Corso Computer Forensics

Durata: 4 giorni

A chi è rivolto: Tecnici, Sistemisti, Responsabili IT, Giornalisti, Liberi Professionisti, Avvocati, Forze dell'Ordine, Militari, Security Manager

Scopo del corso: Il corso è pensato per quei professionisti del settore informatico e legale che siano interessati ad approfondire le proprie conoscenze nell'ambito delle procedure tecnologiche e delle best pratics forensi. Verranno illustrati e utilizzati i software applicativi più diffusi ed utilizzati, seguendo le linee guida delle più eminenti associazioni professionali.

Le tematiche della Digital Forensics saranno affrontate da un punto di vista procedurale, in modo da creare la "mentalità" forense per poter analizzare gli aspetti legali legati a queste nuove tipologie di prove. L'obiettivo finale è quello di formare le basi di una figura professionale che sia in grado di operare nel campo dell'investigazione, dell'analisi dei risultati e della produzione di evidenze digitali.

Prerequistiti: Buona base del sistema operativo Windows e\o Linux, conoscenza delle tecnologie di rete locale e geografica

Principali Argomenti trattati

Giorno 1

- Introduzione alle problematiche di computer forensics
- Le fasi dell'accertamento forense su dati digitali
- Princìpi, preparazione, precauzioni e utilizzo dei sistemi live
- Introduzione al sistema DEFT e DART
- Utilizzo di DEFT con i principali OS e filesystem
- Tipologie di acquisizione forense e formati
- Attività di preview e triage sicuro con DEFT
- Acquisizione di memorie di massa
- Acquisizione di memoria volatile
- Cenni su acquisizione di smartphone

Giorno 2

- Verifica e apertura delle immagini forensi
- Virtualizzazione delle immagini
- Recupero dei dati cancellati
- Analisi dei metadati
- Ricostruzione delle attività tramite timeline e supertimeline
- Rilevamento di compromissioni
- Analisi delle periferiche USB utilizzate
- Analisi dei documenti aperti e utilizzati
- Estrazione di evidenze tramite Bulk Extractor e Autopsy

Giorno 3

- Riepilogo su metodologie e strumenti di acquisizione
- Acquisizione di memorie di massa via rete
- Acquisizione di dispositivi iOS
- Acquisizione di dispositivi Android
- Analisi di file pList e database SQLite

Giorno 4

- Introduzione a DART
- Panoramica degli strumenti presenti in DART
- Utilizzo di DART in DEFT
- Incident response
- Cracking di password e creazione di dizionari
- Network forensics
- Gestione di un incidente informatico
- Riepilogo degli argomenti

Ogni argomento verrà trattato avvalendosi di esercitazioni pratiche