

# Computer Forensic

*Investigazioni Digitali*

**Codice**  
**R25**

**Orario**  
**dalle ore 09.00 alle 17.00**

**Durata**  
**4 Giornate d’aula**



## Descrizione

La nuova figura professionale dell' **Investigatore Informatico** è oggi molto ricercata nell'ambito specialistico della “**Computer Forensics**”, ossia di quella disciplina che si occupa della acquisizione, analisi e conservazione delle informazioni contenute nei computer e nei sistemi informativi oggetto di **reato informatico**, al fine di evidenziare l'esistenza di prove utili allo **svolgimento di attività investigative**. Nata istituzionalmente nel **1984 con l’FBI**, si utilizza principalmente nei casi di spionaggio industriale e commerciale, frodi finanziarie, lotta alla pedopornografia e cybercrime.

L'investigatore informatico si occupa di **identificare, acquisire, conservare, analizzare, valutare e presentare le prove digitali di reato** nell'ambito del crimine informatico prestando la massima cautela affinché tali evidenze siano ammissibili, autentiche, complete, affidabili e credibili. La scena del crimine potrà essere un computer, un supporto magnetico, una rete o un qualsiasi altro medium digitale.

L'attività prevalente di questa figura professionale si svolge al fianco delle forze dell'ordine nelle **indagini giudiziarie, occupandosi dell'individuazione, della copia, della custodia e dell'autenticazione delle prove di reati informatici**. Inoltre l'investigatore informatico può coadiuvare le imprese nella salvaguardia della sicurezza dei propri sistemi informatici, come dipendente o libero professionista.

## Obiettivi del Corso

Lo scopo principale del corso è quello di **trasferire competenze specialistiche per l'acquisizione, l'analisi e la conservazione di evidenze digitali, in modo corretto, per poter essere anche valutate in sede processuale civile o penale**. 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**.

## Principali Contenuti del Corso

- Introduzione alla Computer Forensics
- Il processo di investigazione informatica
- Analisi file systems e hard disk
- Analisi forense su sistemi Windows e Linux
- Acquisizione di informazioni e dati nascosti
- Duplicazione dei dati
- Utilizzo di forensic tools e strumenti per l'imaging
- Steganografia
- Analisi log su Pc incriminati
- Simulazioni e Casi Studio



Dasa-R&gister  
EN ISO 9001:2008  
IQ-1203-28



**Studiodelta s.r.l.**  
**Microsoft Gold Certified Partner for Learning Solutions**

Via G. Amendola 162/1  
70126 Bari – Executive Center  
Tel. 080.546.18.60  
Fax 080.546.18.78  
E-mail: info@studiodelta.it  
Sito web: www.studiodelta.it



## 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

## Prerequisiti di partecipazione

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

E' consigliata la partecipazione a tecnici in possesso di certificazioni quali MCP, MCSA, MCSE, MCSA Security, MCSE Security, MCITP Enterprise Administrator, MCITP Server Administrator, CompTIA Security + o equivalenti.

## Certificazioni

Attestato di frequenza al corso. Il percorso formativo è propedeutico per il conseguimento di certificazioni internazionali e programmi specifici quali CHFI, EnCe, CCE, IACIS (dettagli su <http://www.investigazionidigitali.com/training.asp>)



Le condizioni , i punteggi ed i vincoli di superamento di ogni esame sono fissate direttamente dagli Enti Internazionali di Certificazione e pertanto si invita a leggere attentamente tutte le informazioni disponibili sui siti internet ufficiali di riferimento. Studiodelta srl non si assume alcuna responsabilità sul contenuto dei Test e sul risultato degli stessi.

A richiesta del partecipante è possibile la presentazione ad aziende, sul territorio nazionale, per stage e selezioni del personale.

I contenuti e la struttura dei percorsi di certificazione possono subire aggiornamenti; pertanto vi consigliamo di visionare la pagina dedicata allo specifico percorso di certificazione

## Qualifica del Docente

Perito CTU, Specialista di Computer Forensics - Project Manager di una delle Live distro più usate al mondo – Autore di libri ed articoli su riviste internazionali – Auditor Iso 19011/27001

## Materiale Didattico

- Indagini Digitali di Nanni Bassetti
- Computer Forensics - A. Ghirardini, G. Faggioli
- Dispense e Manuali rilasciati dal trainer

## Quota di Partecipazione

La quota d'iscrizione al Corso è di **€2.200 + IVA** ed è comprensiva del materiale didattico.



## PIANO DIDATTICO Computer Forensic – Investigazioni Digitali (R25)

<b>Prima giornata</b>	
	<p>Inroduzione alla Computer Forensics Panoramica sulle Best Practices L'immodificabilità della fonte di prova ed il metodo scientifico Analisi live e post mortem (i perchè, pro e contro) Identicità della prova Hash, cosa sono ed il problema della collisione. Catena custodia, nella teoria e nella realtà Ripetibilità delle operazioni Digital profiling e social engineering.</p>
<b>Seconda Giornata</b>	
	<p>Gli strumenti della C.F. - open source vs commerciale Le quattro fasi (Identificazione, acquisizione, analisi, reporting) in pratica GNU/Linux per la C.F. (uso di live distro forensi) Cenni sulla legge 48/2008. Cenni di EnCase Esempio d'analisi live ed uso dei tools. Uso della Windows side delle live distro (Tools: Wintaylor, Deft Extra, ecc.). Esempio attività su pc spento La checklist delle operazioni da compiere. Preview &amp; acquisizione (imaging)</p>
<b>Terza Giornata</b>	
	<p>Attività d'analisi con i tools a disposizione. Acquisizione di un supporto tramite Linux su disco destinazione (DC3DD, AIR, GUYMAGER, DD) Acquisizione di un supporto tramite Linux via rete (dc3dd, dd, netcat) 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 tramite editor esadecimale (XVI32 per Windows o Ghex per Linux). Analisi dei registri di Windows tramite RegRipper per Windows. Analisi dei metadati dei file multimediali.</p>
<b>Quarta Giornata</b>	
	<p>Panoramica su altri tools come: Pasco, Rifiuti, SFDumper, Ink.sh, ecc. Alcune tecniche di anti-forensics. Cenni sulla steganografia (stegdetect, stegbreak, xsteg, jphswin) Alcuni esempi di cattura di network sniffing (Wireshark e Network Miner) ed analisi del PCAP. Virtualizzare un sistema (VirtualBox). Esercizi pratici e challenges da svolgere in classe</p>