P.E.K.I.T.
CoFo

Syllabus PEKIT CoFo

PEKIT CoFo certifica le competenze proprie della figura professionale di "Esperto in Investigazioni Digitali" in ambito giudiziario, penale, civile ed amministrativo. Il soggetto certificato PEKIT CoFo può operare come Analista nel mondo aziendale, come investigatore forense e all'interno di un CSIRT ("Computer Security Incident Response Team").
Generalmente, l'Esperto di Digital Forensics opera come libero professionista, offrendo la sua consulenza ad aziende, uffici giudiziari e forze dell'ordine. In altri casi è un lavoratore dipendente di società specializzate nella sicurezza informatica che offrono, tra i loro servizi, anche indagini di **Computer Forensics***.
Questa figura professionale opera prevalentemente al fianco delle Forze dell'Ordine durante le indagini giudiziarie, occupandosi dell'individuazione, della copia, della custodia e dell'autenticazione delle prove di reati informatici.
**Computer Forensics è la disciplina che si occupa della preservazione, dell'identificazione, dello studio, della documentazione dei computer (o dei sistemi informativi in generale), al fine di evidenziare l'esistenza di prove nello svolgimento dell'attività investigativa. (A.Ghirardini: "Computer forensics" – Apogeo)*

Modulo Uno

Computer Forensics: definizioni e applicazioni

- Computer Forensics: definizioni e applicazioni
- Introduzione del corso
- Cos'è la Computer Forensics: definizioni e applicazioni
- Disciplina giuridica
- Filosofia di base e Best practices
- Catena di custodia
- Impostazioni operative
- Identificazione e marcatura dei supporti e dei media non convenzionali
- Preservazione del dato: il sequestro e l'acquisizione
- Acquisizione di memorie di massa
- Concetto di copia forense
- Verifica d'integrità
- La codifica Hash
- Validazione della prova con Hash
- Cavilli giuridici
- Tecnologie più frequenti
- Strumenti open source
- Evitare i cavilli giuridici/errori
- Blocker hardware
- Strumenti software commerciali o open source?
- Acquisizione di memorie volatili
- Mobile devices

Modulo due

Preservazione del dato: il sequestro e l'acquisizione

- Preservazione del dato: le intercettazioni telematiche
- Disciplina giuridica
- Problemi tecnici
- Applicazioni in reti ethernet
- Problematiche delle tecniche di Man-in-the-middle
- Software utili, Applicazioni in reti wireless
- Dotazione HW e SW
- Limiti giuridici
- Problemi derivanti dall'uso di crittografia
- Analisi del traffico intercettato

Modulo tre

Analisi dei documenti (formati più diffusi) e dei loro metadati

- Analisi e valutazione delle digital evidence
- Costruire il laboratorio di analisi
- Strumentazione hardware e software
- Descrizione dei software commerciali e open source
- Arrivano le Distribuzioni live Linux (Halix, caine, ftk, kali)
- Visualizzatori, player e codec
- Analisi dei documenti (formati più diffusi) e dei loro metadati
- Analisi delle immagini: metadati e individuazione delle manipolazioni
- Dimostrazioni ed esercitazioni pratiche
- Partizioni e Filesystem più diffusi
- FAT, NTFS, EXT, HFS ecc.
- Cluster, allocazione e slack space
- Utilizzo di Virtual Machine
- Live Wiew
- Problematiche sull'aggiornamento delle password
- File di log, File di configurazione / registro di sistema
- Informazioni sull'utilizzo (history, file recenti, ecc.)
- Dati applicativi (browser, client di posta, cartelle temporanee, ecc.)

Modulo quattro

Recupero dati e tecniche di occultamento

- Recupero dati
- Ripristino dei dati cancellati tramite analisi del filesystem
- File carving
- Analisi delle aree di swap e dei file di ibernazione
- Individuazione e analisi del malware
- Software utili, dimostrazioni ed esercitazioni pratiche
- Tecniche di antiforensic e loro contenimento
- Tecniche di distruzione dei dati

- Tecniche di occultamento
- Steganografia
- Tecniche di falsificazione delle digital evidence
- Altre tecniche di elusione
- Contromisure e mitigazione delle tecniche discusse
- Fasi finali: la presentazione dei risultati dell'indagine
- Redazione di una relazione conclusiva
- Bilancio competenze della figura professionale dell'analista forense
- Necessità e opportunità per l'aggiornamento professionale in materia di Computer Forensic