SUPSI

# CAS Informatica forense avanzata

## Descrizione

**Codice**
DTI IA

**Presentazione**

L'informatica forense ha assunto nel tempo un ruolo determinante al punto da essere considerata il miglior cybersecurity ROI. È una disciplina che si occupa di individuare, acquisire e analizzare tutto ciò che si trova in formato digitale. Con l'implementazione del GDPR e la revisione totale della legge Svizzera sulla protezione dei dati (LDP) diventa importante poter disporre in azienda di tecnici adeguatamente preparati alla trattazione professionale del dato informatico.Un errore commesso in fase di manipolazione o acquisizione delle prove potrebbe comprometterebbe irreversibilmente l'esito delle analisi informatico forensi. Per questo motivo, il Servizio di informatica forense SUPSI, offre una formazione avanzata alla sua terza edizione, innovativa e interdisciplinare, utile per apprendere le tecniche, le metodologie e gli strumenti necessari per affrontare correttamente un'analisi informatica forense che possa trattare il dato in modo autorevole e professionale.

**Obiettivi**

Comprendere attraverso un approccio learning-by-doing gli approcci e le metodologie di trattazione del dato informatico per una corretta manipolazione (individuazione, acquisizione e conservazione) attraverso i crismi offerti dall'informatica forense.

In particolare:
- Windows forensics
- Architettura e analisi di un sistema MAC OS X
- Linux come workstation forensics
- Mobile forensics
- Python per applicazioni forensi
- Network forensics
- Audio forensics
- Malware e memory forensics
- Social network forensics
- OSINT e Cloud forensics
- Analisi di sistemi biometrici per l'autenticazione
- IoT, Smartband, acquisizione dati e analisi

**Destinatari**

Il corso si rivolge ai professionisti del settore ICT che si occupano della manutenzione della sicurezza informatica o hanno il compito di gestire le emergenze in seguito a un incidente informatico in cui sono coinvolte le nuove tecnologie e i rispettivi dati aziendali, come per esempio tecnici informatici, amministratori di rete, periti e consulenti informatici.

**Requisiti**

Il corso richiede una comprovata esperienza nel campo informatico.

**Certificato**

Certificate of Advanced Studies Certificate of Advanced Studies SUPSI in Informatica forense avanzata , subordinato al superamento di tutti gli esami previsti.

**Crediti di studio**

18 ECTS

## Contenuti

### Programma

Modulo 1: Windows Forensics
- Acquisizione, analisi e data recovery del file system FAT32 e NTFS.
- Acquisizione, analisi e data recovery del file system EXT4 e HFS+.
- Introduzione di X-WAYS Forensics e il suo utilizzo durante le analisi.
- Ricerca delle evidenze mediante l'analisi del registro e degli eventi di sistema.
- Creazione e analisi di una Timeline.
- Analisi delle shadow copy.
- Analisi delle criptazioni con bitlocker.
- Analisi di un sistema virtualizzato.
- Scripting in Python.

Modulo 2: MAC OS X and Linux Forensics
- Virtualizzazione di una workstation di lavoro con MAC OS X.
- Acquisizione di un MAC OS X: CD-DVD, Single User Mode, Live, Target mode.
- Acquisizione e analisi della memoria di un MAC OS X (Analisi con Volatility).
- File System HFS+ e APFS (parsing del file system).
- APPLE time machine e recupero password di un backup criptato.
- Acquisizione di un backup criptato.
- Acquisizione di una macchina GNU\LINUX.
- Acquisizione e analisi della memoria di un GNU\LINUX.
- Ricerca delle evidenze all'interno di una macchina GNU\LINUX.
- Scripting in Python.

Modulo 3: Mobile Forensics
- Tecniche di repertazione dei dispositivi mobili.
- Tecniche di repertazione di una scheda SIM.
- Tecniche di acquisizione logica di un dispositivo con Android.
- Tecniche di acquisizione fisica di un dispositivo con Android.
- Analisi di un dispositivo con Android.
- Tecniche di acquisizione logica e fisica di un dispositivo APPLE.
- Analisi di un dispositivo APPLE.
- Acquisizione logica di un backup estratto da iCloud.
- Scripting in Python.

Modulo 4: Malware Forensics
- Introduzione alla malware analysis e all'incident response.
- Analisi delle proprietà statiche di un file "PE", analisi comportamentale e sandboxing.
- Malware persistence su sistemi Microsoft Windows.
- Simulazione di un incident response.
- Introduzione all'assembler x86/x86_64 e al reverse engineering.
- Analisi di un codice malware.
- Self defending malwares, anti-debugging e anti reversing.
- Memory forensics orientata all'incident response.
- Scripting in Python.

Modulo 5: Biometria e Tecnologie Emergenti
- Repertazione IoT e analisi di una smartband e smartwatch
- Tecniche di anti-forensics applicate ai computer e ai dispositivi mobili.
- Tecniche di repertazione delle evidenze presenti nel cloud.
- Tecniche di repertazione per la live forensics.
- Sistemi biometrici per l'autenticazione.

- Blockchain analysis e Bitcoin Forensics.
- Audio forensics: principi, metodi e strumenti usati.

Modulo 6: Advanced Network Forensics
- Introduzione al Networking dal protocollo TCP/IP alle VLAN.
- Switch di rete: analisi delle configurazioni di uno switch cisco.
- Router: analisi delle configurazione di un router cisco.
- Firewall: analisi delle configurazioni di un firewall cisco.
- IDS: configurazione e analisi di un IDS open source.
- Switch FC: introduzione al Fibre channel e analisi di uno switch cisco MDS.

### Durata

224 ore-lezione

### Responsabile/i

Dr. Alessandro Trivilini, responsabile del servizio di informatica forense SUPSI

### Relatore/i

Docenti SUPSI e professionisti ed esperti nazionali e internazionali del settore con esperienze rilevanti nel proprio ambito di specializzazione.

## Informazioni

### Iscrizione ai corsi

Entro il 15 dicembre 2018
Il numero massimo di iscritti è fissato a 15.

### Date

Modulo 1: Windows Forensics
10, 17, 24, 31 Gennaio 2019
7, 14, 21, 28 Febbraio 2019
14, 21, 28 Marzo 2019

Modulo 2: MAC OS X and Linux Forensics
4, 11, 18 Aprile 2019
2, 9, 16, 23, 29 Maggio 2019
6, 13, 18 Giugno 2019

Modulo 3: Mobile Forensics
12, 19, 26 settembre
3, 10, 17, 24 ottobre
7, 14, 21, 28 novembre 2019

Per i moduli 4, 5, e 6 previsti nell’anno accademico 2019-20 le date sono ancora da definire.

### Orari

Giovedì 17.30-21.00
Nelle seguenti date le lezioni sono previste dalle 17.30 alle 19.00 (esami di fine modulo)
28 marzo, 18 giugno e 28 novembre 2019

### Luogo

SUPSI, Dipartimento tecnologie innovative, Manno

### Costo

CHF 7’500.–
Il costo è comprensivo dei due anni di formazione, di tutti gli esami di certificazione e della documentazione didattica.

### Osservazioni

Se necessario, l’accesso alla formazione verrà convalidato dopo un colloquio individuale.

### Informazioni

SUPSI, Dipartimento tecnologie innovative, Galleria 2, 6928 Manno
tel.+41 (0)58 666 66 84
fax +41 (0)58 666 65 71
dti.fc@supsi.ch
www.supsi.ch/dti

Informazioni tecniche
alessandro.trivilini@supsi.ch