COMPUTER FORENSICS

Lezione 20: L'Analisi *i File System*

(4ª parte)

A.A. 2021/22

Dott. Lorenzo LAURATO

File System

- NT File System

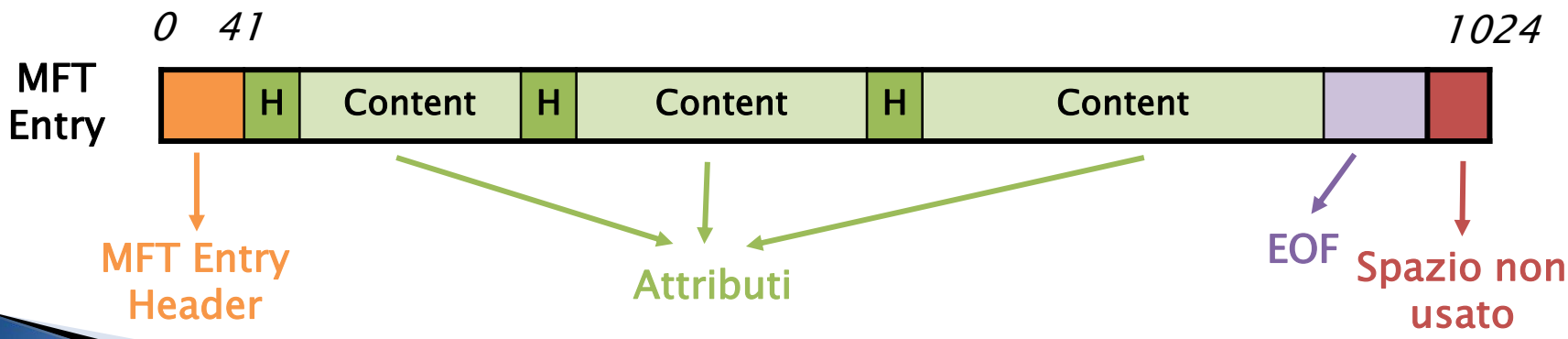
Nella lezione precedente…

- NTFS gestisce tutto con i file
- Master File Table (MFT):
  - prime 12 entry:

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

Nella lezione precedente…

- **Entry MFT:**
  - Header MFT: 42byte
  - Attributi:
    - *Header*
    - *Content:*
      - *Residente*
      - *Non residente: Cluster Run*

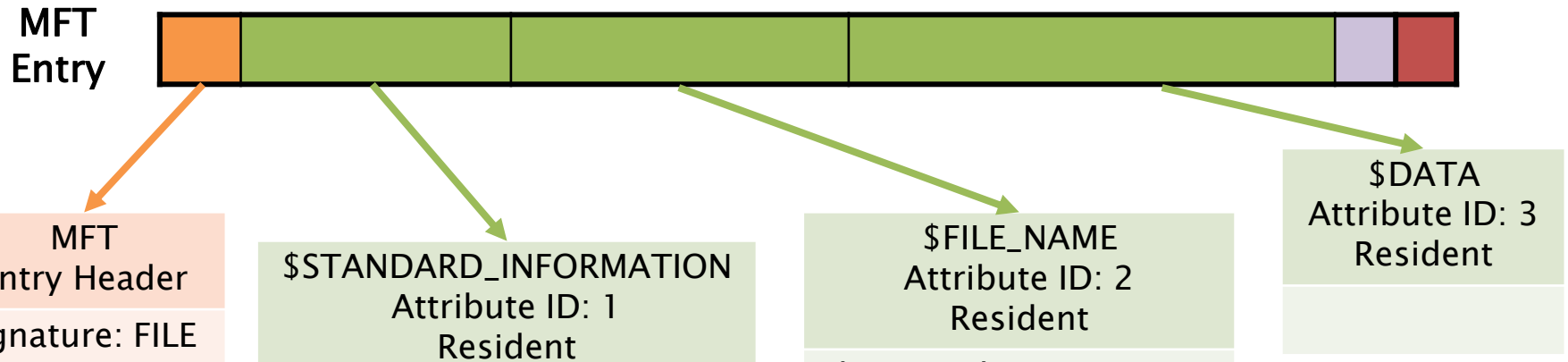


Nella lezione precedente…

- File System Category:
  - File System Metadata File:
    - $MFTMirr
    - $BootFile:
    - $Volume
    - $AttrDef
- Content Category
  - Attributo $Data
  - FS Metadata File:
    - $BitMap
    - $BadClus

NT File System
Metadata Category

- Reperibili dagli attributi:



NT File System
Metadata Category

$STANDARD_INFORMATION Attribute

- Esiste per ogni file e directory
- Contiene i metadati principali:
  - Informazioni temporali
  - Proprietà
  - Sicurezza e quota
- Type ID: 16

NT File System

$STANDARD_INFORMATION Attribute

Byte	Description	Es.
0–7	Creation time	NO
8–15	File altered time	NO
16–23	MFT altered time	NO
24–31	File accessed time	NO
32–35	Flags	NO
36–39	Maximum number of versions	NO
40–43	Version number	NO
44–47	Class ID	NO
48–51	Owner ID	NO
52–55	Security ID	NO
56–63	Quota Charged	NO
64–71	Update Sequence Number (USN)	NO

NT File System
Metadata Category

$STANDARD_INFORMATION Attribute

- Quattro valori temporali (timestamp):
  - **Data di creazione**: creazione del file
  - **Data di ultima modifica**: modifica del contenuto degli attributi $DATA e $INDEX
  - **Data di ultima modica MFT**: modifica dei metadati del file
  - **Data di ultimo accesso**: accesso al contenuto del file

NT File System

$STANDARD_INFORMATION Attribute

Byte	Description	Es.
0–7	Creation time	NO
8–15	File altered time	NO
16–23	MFT altered time	NO
24–31	File accessed time	NO
32–35	Flags	NO
36–39	Maximum number of versions	NO
40–43	Version number	NO
44–47	Class ID	NO
48–51	Owner ID	NO
52–55	Security ID	NO
56–63	Quota Charged	NO
64–71	Update Sequence Number (USN)	NO

Flags	
0x0001	Read Only
0x0002	Hidden
0x0004	System
0x0020	Archive
0x0040	Device
0x0080	#Normal
0x0100	Temporary
0x0200	Sparse file
0x0400	Reparse point
0x0800	Compressed
0x1000	Offline
0x2000	Content is not being indexed for faster searches
0x4000	Encrypted

NT File System
Metadata Category

$FILE_NAME Attribute

- Ogni file e directory ha almeno un attributo $FILE_NAME
- Dimensione: 66byte + lunghezza nome
- Type ID: 48
- Riferimento al Parent Directory

NT File System
$FILE_NAME Attribute

Namespace	
0	**POSIX**: The name is case sensitive and allows all Unicode characters except for '/' and NULL.
1	**Win32**: The name is case insensitive and allows most Unicode characters except for special values such as '/', '\', ':', '>', '<', and '?'.
2	**DOS**: The name is case insensitive, upper case, and no special characters. The name must have eight or fewer characters in the name and three or less in the extension
3	**Win32 & DOS**: Used when the original name already fits in the DOS namespace and two names are not needed.

NT File System

$FILE_NAME Attribute

Byte	Description	Es.
0–7	File reference of parent directory	NO
8–15	File creation time	NO
16–23	File modification time	NO
24–31	MFT modification time	NO
32–39	File accessed time	NO
40–47	Allocated size of file	NO
48–55	Real size of file	NO
56–59	Flags	NO
60–63	Reparse value	NO
64	Length of name	NO
65	Namespace	NO
66+	Name	NO

Flags	
0x0001	Read Only
0x0002	Hidden
0x0004	System
0x0020	Archive
0x0040	Device
0x0080	#Normal
0x0100	Temporary
0x0200	Sparse file
0x0400	Reparse point
0x0800	Compressed
0x1000	Offline
0x2000	Content is not being indexed for faster searches
0x4000	Encrypted

NT File System
Metadata Category

$DATA Attribute

- Impiegato per memorizzare qualsiasi forma di dati:
  - Non ha formato e valori definiti
- Dimensione: $\geq$ 0 Byte
  - >700Byte: non residente
- Type ID: 128
- Alternative Data Stream (ADS): attributi $DATA aggiuntivi
  - Es.: C:\> echo «Ciao a tutti»>file.txt:pippo

NT File System
Metadata Category

$ATTRIBUTE_LIST Attribute

- Lista degli attributi nella entry:
  - Quando un file/directory necessita di più entry per gli attributi
  - Tipo di attributo->Posizione della entry che lo contiene

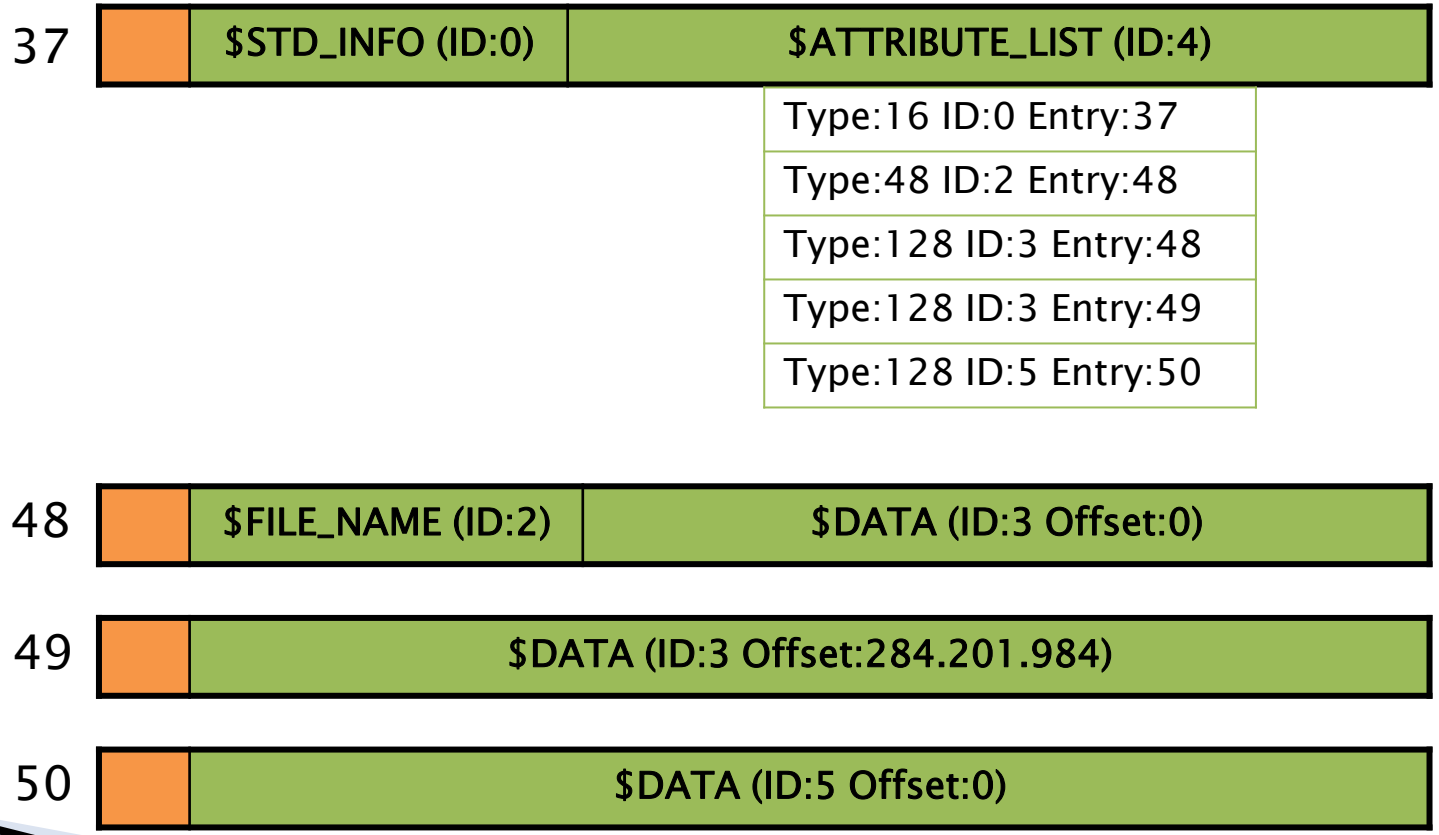
- Type ID: 32

NT File System
$ATTRIBUTE_LIST Attribute

Byte	Description	Es.
0–3	Attribute type	YES
4–5	Length of this entry	YES
6	Length of name	YES
7	Offset to name (relative to start of this entry)	YES
8–15	Starting VCN in attribute	YES
16–23	File reference where attribute is located	YES
24	Attribute ID	YES

NT File System
Metadata Category

$ATTRIBUTE_LIST Attribute



NT File System
Metadata Category

$SECURITY_DESCRIPTOR Attribute

- descrive i criteri di controllo dell'accesso che devono essere applicati a un file o una directory

- Type ID: 80

Solo versioni NTFS < 3.0

NT File System
Metadata Category

File System Metadata $Secure File

- descrive i criteri di controllo dell'accesso che devono essere applicati a un file o una directory

- Entry[9] di MFT
  - Indice $SDH
  - Indice $SII
  - attributo $DATA ($SDS).

- Ogni File\Directory
  - $STANDARD_INFORMATION:
    - Security ID: Indice nel $Secure File

Solo versioni NTFS $\geq$ 3.0

NT File System
Metadata Category

Algoritmi di allocazione

- Allocazione delle Entry MFT:
  - Strategia del primo disponibile: dalla entry 24
  - Allocato->Non allocato: cambio della flag «in uso»
  - Non Allocato->Allocato: pulizia della entry

- Allocazione degli attributi:
  - riduzione dell'ultimo attributo ($DATA)
  - Crescita dell'attributo: residente->non residente

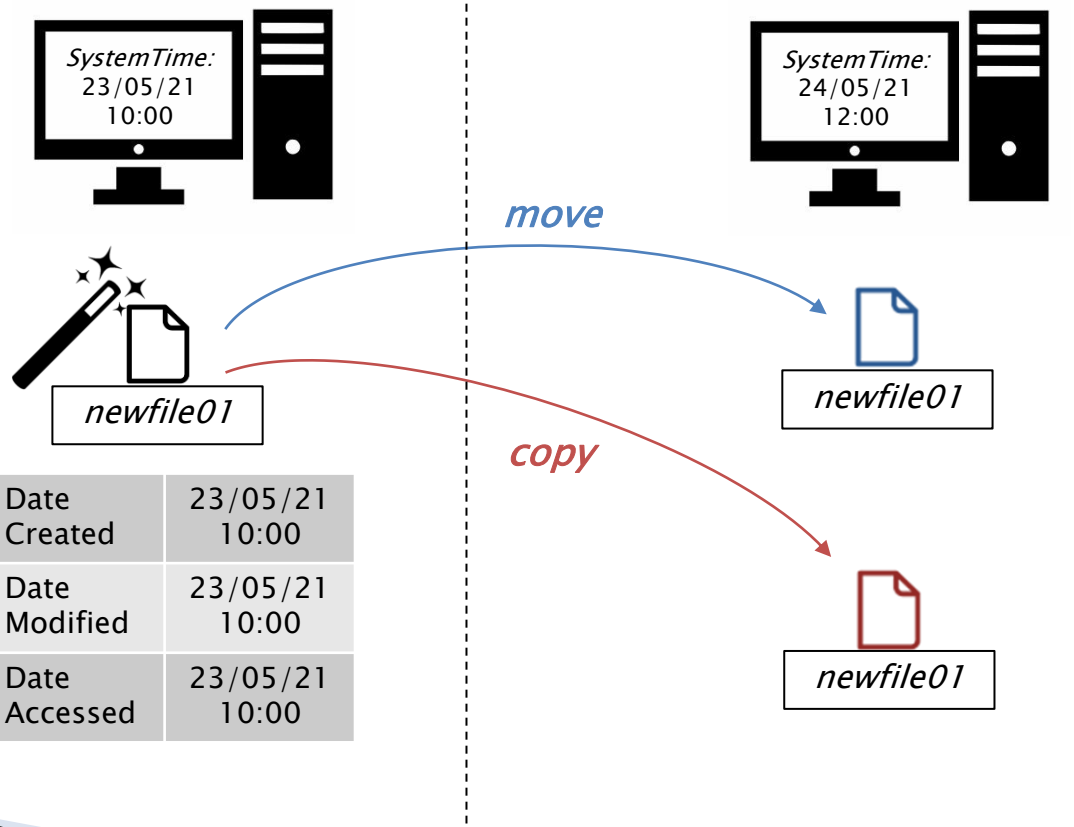
NT File System
Metadata Category

Aggiornamento informazioni temporali

- **$FILE_NAME:**
  - Aggiornamento creazione/spostamento file
- **$STANDARD_INFORMATION**:
  - Data di creazione: creazione nuovo file o copia
  - Data di ultima modifica: variazione degli attributi DATA, $INDEX_ROOT o $ INDEX_ALLOCATION
  - Data di ultima modifica MFT: modifica degli attributi
  - Data di accesso: viene fatto accesso alla entry (metadati o contenuto)

NT File System
Metadata Category

Aggiornamento informazioni temporali



Date Created	23/05/21 10:00
Date Modified	23/05/21 10:00
Date Accessed	23/05/21 10:00

Date Created	23/05/21 10:00
Date Modified	23/05/21 10:00
Date Accessed	24/05/21 12:00

Date Created	24/05/21 12:00
Date Modified	23/05/21 10:00
Date Accessed	24/05/21 12:00

NT File System
Metadata Category: Analisi

1) Individuazione di una entry MFT:
   - individuare la MFT tramite il boot sector

2) elaborazione del contenuto della entry:
   - Elaborazione degli attributi:
     - STANDARD_INFORMATION
     - $DATA:
       - NON RESIDENTE: Processare la RUNLIST
     - $FILE_NAME
   - Elaborazione delle possibili entry secondarie:
     - $ATTRIBUTE_LIST

NT File System
File Name Category

- Correlazione dei nomi: indici
  - Raccolta di strutture dati ordinate per chiave

- Struttura B-Tree:
  - Nodi:
    - $INDEX_ROOT: radice dell'albero
    - $INDEX_ALLOCATION: indici utilizzati

NT File System

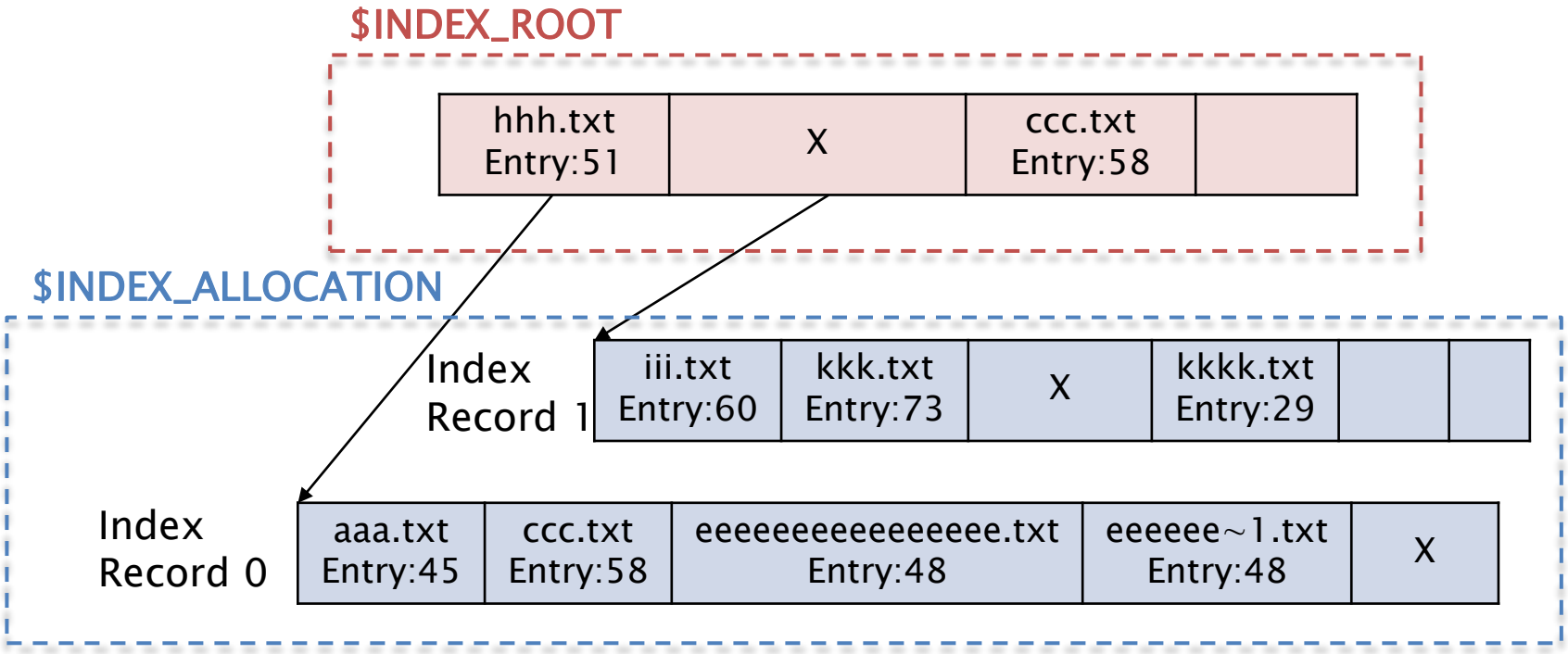
Directory Index Entry Data Structure

Byte	Description	Es.
0-7	MFT file reference for file name	YES
8-9	Length of this entry	YES
10-11	Length of $FILE_NAME attribute	NO
12-15	Flags	YES
16+	$FILE_NAME Attribute	YES
Last 8	VCN of child node in $INDEX_ALLOCATION	YES

NT File System

File Name Category

Directory Indexes



NT File System
File Name Category

Root directory

- ENTRY[5] di MFT
  - Nome: « . »

- risiedono tutti i «File System Metadata File»

NT File System
Application Category

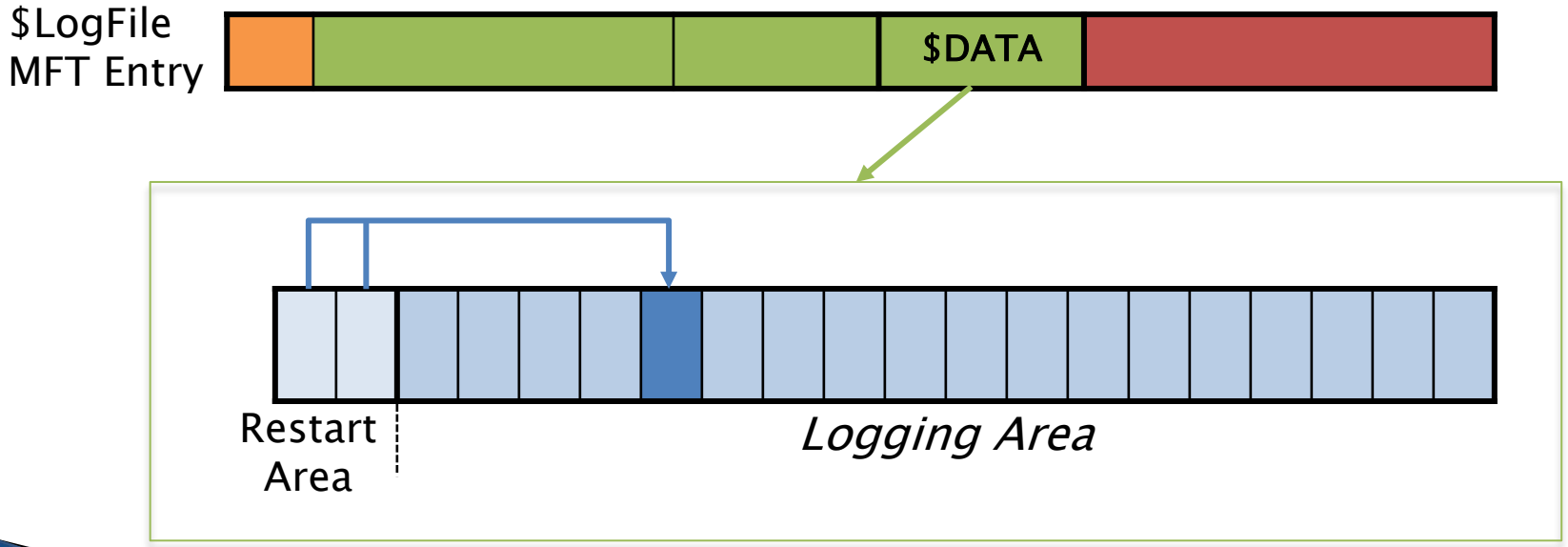
Disk Quotas ($Quota)

- Supporto alle quote di spazio su disco:
  - Limitare lo spazio allocata ad un utente
- Dati nel File System:
  - NTFS vers. $<$ 3.0: Entry[9] di MFT
    - \$Quota
  - NTFS vers. $\geq$ 3.0: qualsiasi posizione di MFT
    - \$Extend directory
- Registro di Windows

NT File System
Application Category

Logging/Journaling ($LogFile)

- Consente di mantenere il File System in uno stato di consistenza
- Entry[2] di MFT

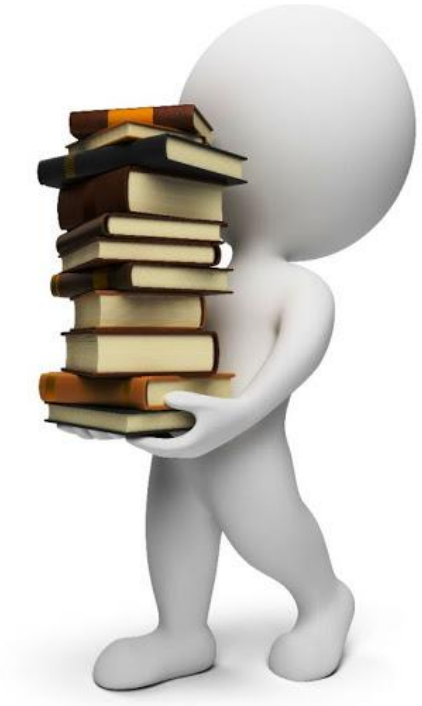


NT File System
Analisi: *File Recovery*

- Eliminazione file:
  - File name eliminato dall'index directory
  - Recupero entry MFT: attributo $FILE_NAME (Parent Directory)
  - Controllare la presenza di ulteriori $DATA (ADS)

Bibliografia

- **File System Forensics Analysis**
  Brian Carrier – (2005)
  Addison Wesley Professional



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