

## Computer forensics

Per computer forensics s'intende l'applicazione di un metodo investigativo di tipo scientifico ai media digitali, al fine di evidenziare fatti oggettivi, come informazioni o elementi di prova, da sottoporre a giudizio in sede processuale. Negli scenari contemporanei, in cui la tecnologia ha un ruolo pervasivo nella vita quotidiana, la necessità di figure professionali altamente specializzate in questa complessa disciplina informatica assume sempre maggiore importanza.

**A chi è indirizzato il corso:** tecnici della sicurezza informatica; Consulenti Tecnici e Periti dell'Autorità Giudiziaria o aspiranti tali; Forze di Polizia impegnate sui cyber crime.

**Requisiti per la frequentazione:** conoscenze di base di sistemi Windows e Linux e del funzionamento delle reti.

### I Docenti:

**Andrea Ghirardini** è uno dei precursori della Computer Forensics in Italia. Certificato CISSP e socio CLUSIT, presta consulenza a Forze dell'Ordine e ad organizzazioni private. Fino ad oggi ha partecipato ad oltre 250 indagini che spaziano dalla violazione informatica al narcotraffico, dall'eversione alle frodi fiscali.

**Davide Gabrini** non ha tenuto il conto delle indagini a cui ha partecipato, ma nell'ultimo decennio si è comunque guadagnato da vivere grazie ai reati informatici altrui, occupandosi del contrasto ai crimini informatici in senso proprio, alla pedopornografia (anche tramite operazioni sotto copertura) e al terrorismo, prendendo parte ad importanti indagini di rilievo nazionale. Attualmente lavora per la Polizia Postale di Milano e si occupa prevalentemente di ricerca e sviluppo, computer forensics e formazione del personale.

**Materiale didattico:** a tutti i frequentatori sarà fornita una copia del libro "Computer Forensics", di A. Ghirardini e G. Faggioli, ed. Apogeo.

### Programma delle lezioni:

#### 1 Lezione 1 (4 ore)

- Introduzione del corso
- Cos'è la Computer Forensics: definizioni e applicazioni
- Disciplina giuridica
- Filosofia di base e Best practices
- Catena di custodia
- Impostazioni operative
- Identificazione e marcatura dei supporti e dei media non convenzionali

#### 2 Lezione 2 (4 ore)

- Preservazione del dato: il sequestro e l'acquisizione
- Acquisizione di memorie di massa
  - Concetto di copia forense
  - Verifica d'integrità
  - Tecnologie più frequenti
  - Blocker hardware
  - Strumenti software

- Acquisizione di memorie volatili

### 3 Lezione 3 (4 ore)

- Preservazione del dato: le intercettazioni
  - Disciplina giuridica
  - Problemi tecnici
- Applicazioni in reti ethernet
  - Problematiche delle tecniche di Man-in-the-middle
  - Software utili
- Applicazioni in reti wireless
  - Dotazione HW e SW
  - Problemi derivanti dall'uso di crittografia
- Analisi del traffico intercettato

### 4 Lezione 4 (4 ore)

- Analisi e valutazione delle digital evidence
- Strumentazione hardware e software
- Descrizione dei software commerciali e open source
- Distribuzioni live Linux
- Visualizzatori, player e codec
  - Analisi dei documenti (formati più diffusi) e dei loro metadati
  - Analisi delle immagini: metadati e individuazione delle manipolazioni
- Dimostrazioni ed esercitazioni pratiche

### 5 Lezione 5 (4 ore)

- Partizioni e Filesystem più diffusi
  - FAT, NTFS, EXT, HFS ecc.
  - Cluster, allocazione e slack space
- Utilizzo di Virtual Machine
- Problematiche sull'aggiornamento delle password

### 6 Lezione 6 (4 ore)

- Analisi dei sistemi Windows, Mac e Unix-like. Per ogni sistema:
  - File di log
  - File di configurazione / registro di sistema
  - Informazioni sull'utilizzo (history, file recenti, ecc.)
  - Dati applicativi (browser, client di posta, cartelle temporanee, ecc.)

### 7 Lezione 7 (4 ore)

- Recupero dati
  - Ripristino dei dati cancellati tramite analisi del filesystem
  - File carving
- Analisi delle aree di swap e dei file di ibernazione

- Individuazione e analisi del malware
- Software utili, dimostrazioni ed esercitazioni pratiche

#### Lezione 8 (4 ore)

- Tecniche di antifoensic e loro contenimento
  - Tecniche di distruzione dei dati
  - Tecniche di occultamento
  - Tecniche di falsificazione delle digital evidence
  - Altre tecniche di elusione
- Contromisure e mitigazione delle tecniche discusse
- Fasi finali: la presentazione dei risultati dell'indagine
- Necessità e opportunità per l'aggiornamento professionale in materia di Computer Forensic