CDFE
Certified Digital Forensics Examiner

Overview
The Certified Digital Forensics Examiner vendor-neutral certification 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. Mile2's Certified Digital Forensics Examiner training teaches the methodology for conducting a computer forensic examination. Students will learn to use 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.

Upon Completion
Upon completion, the Certified Digital Forensics Examnier candidate will be able to competently take the CDFE exam.

Course Length
5 days

Format
- Instructor-led classroom
- Instructor-led Online Training

Prerequisites
- A minimum 1 year in computers

Student Materials
- Student Workbook
- Student Lab Guide
- Exam Prep Guide

Certification Exam

The Certified Digital Forensics Examiner exam is taken online through Mile2's Assessment and Certification System ("MACS"), which is accessible on your mile2.com account. The exam will take 2 hours and consist of 100 multiple-choice questions.

Who Should Attend?

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

Course Contents

- Module 0 - Introduction
- Module 1 – Computer Forensic Incidents
- Module 2 - Incident Handling
- Module 3 - Computer Forensic Investigative Theory
- Module 4 - Computer Forensic Investigative Process
- Module 5 - Digital Acquisition
- Module 6 - Disks and Storages
- Module 7 - Forensic Evidence Protocols
- Module 8 - Digital Evidence Protocols
- Module 9 - Digital Evidence Presentation
- Module 10 – Computer Forensic Laboratory Protocols
- Module 11- Computer Forensic Processing Techniques
- Module 12 - Specialized Artifact Recovery
- Module 13- e-Discovery and ESI
- Module 14- Mobile Device Forensics
- Module 15- Digital Forensics Reporting

Lab Outline

- Scenario
- Lab 1 - Chain of Custody
- Lab 2 – Identify Seized Evidence
- Lab 3 - Device Acquisition
- Lab 4 - Prepare the Case Evidence
- Lab 5 - Investigate the Acquired Evidence
- Lab 6 - Prepare the Case Evidence
- Lab 7 - Finding Clues
- Lab 8 - Construct the Case Events
- Lab 9 - Tie Evidence found to the seized Android Device
- Lab 10 - Incident Response