STUDIO TECNICO DI INGEGNERIA INFORMATICA

ING. GIANLUCA GOLINELLI

Informatica Forense e Sicurezza Informatica

www.gianlucagolinelli.it – g.golinelli@gianlucagolinelli.it

Introduzione all'Informatica Forense

(Durata: 8 h – 8 crediti formativi)

DOCENTE
Dott. Ing.
Gianluca Golinelli

Ingegnere elettronico, membro del C3I (Comitato Italiano Ingegneria dell'Informazione), board member di A3I (Associazione Italiana Ingegneri dell'Informazione), Coordinatore del Gruppo di lavoro di Informatica dell'Ordine degli Ingegneri della Provincia di Parma. Si occupa da anni di sicurezza informatica come consulente per aziende ed enti della Pubblica Amministrazione, per cui ha svolto attività di formazione e consulenza. Svolge inoltre attività forense in qualità di Consulente Tecnico di Parte e Consulente Tecnico d'Ufficio del Tribunale di Parma.

Destinatari
IT Manager
Responsabile Sicurezza Informatica,
Tecnico di Sicurezza Informatica,
Consulenti Tecnici d'Ufficio,
Consulenti Tecnici di Parte

Obiettivi
Acquisire le competenze tecniche necessarie per poter svolgere l'attività di Digital Investigator. Conoscere ed imparare ad utilizzare gli strumenti per Computer Forensics. Acquisire, analizzare e conservare opportunamente le prove digitali utilizzabili in fase processuale. Esercitarsi concretamente grazie alle simulazioni. Verranno rilasciati 8 crediti validi per l'aggiornamento obbligatorio.

Prerequisiti: conoscenze base di sistemi operativi e di networking;

Introduzione alla Digital Forensic
- Il panorama normativo italiano
- Ambiti di applicazione nel processo civile e nel processo penale

L'identificazione e l'acquisizione delle prove
- Metodologie
- Tecniche
- Strumenti

ESERCITAZIONE PRATICA: simulare la fase di acquisizione di prove digitale
I partecipanti, con la guida del docente, simuleranno la fase di acquisizione di prove digitali da un sistema target.

L'acquisizione delle prove in sistemi attivi
- Acquisizione di prove da fonti volatili
- Acquisizione di prove da sistemi attivi

ESERCITAZIONE PRATICA: simulare la fase di acquisizione di prove da sistemi attivi

La catena di custodia delle prove acquisite
- Tecniche di hashing
- Strumenti
- Reportistica

Acquisizione di prove dalla rete
- Utilizzo di network sniffers
- Acquisizione di prove da IDS
- Acquisizione di prove da firewall e proxy

Acquisizione di prove da sistemi mobile
- Acquisizione di dati da SIM Card
- Acquisizione da altri dispostivi (smartphone, macchine fotografiche digitali, etc)

L'Analisi dei dati acquisiti
- Metodologie
- Tecniche
- Strumenti Open Source e commerciali

L'analisi dei dati per i sistemi operativi più comuni
- Sistemi Windows
- Sistemi Unix
- sistemi MacOS

ESERCITAZIONE PRATICA: effettuare la simulazione dell'analisi di dati acquisiti da un sistema windows

Tecniche avanzate di analisi
- L'esame dello spazio non allocato e dello Slack Space del disco
- Il data carving

ESERCITAZIONE PRATICA: effettuare il data carving di una prova acquisita
Verrà simulata l'analisi mediante tecniche e strumenti per il data carving di una prova acquisita

Tecniche avanzate di analisi per Windows
- Analisi dei registri di windows
- Analisi dei metadati dei file multimediali
- Analisi forense delle email e della cronologia di Internet
- Recupero dei file cancellati

Analisi di dati crittografati
- Tecniche crittografiche
- La steganografia
- Strumenti

ESERCITAZIONE PRATICA: Simulare l'utilizzo di strumenti di crittografia e decrittografia.

Password Cracking
- Metodologie
- Tecniche
- Strumenti

ESERCITAZIONE PRATICA: Simulare l'utilizzo di strumenti di Password Cracking e di Brute Force.

Le certificazioni per competenze di Digital Forensics
- Tipologie principali
- Requisiti