Certified Digital Forensics Examiner

Modality: On Demand

Duration: 8 Hours

About this course:

Certified Digital Forensics Examiner course is part of the Cyber Security Certification training series. After completion of the Certified Digital Forensics Examiner course, an individual will gain knowledge and understanding of electronic discovery, advanced investigation techniques, and computer forensics. Through this course, an individual will also be able to recognize, present, preserve and seize digital evidence. Moreover, the course will provide a sound knowledge of forensic investigation techniques to evaluate the scene efficiently, gather relevant information and documents, maintain chain of custody, interview appropriate personnel, and present findings in report form.

Certified Digital Forensics Examiner course will cover the following topics;

- Computer forensic incidents
- Disk storage concepts
- The investigation process
- Digital acquisition and analysis
- Digital evidence protocols
- Digital evidence presentations
- Forensic examination protocols
- CFI theory
- Computer Forensic laboratory protocols
- Digital forensic reporting
- Specialized artifact recovery
- E-Discovery and ESI
- Cell phone forensics
- USB forensics
- PDA forensics
- Incident handling
- Investigating harassments

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

Course Objective:

The course objectives of the Certified Digital Forensics Examiner course is to enable an individual to develop industry acceptable digital forensic standards in line with current best practices and policies. The course is focused on providing knowledge and understanding of the nine Certified Computer Forensics Examiner (CCFE) Domains, which are as follows.

- Law, Ethics and Legal Issues
- Computer Forensic Tools

- The Investigation Process
- Digital Device Recovery & Integrity
- Hard Disk Evidence Recovery & Integrity
- File System Forensics
- Network and Volatile Memory Forensics
- Evidence Analysis & Correlation
- Evidence Recovery of Windows-Based Systems
- Report Writing

After completing the Certified Digital Forensics Examiner course, an individual will be able to pass the exam successfully.

Audience:

Following individuals can take up the Certified Digital Forensics Examiner course

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

Prerequisite:

- Minimum one-year experience in the relevant field.

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