# COMPUTER FORENSICS

# Lezione 16: L'Analisi
# *i Volumi*

SSRI
SICUREZZA SISTEMI
RETI INFORMATICHE

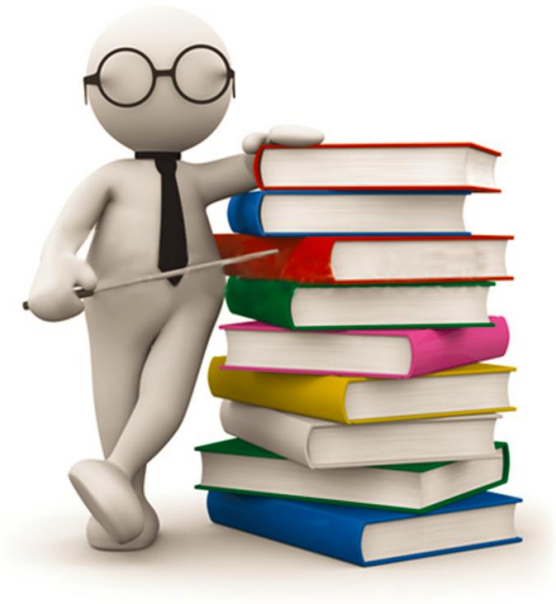
UNIVERSITA' DEGLI STUDI DI NAPOLI FEDERICO II

A.A. 2021/22

**Dott. Lorenzo LAURATO**

# L'analisi

- Il primo strumento di analisi è il proprio bagaglio di conoscenze informatiche.



# I volumi

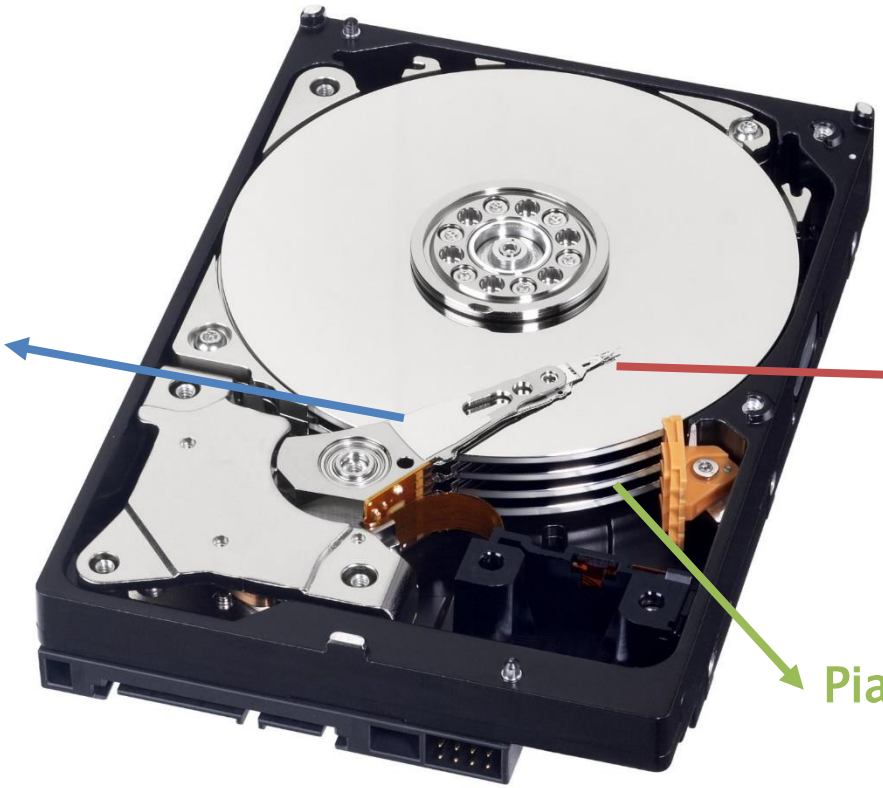
» Overview

SSRI
Sicurezza Sistemi Reti Informatiche

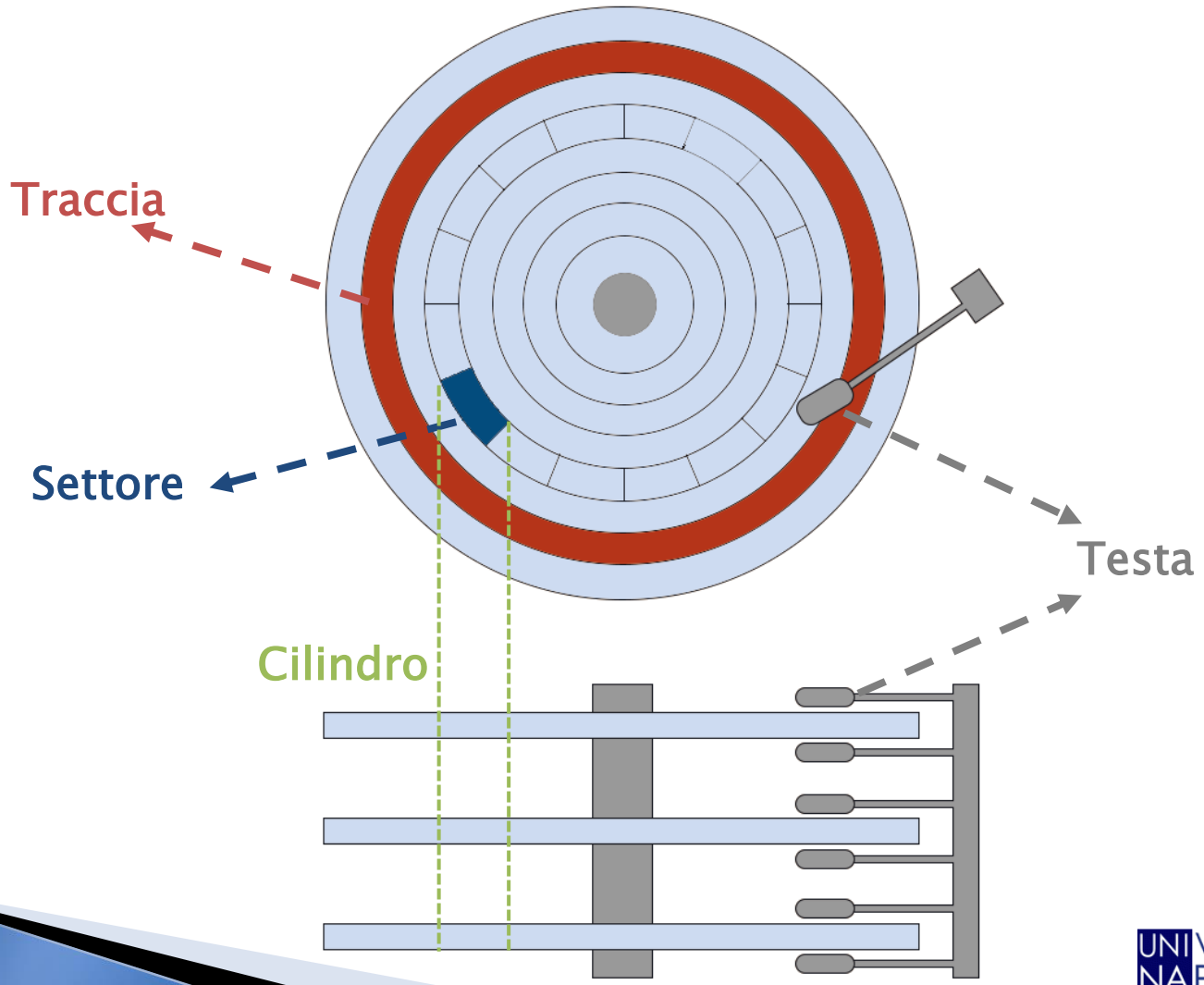
UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

a.a. 2021/22

# L'analisi: il disco



# L'analisi: il disco

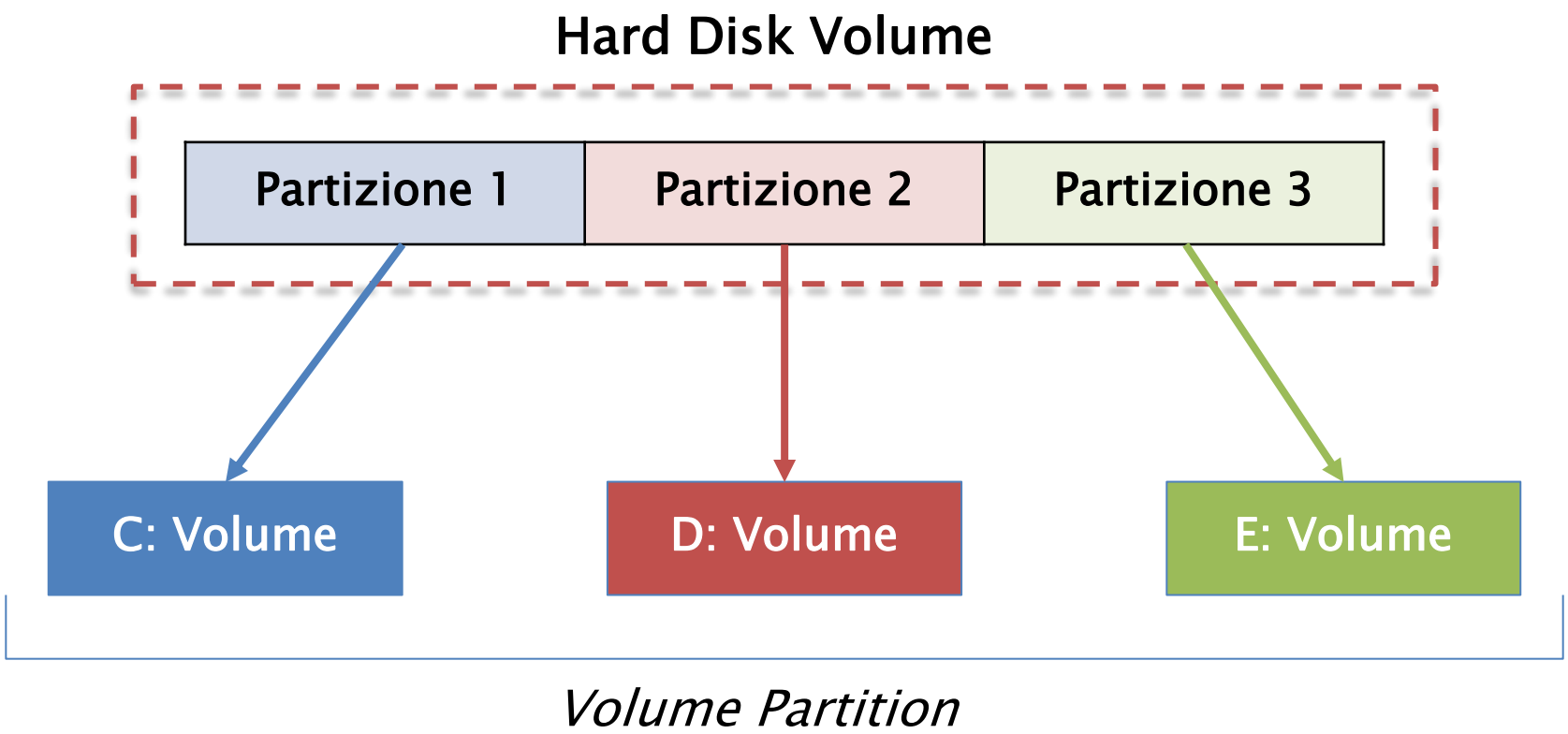


# L'analisi: i volumi

- **Volume System:** si preoccupa di gestire i volumi per raggiungere due obbiettivi
  - Unione di più volumi in unico grande volume
  - Suddivisione del volume in partizioni

- **Volume**: insieme di settori per memorizzare dati;
- **Partizione:** insieme di settori consecutivi in un volume;

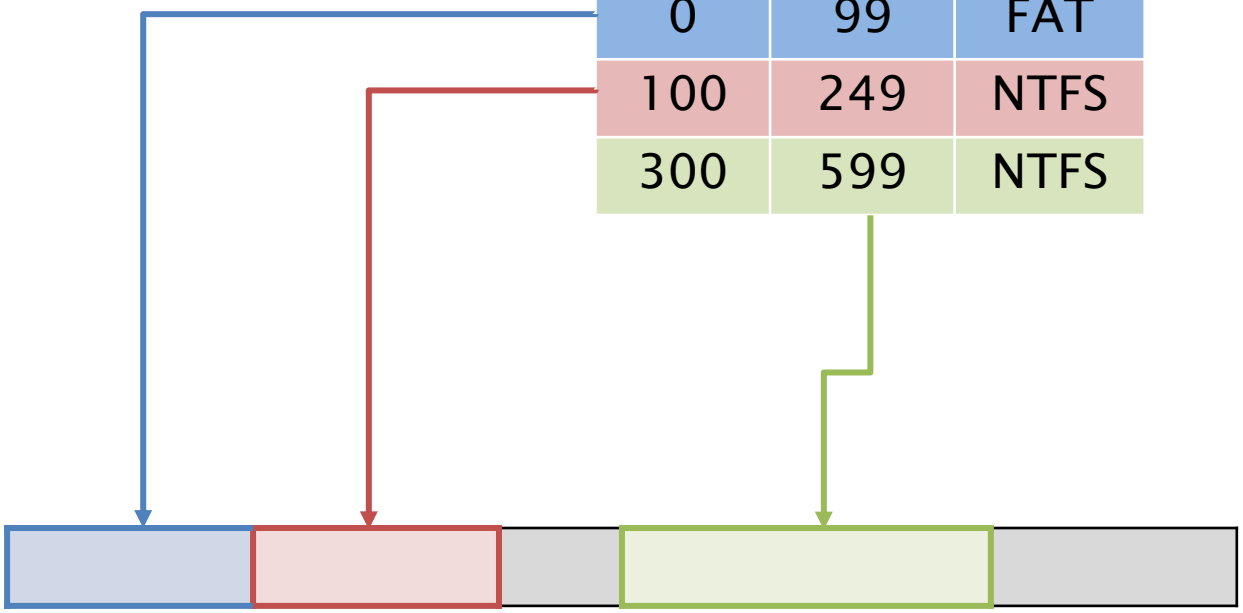
# L'analisi: i volumi



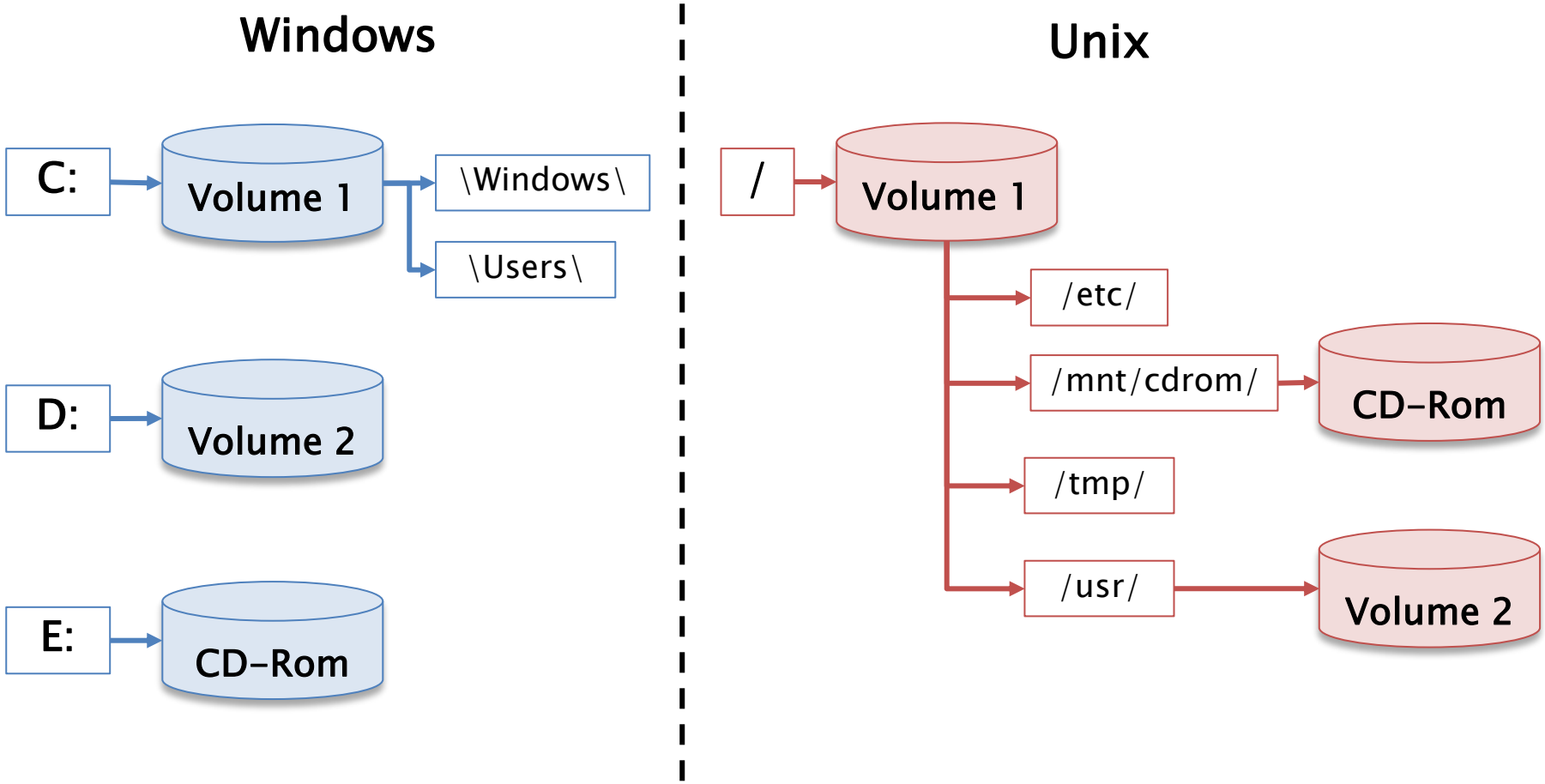
# L'analisi: i volumi

**Partition Table**

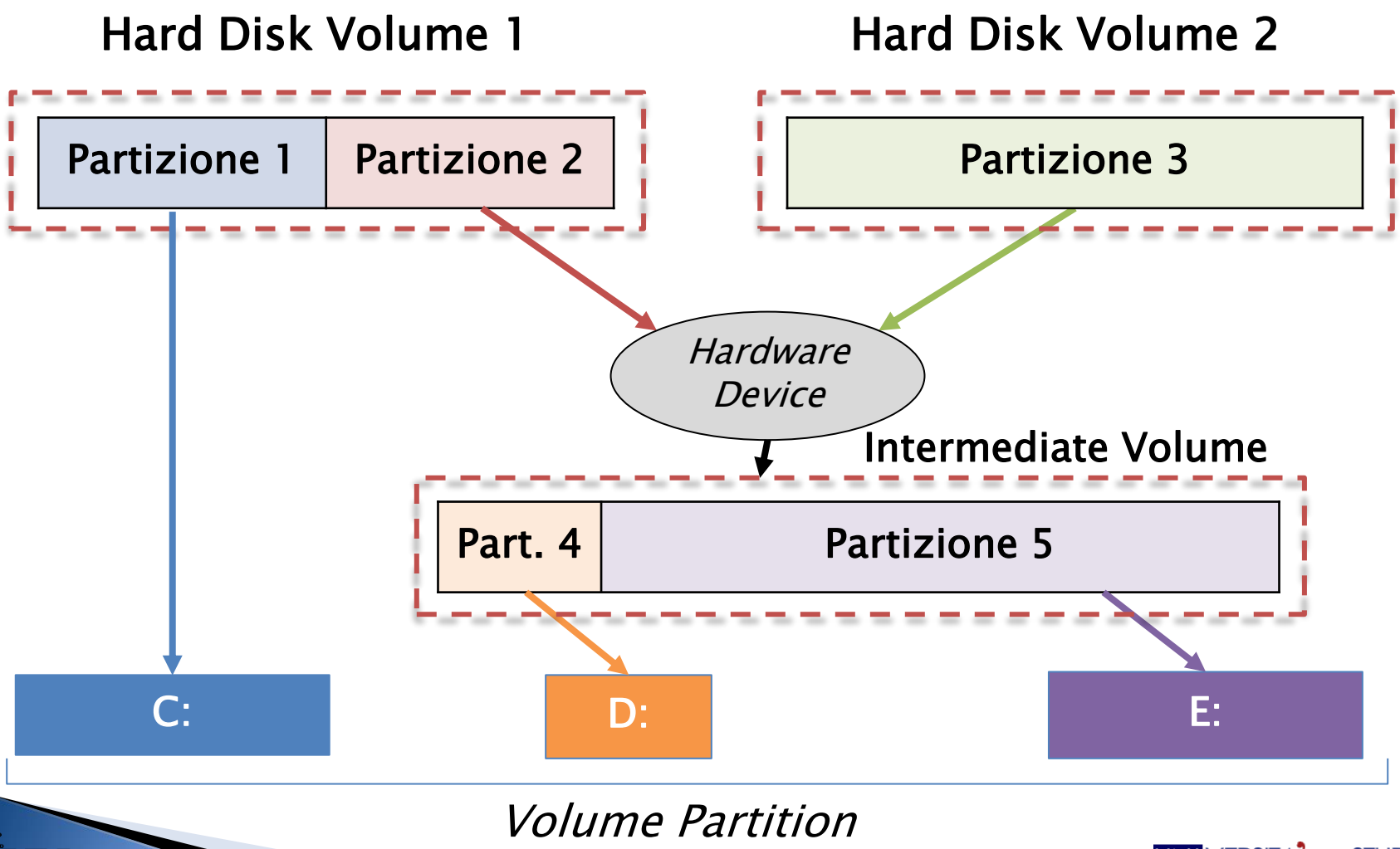
| Start | End | Type |
|---|---|---|
| 0 | 99 | FAT |
| 100 | 249 | NTFS |
| 300 | 599 | NTFS |



# L'analisi: i volumi



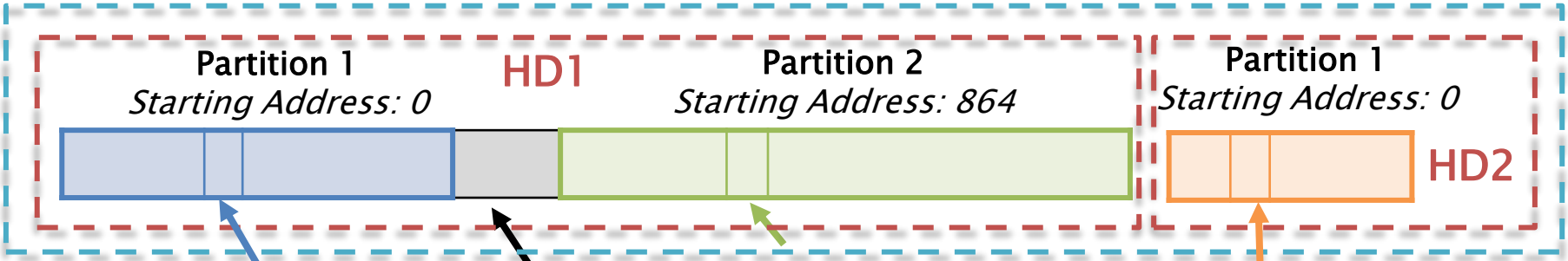
# L'analisi: i volumi



# L'analisi: i volumi

## Indirizzamento dei settori

- **Phisical Address (LBA):** l'indirizzo del settore è calcolato in base al primo settore del disco
- **Logical Disk Volume Address:** l'indirizzo del settore è calcolato in base al primo settore del volume
- **Logical Volume Partition Address:** l'indirizzo del settore è calcolato in base al primo settore della partizione



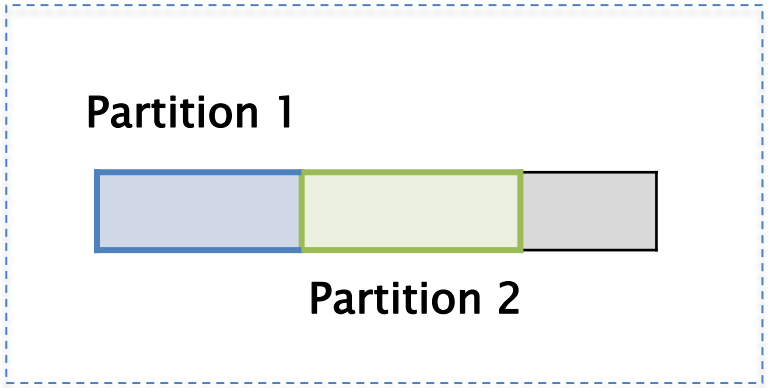

Phisical Address: 100
Logical Disk Volume Address: 100
Logical Volume Partition Address: 100

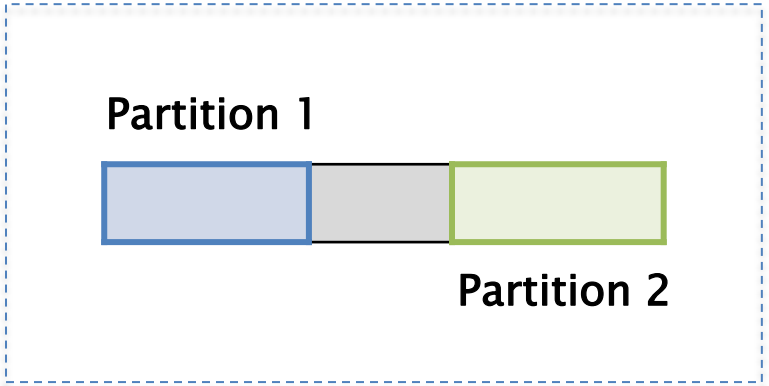
Phisical Address: 964
Logical Disk Volume Address: 964
Logical Volume Partition Address: 100

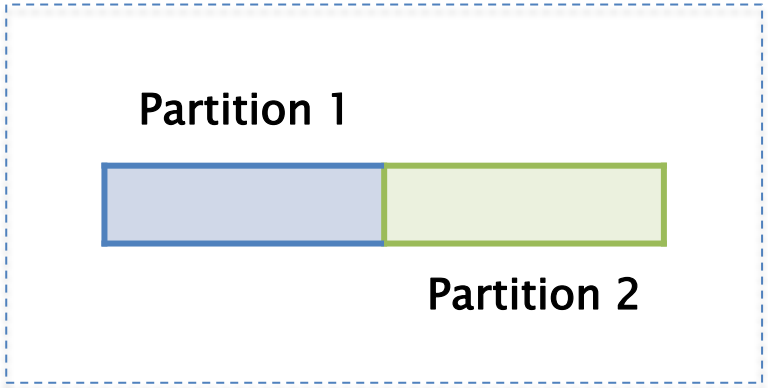
Phisical Address: 569
Logical Disk Volume Address: 569
Logical Volume Partition Address: N.D.

Phisical Address: 30
Logical Disk Volume Address: 1830
Logical Volume Partition Address: 30

# L'analisi: i volumi



# L'Analisi

- I Volumi

SSRI
Sicurezza Sistemi Reti Informatiche

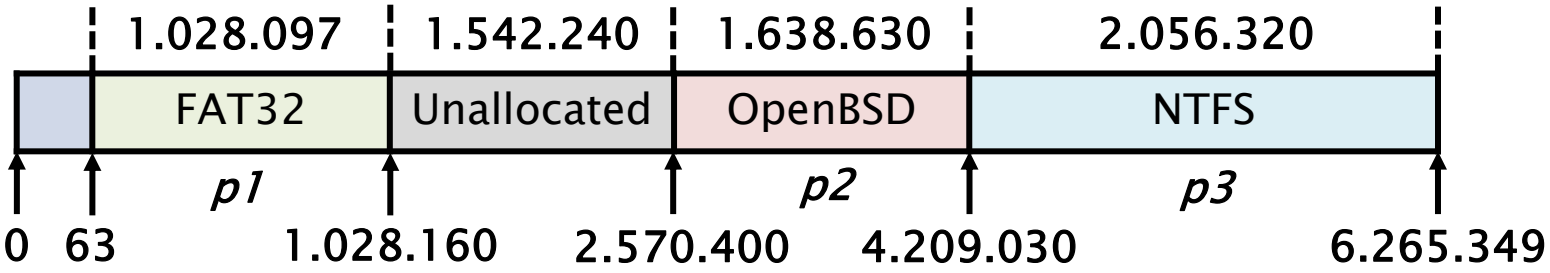
UNIVERSITA' DEGLI STUDI DI NAPOLI FEDERICO II

a.a. 2021/22

# L'analisi: i volumi

- La lista delle partizioni in un file immagine

```
root@caine:/# mmls -t dos disk1.dd
Units are in 512-byte sectors
    Slot  Start      End         Length    Description
00:  ----- 0000000000 0000000000 0000000001 Table #0
01:  ----- 0000000001 0000000062 0000000062 Unallocated
02:  00:00 0000000063 0001028159 0001028097 Win95 FAT32 (0x0B)
03:  ----- 0001028160 0002570399 0001542240 Unallocated
04:  00:03 0002570400 0004209029 0001638630 OpenBSD (0xA6)
05:  00:01 0004209030 0006265349 0002056320 NTFS (0x07)
```



# L'analisi: i volumi

- Estrazione delle partizioni in un file immagine

```
root@caine:/# mmls -t dos disk1.dd

Units are in 512-byte sectors
    Slot  Start      End        Length     Description
00:  ----- 0000000000 0000000000 0000000001 Table #0
01:  ----- 0000000001 0000000062 0000000062 Unallocated
02:  00:00 0000000063 0001028159 0001028097 Win95 FAT32 (0x0B)
03:  ----- 0001028160 0002570399 0001542240 Unallocated
04:  00:03 0002570400 0004209029 0001638630 OpenBSD (0xA6)
05:  00:01 0004209030 0006265349 0002056320 NTFS (0x07)


root@caine:/# dd if=disk1.dd of=disk1_p1.dd bs=512 skip=63 count=1028097   p1

root@caine:/# dd if=disk1.dd of=disk1_p2.dd bs=512 skip=2570400 count=1638630   p2

root@caine:/# dd if=disk1.dd of=disk1_p3.dd bs=512 skip=4209030 count=2056320   p3
```

# L'analisi: i volumi

- Recupero delle partizioni in un file immagine

```
root@caine:/# gpart -v disk2.dd
* Warning: strange partition table magic 0x0000.
                    [. . .]
Begin scan...
Possible partition(DOS FAT), size(800mb), offset(0mb)
    type: 006(0x06)(Primary 'big' DOS (> 32MB))
    size: 800mb #s(1638566) s(63-1638628)
    chs: (0/1/1)-(101/254/62)d (0/1/1)-(101/254/62)r
    hex: 00 01 01 00 06 FE 3E 65 3F 00 00 00 A6 00 19 00
Possible partition(DOS FAT), size(917mb), offset(800mb)
    type: 006(0x06)(Primary 'big' DOS (> 32MB))
    size: 917mb #s(1879604) s(1638630-3518233)
    chs: (102/0/1)-(218/254/62)d (102/0/1)-(218/254/62)r
    hex: 00 00 01 66 06 FE 3E DA E6 00 19 00 34 AE 1C 00
```

# L'analisi: i volumi

- Recupero delle partizioni in un file immagine

```
Possible partition(Linux ext2), size(502mb), offset(1874mb)
    type: 131(0x83)(Linux ext2 filesystem)
    size: 502mb #s(1028160) s(3839535-4867694)
    chs: (239/0/1)-(302/254/63)d (239/0/1)-(302/254/63)r
    hex: 00 00 01 EF 83 FE 7F 2E 2F 96 3A 00 40 B0 0F 00
```

# I Volumi

- DOS Partition

SSRI
Sicurezza Sistemi Reti Informatiche

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

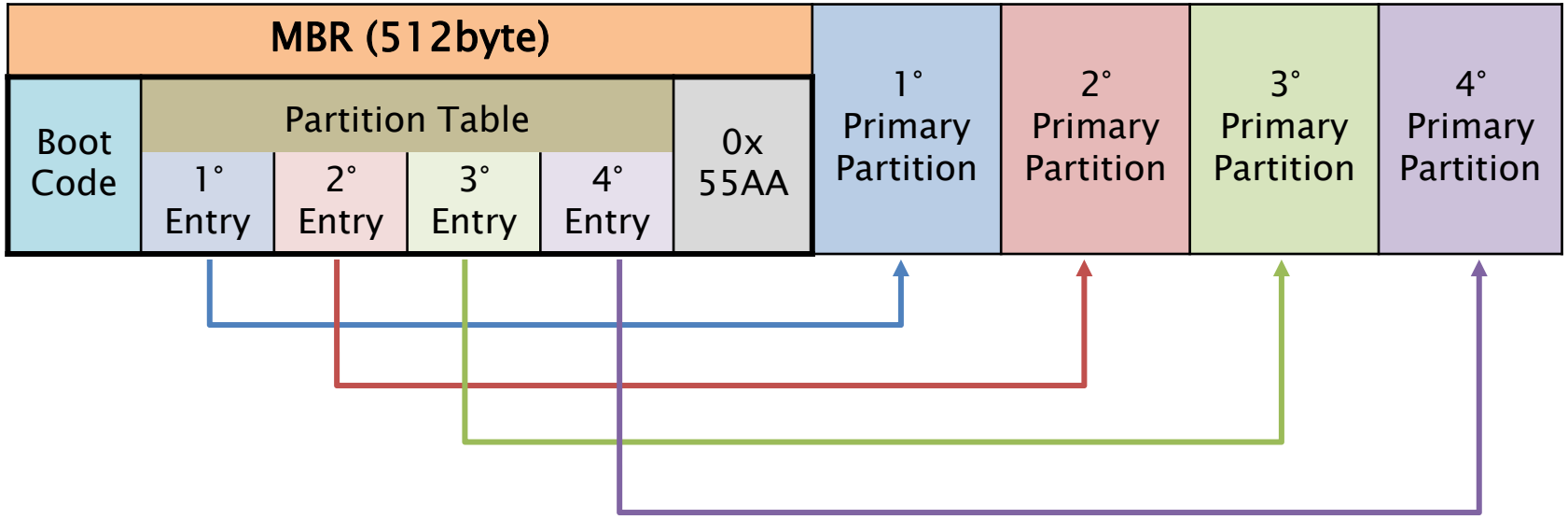
a.a. 2021/22

# I volumi: DOS Partition

- Sistema di partizione più comune

- MBR (Master Boot Record): primo settore *(512byte)*
  - Boot Code
  - Partition Table: *max 4 entry*
    - Starting CHS address
    - Ending CHS address
    - Starting LBA address
    - Number of sectors in partition
    - Type of partition
    - Flags
  - Signature: *0x55AA*

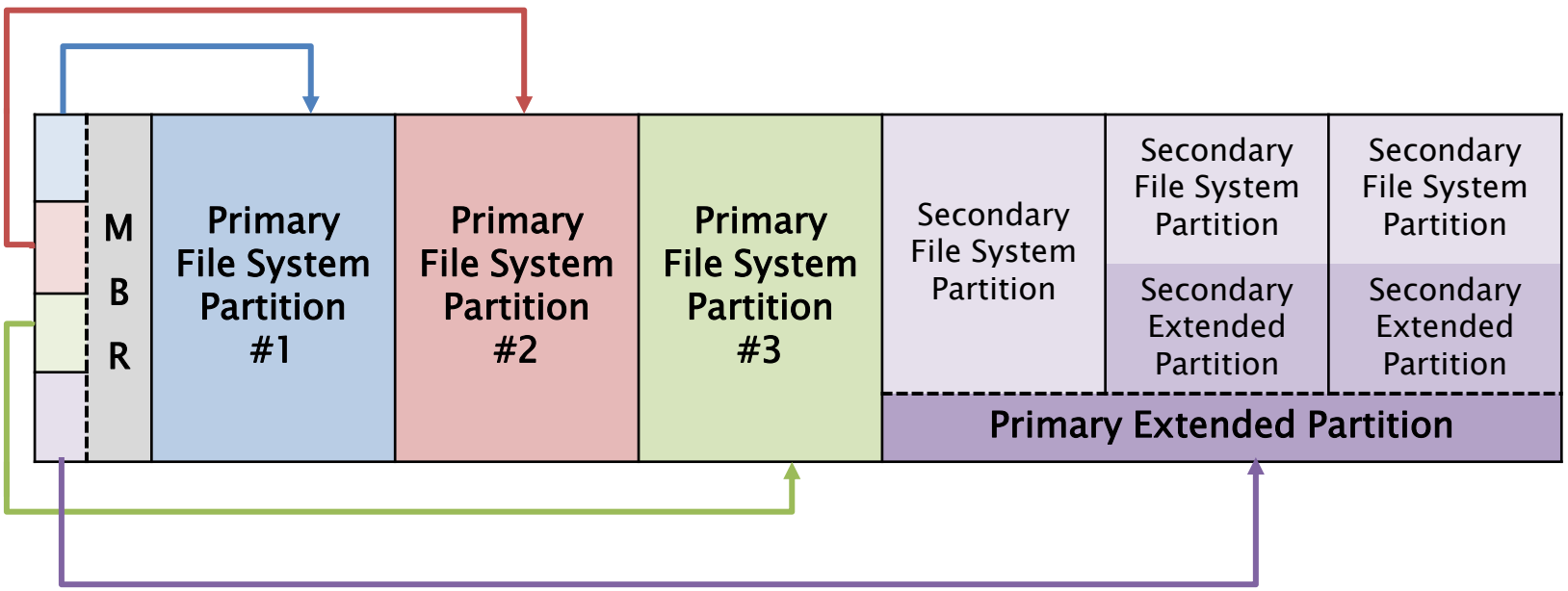
# I volumi: DOS Partition



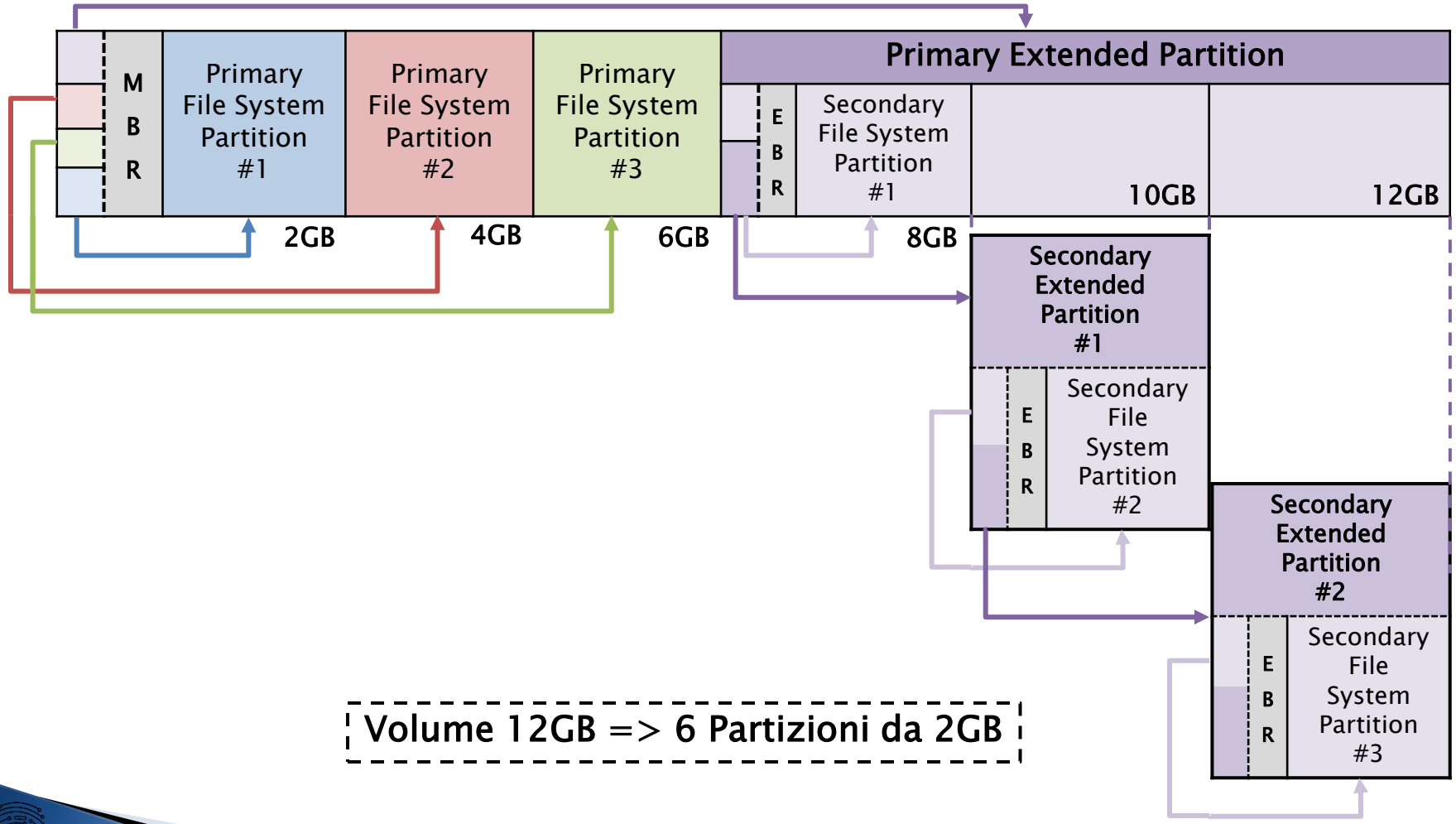
# I volumi: DOS Partition

- **Primary File System Partition**: partizione primaria che contiene un file system
- **Primary Extended Partition:** partizione primaria che contiene altre partizioni
  - **Tabella di partizione**
  - **Secondary File System Partition**: partizione secondaria che contiene un file system *(partizione logica)*
  - **Secondary Extended Partition:**
    - **Tabella di partizione**
    - **Secondary File System Partition**
    - Secondary Extended Partition:
      - …

# I volumi: DOS Partition



# I volumi: DOS Partition




Volume 12GB => 6 Partizioni da 2GB

# I volumi: DOS Partition

- Il Boot Code è situato nei primi 446byte del primo settore (MBR)
  - Microsoft Boot Code: processa la tabella di partizione e ricerca ed identifica quella c.d. «bootable», tramite il Flag.
  - possibile incapsulamento di virus

- Il settore MBR viene allocato all'inizio del «Disk Volume» e di ogni «Extended Partition»
  - EBR (Extended Boot Record) *(512byte)*
    - *La parte riservata al «Boot Code» è inutilizzata*
    - *La parte riservata alle altre due entry nella «Partition Table» è vuota.*

# I volumi: DOS Partition

## *Partition Table*

| Byte Range | Description | Essential |
|---|---|---|
| 0-445 | Boot Code | No |
| 446-461 | Partition Table Entry #1 | Yes |
| 462-477 | Partition Table Entry #2 | Yes |
| 478-493 | Partition Table Entry #3 | Yes |
| 494-509 | Partition Table Entry #4 | Yes |
| 510-511 | Signature value (0xAA55) | No |

| Byte Range | Description | Essential |
|---|---|---|
| 0-0 | Bootable Flag | No |
| 1-3 | Starting CHS Address | Yes |
| 4-4 | Partition Type | No |
| 5-7 | Ending CHS Address | Yes |
| 8-11 | Starting LBA Address | Yes |
| 12-15 | Size in Sectors | Yes |

# I volumi: DOS Partition

## *Partition Table: Type*

| Type | Description |
|---|---|
| 0x00 | Empty |
| 0x01 | FAT12, CHS |
| 0x04 | FAT16, 16-32 MB, CHS |
| 0x05 | Microsoft Extended, CHS |
| 0x06 | FAT16, 32 MB-2GB, CHS |
| 0x07 | NTFS |
| 0x0b | FAT32, CHS |
| 0x0c | FAT32, LBA |
| 0x0e | FAT16, 32 MB-2GB, LBA |
| 0x0f | Microsoft Extended, LBA |

| Type | Description |
|---|---|
| 0x11 | Hidden FAT12, CHS |
| 0x14 | Hidden FAT16, 16-32 MB, CHS |
| 0x16 | Hidden FAT16, 32 MB-2GB, CHS |
| 0x1b | Hidden FAT32, CHS |
| 0x1c | Hidden FAT32, LBA |
| 0x1e | Hidden FAT16, 32 MB-2GB, LBA |
| 0x42 | Microsoft MBR. Dynamic Disk |
| 0x82 | Solaris x86 Linux Swap |
| 0x83 | Linux |
| 0x84 | Hibernation |
| 0x85 | Linux Extended |
| 0x86/7 | NTFS Volume Set |

| Type | Description |
|---|---|
| 0xa0/1 | Hibernation |
| 0xa5 | FreeBSD |
| 0xa6 | OpenBSD |
| 0xa8 | Mac OSX |
| 0xa9 | NetBSD |
| 0xab | Mac OSX Boot |
| 0xb7 | BSDI |
| 0xb8 | BSDI swap |
| 0xee | EFI GPT Disk |
| 0xef | EFI System Partition |
| 0xfb | Vmware File System |
| 0xfc | Vmware swap |

# I Volumi

- DOS Partition

SSRI
Sicurezza Sistemi Reti Informatiche

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

a.a. 2021/22

# I volumi: DOS Partition

## *Partition Table: analisi*

- File Immagine:
  - Nr. 8 partizioni
  - Dual Boot
  - Architettura Little-Endian

- Strumenti:
  - DD
  - Editor Esadecimale (XDD)

# I volumi: DOS Partition

## *Partition Table: analisi*

- Estrazione ed analisi del primo settore: MBR

```
root@caine:/# dd if=disk3.dd bs=512 skip=0 count=1 | xxd
0000000: eb48 9010 8ed0 bc00 b0b8 0000 8ed8 8ec0 .H..............
                          [.  .  .]
0000384: 0048 6172 6420 4469 736b 0052 6561 6400 .Hard Disk.Read.
0000400: 2045 7272 6f72 00bb 0100 b40e cd10 ac3c Error.........<
0000416: 0075 f4c3 0000 0000 0000 0000 0000 0000 .u..............
0000432: 0000 0000 0000 0000 0000 0000 0000 0001 ................
0000448: 0100 07fe 3f7f 3f00 0000 4160 1f00 8000 ....?.?...A`....
0000464: 0180 83fe 3f8c 8060 1f00 cd2f 0300 0000 ....?..`.../....
0000480: 018d 83fe 3fcc 4d90 2200 40b0 0f00 0000 ....?.M.".@.....
0000496: 01cd 05fe ffff 8d40 3200 79eb 9604 55aa .......@2.y...U.
```

*p1*

*p2*

*p3*

*p4*

*Partition Table: 446-509 byte*

# I volumi: DOS Partition

## *Partition Table: analisi*

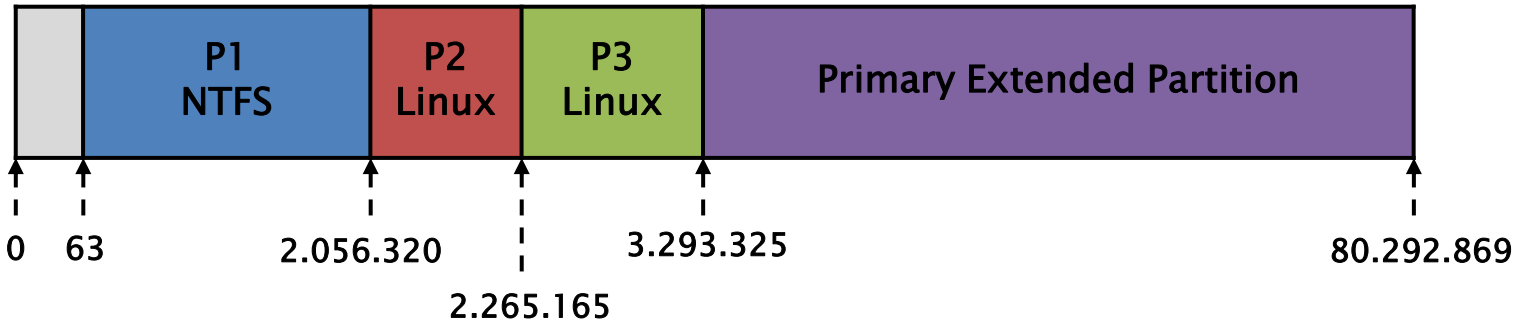
```
P1: 0001 0100 07fe 3f7f 3f00 0000 4160 1f00
P2: 8000 0180 83fe 3f8c 8060 1f00 cd2f 0300
P3: 0000 018d 83fe 3fcc 4d90 2200 40b0 0f00
P4: 0000 01cd 05fe ffff 8d40 3200 79eb 9604
```

| Part. *0-15* | BootFlag *0-0* | Start CHS *1-3* | Type *4-4* | End CHS *5-7* | LBA *8-11* | Size *12-15* |
|---|---|---|---|---|---|---|
| P1 | 00 | 01 01 00 | 07 | fe 3f 7f | 3f 00 00 00 | 41 60 1f 00 |
| | 00 | 00 01 01 | 07 | 7f 3f fe | 00 00 00 3f | 00 1f 60 41 |
| | 00 | - | NTFS | - | 63 | 2.056.257 |
| P2 | 80 | 00 01 80 | 83 | fe 3f 8c | 80 60 1f 00 | cd 2f 03 00 |
| | 80 | 80 01 00 | 83 | 8c 3f fe | 00 1f 60 80 | 00 03 2f cd |
| | 80 | - | Linux | - | 2.056.320 | 208.845 |

# I volumi: DOS Partition

## *Partition Table: analisi*

| Part. *0-15* | BootFlag *0-0* | Start CHS *1-3* | Type *4-4* | End CHS *5-7* | LBA *8-11* | Size *12-15* |
|---|---|---|---|---|---|---|
| P3 | 00 | 00 01 8d | 83 | fe 3f cc | 4d 90 22 00 | 40 b0 0f 00 |
| | 00 | 8d 01 00 | 83 | cc 3f fe | 00 22 90 4d | 00 0f b0 40 |
| | 00 | - | Linux | - | 2.265.165 | 1.028.160 |
| P4 | 00 | 00 01 cd | 05 | fe ff ff | 8d 40 32 00 | 79 eb 96 04 |
| | 00 | cd 01 00 | 05 | ff ff fe | 00 32 40 8d | 04 96 eb 79 |
| | 00 | - | DOS Ext | - | 3.293.325 | 79.999.545 |



# I volumi: DOS Partition

## *Partition Table: analisi*

- Analisi del primo settore del Primary Extended Partition: EBR

```
root@caine:/# dd if=disk3.dd bs=512 skip=3293325 count=1 | xxd
                                [.   .   .]
0000432: 0000 0000 0000 0000 0000 0000 0000 0001 ................
0000448: 01cd 83fe 7fcb 3f00 0000 0082 3e00 0000 ......?.....>...
0000464: 41cc 05fe bf0b 3f82 3e00 40b0 0f00 0000 A.....?.>.@.....
0000480: 0000 0000 0000 0000 0000 0000 0000 0000 ................
0000496: 0000 0000 0000 0000 0000 0000 0000 55aa ..............U.
```

SFSP 1

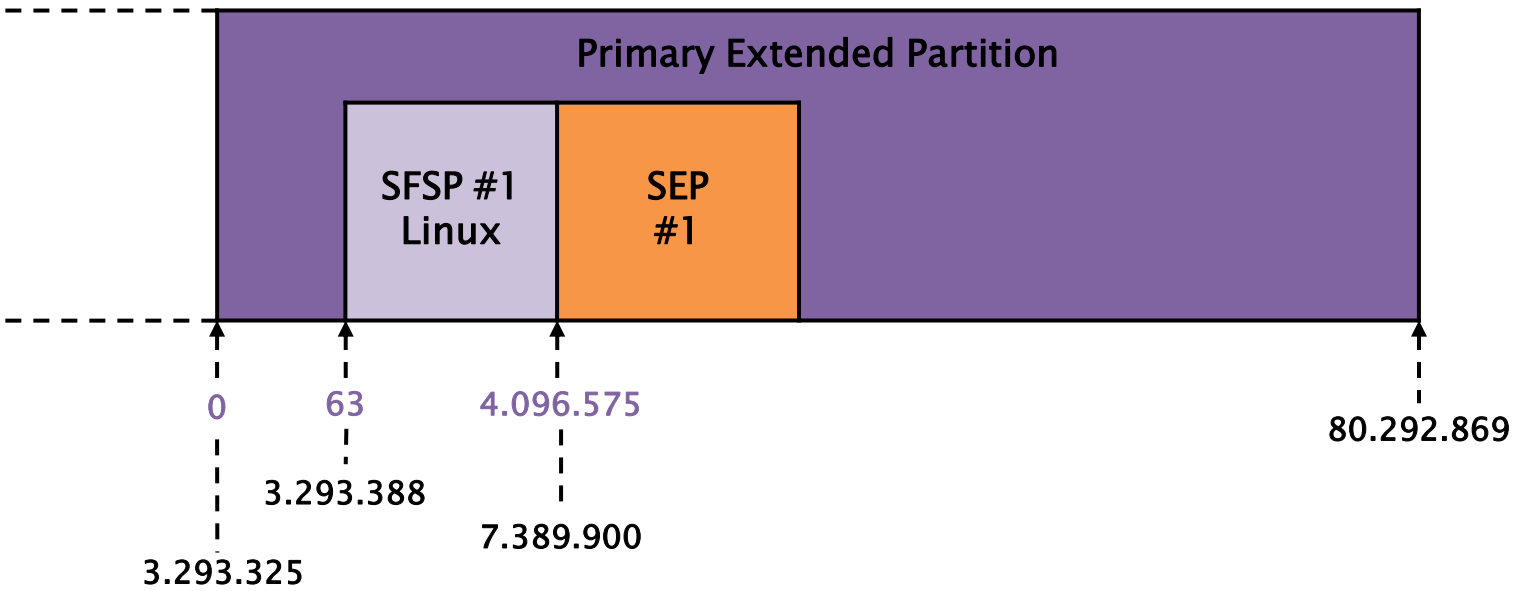
SEP1

| Part. *0-15* | BootFlag *0-0* | Start CHS *1-3* | Type *4-4* | End CHS *5-7* | LBA *8-11* | Size *12-15* |
|---|---|---|---|---|---|---|
| SFSP #1 | 00 | 01 01 cd | 83 | fe 7f cb | 3f 00 00 00 | 00 82 3e 00 |
| | 00 | cd 01 01 | 83 | cb 7f fe | 00 00 00 3f | 00 3e 82 00 |
| | **00** | **-** | **Linux** | **-** | **63** | **4.096.572** |
| SEP #1 | 00 | 00 41 cc | 05 | fe bf 0b | 3f 82 3e 00 | 40 b0 0f 00 |
| | 00 | cc 41 00 | 05 | 0b bf fe | 00 3e 82 3f | 00 0f b0 40 |
| | **00** | **-** | **DOS E** | **-** | **4.096.575** | **1.028.160** |

# I volumi: DOS Partition

## *Partition Table: analisi*

| Part. | Type | LBA | Size |
|---|---|---|---|
| Secondary File System Partition #1 | Linux | 63 | 4.096.572 |
| Secondary Extended Partition #1 | DOS Ext. | 4.096.575 | 1.028.160 |

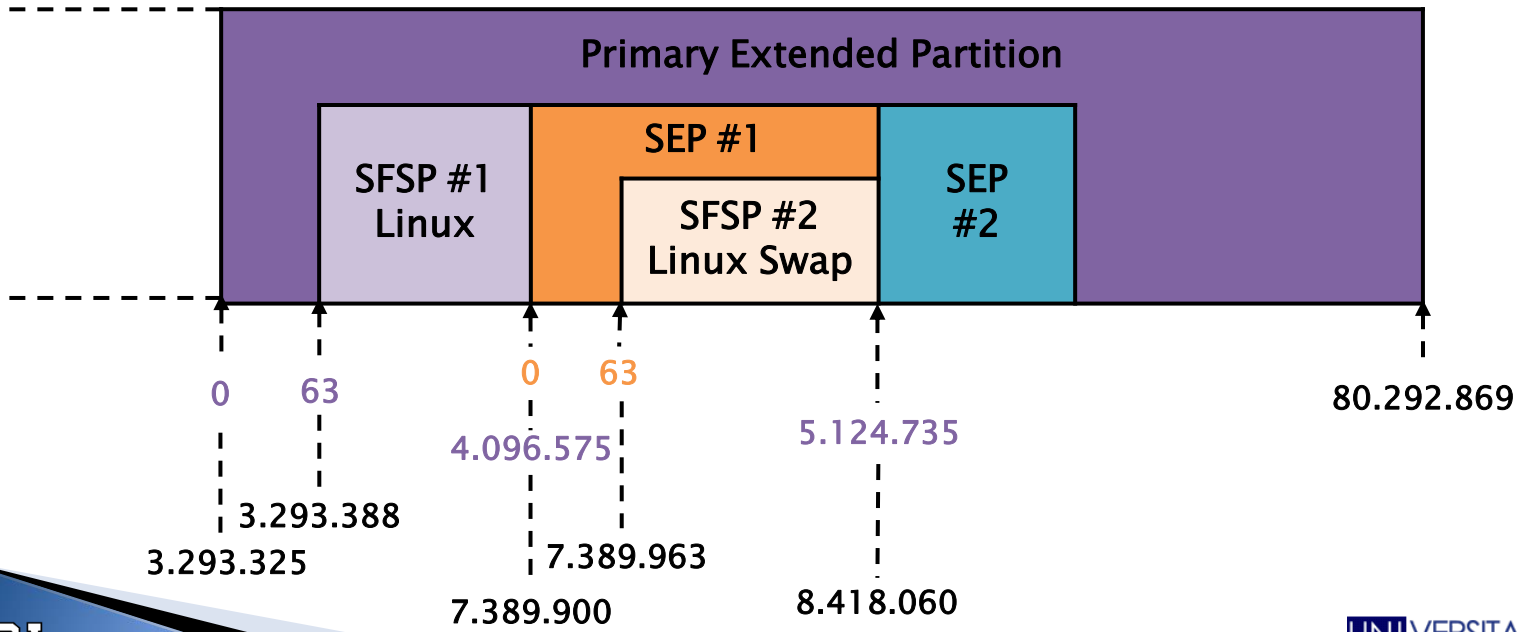


# I volumi: DOS Partition

## *Partition Table: analisi*

```
root@caine:/# dd if=disk3.dd bs=512 skip=7389900 count=1 | xxd
```

| Part. | Type | LBA | Size |
|---|---|---|---|
| Secondary File System Partition #2 | 82 Linux Swap | 63 | 4.096.572 |
| Secondary Extended Partition #2 | DOS Ext. | 5.124.735 | 1.028.160 |



# I volumi: DOS Partition

## *Partition Table: analisi*

- fdisk

```
root@caine:/# fdisk -lu disk3.dd
Disk disk3.dd: 255 heads, 63 sectors, 0 cylinders
Units = sectors of 1 * 512 bytes
Device     Boot  Start       End     Blocks Id System
disk3.dd1           63   2056319   1028128+  7 HPFS/NTFS
disk3.dd2   *   2056320   2265164    104422+ 83 Linux
disk3.dd3       2265165   3293324    514080 83 Linux
disk3.dd4       3293325  80292869  38499772+  5 Extended
disk3.dd5       3293388   7389899   2048256 83 Linux
disk3.dd6       7389963   8418059    514048+ 82 Linux swap
disk3.dd7       8418123   9446219    514048+ 83 Linux
disk3.dd8       9446283  17639369   4096543+  7 HPFS/NTFS
disk3.dd9      17639433  48371714  15366141 83 Linux
```

# I volumi: DOS Partition

## *Partition Table: analisi*

- mmls

```
root@caine:/# mmls -t dos disk3.dd
Disk disk3.dd: 255 heads, 63 sectors, 0 cylinders
Units are in 512-byte sectors
     Slot Start      End        Length     Description
00: ----- 0000000000 0000000000 0000000001 Table #0
01: ----- 0000000001 0000000062 0000000062 Unallocated
02: 00:00 0000000063 0002056319 0002056257 NTFS (0x07)
03: 00:01 0002056320 0002265164 0000208845 Linux (0x83)
04: 00:02 0002265165 0003293324 0001028160 Linux (0x83)
05: 00:03 0003293325 0080292869 0076999545 DOS Extended (0x05)
06: ----- 0003293325 0003293325 0000000001 Table #1
07: ----- 0003293326 0003293387 0000000062 Unallocated
08: 01:00 0003293388 0007389899 0004096512 Linux (0x83)
09: 01:01 0007389900 0008418059 0001028160 DOS Extended (0x05)
```

# I volumi: DOS Partition

## *Partition Table: analisi*

```
10: ----- 0007389900 0007389900 0000000001 Table #2
11: ----- 0007389901 0007389962 0000000062 Unallocated
12: 02:00 0007389963 0008418059 0001028097 Linux Swap (0x82)
13: 02:01 0008418060 0009446219 0001028160 DOS Extended (0x05)
14: ----- 0008418060 0008418060 0000000001 Table #3
15: ----- 0008418061 0008418122 0000000062 Unallocated
16: 03:00 0008418123 0009446219 0001028097 Linux (0x83)
17: 03:01 0009446220 0017639369 0008193150 DOS Extended (0x05)
18: ----- 0009446220 0009446220 0000000001 Table #4
19: ----- 0009446221 0009446282 0000000062 Unallocated
20: 04:00 0009446283 0017639369 0008193087 NTFS (0x07)
21: 04:01 0017639370 0048371714 0030732345 DOS Extended (0x05)
22: ----- 0017639370 0017639370 0000000001 Table #5
23: ----- 0017639371 0017639432 0000000062 Unallocated
24: 05:00 0017639433 0048371714 0030732282 Linux (0x83)
```

# I Volumi

- Apple Partition Map

SSRI
Sicurezza Sistemi Reti Informatiche

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

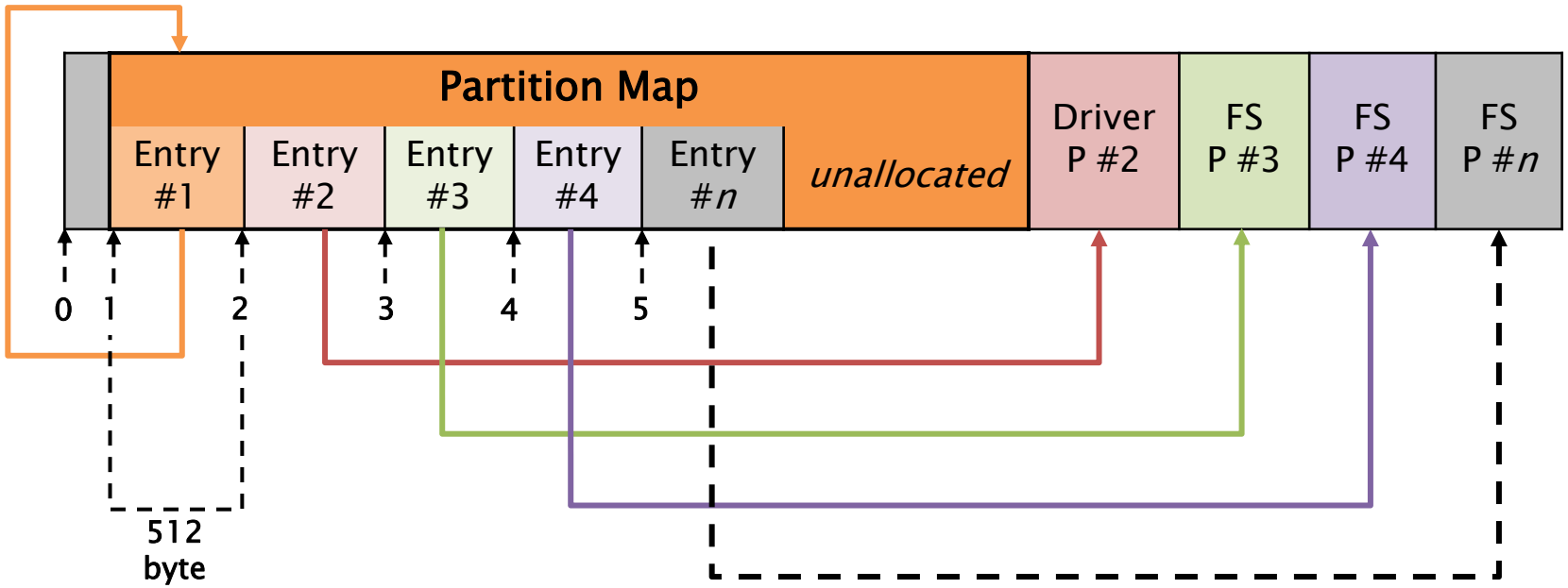
a.a. 2021/22

# I volumi: Apple Partition Map

- Apple Partition Map (APM)
  - Impiegato soprattutto dai vecchi sistemi basati su processori non Intel.
  - Nessun limite massimo di partizioni
  - Gestisce volumi fino a 2TB

- Partition Map: secondo settore *(512byte)*
  - Ogni entry *(512byte)* descrive una partizione
  - La prima entry descrive la «Partition Map»

# I volumi: Apple Partition Map



# I volumi: Apple Partition Map

## *Partition Table*

| Byte Range | Description | Essential |
|---|---|---|
| 0-1 | Signature value (0x504D) | No |
| 2-3 | Reserved | No |
| 4-7 | Total Number of partitions | Yes |
| 8-11 | Starting sector of partition | Yes |
| 12-15 | Size of partition in sectors | Yes |
| 16-47 | Name of partition in ASCII | No |
| 48-79 | Type of partition in ASCII | No |
| 80-83 | Starting sector of data area in partition | No |
| 84-87 | Size of data area in sectors | No |
| 88-91 | Status of partition | No |

| Byte Range | Description | Essential |
|---|---|---|
| 92-95 | Starting sector of boot code | No |
| 96-99 | Size of boot code in sectors | No |
| 100-103 | Address of boot loader code | No |
| 104-107 | Reserved | No |
| 108-111 | Boot code entry point | No |
| 112-115 | Reserved | No |
| 116-119 | Boot code checksum | No |
| 120-135 | Processor type | No |
| 136-511 | Reserved | No |

# I Volumi

- Apple Partition Map

SSRI
Sicurezza Sistemi Reti Informatiche

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

a.a. 2021/22

# I volumi: Apple Partition Map

## *Partition Table: analisi*

- Estrazione ed analisi della prima entry

```
root@caine:/# dd if=mac-disk.dd bs=512 skip=1 count=1 | xxd
0000000: 504d 0000 0000 000a 0000 0001 0000 003f PM.............?
0000016: 4170 706c 6500 0000 0000 0000 0000 0000 Apple...........
0000032: 0000 0000 0000 0000 0000 0000 0000 0000 ................
0000048: 4170 706c 655f 7061 7274 6974 696f 6e5f Apple_partition_
0000064: 6d61 7000 0000 0000 0000 0000 0000 0000 map.............
0000080: 0000 0000 0000 003f 0000 0000 0000 0000 .......?........
0000096: 0000 0000 0000 0000 0000 0000 0000 0000 ................
                         [.  .  .]
```

| Byte Range | Description | Value |
|---|---|---|
| 0-1 | Signature value | 504d |
| 4-7 | Total Number of partitions | 0000000a (10) |
| 8-11 | Starting sector of partition | 00000001 (1) |
| 12-15 | Size of partition in sectors | 0000003f |
| 16-47 | Name of partition in ASCII | Apple |
| 48-79 | Type of partition in ASCII | Apple_partition_map |

# I volumi: Apple Partition Map

## *Partition Table: analisi*

- mmls

```
root@caine:/# mmls -t mac mac-disk.dd


MAC Partition Map
Units are in 512-byte sectors
     Slot Start      End        Length     Description
00: ----- 0000000000 0000000000 0000000001 Unallocated
01: 00    0000000001 0000000063 0000000063 Apple_partition_map
02: ----- 0000000001 0000000010 0000000010 Table
03: ----- 0000000011 0000000063 0000000053 Unallocated
04: 01    0000000064 0000000117 0000000054 Apple_Driver43
05: 02    0000000118 0000000191 0000000074 Apple_Driver43
06: 03    0000000192 0000000245 0000000054 Apple_Driver_ATA
07: 04    0000000246 0000000319 0000000074 Apple_Driver_ATA
08: 05    0000000320 0000000519 0000000200 Apple_FWDriver
09: 06    0000000520 0000001031 0000000512 Apple_Driver_IOKit
10: 07    0000001032 0000001543 0000000512 Apple_Patches
11: 08    0000001544 0039070059 0039068516 Apple_HFS
12: 09    0039070060 0039070079 0000000020 Apple_Free
```

# I Volumi

- GUID Partition Table

SSRI
Sicurezza Sistemi Reti Informatiche

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

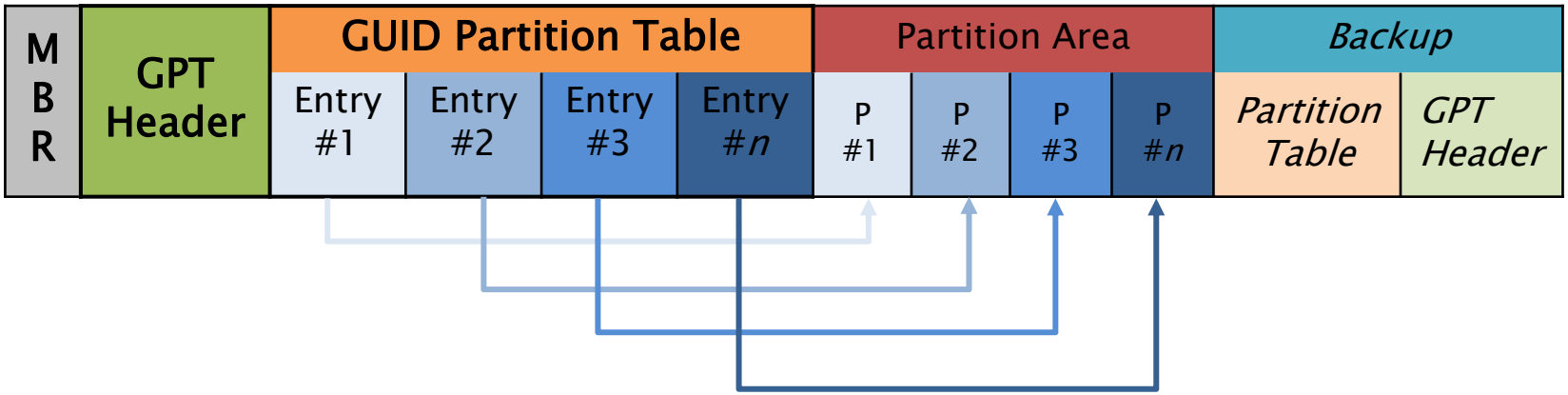
a.a. 2021/22

# I volumi: GUID Partition Table

- Sistema di partizionamento utilizzato da EFI
  - Massimo 128 partizioni
  - Volumi più grandi di 2TB

- Composto da 5 aree\sezioni:
  - Protective MBR: DOS Partition Table (1^ settore)
  - GPT Header: definisce il layout delle aree
  - Partition Table: Ogni entry descrive la partizione
  - Partition Area: locazione riservata alla partizioni
  - Backup Area: copia di backup del GTP Header e della partition Table

# I volumi: GUID Partition Table



# I volumi: GUID Partition Table

## *Analisi*

- Analisi del MBR Partition Table

```
root@caine:/# mmls -t dos gpt-disk.dd

DOS Partition Table
Units are in 512-byte sectors
     Slot Start      End        Length     Description
00: ----- 0000000000 0000000000 0000000001 Primary Table (#0)
01: 00:00 0000000001 0120103199 0120103199 GPT Safety Partition (0xEE)
```

# I volumi: GUID Partition Table

## *GPT Header*

| Byte Range | Description | Essential |
|---|---|---|
| 0–7 | Signature value ("EFI PART") | No |
| 8–11 | Version | Yes |
| 12–15 | Size of GPT header in bytes | Yes |
| 16—19 | CRC32 checksum of GPT header | No |
| 20–23 | Reserved | No |
| 24–31 | LBA of current GPT header structure | No |
| 32–39 | LBA of the other GPT header structure | No |
| 40–47 | LBA of start of partition area | Yes |
| 48–55 | LBA of end of partition area | No |
| 56–71 | Disk GUID | No |
| 72–79 | LBA of the start of the partition table | Yes |
| 80–83 | Number of entries in partition table | Yes |
| 84–87 | Size of each entry in partition table | Yes |
| 88–91 | CRC32 checksum of partition table | No |
| 92–End Sector | Reserved | No |

# I volumi: GUID Partition Table

## *GPT Header: analisi*

```
root@caine:/# dd if=gpt-disk.dd bs=512 skip=1 count=1 | xxd

0000000: 4546 4920 5041 5254 0000 0100 5c00 0000 EFI PART....\...
0000016: 8061 a3b0 0000 0000 0100 0000 0000 0000 .a..............
0000032: 1fa1 2807 0000 0000 2200 0000 0000 0000 ..(.....".......
0000048: fea0 2807 0000 0000 7e5e 4da1 1102 5049 ..(.....~^M...PI
0000064: ab2a 79a6 3ea6 3859 0200 0000 0000 0000 .*y.>.8Y........
0000080: 8000 0000 8000 0000 69a5 7180 0000 0000 ........i.q.....
0000096: 0000 0000 0000 0000 0000 0000 0000 0000 ................
                          [.  .  .]
```

| Byte Range | Description | Value |
|---|---|---|
| 0-7 | Signature value | EFI PART |
| 12-15 | Size of GPT header in bytes | 5c00 (96) |
| 32-39 | LBA of the other GPT header structure | 0728a1af (120.103.199) |
| 40-47 | LBA of start of partition area | 0022(34) |
| 48-55 | LBA of end of partition area | 0728a0fe (120.103.166) |
| 72-79 | LBA of the start of the partition table | 0002 (2) |
| 80-83 | Number of entries in partition table | 0080 (128) |
| 84-87 | Size of each entry in partition table | 0080 (128) |

# I volumi: GUID Partition Table

## *PartitionTable*

| Byte Range | Description | Essential |
|---|---|---|
| 0–15 | Partition type GUID | No |
| 16–31 | Unique partition GUID | No |
| 32–39 | Starting LBA of partition | Yes |
| 40–47 | Ending LBA of partition | Yes |
| 48–55 | Partition attributes | No |
| 56–127 | Partition name in Unicode | No |



## 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


SSRI
Sicurezza Sistemi Reti Informatiche

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

a.a. 2021/22