



# Corso di Digital Forensics

CdLM in Informatica

Università degli Studi di Salerno

Docente: Ugo Fiore

2 – Acquisizione dati

# Acquisizione dei Dati

## Caratteristiche e Concetti | 1/2

- La fase di *raccolta* (o *acquisizione*) del processo di **investigazione**, dovrebbe garantire le seguenti proprietà:
  - Affidabilità
  - Completezza
  - Accuratezza
  - Verificabilità

# Acquisizione dei Dati

## Caratteristiche e Concetti | 1/2

- La fase di *raccolta* (o *acquisizione*) del processo di investigazione, dovrebbe garantire le seguenti proprietà:
  - **Affidabilità**
    - Non devono esservi dubbi e/o perplessità in merito all'autenticità e sui risultati ottenuti
    - Completezza
    - Accuratezza
    - Verificabilità

# Acquisizione dei Dati

## Caratteristiche e Concetti | 1/2

- La fase di *raccolta* (o *acquisizione*) del processo di investigazione, dovrebbe garantire le seguenti proprietà:
  - Affidabilità
  - **Completezza**
    - Devono essere acquisite tutte le informazioni rilevanti, non solo quelle di una parte del caso
  - Accuratezza
  - Verificabilità

# Acquisizione dei Dati

## Caratteristiche e Concetti | 1/2

- La fase di *raccolta* (o *acquisizione*) del processo di investigazione, dovrebbe garantire le seguenti proprietà:
  - Affidabilità
  - Completezza
  - **Accuratezza**
    - Non devono essere presenti errori nella raccolta dei dati
  - Verificabilità

# Acquisizione dei Dati

## Caratteristiche e Concetti | 1/2

- La fase di *raccolta* (o *acquisizione*) del processo di investigazione, dovrebbe garantire le seguenti proprietà:
  - Affidabilità
  - Completezza
  - Accuratezza
  - **Verificabilità**
    - La metodologia deve essere chiara e riproducibile
    - Un altro investigatore dovrebbe essere in grado di arrivare allo stesso risultato, partendo dai medesimi dati

# Acquisizione dei Dati

## Caratteristiche e Concetti | 2/2

- L'acquisizione dei dati (**data acquisition**) è l'attività principale della fase di *raccolta* (o *acquisizione*) del **processo di investigazione**
- I dati rilevanti vengono **acquisiti**, da parte di un investigatore, principalmente da due fonti:
  - *Live Systems*
    - Nel caso ci si trovi in presenza di un *live system*, si considerano anche i *live data*, ad esempio, il contenuto della memoria RAM (*approfondimento nelle prossime lezioni*)
  - *Dead Systems*
    - Nell'acquisizione di dati da un *dead system*, deve essere effettuata una immagine forense, attenendosi scrupolosamente a passi ben stabiliti, in modo che l'acquisizione avvenga in maniera valida, dal punto di vista forense

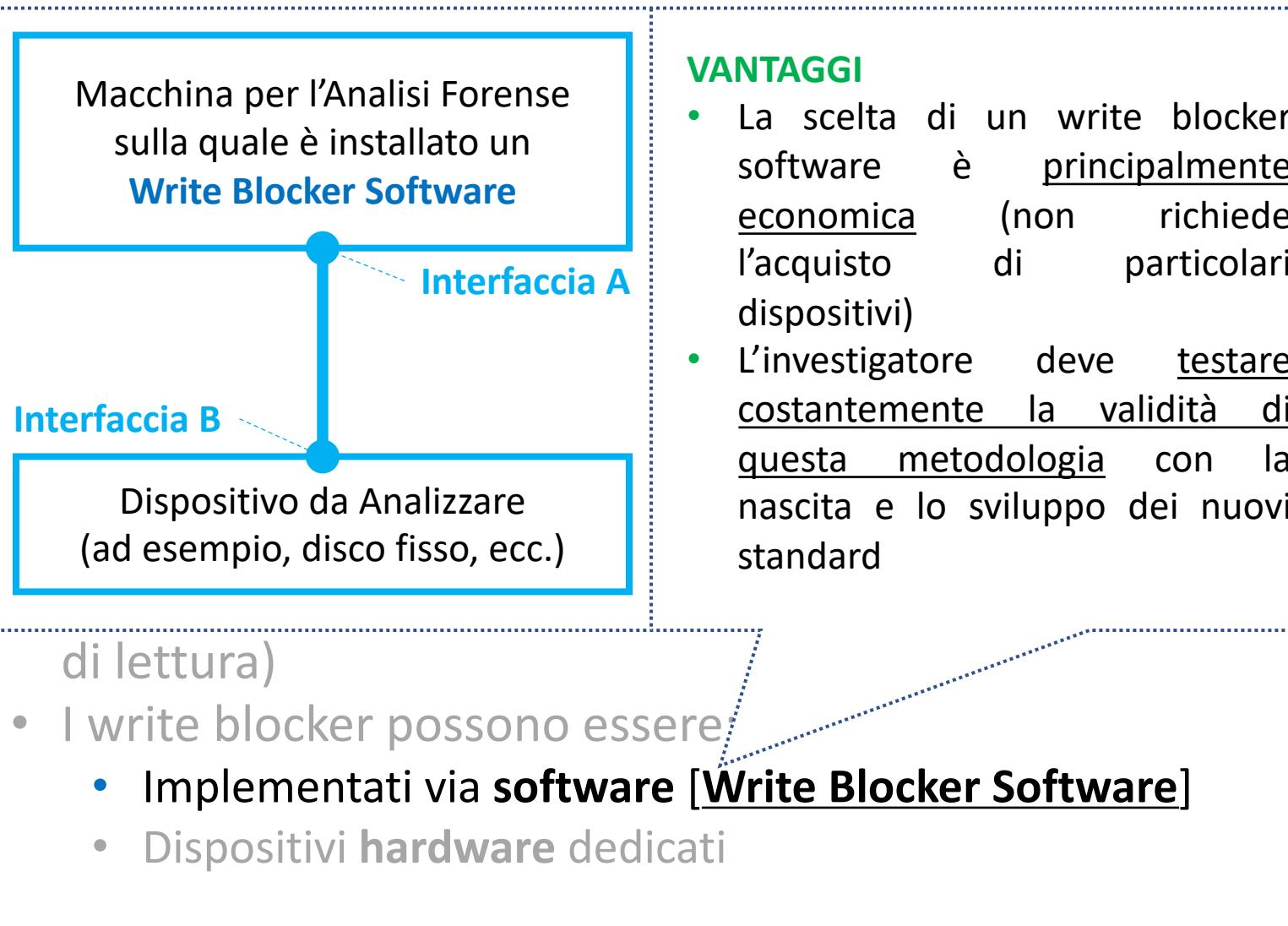
# Acquisizione dei Dati

## Bloccare le Scritture

- Le prove originali devono essere utilizzate esclusivamente per effettuare delle «copie esatte», sulle quali condurre l'analisi forense
- Per evitare che vi siano alterazioni dei dati, durante la creazione di una «copia esatta», è necessario utilizzare un **write blocker** (letteralmente: «*bloccatore*» di scritture)
- Un write blocker ha il compito di **evitare che vi siano scritture sui dati** (è possibile solo effettuare operazioni di lettura)
- I write blocker possono essere:
  - Implementati via **software**
  - Dispositivi **hardware** dedicati

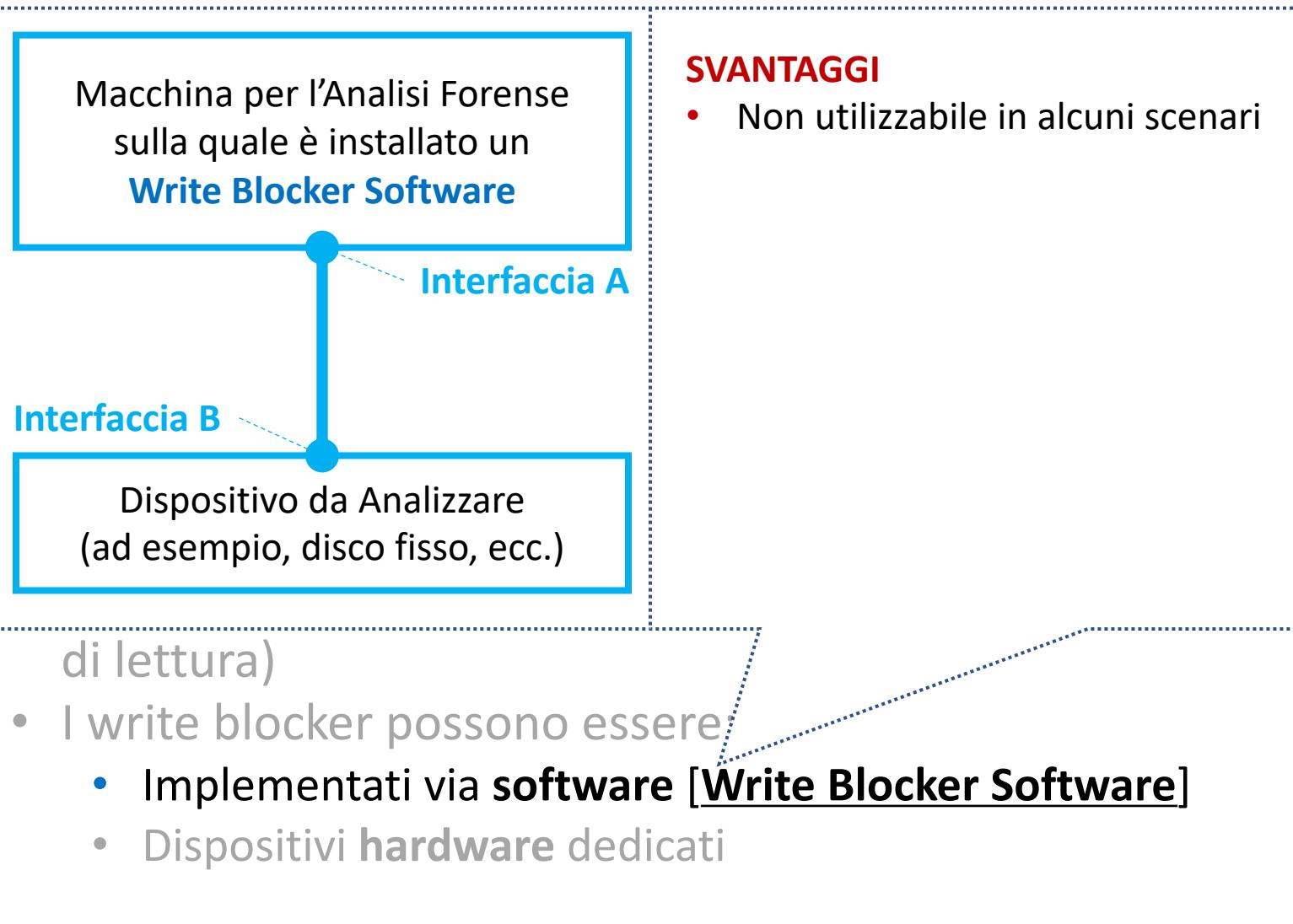
# Acquisizione dei Dati

## Bloccare le Scritture



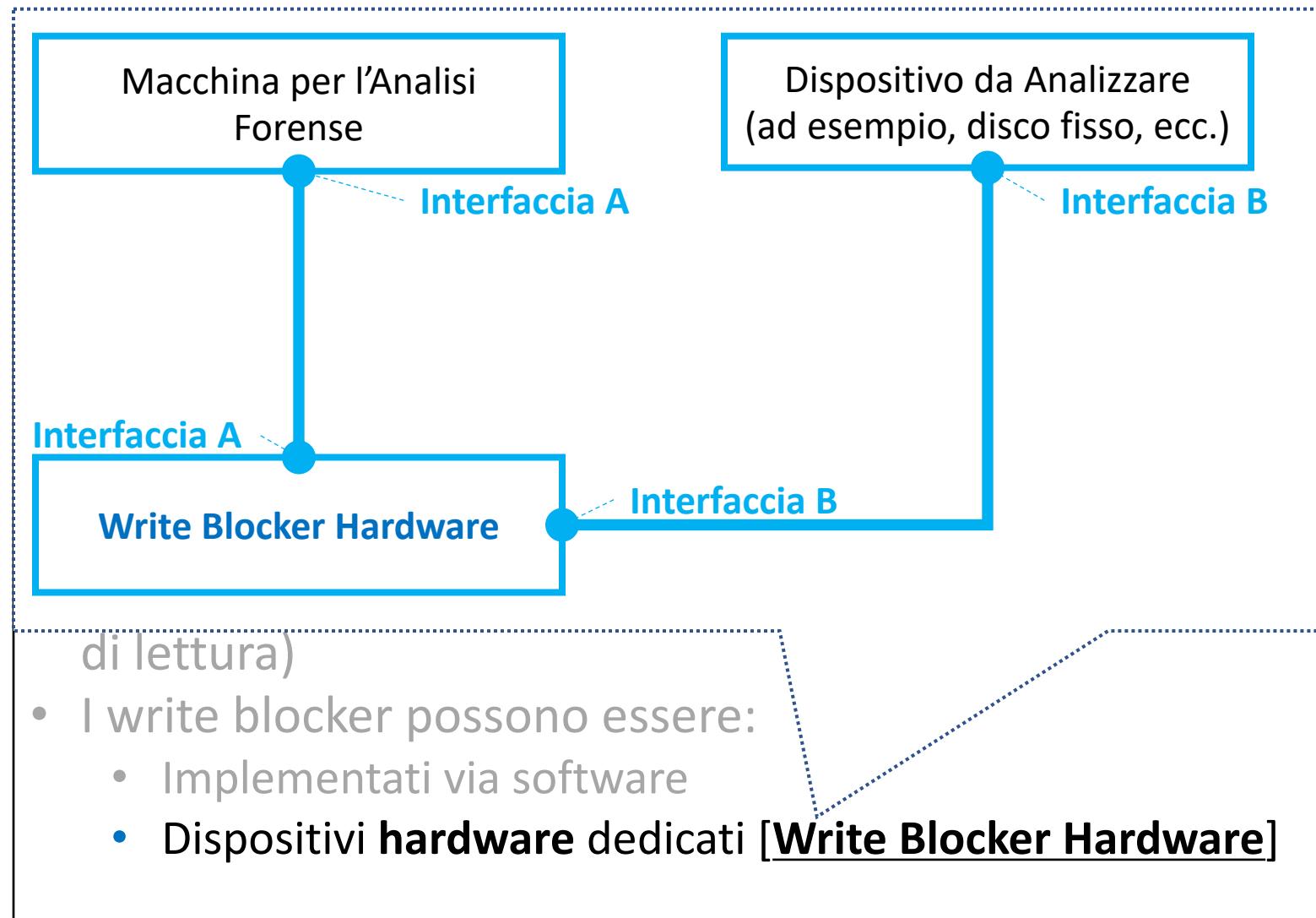
# Acquisizione dei Dati

## Bloccare le Scritture



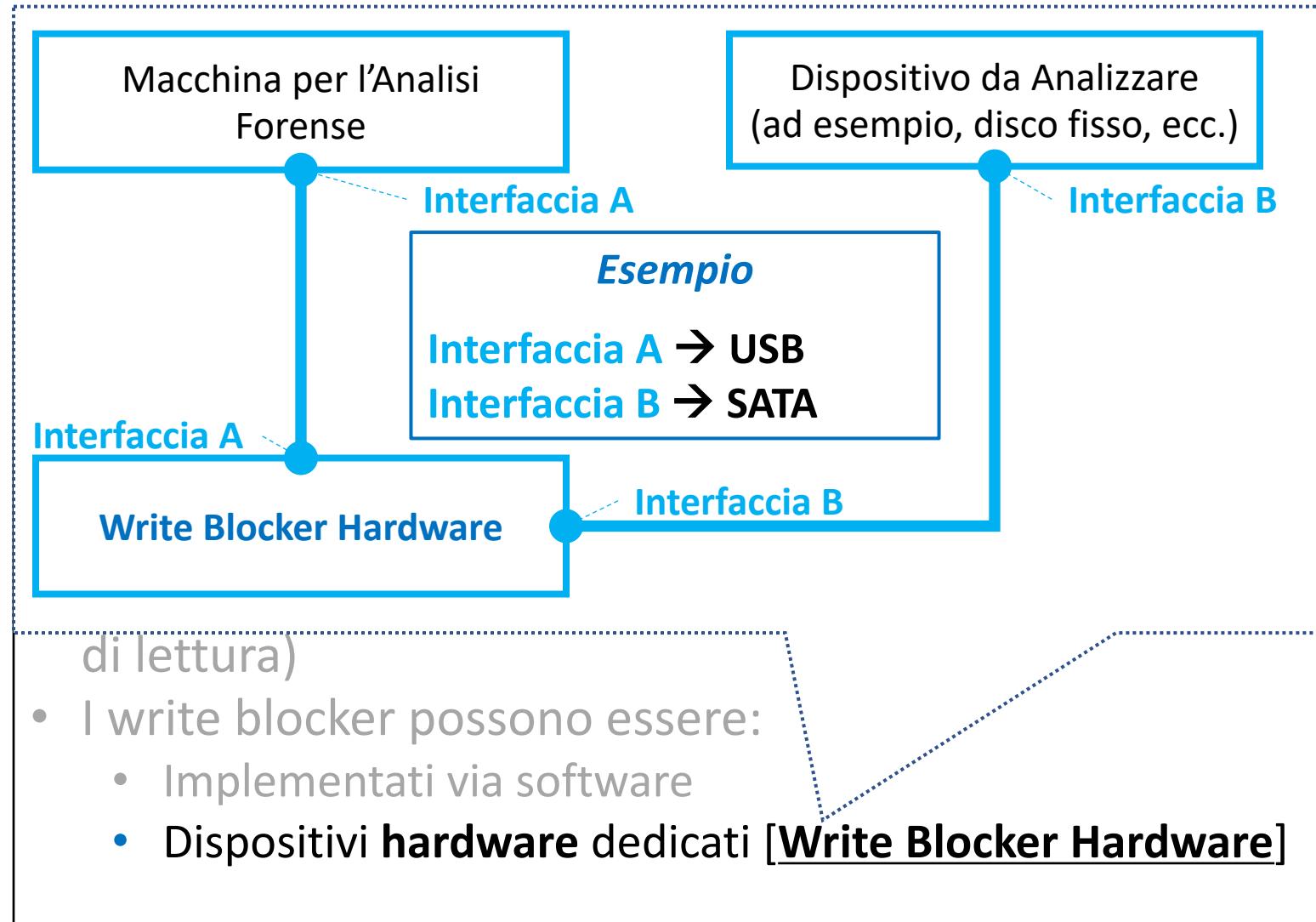
# Acquisizione dei Dati

## Bloccare le Scritture



# Acquisizione dei Dati

## Bloccare le Scritture



# Acquisizione dei Dati

## Bloccare le Scritture



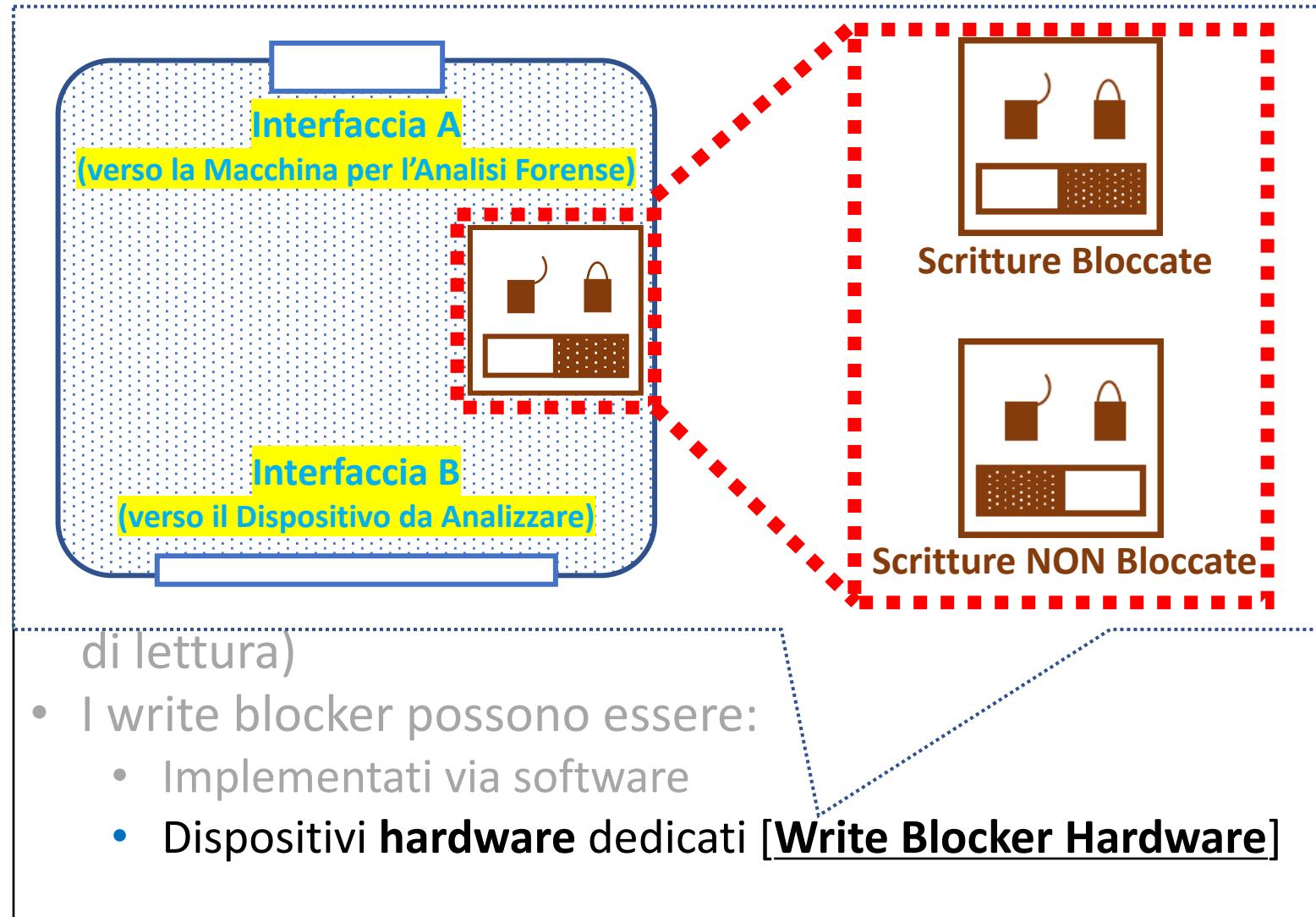
Esempio di **Write Blocker Hardware**, il quale collega una macchina per l'Analisi per Forense (**Interfaccia A**) ad un supporto da analizzare (**Interfaccia B**) e **può bloccarne le scritture** (eventualmente, le scritture possono essere bloccate o meno, a seconda del modello, tramite un **interruttore**, come nell'esempio)

di lettura)

- I write blocker possono essere:
  - Implementati via software
  - Dispositivi **hardware** dedicati [**Write Blocker Hardware**]

# Acquisizione dei Dati

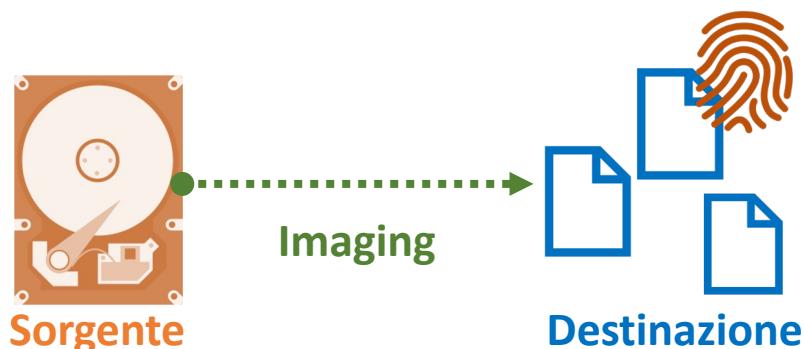
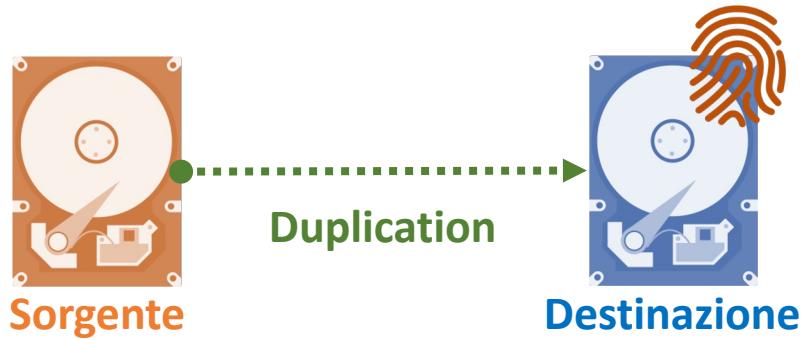
## Bloccare le Scritture



# Acquisizione dei Dati

## Immagini Forensi e Hash | 1/9

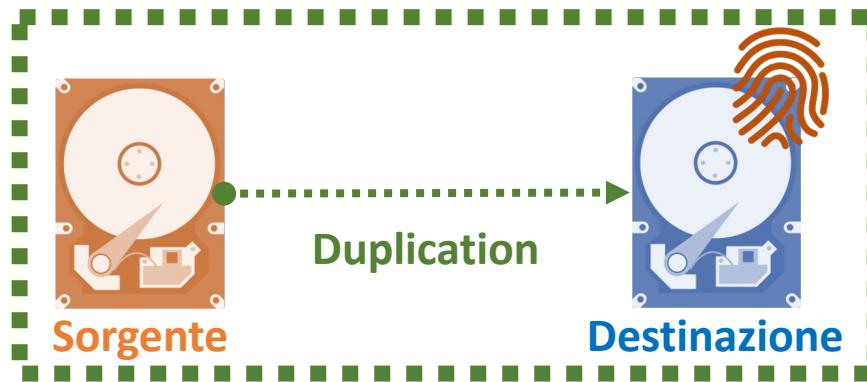
- Per la creazione di una «copia esatta» di un disco fisso (o un altro tipo di supporto di memorizzazione), sono possibili due opzioni:



# Acquisizione dei Dati

## Immagini Forensi e Hash | 2/9

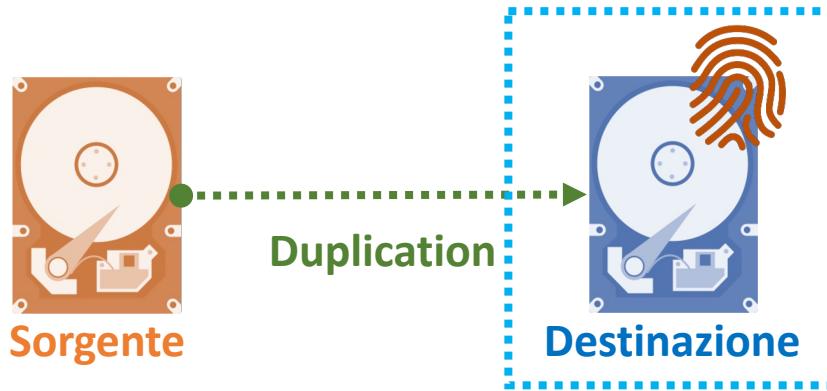
- Per la creazione di una «copia esatta» di un disco fisso (o un altro tipo di supporto di memorizzazione), sono possibili due opzioni:



# Acquisizione dei Dati

## Immagini Forensi e Hash | 3/9

- Con il processo di **duplication**, la **destinazione** è un **altro disco fisso**



- Il disco fisso **destinazione** deve essere della stessa marca, dello stesso modello e della stessa taglia del disco fisso **sorgente**
  - Tutto il disco **sorgente** (ovvero, tutto il contenuto di tutti i settori) viene replicato (duplicato) esattamente nella **destinazione**
    - L'obiettivo è appunto quello di ottenere una copia esatta, identica in ogni aspetto

# Acquisizione dei Dati

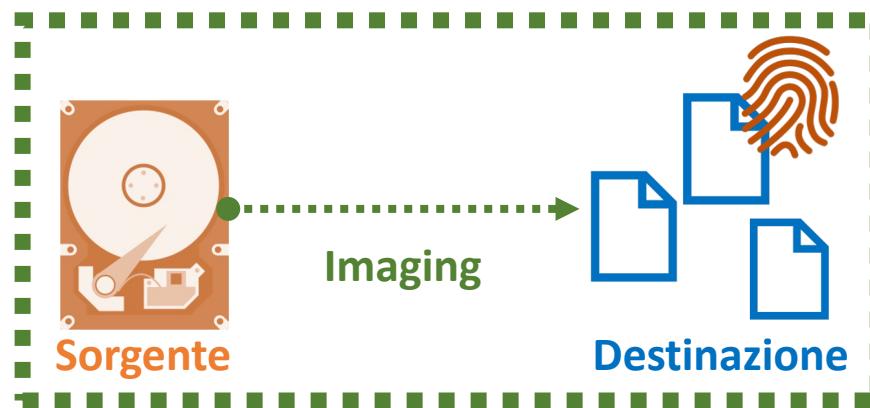
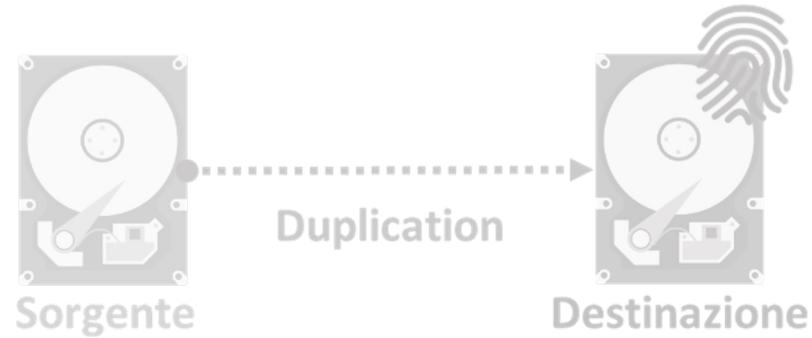
## Immagini Forensi e Hash | 4/9

- Esistono dei dispositivi hardware che si occupano del processo di duplication e sono chiamati **forensic hardware duplicator**
- Tali dispositivi integrano anche la funzionalità di write blocking del disco fisso originale
- Inoltre, effettuano anche la verifica dell'esattezza della copia, ottenuta come risultato del processo (*maggiori dettagli nelle prossime slide*)
- **VANTAGGIO:** Il vantaggio di tali dispositivi è l'estrema rapidità nell'esecuzione del processo di duplication

# Acquisizione dei Dati

## Immagini Forensi e Hash | 5/9

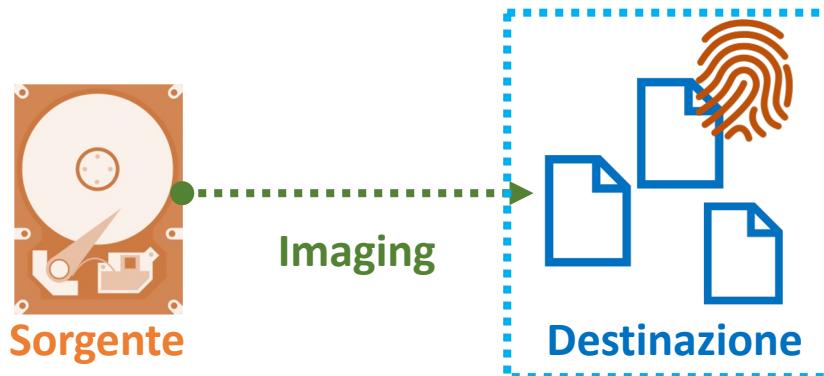
- Per la creazione di una «copia esatta» di un disco fisso (o un altro tipo di supporto di memorizzazione), sono possibili due opzioni:



# Acquisizione dei Dati

## Immagini Forensi e Hash | 6/9

- La **destinazione** del processo di **imaging**, è un insieme costituito da **uno o più file**, i quali conterranno, al termine del processo, la copia esatta dell'intero disco fisso **sorgente**



# Acquisizione dei Dati

## Immagini Forensi e Hash | 6/9

- La **destinazione** del processo di **imaging**, è un insieme costituito da **uno o più file**, i quali conterranno, al termine del processo, la copia esatta dell'intero disco fisso **sorgente**

### OSSERVAZIONE

Quando si effettua una **copia logica** (ovvero, la copia «tradizionale») di file e/o cartelle, non tutti i file potrebbero essere copiati (a causa di mancanza di permessi, file nascosti, ecc.)

# Acquisizione dei Dati

## Immagini Forensi e Hash | 7/9

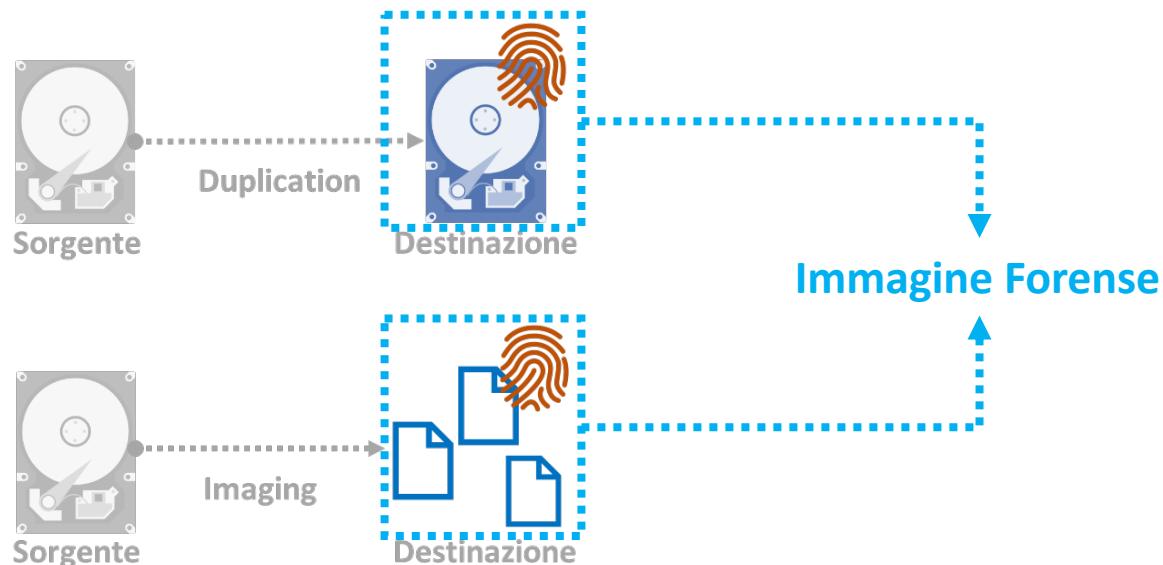
### COPIA BIT-PER-BIT

Per evitare che vengano persi dei file/directory, durante la copia logica, è necessario effettuare una copia bit-per-bit dei dati grezzi («raw») dalla **sorgente** alla **destinazione**, senza che vi sia alcuna aggiunta o modifica

# Acquisizione dei Dati

## Immagini Forensi e Hash | 8/9

- Il risultato del processo di duplication o di imaging, è quindi una copia esatta, denotata come **immagine fisica** (**physical image**) o **immagine forense**



# Acquisizione dei Dati

## Immagini Forensi e Hash | 9/9

- Al fine di verificare che, il processo di duplication o di imaging, abbia effettivamente restituito una copia esatta, si effettuano dei controlli, mediante l'utilizzo di una o più **funzioni crittografiche di hash**

# Acquisizione dei Dati

## Immagini Forensi e Hash | 9/9

- Al fine di verificare che, il processo di duplication o di imaging, abbia effettivamente restituito una copia esatta, si effettuano dei controlli, mediante l'utilizzo di una o più **funzioni crittografiche di hash**

- Calcolo dell'hash della **sorgente**:  $H_S$
- Calcolo dell'hash della **destinazione** (immagine forense):  $H_D$
- Se  $H_S$  e  $H_D$  sono uguali
  - **Sorgente** e **destinazione** risultano **effettivamente «identiche»**
- *Altrimenti*
  - La **destinazione** differisce dalla **sorgente** (anche di un solo bit)

# Acquisizione dei Dati

## Cenni sulle Funzioni Crittografiche di Hash | 1/4

- I valori di hash sono ottenuti da appositi algoritmi
- Un valore di hash può essere immaginato come una sorta di «*digital fingerprint*»
  - È quindi unico e gioca un ruolo fondamentale nella verifica di integrità delle evidenze
- Uno degli algoritmi utilizzati è l'algoritmo crittografico **Message Digest (MD5)**, nonostante non sia recente e contenga delle vulnerabilità, dal punto di vista crittografico
  - MD5 restituisce un valore di hash di 128 bit (generalmente tale valore è riportato in formato esadecimale)

# Acquisizione dei Dati

## Cenni sulle Funzioni Crittografiche di Hash | 2/4

### Esempio Funzione Crittografica MD5

- Stringa: Ciao, Mondo !
  - Valore Hash MD5: **2B0A9B27997C7E4CC82030E26A7D6E14**
- Stringa: Ciao, Mondp !
  - Valore Hash MD5: **EF4C64FB6C7F5414CC92D897CDCC9F80**

# Acquisizione dei Dati

## Cenni sulle Funzioni Crittografiche di Hash | 2/4

### Esempio Funzione Crittografica MD5

- Stringa: Ciao, Mondo !
  - Valore Hash MD5: **2B0A9B27997C7E4CC82030E26A7D6E14**
- Stringa: Ciao, Mondp !
  - Valore Hash MD5: **EF4C64FB6C7F5414CC92D897CDCC9F80**

Valori di hash diversi, su input diversi

# Acquisizione dei Dati

## Cenni sulle Funzioni Crittografiche di Hash | 3/4

- Un altro algoritmo utilizzato è **Secure Hashing Algorithm-1 (SHA-1)**
- Più sicuro di MD5 e produce un valore di hash di **160 bit**
  - Invece dei 128 bit prodotti da MD5
- Ad oggi, comunque, una delle funzioni più valide e sicure è la funzione denominata SHA-2
  - Ci sono poi funzioni di hash denominate SHA-224, SHA-384 e SHA-512, le quali producono rispettivamente output di dimensione 224, 384 e 512 bit
- Da notare che **più la funzione crittografica è robusta, più è difficile che vi siano manomissioni**, pertanto, è possibile accettare che un'immagine forense rimanga inalterata

# Acquisizione dei Dati

## Principali Formati per le Immagini Forensi

- Esistono principalmente tre categorie di formati, in merito alle immagini forensi:

Formati RAW

Formati Proprietari

Advanced Forensics Format (AFF)

# Acquisizione dei Dati

## Principali Formati per le Immagini Forensi

- Esistono principalmente tre categorie di formati, in merito alle immagini forensi:

Formati RAW

Formati Proprietari

Advanced Forensics Format (AFF)

# Acquisizione dei Dati

## Formati RAW

- Restituito da tools che operano a basso livello
- Copia bit-per-bit da un drive a un file

### VANTAGGI



- Velocità di trasferimento
- Tolleranza a errori di natura minore
- Diversi tool, per la digital forensics, sono in grado di leggerli

### SVANTAGGI



- Richiede lo stesso spazio della sorgente
- I controlli di validazione vanno conservati a parte (ad esempio, valore hash di MD5, ecc.)

# Acquisizione dei Dati

## Formati RAW

- Restituito da tools che operano a basso livello
  - Copia bit-per-bit da un drive a un file
- Velocità
  - Tollera
  - Diver
  - Principali estensioni dei file, relativi alle immagini RAW:
    - .dd
    - .raw
    - .img
    - Ecc.
- Richiede lo stesso spazio della sorgente
  - I controlli di validazione vanno conservati a parte (ad esempio, valore hash di MD5, ecc.)

# Acquisizione dei Dati

## Principali Formati per le Immagini Forensi

- Esistono principalmente tre categorie di formati, in merito alle immagini forensi:

Formati RAW

Formati Proprietari

Advanced Forensics Format (AFF)

# Acquisizione dei Dati

## Formati Proprietari | 1/2

- In genere, il formato proprietario Ingloba l'immagine RAW, ma ne può effettuare la compressione *lossless* (*maggiori dettagli in seguito*)
- Suddivisione immagini in più file, detti anche *segmenti* (per memorizzazione su uno o più supporti rimovibili)

### VANTAGGI

- Possono integrare metadati, come, ad esempio:
  - Hash dei dati
  - Data e ora di acquisizione
  - Anagrafica Investigatore, nome/numero del caso, commenti, etc.

### SVANTAGGI

- Non necessariamente supportati da tutti i tool
- Limitazioni nella taglia dei file, in cui si suddivide l'immagine

# Acquisizione dei Dati

## Formati Proprietari | 2/2

- Il formato **Expert Witness Format (EWF)** è ormai uno standard *de facto*
  - Usato da diversi software, fra i quali:
    - EnCase
    - Forensics Toolkit (FTK)
    - X-Ways Forensics
    - Ecc.
  - Permette la produzione di file compressi o non compressi, in base alle preferenze
  - Estensione dei file Expert Witness Format:
    - .E01
    - .E02
    - .E03
    - Ecc.

# Acquisizione dei Dati

## Principali Formati per le Immagini Forensi

- Esistono principalmente tre categorie di formati, in merito alle immagini forensi:

Formati RAW

Formati Proprietari

**Advanced Forensics Format (AFF)**

# Acquisizione dei Dati

## Advanced Forensics Format (AFF)

- Sviluppato da Simson L. Garfinkel presso la Basis Technology Corporation
- **OBIETTIVI**
  - Immagazzinare immagini RAW compresse e non compresse
  - Nessuna restrizione alla taglia delle immagini
  - Aggiunta di metadati
  - Design semplice ed estensibile
  - Formato Open-Source e per multiple piattaforme
  - Check interni di consistenza e integrità
  - Estensioni:
    - .AFD per i segmenti
    - .AFM per i metadati

# Acquisizione dei Dati

## Compressione di Dati Forensi

- Un algoritmo di compressione per dati forensi deve necessariamente utilizzare una strategia lossless (senza perdita di informazioni)
  - Con gli algoritmi di compressione che usano strategie lossless, è possibile riottenere i dati originali, partendo dal file compresso
  - Un buon algoritmo potrebbe ridurre la dimensione di una immagine di oltre il 50%
- In alcuni casi, un algoritmo di compressione può essere inefficace
- Introduce ulteriori rischi di «perdite» di evidenze, in caso di problemi durante il processo di compressione

**II tool DC3DD**

# Il tool DC3DD

## Alcune Caratteristiche

- Il primo tool, preinstallato nella distribuzione Kali Linux, che tratteremo è **DC3DD**
- DC3DD è una variante del tool Data Dump (DD), utilizzato per l'acquisizione forense e l'*hashing*
- Caratteristiche di uno strumento di Data Dump
  - **Acquisizione** e **clonazione** di un supporto di memorizzazione, mediante **Bitstream** (bit-per-bit)
  - **Copia delle partizioni di un disco**
  - Copia delle cartelle e dei file
  - **Check** degli **errori** di un disco fisso
  - **Pulizia forense** di tutti i **dati presenti** su un supporto
    - *Maggiori dettagli in seguito*

# Il tool DC3DD

## Supporti di Memorizzazione e Partizioni su Linux

- Tipicamente un dispositivo di memorizzazione (storage device), in Linux, è indicato nel modo seguente:

/dev/sda

# Il tool DC3DD

## Supporti di Memorizzazione e Partizioni su Linux

- Tipicamente un dispositivo di memorizzazione (storage device), in Linux, è indicato nel modo seguente:

`/dev/sda`

`/dev` fa riferimento al percorso di tutti i device ed i drivers, riconosciuti da Linux

# Il tool DC3DD

## Supporti di Memorizzazione e Partizioni su Linux

- Tipicamente un dispositivo di memorizzazione (storage device), in Linux, è indicato nel modo seguente:

/dev/**sda**

**/sda** fa riferimento ad un dispositivo di memorizzazione

sd è relativo a **storage device** (o driver) ed è seguito da una lettera, la quale rappresenta il numero del device di memorizzazione

### Esempio

- sda è riferito al primo dispositivo riconosciuto
- sdb è riferito al secondo dispositivo riconosciuto

# Il tool DC3DD

## Supporti di Memorizzazione e Partizioni su Linux

- Tipicamente un dispositivo di memorizzazione (storage device), in Linux, è indicato nel modo seguente:

/dev/sda

- Le partizioni...

# Il tool DC3DD

## Supporti di Memorizzazione e Partizioni su Linux

- Tipicamente un dispositivo di memorizzazione (storage device), in Linux, è indicato nel modo seguente:

/dev/sda

- Le **partizioni**...

Suddivisione logica di una unità di memorizzazione (ad esempio, un disco fisso, penna USB, ecc.)

Le **partizioni** vengono definite per varie motivazioni, come, ad esempio, installazione di più sistemi operativi, ecc.

# Il tool DC3DD

## Supporti di Memorizzazione e Partizioni su Linux

- Tipicamente un dispositivo di memorizzazione (storage device), in Linux, è indicato nel modo seguente:

/dev/sda

- Le **partizioni** in Linux sono riconosciute nel seguente modo:
  - sda1 fa riferimento alla *partizione 1* sul primo disco (sda)
  - sda2 fa riferimento alla *partizione 2* sul primo disco (sda)
  - sdb1 fa riferimento alla *partizione 1* sul secondo disco (sdb)
  - sdb2 fa riferimento alla *partizione 2* sul secondo disco (sdb)

# Il tool DC3DD

## Mantenere la Prova Integra

- Per verificare che non vi siano manomissioni, dovrebbe essere calcolato un hash, **prima**, **durante** e **dopo** un'acquisizione
- In Kali Linux, è possibile utilizzare il comando `md5sum` seguito dal path del dispositivo (ad esempio, un dispositivo che costituisce una prova), per ottenere il valore *hash* MD5 associato a tale dispositivo (è possibile utilizzare `md5sum` anche per i file)
  - **Esempio**

```
md5sum /dev/sdb
```

- **NOTA:** Per tutti comandi Linux è possibile avere maggiori dettagli nel modo seguente

```
man <nome_comando>
```

# Il tool DC3DD

## Caratteristiche Principali

- Il tool **DC3DD** è stato sviluppato dal “**Department of Defense Cyber Crime Center**” è un **Data Dump** con diverse caratteristiche rilevanti
- *Caratteristiche*
  - **Hashing «on-the-fly»** usando più algoritmi di hash
    - MD5, SHA-1, SHA-256 e SHA-512
  - Indicazione del progresso ed indicazione del tempo di esecuzione
  - **Scrittura degli errori** individuati su un **file di log**
  - Suddivisione dei file di output, in più parti
  - **Verifica** dei file
  - **Pulizia forense**

# Il tool DC3DD

## Utilizzo su Kali Linux | 1/2

- DC3DD è uno strumento utilizzabile da **linea di comando** (CLI – Command Line Interface)
- Il **comando** è dc3dd e può essere eseguito dal terminale
- Digitando il seguente comando, verrà mostrato l'help del tool

```
dc3dd --help
```

- Output (*parziale*):

```
root@kali:~# dc3dd --help
-----
usage:
-----

dc3dd [OPTION 1] [OPTION 2] ... [OPTION N]
      *or*
dc3dd [HELP OPTION]

where each OPTION is selected from the basic or advanced
options listed below, or HELP OPTION is selected from the
help options listed below.
```

# Il tool DC3DD

## Utilizzo su Kali Linux | 2/2

- DC3DD è uno strumento utilizzabile da **linea di comando** (CLI – Command Line Interface)
- Il **comando** è dc3dd e può essere eseguito dal terminale
- Digitando il seguente comando, verrà mostrato l'help del tool

```
dc3dd --help
```

- Output (*parziale*):

```
root@kali:~# dc3dd --help
-----
usage:
-----
[dc3dd [OPTION 1] [OPTION 2] ... [OPTION N]
 *or*
dc3dd [HELP OPTION]
```

Il comando dc3dd viene utilizzato in questa forma, separando le *opzioni* con lo spazio

where each OPTION is selected from the basic or advanced options listed below, or HELP OPTION is selected from the help options listed below.

# Il tool DC3DD

## Esempio di Utilizzo | 1/12

```
dc3dd if=/dev/sdb hash=md5 log=dc3ddusb of=test_usb.dd
```

# Il tool DC3DD

## Esempio di Utilizzo | 2/12

```
dc3dd if=/dev/sdb hash=md5 log=dc3ddusb of=test_usb.dd
```

- **if**: specifica il *file di input* (ovvero, il dispositivo di cui si intende effettuare la copia esatta)
  - Nell'esempio, si fa riferimento a /dev/sdb

# Il tool DC3DD

## Esempio di Utilizzo | 2/12

```
dc3dd if=/dev/sdb hash=md5 log=dc3ddusb of=test_usb.dd
```

- **if**: specifica il *file di input* (ovvero, il dispositivo di cui si intende effettuare la copia esatta)
  - Nell'esempio, si fa riferimento a /dev/sdb

**NOTA:** Si tratta di un device secondario (una penna USB, da 8 GB)

# Il tool DC3DD

## Esempio di Utilizzo | 3/12

```
dc3dd if=/dev/sdb hash=md5 log=dc3ddusb of=test_usb.dd
```

- **if**: specifica il *file di input* (ovvero, il dispositivo di cui si intende effettuare la copia esatta)
  - Nell'esempio, si fa riferimento a /dev/sdb
- **hash**: specifica l'algoritmo di hash che verrà utilizzato per verificare l'integrità
  - Nell'esempio, si fa riferimento all'algoritmo di hash MD5

# Il tool DC3DD

## Esempio di Utilizzo | 4/12

```
dc3dd if=/dev/sdb hash=md5 log=dc3ddusb of=test_usb.dd
```

- **if**: specifica il *file di input* (ovvero, il dispositivo di cui si intende effettuare la copia esatta)
  - Nell'esempio, si fa riferimento a /dev/sdb
- **hash**: specifica l'algoritmo di hash che verrà utilizzato per verificare l'integrità
  - Nell'esempio, si fa riferimento all'algoritmo di hash MD5
- **log**: specifica il nome del file di *log*, all'interno del quale verranno riportati tutti i dettagli del dispositivo, del processo di acquisizione ed eventuali errori riscontrati
  - Nell'esempio, si fa riferimento al file dc3ddusb

# Il tool DC3DD

## Esempio di Utilizzo | 5/12

```
dc3dd if=/dev/sdb hash=md5 log=dc3ddusb of=test_usb.dd
```

- **if**: specifica il *file di input* (ovvero, il dispositivo di cui si intende effettuare la copia esatta)
  - Nell'esempio, si fa riferimento a /dev/sdb
- **hash**: specifica l'algoritmo di hash che verrà utilizzato per verificare l'integrità
  - Nell'esempio, si fa riferimento all'algoritmo di hash MD5
- **log**: specifica il nome del file di *log*, all'interno del quale verranno riportati tutti i dettagli del dispositivo, del processo di acquisizione ed eventuali errori riscontrati
  - Nell'esempio, si fa riferimento al file dc3ddusb
- **of**: specifica il *file di output* relativo all'immagine forense creata dal tool (l'estensione può essere .dd, come nell'esempio, oppure, .img)

# Il tool DC3DD

## Esempio di Utilizzo | 6/12

- *Durante la fase di esecuzione (e acquisizione)*

```
root@kali:~/Scrivania# dc3dd if=/dev/sdb hash=md5 log=dc3ddusb of=test_usb.dd
dc3dd 7.2.646 started at 2019-02-22 11:39:40 +0100
compiled options:
command line: dc3dd if=/dev/sdb hash=md5 log=dc3ddusb of=test_usb.dd
device size: 15335424 sectors (probed),    7,851,737,088 bytes
sector size: 512 bytes (probed)
█ 504004608 bytes ( 481 M ) copied ( 6% ), 225 s, 2,1 M/s
```

# Il tool DC3DD

## Esempio di Utilizzo | 7/12

- *Durante la fase di esecuzione (e acquisizione)*

```
root@kali:~/Scrivania# dc3dd if=/dev/sdb hash=md5 log=dc3ddusb of=test_usb.dd
dc3dd 7.2.646 started at 2019-02-22 11:39:40 +0100
compiled options:
command line: dc3dd if=/dev/sdb hash=md5 log=dc3ddusb of=test_usb.dd
device size: 15335424 sectors (probed),    7,851,737,088 bytes
sector size: 512 bytes (probed)
█ 504004608 bytes ( 481 M ) copied ( 6% ), 225 s, 2,1 M/s
```

- *Processo di acquisizione terminato*

```
input results for device `/dev/sdb':
15335424 sectors in
0 bad sectors replaced by zeros
ceeeb8218838719e4fe918a99eabfb5d (md5)

output results for file `test_usb.dd':
15335424 sectors out

dc3dd completed at 2019-02-22 17:30:27 +0100

root@kali:~/Scrivania# █
```

# Il tool DC3DD

## Esempio di Utilizzo | 8/12

- *File Prodotti*

```
root@kali:~/Scrivania# ls
dc3ddusb  test_usb.dd
root@kali:~/Scrivania#
```

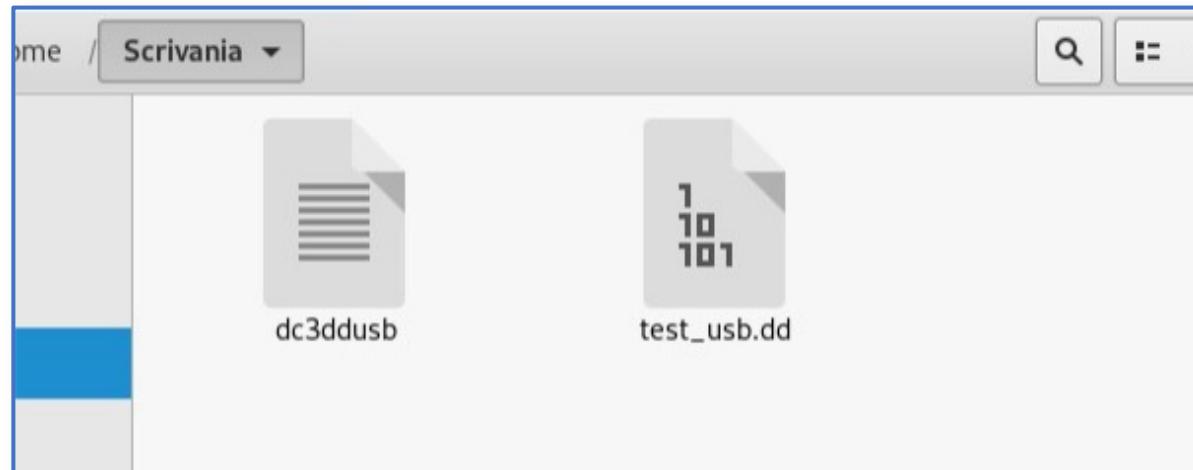
# Il tool DC3DD

## Esempio di Utilizzo | 9/12

- *File Prodotti*

```
root@kali:~/Scrivania# ls
dc3ddusb  test_usb.dd
root@kali:~/Scrivania#
```

- *File Prodotti (Interfaccia Grafica)*



# Il tool DC3DD

## Esempio di Utilizzo | 10/12

- *File Prodotti*

```
root@kali:~/Scrivania# ls  
dc3ddusb  test_usb.dd  
root@kali:~/Scrivania#
```

test\_usb.dd è il file di output prodotto da DC3DD

# Il tool DC3DD

## Esempio di Utilizzo | 11/12

- *File Prodotti*

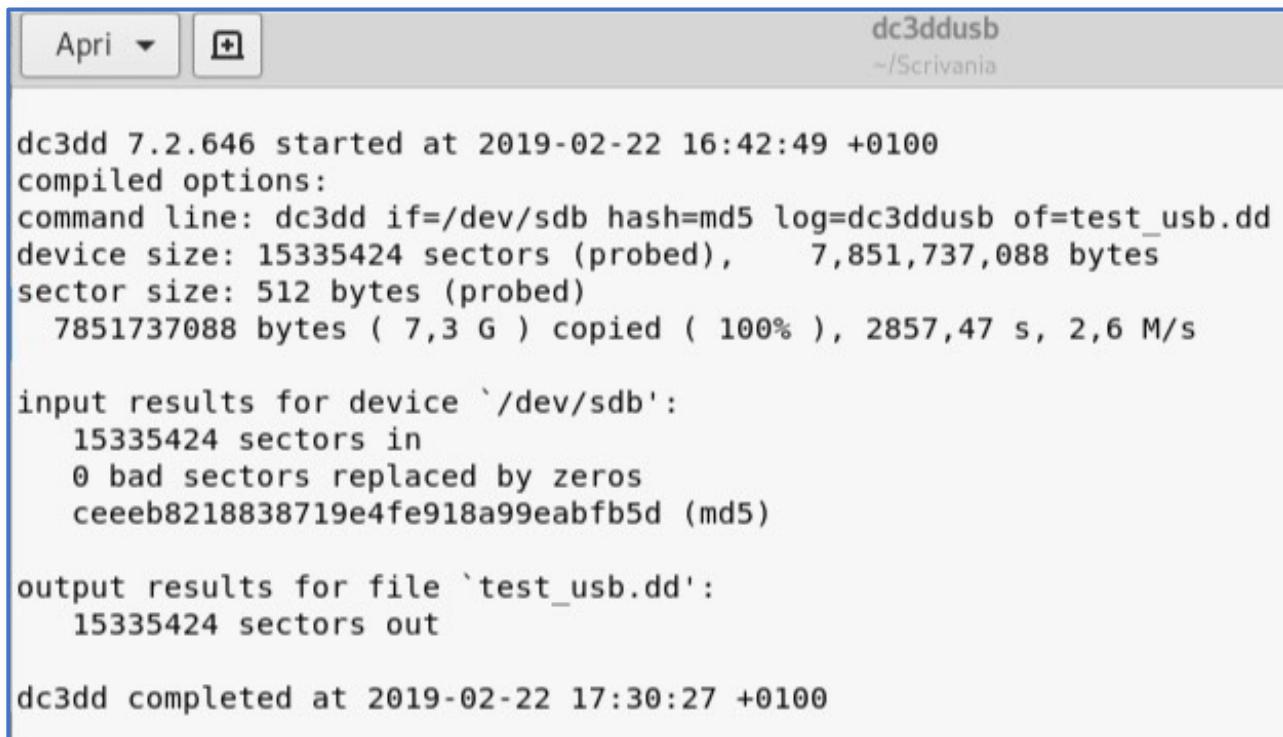
```
root@kali:~/Scrivania# ls  
dc3ddusb  test_usb.dd  
root@kali:~/Scrivania#
```

dc3ddusb è il file di *log* prodotto da DC3DD

# Il tool DC3DD

## Esempio di Utilizzo | 12/12

- *Contenuto del file di log (dc3ddusb)*



```
dc3dd 7.2.646 started at 2019-02-22 16:42:49 +0100
compiled options:
command line: dc3dd if=/dev/sdb hash=md5 log=dc3ddusb of=test_usb.dd
device size: 15335424 sectors (probed),    7,851,737,088 bytes
sector size: 512 bytes (probed)
    7851737088 bytes ( 7,3 G ) copied ( 100% ), 2857,47 s, 2,6 M/s

input results for device `/dev/sdb':
    15335424 sectors in
    0 bad sectors replaced by zeros
    ceeeb8218838719e4fe918a99eabfb5d (md5)

output results for file `test_usb.dd':
    15335424 sectors out

dc3dd completed at 2019-02-22 17:30:27 +0100
```

# Il tool DC3DD

## Processo di Clonazione | 1/2

- DC3DD permette anche di clonare una immagine forense, acquisita precedentemente, su un nuovo dispositivo
  - Questo processo è denominato **processo di clonazione**
- **Esempio**

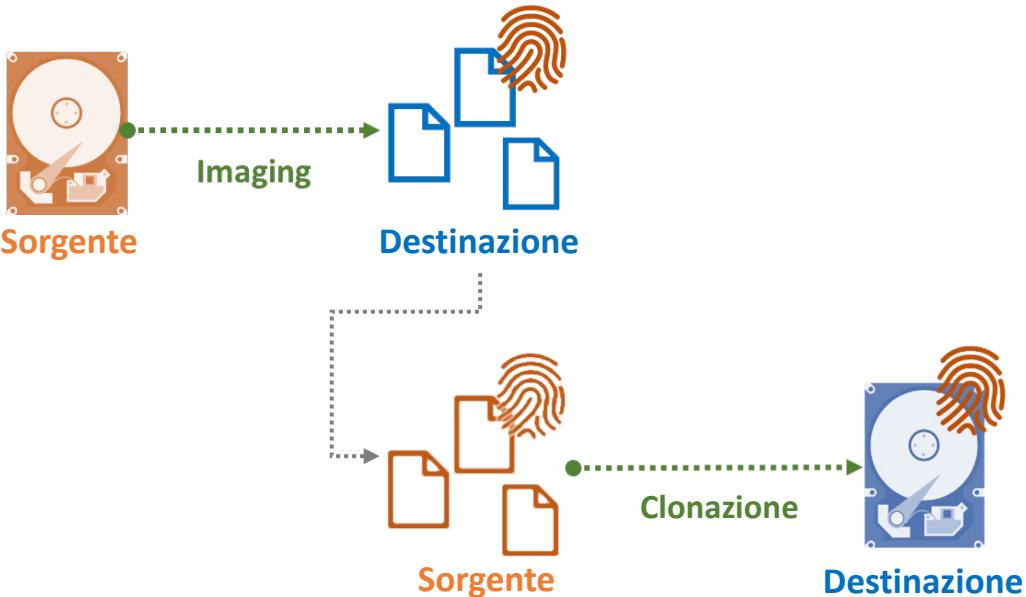
```
dc3dd if=test_usb.dd of=/dev/sdc log=drivecopy.log
```

- *Descrizione*
  - In questo esempio, l'immagine forense, denominata test\_usb.dd, precedentemente acquisita, viene copiata esattamente (clonata) sul device, identificato dal path /dev/sdc

# Il tool DC3DD

## Processo di Clonazione | 2/2

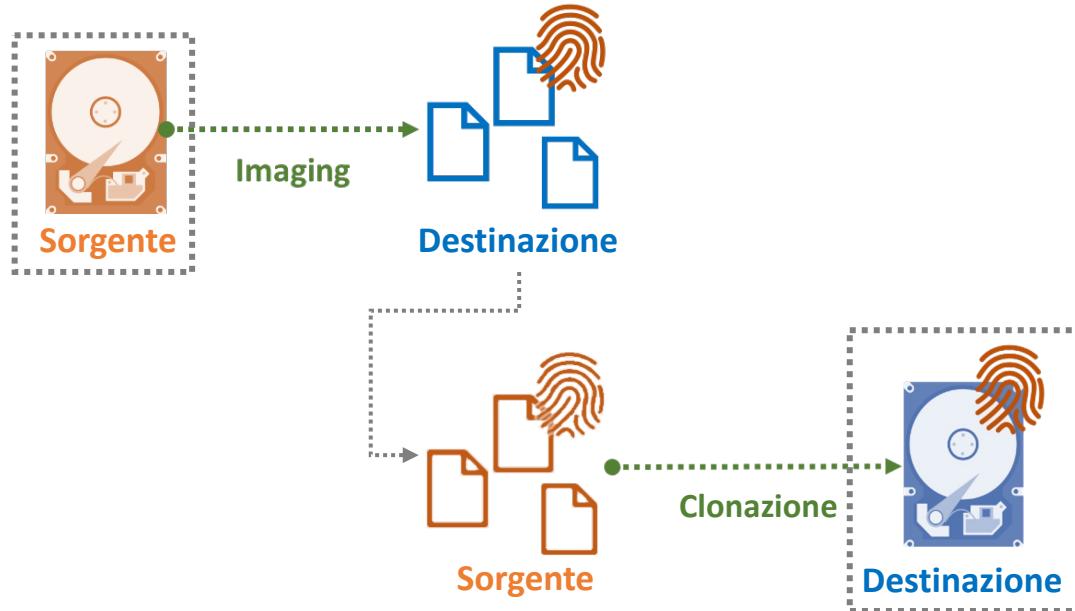
- Esecuzione del processo di duplication, tramite i processi di imaging e di clonazione*



# Il tool DC3DD

## Processo di Clonazione | 2/2

- Esecuzione del processo di *duplication*, tramite i processi di *imaging* e di *clonazione*



Il disco fisso **destinazione**, relativo processo di clonazione,  
deve avere le stesse caratteristiche (modello, marca e taglia)  
del disco fisso **sorgente**, relativo al processo di imaging

# Il tool DC3DD

## Pulizia Forense | 1/15

- Si supponga che un investigatore abbia utilizzato, nell'ambito di una indagine forense, attualmente conclusa, un certo **disco fisso**
- Tale investigatore **NON può riutilizzare il medesimo disco fisso**, così com'è, per una nuova indagine
  - Il suddetto disco fisso deve essere preliminarmente preparato, al fine di essere riutilizzato, mediante una **fase di preparazione**

# Il tool DC3DD

## Pulizia Forense | 2/15

- La **fase di preparazione** del disco fisso è necessaria, onde evitare **qualsiasi rischio** legato al fatto che tracce, relative alla nuova indagine, possano «*interfogliarsi*» con tracce della precedente immagine (conclusa)
  - Questo comporterebbe l'individuazione di potenziali tracce «non corrette» e potrebbe invalidare la nuova indagine
- È consigliabile svolgere la fase di preparazione di un disco fisso, direttamente alla conclusione di una indagine, poiché tale fase potrebbe essere onerosa, in termini di tempo

# Il tool DC3DD

## Pulizia Forense | 3/15

- Per la preparazione di un disco fisso, è necessaria una **pulizia forense (forensic wiping)**, detta anche **secure wiping**) di tale dispositivo
- La pulizia forense, di un disco fisso, prevede la sovrascrittura del contenuto di ciascun settore (di traccia), con valori nulli (zero) o con specifici pattern o con dati random

# Il tool DC3DD

## Pulizia Forense | 4/15

- Il tool DC3DD fornisce anche la possibilità di effettuare la pulizia forense (opzione `wipe`)
- Sono previste tre principali modalità, per la pulizia forense:
  - Modalità 1
  - Modalità 2
  - Modalità 3

# Il tool DC3DD

## Pulizia Forense | 4/15

- Il tool DC3DD fornisce anche la possibilità di effettuare la pulizia forense (opzione `wipe`)
- Sono previste tre principali modalità, per la pulizia forense:
  - **Modalità 1**
  - Modalità 2
  - Modalità 3

# Il tool DC3DD

## Pulizia Forense | 5/15

### Modalità 1 | Descrizione

La pulizia forense viene eseguita sovrascrivendo, con valori zero, il contenuto di ciascun settore del dispositivo specificato

# Il tool DC3DD

## Pulizia Forense | 6/15

### Modalità 1 | Esempio di Utilizzo

#### *Esempio [Parte 1 di 2]*

```
dc3dd wipe=/dev/sdb
```

#### *Descrizione del Comando*

La pulizia forense viene eseguita sul dispositivo, identificato dal path /dev/sdb (specificato nell'opzione wipe)

# Il tool DC3DD

## Pulizia Forense | 7/15

### Modalità 1 | Esempio di Utilizzo

#### *Esempio [Parte 2 di 2]*

##### *Output*

```
dc3dd 7.2.646 started at 2019-02-22 18:03:08 +0100
compiled options:
command line: dc3dd wipe=/dev/sdb
device size: 15335424 sectors (probed),    7,851,737,088 bytes
sector size: 512 bytes (probed)
    7851737088 bytes ( 7,3 G ) copied ( 100% ), 1207 s, 6,2 M/s

input results for pattern `00':
    15335424 sectors in

output results for device `/dev/sdb':
    15335424 sectors out

dc3dd completed at 2019-02-22 18:23:15 +0100
```

# Il tool DC3DD

## Pulizia Forense | 8/15

- Il tool DC3DD fornisce anche la possibilità di effettuare la pulizia forense (opzione `wipe`)
- Sono previste tre principali modalità, per la pulizia forense:
  - Modalità 1
  - **Modalità 2**
  - Modalità 3

# Il tool DC3DD

## Pulizia Forense | 9/15

### Modalità 2 | Descrizione

La pulizia forense viene eseguita sovrascrivendo, con un pattern esadecimale (ripetuto), il contenuto di ciascun settore del dispositivo specificato

- Il pattern viene specificato dall'utente, mediante l'opzione pat

# Il tool DC3DD

## Pulizia Forense | 10/15

### Modalità 2 | Esempio di Utilizzo

#### *Esempio [Parte 1 di 2]*

```
dc3dd wipe=/dev/sdb pat=101010
```

#### *Descrizione del Comando*

La pulizia forense viene eseguita sul dispositivo, identificato dal path /dev/sdb (specificato nell'opzione `wipe`), utilizzando, ripetutamente, il pattern esadecimale 101010 (opzione `pat`), per la sovrascrittura dei settori

# Il tool DC3DD

## Pulizia Forense | 11/15

### Modalità 2 | Esempio di Utilizzo

#### *Esempio [Parte 2 di 2]*

##### *Output*

```
dc3dd 7.2.646 started at 2019-02-22 18:25:19 +0100
compiled options:
command line: dc3dd wipe=/dev/sdb pat=101010
device size: 15335424 sectors (probed),    7,851,737,088 bytes
sector size: 512 bytes (probed)
    7851737088 bytes ( 7,3 G ) copied ( 100% ), 1343 s, 5,6 M/s

input results for pattern `101010':
    15335424 sectors in

output results for device `/dev/sdb':
    15335424 sectors out

dc3dd completed at 2019-02-22 18:47:42 +0100
```

# Il tool DC3DD

## Pulizia Forense | 12/15

- Il tool DC3DD fornisce anche la possibilità di effettuare la pulizia forense (opzione `wipe`)
- Sono previste tre principali modalità, per la pulizia forense:
  - Modalità 1
  - Modalità 2
  - **Modalità 3**

### Modalità 3 | Descrizione

La pulizia forense viene eseguita sovrascrivendo, con una stringa (ripetuta), il contenuto di ciascun settore del dispositivo specificato

- La stringa viene specificata dall'utente, mediante l'opzione tpat

# Il tool DC3DD

## Pulizia Forense | 14/15

### Modalità 3 | Esempio di Utilizzo

#### *Esempio [Parte 1 di 2]*

```
dc3dd wipe=/dev/sdb tpat=digf
```

#### *Descrizione del Comando*

La pulizia forense viene eseguita sul dispositivo, identificato dal path /dev/sdb (specificato nell'opzione `wipe`), utilizzando, ripetutamente, la stringa `digf` (opzione `tpat`), per la sovrascrittura dei settori

# Il tool DC3DD

## Pulizia Forense | 15/15

### Modalità 3 | Esempio di Utilizzo

#### *Esempio [Parte 2 di 2]*

##### *Output*

```
dc3dd 7.2.646 started at 2019-02-22 18:56:01 +0100
compiled options:
command line: dc3dd wipe=/dev/sdb tpat=digf
device size: 15335424 sectors (probed),    7,851,737,088 bytes
sector size: 512 bytes (probed)
    7851737088 bytes ( 7,3 G ) copied ( 100% ), 1545 s, 4,8 M/s

input results for pattern `digf':
    15335424 sectors in

output results for device `/dev/sdb':
    15335424 sectors out

dc3dd completed at 2019-02-22 19:21:46 +0100
```



**Il tool Guymager**

# Il tool Guymager

## Caratteristiche

- Un altro tool per l'acquisizione di immagini forensi è **Guymager**
- Guymager è Open-Source
  - Sviluppato da Guy Voncken
- Presenta **molteplici caratteristiche** di DC3DD ed è disponibile esclusivamente per sistemi operativi Linux-based (preinstallato su Kali Linux)
- **Guymager** fornisce una **interfaccia grafica** (GUI - Graphical User Interface)
- Maggiori Dettagli:
  - <https://guymager.sourceforge.io/>





# Il tool Guymager

## Avvio del Tool | 1/2

- Avvio tramite Interfaccia Grafica





# Il tool Guymager

## Avvio del Tool | 2/2

- *Avvio tramite Command Line*

```
File Modifica Visualizza Cerca Terminale Aiuto
root@kali:~# guymager

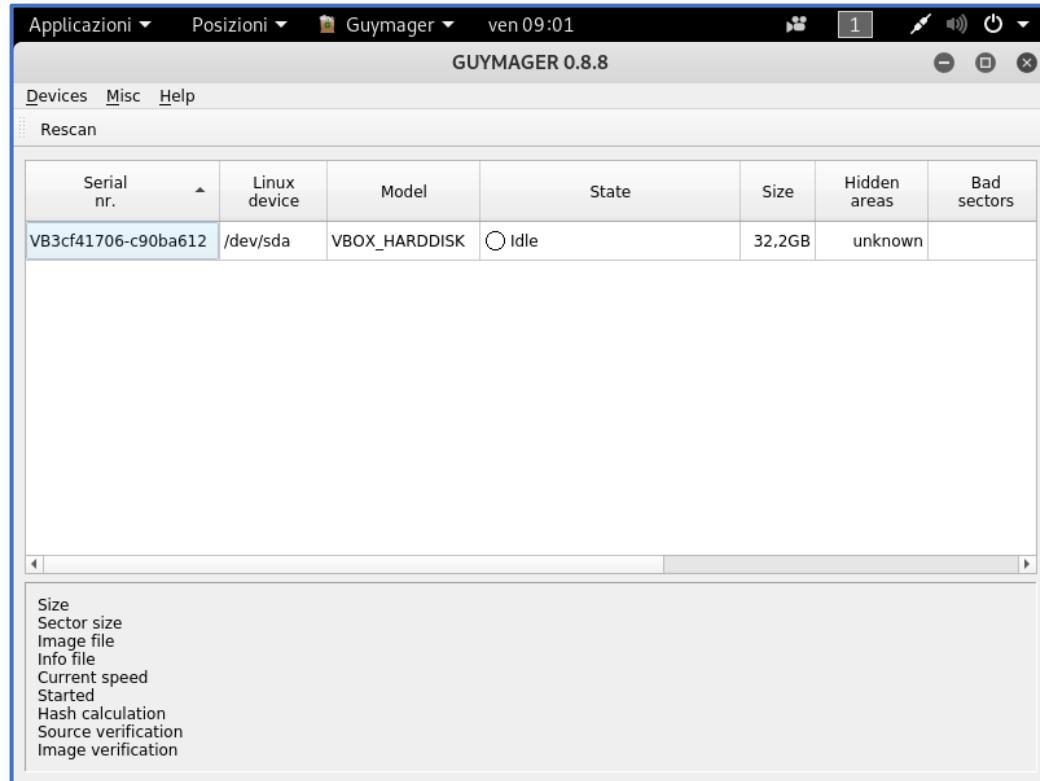
Using default log file name /var/log/guymager.log
Using default cfg file name /etc/guymager/guymager.cfg
```

- Digitare il comando `guymager` da terminale



# Il tool Guymager

## Interfaccia Grafica | 1/6



Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors
VB3cf41706-c90ba612	/dev/sda	VBOX_HARDDISK	Idle	32,2GB	unknown	

Size  
Sector size  
Image file  
Info file  
Current speed  
Started  
Hash calculation  
Source verification  
Image verification



# Il tool Guymager

## Interfaccia Grafica | 2/6

Guymager mostra tutti i supporti di memorizzazione riconosciuti da Kali Linux

The screenshot shows the 'Devices' tab of the Guymager application window. The window title is 'Applicazioni'. The main area displays a table of storage devices with the following columns: Serial nr, Device, Model, State, Size, Hidden areas, and Bad sectors. One entry is visible:

Serial nr	Device	Model	State	Size	Hidden areas	Bad sectors
VB3cf41706-c90ba612	/dev/sda	VBOX_HARDDISK	Idle	32,2GB	unknown	

Below the table, there is a sidebar with the following options:

- Size
- Sector size
- Image file
- Info file
- Current speed
- Started
- Hash calculation
- Source verification
- Image verification



# Il tool Guymager

## Interfaccia Grafica | 3/6

Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors
VB3cf41706-c90ba612	/dev/sda	VBOX_HARDDISK	<input type="radio"/> Idle	32,2GB	unknown	

Per ciascun supporto riconosciuto, vengono visualizzate diverse informazioni, fra cui:

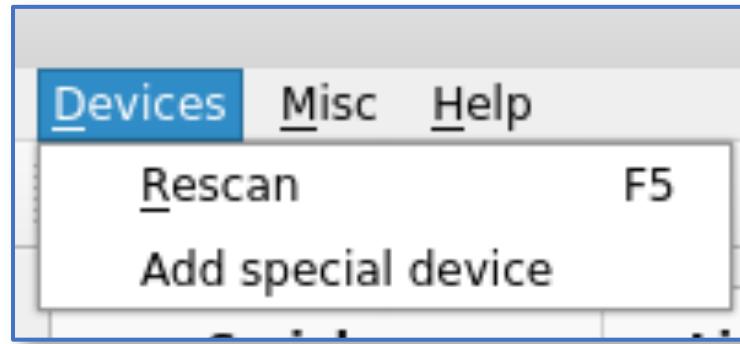
- **Numero seriale** del supporto (*prima colonna*)
- **Path in Kali Linux** (*seconda colonna*)
- **Modello** (*terza colonna*)
- **Stato** (*quarta colonna*)
  - **NOTA:** Viene mostrato lo stato *Idle* quando ancora non è stata avviata la creazione dell'immagine forense
- **Dimensione** (*quinta colonna*)



# Il tool Guymager

## Interfaccia Grafica | 4/6

Il menu a tendina *Devices*

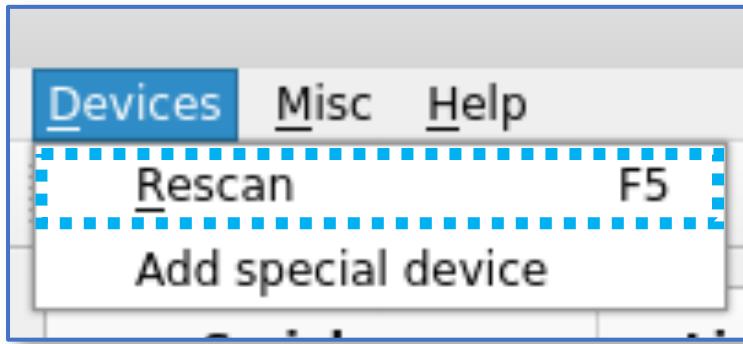




## Il tool Guymager

### Interfaccia Grafica | 5/6

Il menu a tendina *Devices*



Dalla voce *Rescan* del menu *Devices* (oppure, premendo il tasto *F5*) è possibile aggiornare la lista dei device riconosciuti (utile, ad esempio, se vengono aggiunti supporti removibili, ecc.)



## Il tool Guymager

### Interfaccia Grafica | 6/6

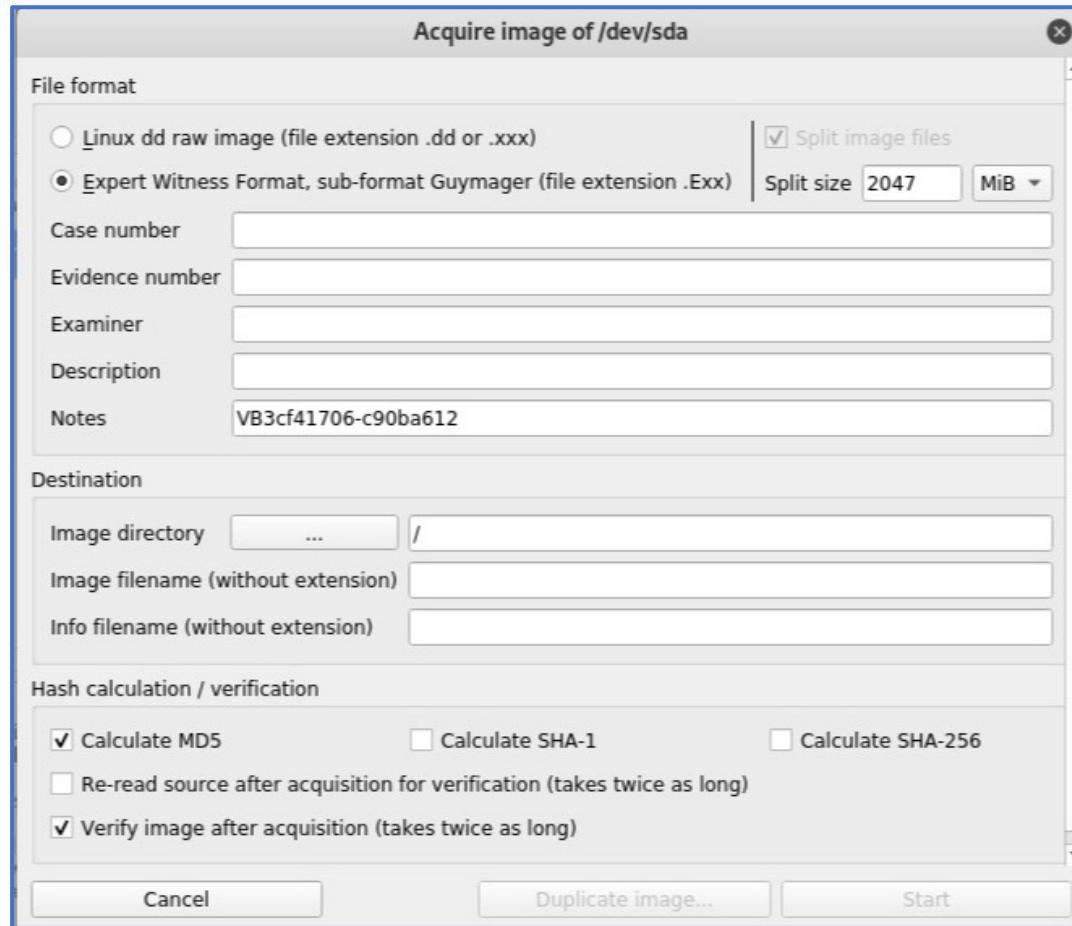
- Per avviare il **processo di imaging**, è sufficiente cliccare su *Acquire image* dal menu contestuale (che appare con il tasto destro del mouse) relativo ad uno dei supporti, mostrati in lista



# Il tool Guymager

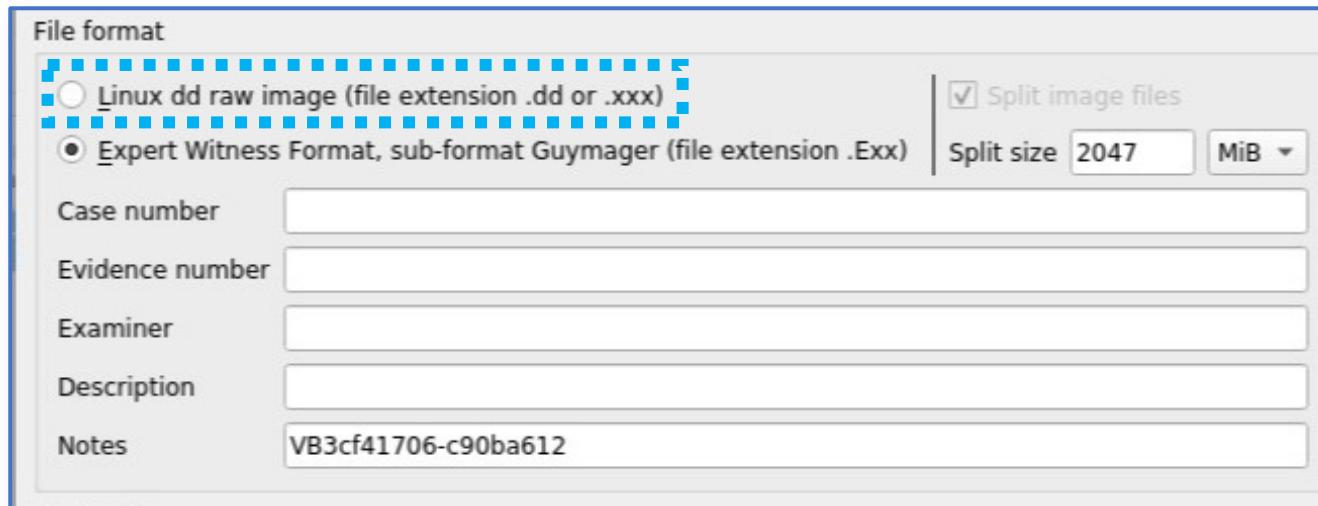
## Definizione delle Specifiche relative all'Output | 1/6

- *Definizione delle Specifiche per la Creazione dell'Immagine Forense*



# Il tool Guymager

## Definizione delle Specifiche relative all'Output | 2/6

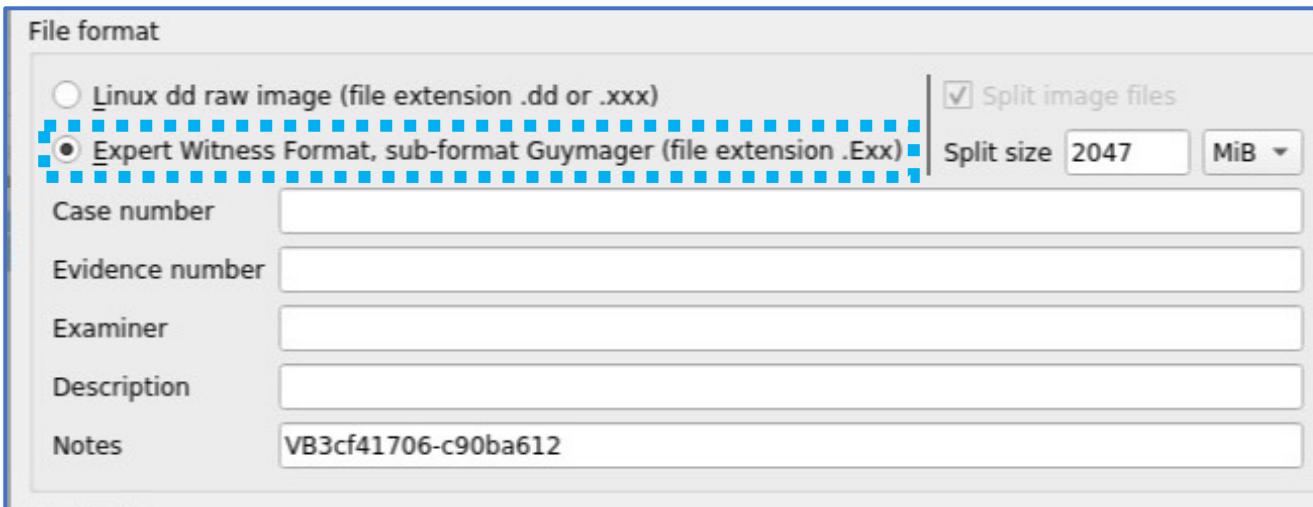


Possibili formati per l'immagine:

- Formato RAW (estensione **.dd**)

# Il tool Guymager

## Definizione delle Specifiche relative all'Output | 2/6

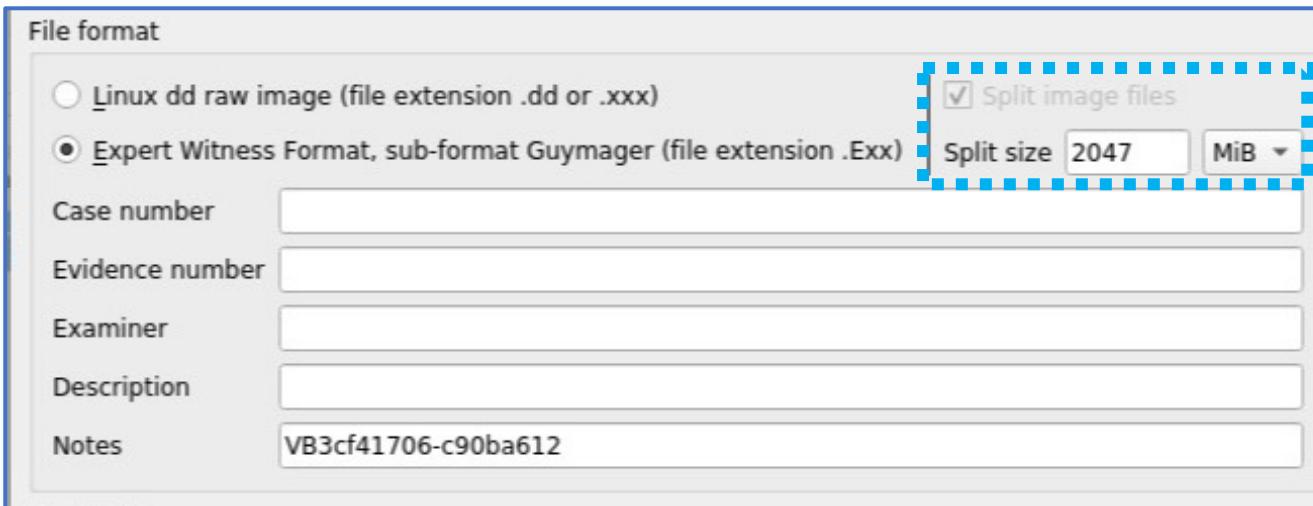


Possibili formati per l'immagine:

- Formato RAW (estensione **.dd**)
- Formato EWF (estensione **.E01**, **.E02**, ...)

# Il tool Guymager

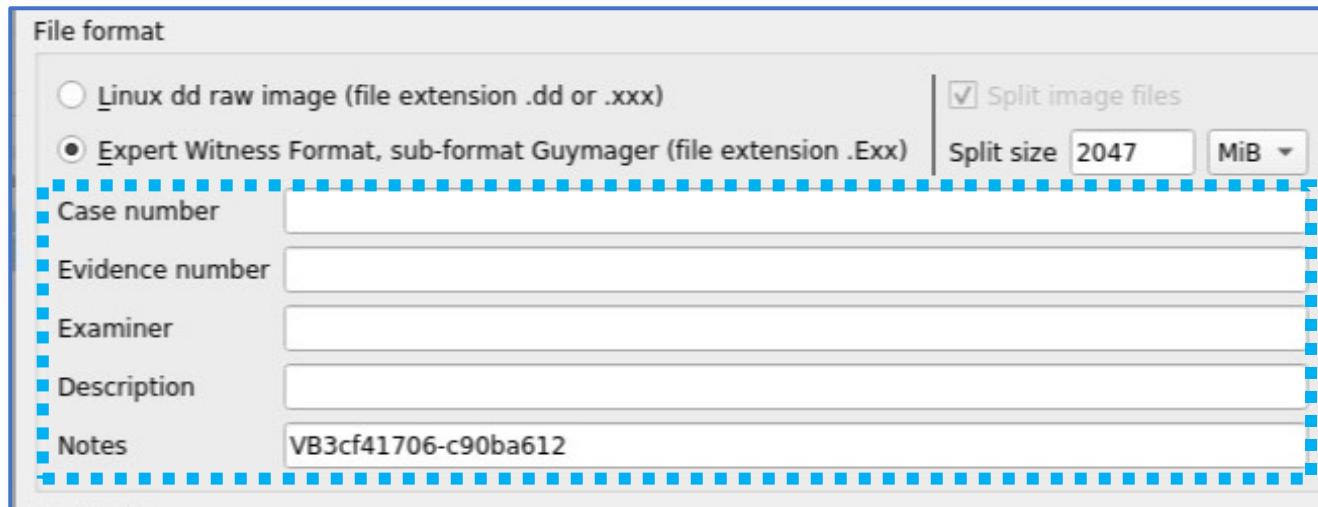
## Definizione delle Specifiche relative all'Output | 2/6



- Con il formato **EWF** è obbligatorio suddividere l'immagine in più segmenti
  - Con il formato **RAW** è invece possibile scegliere se si intende suddividere o meno l'immagine in più segmenti (nel caso in cui si selezioni la volontà di suddividere l'immagine, sarà possibile definire la grandezza di ciascun segmento)
  - La dimensione dei segmenti, può essere indicata alla voce **Split size**

# Il tool Guymager

## Definizione delle Specifiche relative all'Output | 2/6



- Con il formato **EWF** inoltre possiamo specificare diverse informazioni, in relazione al caso che si sta analizzando:
  - Numero (identificativo) del caso (**Case number**)
  - Numero (identificativo) della prova (**Evidence number**)
  - Nome/Identificativo dell'investigatore (**Examiner**)
  - Descrizione della prova (**Description**)
  - Note (**Notes**)

# Il tool Guymager

## Definizione delle Specifiche relative all'Output | 3/6

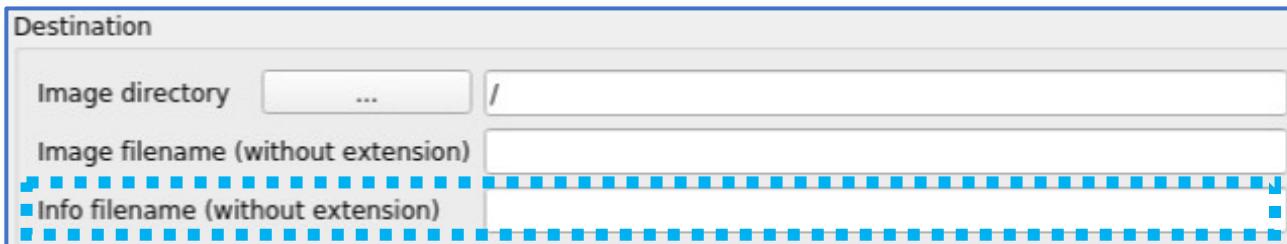
- È possibile specificare la **directory** in cui si intende memorizzare l'immagine acquisita (o i segmenti che la compongono)
- Il nome del file dell'immagine
  - **NOTA:** Non è necessario specificare l'estensione



# Il tool Guymager

## Definizione delle Specifiche relative all'Output | 3/6

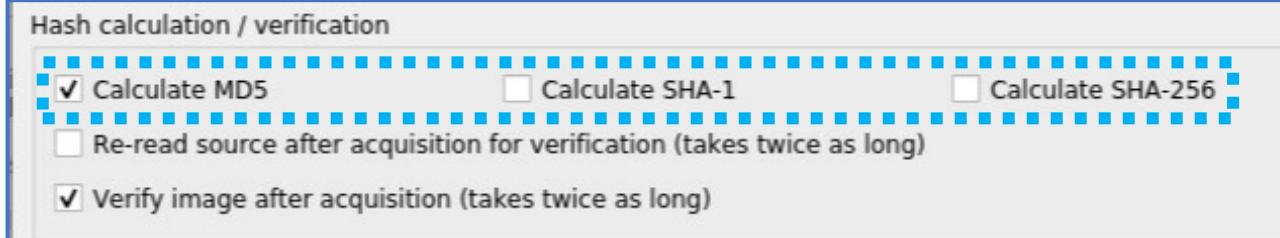
- È possibile specificare la **directory** in cui si intende memorizzare l'immagine acquisita
- Il nome del file dell'immagine
  - **NOTA:** Non è necessario specificare l'estensione
- Il nome del file di *info* (dove verranno riportate informazioni varie sul processo, *maggiori dettagli in seguito...*)



# Il tool Guymager

## Definizione delle Specifiche relative all'Output | 3/6

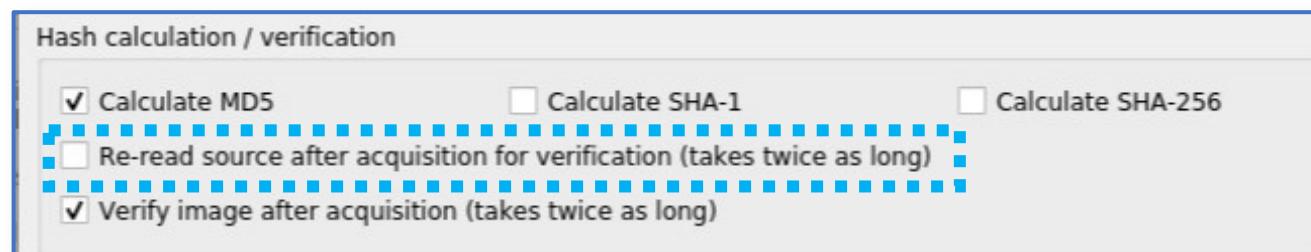
- Da questa finestra è possibile specificare quali **funzioni di hash** devono essere utilizzati, per le successive verifiche
  - MD5, SHA-1 e SHA-256



# Il tool Guymager

## Definizione delle Specifiche relative all'Output | 4/6

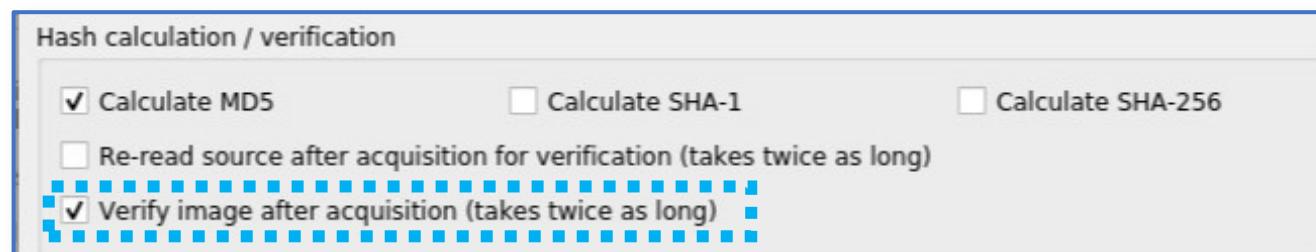
- Da questa finestra è possibile specificare quali **funzioni di hash** devono essere utilizzati, per le successive verifiche
  - MD5, SHA-1 e SHA-256
- Possibilità di **verifica della sorgente**
  - Al termine del processo di imaging, verrà verificata l'integrità della sorgente (per verificare se vi siano o meno alterazioni a seguito del processo di imaging stesso)



# Il tool Guymager

## Definizione delle Specifiche relative all'Output | 4/6

- Da questa finestra è possibile specificare quali **funzioni di hash** devono essere utilizzati, per le successive verifiche
  - MD5, SHA-1 e SHA-256
- Possibilità di **verifica della sorgente**
  - Al termine del processo di imaging, verrà verificata l'integrità della sorgente (per verificare se vi siano o meno alterazioni a seguito del processo di imaging stesso)
- Possibilità di **verifica della destinazione**
  - Verrà verificato se l'immagine forense acquisita è effettivamente una copia esatta, rispetto alla sorgente



# Il tool Guymager

## Definizione delle Specifiche relative all'Output | 5/6



- Dopo aver terminato l'inserimento di tutti i dettagli e le caratteristiche che l'immagine forense dovrà avere, i tasti *Duplicate image...* e *Start* si attiveranno

# Il tool Guymager

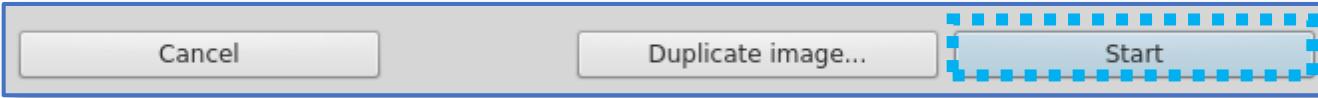
## Definizione delle Specifiche relative all'Output | 5/6



- Con il tasto *Duplicate image...*, sarà possibile duplicare le impostazioni, inserite, al fine di sfruttarle per future immagini forensi

# Il tool Guymager

## Definizione delle Specifiche relative all'Output | 6/6

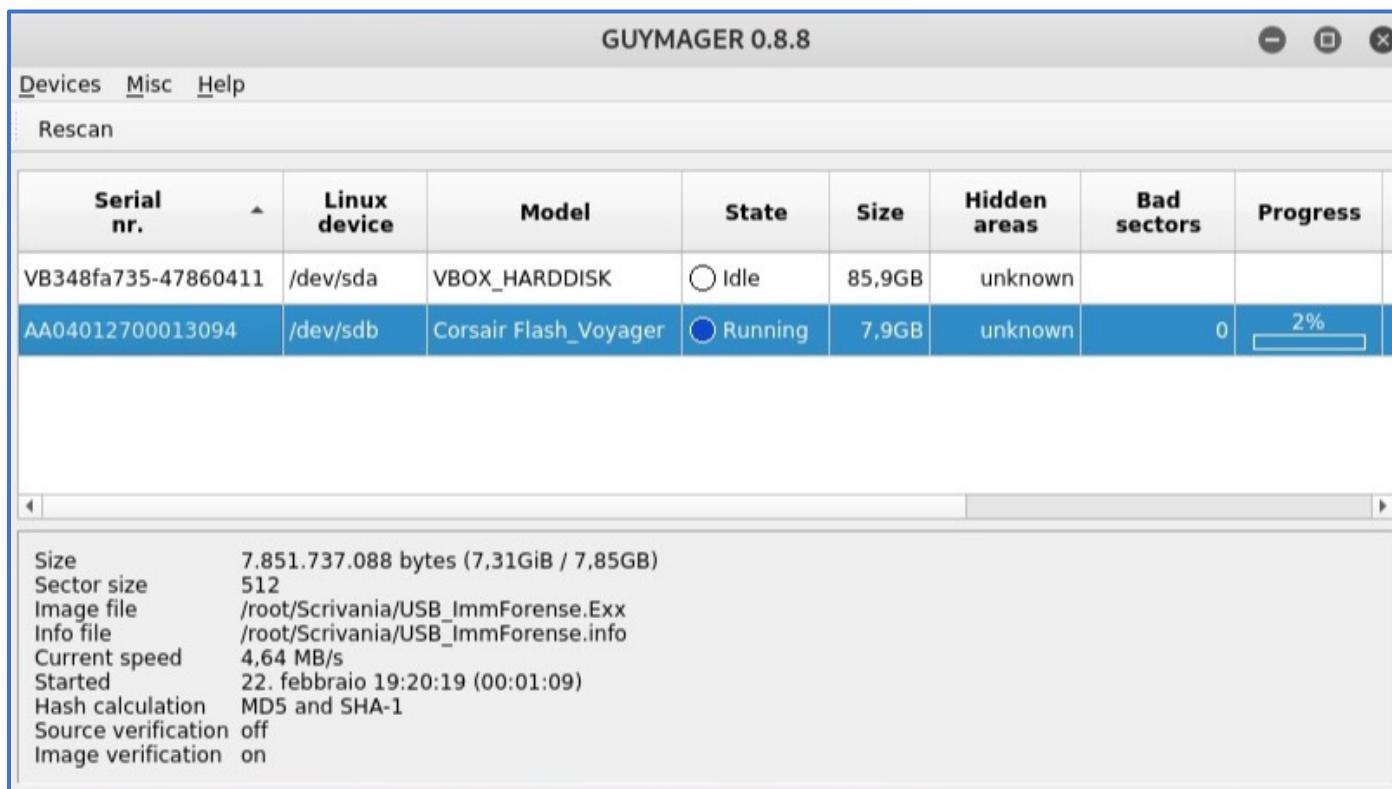


Con il tasto *Start*, il processo di acquisizione **verrà avviato**

# Il tool Guymager

## Esempio di Utilizzo | 1/3

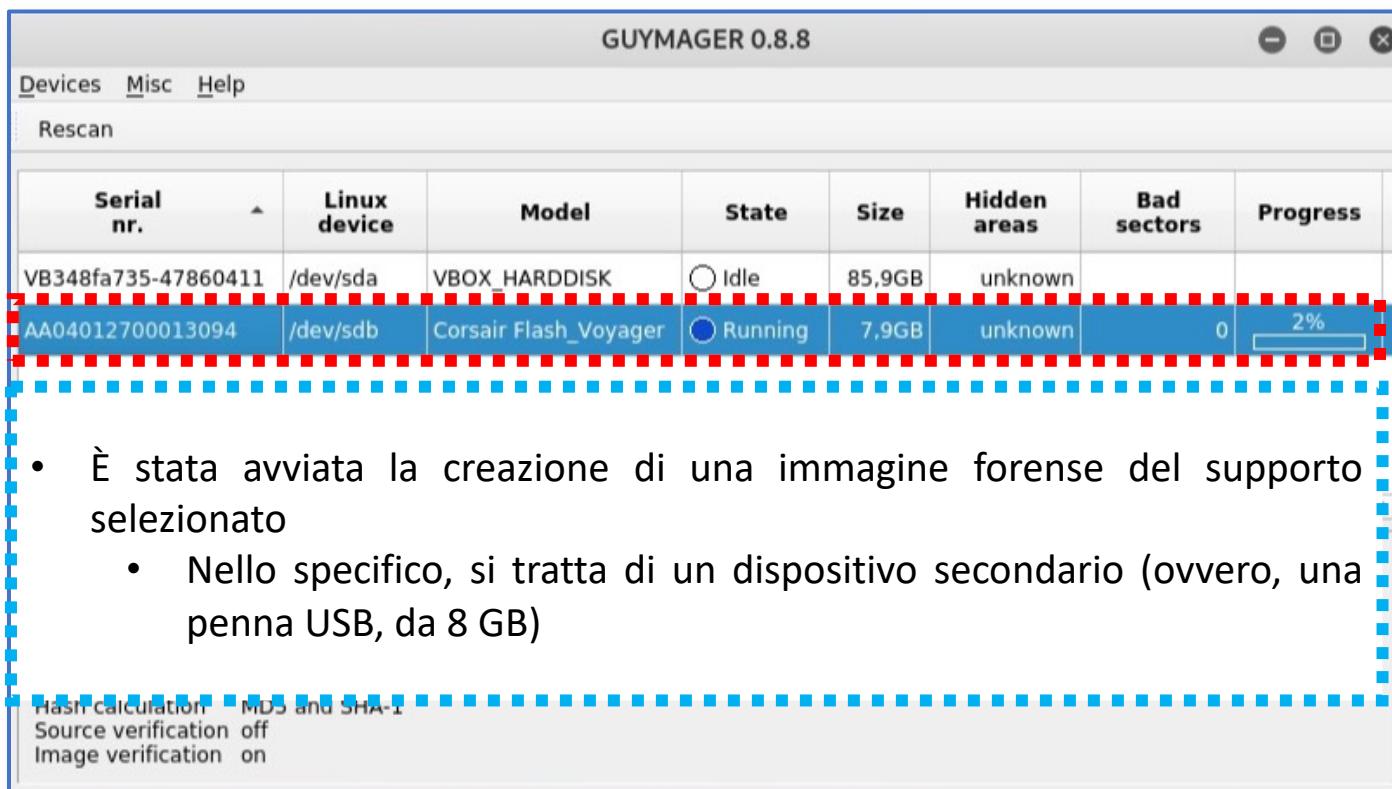
- A seguito dell'avvio del processo, si otterrà una schermata simile alla seguente:



# Il tool Guymager

## Esempio di Utilizzo | 1/3

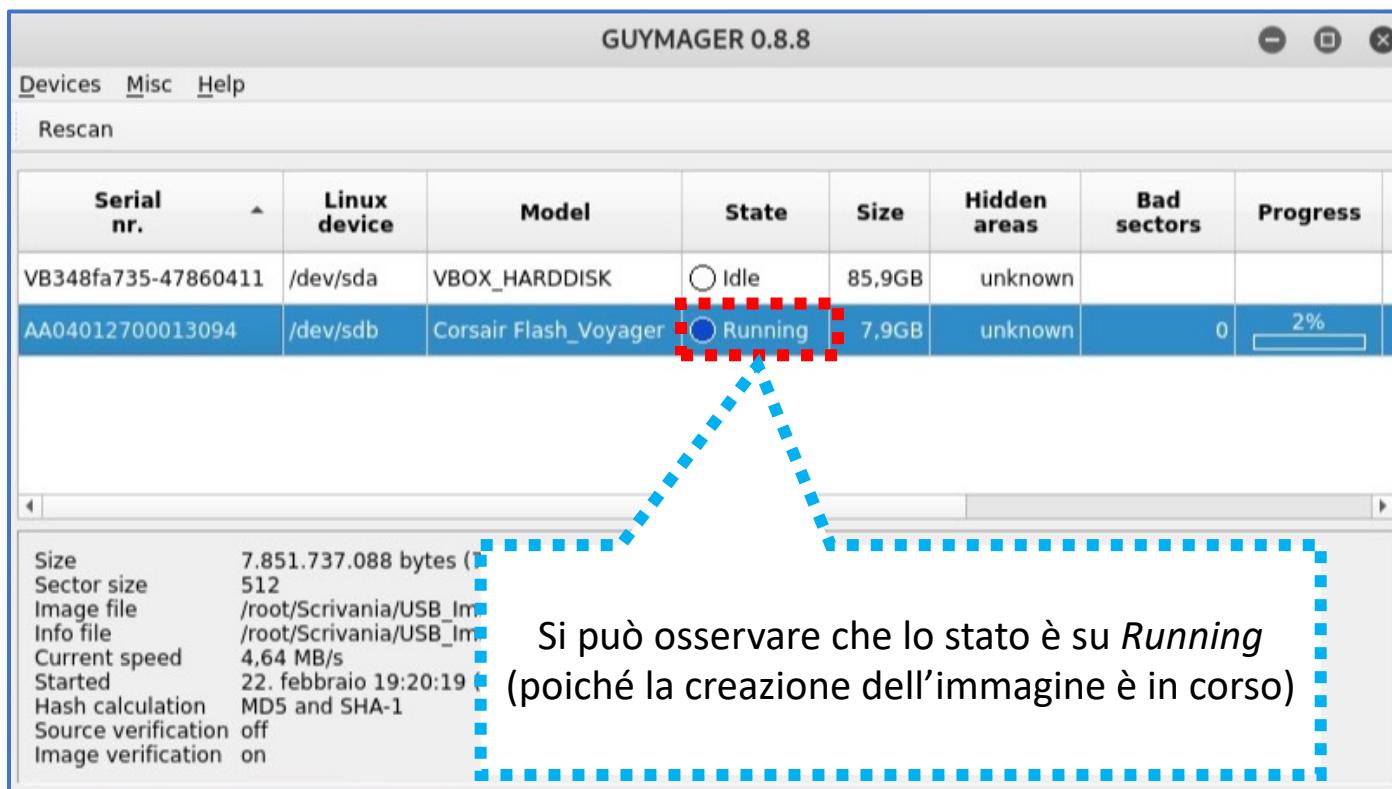
- A seguito dell'avvio del processo, si otterrà una schermata simile alla seguente:



# Il tool Guymager

## Esempio di Utilizzo | 1/3

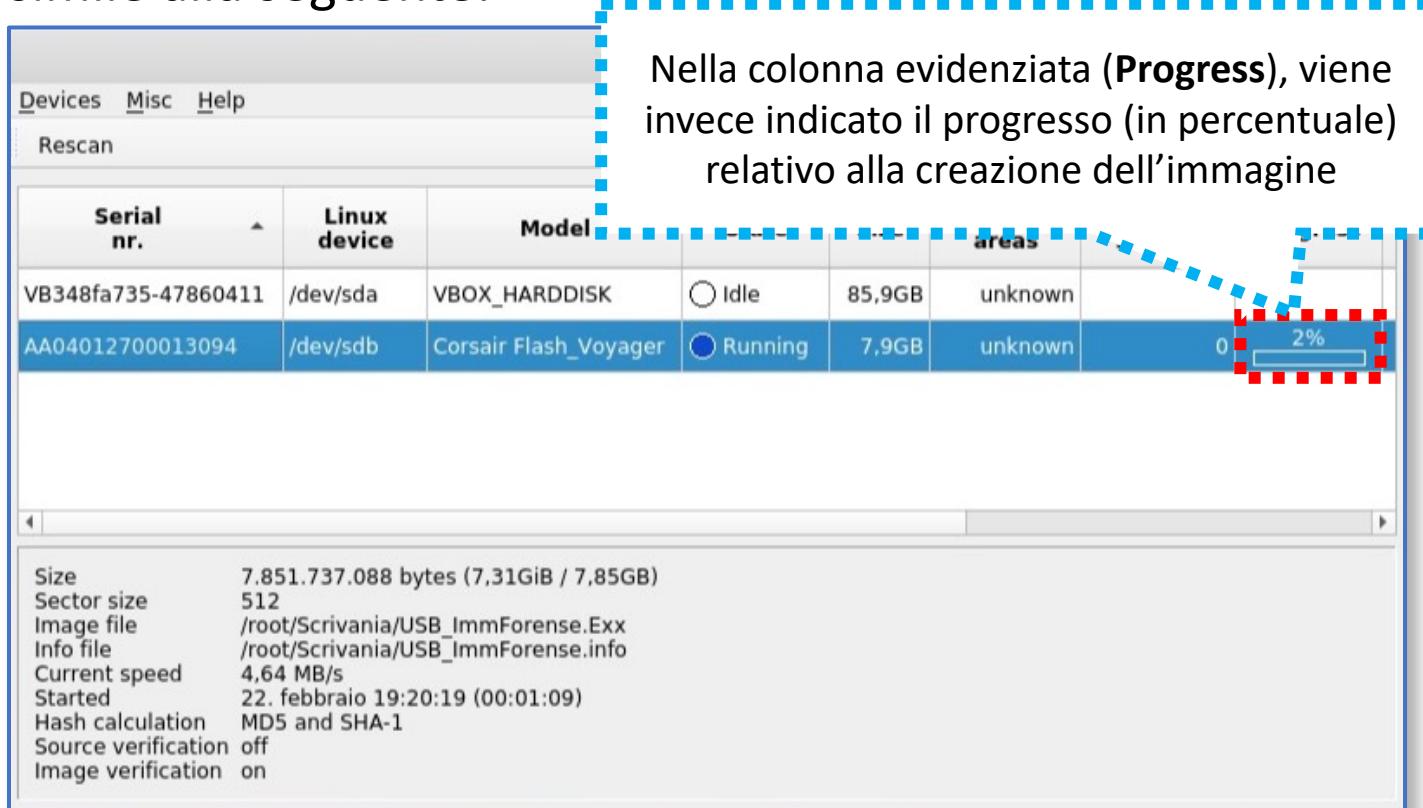
- A seguito dell'avvio del processo, si otterrà una schermata simile alla seguente:



# Il tool Guymager

## Esempio di Utilizzo | 1/3

- A seguito dell'avvio del processo, si otterrà una schermata simile alla seguente:



# Il tool Guymager

## Esempio di Utilizzo | 2/3

- Dai dettagli, possiamo vedere alcune specifiche, in relazione al processo di acquisizione

Size	7.851.737.088 bytes (7,31GiB / 7,85GB)
Sector size	512
Image file	/root/Scrivania/USB_ImmForense.Exx
Info file	/root/Scrivania/USB_ImmForense.info
Current speed	4,64 MB/s
Started	22. febbraio 19:20:19 (00:01:09)
Hash calculation	MD5 and SHA-1
Source verification	off
Image verification	on

# Il tool Guymager

## Esempio di Utilizzo | 2/3

- Dai dettagli, possiamo vedere alcune specifiche, in relazione al processo di acquisizione

Size	7.851.737.088 bytes (7,31GiB / 7,85GB)
Sector size	512
Image file	/root/Scrivania/USB_ImmForense.Exx
Info file	/root/Scrivania/USB_ImmForense.info
Current speed	4,64 MB/s
Started	22. febbraio 19:20:19 (00:01:09)
Hash calculation	MD5 and SHA-1
Source verification	off
Image verification	on

Viene riportata la **dimensione (Size)** del supporto (in questo esempio, si tratta di un supporto di 8 GB) e la **dimensione di un settore di traccia (Sector size)**

# Il tool Guymager

## Esempio di Utilizzo | 2/3

- Dai dettagli, possiamo vedere alcune specifiche, in relazione al processo di acquisizione

Size	7.851.737.088 bytes (7,31GiB / 7,85GB)
Sector size	512
Image file	:/root/Scrivania/USB_ImmForense.Exx
Info file	:/root/Scrivania/USB_ImmForense.info
Current speed	4,64 MB/s
Started	22. febbraio 19:20:19 (00:01:09)
Hash calculation	MD5 and SHA-1
Source verification	off
Image verification	on

Il percorso relativo all'immagine (**Image file**) ed il percorso relativo al file di info (**Info file**)

# Il tool Guymager

## Esempio di Utilizzo | 2/3

- Dai dettagli, possiamo vedere alcune specifiche, in relazione al processo di acquisizione

Size	7.851.737.088 bytes (7,31GiB / 7,85GB)
Sector size	512
Image file	/root/Scrivania/USB_ImmForense.Exx
Info file	/root/Scrivania/USB_ImmForense.info
Current speed	4,64 MB/s
Started	22. febbraio 19:20:19 (00:01:09)
Hash calculation	MD5 and SHA-1
Source verification	off
Image verification	on

La **velocità corrente (Current speed)** del processo di acquisizione (in questo esempio, circa 4,64 MB al secondo)

# Il tool Guymager

## Esempio di Utilizzo | 2/3

- Dai dettagli, possiamo vedere alcune specifiche, in relazione al processo di acquisizione

Size	7.851.737.088 bytes (7,31GiB / 7,85GB)
Sector size	512
Image file	/root/Scrivania/USB_ImmForense.Exx
Info file	/root/Scrivania/USB_ImmForense.info
Current speed	4,64 MB/s
Started	22, febbraio 19:20:19 (00:01:09)
Hash calculation	MD5 and SHA-1
Source verification	off
Image verification	on

Le funzioni per il calcolo dell'hash (**Hash calculation**) per la verifica d'integrità dell'immagine (nell'esempio, sono stati scelti MD5 e SHA-1)

# Il tool Guymager

## Esempio di Utilizzo | 2/3

- Dai dettagli, possiamo vedere alcune specifiche, in relazione al processo di acquisizione

Size	7.851.737.088 bytes (7,31GiB / 7,85GB)
Sector size	512
Image file	/root/Scrivania/USB_ImmForense.Exx
Info file	/root/Scrivania/USB_ImmForense.info
Current speed	4,64 MB/s
Started	22. febbraio 19:20:19 (00:01:09)
Hash calculation	MD5 and SHA-1
Source verification	off
Image verification	on

Attivazione/Disattivazione della verifica della sorgente (**Source verification**) e della verifica dell'immagine (**Image verification**)

Nell'esempio, la verifica della sorgente è disattiva (*off*), mentre la verifica dell'immagine è attiva (*on*)

# Il tool Guymager

## Esempio di Utilizzo | 3/3

- Al termine del processo di acquisizione e verifica, nello stato verrà indicata la stringa *Finished – Verified & ok* e la barra del progresso risulterà al 100%

Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress
VB348fa735-47860411	/dev/sda	VBOX_HARDDISK	Idle	85,9GB	unknown		
AA04012700013094	/dev/sdb	Corsair Flash_Voyager	Finished - Verified & ok	7,9GB	unknown	0	100%

# Il tool Guymager

## Esempio di Utilizzo | 3/3

- Al termine del processo di acquisizione e verifica, nello stato verrà indicata la stringa *Finished – Verified & ok* e la barra del progresso risulterà al 100%

Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress
VB348fa735-47860411	/dev/sda	VBOX_HARDDISK	Idle	85,9GB	unknown		
AA0401270013094	/dev/sdb	Corsair Flash_Voyager	Finished - Verified & ok	7,9GB	unknown	0	100%

- Nella posizione prescelta (sul *Desktop*, nell'esempio), saranno individuabili i file prodotti dal processo di acquisizione

```
root@kali:~/Scrivania# ls
USB_ImmForense.E01  USB_ImmForense.info
root@kali:~/Scrivania#
```

# Il tool Guymager

## Verifica mediante le funzioni di Hash

- Il file *info* prodotto da Guymager contiene diverse e utili informazioni
- È possibile visionare i valori ottenuti dalle funzioni di hash

```
State: Finished successfully

MD5 hash           : 08c4886b1447f6aa0007f98432edea3b
MD5 hash verified source : --
MD5 hash verified image   : 08c4886b1447f6aa0007f98432edea3b
SHA1 hash          : 6260c4f111e0a886976880d33e5fc53dc8a126f2
SHA1 hash verified source : --
SHA1 hash verified image   : 6260c4f111e0a886976880d33e5fc53dc8a126f2
SHA256 hash         : --
SHA256 hash verified source: --
SHA256 hash verified image : --
```

- Viene inoltre riportato se la verifica è stata effettuata con successo o se sono stati individuati errori

```
SHA1 hash verified image   : 6260c4f111e0a886976880d33e5fc53dc8a126f2
SHA256 hash             : --
SHA256 hash verified source: --
SHA256 hash verified image : --
Image verification OK. The image contains exactly the data that was written.
```

# Il tool Guymager

## Immagini Forensi e Live System | 1/3

- Nell'ambito di un live system, è comunque possibile creare una immagine forense del disco fisso, sul quale è in attività il S.O. ed eventuali altri software (questo processo è denominato anche **live disk acquisition**)
- *Passi Principali:*
  1. Esecuzione di un tool per l'acquisizione forense (**NOTA:** Il tool viene eseguito sul S.O., in attività, del live system)
    - *Esempi*
      - Nel caso di live system con un S.O. Linux-based, è possibile utilizzare Guymager, DC3DD, ecc.
      - Nel caso di live system con un S.O. Windows-based, sono disponibili diversi appositi tool (ad esempio, FTK® Imager, ecc.)
    - 2. Acquisizione di una immagine forense del disco fisso su cui è in attività il S.O. ed eventuali altri software (tale disco fisso sarà considerato il disco fisso sorgente, nel processo di imaging)

# Il tool Guymager

## Immagini Forensi e Live System | 2/3

### OSSERVAZIONI IMPORTANTI

- L'immagine forense acquisita sarà relativa ad un certo punto nel tempo
  - Verosimilmente verranno apportate modifiche al contenuto del disco fisso sorgente, anche dopo la creazione dell'immagine forense
    - Le modifiche verranno apportate dai vari software in esecuzione sul live system (ad esempio, S.O., eventuali applicazioni, driver, ecc.)
- In virtù delle suddette considerazioni, **non è quindi possibile preservare l'integrità del disco fisso sorgente**
- Tuttavia, è possibile preservare l'integrità della prova, considerando la prima immagine forense acquisita

# Il tool Guymager

## Immagini Forensi e Live System | 3/3

*Esempio di esecuzione del processo di live data acquisition,  
mediante Guymager*

Serial nr.	Linux device	Model	State	Size	Hidden areas	Ba sect
VBe5ede226-6f19196a	/dev/sda	VBOX_HARDDISK	Running	42.9GB	unknown	

Size	42,949,672,960 bytes (40.0GiB / 42.9GB)
Sector size	512
Image file	/root/test.dd
Info file	/root/test.info
Current speed	162.43 MB/s
Started	10. March 15:15:07 (00:00:08)
Hash calculation	MD5
Source verification	off
Image verification	on

# Il tool Guymager

## Immagini Forensi e Live System | 3/3

*Esempio di esecuzione del processo di live data acquisition,  
mediante Guymager*

Serial nr.	Linux device	Model	State	Size	Hidden areas	Ba sect
VBe5ede226-6f19196a	/dev/sda	VBOX HARDDISK	Running	42.9GB	unknown	

È stata avviata la creazione di una immagine forense del disco fisso  
(avente path /dev/sda), su cui è installato (ed è in attività) un S.O.  
Linux-based (nello specifico, Parrot Security Linux)

Size	42,949,672,960 bytes (40.0GiB / 42.9GB)
Sector size	512
Image file	/root/test.dd
Info file	/root/test.info
Current speed	162.43 MB/s
Started	10. March 15:15:07 (00:00:08)
Hash calculation	MD5
Source verification	off
Image verification	on