Certified Digital Forensics Examiner

Modality: On Demand

Duration: 8 Hours

About this course:

This cyber security certification training series covers everything you need to know about becoming a certified digital forensics examiner. Students will learn about computer forensic incidents, the investigation process, disk storage concepts, digital acquisition & analysis, forensic examination protocols, digital evidence protocols, CFI theory, digital evidence presentation, computer forensic laboratory protocols, computer forensic processing, digital forensics reporting, specialized artifact recovery, e-Discovery and ESI, cell phone forensics, USB forensics, incident handling, PDA forensics, and investigating harassment.

As a Certified Digital Forensics Examiner you will have learned electronic discovery and advanced investigation techniques, and hold computer forensic knowledge that will help organizations recognize, seize, preserve and present digital evidence. You will be certified in using forensically sound investigative techniques in order to evaluate the scene, collect and document all relevant information, interview appropriate personnel, maintain chain-of custody, and write a findings report.

The average salary for a Certified Digital Forensics Examiner is **$75,660** per year.

Course Objective:

Upon completion, Certified Digital Forensics Examiner students will be able to establish industry acceptable digital forensics standards with current best practices and policies. Students will also be prepared to competently take the C)DFE exam.

The 9 Certified Computer Forensics Examiner (CCFE) Domains are as follows:

- Law, Ethics and Legal Issues
- The Investigation Process
- Computer Forensic Tools
- Hard Disk Evidence Recovery & Integrity
- Digital Device Recovery & Integrity
- File System Forensics
- Evidence Analysis & Correlation
- Evidence Recovery of Windows-Based Systems
- Network and Volitile Memory Forensics
- Report Writing

Audience:

- Security Officers
- IS Managers

- Agents/Police Officers
- Attorneys
- Data Owners
- IT managers
- IS Manager/Officers

Prerequisite:

- A minimum of 1 year in computers

Suggested prerequisite courses:

Digital Forensics Tools and Techniques

Course Outline:

- Module 01 - Introduction and Course Overview
- Module 02 - Computer Forensics Incidents
- Module 03 - Investigative Process
- Module 04 - Disk Storage Concepts
- Module 05 - Digital Acquisition and Analysis Tools
- Module 06 - Forensic Examination Protocols
- Module 07 - Digital Evidence Protocols
- Module 08 - CFI Theory
- Module 09 - Digital Evidence Presentation
- Module 10 - Computer Forensic Laboratory Protocols
- Module 11 - Computer Forensic Processing
- Module 12 - Digital Forensics Reporting
- Module 13 - Specialized Artifact Recovery
- Module 14 - e-Discovery and ESI
- Module 15 - Cell Phone Forensics
- Module 16 - USB Forensics
- Module 17 - Incident Handling
- Module 18 - PDA Forensics
- Module 19 - Investigating Harassment