# DIGITAL FORENSICS

## Acquisizione Forense di Evidenze da Memoria

INDAGINI ONLINE

# AGENDA

- Acquisizione e analisi forense
  - Identificazione
  - Raccolta
  - Acquisizione
  - Analisi
- Presentazione dei risultati – Reporting
  - Esempio di Report + Esercitazione
- Conclusioni – Quesiti

# Acquisizione e analisi forense

INDAGINI ONLINE

# Problema

La trasformazione digitale di molteplici attività, che prima si sviluppavano attraverso lo scambio di documenti analogici, interessa anche i fenomeni criminali e, pertanto, è necessario che le tecniche di analisi forense si adeguino alle nuove tecnologie.

La Digital Forensics consiste nella raccolta ed analisi dei reperti che possono essere utilizzati al fine di documentare il fenomeno verificatosi e poter perseguire i responsabili.

Affinché le prove estrapolate dai reperti possano essere utilizzabili in sede processuale è bene adottare una serie di linee guida.

Queste linee guida hanno il compito di:

- Definire i requisiti del reperto digitale
- Stabilire le fasi da seguire e l'obiettivo che si vuole raggiungere
- Individuare le figure professionali che gestiranno le evidenze digitali

# Identificazione

La prova informatica si presenta in forma fisica e logica

- Device
- Rappresentazione dei dati

- 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
- 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 gli eventuali sistemi con cui può aver comunicato

# 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

In fase di identificazione il DEFR deve:

- Documentare marca, tipo e numero di serie di ogni supporto individuato. Inoltre, se i supporti risultano danneggiati esternamente, deve documentare lo stato con l'ausilio di foto
- Identificare tutti i computer e il loro stato (acceso/spento), che deve rimanere inalterato:
  - stato acceso: documentare cosa è visibile sullo schermo (effettuando foto) e inserirlo a verbale
  - stato spento: non effettuare alcuna operazione sul dispositivo.
- Reperire i caricabatterie dei dispositivi alimentati a batteria, per evitare che possano scaricarsi
- Utilizzare un rilevatore di segnali wireless per verificare la presenza di dispositivi nascosti
- In determinate situazioni può essere molto utile prendere in considerazione anche evidenze non digitali, come ad esempio informazioni sui dispositivi fornite da personale impiegato in azienda (ad esempio: scopo di utilizzo del dispositivo, password per l'accesso, ecc. . . )

# Identificazione

Tra le principali tipologie di media in grado di contenere dati, e quindi oggetto di interesse, possiamo annoverare:

- Elaboratori (disco interno, raid, supporti ssd, ecc.)
- Storage esterni (hd esterni, pen drive, schede di memoria)
- Dispositivi ottici (CD, DVD, BLU-RAY)
- Supporti Legacy (Floppy Disk, Nastri backup)
- Dispositivi con memoria embedded (macchine fotografiche, console, cellulari, sistemi di videosorveglianza, lettori multimediali, smart phone, smart watch, smart tv, ecc.)
- Sistemi virtuali
- A distanza (server, cloud, servizi online, ecc.)

# Raccolta (sequestro) o acquisizione?

Una volta terminata la fase di identificazione il DEFR, con gli strumenti in suo possesso, deve decidere se procedere con la raccolta (sequestro) o l'acquisizione.

Per prendere tale decisione vanno presi in considerazione alcuni fattori:

- volatilità della possibile evidenza
- esistenza di cifratura completa o parziale dei supporti (nel qual caso può essere utile effettuare l'acquisizione dei dati volatili in RAM)
- criticità del sistema (es. server che non può essere spento poiché critico per il business aziendale)
- requisiti legali
- carenza delle risorse necessarie (ad es. quantitativo di spazio necessario o disponibilità del personale).

# Raccolta (sequestro) o acquisizione?

Dopo aver identificato i reperti e scelto se sequestrarli o acquisirli in loco occorre:

- Valutare cosa è pertinente e cosa è trascurabile
- Acquisire tutto quello che è necessario
- Assegnare un identificativo ad ogni reperto ed etichettarlo
- Compilare una scheda con le informazioni visibili (marca, modello, seriale, ubicazione, stato, condizioni, collegamenti)
- Stabilire un piano di acquisizione efficace e conforme agli obiettivi dell'indagine

# Raccolta

Nel caso in cui si opti per il sequestro dei dispositivi, la modalità di esecuzione della stessa dipende dallo stato in cui si trova il sistema.

- Sistema trovato spento

  Nel caso in cui il sistema venga trovato spento, vanno prese in considerazione le seguenti attività:

  - assicurarsi che il dispositivo sia effettivamente spento e non in standby
  - rimuovere il cavo di alimentazione, staccando prima l'estremità connessa al dispositivo e poi quella a muro
  - disconnettere e assicurare tutti i cavi connessi al dispositivo ed etichettare le relative porte a cui sono connessi, così da ricostruire le connessioni in seguito
  - proteggere il tasto di accensione, onde evitare accensione casuale del dispositivo
  - mettere in sicurezza eventuali alloggiamenti per floppy disk, cd/dvd con del nastro per evitare apertura/espulsione del contenuto.

# Raccolta

- Sistema trovato acceso

  Nel caso in cui il sistema venga trovato accesso, vanno prese in considerazione le seguenti attività:

  - acquisire i dati volatili del dispositivo prima di spegnerlo, così da poter avere a disposizione eventuali chiavi di cifratura residenti in memoria. Nel caso in cui si sospetti la presenza di meccanismi di cifratura conviene procedere in seguito con acquisizione logica
  - nel caso in cui si voglia lasciare il dispositivo acceso (ad esempio per presenza confermata di meccanismi di cifratura), bisogna prestare particolare cura durante il trasporto (raffreddamento, protezione da shock)
  - nel caso in cui si decida di spegnere il dispositivo, valutare se sia il caso di effettuarlo mediante regolare procedura di spegnimento o staccando il cavo di alimentazione (rimuovendo prima l'estremità attaccata al dispositivo e poi quella attaccata alla presa). Normalmente tale decisione dipende dalla configurazione del sistema
  - etichettare e staccare tutti i cavi dal sistema. Etichettare tutte le porte cosi che lo stato del sistema possa essere ricostruito in laboratorio
  - proteggere il tasto di accensione, onde evitare una accensione casuale del dispositivo
  - infine, nel caso tale dispositivo sia un notebook, acquisire i dati volatili prima di rimuovere batteria e successivamente il cavo di alimentazione. Mettere in sicurezza anche eventuali alloggiamenti per floppy disk, cd/dvd utilizzando del nastro.

# Preservazione

Occorre garantire che sia preservata, con i dovuti accorgimenti, la confidenzialità, l'integrità e la disponibilità della potenziale prova.

L'evidenza, infatti, va preservata sia durante il trasporto che lo stoccaggio, che potrebbe superare il suo tempo di vita a seconda dei tempi di giustizia.

In caso di modifica accidentale o incidentale, deve essere giustificata e documentata con apposito verbale.

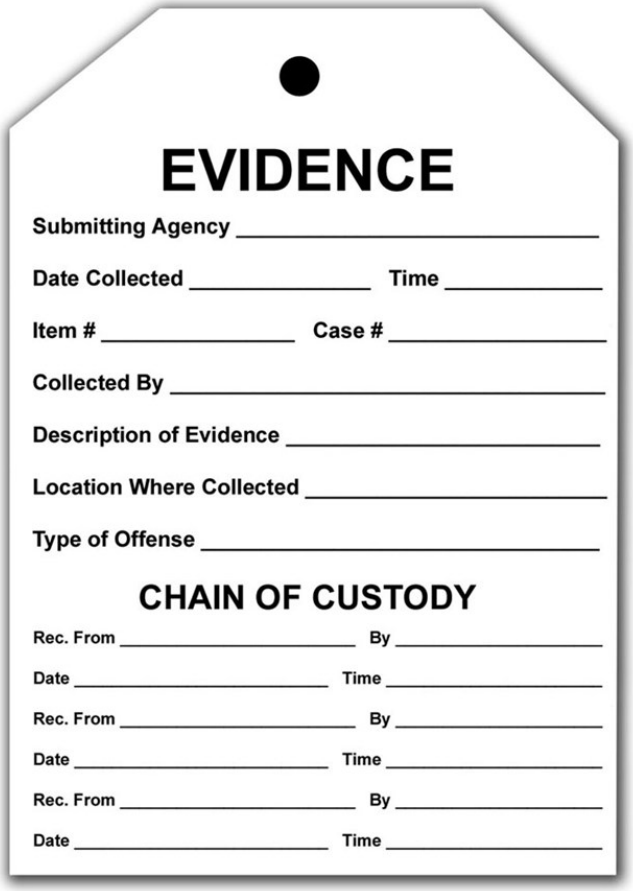
Per far ciò occorre:

- Etichettare tutto
- Verificare che le batterie siano opportunamente caricate (e ricaricare)
- 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

# Conservazione: catena di custodia

Nel caso in cui si decida di procedere al sequestro dei reperti, questi ultimi devono essere protetti e sigillati per evitare modifiche o guasti e deve essere creata la 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



# Acquisizione forense

La copia forense è un duplicato fedele della memoria originale in ogni sua parte.

Le copie eseguite a basso livello sono dette bit stream image.

Possiamo distinguere alcuni tipi di acquisizioni:

- **Post mortem:** (dopo lo spegnimento) si scollega il dispositivo dal sistema di origine e lo si collega ad un postazione forense dotata di write blocker o configurata come tale.
- **On the fly**: (direttamente sul sistema di origine) nel caso in cui non è possibile o è complicato scollegare i supporti di massa (dischi RAID o memoria saldate) la copia è effettuata sulla stessa macchina
- **Tramite rete**: è possibile trasferire la copia attraverso la rete

# Acquisizione

Occorre stabilire e rispettare l'ordine di volatilità:

- Registri, Memoria Cache
- Memoria RAM
- Stato della rete (connessioni, socket in ascolto, applicazioni coinvolte, arp cache, routing table, dns cache, ecc.)
- Processi attivi
- Supporti di massa collegati (memorie interne: hd, pendrive)
- Log remoti
- Dispositivi rimovibili (memorie esterne: floppi, nastri)
- Supporti di backup (ottici e magnetici)

# Acquisizione

- Le copie eseguite devono essere identiche o il più possibile simili all'originale (in tal caso occorre giustificare la scelta)
- Durante la copia dell'origine, quest'ultima non deve essere modificata (integrità)
- Nel caso in cui non ci sia un metodo che consenta di evitare di alterare l'originale, la scelta va giustificata e documentata
- Le procedure devono essere attuate e documentate secondo metodologie e tecnologie riconosciute, in modo da poter essere verificabili dagli altri attori (verificabilità)
- Potrebbe essere necessario eseguire copie parziali della memoria del dispositivo, anche in questo caso la scelta deve essere motivata e documentata

# Acquisizione forense

Nel caso in cui si opti per l'acquisizione dei dispositivi, sia on-site che in laboratorio, la modalità di esecuzione della stessa dipende, allo stesso modo della raccolta dallo stato in cui si trova il sistema.

- Sistema trovato acceso
  - Nel caso in cui il sistema venga trovato accesso, vanno prese in considerazione le seguenti attività:
  - acquisire tutti i dati volatili che verrebbero persi se il dispositivo venisse spento (es. RAM, processi in esecuzione, connessioni di rete, impostazioni di data ed ora). Per effettuare l'acquisizione è consigliabile riversare i dati copiati in un contenitore logico, calcolarne l'hash e documentarne il valore. Ove ciò non sia fattibile è possibile utilizzare un contenitore di tipo ZIP, calcolarne l'hash e documentarlo
  - iniziare il processo di copia forense dei dati non volatili utilizzando strumenti validati. La copia forense ottenuta va memorizzata in un dispositivo preparato per tale scopo (es. Formattato). Se la copia viene invece memorizzata in un contenitore logico bisogna assicurarsi che questa non possa essere corrotta o danneggiata. Al termine del processo di copia calcolare e annotare il valore di hash
  - utilizzare una sorgente affidabile per documentare data e ora e documentare accuratamente inizio e fine di oggi attività

# Acquisizione forense

- Sistema trovato spento

  Nel caso in cui il sistema venga trovato spento, vanno prese in considerazione le seguenti attività:

  - assicurarsi che il sistema sia davvero spento
  - rimuovere il supporto di memoria dal dispositivo spento (se non già fatto), ed etichettarlo accuratamente (es. Produttore, modello, numero di serie)
  - eseguire la copia forense del supporto di memoria utilizzando un tool validato. Calcolarne il valore di hash al termine.

- Sistemi critici

  Un caso particolare nella fase di acquisizione si ha quando ci si trova davanti ad un sistema critico, per cui per svariate ragioni non è possibile procedere all'acquisizione completa dei dati contenuti all'interno del sistema. Alcuni esempi di tali sistemi sono data center, sistemi di sorveglianza o sistemi medici. In tali situazioni vi sono due sole possibili alternative di acquisizione:

  - acquisizione live (acquisizione totale della memoria RAM e di massa)
  - acquisizione parziale (solo determinate porzioni di memoria di interesse investigativo):
    - il sistema di cui si vogliono acquisire i dati ha una capacità di memoria notevolmente grande, contenendo quindi una mole notevole di dati (si pensi ai database server)
    - il sistema, a causa della sua criticità, non può essere spento
    - solo alcuni dati sono rilevanti all'interno del sistema
    - vi sono dei vincoli legali che consentono solo l'acquisizione di alcuni dati.

# Algoritmi di hashing

Al termine della fase di acquisizione bisogna “sigillare” i dati acquisiti attraverso un sigillo digitale (solitamente un impronta hash con l’eventuale aggiunta dell’utilizzo di una firma digitale per associare l’operazione al DEFR) per dimostrare che la copia ottenuta sia inalterata ed identica all’originale.

L'algoritmo di hash (MD5, SHA-1) elabora una qualunque mole di bit e restituisce in output una stringa di bit di dimensione fissa.

L'output è detto digest.

- La stringa di output è univoca per ogni documento e ne è un identificatore
- L'algoritmo non è invertibile, ossia non è possibile ricostruire il documento originale a partire dalla stringa che viene restituita in output (anche se in realtà per ogni digest esistono infiniti input che lo generano – cd. collisioni)

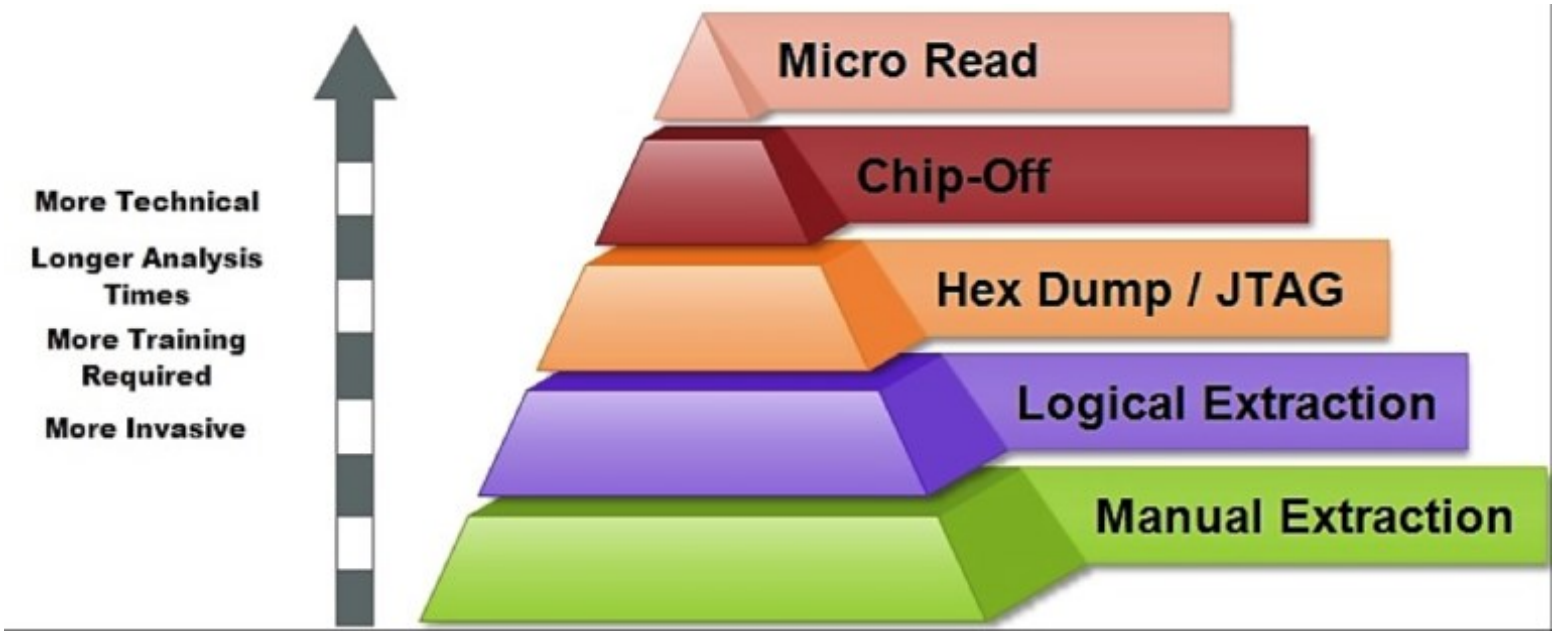
DPCM 8 febbraio 1999: «l'impronta di una sequenza di simboli binari è una sequenza di simboli binari di lunghezza predefinita generata mediante l'applicazione alla prima di un'opportuna funzione di hash»

# Algoritmi di hashing

- L'algoritmo restituisce una stringa di numeri e lettere (detto digest) a partire da un qualsiasi flusso di bit di qualsiasi dimensione finita.
- La stringa di output dell'algoritmo è univoca per ogni documento identificato. Pertanto, l'algoritmo di hashing è utilizzato per la firma digitale.
- La lunghezza del digest varia a seconda degli algoritmo utilizzato
- L'algoritmo non è invertibile, cioè non si può ricavare la sequenza di bit in ingresso a partire dal digest.

# Acquisizione: classificazione

Per acquisizione forense del supporto di memorizzazione si intende l'estrazione del contenuto memorizzato sotto forma di sequenza di bit memorizzati al suo interno.




La copia forense ideale è una copia bit a bit perché include: tutti i file, anche quelli cancellati, lo slack space e lo spazio libero.

# Tipi di copia forense

Un dispositivo di memoria può essere copia in due modalità:

- Device to device
- Device to file

Nel secondo caso, quello più utilizzato, si può scegliere:

- Il formato: RAW (dd), EWF o AFF (compressi)
- Lo split su più file
- Livello di compressione
- La cifratura
- I metadati
- Calcolo degli hash
- È possibile memorizzare più copie sullo stesso device

# Esempio

Acquisizione pendrive usb

INDAGINI ONLINE

# Esercizio

Acquisizione memoria e calcolo impronta hash

INDAGINI ONLINE

# Acquisizione: write blocker

Per dare garanzia del rispetto dei principi enunciati, tutte le operazioni eseguite in fase di acquisizione devono essere accuratamente documentate, meglio se si utilizzando dei dispositivi che registrano automaticamente quanto viene eseguito.

Se possibile è conveniente utilizzare dispositivi che impediscono l'alterazione del supporto di origine: c.d. write-blocker


# Acquisizione live

Nel caso in cui ci dovesse capitare di trovare le apparecchiature in funzione oppure non è possibile spegnerle (macchine critiche),  occorre effettuare l'acquisizione della ram e delle altre informazioni presenti all'interno della macchina.

In questo caso sono utilizzate le distribuzioni che consento di eseguire programmi presenti su altri dispositivi (DVD o Pendrive) senza intaccare la memoria di massa.

Lo stesso tipo di acquisizione può essere sfruttata su quelle macchine dove è complicato raggiungere la memoria, in questo caso il sistema può essere avviato direttamente dalla distribuzione in modalità Live.

# Attività di preview o triage

Potrebbe essere necessario effettuare una preview del contenuto del sistema (per esempio durante un'ispezione) oppure acquisire solo alcune informazioni (perquisizione)

Oppure semplicemente occorre valutare se quel dispositivo è pertinente con l'obiettivo dell'attività oppure no.

Anche in questo caso si possono utilizzare le distribuzioni live.

È importante che qualsiasi attività posta in essere, anche se non comporta alcuna modifica dei dati, sia documentata in un apposito verbale di ispezione o perquisizione.

# Acquisizione logica

In determinate condizioni, potrebbe essere necessario effettuare la copia logica, ovvero una copia parziale del contenuto del dispositivo.

Questa ipotesi si verifica principalmente nei dispositivi:

- Cifrati
- Server
- Mobile
- Condivisi o multifunzione

In pratica in quei dispositivi dove è necessario operare con il sistema operativo acceso oppure dove le informazioni di interesse sono circoscritte a determinati file.

# Esempio

Triage e acquisizione logica

INDAGINI ONLINE

# Acquisizione della RAM

La RAM (Random Access Memory) è una memoria di tipo volatile, che permette l'accesso diretto a qualunque indirizzo di memoria con lo stesso tempo di accesso.

Dopo lo spegnimento del dispositivo i dati vengono persi.

L'acquisizione della RAM si effettua a sistema acceso.

È utile acquisire la RAM quando:

- Si vuole recuperare le password o le informazioni presenti in memoria
- Per tenere traccia dei processi attivi ed analizzarli successivamente
- Per recuperare informazioni dai software che non lasciano tracce
- Nel caso di analisi di malware, rootkit o trojan

# Acquisizione della RAM

- Eseguire il tool di acquisizione da dispositivo esterno (pendrive, DVD)
- Salvare il contenuto su dispositivo esterno per non intaccare i dischi locali
- Se la macchina da clonare è virtuale basta usare il comando «snapshot»

Software per acquisire e analizzare la RAM

- Volatility
- AccessData FTK Imager
- Windows Memory Reader
- Magnet RAM Capture

# Verifica e apertura di un immagine forense

- È possibile verificare l'integrità di una copia forense ricalcolando l'hash sulla stessa immagine e confrontandolo con quello calcolato al momento della realizzazione della copia
- In base alla modalità con cui è stata eseguita la copia forense, (raw, split, ewf, aff, clone) ci sono diverse alternative per l'accesso in fase di analisi
- Il fine è quello di poter accedere al contenuto (filesystem, aree allocate e non) dell'immagine acquisita per poter eseguire le verifiche richieste
- Alcuni formati prevedono solo l'acceso in sola lettura

# Esempio

Acquisizione RAM

Apertura di un'immagine forense, montaggio e analisi del file system

INDAGINI ONLINE

# Analisi

L'analisi deve consentire:

- la ricostruzione degli eventi passati attraverso la lettura dei dati rinvenuti.
- L'estrazione dei dati e l'elaborazione per ricostruire le informazioni
- L'interpretazione delle informazioni per individuare gli elementi utili all'indagine
- La comprensione e correlazione dei dati, in modo da affinare le ricerche e poterne trarre le conclusioni

È sicuramente la fase più laboriosa di tutto il processo e richiede conoscenze multidisciplinari.

# Analisi: caratteristiche

Poiché ogni copia coincide con l'originale, l'analisi va eseguita sulla 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 i dati e non la loro valutazione)
- Metodologie: si può applicare la Regola delle «***5W***»
  - *WHO*? («Chi?»)
  - *WHAT*? («Che cosa?»)
  - *WHEN*? («Quando?»)
  - *WHERE*? («Dove?»)
  - *WHY*? («Perché?»)

# Analisi: correlazione dei dati

- Che cosa è successo e come si è svolto?
  - Individuare i dati utili a ricostruire I fatti
  - Comunicazioni
  - Documenti
  - Log
  - Metadati (date, luoghi, coordinate…)
- Chi è coinvolto?
  - Comunicazioni
  - Metadati (date, utenti)
- Quando è accaduto?
  - Comunicazioni
  - Metadati (date, utenti)
- Da dove a dove?
  - Comunicazioni
  - Documenti
  - Log
  - Metadati (date, luoghi, coordinate…)
  - Tabulati telefonici
- Quante volte si è verificato?
  - Comunicazioni
  - Documenti
  - Log
  - Metadati (date…)
- C'era consapevolezza?
  - Comunicazioni
  - Cancellazione dati
  - Documenti
  - Log
  - Metadati (date…)
  - Navigazione web
  - Competenze utente

# Analisi: strategie operative

- 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
  - Tipologie di attacco
- Artefatti del sistema operativo

# Recupero dei dati cancellati

Quando si cancella un file, i dati non sono immediatamente azzerati, ma soltanto derefenziati, ovvero viene cancellata la voce sul registro del file system che consente di richiamarlo.

I dati, di conseguenza, sono ancora sul supporto di memoria, ma lo spazio precedentemente occupato risulta deallocato (libero)

Anche i metadati potrebbero essere ancora presenti in maniera analoga sul File system (MFT)

Per il recupero dei file cancellati possono essere percorse due soluzioni alternative:

- Analisi dei metadati del file system
- File carving

# Recupero dei dati cancellati

Recupero tramite analisi dei Metadati:

- Strettamente dipendente del File system
- Consente di ricostruire anche i file frammentati
- È possibile recuperare altre informazioni tra cui:
  - il nome del file
  - la data di creazione
  - la data di modifica
  - la data di ultimo accesso
  - il proprietario (dipende dal File system)
  - Permessi scrittura e lettura

# Recupero dei dati cancellati

Recupero tramite File Carving:

- Se il dato è completamente dereferenziato, l'unico recupero possibile è tramite la scansione del Binary Large Object
- Vengono ricercate le intestazioni (header o magic number) identificative di specifici formati di file
- Si cerca di interpretare quello che segue come parte integrante del file (se esiste viene cercato anche il footer)
- Funziona bene nel caso in cui i file siano allocati su cluster contigui, ma non in caso di frammentazione
- Non recupera le informazioni come il nome originario del file e gli altri metadati del file system

# Recupero dei dati cancellati

Il data carving è un processo di estrazione di un set di dati da un insieme di dati molto più ampio.

La tecnica del data carving è utilizzata solitamente durante le indagini di analisi forense per analizzare lo spazio non allocato.

Durante questo procedimento la struttura del file system viene ignorata.

I file sono individuati e catalogati in base all'header e al footer trovato

Distinguiamo

- Data carving base
  - L'header e footer dei file non sono sovrascritti
  - Il file non è frammentato
  - Il file non è compresso
  - Il file estratto è l'insieme di bit contenuti tra header e footer
- Data carving avanzato
  - I frammenti non sono sequenziali
  - I frammenti non sono ordinati
  - Mancano dei frammenti

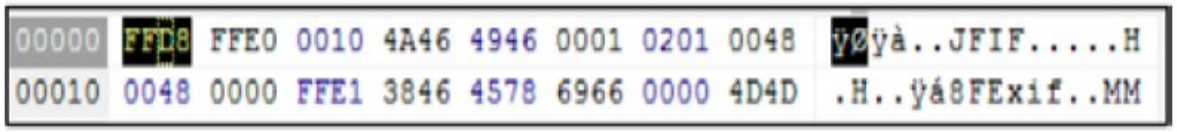



Figure 2. JPEG header.

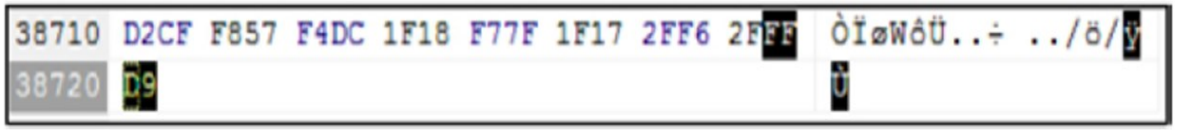



Figure 3. JPEG footer.

IN

# Esempio

Analisi del file system per recupero dei file cancellati e data carving

INDAGINI ONLINE

# Analisi dei metadati

I metadati sono dati riguardanti altri dati.

Spesso i metadati hanno un ruolo fondamentale nelle indagini digitali.

Possono fornire informazioni importanti riguardanti il documento stesso, l'autore e la data e ora di creazione e modifica.

Possono rilevare informazioni che si è tentato di oscurare, nascondere o cancellare

Possono essere utilizzati per correlare i documenti allo loro fonte

Esempi di metadati:

- File system
- Documenti (office, pdf, ecc.)
- Immagini (dati exif)
- Audio / Video
- Email
- Applicazioni

# Esempio

Estrazione metadati

INDAGINI ONLINE

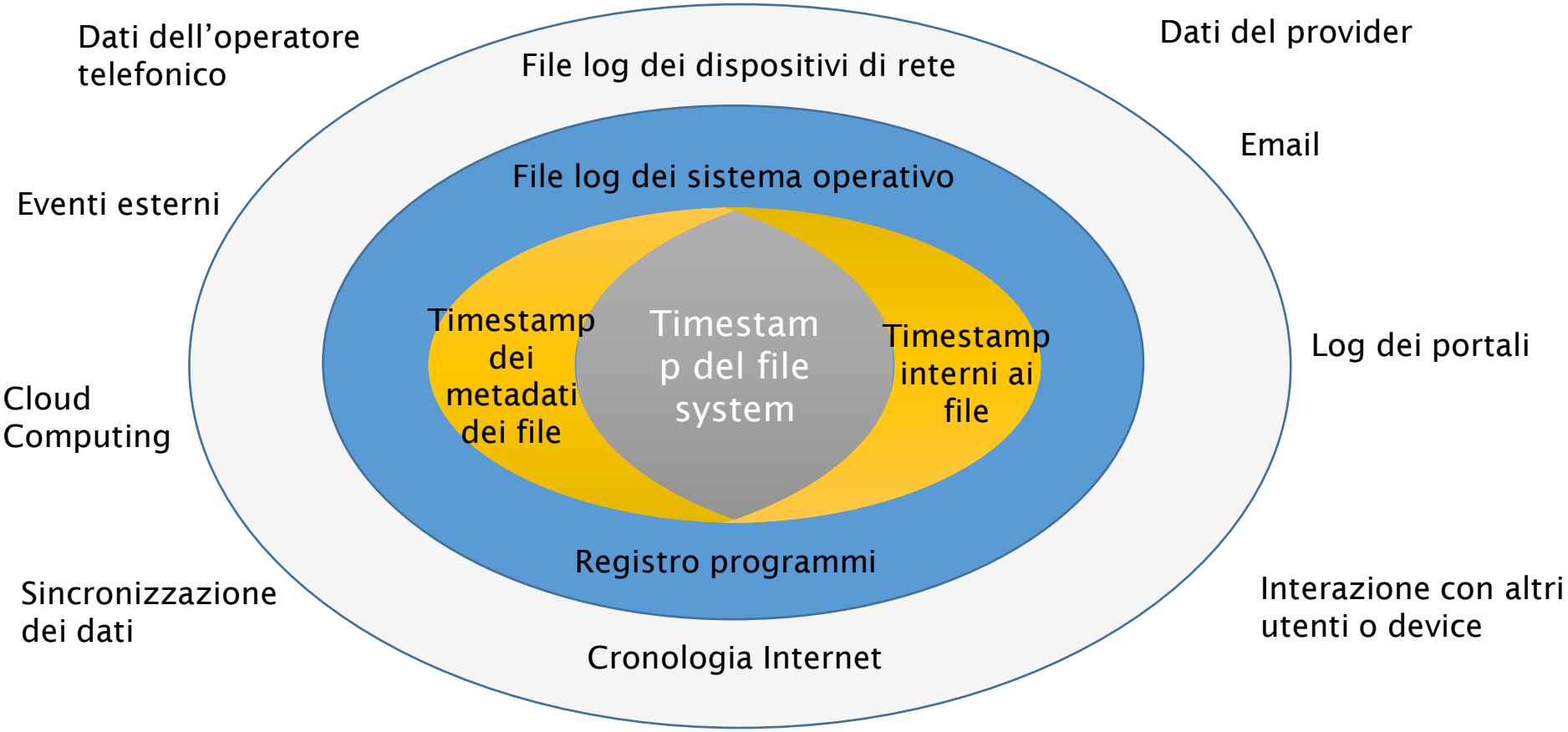
# Analisi: Timeline

Spesso è necessario ricostruire la cronologia delle attività che hanno determinato lo stato del dispositivo con l'obiettivo di individuare gli elementi di prova che concorreranno a dimostrare o confutare dei fatti.

Occorre creare una linea temporale relativa agli eventi verificatesi e richiede l'integrazione delle varie informazioni temporali (timestamp) create dal sistema operativo, dal file system e dalle applicazioni utente.

- Metadata dei file (timestamp della creazione, ultimo accesso ed ultima modifica dei file)
- Esecuzione dei programmi (S.O. registra informazioni sull'esecuzione dei programmi)
  - File prefetch su Windows
  - Registro di Windows
  - File log di sistema ….
- Artefatti generati dai programmi ad ogni esecuzione
  - Elenco file aperti o salvati
  - File di cronologia di navigazione
  - File di log ….

# Analisi: Supertimeline




INDAGINI ONLINE

# Esempio

Ricostruzione timeline

INDAGINI ONLINE

# Virtualizzazione delle immagini forensi

- Potrebbe essere necessario effettuare accertamenti direttamente sulla macchina accesa (p.e. per verificare il funzionamento di un programma o interrogare un database)
- La soluzione che consente di effettuare questo tipo di analisi, consiste nel creare una macchina virtuale a partire dalla copia forense, che deve essere obbligatoriamente bit a bit, e successivamente si esegue
- La macchina virtuale deve avere le schede di rete **disabilitate**
- Possono essere eseguiti programmi, in formato portable, per estrarre informazioni utili alle indagini
- Il vantaggio della macchina virtuale è legato soprattutto alla ripetibilità delle operazioni eseguite

# Esempio

Esempio macchina virtuale

INDAGINI ONLINE

# Valutazione

La valutazione è una fase necessaria per stabilire:

- Se il reperto informatico è stato
  - alterato
  - inquinato
  - contraffatto
- Se le procedure di acquisizione sono state legittime
- Se il reperto è
  - attendibile
  - integro
  - Autentico
- Il significato dei dati presenti sul supporto

# Esempi di ricerche

- Ricerca per parole chiave
- Utilizzo delle periferiche usb
- Analisi dei documenti aperti e utilizzati
- Ricostruzione della navigazione in internet
- Manomissione delle prove
- Cronologia dei programmi
- Conferma di un alibi

# Problematiche

- Dischi cifrati
- Memorie SSD
- Sistemi di sicurezza logica
- Sistemi embedded

# Soluzioni alternative e/o complementari

**Software commerciali:**

- **Forensic Toolkit (FTK)**
- **Magnet Internet Evidence Forenics (IEF)**
- **Oxygen Detective**
- **Encase**

# Esempio

Acquisizione e Analisi con soluzione commerciali

Comparazione dei risultati

INDAGINI ONLINE

# Presentazione dei risultati

Come creare un Report

Firma digitale e Marca temporale

INDAGINI ONLINE

# Presentazione

Dopo aver completato le fasi tecniche, occorre predisporre una sintesi dell'intero processo tramite l'esposizione, entro i limiti concordati, delle informazioni fattuali ricavate dalle prove e dall'insieme di esami ed analisi che hanno costituito l'indagine. Questo obiettivo si concretizza attraverso la redazione di un elaborato o report da cui sia possibile ricavare:

- l'origine delle fonti di prova digitale,
- la metodologia utilizzata per la gestione delle fonti di prova,
- la tecnologia adoperata per il trattamento delle fonti di prova,
- la procedura eseguita per giungere ai risultati conseguiti,
- i risultati ottenuti (anche sottoforma di allegati multimediali),
- la risposta al quesito.

# Presentazione

Un metodo suggerito per la stesura della relazione finale consiste nello sviluppare e strutturare la presentazione seguendo lo stesso ordine delle fasi ISO descritte nei paragrafi precedenti.

La presentazione dei risultati è l'elemento con cui si valuta tutta l'attività svolta. Per cui, durante la stesura, è fortemente consigliato tener conto delle seguenti indicazioni:

- occorre essere semplici e chiari,
- i risultati devono essere esposti in una forma facilmente comprensibile a tutti,
- i destinatari non hanno di solito competenze informatiche,
- molto probabilmente la relazione sarà esaminata da un tecnico della controparte,
- non bisogna essere approssimativi o esprimere giudizi che non siano corroborati dai dati.

# Report

## Tipologia: La Perizia e la Consulenza tecnica

La perizia e la consulenza tecnica sono i due mezzi di prova attraverso i quali fa ingresso nel processo penale il sapere tecnico, scientifico e artistico.

Entrambe si sostanziano, alternativamente o cumulativamente, nello svolgimento di indagini, nell'acquisizione di dati o nell'effettuazione di valutazioni che richiedono per la loro natura particolari competenze tecniche, scientifiche o artistiche.

**La perizia** (artt. 220 e ss.c.p.p.) costituisce mezzo di prova "neutro" (essendone affidato l'espletamento ad un soggetto terzo, quindi imparziale, nominato dal giudice) ed essenzialmente discrezionale (essendo rimessa al giudice la valutazione sul requisito della sua "occorrenza"). Oltre che a richiesta di parte, può essere disposta anche d'ufficio.

**La consulenza tecnica**, invece, può esperirsi: nell'ambito di una perizia già disposta, concedendo alle parti facoltà di nominare propri consulenti che possono partecipare alle operazioni peritali al fine di realizzare il contraddittorio nella formazione della prova (art. 225 c.p.p.).

# Report

Parti essenziali:

- **Premessa**
  - *Curriculum del consulente*
  - **Oggetto dell'Incarico**
  - **Quesiti formulati**
  - *Breve descrizioni dei Fatti*
- **Fasi dell'Attività**
  - *Documenti e/o Evidenze forniti ed analizzati*
  - *Metodologia applicata*
  - **Strumenti (hardware e software) utilizzati**
  - **Descrizione dettagliata delle operazioni eseguite (anche foto e video)**
- **Risultati**
  - **Risposte ai quesiti**
  - **Conclusioni**
  - *Elenco Allegati*

# Esempio

Report di acquisizione

INDAGINI ONLINE

# Firma digitale

La firma che consente di scambiare in rete documenti con piena validità legale.

**CAD Art. 24. Firma digitale**

1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.
2. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.
3. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.

# Marca temporale

La Marca Temporale è un servizio che permette di associare data e ora certe e legalmente valide ad un documento informatico, consentendo quindi di associare una validazione temporale opponibile a terzi. (cfr. Art. 20, comma 3 CAD)

Il servizio di Marcatura Temporale può essere utilizzato anche su file non firmati digitalmente, garantendone una collocazione temporale certa e legalmente valida.

Sui documenti informatici sui quali è stata apposta una Firma Digitale, **la Marca Temporale attesta il preciso momento in cui il documento è stato creato, trasmesso o archiviato**.

# Esempio

Firma e marca temporale

INDAGINI ONLINE

# Esercizio

Redazione di un report

INDAGINI ONLINE

# Contatti

**info@vincenzocalabro.it**

**Linkedin vincenzocalabro**

INDAGINI ONLINE