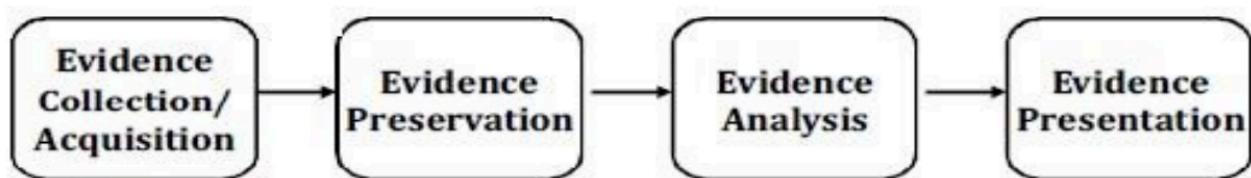


6. Digital Forensics

La **digital forensics** nasce inizialmente solo per trattare i crimini informatici più comuni come: Pedofilia online, frodi bancarie, phishing...

Definizione. Per **digital forensics** si intende la scienza di come **ottenere, preservare, analizzare e documentare** evidenze digitali da dispositivi elettronici.



Ad **oggi** l'analisi delle **evidenze digitali** è necessaria anche per crimini non direttamente legati alla tecnologia come omicidi e processi civili.

Evidenze digitali

Definizione. Per **digital evidence** si intende qualsiasi informazione con valore probatorio che viene immagazzinata o trasmessa sotto forma digitale.

Ad esempio, le evidenze digitali possono essere estratte da smartphone, tablet, traffico internet...

Questa tipologia di dati sono molto "fragili" in quanto facilmente soggetti a modifiche e ad accessibilità. Basta pensare al fatto che la connessione ad internet del dispositivo può già rappresentare un possibile punto d'accesso per chi vuole alterare i dati dall'esterno.

Le evidenze digitali possono dunque essere categorizzate in:

- **Volatile data:** Dati memorizzati in memoria volatile che vengono persi in seguito allo spegnimento del dispositivo (e.g., RAM, Comandi Shell...)
- **Non-Volatile data:** Dati memorizzati in memoria non volatile (e.g., Hard Disk, File, registri...)

Passi operativi

La fasi della **digital forensics** devono essere applicate mediante l'ausilio di **tools**, metodologie e strumenti per il corretto trattamento e acquisizione dei dati.

1- Preparazione e identificazione

La fase di **identificazione** viene fatta sulla scena de crimine seguendo le cosiddette **best practices**. Questa fase viene solitamente svolta sui seguenti dispositivi (lista non esaustiva):

- Personal Computers
- **hard Disk**: Dispositivo non volatile nel quale il **file system** determina come i file sono organizzati all'interno delle sue **partizioni**
- **SSD**: Dispositivo non volatile più efficiente e affidabile di un **hard disk**.
- Memory Card
- Chiavette USB
- Dispositivi di Rete (e.g., Router)
- ...

Sulla scena del crimine possiamo trovarci davanti a due situazioni:

- **Il dispositivo è spento**: In questo caso bisogna documentare con foto o disegni l'ambiente e lo stato del dispositivo in modo tale che se viene portato via esso possa essere "ricostruito" allo stesso modo (e.g., Tenere traccia della posizione dei cavi del Computer). Il dispositivo non deve essere mai acceso e batteria o cavo di alimentazioni devono essere rimossi preventivamente. Infine bisogna identificare sulla scena eventuali documenti che possono contenere informazioni utili come password o altre informazioni sul sistema.
- **Il dispositivo è acceso**: in questo caso bisogna documentare lo stato dell'ambiente e del dispositivo. Se necessario, è possibile raccogliere le informazioni **volatili** dal dispositivo (Live Forensics), registrando tutte le operazioni che vengono fatte. Se ciò non fosse possibile, il dispositivo deve esser spento togliendo direttamente la corrente/batteria dal dispositivo, evitando di chiudere i programmi. Infine le componenti devono essere catalogate e l'ambiente deve essere controllato per eventuali documenti contenenti password o altre informazioni utili.

Le evidenze digitali devono essere trattate con cura e ogni azione e persona che vi interagisce deve essere documentata. In caso di necessità di **trasporto**, devono essere scelti contenitori idonei per il dispositivo incriminato (e.g., Sacchetti anti-elettrostatici, suitcase...).

2- Acquisition and Retention

L'obiettivo è sempre quello di **preservare** l'originale e lavorare solo sulle copie.

L'acquisizione dei dati in modo sicuro e corretto può essere fatto a livello **hardware** o **software**.

Per operare a livello software è necessario assicurarsi che i dati nel dispositivo non vengano alterati da scritture esterne o interne da parte del sistema operativo. Per farlo bisogna assicurarsi di bloccare l'accesso in scrittura al supporto di memoria con software definiti **write blockers**.

L'**integrità di una copia** può essere verificata mediante la verifica **bit a bit**. Questo processo però risulta molto lungo e necessita del supporto originale per la verifica. Un'altra soluzione prevede l'utilizzo di **funzioni hash** (e.g., MD5, SHA-1, SHA-2) che rappresentano in modo univoco lo stato dei dati. Un'alterazione dei dati dunque influenzerà anche la funzione hash, dimostrando così la non validità dei dati.

3- Analisi

La fase di **analisi** rappresenta il momento centrale di un'indagine forense e varia in base alla natura del caso su cui si sta investigando. L'obiettivo principale è quello di esaminare in modo approfondito i dati raccolti per ottenere informazioni utili e rilevanti, cercando di ricostruire gli eventi e collegarli al dispositivo analizzato o all'utente responsabile.

Tra le attività più comuni svolte durante questa fase vi è l'identificazione dei **metadati**, che forniscono dettagli preziosi sull'utilizzo del dispositivo e sulle azioni eseguite. Ad esempio, i metadati dei file possono rivelare quando un documento è stato creato, modificato o copiato, permettendo di costruire una timeline delle attività. Inoltre, l'analisi dei file memorizzati, compresi quelli multimediali o di registro, aiuta a comprendere l'utilizzo generale del dispositivo e a individuare eventuali anomalie.

Un aspetto fondamentale dell'analisi è l'identificazione dell'attività dell'utente. Questo include il tracciamento delle operazioni eseguite sul dispositivo, come l'uso di applicazioni, la navigazione in rete o l'accesso a file specifici. Un'altra tecnica comune consiste nella ricerca di determinate **keyword**, che possono essere parole chiave rilevanti per il caso o frasi che suggeriscono attività sospette.

Un altro elemento critico è l'estrazione di informazioni relative al sistema operativo e alle applicazioni utilizzate. Questo tipo di analisi permette di comprendere il contesto del dispositivo, identificare possibili vulnerabilità sfruttate o verificare l'installazione di software malevolo. Inoltre, durante questa fase si presta particolare attenzione ai **dati cancellati**. Anche se un file è stato eliminato, potrebbe non essere ancora stato sovrascritto sul supporto di memoria e, quindi, può essere recuperato tramite strumenti forensi, fornendo informazioni cruciali.

Per eseguire queste analisi, sono disponibili numerosi strumenti, sia open source che proprietari. Questi software sono progettati per gestire le diverse esigenze dell'indagine,

dalla decodifica di file complessi al recupero di dati cancellati. La scelta dello strumento dipende dal tipo di analisi richiesta, dall'esperienza dell'operatore e dalle risorse disponibili.

In sintesi bisognano conoscere i **tool** e come applicarli nei diversi casi.

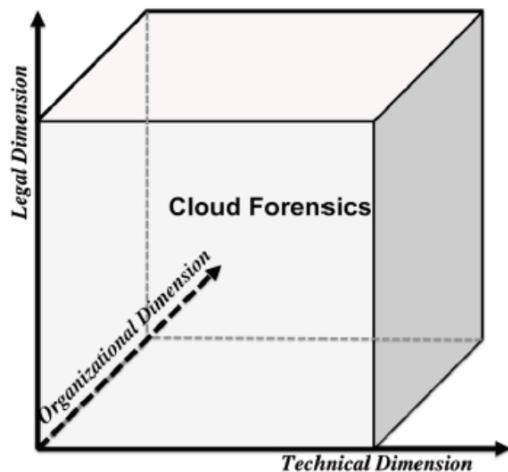
4- Evaluation and presentation

Le informazioni raccolte e i risultati devono essere presentati in un modo comprensibile per chi non ha esperienza o conoscenza del settore (e.g., Giudici, Avvocati...).

Semplicità e chiarezza, evitando di essere superficiali e approssimati.

Cloud Forensics

La **cloud forensics** si sviluppa lungo tre dimensioni principali: **tecnica, organizzativa e legale**.



Dal punto di vista **tecnico**, la cloud forensics si concentra sull'identificazione e acquisizione dei dati da fonti distribuite tra il cliente e il fornitore di servizi cloud. Ogni modello di servizio (IaaS, PaaS, SaaS) richiede strumenti e procedure personalizzate per la raccolta di dati, spesso eseguita in ambienti virtualizzati. La virtualizzazione complica l'individuazione dei server e la segregazione delle prove, richiedendo una combinazione di tecniche statiche, live e elastiche, garantendo al contempo l'integrità dei dati raccolti.

Dal punto di vista **organizzativo**, la collaborazione tra i diversi attori è fondamentale. Investigatori, amministratori di sistema, team di sicurezza e consulenti legali devono lavorare insieme per garantire che le evidenze vengano raccolte e trattate correttamente. I contratti e le policy organizzative, come gli SLA (Service Level Agreements), devono definire in modo chiaro ruoli, responsabilità e procedure di intervento.

Infine, la **dimensione legale** introduce complessità dovute alla multi-giurisdizione e alla multi-tenancy. La distribuzione geografica dei dati implica che le prove debbano essere raccolte rispettando le normative locali di ogni Paese coinvolto, evitando violazioni della privacy o conflitti normativi. La validità delle prove dipende inoltre dalla capacità di dimostrarne autenticità e integrità durante i procedimenti giudiziari.

Queste tre dimensioni lavorano insieme per garantire un'indagine forense efficace e conforme alle sfide tecnologiche e giuridiche del cloud.

In questo caso le **evidenze digitali** potranno essere trovate:

- **Server side** per sequestro di dati informatici presso fornitori di servizi.
- **Client Side** in quanto sono state ottenute le credenziali di accesso

Per definizione il cloud è considerato **anti-forense** in quanto rende difficile la raccolta di evidenze digitali.

Definizione. Per **anti-forense** si intende l'insieme di tecniche e metodologie in grado di rallentare o addirittura fermare la ricerca di evidenze digitali.