Università degli Studi di Salerno

Corso di Laurea Magistrale in Informatica

Appunti del corso

Digital Forensic

Tenuto da

Ugo Fiore

A cura di

Luigi Miranda

Anno Accademico 2023/2024

Indice

Keywords

- Ammissibilità delle prove
- Il dubbio
- Solidità investigazione e presentazione prove
- Riproducibilità del processo investigativo
- Documentazione rigorosa
- Copie esatte
- Integrità prove
- Chain of Custody o catena di custodia

Capitolo 1

Introduzione

Il mondo sta diventando sempre più interconnesso. Troviamo dispositivi connessi in quasi tutte le case e le reti informatiche sono il sistema nervoso delle organizzazioni aziendali e governative di tutto il mondo. Purtroppo per gli investigatori, Internet è stata progettata per la robustezza e la ridondanza, piuttosto che per la sicurezza e la tracciabilità. Questo aumenta la complessità e l'incertezza delle indagini digitali e rappresenta un'ardua sfida per gli informatici forensi. La digital forensics sta diventando sempre più importante con l'aumento del cybercrimine e di altri gravi reati informatici. Le prove digitali sono ovunque e svolgono un ruolo importante in quasi tutte le indagini penali come: piccoli reati, cybercrimine, crimine organizzato e anche il terrorismo. È quindi fondamentale che gli studenti di informatica e sicurezza acquisiscano una buona conoscenza della digital forensics, per poter agire come esperti in un contesto legale.

1.1 Forensic Science

Definition 1.1: Forensic Science

The application of scientific methods to establish factual answers to legal problems.

Le Forensic Science sono **l'applicazione di metodi scientifici che permettono di rispondere a problemi legali.** Uno scienziato forense deve stabilire il cosa, il come, il chi e il quando; e per offrire queste risposte utilizza tool e strumenti relativi a scienze teoriche e applicate. Tuttavia non è sempre possibile ottenere la certezza totale per queste

risposte e quindi uno scienziato forense a volte deve far ricorso a metodi statistici e probabilistici.

1.1.1 Principio di scambio di Locard

Edmond Locard ha formulato il famoso **Locard's Exchange Principle**, che è alla base degli studi delle scienze forensi. Il principio afferma che

> *"quando persone o oggetti entrano in contatto tra loro avviene un passaggio incrociato di materiale."*

Definition 1.2: Locard's Exchange Principle

Whenever two objects come into contact with one another, there is an exchange of materials between them.

Questo scambio di materiale è essenziale perché genera tracce e prove utili per la ricostruzione e l'identificazione di un crimine.

1.1.2 Ricostruzione del crimine

La ricostruzione della scena del crimine è il processo che determina le ipotesi e la sequenza degli eventi attraverso metodi scientifici.

Definition 1.3: Crime Reconstruction

Crime reconstruction is the determination of the actions and events surrounding the commission of a crime.

L'obiettivo della ricostruzione di un crimine è stabilire delle ipotesi e successivamente testarne la veridicità. Se un'ipotesi viene confermata allora può essere fornita una possibile spiegazione al crimine; altrimenti, se viene rifiutata, si passa a considerare le altre possibili ipotesi.

1.1.3 Investigazione

Il processo di investigazione è un'analisi sistematica con l'obiettivo di identificare i fatti chiave di un crimine attraverso comuni metodologie come le 5WH.

Definition 1.4: 5WH

5WH defines the objectives of an investigation as *who*, *where*, *what*, *when*, *why*, and *how*.

- Who: persone coinvolte, compresi sospettati, complici e vittime.
- Where: Le location rilevanti.
- What: Descrizione dei fatti accaduti.
- When: timeline degli eventi.
- Why: Le motivazioni e perché è successo in un dato momento.
- How: Come è stato commesso.

1.1.4 Evidence Dynamics

Definition 1.5: Evidence Dynamics

Evidence dynamics refers to any influence that adds, changes, relocates, obscures, contaminates, or obliterates evidence, regardless of intent.

In rari casi un investigatore o uno scienziato forense avranno l'opportunità di esaminare la scena del crimine nel suo stato originale, piuttosto andranno in contro a una dinamica delle prove. Le dinamiche delle prove consistono in qualsiasi azione, intenzionale o non, atta ad aggiungere, cambiare, oscurare, contaminare, eliminare le prove. Nel campo della digital forensic una dinamica potrebbe essere la cancellazione di un dato settore dell' HDD.

1.2 Digital Forensics

Definition 1.6: Digital Forensics

The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

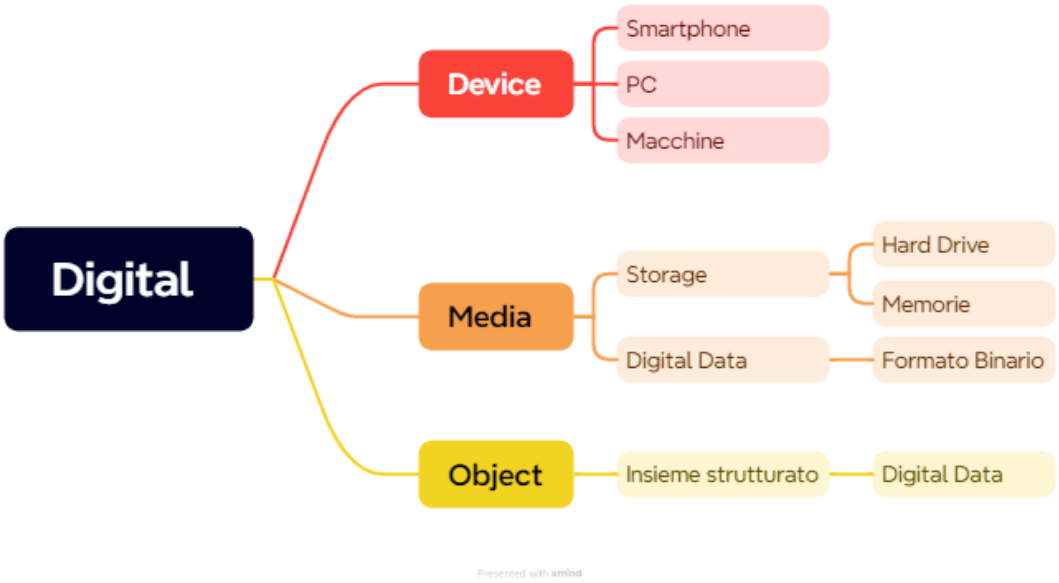
L'obiettivo solitamente è raccogliere dati(prove) per comprendere il comportamento umano, ma per interpretare le prove digitali il prerequisito è comprendere come i sistemi informatici si comportano e perché. È importante notare che le prove digitali possono essere volatili e facilmente manipolabili, quindi nella digital forensics è essenziale una conservazione affidabile delle prove. Inoltre dovendo rispondere a problemi legali è necessario garantire solidità e robustezza all'investigazione e la sua conclusione. La keyword per la raccolta, interpretazione e presentazioni delle prove in tribunale è l'**ammissibilità delle prove.**

1.2.1 Crimini e incidenti(sinistri)

La Digital Forensics è applicata sia in un contesto di diritto penale sia diritto civile. Per il diritto penale si parla di **crimini**; per il diritto civile si parla di **incidenti o sinistri.**

1.2.2 Digital Devices, Media, and Objects

I Digital Devices sono dispositivi fisici come un laptop, uno smartphone o una macchina. Questi contengono una memoria di archiviazione che prende il nome di Digital Media. I Digital Media contengono dati in formato binario che prendono il nome di Digital Data. Un insieme strutturato di Digital Data prende nome di Digital Object.


Digital
Device
Smartphone
PC
Macchine
Media
Storage
Hard Drive
Memorie
Digital Data
Formato Binario
Object
Insieme strutturato
Digital Data

1.2.3 Validità forense e principi fondamentali

Definition 1.7: Forensically Sound

An investigation is forensically sound if it adheres to established digital forensics principles, standards, and processes.

Un'indagine forense risulta valida se rispetta gli standard e principi consolidati. I due principi fondamentali di un'indagine forense sono: ***l'integrità delle prove (evidence integrity)*** *e* ***la catena di custodia (chain of custody).***

L'integrità delle prove si riferisce alla conservazione delle prove nella loro forma originale. Dato che garantire quest'integrità non è sempre possibile, è importante documentare scrupolosamente tutti gli step dell'investigazione, attraverso una catena di custodia. La catena di custodia si riferisce alla documentazione rigorosa dell'acquisizione, controllo, analisi e disposizione delle prove.

Definition 1.8: Evidence Integrity

Evidence integrity refers to the preservation of evidence in its original form.

Definition 1.9: Chain of Custody

Chain of custody refers to the documentation of acquisition, control, analysis, and disposition of physical and electronic evidence.

Nota bene Sarebbe utile evitare troppi passaggi di custodia e limitare l'accesso alle prove soprattutto da soggetti non autorizzati.

1.2.4 Ricostruzione del crimine nella Digital Forensics

Nella Digital Forensics la ricostruzione di un crimine si divide solitamente in 5 step:

- Analisi delle prove
- Classificare il ruolo di una prova come causa effetto di un evento

- Costruire gli eventi e testare la validità
- Combinare gli eventi per creare una catena
- Testare le ipotesi con metodi scientifici

1.3 Prove Digitali

Definition 1.10: Digital Evidence

Digital evidence is defined as any digital data that contains reliable information that can support or refute a hypothesis of an incident or crime.

È importante conservare le prove digitali in modo da preservarne l'integrità e l'ammissibilità in tribunale.

1.3.1 Metadata

I Metadata contengono informazioni riguardo i Data Object. Ad esempio i Metadata associato ad una fotografia può contenere informazioni sul modello di macchina fotografica, sulla data, il luogo e su chi ha scattato la foto. Analizzare con attenzione i Metadata può portare alla scoperta di informazioni chiave utili nella risoluzione di un processo di investigazione forense.