COMPUTER FORENSICS

Lezione 6: Fasi del trattamento *identificazione e raccolta*

SICUREZZA SISTEMI RETI INFORMATICHE

UNIVERSITA' DEGLI STUDI DI NAPOLI FEDERICO II

A.A. 2021/22

Dott. Lorenzo LAURATO

Cosa è la Computer Forensics?

l'insieme di metodologie scientificamente provate finalizzate alla ricostruzione di eventi ai fini probatori che coinvolgono direttamente o indirettamente un supporto digitale

Fasi

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

Identificazione dell'evidence

- Ricercare la fonte di prova che può dare una svolta alle indagini: la prima fase è volta a individuare dove un dato è conservato.

Identificazione dell'evidence

Vanno individuati tutti i dispositivi che possono contenere dati rilevanti:

- Computer/Notebook
- Cellulari e Tablet
- Memory Card, PenDrive, Hard Disk Esterni, CD/DVD
- Fotocamere e Videocamere
- Server
- Stampanti, Fax, Router

Identificazione dell'evidence

il Cloud

Identificazione dell'evidence

individuare i dispositivi che possono contenere
<u>dati rilevanti</u>

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;

Identificazione dell'evidence

la «preview»

DEAD

- è un'analisi eseguita con il S.O. spento.
- uso di **write block**: permette di non alterare il dispositivo da analizzare;
  - Hardware

Identificazione dell'evidence

la «preview»

DEAD

- Software: distro Linux Live

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;

Identificazione dell'evidence

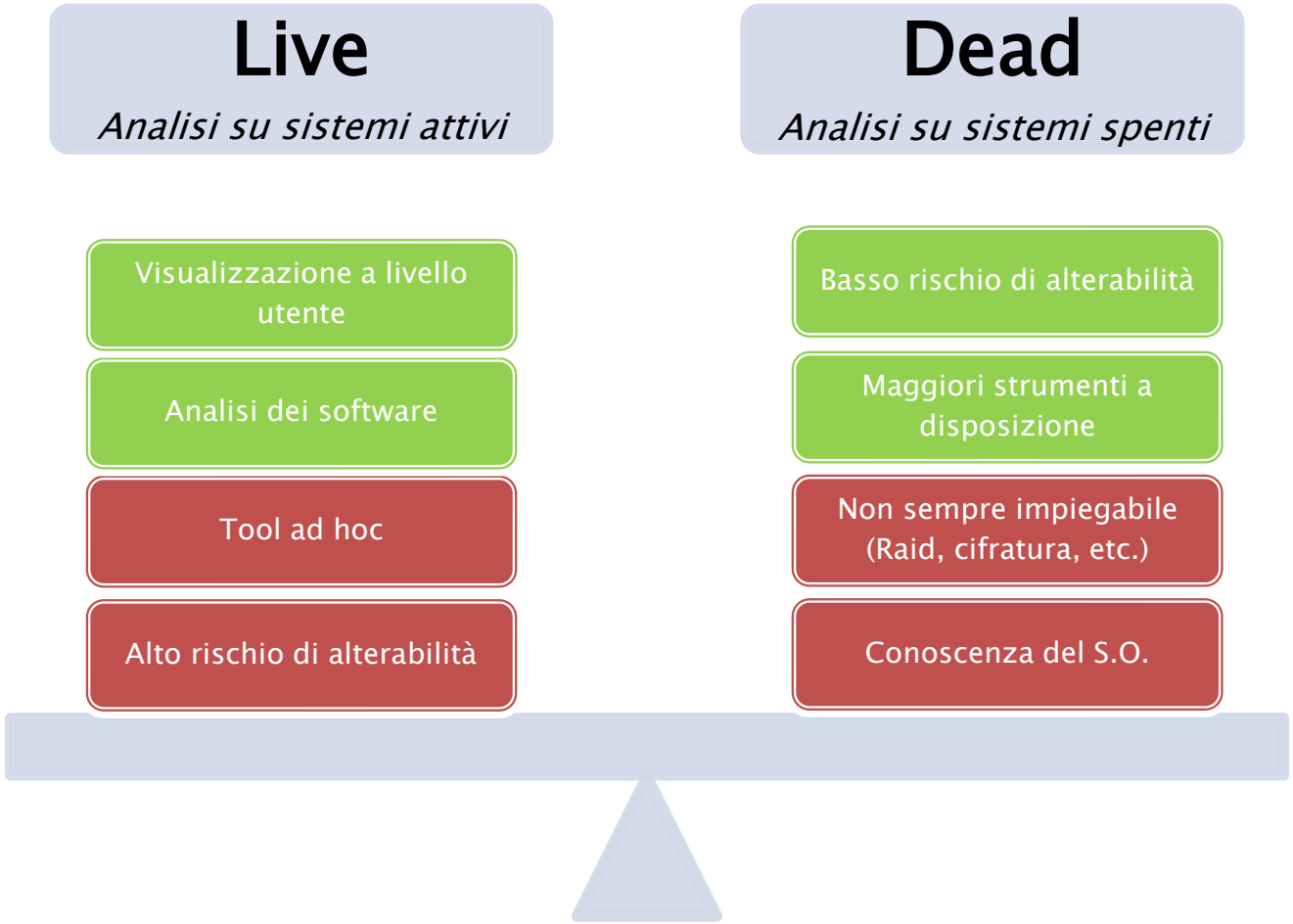
la «preview»

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»



Cambiamento di stato del dispositivo

Acceso → Spento

Spento → Acceso

Cambiamento di stato del dispositivo *shutdown*

- Prima di eseguirlo valutare le seguenti criticità:
  - Cifratura
  - Software in esecuzione
  - Dump della RAM
- Come spegnere il dispositivo che si vuole analizzare/sequestrare:
  - Scollegarlo dalla rete elettrica *(unplug):*
    - Potrebbe compromettere il funzionamento del sistema (Server, Raid, etc.)
  - Eseguire lo spegnimento mediante il S.O.:
    - Vengono eseguite sul disco diverse operazioni (Aggiornamenti, esecuzioni di batch, etc.)

Cambiamento di stato del dispositivo *accensione*

- Valutare se le informazioni che perderemo sono meno importanti dell'urgenza dell'accertamento:
  - Ultimo accesso al sistema;
  - Esecuzione sul disco di diverse operazioni;

Fasi

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

La Raccolta:
il sequestro

- Dopo aver identificato i dispositivi o i dati di possibile interesse investigativo si procede con il sequestro:
  - **Fisico**: prendere fisicamente il supporto su cui il dato di possibile interesse risiede.
  - **Logico**: eseguire una copia totale o parziale della memoria del dispositivo

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:
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

La Raccolta:
il sequestro fisico

non è sempre fattibile

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

La Raccolta:
il sequestro logico

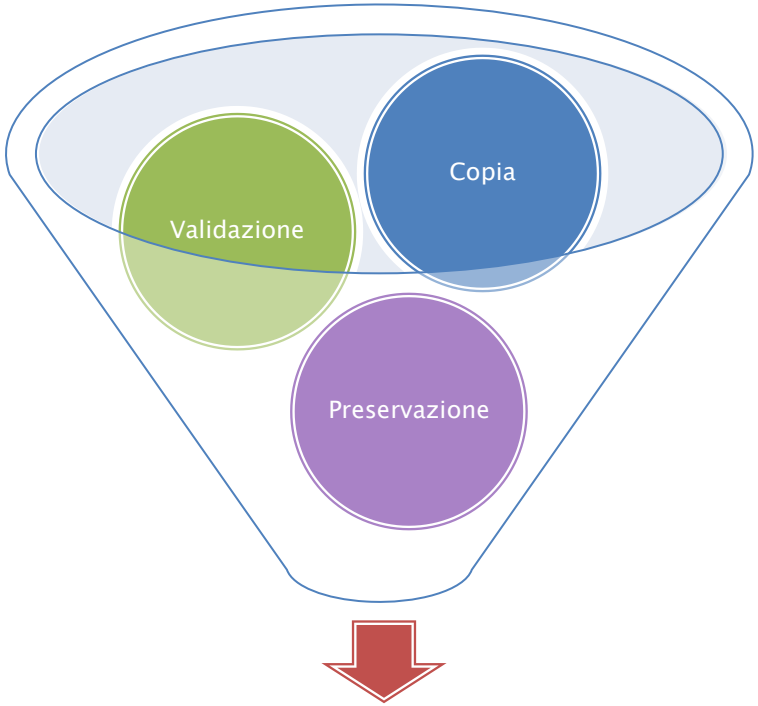
- Duplicazione dei dati di [*possibile*] interesse investigativo;

COPIA FORENSE

La Raccolta:
Copia Forense

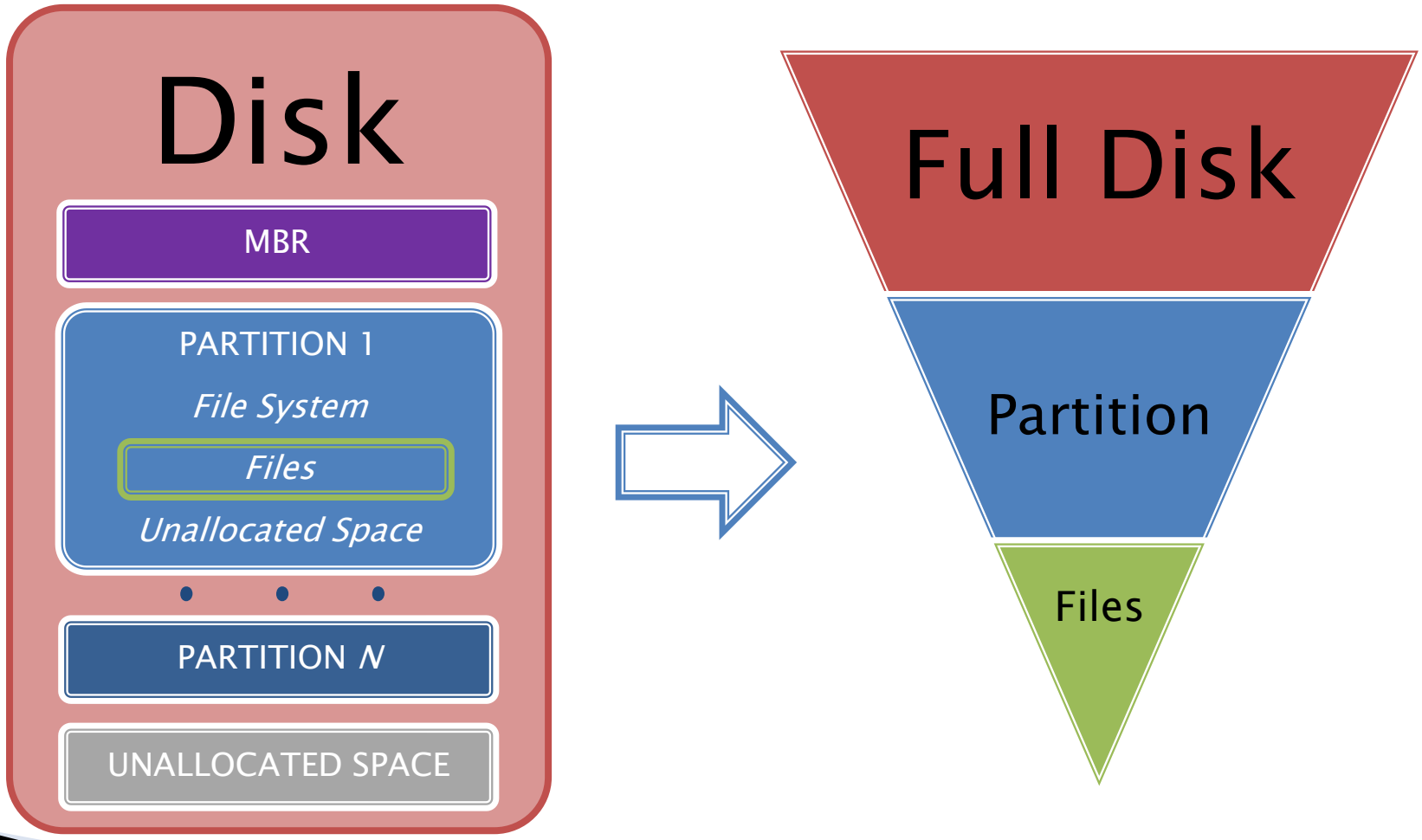
GARANZIA DI RIPETIBILITA' DEI SUCCESSIVI ACCERTAMENTI CHE VERRANNO ESEGUITI SULLA COPIA FORENSE

La Raccolta:
Copia Forense



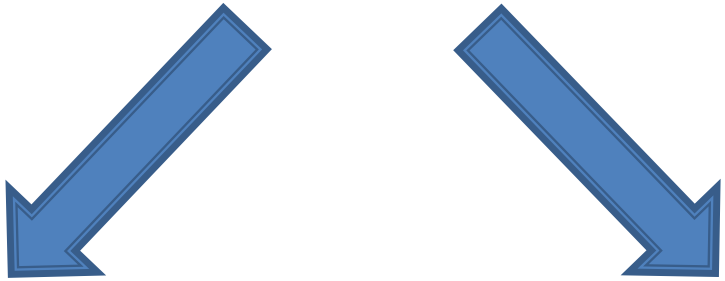
Copia Forense

La Raccolta:
Copia Forense



Copia Forense
Acquisizione Fisica

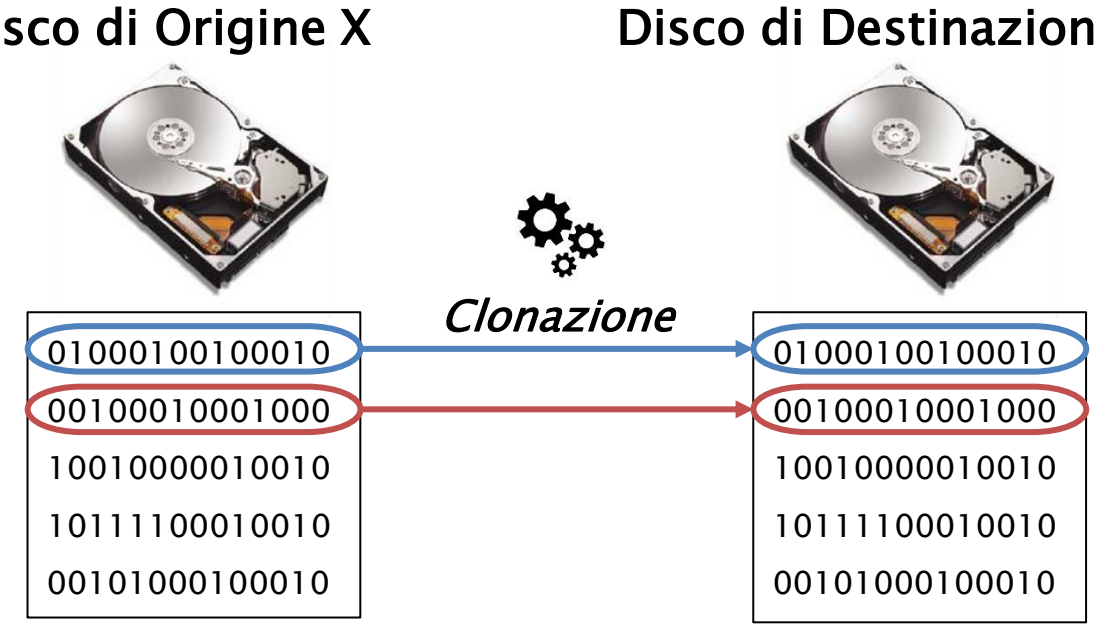
- Copia ***«bit a bit»*** dell'intero supporto di memoria: dati e qualsiasi informazione sulla gestione dei dati (*tabella partizioni, Master Boot Record, meta dati del file system, etc.*):



Clonazione **File Immagine**

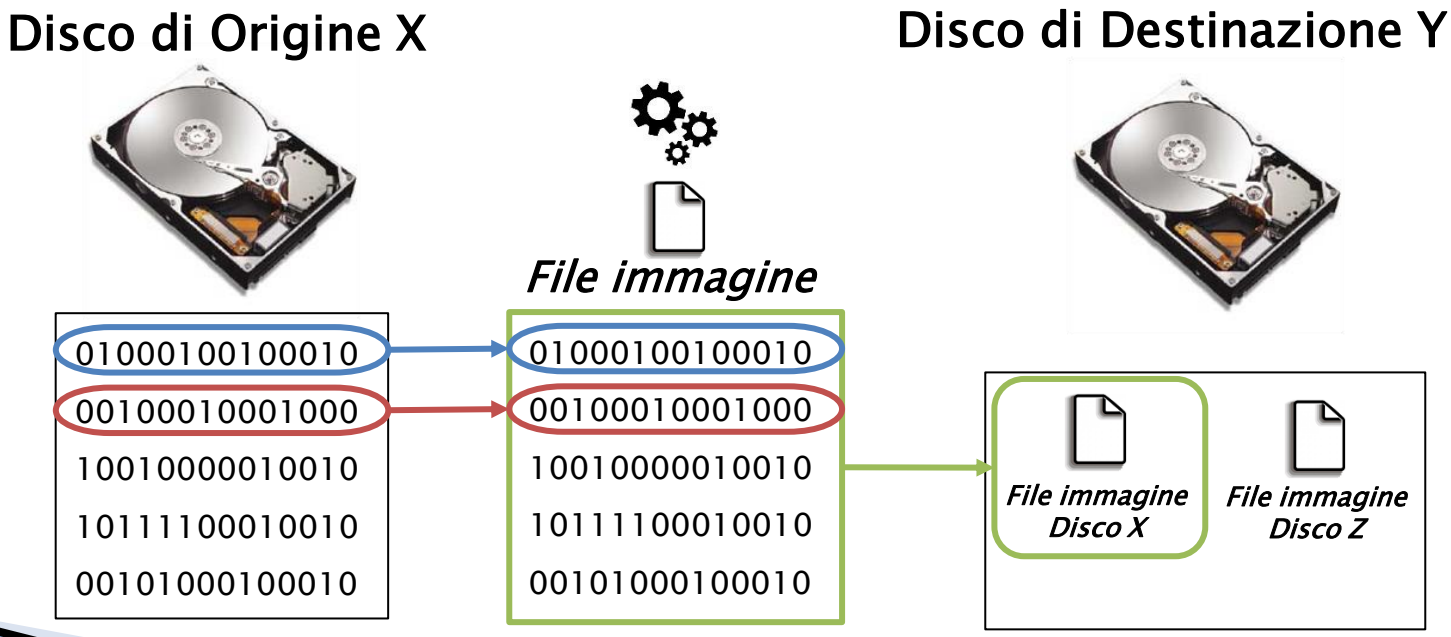
Copia Forense
Acquisizione Fisica

- La **Clonazione** ha come risultato un supporto pressoché identico a quello originale.
  - È facilmente alterabile
  - E' utilizzato solo in casi particolari: bisogna analizzare il supporto reinserendolo all'interno del proprio habitat;



Copia Forense
Acquisizione Fisica

- La generazione di un **file immagine** (*bit stream image*) ha come risultato un file rappresentate il supporto originale.
  - è maneggevole;
  - può essere utilizzato per generare un disco clone;



Copia Forense
gli strumenti

Hardware

VS

Software

deft

HELIX3

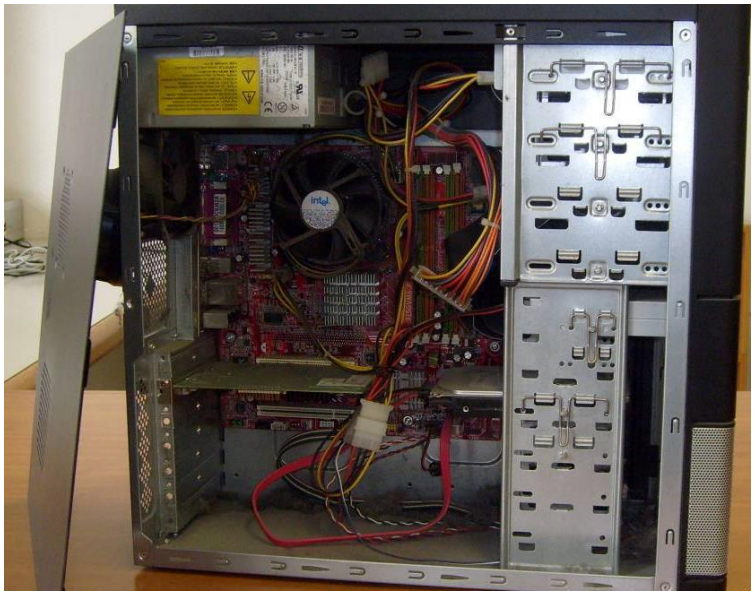
CAINE

Copia Forense
gli strumenti

- **Hardware**: duplicatori forensi
  - Certificati
  - Prestanti
  - Costosi

- **Software**: distro linux live forensi
  - Gratuiti
  - OpenSource
  - Versatili

Copia Forense
gli strumenti



Copia Forense
gli strumenti

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

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