

*Procedure, standard e tecnologie di acquisizione ad analisi di  
dati a uso forense*

Michele Ferrazzano

# **Uno standard internazionale contenente linee guida per identificazione, raccolta, acquisizione e conservazione di evidente digitali**

- Information technology
  - Security techniques
    - **Guidelines for identification, collection, acquisition and preservation of digital evidence**

# ISO e IEC

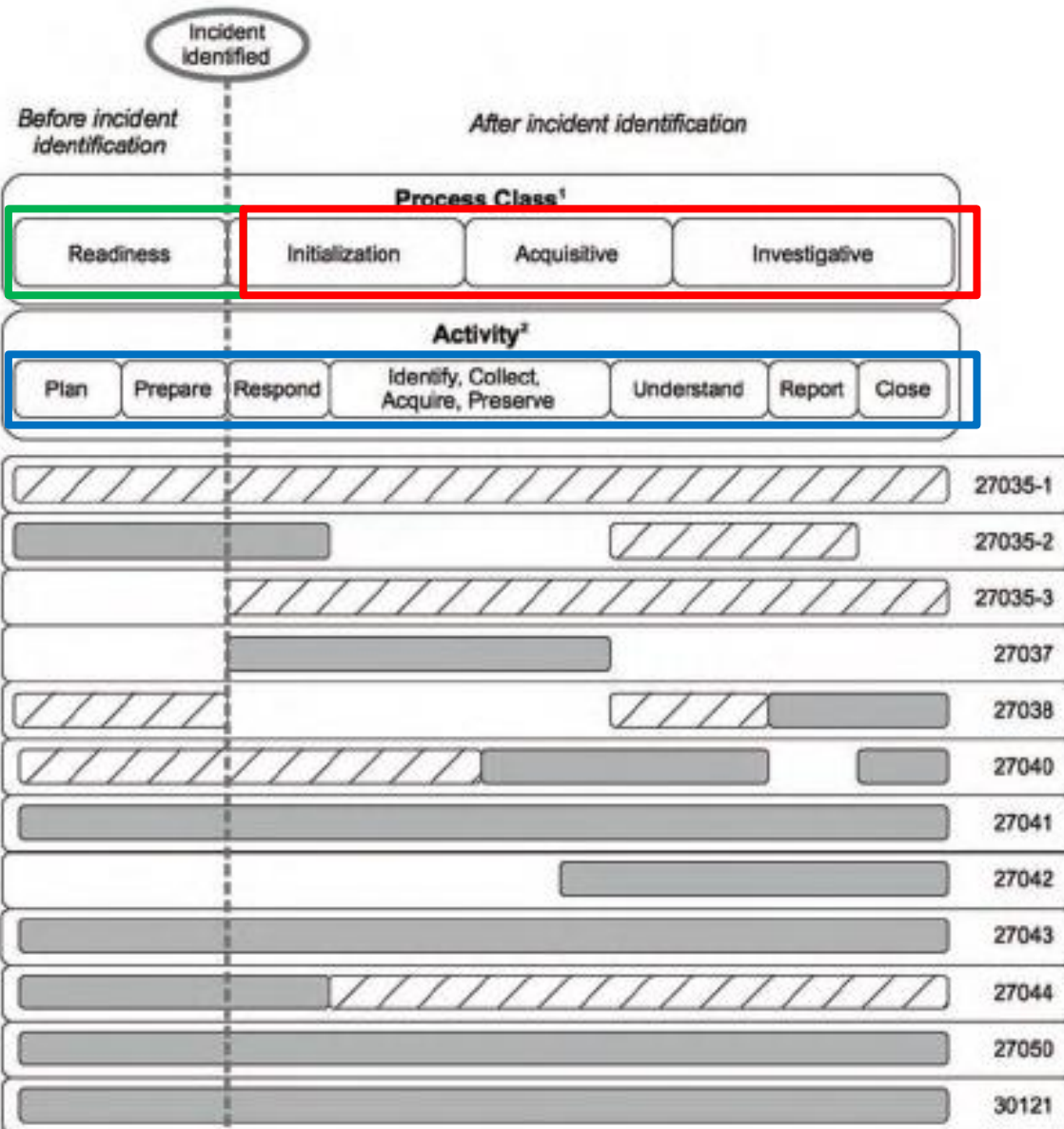


- International Organization for Standardization
- La più importante organizzazione a livello mondiale per la definizione di norme tecniche
- Fondata il 23 febbraio 1947, quartier generale a Ginevra
- Membri dell'ISO sono gli organismi nazionali di standardizzazione di 162 Paesi del mondo
- ISO coopera strettamente con IEC, responsabile per la standardizzazione degli equipaggiamenti elettrici



- International Electrotechnical Commission
- Organizzazione internazionale per la definizione di standard in materia di elettricità, elettronica e tecnologie correlate
- Fondata nel 1906; ed inizialmente aveva sede a Londra; nel 1948 ha spostato la sua sede a Ginevra. Ad essa attualmente partecipano più di 60 paesi.
- Molti dei suoi standard sono definiti in collaborazione con ISO
- Commissione formata da rappresentanti di enti di standardizzazione nazionali

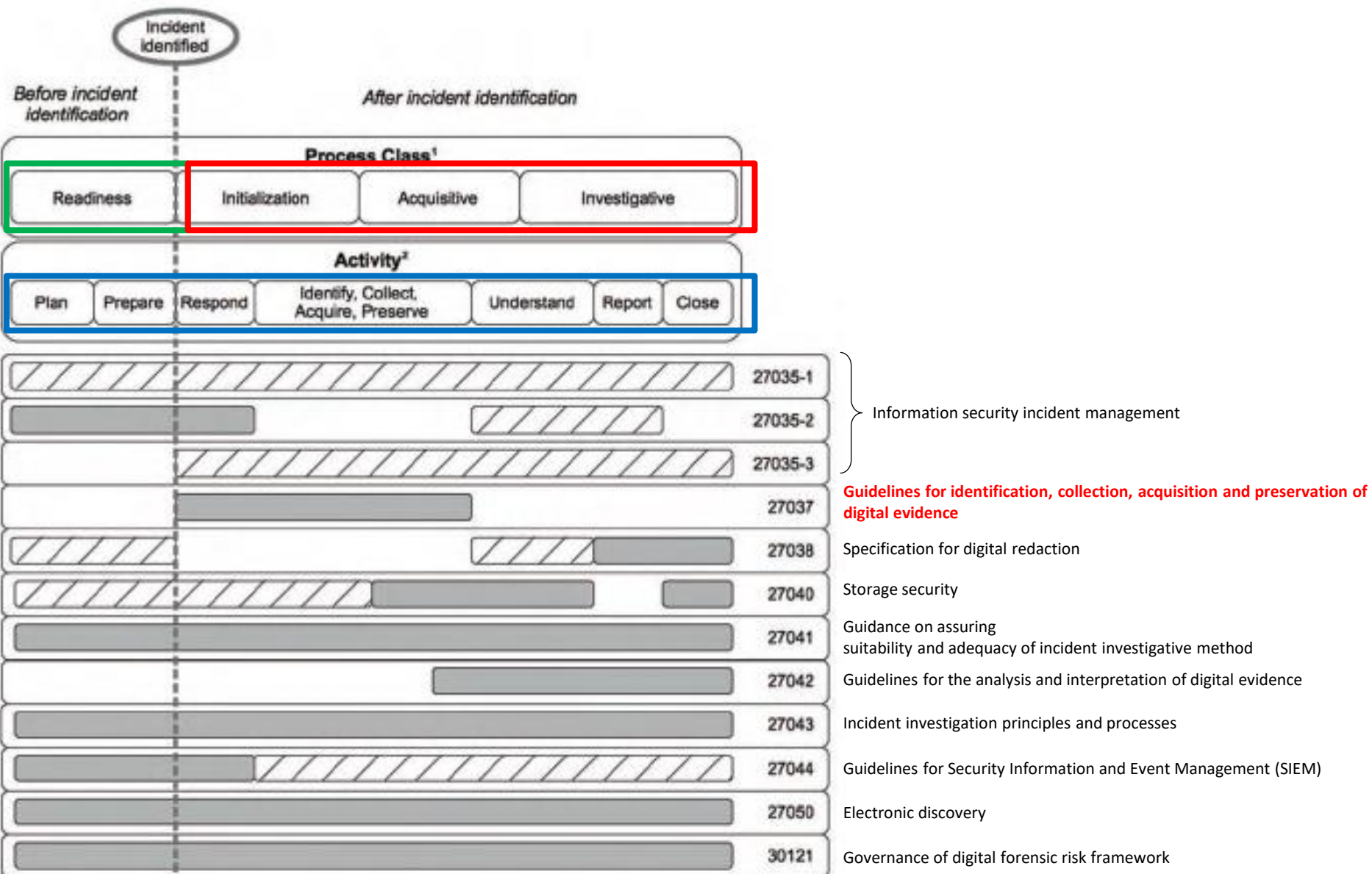
# ISO/IEC – Panoramica generale



Key	
	International standard can be directly applied to these activities.
	International standard contains information which may influence and/or assist with these activities.

<sup>1</sup> Process classes are defined in ISO/IEC 27043.  
<sup>2</sup> Detail of activities is given in ISO/IEC 27035-2, ISO/IEC 27037:2012, and ISO/IEC 27042.

# ISO/IEC – Panoramica generale



# ISO/IEC 27037/2012

## Altri standard di riferimento

- **ISO/TR 15801:2009**
  - Document management - Information stored electronically - Recommendations for trustworthiness and reliability
- **ISO/IEC 17020:2012**
  - Conformity assessment - Requirements for the operation of various types of bodies performing inspection
- **ISO/IEC 17025:2005**
  - General requirements for the competence of testing and calibration laboratories
- **ISO/IEC 27000:2012**
  - Information technology - Security techniques - Information security management systems - Overview and vocabulary



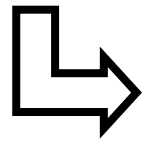
- Trattamento del reperto informatico
- Definizione linee guida nelle fasi di
  - Identificazione (ispezione)
  - Raccolta (sequestro)
  - Acquisizione (sequestro virtuale)
  - Conservazione (conservazione e sigillo)
- Integrità della prova informatica e metodologia al fine di rendere ammissibile la prova in giudizio
  - Per prova informatica si fa riferimento a dati già in formato digitale
  - Esclusi quindi dati in formato analogico convertiti in formato digitale



- Aspetti legali
  - È internazionale, non legata ad un singolo ordinamento
- Analisi
- Strumenti tecnici
- Redazione di report e presentazione
- Trattamento di dati analogici

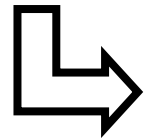
# Le fasi del trattamento del dato e intervento dello standard ISO 27037

Identificazione

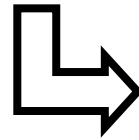


Raccolta

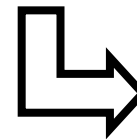
- acquisizione
- conservazione
- trasporto



Analisi



Valutazione



Presentazione



# ISO/IEC 27037/2012

## Di cosa si occupa

- Per ogni fase
  - Documentazione (logging)
  - Tracciabilità (chain of custody)
  - Priorità di intervento (plan)
  - Imballaggio dei reperti (protection)
  - Trasporto dei reperti (real/virtual)
  - Ruoli nel passaggio dei reperti (who & why)

# ISO/IEC 27037/2012

## Persone che trattano reperti informatici



### Digital evidence first responders (DEFs)

Operatore che si avvicina per primo ai sistemi (supporti di memorizzazione e dati) di potenziale interesse  
Adeguate esperienze e competenze  
Può avvalersi di collaboratori

### Digital evidence specialists (DEs)

Operatore esperto di evidenze informatiche

### Incident response specialists

Operatore che si occupa del primo intervento post incidente informatico  
In Italia spesso coincide (ahimè) con l'amministratore di sistema

### Forensic laboratory managers

Operatore responsabile di laboratorio informatico forense

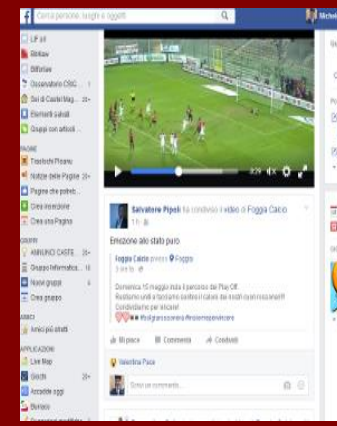
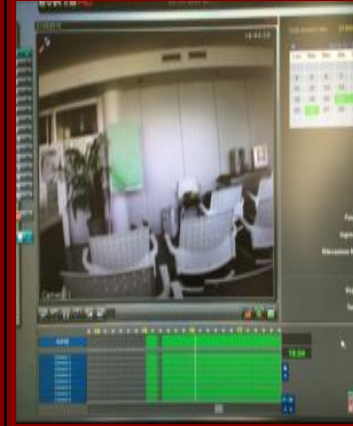
# ISO/IEC 27037/2012

## Persone che trattano reperti informatici e precauzioni - DEFR

- Compiti del DEFR
  - mettere in sicurezza e proteggere il luogo appena possibile
  - controllare l'area che contiene dispositivi di memorizzazione digitale
  - individuare il responsabile dell'area
  - allontanare le persone dai dispositivi digitali e dall'alimentazione elettrica
  - documentare tutti quelli che sono autorizzati ad accedere all'area
    - Individuare persone con possibili moventi o persone chiave nell'organizzazione
  - non mutare lo stato delle apparecchiature
    - se acceso non spegnere, se spento non accendere
  - documentare la scena, componenti, cavi
    - fotografie, video, disegni, schemi, planimetrie
  - individuare note, appunti, diari, fogli, manuali
    - ricerca password, PIN

# ISO/IEC 27037/2012

## Dispositivi di memorizzazione che contengono dati



Dispositivi di memorizzazione utilizzati nei computer quali dischi rigidi, floppy disk, supporti ottici, supporti magneto-ottici e altri dispositivi con funzioni simili

Telefoni cellulari, Personal Digital Assistants (PDAs), Personal Electronic Devices (PEDs), memory cards, sistemi di navigazione mobile (GPS)

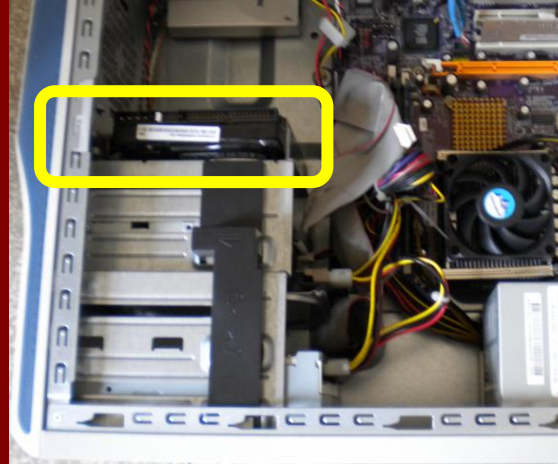
Fotocamere e videocamere (incluse quelle a circuito chiuso)

Sistemi informatici con connessione di rete e reti basate sul protocollo TCP/IP e su altri protocolli

Altri dispositivi assimilabili a quelli sopra definiti e quant'altro verrà inventato ed utilizzato in futuro

*La lista è indicativa e non esaustiva...*

# Glossario



## Dispositivo digitale

## Dispositivo di memorizzazione di dati digitali

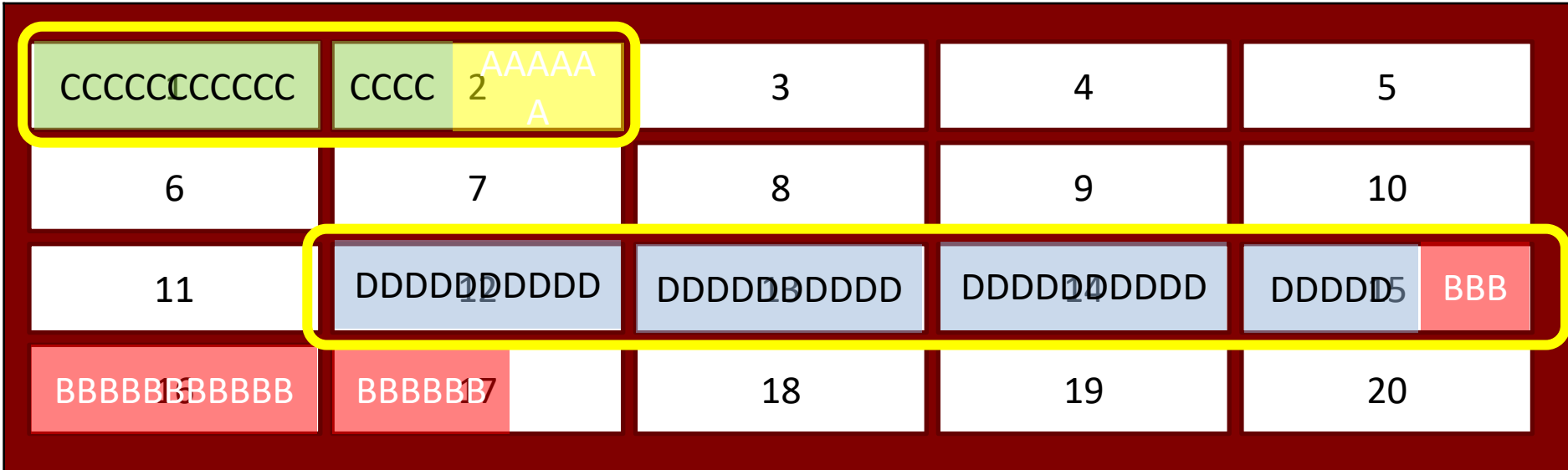
## Periferica

Apparato elettronico usato per processare o memorizzare dati digitali

Dispositivo che è in grado di memorizzare dati digitali  
[ISO/IEC 10027:1990]

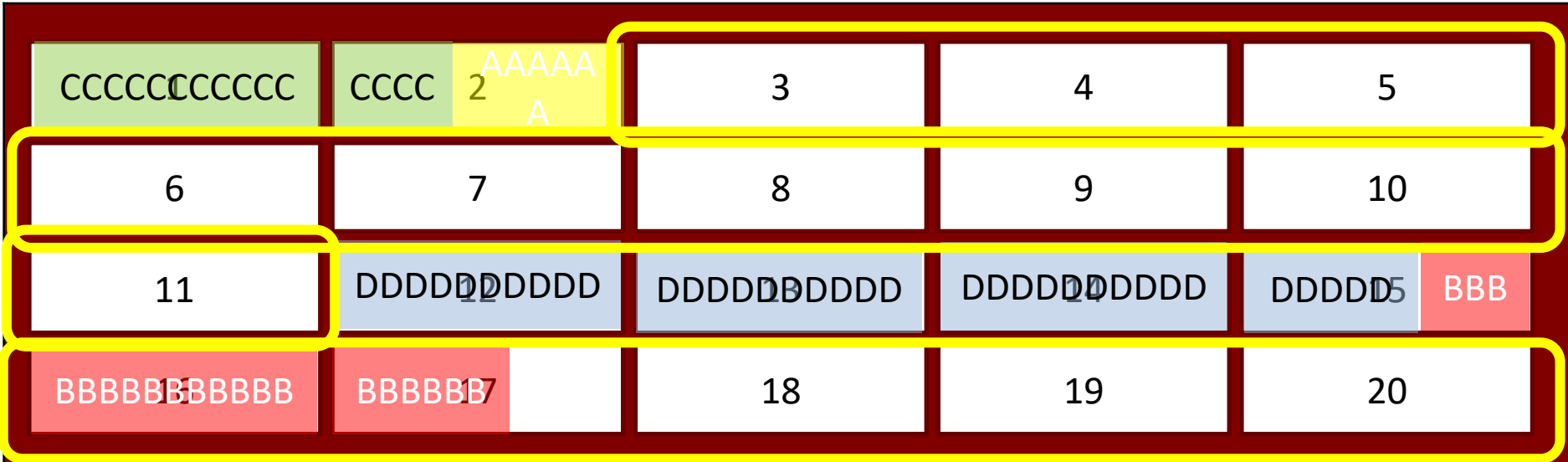
Dispositivo che, connesso ad un dispositivo digitale, ne estende le funzionalità

# Glossario



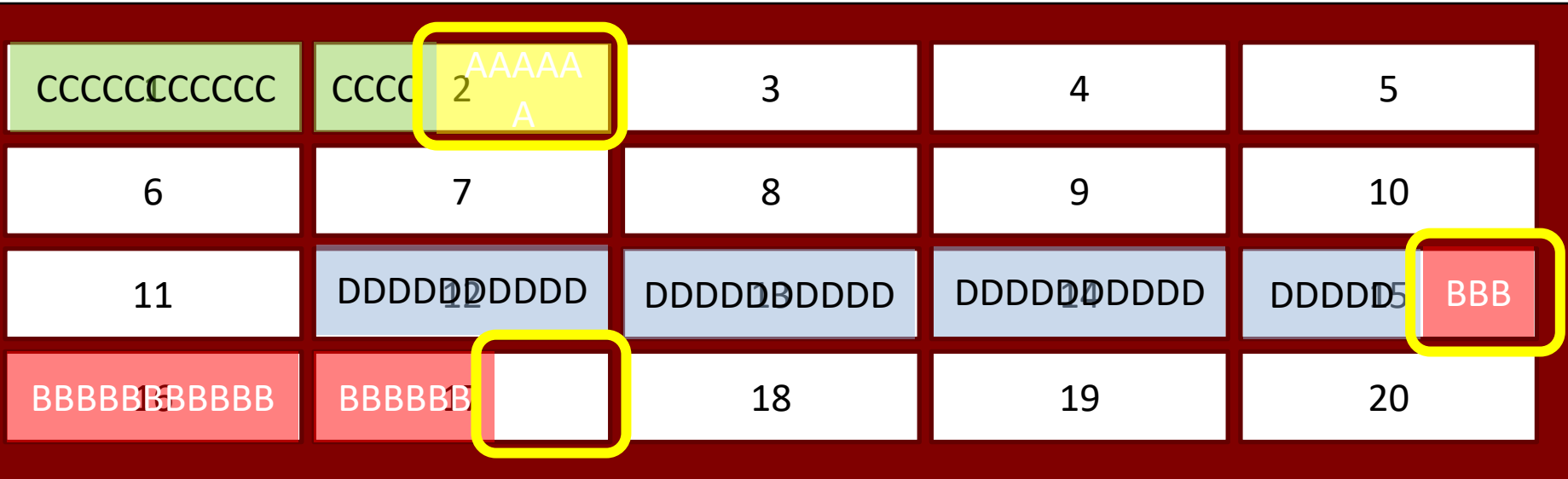
<b>Spazio allocato</b>	<b>Spazio non allocato</b>	<b>Slack space</b>
Area di un dispositivo di memoria che è utilizzata per memorizzare dati, inclusi metadati	Area di un dispositivo di memoria che non è allocato dal sistema operativo ed è a disposizione per memorizzare dati, inclusi metadati	Area (compresa tra l'ultimo bit e la fine del settore) non utilizzata dal file che ha allocato lo spazio per ultimo

# Glossario



<b>Spazio allocato</b>	<b>Spazio non allocato</b>	<b>Slack space</b>
Area di un dispositivo di memoria che è utilizzata per memorizzare dati, inclusi metadati	Area di un dispositivo di memoria che non è allocato dal sistema operativo ed è a disposizione per memorizzare dati, inclusi metadati	Area (compresa tra l'ultimo bit e la fine del settore) non utilizzata dal file che ha allocato lo spazio per ultimo

# Glossario

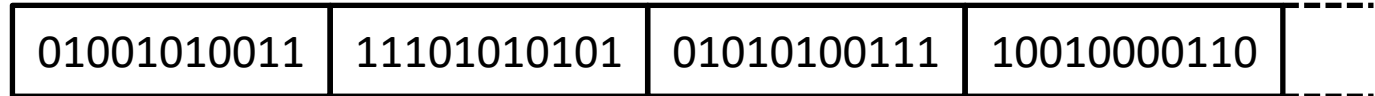


<b>Spazio allocato</b>	<b>Spazio non allocato</b>	<b>Slack space</b>
Area di un dispositivo di memoria che è utilizzata per memorizzare dati, inclusi metadati	Area di un dispositivo di memoria che non è allocato dal sistema operativo ed è a disposizione per memorizzare dati, inclusi metadati	Area (compresa tra l'ultimo bit e la fine del settore) non utilizzata dal file che ha allocato lo spazio per ultimo

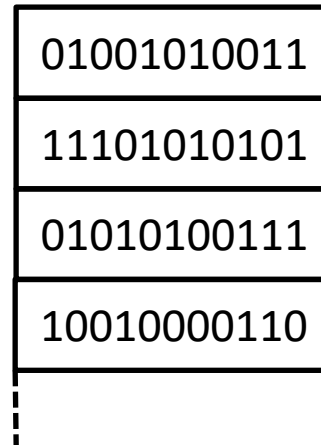


# Glossario

## Spazio allocato vs. non allocato (vs. slack)

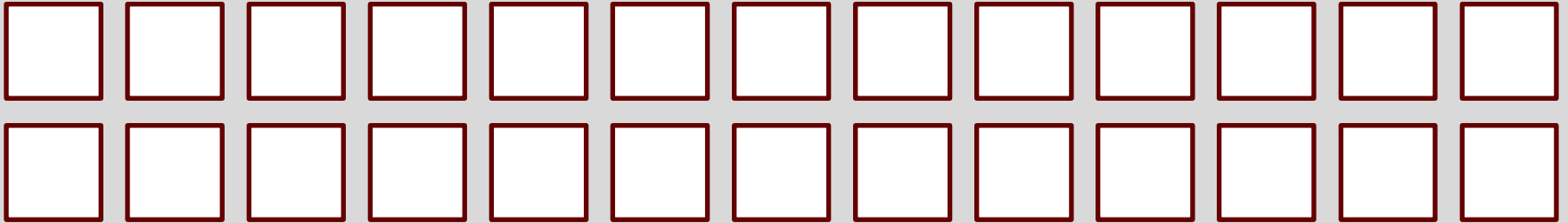


O più comunemente...



# File system: allocazione dei file

## Indice



...

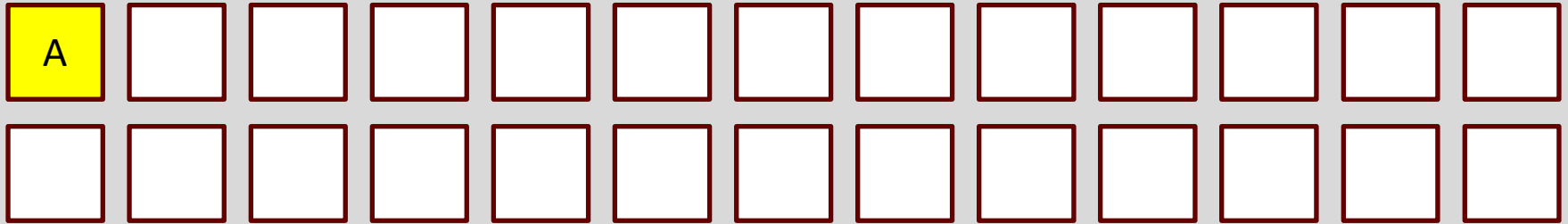
## Settori



...

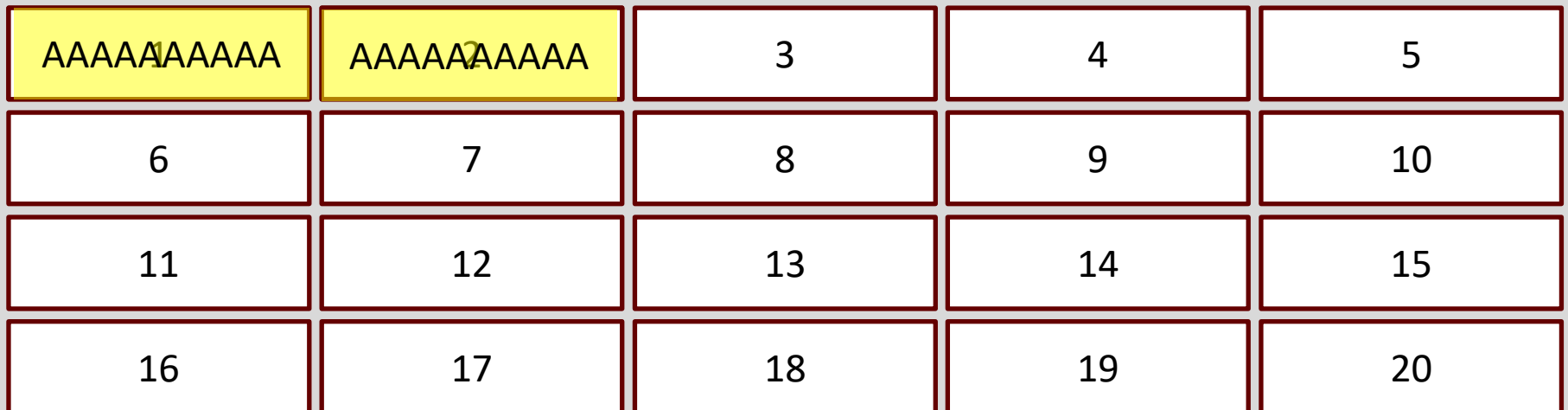
# File system: allocazione dei file

## Indice



...

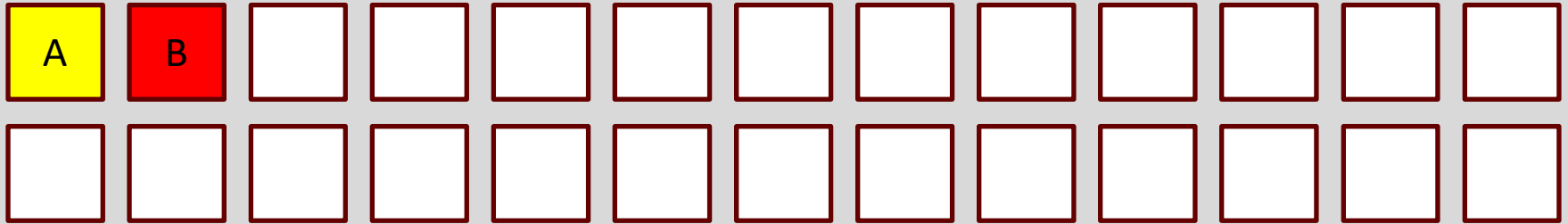
## Settori



...

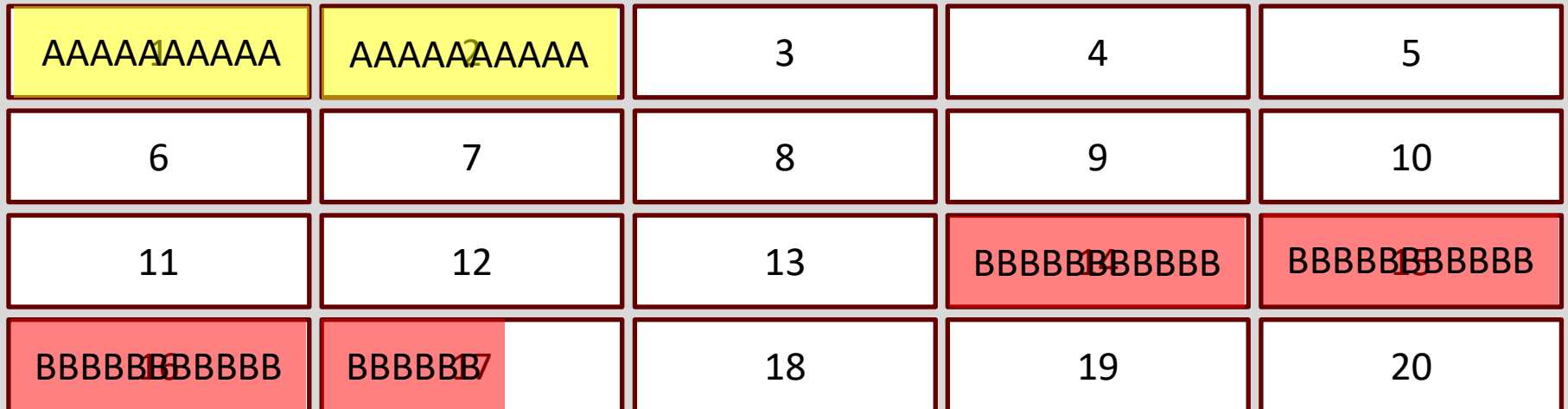
# File system: allocazione dei file

## Indice



...

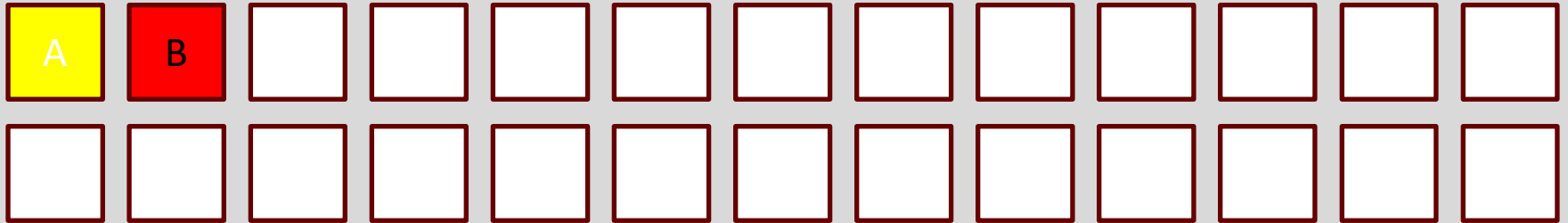
## Settori



...

# File system: allocazione dei file

## Indice



...

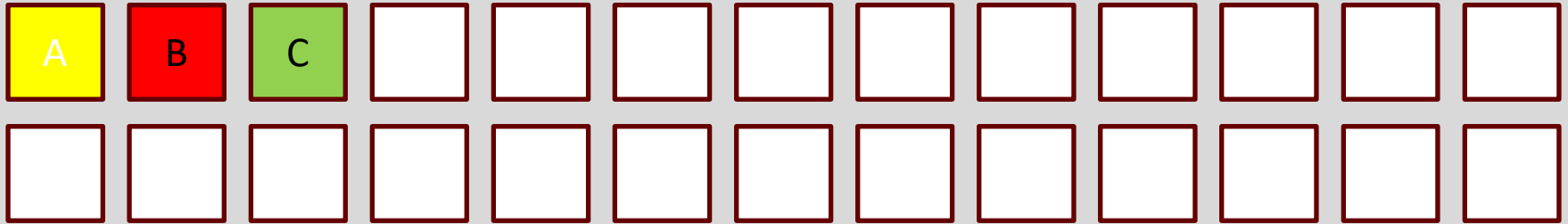
## Settori



...

# File system: allocazione dei file

## Indice



...

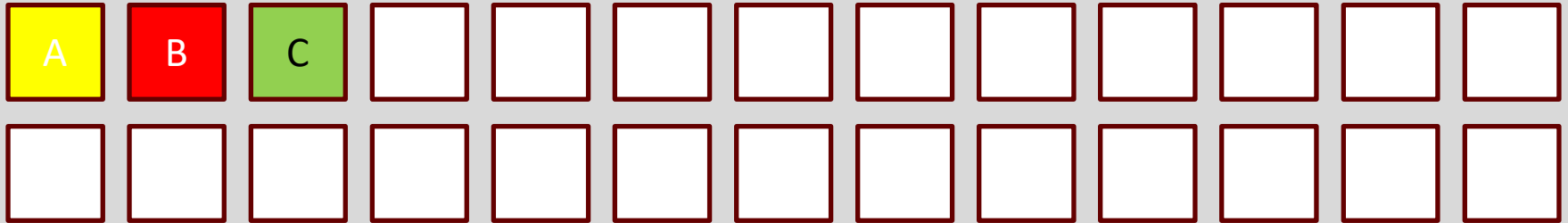
## Settori



...

# File system: allocazione dei file

## Indice



...

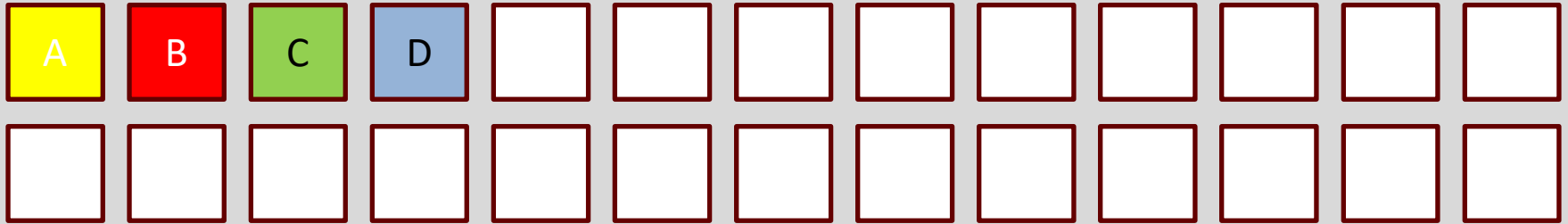
## Settori



...

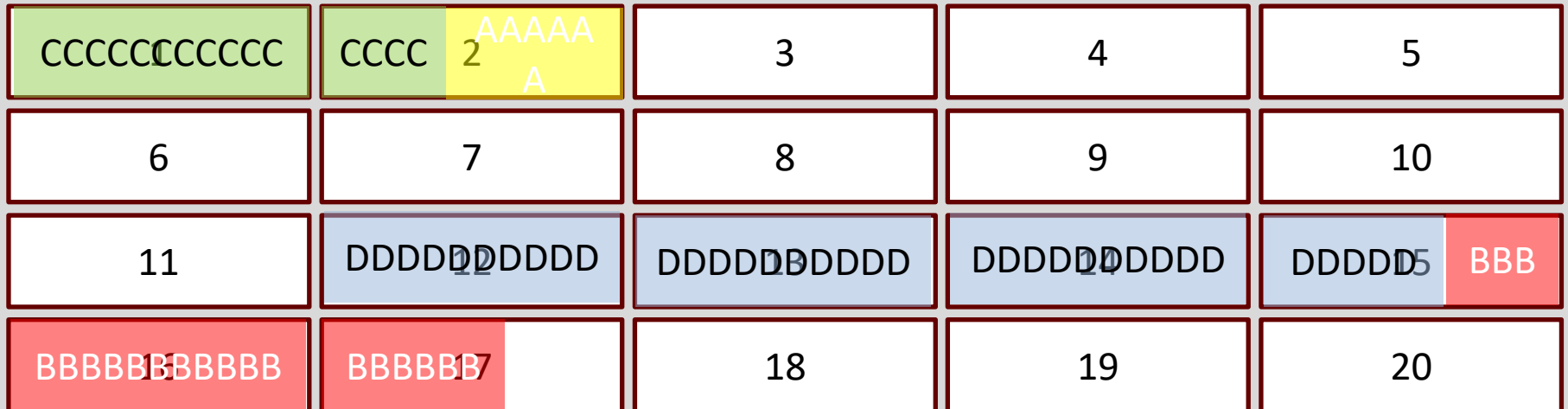
# File system: allocazione dei file

## Indice



...

## Settori

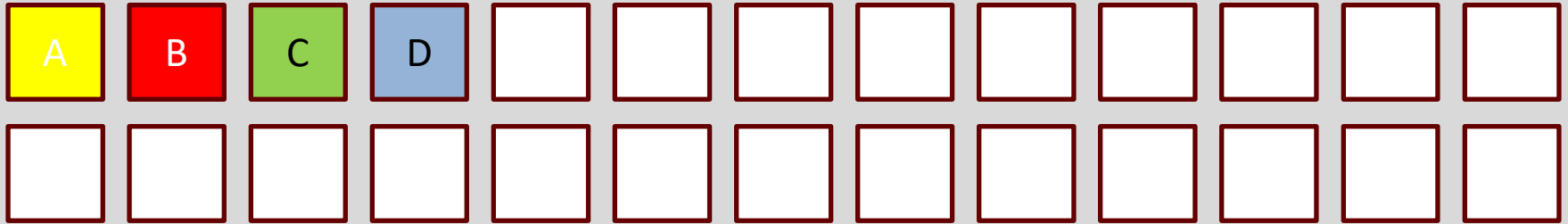


...



# File system: allocazione dei file

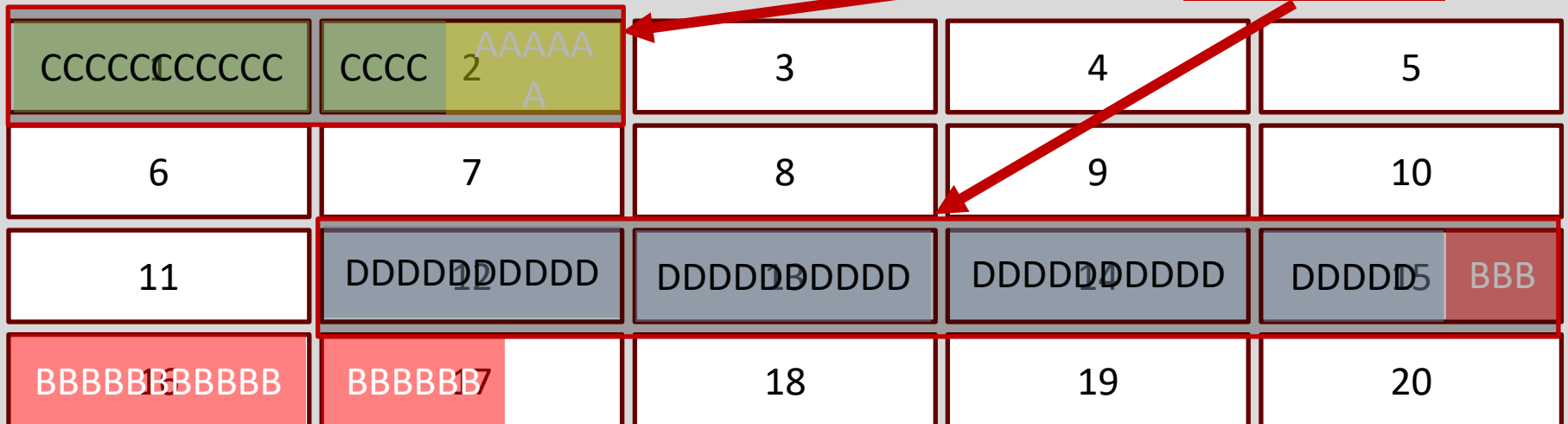
## Indice



...

## Settori

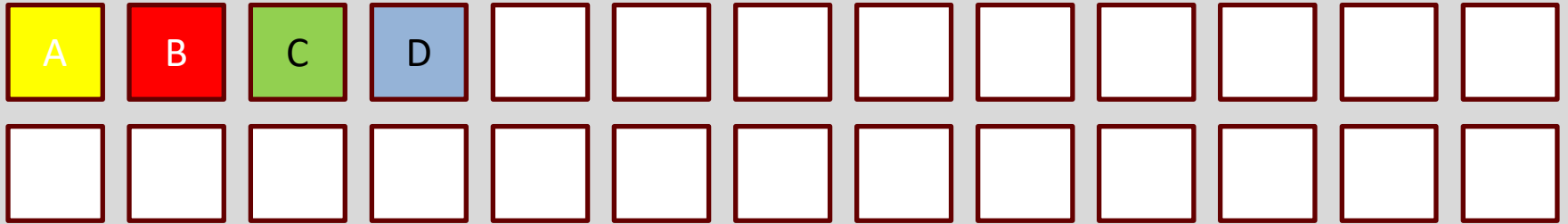
**SETTORI ALLOCATI**



...

# File system: allocazione dei file

## Indice



...

**SETTORI NON ALLOCATI**

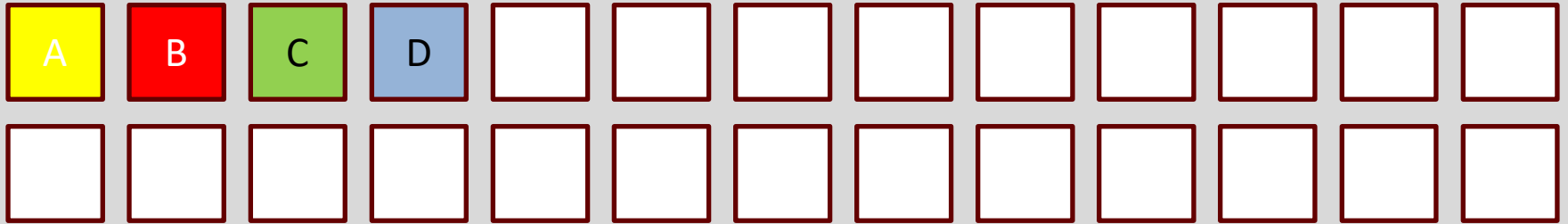
## Settori



...

# File system: allocazione dei file

## Indice



...

## Settori



...

# File system: allocazione dei file

## Indice

Promessi sposi.txt	1
Il Cinque Maggio.txt	7

Quel ramo del lago  
di Como che volge a  
mezzogiorno

Ei fu. Siccome  
immobile, dato il  
mortal sospiro

## Settori

1	Quel ram	1	2
2	o del la	1	3
3	go di Co	1	4
4	mo che v	1	5
5	olge a m	1	6
6	ezzogior	1	7
7	noX	1	/
8	Ei fu. S	1	9
9	iccome i	1	10
10	mmobile,	1	11
11	dato il	1	12
12	mortal	1	13
13	sospiroX	1	/
14		0	/
15		0	/
16		0	/
17		0	/

# File system: cancellazione di un file

## Indice

<del>Promessi sposi.txt</del>	<del>1</del>
Il Cinque Maggio.txt	7

Ei fu. Siccome  
immobile, dato il  
mortal sospiro

## Settori

1	Quel ram	0	2
2	o del la	0	3
3	go di Co	0	4
4	mo che v	0	5
5	olge a m	0	6
6	ezzogior	0	7
7	noX	0	/
8	Ei fu. S	1	9
9	iccome i	1	10
10	mmobile,	1	11
11	dato il	1	12
12	mortal	1	13
13	sospiroX	1	/
14		0	/
15		0	/
16		0	/
17		0	/

# File system: salvataggio di un nuovo file

## Indice

Divina commedia.txt	1
Il Cinque Maggio.txt	7

Nel mezzo del  
cammin di nostra  
vita

Ei fu. Siccome  
immobile, dato il  
mortal sospiro

## Settori

1	Nel mezz	1	2
2	o del ca	1	3
3	mmin di	1	4
4	nostra v	1	5
5	itaX a m	1	/
6	ezzogior	0	7
7	noX	0	/
8	Ei fu. S	1	9
9	iccome i	1	10
10	mmobile,	1	11
11	dato il	1	12
12	mortal	1	13
13	sospiroX	1	/
14		0	/
15		0	/
16		0	/
17		0	/

# File system: slack space

## Indice

Divina commedia.txt	1
Il Cinque Maggio.txt	7

Nel mezzo del  
cammin di nostra  
vita

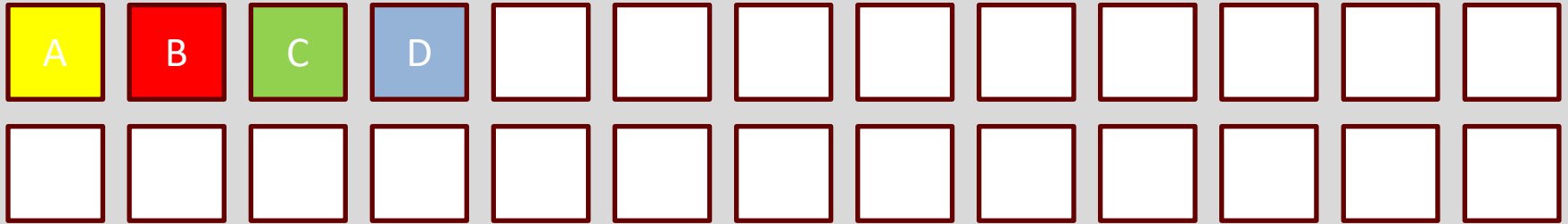
Ei fu. Siccome  
immobile, dato il  
mortal sospiro

## Settori

1	Nel mezz	1	2
2	o del ca	1	3
3	mmin di	1	4
4	nostra v	1	5
5	itaX a m	1	/
6	ezzogior	0	7
7	noX	0	/
8	Ei fu. S	1	9
9	iccome i	1	10
10	mmobile,	1	11
11	dato il	1	12
12	mortal	1	13
13	sospiroX	1	/
14		0	/
15		0	/
16		0	/
17		0	/

# File system: formattazione

## Indice



...

## Settori

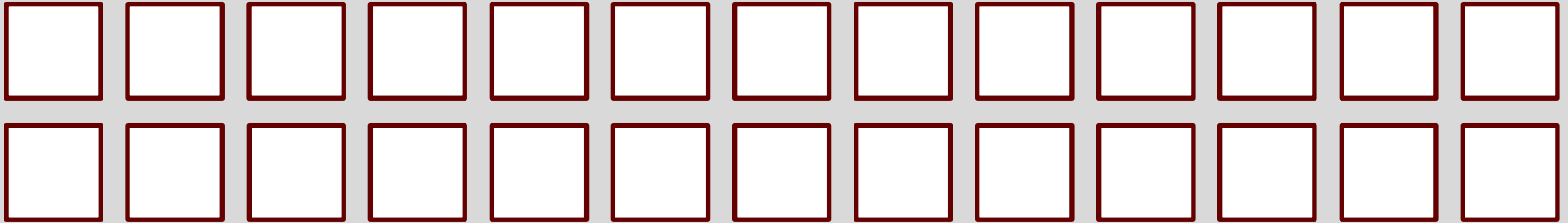


...



# File system: formattazione dopo wiping

## Indice



...

## Settori



...

# Glossario

```
001011100010101000111001100010101001
000111001100010101000111001100001010
100011100110001010100011100010001110
011000101010001110011000100100011100
110010100011100110001010100011100110
001010100011100110001011110011000010
100110001010100011100110100011001010
101010100011101010001110011000101010
001110101000111001100010101000111001
100010101100010101000000101001110011
001010100011100110001010100011100110
```

```
001011100010101000111001100010101
001000111001100010101000111001100
001010100011100110001010100011100
0100011100110001010
1001000111001100101
0101000111001100010
0010111100110000101
0111001101000110010
1010100011100110001
0001110011000101010
1011000101010000001
0101000111001100010
```

```
001011100010101000111001100010101
001000111001100010101000111001100
001010100011100110001010100011100
0100011100110001010100011100001
1001000111001100101000111000001
01010001110011000101010001100110
001011110011000010100110010100
01110011010001100101010100011
101010001110011000101010001110101
000111001100010101000111001100010
101100010101000000101001110011001
010100011100110001010100011100110
```



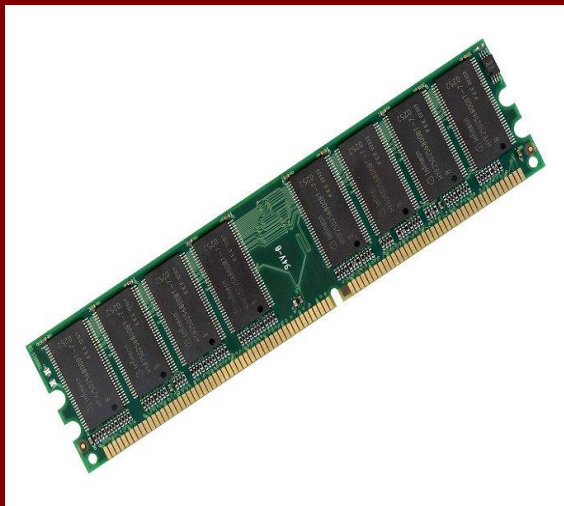
## Prova digitale

Informazione o dato, memorizzato o trasmesso in formato binario, che può essere utilizzato come prova

## Copia di prova digitale

Copia di prova digitale che può essere prodotta per mantenere l'affidabilità della prova, includendo sia la prova digitale che la procedura di verifica

# Glossario



## **Dato volatile**

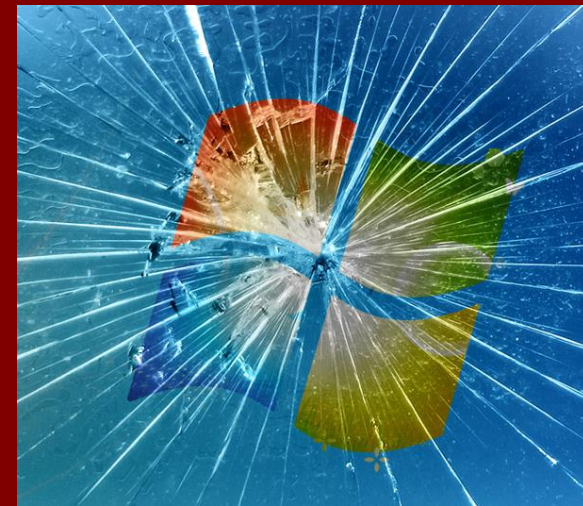
Dato facilmente soggetto a modifica. Una variazione può essere dovuta ad assenza di corrente o ad interventi di campi magnetici, a cambi di stato del sistema

*Es.: dati contenuti in RAM*



## **Alterazione**

Modifica del valore di potenziali evidenze digitali che ne riduce l'eventuale valore probatorio



## **Distruzione di prova**

Modifica volontaria del valore di potenziali evidenze digitali che ne riduce l'eventuale valore probatorio



## **Digital Evidence First Responder (DEFR)**

Persona che è autorizzata, preparata e qualificata per operare per primo sulla scena del crimine al fine di raccogliere e acquisire prove digitali con il compito di imballare e conservare la prova

## **Digital Evidence Specialist (DES)**

Persona che può svolgere i compiti di un DEFR e ha conoscenze, competenze e capacità specialistiche per gestire una vasta gamma di questioni tecniche (ad esempio, acquisizioni in rete, sistemi operativi...)

# Glossario



## Identificazione

## Raccolta

## Acquisizione

## Conservazione

## Deposito per la conservazione delle prove

Processo di ricerca, ricognizione e documentazione di potenziali prove digitali

Processo di raccolta di dispositivi fisici che contengono potenziali prove in formato digitale

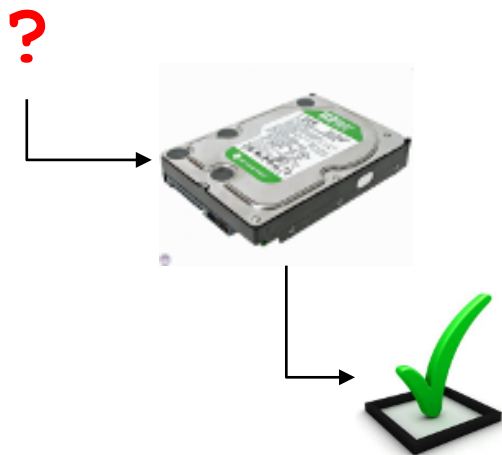
Processo di creazione di una copia di dati  
Il prodotto del processo di acquisizione è una potenziale copia prova digitale

Processo di mantenimento e salvaguardia dell'integrità e delle condizioni originarie della potenziale prova informatica

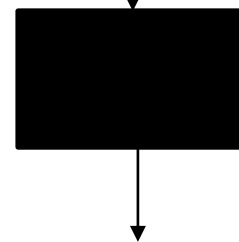
Ambiente sicuro in cui conservare prove (raccolte o acquisite). Evitare esposizione a campi magnetici, polvere, umidità calore...

# Glossario

37710C73BAB48299  
84782BCF3483927A



37710C73BAB4829984782BCF3483927A



37710C73BAB4829984782BCF3483927A

## Valore di hash

Stringa di bit che è prodotta in output da una funzione hash  
[ISO/IEC 10118-1:2000]

## Validazione

Conferma, attraverso una prova, che i requisiti preposti sono stati soddisfatti  
[ISO/IEC 27004:2009]

## Funzione di verifica

Funzione usata per verificare che due insieme di dati sono identici. Il processo di verifica è tipicamente implementato usando una funzione hash (come MD5, SHA1...)

# Acronimi

- **AVI:** Audio Video Interleave
- **CCTV:** Closed Circuit Television
- **CD:** Compact Disk
- **DNA:** Deoxyribonucleic Acid
- **DEFR:** Digital Evidence First Responder
- **DES:** Digital Evidence Specialist
- **DVD:** Digital Video Versatile Disk
- **ESN:** Electronic Serial Number
- **GPS:** Global Positioning System
- **GSM:** Global System for Mobile Communication
- **IMEI:** International Mobile Equipment Identity
- **IP:** Internet Protocol
- **ISIRT:** Information Security Incident Response Team
- **LAN:** Local Area Network
- **MD5:** Message-Digest Algorithm 5
- **MP3:** MPEG Audio Layer 3
- **MPEG:** Moving Picture Experts Group
- **NAS:** Network Attached Storage
- **PDA:** Personal Digital Assistant
- **PED:** Personal Electronic Device
- **PUK:** PIN Unlock Key
- **RAID:** Redundant Array of Independent Disks
- **RAM:** Random Access Memory
- **RFID:** Radio Frequency Identification
- **SAN:** Storage Area Network
- **SHA:** Secure Hash Algorithm
- **SIM:** Subscriber Identity Module
- **USB:** Universal Serial Bus
- **UPS:** Uninterruptible Power Supply
- **USIM:** Universal Subscriber Identity Module
- **uv:** Ultraviolet
- **WiFi:** Wireless Fidelity

# Requisiti per la gestione della prova digitale

## Requisiti generali

- **Pertinenza**

- Serve per incolpare (o discolorpare)
- Dimostrare che il materiale è rilevante, cioè che contiene dati utili e che pertanto esiste una buona ragione per acquisirli

- **Affidabilità**

- Assicurarsi che la prova digitale sia genuina
- Tutti i processi eseguiti devono essere ben documentati e, se possibile, ripetibili. Il risultato dovrebbe essere riproducibile

- **Sufficienza**

- Il DEFR deve valutare quanto materiale deve essere raccolto e le procedure da utilizzare
- Il materiale può essere copiato o acquisito (preso)
- Non è detto che sia sempre necessario acquisire una copia completa
  - Valutare in base al caso (interessa la figura del DEFR)
  - Può dipendere dalla legislazione nazionale



# Requisiti per la gestione della prova digitale

## Aspetti chiave

- **Verificabilità**

- Un terzo deve essere in grado di valutare le attività svolte dal DEFR e dal DES
  - Possibile se esiste documentazione delle azioni svolte
  - Valutare metodo scientifico, tecniche e procedure seguite
- DEFR e DES devono essere in grado di giustificare le azioni svolte

- **Ripetibilità**

- Le operazioni sono ripetibili sempre usando le stesse procedure, lo stesso metodo, gli stessi strumenti, sotto le stesse condizioni

- **Riproducibilità**

- Le operazioni sono ripetibili sempre usando lo stesso metodo, strumenti diversi, sotto condizioni diverse

- **Giustificabilità**

- Dimostrare che le scelte adoperate erano le migliori possibili

# Processo di gestione della prova digitale

## Aspetti chiave

- La ISO/IEC 27037:2012 si limita alle fasi iniziali del processo di gestione della prova informatica
  - Non arriva all'analisi
- La prova digitale è per sua natura fragile
  - Può subire alterazioni naturali, colpose o dolose
- 4 fasi
  - Identificazione
  - Raccolta
  - Acquisizione
  - Conservazione

# Processo di gestione della prova digitale

## Fasi – Identificazione

- La prova informatica si presenta in forma fisica e logica
  - Device
  - Rappresentazione
- Ricerca dei device che possono contenere dati rilevanti
  - Priorità ai dati volatili
  - Considerare dispositivi di difficile identificazione
    - Geografica
      - Es.: Cloud computing, SAN
    - Dimensioni
      - Es.: miniSD



# Processo di gestione della prova digitale

## Fasi – Identificazione



# Processo di gestione della prova digitale

## Fasi – Identificazione

- Si considera computer un dispositivo digitale standalone che riceve, processa e memorizza dati e produce risultati
  - Non connesso in rete
  - Ci possono essere periferiche connesse
- Se il computer ha un'interfaccia di rete, anche se non è connesso in rete al momento dell'intervento, bisogna individuare eventuale sistemi con cui può aver comunicato

# Processo di gestione della prova digitale

## Fasi – Identificazione

- La scena del crimine può contenere diversi tipi di dispositivi di memorizzazione
  - Hard disk, hard disk esterni, floppy disk
  - Memorie flash, memory card, CD, DVD, Blu-ray
- Il DEFR deve
  - Documentare marca, tipo, s/n di ogni supporto
  - Identificare tutti i computer e le periferiche e il loro stato
    - Se acceso, documentare cosa si vede a schermo
      - Fotografia, video, scrivere a verbale
  - Recuperare i cavi di alimentazione dei dispositivi che usano batterie
  - Utilizzare un rilevatore di segnali wireless per eventuali sistemi non visibili
  - Considerare anche evidenze non digitali e/o fornite a voce







# Processo di gestione della prova digitale

## Fasi – Identificazione

- In sede di raccolta o acquisizione bisogna considerare alcuni fattori
  - Volatilità
  - Esistenza di cifratura a livello di supporto o di partizione
  - Criticità del sistema
  - Requisiti legali
  - Risorse
    - Disponibilità di storage, tempo, disponibilità di personale

# Competenze degli operatori

## Identificazione

- Identificare
  - Dati e informazioni utili per il proseguimento delle indagini
  - Strumenti per raccolta e acquisizione
  - Valutazione dei rischi
- Competenze
  - Utente e amministratore di vari tipi di dispositivi
  - Procedure di indagine sulla scena del crimine
  - Capacità di determinare lo stato del sistema
  - Conoscere sistemi e configurazione di log
    - Email, web, accessi, password...
  - Conoscere funzionamento dei dispositivi
  - Conoscere l'importanza dei dati volatili e non volatili
  - Comprensione dei diagrammi di rete
  - Comprendere le connessioni tra indirizzi IP e indirizzi MAC

# Processo di gestione della prova digitale

## Fasi – Raccolta

- Device vengono rimossi dalla posizione originaria e trasportati in laboratorio per acquisizione e analisi
  - Talvolta rimuovere un supporto può essere pericoloso
- Il device può trovarsi in due situazioni
  - Acceso o spento
    - Approcci diversi, tool diversi
- DEFR e DES devono utilizzare il metodo migliore sulla base di situazione, costi, tempi
  - Tutto da documentare
- Raccogliere anche gli accessori

# Competenze degli operatori

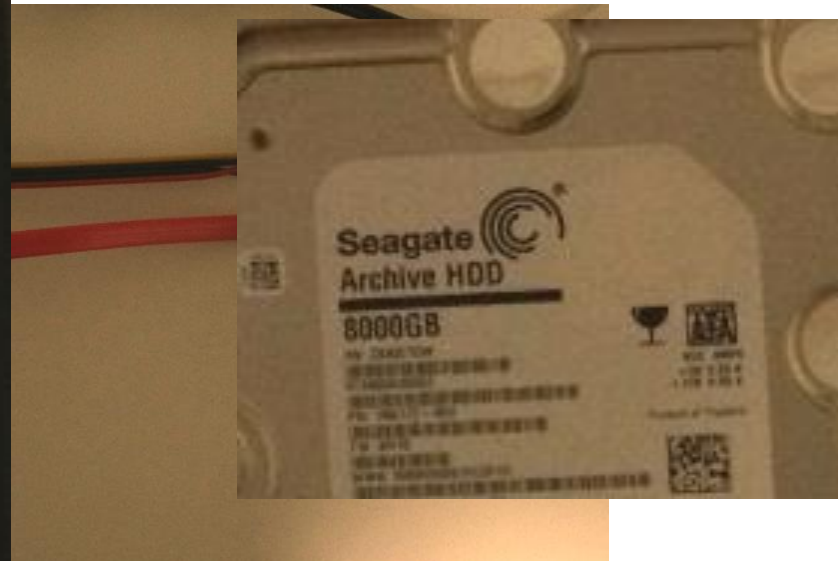
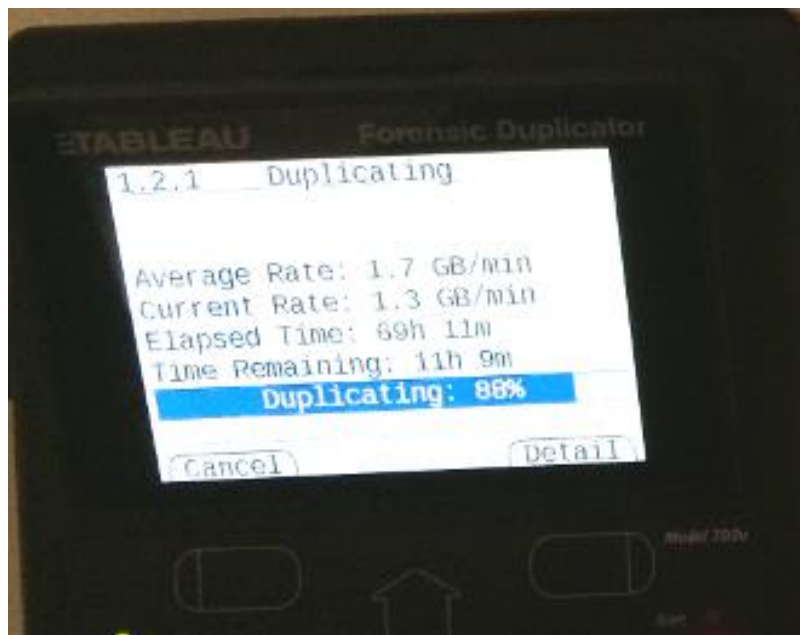
## Raccolta

- Identificare
  - Tool e procedure per imballaggio dei supporti, protezione da minacce ambientali
- Competenze
  - Raccolta in sicurezza di dati e dispositivi digitali
  - Definire il miglior metodo per la raccolta e la conservazione del maggior numero di informazioni
  - Definire documenti di catena di custodia
  - Interrogare persone che utilizzano i sistemi
  - Identificare e raccogliere tutti i dati e gli strumenti che possono tornare utili in fase di analisi
    - Password, dongle, metodologie...

# Processo di gestione della prova digitale

## Fasi – Acquisizione

- Creazione di una copia forense e documentazione di metodo, strumenti, attività
  - Supporto, partizione, gruppo di file
    - Acquisendo solo un gruppo di file si perdono alcuni dati
      - Es.: spazio non allocato, file cancellati, slack space
- Apportare meno alterazioni possibili
  - Tendere a non modificare alcun bit
  - Documentare eventuali alterazioni e giustificare
  - Es.: sistema in esecuzione, settori danneggiati, tempo insufficiente



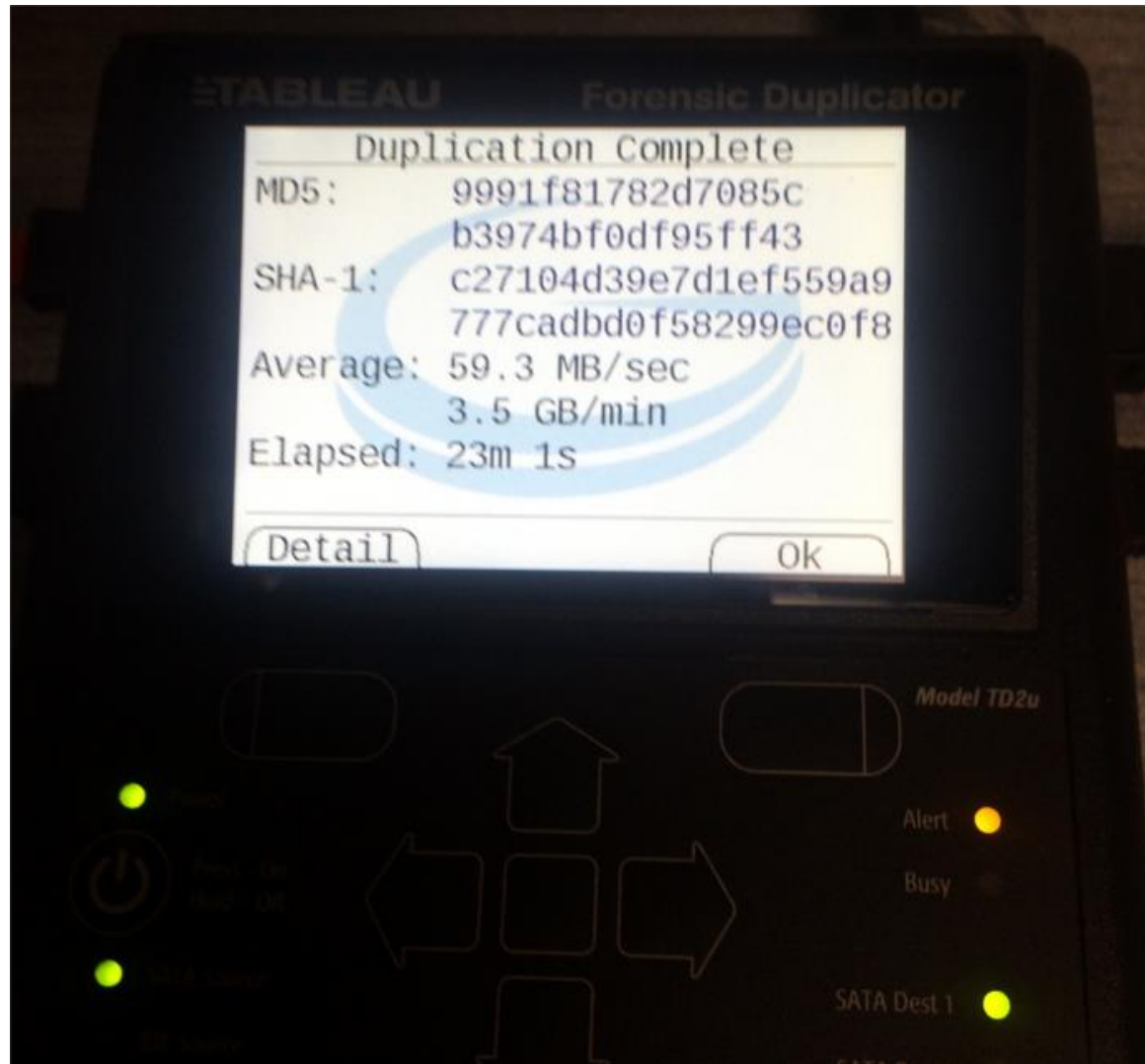
# Processo di gestione della prova digitale

## Fasi – Acquisizione

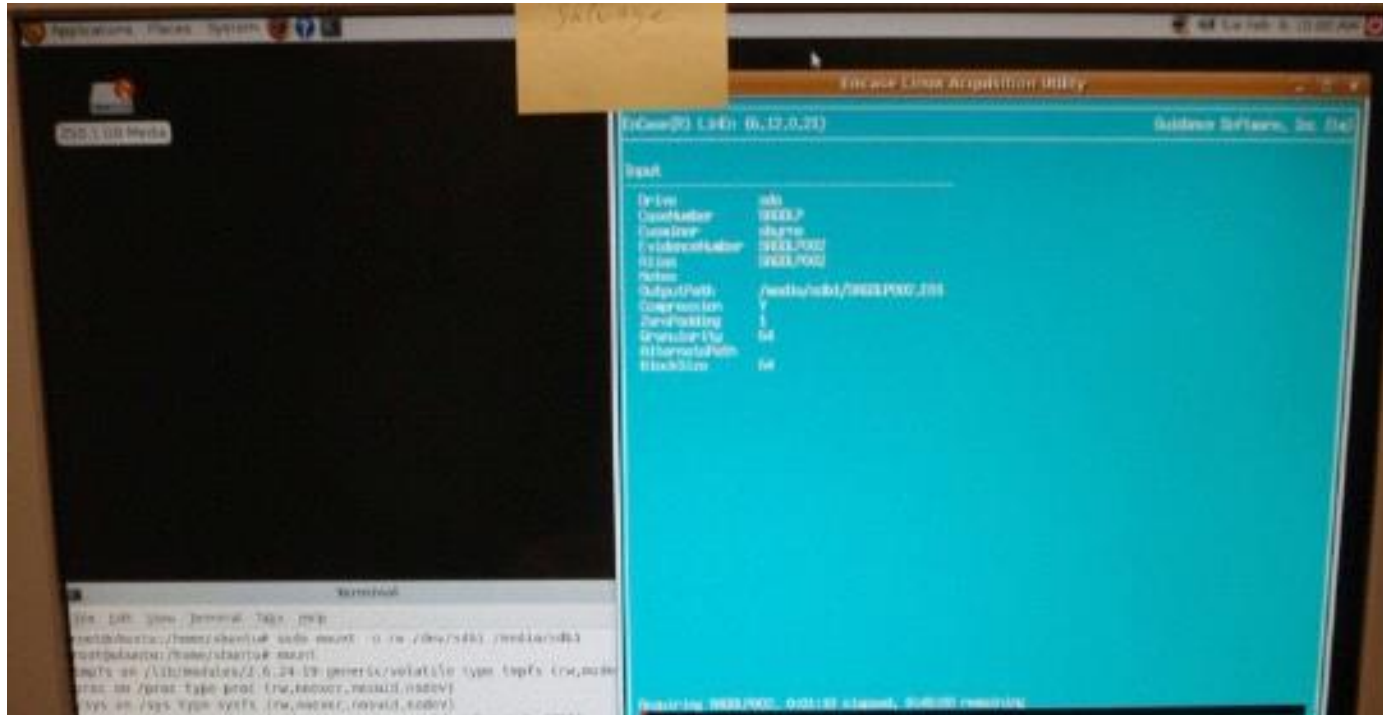


# Processo di gestione della prova digitale

## Fasi – Acquisizione



# Acquisizione post-mortem: live CD





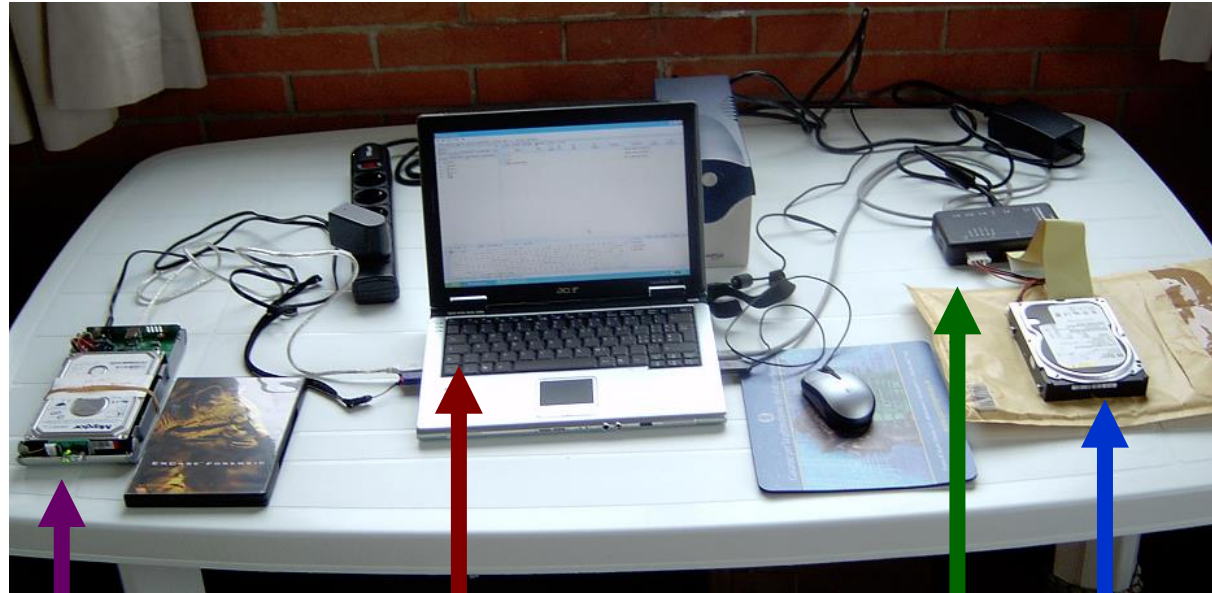
## Acquisizione post-mortem: copiatore hardware



## Acquisizione post-mortem: strumenti per mobile



# Acquisizione post-mortem: write blocker



Hard disk  
destinazione  
contenente la  
copia forense



Workstation con  
EnCase

- Acquisizione
- Calcolo e verifica hash



Writeblocker

Il blocco in scrittura  
dipende dal sistema  
operativo!



Hard disk  
sorgente

# Acquisizione: risultato finale



Master  
(sigillato)



Copia  
lavoro

# Competenze degli operatori

## Acquisizione

- Requisiti
  - Metodologie e strumenti per garantire ripetibilità, riproducibilità, integrità dei dati
  - Acquisire dati e applicare hash
- Competenze
  - Struttura dei file system (e RAID) dei vari sistemi operativi
  - Comprendere l'organizzazione dei dati nei supporti
    - File generati dal sistema, file generati dall'utente
  - Saper definire i requisiti di storage
  - Eseguire le operazioni tecniche di acquisizione
    - Dispositivi spenti, accesi, di rete; Contesti critici; Parziali; Generazione di impronte hash
  - Capire quanto incide una procedura di acquisizione rispetto ad un'altra

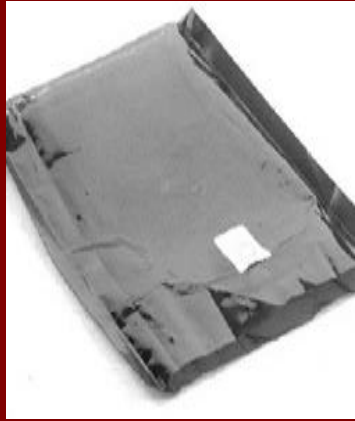
# Processo di gestione della prova digitale

## Fasi – Conservazione

- Proteggere integrità dei dati
  - Da alterazioni naturali, colpose o dolose
- Normalmente, non dovrebbero esserci alterazioni
  - Utilizzare metodologia per dimostrare che non si sono verificate alterazioni
- Proteggere anche la riservatezza dei dati
- Utilizzare imballaggi opportuni
  - Es.: per i supporti magnetici, imballaggi antistatici
  - Non devono danneggiare il supporto
- Etichettare tutto
- Verificare che le batterie siano opportunamente caricate (e ricaricare), ove presenti
- Bloccare parti mobili
- Ridurre rischi in base alla natura del supporto
- Ridurre rischi dovuti al trasporto
- Preservare eventuali altri tracce
  - Es.: tracce biologiche
  - Utilizzare guanti puliti

# Processo di gestione della prova digitale

Fasi – Conservazione ed accesso ai reperti informatici



**ESD Bag**



**Patented  
Wireless  
StrongHold Bag**



**Tablet  
Stronghold Tent**



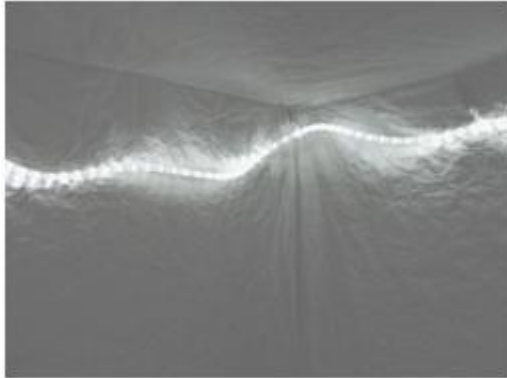
**StrongHold  
Pouch**



**Stronghold Tent**

<http://www.paraben.com/stronghold-bag.html>  
<http://www.paraben.com/tabletop-stronghold.html>  
<http://www.paraben.com/stronghold-pouch.html>  
<http://www.paraben.com/stronghold-tent.html>

# Conservazione StrongHold Tent



<http://www.paraben.com/stronghold-tent.html>



# Competenze degli operatori

## Conservazione

- Requisiti
  - Applicare e valutare requisiti per la conservazione
  - Mantenimento della catena di custodia
- Competenze
  - Impatto delle minacce ambientali
    - Umidità, temperatura...
  - Imballaggio e trasporto di dispositivi digitali

# Processo di gestione della prova digitale

## Catena di custodia

- Documentare movimenti e interazioni con la potenziale prova digitale
- Storia del supporto a partire dalla fase di raccolta
- Formato cartaceo o digitale
- Deve contenere
  - Identificativo unico dell'evidenza
  - Quando, dove, chi e perché ha avuto accesso all'evidenza
  - Documentare e giustificare ogni alterazione inevitabile, con il nome del responsabile

<i>Dettagli reperto informatico e catena di custodia</i>			
Caso:		ID reperto:	
Informazioni sulle evidenze			
Dettagli macchina originaria			
Produttore:			
Modello:			
Serial number:			
Part number:			
Note aggiuntive (adesivi, etichette, username, psw...):			
Dettagli reperto			
Produttore:			
Modello:		Dim. (GB):	
Serial number:			
Part number:			
HASH:	MDS:		
	SHA1:		
Note aggiuntive:			
Reperto informatico originario presentato da			
Nome e cognome:			
Data e ora:			
Luogo:			
Note aggiuntive:			
Catena di custodia			
Data e ora	Incarico a		Descrizione
	Nome	Nome	
	Nome	Nome	
	Nome	Nome	
	Nome	Nome	
	Nome	Nome	

# Processo di gestione della prova digitale

## Catena di custodia

<b><i>Dettagli reperto informatico e catena di custodia</i></b>			
Caso:		ID reperto:	
<b>Informazioni sulle evidenze</b>			
<b>Dettagli macchina originaria</b>			
Produttore:			
Modello:			
Serial number:			
Part number:			
Note aggiuntive (a desivi, etichette, username, pow...):			
<b>Dettagli reperto</b>			
Produttore:			
Modello:		Dim. (GB):	
Serial number:			
Part number:			
HASH:	MD5:		
	SHA1:		
Note aggiuntive:			

# Processo di gestione della prova digitale

## Catena di custodia

Reperito informatico originario presentato da			
Nome e cognome:			
Data e ora:			
Luogo:			
Note aggiuntive:			
Catena di custodia			
Data e ora	Incarico a		Descrizione
	Nome	Posizione	
	Nome	Posizione	
	Nome	Posizione	
	Nome	Posizione	
	Nome	Posizione	

# Briefing

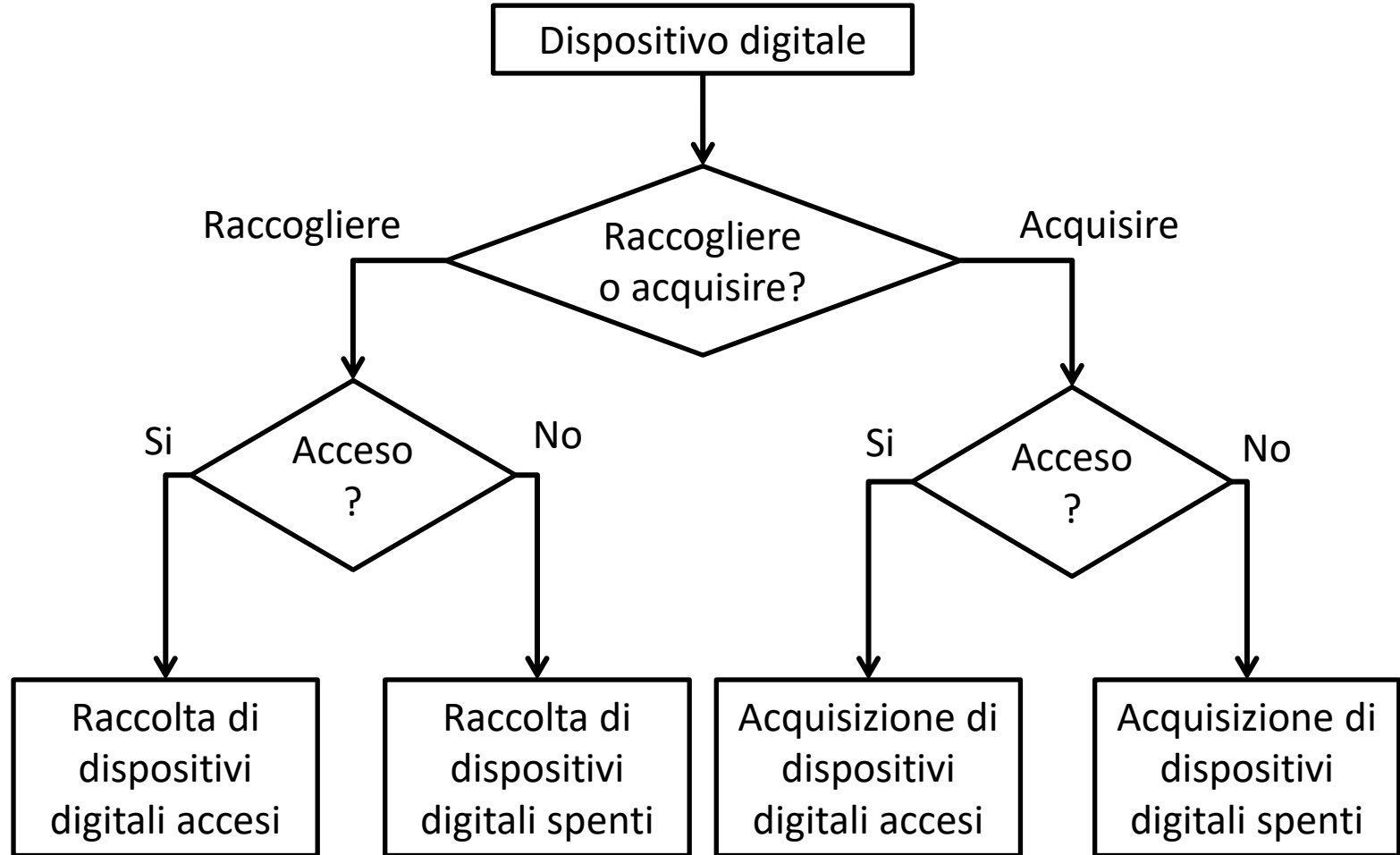
- Capire cosa è accaduto
- Cosa cercare
- Cosa ci si aspetta di trovare e cosa ci si aspetta di non trovare
- Valutare aspetti di riservatezza
- Valutare precauzione per mantenere integrità dei dati
- Tipo di incidente
- Data e ora
- Definire piano di investigazione
- Considerare dove e come l'evidenza digitale è memorizzata/trasportata
- Individuare eventuali tool specifici per le attività di acquisizione
- Definire strumenti necessari
- Disattivare comunicazioni via cavo e senza fili
- Assegnare compiti ai vari soggetti
  - Non accettare ausilio tecnico da non autorizzati
  - Utilizzare materiali opportuni per l'imballaggio

# Precauzioni sulla scena del crimine

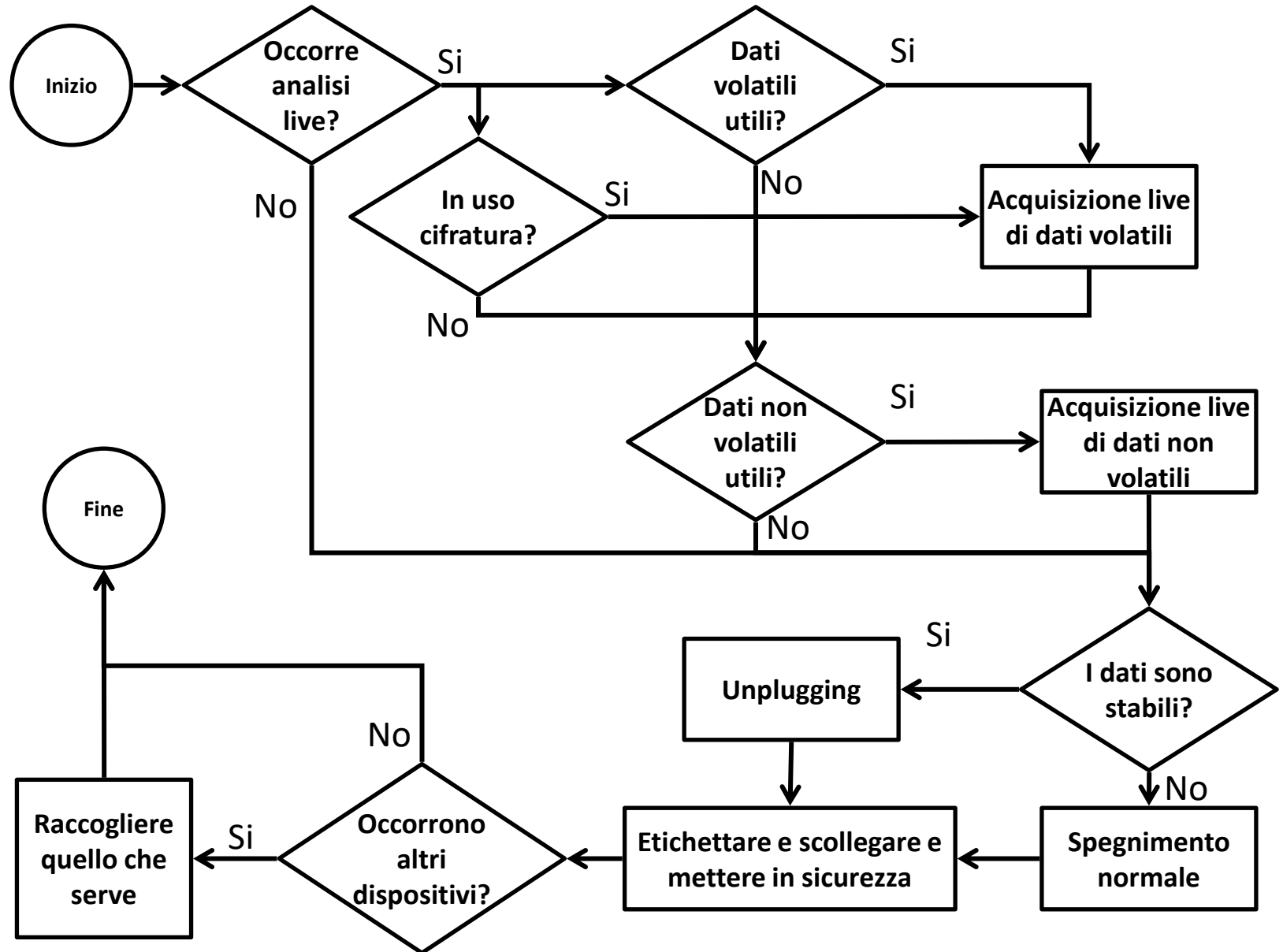
## Valutazione dei rischi

- Scegliere bene tool e metodologie
  - Rischi non calcolati possono compromettere per sempre i dati
- Una valutazione dei rischi riduce al minimo gli errori
  - Che tipo di metodologia applicare per la raccolta e l'acquisizione?
  - Quali strumenti possono essere utili per l'attività?
  - Qual è il livello di volatilità dei dati?
  - I dati sono raggiungibili da remoto? Qual è il rischio di alterazione?
  - Cosa fare se gli strumenti non dovessero funzionare?
  - I dati potrebbero essere stati già compromessi?
  - È possibile che siano state previste bombe logiche per distruggere o nascondere dati?

# Identificazione



# Dispositivi accessi



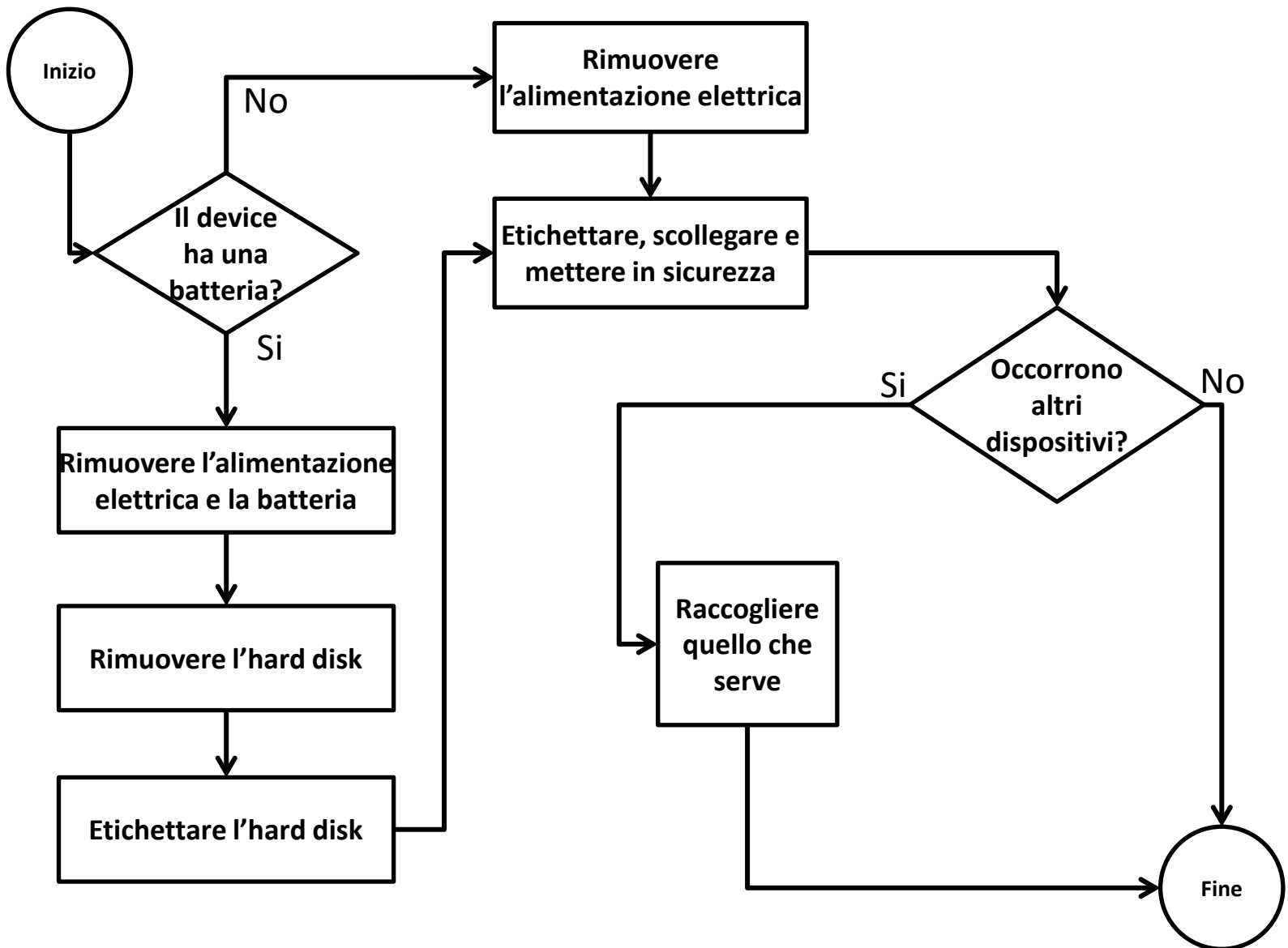


# Linee guida per acquisizione di dispositivi di memorizzazione digitali

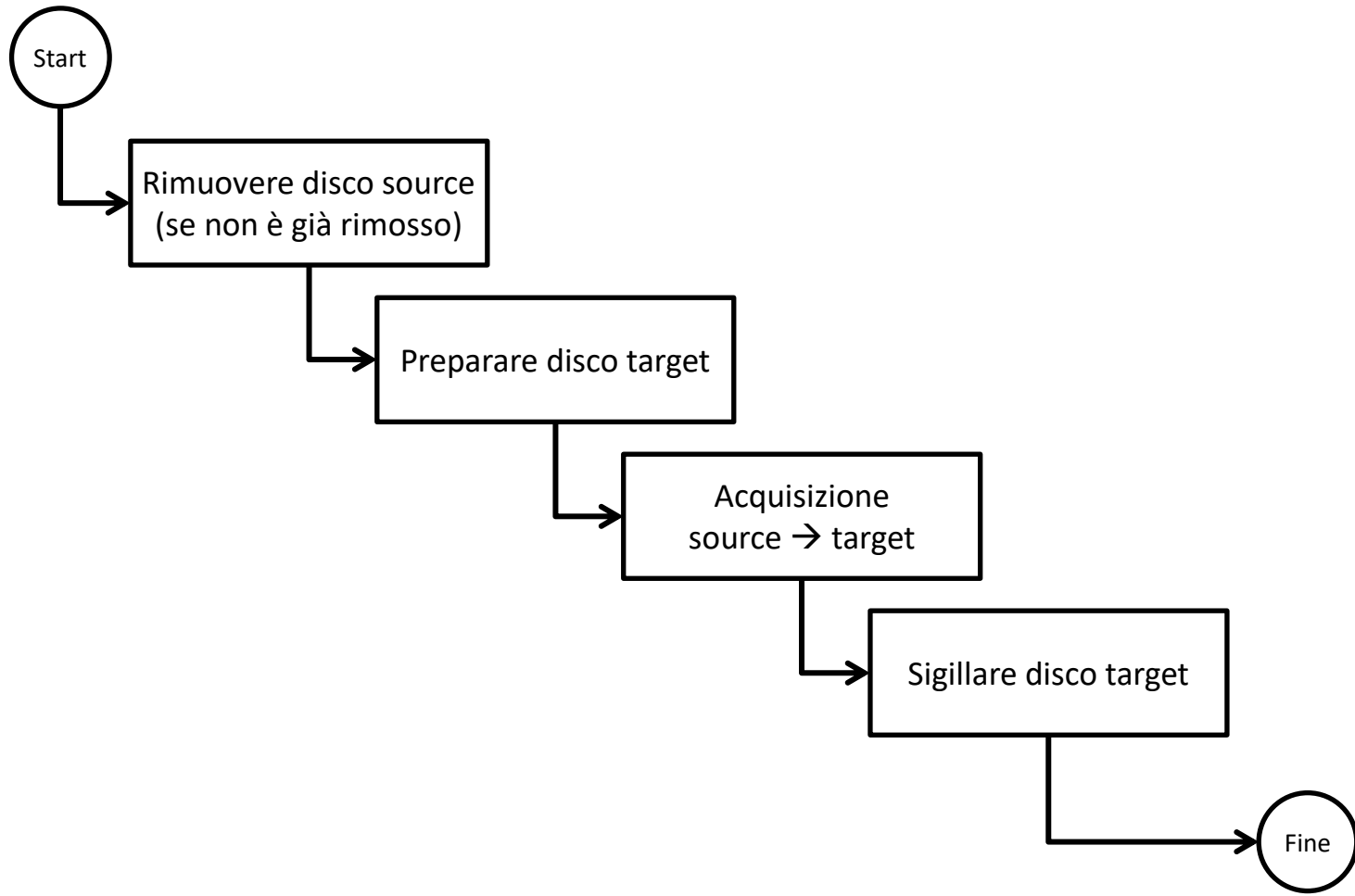
Stato: spento

- No dati volatili
- Procedura:
  - Assicurarsi che i dispositivi siano effettivamente spenti
  - Rimuovere il dispositivo di memorizzazione dal dispositivo spento (se non già rimosso)
    - Porre attenzione quando il dispositivo di memorizzazione viene rimosso: potrebbe essere confuso con altri o danneggiato
  - Etichettare il dispositivo di memorizzazione come “suspect”
  - Documentare tutti i dettagli
    - Produttore, modello, serial number, part number, dimensione
  - Acquisire e calcolare impronta hash

# Dispositivi spenti



# Acquisizione dispositivo spento



# Situazioni critiche

- In alcuni casi, I dispositivi non possono essere spenti a causa della natura del sistema
  - Es.: data center che offrono servizi a terzi, sistemi di sorveglianza, sistemi medici, altri sistemi critici...
- Occorre prevedere particolari attenzioni
- É possibile procedere con
  - Acquisizione live
  - Acquisizione parziale

# Situazioni critiche

## Acquisizione parziale

- Si procede ad un'acquisizione parziale quando intervengono particolari situazioni:
  - Il sistema da acquisire contiene troppi dati
    - Es.: Google server... ma anche “banali” DB server
  - Il sistema non può essere spento
  - Solo alcuni dati sono rilevanti
  - Solo alcuni dati possono essere acquisiti per vincoli legali
- Quando si procede ad un'acquisizione parziale, le attività devono includere (ma non sono limitate a):
  - Identificazione delle cartelle, file ed ogni altra proprietà o opzione rilevante
  - Acquisizione dei sopra indicati dati

# Analisi

- Poiché ogni copia coincide con l'originale, **l'analisi va eseguita su una copia** dei dati acquisiti e non sull'originale

- Caratteristiche dell'analisi

- Riproducibilità
- Ogni singola operazione deve produrre sempre lo stesso risultato
  - *Si intende risultato oggettivo (cioè, **dati!**), non valutazione*

- Cos'è analisi?

- Ricostruzione di eventi passati mediante la lettura di dati digitali

- Regola delle 5W

- WHO? («Chi?»)
- WHAT? («Che cosa?»)
- WHEN? («Quando?»)
- WHERE? («Dove?»)
- WHY? («Perché?»)

# Analisi

- Ricerche
  - Autore
  - Intervallo di date
  - Tipo di file
  - Parola chiave
  - Per hash
  - Per thread (email)
- Recupero dati
  - Recupero dati cancellati, carving...
- Interpretazione dati
- Conversione tra formati
- Crack password
  - File tipicamente protetti
    - Microsoft Office File; PDF; ZIP...
  - Tipologie di attacco
    - Social engineering; Attacco a dizionario; Attacco brute force...
- Artefatti del sistema operativo

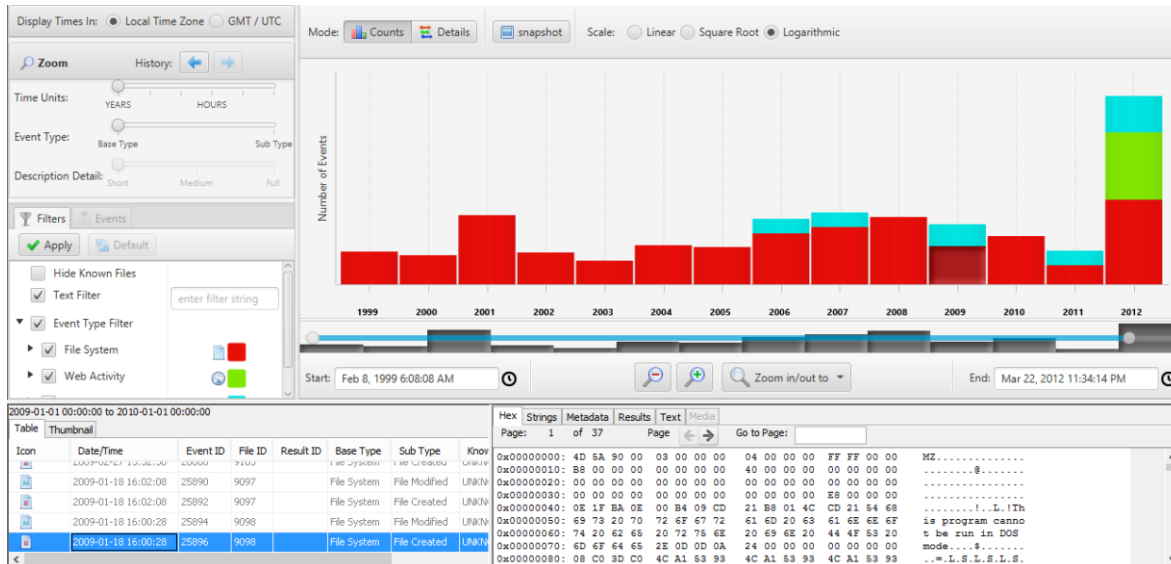
# Analisi: timeline

```

Fri Jan 16 2009 18:24:13      248 .a.. d/drwxrwxrwx 0      0      66-144-1 C:/WINDOWS/Driver Cache/i386
Fri Jan 16 2009 18:24:14      0 m... 0 0      0      0      HKLM-SYSTEM/ControlSet001/Control/Class/{4D36E967-E325
-11CE-BFC1-08002BE10318}/0004
Fri Jan 16 2009 18:24:15      0 m... 0 0      0      0      HKLM-SYSTEM/ControlSet001/Enum/USBSTOR/Disk&Ven_Apple&
Prod_iPod&Rev_2.70/000A270010C4E86E&0
0 m... 0 0      0      0      HKLM-SYSTEM/ControlSet001/Enum/USBSTOR/Disk&Ven_Apple&
Prod_iPod&Rev_2.70/000A270010C4E86E&0/Device Parameters
Fri Jan 16 2009 18:24:16      0 m... 0 0      0      0      HKLM-SYSTEM/ControlSet001/Control/Class/{71A27CDD-812A
-11D0-BEC7-08002BE2092F}
0 m... 0 0      0      0      HKLM-SYSTEM/ControlSet001/Control/Class/{71A27CDD-812A
-11D0-BEC7-08002BE2092F}/0004
0 m... 0 0      0      0      HKLM-SYSTEM/ControlSet001/Control/DeviceClasses/{53f56
30d-b6bf-11d0-94f2-00a0c91efb8b)/###STORAGE#RemovableMedia#7&1d6490f9&0&RM#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b)
0 m... 0 0      0      0      HKLM-SYSTEM/ControlSet001/Control/DeviceClasses/{53f56
30d-b6bf-11d0-94f2-00a0c91efb8b)/###STORAGE#RemovableMedia#7&1d6490f9&0&RM#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b)/#
7&1d6490f9&0&RM
0 m... 0 0      0      0      HKLM-SYSTEM/ControlSet001/Enum/STORAGE/RemovableMedia/
7&1d6490f9&0&RM
1580544 .a.. r/rwxrwxrwx 0      0      2063-128-3 C:/WINDOWS/system32/sfcfiles.dll
984576 .a.. r/rwxrwxrwx 0      0      2249-128-3 C:/WINDOWS/system32/syssetup.dll
204597 mac. r/rwxrwxrwx 0      0      3596-128-3 C:/WINDOWS/setupapi.log
12614 macb r/rwxrwxrwx 0      0      8176-128-4 C:/WINDOWS/Prefetch/RUNDLL32.EXE-35D52528
  
```

.pdf

Fonte sans.org



Fonte sleuthkit.org



# Analisi: supertimeline

A	B	C	D	E	F	G	J	
date	time	timezone	MACB	source	sourcetype	type	short	desc
6/18/2009	22:30:26	EST5EDT	MACB	LOG	WMIprov Log file	Time Written	C:/Windows/system32/DRIVERS/msiscsi.sys[MofResource](Thu Jun 18 22:30:26 2009.29992	Entry in log file: C:/Windows/
6/18/2009	22:30:26	EST5EDT	MACB	LOG	WMIprov Log file	Time Written	C:/Windows/system32/drivers/ndis.sys[MofResourceName](Thu Jun 18 22:30:26 2009.2998	Entry in log file: C:/Windows/
6/18/2009	22:36:15	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	LOGON.SCR-7C80CA1C.pf: LOGON.SCR was executed	LOGON.SCR-7C80CA1C.pf - [L
6/18/2009	22:41:26	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] SYSTEM	[DELETED] SYSTEM
6/18/2009	22:41:54	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	DEFRAG.EXE-738093E8.pf: DEFRAG.EXE was executed	DEFRAG.EXE-738093E8.pf - [T
6/18/2009	22:41:54	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	DFRGNTFS.EXE-4F838A89.pf: DFRGNTFS.EXE was executed	DFRGNTFS.EXE-4F838A89.pf -
6/18/2009	22:41:59	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] emRoot/System32/Config/SOFTWARE	[DELETED] emRoot/System32,
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/0000000E/00000000/	[DELETED] ???/0000000E/000
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/{83da6326-97a6-4088-9453-a1923f573b29}/00000003/00000000/	[DELETED] ???/{83da6326-97a
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000003/00000000/	[DELETED] ???/00000003/000
6/18/2009	23:33:57	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000008/00000000/	[DELETED] ???/00000008/000
6/18/2009	23:34:09	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	PKMAILER.EXE-83FAD500.pf: PKMAILER.EXE was executed	PKMAILER.EXE-83FAD500.pf -
6/18/2009	23:34:35	EST5EDT	MACB	REG	NTUSER key	Last Written	Software/Google/GoogleToolbarNotifier/Stats	Key name: HKEY_USER/Softwa
6/18/2009	23:34:36	EST5EDT	MACB	REG	NTUSER key	Last Written	Software/Google/GoogleToolbarNotifier/Temp	Key name: HKEY_USER/Softwa
6/18/2009	23:34:50	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	IPODSERVICE.EXE-FE1A6FF7.pf: IPODSERVICE.EXE was executed	IPODSERVICE.EXE-FE1A6FF7.pf -
6/18/2009	23:34:59	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	RUNDLL32.EXE-2E65B341.pf: RUNDLL32.EXE was executed	RUNDLL32.EXE-2E65B341.pf -
6/18/2009	23:34:59	EST5EDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:C:/Windows/system32/rundll32.exe	UEME_RUNPATH:C:/Windows
6/18/2009	23:35:05	EST5EDT	MACB	LSO	Flash Cookie	LSO created	Flash Cookie: site ui/preferences	LSO created -> File: C://mnt/v
6/18/2009	23:35:07	EST5EDT	MACB	REG	NTUSER key	Last Written	Software/Microsoft/InternetExplorer/LowRegistry/Audio/PolicyConfig/PropertyStore/5447cc	Key name: HKEY_USER/Softwa
6/18/2009	23:35:38	EST5EDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:Mozilla Firefox.lnk	UEME_RUNPATH:Mozilla Fire
6/18/2009	23:35:39	EST5EDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:C:/Program Files/Mozilla Firefox/firefox.exe	UEME_RUNPATH:C:/Program
6/18/2009	23:35:39	EST5EDT	MACB	PRE	Vista/Win7 Prefetch	Last run	FIREFOX.EXE-E60C0AA7.pf: FIREFOX.EXE was executed	FIREFOX.EXE-E60C0AA7.pf - [
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000003/	[DELETED] ???/00000003/
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/{83da6326-97a6-4088-9453-a1923f573b29}/	[DELETED] ???/{83da6326-97a
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/0000000E/	[DELETED] ???/0000000E/
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000008/	[DELETED] ???/00000008/
6/18/2009	23:41:36	EST5EDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/{83da6326-97a6-4088-9453-a1923f573b29}/00000003/	[DELETED] ???/{83da6326-97a

Fonte sleuthkit.org

# Analisi: Autopsy

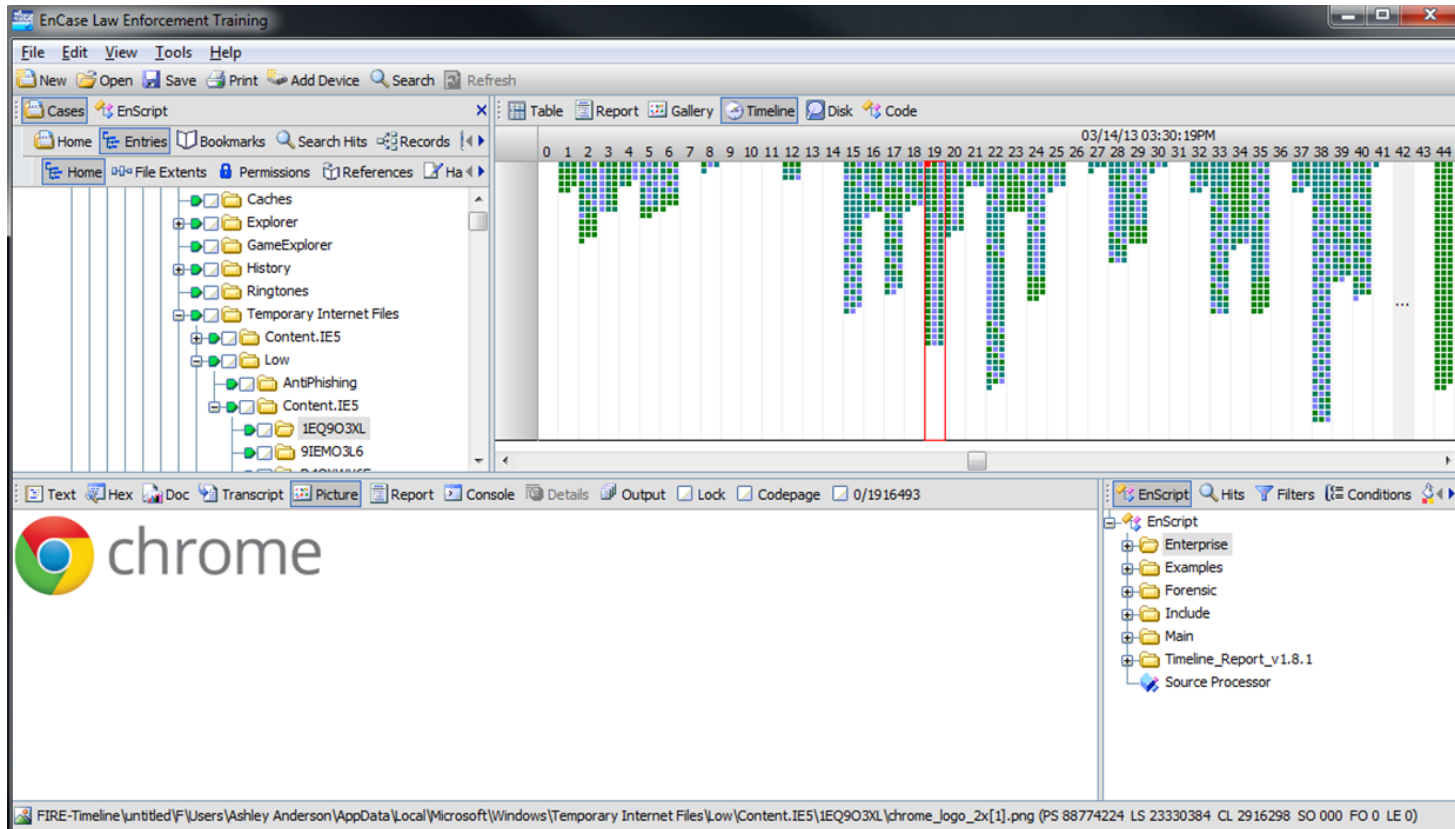
The screenshot displays the Autopsy 3.0.0b3 interface. The main window shows a directory listing of files from a forensic image. The file 'NTDETECT.COM' is highlighted in blue. The interface includes a sidebar with navigation options like 'Images', 'Views', and 'Results', and a main pane with a table of files and a hex view at the bottom.

Name	Mod. Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags
\$boot	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	8192	Allocated	Allocated
\$Extend	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	344	Allocated	Allocated
\$LogFile	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	23085056	Allocated	Allocated
\$MFT	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	15859712	Allocated	Allocated
\$MFTMirr	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	4096	Allocated	Allocated
\$Secure:\$SDS	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	0	Allocated	Allocated
\$UpCase	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	131072	Allocated	Allocated
\$Volume	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	0	Allocated	Allocated
AUTOEXEC.BAT	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Allocated
boot.ini	2012-01-20 17:19:25	2012-01-20 17:20:54	2012-01-20 17:19:25	2012-01-20 12:10:10	211	Allocated	Allocated
CONFIG.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Allocated
Documents and Settings	2012-03-22 19:29:54	2012-03-22 19:29:54	2012-03-10 14:40:46	2012-01-20 12:10:41	56	Allocated	Allocated
IO.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Allocated
MSDOS.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Allocated
NTDETECT.COM	2008-04-13 22:13:04	2012-01-20 12:11:07	2012-01-20 12:10:07	2008-04-13 22:13:04	47564	Allocated	Allocated
ntldr	2008-04-14 00:01:44	2012-01-20 12:11:07	2012-01-20 12:10:07	2008-04-14 00:01:44	250048	Allocated	Allocated
pagefile.sys	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-01-20 12:09:08	20971520	Allocated	Allocated
Program Files	2012-03-20 19:25:02	2012-03-20 19:25:02	2012-03-10 14:40:46	2012-01-20 12:11:01	56	Allocated	Allocated
System Volume Information	2012-01-20 17:21:37	2012-01-20 17:21:37	2012-03-10 14:40:46	2012-01-20 12:10:41	56	Allocated	Allocated
WINDOWS	2012-03-05 19:12:38	2012-03-05 19:12:38	2012-03-10 14:40:46	2012-01-20 12:09:08	56	Allocated	Allocated
\$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated

Hex View: Page: 1 of 3 Page: Go to Page:

```
0x000000: 66 55 66 39 EC 66 FD E5 FF FF 00 00 1E 06 66 53 fU...f.....fS
0x000010: 66 56 66 57 B9 FD A4 C1 E9 04 S2 C8 03 C1 7D D8 fVW.....
0x000020: 7D C0 66 39 CC 66 30 0E 00 00 S2 D1 80 0E 04 00 .f.f.....
0x000030: 66 39 5E 08 66 39 4E 0C 66 39 76 10 66 39 7E 14 .f.f.n.....
0x000040: 66 39 5E 18 66 39 6E 1C 7D D0 66 BC 06 10 00 00 .f.f.n.....
0x000050: 66 55 66 52 66 57 66 56 66 51 66 53 66 33 C0 66 fU9EVEVEE9E9.f
0x000060: 33 DB 66 33 C9 66 33 D2 66 33 F6 66 33 FF E8 B7 3.f.f.f.f.f.f.f
0x000070: 02 66 07 B2 26 00 00 66 5F 66 5E 66 5B 07 1F 66 .f.f.f.f.f.f.f.f
0x000080: 5D CB 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1.....
0x000090: 55 39 EC 56 57 53 60 4E 06 B8 00 D8 CD 15 53 39 U.VMS.N.....S
0x0000A0: 5E 04 C6 27 C6 47 01 58 C6 67 02 C6 47 03 30 4F .f.G.X.g.g.g.O
0x0000B0: 04 C6 77 06 C6 57 07 30 7F 08 30 77 0A 5B 5F 5E .w.W.....w.[_
0x0000C0: 5D C3 55 39 EC 56 B8 01 D8 60 4E 06 60 6E 08 39 1.U.V.....N.n.
0x0000D0: 76 04 CD 1E 60 C4 5E 5D C3 06 53 B8 00 F0 7D C0 v.....1.S.....
```

# Analisi: EnCase



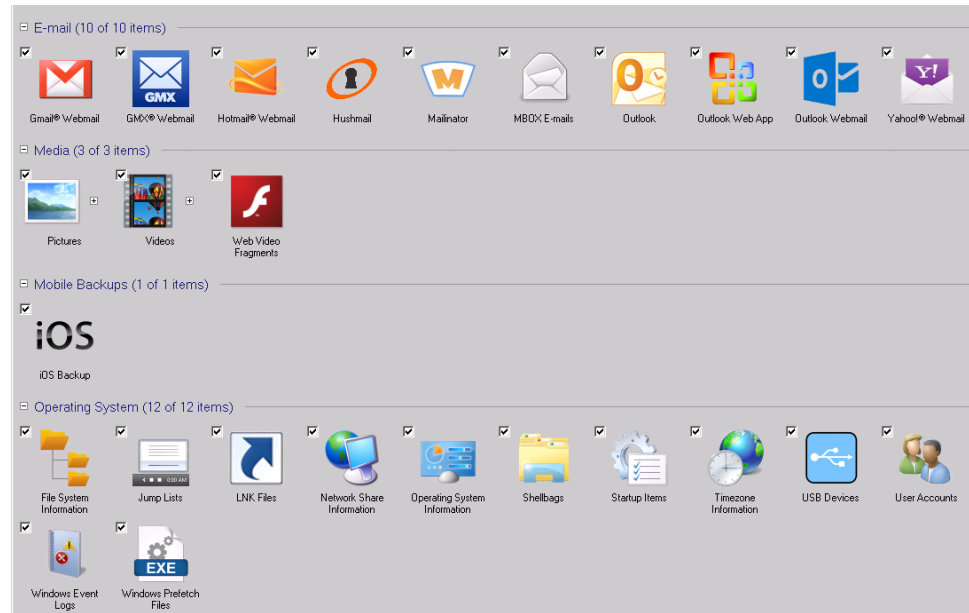
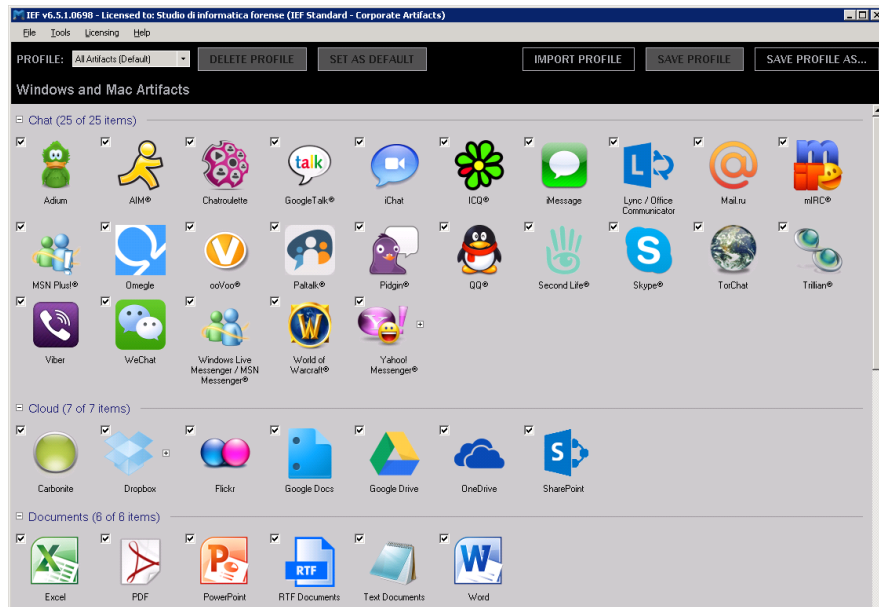
# Analisi: Xways Forensics

The screenshot displays the X-Ways Forensics interface. The main window shows a file list for the NTFS Image.e01. The file list includes columns for Filename, Ext., Path, Size, Created, Modified, Accessed, Attr., 1st cluster, ID, and Comment. A context menu is open over the file list, showing options like View, External Programs, Recover/Copy, Edit comment, Add To Active Case, Add to, Tag, Hide, Position, Logical Search..., Create Hash Set..., Print..., and Open.

Filename	Ext.	Path	Size	Created	Modified	Accessed	Attr.	1st cluster	ID	Comment
0.1020.299484.00[1].jpg	jpg	\Pictures\0003	2.1 KB	03.05.2004 17:17:56	05.04.2004...	12.05.2005 ...	A	25395	382	
Private.jpg	jpg	\Pictures\0001	6.2 KB	03.05.2004 17:17:58	10.09.1997...	12.05.2005 ...	A	31337	511	
350de005.jpg	jpg	\Pictures\0003	7.1 KB	03.05.2004 17:17:56	03.05.2004...	12.05.2005 ...	H	25465	385	
makeup4.jpg	jpg	\Pictures\0003	14.4 KB	03.05.2004 17:17:56	03.05.2004...	13.05.2004 ...	A	26491	403	
necklace1.jpg	jpg	\Pictures\0003	14.6 KB	03.05.2004 17:17:56	03.05.2004...	12.05.2005 ...	A	26449	399	Here
new-york-9400020.jpg	jpg	\Pictures\0003	18.6 KB	03.05.2004 17:17:56	24.03.2004...	12.05.2005 ...	A	26465	401	you can
Nine Planets.jpeg	jpeg	\Pictures\0001	20.6 KB	03.05.2004 17:17:58	30.04.2004...	12.05.2005 ...	A	31032	501	add
jewelry.jpg	jpg	\Pictures\0003	20.7 KB	03.05.2004 17:17:56	03.05.2004...	13.05.2004 ...	A	26383	397	comments.
Neo & Trinity 1.jpg	jpg	\Pictures\0001	26.3 KB	03.05.2004 17:17:58	26.06.1999...	17.05.2005 ...	A	30966	499	
Patrick Stewart 2.jpeg	jpeg	\Pictures\0001	27.2 KB	03.05.2004 17:17:58	24.02.1997...	12.05.2005 ...	A	31169	506	
Tripod 3.jpg	jpg	\Pictures\0002	29.2 KB	03.05.2004 17:17:57	30.04.2004...	13.01.2005 ...	A	29261	457	
Tripod 1.jpg	jpg	\Pictures\0002	29.3 KB	03.05.2004 17:17:57	30.04.2004...	13.01.2005 ...	A	29246	456	
makeup3.jpg	jpg	\Pictures\0003	32.0 KB	03.05.2004 17:17:57	03.05.2004...	12.05.2005 ...	A	26475	402	
Zhang Ziyi 40.jpg	jpg	\Pictures\0001	32.1 KB	03.05.2004 17:17:57	03.05.2004...	12.05.2005 ...	A	31479	517	
sparpreis50.gif	gif	\Pictures\0003	34.2 KB	03.05.2004 17:17:57	03.05.2004...	12.05.2005 ...	A	26631	408	
McCoy.jpeg	jpeg	\Pictures\0001	35.5 KB	03.05.2004 17:17:57	03.05.2004...	12.05.2005 ...	A	30787	494	
Patrick Stewart 5.jpg	jpg	\Pictures\0001	36.5 KB	03.05.2004 17:17:57	03.05.2004...	12.05.2005 ...	A	31185	507	
Spock 1.jpg	jpg	\Pictures\0001	36.9 KB	03.05.2004 17:17:57	03.05.2004...	12.05.2005 ...	A	31409	514	

The gallery view shows a grid of image thumbnails. Two thumbnails are highlighted with red 'X' marks, indicating corrupt files. The first corrupt file is 'McCoy.jpeg' (35.5 KB) with extension '.ip' and a note '(corrupt file)'. The second corrupt file is 'Mist.jpeg' (53.9 KB) with extension '.jpeg' and a note '(corrupt file)'. The gallery also shows various other images, including portraits and landscapes.

# Analisi: Internet Evidence Analyzer



# Analisi: Axiom

Magnet AXIOM Process 0.8.0.304

File Tools Help

### SELECT ARTIFACTS TO INCLUDE IN CASE

#### CASE DETAILS

#### EVIDENCE SOURCES

Acquire evidence	1
Load evidence	2

#### ARTIFACT DETAILS

Computer artifacts	117 of 117
<b>Mobile artifacts</b>	<b>122 of 122</b>













































#### PROCESSING DETAILS

Add keywords to search

#### ANALYZE EVIDENCE

#### MOBILE ARTIFACTS

[SELECT ALL](#) [CLEAR ALL](#) [VIEW ALL](#)

<input checked="" type="checkbox"/> ADVANCED TOOLS (2 of 2)	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> CHAT (23 of 23)	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> CLOUD (1 of 1)	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> DOCUMENTS (6 of 6)	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> EMAIL (11 of 11)	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> MEDIA (5 of 5)	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> MOBILE BACKUPS (2 of 2)	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> OPERATING SYSTEM (38 of 38)	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> PEER TO PEER (1 of 1)	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> SOCIAL NETWORKING (14 of 14)	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> WEB RELATED (19 of 19)	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	

[BACK](#) [GO TO PROCESSING DETAILS](#)

# Analisi: NUIX

The screenshot displays the Nuix eDiscovery Workstation interface. The main window title is "Nuix-Bank-regexp-Test - Nuix". The search bar contains the query "Search: named-entities:bank-regexp-test;\'\*" and shows results for "20/03/2014".

**Document Navigator:** Shows a tree view of the search results. Under "Evidence (2/6 hits; 33.33%)", there are "Documents (2)" including "matching1.txt (1)", "matching2.txt (1)", "non-matching1.txt", and "non-matching2.txt". There are also "Excluded Items (0/6; 0.00%)", "Custodians", "Item Sets", "Automatic Classifiers", "Production Sets", "Filtered Items", "Email Attachments", "Emails and Loose Files (2)", "Irregular Items (0)", "Commented (0)", "Multimedia (?)", "Named Entities (2)", "Bank regexp Test (2)", and "# Personal ID (1)".

**Results:** A table showing the search results:

Name	File Type
matching1.txt	Plain Text
matching2.txt	Plain Text

Below the table, it says "Displaying 2 items." and includes buttons for "Add Tags...", "Exclude Items...", and "Export...".

**Preview:** Shows the content of the selected file "matching1.txt". The text is:

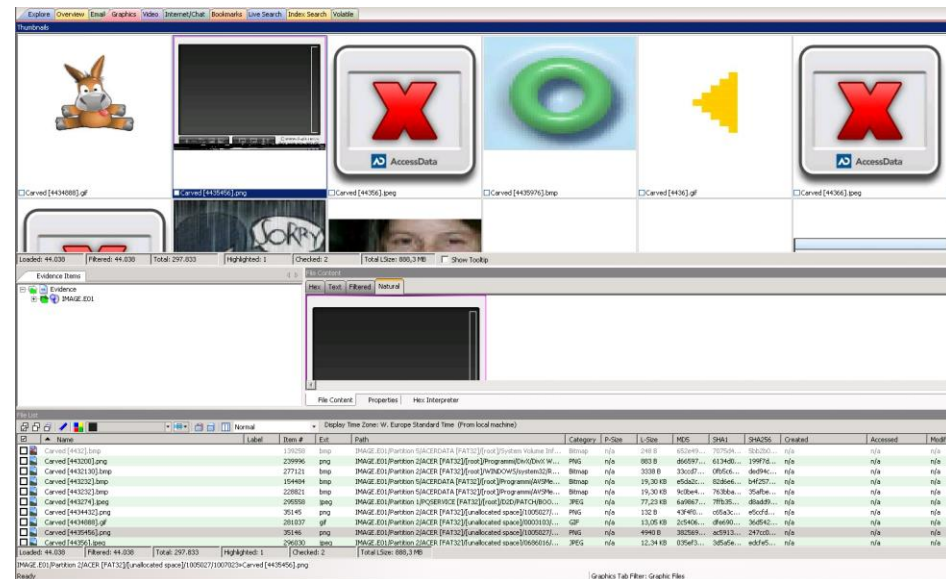
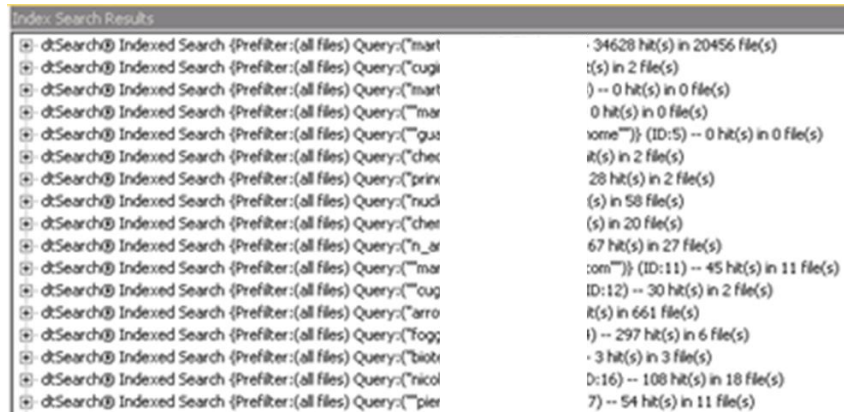
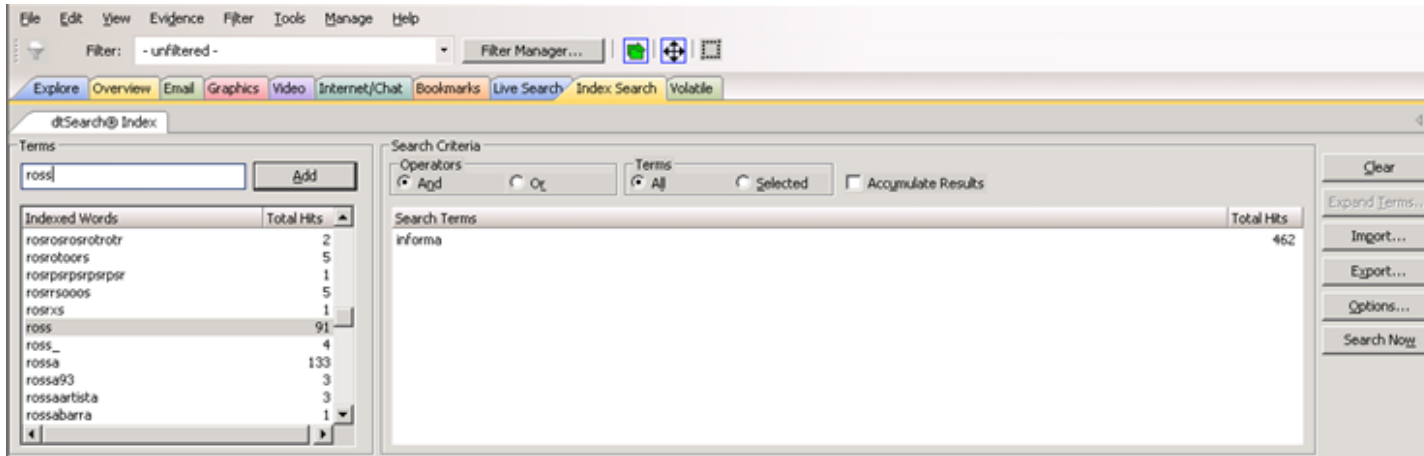
```
Bla bla bla
Bla 1472-58-369 bla bla
Bla bla bla
```

The preview pane also shows metadata: "Created: 20/03/2014 1:37:06 PM", "Last Modified: 20/03/2014 1:38:07 PM", "Last Accessed: 20/03/2014 1:37:06 PM", "Author:", "Company:", and "Keywords:". There are also tabs for "Text", "Family (1)", "Metadata", "PDF", and "Native".

**Review and Tag:** Shows the selected file "matching1.txt" and a link to "Edit Tags".

At the bottom, there is a status bar showing "Nuix eDiscovery Workstation" and "Memory (106.69 MB / 4.66 GB)".

# Analisi: FTK





# Analisi: UFED4PC

**UFED Physical Analyzer 6.3.11.21**

File View Tools Extract Python Plug-ins Report Help

Welcome | Extraction Summary (1) | All Content | Physical

### Extraction Summary

+ Add extraction | Project settings | Generate report

Extractions: 1

**Physical**  
Samsung GSM GT-I9506 Galaxy S4  
Physical [ Bootloader ]

Extraction start date/time: 11/29/2015 07:59(UTC+2)  
Extraction end date/time: 11/29/2015 08:51(UTC+2)  
C:\Users\kerenc\Desktop\Extractions\Sam...

#### Device Info

Bluetooth device name	Galaxy S4	<a href="#">settings.db : 0x235C8</a>
Bluetooth MAC Address	00:73:E0:12:3D:F9	<a href="#">settings.db : 0x22F24</a>
Android ID	c2e3da6cdc5cf975	<a href="#">settings.db : 0x22E4D</a>
Android fingerprint	samsung/ks01texx/ks01lte4.3/JSS15I/9506XX...	<a href="#">build.prop : 0x388</a>
OS Version	4.3	<a href="#">build.prop : 0xED</a>
Detected Phone Vendor	samsung	<a href="#">build.prop : 0x18A</a>
Detected Phone Model	GT-I9506	<a href="#">build.prop : 0x1A0</a>
Mac Address	F0:25:87:1B:4C:FB	<a href="#">.mac.info : 0x0</a>
IMSI	425010773618779	<a href="#">com.android.phone_preferences.xml : 0xE3</a>
ICCID	89972011013031230331	<a href="#">com.android.phone_preferences.xml : 0x119</a>
Phone Activation Time	6/16/2014 11:10(UTC+0)	<a href="#">bt_addr : 0x0</a>
Bluetooth MAC Address	00:73:E0:12:3D:F9	<a href="#">bt_config.xml : 0x0</a>
Bluetooth MAC Address	00:73:E0:12:3D:F9	<a href="#">serial_no : 0x0</a>
Factory number	RFBF10E02SL	<a href="#">persist.sys.language : 0x0</a>
Locale language	en	<a href="#">persist.sys.country : 0x0</a>
Country Name	GB	<a href="#">persist.sys.timezone : 0x0</a>
Time Zone	Asia/Jerusalem	<a href="#">2400257.cfg : 0x100</a>
IMEI	358672055497832	<a href="#">com.android.settings_preferences.xml : 0x693</a>
Mock locations allowed	False	<a href="#">com.android.settings_preferences.xml : 0xEAD</a>
Auto Time Zone	True	<a href="#">com.android.settings_preferences.xml : 0x1172</a>
Auto Time	True	<a href="#">google.settings.db-wal : 0xFA679</a>
Location Services Enabled	True	<a href="#">adid_settings.xml : 0x58</a>
Advertising Id	237a5462-195d-4f0f-93dd-fd2be4ca9791	
<b>Tethering</b>		
Hotspot AP Name	AndroidAP	<a href="#">softap.conf : 0x32</a>
Hotspot Password	yhrv8746	<a href="#">softap.conf : 0x32</a>
<b>Network Interfaces</b>		

#### Device Content

17 data sources can be extracted using UFED Cloud Analyzer

##### Phone Data

Application Usage	237 (6)	Calendar	65 (18)	Call Log	438 (14)
Chats	815 (293)	Contacts	1343 (158)	Cookies	2120 (325)
Device Locations	3858 (19)	Device Notifications	8 (2)	Device Users	1
Emails	485 (60)	Form Data	1	Installed Applications	524 (5)
Instant Messages	31 (3)	Maps	14	MMS Messages	9
Notes	101 (56)	Passwords	45	Powering Events	50
Searched Items	289 (36)	SMS Messages	207 (15)	User Accounts	145 (1)
User Dictionary	3785	Web Bookmarks	142 (8)	Web History	379 (54)

# Analisi: Oxygen Forensics

## iTunes Backup (backup tunes)



Add photo

Nome telefono iTunes Backup (backup iTunes)  
 Nome Vendite Apple iPhone 4  
 Nome interno iPhone3,1  
 Platform IOS  
 Hardware 0127  
 Versione Software 7.1.2  
 Serial number 8512  
 Versione di estrazione 7.0.0.505  
 Extraction started 02/02/2015 18:43:19  
 Extraction finished 02/02/2015 19:15:17

Enter device note here

## Manu



Add photo

Full profile

Ispettore Add inspector  
 Causa Add case  
 Numero indizio Add evidence number  
 Possessore M  
 Mobile phone Add mobile number  
 Email @yahoo.it

Enter owner note here

## Sezioni comuni (16)

- Informazione dispositivo
- Links and Stats
- Search
- Aggregated Contacts (539)
- Messaggi (3345 / 777)
- Sfogliala Risorse (4405)
- Connessioni Web e Postazioni (291)
- Organizer Agenda (95) Note (172)
- Social Graph
- Cronologia (11940 / 1279)
- Registro Eventi (202 / 102)
- Dizionari (5317)
- Reports
- Key Evidence
- Rubrica (402)

## Applicazioni (8)

- Applicazioni (48)
- Messengers Facebook Messenger (2) WhatsApp Messenger (7377)
- Multimedia Voice Memos (258)
- Navigation Apple Maps (20) Waze (47)
- Social Networks Facebook (55)
- Web Browsers Safari (387)

Oxygen Forensic Suite 2015 Analysta (USB Instance)

File Explorer: Tutti i dispositivi > iTunes Backup (backup iTunes) - 02/02/2015 18:43:19 [1274] > Messengers > WhatsApp Messenger

Connect device | Esporta | Stampa | Show viewer | Mostra file | Guida

Informazione: 400 | Dati uploadati: 609 | Informazioni applicazione: 91

Application information: WhatsApp Mess... (7377) | Source: /mnt/c/Users/.../AppData/Local/WhatsApp/Messages/... | Remote party name: D | Text: M

Direction	Remote party	Remote party name	Text	Time stamp (UTC)	Chat
✓	39364	De	Me	28/12/2012 08:47:09	1, 0
✓	39364	De	OK	22/1/2012 19:41:47	1, 0
✓	39364	De	OK	22/1/2012 19:40:24	1, 0
✓	39364	De	OK	22/1/2012 19:39:06	1, 0
✓	39364	De	OK	22/1/2012 15:33:23	1, 0
✓	39364	De	OK	22/1/2012 15:09:14	1, 0
✓	39364	De	OK	14/1/2012 2:02:29	1, 0
✓	39364	De	OK	20/10/2012 10:12:13	1, 0
✓	39364	De	OK	20/10/2012 10:08:17	1, 0
✓	39364	De	OK	19/10/2012 20:18:06	1, 0
✓	39364	De	OK	14/10/2012 18:36:20	1, 0
✓	39364	De	OK	14/10/2012 18:32:24	1, 0
✓	39364	De	OK	14/10/2012 18:32:24	1, 0
✓	39364	De	OK	14/10/2012 18:24:58	1, 0
✓	39364	De	OK	14/10/2012 18:23:25	1, 0
✓	39364	De	OK	14/10/2012 18:19:39	1, 0
✓	39364	De	OK	14/10/2012 18:19:24	1, 0
✓	39364	De	OK	14/10/2012 13:23:47	1, 0
✓	39364	De	OK	08/10/2012 20:07:21	1, 0
✓	39364	De	OK	08/10/2012 20:06:24	1, 0
✓	39364	De	OK	08/10/2012 18:51:52	1, 0
✓	39364	De	OK	06/10/2012 18:33:01	1, 0
✓	39364	De	OK	06/10/2012 18:30:10	1, 0
✓	39364	De	OK	19/09/2012 10:49:05	1, 0
✓	39364	De	OK	19/09/2012 10:32:51	1, 0
✓	39364	De	OK	19/09/2012 10:30:07	1, 0
✓	39364	De	OK	17/09/2012 13:04:07	1, 0
✓	39364	De	OK	06/09/2012 13:01:05	1, 0
✓	39364	De	OK	06/09/2012 13:00:06	1, 0
✓	39364	De	OK	06/09/2012 08:34:34	1, 0
✓	39364	De	OK	06/09/2012 08:34:03	1, 0
✓	39364	De	OK	06/09/2012 08:32:46	1, 0
✓	39364	De	OK	06/09/2012 08:31:10	1, 0

Categories (7377): Account (1), Contact (523), WhatsApp Messenger (178), Phonebook (152), Messages (9230), Group (103), 68, G (932), Private (3303), 2, Dupl...-safone... (34), 3, 2u... (316), 1, 0... (246), 4, 5... (246), 7, 7... (23), 8, 5... (9), 6, 5... (63), 9, 5... (20), 11, 5... (142), 12, G (12), 13, 1... (34), 14, 1... (118), 15, 1... (142), 16, 1... (20), 17, 5... (11), 18, 1... (43), 19, 1... (153), 18, 0... (93), 20, 0... (92), 21, 1... (99)

Category description: Messages/Private category displays all the private messages of the account. Direction column shows the message direction. Remote party column shows the user with whom the device owner communicates. Remote party name column shows the remote party name. Text column shows the message text. Time stamp (UTC) column displays...

Analista version: 7.0.0.505 | iTunes Backup (backup iTunes) | Total: 114 | Filtered: 114

# Analisi: P2C

The screenshot displays an email client interface. On the left is a navigation pane with folders like 'Radice - Pubblico', 'IPM\_SUBTREE', and 'NON\_IPM\_SUBTREE'. The main area shows a list of 31 emails with columns for Subject, From, To, Created, and Sent. The selected email is from 'ni@' to 'it>' with the subject 'Verifica giroconto'. Below the list, the 'E-mail Data' pane shows the email's content, which is a technical message with headers and a body containing technical details.

Subject	From	To	Created	Sent
Ora è	"Mic	F Dt	25/07/2013 14:37:35	25/07/2013 14:37:34
Conf	"Tet	e Dt	25/07/2013 19:21:59	25/07/2013 19:21:58
Hors	"Ma	d Dt	15/01/2014 13:31:25	15/01/2014 13:31:24
Limvi	"me	c Dt	18/02/2014 10:11:33	18/02/2014 10:11:31
caffit	"Dar	F Dt	28/03/2014 17:52:37	28/03/2014 17:52:36
Rif: F	"Rer	u Dt	31/03/2014 14:13:51	31/03/2014 14:13:46
Anali	"pac	B Dt	14/05/2014 18:33:27	14/05/2014 18:33:16
I: STJ	"Dar	F Te	09/06/2014 11:53:40	09/06/2014 11:53:40
I: Ver	"FAI	ij Dt	19/06/2014 15:53:11	19/06/2014 15:52:50
I: Ver	"FAI	ij Dt	19/06/2014 15:53:16	19/06/2014 15:52:59
R: Pa	"Elit	is Dt	24/06/2014 09:38:31	24/06/2014 09:38:30
R: Pa	"Pat	is Dt	25/06/2014 17:09:10	25/06/2014 17:09:10
nuov	"Anc	is Dt	25/06/2014 18:44:45	25/06/2014 18:44:43
Corr	"Nic	F Dt	08/07/2014 13:24:10	08/07/2014 13:24:09
Sen	"42C	F Dt	08/07/2014 14:47:17	08/07/2014 14:47:17

Finished Total: 31

**E-mail Data**

**Verifica giroconto**

To: Da ni@ it> on behalf of " : S.p.A." < ni@ :it>

Received: from mail local (10.0.1.50) by madrid local (10.0.1.71) with Microsoft SMTP Server id 14.2.342.3; Thu, 19 Jun 2014 15:53:16 +0200  
X-AuditID: 0a000132479a56d000019c9-36-53a2eb47ec08  
Received: from mail (mail) by mail local (Symantec Messaging Gateway) with SMTP id 68.62.06601.748E2A35; Thu, 19 Jun 2014 15:53:16 +0200 (CEST)  
Received: from SZK IT ([;-]) by s2k :IT ([;-]) with mapi; Thu, 19 Jun 2014 15:53:00 +0200  
From: To: "Da" ni@ it>  
Disposition-Notification-To: ni@ it>  
Date: Thu, 19 Jun 2014 15:52:59 +0200  
Subject: I: Verifica  
Thread-Topic: Verifica  
Thread-Index: Ac+KxdOvFVTO/TZR62KCGT7Qo3KwA/+2wQ  
Message-ID: <9FC6C0D7DE4DA840BABACD8F4499E0A3FB8F46A96@e2 :IT>  
References: <ADR39000000142410@ :it>  
In-Reply-To: <ADR39000000142410@ :it>  
Accept-Language: it-IT

RFI Header Text RTF HTML Raw HTML Attachments

# Analisi: ricerca per parola chiave

## **Bus**

*“Bus” o “autobus” o “Pullman”?*

## **Anonimo**

*“Anonimo” o “anonimo” o “anonimi” o “nascosto”?*

## **Indirizzo IP**

*(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)*

## **Giovanni Rossi**

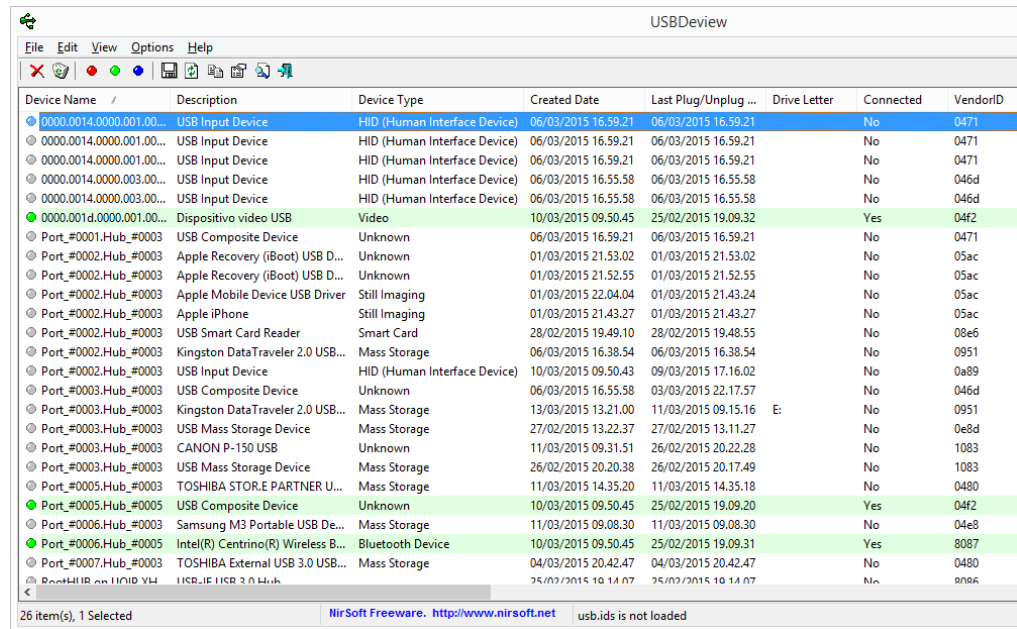
*“Giovanni AND Rossi” o “Giovanni Rossi” o “Rossi Giovanni”  
o “G. Rossi” o “Giovanni NEAR/50 Rossi”*

# Analisi: artefatti di Windows

- Registri
  - Configurazione del sistema operativo e dei software applicative
- Cestino
  - Salvataggio dei file cancellati
- Log eventi
  - Log delle attività degli utenti, del sistema e delle applicazioni
- Punti di ripristino
  - Backup automatico di registry e file rilevanti del sistema operativo
- LNK file (collegamenti)
  - Collegamenti ad altri file
- Dispositivi USB collegati


# Analisi: dispositivi USB

- Dispositivi USB rilevanti collegati al sistema
  - Dispositivi di memorizzazione di dati digitali USB
  - Smartphone
  - Macchine fotografiche
  - Riproduttori audio
- Informazioni rilevanti memorizzate in un computer
  - Ultima connessione
  - Produttore
  - Modello
  - S/N
  - Ultima lettera assegnata



Device Name	Description	Device Type	Created Date	Last Plug/Unplug ...	Drive Letter	Connected	VendorID
0000.0014.0000.001.00...	USB Input Device	HID (Human Interface Device)	06/03/2015 16.59.21	06/03/2015 16.59.21		No	0471
0000.0014.0000.001.00...	USB Input Device	HID (Human Interface Device)	06/03/2015 16.59.21	06/03/2015 16.59.21		No	0471
0000.0014.0000.001.00...	USB Input Device	HID (Human Interface Device)	06/03/2015 16.55.58	06/03/2015 16.55.58		No	046d
0000.0014.0000.003.00...	USB Input Device	HID (Human Interface Device)	06/03/2015 16.55.58	06/03/2015 16.55.58		No	046d
0000.0014.0000.003.00...	USB Input Device	HID (Human Interface Device)	06/03/2015 16.55.58	06/03/2015 16.55.58		No	046d
0000.001d.0000.001.00...	Dispositivo video USB	Video	10/03/2015 09.50.45	25/02/2015 19.09.32		Yes	04f2
Port_#0001.Hub_#0003	USB Composite Device	Unknown	06/03/2015 16.59.21	06/03/2015 16.59.21		No	0471
Port_#0002.Hub_#0003	Apple Recovery (iBoot) USB D...	Unknown	01/03/2015 21.53.02	01/03/2015 21.53.02		No	05ac
Port_#0002.Hub_#0003	Apple Recovery (iBoot) USB D...	Unknown	01/03/2015 21.52.55	01/03/2015 21.52.55		No	05ac
Port_#0002.Hub_#0003	Apple Mobile Device USB Driver	Still Imaging	01/03/2015 22.04.04	01/03/2015 21.43.24		No	05ac
Port_#0002.Hub_#0003	Apple iPhone	Still Imaging	01/03/2015 21.43.27	01/03/2015 21.43.27		No	05ac
Port_#0002.Hub_#0003	USB Smart Card Reader	Smart Card	28/02/2015 19.49.10	28/02/2015 19.48.55		No	08e6
Port_#0002.Hub_#0003	Kingston DataTraveler 2.0 USB...	Mass Storage	06/03/2015 16.38.54	06/03/2015 16.38.54		No	0951
Port_#0002.Hub_#0003	USB Input Device	HID (Human Interface Device)	10/03/2015 09.50.43	09/03/2015 17.16.02		No	0a89
Port_#0003.Hub_#0003	USB Composite Device	Unknown	06/03/2015 16.55.58	03/03/2015 22.17.57		No	046d
Port_#0003.Hub_#0003	Kingston DataTraveler 2.0 USB...	Mass Storage	13/03/2015 13.21.00	11/03/2015 09.15.16	E:	No	0951
Port_#0003.Hub_#0003	USB Mass Storage Device	Mass Storage	27/02/2015 13.22.37	27/02/2015 13.11.27		No	0e8d
Port_#0003.Hub_#0003	CANON P-150 USB	Unknown	11/03/2015 09.31.51	26/02/2015 20.22.28		No	1083
Port_#0003.Hub_#0003	USB Mass Storage Device	Mass Storage	26/02/2015 20.20.38	26/02/2015 20.17.49		No	1083
Port_#0005.Hub_#0003	TOSHIBA STORE PARTNER U...	Mass Storage	11/03/2015 14.35.20	11/03/2015 14.35.18		No	0480
Port_#0005.Hub_#0005	USB Composite Device	Unknown	10/03/2015 09.50.45	25/02/2015 19.09.20		Yes	04f2
Port_#0006.Hub_#0003	Samsung M3 Portable USB De...	Mass Storage	11/03/2015 09.08.30	11/03/2015 09.08.30		No	04e8
Port_#0006.Hub_#0005	Intel(R) Centrino(R) Wireless B...	Bluetooth Device	10/03/2015 09.50.45	25/02/2015 19.09.31		Yes	8087
Port_#0007.Hub_#0003	TOSHIBA External USB 3.0 USB...	Mass Storage	04/03/2015 20.42.47	04/03/2015 20.42.47		No	0480
Port_#0007.Hub_#0003	TOSHIBA External USB 3.0 USB...	Mass Storage	25/02/2015 10.14.07	25/02/2015 10.14.07		No	8086

# Analisi: dispositivi USB

Name ▲	Date Created	Date Modified
 Marketing Plans	23/07/2007 11:44 AM	23/07/2007 11:44 AM

## Link target information

Local Path	E:\Marketing Plans.doc
Volume Type	Removeable Disk
Volume Label	BIGSTORE
Volume Serial Number	6CA3-55E3
File size	30720
Creation time (UTC)	9/04/2007 11:39:59 PM
Last write time (UTC)	7/04/2007 10:56:04 AM
Last access time (UTC)	9/04/2007 4:00:00 PM



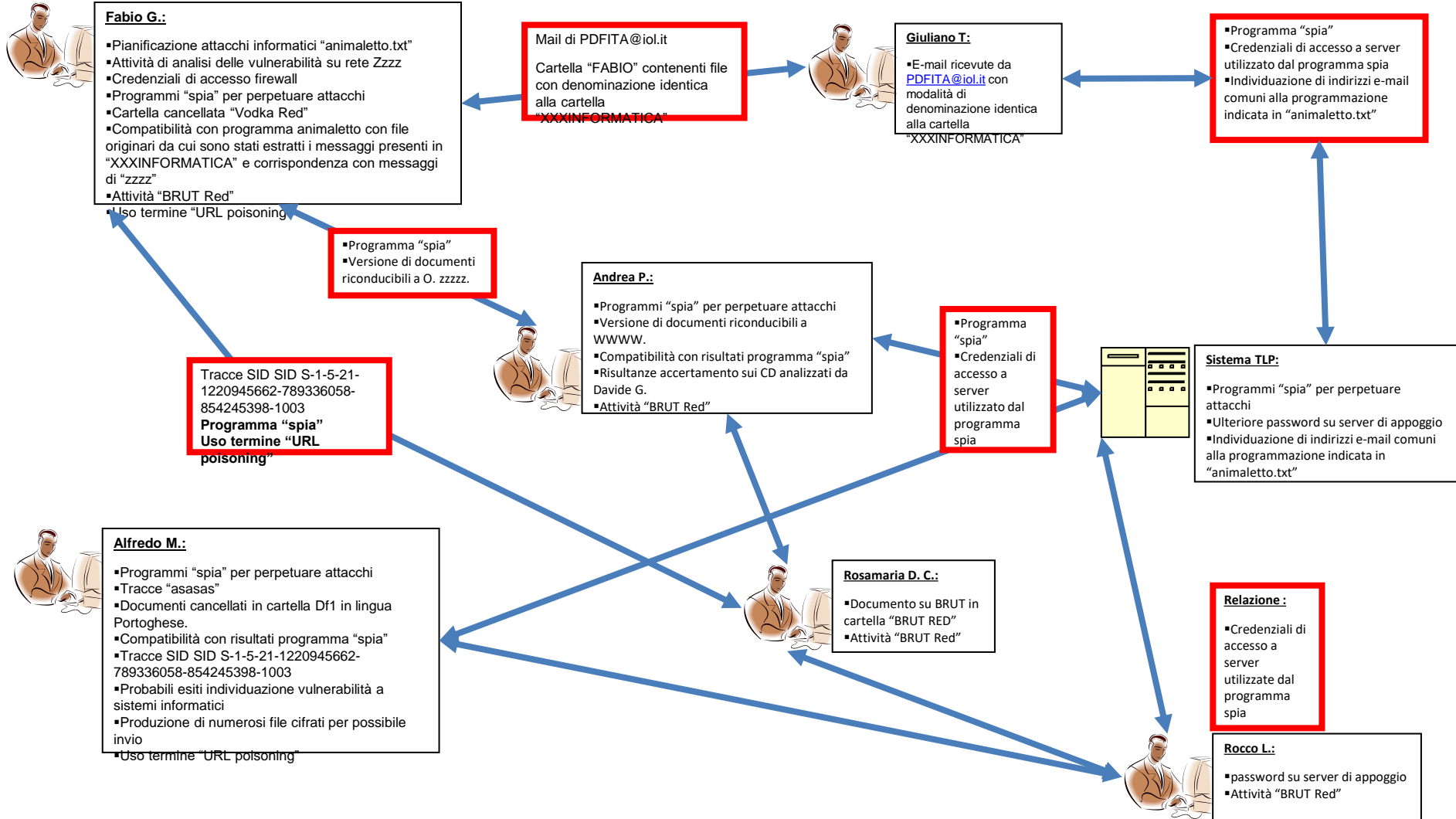
# La link analysis

Si pone inoltre il problema in generale di analizzare banche dati sempre più voluminose spesso non strutturate difficilmente interrogabili in modo “fuzzy”

La link analysis è il processo di costruzione di una rete di oggetti o item interconnessi nel tempo e con l'uso di tecniche speciali, di strumenti software finalizzati a: formare, esaminare, modificare, analizzare, cercare e mostrare modelli di comportamento, specialmente di tipo illecito



# Esempio di link analysis



# Valutazione

Perché è necessario anche un momento di valutazione del reperto, se il bit può assumere solo il valore di 0 o 1 ?

010000110100000101001101010001010101001001000001

CAMERA



# Valutazione

Perché il reperto informatico può essere facilmente:

- **Alterato**
- **Inquinato**
- **Contraffatto**

Inoltre, bisogna verificare se le operazioni di acquisizione del reperto informatico sono state legittime

# Valutazione

- Valutazione necessaria per comprendere il significato dei dati presenti sul supporto
- Esempio di valutazione:
  - Data di ultima lettura: 3 maggio 2014
  - Data di ultima modifica: 5 aprile 2013
  - Data di creazione: 3 maggio 2014
- Cosa significano questi dati relativi ad un file?



Valutazione: facciamo un esempio



**Yara Gambirasio, "Bossetti accedeva a siti pedopornografici. Ricercava 'tredicenni'"**

## Valutazione: facciamo un esempio

“L’unica ricerca datata – sottolineano gli avvocati **Silvia Gazzetti** e **Claudio Salvagni** – risale al maggio 2014, stiamo parlando di una ricerca ‘postuma’ se pensiamo all’omicidio di Yara” e “che non tiene conto che l’assistito ha un figlio 13enne. Come padre avrebbe potuto cercare su internet spiegazioni, per un figlio adolescente, su un argomento delicato”. Inoltre è “un pc a cui ha accesso tutta la famiglia Bossetti”, precisano. Non solo: il computer “non è un

## Valutazione: facciamo un esempio

Yara, l'avvocato di Bossetti: "Ricerca di 13enni su internet? Era un pop-up"





# Presentazione

- Si manifesta in due modalità
  - Scritta
    - Relazione tecnica, memorie, verbali
  - Orale
    - Udienze, CTU/Perizie, incontri con legali e committenti
- Mettersi nei panni dell'interlocutore
- Capire punto di vista altrui
- Stimolare domande nel territorio dove si è forti
- Linguaggio semplice

## Elementi di disturbo

- Background culturale
  - Linguaggio troppo difficile
    - Restare comunque rigorosi
- Stress del momento
- Stanchezza
- Ambiente fisico
  - Locali angusti
- Disturbi audio
  - Voce bassa, rumore di fondo, chiacchiericcio, interruzioni
- Distrazione dell'interlocutore
- Interlocutore indisposto o prevenuto
  - Fretta, fattori emotivi, problemi personali...