

CERTIFIED DIGITAL FORENSICS EXAMINER

KEY DATA

Course Title: C)DFE

Duration: 5 days

CPE Credits: 40

Class Format Options:

Instructor-led classroom
Live Online Training
Computer Based Training

Who Should Attend:

Forensic Auditors
Law Enforcement
IS Managers

Prerequisite:

Experience in using a computer.

Provided Materials:

Student Workbook
Student Reference Manual
Student Lab Guide
Software/Tools (DVDs)

Certification Exam:

C)DFE: Certified Digital Forensics Examiner

Certification Track:

C)DFE – Certified Digital Forensics Examiner
C)PTE– Certified Pen Testing Engineer
C)PTC -- Certified Pen Testing Consultant

COURSE OVERVIEW

Digital Forensics is the investigation and recovery of data contained in digital devices. This data is often the subject of investigations in litigation, proof of guilt, and corrective action in an organization. When the time comes that you need to investigate your organization, will you have the skill set necessary to gather the digital data that you need? The Certified Digital Forensics Examiner course will benefit organizations, individuals, government offices, and law enforcement agencies in performing these investigations and reporting their findings.

To illustrate, let's say an employee needs to be terminated for a violation of computer usage rules. To do so the organization must furnish an irrefutable burden of proof based on digital evidence. If not irrefutable, an attorney knowledgeable about Digital Forensics could have the case thrown out of court. Government and investigative agencies need proper training to succeed in cases like the above as well as those including acts of fraud, computer misuse, illegal pornography, counterfeiting, and so forth. A C)DFE is aptly prepared to handle these types of situations.

UPON COMPLETION

Students will:

- Have knowledge to perform digital forensic examinations
- Have knowledge to accurately report on their findings from examinations
- Be ready to sit for the C)DFE Exam.

COURSE HISTORY

Computer Forensics as a field was born and developed by U.S. federal law enforcement agents during the mid to late 1980s. New techniques were needed to meet the challenges of white-collar crimes being committed with the assistance of a PC. By 1985 enforcement agents were being trained in the automated environment and by 1989 software and protocols were beginning to emerge in the discipline. Mile2 originally had two forensics courses: CFED (Computer Forensics and Electronic Discovery) and AFCT (Advanced Forensics Computer Techniques). These courses and related materials were created by practitioners in the forensics field. In 2008 CFED and AFCT were combined into the CDFE course. Course content and materials are updated regularly to keep up with technology and concepts in the digital forensics field.

Also available as:

LIVE VIRTUAL TRAINING

Attend live classes from anywhere in the world!

Visit Mile2.com for more information

ABOUT THE AUTHOR

Johnny Justice - C)DFE, CEI, CSSA, ECSA, CHFI, Linux+, and CEH

Johnny Justice has been working with computers since 2005. He has been in the U.S. Army for over 13 years working as a Counterintelligence Agent (Computer Forensics, 8 years). He has taught Introduction to UNIX/ LINUX, Network Essentials, and Theories and Application / Digital Technology. Johnny has developed courseware and training materials as well as presented these materials in the classroom. Johnny is working with an IT Security company to create an Online Learning Management System that provides training for IT Certifications (i.e. CompTIA, Cisco, Microsoft, ISC2 and Mile2). Johnny holds a variety of certifications: C) DFE, CEI, CSSA, ECSA, CHFI, Linux+, and CEH. He co-authored the 2012 update to the Certified Digital Forensics Examiner course and the 2013 Certified Network Forensics Engineer at Mile2. He graduated from American Military University in May 2008 with a Bachelor's of Science degree in Information Technology Management. Also, he graduated Magna Cum-Laude in 2012 from Nova Southeastern University with a Master's of Science degree in Computer Science Education.

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
Module 12: Digital Forensics Reporting

Module 13: Specialized Artifact Recovery
Module 14: e-Discovery and ESI
Module 15: Cell Phone Forensics
Module 16: USB Forensics
Module 17: Incident Handling
Appendix 1: PDA Forensics
Appendix 2: Investigating Harassment
Lab 1: Preparing Forensic Workstation
Lab 2: Chain of Custody
Lab 3: Imaging Case Evidence / FTK Manager
Lab 4: Reviewing Evidence / Access Data Tools
Review and Exam

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 C)DFE exam will take roughly 2 hours and consist of 100 multiple choice questions. The cost is \$300 USD and must be purchased from the store on Mile2.com.

DETAILED LAB DESCRIPTION

Labs 1-4 Objective Summary

Recovering electronically stored data for civil litigation
Recovering, categorizing and analyzing data
Hiding and discovering potential evidence
Investigating a misappropriations of proprietary information complaints
Bit-by-bit imaging digital media and preserving the integrity of the image
Identifying and reconstructing information within various file systems
Conducting an investigation into a complaint of sexual harassment
Understanding anti-forensics and steganography
Discover how a computer has been used and learn:
What websites have been visited?
What data has been deleted, and why?
What data is stored on the hard drive?
What e-mails have been sent and received?
Has data been copied off of the computer?

Lab 1 - Preparing Forensic Workstations

AccessData FTK Imager Installation
AccessData FTK Installation
KFF Library Database Installation

AccessData Registry Viewer Installation
AccessData Password Recovery Toolkit Installation

Lab 2 - Chain of Custody

Chain of Custody Search and Seizure

Chain of Custody Forensic Imaging

Lab 3 - Imaging Case Evidence / FTK Imager

Lab 4 - Reviewing Evidence / AccessData Tools

Creating a Case in AccessData Forensic Toolkit
Review Evidence in AccessData FTK Imager
Review Software File in AccessData Registry View

Review System File in AccessData Registry Viewer
Review SAM File in AccessData Registry Viewer

DETAILED MODULE DESCRIPTION

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

Internal Threats

The Legal System
Criminal Incidents
Civil Incidents
Computer Fraud

Investigative Challenges
Common Frame of Reference
Media Volume

Module 3 - Investigation Process

Lesson Objectives
Investigating Computer Crimes
Prior to the Investigation
Forensics Workstation
Building Your Team of Investigators
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

Who is involved in Computer Forensics?
Decision Makers and Authorization
Risk Assessment
Forensic Investigation Toolkit
Investigation Methodology
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 – Computer Forensic Investigative 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
Reports
Peer Review
Who should review?
Peer Review
Consistency
Accuracy
Research
Validation

Quality Assurance
Standard Operating Procedures
Relevance
Peer Review
Annual Review
Deviation
Lab Intake
Tracking
Storage
Discovery

Module 11 - Computer Forensics 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
Request
Summary of Findings
Forensic Examination
Tools
Evidence

Cover Page
Table of Contents
Examination Report
Background
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 Products

eDiscovery
Discoverable ESI Material
eDiscovery Notification
Required Disclosure
eDiscovery Conference
Preserving Information
eDiscovery Liaison

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: Remote Charger
Paraben: Device Seizure Toolbox
Paraben: Wireless Stronghold Tent
Paraben: Passport Stronghold Bag
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

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

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
Restore System(s) to Operation
Goal
Report Findings
Restore System
Verify

Capture Digital Evidence
Change Passwords
Goal
Determine Cause
Defend Against Follow-on Attacks
More Defenses
Analyze Threat and Vulnerability
Decide
Monitor Systems
Goal
Follow-up Report

Appendix 1 - PDA Forensics

Lesson Objectives
Personal Digital Assistants
Characteristics
Palm OS
Palm OS Architecture
Pocket PC
Windows Mobile Architecture
Linux-based PDAs

Linux OS for PDAs-Architecture
Typical PDA State
Security Issues
ActiveSync and HotSync
PDA Forensic Steps
Tips for Conducting the Investigation
PDA Forensic Tools
Countermeasures

Appendix 2 - Investigating Harassment

Lesson Objectives
Sexual Harassment Overview
Examples of Sexual Harassment
What it is not?

Approach of General Investigation
Conduct Your Investigation
Preventative Action