



# Forenzika datotečnih sustava

Predrag Pale



# Second hand disks



NEWS

## Survey: 40% of hard drives bought on eBay hold personal, corporate data

*„A New York computer forensics firm found that 40% of the hard disk drives it recently purchased in bulk orders on eBay contained personal, private and sensitive information.”*

*(Computer World, 2009)*

<http://www.computerworld.com/article/2530795/data-center/survey--40--of-hard-drives-bought-on-ebay-hold-personal--corporate-data.html>

# Thrown away hard disks



## Missile data found on hard drives

**Sensitive information for shooting down intercontinental missiles as well as bank details and NHS records was found on old computers, researchers say.**

Of 300 hard disks bought randomly at computer fairs and an online auction site, 34% still held personal data.



Prof Andrew Blyth said he found pictures of someone with a gun and also pornography

*„Details of test launch procedures for the THAAD (Terminal High Altitude Area Defense) ground-to-air missile defense system were found on a disk bought on eBay.”*

(BBC News, 2009)

# Ciljevi ovog predavanja



- Cilj ovog predavanja **NIJE**
  - poučiti kako **koristiti** moderne forenzičke softverske **alate** i metode
    - **iako će i oni biti spomenuti**
- Cilj je
  - pokazati forenziku na **najosnovnijoj razini**
  - te dati uvid kako **datotečni sustavi funkcioniraju**,
  - jer to je ujedno i **temelj** svakog naprednijeg forenzičkog alata
- U sklopu ovog predavanja
  - obradit će se **osnovni koncepti** najpopularnijih datotečnih sustava
  - čime će studenti steći potrebno znanje za nastavak samostalnog istraživanja teme o datotečnim sustavima

# Preduvjeti za razumijevanje



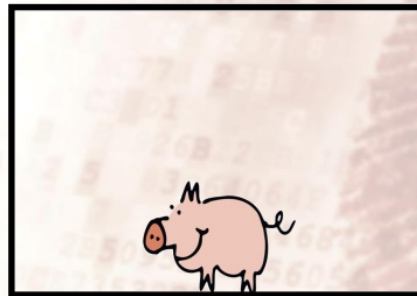
- Student mora poznavati pretvaranje vrijednosti između dekadskog, heksadekadskog i binarnog brojevnog sustava
  - gradivo kolegija Digitalna logika

- Razlikovati

- *Big-endian*

- “network byte order”
    - $2015 = 0x07\ 0XDF$

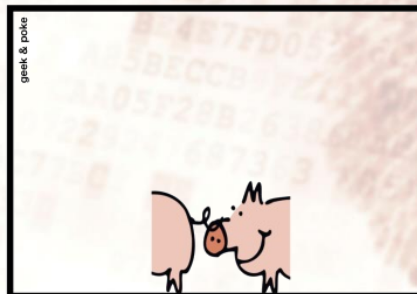
## SIMPLY EXPLAINED



BIG-ENDIAN

- *Little-endian*

- *microprocessors*
    - *Intel*
    - $2015 = 0XDF\ 0x07$



LITTLE-ENDIAN

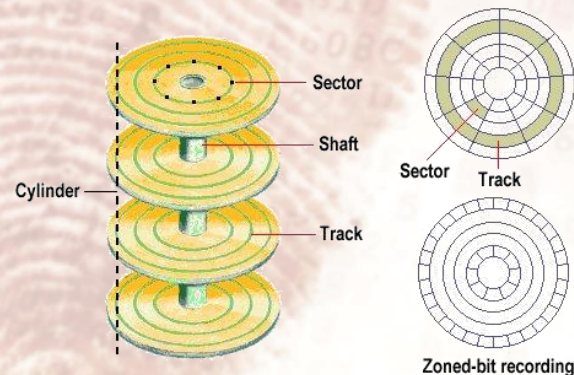
Picture taken from:

[geekandpoke.typepad.com/.a/6a00d8341d3df553ef01543533e604970c-pi](http://geekandpoke.typepad.com/.a/6a00d8341d3df553ef01543533e604970c-pi)

# Datotečni sustav



- U **fokusu** računalne forenzike nalazi se **trajna** memorija računala
  - koja **čuva** podatke i **nakon gašenja** računala
    - **tipično: diskovi, memorijske kartice, USB drive, ...**
- Kako bi računalo moglo upravljati memorijom i prepoznati značenje svakog pojedinog bita
  - svaka trajna memorija mora biti oblikovana (engl. *format*)
  - u **DATOTEČNI SUSTAV**
- Prilikom analize datotečnog sustava
  - najčešći ciljevi su **pronaći** datoteke,
  - **vratiti** obrisane datoteke i
  - **prepoznati** sakrivene podatke

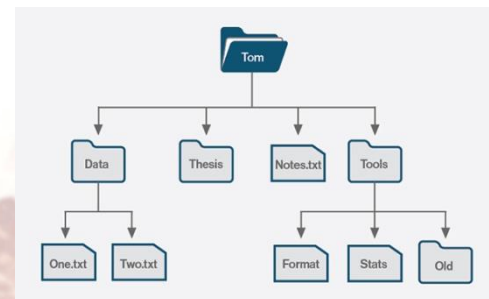


# Što je datotečni sustav



## • Datotečni sustav je

- **Apstrakcija**, pojam
- organizacijska **shema** za trajne memorije
- napravljena za **potrebe**
  - organiziranja, spremanja i dohvaćanja podataka
- **omogućuje** računalu rad s datotekama/podatcima
- danas je uglavnom **hijerarhijski/stablast**



# Kako bi mogao izgledati datotečni sustav?



- Sekvencijalni datotečni sustav
- Tipičan za neke (sekvencijalne) medije.

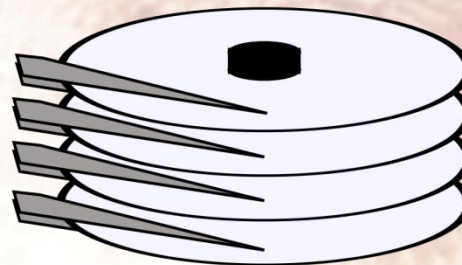
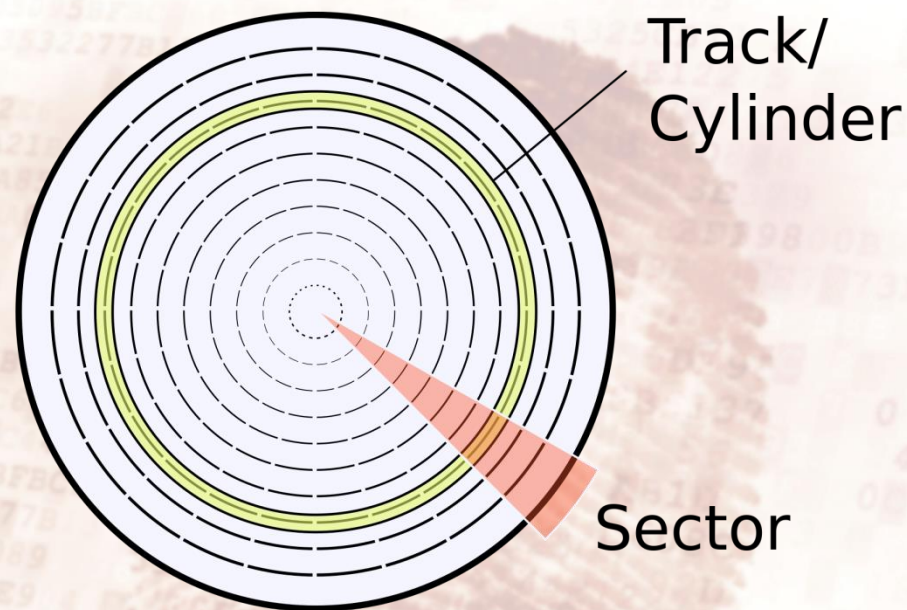
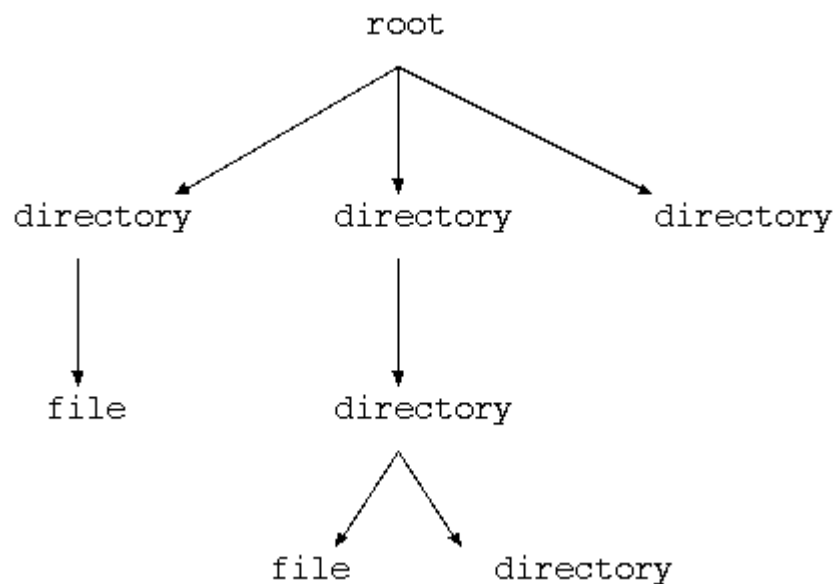




# Nasumični pristup (random access)



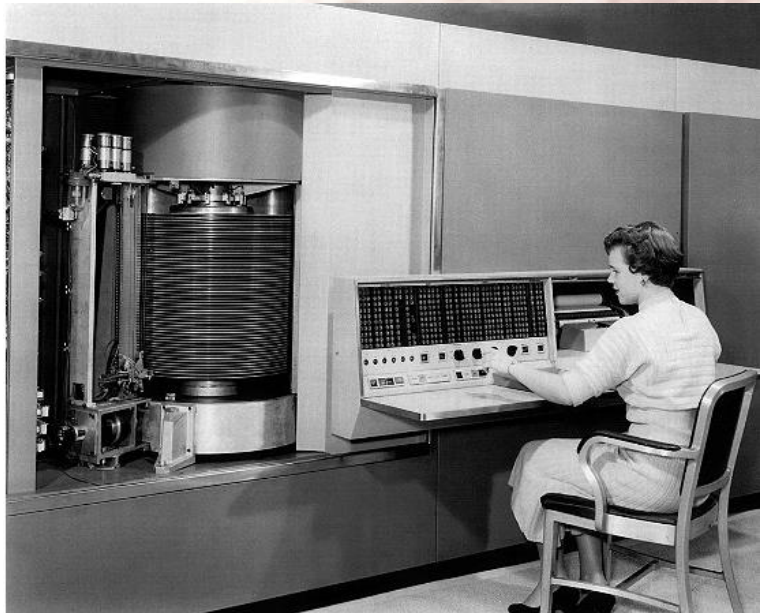
- ali medij je ipak i dalje djelomično sekvencijalan
- no, omogućuje
  - Hijerarhijski datotečni sustav



Heads

8 Heads,  
4 Platters

# Datotečni sustav je neovisan o uređaju



# Različite vrste datotečnih sustava



Local Disk (C:) Properties

General | Previous Versions | Quota  
Tools | Hardware | Sharing

Type: Local Disk  
File system: **NTFS**

Used space:	76.630.810.624 bytes	71,3 GB
Free space:	14.628.851.712 bytes	13,6 GB

Capacity: 91.259.662.336 bytes 84,9 GB

Drive C: [Disk Cleanup]

Compress this drive to save disk space  
 Allow files on this drive to have contents indexed in addition to file properties

OK Cancel Apply

Removable Disk (G:) Properties

General | Tools | Hardware | Sharing | ReadyBoost | Customize

Type: Removable Disk  
File system: **FAT**

Used space:	589.824 bytes	576 KB
Free space:	4.025.614.336 bytes	3,74 GB

Capacity: 4.026.204.160 bytes 3,74 GB

Drive G:

OK Cancel Apply

## Različita svojstva i fizički raspored

# Najčešće korišteni datotečni sustavi



- **Najčešći:**

- Windows: FAT12, FAT16, **FAT32**, exFAT, NTFS
- UNIX: **ext**, ext2, ext3, ext4

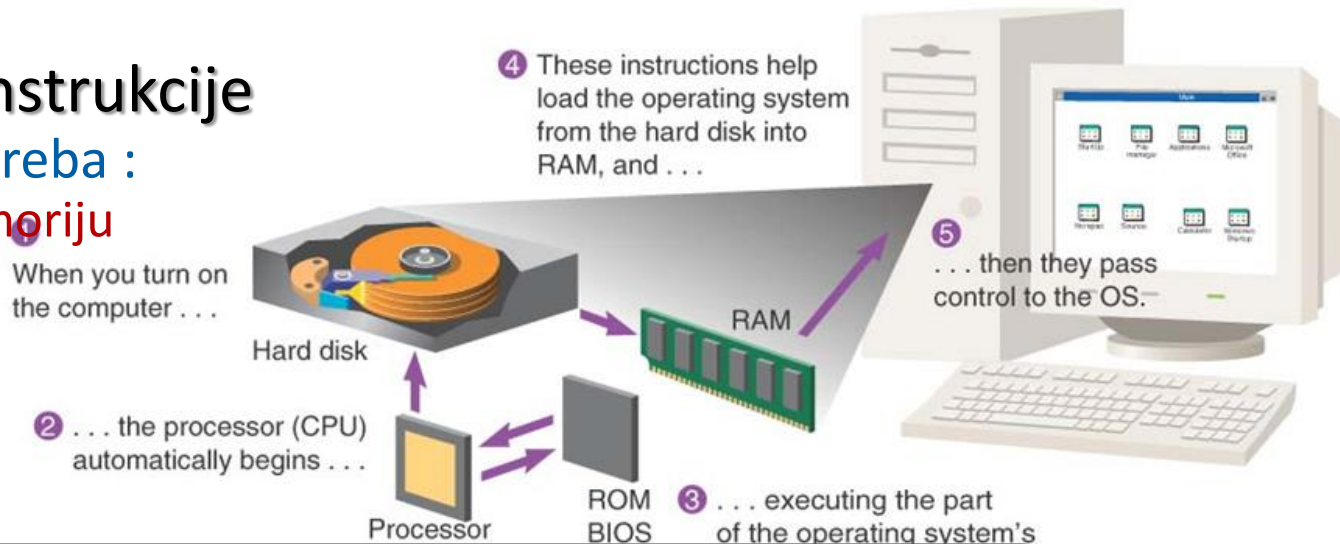
- **ostali**

- HFS, HFS+ (Mac OS)
- ISO9660, UDF (CD/DVD)
- JFS, ReiserFS, XFS, UFS
- Google File System, Hadoop Distributed File System
- ... i mnogi drugi

# Pokretanje računala



- Kada se računalo pokreće, obično traži pristup nekoj vrsti trajne memorije
  - najčešće tvrdom disku, no može biti i
    - prijenosna memorija, CD, DVD
- s koje čita te traži daljnje instrukcije
  - aplikaciju koju treba :
    - učitati u memoriju
    - i pokrenuti



- No, kako računalo zna kojim je datotečnim sustavom oblikovana memorija?
- Gdje da traži upute o pokretanju?

# Organizacija diska

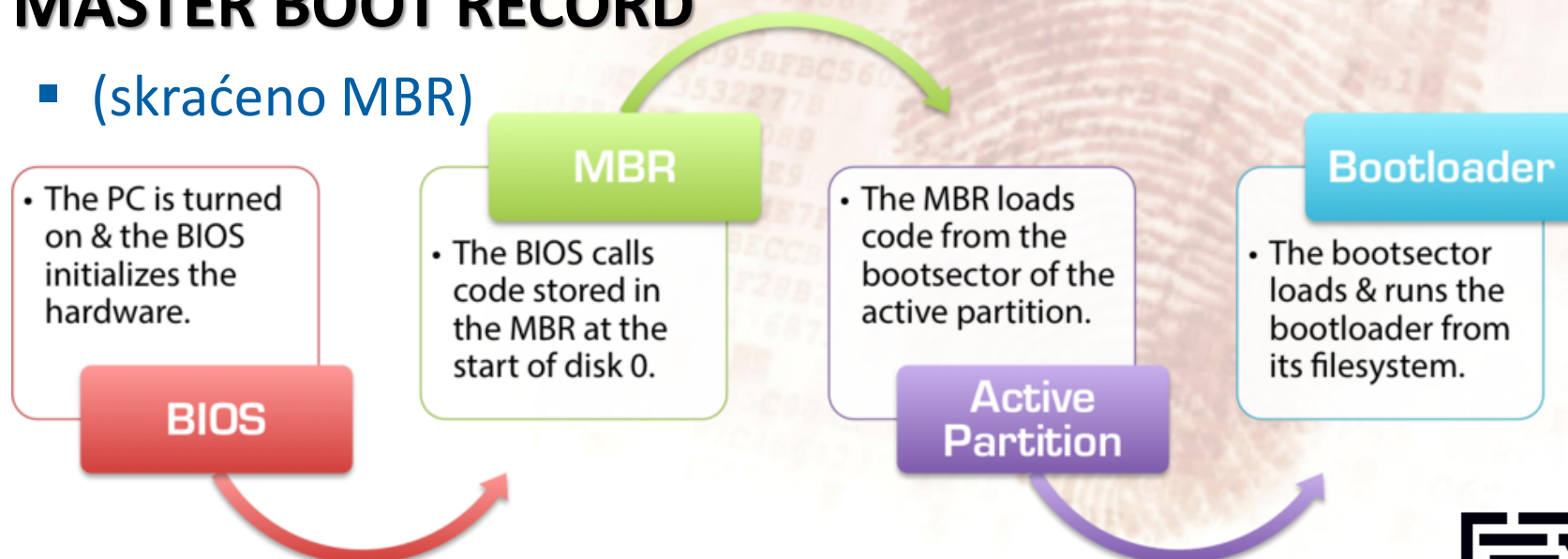


- Radi bolje organizacije i lakšeg upravljanja, svaka memorija je podijeljena na **SEKTORE**

- memorijske skupine od 512 bajtova

- U prvom fizičkom sektoru memorije računalo očekuje **MASTER BOOT RECORD**

- (skraćeno MBR)



# MBR = Master Boot Record



**MBR** ima 512 bajta, a sastoji se od tri dijela:

- 1 Bootstrap **kod**, 446 bajta
- 2 Tablica s **particijama**,  $4 * 16$  bajta = 64 bajta
- 3 **Potpis**/Magični broj, 2 bajta 0x55 0xAA

## Master Boot Record



# Sadržaj MBR-a



Bootstrap kod

Tablica s  
particijama

Potpis/  
Magični broj

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	33	ED	90	90	90	90	90	90	90	90	90	90	90	90	90	90	3í.....
00000010	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	.....
00000020	33	ED	FA	8E	D5	BC	00	7C	FB	FC	66	31	DB	66	31	C9	3iúŽÖL.  üüf1Ūf1É
00000030	66	53	66	51	06	57	8E	DD	8E	C5	52	BE	00	7C	BF	00	fsfQ.WŽÝŽÍRI.  ž.
00000040	06	B9	00	01	F3	A5	EA	4B	06	00	00	52	B4	41	BB	AA	.a..óAęK...R'A»Ş
00000050	55	31	C9	30	F6	F9	CD	13	72	16	81	FB	55	AA	75	10	U1É0öúÍ.r..üUŞu.
00000060	83	E1	01	74	0B	66	C7	06	F1	06	B4	42	EB	15	EB	00	.á.t.fÇ.n.´Bē.ē.
00000070	5A	51	B4	08	CD	13	83	E1	3F	5B	51	0F	B6	C6	40	50	ZQ´.Í..á?[Q.řČ@P
00000080	F7	E1	53	52	50	BB	00	7C	B9	04	00	66	A1	B0	07	E8	÷áSRP».. a..f`°.č
00000090	44	00	0F	82	80	00	66	40	80	C7	02	E2	F2	66	81	3E	D.,,€..f@€Ç.áñf.>
000000A0	40	7C	FB	C0	78	70	75	09	FA	BC	EC	7B	EA	44	7C	00	@ úŘxpu.úLě{ęD .
000000B0	00	E8	83	00	69	73	6F	6C	69	6E	75	78	2E	62	69	6E	.č..isolinux.bin
000000C0	20	6D	69	73	73	69	6E	67	20	6F	72	20	63	6F	72	72	missing or corr
000000D0	75	70	74	2E	0D	0A	66	60	66	31	D2	66	03	06	F8	7B	upt...f`f1Ñf..ř{
000000E0	66	13	16	FC	7B	66	52	66	50	06	53	6A	01	6A	10	89	f..ú{fRfP.Sj.j.‰
000000F0	E6	66	F7	36	E8	7B	C0	E4	06	88	E1	88	C5	92	F6	36	čf÷6č{Řä..á.Í'ö6
00000100	EE	7B	88	C6	08	E1	41	B8	01	02	8A	16	F2	7B	CD	13	î{.Č.áA,..Š.ñ{Í.
00000110	8D	64	10	66	61	C3	E8	1E	00	4F	70	65	72	61	74	69	Ťd.faĂč..Operati
00000120	6E	67	20	73	79	73	74	65	6D	20	6C	6F	61	64	20	65	ng system load e
00000130	72	72	6F	72	2E	0D	0A	5E	AC	B4	0E	8A	3E	62	04	B3	rror...^~´.Š>b.ž
00000140	07	CD	10	3C	0A	75	F1	CD	18	F4	EB	FD	00	00	00	00	.Í.<.uñí.ôëý....
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	DC	50	03	00	00	00	00	00	7C	78	5D	7D	00	00	80	02	ŪP..... x }..€.
000001C0	01	00	06	B0	E0	FD	40	00	00	00	B6	FF	77	00	00	00	...°řý@...Ť`w...
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	55	AA	.....UŞ





- **izvršivi kod** (program) čiji je zadatak
  1. **pronaći** aktivnu particiju
    - **skeniranjem particijskih tablica,**
  2. **pročitati** koji je početni sektor aktivne particije,
  3. **prekopirati program** iz početnog sektora aktivne particije **u memoriju** te
  4. **pokrenuti** učitani program



- **Particija (podjela)**

- je jedan dio na fizičkom disku
  - Može se gledati kao manja, logička jedinica diska
  - cijeli disk je podijeljen na jednu ili više particija
    - prema želji i potrebama korisnika računala
- Korisna je za razvdajanje
  - sistemskih aplikacija od podataka ili
  - nekoliko (različitih) operacijskih sustava,
  - područje za straničenje (swapping/paging) za operacijske sustave, itd.
- može pomoći ukoliko su dijelovi diska oštećeni



- MBR ima prostor (zapise) za definiranje 4 particije

- svaka ima **16 bajtova**

- **Svaki zapis particije** sadrži podatke koji nam govore:

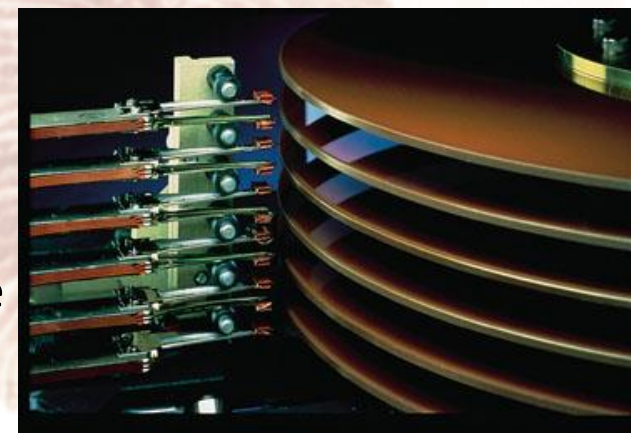
- je li particija **aktivna**?
- kojim datotečnim sustavom je **formatirana**
- na kojem sektoru **počinje**
- koliko je **velika**

# Particijska tablica



Structure of a 16-byte Partition Table Entry		
Relative Offsets (within entry)	Length (bytes)	Contents
0	1	Boot Indicator (80h = active)
1 - 3	3	Starting CHS values
4	1	Partition-type Descriptor
5 - 7	3	Ending CHS values
8 - 11	4	Starting Sector
12 - 15	4	Partition Size (in sectors)

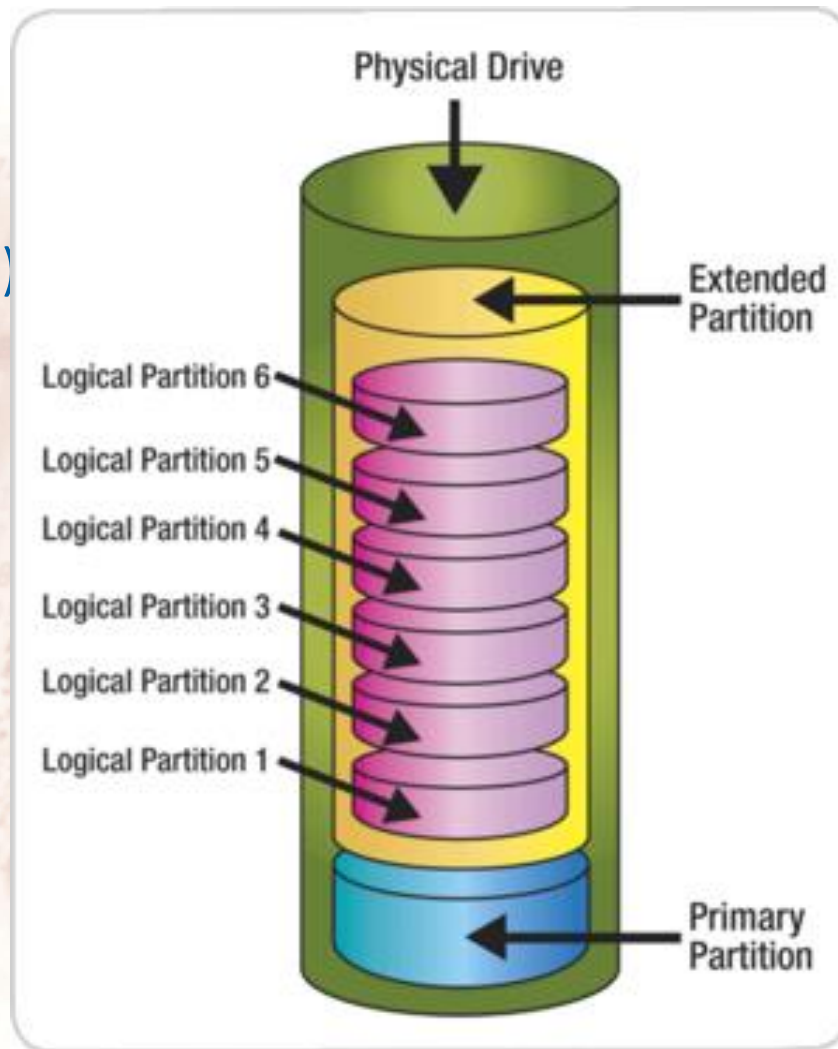
- CHS je kratica za Cilindar – Glava – Sektor (**Cylinder – Head – Sector**)
- ta polja su relevantna jedino ako se radi o mehaničkom tipu tvrdog diska
  - *flash* memorija ili SSD diskovi ne sadrže ove dijelove
- CHS se i dalje koristi iz povijesnih razloga



# Tipovi particija



- Primarne particije (max 4)
- Produžene particije (max 1)
  - extended boot record (EBR)
  - extended partition boot record (EPBR)
- Prvi sektor sadrži EBR
  - EBR je sličan kao i MBR
    - što znači da ima i partijsku tablicu
  - Ali samo prva dva zapisa te partijske tablice se koriste
    - Prvi opisuje **trenutnu** logičku particiju
    - Drugi opisuje gdje se **nalazi početak iduće** particije
      - znači, može se napraviti povezana lista s neograničenim brojem particija



# Potpis/Magični broj



- na kraju **MBR** zapisa
  - je polje veličine **2 bajta**,
  - uvijek sadrži vrijednost

0x55 0xAA

- Označava kraj MBR-a

- Služi i za provjeru je li

- MBR uopće tamo
- te je li ispravan

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	F
00000000	33	ED	90	90	90	90	90	90	90	90	90	90	90	90	90	0
00000010	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90	0
00000020	33	ED	FA	8E	D5	BC	00	7C	FB	FC	66	31	DB	66	31	9
00000030	66	53	66	51	06	57	8E	DD	8E	C5	52	BE	00	7C	BF	0
00000040	06	B9	00	01	F3	A5	EA	4B	06	00	52	B4	41	BB	A	
00000050	55	31	C9	30	F6	F9	CD	13	72	16	81	FB	55	AA	75	0
00000060	83	E1	01	74	0B	66	C7	06	F1	06	B4	42	EB	15	EB	0
00000070	5A	51	B4	08	CD	13	83	E1	3F	5B	51	0F	B6	C6	40	0
00000080	F7	E1	53	52	50	BB	00	7C	B9	04	00	66	A1	B0	07	8
00000090	44	00	0F	82	80	00	66	40	80	C7	02	E2	F2	66	81	E
000000A0	40	7C	FB	C0	78	70	75	09	FA	BC	EC	7B	EA	44	7C	0
000000B0	00	E8	83	00	69	73	6F	6C	69	6E	75	78	2E	62	69	E
000000C0	20	6D	69	73	73	69	6E	67	20	6F	72	20	63	6F	72	2
000000D0	75	70	74	2E	0D	0A	66	60	66	31	D2	66	03	06	F8	B
000000E0	66	13	16	FC	7B	66	52	66	50	06	53	6A	01	6A	10	9
000000F0	E6	66	F7	36	E8	7B	C0	E4	06	88	E1	88	C5	92	F6	6
00000100	EE	7B	88	C6	08	E1	41	B8	01	02	8A	16	F2	7B	CD	3
00000110	8D	64	10	66	61	C3	E8	1E	00	4F	70	65	72	61	74	9
00000120	6E	67	20	73	79	73	74	65	6D	20	6C	6F	61	64	20	5
00000130	72	72	6F	72	2E	0D	0A	5E	AC	B4	0E	8A	3E	62	04	3
00000140	07	CD	10	3C	0A	75	F1	CD	18	F4	EB	FD	00	00	00	0
00000150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0
000001B0	DC	50	03	00	00	00	00	7C	78	5D	7D	00	00	80	2	
000001C0	01	00	06	B0	E0	FD	40	00	00	00	B6	FF	77	00	00	0
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0

# Nedostaci MBR-a



1. Samo četiri unosa u tablici za particije
  - ograničavaju disk na **maksimalno četiri fizičke particije**
    - može se donekle rješiti kreiranjem logičkih particija
2. Polje za veličinu particije u particijskoj tablici je veličine 32 bita, što znači da je **maksimalna veličina particije  $2^{32}$  sektora od 512 bajtova, odnosno 2 TiB**
- Shodno tome, pojavila se alternativa Master Boot Recordu
  - **GUID Partition Table (GPT)**

# GPT – GUID partition table



- novi standard koji polako zamjenjuje MBR
  - Linux, Mac OS X, Windows 8.x & 10
- naziv dolazi od činjenice da
  - svaka particija ima globalno jedinstveni identifikator (GUID)
- za razliku od MBR
  - nema ograničenja na broj i veličine particija
- za razliku od MBR
  - koji je spremljen na samo jednom mjestu u memoriji,
  - **GPT sprema kopije**
    - po čitavom disku,
    - tako osiguravajući konzistentnost diska

# Što se događa dalje?



## Drugi stupanj

- Dakle, boot code iz MBR

- u particijskoj tablici
- traži onu koja je označena kao “active”, **bootable**
- kojim datotečnim sustavom je formatirana particija

- **0x07** = NTFS

- **0x83** = Linux

- *Više kodova* = FAT

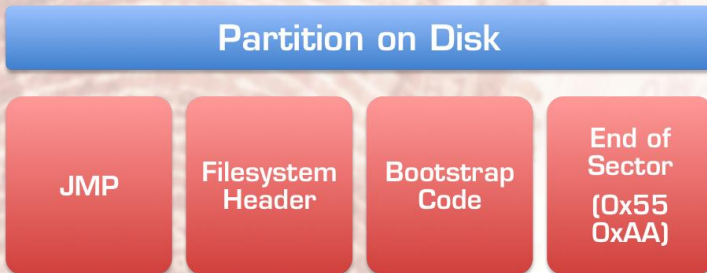
<http://datarecovery.com/rd/hexadecimal-flags-for-partition-type/>

- i gdje se nalazi

- na kojem sektoru počinje
  - brojeći od početka diska

- zatim učitava ponovno prvi sektor

- i sljedećih nekoliko



- taj program učitava **bootloader**

- potraži datoteku u datotečnom sustavu i onda pokreće aplikaciju - **bootloader**

Ovdje se datotečni sustavi počinju razlikovati

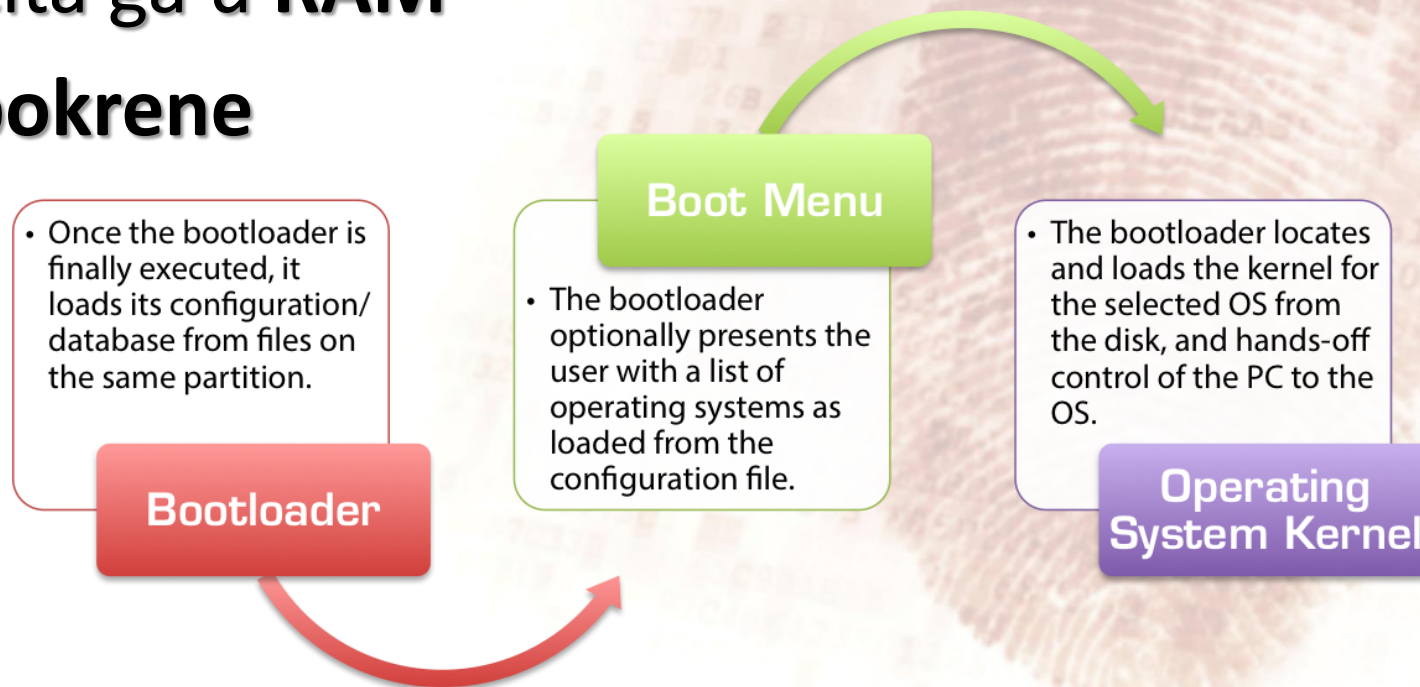




# Bootloader



- **bootloader**
  - potpuno “razumije” konkretni datotečni sustav
- i u njemu potraži **jezgru** operacijskog sustava
- učita ga u **RAM**
- i pokrene



# Što je to dual boot?



- Više particija može biti na kraju “bootable”
  - sadržati operacijske sustave
  - Ali samo neke particije su označene kao aktivne (bootable)
- *bootloader* je na toj aktivnoj particiji
  - suvremeni bootloader može učitati OS s bilo koje particije
    - LILO, GRUB, NTLDR
  - obično Linux
    - dolazi u distribuciji
- **Detektira** sve bootable OS na disku
- **Pita korisnika** koji OS želi pokrenuti
- Zatim **učita** *bootloader* s odabrane particije
- I **pokrene** OS

# Koliko ima bootloadera?



- Acronis OS Selector
- AiR-Boot
- AKernelLoader
- Barebox
- Boot Camp
- BootIt Bare Metal
- BootKey
- BootManager
- BootX (Apple)
- BootX (Linux)
- Darwin Boot Loader
- Das U-Boot
- FreeLoader
- GAG
- GNU GRUB
- GRUB Legacy
- GRUB4DOS
- Gujin [1]
- iBoot
- LILO
- loadlin
- MasterBooter
- NTLDR
- OSL2000 Boot Manager
- PLoP Bootmanager
- RedBoot
- rEFInd
- Smart Boot Manager
- SPFDisk
- SYSLINUX
- systemd-boot / Gummiboot
- Windows Boot Manager
- XOSL

# Bootloader



## NTLDR

- NTLDR is the default bootloader for Windows NT, 2000, and XP.
- BOOT.INI on the active partition contains the list of operating systems and their locations.
- NTDETECT.COM is a helper program that runs to detect hardware and identify devices.

## BOOTMGR

- BOOTMGR is the new Windows and is used on Windows Vista, 7, 8, and 10.
- The list of operating systems is now read from the BCD file in the BOOT directory on the active partition.
- BOOTMGR is self-contained, and does not need any helper programs or routines.

## GRUB(2)

- GRUB is the most-popular bootloader for Linux, though it can boot numerous other OSes as well.
- Its boot settings are stored in a file usually called grub.cfg (GRUB2) or menu.lst (GRUB).
- GRUB is a modular bootloader, that can load additional modules from disk.



# ORGANIZACIJA DATOTEČNIH SUSTAVA

# Kako su datotečni sustavi organizirani

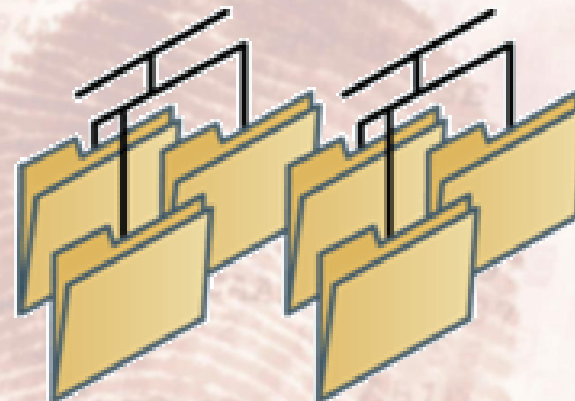


FAT16, FAT32

NTFS

ext2

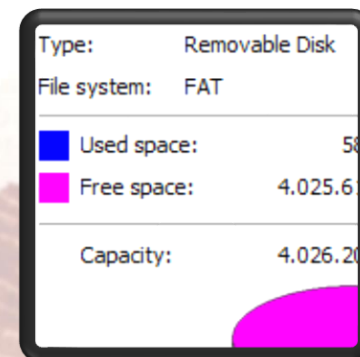
ext3



# FAT16



<b>Puno ime</b>	16-bit File Allocation System
<b>Pripadnost</b>	DOS/Windows
<b>God. pojavljivanja</b>	1984
<b>MBR identifikator</b>	0x04, 0x06



## Prednosti:

- Najbolja prenosivost među platformama
- Jednostavan povrat obrisanih datoteka

## Mane:

- Veličina particije je ograničena na 4 GB
- Maksimalna veličina datoteke je 4 GB (minus 1 bajt)
- Jednostavan povrat obrisanih datoteka (?!)
- Nema kontrole nad korisničkim pristupom datotekama
- Ograničen broj zapisa u korijenskom direktoriju (512)

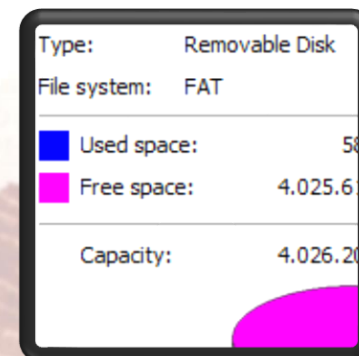
## Bio:

Datotečni sustav kojeg je razvio Microsoft, prethodile su mu 8-bitna i 12-bitna inačica. Odlike su mu **jednostavnost** i **robustnost**. Kompatibilan je s gotovo svim operacijskim sustavima. Memorija je podijeljena u skupine sektora naziva **klasteri**. Naziv datotečnog sustava dolazi od tablice koju koristi za alokaciju klastera po datotekama.

# FAT32



<b>Puno ime</b>	<b>32-bit File Allocation System</b>
<b>Pripadnost</b>	DOS/Windows
<b>God. pojavljivanja</b>	1996
<b>MBR identifikator</b>	0x0B, 0x0C



## Prednosti:

- Dobra prenosivost među platformama
- Nema 4 GB ograničenja za veličinu particija kao kod FAT16 inačice

## Mane:

- Veličina particije je ograničena na 2 TB
- Maksimalna veličina datoteke je 4 GB (minus 1 bajt)
- Nema kontrole nad korisnikovim pristupom datotekama

## Bio:

Nova inačica datotečnog sustava iz FAT obitelji, nastala nakon FAT16 sustava.

Veličina particije je porasla, kao i maksimalni broj zapisa u korijenskom direktoriju.

FAT32 se smatra 10-15 % efikasniji u korištenju memorije od FAT16 sustava.





<b>Puno ime</b>	<b>32-bit File Allocation System</b>
<b>Pripadnost</b>	DOS/Windows
<b>God. pojavljivanja</b>	1996
<b>MBR identifikator</b>	0x0B, 0x0C

## Prednosti:

- Dobra prenosivost među platformama
- $2^{60}N$  max veličina datoteke, ograničeno particijom
- $25^0N$  max veličina particije

## Mane:

- sporiji za datoteke manje od 4 GB
- Nema dnevnika ni provjere konzistencije

## Bio:

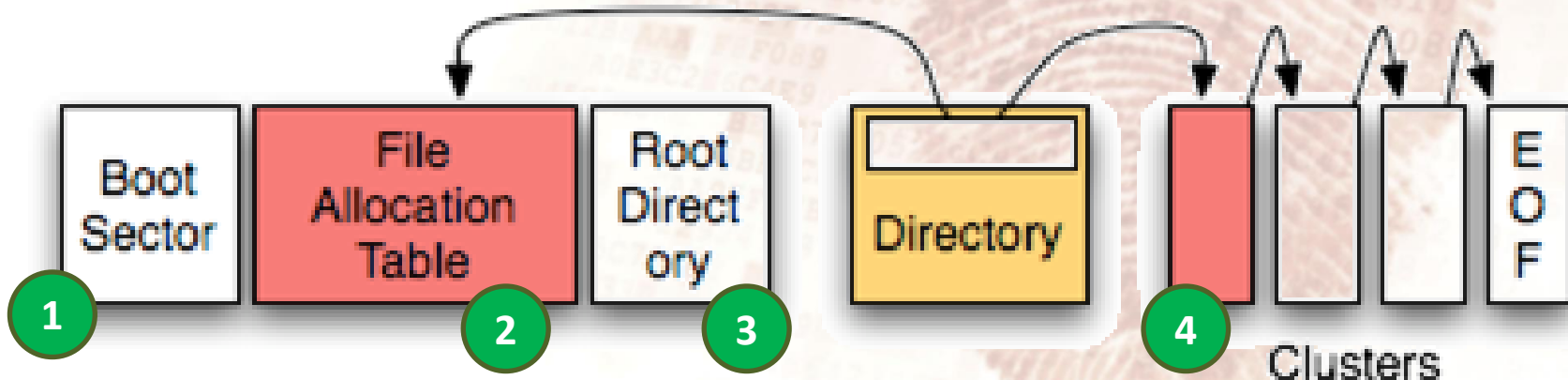
Microsoft 2006.

# FAT datotečni sustavi



FAT16 datotečni sustav sastoji se od:

- 1 **Boot sektora**
- 2 **Tablice za alokaciju datoteka (FAT)**
- 3 **Korijenskog direktorija (*root directory*)**
- 4 **Klastera s podacima**



# 1 Boot sektor



## Naredba skoka

- Naredba **EB, 3C, 90** se prevodi u:  
| JUMP TO | OFFSET 3C | NO OPERATION |
- procesor **skače** na početak izvršivog (*boot*) koda.

## OEM naziv

## BIOS blok parametara

- ključni podaci o particiji
  - broj bajtova po sektoru,
  - ukupni broj sektora u klasteru,
  - broja rezerviranih sektora
  - itd.

## Izvršivi *boot* kôd

## Potpis

- **0xAA55**

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00008000	EB	3C	90	4D	53	44	4F	53	35	2E	30	00	02	80	08	00
00008010	02	00	02	00	00	F8	F0	00	3F	00	FF	00	40	00	00	00
00008020	B6	FF	77	00	80	00	29	A8	96	92	32	4E	4F	20	4E	41
00008030	4D	45	20	20	20	20	46	41	54	31	36	20	20	20	33	C9
00008040	8E	D1	BC	F0	7B	8E	D9	B8	00	20	8E	C0	FC	BD	00	7C
00008050	38	4E	24	7D	24	8B	C1	99	E8	3C	01	72	1C	83	EB	3A
00008060	66	A1	1C	7C	26	66	3B	07	26	8A	57	FC	75	06	80	CA
00008070	02	88	56	02	80	C3	10	73	EB	33	C9	8A	46	10	98	F7
00008080	66	16	03	46	1C	13	56	1E	03	46	0E	13	D1	8B	76	11
00008090	60	89	46	FC	89	56	FE	B8	20	00	F7	E6	8B	5E	0B	03
000080A0	C3	48	F7	F3	01	46	FC	11	4E	FE	61	BF	00	00	E8	E6
000080B0	00	72	39	26	38	2D	74	17	60	B1	0B	BE	A1	7D	F3	A6
000080C0	61	74	32	4E	74	09	83	C7	20	3B	FB	72	E6	EB	DC	A0
000080D0	FB	7D	B4	7D	8B	F0	AC	98	40	74	0C	48	74	13	B4	0E
000080E0	BB	07	00	CD	10	EB	EF	A0	FD	7D	EB	E6	A0	FC	7D	EB
000080F0	E1	CD	16	CD	19	26	8B	55	1A	52	B0	01	BB	00	00	E8
00008100	3B	00	72	E8	5B	8A	56	24	BE	0B	7C	8B	FC	C7	46	F0
00008110	3D	7D	C7	46	F4	29	7D	8C	D9	89	4E	F2	89	4E	F6	C6
00008120	06	96	7D	CB	EA	03	00	00	20	0F	B6	C8	66	8B	46	F8
00008130	66	03	46	1C	66	8B	D0	66	C1	EA	10	EB	5E	0F	B6	C8
00008140	4A	4A	8A	46	0D	32	E4	F7	E2	03	46	FC	13	56	FE	EB
00008150	4A	52	50	06	53	6A	01	6A	10	91	8B	46	18	96	92	33
00008160	D2	F7	F6	91	F7	F6	42	87	CA	F7	76	1A	8A	F2	8A	E8
00008170	C0	CC	02	0A	CC	B8	01	02	80	7E	02	0E	75	04	B4	42
00008180	8B	F4	8A	56	24	CD	13	61	61	72	0B	40	75	01	42	03
00008190	5E	0B	49	75	06	F8	C3	41	BB	00	00	60	66	6A	00	EB
000081A0	B0	42	4F	4F	54	4D	47	52	20	20	20	20	0D	0A	52	65
000081B0	6D	6F	76	65	20	64	69	73	6B	73	20	6F	72	20	6F	74
000081C0	68	65	72	20	6D	65	64	69	61	2E	FF	0D	0A	44	69	73
000081D0	6B	20	65	72	72	6F	72	FF	0D	0A	50	72	65	73	73	20
000081E0	61	6E	79	20	6B	65	79	20	74	6F	20	72	65	73	74	61
000081F0	72	74	0D	0A	00	00	00	00	00	00	00	AC	CB	D8	55	AA

ë<.MSDOS5.  
.....řd.?  
ř'w.€.)`-'  
ME FAT1  
ŽŇŇd{ŽŮ,.  
8N\$}\$<Á™ö<  
f~.|&f;.&Š  
..V.€Ā.se3  
f..F..V..E  
`%Fü%Vř,  
ĀH÷ó.Fü.Nř  
.r9&8-t.`t  
at2Nt..Ç  
ů}´|<d~.(t  
»..Í.ėd' ý)  
áí.í.&<U.R  
;.rč[ŠV\$Í.  
=)ÇFô)}ŠŮ  
.-)Ěę...  
f.F.f<ĐfĀę  
JŮŠF.2ă÷ă.  
JRP.Sj.j.`  
Ň÷ö'÷öB+E  
ŘĚ..Ě,..€-  
<ôŠV\$Í.aar  
^..Iu.řĀA»  
°BOOTMGR  
move disks  
her media.  
k error`..  
any key to  
rt.....

# Korijenski (root) direktorij



- sektor (ili više sektora) koji sadrže 32 bitne zapise o datotekama sadržanim u korijenskom direktoriju

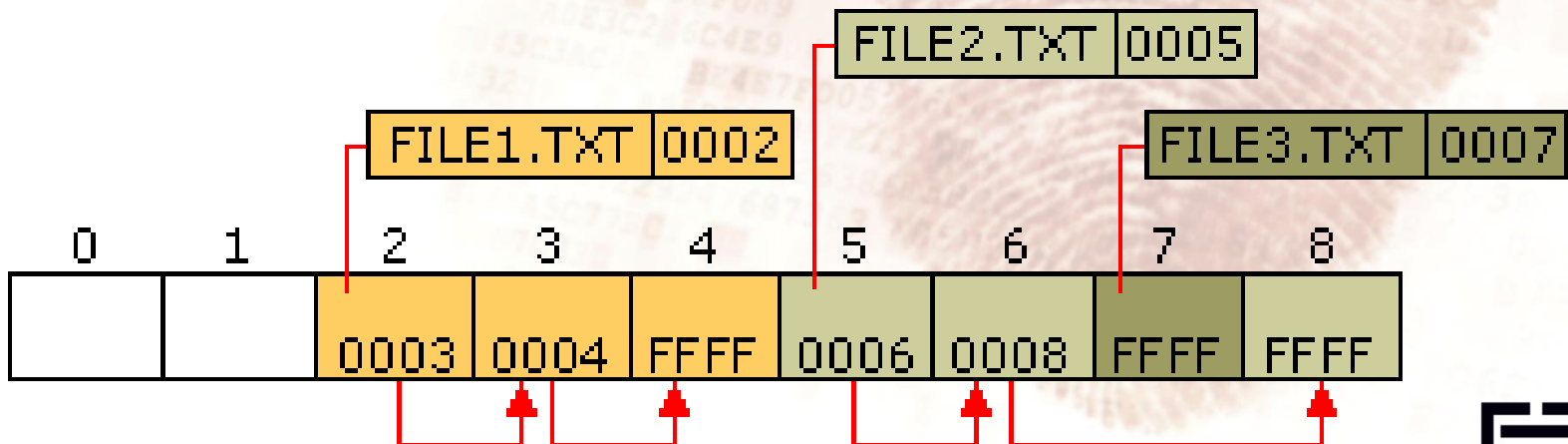
- zapisi sadrže podatke poput:

- naziva datoteke,
- programske ekstenzije
  - .txt, .pdf, .rar
- vremena
  - stvaranja datoteke,
  - zadnjeg pristupa i
  - modifikacije
- lokacije na disku (starting cluster)
- veličine

byte offset	
0	Filename (8 bytes)
8	Extension (3 bytes)
11	File attribute (1 byte)
12	Case (1 byte)
13	Creation time (milliseconds) (1 byte)
14	Creation time (2 bytes)
16	Creation date (2 bytes)
18	Last access date (2 bytes)
20	Reserved (2 bytes)
22	Last modification time (2 bytes)
24	Last modification date (2 bytes)
26	Starting Cluster (2 bytes)
28	File size (4 bytes)

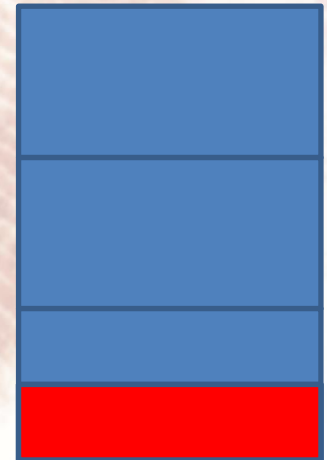


- tablica sadrži unos za **svaki klaster** na particiji
  - koji sadrži podatke
- svaki klaster sadrži pokazivač na **idući** klaster u datoteci
  - ili na indikator kraja datoteke (oznaka **0xFFFF**)
  - tvoreći tako povezanu listu (*eng. linked list*)
- tablica može biti **duplicirana** (redundancija podataka), broj kopija je zapisan u *boot* sektoru
- **Primjer: 3 datoteke raspoređene u 7 klastera:**





- nalaze se u memoriji neposredno **nakon korijenskog direktorija**
- korisnički podaci su pohranjeni u **klasterima**
  - u nekoliko uzastopnih sektora na disku
- **veličina** klastera je određena u *boot* sektoru (npr. 64 kB)
  - zapisano na lokaciji 0x0D
  - brojem disk sektora (512 bajtova svaka) koji čine jedan klaster
    - 1, 2, 4, 8, 16, 32, 64, 128
- **Klaster** je najmanja jedinica granulacije
  - primjerice:  
ako je datoteka veličine 10 kB, ona će i dalje zauzeti čitav klaster od 64 kB
  - javlja se problem neiskorištenog prostora
- Stvara problem **neiskorištenog prostora**
  - mogućnost **sakrivanja podataka** u njemu!





<b>Puno ime</b>	New Technology File System
<b>Pripadnost</b>	Windows
<b>God. pojavljivanja</b>	1993
<b>MBR identifikator</b>	0x07



## Prednosti:

- **Nema ograničenja** za veličine datoteka kao FAT
- Efikasnije od FAT32 sustava koristi prostor
- ima sustav vođenja dnevnika (engl. *journaling*) kojim kompenzira oštećenje podataka

## Mane:

- Nekompatibilan je s nekim programima i sustavima
- Noviteti ne odgovaraju svim tipovima diskova

## Bio:

Još jedan datotečni sustav kojeg je stvorio Microsoft, prvenstveno kako bi rješio neke nedostatke koje je imao FAT kao što su veličina datoteka, manjak sigurnosti i nedostatak sustava vođenja dnevnika.

Unatoč tome, noviteti koje je donio NTFS su kod nekih memorija suvišni (npr. prijenosni *flash* diskovi) te ne donose uvijek poboljšanje.



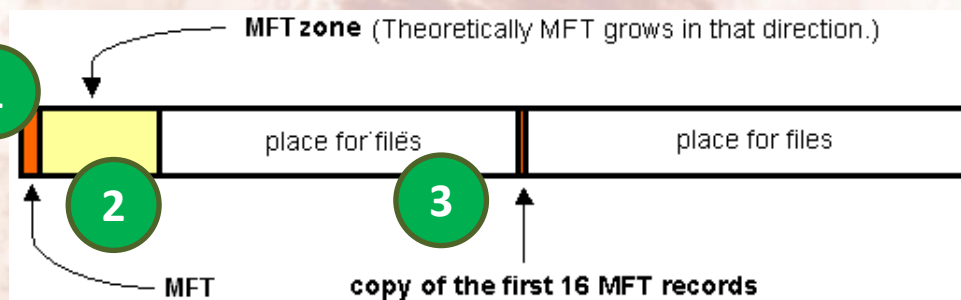
- Stvoren je za brzo obavljanje operacija čitanja, pisanja i pretraživanja na velikim diskovima

## 1. Particijski boot sector

1 MFT= Master File Table

2 Područje za datoteke

3



- sve u NTFS sustavu je datoteka
- NTFS je zamišljen kao baza podataka
- Microsoft-ova dokumentacija kaže:

*“MFT je relacijska baza podataka*

*koja se sastoji od redova datoteka zapisa i stupaca atributa datoteka. Ona sadrži barem jedan unos za svaku datoteku na NTFS jedinici, uključujući i samog MFT.”*



# 1 Boot sektor particije



## 1. Boot sektor particije

- Sličan boot sektorima u FAT datotečnom sustavu
- BPB (BIOS parameter block) i produženi (extended) BPB sadrže polja koji opisuju:
  - Broj bajtova po sektoru, broj sektora po klasteru, broj rezerviranih sektora, ukupan broj sektora itd.
  - ali, najvažnije, sadrži lokaciju Master File Table (MFT)

```
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00  ěR.NTFS .....
00000010 00 00 00 00 00 00 F8 00 00 3F 00 FF 00 3F 00 00 00  .....ř...?..?...
00000020 00 00 00 00 80 00 80 00 89 34 02 00 00 00 00 00  .....€..%4.....
00000030 85 17 00 00 00 00 00 00 02 00 00 00 00 00 00 00  .....
```

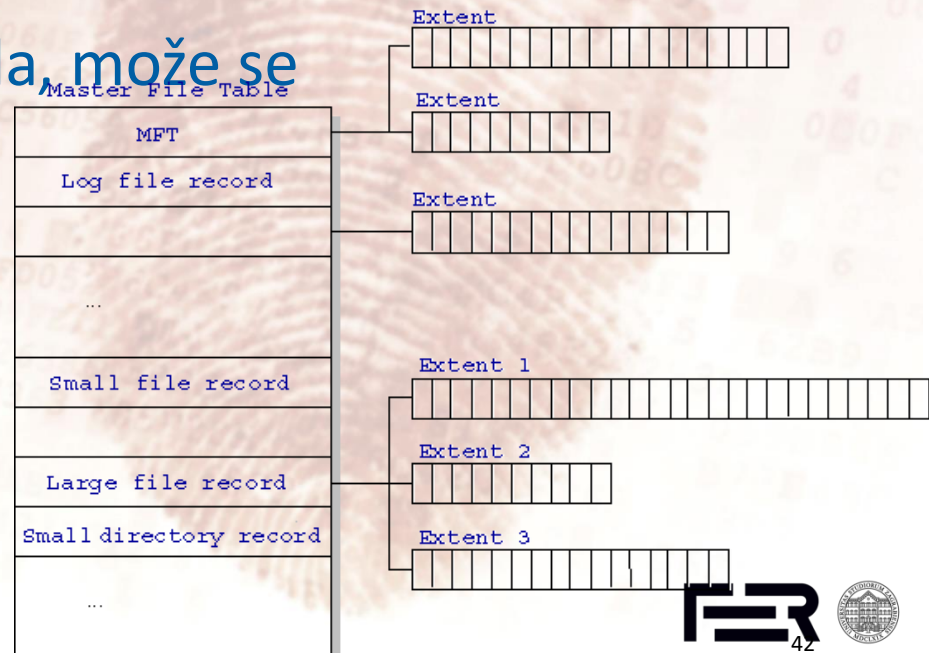
e.g. Ukupan broj sektora (0x023489 = 144521 bytes = 70 MB)  
Lokacija MFT (0x1785 = cluster 6021)

Opis svih polja je dostupan na: <http://ntfs.com/ntfs-partition-boot-sector.htm>



## Master File Table (MFT)

- Svaka datoteka na NTFS jedinici je predstavljena zapisom
  - Zapisi su pohranjeni u MFT
  - Veličina zapisa je varijabilno (obično 1024 bajta)
- Ako je prvi MFT zapis korumpiran/oštećen, NTFS čita idući zapis kako bi pronašao MFT mirror datoteku
- Ako je datoteka dovoljno mala, može se pohraniti u MFT zapisu, unutar **'data attribute'** polja
- Velike datoteke će svoje podatke pohraniti kao vanjske attribute



# Brisanje datoteka u NTFS sustavu



- Kada se datoteka obriše u NTFS sustavu, ona se samo **označava kao obrisana** unutar MFT zapisa te datoteke
- primjer:
  - Zapis datoteke, prije i poslije nego što se datoteke obrišu:

**PRIJE:**

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0178F000 46 49 4C 45 30 00 03 00 B0 50 10 00 00 00 00 00 FILE0...°P.....
0178F010 01 00 02 00 38 00 01 00 E0 01 00 00 00 04 00 00 ....8...ř.....
0178F020 00 00 00 00 00 00 00 00 08 00 00 00 28 00 00 00 ..... (...
```

**POSILIJE:**

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0178F000 46 49 4C 45 30 00 03 00 0F 63 10 00 00 00 00 00 FILE0....c.....
0178F010 02 00 01 00 38 00 00 00 68 01 00 00 00 04 00 00 ....8...h.....
0178F020 00 00 00 00 00 00 00 00 09 00 00 00 28 00 00 00 ..... (...
```

- 2 bajta udaljeni za 22 pokazuju da je datoteka obrisana
  - tj bajtovi 22. i 23. MFT za taj upis



<b>Puno ime</b>	extended file system 2
<b>Pripadnost</b>	Unix
<b>God. pojavljivanja</b>	1993
<b>MBR identifikator</b>	0x83



## Prednosti:

- Ograničenja za maksimalnu veličinu datoteke i particije su puno bolja u odnosu na FAT sustave (do 2 TB za datoteke i 32 TB za particije)

## Mane:

- Windows operacijski sustavi ga ne prepoznaju bez dodatnih *drivera*
- Nema sustav vođenja dnevnika

## Bio:

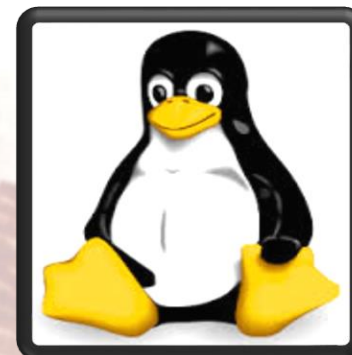
Razvio ga je Remy Card za Linux kao unaprijeđenje ext sustava.

Ext2 je razvijan prvenstveno na Linux OS te nije nativno podržan na Windowsima.

Obrisane datoteke je relativno lako vratiti.



<b>Puno ime</b>	extended file system 3
<b>Pripadnost</b>	Unix
<b>God. pojavljivanja</b>	2001
<b>MBR identifikator</b>	0x83



## Prednosti:

- Ograničenja za maksimalnu veličinu datoteke i particije su puno bolja u odnosu na FAT sustave (do 2 TB za datoteke i 32 TB za particije)

## Mane:

- Windows operacijski sustavi ga ne prepoznaju bez dodatnih *drivera*
- Obrisane datoteke je često nemoguće vratiti

## Bio:

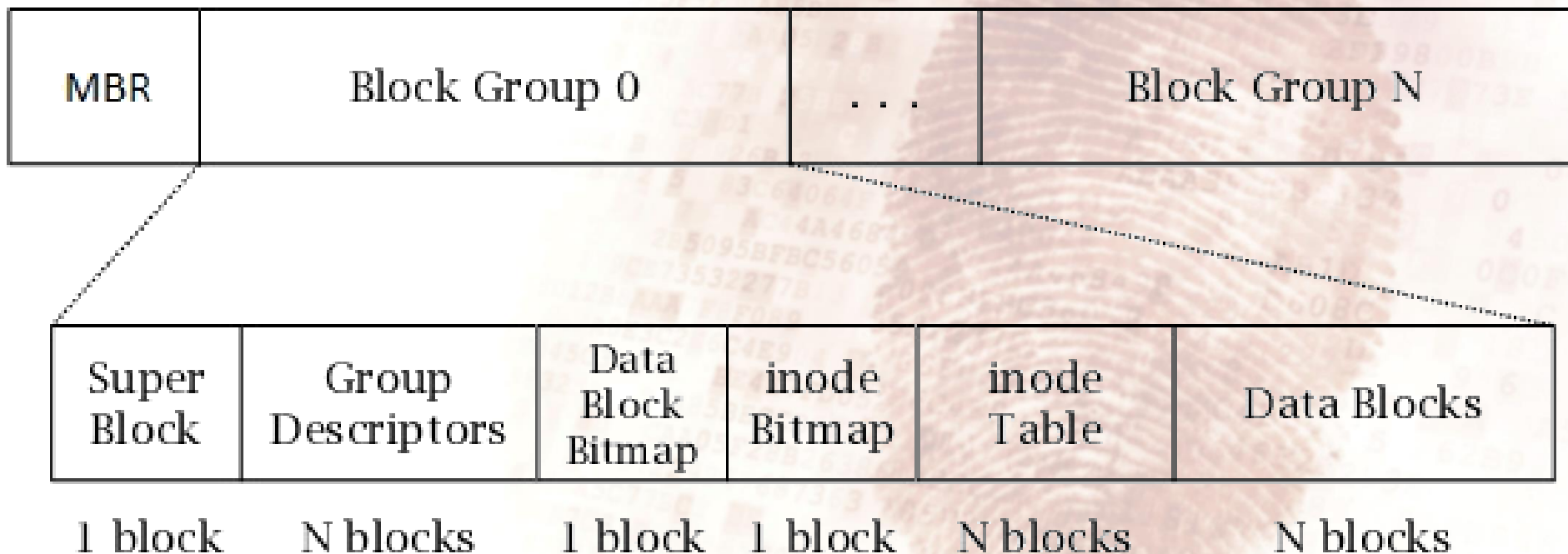
Razvio ga je Stephen Tweedie za Linux kao unaprijeđenje ext2 sustava.

Ext3 je strukturom izuzetno sličan ext2. Temeljne razlike su način na koji ext3 briše datoteke i sustav vođenja dnevnika koji ext3 uvodi.

# Ext datotečni sustavi



- struktura svih datotečnih sustava iz ext obitelji je slična
  - ext, ext2, ext3, ext4



# Ext datotečni sustavi

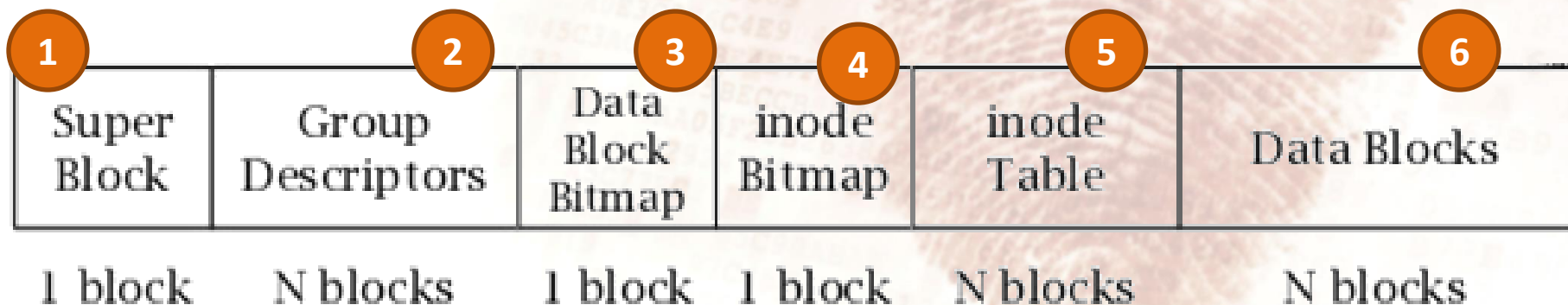


- koncept **svih ext** datotečnih sustava zasniva se na:
  - **blokovima,**
  - **grupama blokova i**
  - **indeksnim čvorovima (eng. *inode*)**
- **BLOK =**
  - osnovna jedinica pohrane
  - koja se sastoji od skupine sektora
    - može biti velik 1, 2, 4 ili 8 kB
- **GRUPA BLOKOVA –**  
više blokova spojenih u logičku cjelinu

# Struktura Ext datotečnog sustava



- 1 Superblok
- 2 **Opisnik** grupe blokova (eng. *block group descriptor*)
- 3 Bitovna **mapa blokova** (eng. *data block bitmap*)
- 4 Bitovna **mapa indeksnih čvorova** (eng. *inode bitmap*)
- 5 **Tablica** indeksnih čvorova
- 6 Blokovi **podataka**





# 1 Superblok



- ekvivalent **boot** sektoru u FAT sustavima
- original se nalazi **na početku particije** u prvoj grupi blokova,
  - a svaka iduća grupa blokova sadrži njegovu kopiju (redundancija)
- sadrži osnovne podatke o particiji poput
  - ukupnog broja **indeksnih čvorova**,
  - ukupnog broja **blokova**,
  - ukupnog broja slobodnih indeksnih čvorova i slobodnih blokova,
  - veličine blokova,
  - broja blokova u jednoj grupi blokova i sl.



(eng. *block group descriptor*)

- prvi blok u grupi blokova nakon superbloka,
- u njemu su definirani parametri grupe blokova poput:
  - **položaja** bitovne **mape** blokova,
  - **bitovne mape** indeksnih čvorova,
  - **položaja** **tablice** indeksnih čvorova



## 3 Bitovna mapa blokova (engl. *data block bitmap*)

- polje bajtova u kojem svaki BIT označava jedan podatkovni blok;
  - ako je bit postavljen na 0, blok je slobodan,
  - ako je bit postavljen na 1, blok je zauzet
- ekvivalent tablici za alokaciju datoteka (FAT) u FAT datotečnim sustavima

## 4 Bitovna mapa indeksnih čvorova (engl. *inode bitmap*)

- isto kao i bitovna mapa blokova,
- samo se odnosi na indeksne čvorove u tablici indeksnih čvorova

## 5 Tablica indeksnih čvorova

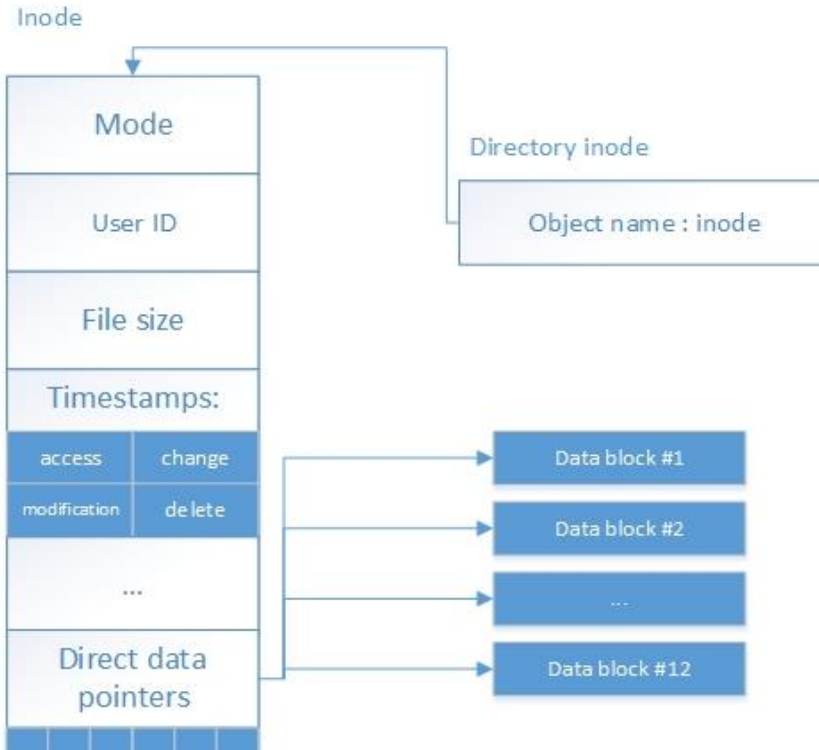
- sadrži sve indeksne čvorove za grupu blokova



- glavna podatkovna **struktura** ext sustava
- **svaki objekt** unutar datotečnog sustava je **predstavljen** odgovarajućim **indeksnim čvorom**
  - npr. datoteka, direktorij ...
- podrazumijevana veličina je **128 bajtova**
- sadrži polja koja određuju:
  - **vrstu objekta** koju indeksni čvor opisuje
    - npr. datoteka, direktorij ...
  - **veličinu** objekta kojeg indeksni čvor predstavlja (u bajtovima)
  - **pravo pristupa**
    - za vlasnika, grupu i javnost
  - **vremena** stvaranja, zadnjeg pristupa i uređivanja objekta na koji se čvor odnosi
  - **polje pokazivača** na blokove gdje je pohranjen sadržaj objekta
- **indeksni čvor NE sadrži**
  - **sadržaj** datoteke
  - **ime** datoteke

mode	
owners (2)	
timestamps (3)	
size block	
count	
direct blocks	—
⋮	⋮
single indirect	—
double indirect	—
triple indirect	—

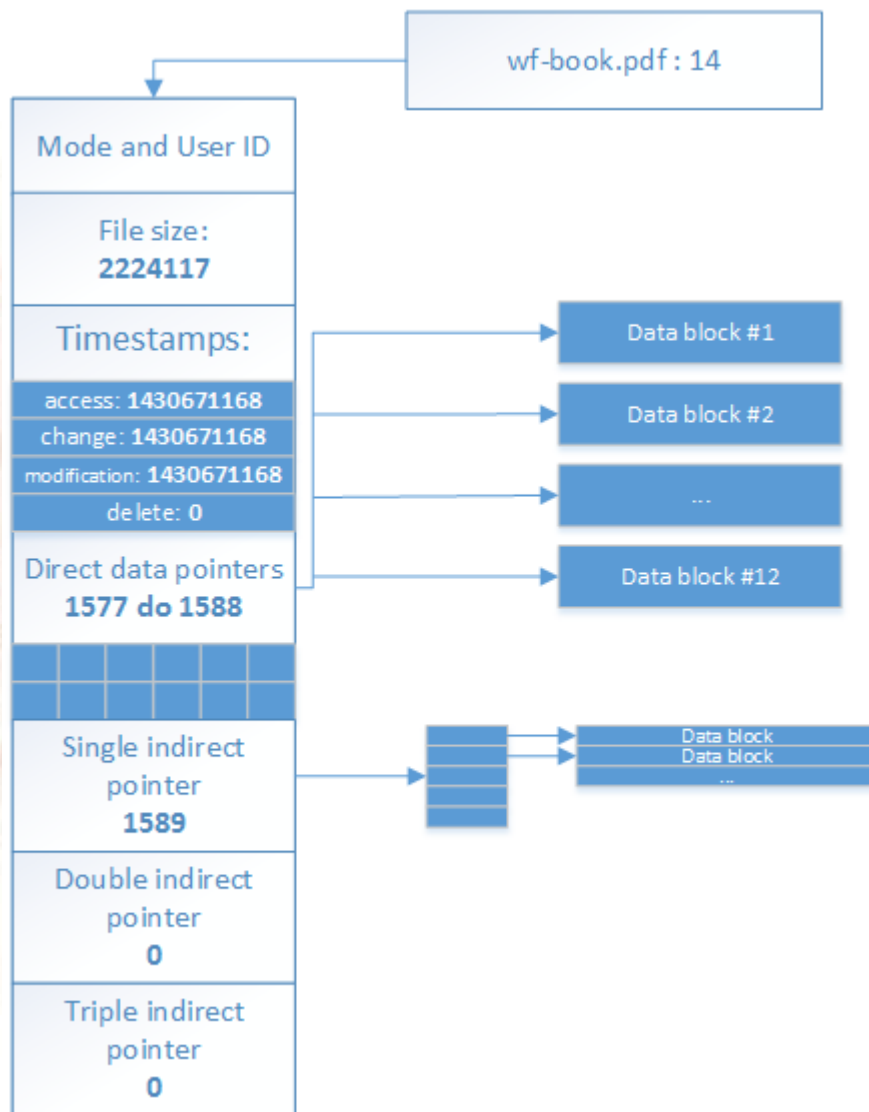
# Inode



# Inode - sadržaj



- Ova slika prikazuje indeks čvora datoteke pohranjene na ext datotečnom sustavu
- brisanje datoteka je vrlo različito na ext2 i ext3 / 4 datotečnim sustavima
- Sljedeće dvije prikaznice objašnjavaju proces brisanja datoteke na ext2 i ext3 datotečnim sustavima



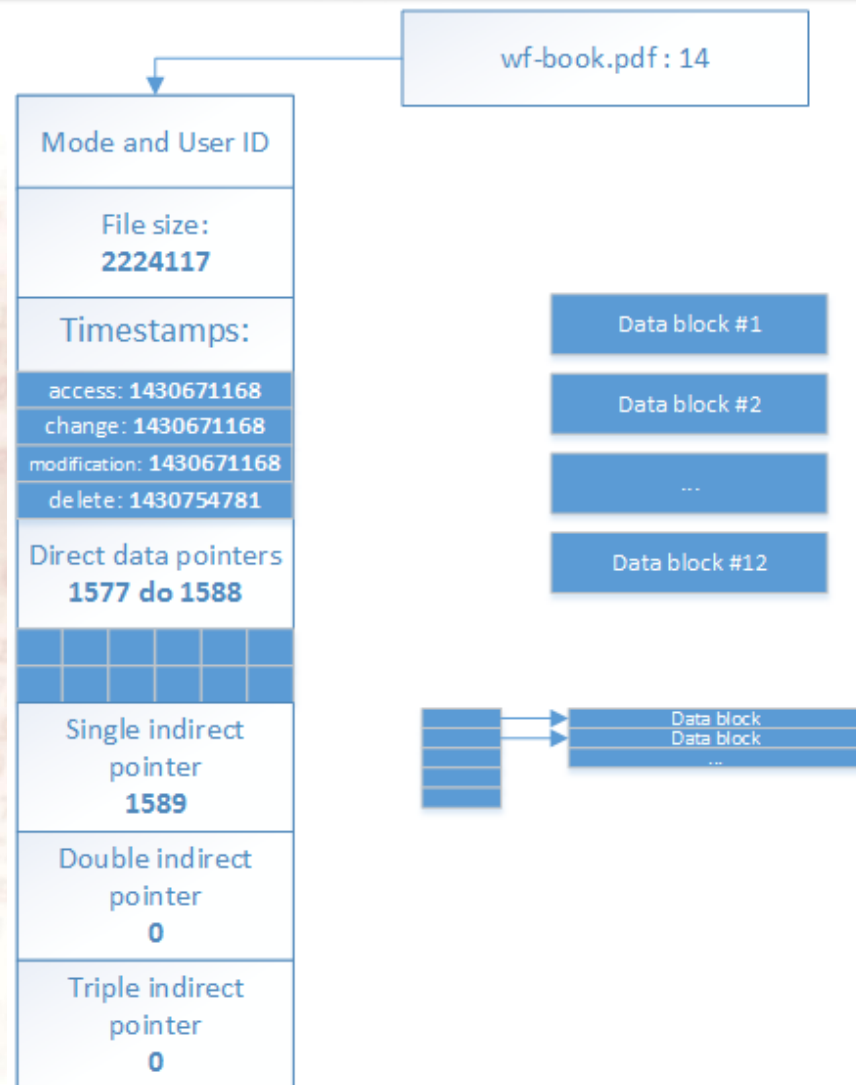
# ext2 inode



- **nakon brisanja datoteke**
  - dotad zauzeti blokovi u bitovnim mapama
    - prebacuju iz 1 u 0
- a **sadržaj** indeksnog čvora **ostaje isti**
- pa je **lako vratiti** obrisane datoteke
- **referirajući se** na vrijednosti u indeksnom čvoru

ali samo pod uvjetom

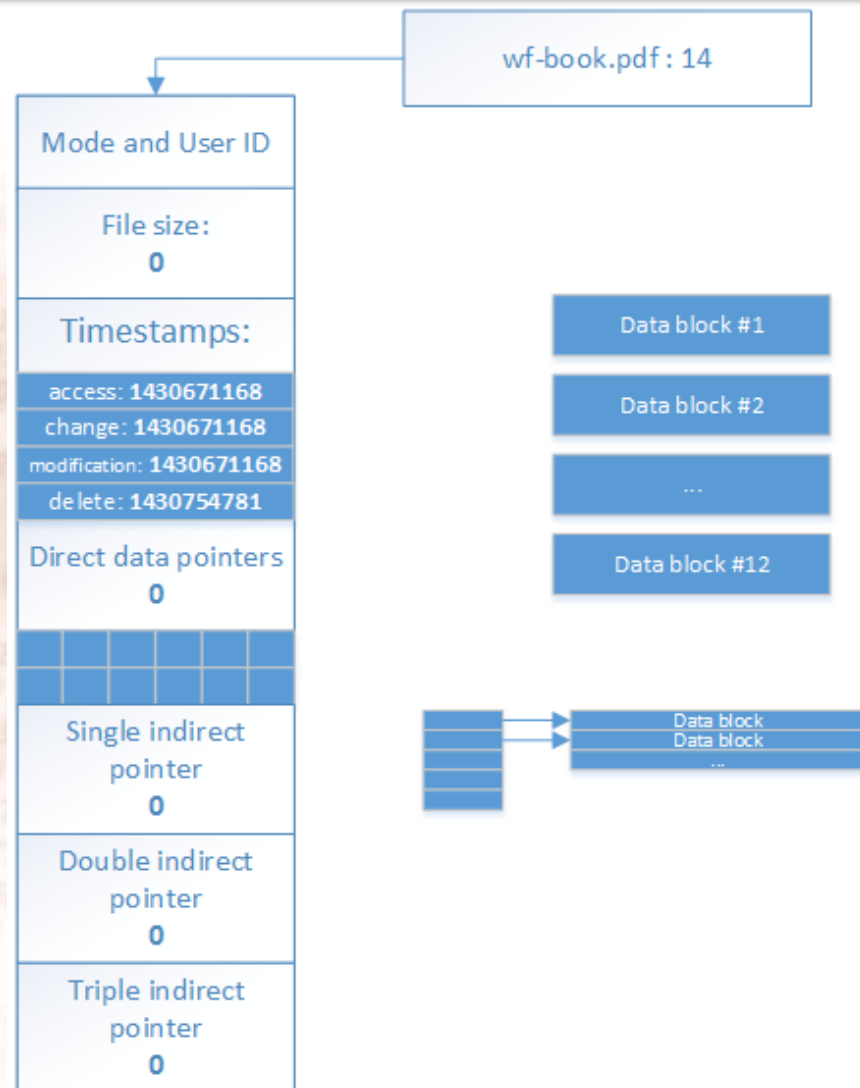
- da sadržaj ili indeksni čvor već nije “pregažen” drugim podacima



# ext3/ext4 inode



- **osim** promjena u bitovnim mapama
  - **na 0** se postavljaju i
    - pokazivači na klustere
    - te veličina datoteke
- **sadržaj** datoteke i dalje **postoji** na disku,
  - ali ga više nije moguće povezati u smislenu cjelinu
- zbog ovoga se datoteke na ext3/ext4 sustavima
  - u većini slučajeva smatraju trajno obrisanim





# Ext datotečni sustavi



No, unatoč tvrdnjama s prošle stranice, ipak postoje načini kako vratiti podatke na ext3/ext4 sustavima:

## 1. Pretraga običnog teksta

- metoda primjenjiva i na svakom drugom datotečnom sustavu
- memorija se pretražuje u potrazi za određenim riječima
- ukoliko je datoteka s traženom riječi bila zapisana u *plain textu*
  - primjerice: **.txt**, **.html**, **.cpp**, **.java**
- program za analizu memorije će je pronaći
- no, ako datoteka nije u *plain textu*
  - primjerice **.rar**, **.pdf**, **.doc**
- ili ako je riječ o slici,
- pretraga običnog teksta će se vjerojatno pokazati beskorisnom
- također, ova metoda neće uspjeti sastaviti datoteku ukoliko je ona zauzimala više blokova



## Sustav vođenja dnevnika (engl. *journaling*)

- svojstvo ext3/ext4 sustava na koje se oslanjaju mnogi programi za povrat podataka
  - npr. *extundelete*
- sustav vodi **dnevnik svih promjena** koje se događaju inodovima s namjerom da se podaci zaštite u slučaju “pada” sustava
- tri moda rada dnevnika:
  - **Journal** (čuvaju se i podaci i meta podaci mijenjanih datoteka),
  - **Write Back** (čuvaju se samo meta podaci) i
  - **Ordered** (kompromis između dvije opcije, čuvaju se samo meta podaci no promjene se prvo zapisuju u dnevnik, a tek onda na disk)

# Journaling + i -



- metoda očuvanja konzistencije podataka
- može se iskoristiti u forenzičkoj analizi
- ukoliko je datoteka obrisana
  - onda su na ext3/ext4 također nulu postavljeni i pokazivači u indeksnom čvoru
- međutim
  - ako nađemo spomenuti indeksni čvor u dnevniku i pročitamo vrijednost pokazivača;
  - saznali smo koji sve blokovi spremaju sadržaj tražene datoteke
- nedostaci povrata podataka pomoću dnevnika:
  - popunjavanje dnevnika kreće ponovno ispočetka prilikom svakog demontiranja (engl. *unmount*) i montiranja (engl. *mount*) sustava
  - u dnevnik se zapisuje na principu cirkularne liste,
    - kada je dnevnik prepun, popunjavanje kreće ispočetka i prepisuju se najstariji podaci
  - Najveća moguća veličina dnevnika na uređaju je 400 MiB (102400 blokova)
- zato povrat podataka treba napraviti što brže nakon brisanja, jer ti podaci mogu uskoro biti prepisani i nedostupni



- brz, robusan i svestran *hex* editor za Windows platformu
- *freeware*, preuzimanje i korištenje je besplatno
- instalacija nije potrebna,
  - postoji prenosiva (engl. *portable*) inačica
- **Mogućnosti:**
  - uređivanje diska i memorije,
  - pretraga memorije,
  - provjera zaštitnih suma,
  - sigurno brisanje datoteka (engl. *file shredding*),
  - usporedba datoteka,
  - izvoz dijelova memorije u zasebne datoteke itd.

<http://mh-nexus.de/en/hxd/>

# Autopsy



- jedan od popularnijih alata za forenzičku analizu memorije
- *freeware, open source*
- dostupan za:
  - Windows, UNIX i OS X platforme
- Mogućnosti:
  - pretraga ključnih riječi,
  - *hash* filtriranje,
  - ekstrakcija *web* artefakata poput kolačića,
  - povijesti pretraživanja,
  - rekonstrukcija i ekstrakcija obrisanih datoteka
  - itd.

<http://www.sleuthkit.org/>

# Autopsy primjer



test case - Autopsy 3.1.3

File View Tools Window Help

Close Case Add Data Source Generate Report

Keyword Lists Keyword Search

Directory Listing

/img\_image.img 23 Results

Name	Modified Time	Change Time	Access Time	Created Time	Size
\$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
\$RECYCLE.BIN	2015-10-29 21:47:28 CET	0000-00-00 00:00:00	2015-10-28 23:00:00 CET	2015-10-29 21:47:26 CET	2048
\$Unalloc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
pictures	2015-10-21 10:50:16 CEST	0000-00-00 00:00:00	2015-10-28 23:00:00 CET	2015-10-29 21:46:51 CET	2048
ppt	2015-10-29 01:03:02 CET	0000-00-00 00:00:00	2015-10-28 23:00:00 CET	2015-10-29 21:46:51 CET	2048
software	2015-10-21 10:51:10 CEST	0000-00-00 00:00:00	2015-10-28 23:00:00 CET	2015-10-29 21:46:52 CET	2048
5-Oct-2001.ppt	2015-04-16 11:44:06 CEST	0000-00-00 00:00:00	2015-10-28 23:00:00 CET	2015-10-29 21:47:17 CET	53760
_f-book.pdf	2015-04-16 12:18:16 CEST	0000-00-00 00:00:00	2015-10-28 23:00:00 CET	2015-10-29 21:47:17 CET	2224117
advantage-ext3-journaling-file-system-forens	2015-03-23 21:00:22 CET	0000-00-00 00:00:00	2015-10-28 23:00:00 CET	2015-10-29 21:47:17 CET	581840
Drawing1.bmp	2015-05-04 20:56:34 CEST	0000-00-00 00:00:00	2015-10-28 23:00:00 CET	2015-10-29 21:47:17 CET	1489850

Hex Strings Metadata Results Text Media

Matches on page: - of - Match Page: 1 of 1 Page

Times New Roman  
ext3 Journaling File System  
absolute consistency of the filesystem in every respect after a reboot, with no loss of existing f  
unctionality  
chadd williams  
SHRUG  
10/04/2001

# Brisanje datoteka - pregled

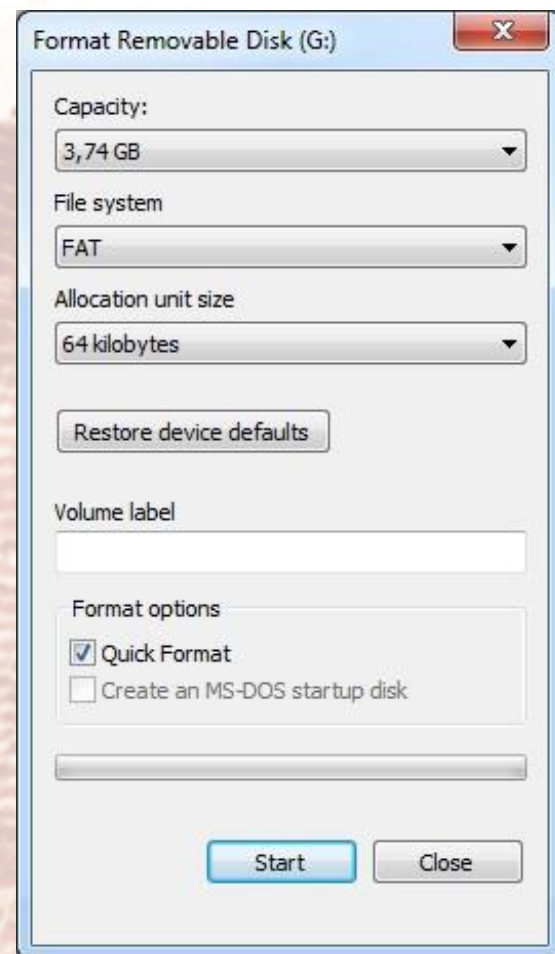


- svaki datotečni sustav briše datoteke na svoj način:
  - FAT, ext2
    - **povrat** datoteka vrlo **jednostavan**
  - ext3, ext4
    - **mala vjerojatnost** uspješnog povrata obrisanih datoteka
  - NTFS, ostali datotečni sustavi ?

# Sigurno brisanje – Formatiranje diska



- prikaz stanja diska
  - prije formatiranja,
  - nakon brzog formatiranja (engl. *quick format*) i
  - nakon običnog formatiranja
- Je li formatiranje sigurno?
- Format vs *zero-fill*?
- Povrat podataka nakon *zero-fill* metode?
- Idući slajdovi prikazuju različite načine formatiranja
  - s USB flash diskom od 4 GB na Win7





# Disk – prije formatiranja



```
00008000 EB 3C 90 4D 53 44 4F 53 35 2E 30 00 02 80 08 00  ě<.MSDOS5.0..€..
00008010 02 00 02 00 00 F8 F0 00 3F 00 FF 00 40 00 00 00  ....řd.?.'.@...
00008020 B6 FF 77 00 80 00 29 3F 1F 66 3C 4E 4F 20 4E 41  ħ'w.€.)?.f<NO NA
00008030 4D 45 20 20 20 20 46 41 54 31 36 20 20 20 33 C9  ME  FAT16  3É
00008040 8E D1 BC F0 7B 8E D9 B8 00 20 8E C0 FC BD 00 7C  ŽŃŁd{ŽŮ,. ŽŘů".|
```

Boot block

```
00009000 F8 FF FF FF FF FF 04 00 FF FF FF FF FF FF FF FF  ř'.....
00009010 09 00 0A 00 FF FF 0C 00 0D 00 0E 00 0F 00 10 00  ....
00009020 11 00 12 00 FF FF 14 00 15 00 16 00 17 00 18 00  ....
00009030 19 00 1A 00 1B 00 1C 00 1D 00 1E 00 1F 00 20 00  ....
00009040 21 00 22 00 23 00 24 00 25 00 26 00 27 00 28 00  !."#$.%&'.(
00009050 29 00 2A 00 2B 00 2C 00 2D 00 2E 00 2F 00 30 00  ).*+.,-.../.0.
00009060 31 00 32 00 33 00 34 00 35 00 36 00 37 00 38 00  1.2.3.4.5.6.7.8.
00009070 39 00 3A 00 3B 00 3C 00 3D 00 3E 00 3F 00 40 00  9...;<.=.>.?@.
00009080 41 00 42 00 43 00 44 00 45 00 46 00 47 00 48 00  A.B.C.D.E.F.G.H.
```

FAT tablica

```
00045000 43 4F 44 45 53 20 20 20 54 58 54 20 18 82 52 A1  CODES  TXT  ,,R~
00045010 47 47 5D 47 00 00 17 A1 47 47 02 00 28 00 00 00  GG]G...~GG..(...
00045020 46 45 52 2D 4C 4F 47 4F 50 4E 47 20 18 7A C1 A1  FER-LOGOPNG .zÁ~
00045030 47 47 5D 47 00 00 4A A1 47 47 03 00 21 05 01 00  GG]G..J~GG..!...
00045040 4D 4F 42 49 4C 45 20 20 20 20 20 10 08 4C D0 A1  MOBILE  ..LÐ~
00045050 47 47 47 47 00 00 1D A1 47 47 05 00 00 00 00 00  GGGG...~GG.....
00045060 E5 45 4C 45 54 45 44 20 20 20 20 08 55 97 0E  ÍELETED  .U-.
00045070 48 47 48 47 00 00 35 A1 47 47 0B 00 14 00 00 00  HGHG..5~GG.....
```

Korijenski direktorij

```
00049000 53 6F 6D 65 20 74 65 78 74 0D 0A 49 6E 73 74 72  Some text..Instr
00049010 75 63 74 69 6F 6E 73 0D 0A 53 6F 6D 65 20 6F 74  uctions..Some ot
00049020 68 65 72 20 74 65 78 74 00 00 00 00 00 00 00 00  her text.....
00049030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

Nasumična datoteka na disku

# Disk – nakon brzog formatiranja



```
00008000 EB 3C 90 4D 53 44 4F 53 35 2E 30 00 02 80 08 00  ě<.MSDOS5.0..€..
00008010 02 00 02 00 00 F8 F0 00 3F 00 FF 00 40 00 00 00  ....řd.?.'.@...
00008020 B6 FF 77 00 80 00 29 9A 77 F3 D4 4E 4F 20 4E 41  ě'w.€.)šwóŃNO NA
00008030 4D 45 20 20 20 20 46 41 54 31 36 20 20 20 33 C9  ME FAT16 3Ě
00008040 8E D1 BC F0 7B 8E D9 B8 00 20 8E C0 FC BD 00 7C  ŽŃLd{ŽŮ,. Žřü~.|
```

Boot block

```
00009000 F8 FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00  ř'.....
00009010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00009020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00009030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00009040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00009050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00009060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00009070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00009080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

FAT tablica

Nule

```
00045000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00045010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00045020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00045030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00045040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00045050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00045060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00045070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

Korijenski direktorij

```
00049000 53 6F 6D 65 20 74 65 78 74 0D 0A 49 6E 73 74 72  Some text..Instr
00049010 75 63 74 69 6F 6E 73 0D 0A 53 6F 6D 65 20 6F 74  uctions..Some ot
00049020 68 65 72 20 74 65 78 74 00 00 00 00 00 00 00 00  her text.....
00049030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

Nasumična datoteka na disku

Potrebno vrijeme: ~ 3 sekunde

# Disk – nakon formatiranja



```
00008000 EB 3C 90 4D 53 44 4F 53 35 2E 30 00 02 80 08 00  ě<.MSDOS5.0..€..
00008010 02 00 02 00 00 F8 F0 00 3F 00 FF 00 40 00 00 00  ....řd.?.'.@...
00008020 B6 FF 77 00 80 00 29 9A 77 F3 D4 4E 4F 20 4E 41  Ě'w.€.)šwóŃNO NA
00008030 4D 45 20 20 20 20 46 41 54 31 36 20 20 20 33 C9  ME  FAT16 3Ě
00008040 8E D1 BC F0 7B 8E D9 B8 00 20 8E C0 FC BD 00 7C  ŽŃLd{ŽŮ,. ŽŘü~.|
```

Boot block

```
00009000 F8 FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00  ř'.....
00009010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00009020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00009030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00009040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00009050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00009060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00009070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00009080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

FAT tablica

Nule

```
00045000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00045010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00045020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00045030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00045040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00045050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00045060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00045070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

Korijenski direktorij

```
00049000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00049010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00049020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00049030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

Nasumična datoteka na disku

Potrebno vrijeme: ~ 12 minuta

# Kako sigurno obrisati podatke?



- **Brisanje datoteka, quick format**
  - Samo metapodatci se brišu, podatci se mogu rekonstruirati, **NIJE SIGURNO**
- **Formatiranje, zero-fill**
  - disk se **popunjava nulama**
    - *Windows format,*
    - *dd na Linux,*
    - *DBAN, KillDisk*
  - Ova metoda bi trebala biti sigurna za prosječnog korisnika
  - problem loših sektora
    - format će ih preskočiti
    - podatci će ostati
    - i moguće ih je rekonstruirati

## Darik's Boot and Nuke

**Warning:** This software irrecoverably destroys data.

This software is provided without any warranty; without even the implied warranty of merchantability or fitness for a particular purpose. In no event shall the software authors or contributors be liable for any damages arising from the use of this software. This software is provided "as is".

<http://www.dban.org/>

- \* Press the **F2** key to learn about DBAN.
- \* Press the **F3** key for a list of quick commands.
- \* Press the **F4** key for troubleshooting hints.
- \* Press the **ENTER** key to start DBAN in interactive mode.
- \* Enter **autonuke** at this prompt to start DBAN in automatic mode.

boot: \_

# Kako sigurno obrisati podatke?

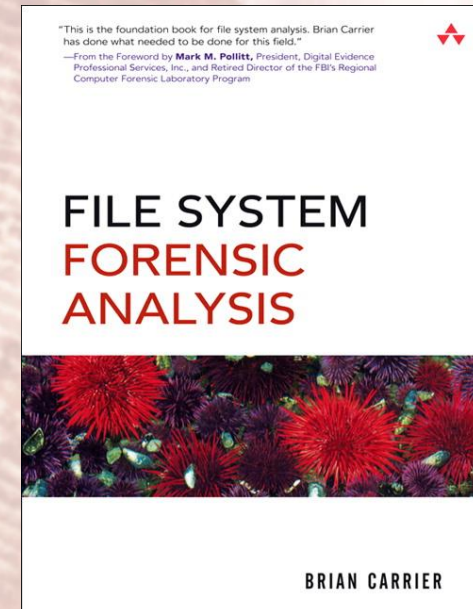


- Rad Petera Gutmanna (s novim diskovima, njegov rad je možda zastarjeo)
  - Nula koje je obrisana nulom
  - Može se razlikovati od
  - One koja je obrisana jedinicom
  - Uz vjerojatnost višu od 50%
- Disk wipe
  - Standard US vlade DoD 5220.22-M (3-pass) predlaže da se proces brisanja sastoji od tri faze
  - Prebriši sve lokacije koje je moguće adresirati:
    - znak (nula)
    - komplement znaka (jedinica)
    - nasumični znak
- Fizičko uništavanje
  - jaki magneti,
  - bušilice, čekić,
  - kiselina
  - su najučinkovitiji način





- Brian Carrier:  
„File system forensic analysis”
  - Jedna od najboljih knjiga o datotečnim sustavima
- D. Farmer, W. Venema:  
„Forensic discovery”
- D. Poirier:  
„The Second Extended File System”





RacFor.zesoi.fer.hr

RacFor@zesoi.fer.hr

