# CORSI DI FORMAZIONE INFORMATICA FORENSE

## Modulo 1 – Digital Forensics (4 ore)

Modulo pensato per offrire le informazioni necessarie ad affacciarsi al mondo della Digital Forensics, le principali discipline che la compongono e le fasi che vanno seguite per compiere un lavoro degno di essere chiamato tale, esponendo qualche caso esemplificativo, aneddoti e credenze. Verranno infine esposte anche le principali leggi che regolano il mondo della Digital Forensics.

- Definizione di Digital Forensics
- Leggi che regolano il mondo della Digital Forensics
- Le fasi della Digital Forensics
- Identificazione
- Acquisizione
- Preservazione
- Analisi
- Presentazione dei risultati
- Le principali discipline della Digital Forensics
- Computer Forensics
- Mobile Forensics
- Electronic Forensics
- Multimedia Forensics
- Network Forensics
- Effetto CSI
- Casi reali esemplificativi, aneddoti e credenze

## Modulo 2 – Computer Forensics (4 ore)

Modulo pensato per offrire le informazioni necessarie ad approfondire il mondo della Computer Forensics, i principali strumenti hardware e software utilizzati, le informazioni che è possibile estrapolare dalle varie tipologie di dispositivo. Verranno infine esposti tutti i trucchi acquisiti in anni di esperienza e le principali problematiche che caratterizzano questo complicato mondo.

- In cosa consiste la disciplina della Computer Forensics
- I supporti di memoria
- Quali informazioni possono contenere le evidenze acquisite
- Fase di repertamento delle evidenze
- Tipologia di acquisizioni
- Writeblocker
- Duplicatori forensi e principali funzionalità
- Tool software per acquisizione e principali funzionalità
- Tool software per analisi e principali funzionalità
- Live Distro e principali software integrati
- Trucchi legati al mondo della computer forensics
- Principali problemi che caratterizzano la computer forensics

## Modulo 3 – Laboratorio di Computer Forensics (4 ore)

Modulo pratico incentrato all'apprendimento delle tecniche e all'utilizzo delle principali strumentazioni atte ad acquisire e analizzare le fonti di prova presenti all'interno di dispositivi elettronici quali Pc, hard disk, memorie di massa.

- FTK Imager
- Logicube Falcon
- Tableau TD2u
- Write Blocker hardware e software
- Distribuzioni Linux – Caine, Deft, Kali e Parrot Security
- Magnet Axiom
- Blackbag Blacklight
- Tool gratuiti Nirsoft
- Analisi delle evidenze
- Tag, filtri e generazione dei report

## Modulo 4 – Mobile Forensics (4 ore)

Modulo pensato per offrire le informazioni necessarie ad approfondire il mondo della Mobile Forensics, i principali strumenti utilizzati, le tipologie di acquisizioni e le informazioni che è possibile estrapolare dalle varie tipologie di dispositivo. Verranno infine esposti tutti i trucchi acquisiti in anni di esperienza e le principali problematiche che caratterizzano questo complicato mondo.

- In cosa consiste la disciplina della Mobile Forensics
- I dispositivi
- Quali informazioni possono contenere le evidenze acquisite
- Fase di repertamento delle evidenze
- Tipologia di acquisizioni
- Acquisizione Fisica
- Acquisizione File System
- Acquisizione Logica
- Dati che è possibile estrapolare in base alla tipologia di acquisizione
- Tool software commerciali per acquisizione e principali funzionalità
- Tool software gratuiti per acquisizione e principali funzionalità
- Tool software commerciali e gratuiti per analisi e principali funzionalità
- Trucchi legati al mondo della mobile forensics
- Principali problemi che caratterizzano la mobile forensics

## Modulo 5 – Laboratorio di Mobile Forensics (4 ore)

Modulo pratico incentrato all'apprendimento delle tecniche e all'utilizzo delle principali strumentazioni atte ad acquisire e analizzare le fonti di prova presenti all'interno di dispositivi mobili come telefoni cellulari, smartphone, tablet, schede SIM, navigatori satellitari e droni.

- Suite Cellebrite UFED
- Oxygen Forensics
- Magnet Axiom
- Root e Jailbreack
- Analisi delle evidenze
- Tag, filtri e generazione dei report

## Modulo 6 – Internet e Cloud Forensics (4 ore)

Modulo teorico-pratico incentrato all'apprendimento delle tecniche e all'utilizzo delle principali strumentazioni atte ad acquisire e analizzare le fonti di prova presenti sulla rete come siti e pagine web, account email, backup e dati di dispositivi mobili.

- Acquisizione di contenuti siti web online
- FAW (Forensics Acquisition of Website)
- Httrack (Acquisizione completa di siti web)
- Acquisizioni dati e backup dei dispositivi mobili presenti nel cloud
- UFED Cloud Analyzer
- Elcomsoft Phone Breaker
- Acquisizione di posta elettronica
- Thunderbird Portable e client di posta
- Securcube IMAP Downloader

## Modulo 7 – Audio, Image e Video Forensics (8 ore)

Quando dei contenuti multimediali (immagini digitali, flussi video, tracce audio) diventano possibili fonti di prova, la loro corretta analisi permette l'accesso a molteplici informazioni relative al dato digitale e al suo contenuto semantico. Seguire un'appropriata metodologia per l'investigazione digitale consente di conoscere la storia del contenuto multimediale: attraverso l'applicazione di tecnologie di Multimedia Forensics è possibile risalire al dispositivo di acquisizione, conoscere la data e il luogo di acquisizione, verificare l'autenticità del dato digitale e determinare eventuali falsificazioni, migliorare l'intelligibilità del contenuto ed estrarre importati informazioni semantiche. Verranno inoltre illustrate le competenze necessarie all'esperto forense per la presentazione dei risultati emersi nella fase di accertamento.

- AUDIO FORENSICS
    - Il Perito Fonico Forense, prospettive ed opportunità
    - Il Perito Trascrittore del Tribunale
    - Principi base del suono e fondamenti di audio digitale
    - Metodologie e best-practices per la gestione, analisi e presentazione dell'audio digitale in ambito forense
    - Autenticazione di file audio digitali
    - Elaborazione e miglioramento di file audio digitali
    - Interpretazione di file audio digitali: trascrizioni intercettazioni telefoniche e ambientali come consulenti della Procura o Periti del Giudice
    - Comparazione fonica con riconoscimento del parlante
    - Sessione pratica: esempi di elaborazione e miglioramento di file audio; esempi di analisi di integrità e autenticità di file audio
- IMAGE E VIDEO FORENSICS
    - Il dato digitale come possibile fonte di prova: integrità e autenticità
    - La catena di custodia del dato digitale
    - Metodologia per l'investigazione digitale dei contenuti multimediali
    - Analisi dei metadati e del formato dei dati
    - Analisi audio-visuale
    - Identificazione del dispositivo sorgente
    - Verifica autenticità
    - Miglioramento e analisi dei contenuti
    - Sessione pratica: estrazione e analisi metadati
    - Identificazione del dispositivo sorgente
    - Verifica di autenticità
    - Miglioramento e analisi dei contenuti

## Modulo 8 – Telecommunication Forensics (8 ore)

Modulo pensato per chi è interessato ad approfondire le proprie conoscenze in materia tecnico/legale delle Telecomunicazioni, nello specifico su Celle Telefoniche e Tabulati di Traffico Telefonico. Saranno oggetto del corso gli aspetti normativi e tecnici, sulla disamina di tabulati e sulla geolocalizzazione. È prevista una parte teorica e una parte pratica di laboratorio, basata sulle misurazioni sul campo della reale copertura di una cella. Lo scopo del corso è quello di fornire delle solide fondamenta per poter effettuare la disamina di tabulati telefonici, analisi di celle, normativa e legislazione sui tempi di conservazione dei dati di traffico telefonico e telematico alla luce delle recenti disposizioni. Vedranno casi reali in cui un consulente informatico forense è chiamato a rispondere, ci saranno dei cenni alle tecniche di acquisizione dei dati da dispositivi mobili.

- INTRODUZIONE ALLA RETE GSM
  - Cenni storici
  - Schema della rete GSM
  - Mobile Station
  - Configurazione e copertura delle celle
  - Procedure e caratteristiche reti 2G, 3G e 4G
- ANALISI DEI TABULATI TELEFONICI
  - Richiami sulla normativa per la conservazione dei dati
  - La direttiva 2006/24/CE
  - Come si legge un tabulato telefonico
  - Le caratteristiche dei tabulati dei principali operatori
  - Gli strumenti per l'analisi automatica
- ANALISI DELLE LOCALIZZAZIONI
  - Premesse generali sull'analisi delle celle telefoniche
  - Le mappe di copertura radioelettrica
  - Le misure sul campo
  - Strumenti di misura e di analisi
  - Le ipotesi di localizzazione

## Modulo 9 – Il Consulente Informatico Forense (4 ore)

Modulo incentrato sulla figura dell'informatico forense il quale spiega i diritti, i doveri e le procedure che un professionista del settore deve rispettare al fine di compiere al meglio il proprio lavoro. Vengono spiegate inoltre le operazioni di Descrizione e Sequestro e come è possibile redigere le Relazioni Tecniche e le varie tipologie di verbali che siano corretti e precisi sia dal punto di vista tecnico che formale.

- Figura del Consulente Informatico Forense
- Come si diventa Consulente Informatico Forense
- CTP
- CTU e Perito
- CT del PM
- Ausiliario di P.G.
- Operazione di Descrizione
- Operazione di Perquisizione e Sequestro
- Verbale di nomina Ausiliario
- Verbale di Operazioni Peritali
- Verbale di Conferimento Incarico
- Verbale di Presa in carico e riconsegna reperti
- Verbale di repertamento e catena di custodia
- La richiesta di liquidazione del compenso
- Calcolo delle vacazioni
- Lettera d'incarico
- La polizza assicurativa
- Differenza tra i vari ruoli nei procedimenti Civili e Penali
- PCT – Processo Civile Telematico
- Come si scrive una Relazione Tecnica o una Perizia

## Modulo 10 – Open Source Intelligence, Computer Vision e Riconoscimenti Facciali (4 ore)

Durante questo modulo i partecipanti impareranno le principali tecniche di ricerca da fonti aperte, vedranno software di face recognition e come si possono fare attività investigative informatiche nel complesso mondo attuale. Ci sarà una parte teorica e una parte pratica. Verranno mostrati test ed esempi di attività in tempo reale.

- OSINT
  - Definizione
  - Campi di applicazione
  - Aspetti Legali, limiti di utilizzo nei procedimenti civili e penali
  - Tecniche di indagini per tutti – le fonti aperte
  - Analisi “single shot” VS “Paterva maltego”
  - S.N.A. i software cosiddetti “Social Network Analisys” per analisi di insiemi relazionali – visione di insieme VS visione dettagliata – esempi pratici GEPHI
  - Dati di analisi in stringa VS oggetti particolari le immagini ed i video
  - Reverse search e metadati su video e immagini
- COMPUTER VISION E RICONOSCIMENTI FACCIALI
  - Il riconoscimento facciale per verifica
  - Aspetti Legali, limiti di utilizzo nei procedimenti civili e penali
  - Il riconoscimento facciale per identificazione
  - Algoritmi closed source
  - Algoritmi open source
  - OpenBr e Open Cv
  - Face_recognition e Dlib Python
  - Installazione ed utilizzo del software
  - Kairos API – ruby – pthon – php
  - Face_recognition python

## Modulo 11 – Web Reputation e Social Network Analysis (4 ore)

Durante il modulo i partecipanti impareranno le principali tecniche di ricerca da fonti aperte, in particolare verranno spiegati i principali pericoli insiti all'interno dei social network (Facebook, Twitter, Linkedin, Instagram), le relative contromisure e cosa si intende per Web Reputation. Il corso è pensato per Avvocati, Tecnici, Investigatori e Forze di Polizia, per chi è interessato ad approfondire le proprie conoscenze sulle procedure teoriche-pratiche sia tecniche sia legali di ricerca di informazioni di fonti aperte anche con l'utilizzo di software Open Source e come si effettuano attività investigative sui Social Network.

- WEB REPUTATION
  - Definizione
  - Analisi delle esigenze Aziendali del Web 3.0
  - Nuova tipologia di attacco reputazionale "fake news" & "fake phishing"
  - analisi delle esigenze dei soggetti privati e protezione delle informazioni
  - Truffe e sostituzione di persona
  - Perché non è possibile cancellare completamente la nostra Web Reputation? "robots.txt VS way-back-machine" esempi pratici con ausilio di programmi
  - Contromisure, difesa e cancellazione di alcune informazioni tramite tecniche di "confusion web reputation", esempi pratici.
- SOCIAL NETWORK ANALISYS
  - I social network in relazione alla Web Reputation
  - Analisi dei principali Social Network in relazione alla Web Reputation Aziendale e dei soggetti privati
  - Facebook analisi delle fonti aperte
  - Linkedin analisi delle fonti aperte
  - Twitter analisi delle fonti aperte
  - Instagram analisi delle fonti aperte
  - Analisi di profili fake e sostituzioni di persone
  - Social Network Analysis (SNA)
  - Contromisure

## Modulo 12 - Restauro File Audio (4 ore)

In questo modulo teorico-pratico verranno insegnate le principali tecniche di miglioramento e restauro di file audio con approfondimenti sulla teoria del suono e la sua visualizzazione. Verrà insegnato l'utilizzo di programmi professionali mostrando esempi di restauri effettuati.

- Teoria del suono
- Interpretazione dello spettrogramma e delle forme d'onda
- Introduzione ai software di restauro
- Funzionalità utilizzate nel miglioramento dei file audio
- Conversione e salvataggio degli audio

## Modulo 13 – Ethical Hacking, Penetration Testing e Sicurezza Informatica (8 ore)

Lo scopo del modulo è quello di fornire delle solide fondamenta nel mondo della Sicurezza Informatica, materia in continua trasformazione e divenire. Durante il corso i partecipanti impareranno le principali tecniche di attacco informatico, le modalità di protezione, le tecniche di valutazione del grado di sicurezza di una rete, potranno vedere un laboratorio che il relatore ha creato ad hoc appositamente per il corso. Verranno mostrati test ed esempi di attività in tempo reale.

- Information gathering - Tecniche di acquisizione di dati da fonti aperte
- Scanning & enumerazione - Sniffing di rete con wireshark e tcpdump, scansione di porte con nmap
- Vulnerability assessment - Tools per il web application
- Exploitation - Metasploit framework e nozioni di base di exploitation backdoors con metasploit e weevely
- Maintaining access - Creazione di backdoor e canali di accesso persistenti
- Nuove tipologie di minaccia - Disamina di alcune nuove tecniche di attacco relative al mondo IoT e alle nuove tecnologie emergenti
- Cenni di reportistica - Come scrivere un report di successo

# TIPOLOGIE DI CORSI CONSIGLIATI

## INFORMATICO FORENSE JUNIOR

Durata di 1 giorno (8 ore)

Corso per principianti dedicato alla chi vuole conoscere concetti di introduzione alla Digital Forensics e muovere i primi passi nell'informatica forense.
Modulo 1 – Digital Forensics (4 ore)
Modulo 2 – Computer Forensics (4 ore)

## INFORMATICO FORENSE BASE

Durata di 2 giorni (16 ore)

Corso base dedicato a chi ha voglia di imparare le best practices della Digital Forensics, come si effettua una copia forense e iniziare a fare pratica di acquisizione di dispositivi mobili.
Modulo 1 – Digital Forensics (4 ore)
Modulo 2 – Computer Forensics (4 ore)
Modulo 4 – Mobile Forensics (4 ore)
Modulo 5 – Laboratorio di Mobile Forensics (4 ore)

## INFORMATICO FORENSE MEDIO

Durata di 4 giorni (32 ore)

Corso intermedio teorico-pratico dedicato a chi ha voglia di imparare le best practices della Digital Forensics, come si effettua una copia forense e iniziare a fare pratica di acquisizione di dispositivi fissi, mobili e dati presenti nel cloud. Verrà inoltre spiegata la figura del Consulente Informatico Forense e le tecniche per effettuare restauri e pulizie di file audio.
Modulo 1 – Digital Forensics (4 ore)
Modulo 2 – Computer Forensics (4 ore)
Modulo 3 – Laboratorio di Computer Forensics (4 ore)
Modulo 4 – Mobile Forensics (4 ore)
Modulo 5 – Laboratorio di Mobile Forensics (4 ore)
Modulo 6 – Internet e Cloud Forensics (4 ore)
Modulo 9 – Il Consulente Informatico Forense (4 ore)
Modulo 12 - Restauro File Audio (4 ore)



STUDIO INGEGNERIA INFORMATICA FORENSE – Ing. Michele Vitiello Via Cefalonia, 70 25124 Brescia (BS)
Tel 030 3540238 - Cell 347 1527252 Fax 030 7771728 C.F. VTLMHL78T02G793A P.I. 01931260507
info@michelevitiello.it michele.vitiello2@ingpec.eu www.perizieforensics.it www.michelevitiello.it

## INFORMATICO FORENSE AVANZATO

Durata di 6 giorni (48 ore)

Corso avanzato teorico-pratico dedicato a chi ha voglia di padroneggiare al meglio le best practices della Digital Forensics, come si effettua una copia forense e fare pratica di acquisizione di dispositivi fissi, mobili e dati presenti nel cloud. Verrà inoltre spiegata la figura del Consulente Informatico Forense, i concetti legati alla Multimedia Forensics e il restauro dei file audio. Infine verrà proposta una panoramica completa legata alla open source intelligence, web reputation, social network analisys e riconoscimenti facciali.

Modulo 1 – Digital Forensics (4 ore)
Modulo 2 – Computer Forensics (4 ore)
Modulo 3 – Laboratorio di Computer Forensics (4 ore)
Modulo 4 – Mobile Forensics (4 ore)
Modulo 5 – Laboratorio di Mobile Forensics (4 ore)
Modulo 6 – Internet e Cloud Forensics (4 ore)
Modulo 7 – Audio, Image e Video Forensics (8 ore)
Modulo 9 – Il Consulente Informatico Forense (4 ore)
Modulo 10 – Open Source Intelligence, Computer Vision e Riconoscimenti Facciali (4 ore)
Modulo 11 – Web Reputation e Social Network Analysis (4 ore)
Modulo 12 - Restauro File Audio (4 ore)

## INFORMATICO FORENSE TOP

Durata di 8 giorni (64 ore)

Corso avanzato teorico-pratico dedicato a chi ha voglia di padroneggiare al meglio le best practices della Digital Forensics, come si effettua una copia forense e fare pratica di acquisizione di dispositivi fissi, mobili e dati presenti nel cloud. Verrà inoltre spiegata la figura del Consulente Informatico Forense, i concetti legati alla Multimedia Forensics e il restauro dei file audio. Verrà proposta una panoramica completa legata alla open source intelligence, web reputation, social network intelligence e riconoscimenti facciali. Verranno anche spiegati i concetti da conoscere per approcciare il mondo della Telecommunication Forensics e della Sicurezza Informatica.

Modulo 1 – Digital Forensics (4 ore)
Modulo 2 – Computer Forensics (4 ore)
Modulo 3 – Laboratorio di Computer Forensics (4 ore)
Modulo 4 – Mobile Forensics (4 ore)
Modulo 5 – Laboratorio di Mobile Forensics (4 ore)
Modulo 6 – Internet e Cloud Forensics (4 ore)
Modulo 7 – Audio, Image e Video Forensics (8 ore)
Modulo 8 – Telecommunication Forensics (8 ore)
Modulo 9 – Il Consulente Informatico Forense (4 ore)
Modulo 10 – Open Source Intelligence, Computer Vision e Riconoscimenti Facciali (4 ore)
Modulo 11 – Web Reputation e Social Network Analysis (4 ore)
Modulo 12 - Restauro File Audio (4 ore)
Modulo 13 – Ethical Hacking, Penetration Testing e Sicurezza Informatica (8 ore)

# DOMANDE FREQUENTI

DOV'È LA SEDE DEL CORSO E QUALI SONO LE OPZIONI DI TRASPORTO/PARCHEGGIO?

Lo STUDIO INGEGNERIA INFORMATICA FORENSE si trova a Brescia, in una posizione molto comoda ove sono presenti numerosi parcheggi, multipiano del Crystal Palace (a pagamento) o a 200 metri lungo la strada si possono trovare parcheggi gratuiti. La stazione centrale è a meno di 10 minuti a piedi, a 2 fermate di metropolitana o a 5 minuti di taxi. Gli aeroporti più vicini (circa 30-40 minuti di auto) sono Bergamo, Verona o Milano Linate. Dall'aeroporto di Bergamo Orio al Serio è disponibile una navetta che porta sino alla stazione di Brescia in circa 1 ora, con diverse corse durante la giornata per info https://autostradale.it/

È POSSIBILE PARTECIPARE AL CORSO ANCHE DA REMOTO O AVERLO NELLA PROPRIA SEDE?

Per i moduli puramente teorici è possibile effettuare il corso in videoconferenza, per le sessioni pratiche è consigliata ma non obbligatoria la presenza in studio, per le aziende è possibile averlo anche presso la propria sede.

COSA DEVO/POSSO PORTARE AL CORSO?

È utile portare un Notebook, in particolare per i moduli pratici, in modo da poter utilizzare il proprio dispositivo per fare prove e simulazioni.

COME POSSO CONTATTARE L'ORGANIZZATORE PER EVENTUALI DOMANDE?

Segreteria dal lun. al ven. 9-13 /14-18 tel. 030-3540238 info@michelevitiello.it

POSSO AVERE QUALCHE CONSIGLIO RIGUARDO AGLI ALLOGGI?

Lo studio consiglia una selezione di alberghi e bed & breackfast convenzionati, trattasi di strutture vicine alla sede e semplici da raggiungere.

VIENE RILASCIATO UN ATTESTATO?

Al termine del corso viene rilasciato un attestato di partecipazione stampato su elegante pergamena e firmato dai docenti.

POSSO AVERE LA FATTURA?

A ciascun partecipante viene rilasciata la fattura, per i possessori di partita iva verrà detratta la ritenuta d'acconto in fattura, per maggiori dettagli si prega di contattare la segreteria dal lun. al ven. 9-13 /14-18 al numero 030-3540238.

QUANTO COSTA PARTECIPARE AI CORSI?

I costi sono variabili in base alla durata, ai moduli prescelti, alla tipologia dei corsi, al numero di partecipanti, è possibile avere preventivi personalizzati.