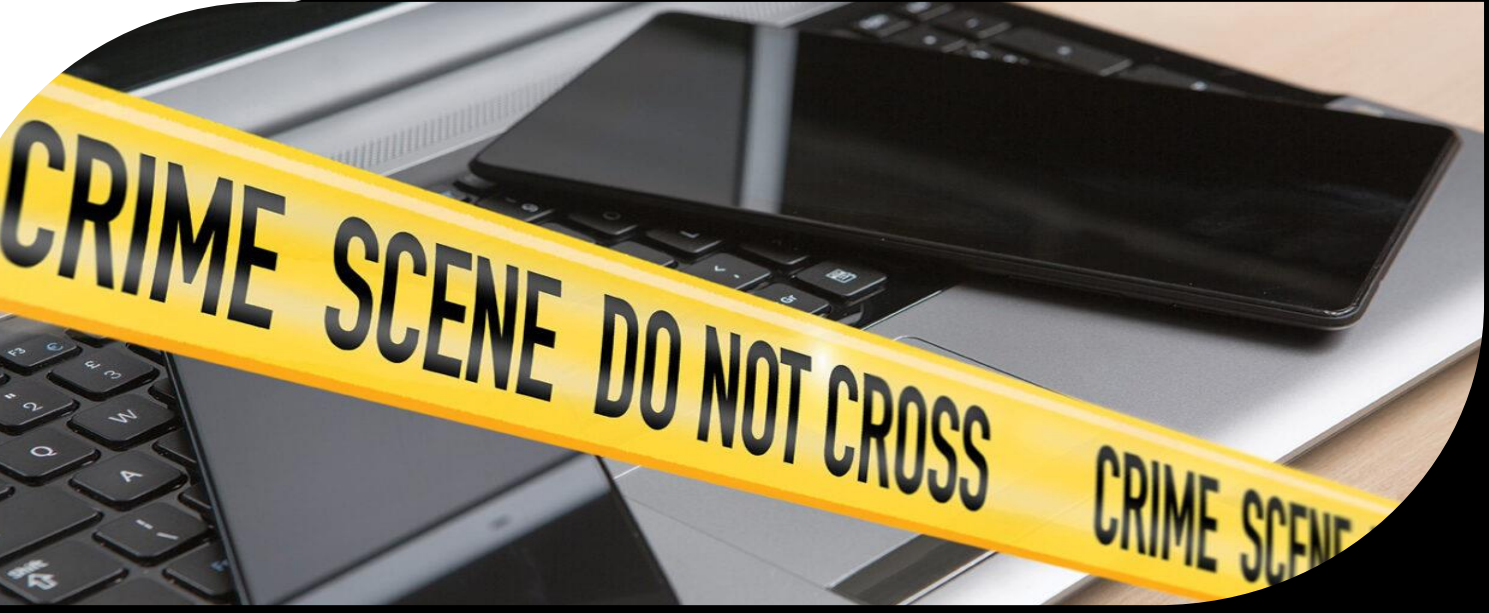

CORSO DIGITAL FORENSICS EXPERT

Corso completo di Digital Forensics

OBIETTIVO DEL CORSO

Il programma del corso racchiude tutte le attività e le competenze erogate nei moduli di Computer Forensics, Computer Forensics Lab, Computer Forensics Analysis, Mobile Forensics, Mobile Forensics Lab, Mobile Forensics Analysis, Digital Forensics e Digital Investigation. Obiettivo del corso è offrire una formazione completa sulle tematiche inerenti all'informatica forense.

DATA DELL'EVENTO

https://www.michelevitiello.it/corsi-digital-forensics/

DESTINATARI

I corsi si rivolgono a Informatici Forensi, Avvocati, Periti, CTU, CTP, CTPM, Criminologi, Criminalisti, Tecnici ICT, Studenti, Investigatori Privati che vogliono avvicinarsi al mondo dell'investigazione digitale.

DURATA 32 ore

METODOLOGIA

Online in streaming , tramite la piattaforma Google Meet. È possibile seguire direttamente da qualsiasi parte del mondo sia in forma individuale che collettiva.

Relatore: Michele Vitiello è laureato in Ingegneria delle Telecomunicazioni presso l' Università di Pisa , Professore a contratto dell'Università Telematica Internazionale Uninettuno di Roma, **Perfezionato post Laurea presso l'Università di Milano in Computer Forensics e Investigazioni Digitali, iscritto all'Ordine degli Ingegneri di Brescia, Commissario della Commissione per l'Ingegneria Forense dell'Ordine degli Ingegneri della provincia di Brescia, membro dell' IISFA, membro del DFA, socio fondatore di ONIF, Perito del Giudice, CTU, Consulente della Procura della Repubblica e Ausiliario di Polizia Giudiziaria.** Il Dott. Ing. Michele Vitiello, Titolare nonché Responsabile Scientifico dello studio, è iscritto all' Albo dei Periti n° 110 e all' Albo dei CTU n° 844 del Tribunale di Brescia, lavora sia come CTP che come CT PM/Perito/CTU. È stato nominato CTU, Perito del giudice e Consulente Tecnico del Pubblico Ministero per molte Procure della Repubblica e Tribunali di tutta Italia.

Programma del corso: verranno trattati i seguenti argomenti:

DIGITAL FORENSICS

- Definizione di Digital Forensics
- Leggi che regolano il mondo della Digital Forensics
- Le fasi della Digital Forensics
- Identificazione
- Acquisizione
- Preservazione
- Lo standard 27037/2012
- La catena di custodia
- Analisi delle evidenze
- Presentazione dei risultati
- Le principali discipline della Digital Forensics
- Computer Forensics
- Mobile Forensics
- Electronic Forensics
- Audio Forensics
- Video e Image Forensics
- Web e Cloud Forensics
- Telecommunications Forensics
- Effetto CSI
- Casi reali esemplificativi, aneddoti e credenze

DIGITAL INVESTIGATION

- La 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,di Perquisizione e Sequestro

- Verbale di nomina Ausiliario, Operazioni Peritali e di Conferimento Incarico (cenni descrittivi)
- Verbale di Presa in carico e riconsegna reperti
- Lettera d'incarico e verbale di nomina
- Catena di custodia
- La polizza assicurativa
- Differenza tra i vari ruoli nei procedimenti Civili e Penali
- PCT – Processo Civile Telematico
- Verbale di Conferimento Incarico
- La richiesta di liquidazione del compenso
- Calcolo delle vacazioni

COMPUTER FORENSICS

- La disciplina della Computer Forensics
- I supporti di memoria
- Il file system
- Dati presenti nelle evidenze
- Fase di repertamento delle evidenze
- Tipologia di acquisizioni
- Write-blocker
- Duplicatori forensi e principali funzionalità
- Il duplicatore Logicube Falcon
- Tool software per acquisizione e principali funzionalità
- Il tool FTK IMAGER
- Live Distro e principali software integrati
- Le distribuzioni Kali Linux e Parrot Security
- Le live CAINE e DEFT
- Acquisizione di caselle e-mail per indagini informatiche aziendali
- Soluzioni per acquisizione e-mail (Securecube IMAP Downloader, Mailstore)
- Acquisizione di contenuti online
- La preservazione delle copie forensi
- La funzione di hash e l'integrità
- Tool software per analisi e principali funzionalità
- Introduzione a Magnet Axiom
- Trucchi legati al mondo della computer Forensics
- Principali problemi che caratterizzano la computer Forensics

COMPUTER FORENSICS LAB

- FTK Imager
- Logicube Falcon
- Tableau TD2u

- Write Blocker hardware e software
- Acquisizione con Kali Linux
- Acquisizione con Parrot Security
- Acquisizione LIVE
- CAINE
- DEFT
- Xways Forensics
- Magnet Axiom
- Blackbag Blacklight
- Tool gratuiti Nirsoft
- Acquisizione di caselle e-mail per indagini informatiche aziendali
- Soluzioni per acquisizione e-mail (Securecube IMAP Downloader, Mailstore)
- Acquisizione di contenuti online con FAW e HTTRACK
- Fase di indicizzazione e generazione dei report con Magnet Axiom

COMPUTER FORENSICS ANALYSIS

- Introduzione a Magnet Axiom
- Report e formati portable
- Indici, tag, filtri e altri strumenti di analisi
- Tecniche investigative
- Presentazione dei risultati
- La relazione di consulenza tecnica

MOBILE FORENSICS

- 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, gratuiti per l'acquisizione
- Tool software commerciali e gratuiti per analisi e principali funzionalità
- Acquisizione di contenuti Cloud
- Trucchi legati al mondo della Mobile Forensics
- Principali problemi che caratterizzano la Mobile Forensics

MOBILE FORENSICS LAB

- Tecniche di acquisizione
- Sistemi operativi mobili
- Tipologie di acquisizione
- Acquisizione logica
- Acquisizione fisica
- Acquisizione File System
- Bootloader
- Principali problematiche di acquisizione
- La Suite Cellebrite UFED
- Oxygen Forensics
- Magnet Axiom
- Root e Jailbreak
- Acquisizione di contenuti Cloud
- Oxygen Cloud, Magnet Cloud, Google Takeout
- Indicizzazione e processing della copia forense utilizzando Cellebrite UFED

MOBILE FORENSICS ANALYSIS

- Il tool UFED Physical Analyzer
- Report e formati portable
- Indici, tag, filtri e altri strumenti di analisi
- Tecniche investigative
- Stesura dei risultati nella relazione di consulenza tecnica
- Caratteristiche della relazione tecnica

Attestati e materiale di studio fornito: per tutti i corsi viene rilasciato un Certificato di Frequenza su pergamena, che potrà essere utilizzato per gli usi di legge. Per tutti i corsi vengono rilasciati le slide complete, le dispense di studio e materiale utile di libero utilizzo (verbalistica, relazioni tecniche specifiche di base, software free o open source).

La partecipazione al corso fornisce n.20 crediti formativi professionali ANCRIM (Associazione Nazionale Criminologi e Criminalisti).

https://www.ancrim.it/