

Digital Forensics – Computer Forensics and Electronic Discovery (Mile2)

Course Number: CFED

Length: 3 Day(s)

Certification Exam

This course will help you prepare for the following exams:

- **CCE:** Certified Computer Examiner
- **CFCE:** Certified Forensic Computer Examiner

Course Overview

The CFED course provides coverage on techniques concerning electronic records such as computer network logs, e-mails, word processing files, and .jpg picture files that provide government and corporations with important (and sometimes essential) evidence in criminal and civil cases.

Prerequisites

Students should have experience using a computer.

Audience

CFED is intended for law enforcement agents, legal professionals, corporate security personnel and other IT professionals who require systematic guidance on issues that arise in connection with electronic evidence in criminal and civil investigations.

Course Outline

- **Module 1 - Computer Forensic Incidents**
- Computer Forensic Incidents
- Introduction
- The Legal System
- Criminal Incidents
- Civil Incidents
- Computer Fraud
- Internal Threats
- External Threats
- Investigative Challenges
- Module 1 Review
- **Module 2 - Digital Incident Response**
- Digital Incident Response
- Digital Incident Assessment

- Initial Assessment
- Type of Incident
- Parties Involved
- Incident / Equipment Location
- Available Response Resources
- Securing Digital Evidence
- Chain of Custody
- Potential Digital Evidence
- Module 2 Review
- **Module 3 - OS / Disk Storage Concepts**
- OS / Disk Storage Concepts
- Disk Based Operating Systems
- OS / File Storage Concepts
- Disk Storage Concepts 1
- Demo - Creating a file and writing it to FAT/NTFS
- Disk Storage Concepts 2
- Slack Space
- File Management
- File Formats
- Demo - Using Quick View Plus
- Module 3 Review
- **Module 4 - Digital Acquisition & Analysis Tools**
- Digital Acquisition & Analysis Tools
- Digital Acquisition
- Terms Defined
- Demo - Generic Hash Demo / CryptoDemo
- Demo - Hashing a File
- Digital Acquisition Procedures 1
- Demo - Winhex Software
- FTK Explorer / EnCase
- Demo - EnCase Acquisition
- Digital Acquisition Procedures 2
- Digital Forensic Analysis Tools
- Demo - FTK
- Module 4 Review
- **Module 5 - Forensic Examination Protocols**
- Forensic Examination Protocols
- What is Forensic Science?
- Applying the Scientific Method
- Cardinal Rules
- Alpha “5”
- Demo - Create Disk Images
- Demo - Data Recovery Exercise
- “The 20 Basic Steps”
- Demo - File Carving Exercise
- Module 5 Review

- **Module 6 - Digital Evidence Protocols**
- Digital Evidence Protocols
- Digital Evidence Concepts
- Data Files: Active Data
- Data Files: Archival Data
- Data Files: Backup Data
- Data Files: Residual Data
- Data Files: Electronic Mail (E-Mail)
- Data Files: Background Data
- Data Files: Metadata
- Digital Evidence: Admissibility
- Digital Evidence: In Summary
- Demo - Viewing Metadata of a Graphic File
- Demo - Detailed Lab Exam of Evidence
- Module 6 Review
- **Module 7 - Digital Evidence Presentation**
- Digital Evidence Presentation
- The Best Evidence Rule
- Digital Evidence: Hearsay
- Authenticity and Alteration
- Layman's Analogies
- Module 7 Review
- Course Closure