# Certified Digital Forensics Examiner

The **Certified Digital Forensics Examiner (CDFE)** course delivers a complete, modern approach to digital investigations. Students will learn the methodology and processes needed to properly seize, preserve, acquire, and analyze digital evidence across diverse environments. From traditional computer systems to mobile devices and emerging IoT technologies, the course ensures examiners are prepared for today's investigative challenges.


Designed for both hands-on practitioners and managers overseeing forensic operations, CDFE blends technical depth with legal and managerial perspective. Every step of the forensic process is aligned with international standards (**ISO/IEC 27037, NIST 800-101**) to ensure findings are defensible in court.

## COURSE DETAILS:

- **Core Forensic Methodology** – Evidence handling, acquisition methods, and analytical best practices.
- **Operating System Forensics** – Windows, Linux, and macOS investigations with emphasis on system artifacts and timeline reconstruction.
- **Data Acquisition Techniques** – Logical, file system, physical, and cloud acquisitions, with comparisons of strengths and limitations.
- **Specialized Investigations** – Artifact recovery, eDiscovery/ESI, live acquisitions, and memory forensics.
- **Mobile & IoT Forensics** – A focused overview of processes and tools for iOS, Android, wearables, and smart devices.
- **Forensic Tools Mastery** – Exposure to leading platforms (Cellebrite, Magnet AXIOM, Oxygen, MSAB XRY, Paraben E3:DS, GrayKey).
- **Legal & Ethical Considerations** – Chain of custody, admissibility, privacy issues, and expert witness testimony.
- **Comprehensive Scope** – Covers the full spectrum of digital forensics while addressing current trends like cloud, mobile, and IoT.
- **Courtroom Ready** – Evidence handling and reporting practices aligned with global standards.
- **For All Roles** – Balanced for technical examiners, investigators, managers, and compliance/legal professionals.
- **Career Impact** – Strengthens credibility and career advancement in law enforcement, cybersecurity, corporate security, and consulting.

**Annual Salary Potential: $65,000 AVG/YR**

# Certified Digital Forensics Examiner

## 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

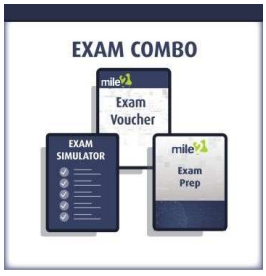
**Module 01** – Forensics Incidents
**Module 02** – Forensic Investigative Theory
**Module 03** – Forensic Prerequisites and Standards
**Module 04** – Forensic Investigative Process
**Module 05** – Forensic Examination/Evidence Protocols
**Module 06** – Digital Acquisition and Analysis Tools
**Module 07** – Disks and Storages
**Module 08** – Live Acquisitions
**Module 09** – Windows Forensics
**Module 10** – Linux Forensics
**Module 11** – MAC Forensics
**Module 12** – Specialized Artifact Recovery
**Module 13** – Advanced Search Strings and File Signatures
**Module 14** – Mobile Forensics
**Module 15** – eDiscovery
**Module 16** – Computer Forensic Laboratory Protocols
**Module 17** – Digital Evidence Presentation and Reporting

## Labs

**Lab 01** – Chain of Custody
**Lab 02** – Identify Seized Evidence
**Lab 03** – Device Acquisition
**Lab 04** – Memory Acquisition
**Lab 05** – Prepare the Case Evidence
**Lab 06** – Investigate the Acquired Evidence
**Lab 07** – Add Additional Case Evidence
**Lab 08** – Windows Event Logs Analysis
**Lab 09** – Linux Primary Info Retrieval
**Lab 10** – Investigate OSX Evidence
**Lab 11** – Finding Clues
**Lab 12** – Regex
**Lab 13** – Data Carving
**Lab 14** – Specialized Artifact Recovery
**Lab 15** – Construct the Case Events
**Lab 16** – Tie Evidence to Android
**Lab 17** – Incident Response

## Course and Certification Learning Options





# Certified Digital Forensics Examiner

## Who Should Attend

- Digital Forensic Examiners & Investigators
- Law Enforcement & Military Personnel
- Cybersecurity Professionals & Incident Responders
- Legal & Compliance Specialists
- IT Managers & Security Leaders
- Corporate Investigators & Fraud Analysts

## 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.

## Exam Information

The Certified Digital Forensics Examiner exam is taken online through Mile2's Learning Management System and is accessible on your Mile2.com account. The exam will take approximately 2 hours and consists 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 FAQs

**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.

## Accreditations

## DETAILED OUTLINE

**Module 1 – Computer Forensics Incidents**

- Origins of digital forensic science
- Legal System
- Types of Cybercrime Incidents
- Internal and external threats

**Module 2 – Computer Forensic Investigative Theory**

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

**Module 3 – Computer Forensic Prerequisites and Standards**

- Investigative Prerequisites
- Scene Management
- Industry Standards

**Module 4 – Computer Forensic Investigative Process**

- Foundations of the Digital Forensics Process
- Identification & Scope
- Collection & Preservation
- Examination
- Analysis & Interpretation
- Documentation & Interim Reporting
- Quality Control & Review

**Module 5 – Forensic Examination/Evidence Protocols**

- Science Applied to Forensics
- Digital Evidence Categories
- Evidence Admissibility

**Module 6 – Digital Acquisition and Analysis Tools**

- Acquisition Procedures
- Computer forensics field triage process model (CFFTPM)
- Evidence Authentication
- Forensic Tools
- AI and Forensics

**Module 7 – Disks and Storages**

- Disk OS and Filesystems
- Spinning Disks Forensics
- SSD Forensics (IoT-Mention)
- Cloud Storage
- Handling Damaged Drives

**Module 8 – Live Acquisitions**

- Live Acquisition
- Windows Acquisition
- MacOS Acquisition
- Linux/UNIX Acquisition
- Cloud/Virtualization Acquisition

**Module 9 – Windows Forensics**

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

**Module 10 – Linux Forensics**

- Linux Artifacts
    - File System Structure
    - Basic Identifiers
    - Common Log Files

**Module 11 – MAC Forensics**

- OSX Artifacts
    - File System Structure
    - Default Apps
    - Other Artifacts

**Module 12 – Specialized Artifact Recovery**

- Windows Components with Investigative Interest
- Files Containing Historical Information
- Web Forensics
- Memory Forensics

**Module 13 – Advanced Search Strings and File Signatures**

- Search Strings
- REGEX (Regular Expressions)
- Files Signatures (Formats, Headers, and HEX Analysis)

**Module 14 – Mobile Forensics**

- Forensic Process
- Tools
- IoT and Wearables
- Legal Considerations

**Module 15 – eDiscovery**

- eDiscovery
- Laws and Regulations
- eDiscovery Process

**Module 16 – Computer Forensic Laboratory Protocols**

- Forensics Workstation Prep
- Forensics Lab Standard Operating Procedures
- Quality Assurance
- Quality Control
- Peer Review
- Annual Review
- Deviations
- Lab Intake

**Module 17 – Digital Evidence Presentation and Reporting**

- The Best Evidence Rule
- Hearsay
- Authenticity and Alteration
- Report Sections and Content