SecurityBrokers
GLOBAL CYBER DEFENSE & SECURITY SERVICES

Frodi su mainframes: Digital Forensics su AS/400, un caso reale

Ing. Selene Giupponi
HTCC – High Tech Crime Consortium

Chi sono

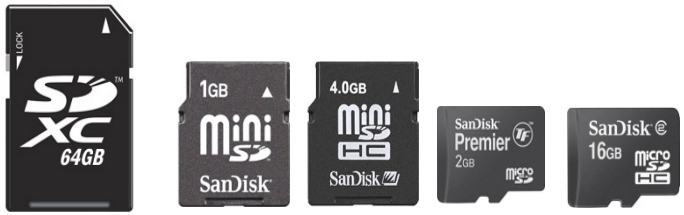
- Ingegnere Informatico, specializzato in Computer Forensics & Digital Investigations.
- Membro della Commissione ICT dell'Ordine degli Ingegneri della Provincia di Latina.
- Socio CLUSIT.
- Socio IISFA (INFORMATION SYSTEM FORENSICS ASSOCIATION ITALIAN CHAPTER).
- CTU Albo Penale e Civile del Tribunale di Latina.
- Head of Digital Forensics Unit (Corporate), Security Brokers ScpA.
- Advisor European Courage Focus Group – Cyber Terrorism & CyberCrime – EOS Member Board
- ITU ROSTER OF EXPERTS
- HTCC HIGH TECH CRIME CONSORTIUM - https://www.hightechcrimecops.org/

Agenda

- Introduzione
- Digital Forensics in Ambiente Finanziario: why?
- AS/400 (IBM iSeries) Forensics
- Tool in R&D
- Conclusioni

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 di



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 ☹

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**

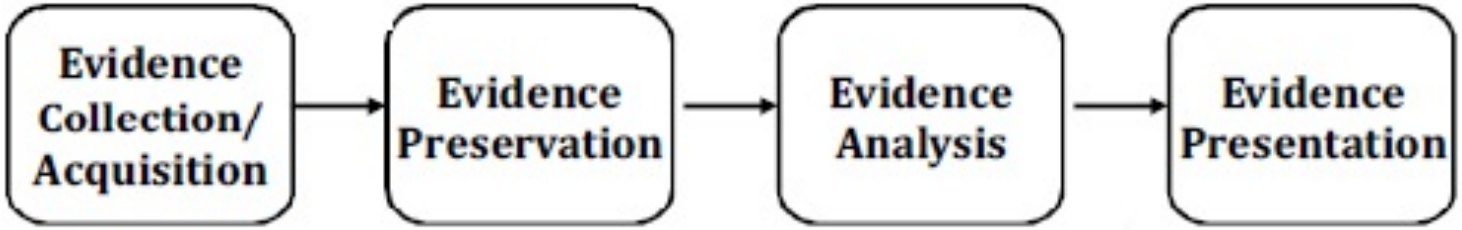
- Se il dispositivo è connesso ad Internet o ad una rete aziendale, **possono avvenire accessi dall'esterno con l'obiettivo di cancellare le informazioni**

- 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.

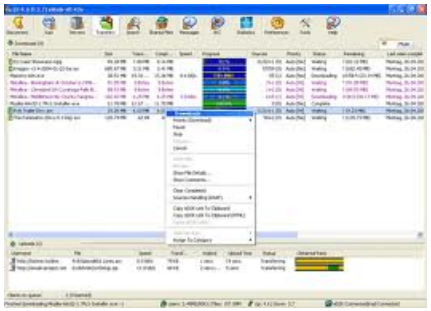
La Digital Forensics/4

→Agenda - Analisi Post Mortem e Analisi Live

Digital Forensics

Dead Analysis

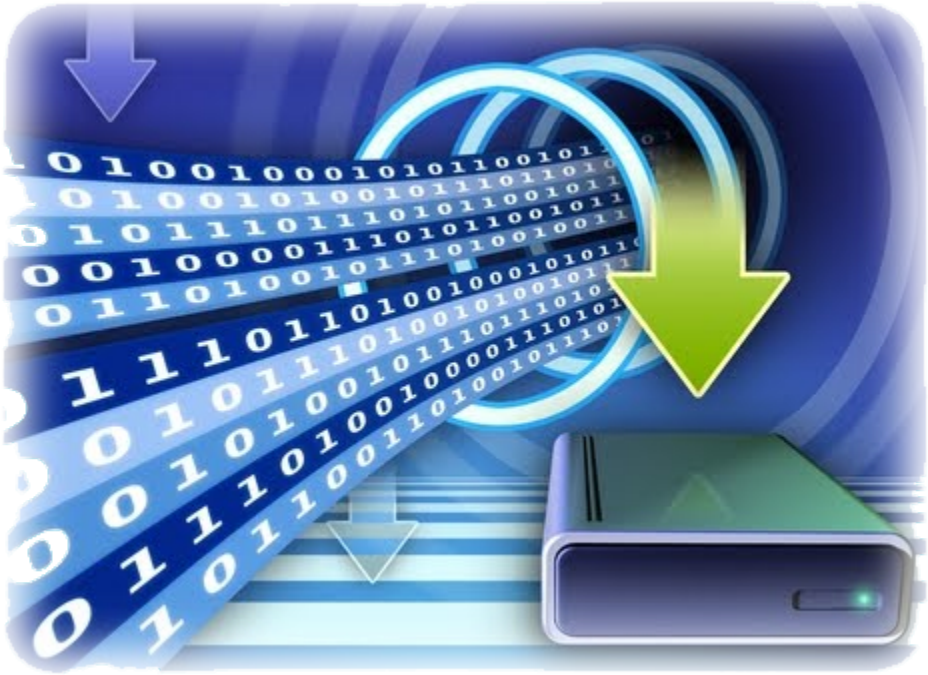
Live Analysis



Il dato

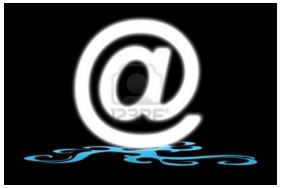
Il dato digitale, **per sua natura immateriale**, può essere tipicamente ritrovato sul campo in **tre diverse modalità**:

1. Sequestrato
2. Copiato
3. Intercettato

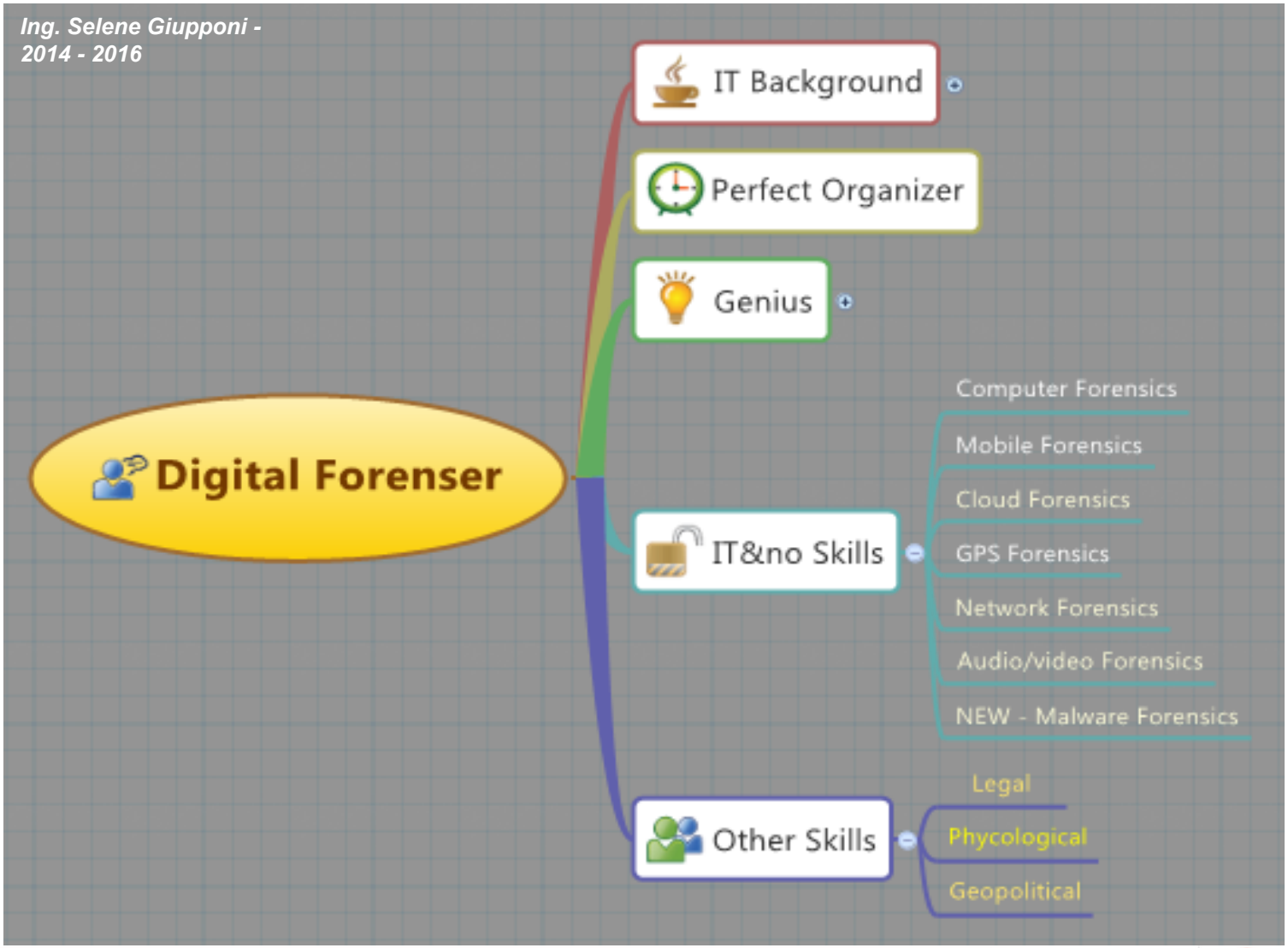


Qualunque altra situazione può essere **ricondotta a una di queste tre**.

DF - Introduzione



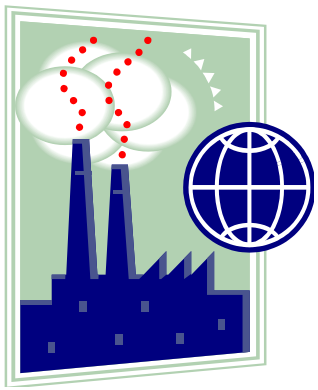
Ing. Selene Giupponi - 2014 - 2016



Chi utilizza ad oggi IBM iSeries Systems?

- Banche
- Small, Medium & Large Enterprise (Logistics & Transportation, Fashion&Luxury, Food chains, etc….)
- Accounting Firms

…….. As/400 anche in qualche aeroporto……



Entering AS/400 Forensics

A long time ago, when I was 2 years old, I had a computer that every morning used to tell me: «Good morning Selene…..» ☺

Entering AS/400 Forensics/1

Perchè ho iniziato questo progetto?

- Alcune Forze dell'Ordine mi hanno chiesto come si poteva fare per il sequestro e il recupero di dati cancellati.
- Un semplice Digital Forensics expert non è in grado di eseguire una analisi forense su dispositive iSeries;
- Ognuno ha expertise differenti.

Recuperare dati cancellati

Ho condiviso con mio padre che si occupa di AS/400

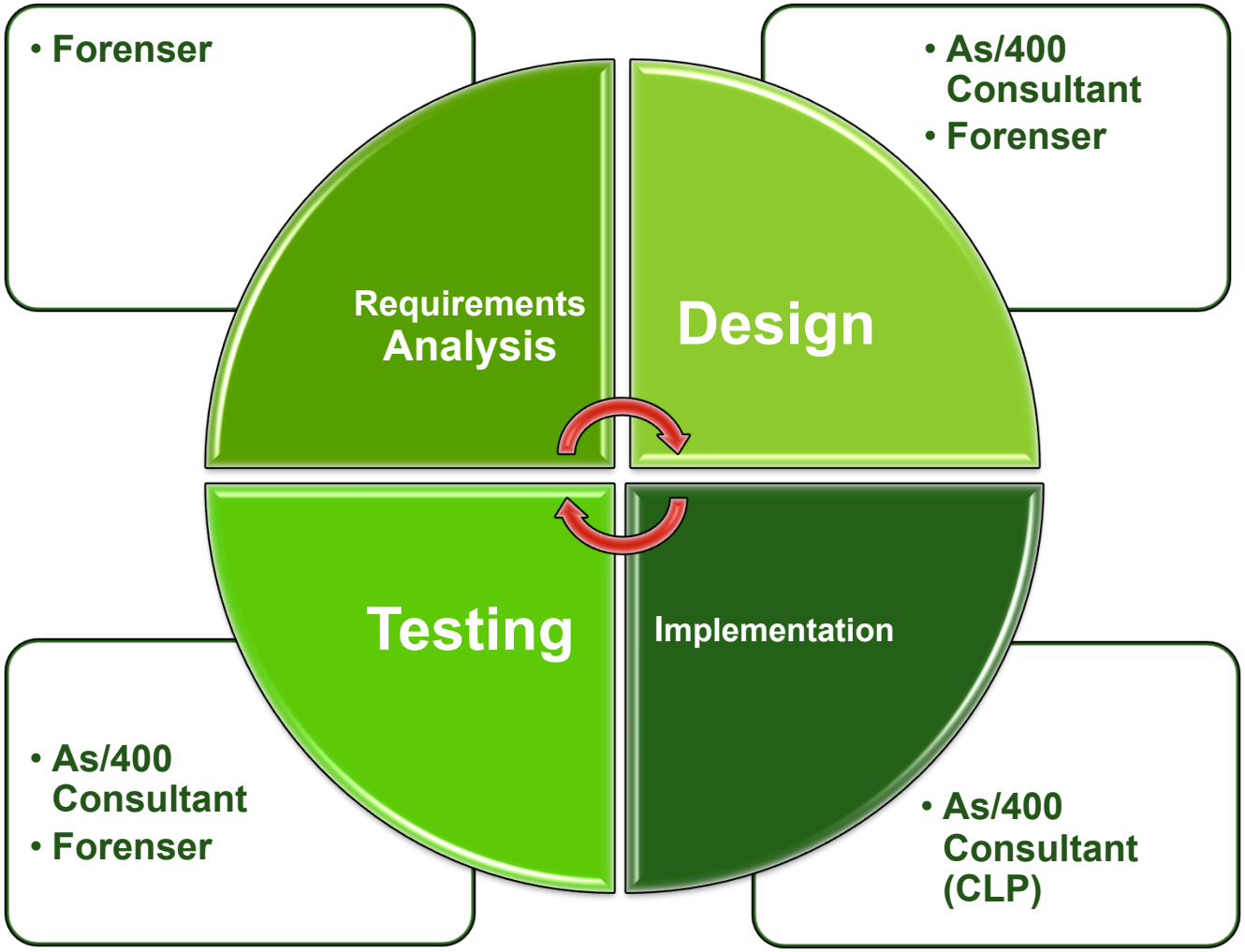
- Siamo stati in grado di implementare un software che è in grado di recuperare dati cancellati da sistemi IBM iSeries

```
UFMAP30                MAPPING FILE MAINTENANCE          23.01.01 15:59:39

  AS400 Database File: CPTRAN                          FTP File: FTPTRAN

Seq AS400 Fld  Description                                Typ Len D From
No.  Name                                                          FldNo
  1 CT0010     COUNTRY-CODE                                P   2     1
  2 CT0020     BRANCH CODE                                 P   2     2
  3 CT0030     VENDOR CODE                                 P
  4 CT0040     VENDOR PGM-NO                               P
  5 CT0050     VENDOR POOL-NO                              P
  6 CT0060     TRANSACTION-NO                              P
  7 CT0061     STATUS CODE                                 P
  8 CT0080     CRL-NUMBER LESSEE                           P
  9 CT0110     TRANSACTION FILE STATUS                     A
 10 CT0111     RENTAL STR. FILE STATUS                     A
 11 CT0112     DOCUMENT FILE STATUS                        A
 12 CT0113     EQUIPMENT FILE STATUS                       A
 13 CT0114     PROPOSAL FILE STATUS                        A
 14 CT0115     TRANSACTION FILE ERROR-KZ                   A
 15 CT0116     RENTAL STR. FILE ERROR-KZ                   A

 F3=Exit          F6=Update Mappings          F9=Assign sequential
```

```
                    Scelta Lingua                TEXT05
Immetti una scelta e premi INVIO
  1. Italiano       5. Spagnolo
  2. Inglese        6. Portoghese
  3. Tedesco        7. Arabo
  4. Francese       8. ....
                    9. ....

  F3=Fine      Scelta o Fx ===>  1
```

FASI

S
D
L
C


• Forenser
• As/400 Consultant
• Forenser
Requirements Analysis
Design
Testing
Implementation
• As/400 Consultant
• Forenser
• As/400 Consultant (CLP)

Real Case Study

Insider in una Banca : lui/lei hanno cancellato dei record importanti dal sistema, nascondendo le loro tracce. Il team Security della Banca ci ha chiamato immediatamente (when the bank was close) per trovare l'insider e recuperare i dati cancellati.

Real Case Study

Cosa ha fatto l'Insider

La nostra analisi ha scoperto:

- L'insider era una donna…..
- Ha cancellato 5 record dal sistema
- Ha preso denaro per conto di un cliente nascondendo le tracce
- Ogni volta che accadono tali reati l'insider opera per quantità di denaro sostanziose.

La situazione ad oggi

- Collaboriamo con Tribunali e Procure italiane, per Clienti Bancari a livello Italiano e Internazionale.
- Non vendiamo questo software – at least at the moment ☺
- Il Software è implementato solamente per ambiente iSeries.

DF - Conclusione

- 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…** ☹

Ing. Selene Giupponi
Vice President & Head of Digital Forensics Unit
HTCC – High Tech Crime Consortium

sg@security-brokers.com

SecurityBrokers
GLOBAL CYBER DEFENSE & SECURITY SERVICES

Security Brokers scpa
Via Appia Nuova, 113 - 00183 Rome Italy
Email: info@security-brokers.com - Website: http://www.security-brokers.com