

Certified Digital Forensics Examiner™

KEY DATA



Course Name: CDFE V3.0

Duration: 5 days

Language: English

Format: Instructor-led
(Lecture and Lab)

Prerequisite:

Experience in using a computer

Student Materials:

- Student workbook
- Student reference manual
- Software/ tools 2 x DVDs

Certification Exam:

- CDFE – Certified Digital Forensics Examiner

Certification Track:

- CDFE – Certified Digital Forensics Examiner
- CPTEng – Certified Pen Testing Engineer
- CPTC -- Certified Pen Testing Consultant

BENEFITS OF THIS COURSE

This course will benefit companies, organizations, individuals and government security agencies intent on pursuing any corrective action, litigation or proof of guilt based on digital evidence.

A case in point could be the termination of an employee for a violation that may involve a digital artifact to support the allegation. The investigator must furnish irrefutable burden of proof derived from the digital artifact. If not, then an attorney who is knowledgeable about Computer Forensics would have the case thrown out. Similarly, Government or investigative agencies need to be able to successfully prosecute or defend cases such as acts of fraud, computer misuse, illegal pornography or counterfeiting and so forth.

COURSE OVERVIEW

Computer Forensics was developed by U.S. federal law enforcement agents during the mid to late 1980s to meet the challenges of white-collar crimes being committed with the assistance of a PC. By 1985 enforcement agents were being trained in the automated environment and by 1989 software and protocols were beginning to emerge in the discipline.



The Certified Digital Forensics Examiner program is designed to train Cyber Crime and Fraud Investigators whereby students are taught electronic discovery and advanced investigation techniques. This course is essential to anyone encountering digital evidence while conducting an investigation.

UPON COMPLETION

Certified Digital Forensics Examiner graduates will obtain real world computer forensic knowledge that will help them recognize, seize, preserve and present digital evidence. Graduates will be able to confidently attempt mile2's Forensics certification:

Certified Digital Forensics Examiner (CDFE)

COURSE DETAILS

Topics Covered

- Module 1:** Computer Forensic Incidents
- Module 2:** Digital Incident Response
- Module 3:** OS/Disk Storage Concepts
- Module 4:** Digital Acquisition & Analysis Tool
- Module 5:** Forensic Examination Protocols
- Module 6:** Digital Evidence Protocols
- Module 7:** Digital Evidence Presentation
- Module 8:** Computer Forensic Investigative Theory
- Module 9:** Computer Forensic Laboratory Protocols
- Module 10:** Computer Forensic Processing Techniques
- Module 11:** e-Discovery and Electronically Stored Information
- Module 12:** Crypto and Password Recovery
- Module 13:** Specialized Artifact Recovery



I. Computer Forensic Incidents

- Lesson Objectives
- The Legal System
- Criminal Incidents
- Civil Incidents
- Criminal Incidents
- Computer Fraud
- Internal Threats
- External Threats
- Investigative Challenges
- Power of Digital Forensics
- Common Frame of Reference
- Removable Media Volume
- Media Volume
- PC Hard Drive Capacities

- Typical Household Plus Work Site?
- Investigative Challenges

II. Digital Incident Response

- Lesson Objectives
- Digital Incident Assessment
- Type of Incident
- Parties Involved
- Incident/Equipment Location
- Available Response Resources
- Securing Digital Evidence
- Chain of Custody
- Potential Digital Evidence
- Summary

III. OS/Disk Storage Concepts

- Lesson Objectives
- Disk Based Operating Systems
- OS / File Storage Concepts
- Disk Storage Concepts
- Slack Space
- File Management
- File Formats

IV. Digital Acquisition & Analysis Tool

- Lesson Objectives
- Digital Acquisition
- Digital Acquisition Procedures
- DC3 Operations

Digital Forensic Analysis Tools

- Forensic Toolkit (FTK)™

- EnCaseTM
- I-Look InvestigatorTM
- ProDiscover DFTTM

V. Forensic Examination Protocols

- Lesson Objectives
- Forensic Examination Protocols
- Cardinal Rules
- Alpha “5”
- The 20 Basic Steps

LAB 1- Forensic Examination

VI. Digital Evidence Protocols

- Lesson Objectives
- Digital Evidence Concepts
- Digital Evidence Categories
- Digital Evidence: Admissibility
- Digital Evidence: In Summary
- Case Study Exercise

VII. Digital Evidence Presentation

- Lesson Objectives
- Digital Evidence Presentation
- The Best Evidence Rule
- Hearsay
- Authenticity and Alteration
- Layman’s Analogies
- Layman’s Analogy for Storage
- Digital Evidence: Summary
- Case Study Final

VIII. Computer Forensic Investigative Theory

- Lesson Objectives
- Digital Evidence
- Locard Exchange Principle
- Digital Forensic Science
- Three Aspects to Digital Evidence Reconstruction
- "Attack" Guidelines for recovery
- Classification
- Comparison and Individualization
- Melissa Virus
- Contents, Function, and Characteristics
- Reconstruction
- Temporal Aspects of Digital Evidence
- Behavioral Evidence Analysis
- Equivocal Forensic Analysis
- Stages of Digital Evidence Examination
- Victimology
- Incident Scene Analysis

IX. Computer Forensic Laboratory Protocols

- Lesson Objectives
- Overview
- Quality Assurance
- Standard Operating Procedures
- Reports
- Peer Review
- Who Should Review?
- Consistency
- Accuracy
- Research
- Validation
- Relevance

- Liability/Legal Considerations
- Peer Review
- Annual Review
- Deviation
- Lab Intake
- Tracking
- Storage
- Discovery

X. Computer Forensic Processing Techniques

- Lesson Objectives
- Goal of Digital Processing Techniques
- Pre-Exam Analysis
- Duplication
- Documentation
- Disassemble
- Disconnect
- Exceptional Circumstances
- Write Protection
- Storage Devices
- Host Protected Area
- Hardware Equipment
- Software
- Prepare for Media/Digital Evidence Examination
- Recording the Logical Drive Structure
- Examine FAT Tables
- Logical Processes
- Reference Data Sets
- Examine System Files
- File Signature
- Final Investigative Report

XI. e-Discovery and Electronically Stored Information

- What is e-Discovery?
- What is ESI?
- Discoverable ESI Material
- eDiscovery Notification
- Required Disclosures: Initial Disclosures
- eDiscovery Conference
- About Preserving Information
- Merely Agreeing to Preserve ESI is Not Sufficient
- eDiscovery Liaison
- The Form of eDiscovery Products
- Metadata
- What is Metadata?
- The Real Deal, Metadata
- A Data Retention Architecture
- “Safe Harbor” : Rule 37 (f)
- eDiscovery Spoliation
- Tools for eDiscovery
- In Summary: eDiscovery

XII. Crypto and Password Recovery

- Lesson Objectives
- Cryptography
- Steganography
- History
- Concepts
- File Protection
- Options

XIII. Specialized Artifact Recovery

- Lesson Objectives
- Background

- Overview
- System Preparation Stage
- Windows File Date/Time Stamps
- File Signatures
- Image File Databases
- The Windows OS
- Windows Registry
- Windows Registry Hives
- Windows Alternate Data Streams
- Windows Unique ID Numbers
- Decode GUID's
- Other ID's
- Historical Files
- Windows Recycle Bin
- Copy out INFO2 for Analysis
- Process INFO2 with Data-Lifter
- Outlook E-mail
- Outlook 2k/Workgroup E-mail
- Outlook Express 4/5/6
- Web E-mail