

Corso di Specializzazione

# Computer Forensics

## Investigazioni Digitali **Serale**

Codice  
R25-S

Orario  
dalle ore 18.00 alle 21.00

Durata  
5 Incontri 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 preservazione, acquisizione e studio delle informazioni contenute nei computer e nei sistemi informativi, al fine di evidenziare l'esistenza di prove utili allo svolgimento di attività investigative.

L'investigatore deve essere in grado di avvicinarsi ad un sistema informativo per determinare se esso sia stato utilizzato in attività illecite o non autorizzate, avendo cura di non alterare le possibili prove o tracce digitali. La scena del crimine può quindi essere un computer, un supporto magnetico, una rete o altro medium digitale.

### Descrizione del Profilo

L'analista Forense si occupa di ricercare e conservare le evidenze digitali di reato nell'ambito del crimine informatico prestando la massima cautela affinché tali prove siano ammissibili, autentiche, complete, affidabili e credibili. Le competenze del Forensics Analyst consentono allo specialista di intervenire in caso di incidente informatico (security), durante una causa legale in sede di perizia e durante le indagini relative ad un reato.

### Obiettivi del Corso

Lo scopo principale del corso è quello di trasferire competenze per l'acquisizione e la conservazione delle prove digitali, in modo corretto, per poter essere valutate in sede processuale civile o penale. Durante il corso i partecipanti apprenderanno le tecniche per acquisire file nascosti, recuperare dati cancellati e duplicare informazioni integre e non ripudiabili.

### Principali Contenuti del Corso

- Introduzione all' Analisi Forense
- Il processo investigativo
- Rilevazione dell'incidente
- Identificazione ed acquisizione delle fonti di prova
- Organizzazione delle informazioni
- Esame ed analisi delle prove raccolte
- Ricostruzione degli eventi
- Presentazione dei risultati
- L'efficacia probatoria
- La duplicazione dei supporti
- Backup preventivi e di indagine
- Realizzazione dell'Immagine
- Integrità e disponibilità delle fonti di prova (chain of custody)
- Tools di analisi dei dischi : presentazione e laboratorio
- Tools di immagini dei dischi : presentazione e laboratorio
- Tools di analisi di rete : presentazione e laboratorio
- Esempi di Analisi Forense
- Ambito Normativo (civile e penale)

Dasa-Rägister  
EN ISO 9001 (2000)  
IQ-1203-28



Microsoft  
GOLD CERTIFIED  
Partner

Learning Solutions  
Security Solutions  
ISV/Software Solutions  
Networking Infrastructure Solutions

**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 del Corso

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

Sono richieste buone conoscenze sul networking & Security e sul Sistema Operativo Microsoft Windows (NT/2000/2003).

## Certificazioni

Attestato di frequenza

## Qualifiche dei Docenti

Microsoft Certified Trainer, Microsoft Certified Systems Engineer, Microsoft Certified Systems Administrator, Cisco Certified Network Associate, CompTIA Security+

## Materiale Didattico

- Computer Forensics – Apogeo di Andrea Ghirardini e Gabriele Faggioli
- Dispense della Divisione Networking & Security Studiodelta.

## Quota di Partecipazione

- La quota di partecipazione al corso è di **€450,00** iva esclusa.



## R25-S – PIANO DIDATTICO - CORSO COMPUTER FORENSICS

---

### PRIMA GIORNATA

---

Introduzione all' Analisi Forense  
Il processo investigativo  
Rilevazione dell'incidente  
Identificazione ed acquisizione delle fonti di prova

---

### SECONDA GIORNATA

---

Organizzazione delle informazioni  
Esame ed analisi delle prove raccolte  
Ricostruzione degli eventi  
Presentazione dei risultati

---

### TERZA GIORNATA

---

L'efficacia probatoria  
La duplicazione dei supporti  
Backup preventivi e di indagine

---

### QUARTA GIORNATA

---

Realizzazione dell'Immagine  
Integrità e disponibilità delle fonti di prova (chain of custody)  
Tools di analisi dei dischi : presentazione e laboratorio

---

### QUINTA GIORNATA

---

Tools di immagini dei dischi : presentazione e laboratorio  
Tools di analisi di rete : presentazione e laboratorio  
Esempi di Analisi Forense  
Ambito Normativo (civile e penale)

---