

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

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.

BENEFITS OF THIS COURSE

The CDFE course will benefit organizations, individuals, government offices, and law enforcement agencies interested in pursuing litigation, proof of guilt, or corrective action based on digital evidence.

An example of “corrective action” would be the termination of an employee for a violation of computer usage where digital evidence was needed to support the allegation. The investigator must furnish an irrefutable burden of proof based on that digital evidence. If not irrefutable, an attorney knowledgeable about Computer Forensics could have the case thrown out of court. Government or investigative agencies need proper training to succeed in cases like the above as well as those including acts of fraud, computer misuse, illegal pornography, counterfeiting, and so forth.

WHO IS THIS COURSE FOR

Anyone who is or may be to be involved in examining electronic devices for digital artifacts (i.e. evidence) needed for company, legal, or law enforcement investigations.

Also available as:

LIVE REMOTE TRAINING

Attend live class from anywhere in the world!

- Live Presentations with Powerful functionality that delivers easy viewing of slides and other documents, shared Internet access, virtual whiteboard, and a media center all through an easy-to-use toolbar.
- Application, file, and desktop sharing enable you to view live demonstrations.
- Dedicated high spec remote PC per student with full access as if you are sitting in-front of the PC in the classroom.
- Instructor views each students session when you perform your hands on labs, the instructor can access your remote system to demonstrate and assist while you sit back to absorb the classroom style mentoring you expect.
- Public and private text chat allows for increased interactivity between students and instructor



COURSE HISTORY

Computer Forensics as a field was born and developed by U.S. federal law enforcement agents during the mid to late 1980s. New techniques were needed 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. mile2's originally had two courses forensics related courses: CFED (Computer Forensics and Electronic Discovery) and AFCT (Advanced Forensics Computer Techniques). These courses and related materials were created by practitioners in the forensics field. In 2008 CFED and AFCT were combined into the CDFE course. Course content and materials are updated periodically to keep up with technology and concepts in the digital forensics field.

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:

MAJOR TOPICS COVERED

- Module 0: **Introduction**
- Module 1: **Computer Forensic Incidents**
- Module 2: **Digital Incident Response**
- Module 3: **OS/Disk Storage Concepts**
- Module 4: **Digital Acquisition & Analysis Tools**
- 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**

C)DFE COURSE OUTLINE

I. Computer Forensics Incidents

This is an introduction to the field of computer forensics and the basis for gathering electronic digital artifacts. Students are introduced to the concepts, situations and personalities they may encounter while investigating a computer incident.

- Origins of Computer Forensic Science
- 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

Proper seizure of digital media is the start of every computer investigation. Students learn the correct protocol relating to handling of evidence.

- 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

Having a clear understanding of how data is stored is having the upper hand during any investigation. Operating systems have a systematic way of storing data that is not understood by most users. Here you will learn hard drive storage dynamics and understand "lost" data recovery methods

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

IV. Digital Acquisition & Analysis Tools

Multiple software and hardware solutions are covered during this session. Students learn the numerous tools available to them in a vendor neutral environment. A clear understanding of what the tools do and how they work is presented in layman's terms.

- Digital Acquisition
- Digital Acquisition Procedures
- DC3 Operations
- Digital Forensic Analysis Tools
 - Forensic Toolkit (FTK)™
 - EnCase™
 - I-Look Investigator™
 - ProDiscover DFT™

V. Forensic Examination

Protocols This section covers the advanced procedures necessary to conduct an accurate and carefully documented computer forensic examination.

- Forensic Examination Protocols
- Four Cardinal Rules
- Alpha 5
- The 20 Basic Steps
- **LAB 1- Forensic Examination**

VI. Digital Evidence Protocols

Students learn core principles surrounding the topic of digital evidence, including how it is viewed from a legal perspective.

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

VII. Digital Evidence Presentation

Students are introduced to aspects of presenting digital evidence in a courtroom environment. They are exposed to the specialized tools necessary to effectively create and present the results of a cyber crime investigation to an administrative body or court of law. Both civil and criminal incidents are covered during this lesson..

- 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

- 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

- 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

- 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 & 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. Cryptography & Password Recovery

Covers digital encryption file structures and password-protected data that an investigator may encounter while conducting and examining. Students are exposed to methods to decode and crack passwords that are used to protect potential evidence. They also learn techniques to gain access to encrypted files that may reside within the information.

- Cryptography
- Steganography
- History

- Concepts
- File Protection
- Options

XIII. Specialized Artifact Recovery

This module teaches forensic examination of certain specialized aspects of digital media. The focus is on utilizing advanced automated tools for the recovery of digital artifacts that are unattainable by conventional methods.

- 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

