



CCE Bootcamp Computer Forensics Course Key Computer Service, LLC

www.cce-bootcamp.com / www.cftco.com

The CCE Bootcamp Computer Forensic Examiner course is an intense 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.

- **Strong Course Material**
- **Outstanding Instructors**
- **Industry Standard Software Provided**
- **Self-paced Distance Learning Available**
- **Windows 2000, XP, Vista, Windows 7 Supported**
- **Worldwide Offerings**
- **Enroll and Start Anytime**

You can take our course from any place in the world. We currently have classroom locations found through the United States as well as Canada, Australia, and parts of Europe. If you are unable to attend a classroom session and 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 any place 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 cost for enrollment into a classroom CCE Bootcamp course is \$2995. There is a discounted fee of \$2795 for government / law enforcement / military / education employees.

The fee for the Guided Self-Study CCE Bootcamp course is \$2895. There is a discounted fee of \$2645 for government / law enforcement / military / education employees. A "pay as you go" payment plan and financial aid are also available.

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. Because of the time constraints of the Bootcamp, the reports will be written after the course and submitted to your instructor. 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.

*****Why do we still teach the DOS FAT file system?*****

We believe a sound understanding of the FAT file system is essential. Flash media is very portable and in use everywhere. It is frequently overlooked. That "Thumb" drive hanging around someone's neck, could contain valuable evidence. Flash media, such as "Thumb " Drives, flash cards in digital cameras, most cell phones, etc. are all stored on disk using the FAT file system. Your tools may understand the FAT file system, but you, the expert witness, must understand the FAT file system also. You must be able to clearly explain how files are stored, deleted, etc. and how your tools found the evidence. We frequently see "experienced" examiners, using expensive tools, examine a formatted diskette, that contains all sorts of evidentiary data, and report that the diskette was blank. Is this a problem with the tool or the examiner's training?

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

Module 1 – Introduction to Computer Forensics

- Recommended Machine Configurations
- What makes a good computer forensic examiner?
- Computer Forensics vs. E Discovery
- Dealing with clients or employers
 - Work Product
 - Client Contracts
 - Legal and privacy issues
- Software Licensing
- Ethical Conduct Issues
- Cases that may include digital evidence
- Forensic Examination Procedures
- Determining Scope of Examinations
- Hardware and Imaging Issues
- Floppy Diskette, USB and Optical Media Examination
- Limited Examinations
- Forensically Sterile Examination Media
- Examination Documentation and Reports
- ASCII Table
- General Overview of Boot Process and Operating Systems
- Floppy Diskette Sides, FD Tracks, Hard Disk Drives
- BIOS History
- Networked Computers
- Media Acquisition
- Acquisition Documentation
- Chain of Custody

Module 2 – Imaging

- Imaging Theory and Process

- **Imaging Methods**
- **Write Blocking**
- **Imaging Flash Drives**
- **Wiping, Hashing, Validation, Image Restoration, Cloning, Unallocated Space**
- **Drive Partitioning**
- **One (1) Student Lab Practical Exercise**

Module 3 – File Signatures, Data Formats & Unallocated Space

- **File Identification**
- **File Headers**
- **General File Types**
- **File Viewers**
- **Examination of Compressed Files**
- **Data Carving – Using Simple Carver**
- **One (1) Student Lab Practical Exercise**

Module 4 – FAT File System

- **Logical structures of DOS, Windows 95, Windows 98**
- **Master Boot Record**
- **File Allocation Table**
 - **16 Bit FAT**
 - **32 Bit FAT**
- **Directory Entries**
- **Clusters**
- **Unallocated Space**
- **Sub-Directories**
- **FORMAT**
- **Six (6) Student Lab Practical Exercises**

Module 5 – NTFS

- **Introduction and Overview**
- **Basic Terms**
- **Basic Boot Record Information**
- **Time Stamps**
- **Root Directory**
- **Recycle Bin**
- **File Creation**
- **File Deletion**
- **Examining NTFS Drives**
- **Two (2) Student Lab Practical Exercises**

Module 6 – Registry & Artifacts

- **Creating an Examination Boot Disk**
- **Data Recovery**
- **Windows Swap and Page Files**
- **Forensic Analysis of the Windows Registry**
- **Internet Cache Files, Cookies and Internet Sites**
- **Microsoft Outlook**
- **MSMAIL**
- **Logical Structures**
- **Tracking User Specific Computer Use**
- **Internet Explorer Cache Index**
- **VISTA**
- **Basic Mail Issues**
- **Basic Internet Issues**
- **Common Situations Encountered during Examinations**
- **Password Protection and Defeating Passwords**
- **Compound Documents**
- **Examining CDR Media**
- **FTK**
- **Three (3) Student Lab Practical Exercises**

Module 7 – Forensic Policy, Case Writing, Legal Process & Forensic Tool Kits

- **Use of Policy and Checklists in Forensic Practice**
- **Data Presentation to Client**
- **Case Report Writing**
- **Legal Process**
- **Expert Admission**
- **Going to Court**
- **Use of Forensic Tools and Software**
- **One (1) Student Lab Practical Exercise – Hard drive examination**

Approximately 40% of the CCE BootCamp® consists of hands-on, comprehensive practical exercises. All instructors are CCE Certified and have impressive professional experience as digital forensics examiners, both civil and criminal.

Students must have strong computer skills, including the ability or desire to work outside the Windows GUI interface. The ability or desire to work with computer hardware, including the removal of hard-disk drives and changing jumpers is required. Certified Computer Examiner (CCE)® candidates must agree and abide to the ISFCE Code of Ethics and may be subject to a criminal background check. The written portion of the CCE certification test is administered at the end of each CCE BootCamp®.

All CCE BOOTCAMP® students receive fully licensed copies of the following software:

- Branded Linux Imaging Tool
- WinHex Specialist - www.X-Ways.net
- Simple Carver - www.SimpleCarver.com
- Passware Kit - www.LostPassword.com
- Forensic Tool Kit (Demo version) - www.AccessData.com (Student discount offered through developer)

On the final day of the CCE BootCamp® training course, the online portion of the CCE certification examination will be administered. Following this, all students will be required to contact the ISFCE for further instructions on moving forward in the certification process.

Training materials are provided in advance of the training for self study before the actual Bootcamp training course. Sample reports, additional practical exercises, and other useful information will be provided. You will be subscribed to our Student Listserv that provides both administrative and technical information.

We will provide all of the forensic software necessary for the course and Certified Computer Examiner (CCE)® testing.

All questions surrounding the training offerings of Key Computer Service, LLC may be directed to info@keycomputer.net or (615) 236-1249.