COMPUTER FORENSICS

Lezione 19: L’Analisi *i File System*

(3ª parte)

SSRI
Sicurezza Sistemi
Reti Informatiche

UNINA UNIVERSITA’ DEGLI STUDI DI NAPOLI FEDERICO II

A.A. 2021/22

Dott. Lorenzo LAURATO

File System

» NT File System

SSRI
Sicurezza Sistemi
Reti Informatiche

Università degli Studi di Napoli Federico II

a.a. 2021/22

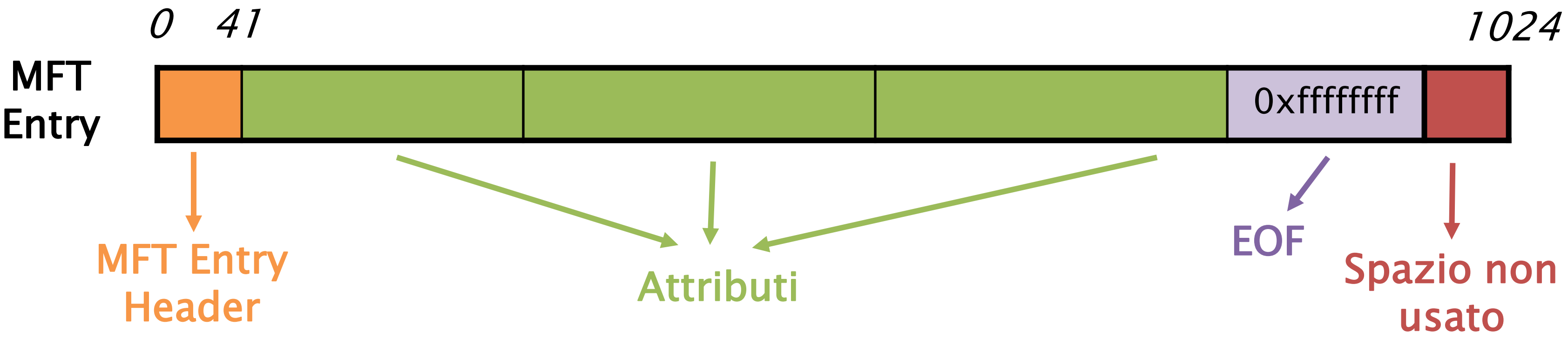
NT File System

- **New Technologies File System (NTFS)**
  - Microsoft 1993

- Ogni cosa è un file:
  - **$MFT**: *Master File Table*
  - **$MFTMirr**: *backup della MFT*
  - **$Boot**: *boot sector*
  - **$Volume:** *informazioni del volume*
  - **$Bitmap:** *stato di allocazione dei cluster*
  - **$AttDef:** *definizione degli attributi*
  - **$BadClus:** *elenco dei cluster danneggiati*
  - **$Secure:** *descrittore di sicurezza*
  - **$I30**: *Index*
  - …

NT File System
Master File Table ($MFT)

- Contiene informazioni sul file e directory:
  - Ogni file/directory ha almeno una entry *(File Record)*
    - 1024 byte *(boot sector)*
  - Entry[0]: $MFT
- Starter Cluster *(Boot Sector)*

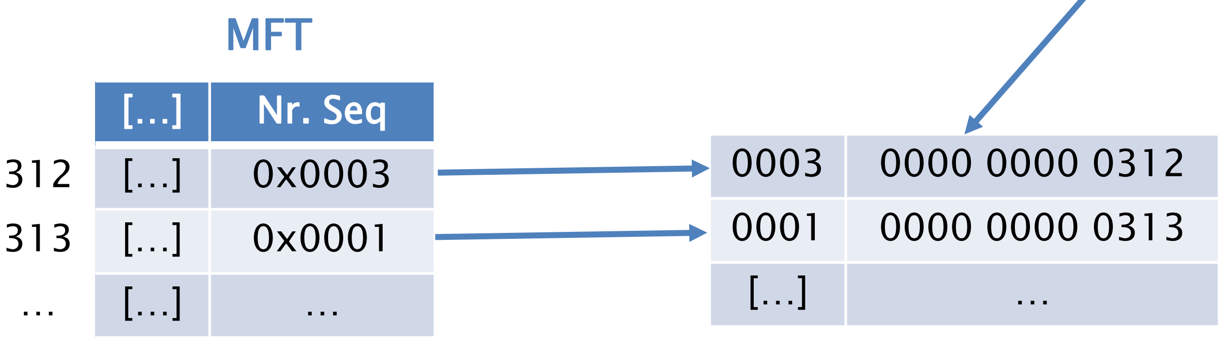


NT File System
Master File Table ($MFT)

MFT Entry

- **Dimensione** 1024 Byte:
  - Header: 42byte
  - Attributi: *strutture dati*
- **Signature**: *«FILE» / «BAAD»*
- **Stato di allocazione**: attributo ***$BITMAP*** nella *entry[0]* $MFT
- **Indirizzo sequenziale**: 48bit *(File Number)*
- **Numero sequenziale:** 16bit *(contatore allocazione)*

File Reference Address



MFT

	[...]	Nr. Seq
312	[...]	0x0003
313	[...]	0x0001
...	[...]	...

0003	0000 0000 0312
0001	0000 0000 0313
[...]	...

NT File System

Master File Table ($MFT)

Byte	Description	Es.
0-3	Signature (ASCII) [FILE|BAAD]	NO
4-5	Offset to fixup array	YES
6-7	Number of entries in fixup array	YES
8-15	$LogFile Sequence Number	NO
16-17	Sequence value	NO
18-19	Link count	NO
20-21	Offset to first attribute	YES
22-23	Flags [01:in use | 02:directory]	YES
24-27	Used size of MFT entry	YES
28-31	Allocated size of MFT entry	YES
32-39	File reference to base record	NO
40-41	Next attribute ID	NO
42-1023	Attributes and fixup values	YES

NT File System

Master File Table ($MFT)

```
root@caine:/# icat -f ntfs ntfs1.dd 0-128 | xxd
0000000: 4649 4c45 3000 0300 4ba7 6401 0000 0000 FILE0...K.d.....
0000016: 0100 0100 3800 0100 b801 0000 0004 0000 ....8...........
0000032: 0000 0000 0000 0000 0600 0000 0000 0000 ................
0000048: 5800 0000 0000 0000 1000 0000 6000 0000 X...........`...
                             [...]
0000496: 3101 b43a 0500 0000 ffff ffff 0000 5800 1..:..........X.
0000512: 0000 0000 0000 0000 0000 0000 0000 0000 ................
                             [...]
0001008: 0000 0000 0000 0000 0000 0000 0000 5800 ..............X.
```

Byte	Description	Value
0–3	Signature (ASCII)	«FILE»
16–17	Sequence value	0001 (1)
18–19	Link count	0001 (1)
20–21	Offset to first attribute	0038 (56)
22–23	Flags [01:in use | 02:directory]	0001 (1)
32–39	File reference to base record	0
40–41	Next attribute id	0006 (1)
42–1023	Attributes and fixup values	

NT File System

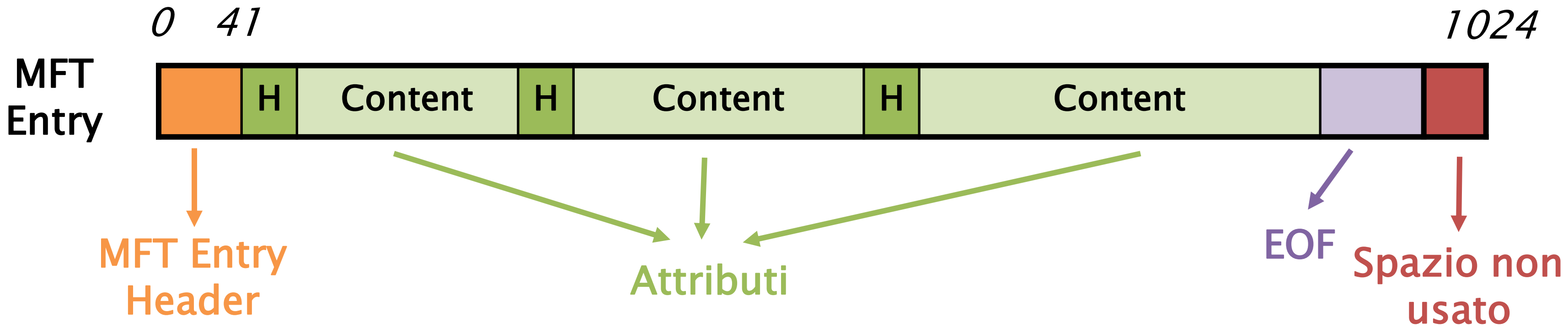
File System Metadata

- File contenenti dati per l’amministrazione del FS
- Prime 12 entry MFT

0	**$MFT**	MFT Entry
1	**$MFTMirr**	MFT Backup
2	**$LogFile**	Journal
3	**$Volume**	Volume Info
4	**$AttrDef**	Attribute info
5	**.**	Root directory
6	**$Bitmap**	Allocation status
7	**$Boot**	Boot Sector, BootCode
8	**$BadClus**	Cluster that have bad sector
9	**$Secure**	Security Info
10	**$Upcase**	Uppercase version of every Unicode character
11	**$Extend**	Application category

NT File System

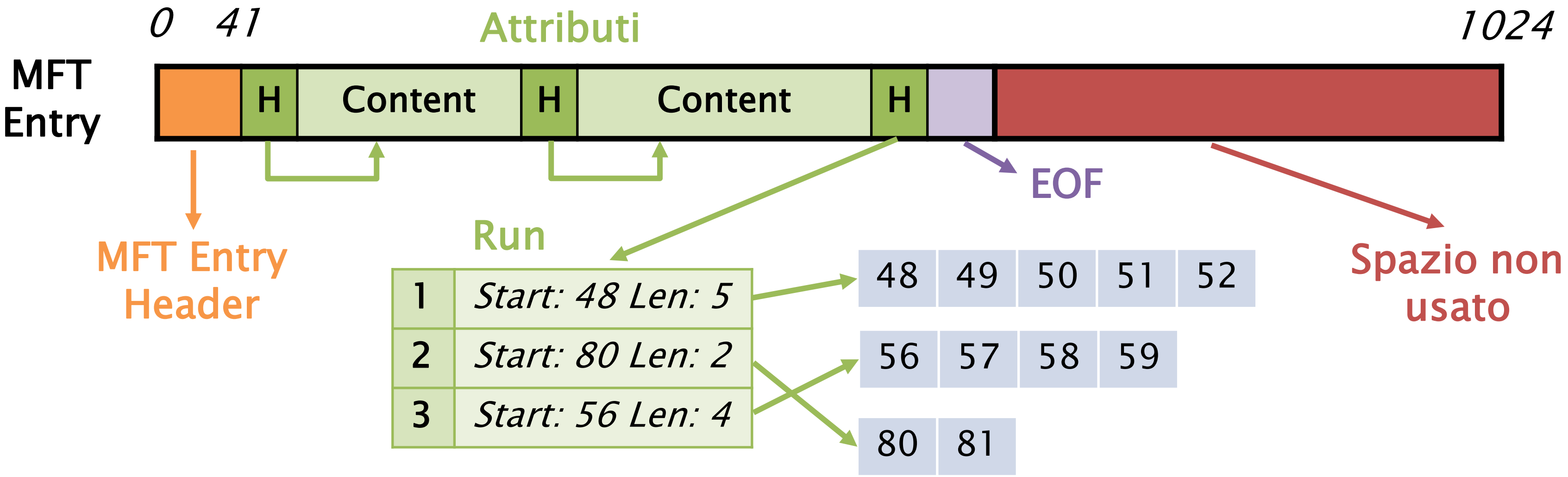
Attributes



- **Attribute Header:** descrive l'attributo *(tipo, dimensione, nome)*
  - **ID**: identificatore univoco nell'entry (16 bit)
  - **Type ID**: identificatore tipo attributo
  - **OFFSet** attribute Content

NT File System
Attributes

- **Attribute Content:**
  - **Residente:** viene posizionato all'interno della stessa entry
  - **Non residente:** viene posizionato in cluster esterni
    - *cluster run:* cluster consecutivi



Run	
1	*Start: 48 Len: 5*
2	*Start: 80 Len: 2*
3	*Start: 56 Len: 4*

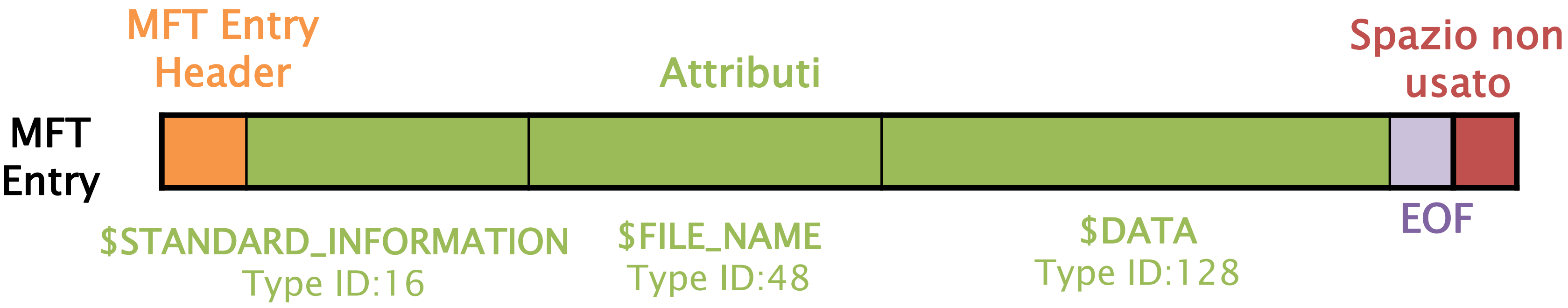
Virtual Cluster Number

0	1	2	3	4	5	6	7	8	9	10
48	49	50	51	52	80	81	56	57	58	59

NT File System

Standard Attribute Types

- Definiti nel FS Metadata ***$AttrDef***



16	$STANDARD_INFORMATION	*General information, such as flags; the last accessed, written, and created times; and the owner and security ID*
32	$ATTRIBUTE_LIST	*List where other attributes for file can be found*
48	$FILE_NAME	*File name, in Unicode, and the last accessed, written, and created times*
64	$VOLUME_VERSION	*Volume information*
64	$OBJECT_ID	*A 16-byte unique identifier for the file ordirectory*

NT File System

Standard Attribute Types

80	$SECURITY_ DESCRIPTOR	*The access control and security properties of the file*
96	$VOLUME_NAME	*Volume name*
112	$VOLUME_ INFORMATION	*File system version and other flags*
128	$DATA	*File contents*
144	$INDEX_ROOT	*Root node of an index tree*
160	$INDEX_ALLOCATION	*Nodes of an index tree rooted in $INDEX_ROOT attribute*
176	$BITMAP	*A bitmap for the $MFT file and for indexes*
192	$SYMBOLIC_LINK	*Soft link information*
192	$REPARSE_POINT	*Contains data about a reparse point*
208	$EA_INFORMATION	*Used for backward compatibility with OS/2 applications (HPFS)*
224	$EA	*Used for backward compatibility with OS/2 applications (HPFS)*
256	$LOGGED_UTILITY_STREAM	*Contains keys and information about encrypted attributes*

NT File System

Base/Non-Base MFT Entry

- Quando una entry riesce a contenere\descrivere tutti gli attributi per uno specifico file

**Base
MFT Entry**

🟧	$STANDARD_INFORMATION	$ATTRIBUTE_LIST	$FILE_NAME	$[ID3]	🟥

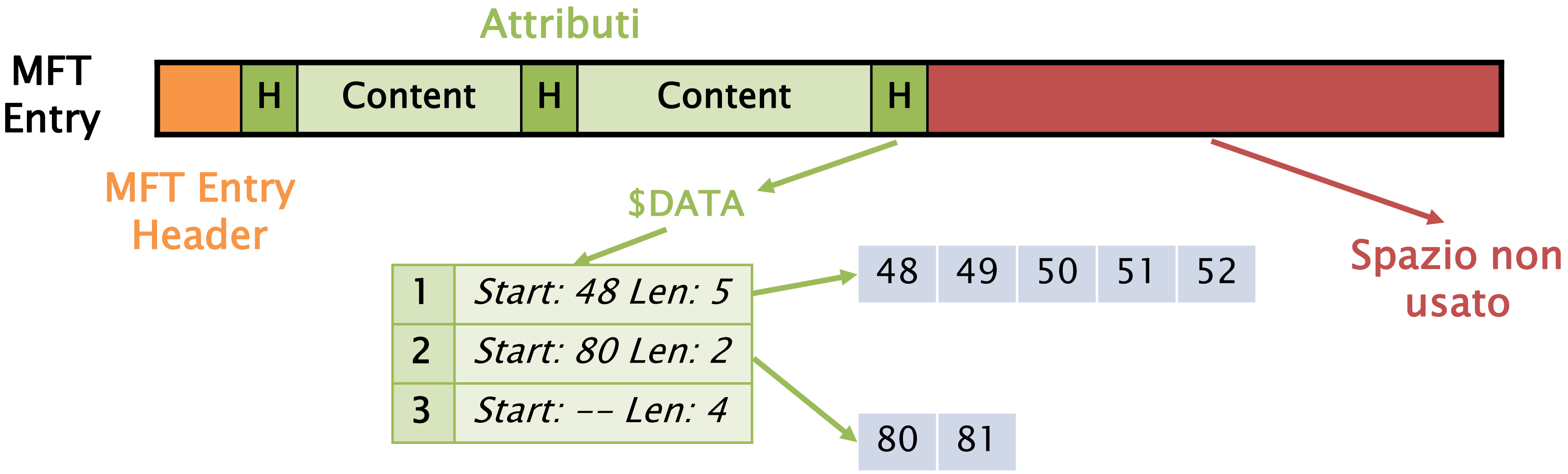
**Non-Base
MFT Entry**

🟧	$[ID4]	$[ID5]	$[ID6]	$[ID7]	🟥

NT File System

Sparse Attributes

- Risparmiare di allocare cluster ZERO per l’attributo **$DATA**



1	*Start: 48 Len: 5*
2	*Start: 80 Len: 2*
3	*Start: -- Len: 4*

Virtual Cluster Number

0	1	2	3	4	5	6	7	8	9	10
48	49	50	51	52	80	81	–	–	–	–

NT File System
altre caratteristiche

- **Compressione**: gli attributi non residenti $DATA
- **Indicizzazione**: collezione di attributi memorizzata in maniera ordinata (B-Tree)

NT File System

Attribute Header

Byte	Description	Es.
0–3	Attribute type ID	YES
4–7	Length of attribute	YES
8	Non-resident flag	YES
9	Length of name	YES
10–11	Offset to name	YES
12–13	Flags	YES
14–15	Attribute identifier	YES
16–19	Size of content	YES
20–21	Offset to content	YES

Resident Attribute

Flags	
0x0001	compressed
0x4000	encrypted
0x8000	sparse

NT File System

Resident Attribute Header

- **Starter Byte 56:**

```
0000000: 1000 0000 6000 0000 0000 1800 0000 0000 ....`...........
0000016: 4800 0000 1800 0000 305a 7a1f f63b c301 H.......0Zz..;..
```

Byte	Description	Value
0-3	Attribute type ID	00000010 (16) $STANDARD_INFORMATION
4-7	Length of attribute	00000060 (96)
8	Non-resident flag	00 (0)
9	Length of name	00 (0)
12-13	Flags	0000 (0)
14-15	Attribute ID	0000 (0)
16-19	Size of content	00000048 (72)
20-21	Offset to content	0018 (24)

NT File System

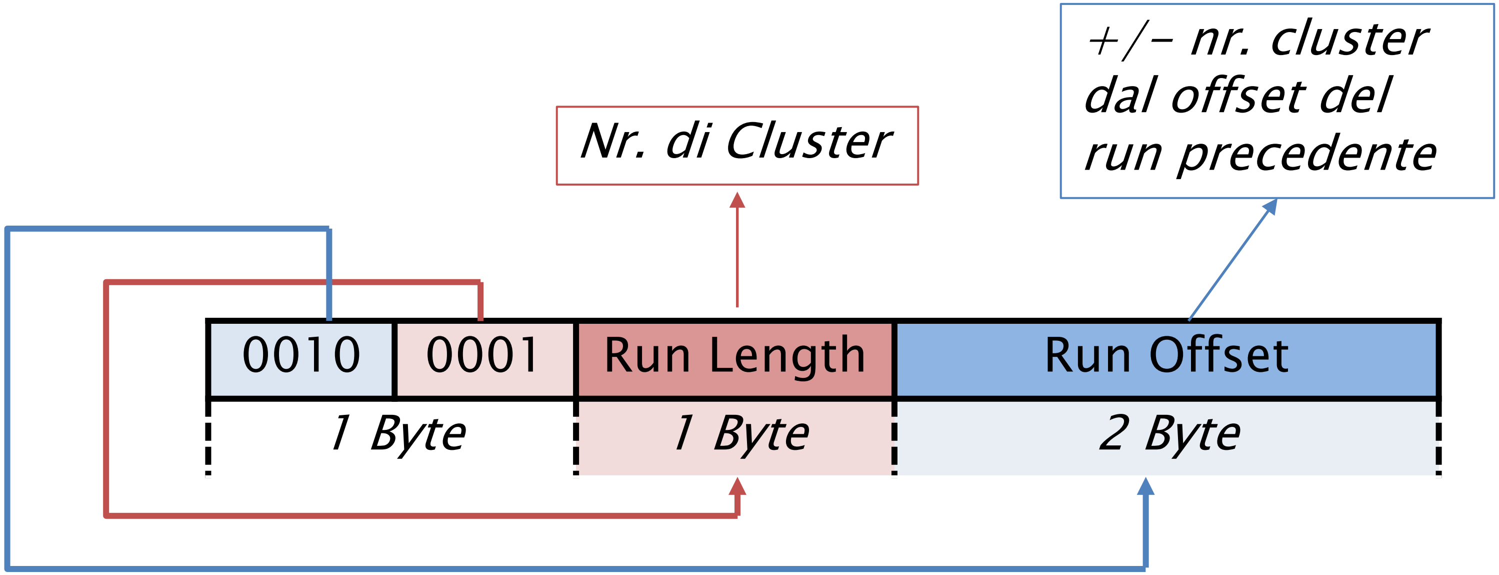
Attribute Header

Byte	Description	Es.
0-15	General Header	YES
16-23	Starting Virtual Cluster Number (VCN) of the runlist	YES
24-31	Ending VCN of the runlist	YES
32-33	Offset to the runlist	YES
34-35	Compression unit size	YES
36-39	Unused	NO
40-47	Allocated size of attribute content	NO
48-55	Actual size of attribute content	YES
56-63	Initialized size of attribute content	NO

Non-Resident
Attribute

NT File System

Run



NT File System

Non-Residente Attribute Header

- **Attributo $DATA:**

```
0000000: 8000 0000 6000 0000 0100 4000 0000 0100 ....`.....@.....
0000016: 0000 0000 0000 0000 ef20 0000 0000 0000 ......... ......
0000032: 4000 0000 0000 0000 00c0 8300 0000 0000 @...............
0000048: 00c0 8300 0000 0000 00c0 8300 0000 0000 ................
0000064: 32c0 1eb5 3a05 2170 1b1f 2290 015f 7e31 2...:.!p..".._~1
0000080: 2076 ed00 2110 8700 00b0 6e82 4844 7e82 v..!.....n.HD~.
```

Byte	Description	Value
0-3	Attribute type ID	00000080 (128) $DATA
4-7	Length of attribute	00000060 (96)
8	Non-resident flag	01 (1)
9	Length of name	00 (0)
12-13	Flags	0000 (0)
14-15	Attribute identifier	0001 (1)
16-23	Starting VCN runlist	0
24-31	Ending VCN runlist	20ef (8.431)

NT File System

Non-Residente Attribute Header

- **Attributo $DATA:**

```
0000000: 8000 0000 6000 0000 0100 4000 0000 0100 ....`.....@.....
0000016: 0000 0000 0000 0000 ef20 0000 0000 0000 ......... ......
0000032: 4000 0000 0000 0000 00c0 8300 0000 0000 @...............
0000048: 00c0 8300 0000 0000 00c0 8300 0000 0000 ................
0000064: 32c0 1eb5 3a05 2170 1b1f 2290 015f 7e31 2...:.!p..".._~1
0000080: 2076 ed00 2110 8700 00b0 6e82 4844 7e82 v..!.....n.HD~.
```

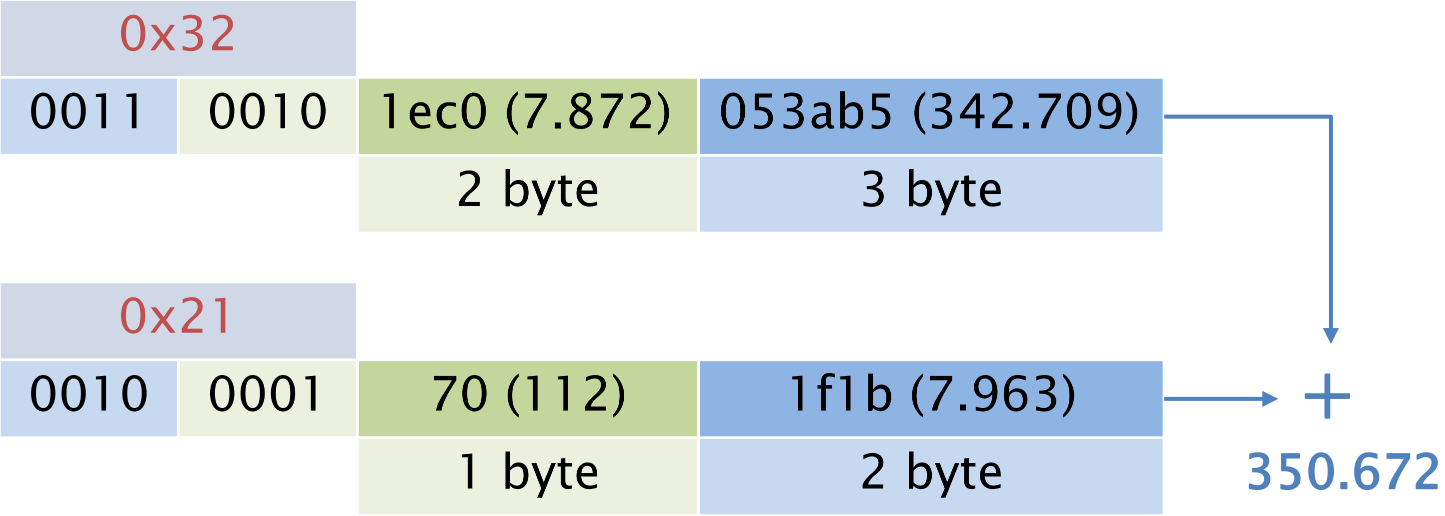
Byte	Description	Value
32-33	Offset to the runlist	0040 (64)
40-47	Allocated size of attribute content	0083c000 (8.634.368)
48-55	Actual size of attribute content	0083c000 (8.634.368)
56-63	Initialized size of attribute content	0083c000 (8.634.368)

NT File System

Non-Residente Attribute Header

- **Run List:**

```
0000000: 8000 0000 6000 0000 0100 4000 0000 0100 ....`.....@.....
0000016: 0000 0000 0000 0000 ef20 0000 0000 0000 ......... ......
0000032: 4000 0000 0000 0000 00c0 8300 0000 0000 @...............
0000048: 00c0 8300 0000 0000 00c0 8300 0000 0000 ................
0000064: 32c0 1eb5 3a05 2170 1b1f 2290 015f 7e31 2...:.!p..".._~1
0000080: 2076 ed00 2110 8700 00b0 6e82 4844 7e82 v..!.....n.HD~.
```



0x32			
0011	0010	1ec0 (7.872)	053ab5 (342.709)
		2 byte	3 byte

0x21			
0010	0001	70 (112)	1f1b (7.963)
		1 byte	2 byte

+

350.672

NT File System
File System Category

File System Metadata $MFT File

- contiene la Master File Table
  - Cluster Iniziale: Boot Sector

- Layout:
  - ≥ Windows 7: cluster 786432 (0x0C0000)

- Entry[0] di MFT
  - $DATA: cluster usati
  - $BITMAP: stato di allocazione delle entry

NT File System

File System Category

File System Metadata $MFT File

```
root@caine:/# istat -f ntfs ntfs1.dd 0

                  [...]
$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0 Security ID: 256
Created: Thu Jun 26 10:17:57 2003
File Modified: Thu Jun 26 10:17:57 2003
MFT Modified: Thu Jun 26 10:17:57 2003
Accessed: Thu Jun 26 10:17:57 2003
                  [...]
Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-3) Name: N/A Resident size: 74
Type: $DATA (128-1) Name: $Data Non-Resident size: 8634368
342709 342710 342711 342712 342713 342714 342715 342716
342717 342718 342719 342720 342721 342722 342723 342724
                  [...]
443956 443957 443958 443959 443960 443961 443962 443963

Type: $BITMAP (176-5) Name: N/A Non-Resident size: 1056
342708 414477 414478 414479
```

NT File System
File System Category

File System Metadata $MFTMirr File

- **Copia di backup della Master File Table**
  - Prime 4 entry: *$MFT, $MFTMirr, $LogFile, $Volume*
- Entry[1] di MFT
- **Layout**:
  - ≥ Windows 7: dopo il Boot Sector (16° settore)
  - < Windows 7: a metà del File System

NT File System

File System Category

File System Metadata $MFTMirr File

```
root@caine:/# istat -f ntfs ntfs1.dd 1

                    [...]
Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-2) Name: N/A Resident size: 82
Type: $DATA (128-1) Name: $Data Non-Resident size: 4096
514064 514065 514066 514067
```

NT File System

File System Category

File System Metadata $Boot File

- **Boot Sector**
  - Dimensione dei cluster
  - Nr. settori del File System
  - Layout MFT
    - Cluster iniziale
    - Dimensione entry
- Entry[7] di MFT
- **Layout**: primi 16 settori del File System
  - Signature: *0xAA55*

NT File System

$Boot File

Byte	Description	Es.
0-2	Istruzioni assembly per saltare al bootcode	NO
3-10	OEM Name (ASCII)	NO
11-12	Dimensione settore (Byte)	YES
13	Dimensione Cluster (Settori)	YES
14-15	Settori riservati	NO
16-20	Non usati	NO
21	Descrizione Media	NO
22-23	Non usati	NO
24-31	Non usati	NO
32-35	Non usati	NO
36-39	Non usati	NO
40-47	Tot. settori FS	YES
48-55	Indirizzo del cluster iniziale di MFT	YES
56-63	Indirizzo del cluster iniziale di MFT Mirror	NO

NT File System
$Boot File

Byte	Description	Es.
64	Dimensione delle entry MFT	YES
65-67	Non usati	NO
68	Dimensione dei record dell'index	YES
69-71	Non usati	NO
72-79	Serial Number	NO
80-83	Non usati	NO
84-509	Boot Code	NO
510-511	Signature (0xaa55)	NO

NT File System

File System Category

File System Metadata $Boot File

```
root@caine:/# istat -f ntfs ntfs1.dd 7

                   [...]
Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 48
Type: $FILE_NAME (48-2) Name: N/A Resident size: 76
Type: $SECURITY_DESCRIPTOR (80-3) Name: N/A Resident size: 104
Type: $DATA (128-1) Name: $Data Non-Resident size: 8192
0 1 2 3 4 5 6 7
```

NT File System

File System Category

File System Metadata $Volume File

- **Informazioni sul volume:**
  - etichetta
  - versione

- Entry[3] di MFT:
  - $VOLUME_NAME: nome in UNICode del volume
    - ID Type: 96
  - $VOLUME_INFORMATION:
    - versione di NTFS
    - dirty status
  - $DATA: 0 Byte

NT File System

$VOLUME_INFORMATION Attribute

Type ID 112

Byte	Description	Es.
0–7	Unused	NO
8	Major version	YES
9	Minor version	YES
10–11	Flags	NO

Flags	
0x0001	Dirty
0x0002	Resize $LogFile
0x0004	Upgrade volume next time
0x0008	Mounted in NT
0x0010	Deleting change journal
0x0020	Repair object IDs
0x8000	Modified by chkdsk

NT File System

File System Category

File System Metadata $Volume File

```
root@caine:/# istat -f ntfs ntfs1.dd 3

                    [...]
Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 48
Type: $FILE_NAME (48-1) Name: N/A Resident size: 80
Type: $OBJECT_ID (64-6) Name: N/A Resident size: 16
Type: $SECURITY_DESCRIPTOR (80-2) Name: N/A Resident size: 104
Type: $VOLUME_NAME (96-4) Name: N/A Resident size: 22
Type: $VOLUME_INFORMATION (112-5) Name: N/A Resident size: 12
Type: $DATA (128-3) Name: $Data Resident size: 0
```

NT File System
File System Category

File System Metadata $AttrDef File

- definisce gli attributi:
  - Nomi
  - Type ID

- Entry[4] di MFT

NT File System

$AttrDef File

Byte	Description	Es.
0-127	Name of attribute	YES
128-131	Type identifier	YES
132-135	Display rule	NO
136-139	Collation rule	NO
140-143	Flags	YES
144-151	Minimum size	NO
152-159	Maximum size	NO

Flags	
0x02	Attribute can be used in an index
0x04	Attribute is always resident
0x08	Attribute can be non-resident

NT File System

File System Category

File System Metadata $AttrDef File

```
root@caine:/# istat -f ntfs ntfs1.dd 4

                    [...]
Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 48
Type: $FILE_NAME (48-2) Name: N/A Resident size: 82
Type: $SECURITY_DESCRIPTOR (80-3) Name: N/A Resident size: 104
Type: $DATA (128-4) Name: $Data Non-Resident size: 2560
342701 342702 342703
```

NT File System

File System Category: Analisi

1) Processare il primo settore del File System: Boot Sector
   - Layout MFT
2) Processare la MFT[0]:
   - $MFTMirr
3) Processare $Volume
4) Processare $AttrDef
5) Processare le altre entry MFT

NT File System

Content Category

- Contenuto degli attributi:
  - Residenti: all’interno delle entry MFT
  - Non Residenti: cluster esterni
- Cluster:
  - Cluster[0] = settore[0] del File System
    - Settore= Cluster x Settori_Cluster

NT File System
Content Category

File System Metadata $Bitmap File

- Informazioni sullo stato di allocazione dei cluster
  - **Bit[x]=cluster[x]**
    - Bit[x]=1 cluster x è allocato
    - Bit[x]=0: cluster x non è allocato

- Entry[6] di MFT

NT File System

Content Category

File System Metadata $Bitmap File

```
root@caine:/# istat -f ntfs ntfs1.dd 6

                              [...]
Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-2) Name: N/A Resident size: 80
Type: $DATA (128-1) Name: $Data Non-Resident size: 128520
514113 514114 514115 514116 514117 514118 514119 514120
514121 514122 514123 514124 514125 514126 514127 514128
                              [...]
```

NT File System
Content Category

File System Metadata $BadClus File

- **traccia i cluster con settori danneggiati**
- Entry[8] di MFT
  - $DATA= «$Bad»
    - Flag = Sparse
    - Size = File System

NT File System

Content Category

File System Metadata $BadClus File

```
root@caine:/# istat -f ntfs ntfs1.dd 8

                             [...]

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-3) Name: N/A Resident size: 82
Type: $DATA (128-2) Name: $Data Resident size: 0
Type: $DATA (128-1) Name: $Bad Non-Resident size: 1052803072
```

NT File System
Content Category: Layout

- **Diverso a seconda della versione NTFS**

- **Zona MFT**
  - Settori consecutivi riservati per MTF:
    - 12,5% del File System

- **Boot Sector**: primo settore
  - File System Metadata File dopo il Boot Sector

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