Informatica Forense (Computer Forensics): aspetti pratici

Il corso affronta, con un approccio orientato alla sperimentazione, la scienza che studia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione e ogni altra forma di trattamento del dato informatico al fine di essere valutato in sede processuale.Al termine del corso si acquisiranno le competenze necessarie al "computer forensic expert" ovvero la figura professionale che presta la sua opera nell'ambito dei reati informatici o del computer crime con lo scopo di "preservare, identificare, studiare ed analizzare i contenuti memorizzati all'interno di qualsiasi supporto o dispositivo di memorizzazione". Le attività sono dirette non solo a tutte le categorie di computer, ma a qualsiasi attrezzatura elettronica con potenzialità di memorizzazione dei dati (ad esempio, cellulari, smartphone, sistemi di domotica, autoveicoli e tutto ciò che contiene dati memorizzati.

Agenda (3 giorni)

Individuazione:

Conservazione e Protezione:

il computer forensic expert deve garantire il massimo impegno per conservare l'integrità della prova informatica. Il dato originale non deve essere modificato e danneggiato e quindi si procede realizzandone una copia (bit-a-bit), su cui il computer forensic expert compie l'analisi. Dopo aver effettuato la copia è necessario verificarne la consistenza rispetto al dato originale: per questo motivo si firmano digitalmente il dato originale e la copia, che devono coincidere.
esercitazioni in laboratorio su: dd, ddrescue, md5sum, autopsy (calcolo hash e analisi di device).

Estrazione:

è il processo attraverso il quale il computer forensic expert, servendosi di diverse tecniche e della sua esperienza, trova la posizione del dato informatico ricercato e lo estrae. Verrà fatta una panoramica sui forensics tool Helix, CAINE ed Encase
esercitazioni in laboratorio su: recupero file cancellati, ricerche su file e settori allocati/non allocati, creazione ed interpretazione della timeline, analisi di pagefile.sys/hiberfile.sys/NTUSER.DAT, funzionamento di Emule, utilizzo dell'analizzatore di protocolli di rete Wireshark.

Documentazione:

l'intero lavoro del digital forenser deve essere costantemente documentato, a partire dall'inizio dell'investigazione fino al termine del processo. La documentazione prodotta comprende, oltre alla catena di custodia, un'analisi dei dati rinvenuti e del processo seguito. Un'accurata documentazione è di fondamentale importanza per minimizzare le obiezioni e spiegare come ripetere l'estrazione con un analogo processo sulla copia.

Obiettivi

Al termine del corso i partecipanti sono in grado di investigare (individuare, estrarre) mediante utilizzo di strumenti open source e documentare con precisione il processo seguito ed i risultati ottenuti.

Destinatari e Prerequisiti

A chi è rivolto

Tecnici informatici, Ingegneri informatici, CTP/CTU, membri delle Forze dell'Ordine e cultori della materia.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: sistema operativo linux, principi di base di networking.

Iscrizione

Quota di Iscrizione: 1.790,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:

10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com