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

Michele Ferrazzano

ISO/IEC 27037/2012

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

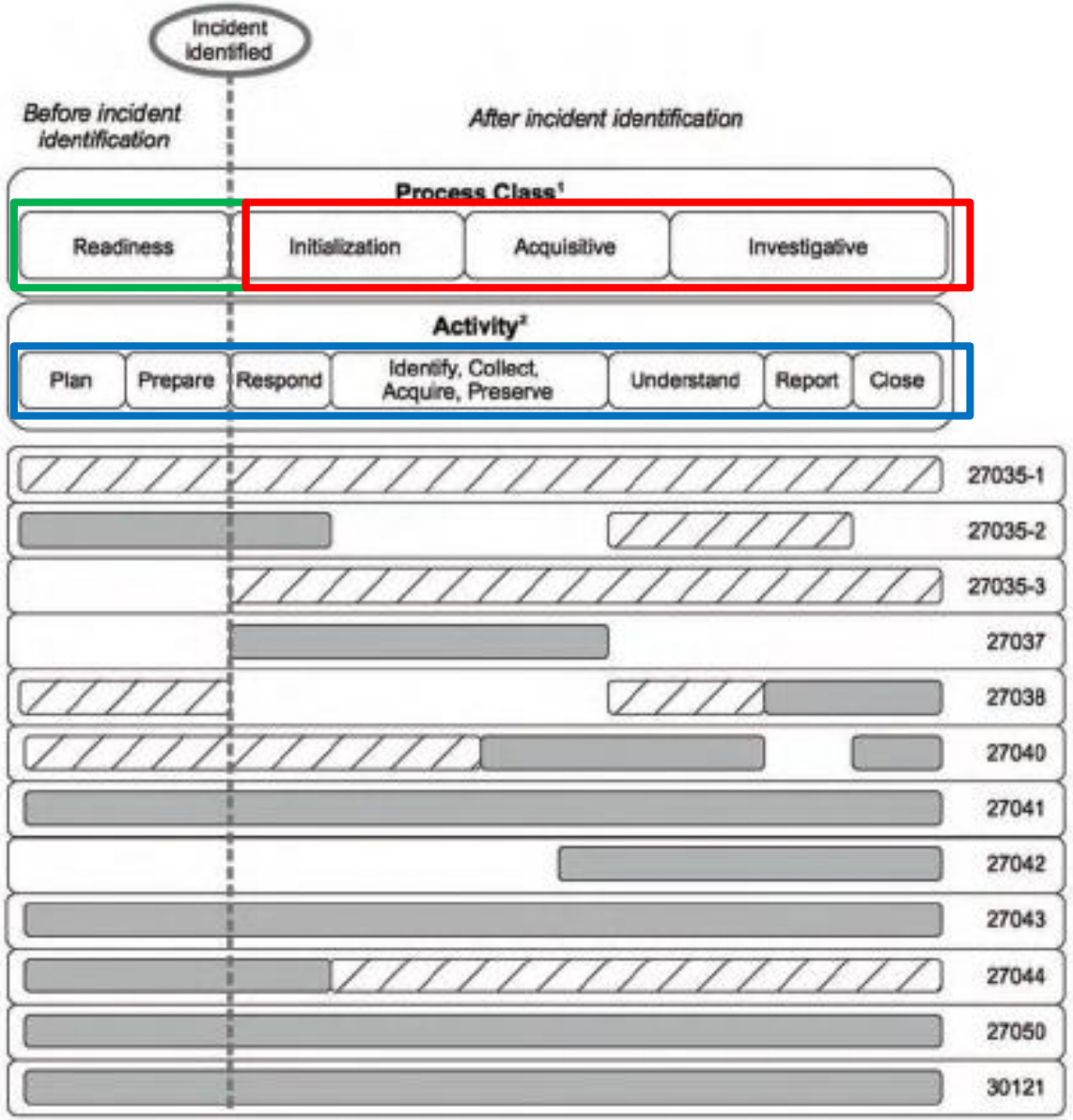
- Information technology
  - Security techniques
    - **Guidelines for identification, collection, acquisition and preservation of digital evidence**

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



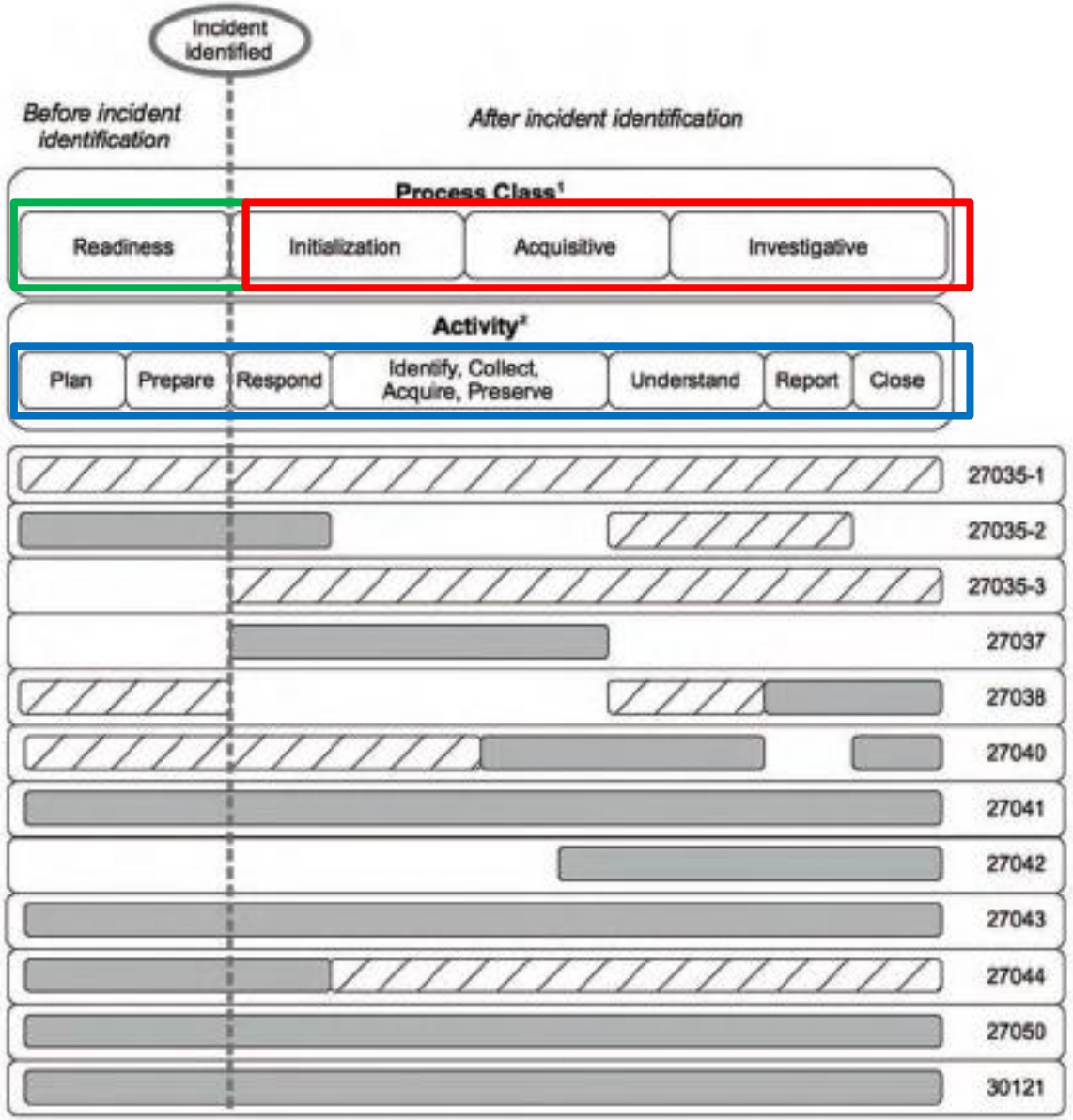
Key

International standard can be directly applied to these activities.

International standard contains information which may influence and/or assist with these activities.

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

ISO/IEC – Panoramica generale



Information security incident management

Guidelines for identification, collection, acquisition and preservation of digital evidence

Specification for digital redaction

Storage security

Guidance on assuring suitability and adequacy of incident investigative method

Guidelines for the analysis and interpretation of digital evidence

Incident investigation principles and processes

Guidelines for Security Information and Event Management (SIEM)

Electronic discovery

Governance of digital forensic risk framework

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

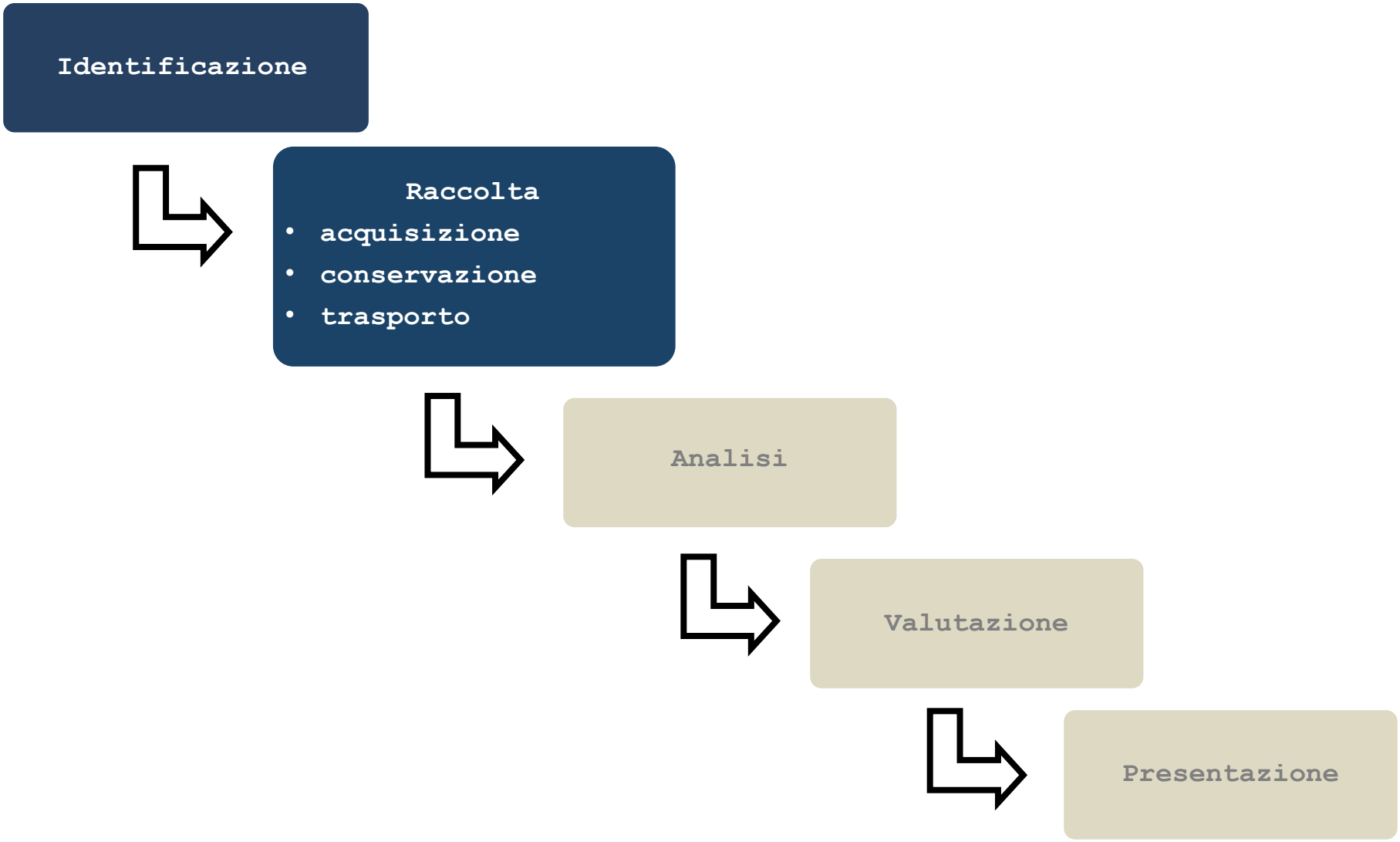
ISO/IEC 27037/2012

- 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



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 (DEFRs)	**Digital evidence specialists (DESs)**	**Incident response specialists**	**Forensic laboratory managers**
Operatore che si approccia per primo ai sistemi (supporti di memorizzazione e dati) di potenziale interesse Adeguata esperienza e competenze Può avvalersi di collaboratori	Operatore esperto di evidenze informatiche	Operatore che si occupa del primo intervento post incidente informatico In Italia spesso coincide (ahimè) con l'amministratore di sistema	Operatore responsabile di laboratorio informatico forense

ISO/IEC 27037/2012

Persone che trattano reperti informatici e precauzioni - DEFR

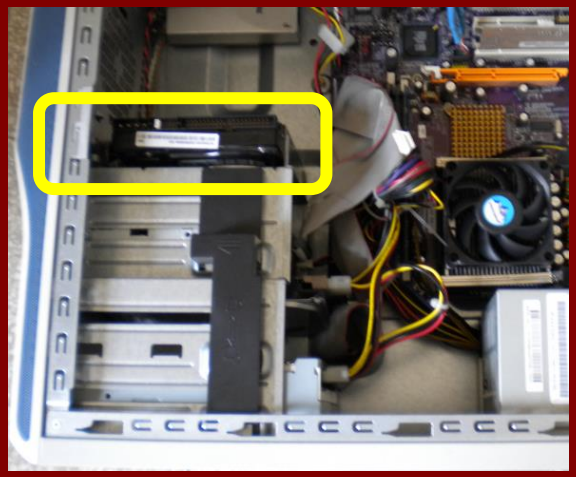
- Compiti del DEFR
  - mettere in sicurezza e proteggere il luogo appena possibile
  - controllare l'area che contiene dispositivi di memorizzazione digitale
  - individuare il responsabile dell'area
  - allontanare le persone dai dispositivi digitali e dall'alimentazione elettrica
  - documentare tutti 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

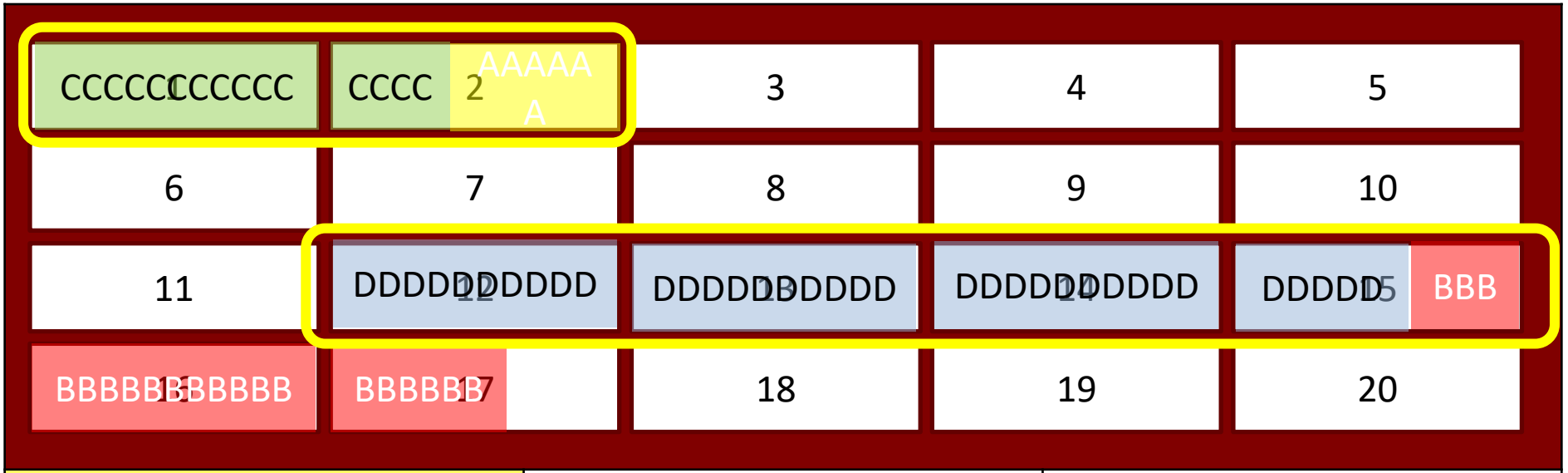
Dispositivi di memorizzazione che contengono dati

				
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

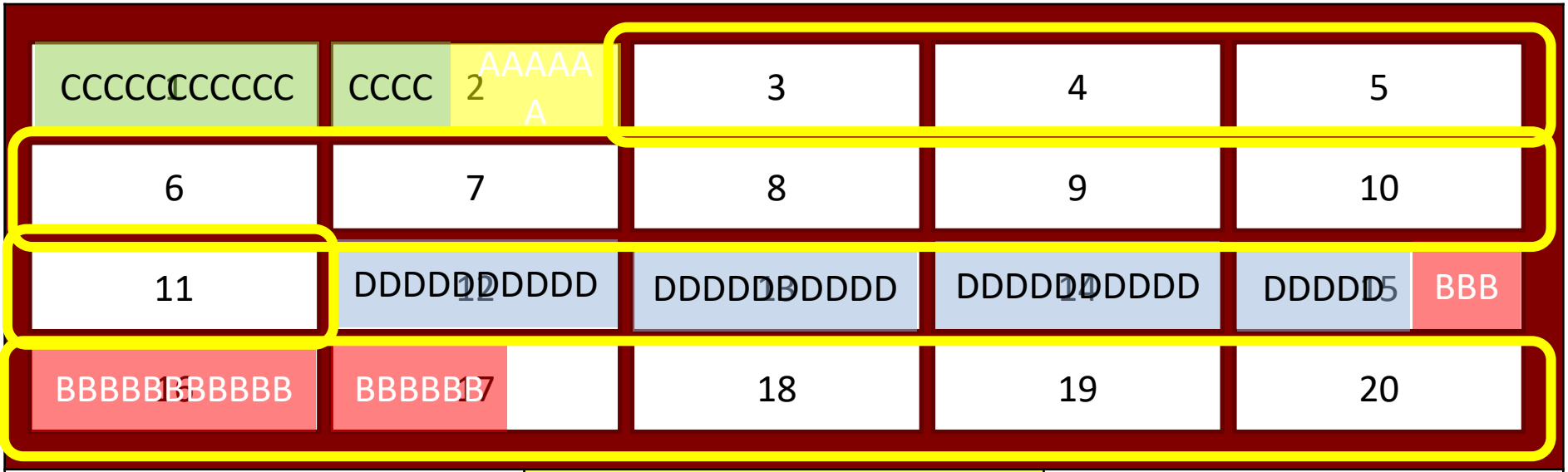
		
Dispositivo digitale	**Dispositivo di memorizzazione di dati digitali**	**Periferica**
Apparato elettronico usato per processare o memorizzare dati digitali	Dispositivo che è in grado di memorizzare dati digitali [*ISO/IEC 10027:1990*]	Dispositivo che, connesso ad un dispositivo digitale, ne estende le funzionalità

Glossario



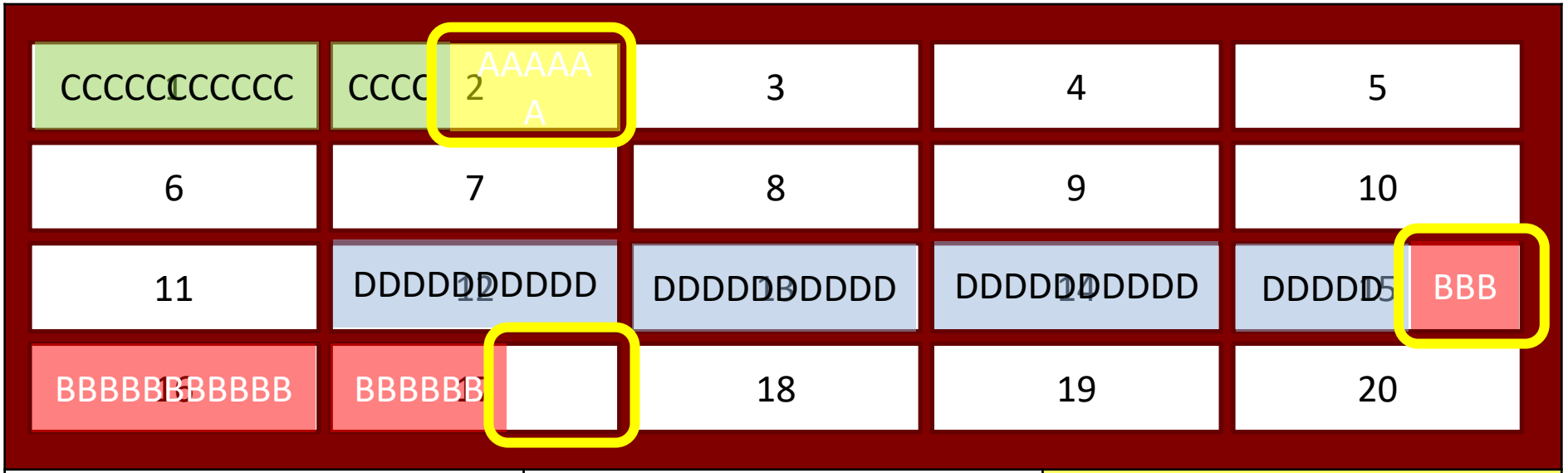
Spazio allocato	Spazio non allocato	Slack space
Area di un dispositivo di memoria che è utilizzata per memorizzare dati, inclusi metadati	Area di un dispositivo di memoria che non è allocato dal sistema operativo ed è a disposizione per memorizzare dati, inclusi metadati	Area (compresa tra l'ultimo bit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

Glossario



Spazio allocato	Spazio non allocato	Slack space
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

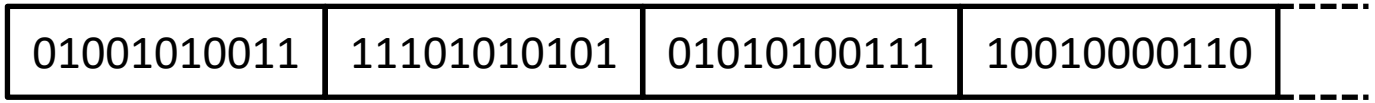
Glossario



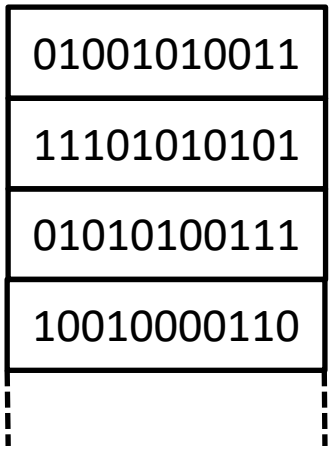
Spazio allocato	Spazio non allocato	Slack space
Area di un dispositivo di memoria che è utilizzata per memorizzare dati, inclusi metadati	Area di un dispositivo di memoria che non è allocato dal sistema operativo ed è a disposizione per memorizzare dati, inclusi metadati	Area (compresa tra l'ultimo bit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

Glossario

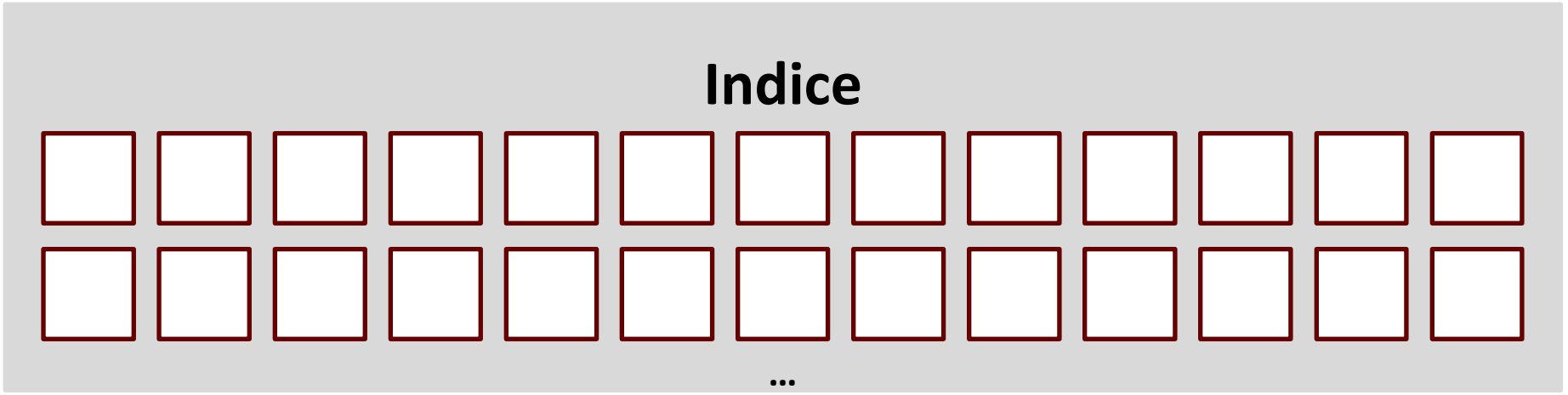
Spazio allocato *vs.* non allocato (*vs.* slack)



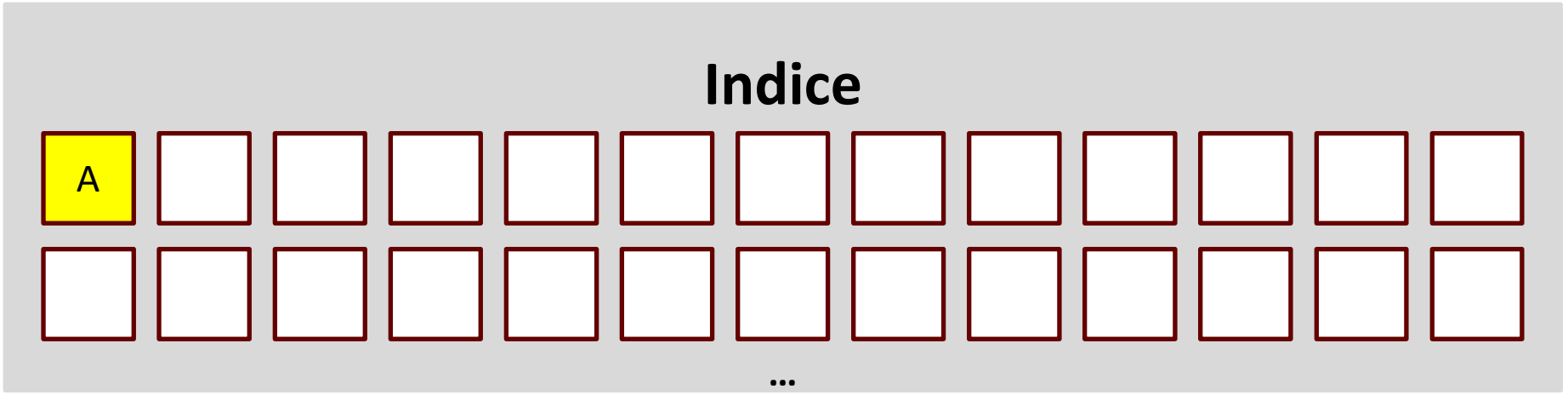
O più comunemente…

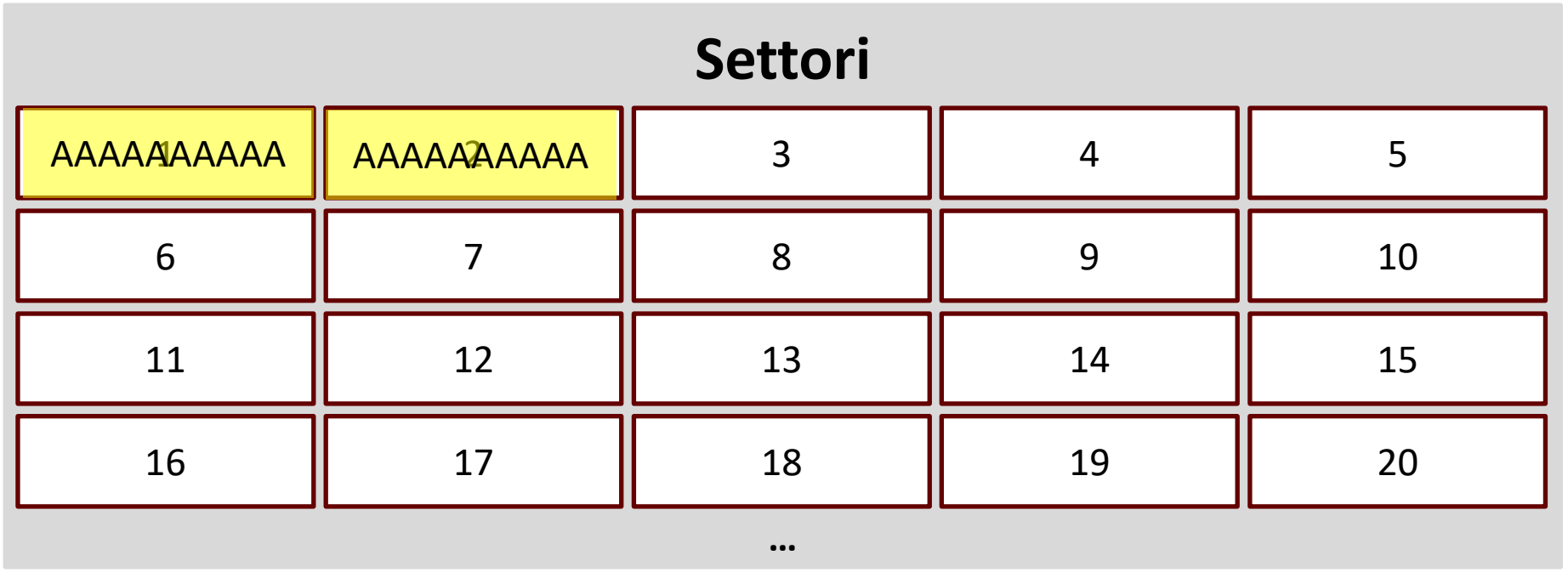


File system: allocazione dei file

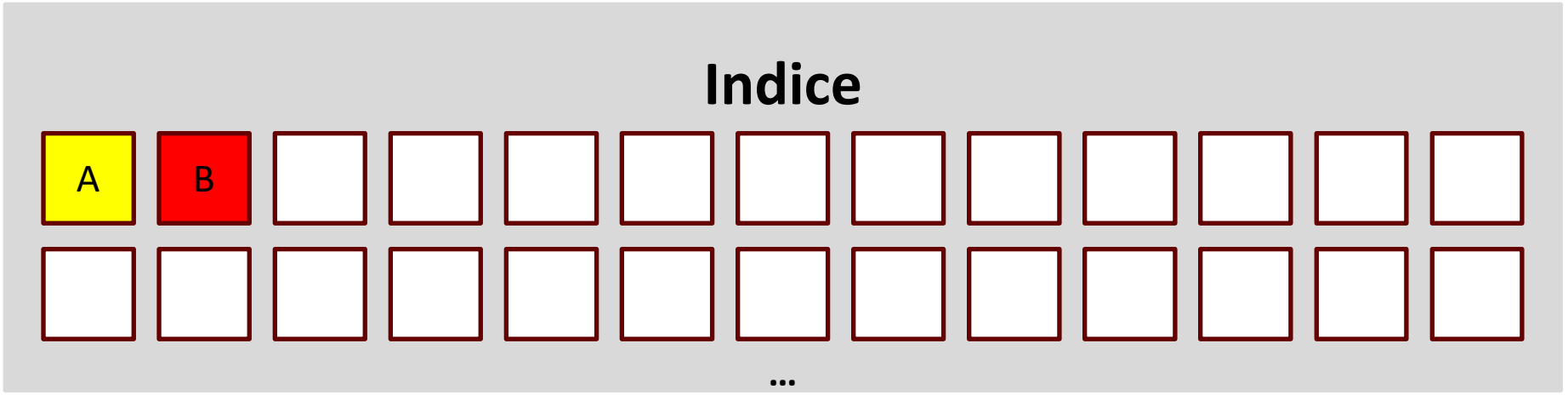


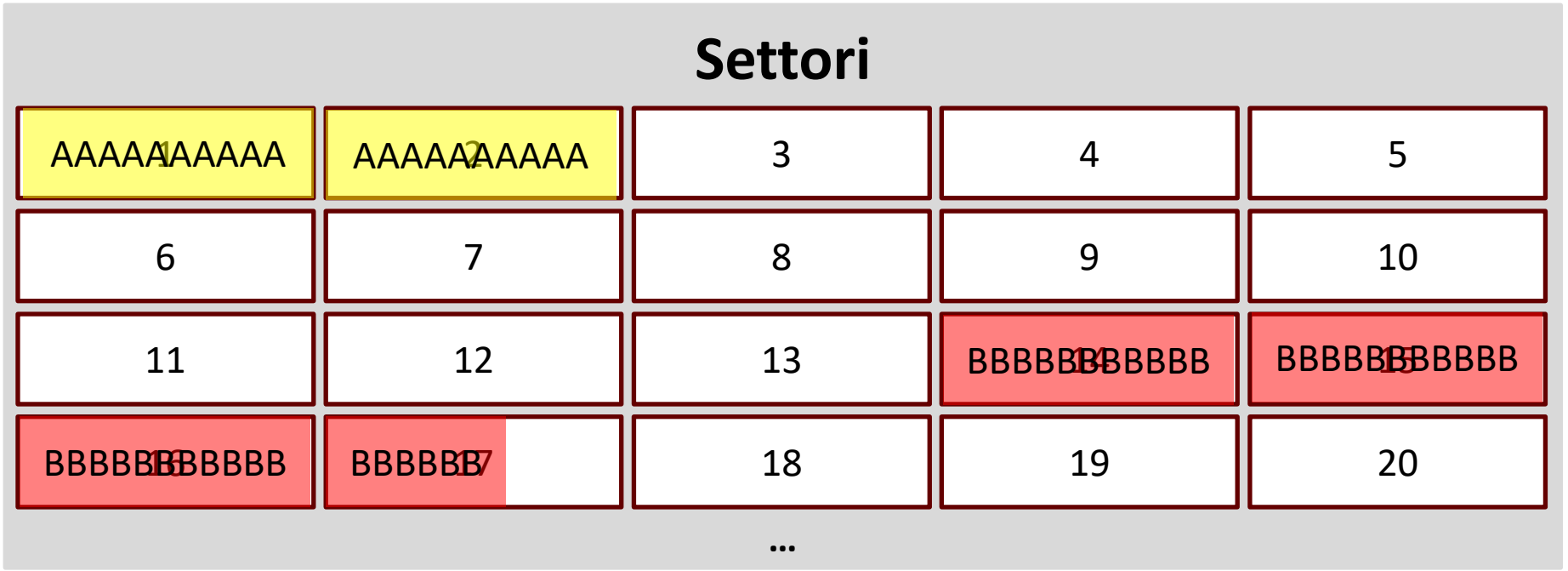
File system: allocazione dei file



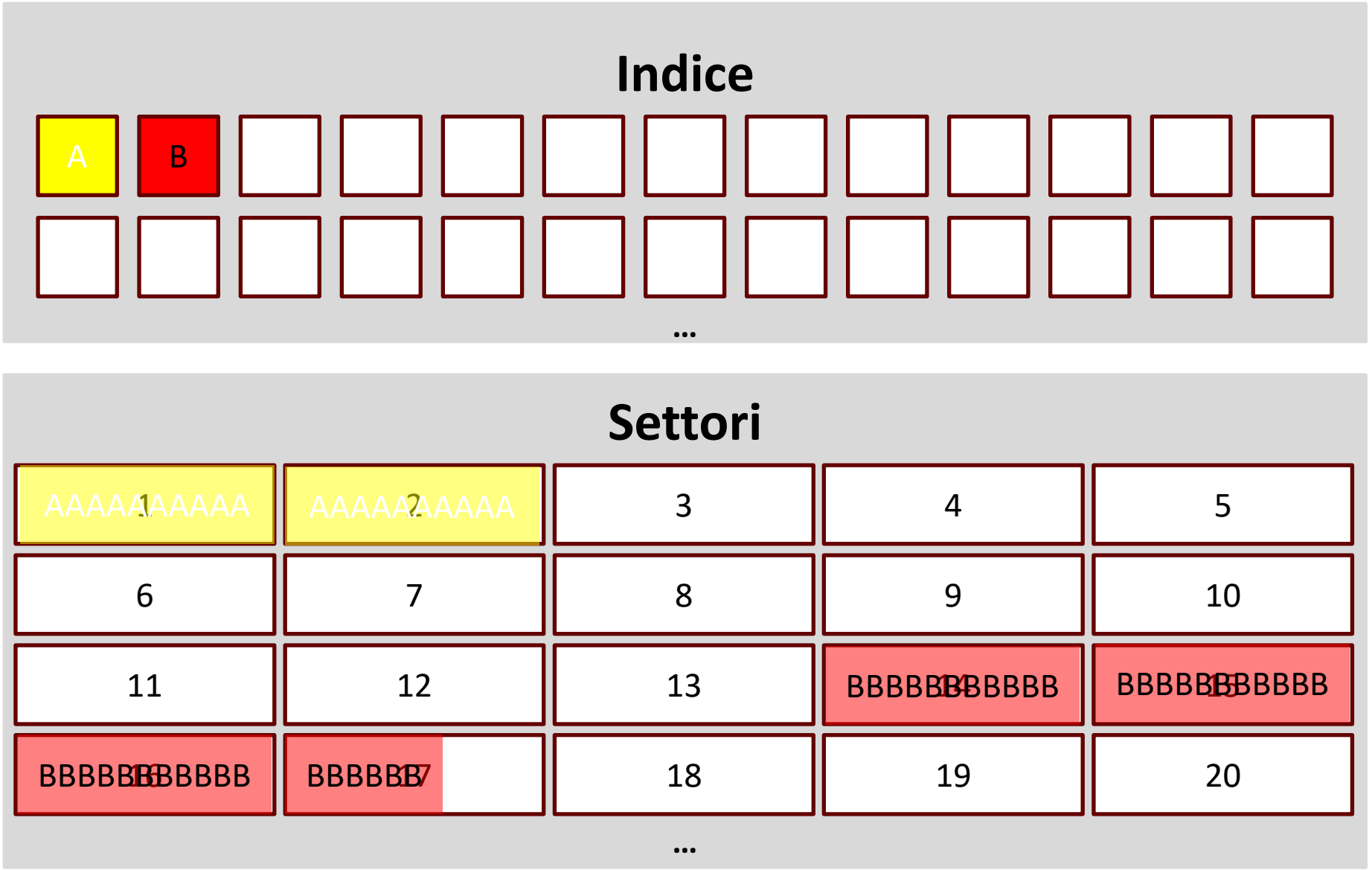


File system: allocazione dei file

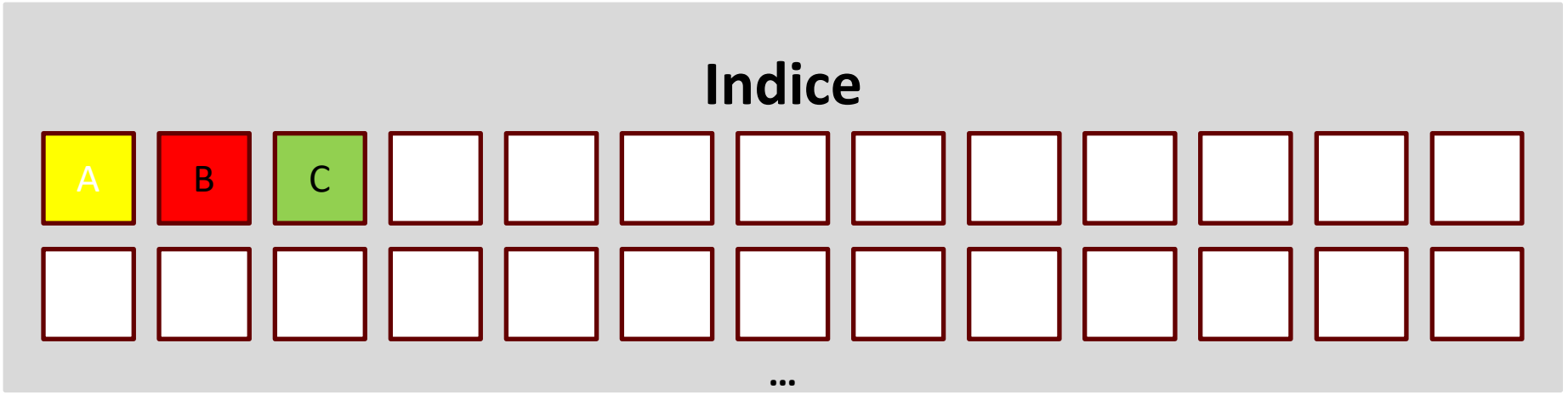


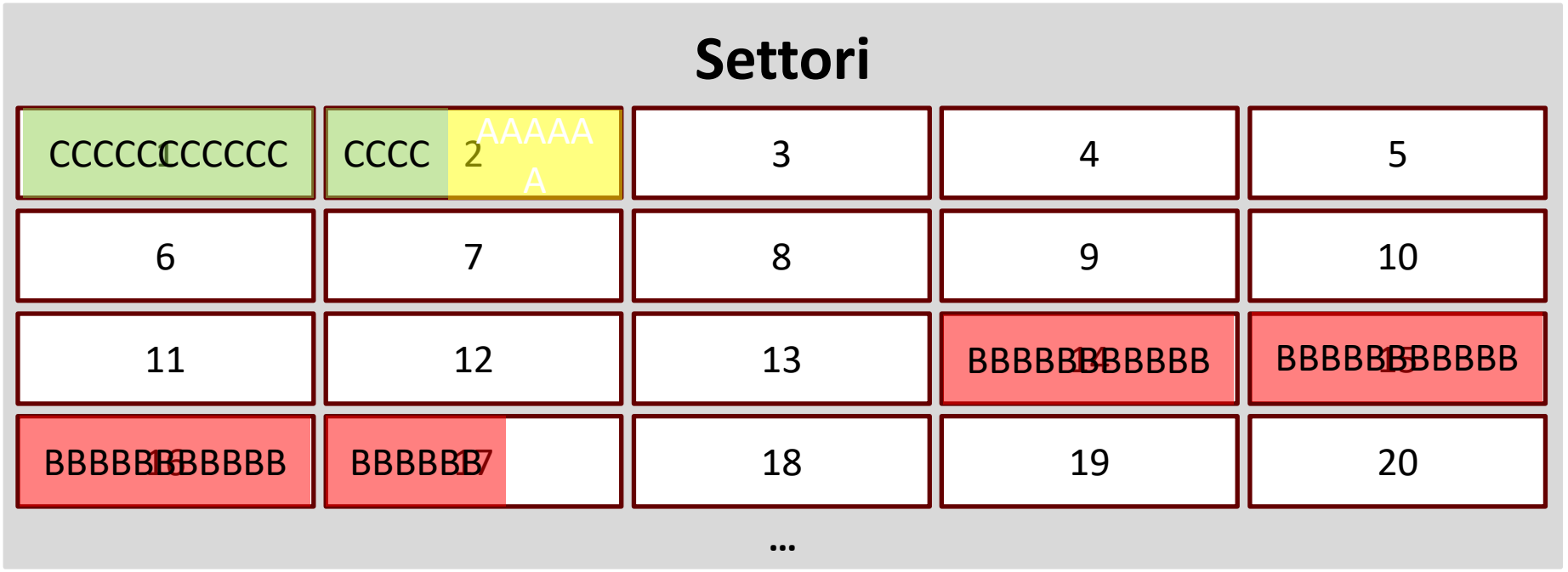


File system: allocazione dei file

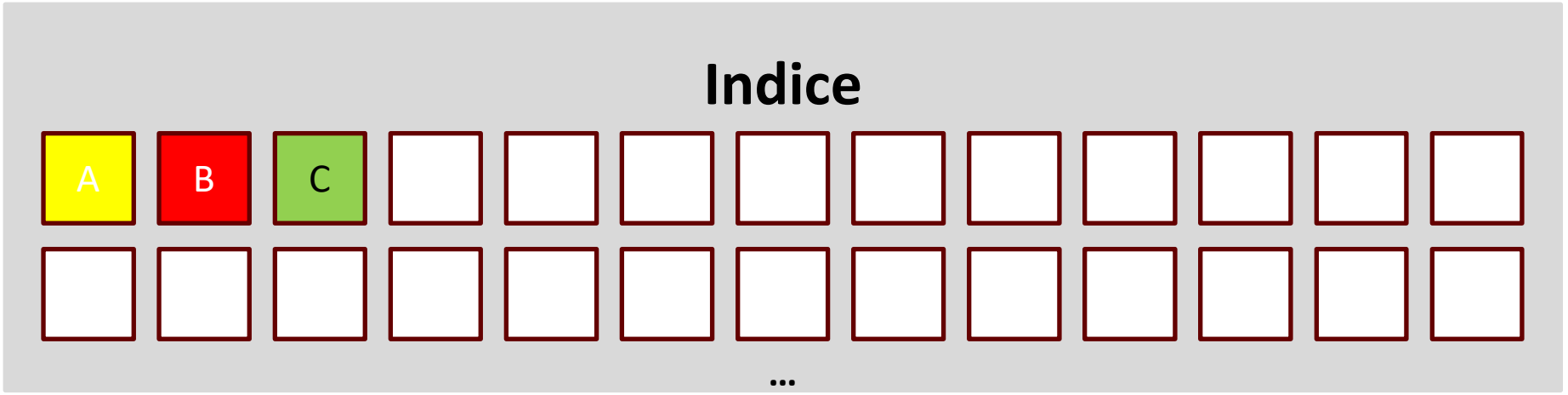


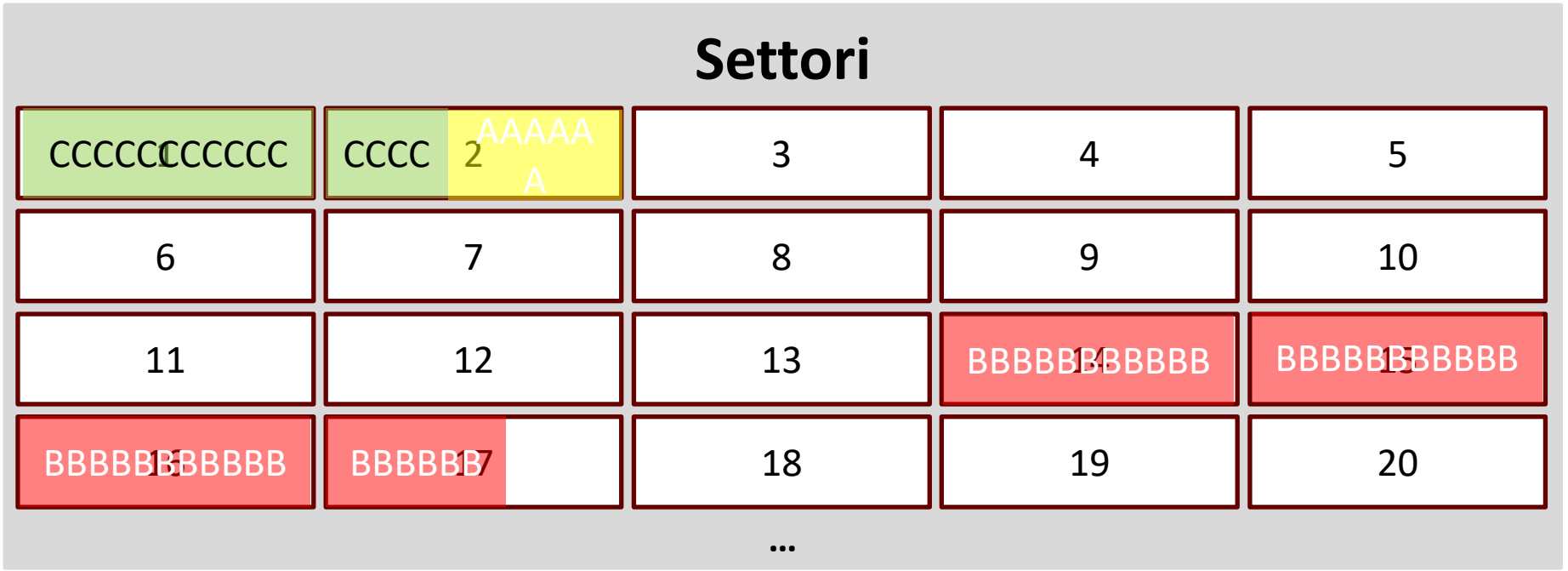
File system: allocazione dei file



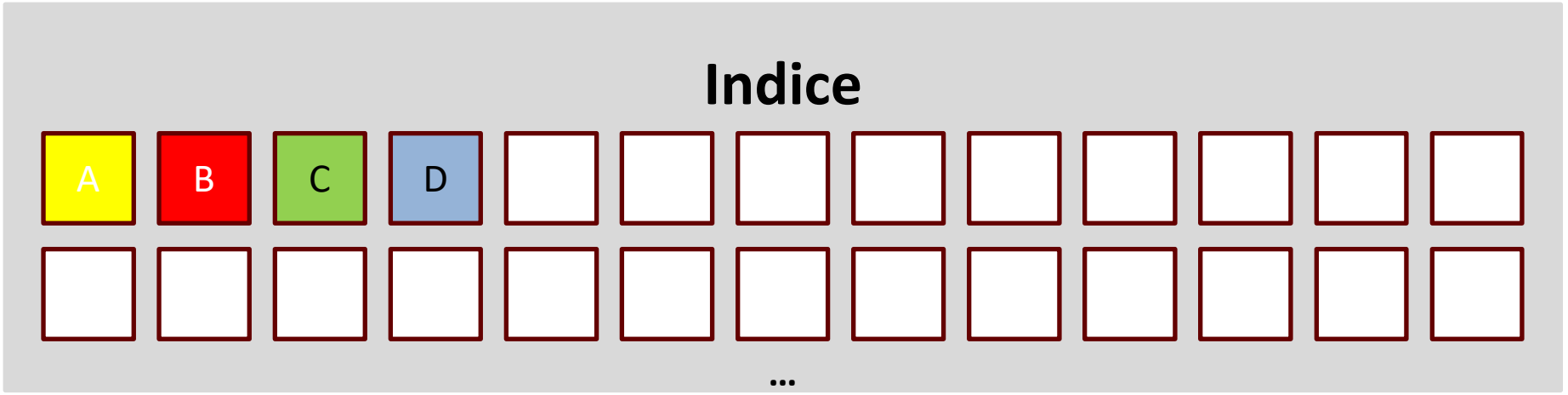


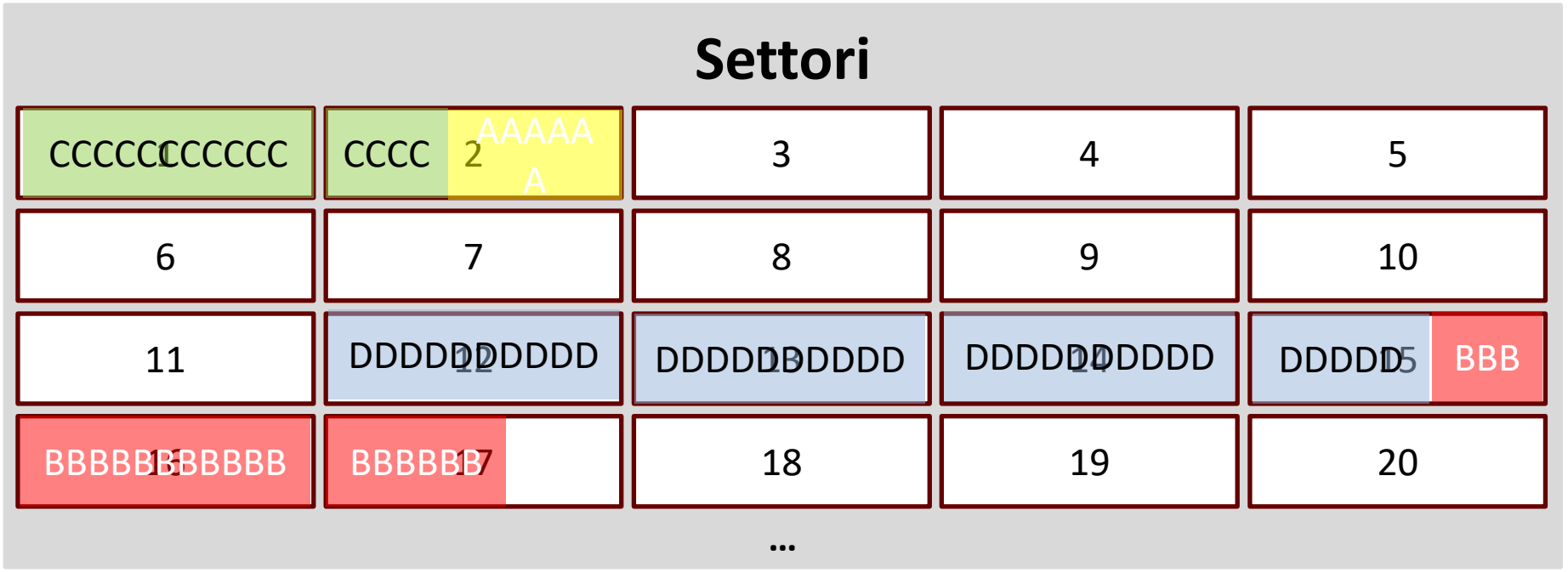
File system: allocazione dei file



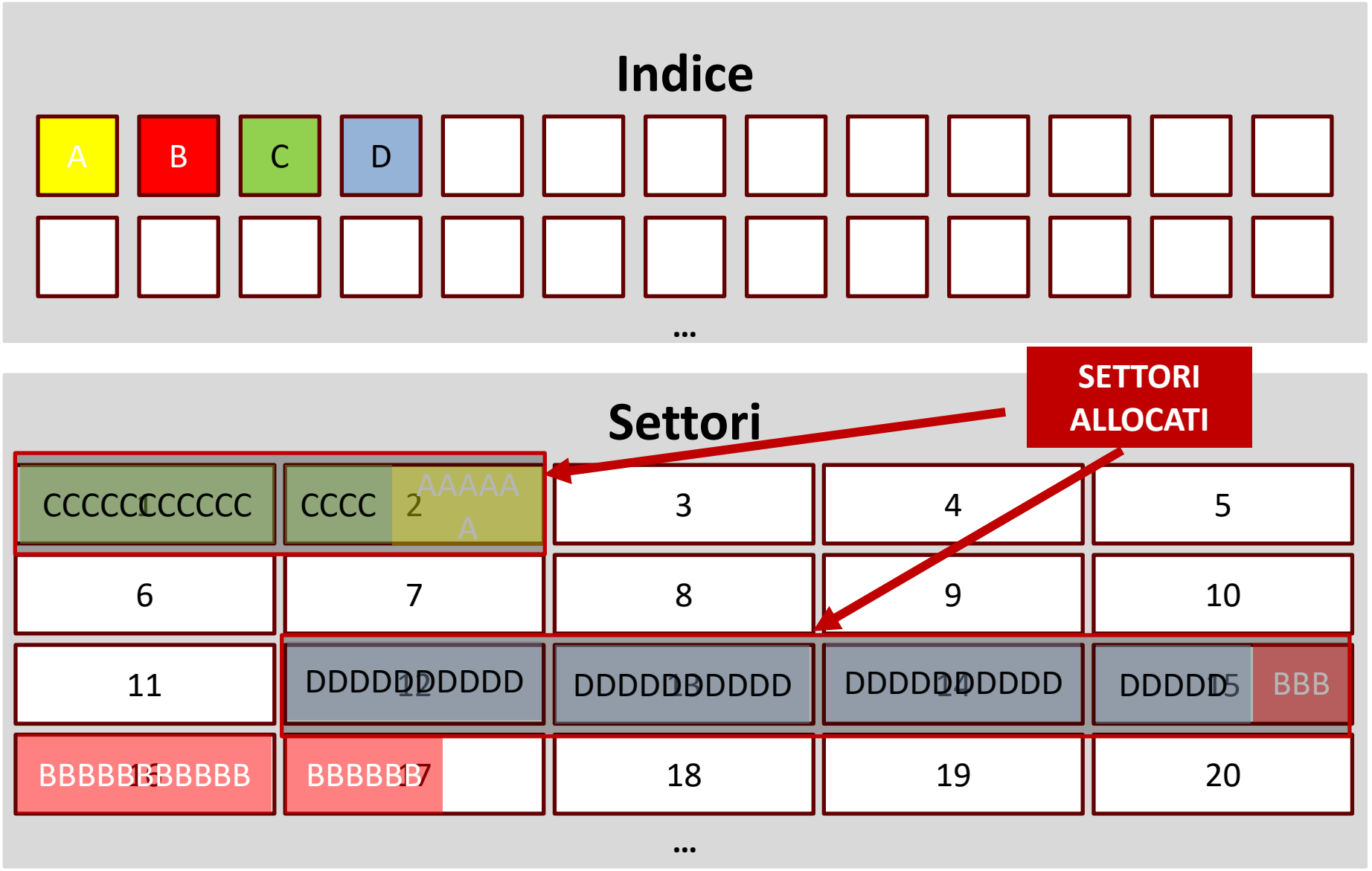


File system: allocazione dei file

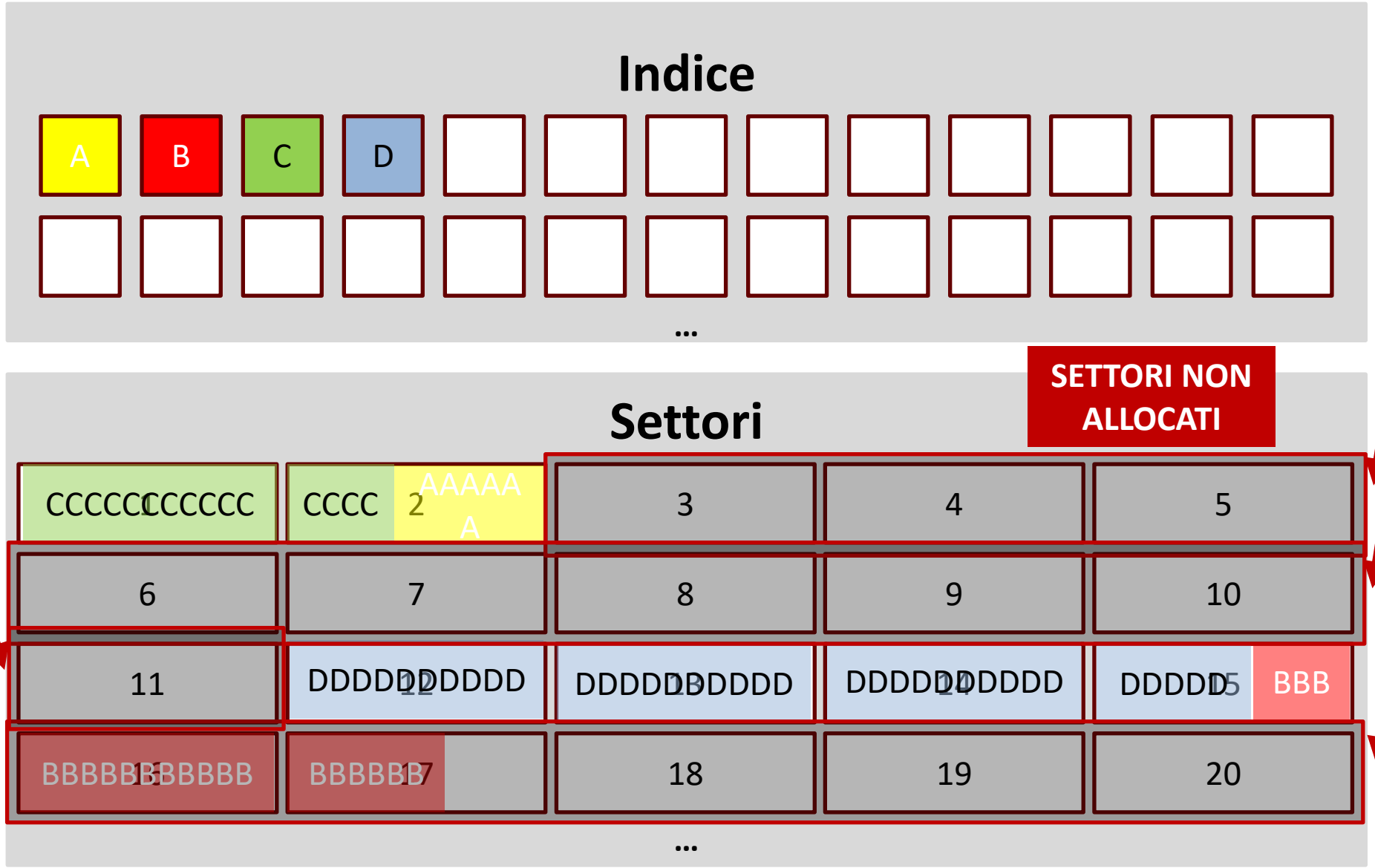




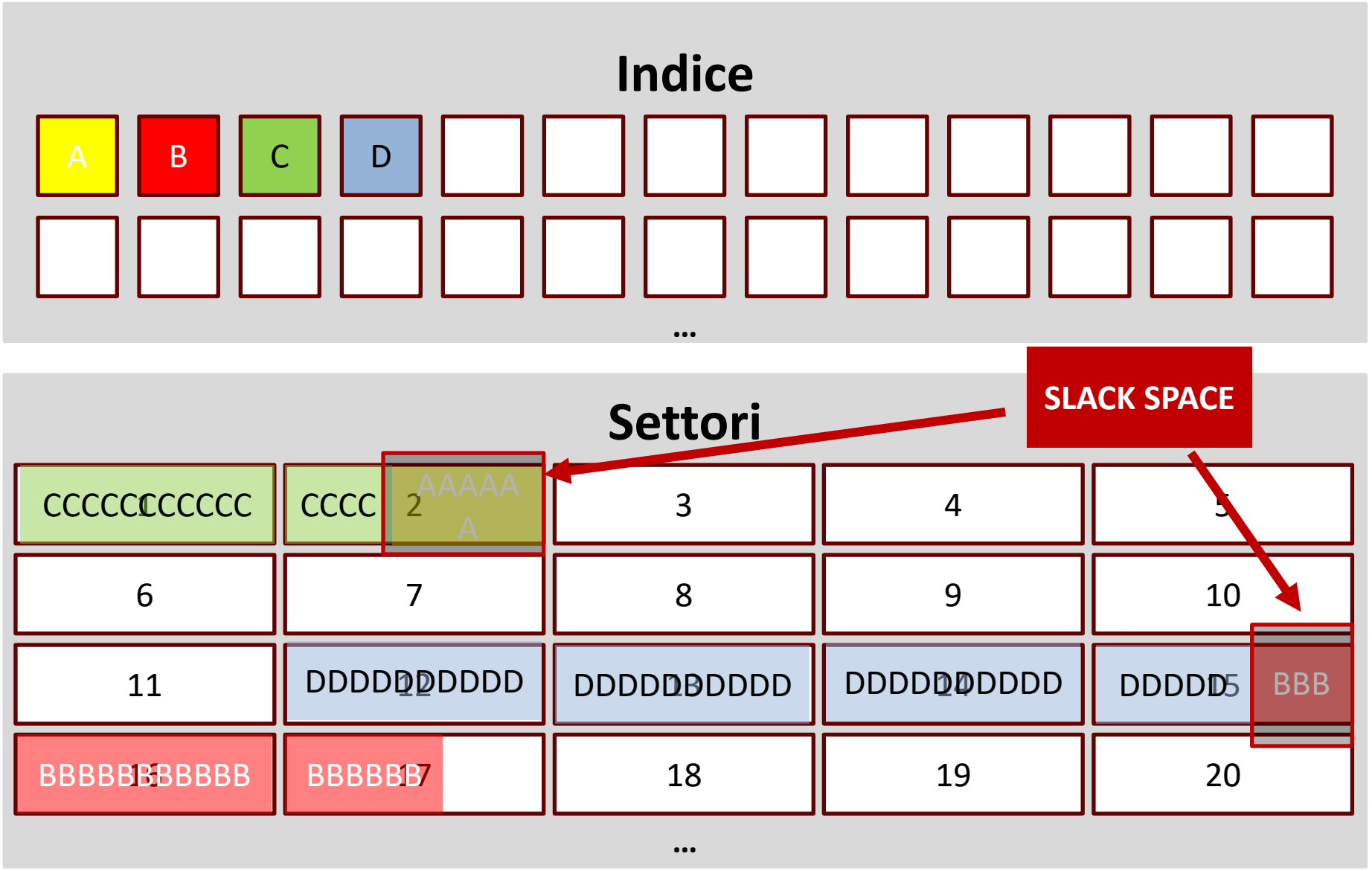
File system: allocazione dei file



File system: allocazione dei file



File system: allocazione dei file



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

~~Promessi sposi.txt~~	1
Il Cinque Maggio.txt	7

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	/

Ei fu. Siccome immobile, dato il mortal sospiro

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

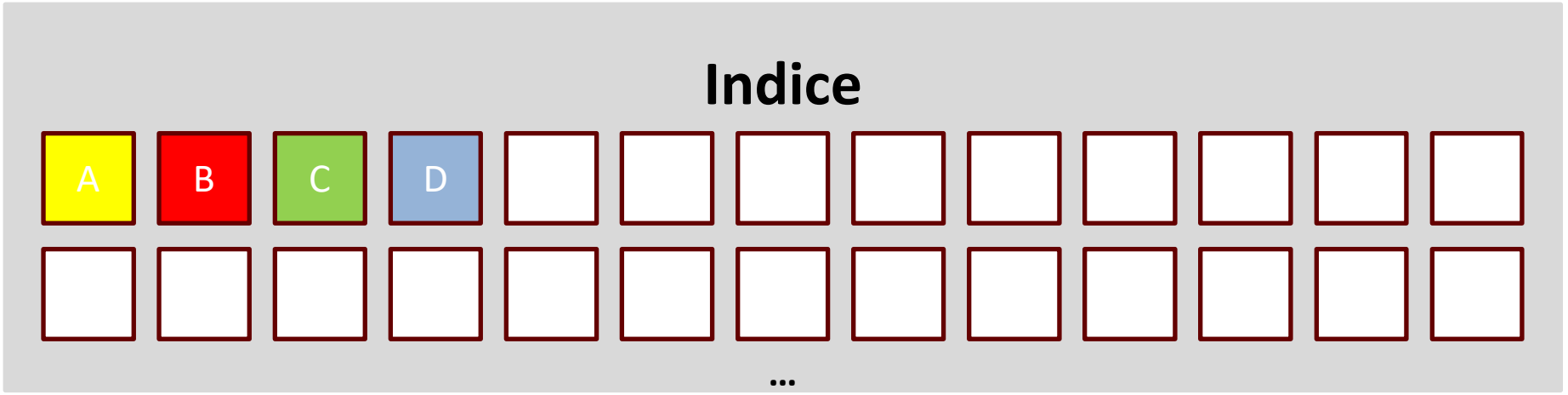
Nel mezzo del cammin di nostra vita

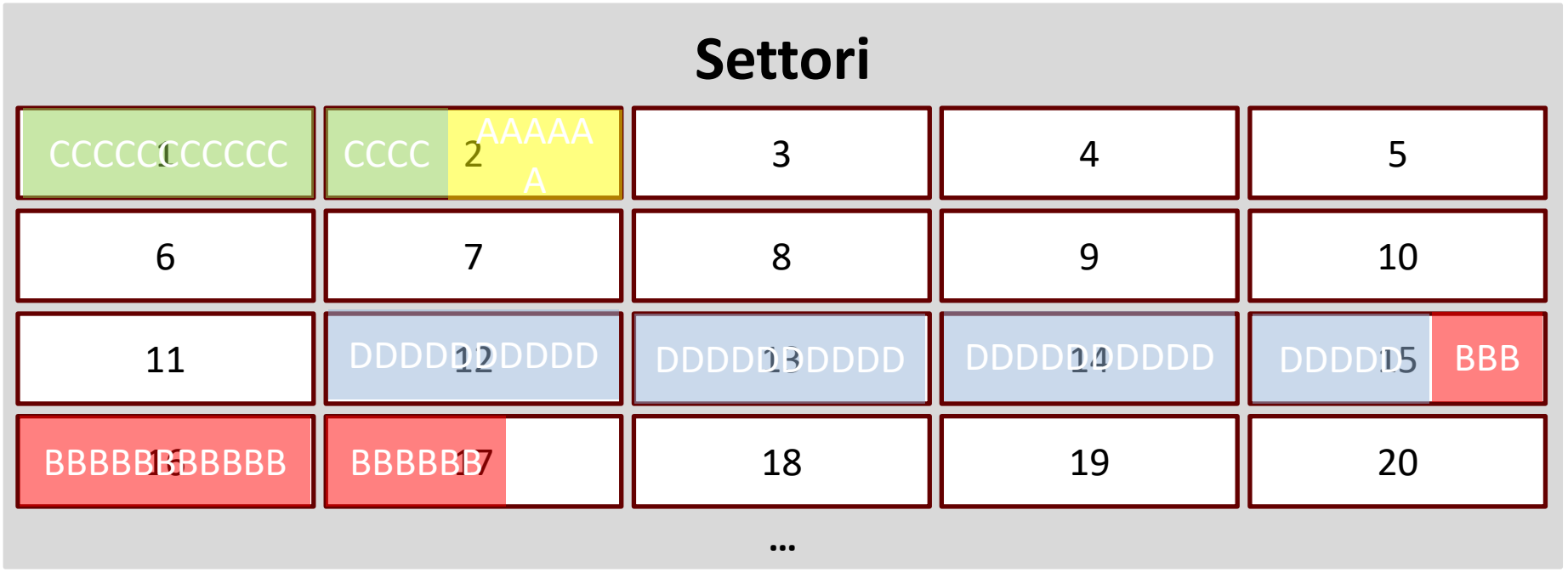
Ei fu. Siccome immobile, dato il mortal sospiro

Settori

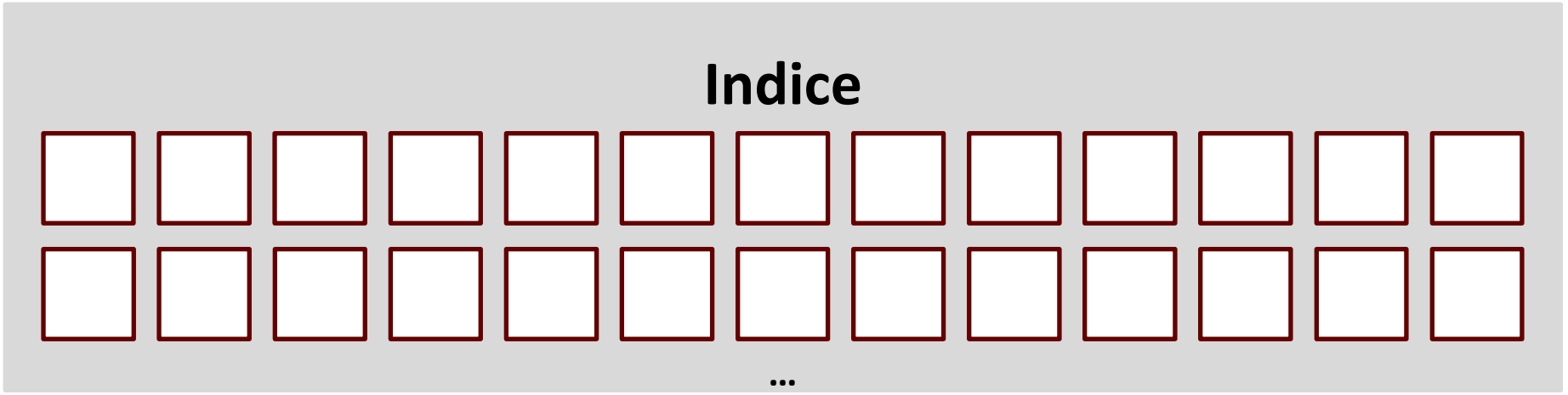
1	Nel mezz	1	2
2	o del ca	1	3
3	mmin di	1	4
4	nostra v	1	5
5	itaX a m	1	/
6	ezzogior	0	7
7	noX	0	/
8	Ei fu. S	1	9
9	iccome i	1	10
10	mmobile,	1	11
11	dato il	1	12
12	mortal	1	13
13	sospiroX	1	/
14		0	/
15		0	/
16		0	/
17		0	/

File system: formattazione

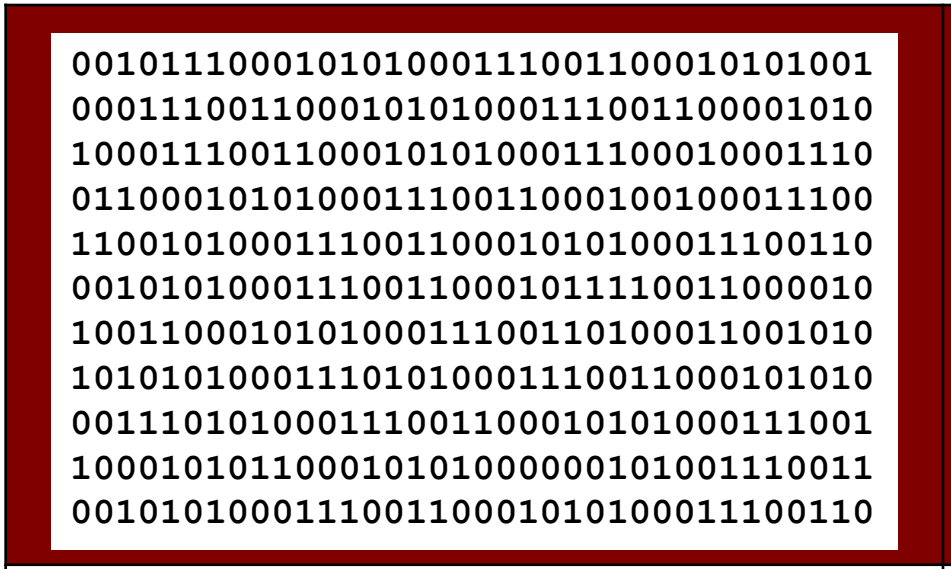




File system: formattazione dopo wiping

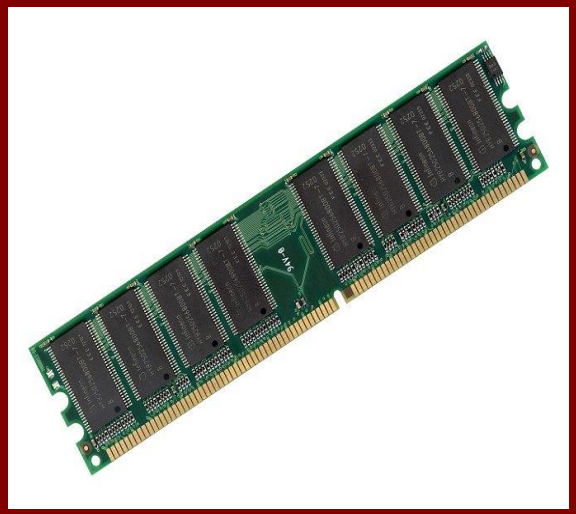


Glossario



Prova digitale	Copia di prova digitale
Informazione o dato, memorizzato o trasmesso in formato binario, che può essere utilizzato come prova	Copia di prova digitale che può essere prodotta per mantenere l'affidabilità della prova, includendo sia la prova digitale che la procedura di verifica

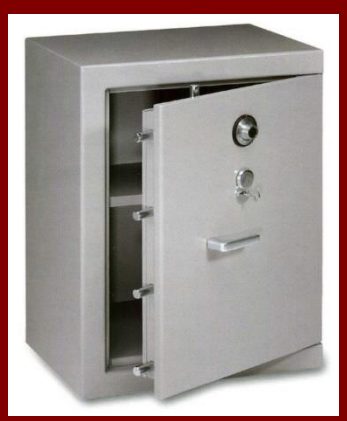
Glossario

		
Dato volatile	**Alterazione**	**Distruzione di prova**
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*	Modifica del valore di potenziali evidenze digitali che ne riduce l'eventuale valore probatorio	Modifica volontaria del valore di potenziali evidenze digitali che ne riduce l'eventuale valore probatorio

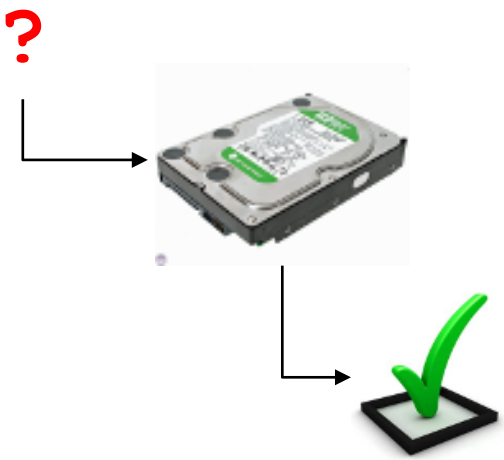
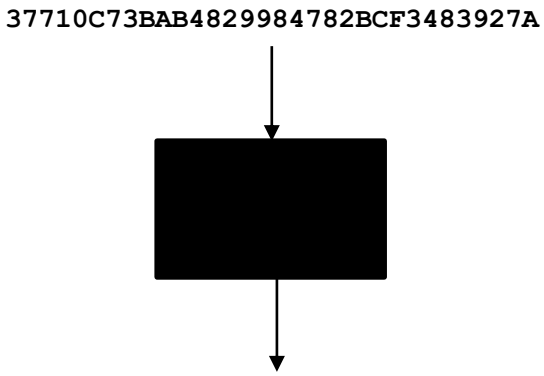
Glossario

	
Digital Evidence First Responder (DEFR)	**Digital Evidence Specialist (DES)**
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	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 ampi magnetici, polvere, umidità calore…

Glossario

37710C73BAB48299 84782BCF3483927A		
Valore di hash	**Validazione**	**Funzione di verifica**
Stringa di bit che è prodotta in output da una funziona hash [*ISO/IEC 10118-1:2000*]	Conferma, attraverso una prova, che i requisiti preposti sono stati soddisfatti [*ISO/IEC 27004:2009*]	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**: Digitai Evidence First Responder
- **DES**: Digitai Evidence Specialist
- **DVD**: Digitai VideoNersatile 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 Digitai 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 discolpare)
  - 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 dipende 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


Samsung SSD
840 EVO
250GB
P/N: MZ7TE250HMHP
Model: MZ-7TE250
S/N: S1DBNSBF372990W
RATED: DC+5.0V 0.86A
WWN: 50025388A0309A2E
PSID:CHZYYGXNB3UL1KJQ5MKA6JU02GKTS7MJ


NOKIA
Nokia Corporation
Model: 100
Type: RH-130
CODE: 059H2D2
IMEI: 354585/05/396794/1
0434
MADE IN INDIA


Transcend 1 4GB
Transcend 2 4GB
Transcend 3 4GB
Transcend 4 4GB
Transcend 5 4GB
Panasonic 6 4GB
Panasonic 7 4GB
Panasonic 8 4GB
Panasonic 9 4GB
4GB 10 SDHC Memory Card TOSHIBA
4GB 11 SDHC Memory Card TOSHIBA
Kingston 12 SD4/4GB
Panasonic 13 4GB
Kingston 14 SD4/4GB
4GB 15 SDHC Memory Card TOSHIBA
Panasonic 16 4GB
Panasonic 17 4GB
Panasonic 18 4GB
4GB 19 SDHC Memory Card TOSHIBA
Panasonic 20 4GB
4GB 21 SDHC Memory Card TOSHIBA
4GB 22 SDHC Memory Card TOSHIBA
23 1201W12292N MADE IN JAPAN
4GB 24 SDHC Memory Card TOSHIBA
Panasonic 25 4GB
26 1201W12292N MADE IN JAPAN
4GB 27 SDHC Memory Card TOSHIBA
Kingston 28 4GB SD4/4GB
4GB 29 SDHC Memory Card TOSHIBA
4GB 30 SDHC Memory Card TOSHIBA
Kingston 31 SD4/4GB
4GB 32 SDHC Memory Card TOSHIBA
Kingston 33 SDHC 4GB SD4/4GB
4GB 34 SDHC Memory Card TOSHIBA
4GB 35 SDHC Memory Card TOSHIBA
Panasonic 36 4GB
Kingston 37 4GB SD4/4GB
4GB 38 SDHC Memory Card TOSHIBA
39 4GB marantz PROFESSIONAL
19.06.2006 Kingston SDHC 4GB 40
41
Panasonic 42 4GB
8GB 43 SDHC Memory Card TOSHIBA
Kingston 44 4GB SD4/4GB
4GB 45 SDHC Memory Card TOSHIBA
4GB 46 SDHC Memory Card TOSHIBA
Transcend 47 4GB
Transcend 48 4GB
Kingston 49 4GB SD4/4GB
Kingston 50 SD4/4GB
Kingston 51 4GB SD4/4GB
Kingston 52 SDHC 4GB SD4/4GB
cruzer 53

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

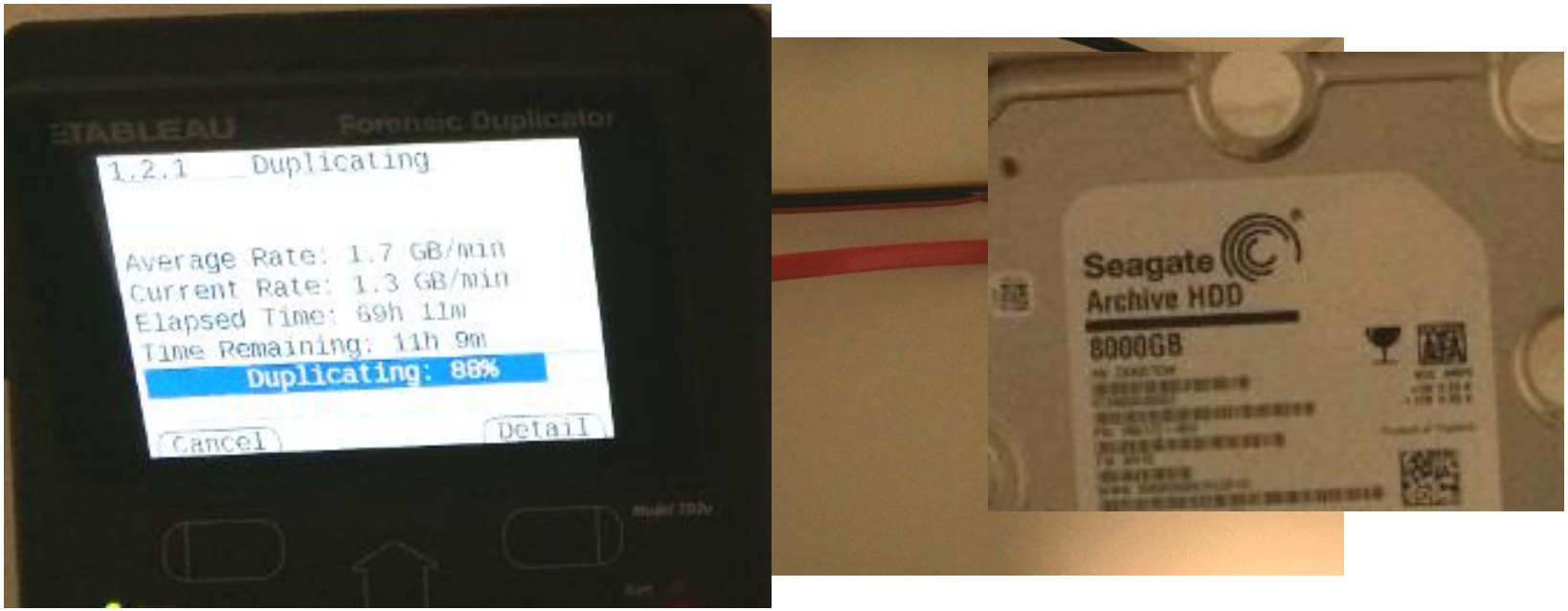
Competenze degli operatori
Raccolta

- 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



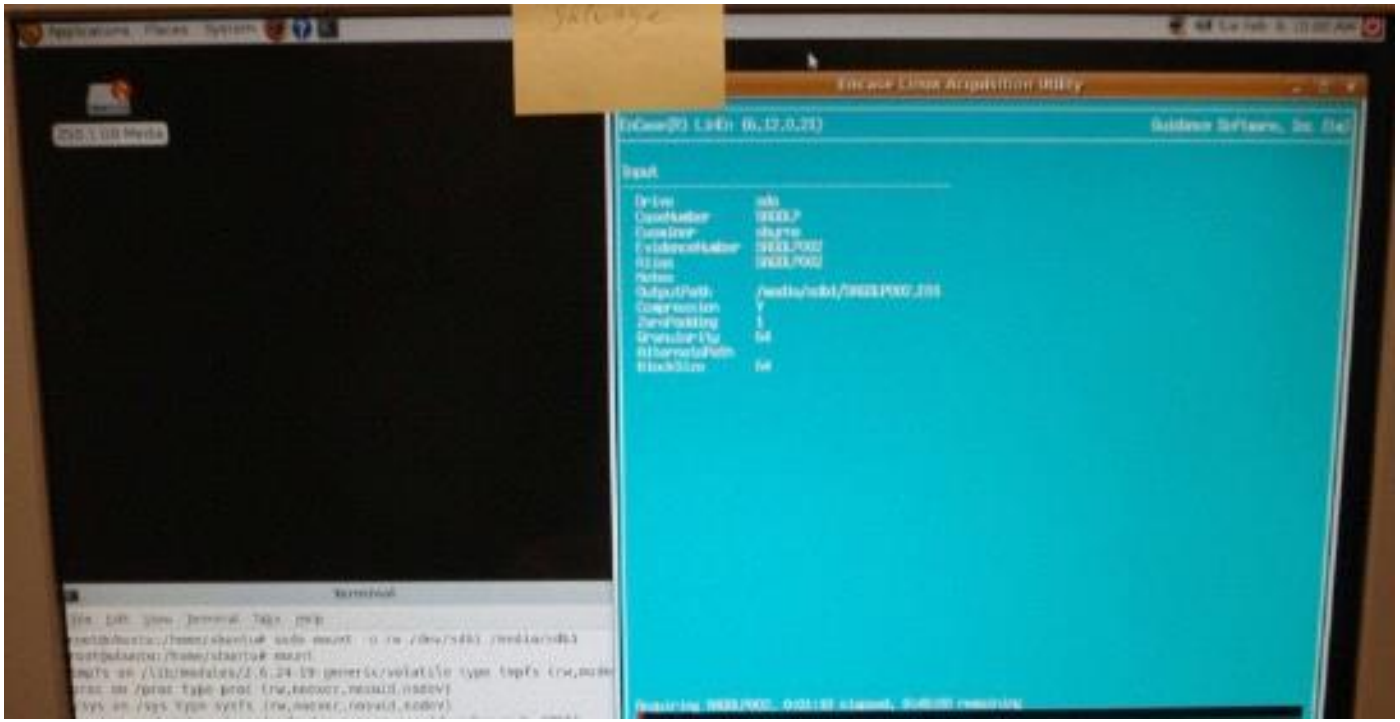
Processo di gestione della prova digitale

Fasi – Acquisizione

Processo di gestione della prova digitale

Fasi – Acquisizione

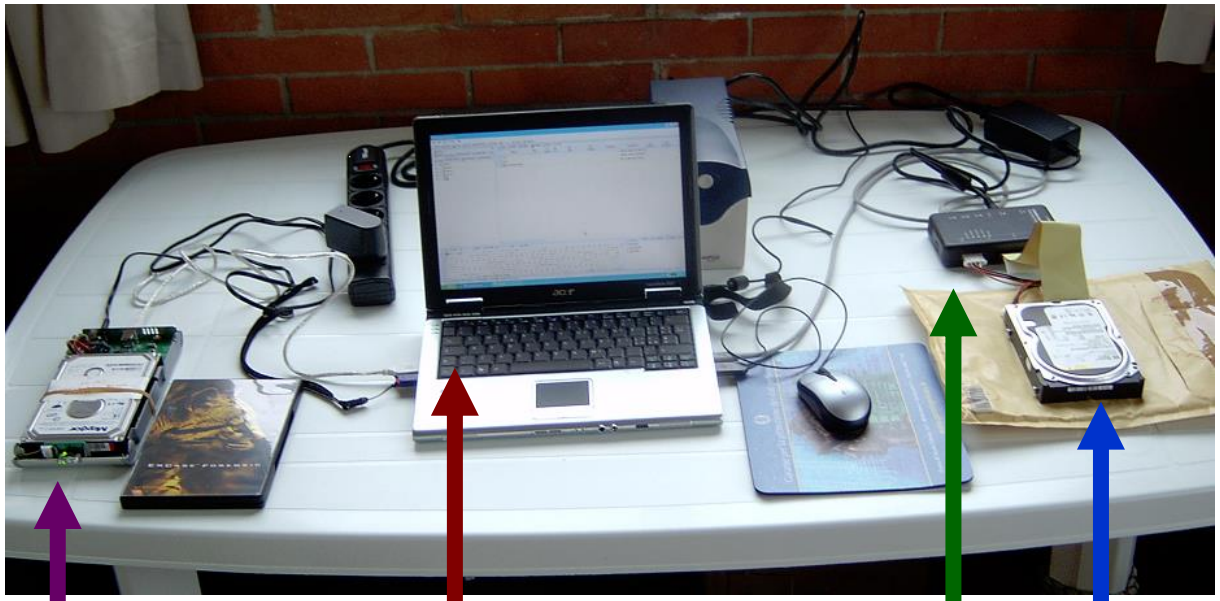
Acquisizione post-mortem: live CD



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

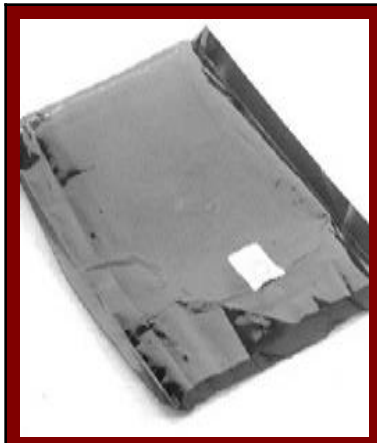
Processo di gestione della prova digitale

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**

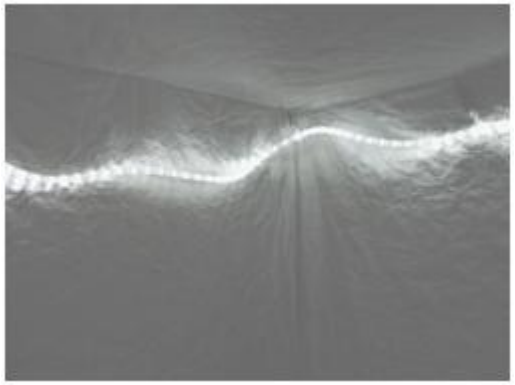
http://www.paraben.com/stronghold-bag.html

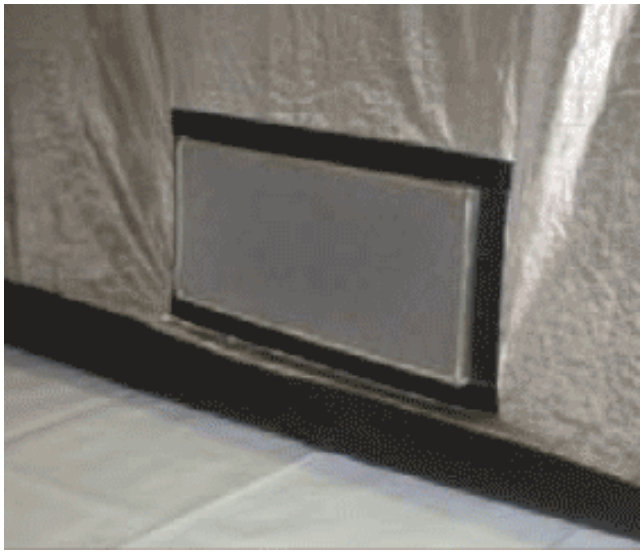
http://www.paraben.com/tabletop-stronghold.html

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

Dettagli reperto informatico e catena di custodia			
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:	MD5:		
	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	Firma	
	Nome	Firma	
	Nome	Firma	
	Nome	Firma	
	Nome	Firma	

Processo di gestione della prova digitale

Catena di custodia

Dettagli reperto informatico e catena di custodia			
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:	MD5:		
	SHA1:		
Note aggiuntive:			

Processo di gestione della prova digitale

Catena di custodia

Reperto informatico originario presentato da			
Nome e cognome:			
Data e ora:			
Luogo:			
Note aggiuntive:			
Catena di custodia			
Data e ora	Incaricato a		Descrizione
	Nome	Nome	
	Nome	Nome	
	Nome	Nome	
	Nome	Nome	
	Nome	Nome	

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

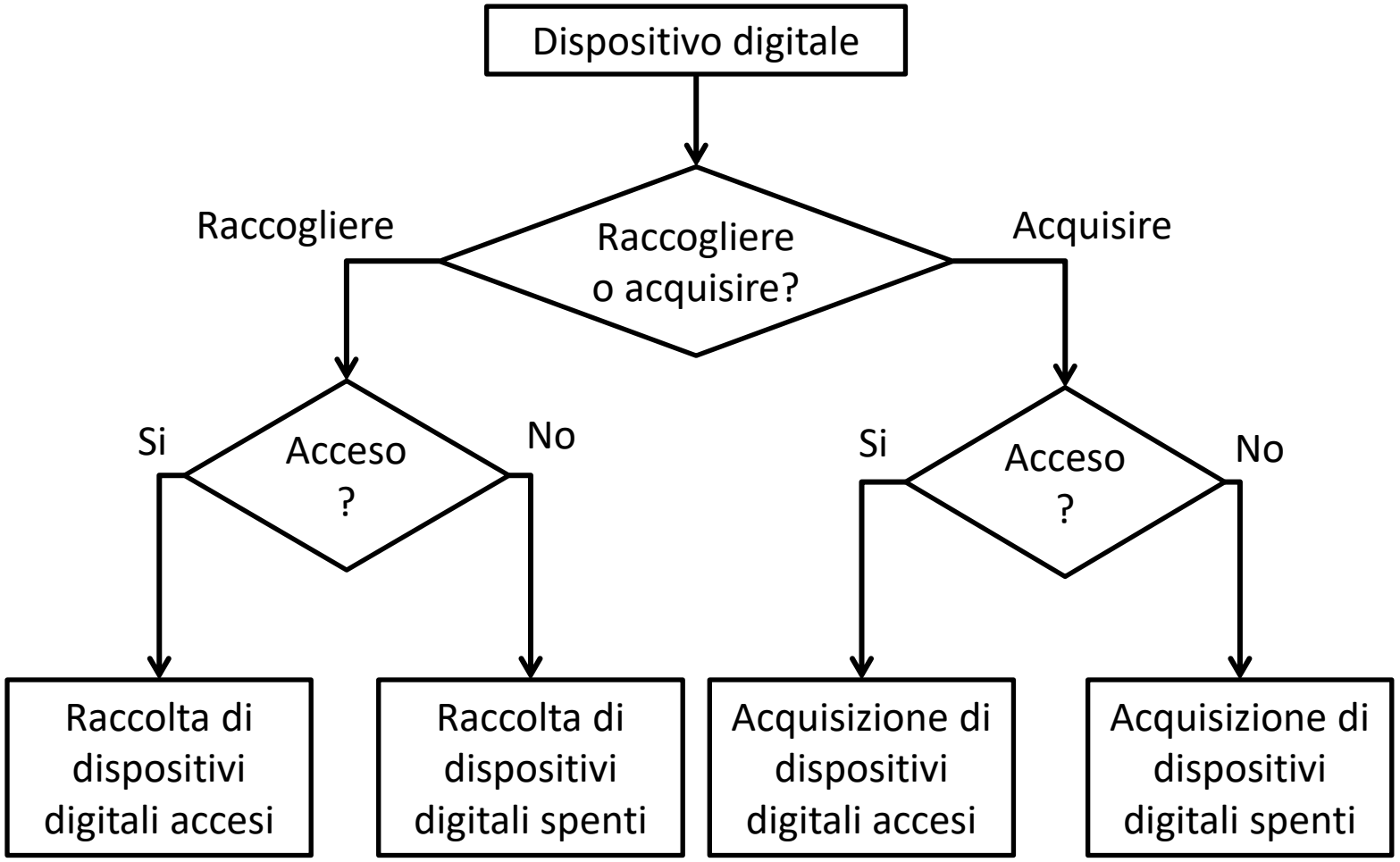
- Tipo di incidente
- Data e ora
- Definire piano di investigazione
- Considerare dove e come l'evidenza digitale è memorizzata/trasportata
- Individuare eventuali tool specifici per le attività di acquisizione
- Definire strumenti necessari
- Disattivare comunicazioni via cavo e senza fili
- Assegnare compiti ai vari soggetti
  - Non accettare ausilio tecnico da non autorizzati
  - Utilizzare materiali opportuni per l'imballaggio

Precauzioni sulla scena del crimine

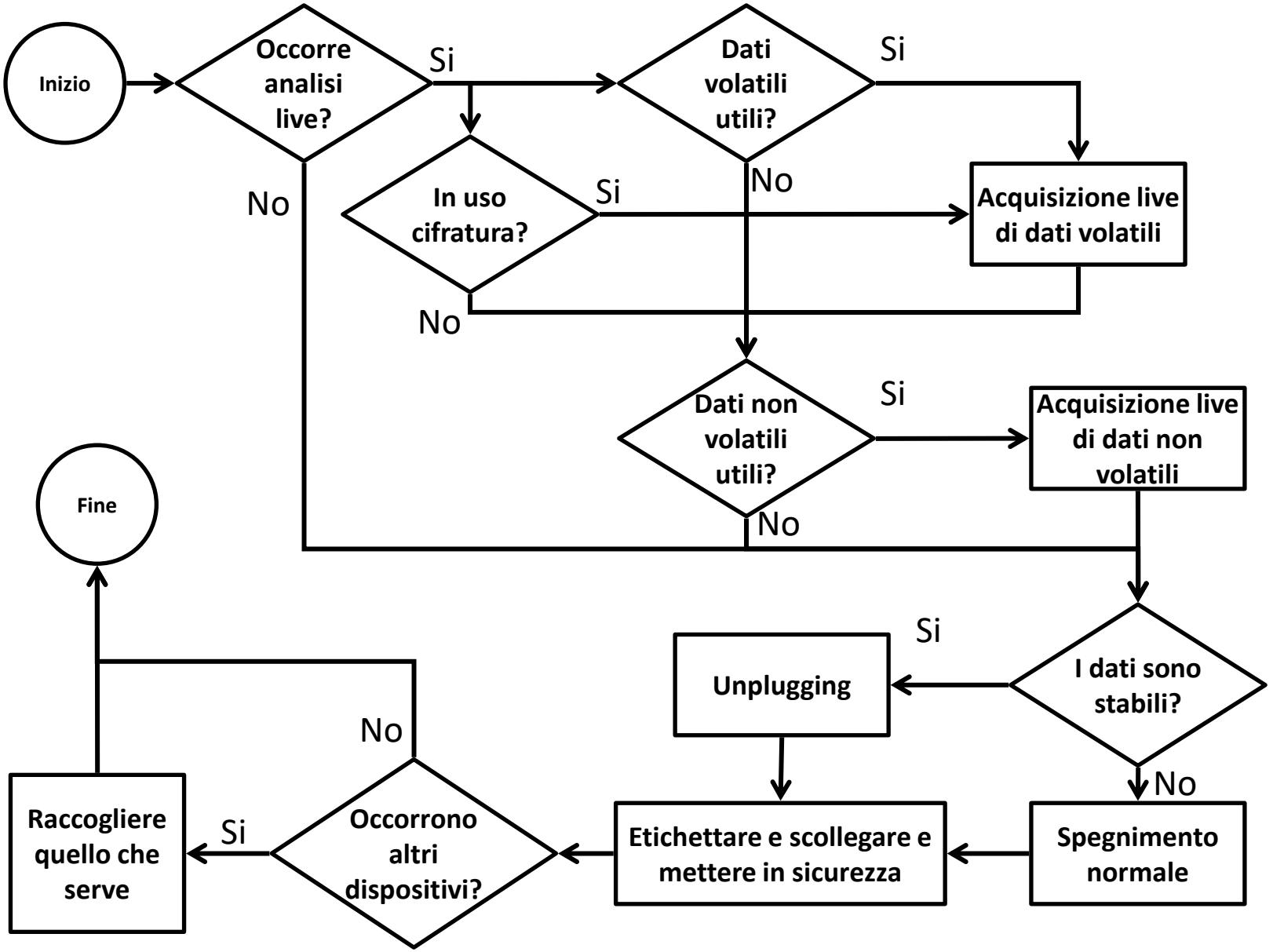
Valutazione dei rischi

- 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

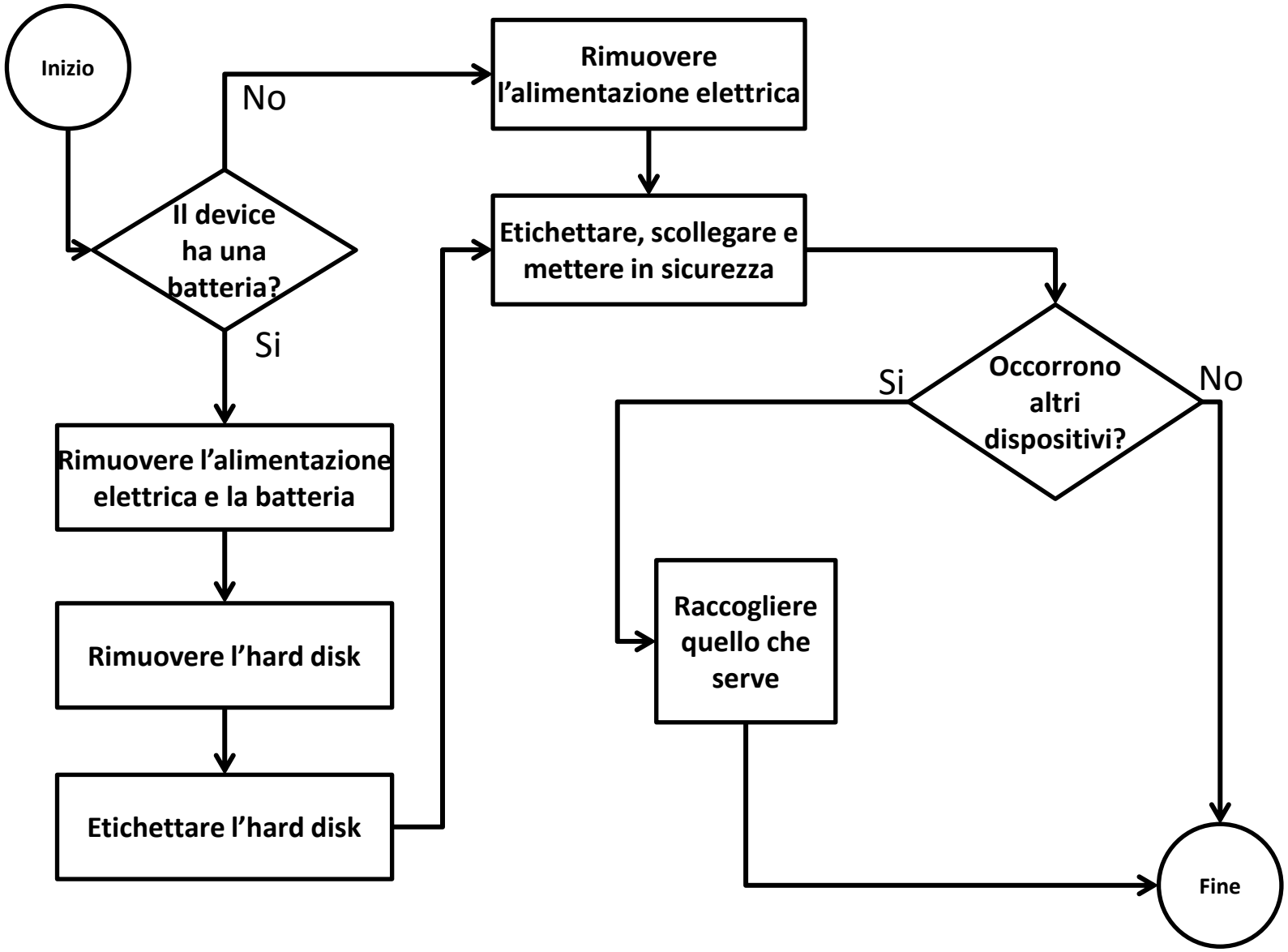


Linee guida per acquisizione di dispositivi di memorizzazione digitali

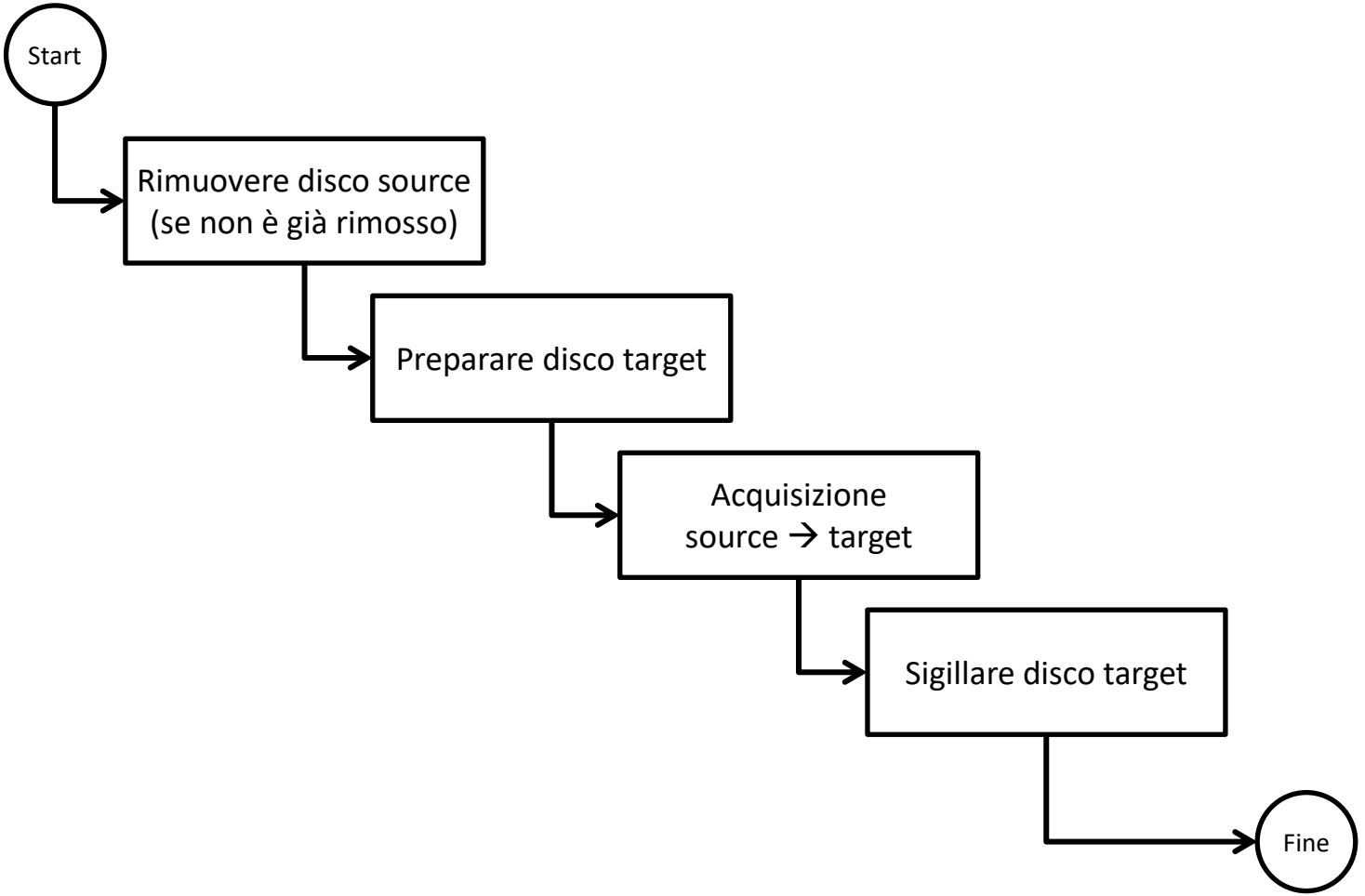
Stato: spento

- 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?»)

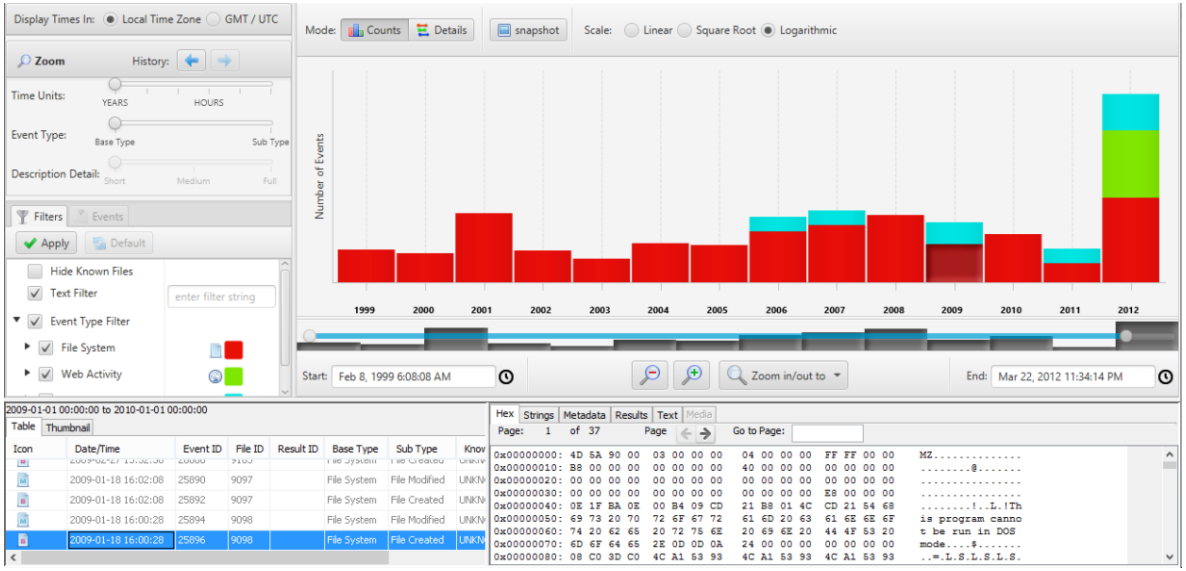
Analisi

- 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}/#
                                 0 m... 0 0          0        0        HKLM-SYSTEM/ControlSet001/Enum/STORAGE/RemovableMedia/
7&1d6490f9&0&RM
                           1580544 .a.. r/rrwxrwxrwx 0        0          2063-128-3 C:/WINDOWS/system32/sfcfiles.dll
                            984576 .a.. r/rrwxrwxrwx 0        0          2249-128-3 C:/WINDOWS/system32/syssetup.dll
                            204597 mac. r/rrwxrwxrwx 0        0          3596-128-3 C:/WINDOWS/setupapi.log
                             12614 macb r/rrwxrwxrwx 0        0          8176-128-4 C:/WINDOWS/Prefetch/RUNDLL32.EXE-35D52528
.pf
```

Fonte *sans.org*



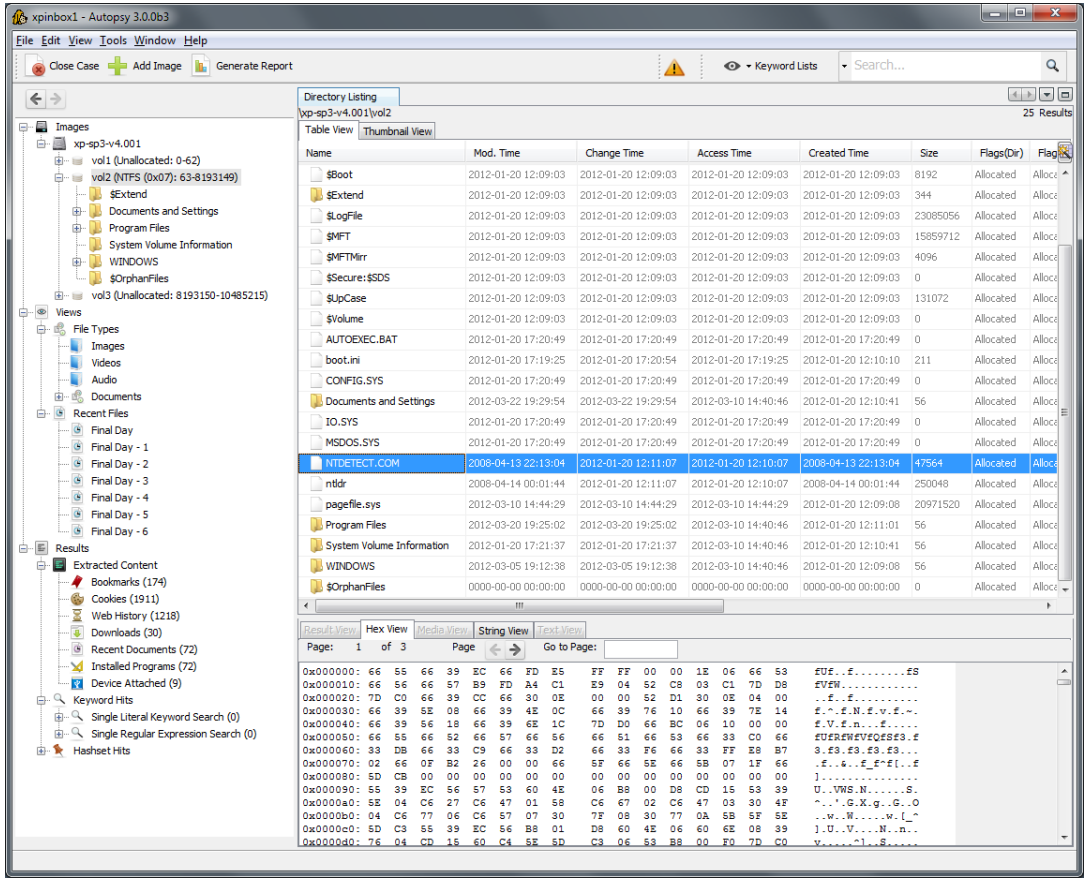
Fonte *sleuthkit.org*

Analisi: *supertimeline*

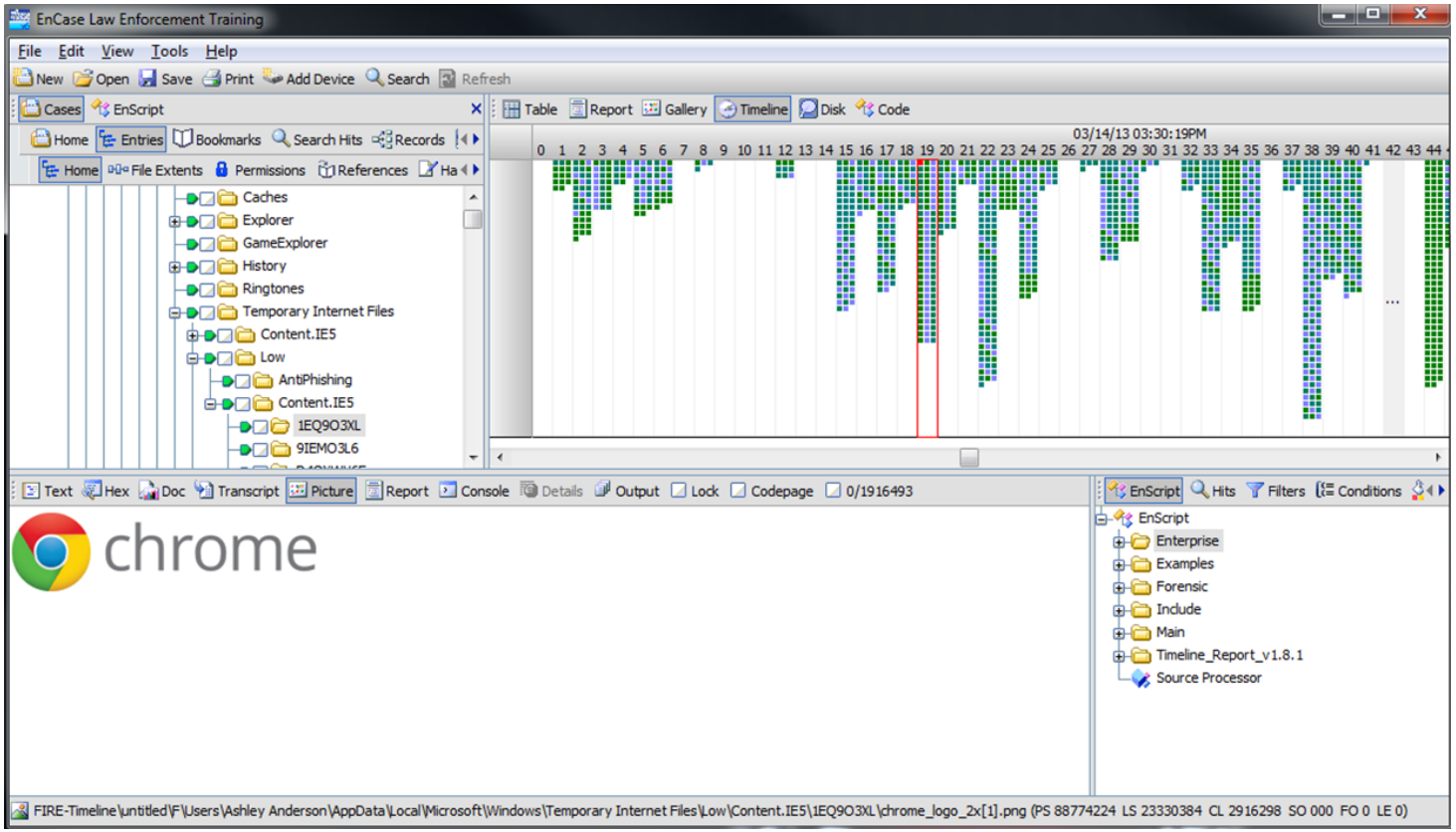
A	B	C	D	E	F	G	J	
date	time	timezon	MAC	source	sourcetype	type	short	desc
6/18/2009	22:30:26	EST5EDT	MACB	LOG	WMIprov Log file	Time Written	C:/Windows/system32/DRIVERS/msiscsi.sys[MofResource](Thu Jun 18 22:30:26 2009.29992	Entry in log file: C:/Windows/
6/18/2009	22:30:26	EST5EDT	MACB	LOG	WMIprov Log 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 - [D
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.p
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 Firef
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*

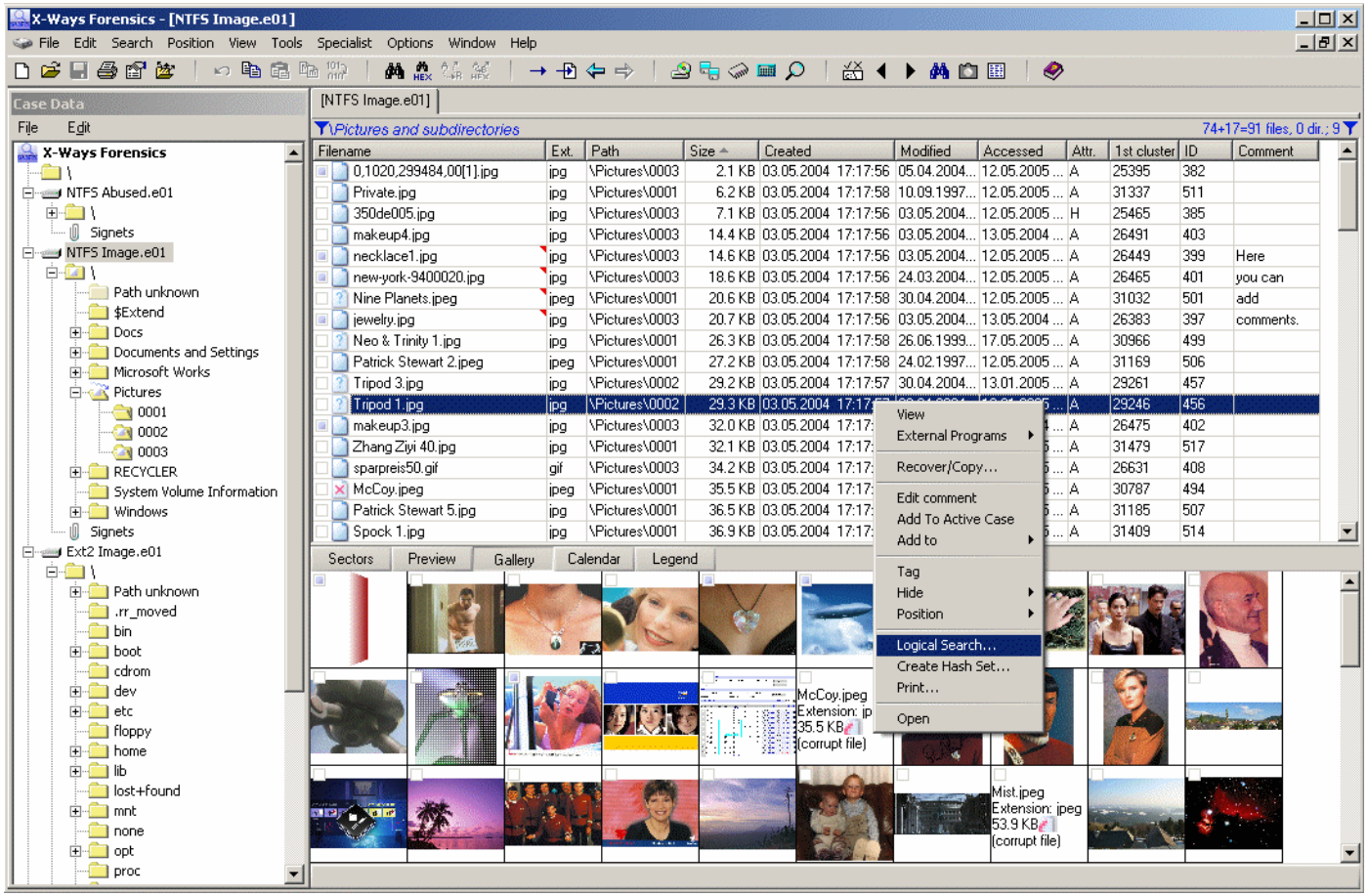
Analisi: Autopsy



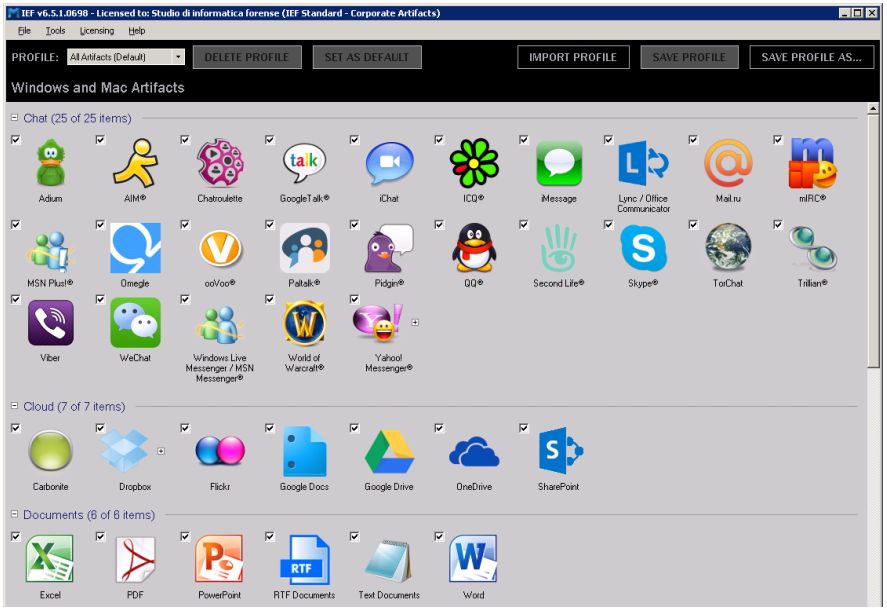
Analisi: EnCase

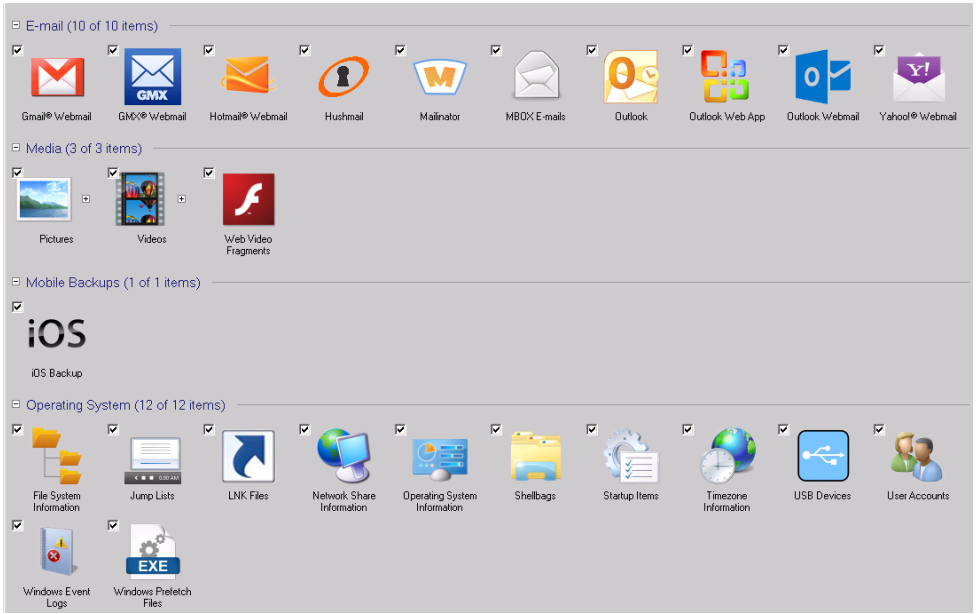


Analisi: Xways Forensics



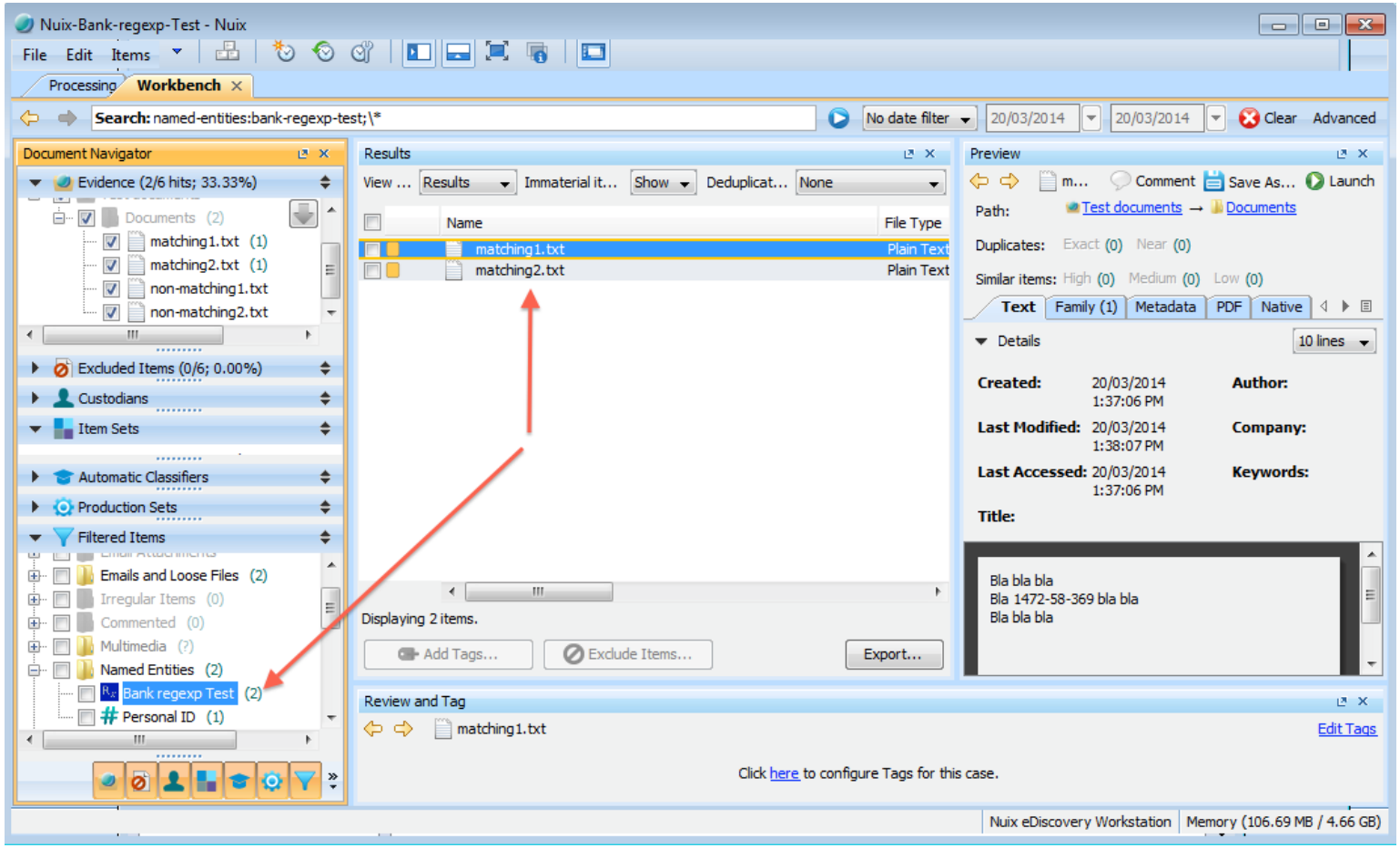
Analisi: Internet Evidence Analyzer



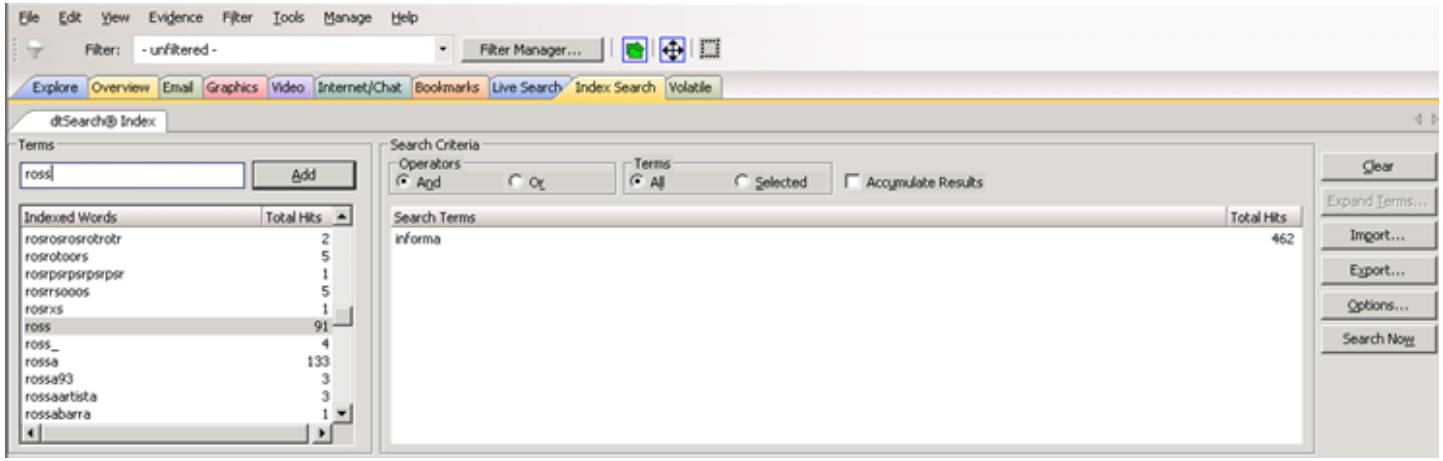


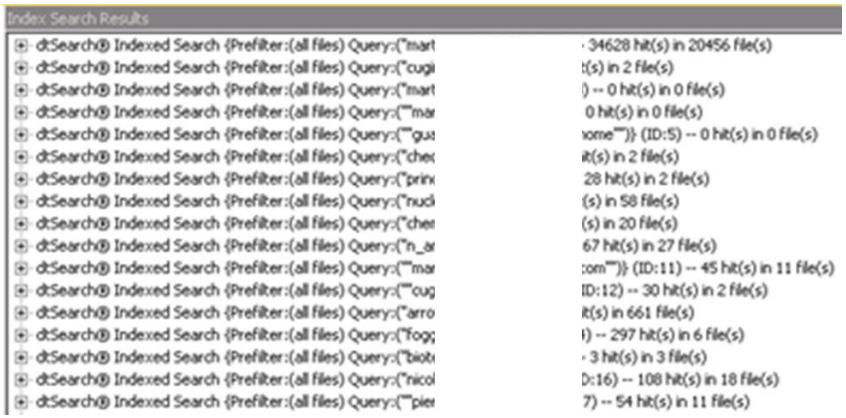
Analisi: Axiom

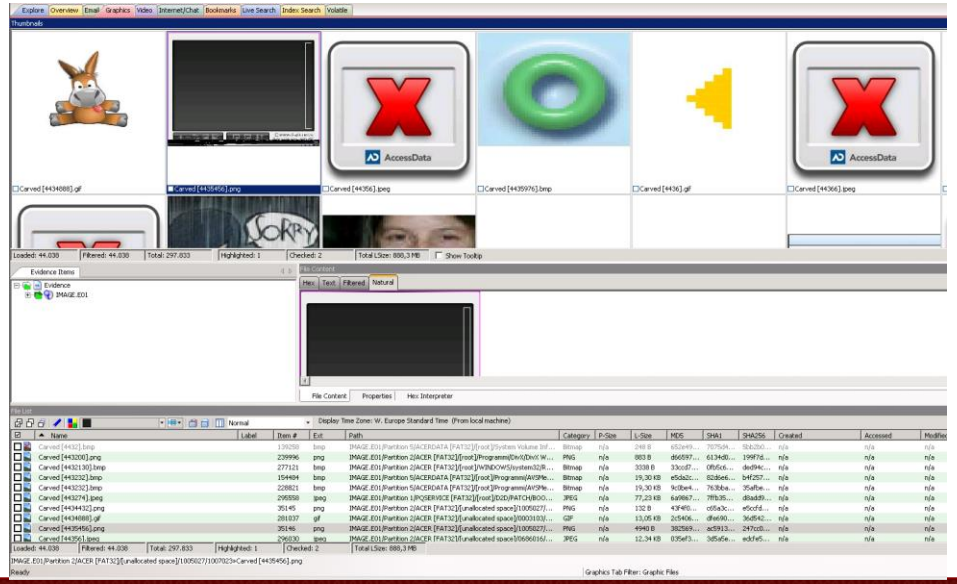
Analisi: NUIX



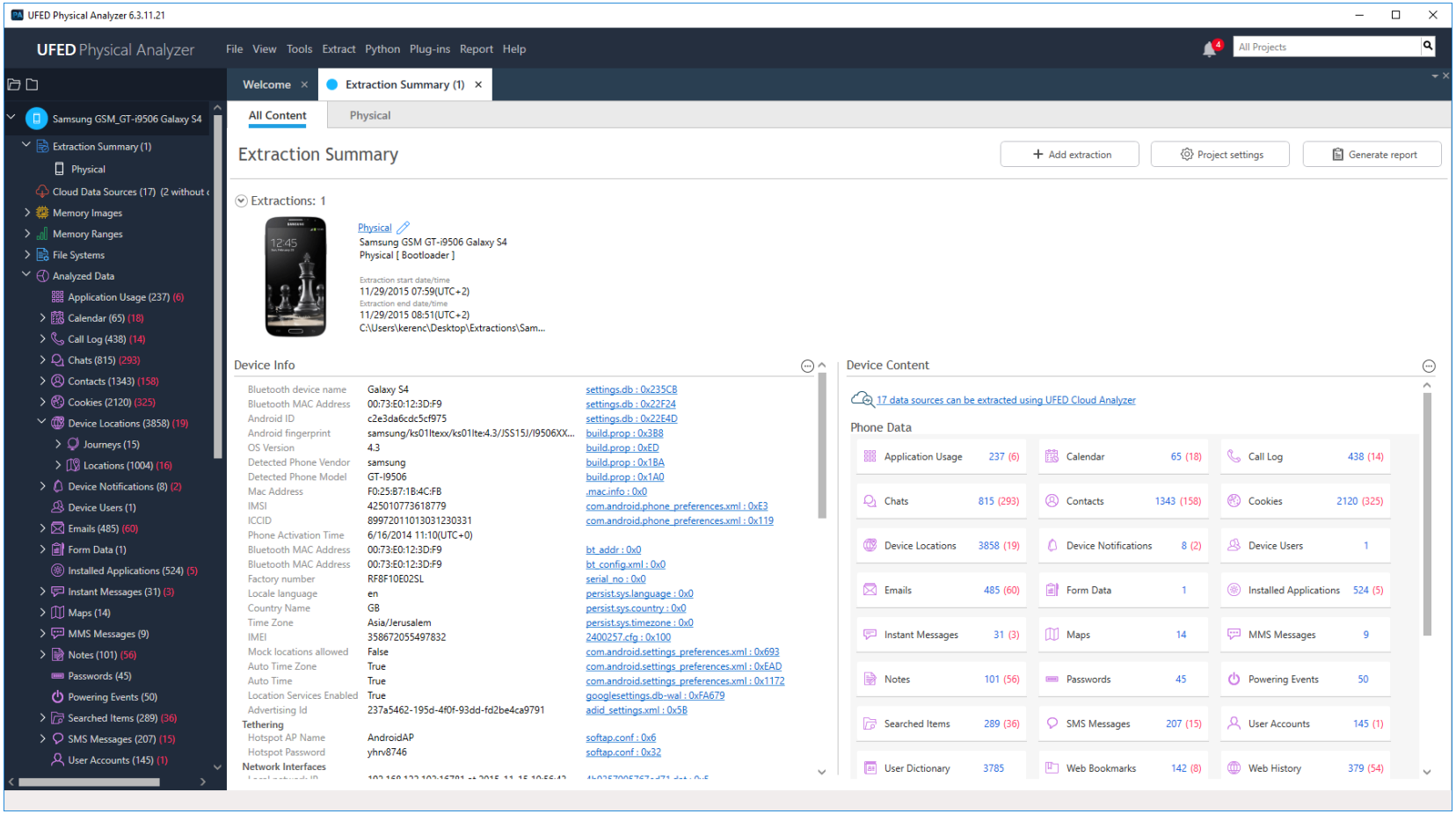
Analisi: FTK


File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search Volatile
dtSearch® Index
Terms
ross
Add
Indexed Words Total Hits
rosrosrosrotrotr 2
rosrotoors 5
rosrpsrpsrpsrpsr 1
rosrrsooos 5
rosrxs 1
ross 91
ross_ 4
rossa 133
rossa93 3
rossaartista 3
rossabarra 1
Search Criteria
Operators
And Or
Terms
All Selected
Accumulate Results
Search Terms Total Hits
informa 462
Clear
Expand Terms...
Import...
Export...
Options...
Search Now

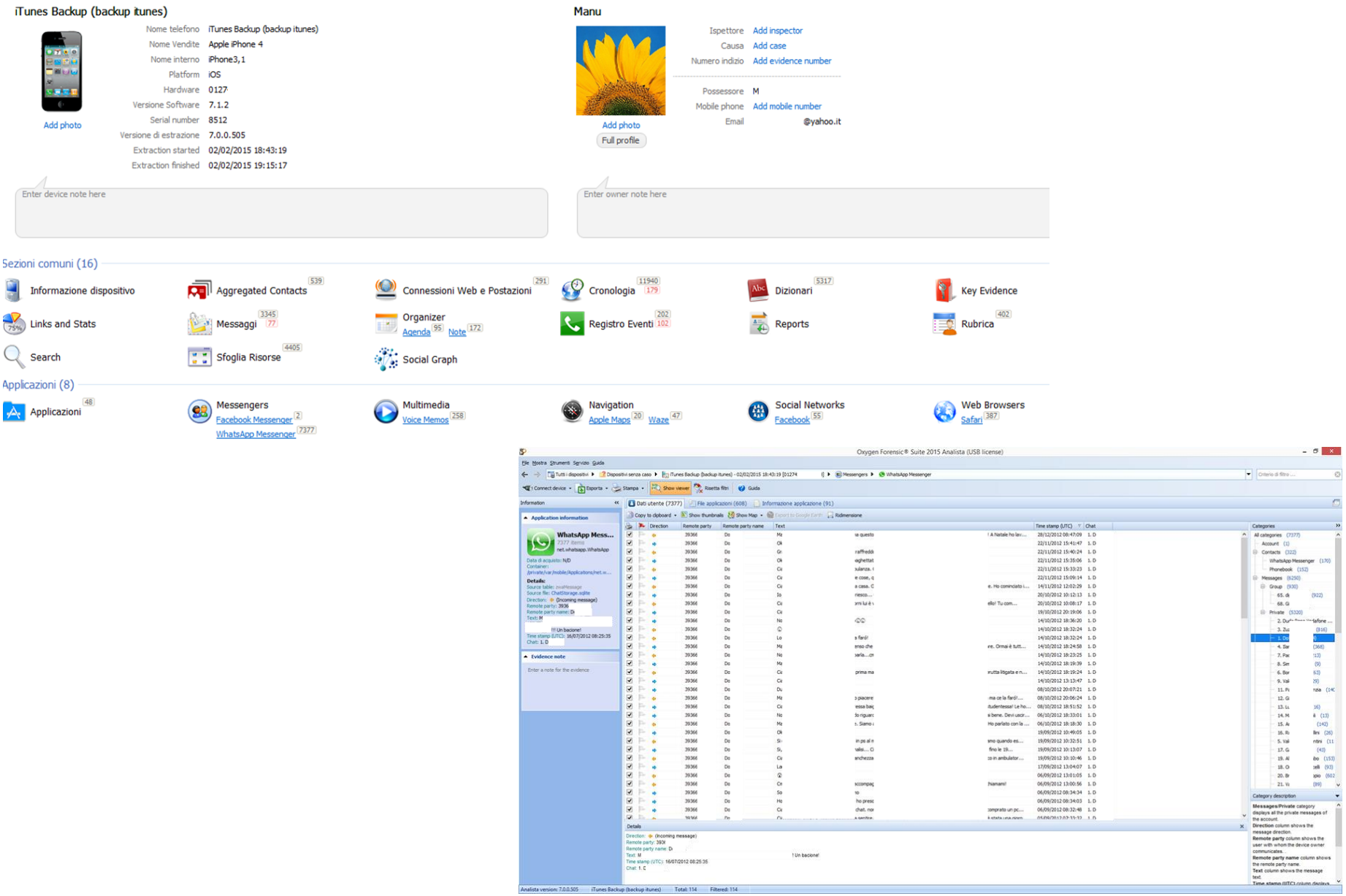

Index Search Results
dtSearch® Indexed Search {Prefilter:(all files) Query:("mart · 34628 hit(s) in 20456 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("cugi t(s) in 2 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("mart) -- 0 hit(s) in 0 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:(""ma 0 hit(s) in 0 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:(""gus ome"")} (ID:5) -- 0 hit(s) in 0 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("chec it(s) in 2 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("prin 28 hit(s) in 2 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("nuck (s) in 58 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("cher (s) in 20 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("n_a 67 hit(s) in 27 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:(""ma :om"")} (ID:11) -- 45 hit(s) in 11 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:(""cug ID:12) -- 30 hit(s) in 2 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("arro it(s) in 661 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("fogg l) -- 297 hit(s) in 6 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("biot · 3 hit(s) in 3 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:("nicol D:16) -- 108 hit(s) in 18 file(s)
dtSearch® Indexed Search {Prefilter:(all files) Query:(""pier 7) -- 54 hit(s) in 11 file(s)


Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search Volatile
Thumbnails
AccessData
AccessData
Evidence Items
Evidence
IMAGE.E01
File Content
Properties
Hex Interpreter

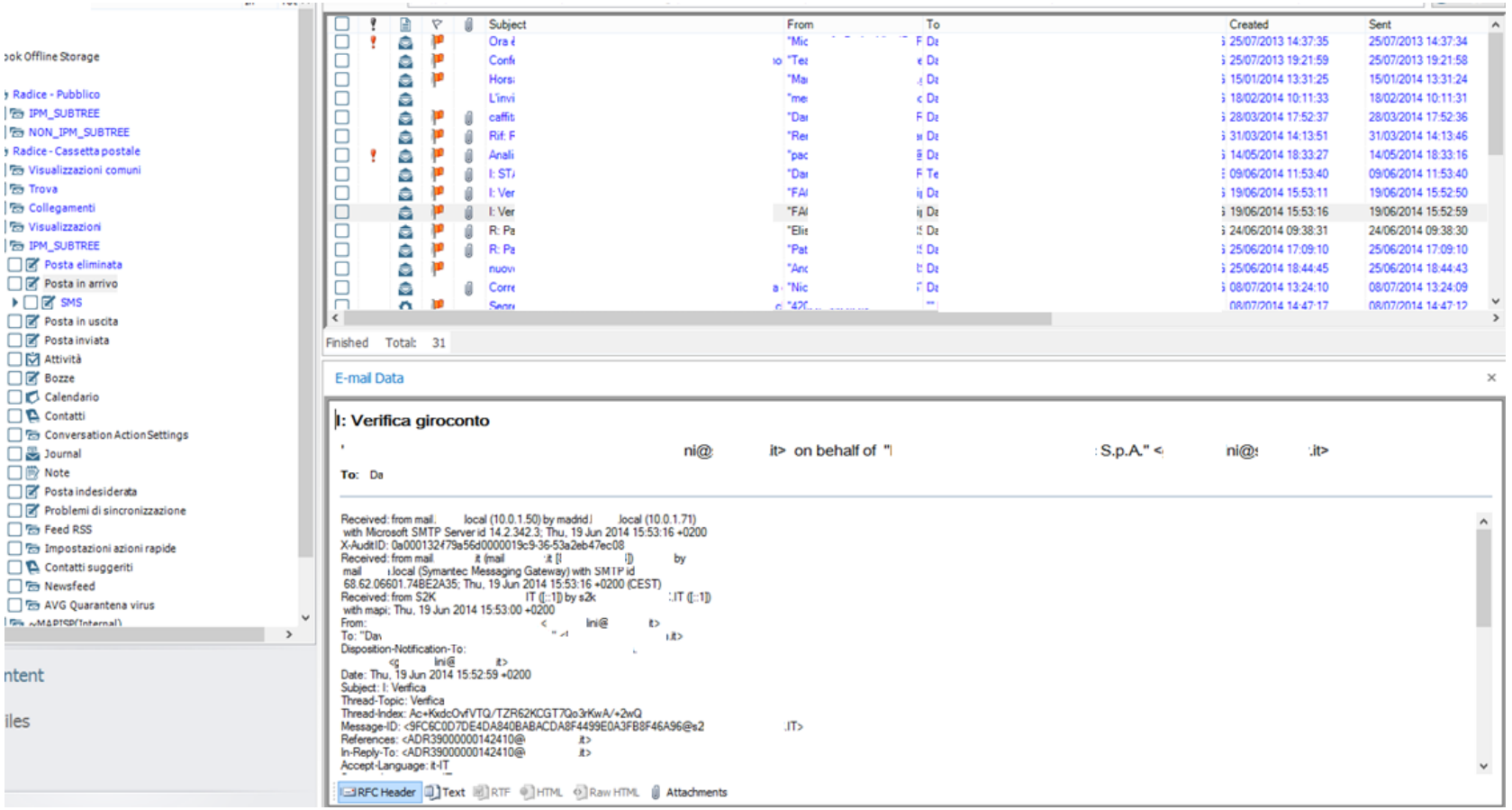
Analisi: UFED4PC



Analisi: Oxygen Forensics



Analisi: P2C


Subject
From
To
Created
Sent
Finished
Total: 31
E-mail Data
I: Verifica giroconto
To: Da
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: 0a000132-f79a56d0000019c9-36-53a2eb47ec08
Received: from mail by
mail local (Symantec Messaging Gateway) with SMTP id
68.62.06601.74BE2A35; Thu, 19 Jun 2014 15:53:16 +0200 (CEST)
Received: from S2K IT ([::1]) by s2k :IT ([::1])
with mapi; Thu, 19 Jun 2014 15:53:00 +0200
From:
To: "Da
Disposition-Notification-To:
Date: Thu, 19 Jun 2014 15:52:59 +0200
Subject: I: Verifica
Thread-Topic: Verifica
Thread-Index: Ac+KxdcOvfVTQ/TZR62KCGT7Qo3rKwA/+2wQ
Message-ID: <9FC6C0D7DE4DA840BABACDA8F4499E0A3FB8F46A96@s2 :IT>
References: <ADR390000000142410@ it>
In-Reply-To: <ADR390000000142410@ it>
Accept-Language: it-IT
RFC 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*"

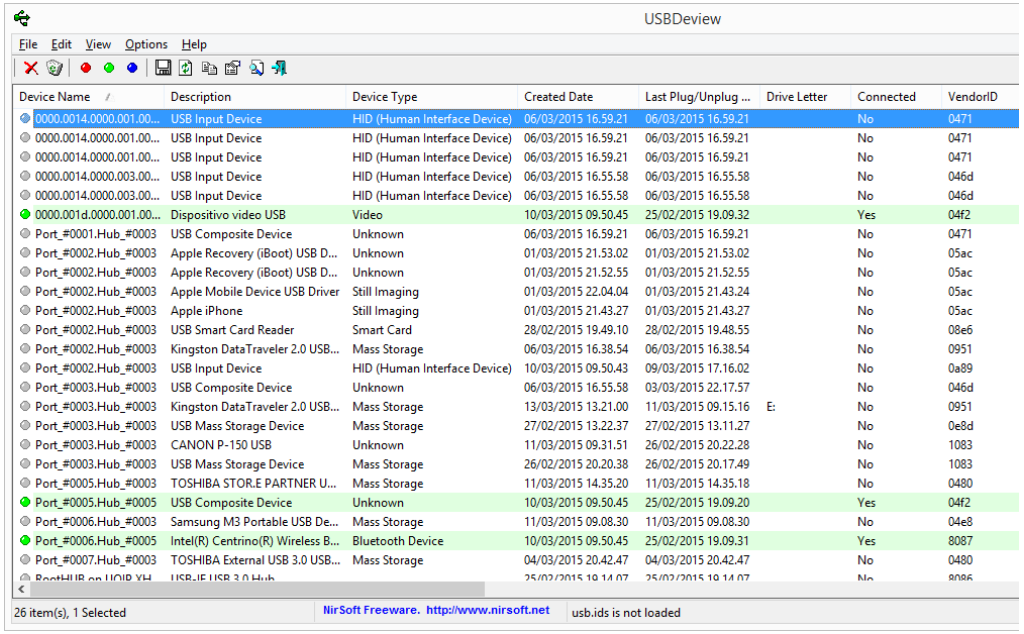
o "*G. Rossi*" o "*Giovanni NEAR/50 Rossi*"

Analisi: artefatti di Windows

- Registri
  - Configurazione del sistema operative 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 operative
- 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



Analisi: dispositivi USB

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

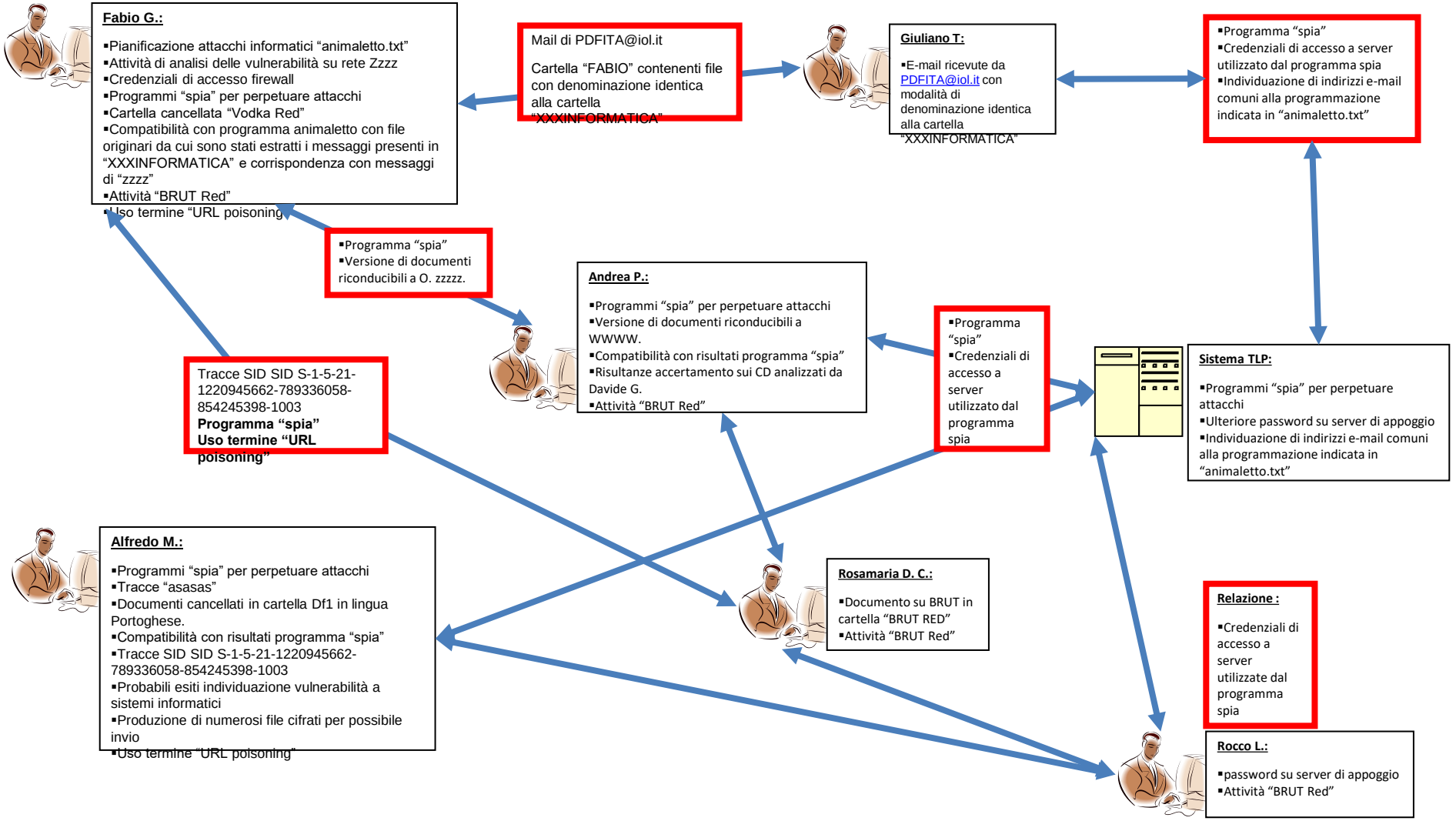
Link target information	
Local Path	E:\Marketing Plans.doc
Volume Type	Removeable Disk
Volume Label	BIGSTORE
Volume Serial Number	6CA3-55E3
File size	30720
Creation time (UTC)	9/04/2007 11:39:59 PM
Last write time (UTC)	7/04/2007 10:56:04 AM
Last access time (UTC)	9/04/2007 4:00:00 PM

La link analysis

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

La link analisys 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

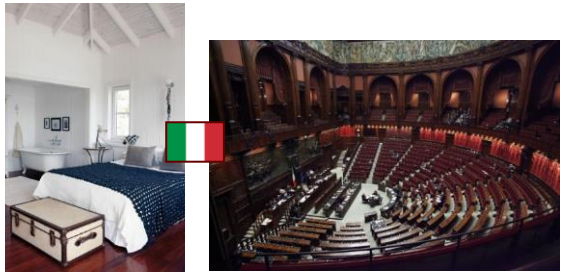


Valutazione

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

0100001101000001010011010100010101010010010000001

CAMERA



Valutazione

Perché il reperto informatico può essere facilmente:

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

Inoltre, bisogna verificare se le operazione 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

- Dall'analisi del pc emerge che in data 05/06/2014 l'utilizzatore del computer ha cercato sul motore di ricerca Google

"come far eccitare una ragazzina di 12 anni"

- Ognuno fornisca la propria valutazione

Valutazione	Votanti

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 rigoriosi
- 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…