COMPUTER FORENSICS

Lezione 11: Question Time

A.A. 2021/22

Dott. Lorenzo LAURATO

Domanda nr. 01

Nella fase di identificazione, la preview...

- [x] è una perquisizione informatica ✓
- [ ] è una fase in cui non vi è alcun rischio di alterare il reperto ✗
- [ ] deve essere sempre eseguita su un sistema spento ✗
- [ ] non possono essere accesi i dispositivi rinvenuti spenti ✗

Legge n. 48 del 18/03/2008

art. 247 c.p.p.

(Casi e forme delle perquisizioni)

[…]

1bis *Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.*

[…]

Identificazione dell'evidence
la «preview»

- Consente di eseguire un'analisi di primo livello delle memorie dei dispositivi allo scopo di individuare possibili elementi di interesse investigativo.
- utilizzo di **write blocker** (*software/hardware ad hoc)*
- rischio di alterazione dei contenuti con conseguente dispersione di una possibile prova;

Domanda nr. 02

la preview in un sistema acceso (LIVE)

- [ ] può essere eseguita con una distro live forensic oriented ✗
- [x] rende veloce l'analisi dei software presenti nel sistema ✓
- [ ] può essere eseguito con qualsiasi tool forensic oriented indipendentemente dal sistema da analizzare ✗
- [ ] è consigliabile eseguirla con un "write blocker" ✗

Identificazione dell'evidence

la «preview»

LIVE

- è un'analisi eseguita impiegando il S.O. presente sul dispositivo da analizzare;
- deve essere documentata e verbalizzata;
- **PRO**:
  - consente di avere una visione dell'ambiente in cui opera l'utente;
  - è veloce nell'analisi dei software installati;
- **CONTRO**:
  - Alterazione del reperto
  - Strumenti adeguati al sistema

Identificazione dell'evidence

la «preview»

DEAD

- **PRO**:
  - Permette di non alterare il dispositivo;
  - Consente di utilizzare diversi strumenti per analizzare la memoria del dispositivo.

- **CONTRO**:
  - Buona conoscenza del sistema e dei software da analizzare
  - Non sempre praticabile: sistemi embedded;

Domanda nr. 03

il sequestro fisico...

- [ ] viene eseguito elaborando la c.d. copia forense ✗
- [ ] è sempre possibile eseguirlo ✗
- [x] se il dispositivo è accesso bisogna preoccuparsi del problema dello "shutdown" ✓

La Raccolta:
il sequestro fisico

- Prendere semplicemente il supporto contenente i dati, posticipando le problematiche derivanti dall'acquisizione del dato;

- Preoccuparsi solo di identificare e verbalizzare i reperti:
  - *Catena di custodia (Chain of Custody)*

La Raccolta:
il sequestro fisico

non è sempre fattibile

- sistemi che non possono essere fermati/spenti;
- sistemi distribuiti su decine di rack;

Domanda nr. 04

il sequestro logico

- [x] viene eseguito elaborando la c.d. copia forense ✓
- [x] deve essere descritto dalla catena di custodia ✓
- [ ] se il dispositivo è accesso bisogna obbligatoriamente preoccuparsi del problema dello "shutdown" ✗

La Raccolta:
il sequestro logico

- Duplicazione dei dati di [*possibile*] interesse investigativo;

COPIA FORENSE

La Raccolta:
la catena di custodia

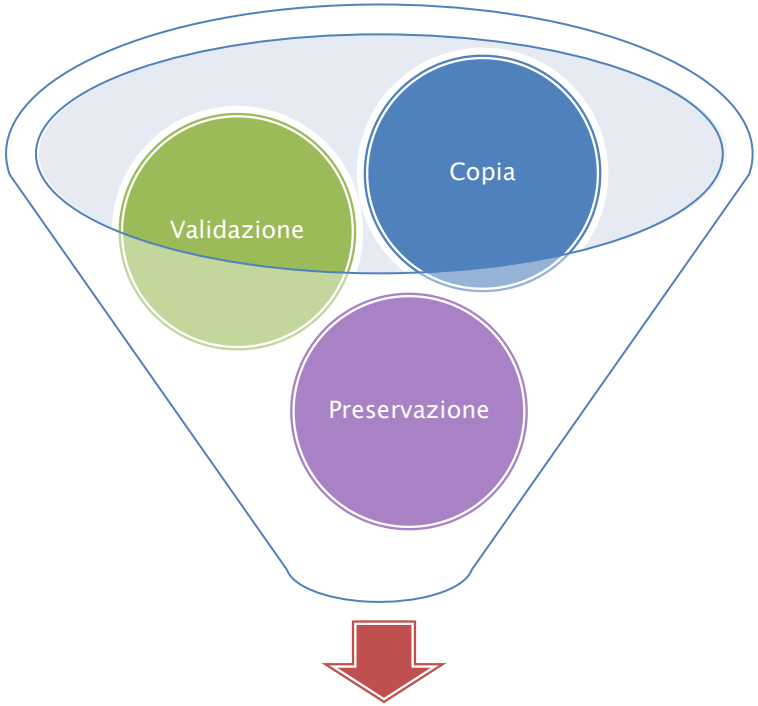
- Uno o più documenti (verbale/i) in cui devono essere riportati tutte le informazioni sul dispositivo che è stato sottoposto a sequestrato (fisico o logico):
  - Luogo, data e operatore che ha reperito e collezionato la fonte di prova;
  - Luogo, data e operatore che ha gestito e/o esaminato la fonte di prova;
  - Chi ha la responsabilità della custodia delle digital evidences.
  - Metodo di conservazione del reperto;
  - Eventuali trasferimenti di location dell'evidenza

Domanda nr. 05

la copia forense è...

- ○ una duplicazine dei dati di interesse investigativo ✗
- ○ una copia "bit a bit" dell'intero supporto di memoria ✗
- ◉ una qualunque copia di dati che rispetta le caratteristiche di validazione e preservazione ✓
- ○ una duplicazione dei dati eseguita in modo da garantire sempre la ripetibilità dell'operazione di copia ✗

La Raccolta:
Copia Forense



Copia Forense

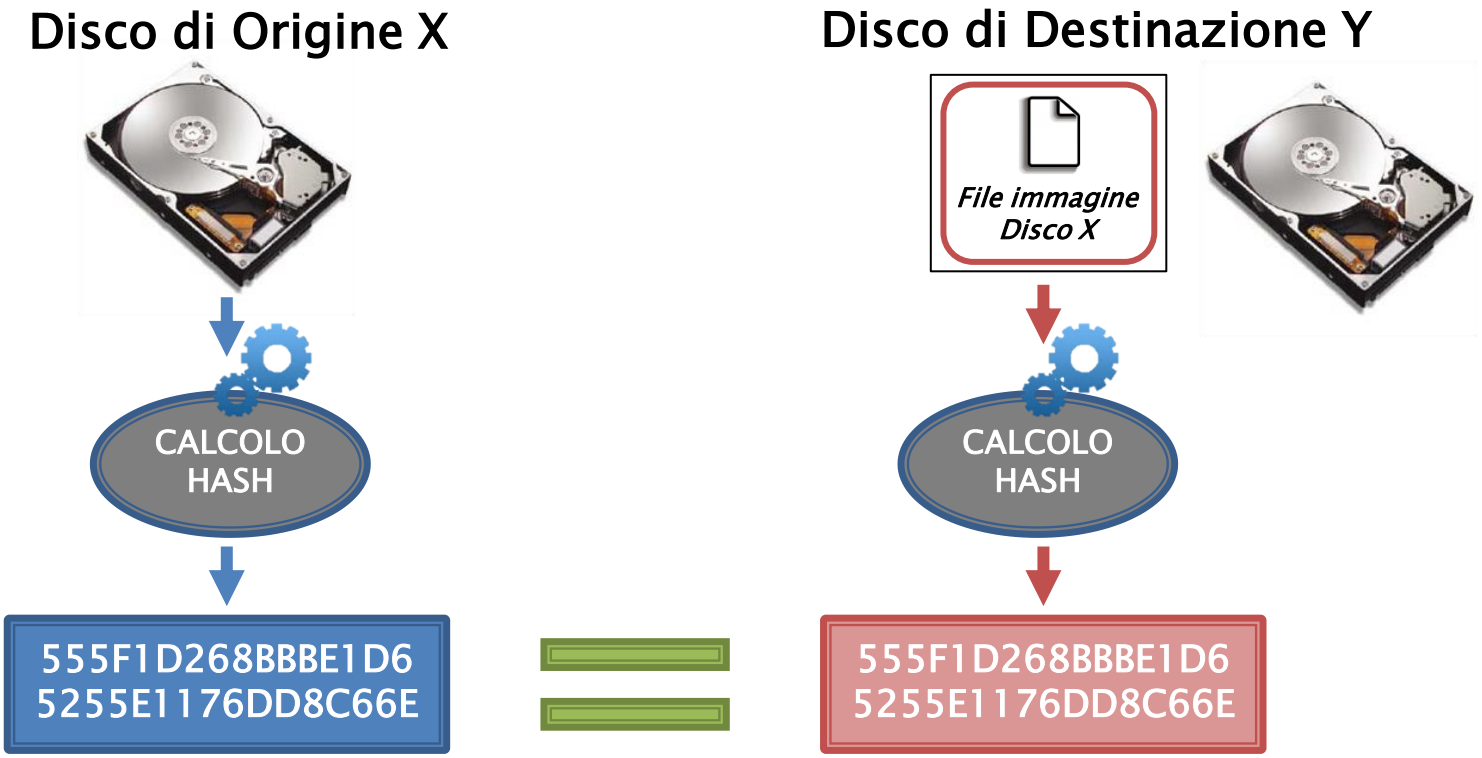
Domanda nr. 06

Per validazione si intende che...

- [x] l'hash della copia forense coincide con l'hash calcolato dal supporto originale ✓
- [ ] l'hash della copia forense coinciderà sempre con l'hash calcolato da una successiva copia forense ✗
- [ ] l'hash della copia forense coincide con l'hash ricalcolato dalla medesima copia dopo la fase di analisi ✗
- [x] i dati della copia forense sono identici ai dati originali ✓

Copia Forense
hash

- **Validazione**: garantisce che la copia eseguita è identica al dato originale.



Domanda nr. 07

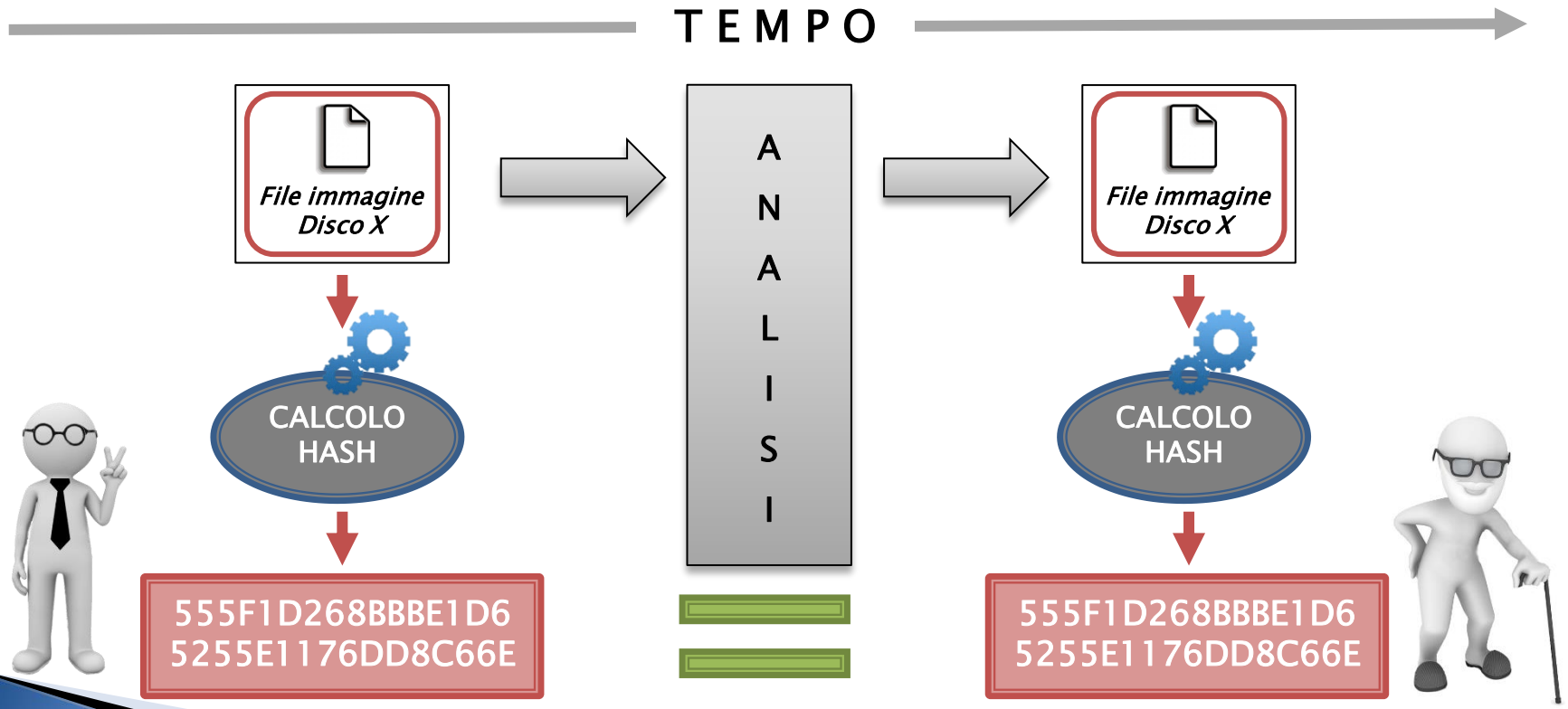
Per preservazione si intende che...

- [x] l'hash della copia forense coincide con l'hash ricalcolato dalla medesima copia dopo la fase di analisi ✓
- [ ] la copia forense è inalterabile ✗
- [ ] l'hash della copia forense coincide con l'hash calcolato da una successiva copia forense ✗
- [ ] i dati della copia forense sono identici ai dati originali ✗

Copia Forense

hash

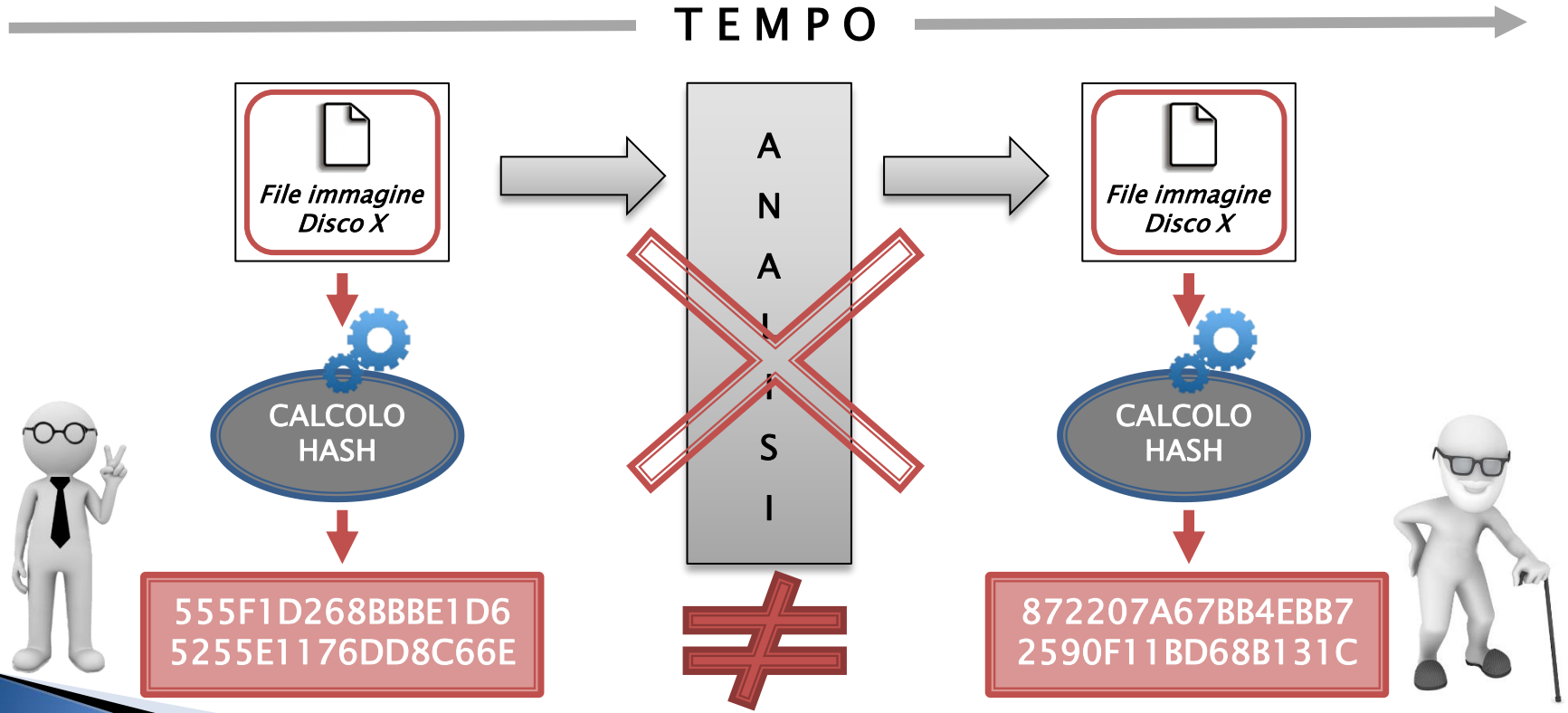
- **Preservazione**: garantisce che non vengano eseguite modifiche\alterazioni alla copia forense, se ciò avviene l'hash cambierà



Copia Forense

hash

- **Preservazione**: garantisce che non vengano eseguite modifiche\alterazioni alla copia forense, se ciò avviene l'hash cambierà



Domanda nr. 08

il comando DD

- [ ] da solo permette di produrre una copia forense ✗
- [ ] garantisce la non alterazione del disco originale ✗
- [x] esegue una copia "bit a bit" di un supporto di memoria generando un file immagine ✓
- [x] permette di eseguire una copia di un solo file ✓

Copia Forense
comando «*DD*»

- Eseguiamo la copia forense

```
root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda.dd bs=2048 conv=noerror,sync
```

IF = input file *[disco sorgente «**sda**»]*

OF = output file *[file immagine «**sda.dd**»]*

BS = block size in byte (default 512) *[dimensione del blocco di lettura «**2048 byte**»]*

CONV = esegue l'elaborazione in base ai parametri indicati

noerror = continua ad elaborare in caso di errore di lettura

sync = sostituisce i blocchi di memoria non letti nella destinazione con NULs (mantiene sincronizzata la dimensione della destinazione con quella della sorgente)

Domanda nr. 09

Per eseguire una copia forense, il seguente comando: dd if=/dev/sda bs=2048 | tee mnt/dd_image/sda.dd | md5sum > mnt/dd_image/sda.hash

- [ ] produce un file immagine segmentato\diviso in parti da massimo 2048MB ✗
- [ ] non è corretto ✗
- [x] è corretto ✓
- [x] esegue la copia forense della sorgente "sda" ✓
- [ ] esegue il calcolo dell'hash on-the-fly dell'immagine "sda.dd" ✗

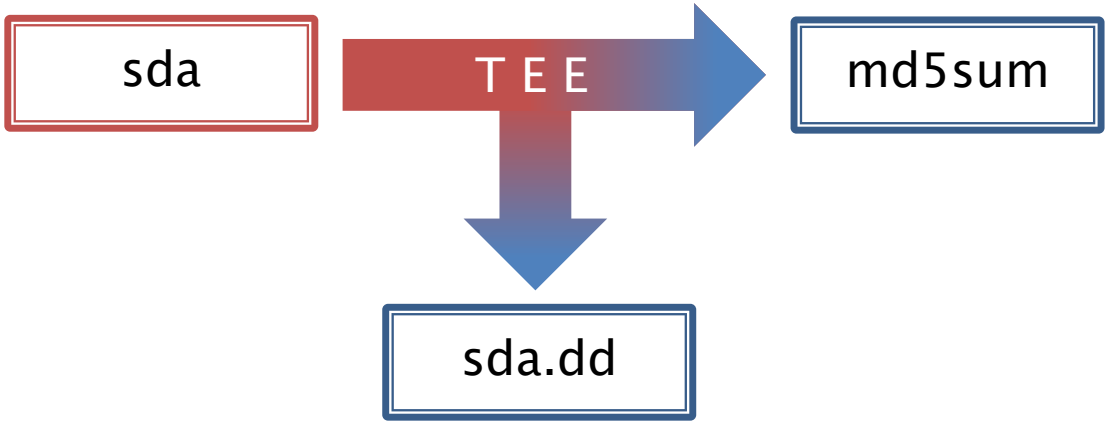
Copia Forense
comando «*DD*»

Calcolare l'Hash

- Metodo nr. 2:
  - Calcoliamo l'hash durante l'elaborazione della copia

```
root@caine:/# dd if=/dev/sda bs=2048 | tee /mnt/dest/dd_image/sda.dd |
              md5sum > /mnt/dest/dd_image/ sda.hash
```

TEE = biforca\duplica lo stream [una viene utilizzata per generare il file immagine, l'altra viene trasmesso al comando successivo «md5sum»]



Domanda nr. 10

Per eseguire una copia forense, il seguente comando: dd if=/mnt/sda.dd of=/dev/sda conv=noerror, sync

- ○ è errato in quanto non è stato specificato il "blocksize" ✗
- ○ è corretto ✗
- ○ non è completo, in quanto manca il calcolo dell'hash ✗
- ○ non è corretto poiché le opzioni "noerror" e "sync" non possono essere combinate ✗
- ◉ non è corretto per altri motivi ✓

Copia Forense
comando «*DD*»

- Eseguiamo la copia forense

```
root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda.dd bs=2048 conv=noerror,sync
```

IF = input file *[disco sorgente «**sda**»]*

OF = output file *[file immagine «**sda.dd**»]*

BS = block size in byte (default 512) *[dimensione del blocco di lettura «**2048 byte**»]*

CONV = esegue l'elaborazione in base ai parametri indicati

noerror = continua ad elaborare in caso di errore di lettura

sync = sostituisce i blocchi di memoria non letti nella destinazione con NULs (mantiene sincronizzata la dimensione della destinazione con quella della sorgente)

Domanda nr. 11

il formato DD/RAW:

- [ ] conserva nell'header solo il calcolo dell'hash MD5 ✗
- [x] non conserva alcun metadato del reperto sorgente ✓
- [x] non permette la compressione ✓
- [x] rappresenta la copia di un solo "file/stream" ✓

Disk Image:
formato DD/RAW

Formato semplice: è un container dello stream

- Problematiche:
  - Non conserva metadati dell'evidence: *modello, seriale, dimensione, etc.*
  - Non conserva hash calcolati;
  - Non esegue compressione;
  - Non può contenere più di un file/stream;

Domanda nr. 12

E' un formato per "disk image"

- [x] ISO ✓
- [x] .bin/.cue ✓
- [x] Smart (.s01, .s02, ...) ✓
- [x] DD ✓
- [ ] Encase L01 (.L01, .L02, ...) ✗

Disk Image:
Encase L01 Logical (Famiglia EWF)

- Acquisizione di file logici.
- Segmentazione dell'immagine: *.l01, .l02, etc.*
- Impiega nr. 15 sezioni (+ 2 al formato E01):
  - Ltree section
  - Ltypes section

Domanda nr. 13

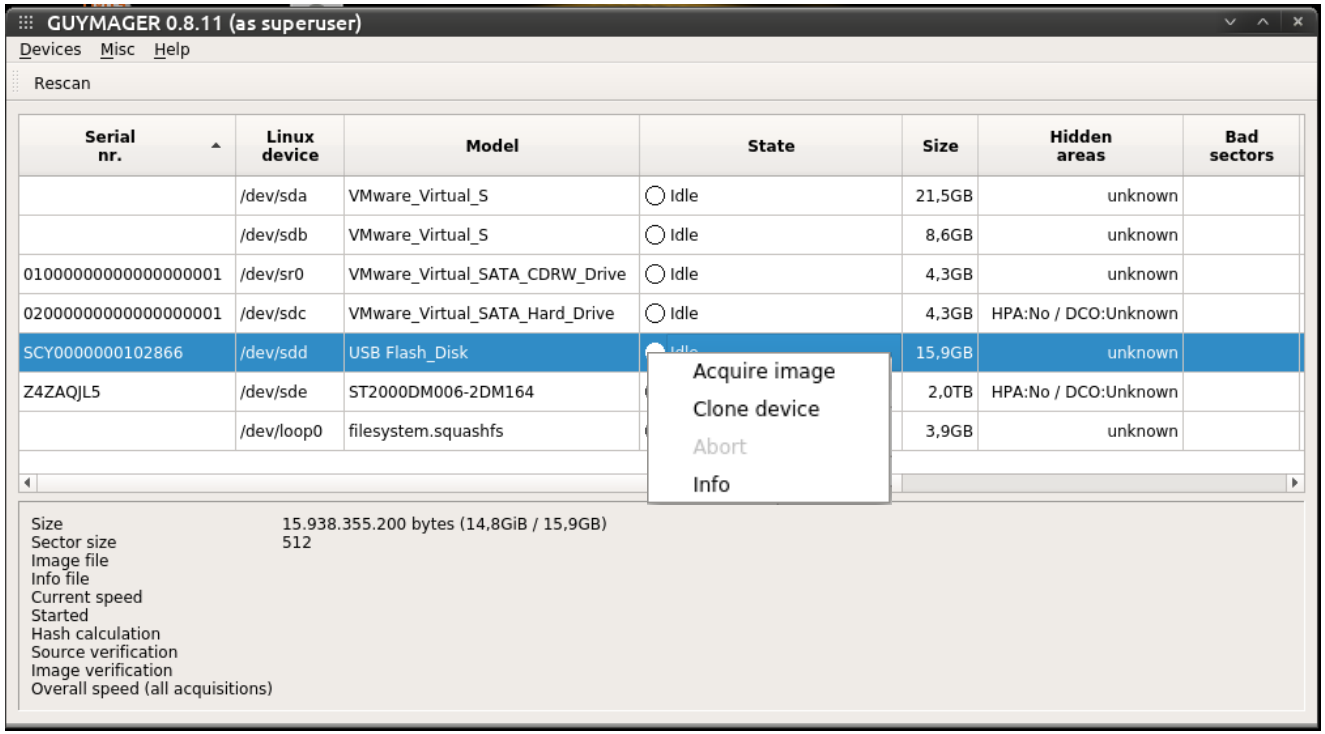
Guymager

- [x] è uno strumento per elaborare copie forensi ✓
- [ ] non fa uso dell'hashing on-the-fly ✗
- [ ] non permette di segmentare/splittare l'immagine ✗
- [x] permette di scegliere tra i seguenti hash: MD5, SHA-1, SHA-256 ✓
- [x] esegue copie forensi solo di tipo "full disk" ✓

Tool di acquisizione

Guymager: Disk Image

- scelta del dispositivo da acquisire *(/dev/sdd – USB Flash_Disk)*



Tool di acquisizione

Guymager: Disk Image

- Settaggio dell'elaborazione

Formato dell'immagine e dimensione dei segmenti

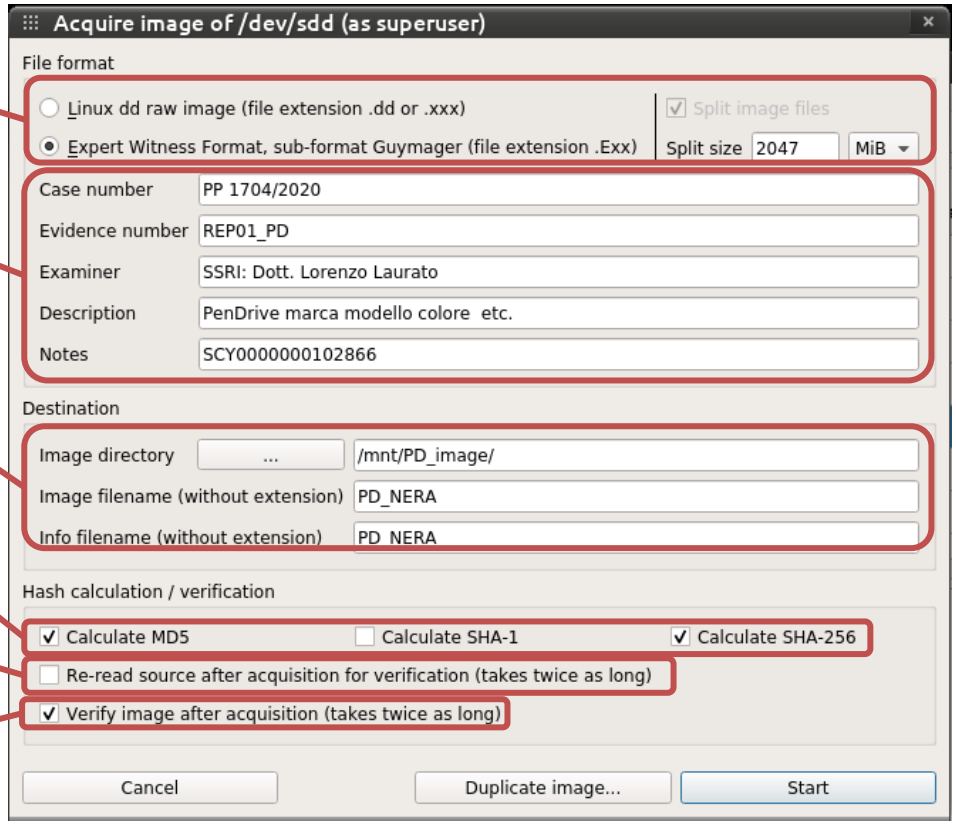
Informazioni elaborazione

Nome e destinazione del file immagine

Scelta dell'HASH

Calcolo dell'Hash del dispositivo target, dopo l'acquisizione

Calcolo dell'Hash del file immagine



Domanda nr. 14

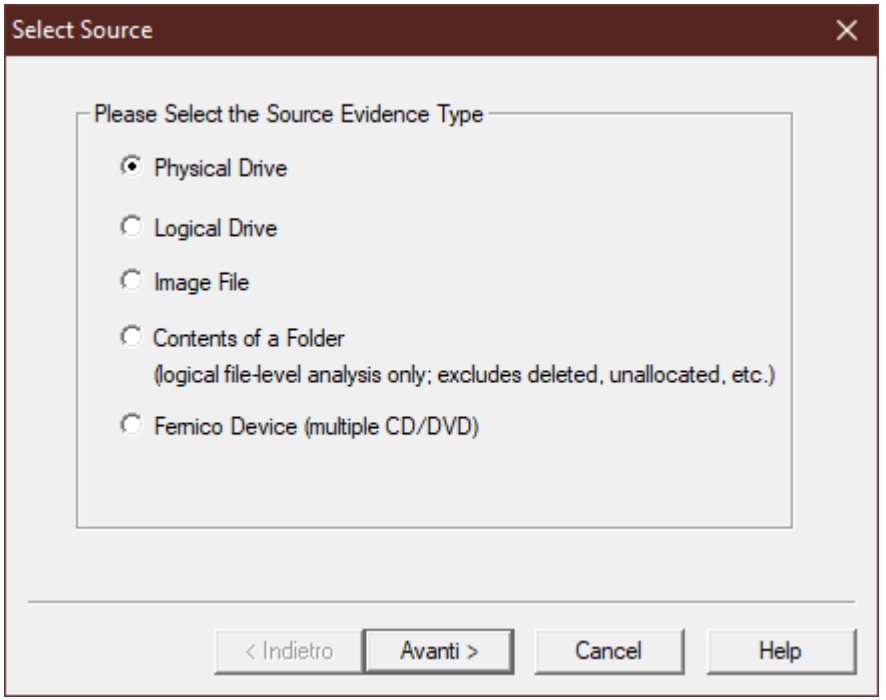
FTK Imager

- [x] è uno strumento per elaborare copie forensi ✓
- [ ] esegue copie forensi solo di tipo "full disk" ✗
- [ ] permette di scegliere tra i seguenti hash: MD5, SHA-1, SHA-256 ✗
- [x] può eseguire una copia della memoria volatile ✓

Tool di acquisizione
FTK Imager

- File>**Create Disk Image…**

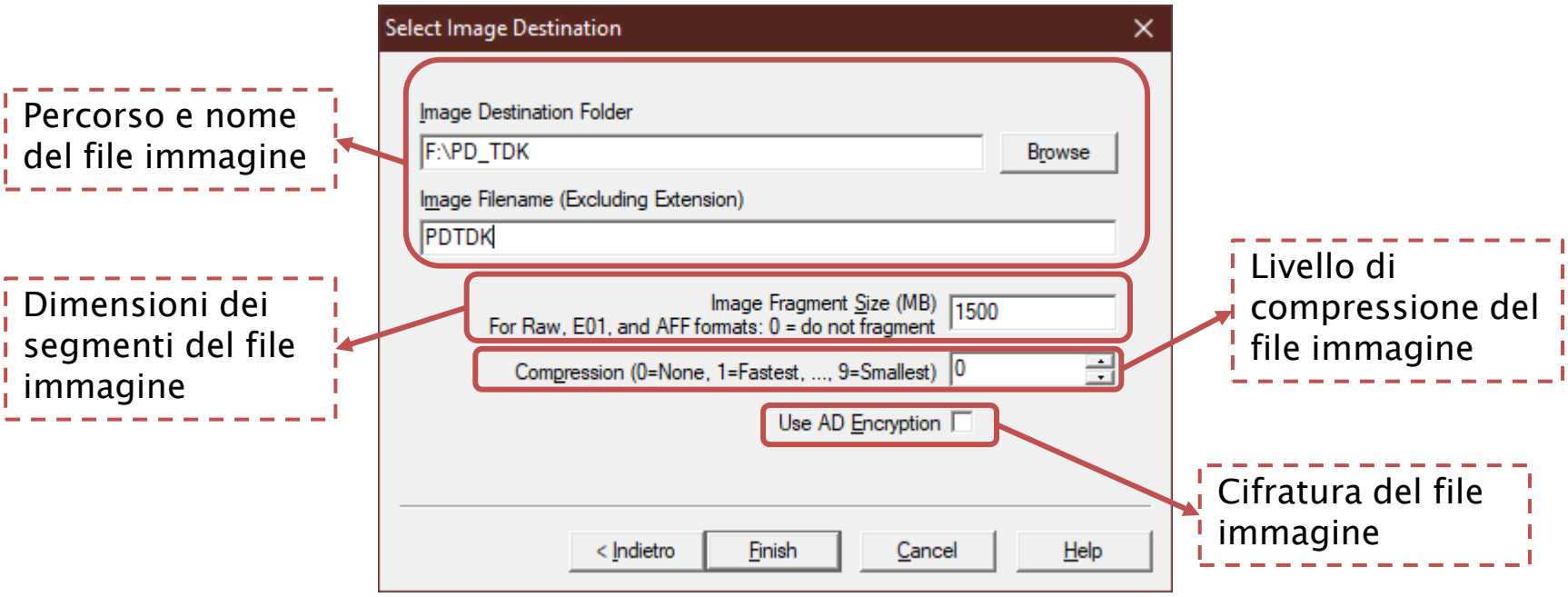
- Tipi di acquisizioni:
  - Phisical Drive
  - Logical Drive
  - Image File
  - Content of folder
  - Fenico Device



Tool di acquisizione

FTK Imager: Physical Drive

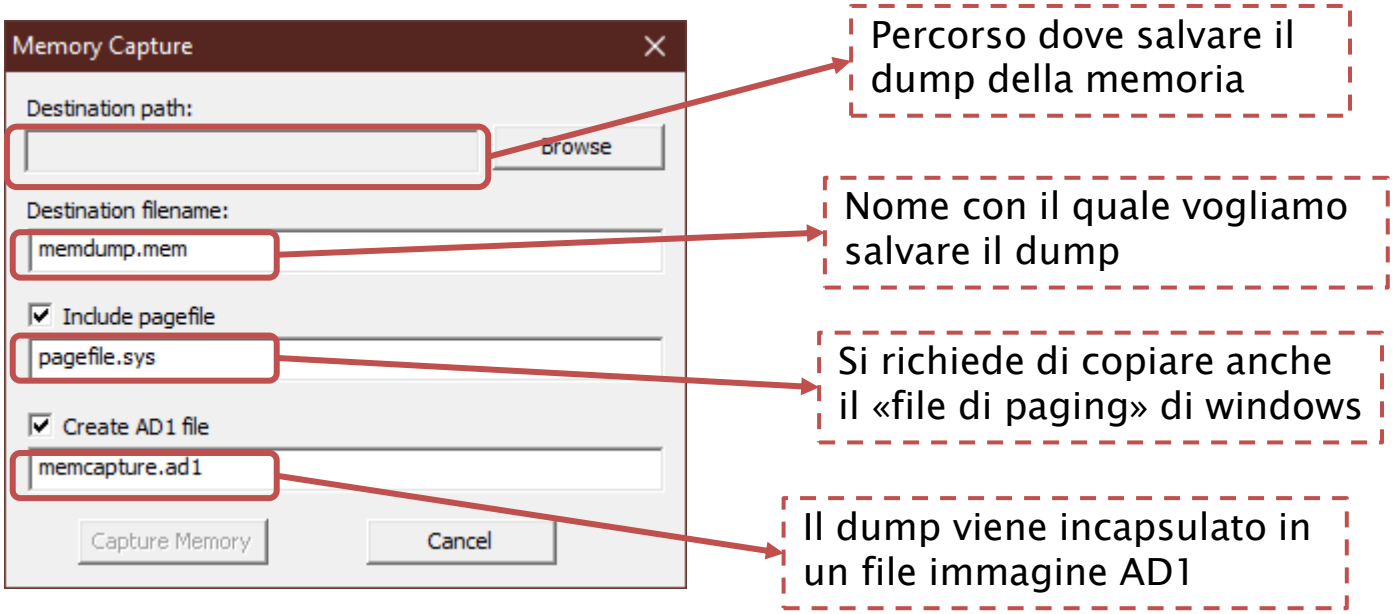
- **Definizione del file immagine**



Tool di acquisizione

FTK Imager: dump memoria volatile

- File>**Capture Memory**



Domanda nr. 15

L'algoritmo di Hash MD5

- [x] processa il messaggio in blocchi di 512bit ✓
- [ ] è costituito da 4 round e 3 funzioni logiche ✗
- [x] rispetto a MD4 fa uso di 62 costanti in più ✓
- [ ] l'output è un digest a 160bit ✗

Funzione Hash

MD4/MD5: padding del messaggio

- **MD4/MD5** processa il messaggio in <u>blocchi di 512 bit</u>
  - Ogni blocco consta di 16 parole di 32 bit
- **M'** sarà costituito da:
  - messaggio originario **M**
  - ***p** bit* di padding
  - ***b** bit* di rappresentazione della lunghezza di M (*max* 2^{64})

$$M' = M\ \underbrace{100\ldots0}_{p}\ \underbrace{b}_{64bit}$$

$$p \mid (p+M) \bmod_{512} = 448 \Longleftrightarrow 512-[(M+b) \bmod_{512}]$$

- **M'** consta di un numero di bit multiplo di 512, ovvero di un numero *L blocchi* di 512 bit
  - Ovvero di N parole con N multiplo di 16:
    - L=N/16 blocchi di 512 bit

Funzione Hash

MD4/MD5: funzioni

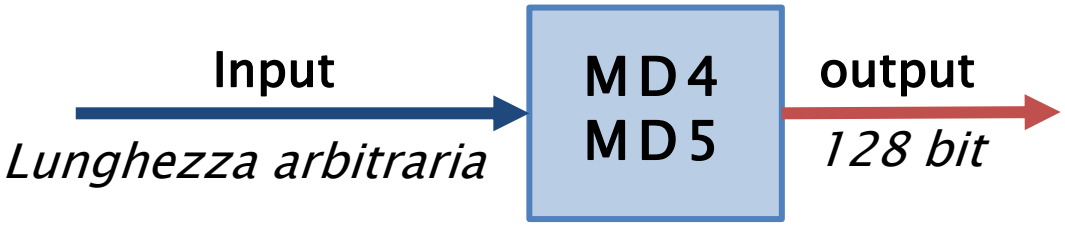
- **Funzioni definite su parole di 32 bit:**
  - round 1: $F(X,Y,Z) = (X \wedge Y) \vee ((\neg X) \wedge Z)$ [if X then Y else Z]
  - round 2: $G(X,Y,Z) = (X \wedge Z) \vee ((Y \wedge (\neg Z))$ **[MD5]** [if Z then X else Y]
  - round 2: $G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge Z) \vee (X \wedge Y)$ **[MD4]** [2 su 3]
  - round 3: $H(X,Y,Z) = X \oplus Y \oplus Z$ [bit di parità]
  - round 4: $I(X,Y,Z) = Y \oplus (X \vee (\neg Z))$ **[MD5]**

X	Y	Z	F	G	H	I
0	0	0	0	0	0	1
0	0	1	1	0	1	0
0	1	0	0	1	1	0
0	1	1	1	0	0	1
1	0	0	0	0	1	1
1	0	1	0	1	0	1
1	1	0	1	1	0	0
1	1	1	1	1	1	0

Funzione Hash
MD4/MD5

MD = **M**essage **D**igest

- **MD4**: Progettata nel 1990 da Ron Rivest
  - *RFC1320 -> RFC6150*
- **MD5**: Progettata nel 1991 da Ron Rivest
  - *RFC1321 -> RFC6151*
- Operazioni efficienti su architetture 32 bit little-endian



Funzione Hash

MD5/MD4: differenze

MD5

- 4 round = 4 · 16 operazioni
- 4 funzioni logiche
- 64 costanti additive
- ogni passo aggiunge il risultato del passo precedente

MD4

- 3 round = 3 · 16 operazioni
- 3 funzioni logiche
- 2 costanti additive

Domanda nr. 16

Nell'algoritmo di SHA-1 se il messaggio di input M è di 968bit, dopo il padding avremo che M' sarà costituito da :

- [x] 3 blocchi da 512bit ✓
- [ ] 60bit per la lunghezza del messaggio ✗
- [x] un bit a "1" al 969° bit ✓
- [ ] nessun bit di padding ✗
- [x] 1536bit ✓

Funzione Hash
SHA: padding del messaggio

- **SHA** processa il messaggio in <u>blocchi di 512 bit</u>
  - Ogni blocco consta di 16 parole di 32 bit
- **M'** sarà costituito da:
  - messaggio originario **M**
  - ***p** bit* di padding
  - ***b** bit* di rappresentazione della lunghezza di M (*max* 2^{64})

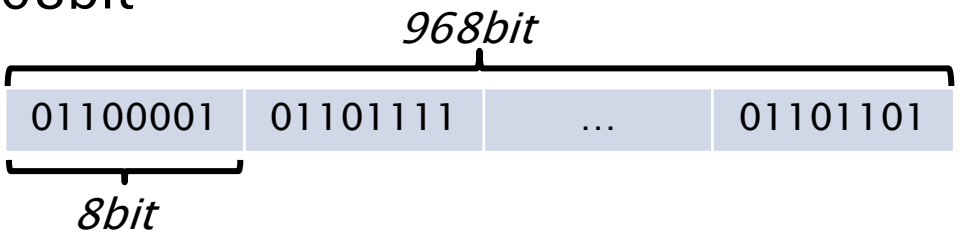
$$M' = M\ \underbrace{100\ldots0}_{p}\ \underbrace{b}_{64bit}$$

$$p \mid (p+M) \bmod_{512} = 448 \Longleftrightarrow 512-[(M+b) \bmod_{512}]$$

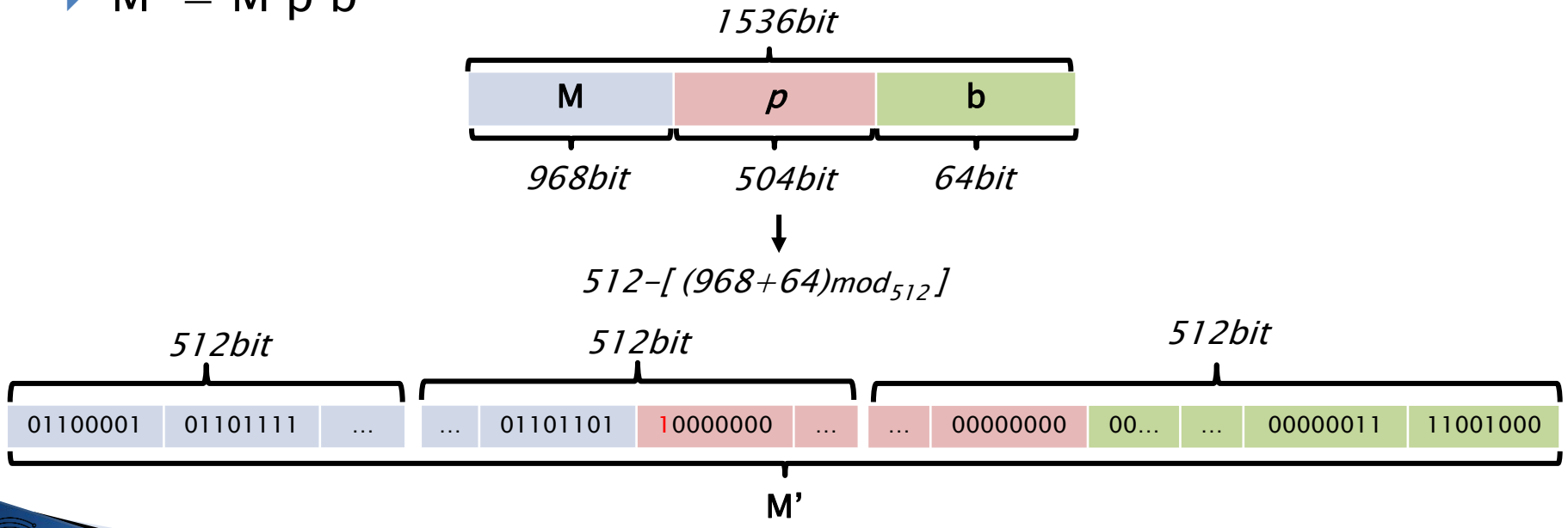
- **M'** consta di un numero di bit multiplo di 512, ovvero di un numero *L blocchi* di 512 bit
  - Ovvero di N parole con N multiplo di 16:
    - L=N/16 blocchi di 512 bit

Funzione Hash
padding del messaggio

- |M|=968bit



- M' = M p b



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