Studio d'Ingegneria Informatica & Forense
Prof. Ing. Ugo LOPEZ
CF: LPZGUO74S14A662R PI: 06403550723

Programma didattico corso online di Digital Forensics

Corso pensato per professionisti del settore informatico e tecnico interessati ad approfondire le proprie conoscenze sulle procedure teoriche e pratiche di **Informatica Forense**.

Saranno oggetto del corso gli aspetti relativi all'**identificazione**, alla **repertazione delle fonti di prova** in modo corretto, per poter essere anche valutate in sede processuale civile o penale, all'analisi ed alla presentazione delle conclusioni. Parte pratica di laboratorio, basata sul software Open Source.

Il target

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

Durante il corso i partecipanti impareranno anche a **trovare files nascosti**, a **recuperare dati cancellati** e **duplicare informazioni integre e non ripudiabili**, anche attraverso l'utilizzo di tools in aula e l'analisi di casi studio reali.

Il corso è pensato quindi per professionisti del settore informatico interessati ad approfondire le proprie conoscenze sulle procedure teoriche e pratiche di Informatica Forense.

Destinatari

Responsabili dei Sistemi Informativi; Forze dell'Ordine; Responsabili della Sicurezza Informatica; Responsabili di Sistemi di Pagamento; Responsabili di Progetti Internet/Intranet; Responsabili E-Commerce; Sistemisti e operatori del settore ICT; Responsabili EDP e CED; Responsabili di Rete; Amministratori di Rete; Responsabili di Siti Web; Studenti Universitari; Consulenti.

Requisiti

Buona conoscenza del sistema operativo Windows, basi di Linux e dei concetti base sui File System (FAT/NTFS/EXT3). Fondamenti di Networking.

Durata

Modulo introduttivo: 6h - Laboratorio: 6h

Via Aurelio Carrante, 1/F
70124 BARI
Tel: 080-2229894 Fax: 080-2229886
E-mail: gruppo@ugolopez.it

Studio d'Ingegneria Informatica & Forense
Prof. Ing. Ugo LOPEZ
CF: LPZGUO74S14A662R PI: 06403550723

PROGRAMMA CORSO (compatibilmente con I tempi d'apprendimento)

MODULO INTRODUTTIVO

1. Panoramica sulle Best Practices Computer forensics
    1.1 – L'immodificabilità della fonte di prova ed il metodo scientifico.
        1.1.1 Il sopralluogo informatico.
    1.2 - Analisi live e post mortem (i perché, pro e contro)
    1.3 - Identicità della prova
        1.3.1 - hash, cosa sono ed il problema della collisione.
        1.3.2 - catena custodia.
        1.3.3 - ripetibilità delle operazioni.
    1.4 – Digital profiling e social engineering.
2. Gli strumenti della C.F. - open source vs commerciale.
3. Write blocker ed hardware forense.
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 live distro forense).
5. Cenni su casi reali.
6. Panoramica sulla mobile forensics: tecniche di acquisizione ed analisi sui cellulari/tablet
7. Cenni sulla legge 48/2008, art. 359 e 360 c.p.p. e DPR 115/02.
8. Live analysis ed acquisizione su un sistema acceso.

Via Aurelio Carrante, 1/F
70124 BARI
Tel: 080-2229894 Fax: 080-2229886
E-mail: gruppo@ugolopez.it

9. Elementi di mobile forensics

10. Il futuro della D.F.

11. I miti e le leggende.

Via Aurelio Carrante, 1/F
70124 BARI
Tel: 080-2229894 Fax: 080-2229886
E-mail: gruppo@ugolopez.it

Studio d'Ingegneria Informatica & Forense
Prof. Ing. Ugo LOPEZ
CF: LPZGUO74S14A662R PI: 06403550723

LABORATORIO (compatibilmente con I tempi d'apprendimento)

Alcuni temi del programma sono inclusi negli esercizi che saranno svolti.

Introduzione ed utilizzo avanzato della live distro forense CAINE

- esempio d'analisi live ed uso dei tools.

– Uso della Windows side delle live distro.

- Esempio attività su pc spento

– La checklist delle operazioni da compiere.

- Preview & acquisizione (imaging)

- Attività d'analisi con i tools a disposizione.

– Esercizi:

– Acquisizione di un supporto tramite Linux su disco destinazione.

– Acquisizione di un supporto tramite Linux via rete.

– Acquisizione di un supporto tramite Windows con FTK Imager.

- Il carving (Foremost, Photorec, Scalpel) e come risalire al nome file dal numero di settore.

– Analisi tramite Autopsy e Sleuthkit su un supporto (browsing il filesystem, ricerca per stringhe,
recupero dei file cancellati, timeline, ecc.)

– Ricostruzione degli headers tramiter editor esadecimale.

- Analisi dei registri di Windows tramite RegRipper per Windows.

- Analisi dei metadati dei file multimediali.

- Panoramica su altri tools.

- Alcune tecniche di anti-forensics.

Via Aurelio Carrante, 1/F
70124 BARI
Tel: 080-2229894 Fax: 080-2229886
E-mail: gruppo@ugolopez.it

- Cenni sulla steganografia.

- Alcuni esempi di cattura di network sniffing ed analisi del PCAP.

- Virtualizzare un sistema.

- Memory forensics con open source e freeware

- Cristallizzazione sito web ed elementi di OSINT.

- Analisi con bulk_extractor per la ricerca di siti visitati col sistema TOR.

- Esercizi pratici e challenges da svolgere in classe.