

Computer Forensics & Electronic Discovery™

KEY DATA



Course Name: CFED V2.0

Duration: 5 days

Language: English

Format: Instructor-led
CBT & LVT
(Lecture and Lab)

Prerequisite:

Experience in using a computer

Student Materials:

- Student workbook
- Student reference manual
- Software/ tools 2 x DVDs

Certification Exam:

- CCE -- Certified Computer Examiner
- CFCE -- Certified Forensic Computer Examiner

Certification Track:

- CEDL – Certified Electronic Discovery Litigator
- CCE – Certified Computer Examiner
- CFCE-- Certified Forensic Computer Examiner
- CPTS – Certified Pen Testing Specialist
- CPTE -- Certified Pen Testing Expert

BENEFITS OF THIS COURSE

This course will benefit private or government security agencies as well as companies and organizations intent on pursuing any corrective action, litigation or proof of guilt based on digital evidence.

A case in point could be the termination of an employee for a violation that may involve a digital artifact to support the allegation. The investigator must furnish irrefutable burden of proof derived from the digital artifact. If not, then an attorney who is knowledgeable about Computer Forensics would have the case thrown out. Similarly, Government or investigative agencies need to be able to successfully prosecute or defend cases such as terrorist activities, illegal pornography, acts of fraud or counterfeiting and so forth.

COURSE OVERVIEW

Computer Forensics was developed by U.S. federal law enforcement agents during the mid to late 1980s 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.

The Computer Forensics Training Boot Camp program is designed to train Cyber Crime Investigators whereby students are taught electronic discovery and advanced investigation techniques. This course is essential to anyone encountering digital evidence while conducting an investigation.

Also available as..

Live Virtual Training (LVT)

bringing live instructors to you anywhere.....

Features:

- Live presentations & powerful functionality delivering our proprietary slides, documents, virtual whiteboards, and a media-center through an easy-to-use toolbar.
- Application, file, and desktop sharing.
- One dedicated high-spec remote PC per student with full access as if sitting in our classroom.
- Instructors view your remote session when you perform hands on labs.
- Instructor can access your remote system to demonstrate or assist! Real classroom style mentoring.
- Public and private text chat for increased interactivity between participants and easily saved to file.



UPON COMPLETION

Computer Forensics Training Boot Camp graduates will obtain real world computer forensic knowledge that will help them recognize, seize, preserve and present digital evidence. Graduates will be able to confidently attempt the following professional computer forensic certifications:

1. The Certified Computer Examiner (CCE) ® certification.
2. The external Certified Forensic Computer Examiner (CFCE) certification.

COURSE DETAILS

Topics Covered

- Module 1:** Introduction to Computer Crime
- Module 2:** Disk Storage Concepts
- Module 3:** Forensic Examination
- Module 4:** Electronic Discovery and Digital Evidence
- Module 5:** Specialized Examination Tools
- Module 6:** Seizure Concepts
- Module 7:** Forensic Examination
- Module 8:** Advanced Artifact Recovery
- Module 9:** Crypto and Password Recovery
- Module 10:** Specialized Digital Media Analysis and Recovery
- Module 11:** Cyber-terrorism and Internet Investigations
- Module 12:** Electronic Discovery, Acquisition and Analysis Laboratory
- Module 13:** Documenting and Reporting Digital Evidence
- Module 14:** Presentation of Digital Evidence



Module 1: Introduction to Computer Crime

This is an introduction to the field of computer forensics and the basis for gathering electronic digital artifacts. Students are introduced to the concepts, situations and personalities they may encounter while investigating a computer incident.

- Origins of Computer Forensic science
- Criminal and civil incidents
- Types of computer fraud incidents
- Internal and external threats
- Investigative challenges

Module 2: Disk Storage Concepts

Having a clear understanding of how data is stored is having the upper hand during any investigation. Microsoft operating systems have a systematic way of storing data that is unknown to most end users. Here you will learn hard drive storage dynamics and understand “lost” data recovery methods.

- Operating systems and file structures
- Disk storage methodologies
- OS procedures involving file & directory creation
- Disk-based media file storage concepts
- “Slack space” & the recovery of digital evidence
- “File management” and “file format” concepts

Module 3: Computer Forensics

This is a detailed review of standard and advanced procedures and how you can effectively implement these procedures into your organization. This section covers the advanced procedures necessary to conduct an accurate and carefully documented computer forensic examination. Advanced methods of computer forensic protocols are implemented.

- Application of scientific methods
- Three major categories of digital evidence
- Four cardinal rules of Computer Forensics
- “ALPHA 5” system
- Best practices - the twenty steps

Module 4: Electronic Discovery and Digital Evidence

Students learn recovery methods of digital artifacts from various file structures and gain an overview of different operating systems and file structures encountered. Exercises detail what to look for, as well as the various techniques for retrieving the information in a forensically sound manner.

- The digital acquisition process
- Procedures used in digital duplication
- Digital authentication types
- Identifying types of digital evidence attacks
- Digital evidence classification/comparison
- Identify types of digital evidence clues
- Identify aspects of a Computer Forensic behavioral analysis

Module 5: Specialized Examination Tools

Multiple software and hardware solutions are covered during this session. Students learn the numerous tools available to them in a vendor neutral environment. A clear understanding of what the tools do and how they work is presented in layman’s terms.

- Forensic tools (hardware & software) available
- Forensic Tool Kit
- EnCase
- WinHe

Module 6: Seizure Concepts

Proper seizure of digital media is the start of every computer investigation. Students learn the correct protocol relating to handling of evidence.

- Digital incident situation assessment
- Procedures necessary to secure digital evidence
- Protocols required establishing a “chain of custody” and submitting items as “digital evidence”
- Identification of equipment encountered during a digital incident situation

Module 7: Forensic Examination

Covers the advanced procedures necessary to conduct an accurate and carefully documented computer forensic examination. Advanced methods of computer forensic protocols are implemented, including physical evidence recovery.

- “Pre-exam” analysis employment
- Computer Forensic duplication types
- Digital evidence processing methods
- Digital data extraction techniques from nontraditional areas of digital media

Module 8: Advanced Artifact Recovery

A hands-on laboratory where students conduct an advanced forensic examination of digital media. The focus of this lesson is to utilize advanced automated tools for the recovery of digital artifacts that are unattainable by conventional methods. There are several practical exercises that challenge even the senior cyber crime investigator. Focus is placed on using the advanced tools and thinking “outside the box” to try to discover incriminating digital evidence on a live case file.

Module 9: Crypto and Password Recovery

Covers digital encryption file structures and password-protected data that an investigator may encounter while conducting and examining. Students are exposed to methods to decode and crack passwords that are used to protect potential evidence. They also learn techniques to gain access to encrypted files that may reside within the information.

- Origins of cryptology and cryptography
- Cryptography and cryptanalysis
- Steganography and Alternate Data Streams
- Types of encryption concepts
- Principles of “diffusion” and “confusion”
- Investigative options available to crack password-protected files

Module 10: Specialized Digital Media Analysis and Recovery

Covers state of the art software where students are required to examine digital media in an attempt to recover data pertaining to a civil or criminal offence. Students will present their findings to the class during an evidence presentation exercise. Students will compete to see who completes the most thorough investigation. This exercise is very in-depth and competitive.

- MAC times and image metadata
- Windows Registry
- System identifiers
- Sources of unique identification within OS
- Aspects of OS data files, to include Index.dat and AOL system files
- “Recycle” folder and deleted files

Module 11: Cyber-terrorism and Internet Investigations

Students are exposed to possible threats to their infrastructure and learn to effectively combat cyber-terrorism. These are hands-on exercises where students learn how to identify digital Internet artifacts left by potential cyber-terrorists.

- Definition of digital evidence
- Concepts and protocols associated with digital evidence and “levels of proof”
- Categories of digital evidence

Module 12: Electronic Discovery, Acquisition and Analysis Laboratory

Students acquire and analyze digital evidence using specialized forensic tools and will conduct a proper “seizure and search” for digital evidence. Proper authentication and analysis skills are taught using advanced forensic utilities and software tools.

- Hands-on case file
- Live/Indexed Keyword searching
- Analysis and identification of relevant digital evidence
- Quality assurance and documentation
- Peer review process
- Annual review procedures
- Forensic lab deviation policy
- Long term storage options
- Lab items subject to the legal discovery process
- Report compilation and presentation



Module 13: Documenting and Reporting Digital Evidence

Reviews and analyzes the methods used to document and report the results of a computer forensic examination. Students will present their finding and electronic discoveries in an exercise to demonstrate their abilities to create an effective presentation.

Module 14: Presentation of Digital Evidence

Students are introduced to aspects of presenting digital evidence in a courtroom environment. They are exposed to the specialized tools necessary to effectively create and present the results of a cyber crime investigation to an administrative body or court of law. Both civil and criminal incidents are covered during this lesson. This is the final exercise where students are faced with the challenge of presenting their findings in a low-tech format where non-technical personnel are able to decipher and understand the results. The students will physically present their findings in “layman’s terms,” which is critical during any investigation. Students will have mastered this critical skill by the end of this exercise.

- “Best evidence” concept
- “Hearsay” concept
- “Authenticity” and “Alteration of Computer Records” concepts
- “Layman’s analogies” available to the Computer Forensic practitioner
- Admissibility of digital evidence in a court of law