

Description:

The Certified Digital Forensics Examiner, C)DFE certification is designed to train Cyber Crime and Fraud Investigators. 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.

Through the use of a risk -based approach, the C)DFE is able to implement and maintain cost-effective security controls that are closely aligned with both business and industry standards.

Annual Salary Potential

$

65,000

AVG/year



|  |  |  |  |
| --- | --- | --- | --- |
| Key Course Information |  | Modules/Lessons | Labs |
| **Live Class Duration:** 5 Days  **CEUs:** 40  **Language:** English    **Class Formats Available:**    Instructor Led    Self-Study    Live Virtual Training    **Suggested Prerequisites:**   * 1 YR experience in computers * Mile2’s C)SP course * Mile2’s Foundational Course Pack |  | **Module 1** – Computer Forensic  Incidents  **Module 2** – Investigative Theory  **Module 3** – Investigative Process  **Module 4** – Digital Acquisition and  Analysis Tools  **Module 5** – Disks and Storages  **Module 6** – Live Acquisitions  **Module 7** – Windows Forensics  **Module 8** – Linux Forensics  **Module 9** – Mac Forensics  **Module 10** – Examination Protocols  **Module 11** – Digital Evidence  Protocols  **Module 12** – Digital Evidence  Presentation  **Module 13** – Laboratory Protocols  **Module 14** – Artifact Recovery  **Module 15** – Advanced Search Strings  **Module 16** – eDiscovery and ESI  **Module 17** –Mobile Forensics  **Module 18** – Incident Handling  **Module 19** – Reporting | **Lab 1** – Chain of Custody  **Lab 2** – Identify Seized Evidences  **Lab 3** – Devices Acquisition  **Lab 4** – Memory Acquisition  **Lab 5** – Prepare the Case Evidence  **Lab 6** – Investigate the Acquired  Evidence  **Lab 7** – Prepare the Case Evidence  **Lab 8** – Windows Event Logs  Analysis  **Lab 9 –** Linux Primary Info  Retrieval  **Lab 10** – Investigate OSX Evidence  **Lab 11** – Finding Clues  **Lab 12** – Construct the Case  Events    **Lab 13** -Evidence found from a  Seized Android Device  **Lab 14** – Incident Response |

# Who Should Attend

* Virtualization Admins
* Cloud Security Officers
* CIO
* Virtualization and Cloud Auditors
* Virtualization and Cloud

Compliance Officers

# 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..

# Accreditations Exam Information

The Certified Digital Forensics Examiner exam is taken online through Mile2’s Learning Management System and is accessible on you Mile2.com account. The exam will take approximately 2 hours and consist of 100 multiple choice questions.



A minimum grade of 70% is required for certification.

Re-Certification

Requirements

All Mile2 certifications will be awarded a 3-year expiration date.

There are two requirements to maintain Mile2 certification:

1. Pass the most current version of the exam for your respective existing certification
2. Earn and submit 20 CEUs per year in your Mile2 account.

# Course FAQ’s

**Question:** Do I have to purchase a course to buy a certification exam?

**Answer**: No

**Question:** Do all Mile2 courses map to a role-based career path?

**Answer**: Yes. You can find the career path and other courses associated with it at [www.mile2.com.](http://www.mile2.com/)

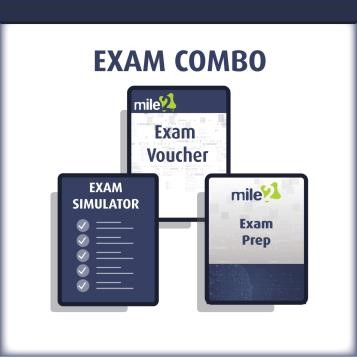
**Question:** Are all courses available as self-study courses?

**Answer**: Yes. There is however 1 exception. The Red Team vs Blue Team course is only available as a live class.

**Question:** Are Mile2 courses transferable/shareable?

**Answer:** No. The course materials, videos, and exams are not meant to be shared or transferred.

Course and Certification Learning Options



# DETAILED OUTLINE

## Module 1 – Computer Forensics Incidents

* Origins of digital forensic science
* Differences between criminal and civil incidents
* Types of computer fraud incidents
* Internal and external threats
* Investigative challenges
* Industry Standards

## Module 2 – Computer Forensic Investigative Theory

* Investigative Theory
* Investigative Concepts
* Behavioral evidence analysis (BEA) & Equivocal Forensic Analysis (EFA)

## Module 3 – Computer Forensic Investigative Process

* Investigative Prerequisites
* Scene Management
* The digital forensics process
* ISO 27043

## Module 4 – Digital Acquisition and Analysis Tools

* Acquisition Procedures
* Computer forensics field triage process model (CFFTPM)
* Acquisition Authentication
* Forensic Tools

## Module 5 – Disks and Storages

* Disk OS and Filesystems
* Spinning Disks Forensics
* SSD Forensics
* Files Management
* Handling Damaged Drives

## Module 6 – Live Acquisitions

* Live Acquisition
* Apple Acquisition
* Linux/UNIX Acquisition

## Module 7 – Windows Forensics

* Windows Event Viewer Overview
* EVTX and EVT Logs
* Logs Analysis to Identify Breaches and Attacks

## Module 8 - Linux Forensics

• Linux Artifacts o File System Structure o Basic Identifiers

* Common Log Files

**Module 9 – MAC Forensics** • OSX Artifacts o File System Structure o Core Storage o Default Apps

* Other Artifacts

## Module 10 – Forensic Examination Protocols

* Science Applied to Forensics
* Cardinal Rules
* Alpha 5
* The 20 Basic Steps of Forensics
* Scientific Working Group on Digital Evidence (SWGDE) Standard
* International Organization on Computer Evidence (IOCE) Standard

## Module 11 – Digital Evidence Protocols

* Digital Evidence Categories
* Evidence Admissibility

## Module 12 – Digital Evidence Presentation

* The Best Evidence Rule
* Hearsay
* Authenticity and Alteration

**Module 13 – Computer Forensic Laboratory Protocols** • Forensics Lab Standard Operating Procedures o Quality Assurance o Quality Control o Peer Review o Annual Review o Deviations o Lab Intake

## Module 14 – Specialized Artifact Recovery

* Forensics Workstation Prep
* Windows Components with Investigative Interest
* Files Containing Historical Information
* Web Forensics

## Module 15 – Advanced Search Strings and File Signatures

* Search Strings
* RegEx
* File Signatures

## Module 16 – eDiscovery and ESI

• Electronically Stored Information Rules o Legal System o Disclosure o Rule 37 o eDiscovery Tools

## Module 17 – Mobile Forensics

* Cellular Network
* Forensic Process
* Tools
* Paraben Forensics

**Module 18 – Incident Handling** • What is an Incident?

* Incident Handling Steps o Preparation o Identification and Initial Response

o Containment o Eradication o Recovery o Follow-up

## Module 19 – Digital Forensics Reporting

• Report Sections and Content