

Oggetto: Programma didattico

Corso pensato per professionisti del settore dell'informazione interessati ad approfondire le proprie conoscenze sulle procedure teoriche e pratiche di Informatica Forense. Saranno oggetto del corso gli aspetti relativi all'identificazione, al repertaggio corretto delle fonti di prova, all'analisi ed alla presentazione delle conclusioni. Parte pratica di laboratorio, basata sul software Open Source.

Il target

L'obbiettivo del corso è quello di fornire delle solide fondamenta per intraprendere attività nel mondo dell'investigazione digitale, materia in continua trasformazione e divenire.

Requisiti

Buona conoscenza del sistema operativo Windows, basi di Linux e dei concetti base sui File System.

TITOLO: Introduzione alla computer forensics

Durata: 8 ore.

Computer Forensics – Teoria e Pratica.

1. Panoramica sulle Best Practices
 - 1.1 - non modificare la prova
 - 1.2 - analisi live e post (i perchè, pro e contro)
 - 1.3 - identità della prova
 - 1.3.1 - hash, cosa sono.
 - 1.3.2 - catena custodia, nella teoria e nella realtà
 - 1.3.3 - ripetibilità delle operazioni
 2. Gli strumenti della C.F. - open source vs commerciale
 3. Le quattro fasi (Identificazione, acquisizione, analisi, reporting) in pratica.
 4. GNU/Linux per la C.F. (uso della distro C.A.I.N.E. <http://www.caine-live.net>)
 5. Le cartelle cliniche: risvolti ed aspetti tecnici.
-
5. LABORATORIO
 - 5.1 - esempio d'analisi live ed uso dei tools
 - 5.2 - esempio attività su pc spento
 - 5.3 - preview & acquisizione (imaging)
 - 5.4 - attività d'analisi con i tools a disposizione