Certified Digital Forensics Examiner

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

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

Modules/Lessons

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 – Digital Forensics Examiner Protocols
Module 8 – Evidence Protocols
Module 9 – Evidence Presentation
Module 10 – Computer Forensic Laboratory Protocols
Module 11 – Computer Forensic Processing Techniques
Module 12 – Artifact Recovery
Module 13 – e-Discovery and ESI
Module 14 – Device Forensics
Module 15 – Reporting

Labs

Lab 1 – Chain of Custody
Lab 2 – Identify Seized Evidences
Lab 3 – Devices Acquisition
Lab 4 – Prepare 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

*All labs are performed in our Cyber Range® on our Ghost Pentesting Platform®

Certified Digital Forensics Examiner

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.

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:

Course Introduction

Module 1 – Computer Forensics Incidents

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

Module 2 – Incident Handling

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

Module 3 – Computer Forensic Investigative Theory

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

Module 4 – Computer Forensic Investigative Process

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

Module 5 – Digital Acquisition

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

Module 6 – Data Security

1. Section 1 – Disk OS and Filesystems
2. Section 2 – Spinning Disks Forensics

3. Section 3 – SSD Forensics
4. Section 4 – Files Management

Module 7 – Forensic Examination Protocols

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

Module 8 – Digital Evidence Protocols

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

Module 9 – Digital Evidence Presentation

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

Module 10 – Computer Forensic Laboratory Protocols

Module 11 – Computer Forensic Processing Techniques

Module 12 – Specialized Artifact Recovery

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

Module 13 – eDiscovery and ESI

Module 14 – Mobile Forensics

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

Module 15 – Digital Forensics Reporting

Detailed Lab Outline:

Lab 1: Chain of Custody

Lab 2: Identify Seized Evidences

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

Lab 3: Devices Acquisition

1. Section 1 – Acquire the Server
2. Section 2 – Acquire the Windows 10 Laptop

Lab 4: Prepare the Case Evidence

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

Lab 5: Investigate the Acquired Evidence

Lab 6: Prepare the Case Evidence

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

Lab 7: Finding Clues

Lab 8: Construct Case Events

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

Lab 9: Tie Evidence Found to the Seized Android Device

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

Lab 10: Incident Response

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