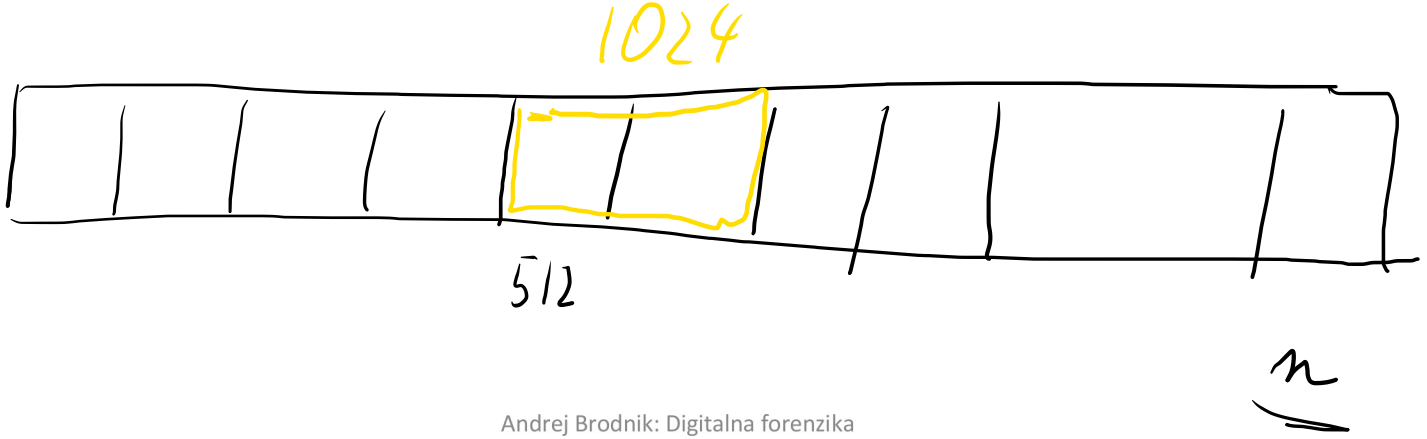
# Shramba podatkov in skrivanje

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



# Shramba podatkov in skrivanje

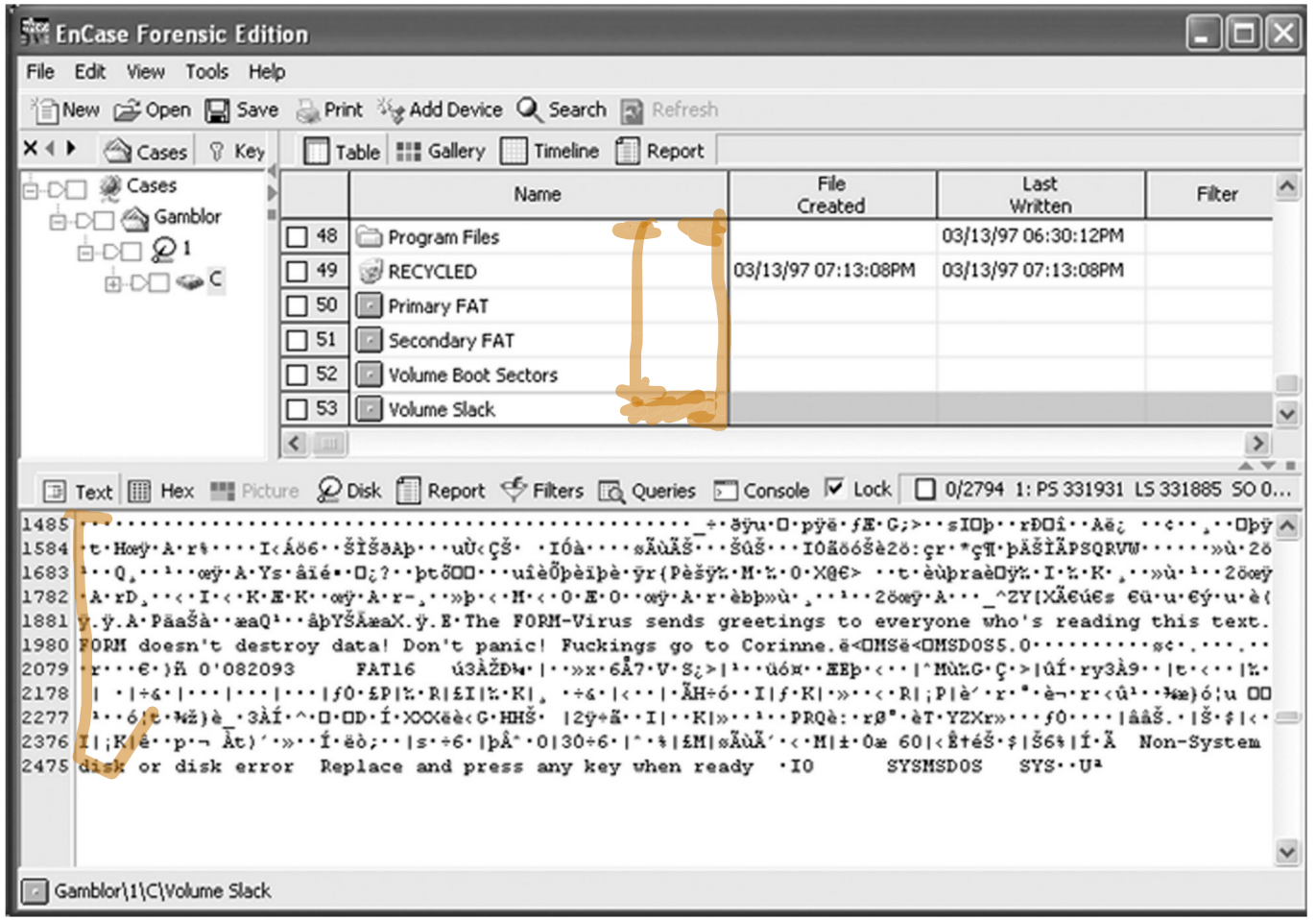
- skrivanje podatkov zaradi notranje in zunanje fragmentacije:
  - skrivanje znotraj sektorja (bloka) – težko in neobičajno
  - skrivanje znotraj gruče
  - skrivanje znotraj particije (particije se običajno začnejo na začetku sledi
  - skrivanje particije
- kriptiranje particije
- servisni podatki: DCO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



# Shramba podatkov in skrivanje

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

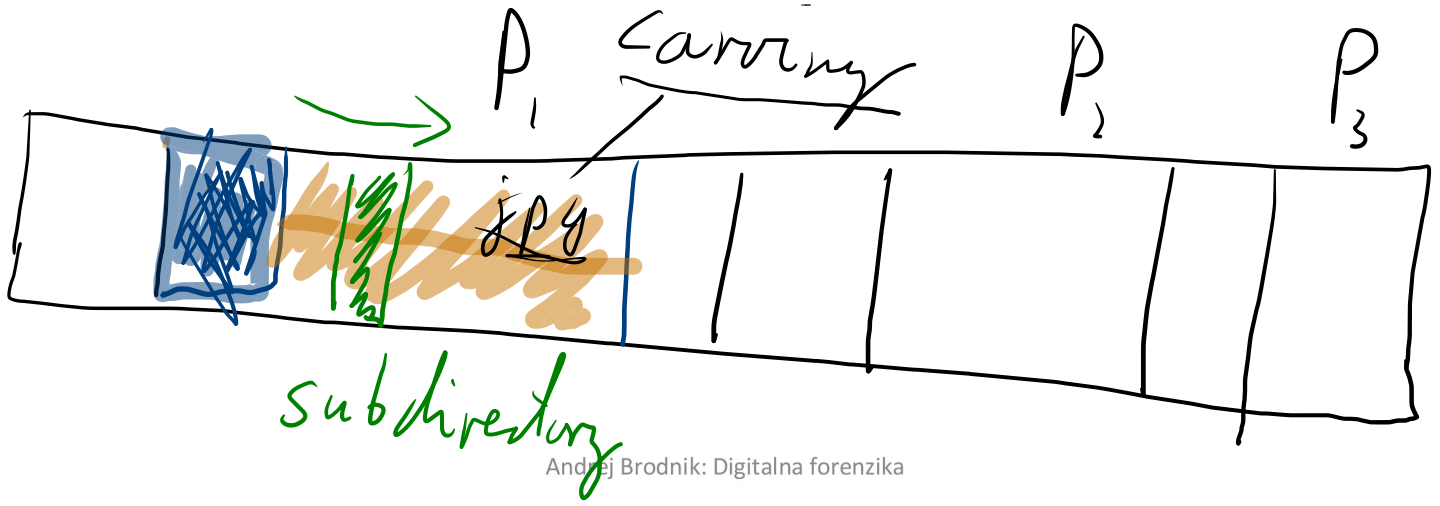
- disk
- block array
- partition
- volume / FS
- files, not used part



# Shramba podatkov in skrivanje

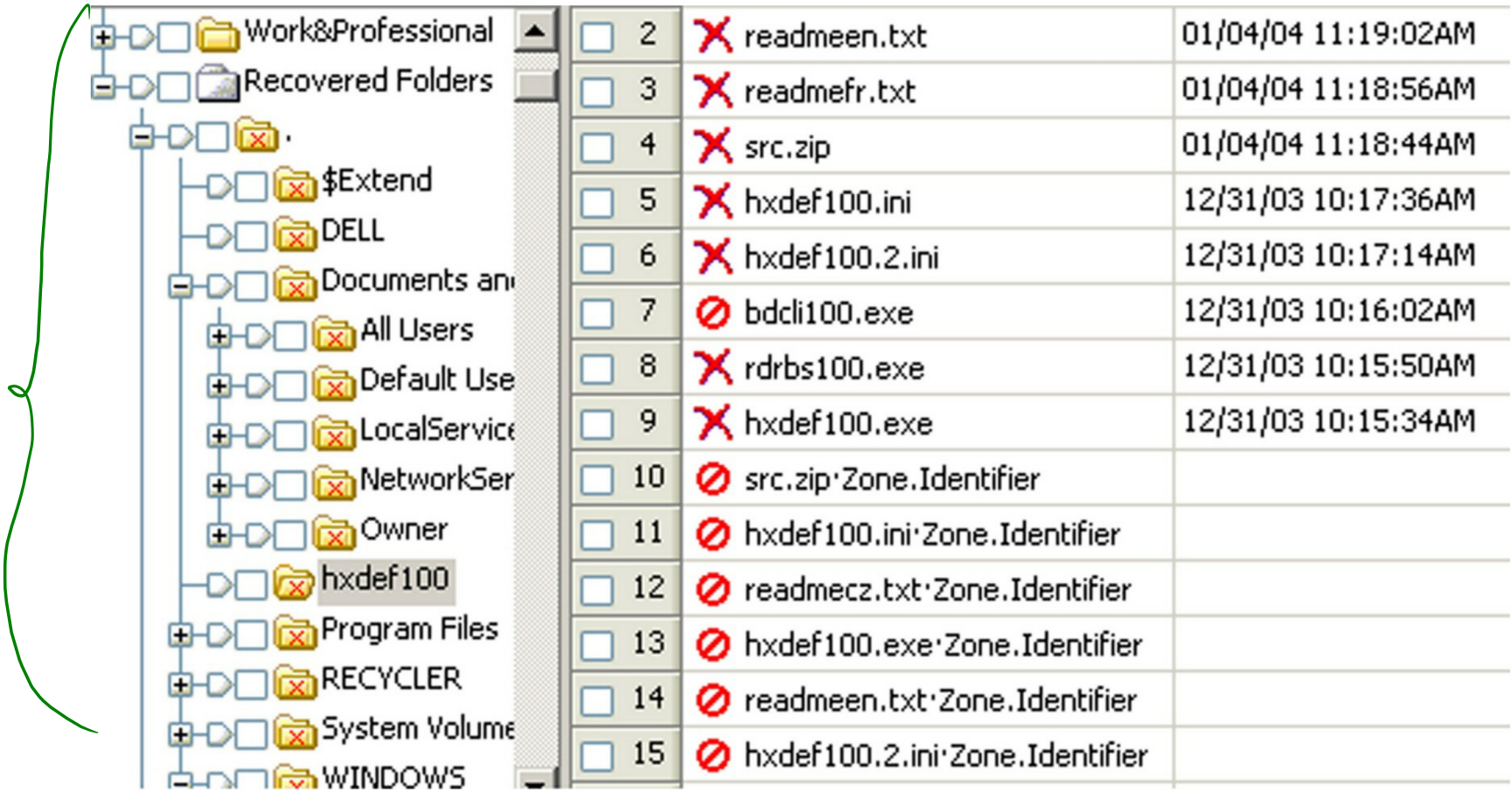
- ko je datoteka izbrisana, podatki ne izginejo
- tudi, ko formatiramo disk, podatki ne izginejo
  - poglejte orodje **`fdisk`**
- rezultat obeh operacij je pravilen datotečni sistem in kopica praznih blokov

- orodja: **`sleuthkit`** (http://www.sleuthkit.org/), Norton DiskEdit, …



# Shramba podatkov in skrivanje

- primer rekonstrukcije datotek na sveže formatiranem disku z orodjem EnCase

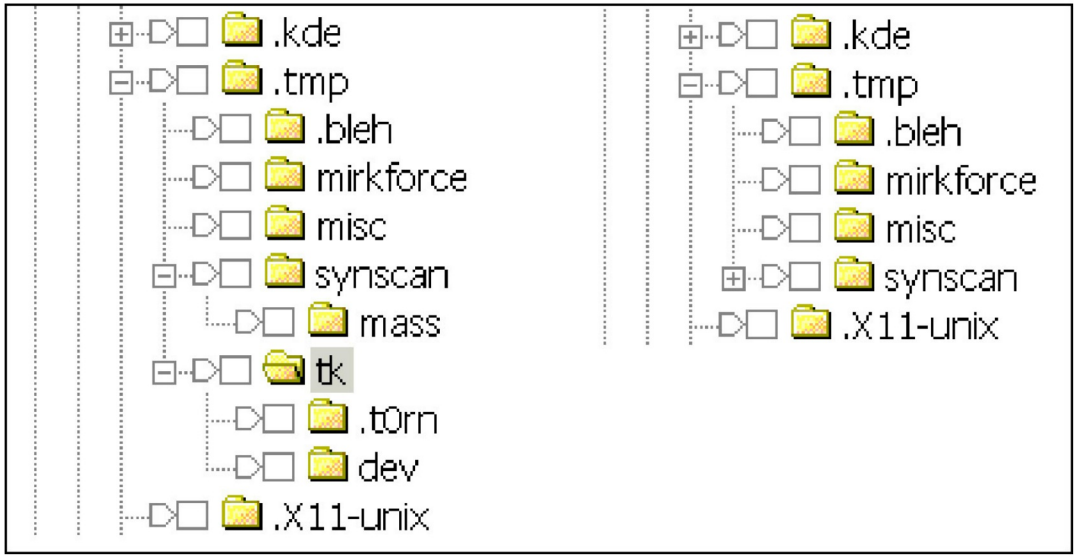


# Shramba podatkov in skrivanje

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

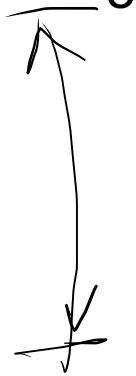
# Skrivanje podatkov

- 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



# Gesla in kriptiranje

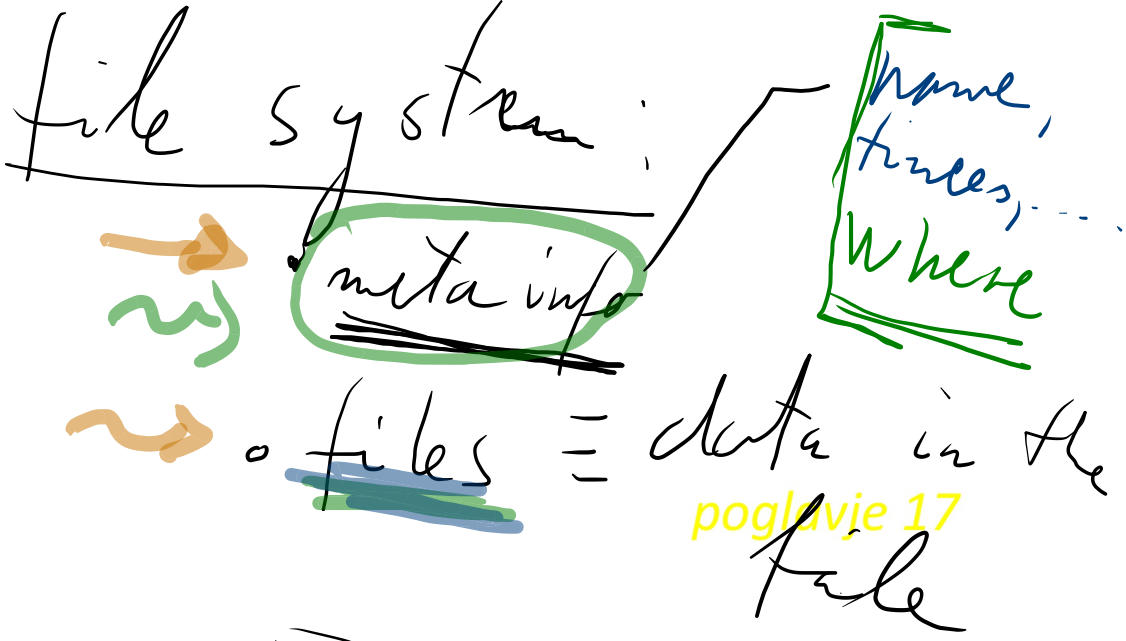
- orodja za razbijanje in iskanje gesel
  - Password Recovery Tool – PRTK in Distributed Network Attack – DNA (http://accessdata.com/products/computer-forensics/decryption)
  - John the Ripper (www.openwall.com/john/)
  - Cain and Abel (www.oxid.it/cain.html)
  - Advanced Archive Password Recovery (www.elcomsoft.com/azpr.html)



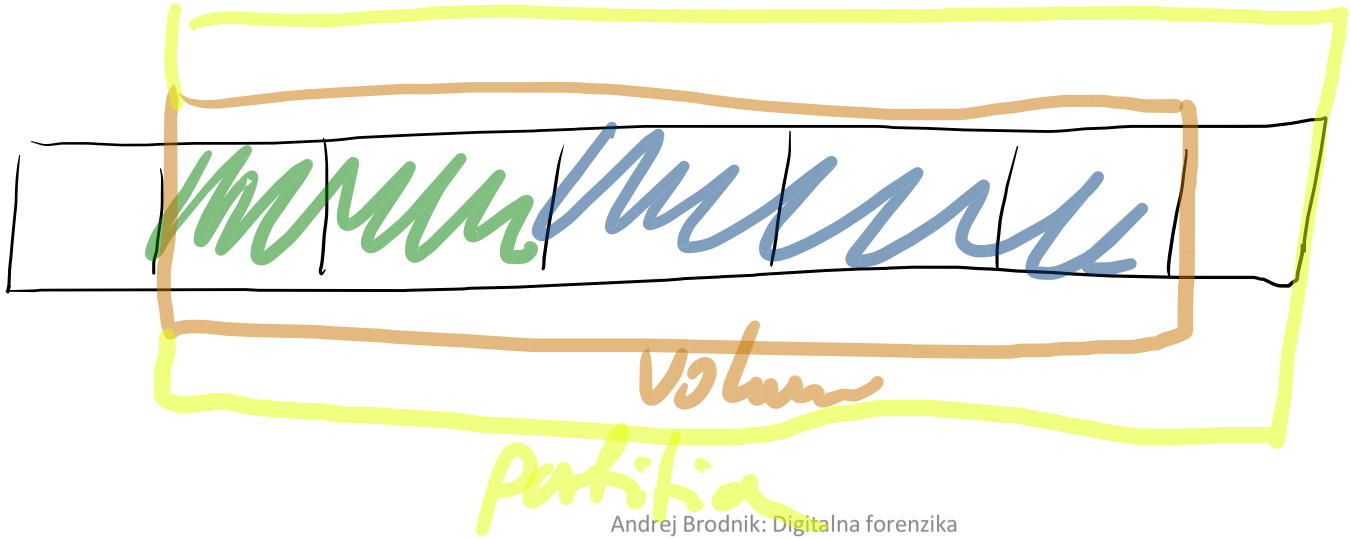
# Gesla in kriptiranje

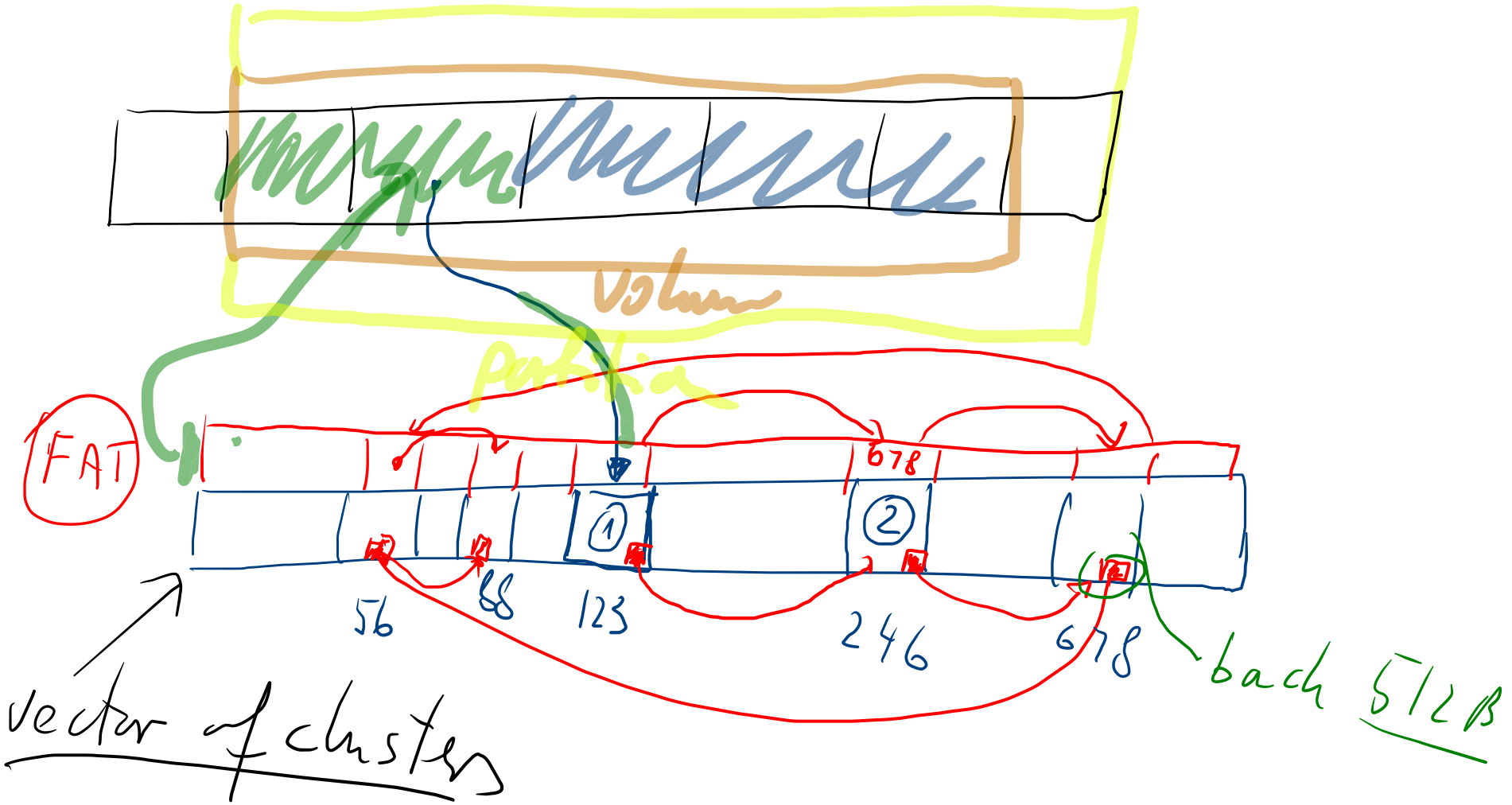
- več o kriptiranju in kriptografiji kasneje
- nekaj primerov
  - orodje caesar, rot13
  - podpora za PGP
  - orodje crypt

# OS Windows




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




512 → 506

# of indexes = # of blocks

12345 ⇒ FAT last index 12345

|inode| ~ 326 bits = 4B

# OS Windows – datotečni sistemi

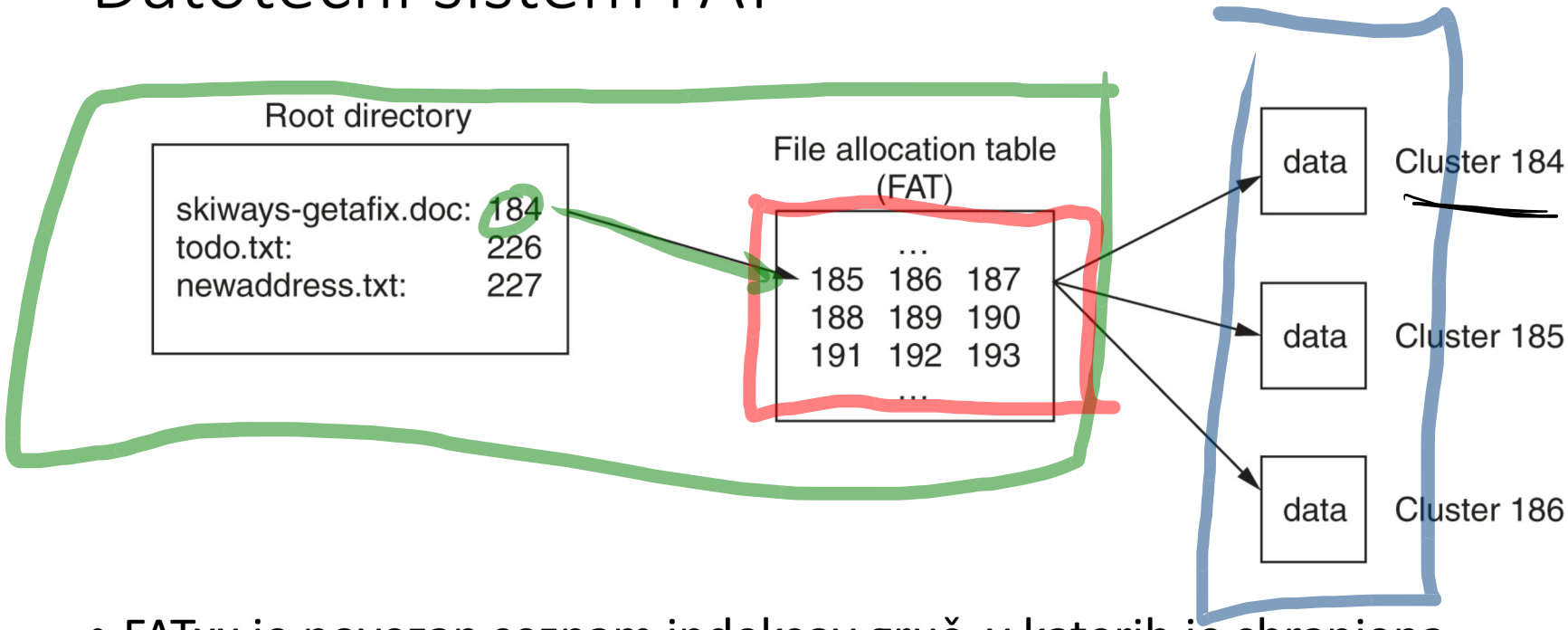
- dva osnovna datotečna sistema FAT (*File Allocation Table*) in NTFS (*New Technology File System*)

- FAT
  - razvit najprej za gibke diske (diskete)
  - FAT12, FAT16, FAT32

index = 8 bits → 256 clusters

1 GB disk → |cluster| = $\frac{2^{32} B}{2^8} = 2^{24} B =$ 16 MB

# 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

1 GB = $2^{30}$ B ⇒ 12 ⇒ |cluster| = 1MB

|cluster| = 512 B

16 ⇒ |cluster| = 64B

# Datotečni sistem FAT

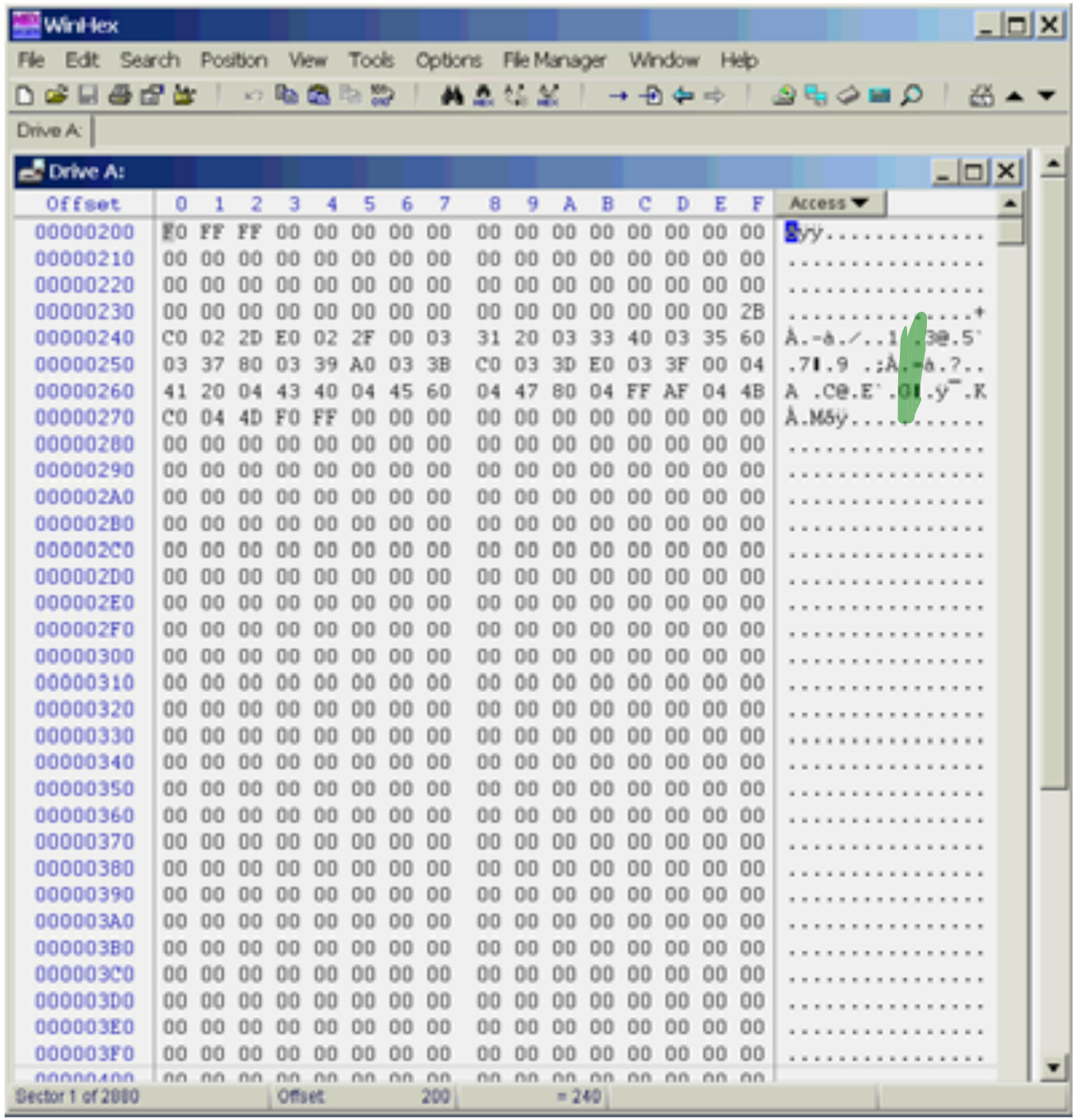
hunter-floppy

\

| Name | Type | Size | Created | Modified | Accessed | Attr. | 1st sector |
|---|---|---|---|---|---|---|---|
| (Root directory) | | 7.0 KB | | | | | 19 |
| april | | 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 |
| skiways-getafix.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 | 122 B | 05/13/2003 12:37:54 | 05/13/2003 12:40:48 | 05/13/2003 | A | 257 |
| newaddress.txt | txt | 122 B | 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 | | | | | |
| Idle space | | | | | | | |

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

# FAT


WinHex
File Edit Search Position View Tools Options File Manager Window Help
Drive A:
Drive A:
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F Access
00000200 E0 FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00
00000210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2B
00000240 C0 02 2D E0 02 2F 00 03 31 20 03 33 40 03 35 60
00000250 03 37 80 03 39 A0 03 3B C0 03 3D E0 03 3F 00 04
00000260 41 20 04 43 40 04 45 60 04 47 80 04 FF AF 04 4B
00000270 C0 04 4D F0 FF 00 00 00 00 00 00 00 00 00 00 00
00000280 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000290 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000002A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000002B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000002C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000002D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000002E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000002F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000310 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000320 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000330 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000340 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000350 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000360 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000370 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000380 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000390 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Sector 1 of 2080
Offset 200
= 240

# 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.

# 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 $LogFile
- podpira več funkcionalnosti glede datotek
  - pravica dostopa (*ACL – Access Control List*)
- bolje varovan, saj hrani kopije podatkov o datotečnem sistemu na večih mestih ($MFTMirr)

# 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) |

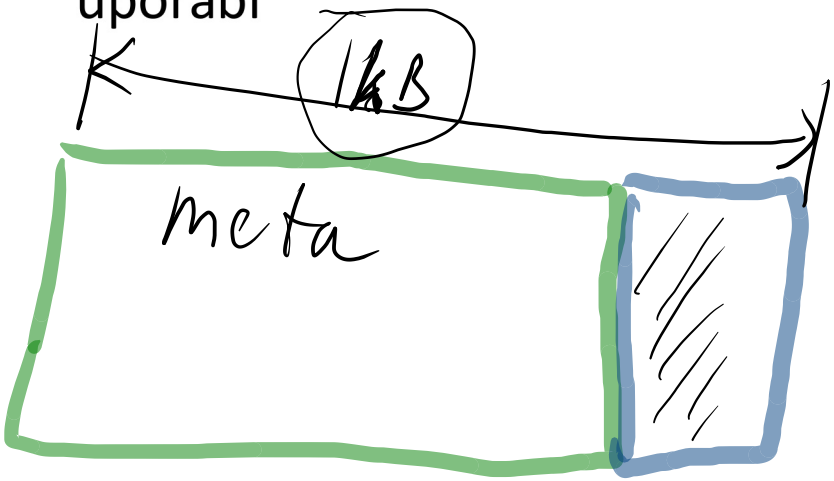
Table 3.1.1 – NTFS 3.0+ Metafiles

# Datotečni sistem NTFS

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

# NTFS – $MFT

- primer enega zapisa v $MFT
- zapis sestoji 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



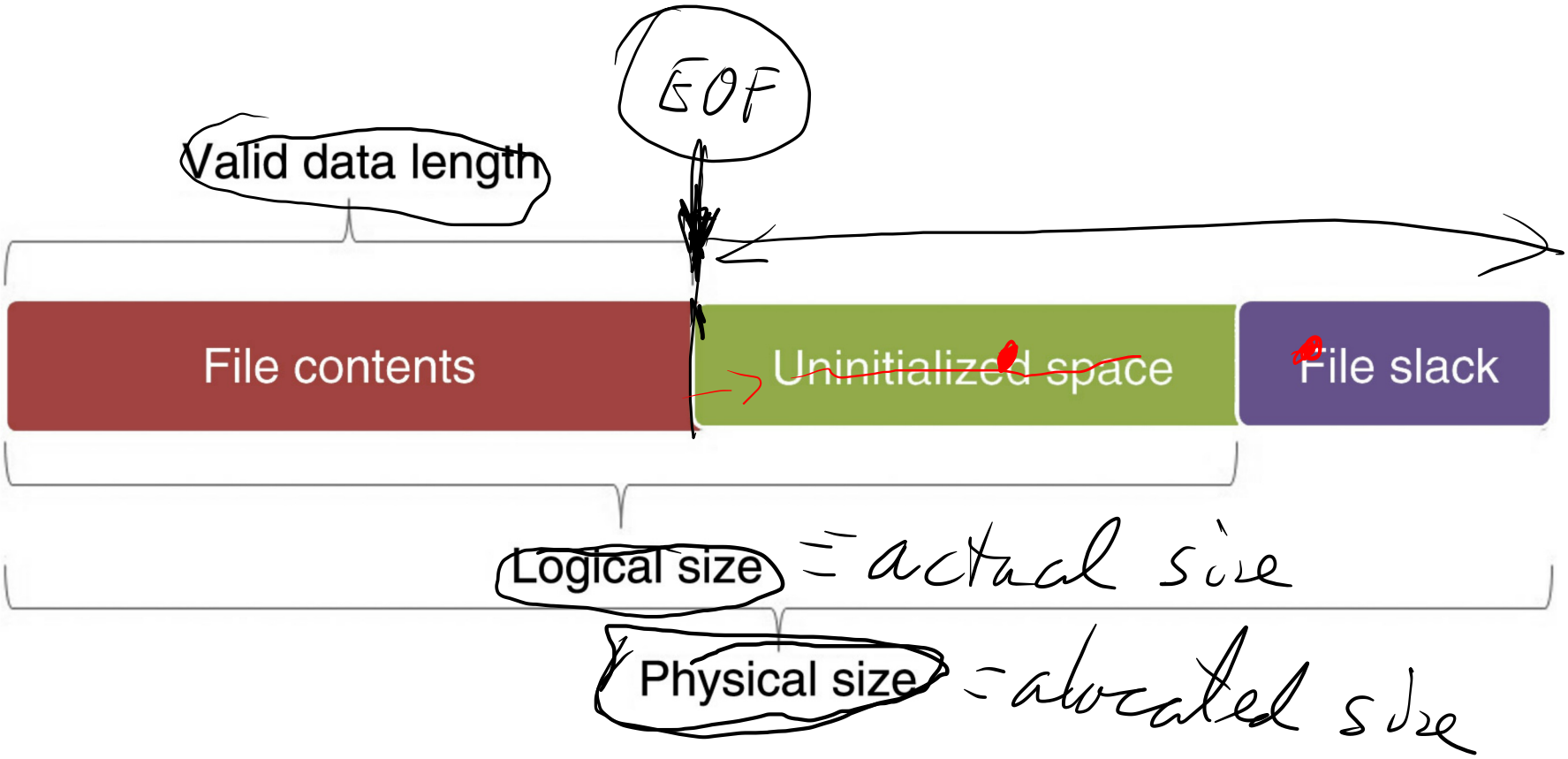

**Pointed to by file:**
E:\/review.pgd
**File Type:**
data
**MD5 of content:**
19d3508b078a10b3852b75f46ef9be5a
**SHA-1 of content:**
3229c020dcbd2c38ba44c462c1970cbc13db473b
**Details:**
MFT Entry Header Values:
Entry: 29 Sequence: 1
$LogFile Sequence Number: 16842551
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0 Security ID: 260
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

$FILE_NAME Attribute Values:
Flags: Archive
Name: review.pgd
Parent MFT Entry: 5 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

# NTFS – iskanje podatkov

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



# NTFS – MFT zapis

- pogled na MFT zapis in razlika med obema velikostima

'00 04' = 0400 16

'E8 03' = 03E8 16

```
0C07F5000  46 49 4C 45 30 00 03 00  31 43 0C 8F 00 00 00 00  FILE0    1C ▌
0C07F5010  03 00 02 00 38 00 01 00  E0 01 00 00 00 04 00 00      8    à
0C07F5020  00 00 00 00 00 00 00 00  05 00 00 00 D4 1F 00 00                Ô
0C07F5030  02 00 00 00 00 00 00 00  10 00 00 00 60 00 00 00                `
0C07F5040  00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00            H
0C07F5050  48 08 C6 77 A8 C5 CA 01  48 08 C6 77 A8 C5 CA 01  H Æw¨ÅÊ H Æw¨ÅÊ
0C07F5060  48 08 C6 77 A8 C5 CA 01  28 D3 9A 7A A8 C5 CA 01  H Æw¨ÅÊ (Ó▌z¨ÅÊ
0C07F5070  20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0C07F5080  00 00 00 00 69 01 00 00  00 00 00 00 00 00 00 00      i
0C07F5090  00 00 00 00 00 00 00 00  30 00 00 00 70 00 00 00            0   p
0C07F50A0  00 00 00 00 00 00 03 00  52 00 00 00 18 00 01 00            R
0C07F50B0  E6 24 00 00 00 00 01 00  48 08 C6 77 A8 C5 CA 01  æ$       H Æw¨ÅÊ
0C07F50C0  48 08 C6 77 A8 C5 CA 01  48 08 C6 77 A8 C5 CA 01  H Æw¨ÅÊ H Æw¨ÅÊ
0C07F50D0  48 08 C6 77 A8 C5 CA 01  00 00 00 00 00 00 00 00  H Æw¨ÅÊ
0C07F50E0  00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00
0C07F50F0  08 02 43 00 4D 00 44 00  4C 00 41 00 42 00 7E 00    C M D L A B ~
0C07F5100  32 00 73 00 65 00 74 00  30 00 00 00 88 00 00 00  2 s e t 0   ▌
0C07F5110  00 00 00 00 00 00 02 00  6A 00 00 00 18 00 01 00            j
0C07F5120  E6 24 00 00 00 00 01 00  48 08 C6 77 A8 C5 CA 01  æ$       H Æw¨ÅÊ
0C07F5130  48 08 C6 77 A8 C5 CA 01  48 08 C6 77 A8 C5 CA 01  H Æw¨ÅÊ H Æw¨ÅÊ
0C07F5140  48 08 C6 77 A8 C5 CA 01  00 00 00 00 00 00 00 00  H Æw¨ÅÊ
0C07F5150  00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00
0C07F5160  14 01 63 00 6D 00 64 00  4C 00 61 00 62 00 73 00    c m d L a b s
0C07F5170  2D 00 73 00 65 00 74 00  76 00 61 00 6C 00 69 00  - s e t v a l i
0C07F5180  64 00 64 00 61 00 74 00  61 00 00 00 00 00 00 00  d d a t a
0C07F5190  80 00 00 00 48 00 00 00  01 00 00 00 00 00 04 00  ▌   H
0C07F51A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0C07F51B0  40 00 00 00 00 00 00 00  00 10 00 00 00 00 00 00  @
0C07F51C0  00 04 Logical Size 00 00 00  E8 03 Valid Data Length 0 00      è
0C07F51D0  31 01 CE AB 03 00 01 00  FF FF FF FF 82 79 47 11  1 Î«    ÿÿÿÿ▌yG
```

# NTFS – iskanje podatkov

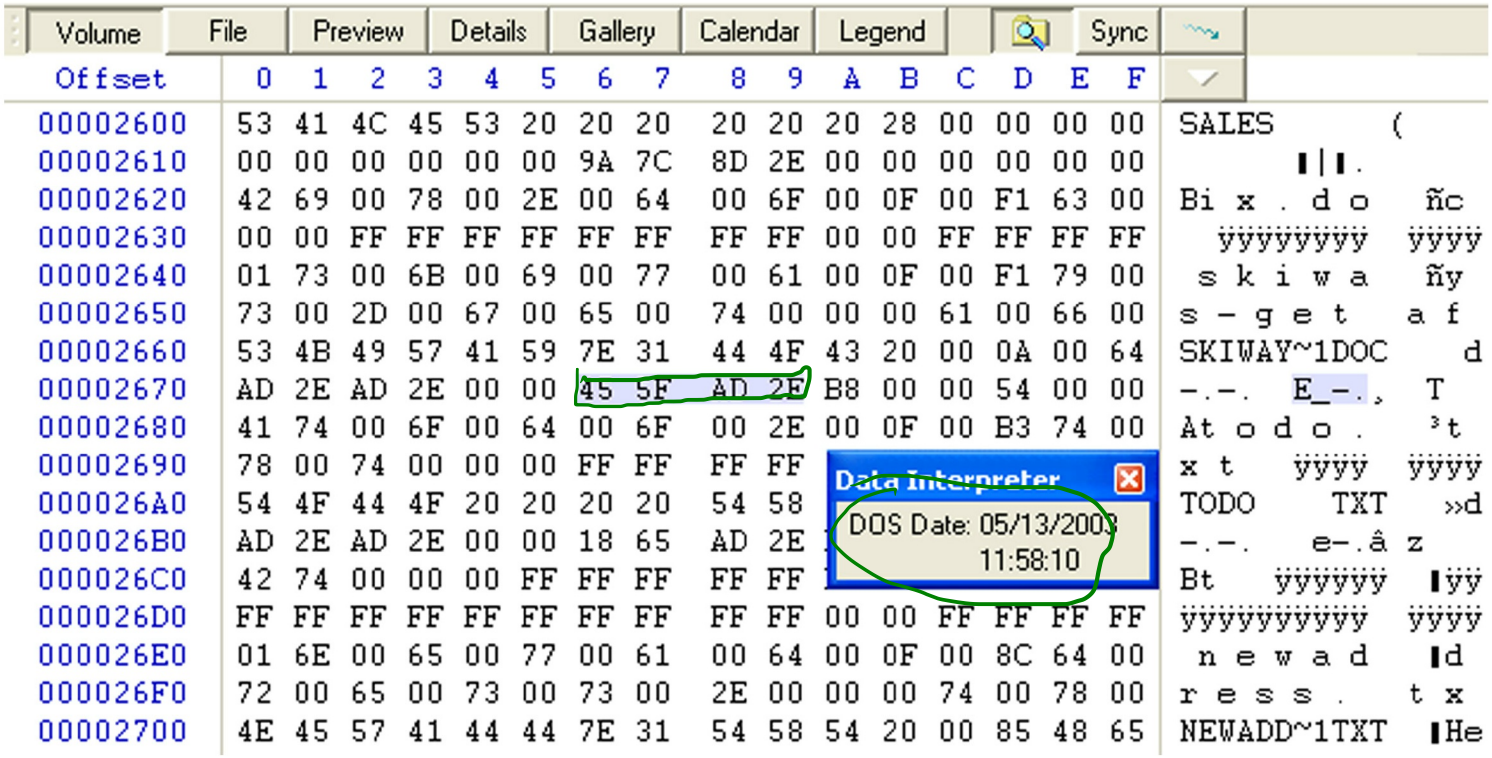
- v imeniku lahko obstajajo datoteke z enakimi imeni

# 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?

# Kodiranje časa pri datotekah

- FAT: 1.1.1980 + LLLLLLLM MMMDDDDD hhhhhmmm mmmsssss



# Kodiranje časa pri datotekah

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

# 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(*)
  - zbriši: ZD, VS
- posebnosti:
  - datoteka na palčki, lahko preko scp/...: TV > ZS
  - pri brisanju imenika, se podatki o datotekah ne spreminjajo

# 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 prepiše datoteko v poseben imenik ter jo šele nato natisne
  - *C:\Windows\Spool\Printers*, *C:\WinNT\System32\Spool\Printers*
  - tudi, ko tiskamo spletno vsebino ipd.

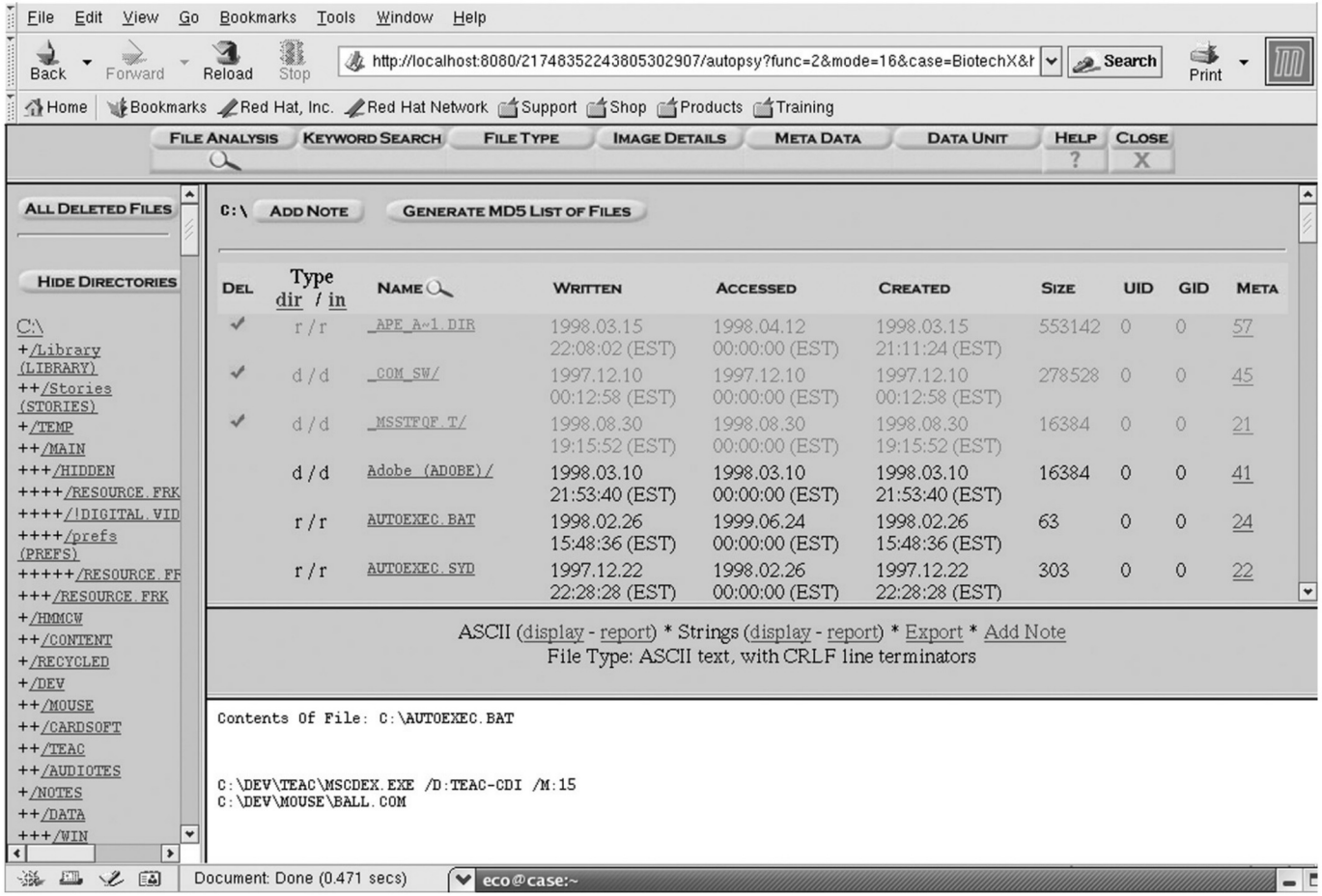
# NTFS – sledi datotek ...

- *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*)?

# 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/)



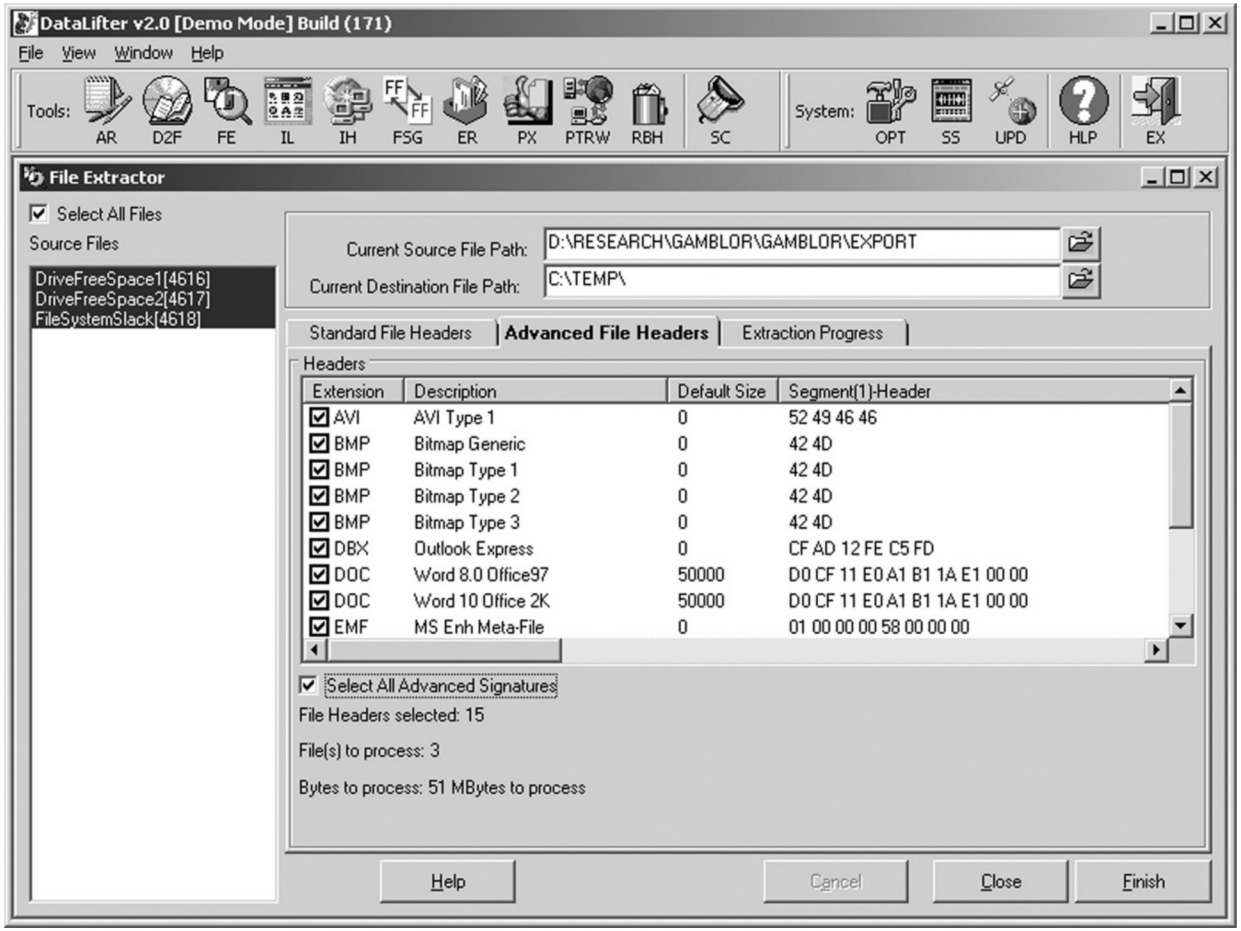
# Reševanje podatkov ...

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

# Reševanje podatkov ...

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

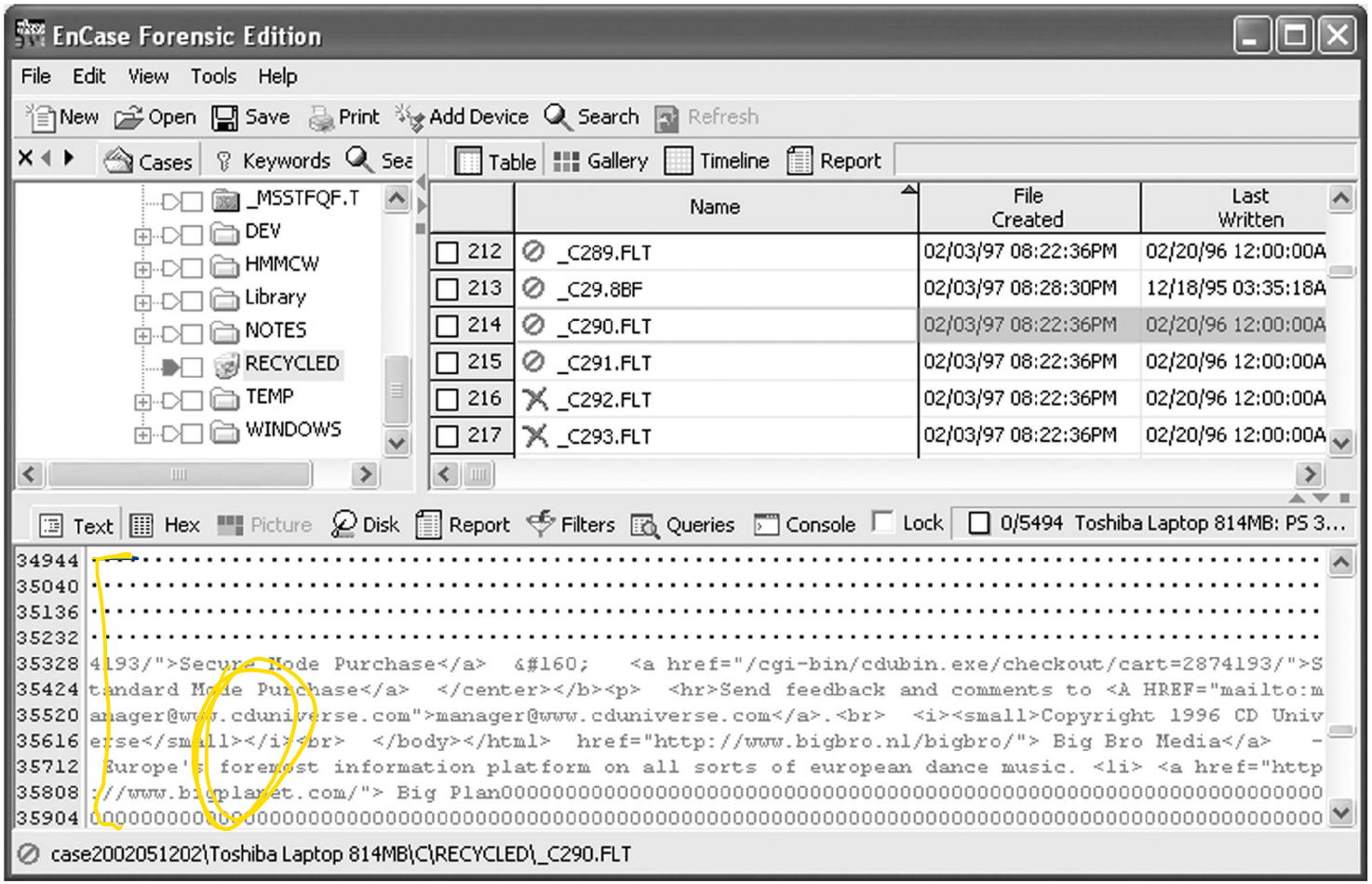
- orodje DataLifter: iščemo izgubljeno datoteko iz dveh gmot praznega prostora in enega preostanka datotečnega sistema



# Reševanje podatkov ...

- če majhna datoteka prepiše veliko, lahko večino velike datoteke rekonstruiramo

- 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,
  - pojavljanje in brisanje virov,
  - napake itd.
- shranjene na *%systemroot%\system32\config* (*c:\winnt\...*)
  - različne zabelžke 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.

# Register

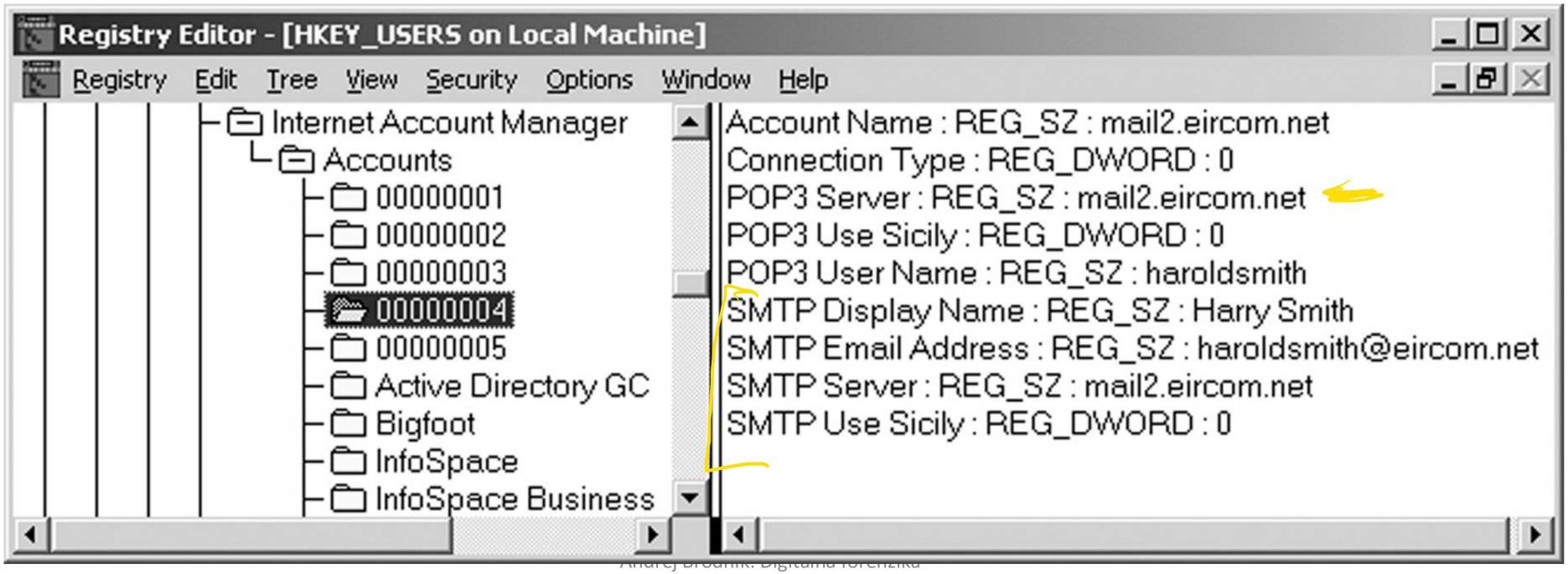
- v OS Windows so spremenljivke okolja procesa definirane v registru
- dejansko so podatki shranjeni v datotekah (*hives*) v sistemskem imeniku *%systemroot%\system32\config*
  - *ntuser.dat* za vsakega uporabnika svoja datoteka
- datoteke lahko pregledujemo z Windows orodjem regedt32 (EnCase, FTK, ...)

# Register

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

# Omrežne sledi

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

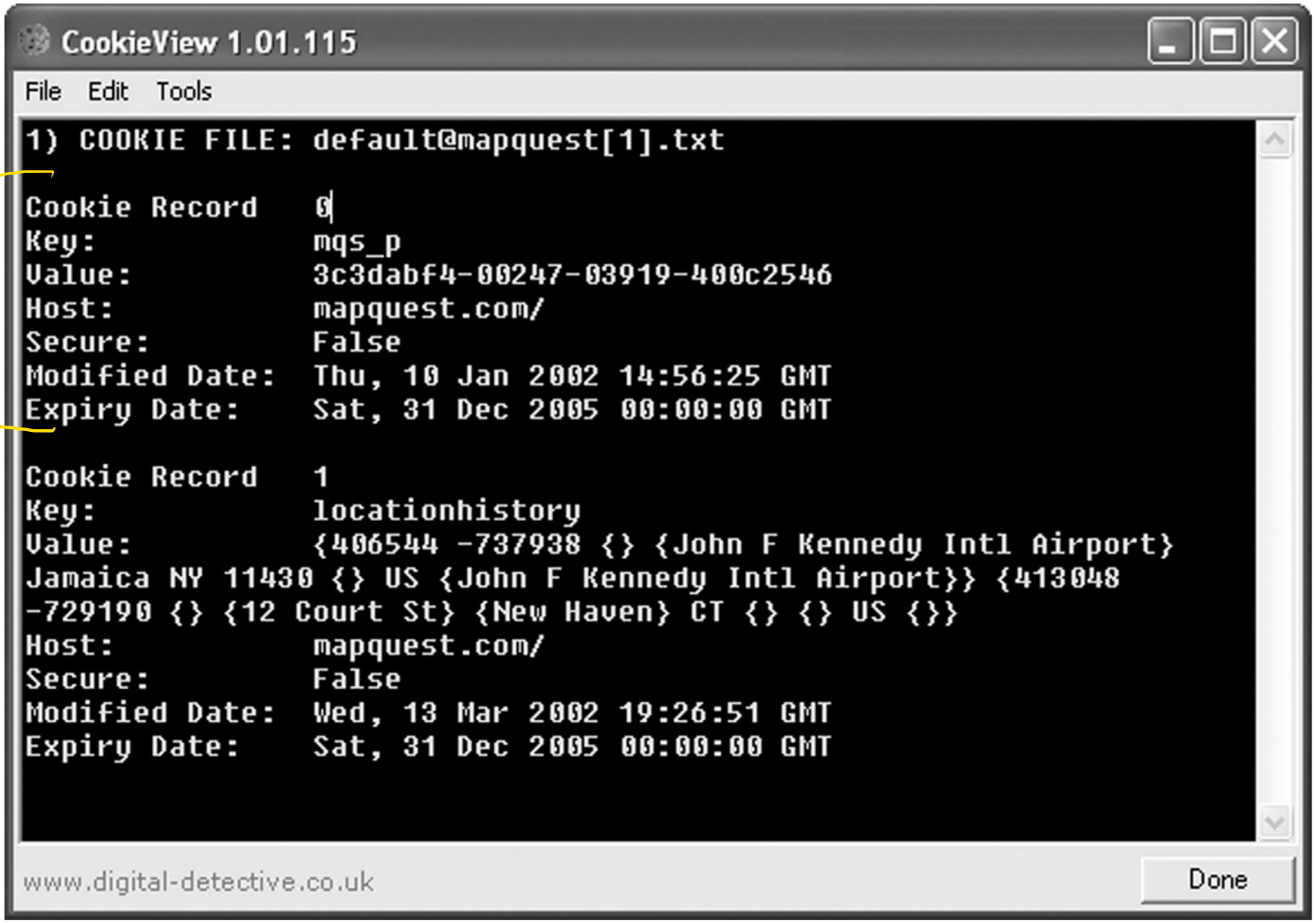


# Omrežne sledi - brskalniki

- 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: *Oddesa* (www.odessa.sourceforge.net)
- lokalni predpomnilnik
- piškoti

# Brskalniki – piškoti

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

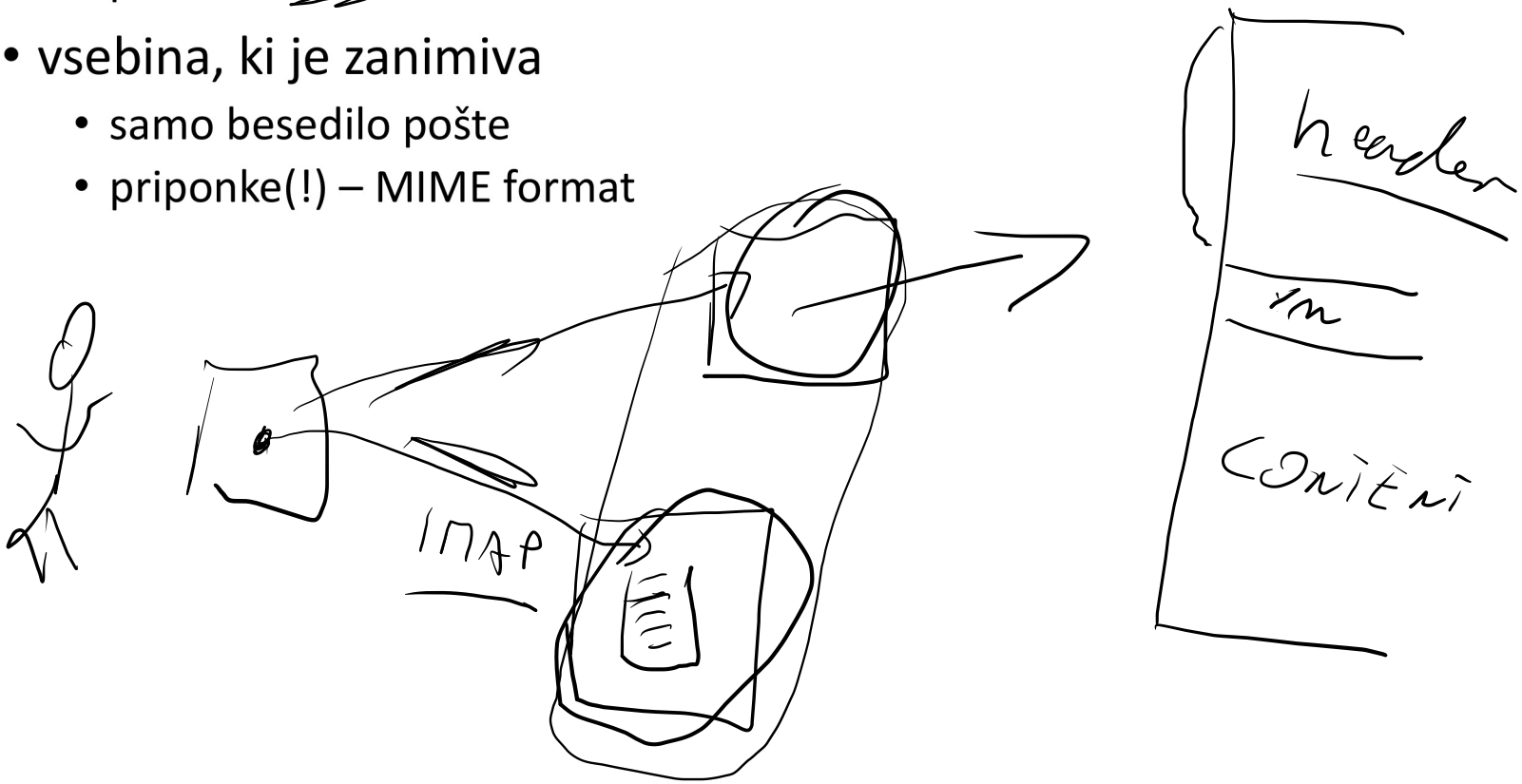


# Brskalniki

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

# 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
  - priponke(!) – MIME format



# 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

# Sledi omrežnega dostopa

- telnet dostop do acf2.nyu.edu