Certified Digital Forensics Examiner

Duration: *5 Day(s)*

Course Overview

The Certified Digital Forensics Examiner vendor neutral certificationis 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 aninvestigation. 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.The Certified Digital Forensics Examiner 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. **Mile2 Accreditations:**

1. Accredited by the **NSA CNSS 4011-4016**
2. Is approved and has been placed on Homeland Security's National Initiative for Cyber Security Careers and Studies (**NICCS) training providers** and maps to the **National Cybersecurity Workforce Framework**
3. Preferred cyber certification for the **FBI**

Review this course online at https://www.alta3.com/courses/C)DFE

Objectives

- Establish industry-acceptable digital forensics standards.
- Implement best practices and policies for digital evidence handling.
- Conduct comprehensive computer forensic examinations.
- Prepare to competently take the Certified Digital Forensics Examiner exam.

Who Should Attend

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

Prerequisites

A minimum of 1 year in computers

Course Outline

Module 1: Introduction

Module 2: Computer Forensic Incidents

Module 3: Investigation Process

Module 4: Disk Storage Concepts

Module 5: Digital Acquisition & Analysis

Module 6: Forensic Examination Protocols

Module 7: Digital Evidence Protocols

Module 8: CFI Theory

Module 9: Digital Evidence Presentation

Module 10: Computer Forensic Laboratory Protocols

Module 11: Computer Forensic Processing Techniques

Module 12: Digital Forensics Reporting

Module 13: Specialized Artifact Recovery

Module 14: e-Discovery and ESI

Module 15: Mobile Device Forensics

Module 16: USB Forensics

Module 17: Incident Handling