Certified Digital Forensics Examiner

Course Title: Certified Digital Forensics Examiner

Duration: 5 days

Class Format Options:

Instructor-led classroom
Live Online Training

Prerequisites:

- A minimum of 1 year in computers

Student Materials:

- Student Workbook
- Student Lab guide
- Exam Prep guide

Certification Exams:

- Mile2 C)DFE – Certified Digital Forensics Examiner

CPEs: 40 Hours

WHO SHOULD ATTEND?

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

COURSE 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.

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.

UPON COMPLETION

Upon completion, **Certified Digital Forensics Examiner** students will be able to establish industry acceptable digital forensics standards with current best practices and policies. Students will also be prepared to competently take the C)DFE exam.

Forensics Career

C)DFE™ *

C)NFE™ CERTIFIED NETWORK FORENSICS ENGINEER

All combos include:

- Online Video
- Electronic Book (Workbook/Lab guide*)
- Exam Prep Questions
- Exam

C)DFE™

mile2®
CYBER SECURITY CERTIFICATIONS

ACCREDITATIONS

NICCS™
NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

mile2 is **ACCREDITED** by the **NSA CNSS 4011-4016**
Is **MAPPED** to NIST/Homeland Security NICCS's Cyber Security Workforce Framework
is **APPROVED** on the **FBI Cyber Security Certification Requirement list (Tier 1-3)**

EXAM INFORMATION

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. The cost is $400 USD and must be purchased from Mile2.com.

macs Assessment & Certification System

COURSE CONTENT

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 Forensics**
Module 15: **Digital Forensics Reporting**

LAB OUTLINE

Scenario
Lab 1 – Chain of Custody
Lab 2 – Identify Seized Evidences
Lab 3 – Devices 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

COURSE OUTLINE

Module 0 – Course Introduction

Module 1 – Computer Forensics Incidents

- Section 1 – Origins of digital forensic science
- Section 2 – Differences between criminal and civil incidents
- Section 3 – Types of computer fraud incidents
- Section 4 – Internal and external threats
- Section 5 – Investigative challenges

Module 2 – Incident Handling

- Section 1 – What is an Incident?
- Section 2 – Incident Handling Steps
- Phase 1: Preparation
- Phase 2: Identification and Initial Response
- Phase 3: Containment
- Phase 4: Eradication
- Phase 5: Recovery
- Phase 6: Follow-up

Module 3 – Computer Forensic Investigative Theory

- Section 1 – Investigative Theory
- Section 2 – Investigative Concepts
- Section 3 – BEA & EFA

Module 4 – Computer Forensic Investigative Process

- Section 1 – Investigative Prerequisites
- Section 2 – Investigation Process

Module 5 – Digital Acquisition

- Section 1 – Acquisition Procedures
- Section 2 – Evidence Authentication
- Section 3 - Tools

Module 6 – Disks and Storages

- Section 1 – Disk OS and Filesystems
- Section 2 – Spinning Disks Forensics
- Section 3 – SSD Forensics
- Section 4 – Files Management

Module 7 – Forensic Examination Protocols

- Section 1 – Science Applied to Forensics
- Section 2 – Cardinal Rules & Alpha 5
- Section 3 – The 20 Basic Steps of Forensics

Module 8 – Digital Evidence Protocols

- Section 1 – Digital Evidence Categories
- Section 2 – Evidence Admissibility

Module 9 – Digital Evidence Presentation

- Section 1 – The Best Evidence Rule
- Section 2 - Hearsay
- Section 3 – Authenticity and Alteration

Module 10 – Computer Forensic Laboratory Protocols
Module 11 – Computer Forensic Processing Techniques
Module 12 – Specialized Artifact Recovery

- Section 1 – Forensics Workstation Prep
- Section 2 – Windows Components with Investigative Interest
- Section 3 – Files Containing Historical Information
- Section 4 – Web Forensics

Module 13 – eDiscovery and ESI
Module 14 – Mobile Forensics

- Section 1 – Cellular Network
- Section 2 – Forensic Process
- Section 3 - Tools
- Section 4 – Paraben Forensics

Module 15 – Digital Forensics Reporting

DETAILED LAB OUTLINE

Scenario
Lab 1 – Chain of Custody

- Section 1 – Create logs for each piece of evidence available

Lab 2 – Identify Seized Evidences

- Section 1 – Identify the Evidences
- Section 2 – Update Chain of Custody Document

Lab 3 – Devices Acquisition

- Section 1 – Acquire the 2012 Server
- Section 2 – Acquire the Windows 10 Laptop

Lab 4 – Prepare the Case Evidence

- Section 1 – Add 1st Evidence to Autopsy
- Section 2 – Learn to Navigate with Autopsy
- Section 3 – Extract Registry

Lab 5 – Investigate the Acquired Evidence

- Section 1 – Find and record basic information
- Notes and Answer

Lab 6 – Prepare the Case Evidence

- Section 1 – Add 2nd Evidence to Autopsy
- Section 2 – Extract Registry
- Section 3 – Investigate the Evidence

Lab 7 – Finding Clues

- Section 1 – Find Installed Applications
- Notes and Answers

Lab 8 – Construct the Case events

- Section 1 – Using emails information, answer the questions below
- Section 2 – Using gathered information, answer the questions below
- Section 3 – Testing the discovered tools in an isolated VM
- Notes and Answers

Lab 9 – Tie evidence found to the seized Android device

- Section 1 – Add Android Image to Autopsy
- Section 2 – Continue constructing the case
- Notes and Answers

Lab 10 – Incident Response

- Section 1 – Memory Capture
- Section 2 – Registry Hives
- Section 3 – Export directories from the Hard Drive
- Section 4– Analysis
- Section 5– Memory Analysis
- Section 5– Static Analysis