



Corso di

# Digital Forensics

SLAS//SCHOC/

— alta formazione —

# \* Partner e certificazioni \*



APP DEVELOPMENT  
WITH SWIFT  
LEVEL 1



EC-Council Associate

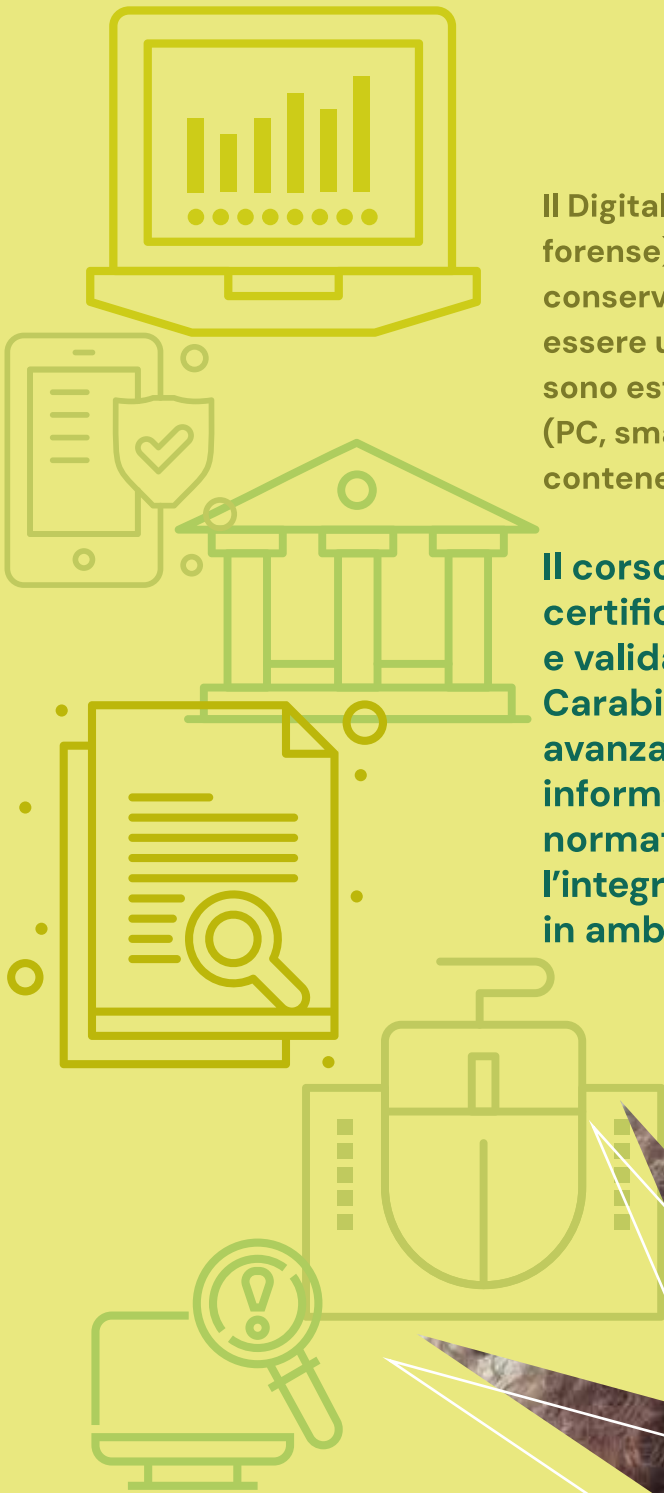


# \* Esperto in Digital Forensics? \*

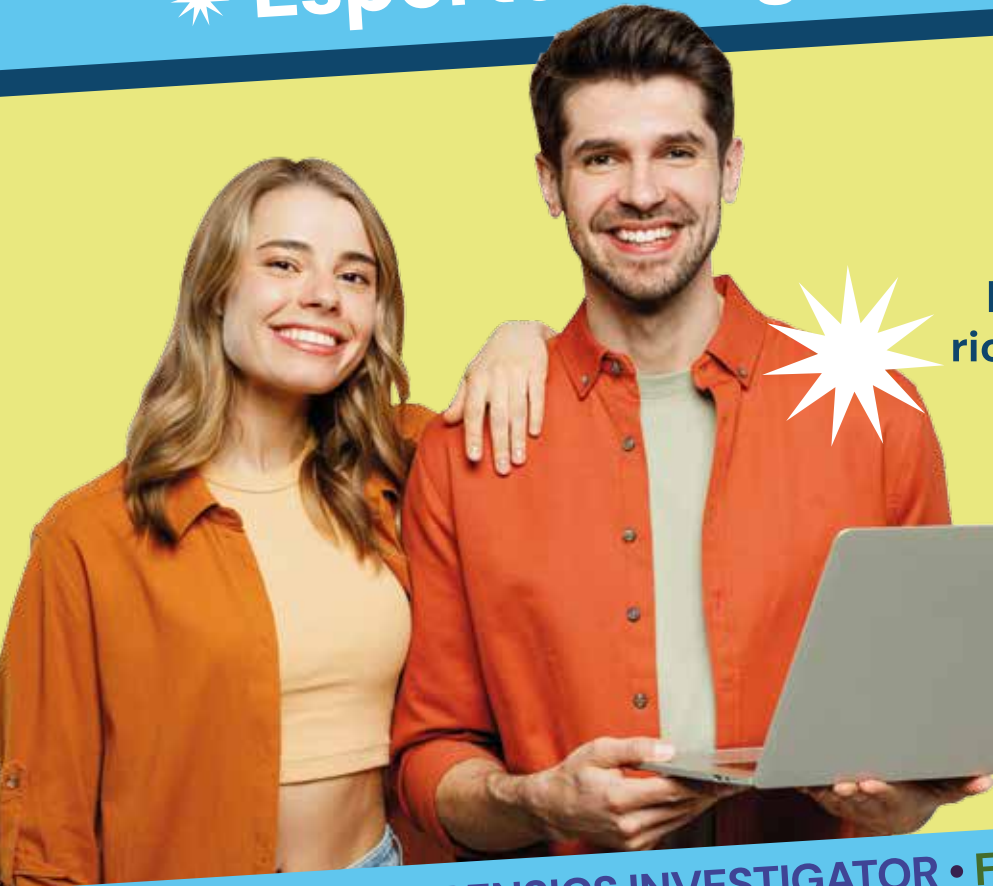


Il Digital Forensics (o esperto in Informatica forense) si occupa di raccogliere, analizzare e conservare prove digitali in modo che possano essere utilizzate in procedimenti legali. Le prove sono estratte da tutti i dispositivi elettronici (PC, smartphone, hard disk, server) che possano contenere dati digitali.

**Il corso di Digital Forensics è basato sulla certificazione CIFI, sviluppata da IISFA e valida per i concorsi dell'Arma dei Carabinieri e fornisce competenze avanzate nel settore dell'investigazione informatica, coprendo anche aspetti normativi e procedurali per garantire l'integrità delle prove e la loro ammissibilità in ambito legale.**



# Lavorare come \* Esperto in Digital Forensics \*



Ecco un esempio dei  
profili che è possibile  
ricoprire al termine del  
percorso formativo:



**DIGITAL FORENSICS INVESTIGATOR • FORENSIC ANALYST**  
**CYBERCRIME INVESTIGATOR • SECURITY CONSULTANT**  
**INCIDENT RESPONSE SPECIALIST • FRAUD ANALYST**  
**EXPERT WITNESS IN AMBITO FORENSE**  
**THREAT INTELLIGENCE SPECIALIST**



## Destinatari

Professionisti della sicurezza IT, esperti di Incident Response, esperti in Cybersecurity, forze dell'ordine e investigatori privati con interesse nella digital forensics, analisti di sicurezza e risk manager, neolaureati in informatica e cybersecurity che vogliono avviare una carriera nella Digital forensics.



## Pre-requisiti

- **Conoscenza di base dei sistemi operativi**
- **Nozioni di networking e sicurezza informatica**
- **Nozioni di sicurezza e privacy dei dati**

# ✦ Cosa ti offriamo ✦



## LEZIONI ONLINE IN DIRETTA

con registrazioni accessibili  
in qualsiasi momento



## CORSO PRATICO CON SFIDE REALI

e simulazioni degli scenari  
del contesto professionale



## PROJECT WORK FINALE

da far valere come  
tuo portfolio



## NESSUN REQUISITO DI ACCESSO

se non la volontà di  
conseguire il risultato!



## ORARI FLESSIBILI

concordati in base  
ai tuoi impegni



## AREA RISERVATA ALLO STUDENTE

con materiale didattico, test  
e simulatori esami



## SUPPORTO COSTANTE DEI DOCENTI

per facilitare  
l'apprendimento



## CERTIFICAZIONI INTERNAZIONALI

per le tue opportunità  
di carriera



## COACHING DI CARRIERA

Servizio opzionale per facilitare  
l'accesso al mondo del lavoro

# \* Il nostro piano di studi \*

## 12 MODULI DIDATTICI PER DIVENTARE ESPERTO IN DIGITAL FORENSICS

1. INTRODUZIONE ALLA DIGITAL FORENSICS
2. QUADRO LEGISLATIVO E NORMATIVO
3. RACCOLTA DELLE PROVE E CATENA DI CUSTODIA
4. ANALISI FORENSE DEI FILE SYSTEM
5. MEMORY FORENSICS E ANALISI RAM
6. NETWORK FORENSICS E ANALISI DEL TRAFFICO
7. MALWARE FORENSICS E ANALISI DI CODICE MALEVOLE
8. MOBILE FORENSICS
9. CLOUD FORENSICS E DATA RECOVERY
10. REPORTISTICA E PRESENTAZIONE DELLE PROVE
11. PORTFOLIO E PROGETTO FINALE
12. PREPARAZIONE AGLI ESAMI DI CERTIFICAZIONE

✦ Scopri il nostro ✦

# Piano di studi

nel dettaglio



# \* Piano di studi \*

## 1 > INTRODUZIONE ALLA DIGITAL FORENSICS

Affrontare una panoramica sulla Digital Forensics e il suo ruolo nell'investigazione informatica e nella sicurezza aziendale.

### Unità didattiche

- Digital Forensics e suo ambito di applicazione
  - Differenze tra Computer, Network, e Mobile forensics
  - Ciclo dell'investigazione digitale
  - Principi di integrità e affidabilità delle prove digitali
  - Introduzione agli strumenti di analisi forense
- 

## 2 > QUADRO LEGISLATIVO E NORMATIVO

Esaminare le normative e delle best practice internazionali relative alla Digital Forensics.

### Unità didattiche

- Leggi sulla privacy e protezione dei dati
  - Procedure legali per la raccolta delle prove digitali
  - Ammissibilità delle prove in tribunale
  - Catena di custodia e preservazione delle prove
  - Best practice forensi e standard internazionali
- 

## 3 > RACCOLTA DELLE PROVE E CATENA DI CUSTODIA

Esaminare le metodologie per l'identificazione, acquisizione e conservazione delle prove digitali.

### Unità didattiche

- Metodi di acquisizione delle prove digitali
  - Imaging forense e bitstream copy
  - Identificazione di dispositivi e storage media
  - Protezione della catena di custodia
  - Tecniche di write-blocking per l'integrità delle prove
- 

## 4 > ANALISI FORENSE DEI FILE SYSTEM

Approfondire i principali file system e le tecniche di recupero dei dati.

### Unità didattiche

- Analisi forense di FAT, NTFS, EXT, HFS+
- Recupero di file cancellati e frammentati
- Identificazione di timestamp e metadati
- Tecniche di carving dei dati
- Strumenti di analisi: Autopsy, FTK Imager, X-Ways

## 5 > MEMORY FORENSICS E ANALISI RAM

Conoscere le tecniche per acquisire e analizzare la memoria volatile di un sistema compromesso.

### Unità didattiche

- Fondamenti della RAM forensics
  - Strumenti di acquisizione della memoria
  - Identificazione di processi malevoli
  - Dump di credenziali e analisi malware in memoria
  - Correlazione tra memoria volatile e storage persistente
- 

## 6 > NETWORK FORENSICS E ANALISI DEL TRAFFICO

Analizzare le comunicazioni di rete per identificare attività sospette e intrusioni.

### Unità didattiche

- Introduzione alla Network Forensics
  - Strumenti di analisi del traffico (Wireshark, Zeek)
  - Identificazione di attacchi tramite analisi dei pacchetti
  - Log analysis e correlazione eventi
  - Tecniche per il tracciamento delle connessioni sospette
- 

## 7 > MALWARE FORENSICS E ANALISI DI CODICE MALEVOLE

Identificare e analizzare malware, rootkit e trojan attraverso tecniche di reverse engineering.

### Unità didattiche

- Introduzione al malware forensics
  - Tecniche di static analysis e dynamic analysis
  - Reverse engineering con IDA Pro e Ghidra
  - Strumenti di sandboxing ed emulazione
  - Rilevamento e mitigazione delle minacce
- 

## 8 > MOBILE FORENSICS

Condurre l'analisi forense su dispositivi mobili Android e iOS.

### Unità didattiche

- Fondamenti di Mobile forensics
- Tecniche di acquisizione logica e fisica
- Analisi di applicazioni e registri di sistema
- Decodifica e recupero di dati criptati
- Strumenti di mobile forensics

## 9 > CLOUD FORENSICS E DATA RECOVERY

Analizzare le prove digitali in ambienti cloud e mettere in pratica le strategie di recupero dati.

### Unità didattiche

- Introduzione alla Cloud Forensics
  - Rintracciabilità dei dati in ambienti cloud
  - Strumenti di investigazione su AWS, Azure e Google Cloud
  - Tecniche di data recovery e ripristino file
  - Implicazioni legali della Cloud Forensics
- 

## 10 > REPORTISTICA E PRESENTAZIONE DELLE PROVE

Creare report professionali e sviluppare tecniche di presentazione delle prove in tribunale.

### Unità didattiche

- Struttura di un report forense
  - Tecniche di documentazione e redazione
  - Comunicazione efficace dei risultati dell'indagine
  - Simulazione di una testimonianza forense
  - Best practice per produrre report chiari e comprensibili
- 

## 11 > PORTFOLIO E PROGETTO FINALE

Sviluppare un progetto pratico da far valere come portfolio per mostrare le proprie competenze e la capacità di applicarle in contesti reali. Affrontare scenari e studi di caso per consolidare le abilità tecniche.

### Unità didattiche

- Simulazione di un caso di Digital Forensics
  - Analisi, documentazione e presentazione delle prove
  - Creazione di un portfolio professionale
  - Simulazione di un'audizione come esperto forense
- 

## 12 > PREPARAZIONE ALL'ESAME DI CERTIFICAZIONE

Certificare le conoscenze e le competenze per aumentare la credibilità professionale, ottenere un vantaggio competitivo nel mondo del lavoro e migliorare le opportunità di carriera.

### Unità didattiche

- Analisi del syllabus delle competenze
- Svolgimento delle prove di simulazione
- Strategie e tecniche per affrontare l'esame

# \* Certificazione \*

## IISFA CIFI

La Certificazione CIFI (Certified Information Forensics Investigator) è una designazione che viene conseguita esclusivamente dai professionisti forensi più qualificati nel settore. Oltre all'adesione del codice etico IISFA, la CIFI incarna i più alti standard di conoscenza e competenza nell'ambito forense.



La CIFI comprende più domini di conoscenza, e viene rilasciata dopo il superamento di un rigoroso esame sui seguenti domini:

- IT & Fraud Auditing
- Incident Response
- Law and investigation
- Tools and techniques
- Traceback
- Contermeasures

### Il conseguimento della CIFI avviene attraverso:

1. Iscrizione come socio IISFA, effettuata per il tramite di Slash School
2. Utilizzo dei materiali didattici predisposti da IISFA sulla piattaforma <https://iisfa-elearning.com>
3. Acquisto (per il tramite di Slash School) del voucher esame CIFI

**MILANO** Via Caldera, 21

**ROMA** Via Vittorio Veneto, 54 b

**NAPOLI** Centro Direzionale, Isola E/2, 1° piano, int. 4

**AVELLINO** Piazza Libertà, 45

**MISTERBIANCO (CT)** Via A.B. Sabin angolo via Milicia, sn

**Tel. 02 30 35 76 98**

**Fax 02 30 35 76 00**

**[info@slashschool.it](mailto:info@slashschool.it)**

**SLAS//SCHOO/**  
— alta formazione —

**[www.slashschool.it](http://www.slashschool.it)**