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 Examinervendor 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)SS™ CERTIFIED SECURITY SENTINEL

C)ISSO™ Certified Information Systems Security Officer

C)DFE*™

C)NFE™ CERTIFIED NETWORK FORENSICS ENGINEER

All combos include:

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

ias™ INFORMATION ASSURANCE SERVICES · pt™ PENETRATION TESTING · dr™ DISASTER RECOVERY · gs™ GENERAL SECURITY · sc™ SECURE CODING · vbp™ VIRTUALIZATION BEST PRACTICES · ws™ WIRELESS SECURITY · cf™ COMPUTER FORENSICS

ACCREDITATIONS

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.

COURSE CONTENT

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**

LAB OUTLINE

Mile2 - Lab 1: Preparing Forensic Workstation
AccessData FTK Imager Installation
Autopsy Installation
National Software Reference Library (NSRL) for autopsy
7z Installation
Install Registry Viewer
Install Password Recovery Tool Kit (PRTK – 5.21)
Mile2 - Lab 2: Chain of Custody
Chain of Custody Search and Seizure
Chain of Custody Forensic Imaging
Mile2 - Lab 3: Imaging Case Evidence / FTK Imager

Mile2 - Lab 4: Create a new case for Autopsy
Creating a Case in Autopsy

Mile2 - Lab 5: Reviewing Evidence / Autopsy (Case #1)
User MTBG attempting to hack his/her previous employer
Reviewing Evidence in Autopsy
Case Study scenario:
The evidence you are required to discover (Challenge)
Final Report for MTBG case
Mile2 - Lab 6: Reviewing Evidence / Autopsy (Case #2)
Greg Schardt case
Case Study Scenario:
The evidence you are required to discover (Challenge)
Final Report for Greg Schardt case

C)DFE™

mile2®
CYBER SECURITY CERTIFICATIONS

COURSE OUTLINE

Module 1 – Introduction

- Lesson Objectives
- Introductions (Instructor)
- Introductions (Students)
- Disclaimers
- Notice
- Course Schedule
- Student Guide (Layout)
- Introduction to Computer Forensics
- Course Objectives

Module 2 - Computer Forensic Incidents

- Lesson Objectives
- The Legal System
- Criminal Incidents
- Civil Incidents
- Computer Fraud
- Internal Threats
- Investigative Challenges
- Common Frame of Reference
- Media Volume

CDFE Module 3 – Investigation Process

- Lesson Objectives
- Investigating Computer Crimes
- Prior to the Investigation
- Forensics Workstation
- Building Your Team of Investigators
- Who is involved in Computer Forensics?
- Decision Makers and Authorization
- Risk Assessment
- Forensic Investigation Toolkit
- Investigation Methodology
- Preparing for an Investigation
- Search Warrant
- Forensic Photography
- Preliminary Information
- First Responder
- Collecting Physical Evidence
- Collecting Electronic Evidence
- Guideline for Acquiring Electronic Evidence
- Securing the Evidence
- Managing the Evidence
- Chain of Custody
- Duplicate the Data
- Verify the Integrity of the Image
- Recover Last Data
- Data Analysis
- Data Analysis Tools
- Assessing the Evidence
- Assessing the Case
- Location Assessment
- Best Practices
- Documentation
- Gathering and Organizing Information
- Writing the Report
- Expert Witness
- Closing the Case

Module 4 - OS Disk Storage Concepts

- Lesson Objectives
- Disk Based Operating Systems
- OS / File Storage Concepts

- Disk Storage Concepts

Module 5- Digital Acquisition and Analysis

- Lesson Objectives
- Digital Acquisition
- Digital Acquisition Procedures
- Digital Forensic Analysis Tools

Module 6 - Forensic Examination Protocols

- Lesson Objectives
- Forensic Examination Protocols
- Forensic Examination

Module 7 - Digital Evidence Protocols

- Lesson Objectives
- Digital Evidence Concepts
- Digital Evidence Categories
- Digital Evidence: Admissibility

Module 8 - CFI Theory

- Lesson Objectives
- Computer Forensic Investigative Theory

Module 9 - Digital Evidence Presentation

- Lesson Objectives
- Digital Evidence Presentation
- Digital Evidence
- Digital Evidence: Hearsay
- Digital Evidence: Summary

Module 10 Computer Forensics Lab Protocols

- Lesson Objectives
- Overview
- Quality Assurance
- Standard Operating Procedures
- Reports
- Peer Review
- Who should review?
- Peer Review
- Consistency
- Accuracy
- Research
- Validation
- Relevance
- Peer Review
- Annual Review
- Deviation
- Lab Intake
- Tracking
- Storage
- Discovery

Module 11 CF Processing Techniques

- Lesson Objectives
- Computer Forensic Processing Techniques

Module 12 - Digital Forensics Reporting

- Lesson Objectives
- Analysis Report
- Definition
- Computer Sciences
- Ten Laws of Good Report Writing

- Cover Page
- Table of Contents
- Examination Report
- Background
- Request
- Summary of Findings
- Forensic Examination
- Tools
- Evidence
- Items of Evidence
- Analysis
- Findings
- Conclusion
- Exhibits
- Signatures

Module 13 - Specialized Artifact Recovery

- Lesson Objectives
- Prep System Stage
- Lesson Objectives
- Background
- Overview
- Prep System Stage
- Windows File Date/Time Stamps
- File Signatures
- Image File Databases
- The Windows OS
- Windows Registry
- Alternate Data Streams
- Windows Unique ID Numbers
- Decode GUID's

- Historical Files
- Windows Recycle Bin
- Copy out INFO2 for Analysis
- Web E-mail

Module 14 - eDiscovery and ESI

- Lesson Objectives
- eDiscovery
- Discoverable ESI Material
- eDiscovery Notification
- Required Disclosure
- eDiscovery Conference
- Preserving Information
- eDiscovery Liaison
- eDiscovery Products
- Metadata
- What is Metadata?
- Data Retention Architecture
- “Safe Harbor” Rule 37(f)
- eDiscovery Spoliation
- Tools for eDiscovery

Module 15 - Cell Phone Forensics

- Lesson Objectives
- Cell Phones
- Types of Cell Networks
- What can a criminal do with Cell Phones?
- Cell Phone Forensics
- Forensics Information in Cell Phones
- Subscriber Identity Module (SIM)
- Integrated Circuit Card Identification (ICCID)
- International Mobile Equipment Identifier (IMEI)
- Electronic Seal Number (ESN)
- Helpful Hints for the Investigation
- Things to Remember when Collecting Evidence
- Acquire Data from SIM Cards

- SIM Cards
- Cell Phone Memory
- Analyze Information
- Analyze
- Cell Phone Forensic Tools
- Device and SIM Card Seizure
- Cell Phone Analyzer
- Tools
- Forensic Card Reader
- ForensicSIM Tool
- Forensic Challenges
- Paraben Forensics Hardware
- Paraben Forensics Hardware
- Paraben: Remote Charger
- Paraben: Device Seizure Toolbox
- Paraben: Wireless Stronghold Tent
- Paraben: Passport Stronghold Bag
- Paraben: Project-a-phone
- Paraben: Project-a-phone
- Paraben: SATA Adapter
- Paraben: Lockdown
- Paraben: SIM Card Reader
- Paraben: Sony Clie
- Paraben: CSI Stick
- Paraben: USB Serial DB9 Adapter
- Paraben: P2 Commander

Module 16 - USB Forensics

- Lesson Objectives
- USB Components
- USB Forensics
- USB Forensics Investigation
- Determine USB Device Connected
- Tools for USB Imaging

Module 17 - Incident Handling

- Lesson Objectives
- Incident Handling Defined
- What is a security event?
- Common Security Events of Interest
- What is a security incident?
- What is an incident response plan?
- When does the plan get initiated?
- Common Goals of Incident Response Management
- Incident Handling Steps
- Goal
- Be Prepared
- The Incident Response Plan
- Incident Handling
- Incident Response Plan
- Roles of the Incident Response Team
- Incident Response Team Makeup
- Challenges of building an IRT
- Incident Response Training and Awareness
- Jump Kit
- Prepare Your Sites and Systems
- Goal
- Identification of an Incident
- Basic Incident Response Steps
- Proper Evidence Handling
- Goal
- Containment
- Onsite Response
- Secure the Area
- Conduct Research
- Make Recommendations
- Establish Intervals

- Capture Digital Evidence
- Change Passwords
- Goal
- Determine Cause
- Defend Against Follow-on Attacks
- More Defenses
- Analyze Threat and Vulnerability
- Restore System(s) to Operation
- Goal
- Report Findings
- Restore System
- Verify
- Decide
- Monitor Systems
- Goal
- Follow-up Report