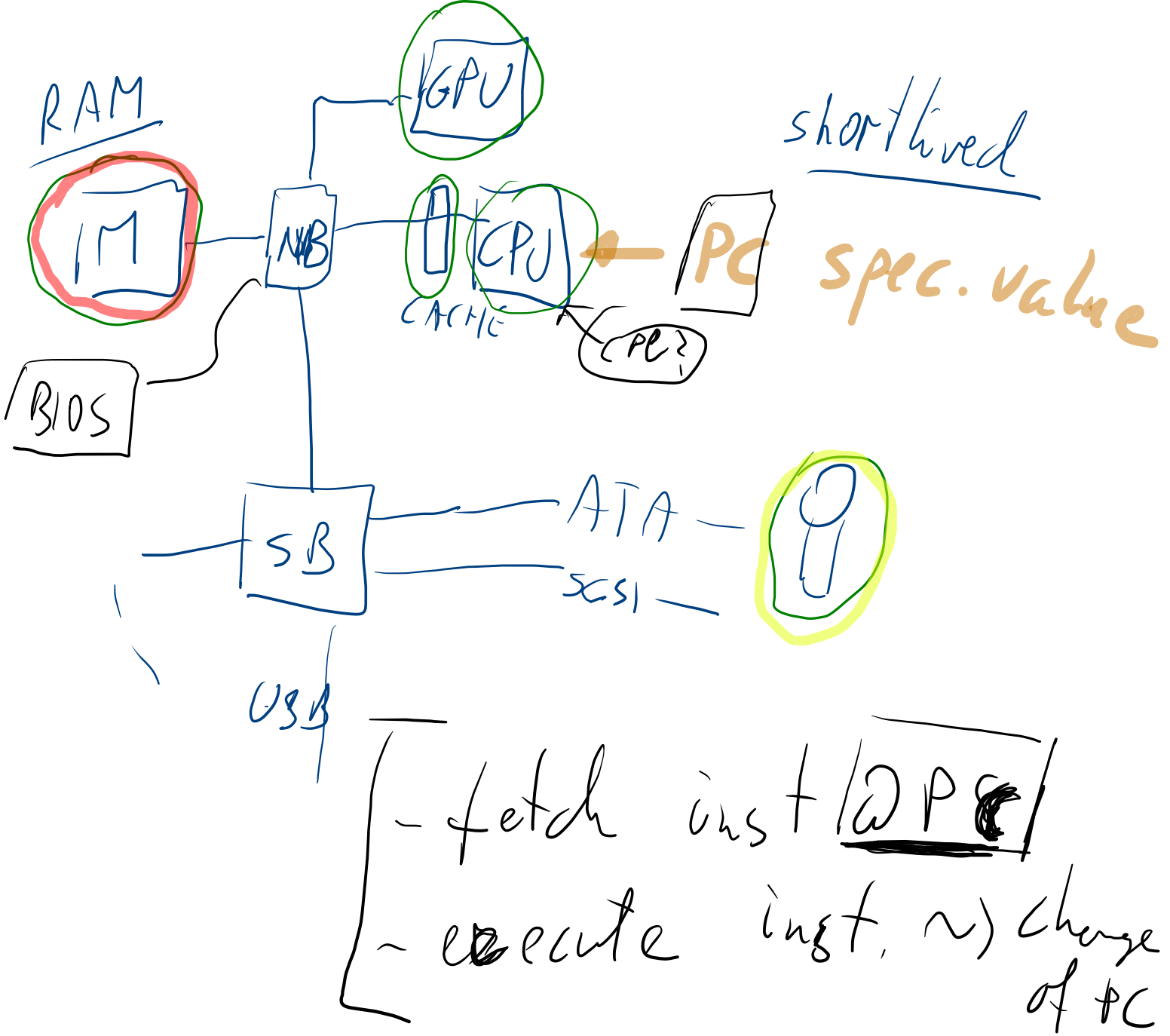
Digitalna forenzika

Andrej Brodnik

Računalnik

poglavje 15

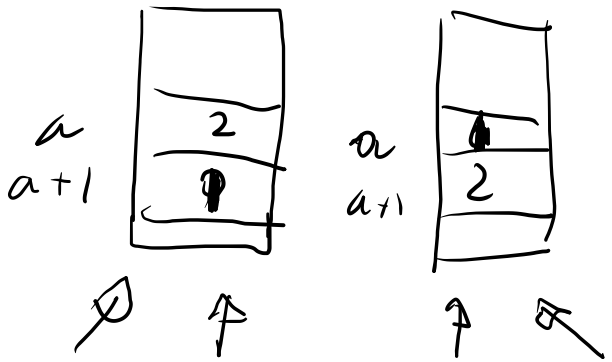
- pričakovano predznanje:
  - arhitektura računalnikov
  - osnove delovanja (BIOS)
  - operacijski sistem
  - sekundarni pomnilnik (disk) in njegova organizacija
  - datotečni sistemi


RAM
IM
GPU
NB
CPU
CACHE
PC
PC'
BIOS
SB
ATA
SCSI
USB
?
shortlived
spec. value
- fetch inst @ PC
- execute inst. ~) change of PC

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

Zagon računalnika ...



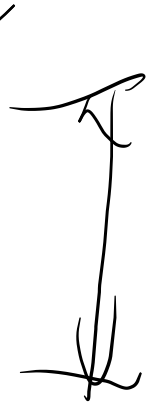
- primer *Moussawi*:

> 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

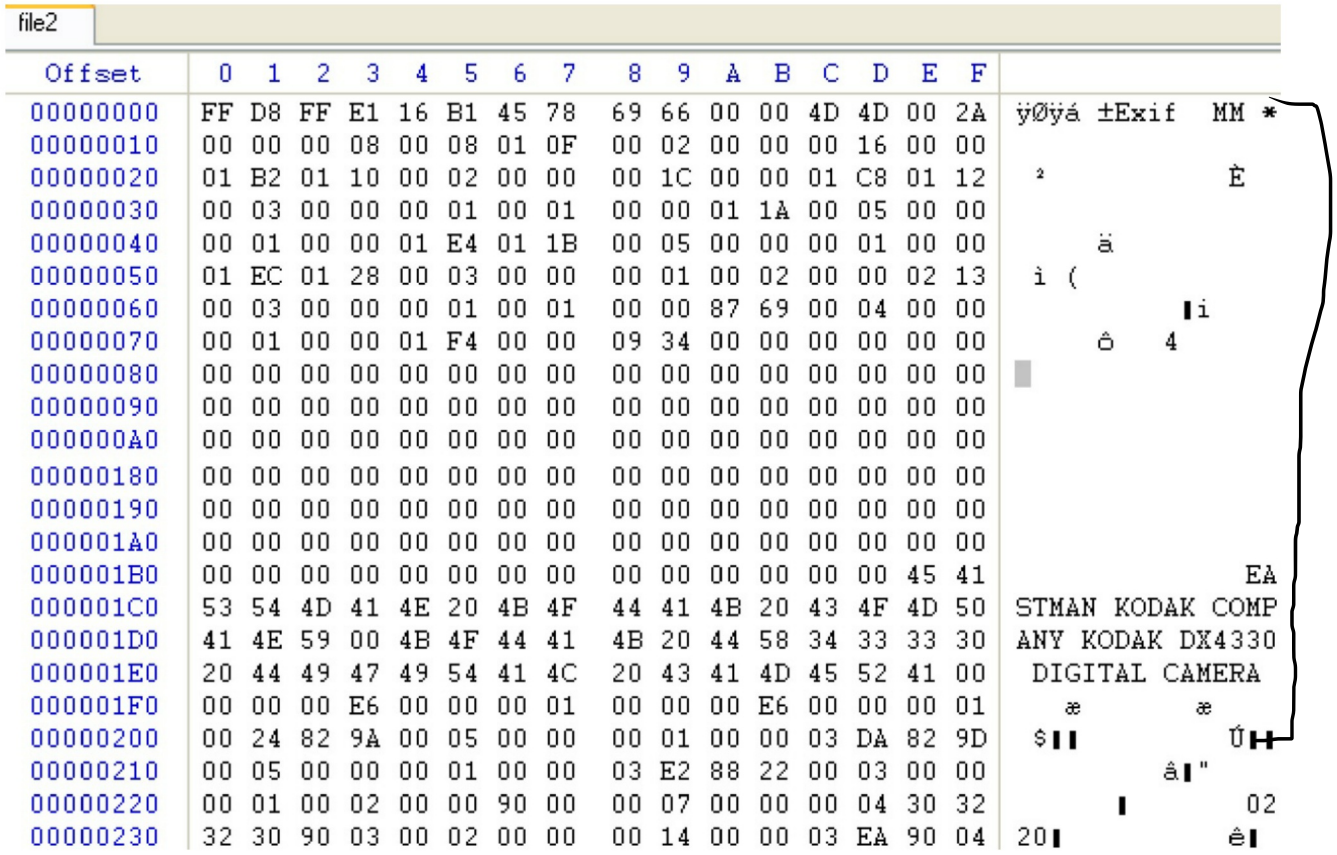
Format datoteke

- datoteke imajo na začetku posebne podpise (www.garykessler.net/library/file_sigs.html)
- 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*



Format datoteke –primer

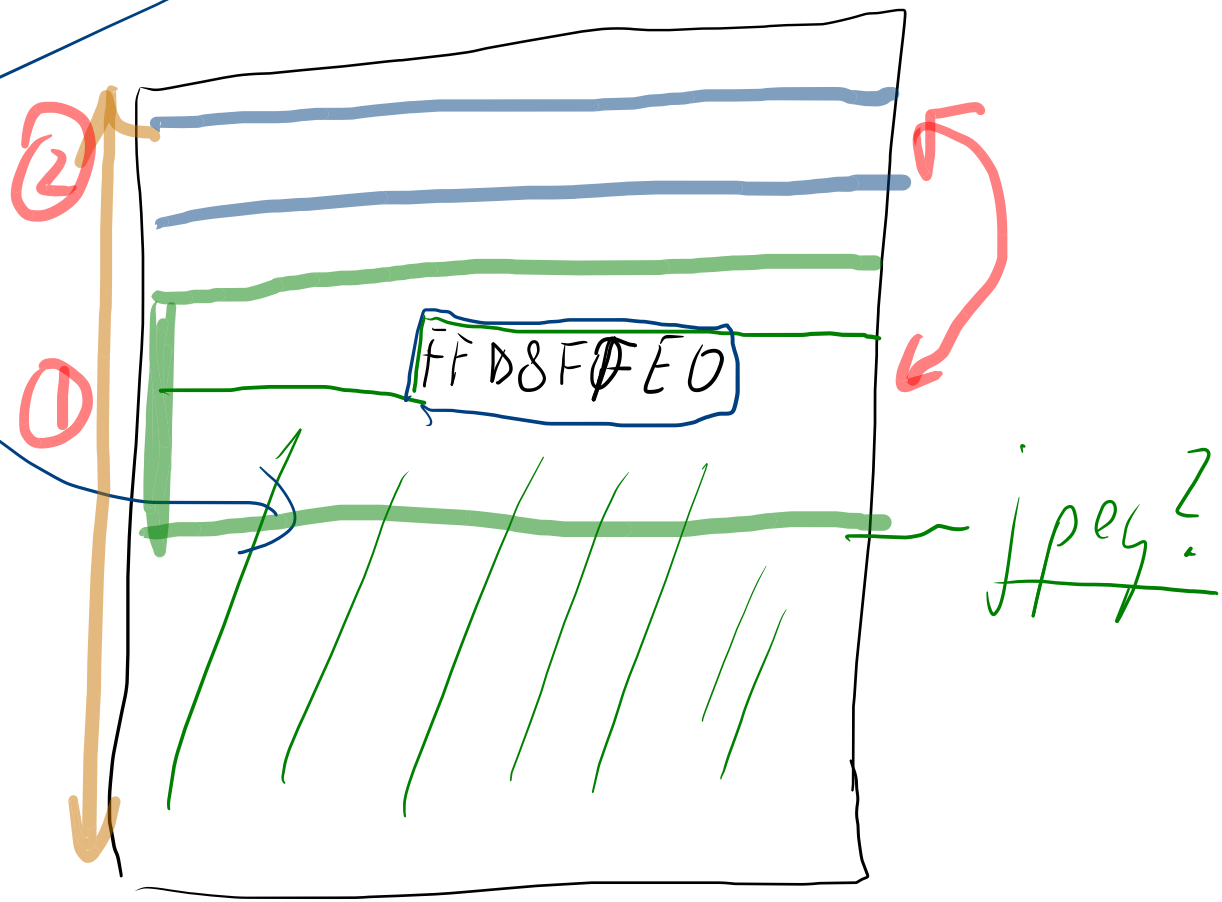
- jpeg zakodirana exif (*Exchangeable image file format*) datoteka



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/)

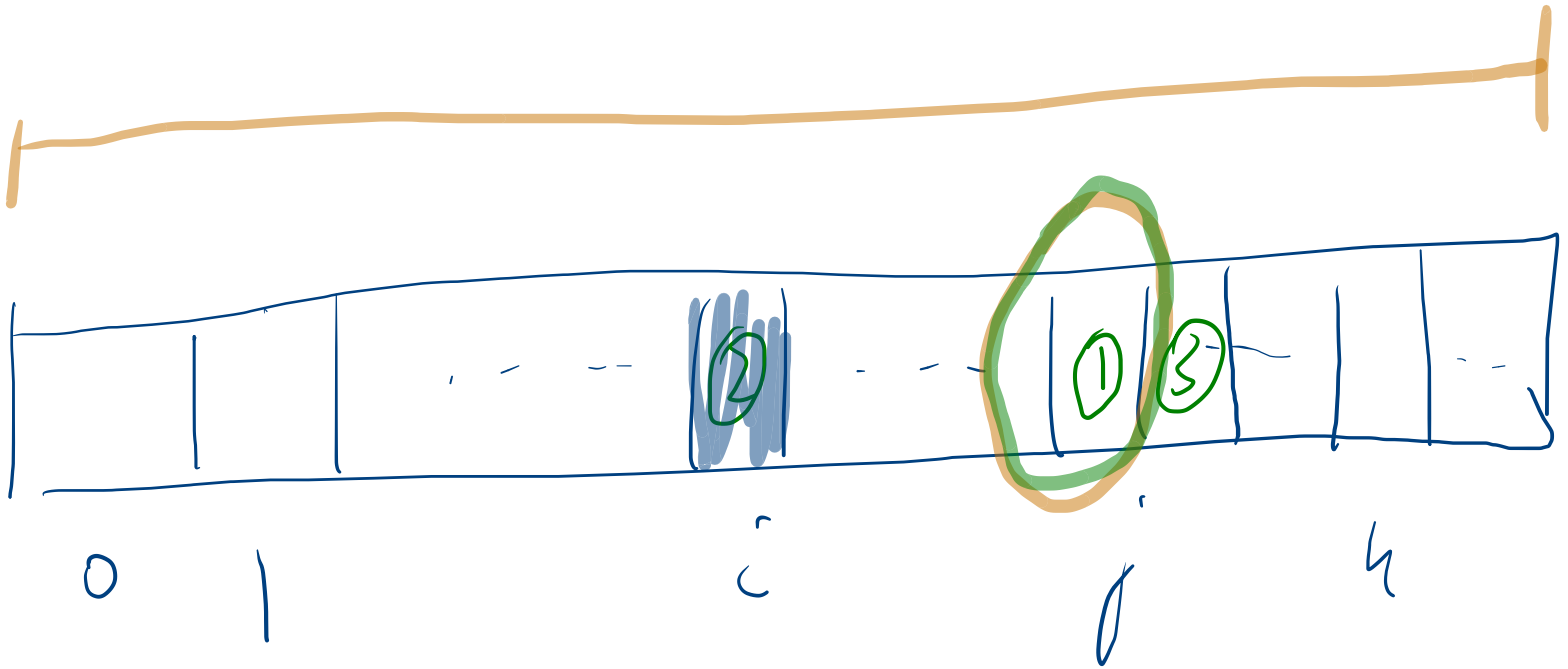
jpeg files have internal structure

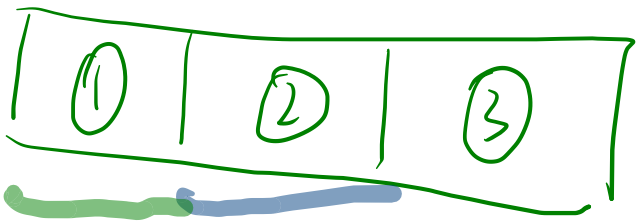


Disk:

- map / folder / directory:
  - list of entries
  - with each entry metainformation
    - name
    - extension
    - date
    - ...

- data / content is stored elsewhere


0
1
i
j
k


1
2
3

Izrezovanje

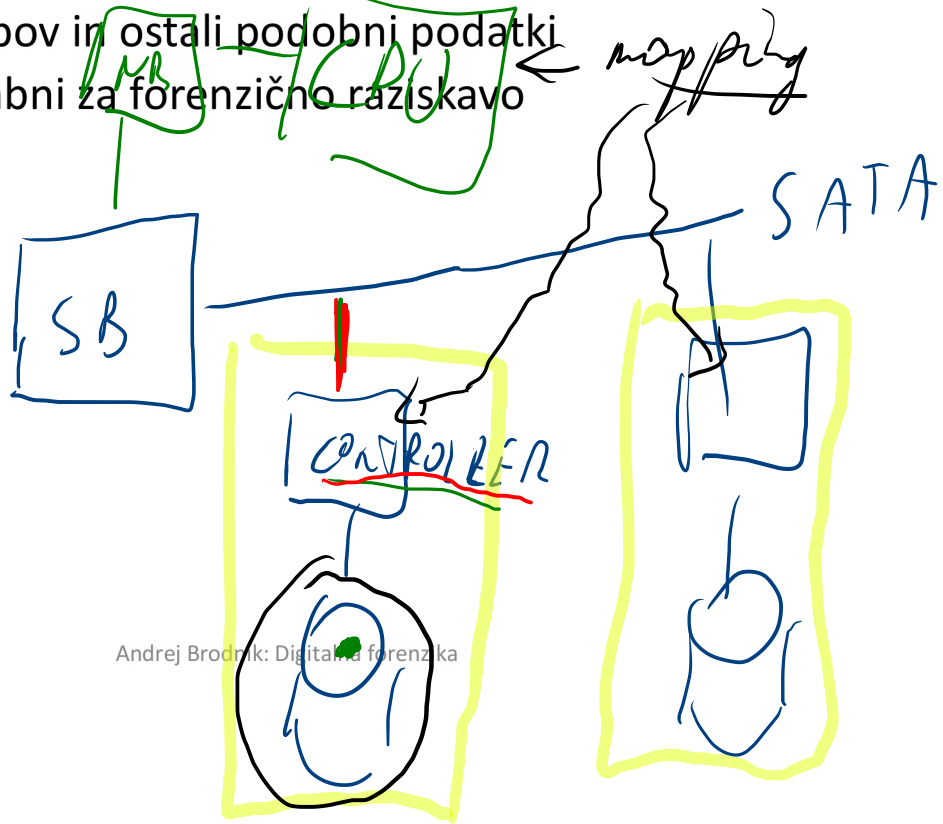
- na koncu dobimo samo vsebino in ne meta-podatkov iz imenika
- drugi problem je, da so lahko podatki razmetani po disku
  - Adroit (http://digital-assembly.com/products/adroit-photo-forensics/)

Format datoteke – izziv

- *Izziv:* vgnezdite 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.

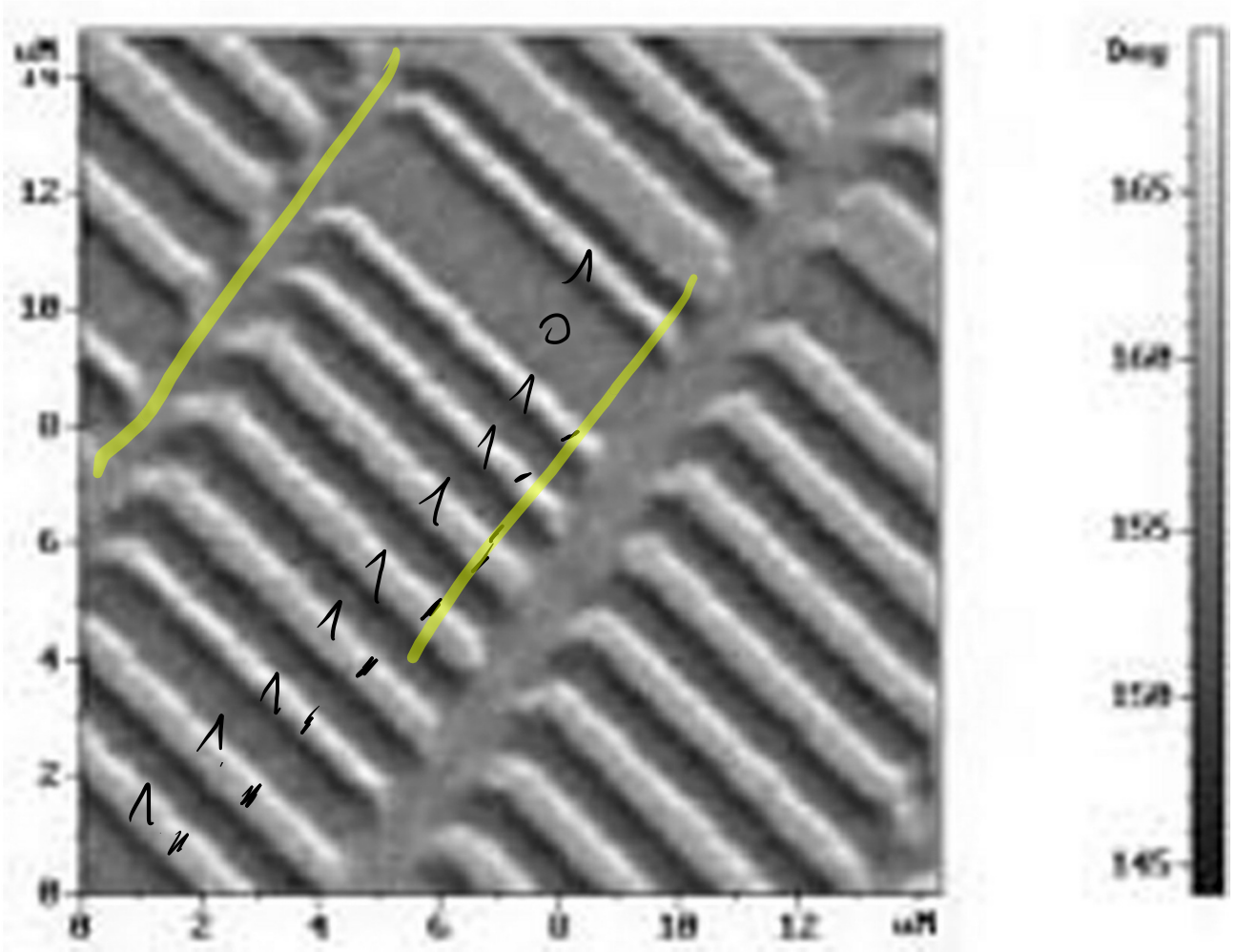
Shramba podatkov in skrivanje

- 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



Shramba podatkov in skrivanje

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



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?