FORENSICS GROUP

forensics
IT F CERTIFICATIONS

# IT FORENSICS

## corso di perfezionamento

***Lecce, ottobre-dicembre 2013***

**www.forensicsgroup.it**


**L'Esperto di IT Forensics** è un consulente altamente specializzato nella sicurezza informatica e nei crimini ad essa connessi.

Con il termine di Computer Forensics si indica l'investigazione dei crimini informatici, includendo la raccolta, l'analisi e la presentazione in tribunale delle prove elettroniche.

L'esigenza di una figura con adeguate conoscenze dei metodi idonei al trattamento e alla gestione di prove informatiche utili nell'ambito di indagini giudiziarie è nata con l'avvento di Internet.

La sicurezza informatica, cioè la protezione delle informazioni presenti nei sistemi informatici, è di fondamentale importanza per imprese ed organizzazioni. Tali sistemi, nonostante le più efficienti misure di sicurezza adottate dalle aziende, possono essere violati da persone (hackers) che, dall'esterno o dall'interno, riescono ad accedervi per impossessarsi, cancellare o modificare le informazioni che vi sono contenute.

Generalmente l'Esperto di IT 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 le indagini di Computer Forensics.

L'attività prevalente di questa figura 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. L'Esperto di IT Forensics può altrimenti coadiuvare le imprese nella salvaguardia della sicurezza dei propri sistemi informatici.


Questa figura professionale deve avere molteplici competenze, sia tecniche che giuridiche. In ambito tecnologico deve avere la preparazione del Tecnico hardware , dell'Analista di sistema , del Security administrator e del Security auditor, mentre in ambito giuridico deve conoscere le procedure forensi, le norme che tutelano i dati personali e i patrimoni informativi ed infine possedere nozioni approfondite sul crimine informatico.

L'Esperto di IT Forensics deve conoscere approfonditamente i più diffusi sistemi operativi, le architetture ed i protocolli di rete, le strutture dei database, le tecniche di crittografia dei dati

ed i metodi utilizzati dagli hacker per aggirare le difese poste a salvaguardia della sicurezza informatica.

Deve anche conoscere altrettanto bene la disciplina giuridica in materia di crimine informatico e di protezione dei dati personali, con particolare riferimento al quadro normativo delineato dal DPR 196/2003 sulla privacy e successive modifiche ed integrazioni.

Per quanto riguarda le competenze di base, sono necessari un buon livello di cultura generale e la padronanza della lingua inglese (importante per tutte le professioni dell'IT).

È anche necessario che l'Esperto di IT Forensics possegga capacità di analisi, tenacia, precisione e, soprattutto, sia in grado di esprimersi con un linguaggio rigoroso sul piano giuridico ma al tempo stesso comprensibile sul piano tecnico, anche per chi non possieda conoscenze informatiche.

Infine questa figura deve avere una fortissima predisposizione all'aggiornamento: la capacità di mantenersi informati è fondamentale se si considerano le continue novità in un campo in cui si può, in un certo senso, parlare di lotta senza quartiere fra chi, da un lato, inventa sempre più efficaci barriere di difesa e chi, dall'altro, escogita altrettanto ingegnosi metodi per superarle.


Buona conoscenza informatica e sufficiente conoscenza della lingua inglese. A seconda del numero dei partecipanti, sarà prevista una prova selettiva ed un colloquio motivazionale.


L'accesso alla professione avviene dopo alcuni anni di esperienza nel settore della sicurezza informatica.

L'Esperto di IT Forensics può essere un dipendente di aziende di servizi di sicurezza o dei corpi di polizia oppure può lavorare come libero professionista. Quest'attività, tipicamente senza orari definiti, comporta frequenti spostamenti nelle sedi dove si trovano i computer da analizzare e spesso si svolge sotto il diretto controllo delle forze dell'ordine.

I compensi lordi annui oscillano, in base all'esperienza e al tipo di incarico, tra gli 80 e i 180 mila euro.

Nei prossimi anni è prevista una fortissima diffusione di questa figura, con una significativa presenza femminile.


**Ore totali:** **50 ore** complessive con modalità del fine settimana.

**Location:** *Lecce*

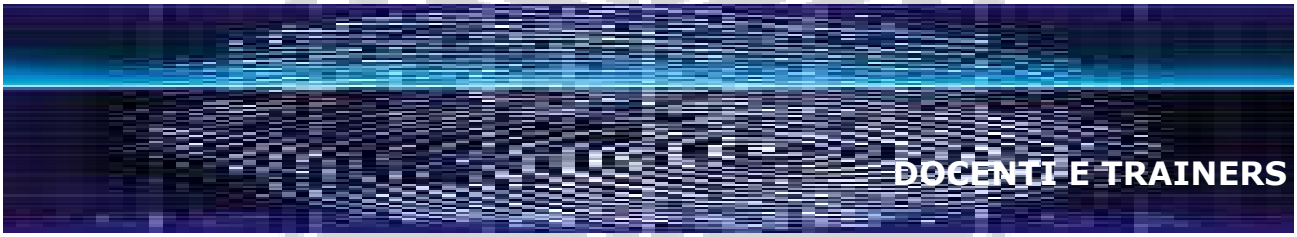

**Modulo TECNICO:** Il modulo intende fornire allo studente una conoscenza dell'architettura degli elaboratori elettronici, con particolare riferimento ai suoi componenti; fornire i principi base su sistemi operativi, sulla struttura degli elaboratori e sulla macchine virtuali.

**Modulo GIURIDICO**: Far conoscere e applicare tecniche di indagine su supporti informatici o elettronici e comprendere i processi legislativi del nuovo codice digitale. A partire da concetti di base della legislazione, si studierà la disciplina che si occupa della preservazione, dell'identificazione, dello studio, della documentazione dei sistemi informativi, al fine di evidenziare l'esistenza di prove nello svolgimento dell'attività investigativa.

**Modulo INVESTIGATIVO**: Far trasferire le competenze per l'acquisizione e la conservazione delle prove digitali, in modo corretto, per poter essere valutate in sede processuale civile e penale. Durante il modulo gli studenti apprenderanno le tecniche per acquisire file nascosti, recuperare dati cancellati e duplicare informazioni integre e non ripudiabili. Saranno anche fornite nozioni di Digital profiling.

**Modulo ANALISI**: Il modulo intende realizzare in maniera pratica le competenze di acquisizione, conservazione e reporting trasferite nel corso dei moduli precedenti.


Elaboratori elettronici, Architettura dei Calcolatori; Sistemi Operativi; Reti e protocolli di rete; Virtualizzazione di un Sistema; Indagine forense; Digital Forensics; Il documento informatico; I reati informatici; Tutela della Privacy; Le firme elettroniche; E-commerce; Il diritto d'autore; Il pagamento elettronico; Indagini P.G.: modalità operative; L'evidenza informatica; Accertamenti tecnici; Identificazione, acquisizione, analisi, reporting; Analisi live e post-mortem; Attività di analisi: tools open source e/o commerciali; Computer Crime Investigation & Cybercrime; Elementi di Corporate Security; Mobile Forensics; Network Forensics.




| | |
|---|---|
| Giuseppe LODESERTO, | Digital Expert, E-Crime Spelcialist, ICT Forensics; Forensics Group. |
| Mirco TURCO, | Psicologo, Criminal Investigation Expert, Forensics Group; |
| Rosario CARRISI, | Privacy e Security Specialist; Auditor SGSI; ICT Forensics. |
| Alessandro LAZARI, | Avvocato Joint Research Center - European Commission (Ispra) |

Altri esperti e professionisti del settore

## INVESTIMENTO

Euro 600,00. La quota è ridotta a 500,00 euro per coloro che hanno frequentato i seminari organizzati dal Forensics Group. Occorre versare una quota di euro 100,00 in fase di iscrizione. Il restante importo, a saldo, prima dell'inizio del corso. I costi si intendono esclusi di iva.

## MATERIALI ED ESAME FINALE

Tutti i corsisti riceveranno un kit didattico formativo e il relativo materiale inerente i diversi moduli e gli argomenti trattati. A fine percorso, oltre all'esame conclusivo, è prevista la discussione di una tesi. Il corsista che presenterà il lavoro più innovativo in termini scientifici sarà premiato con una targa di riconoscimento e un Tablet.

## CERTIFICAZIONE

I Corsisti che hanno superato l'esame conclusivo, oltre all'attestato finale, riceveranno anche la certificazione **IT FE** (it forensics expert). Consultare il sito www.forensicsgroup.it per dettagli.