[t]esla
consulting

Corso di alta formazione in Digital Forensics

Il corso di alta formazione in Digital Forensics, basato sugli standard ISO/IEC 27037:2012 e le best practice del NIST, è pensato per rispondere alle sempre più frequenti esigenze formative di istruire tecnici professionisti esperti di Digital Forensics in grado di analizzare il dato salvato all'interno di una memoria informatica, il tutto senza esser troppo legati ad una soluzione software ben precisa.
Il corso prevede un 40% di approccio teorico e un 60% di approccio pratico operativo, per un totale di 4 giorni di alta formazione.

Prerequisiti

Ciascun partecipante dovrà dotarsi di

- Computer portatile con Windows 7 o superiore a 64 bit (oppure Mac OSX o Linux), 4 GB di memoria RAM e 50 GB di spazio disco liberi
- VMware Player o Fusion

ed avere conoscenze basilari dei sistemi operativi e della shell Linux.

Programma del corso

Giorno 1:

- Introduzione alle problematiche di Computer Forensics
- La Digital Forensics nell'accertamento civilistico
- La convenzione di Budapest e le modifiche al codice di procedura penale
- Le 6 fasi operative di un accertamento tecnico
- Introduzione al sistema DEFT
- Preparazione della macchina di analisi e del laboratorio
- Laboratorio di acquisizione di memorie di massa
- Panoramica sull'acquisizione di memorie di massa di cellulari e smarthphone.
- Approfondimenti sui principali file system: FAT*, NTFS, HFS e HFS+, EXT2/3/4, etc
- Riferimenti temporali e time line dei sistemi

Giorno 2:

- Laboratorio di analisi delle timeline utilizzando Splunk e Autopsy
- Sistemi raid e problematiche di acquisizione
- Recupero dati - File carving
- Laboratorio di recupero dati su diversi sistemi
- Architettura dei sistemi operativi Microsoft Windows - Artefatti per l'analisi forense
- Architettura dei sistemi Mac OS X - Artefatti per l'analisi forense
- Architettura dei sistemi Linux - Artefatti per l'analisi forense
- Individuazione delle informazioni di interesse
- Charcode e gli standard internazionali
- Bash script per la Computer Forensics

Giorno 3:

- Indicizzazione e preparazione dei contenuti con interfacce utente per analisti non tecnici
- Introduzione a DART per le "live forensics"
- Utilizzo di Bulk extractor
- Modello di documentazione per consulenze tecniche
- Modello di documentazione per la catena di custodia
- Esercitazioni di laboratorio di analisi forense

Giorno 4:

- Architettura dei sistemi Android
- Architettura dei sistemi Apple
- Rooting e Jailbreaking
- Pin code e cloud
- Modalità di acquisizione logica e fisica
- Metodologia di analisi
- Ricerca di informazioni cancellate
- Laboratorio di Mobile Forensics

Materiale didattico

Slide e libro in formato epub.

Location

Sede operativa di Tesla Consulting srsl

Via Enrico Mattei 88, 40138 Bologna

Costi

Prezzo di listino 3.000 € + iva a partecipante (sono previsti sconti nel caso di prenotazione almeno un mese prima del corso e per aziende che vogliono iscrivere più persone)

Compreso nel prezzo:

- Materiale didattico del corso in pdf e epub
- Penna usb usata per le esercitazioni
- un pasto in ristorante e due coffee break al giorno
- attestato di frequenza

Info e prenotazioni

Silvia Castellari

Mail: segreteria@teslaconsulting.it

Tel: +39 051.0548633