

COMPUTER FORENSICS

Lezione 18: L'Analisi *i File System* (2^a parte)



A.A. 2021/22

Dott. Lorenzo LAURATO

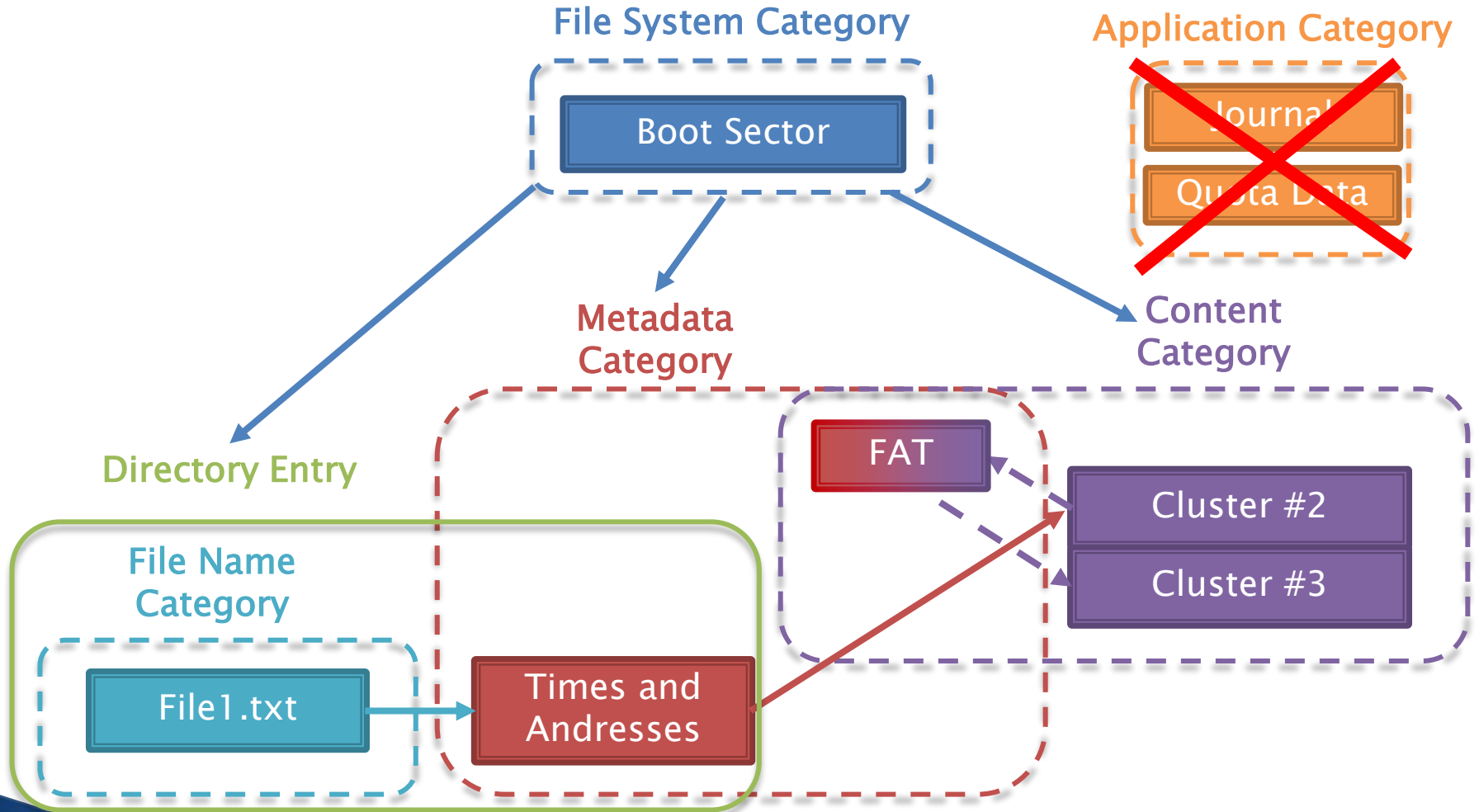


File System

»» FAT File System

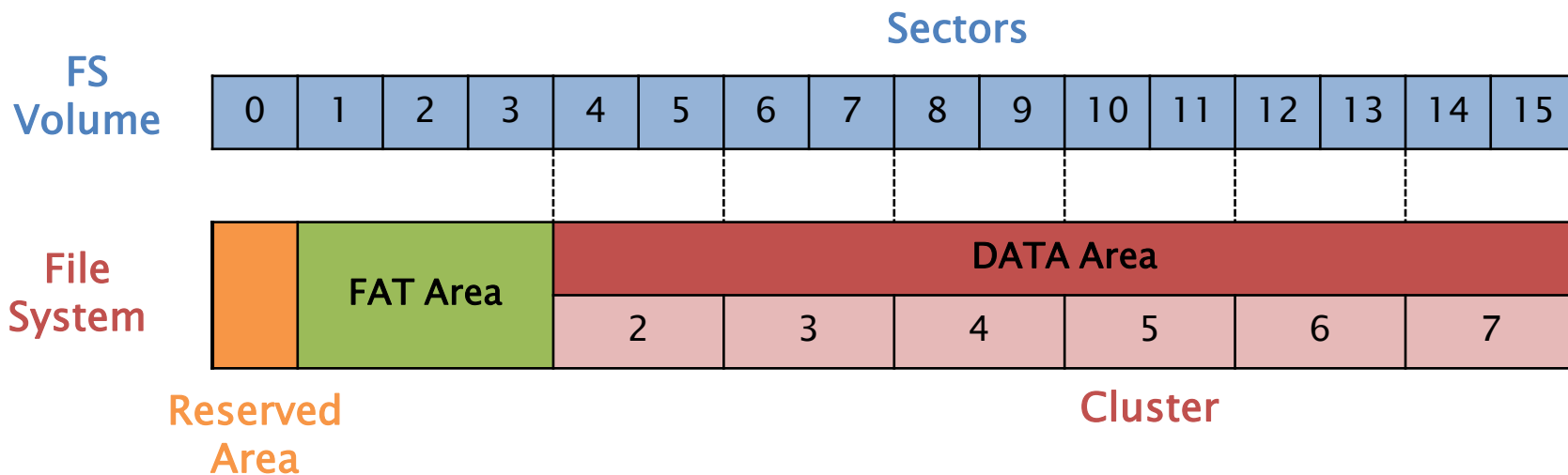


FAT File System



FAT File System

Physical Layout



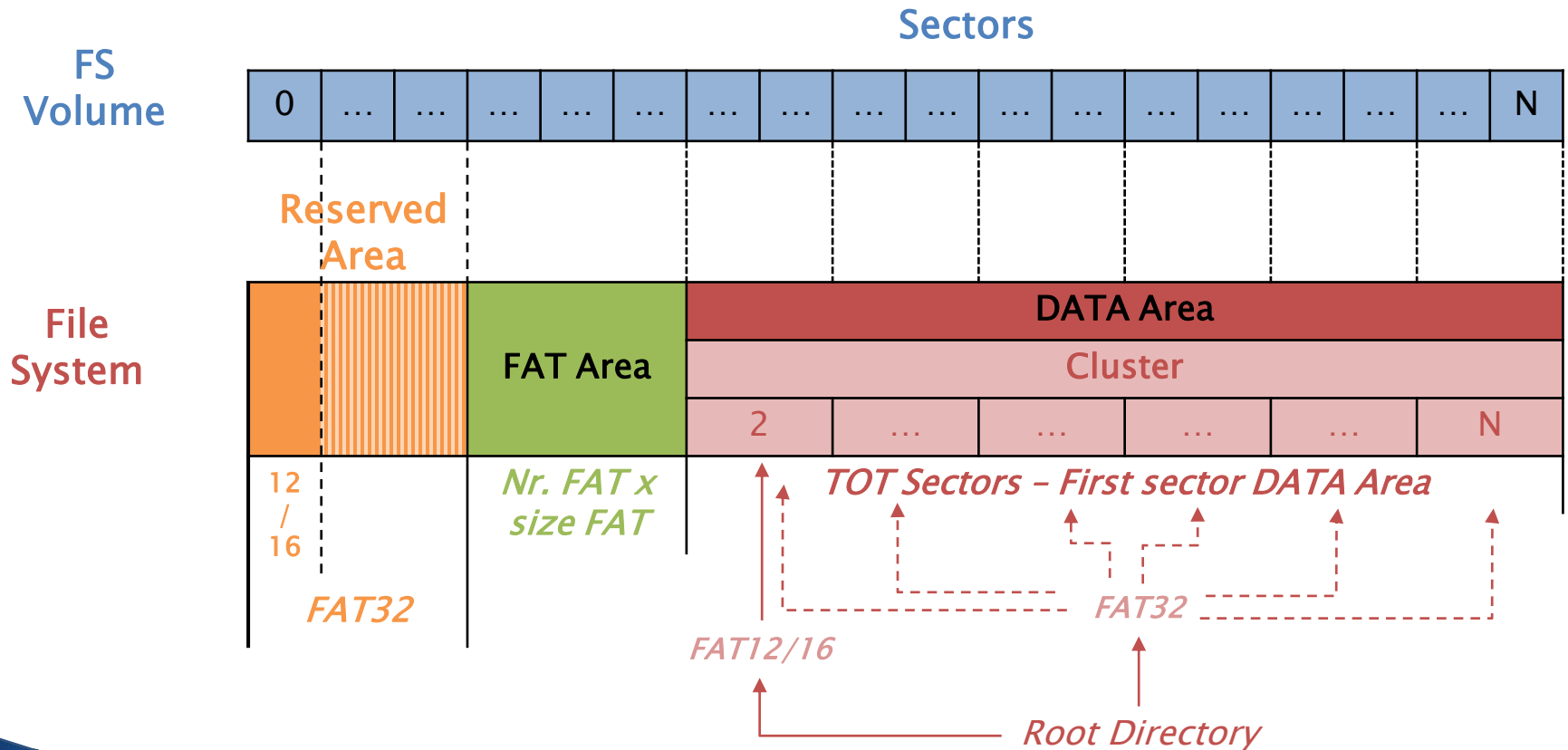
FAT File System

File System Category

- ▶ **FSINFO (FAT32):** Reserved Area (*BootSector*)
 - Cluster liberi
 - Prossimo Cluster libero
- ▶ **Boot Sector:** primo settore (*Reserved Area*)
 - *Physical Layout (Essential Data):*
 - **Reserved Area:** *settore 0*
 - FAT12/16: Dimensione 1 Settore
 - FAT32: Dimensione variabile
 - **FAT Area:** *dopo la «Reserved Area»*
 - Dimensione: Nr. FAT x Size FAT
 - **Data Area:** *dopo la «FAT Area»*
 - Dimensione: tot. settori – Inizio Area
 - Dimensione Cluster
 - Root directory:
 - Posizione (FAT32)
 - Dimensione (FAT12/16)

FAT File System

Physical Layout



FAT File System

File System Category

- ▶ **Boot Sector:** primo settore (*Reserved Area*)
 - *NO Essential Data:*
 - OEM Name: info strumento creazione del FS
 - Volume Serial Number: data di creazione (Microsoft)
 - File System Label: *FAT, FAT12, FAT16, FAT32*

FAT File System

Boot Sector

Byte	Description	Es.
0-2	Istruzioni assembly per saltare al bootcode	NO
3-10	OEM Name (ASCII)	NO
11-12	Dimensione settore (Byte)	SI
13	Dimensione Cluster (Settori) [x^2 max 32kb]	SI
14-15	Dimensione Reserved Area (Settori)	SI
16	Nr. di FAT [solitamente 2]	SI
17-18	Max nr. File in root directory [FAT12/16] 0 (ZERO) [FAT32] => Byte 36-39	SI
19-20	Tot. settori FS [se > 65.536 => 0; usare Byte 32-35]	SI
21	Media Type [f8 - dischi fissi, f0 - disp. removibili]	NO
22-23	Dimensione FAT (settori) [FAT12/16] 0 (ZERO) [FAT32]	SI
24-25	Nr. settori per traccia INT.13h	NO
26-27	Nr. Head dispositivo INT.13h	NO
28-31	Nr. settori prima dell'inizio della partizione	NO
32-35	Tot. settori FS [se < 65.536 => 0; usare Byte 19-20]	NO

FAT File System

Boot Sector (FAT12/16)

Byte	Description	Es.
36	BIOS INT.13h	NO
37	Non usato	NO
38	Extended boot signature: identifica se i successivi tre valori sono validi [29]	NO
39-42	Volume Serial Number [Windows lo genera utilizzando la data di creazione]	NO
43-53	Etichetta Volume (ASCII) [scelto dall'utente\tool al momento della creazione del FS]	NO
54-61	File System type (ASCII) [FAT, FAT12, FAT16]	NO
62-509	Non usato [boot code]	NO
510-511	Signature [AA55]	NO

FAT File System

Boot Sector (FAT32)

Byte	Description	Es.
36-39	Dimensione della FAT (settori)	SI
40-41	Nr. di FAT [se bit[7]=1 solo una delle FAT bit[0-3] è attiva, altrimenti mirror]	SI
42-43	Nr. di versione	SI
44-47	Posizione root directory (cluster)	SI
48-49	Posizione della struttura FSINFO (settori)	NO
50-51	Copia di backup del Boot Sector (settori) [6]	NO
52-63	Riservati	NO
64	BIOS INT.	NO
65	Non usato	NO
66	Extended boot signature: identifica se i successivi tre valori sono validi [29]	NO
67-70	Volume SN [Windows lo genera utilizzando la data di creazione]	NO
71-81	Etichetta Volume (ASCII)	NO
82-89	File System type (ASCII) [FAT32]	NO
90-509	Non usato [boot code]	NO
510-511	Signature [AA55]	NO

FAT File System

Boot Sector: analisi

```
root@caine:/# blkcat -f fat fat-4.dd 0 | xxd
00000000: eb58 904d 5344 4f53 352e 3000 0202 2600 .X.MSDOS5.0...&
00000016: 0200 0000 00f8 0000 3f00 4000 c089 0100 .....?..@.....
00000032: 4023 0300 1d03 0000 0000 0000 0200 0000 @#.....
[...]
```

Byte	Description	Value
3-10	OEM Name (ASCII)	MSDOS5.0
11-12	Dim. settore (Byte)	0200 (512)
13	Dim. Cluster (Settori)	2
14-15	Dim. Reserved Area (Settori)	0026 (38)
16	Nr. di FAT	2
17-18	Max nr. File in root directory	0
19-20	Tot. settori FS	0
21	Media Type	f8(disco fisso)
22-23	Dim. FAT (settori)	0
28-31	Nr. settori prima dell'inizio della partizione	000189c0 (100.800)
32-35	Tot. settori FS	00032340 (205.632)

FAT File System

Boot Sector: analisi

```
root@caine:/# blkcat -f fat fat-4.dd 0 | xxd
```

```
[...]
```

```
0000032: 4023 0300 1d03 0000 0000 0000 0200 0000 @#.....
```

```
0000048: 0100 0600 0000 0000 0000 0000 0000 0000 .....
```

```
0000064: 8000 2903 4619 4c4e 4f20 4e41 4d45 2020 ..).F.LNO NAME
```

```
0000080: 2020 4641 5433 3220 2020 33c9 8ed1 bcf4 FAT32 3.....
```

```
[...]
```

```
0000496: 7274 0d0a 0000 0000 00ac cbd8 0000 55aa rt.....U.
```

Byte	Description	Value
36-39	Dimensione della FAT (settori)	00031d (797)
44-47	Posizione root directory (cluster)	00000002 (2)
48-49	Posizione della struttura FSINFO (settori)	0001 (1)
50-51	Copia di backup del Boot Sector (settori)	0006 (6)
67-70	Volume SN	4c194603
71-81	Etichetta Volume (ASCII)	«NO NAME »
82-89	File System type (ASCII) [FAT32]	«FAT32 »
510-511	Signature	AA55

FAT File System

FSINFO

Byte	Description	Es.
0-3	Signature [41615252]	NO
4-483	Non usato	NO
484-487	Signature [61417272]	NO
488-491	Nr. di Cluster liberi	NO
492-495	Prossimo Cluster libero	NO
496-507	Non usato	NO
508-511	Signature [AA550000]	NO

FAT File System

FSINFO: analisi

```
root@caine:/# blkcat -f fat fat-4.dd 1 | xxd
```

```
0000000: 5252 6141 0000 0000 0000 0000 0000 0000 RRaA.....
0000016: 0000 0000 0000 0000 0000 0000 0000 0000 .....
          [...]
0000464: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0000480: 0000 0000 7272 4161 1e8e 0100 4b00 0000 ....rrAa....K...
0000496: 0000 0000 0000 0000 0000 0000 0000 0000 .....U.
```

Byte	Description	Value
0-3	Signature	41615252
484-487	Signature	61417272
488-491	Nr. di Cluster liberi	00018e1e (101.918)
492-495	Prossimo Cluster libero	0000004b (75)
508-511	Signature	AA550000

FAT File System

Boot Sector: analisi

```
root@caine:/# fsstat -f fat fat-4.dd
```

FILE SYSTEM INFORMATION

File System Type: FAT
OEM Name: MSDOS5.0
Volume ID: 0x4c194603
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory): FAT DISK
File System Type Label: FAT32

Backup Boot Sector Location: 6
FS Info Sector Location: 1
Next Free Sector (FS Info): 1778
Free Sector Count (FS Info): 203836
Sectors before file system: 100800

File System Layout (in sectors)

Total Range: 0 - 205631

* Reserved: 0 - 37

** Boot Sector: 0

** FS Info Sector: 1

** Backup Boot Sector: 6

* FAT 0: 38 - 834

* FAT 1: 835 - 1631

* Data Area: 1632 - 205631

** Cluster Area: 1632 - 205631

*** Root Directory: 1632 - 1635

CONTENT-DATA INFORMATION

Sector Size: 512

Cluster Size: 1024

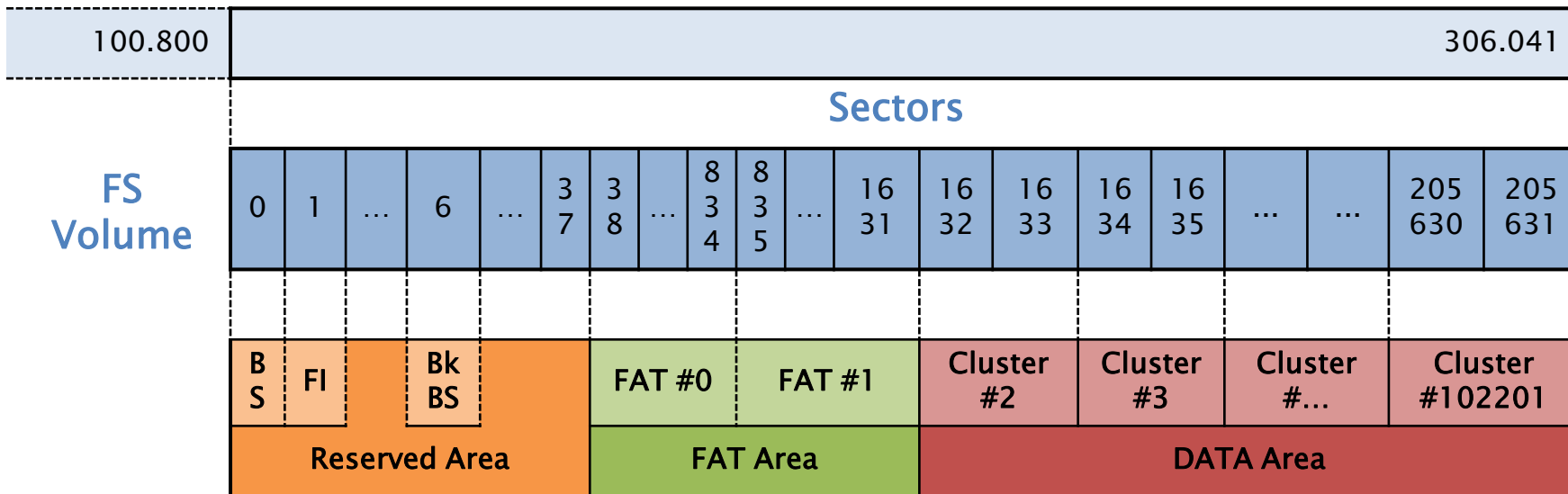
Total Cluster Range: 2 - 102001

[...]

FAT File System

Physical Layout

Disk Volume



FAT File System

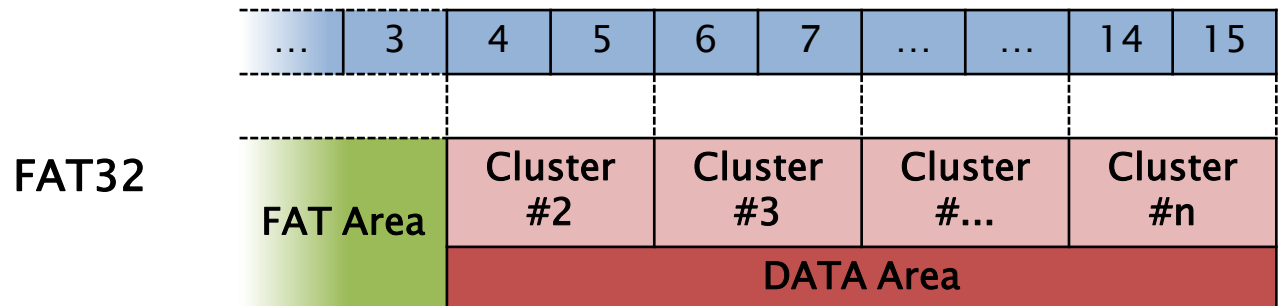
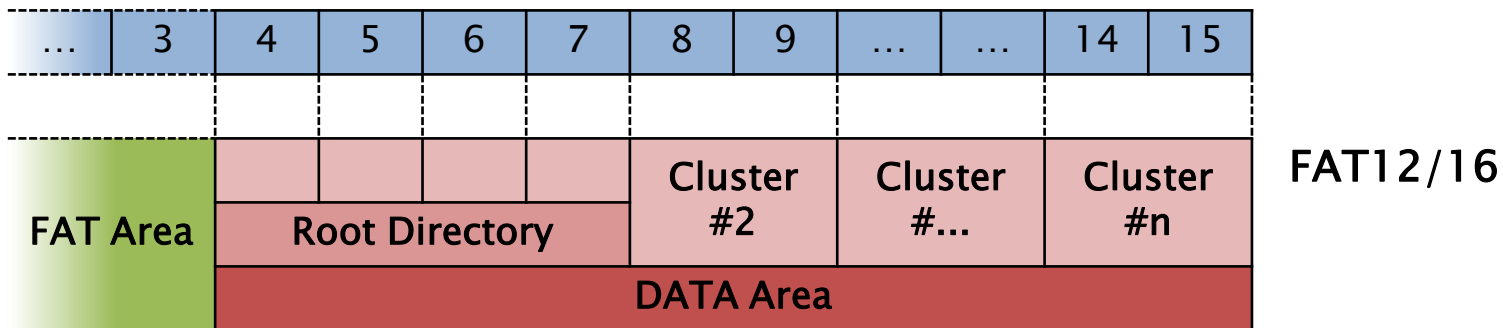
File System Category: analisi

- ▶ Recuperare informazioni sul layout
- ▶ Controllare possibili dati nascosti:
 - Bootcode
 - Settori in Reserved Area:
 - FSINFO
 - Volume slack
- ▶ Confronto tra il Boot Sector ed il backup del Boot Sector

FAT File System

Content Category

- ▶ Contenuto di File e Directory
- ▶ Cluster: 2^x settori (*max 32KB*)
 - Primo Cluster: indirizzo 2
 - Solo in Data Area



FAT File System

FAT

- ▶ Identificare lo stato di allocazione dei Cluster
- ▶ Successivo Cluster del file: *Cluster Chain*
- ▶ Layout: *Boot Sector*
- ▶ Entry di ugual dimensione: FAT12: 12bit, FAT16: 16bit, FAT32: 32bit
 - Indirizzamento diretto:
 - La prima entry ha indirizzo 0 ZERO
 - Indirizzo entry = Indirizzo Cluster: *Es. Entry[10]=Cluster[10]*
 - Entry[0]: informazione del media
 - Entry[1]: dirty status
 - Entry[2] -> Cluster[2]
 - Entry[n] -> Cluster[n]

FAT File System

FAT

► Contenuto delle Entry:

DATA Area					
2	3	4	5	...	n

	FAT
0	<i>Info Media</i>
1	<i>Dirty status</i>
2	
3	
4	
5	
...	
n	

- Cluster non allocato: 0 (Zero)
- Cluster allocato:
 - Prossimo cluster (*Cluster Chain*)
 - EOF:
 - *0xff8 [FAT12]*
 - *0xfff8 [FAT16]*
 - *0x0fff fff8 [FAT32]*
- Cluster danneggiato:
 - *0xff7 [FAT12]*
 - *0xfff7 [FAT16]*
 - *0x0fff fff7 [FAT32]*

FAT File System

FAT: analisi

```
root@caine:/# blkcat -f fat fat-4.dd 38 | xxd
```

[...]

```
0000288: 4900 0000 4a00 0000 4c00 0000 0000 0000 I...J...L.....
0000304: 4d00 0000 ffff ff0f 4f00 0000 ffff ff0f M.....O.....
0000320: 5100 0000 5200 0000 ffff ff0f ffff ff0f Q...R.....
0000336: ffff ff0f 0000 0000 0000 0000 0000 0000 .....
0000352: 0000 0000 0000 0000 0000 0000 0000 0000 .....
```

Entry: 32Byte
(Offset/4)

Entry #	Byte	Valore
72	288-291	00000049 (73)
73	292-295	0000004a (74)
74	296-299	0000004c (76)
75	300-303	00000000 (0)
76	304-307	0000004d (77)
...
85	340-343	00000000 (0)

FAT File System

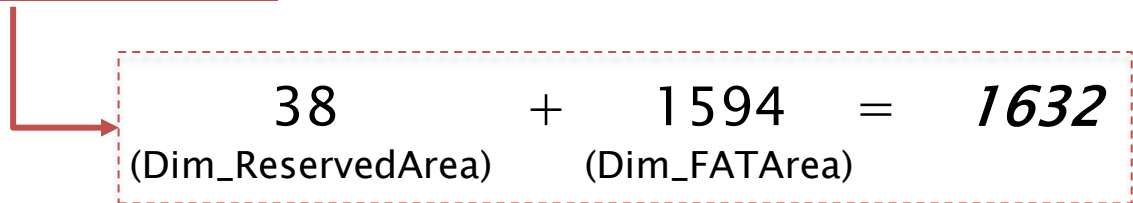
FAT

► Indirizzamento:

- Cluster => Settore ?
- **Settore** = (Cluster_Address - 2) x N_Sect_Cluster + Sect_Cluster_2
(Boot Sector) (Sect_DataArea)

Es.: Cluster 75:

$$(75 - 2) \times 2 + \text{Sect_Cluster_2}$$


$$\begin{array}{rcccl} 38 & + & 1594 & = & 1632 \\ \text{(Dim_ReservedArea)} & & \text{(Dim_FATArea)} & & \end{array}$$

$$(75 - 2) \times 2 + 1632 \Rightarrow 1778$$

FAT File System

FAT

- ▶ Indirizzamento:
 - Cluster => Settore ?

```
root@caine:/# blkstat -f fat fat-4.dd 1778
```

Sector: 1778

Not Allocated

Cluster: 75

FAT File System

Metadata Category

- ▶ Informazioni su file e directory
 - Indirizzo del primo cluster
- ▶ Parent Directory:
 - Directory Entry: 32KB
 - File
 - Directory
 - Posizionata nella Data Area (Cluster)
 - File Name Category:
 - Nome File (8 caratteri) + Estensione (3 caratteri)
 - > Long File Name Directory Entry

FAT File System

Directory Entries

Byte	Description	Es.
0	<ul style="list-style-type: none"> – Primo carattere del filename (ASCII) – 0xe5 o 0x00 [non allocato] 	SI
1–10	Caratteri da 2 a 11 del filename (ASCII)	SI
11	Attributo File	SI
12	Riservato	NO
13	Ora di creazione (decimi di secondo)	NO
14–15	Ora di creazione (ora, minuti, secondi)	NO
16–17	Data di Creazione	NO
18–19	Data di Accesso	NO
20–21	<ul style="list-style-type: none"> – Indirizzo del primo cluster (High Byte) – 0 (ZERO) [FAT12/16] 	SI
22–23	Ora di Modifica (ora, minuti, secondi)	NO
24–25	Data di Modifica	
26–27	Indirizzo del primo cluster (Low Byte)	SI
28–31	<ul style="list-style-type: none"> – Dimensione del file – 0 (ZERO) per le directory 	SI

FAT File System

Directory Entries: attributes

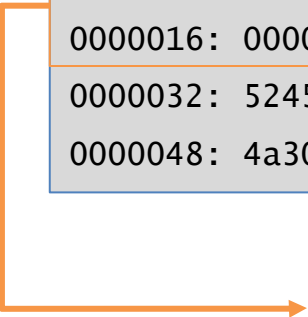
Attributo File [Byte 11]		
Flag Value bit	Description	Es.
0000 0001 (01)	Sola lettura	NO
0000 0010 (02)	File nascosto	NO
0000 0100 (04)	File di sistema	NO
0000 1000 (08)	Etichetta volume	SI
0000 1111 (0f)	Long File name	SI
0001 0000 (10)	Directory	SI
0010 0000 (20)	Archive	NO

FAT File System

Directory Entries: analisi

```
root@caine:/# blkcat -f fat fat-4.dd 1632 | xxd
```

```
00000000: 4641 5420 4449 534b 2020 2008 0000 0000 FAT DISK      ....
0000016: 0000 0000 0000 874d 252b 0000 0000 0000 .....M%+.....
0000032: 5245 5355 4d45 2d31 5254 4620 00a3 347e RESUME-1RTF ..4~
0000048: 4a30 8830 0000 4a33 7830 0900 f121 0000 .0.0.....0...!..
```



Byte	Description	Value
0	Fila Name - Primo carattere	F
1-10	Fila Name - Dieci caratteri	«AT DISK »
11	Attributo File	08 (0000 1000) [Etichetta Volume]
22-23	Ora di Modifica	4d87
24-25	Data di Modifica	2b25

FAT File System

Directory Entries: analisi

Byte	Description	Value
22-23	Ora di Modifica	4d87
24-25	Data di Modifica	2b25

0	0	1	0	1	0	1	1	0	0	1	0	0	1	0	1
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Anno (0-127) + 1980							Mese (1-12)				Giorno (1-31)				
2001							9				5				

0	1	0	0	1	1	0	1	1	0	0	0	0	1	1	1
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Ora (0-23)						Minuti (0-59)					Secondi (0-29) x 2				
9						44					14				

FAT File System

Directory Entries: analisi

```
root@caine:/# blkcat -f fat fat-4.dd 1632 | xxd
00000000: 4641 5420 4449 534b 2020 2008 0000 0000 FAT DISK      .....
00000016: 0000 0000 0000 874d 252b 0000 0000 0000 .....M%+.....
00000032: 5245 5355 4d45 2d31 5254 4620 00a3 347e RESUME-1RTF ..4~
00000048: 4a30 8830 0000 4a33 7830 0900 f121 0000 .0.0.....0...!..
```

Byte	Description	Value
0	Fila Name - Primo carattere	R
1-10	Fila Name - Dieci caratteri	«ESUME-1.RTF»
11	Attributo File	20 (0010 0000) [Archive]
13	Ora di Creazione (decimi s)	a3 (163)
14-15	Ora di Creazione	7e34 (15:49:40)
16-17	Data di Creazione	304a (10/02/2004)
20-21 26-27	Indirizzo Primo cluster File	0000 0009 (9)
28-31	Dimensione del file	000021f1 (8.689)


FAT File System

FAT: analisi

```
root@caine:/# blkcat -f fat-fat-4.dd 38 | xxd
```

```
[...]
```

```
0000032: ffff ff0f 0a00 0000 0b00 0000 0c00 0000 .....  
0000048: 0d00 0000 0e00 0000 0f00 0000 1000 0000 .....  
0000064: 1100 0000 ffff ff0f 1300 0000 1400 0000 .....
```



Entry #	Byte	Valore
9	36-39	0000000a (10)
10	40-43	0000000b (11)
11	44-47	0000000c (12)
12	48-51	0000000d (13)
13	52-55	0000000e (14)
14	56-59	0000000f (15)
15	60-63	00000010 (16)
16	64-67	00000011 (17)
17	68-71	0ffffff (EOF)

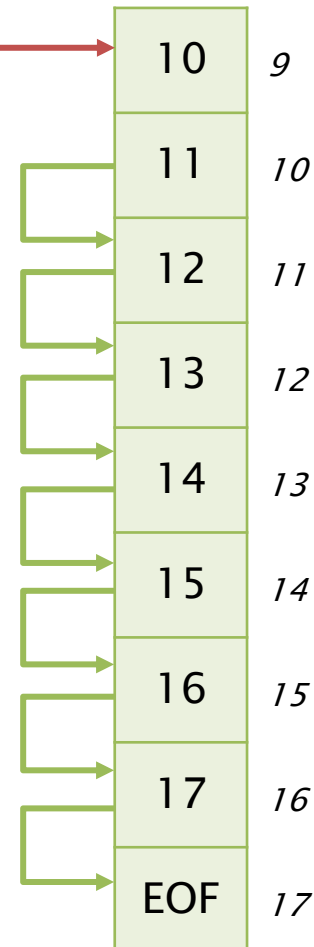
FAT File System

FAT: cluster chain

Directory Entry

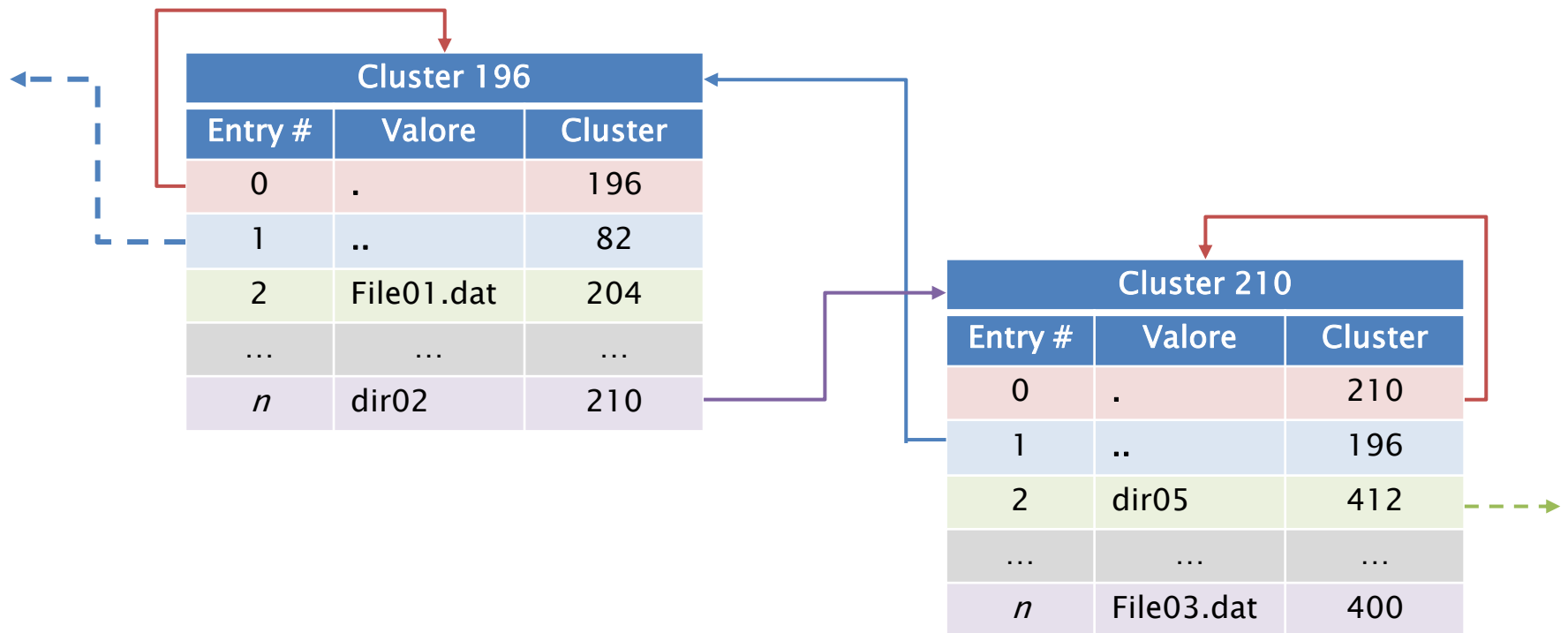
File Name	Start	Dimensione
RESUME-1.RTF	9	8.689

FAT



FAT File System

Metadata Category: Directory



FAT File System

Metadata Category

- ▶ Informazioni temporali (*non essential data*)
 - Data di creazione (Windows)
 - Nuovo File/Copia File => Nuova data
 - Sposto/Rinomino => copia della data
 - Data di Modifica (Windows): modifica del contenuto
 - Copia/Sposto/Rinomino File => copia della data
 - Data di Accesso (Windows):
 - Modificata anche visualizzando le proprietà

FAT File System

File Name Category

- ▶ Mappare le strutture «Metadata» con un etichetta: Filename
- ▶ Directory Entry: insieme ai «Metadata Category»
 - FileName 11 caratteri
 - Long File Name (LFN) directory entry: +13 caratteri

Cluster 196		
Entry #	Valore	Cluster
0	.	196
1	..	82
2	FileSys.TXT	204
3	TextFileFAT	204
4	TE021F~1.TXT	204
...

FAT File System

File Name Category

Byte	Description	Es.
0	Nr. sequenza (bit)	SI
1-10	Nome File [caratteri da 1 a 5]	SI
11	Attributo file [0f]	SI
12	Reserved	NO
13	Checksum	SI
14-25	Nome File [caratteri da 6 a 11]	SI
26-27	Reserved	NO
28-31	Nome File [caratteri da 12 a 13]	SI



SSRI Lorenzo Laurato s.r.l.



Via Coroglio nr. 57/D (BIC- Città della Scienza)
80124 Napoli



Tel. 081.19804755

Fax 081.19576037



lorenzo.laurato@unina.it

lorenzo.laurato@ssrilab.com



www.docenti.unina.it/lorenzo.laurato

www.computerforensicsunina.forumcommunity.net