

Master di Alta Formazione

Master Digital Forensics

Esperto in Investigazioni Digitali

22 POSTI
DISPONIBILI

Codice
IDF

Orario
dalle 14.30 alle 19:30

Frequenza
500 ore d'aula + 50 e-Learning
320 ore Stage



con il patrocinio di




ANORC
Associazione Nazionale per Operatori e Responsabili della
Conservazione Sostitutiva



Descrizione

La ampia diffusione degli strumenti informatici per il trattamento dei dati in organizzazioni pubbliche e private, apre uno scenario nuovo di reperimento di prove per istruire posizioni di difesa o accusa in presenza di giudizi civili, penali ed amministrativi.

L' "Informatica Forense" è la disciplina che studia l'insieme delle attività che sono rivolte all'analisi e alla soluzione dei casi legati alla criminalità informatica, comprendendo tra questi i crimini realizzati con l'uso di un computer, diretti a un computer o in cui il computer può comunque rappresentare una fonte di prova. Gli scopi dell'informatica forense sono di conservare, identificare, acquisire, documentare e interpretare i dati presenti su un pc o all'interno di un sistema informativo .

A livello generale si tratta di individuare le modalità migliori per :

- *Acquisire* le prove senza alterare o modificare il sistema informatico su cui si trovano,
- *Garantire* che le prove acquisite su altro supporto siano identiche a quelle originarie,
- *Analizzare* i dati senza alterarli.

L'informatica forense comprende le attività di verifica dei supporti di memorizzazione dei dati e delle componenti informatiche, delle immagini, audio e video generate da computer, dei contenuti di archivi e basi dati e delle azioni svolte nelle reti telematiche.

Importanti aspetti della disciplina riguardano, a un livello di maggior dettaglio, il ruolo della progettazione e mantenimento di una catena di custodia e gli argomenti principali da prendere in esame quando si presentano prove in sede processuale.

Il sistema informatico oggetto dell'indagine può essere un personal computer o un server isolato, nel qual caso si parla di **Computer Forensics**, ovvero può trattarsi di almeno due elaboratori connessi tra loro; in tal caso si parla di **Network Forensics**.



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

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. L'informatica forense agisce dopo che un sistema informatico è stato violato per esaminare i reperti informatici in modo esaustivo, completo, accurato, incontaminato e documentato. L'informatica forense opera dopo che sono stati utilizzati gli strumenti di risposta a un incidente, allorché intervengono gli organi inquirenti.

L'informatica forense non solo è significativa laddove si verificano reati informatici ma anche e soprattutto in molte situazioni in campo fiscale, commerciale, conferme di alibi, contenzioso del personale con la direzione, rapporti tra un cliente e un istituto di credito, rapporti tra cliente e gestore di servizi di commercio elettronico o di telecomunicazioni.

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 Digital 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 Digital Forensics può altrimenti coadiuvare le imprese nella salvaguardia della sicurezza dei propri sistemi informatici. In generale il Consulente Tecnico di Informatica Forense nell'adempimento del proprio incarico deve ricercare la prova tecnica, analizzarla con le più avanzate tecniche informatiche e rielaborarla con l'osservanza dell'impianto normativo cogente. Il consulente tecnico in informatica forense è in grado di estrarre informazioni utili da qualsiasi sistema informativo, le informazioni estratte verranno poi utilizzate a sostegno dell'accusa o della difesa.

Obiettivi

Il percorso formativo comprende le discipline basiche del diritto civile, penale ed amministrativo delle nuove tecnologie, quelle di base dell'informatica giuridica, principi di criminologia, modalità di attacco ai sistemi informatici, metodi di accesso ai sistemi informatici e di trasmissione dati, comportamenti dei più diffusi file system, struttura degli strumenti di memorizzazione, dei sistemi di compressione, di crittografia, applicazioni internet, ingegneria del software, crittografia e firma digitale, privacy, commercio elettronico, prove informatiche (acquisizione, integrità, attendibilità), validazione temporale dei dati (compresa la stima delle date di utilizzo dei file utilizzando date riferite ad altri eventi temporalmente confrontabili), strumenti e tecniche di effrazione degli strumenti informatici di sicurezza, redazione di atti peritali.

Il Master si focalizza sullo sviluppo delle competenze per eseguire l'analisi forense, con l'obiettivo di fornire la "**prova tecnica**" e cioè l'evidenza digitale di una specifica o generica attività e di eseguire una vera e propria investigazione forense che non si limita ad analizzare, in modo acritico, informazioni in formato digitale ma bensì a rielaborarle per il perseguimento della utilità giuridica.

Prerequisiti

Il Master " **Digital Forensics**" è rivolto a laureati, sia di primo livello che di secondo, in Giurisprudenza ed Informatica che vogliono specializzarsi nella conduzione di indagini su dati digitali e raccordare conoscenze giuridiche e tecnologiche per rafforzare le proprie competenze. E' richiesta familiarità con l'utilizzo del personal computer, conoscenza delle nozioni di base dell'informatica e della lingua inglese.

DENOMINAZIONE MODULI	Ore
Sistemi di telecomunicazione e formati digitali	56
Conservazione sostitutiva dei documenti: normativa e applicazioni	14
Diritto di autore e nuove tecnologie	20
Sicurezza e Privacy: l'impianto normativo	15
Metodologie e Tecnologie per la Sicurezza dell'informazione	75
Principi di Sicurezza Informatica	20
La responsabilità civile in internet	10
La disciplina del contratto telematico	10
Sistemi di pagamento on-line: tecnologie	15
Sistemi di pagamento on-line: impianto normativo	10
Investigazioni digitali: le tecnologie	50
Investigazioni digitali: l'impianto normativo	35
Detection e prevenzione delle frodi	45
La formazione della prova nei processi di criminalità informatica	25
Hacking e Cybercrimes	40
Istruire una indagine digitale	40
Elementi di Criminologia	10
Psicologia Forense nelle indagini digitali	10
Stage	320
Totale	820

Qualifiche dei docenti

La Faculty è composta da Docenti di comprovata e pluriennale esperienza professionale e di consulenza provenienti dal mondo IT Security ed area giuridica.

MCT (Microsoft Certified Trainer)
CompTIA Security+
MCITP Enterprise Administrator (Microsoft Certified IT Professional)
MCSE Security (Microsoft Certified Systems Engineer)
Cisco CCNA (Cisco Certified Network Associate)
Consulente Digital Forense
Consulente Giuridico
Magistrati e Legali
Funzionari di Polizia Postale
Linux LPI Certified Professional

Materiale didattico

Durante tutta l'erogazione del Master gli studenti avranno a disposizione la piattaforma per la **Formazione a Distanza Bridge LMS** (www.bridge.it) per :

- *La Gestione di materiali didattici dei Docenti*
- *Il Monitoraggio della attività di studio, dei risultati, dei progressi degli studenti.*
- *La Interazione/animazione e cooperazione (interazione sia sincrona che asincrona con il tutor: forum di discussione e chat).*
- *Comunicazione (in modalità privata one-to-one o pubblica one-to-many).*
- *Profilazione dell'allievo e tracciamento delle sue attività.*
- *Pianificazione delle attività di erogazione/fruizione.*

Per la Fruizione dei contenuti e-learning, lo studente, necessita solo, di un PC multimediale, connesso ad internet e di cuffie e microfono .

Il materiale didattico compreso nella quota di partecipazione, oltre alle dispense, pubblicazioni e distribuite attraverso la piattaforma di e-learning Bridge è il seguente:

- Computer Forensics - Apogeo di Andrea Ghirardini e Gabriele Faggioli
- Challenges to Digital Forensic Evidence - F Cohen

Attestati

Al termine del percorso formativo i partecipanti, che non abbiano superato il 20% di assenze alle lezioni, riceveranno l'**Attestato Master Digital Forensics – Esperto in Investigazioni Digitali**.

Quota di Partecipazione

La quota di partecipazione al Master è di **€7.500,00** + Iva, (cioè €9.000 iva inclusa).

Selezione

Ai fini del buon esito dell'attività formativa e per predisporre aule omogenee, verrà effettuato un colloquio, motivazionale ed attitudinale, con un selezionatore nominato dal Comitato Tecnico-Scientifico (composto da docenti e da consulenti in Digital Forensics) o, se necessario, un test preliminare al fine di valutare la rispondenza del partecipante alle propedeuticità richieste.

Finanziamento

Il pagamento della quota di partecipazione al percorso formativo può essere dilazionato fino a 36 mesi usufruendo della nostra convenzione con "Citifinancial"

Per maggiori informazioni o per una personalizzazione del finanziamento contattaci **info@studiodelta.it** – **0805461860** specificando il percorso formativo di interesse e la durata del finanziamento.