mediaservice.net
CORPORATE SECURITY & IMAGE

Corso Base Digital Forensics Legali

Executive Summary

Per affrontare le difficoltà inerenti all'acquisizione, conservazione ed elaborazione della prova digitale, @ Mediaservice.net offre un corso sulla Digital Forensics di facile comprensione per orientare i partecipanti sull'attuale realtà degli strumenti informatici come mezzo, non solo per attuare crimini informatici ma anche crimini convenzionali, e sulle più appropriate metodologie per il sequestro delle prove informatiche e l'analisi delle stesse, unitamente ad una panoramica sulle attuali tecniche e strumenti di Forensics e anti-Forensics.

Audience

Questo corso è destinato a quelle figure professionali che necessitano di avere le competenze tecniche e teoriche per intervenire in prima linea in casi di incidenti informatici e/o reati a mezzo informatico. Alcuni tra i destinatari:

- Avvocati
- Procuratori della Repubblica
- Ufficiali di Polizia di stampo "non tecnico"
- Amministratori di sistema o di rete
- Studenti e ricercatori interessati alla Digital Forensics
- Consulenti per il Tribunale

Prerequisiti

Tutti i partecipanti dovranno avere un PC o altri supporti per poter meglio apprezzare e comprendere il materiale del corso.
Le slide illustrate dai docenti saranno fornite durante lo svolgimento del corso.

Capacità e competenze acquisite

Al termine del corso i partecipanti saranno in grado di:

- effettuare sequestri/acquisizioni di dispositivi digitali secondo le migliori best practice riconosciute a livello internazionale;
- effettuare analisi forensi complete su diverse tipologie di media, dai pc client agli smartphone, dai server alle consolle;
- effettuare il recovery di dati e la sanitizzazione di dispositivi e sistemi;
- redirigere in maniera esaustiva la reportistica finale e la catena di custodia, siano essi per fini giudiziari o per investigazioni private;

Validità della prova informatica:

- **Deve essere trattata da esperti.**
- **Deve essere acquisita secondo procedure , tecniche e strumenti appropriati.**
- **Deve essere ammissibile in sede di giudizio di conseguenza acqusita secondo la legislazione nazionale**
- **Deve essere autentica.**
- **Deve essere completa, deve raccontare l'intera storia, non soltanto un punto di vista.**
- **Deve essere affidabile, il metodo con cui viene trattata non deve creare dubbi o sospetti.**
- **Deve essere credibile di fronte ad un Magistrato o un avvocato**

Programma (2 Giorni)

Il corso si articola su 2 giorni, nell'ultimo dei quali è previsto un test di valutazione su quanto appreso. I contenuti che verranno esposti possono essere raggruppati nelle seguenti aree:

Informatica: concetti di base: Dai bit e Byte al documento Word, Computer: cosa c'è dentro la scatola magica,Hardware, Software, Dispositivi di memorizzazione, Internet: cos'è e come funziona.

La Metodologia: I principi della digital forensics, passo passo dalla verifica dell'incidente al report finale , ISO27037.

Sistemi digitali coinvolti in crimini informatici ed in crimini convenzionali: Digital Forensics: le tre aree principali, individuazione del dato.

Sequestro, Acquisizione e Preservazione delle Digital Evidence: Capire quando è necessario/possibile effettuare il sequestro di un sistema e quando, invece, è indispensabile "congelarne" lo stato. Verranno illustrate le tecniche di base ed i tool per effettuare acquisizioni standard di dispositivi di memorizzazione e di sistemi live, per acquisire ed analizzare i dati volatili, nonchè le modalità di preservazione fisica delle evidenze e le funzioni di hashing per la preservazione logica. Catena di custodia

Analisi: Si apprenderanno le tecniche e l'utilizzo dei tool necessari per la ricerca di evidenze a basso livello, dall'analisi dello slack space e delle aree non allocate al file carving.

CD/DVD Forensics: sono davvero supporti inalterabili? Come nascondere un dato e come recuperarlo.

Crittografia: protezione dei dati sensibili ed antiforensics:

- Disk encryption: cos'è e come funziona.
- Principali applicazioni.
- Antiforensics e wiping.

Mobile Forensics: Cos'è la mobile forensics, l'importanza della mobile forensics al giorno d'oggi, la metodologia. Acquisizione ed Analisi: cosa cambia rispetto al computer? Tool e dimostrazioni pratiche:UFED CelleBrite.

Software Open Source vs Software Proprietario:

- Quale scegliere e perché.

Confidenzialità delle comunicazioni:

- How to sull'utilizzo di PGP.

Codice di Procedura Penale - Art. 244

Casi e forme delle ispezioni

- **1.** L'ispezione delle persone, dei luoghi e delle cose è disposta con decreto motivato quando occorre accertare le tracce e gli altri effetti materiali del reato.

- **2**. Se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autorità giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. ***L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.***

Costi

Prezzo di listino	560 € + iva per partecipante
Sconti	5% se si effettua il pagamento almeno 10 giorni prima della scadenza delle iscrizioni
	10% per gli appartenenti alle Forze Armate, Forze dell' ordine e Studenti Universitari

Compreso nel prezzo:

- 8 ore di lezione con docenti qualificati ed esperti in materia
- materiale didattico del corso in formato digitale
- test di verifica dell'apprendimento degli argomenti trattati
- attestato di frequenza

mediaservice.net
CORPORATE SECURITY & IMAGE

@ Mediaservice.net S.r.l. con Socio Unico
Via Santorelli, 15 - 10095 Grugliasco (TO)
Tel +39 011-3272100 - Fax +39 011-3246497
info@mediaservice.net - **www.mediaservice.net**