CCFP Certification

Certified Cyber Forensics Professional

Certified Cyber Forensics Professional training course endeavors to enhance the technical understanding of the forensic techniques and processes for solving cyber-crime cases. Students will learn about malware analysis, incident response and e-discovery with forensic implementation. CCFP certification is one of the most prominent cyber forensics courses that explains how to create reports based on evidence analysis thus providing a comprehensive view of the CCFP training. As a Certified Cyber Forensics Professional you'll understand and show competence in established disciplines as well as new challenges, such as mobile forensics, cloud forensics and anti-forensics.

You must know!

Duration:
40 Hours

Who should attend?
For individuals who wish to get advanced practice in forensics techniques and procedures, standards of practice, and legal and ethical principles to assure accurate, complete and reliable digital evidence admissible to a court of law, as well as the ability to apply forensics techniques to other information security disciplines, such as e-discovery, malware analysis, or incident response

Prerequisites:
In order to get your CCFP certification you must have a four-year Bachelor's degree, or regional equivalent, as well as three years of full-time IT security or digital forensics experience in three out of the six domains of CCFP. If you do not hold a four-year Bachelor's degree, you must have six years of full time experience in three out of six domains. If you have a different forensics certification approved by (ISC)2®, you may get a one-year professional experience waiver.

CCFP Certification

Course Modules

Module 1 - Legal and Ethical Principles
This domain addresses ethical behavior and compliance with regulatory frameworks

- Nature of Evidence
- Chain of Custody
- Rules of Procedure
- Role of Expert Witness
- Codes of Ethics

Module 2 – Investigations
This domain encompasses the investigative measures and techniques required to gather digital evidence

- Investigative Process
- Evidence Management
- Criminal Investigations
- Civil Investigations
- Administrative Investigations
- Response to Security Incidents
- e-Discovery
- Intellectual Property

Module 3 – Forensic Science
This domain entails applying a broad spectrum of sciences and technologies to investigate and establish facts in relation to criminal or civil law

- Fundamental Principles
- Forensic Methods
- Forensic Planning & Analysis
- Report Writing & Presentation
- QA, Control, Management
- Evidence Analysis Correlation

CCFP Certification

Module 4 – Digital Forensics

This domain refers to the collection of any digital evidence which can be defined as data stored or transmitted via electronic means

- Media & File System Forensics
- Operating Systems Forensics
- Network Forensics
- Mobile Devices
- Multimedia & Content
- Virtual System Forensics
- Forensic Techniques & Tools
- Anti-Forensic Tech & Tools

Module 5 – Application Forensics

This domain addresses the forensics complexities of the many application types that a CCFP candidate may encounter during a forensic investigation

- Software Forensics
- Web, Email, Messaging
- Database Forensics
- Malware Forensics

Module 6 – Hybrid and Emerging Technologies

This domain contains the ever-evolving technologies that a CCFP candidate will be expected to understand

- Cloud Forensics
- Social Networks
- Big Data Paradigm
- Control Systems
- Critical Infrastructure
- Virtual/Augmented Reality

תל אביב

המרץ 2