



DOCENTE

Professionisti esperti di
Computer Forensics, CTU
del Tribunale

Strumenti e Metodologie per Computer Forensics

(codice corso IT06FORENS)

Destinatari

IT Manager
Responsabile Sicurezza
Informatica
Tecnico di Sicurezza
Informatica
Personale delle Forze
dell'Ordine
Personale di Intelligence ed
Investigatori Digitali

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
pratiche

**Prerequisiti: conoscenze
base di sistemi operativi
e di networking;
conoscenze di base
dell'hardware dei
calcolatori informatici**

Prima giornata

8.45 Registrazione dei partecipanti

9.00 Introduzione alla Computer Forensic

- > Il panorama normativo italiano
- > Ambiti di applicazione nel processo civile e nel processo penale

10.00 L'identificazione e l'acquisizione delle prove

- > Metodologie
- > Tecniche
- > Strumenti

10.45 Coffee break

11.00 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.

12.00 L'acquisizione delle prove in sistemi attivi

- > Acquisizione di prove da fonti volatili
- > Acquisizione di prove da sistemi attivi

13.00 Colazione di lavoro

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

15.00 La catena di custodia delle prove acquisite

- > Tecniche di hashing
- > Strumenti
- > Reportistica

15.45 Tea break

16.00 Acquisizione di prove dalla rete

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

17.00 Acquisizione di prove da sistemi mobile

- > Acquisizione di dati da SIM Card
- > Acquisizione da altri dispositivi (smartphone, macchine fotografiche digitali, etc)

17.45 Conclusione della prima giornata

Seconda giornata

8.45 Registrazione dei partecipanti

9.00 L'Analisi dei dati acquisiti

- > Metodologie
- > Tecniche
- > Strumenti Open Source e commerciali

10.00 L'analisi dei dati per i sistemi operativi più comuni

- > Sistemi Windows
- > Sistemi Unix
- > sistemi MacOS

10.45 Coffee break

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

12.00 Tecniche avanzate di analisi

- > L'esame dello spazio non allocato e dello Slack Space del disco
- > Il data carving

13.00 Colazione di lavoro

14.00 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

15.00 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

15.45 Tea break

16.00 Analisi di dati crittografati

- > Tecniche crittografiche
- > La steganografia
- > Strumenti

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

17.45 Conclusione della seconda giornata

Terza giornata

8.45 Registrazione dei partecipanti

09.00 Password Cracking

- > Metodologie
- > Tecniche
- > Strumenti

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

10.45 Coffee break

11.00 La redazione della reportistica

- > La relazione peritale
 - o Strutturazione
 - o Sezioni
 - o Gli allegati

12.00 La figura del CTU e del CTP

- > La relazione del CTU
- > La relazione del CTP

13.00 Colazione di lavoro

14.00 CASE STUDY: Esame della strutturazione di una relazione peritale di CTU e di CTP relativa ad una causa penale o civile

15.00 L'Anti-Forensics

- > Metodologie
- > Tecniche
- > Strumenti

15.45 Tea break

16.00 ESERCITAZIONE PRATICA: Simulare una procedura di anti-forensics su una macchina target

17.00 Le certificazioni per competenze di Computer Forensics

- > Tipologie principali
- > Requisiti

17.45 Conclusione del corso e consegna degli attestati