

Digitalna forenzika

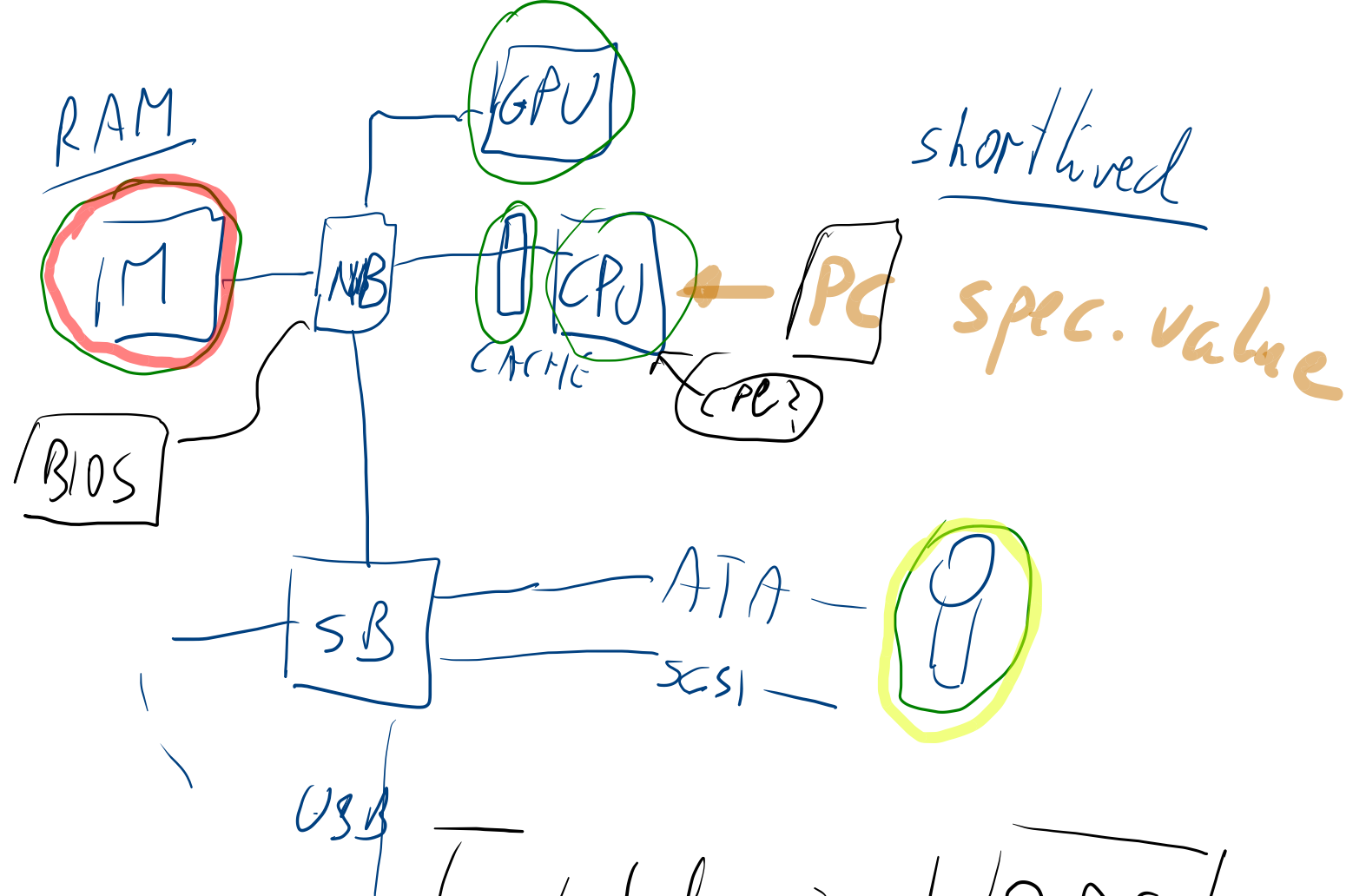
Andrej Brodnik

Računalnik

- pričakovano predznanje:

- arhitektura računalnikov VON NEUMANN
- osnove delovanja (BIOS) ←
- operacijski sistem
- sekundarni pomnilnik (disk) in njegova organizacija
- datotečni sistemi

poglavje 15



- fetch inst / PC
- execute inst, ~) change of PC

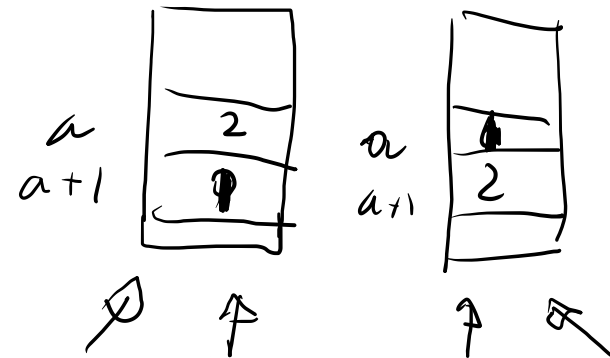
Zagon računalnika

- koraki ob zagonu računalnika ← SFARI - UP
- 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

~~Battery protected~~

$$258 = 1 \cdot 256 + 2$$

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

8-bit code

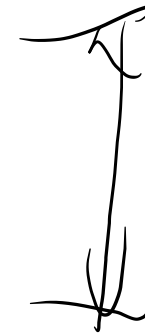
Latin 1 : 28 → 555

Latin-2



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

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	ÿØÿá ±Exif MM *
00000010	00	00	00	08	00	08	01	0F	00	02	00	00	00	16	00	00	È
00000020	01	B2	01	10	00	02	00	00	00	1C	00	00	01	C8	01	12	²
00000030	00	03	00	00	00	01	00	01	00	00	01	1A	00	05	00	00	ä
00000040	00	01	00	00	01	E4	01	1B	00	05	00	00	00	01	00	00	i (
00000050	01	EC	01	28	00	03	00	00	00	01	00	02	00	00	02	13	i (
00000060	00	03	00	00	00	01	00	01	00	00	87	69	00	04	00	00	i
00000070	00	01	00	00	01	F4	00	00	09	34	00	00	00	00	00	00	ô 4
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	
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	45	41	EA
000001C0	53	54	4D	41	4E	20	4B	4F	44	41	4B	20	43	4F	4D	50	STMAN KODAK COMP
000001D0	41	4E	59	00	4B	4F	44	41	4B	20	44	58	34	33	33	30	ANY KODAK DX4330
000001E0	20	44	49	47	49	54	41	4C	20	43	41	4D	45	52	41	00	DIGITAL CAMERA
000001F0	00	00	00	E6	00	00	00	01	00	00	00	E6	00	00	00	01	æ æ
00000200	00	24	82	9A	00	05	00	00	00	01	00	00	03	DA	82	9D	§ Û
00000210	00	05	00	00	00	01	00	00	03	E2	88	22	00	03	00	00	â "
00000220	00	01	00	02	00	00	90	00	00	07	00	00	00	04	30	32	02
00000230	32	30	90	03	00	02	00	00	00	14	00	00	03	EA	90	04	è

Format datoteke

- datoteka je lahko gnezdena v drugi datoteki

- poiščemo datoteko
- jo lahko označimo in prepíšemo (*copy-paste*)
- ali uporabimo orodje dd

STUDY the copied
and content

- 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/>)

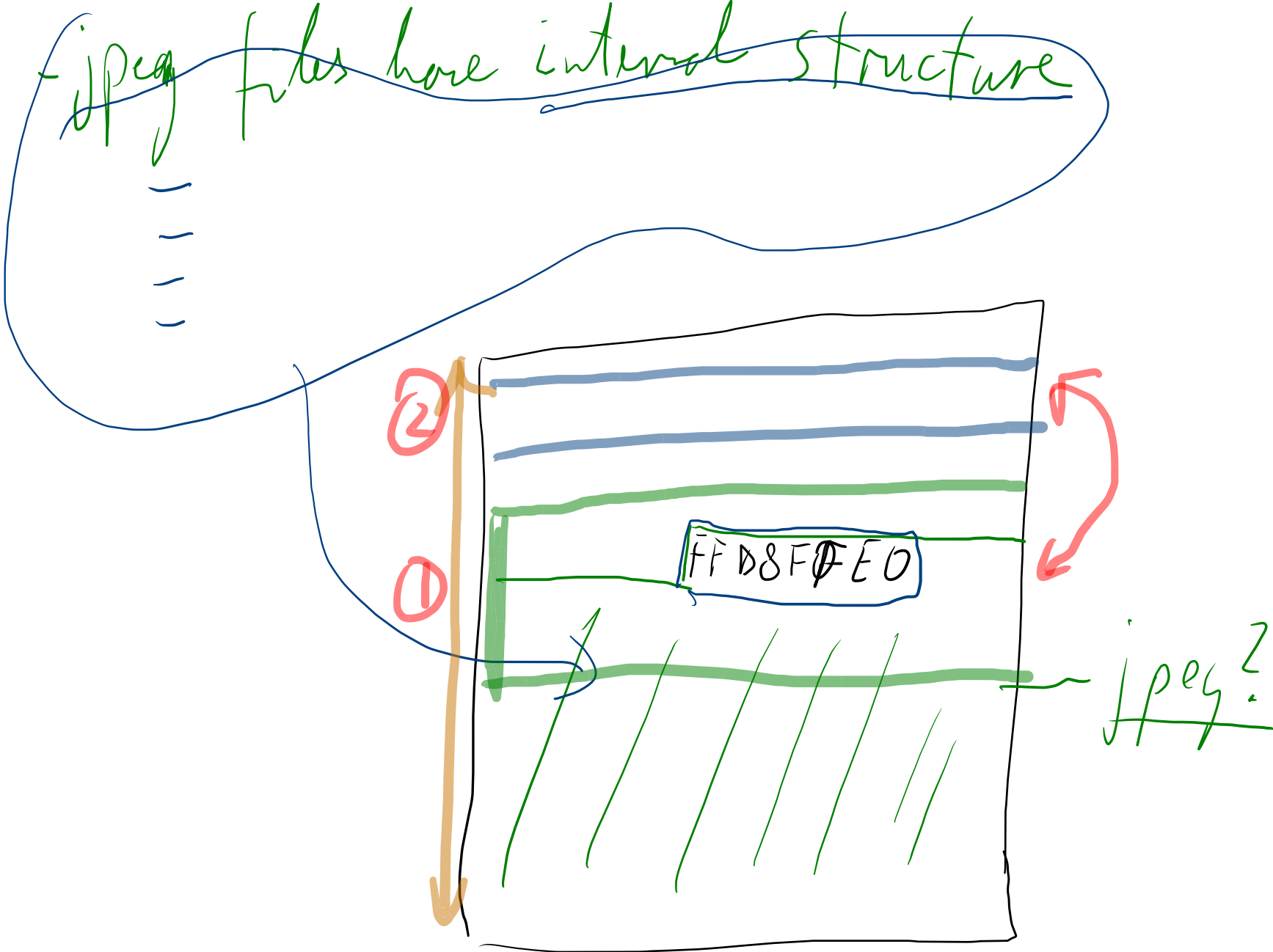
jpeg files have internal structure

②

①

FFD8F0E0

jpeg?



Disk:

- map / folder / directory:

- list of entries

- with each entry meta-information

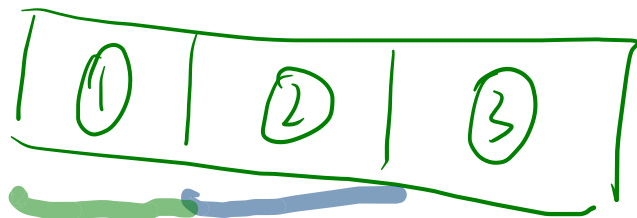
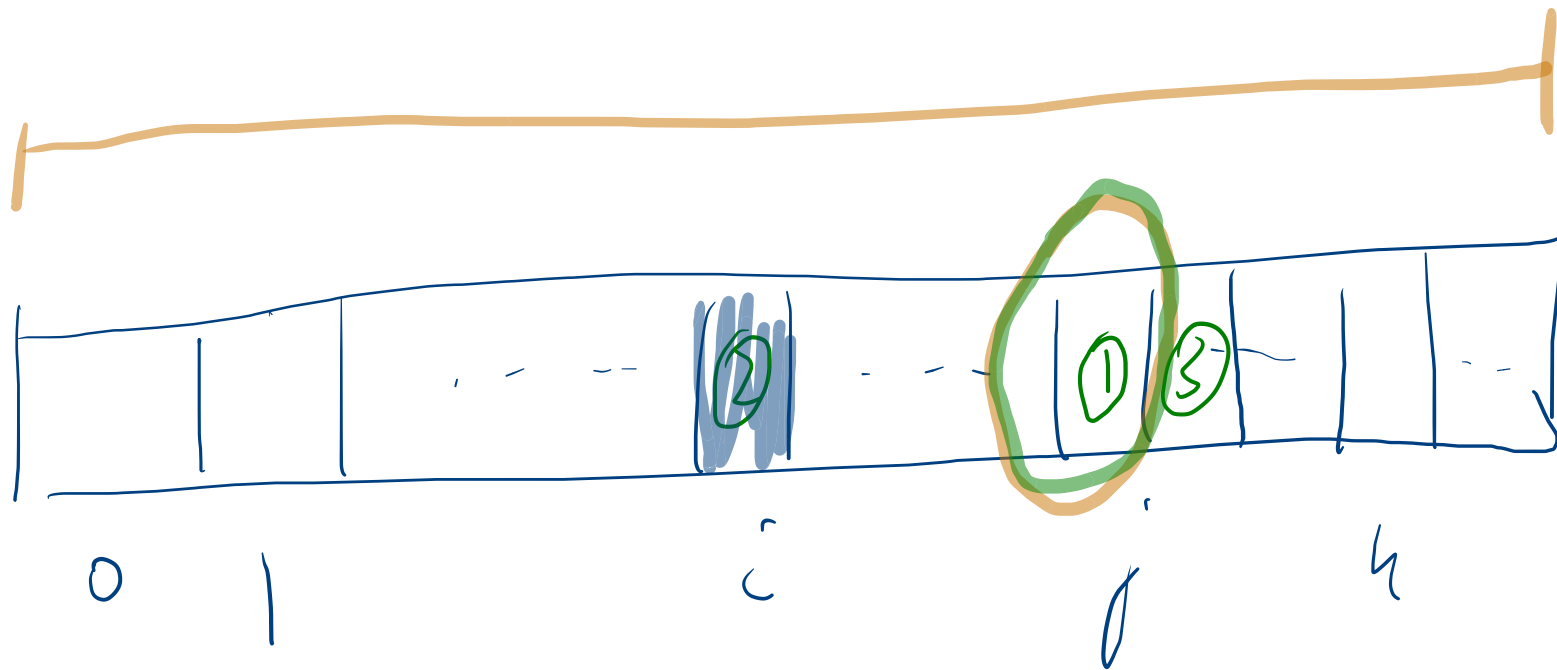
 - name

 - extension

 - date

 - ...

= data / content is stored elsewhere



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.

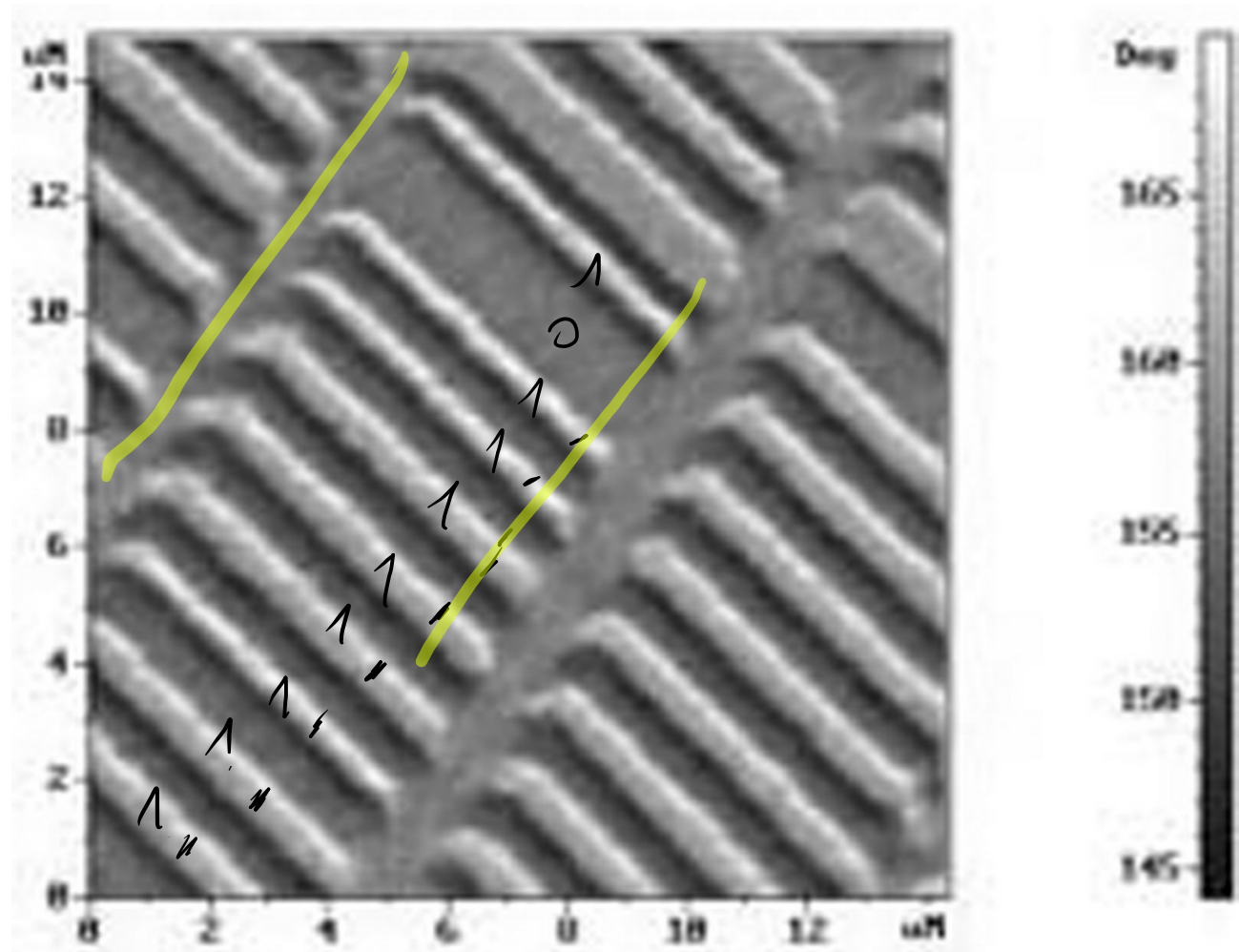
Shramba podatkov in skrivanje

- 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?





Cylinder



track
sectors

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, ...

⓪ kako izgleda organizacija pri SSD?

