



**Online Training Computer Forensic Examiner Training Course  
Key Computer Service, LLC**

[www.cftco.com](http://www.cftco.com)

**The Computer Forensic Examiner course is a self paced training course in computer forensic examinations that will teach you how to conduct thorough, forensically sound computer examinations and will prepare you to take the CCE certification examination. This is not a "data mining" course. Our students will learn how to conduct thorough examinations and how to explain, interpret and draw the appropriate conclusions on what has been found and what it may mean.**

**Our course does not focus on how to use automated forensic examination products. We will teach you how data is stored, where the data is located and how to recover all of the data. Regardless of which automated product that you may use, you will understand what the product is doing and you will be able to explain or testify about how and what you have found.**

- o **Outstanding Course Material**
- o **Outstanding Instructors**
- o **Distance Learning**
- o **Self Paced**
- o **DOS, Windows 9.x, Windows NTFS**
- o **Worldwide**
- o **Enroll and Start Anytime**

**You can take our course from any place in the world. If you have access to the Internet, you can learn how to conduct sound computer forensic examinations from your home, from the office, while "on the road" or anyplace that you have access to a computer. Our typical students are those who wish to start their own forensic examination business or professionals such as network administrators, MIS and IS specialists, auditors, fraud examiners, private investigators and similar specialists who may encounter computer media that contains potential evidence or other significant data.**

# Course Fee

The fee for the online Computer Forensic Examiner course is \$2750. There is a discounted fee of \$2500 for government employees and educators and for law enforcement officers. A "pay as you go" payment plan and financial aid are also available. Please [click here](#) for financial aid information from Kennesaw State University.

# Course Details

This is not a "watered down" training course. Not like other courses, we tell you in detail what we cover during the course and what our experience and expertise is. We have a great training course, great material, experienced instructors and we truly want you to learn the material and to become good forensic examiners. We want you to compare and decide what is best for you.

You will be provided well developed, detailed handouts of the course material. The course contains a number of practical exercise problems in the form of specially prepared diskettes or a hard disk drive that must be examined. The practical exercises will reinforce the material and teach "hands-on" skills. A case scenario will be used where a fictional private investigator brings you, the examiner, each diskette or a hard disk drive for examination. Each diskette will build to the next exercise, until finally a hard disk drive is examined and the case is concluded. Real life computer forensic issues will be covered by the practical exercises.

Clear, concise, accurate reports that draw appropriate conclusions are a very important factor in presenting the results of a forensic examination. We require reports detailing each "practical exercise" examination. We critically review your reports as if we were the "other side" and will help you develop excellent report writing skills. Your final reports can be used as your "template" for real examinations.

Our instructors are all Certified Forensic Computer Examiners or Certified Computer Examiners (CCE)® who are currently involved in computer forensic examinations. They will coach and tutor you through the practical exercises, your reports and through the test questions for each module. Our instructors are highly qualified, experienced and understand forensic examinations far beyond the material in this course. Your interaction with your instructor will normally be via email, but direct assistance is available. We truly want you to learn the material and to become a good forensic examiner.

The on-line course is broken up into five modules. The material is constantly being revised and is subject to change. The current modules consist of:

## Module 1

- An overview of what types of crimes computer evidence might be used in.
- How to deal with clients and employers.
- How to initially determine the scope of the examination.
- How to determine what must be done and how you should proceed in an examination.
- An overview of why trained forensic examiners should be used and what they may expect to encounter.
- Software ethics.
- Forensic ethical standards.
- Forensic examination procedures.
- Preparing and verifying forensically sterile examination media.
- Note taking and report writing.
- Personal computer construction, hardware and software with focus on the BIOS, BIOS limitations, hard disk translation schemes and how they can effect forensic examinations.
- A very broad overview of several operating systems including:
  - Windows NT/2000
  - Novell
  - Unix/Linux
  - DOS
  - Windows 95/98
- A broad overview of networks.
- Instruction on the acquisition, collection and seizure of magnetic media.
- How to best acquire, collect or seize the various operating systems.
- Legal and privacy issues.
- Establishing a sound "chain of custody".
- The beginning logical structures of the Microsoft operating system FAT file system.
- How to recover simple deleted files.
- There are four practical exercises in preparing and verifying forensically sterile media, using a "carving" utility to recover data from unallocated space and the manual recovery of simple deleted files.
- A written examination regarding the material covered in this module.

## Module 2

- The DOS and Windows boot process.
- A continuation of how files are created and stored.
- How to recover more complex deleted files.
- The significance and determination of the creation date and time.
- The significance and determination of the last accessed date and the modification date and time.
- How Windows long file names are stored.
- What happens when Windows long file names are deleted.
- How to recover Windows long file names.
- How sub-directories are stored.
- What happens when sub-directories are deleted.

- How to recover a deleted sub-directory and it's files.
- What happens when a diskette or hard disk drive is formatted.
- How to recover files, sub-directories and data from formatted disks.
- How to determine which files had been deleted prior to formatting.
- What file slack is and how to recover data from file slack.
- There are five practical exercises on the logical structure of FAT file systems, file storage and the recovery of fragmented deleted files, the recovery of long file names, the recovery of deleted sub directories, and the recovery of formatted disks.
- A written examination regarding the material covered in this module.

## Module 3

- An in-depth exploration of NTFS logical structures (nothing similar is available *anywhere*) , including:
  - The partition table
  - The boot record
  - Bitmaps
  - The root directory
  - The MFT
  - Headers
  - Attributes
  - Resident files
  - Non-resident files
  - Run lists, etc.
  - Alternate data streams
  - File storage
  - The various dates and times stored in attributes
  - File deletion
  - File recovery
  - Directory storage
  - Tracing files/directories
  - The NTFS registry "hive".
  - Examining NTFS drives
- A practical exercise involving the detailed exploration of the NTFS logical structures on a specially prepared NTFS drive.
- A written examination regarding the material covered in this module.

## Module 4

- How to make a Windows 98 forensic boot disk
- How to make "exact" images of media - the various imaging methods
- The use of Firewire write blockers
- The significance, location and recovering data from:
  - Swap Files
  - Temporary Files
  - Internet Cache Files
  - The various types of Email files

- Internet Cookies
- Internet Sites Visited
- Basic Internet issues. Doing a basic "whois" and similar Internet checks.
- How to preserve the original media.
- How to prevent inadvertent writes to the original media, virus introduction to the original media, and activation of "booby" traps on the original media.
- How to make bitstream (exact copies) of the original media.
- The safe handling of the media by the forensic examiner.
- The most common situations that an examiner may encounter during an examination.
- Finding and documenting normal data or graphical files.
- How people commonly try to hide data.
- Finding and documenting data and files in unallocated space.
- Finding hidden data.
- An overview of password protection and unlocking passwords.
- Accessing and interpreting "metadata" in MS Office documents.
- There are three practical exercises on recovering data from swap files, temporary files, etc., determining registration of a URL, finding and documenting normal data on magnetic media, finding hidden data and unlocking passwords, unlocking passwords and accessing metadata.
- A written examination regarding the material covered in this module.

## Module 5

- Data formats and types.
- Basic data format conversion.
- Examining CDR media and accessing multiple unclosed sessions.
- Managing data.
- Presenting the data to the client in a useful format.
- Presenting data in court or other proceedings in a clear and understandable manner.
- The marking, storage and transmittal of evidence.
- The basic use of automated forensic suites (Access Data's Forensic Tool Kit (FTK))
- A practical exercise where you examine a specially prepared hard disk drive. This hard disk drive will contain many current "real life" issues covered in this course and will require you to conduct a complete examination of the media. You must examine this hard drive, draw the appropriate conclusions, write a good report and present the evidence found in a manner that is clear and understandable.
- A written final examination will be given.

We will provide a detailed handout for each module covered. The handouts can be used as a reference manual. Sample reports, additional practical exercises, a DOS primer, Diskedit primer and other useful information and applications will be provided. You will be subscribed to our listservers that provide both administrative and technical information. Even after you complete the course, as material is updated, you will be able to download the new material from our web site.