Digital Forensics e casi pratici

ORDINE AVVOCATI VELLETRI

SecurityBrokers
GLOBAL CYBER DEFENSE & SECURITY SERVICES

Chi sono

→Presentazione

- Ingegnere Informatico, specializzato in Computer Forensics & Digital Investigations.
- Membro della Commissione ICT dell'Ordine degli Ingegneri della Provincia di Latina.
- Socio CLUSIT.
- Socio IISFA (INFORMATION SYSTEM FORENSICS ASSOCIATION ITALIAN CHAPTER).
- CTU Albo Penale e Civile.
- Head of Digital Forensics Unit (Corporate), Security Brokers.
- CASD (Centro Alti Studi della Difesa) – CeMiSS - OSN (Osservatorio di Sicurezza Nazionale) – Membro del GDL CyberWorld.

Origini

Inizialmente la Digital Forensics è stata usata **solo per i crimini tecnologici (i «più comuni»)**.

- ✓ Intrusioni informatiche;
- ✓ Web defacement;
- ✓ Danneggiamento/Furto di dati;
- ✓ Pedofilia online;
- ✓ Azioni di Phishing/Whaling e/o Furto di Identità e Frode Bancaria.

Negli altri casi i computer sono stati *semplicemente ignorati* (e non solo quelli ☹

Alcuni casi “non informatici” risolti negli ultimi anni e di cui si è letto sui media nazionali:

- ✓ **Frode telefonica:** analisi di dispositivi “GSM-box”-like al fine di individuare il *Modus Operandi tecnologico* ed il *modello di business* criminale.
- ✓ **Spionaggio Industriale:** supporto ad azienda nella risoluzione e conseguenti azioni in Tribunale (furto di disegni e progetti industriali).
- ✓ **Antipedofilia digitale:** analisi di evidence elettroniche a supporto dell’AA.GG., verso PC e smartphone sequestrati all’indagato.

DF - Introduzione

- È quindi lampante come l'analisi delle evidenze digitali si rende **necessaria** anche per **crimini che nulla hanno a che fare con la tecnologia**.

- Dal **palmare della Lioce** al **delitto di Garlasco e di Avetrana**…sino agli **atti di bullismo e cyberstalking a mezzo Facebook,** ed altre cronache recenti

- Non sono stati portati all'attenzione del grande pubblico **molti altri casi**, risolti per merito delle evidenze digitali.

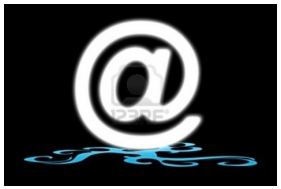
DF - Introduzione

- Adesso la Digital Forensics "**è di moda**"!!!

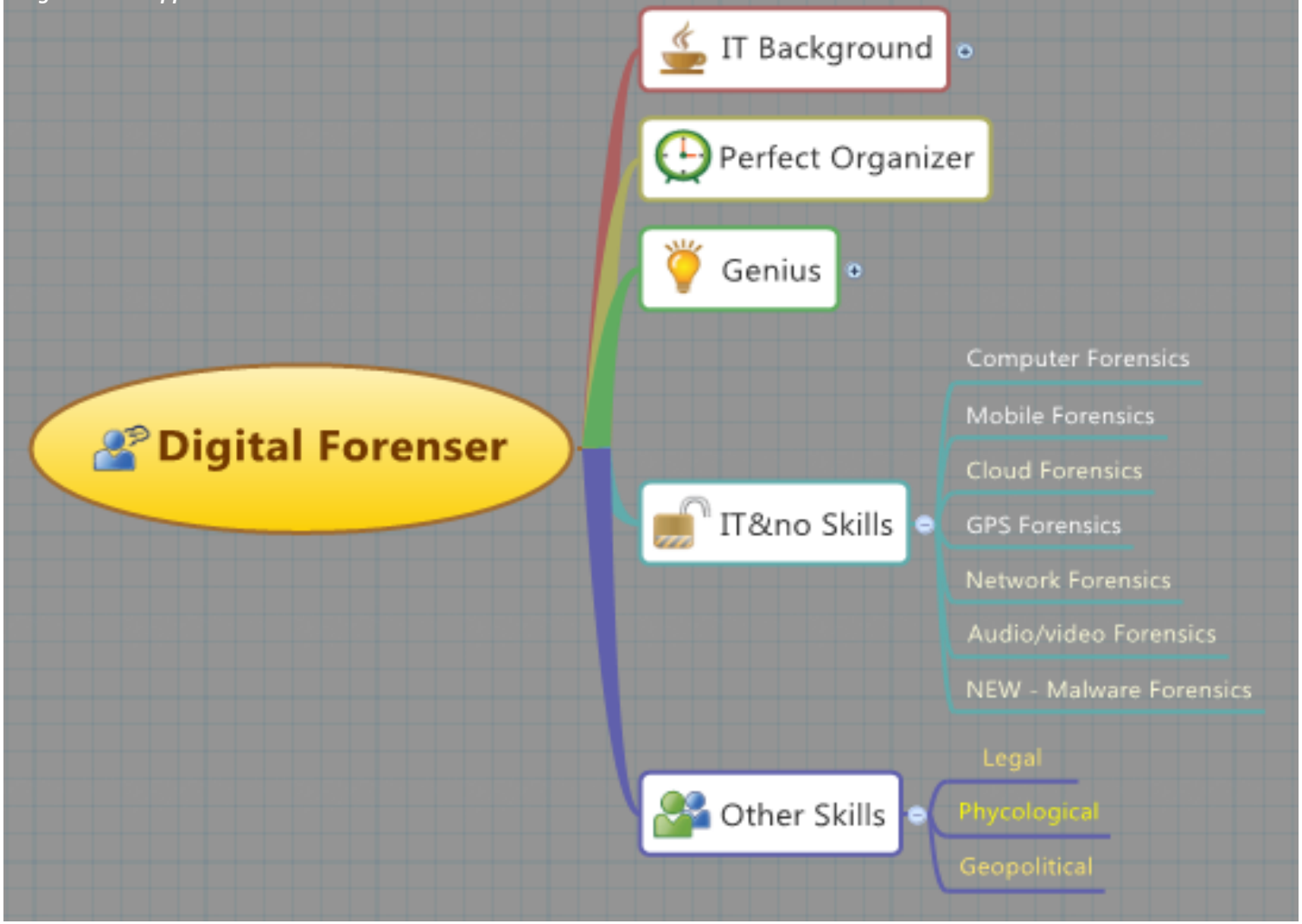
- Questo è **un bene** in quanto vi è:
  - **Maggiore scambio** di informazioni;
  - **Nuovi** tools e nuove tecnologie;
  - Un **più rapido sviluppo**;
  - Una **maggiore sensibilità** al problema.

- Questo è **un male** perché:
  - **Tutti vogliono lanciarsi** in questo mercato;
  - Ci sono **molti** "presunti esperti", **improvvisati** e molto **spesso privi dei necessari** skills, strumenti, laboratori ed esperienza sul campo;
  - Tutti **promettono tool** "facili da usare";
  - Il fatto di scrivere "forensics" su un programma di 10 anni fa **non lo rende necessariamente più adatto allo scopo…** ☹

DF - Introduzione

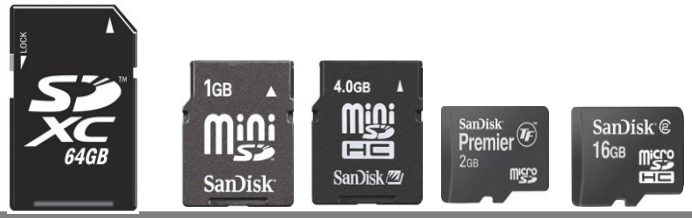


Ing. Selene Giupponi - 2014



La Digital Forensics

La **Digital Forensics** è la scienza che studia come **ottenere**, **preservare**, **analizzare** e **documentare** le evidenze digitali (prove) dai dispositivi elettronici come: Tablet PC, Server, PDA, fax machine, digital camera, iPod, Smartphone (Mobile Forensics) e tutti gli altri dispositivi di memorizzazione.



La Digital Forensics/1

- Una **digital evidence** può essere definita come **qualsiasi informazione avente valore probatorio che sia memorizzata o trasmessa in forma digitale**

- Una digital evidence può quindi essere estratta da:
  - Un **dispositivo di memorizzazione digitale**
    - Personal computer, notebook, hard disk esterno, floppy, nastro, CD/DVD, memory card, USB drive,…
    - **Telefoni cellulari, SIM, SmartPhone, Tablet, Navigatori satellitari**,…
  - Una **Rete Intranet/Internet**
    - Intercettazione di traffico dati
    - Pagine Web, Blog, Social Network, Chat/IM, P2P, ecc.

La Digital Forensics/2

- Una **digital evidence** è **fragile per natura**, ovvero facilmente modificabile

- Se il dispositivo che contiene le informazioni di interesse **viene spento**, i dati che non sono stati salvati possono andare definitivamente persi

- Se il dispositivo viene rivenuto spento, **l'accensione comporta modifiche al sistema e/o ai dati in esso contenuti**

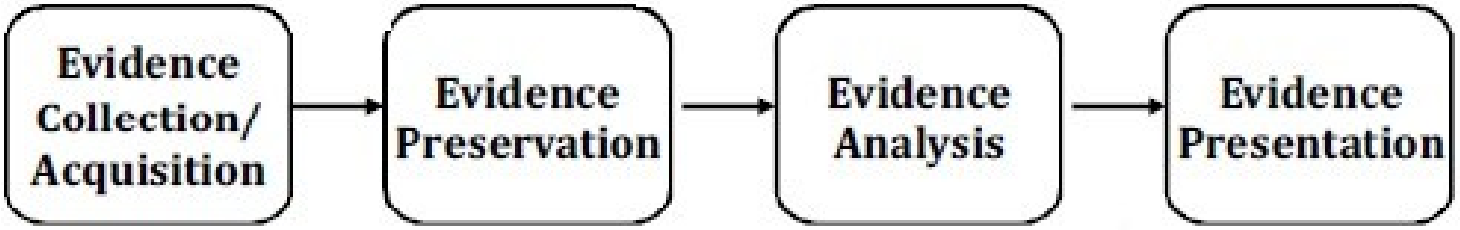
- Se il dispositivo è connesso ad Internet o ad una rete aziendale, **possono avvenire accessi dall'esterno con l'obiettivo di cancellare le informazioni**

- Se la digital evidence si trova su Internet (sito web, profilo di social network, ecc.), **può essere modificata e/o rimossa dall'owner della pagina**

La Digital Forensics/3

→Agenda - Classiche fasi della Computer Forensics

Fasi della Computer Forensics:



- **Identificazione**, **Collezione ed Acquisizione**;
- **Preservazione** (Chain of Custody);
- **Analisi**: estrazione delle informazioni significative per l'investigazione;
- **Evidence Presentation**: è la fase finale ma anche la più importante, nella quale anche i non addetti ai lavori riescono a capire il lavoro eseguito. È la redazione di un documento nel quale vengono analizzati passo passo tutti i risultati ottenuti ed estratti dalle digital evidence.

La Digital Forensics/5

→Agenda - Analisi Post Mortem e Analisi Live

Digital Forensics

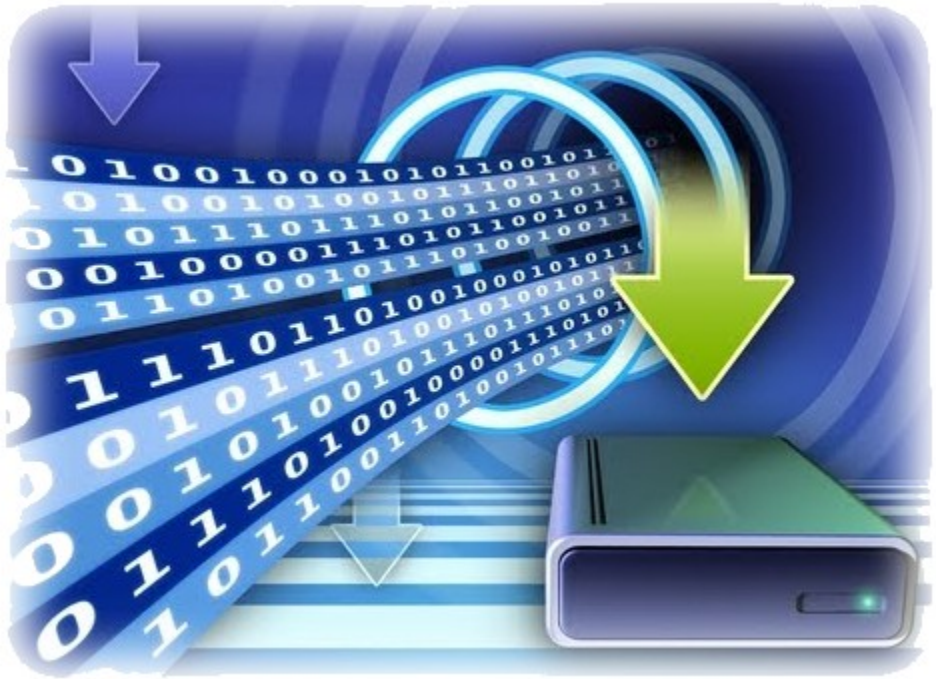
Dead Analysis

Live Analysis

Il dato

Il dato digitale, **per sua natura immateriale**, può essere tipicamente ritrovato sul campo in **tre diverse modalità**:

1. Sequestrato
2. Copiato
3. Intercettato



Qualunque altra situazione può essere **ricondotta a una di queste tre**.

Casi reali

Casi Reali – Digital e Mobile Forensics

Caso #1

Scenario: infedeltà matrimoniale

Azione: Il soggetto 'A' che crittografa con FileVault il computer di proprietà dell'azienda del coniuge ('soggetto B') per non far trapelare immagini, video e chat.

Effetto: Il soggetto B non dispone più dei suoi dati aziendali poiché il soggetto A ha utilizzato il sistema di cifratura citato in precedenza.

Caso #2

Scenario: Stalking

Azione: viene installato uno spy tool nello smartphone per vedere tutti gli spostamenti di un soggetto, leggere mail, messaggi, chiamate effettuate e ricevute.

Effetto: alcuni spy tools sono invisibili e prima che il soggetto se ne accorga possono passare anche mesi.

Caso #3

Scenario: Minacce

Azione: soggetto X minaccia su un blog o un sito web un soggetto Y di pubblica autorità.

Effetto: Primo step - **denuncia contro ignoti poiché il reato è avvenuto nel cyberspazio.**

Caso #4

Scenario: Spaccio

Azione: comunicazione tra lo spacciatore e i suoi clienti che avveniva tramite la chat di un gioco della playstation.

Effetto: è venuto il lampo di genio di sequestrare il dispositivo di gioco ed analizzarlo.

Casi Reali – Mobile Forensics

- **CASO A**: Un consulente recupera un **Palmare Palm V** durante un sequestro. **Lo consegna al PM** per farlo **analizzare un mese dopo**.

- Peccato... **la batteria si è scaricata e i dati sono stati persi**.

- ✓ Qui la **conservazione**: uno dei **punti principali** sulla conservazione del reperto nel campo mobile forensics è proprio il **dover mantenere alimentato il dispositivo** (in base alla situazione, questa lo richiedeva).

***

- **CASO B**: Durante una perquisizione, viene **sequestrato e repertato un palmare**;

- **Non viene** né spento, né isolato;

- Durante la perquisizione, l'indagato si è premunito **di cancellare i dati via Wi-Fi**.

- ✓ Altro punto della mobile forensics… **isolamento** (jammer o altre soluzioni).

Casi Reali – Mobile Forensics

- Il cellulare è oggi lo strumento più **personale** ed "intimo" che ci sia, ed è sempre addosso alla persona.

- …In un corso di formazione lo scorso 3 Aprile alla base NATO di Oberammergau in Germania, ho chiesto:
  - ✓ **"Who could lend me his phone to be analyzed?"**
  - ✓ **"Use your own" has been the global answer ☺**

Insider in una Banca : lei/lui hanno effettuato la cancellazione di record importanti all'interno del sistema. Il direttore della banca ci ha chiamato immediatamente dopo la chiusura per trovare il colpevole e recuperare i record cancellati.

Cosa ha fatto l'insider?

La nostra analisi ha rivelato:

- L'insider era una donna…..
- Ha cancellato 5 records riguardanti debiti di clienti sul sistema
- Ha preso dei soldi da questi clienti

Ogniqualvolta abbiamo un insider, sappiamo che esso/essa opera per grandi quantità di **denaro**, o per **insoddisfazione** personale, oppure perché ha dei **litigi interni** (colleghi, capo, etc…)

Conclusioni

- La Digital Forensics è oramai una **realtà quotidiana:** bisogna approfittarne per cogliere **nuove occasioni** e **restare aggiornati**.

- Infatti, quello che forse "manca" è una totale *presa di coscienza* da parte **di tutti** (soprattutto le figure legali): serve "masticare" un pò i **termini tecnici** e conoscere le **procedure operative** e gli **standard.**

- Mi auguro che questo intervento **vi sia stato utile** in tal senso!

- Nel caso di **dubbi**, prima di procedere è bene **sentire il parere** degli **esperti** di Digital Forensics.

Conclusioni

Ed, in merito agli “esperti”, **alcuni consigli**:

- ✓ Affidarsi a professionisti di **comprovata e documentata esperienza**, evitando gli “improvvisati” e “quelli dell’ultima ora”;
- ✓ Non richiedere all’esperto informatico ciò che **non è tecnicamente possibile**;
- ✓ Non chiedere di “**fabbricare prove**”;
- ✓ Richiedere il **possesso di** certificazioni di settore, nazionali ed internazionali, e l’**appartenenza ad Associazioni** di Categoria (CLUSIT, IISFA, etc.).

Conclusioni e Consigli ☺

- ***Ad oggi ci fidiamo ancora "troppo" degli altri;***
- ***Oggigiorno chi ha l'informazione ha il potere, proteggiamo i nostri dati.***
- **Non consideriamo d'oro le nostre informazioni*;***
- ***A volte non è possibile recuperare tutto dal punto di vista forense come ci fa vedere CSI ☺***

Thanks for your attention!

sg@security-brokers.com

SecurityBrokers
GLOBAL CYBER DEFENSE & SECURITY SERVICES

www.security-brokers.com