COMPUTER FORENSICS

Lezione 7: Fasi del trattamento
validazione e preservazione

A.A. 2021/22

Dott. Lorenzo LAURATO

Nella puntata precedente…

Identificazione

Ricercare la fonte di prova, individuare dove il dato di possibile interesse è conservato.

Preview

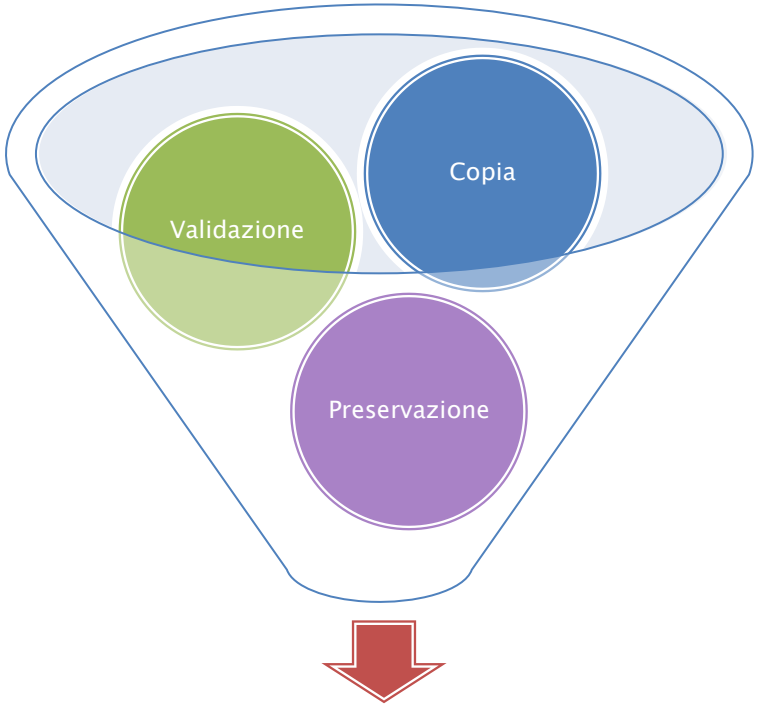
(Perquisizione informatica)

Nella puntata precedente…

Raccogliere i dati di possibile interesse investigativo unitamente ai dati che permettono la ricostruzione dell'evento probatorio.

Copia Forense

La Raccolta:
Copia Forense



Copia Forense

Legge n. 48 del 18/03/2008

art. 354 c.p.p.

(Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro)

2. […] In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità. […]

Copia Forense
Hash

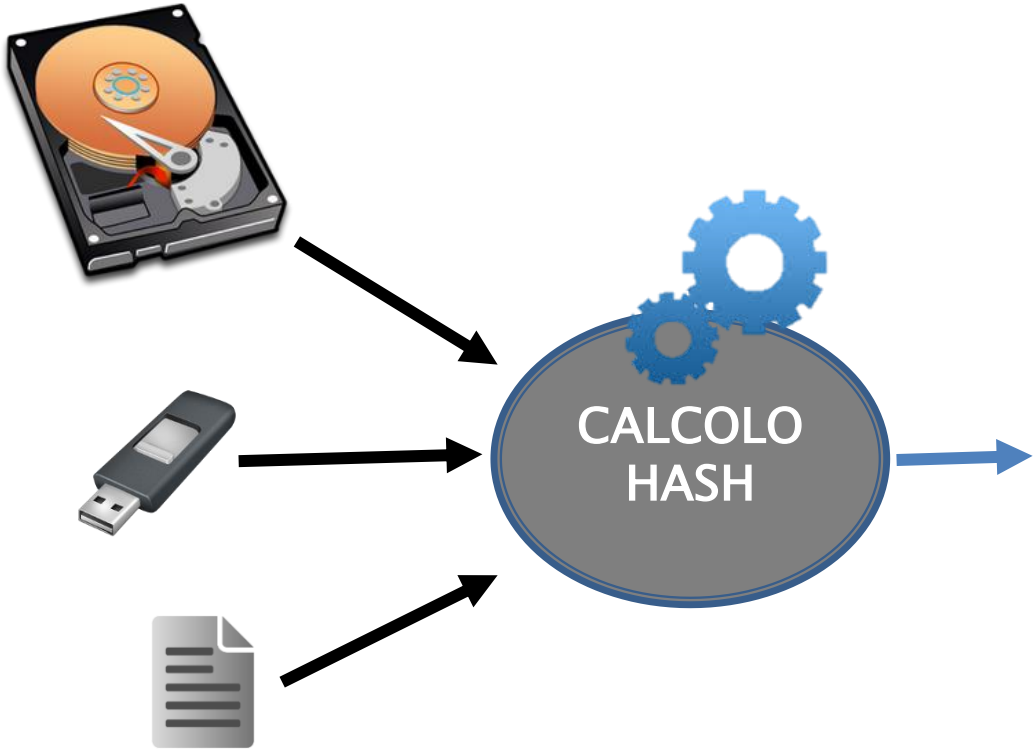
- L'algoritmo restituisce una stringa a lunghezza fissa di esadecimali a partire da un flusso di bit (dati) di dimensione qualsiasi.

- La stringa prodotta in output è univoca per ogni file e ne è un identificatore.

- L'algoritmo non è invertibile, ossia non è possibile ricostruire il dato originale a partire dalla stringa che viene restituita in output.

Copia Forense

Hash



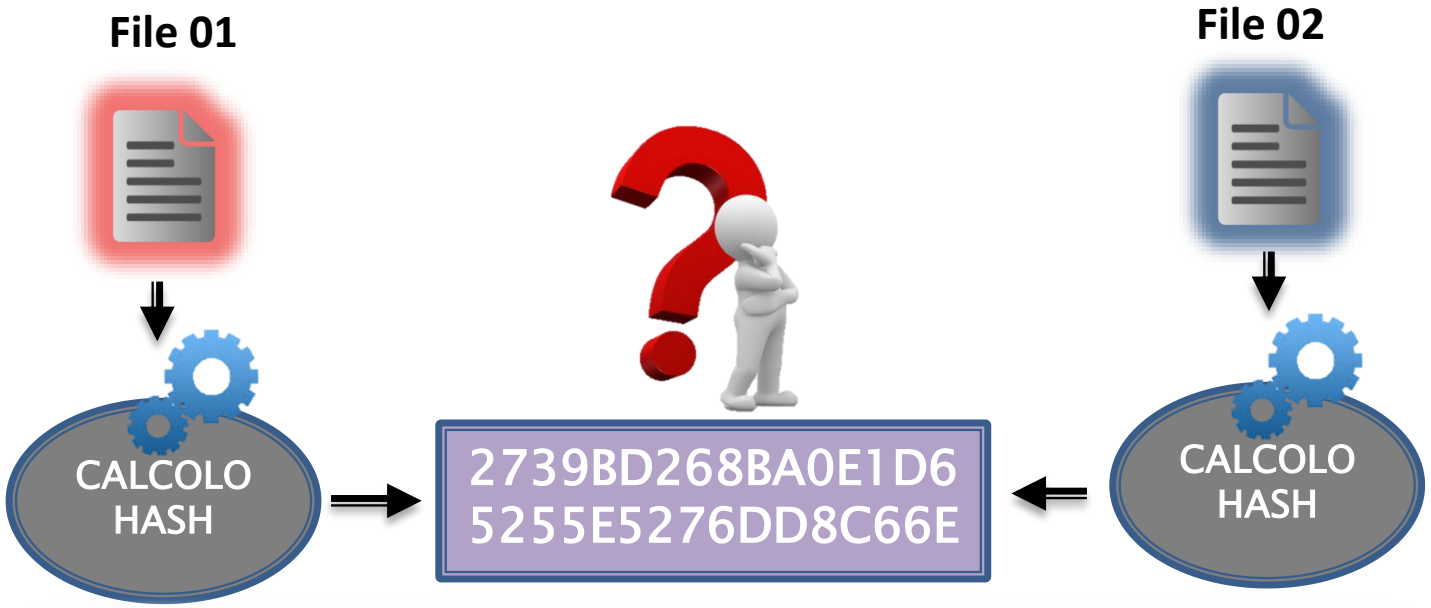
HASH 1:
12ADHG56CEEE3984
66PIZXXXK334F6GC3

HASH 2:
HHBN78FV54090934
346HHFC53JHCORUY

HASH 3:
2739BD268BA0E1D6
5255E5276DD8C66E

Copia Forense

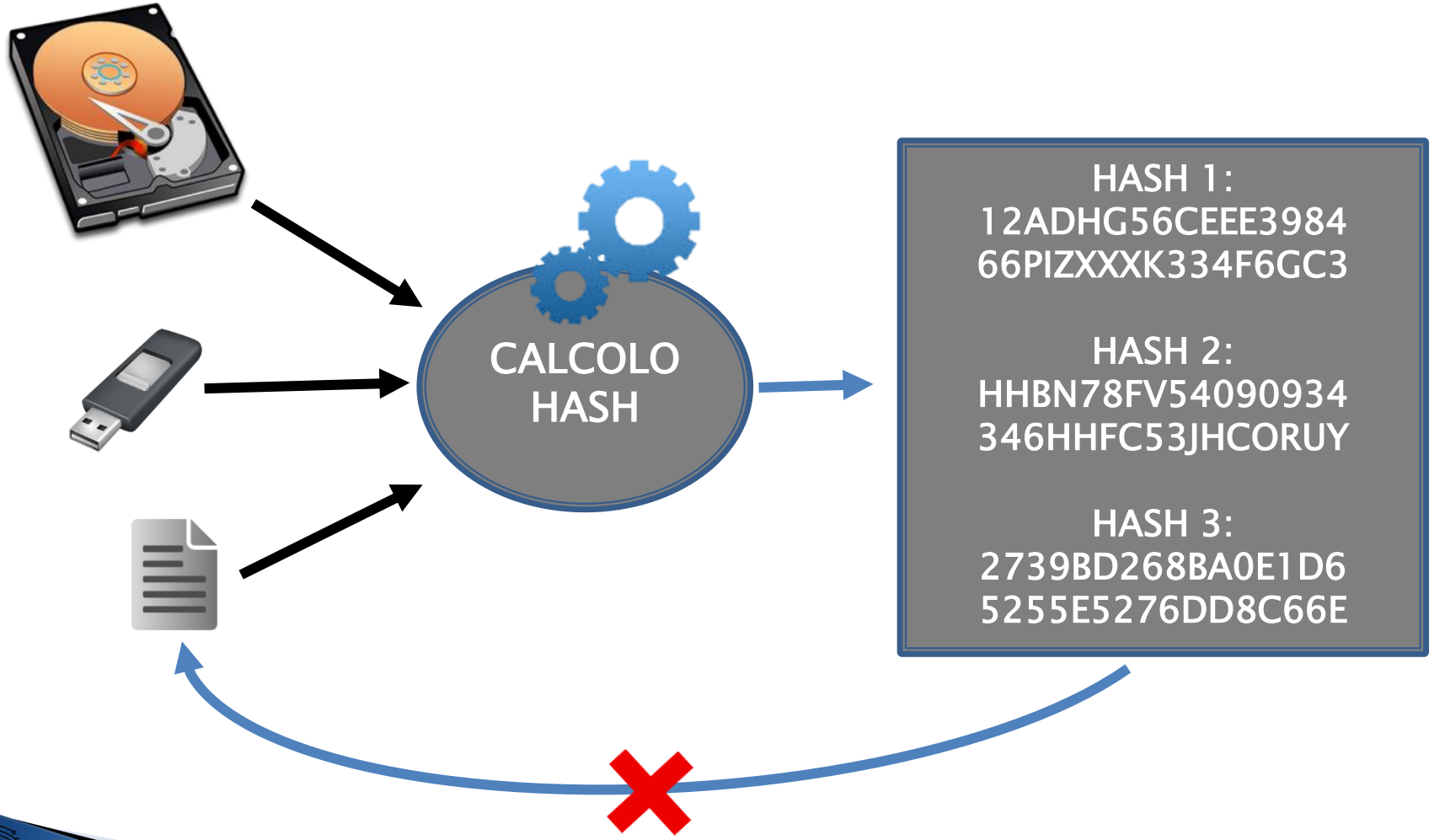
Hash



COLLISIONE

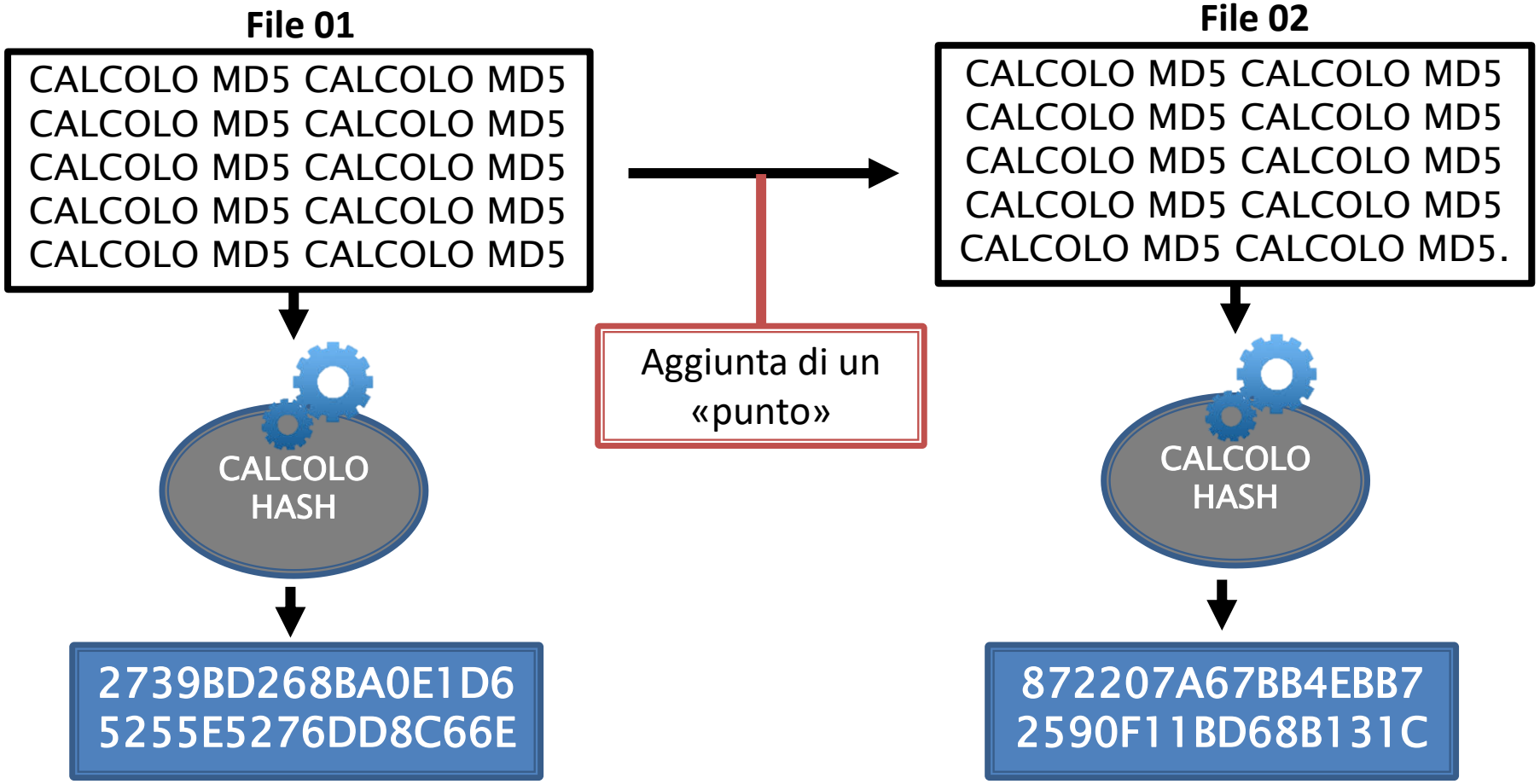
Copia Forense

Hash



Copia Forense

Hash

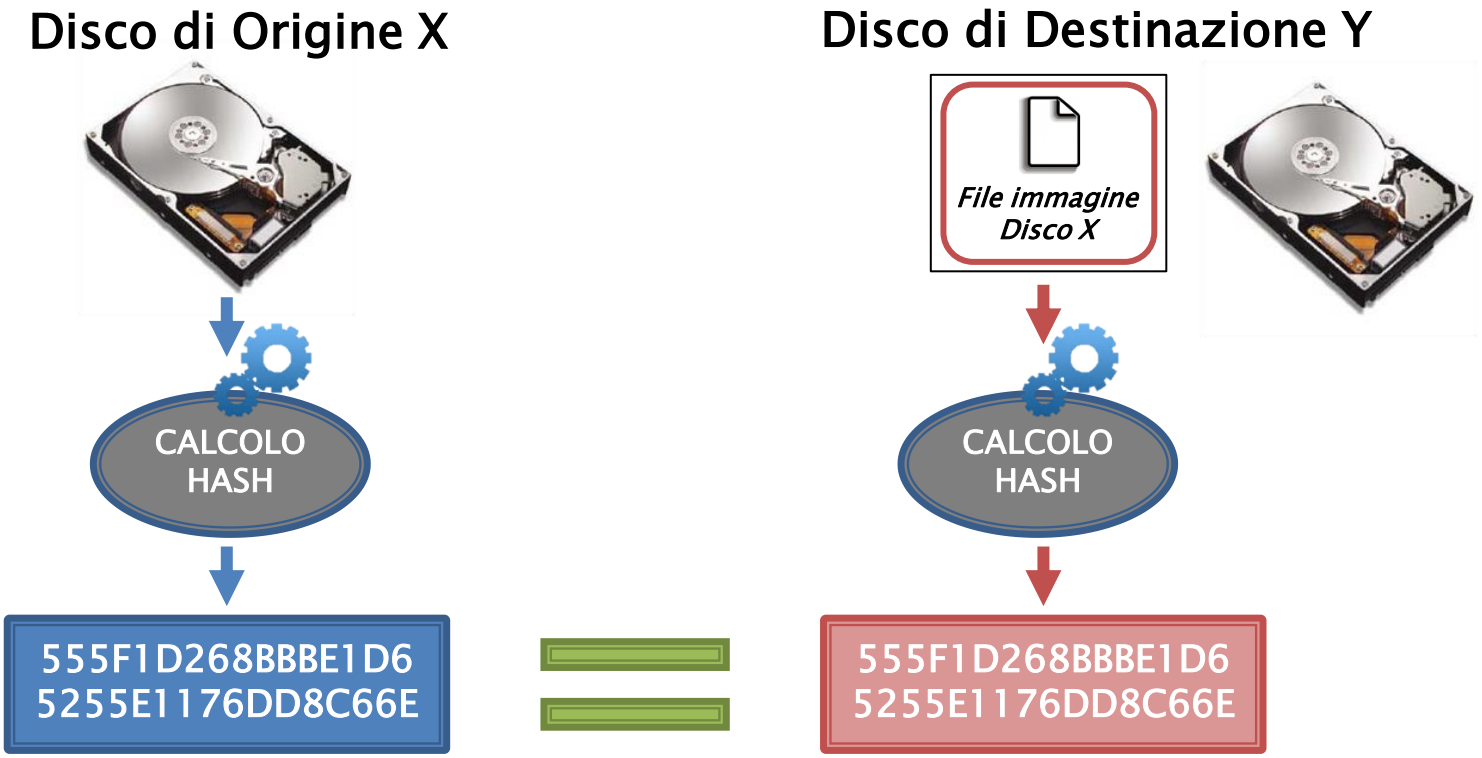


Fasi

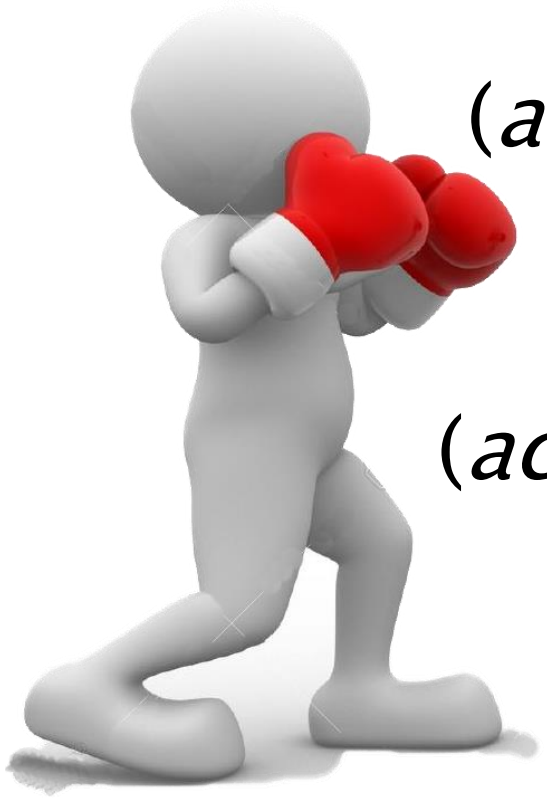
- Identificazione
- Raccolta
- **Validazione**
- Preservazione
- Analisi
- Interpretazione
- Documentazione
- Presentazione

Copia Forense
hash

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



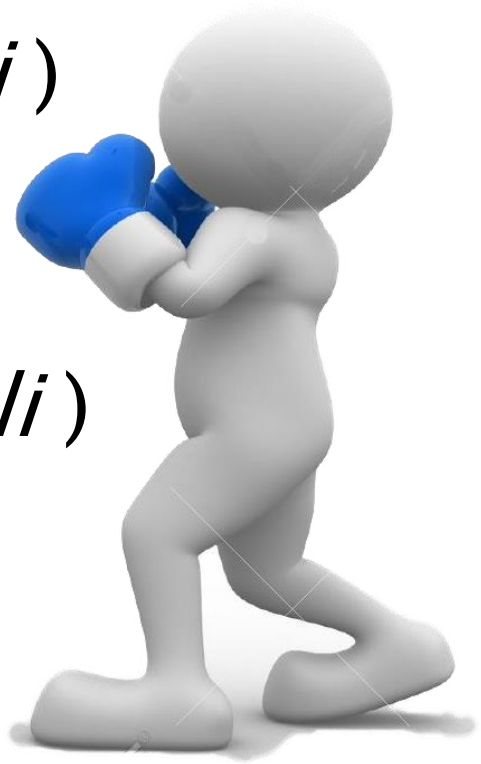
Copia Forense



Art. 359 c.p.p
(*accertamenti ripetibili*)

VS

Art. 360 c.p.p.
(*accertamenti irripetibili*)



Copia Forense

Art. 359 c.p.p

(*accertamenti ripetibili*)

**Sempre disponibile*

Copia Forense 1 — *Hash* → 872207A67BB4EBB7 2590F11BD68B131C

=

Copia Forense 2 — *Hash* → 872207A67BB4EBB7 2590F11BD68B131C

. . .

=

Copia Forense N — *Hash* → 872207A67BB4EBB7 2590F11BD68B131C

Memorie di massa in buono stato

Copia Forense

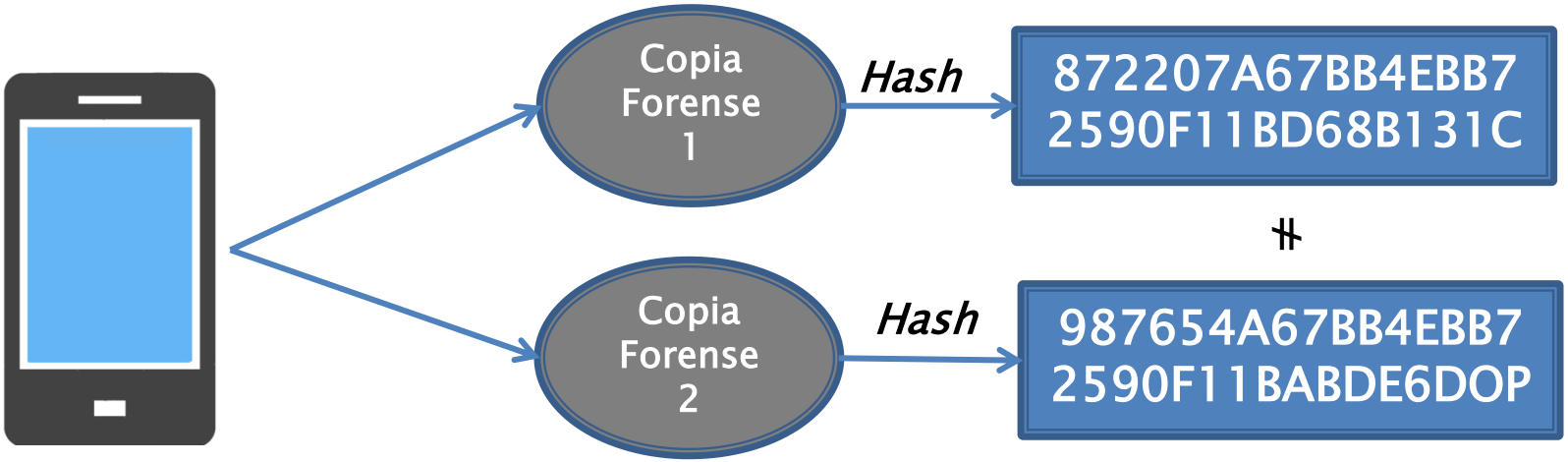
Art. 360 c.p.p
(*accertamenti irripetibili*)

- Memorie di massa non in buono stato;
- Live Acquisition: il sistema operativo del dispositivo deve essere avviato per poter realizzare la copia forense (*Es.: dispositivi cellullare, server, etc.*);
- Cloud (Acquisizione remota);
- Dispositivo di origine non disponibile nel tempo (*Es.: dissequestro, restituzione, etc.*);

Copia Forense

Art. 360 c.p.p

(*accertamenti irripetibili*)



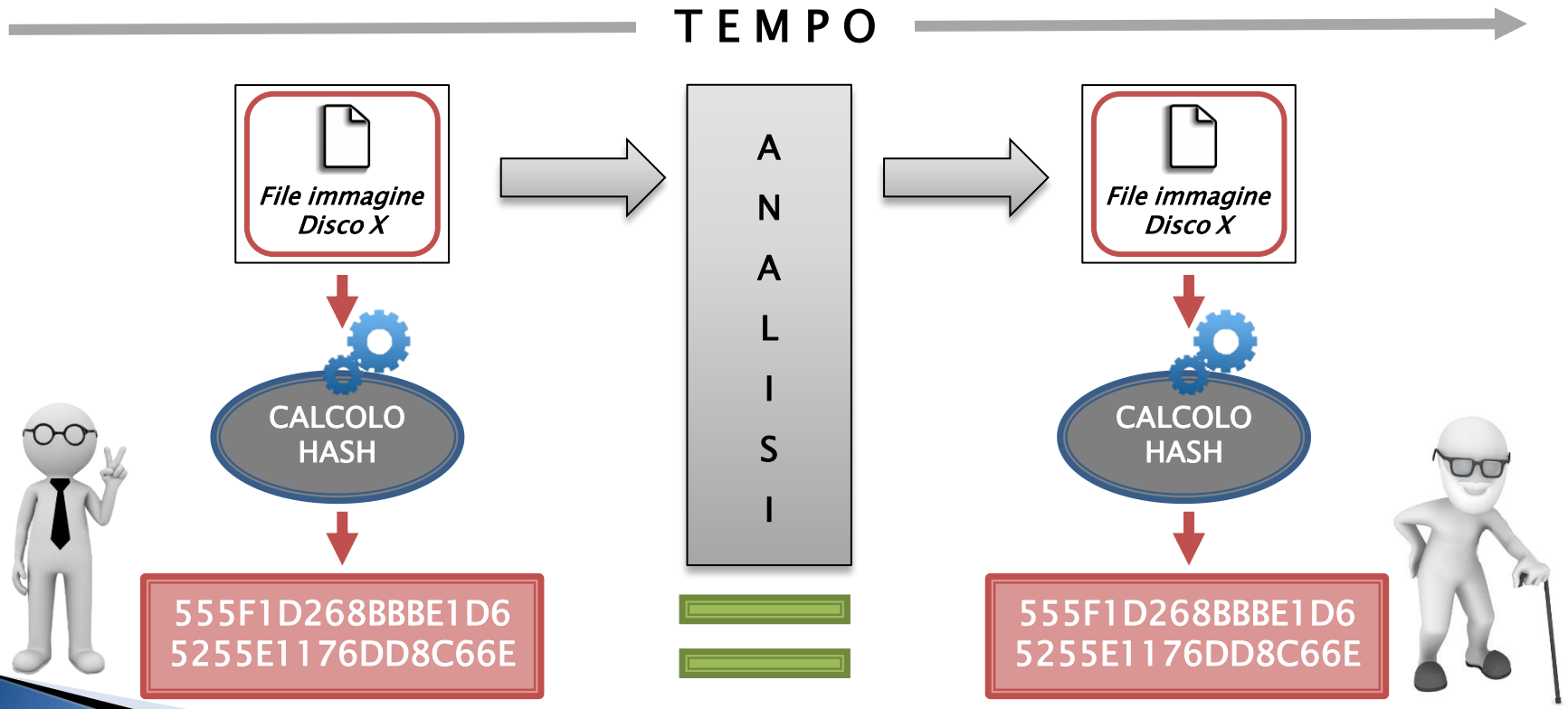
Fasi

- Identificazione
- Raccolta
- Validazione
- **Preservazione**
- Analisi
- Interpretazione
- Documentazione
- Presentazione

Copia Forense

hash

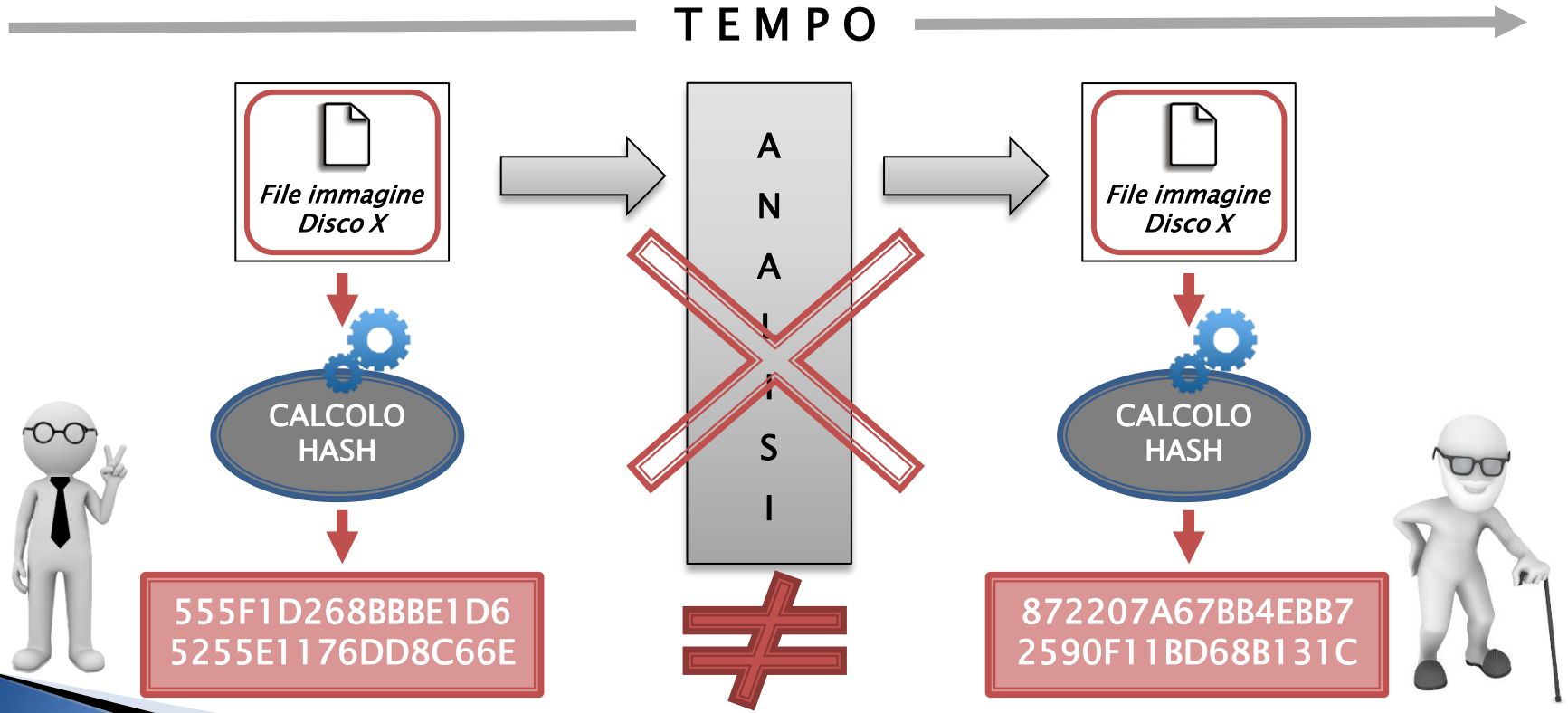
- **Preservazione**: garantisce che non vengano eseguite modifiche\alterazioni alla copia forense, se ciò avviene l'hash cambierà



Copia Forense

hash

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



Copia Forense

Copia Forense del «Disco Origine»

- PC_OLI.E01
- PC_OLI.E02
- PC_OLI.E03
- PC_OLI.E04
- PC_OLI.E05
- PC_OLI.E06
- PC_OLI.E07
- PC_OLI.E08
- PC_OLI.E09
- PC_OLI.E10
- PC_OLI.E11
- PC_OLI.E12
- PC_OLI.E13
- PC_OLI.E14
- PC_OLI.E15
- PC_OLI.E16
- PC_OLI.LOG

Immagine (*formato E01*) diviso in 16 file del «Disco Origine»

File LOG della realizzazione della copia forense

Copia Forense
File LOG

- File descrittivo in cui sono presenti le informazioni sulla copia forense realizzata:
  - Informazioni sullo strumento impiegato: *nome, versione, etc.*
  - Informazioni del disco di origine: *modello, capacità, S/N, etc.*
  - Informazioni dell'immagine forense: *nr. di file, dimensioni, etc.*
  - Altre informazioni: *data e ora, nr. di settori saltati, etc.*
  - ➢ **HASH**: *MD5, SHA1, SH256, SHA512, etc.*

Copia Forense

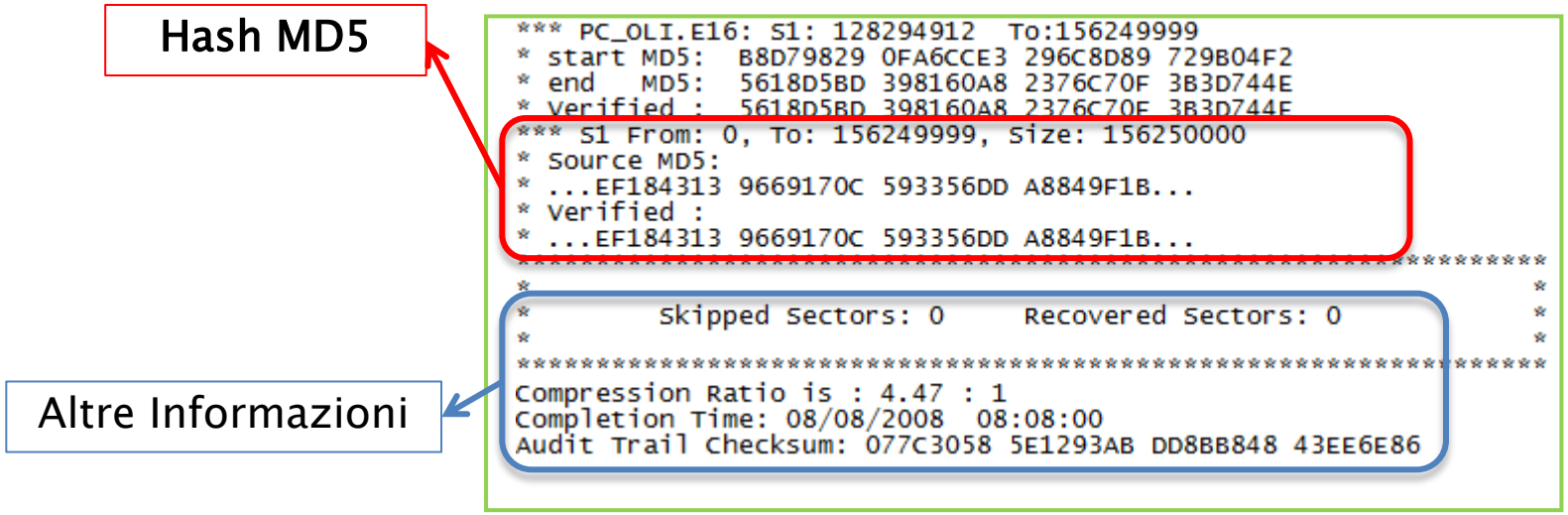
File LOG

Nome e Versione dello strumento

Informazioni del «disco sorgente»

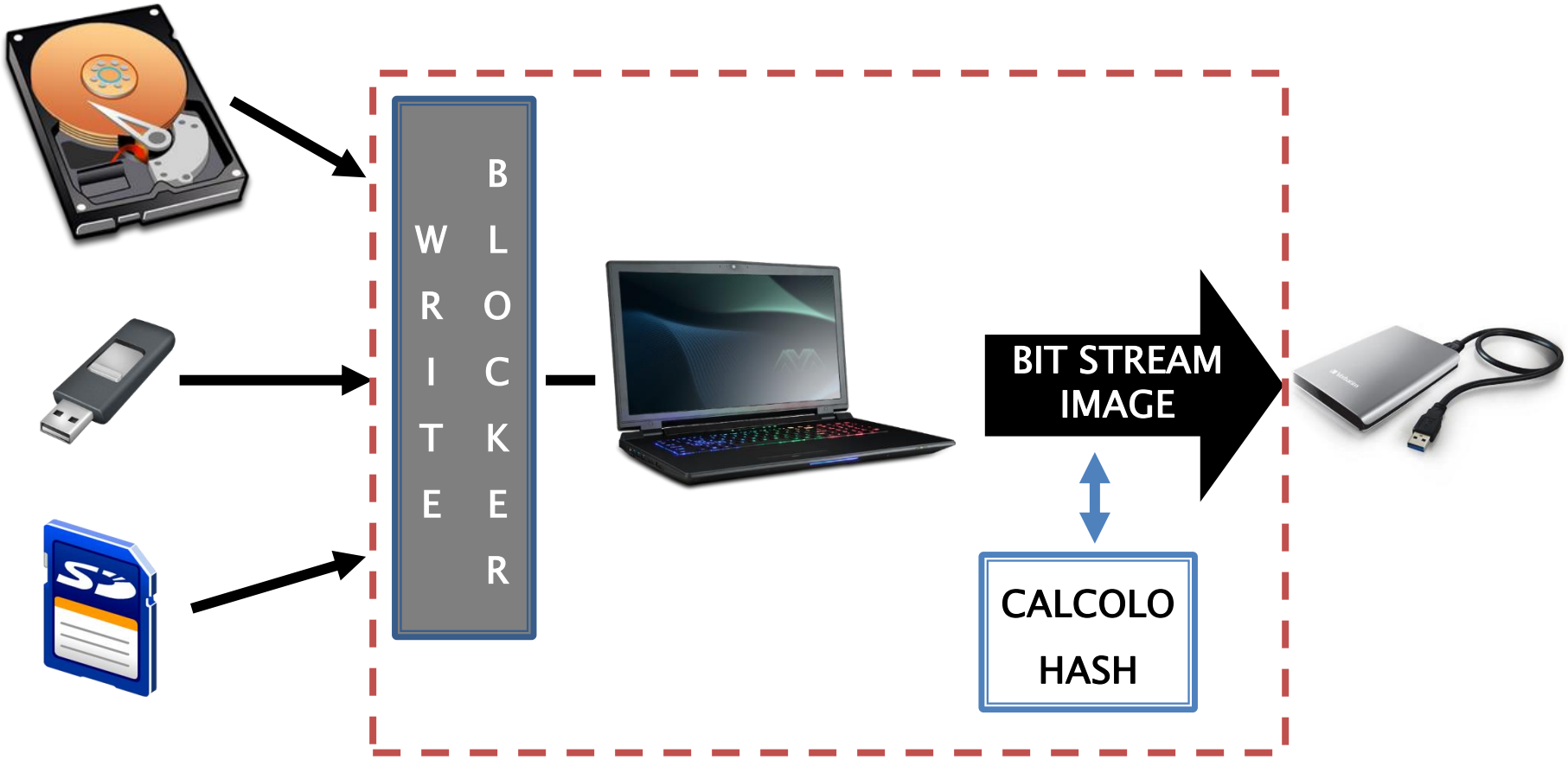
```
*** Forensic Dossier      --  Serial No.:78265 --                    *****
*  Software: V3.3.3RC16     Firmware: V1.14.2 fs:NTFS                    *
*                                                                        *
* Acquired by_____________________ Location _____________________       *
*                                                                        *
* Acquired on_____________________________ AT_____________________      *
************************ SESSION SETTINGS ************************
* Operating Mode: 4G E01:S2=>D2              Address Mode: LBA     *
* Verify        : Hash-Dsk+V                 Speed    :    UDMA-5 *
* Connection    : Direct                                           *
*                                                                  *
*                                                                  *
*              E01 CAPTURE OF S2 HAS BEEN ACHIEVED.                *
*                                                                  *
******* SOURCE DRIVE(S) ************** DESTINATION DRIVE(S) ******
*              S1                    |            D1               *
* Model : ST380815AS                 | Model : ST2000DM008-2FR102  *
* Serial: 5RW2FPXX                   | Serial: WFL1C8EV            *
*                                    |                             *
* C: 155009  H:  16    S: 63         | C: 3876021H: 16    S: 63    *
* Total Sectors   Drive Size         | Total Sectors   Drive Size  *
*    156250000     74.0GB            |    3907029168    1863.0GB   *
*                                    |                             *
********************************************************************
*** PC_OLI.E01: S1: 0  To:8667135
* start MD5:  67452301 EFCDAB89 98BADCFE 10325476
* end   MD5:  A18B0EE6 C7E71924 EEA6B83F 88ADF742
* Verified :  A18B0EE6 C7E71924 EEA6B83F 88ADF742
*** PC_OLI.E02: S1: 8667136  To:18759679
* start MD5:  A18B0EE6 C7E71924 EEA6B83F 88ADF742
* end   MD5:  DEB75F20 10AA171F 9B05B385 AF4EEC01
* Verified :  DEB75F20 10AA171F 9B05B385 AF4EEC01
*** PC_OLI.E03: S1: 18759680  To:27312127
* start MD5:  DEB75F20 10AA171F 9B05B385 AF4EEC01
* end   MD5:  46FA2898 B2528064 2BB26D4D B9E6F5EF
* Verified :  46FA2898 B2528064 2BB26D4D B9E6F5EF
```

Copia Forense
File LOG



Copia Forense

riepilogando…



Copia Forense

- Comandi

Copia Forense
comando «*DD*»

- È presente nella gran parte di tutte le distribuzioni UNIX Like

```
DD(1)                                                User Commands

NAME
       dd - convert and copy a file

SYNOPSIS
       dd [OPERAND]...
       dd OPTION
```

Copia Forense
comando «*DD*»

/dev

tutti i file al suo interno rappresentano dispositivi:

- **Character device:** dispositivi che trasmettono/trasferiscono dati
  - *dsp[0]: dispositivo audio*
  - *lp[0]: porta parallela*

- **Block device:** dispositivi che memorizzano/conservano dati
  - *hd[a]: hard disk ide*
  - *sd[a]: hard disk scsi, memory stick, memory card, etc.*

Copia Forense
comando «*DD*»

- Lista dei dispositivi agganciati:

```
root@caine:/# fdisk-l

Disk /dev/sda: 4 GiB, 4294967296 bytes, 8388608 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x72a3c36c

Device     Boot   Start     End Sectors Size Id Type
/dev/sda1          2048 2099199 2097152   1G  b W95 FAT32
/dev/sda2       2099200 8388607 6289408   3G  b W95 FAT32



Disk /dev/sdb: 20 GiB, 21474836480 bytes, 41943040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

Disco target

Copia Forense
comando «*DD*»

- Lista dei dispositivi agganciati:

```
Disk /dev/sdc: 8 GiB, 8589934592 bytes, 16777216 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x9a847d68

Device     Boot Start      End  Sectors Size Id Type
/dev/sdc1        2048 16777215 16775168   8G  7 HPFS/NTFS/exFAT
```

Disco di destinazione

Copia Forense
comando «*DD*»

- Prepariamo il nostro disco di destinazione della copia forense:

```
root@caine:/# mkdir /mnt/dest
root@caine:/# mount /dev/sdc1 /mnt/dest/
root@caine:/# mkdir /mnt/dest/dd_image
```

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)

Copia Forense
comando «*DD*»

- Risultato della copia forense

```
root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda.dd bs=2048 conv=noerror,sync
2097152+0 records in
2097152+0 records out
4294967296 bytes (4,3 GB, 4,0 GiB) copied, 302,094 s, 14,2 MB/s


root@caine:/# ls -l /mnt/dest/dd_image/
total 4194304
-rwxrwxrwx 1 root root 4294967296 apr  7 23:26 sda.dd
```

Copia Forense
comando «*DD*»

- Comandi avanzati:

SKIP = *[n]* salta la lettura del numero «**n**» di blocchi di memoria, partendo dall'inizio

COUNT= *[n]* indica all'elaborazione di terminare dopo aver letto il numero «n» di blocchi di memoria

Copia Forense
comando «*DD*»

- Acquisire una sola partizione

```
Disk /dev/sda: 4 GiB, 4294967296 bytes, 8388608 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x72a3c36c
Device     Boot   Start     End Sectors Size Id Type
/dev/sda1          2048 2099199 2097152   1G  b W95 FAT32
/dev/sda2       2099200 8388607 6289408   3G  b W95 FAT32


root@caine:/# dd if=/dev/sda2 of=/mnt/dest/dd_image/sda_p2.dd bs=2048
572352+0 records in
1572352+0 records out
3220176896 bytes (3,2 GB, 3,0 GiB) copied, 238,845 s, 13,5 MB/s


root@caine:/# ls -l /mnt/dest/dd_image/
total 3144704
-rwxrwxrwx 1 root root 3220176896 apr  7 23:36 sda_p2.dd
```

Copia Forense
comando «*DD*»

- Acquisire una sola partizione

```
root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda_p2.dd skip=2099199 count=6289408
6289408+0 records in
6289408+0 records out
3220176896 bytes (3,2 GB, 3,0 GiB) copied, 764,928 s, 4,2 MB/s

root@caine:/# ls -l /mnt/dest/dd_image/
total 3144704
-rwxrwxrwx 1 root root 3220176896 apr  7 23:55 sda_p2.dd
```

Copia Forense
comando «*DD*»

- Dividere il file immagine:

Blocchi da 1GB (1024 Byte x 1.000.000)

```
root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda.000 bs=1024 count=1000000
1000000+0 records in
1000000+0 records out
1024000000 bytes (1,0 GB, 977 MiB) copied, 200,268 s, 5,1 MB/s


root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda.001 bs=1024 skip=1000000
              count=1000000
1000000+0 records in
1000000+0 records out
1024000000 bytes (1,0 GB, 977 MiB) copied, 226,651 s, 4,5 MB/s

root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda.002 bs=1024 skip=2000000
              count=1000000
1000000+0 records in
1000000+0 records out
1024000000 bytes (1,0 GB, 977 MiB) copied, 213,783 s, 4,8 MB/s
```

Copia Forense
comando «*DD*»

```
root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda.003 bs=1024 skip=3000000
              count=1000000
1000000+0 records in
1000000+0 records out
1024000000 bytes (1,0 GB, 977 MiB) copied, 220,863 s, 4,6 MB/s

root@caine:/# dd if=/dev/sda of=/mnt/dest/dd_image/sda.004 bs=1024 skip=4000000
194304+0 records in
194304+0 records out
198967296 bytes (194,3 MB, 185 MiB) copied, 220,863 s, 3,7 MB/s

root@caine:/# ls -l /mnt/dest/dd_image/
total 4194304
-rwxrwxrwx 1 root root 1024000000 apr  8 00:03 sda.000
-rwxrwxrwx 1 root root 1024000000 apr  8 00:04 sda.001
-rwxrwxrwx 1 root root 1024000000 apr  8 00:04 sda.002
-rwxrwxrwx 1 root root 1024000000 apr  8 00:05 sda.003
-rwxrwxrwx 1 root root 1024000000 apr  8 00:06 sda.004
```

Copia Forense
comando «*DD*»

- Dividere il file immagine:

```
root@caine:/# dd if=/dev/sda bs=2048 | split -d -b 2G - mnt/dest/dd_image/sda.
```

- **SPLIT**
  - **-D** = indica di appendere al nome del file un contatore decimale [*sda.00*]
  - **-B** = *[n/n(K/M/G/T/P/E/Z/Y)]* specifica la dimensione massima di ciascuna parte *[2GB]*

```
2097152+0 records in
2097152+0 records out
4294967296 bytes (4,3 GB, 4,0 GiB) copied, 157,836 s, 27,2 MB/s
root@caine:/# ls -l /mnt/dest/dd_image/
total 4194304
-rwxrwxrwx 1 root root 2147483648 apr  8 00:12 sda.00
-rwxrwxrwx 1 root root 2147483648 apr  8 00:13 sda.01
```

Copia Forense
comando «*DD*»

Calcolare l'Hash

- Metodo nr. 1:
  - Calcoliamo l'hash del dispositivo sorgente «**sda**» e lo memorizziamo in un file «**sda_orig.hash**»

```
root@caine:/# md5sum /dev/sda > /mnt/dest/dd_image/sda_orig.hash
root@caine:/# cat /mnt/dest/dd_image/sda_orig.hash
d7a09df1018710f2b40744ba62445c7b  /dev/sda
```

  - Calcoliamo l'hash dell'immagine «**sda.dd**» ottenuta in precedenza ed anche esso lo memorizziamo all'interno di un file «**sda_dd.hash**»

```
root@caine:/# md5sum /mnt/dest/dd_image/sda.dd > /mnt/dest/dd_image/sda_dd.hash
root@caine:/# cat /mnt/dest/dd_image/sda_dd.hash
d7a09df1018710f2b40744ba62445c7b  /mnt/dest/dd_image/sda.dd
```

Copia Forense
comando «*DD*»

Calcolare l'Hash

- Oppure se la nostra immagine è divisa in più file, dovremo adoperare **CAT**:

```
root@caine:/# cat /mnt/dest/dd_image/sda.* | md5sum >> /mnt/dest/dd_image/sda_merge.hash
root@caine:/# cat /mnt/dest/dd_image/sda_merge.hash
d7a09df1018710f2b40744ba62445c7b  -
```

Hash dispositivo di origine = Hash file immagine
(*to match*)

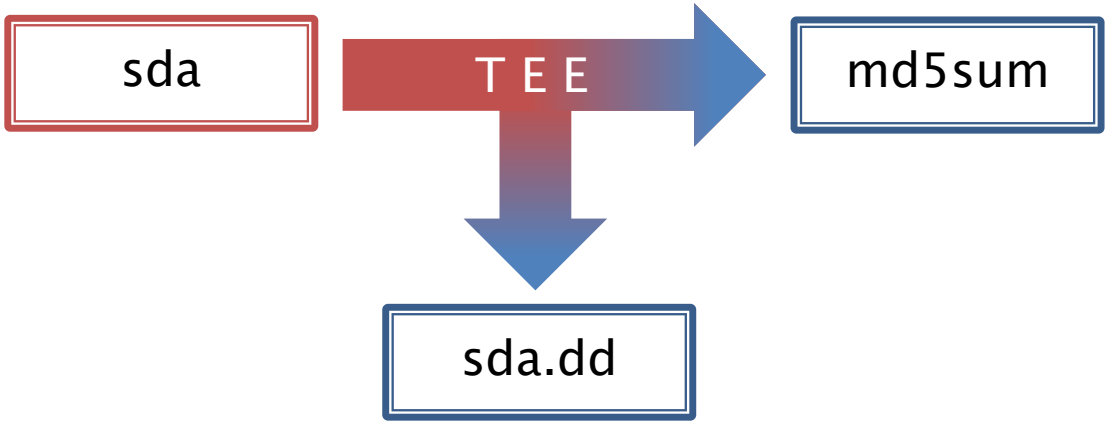
Copia Forense
comando «*DD*»

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»]



Copia Forense
comando «*DD*»

Calcolare l'Hash

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

root@caine:/# ls -l /mnt/dest/dd_image/
total 4194305
-rwxrwxrwx 1 root root 4294967296 apr  8 00:56 sda.dd
-rwxrwxrwx 1 root root         36 apr  8 00:56 sda.hash

root@caine:/# cat /mnt/dest/dd_image/sda.hash
d7a09df1018710f2b40744ba62445c7b  -
```

Copia Forense
comando «*DC3DD*»

- Patch del comando DD

```
root@caine:/# dc3dd if=/dev/sda ofs=/mnt/dest/dd_image/sda.000 ofsz=2G bufsz=2k hash=md5
hash=sha256 log=/mnt/dest/dd_image/sda.log verb=on
```

OFS = output diviso in più file *[file immagine «**sda.000**»]*

OFSZ = dimensione massima di ogni file [2 GB]

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

HASH = [MD5|SHA1|SHA256|SHA512] calcola dell'Hash indicato [***MD5 e SHA256***]

LOG = salva il report dell'elaborazione in un file [***sda.log***]

VERB=ON indica di generare un report dettagliato (verbose)

Copia Forense
comando «*DC3DD*»

```
root@caine:/# dc3dd if=/dev/sda ofs=/mnt/dest/dd_image/sda.000 ofsz=2G bufsz=2k hash=md5
hash=sha256 log=/mnt/dest/dd_image/sda.log verb=on

dc3dd 7.2.646 started at 2020-04-08 01:07:42 +0200
compiled options:command line: dc3dd if=/dev/sda ofs=/mnt/dest/dd_image/sda.000 ofsz=2G
bufsz=2k hash=md5 hash=sha256 log=/mnt/dest/dd_image/sda.log verb=on
device size: 8388608 sectors (probed),    4,294,967,296 bytes
sector size: 512 bytes (probed)
  4294967296 bytes ( 4 G ) copied ( 100% ),  959 s, 4,3 M/s

input results for device `/dev/sda':
   8388608 sectors in
   0 bad sectors replaced by zeros
   d7a09df1018710f2b40744ba62445c7b (md5)
   f4d40a9fc0979b1dce6c9f45cf3fedc1f9d6fea23725511356d8fb1b99b7ef3a (sha256)

output results for files `/mnt/dest/dd_image/sda.000':
   8388608 sectors out
      4194304 sectors out to `/mnt/dest/dd_image/sda.000‘
      4194304 sectors out to `/mnt/dest/dd_image/sda.001‘
dc3dd completed at 2020-04-08 01:23:41 +0200
```

Copia Forense
comando «*DC3DD*»

```
root@caine:/# ls -l /mnt/dest/dd_image/
total 4194308
-rwxrwxrwx 1 root root 2147483648 apr  8 01:16 sda.000
-rwxrwxrwx 1 root root 2147483648 apr  8 01:23 sda.001
-rwxrwxrwx 1 root root        823 apr  8 01:23 sda.log
```

Copia Forense
comando «*DC3DD*»

- Comandi avanzati:

REC=OFF interrompe l'elaborazione in caso di un errore di lettura di un blocco di memoria

HOFS= l'output viene diviso in più file e per ciascuno di essi viene calcolato l'hash;

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