

The material used in this course is based on the concept of teaching computer forensics from a vendor neutral perspective. This course teaches the low level mechanics of commonly encountered file systems. Computer forensics is not a point and click process, neither is the Key Computer approach to training. If a student can gain a solid understanding of one file system and how it functions at a low level then that student will be prepared to learn other file systems as well.

This course material will teach low level mechanics and functions of both the FAT file system and the New Technology File System (NTFS). Although the FAT file system is not available on new computers, it is the default file system on floppy diskettes and USB devices. Many computer forensic incidents involve USB devices and will continue to involve these devices for years to come. Consequently, students studying to become successful forensic computer examiners must understand the FAT file system.

A computer formatted with Windows 2000 may be formatted with the FAT file system or NTFS.

NTFS is the native file system for Windows XP and Vista.

The completion of several practical exercises is a requirement of this course. Some include floppy diskettes. Although the floppy diskette is no longer commonly encountered in the field, it is the exercise that is significant and any action taken on a floppy diskette can be replicated on a hard drive.

TRAINING

The computer forensic field has grown over the past several years. Historically, law enforcement officers have been the primary forensic computer examiners. However, as the need for these services in the private sector also continues to grow, the need for qualified civilian forensic computer examiners as well as law enforcement examiners is on the rise. Comprehensive forensic training, independent of any forensic tools, is the first step to becoming a successful forensic computer examiner.

While searching for the right forensic training provider, please take a close look at their history, reputation and staff. Pay close attention to important factors such as experience in the forensic industry, qualifications of instructors and development of the course material. Key Computer Service takes pride in offering current and comprehensive training developed and delivered by industry leaders who are actively practicing forensics.

The CCE BootCamp training will cover core forensic procedures based upon the *Key Philosophy* emphasizing the expertise and knowledge of the examiner forensic practices NOT the forensic tools.

The training focus is not only on forensic recovery techniques, but on ensuring what the examiner finds will be admitted in court. Both sound examination and evidence handling procedures are taught. The examiner, not the forensic tool used, must qualify as an expert witness. An understanding of how to articulate what evidence forensic tools uncover is critical. Too frequently, experienced examiners using automated tools examine a formatted diskette containing evidentiary data and report the diskette is blank. Is this a problem with the tool or the examiner's training?

Clear, concise, accurate reports that draw appropriate conclusions are a very important factor in presenting the results of a forensic examination. Our instructors require reports detailing each practical exercise examination. All reports are critically reviewed as if representing the opposing side. This will help develop excellent report writing skills. Final reports can be used as a template for real examinations.

Students are typically professionals, both civilian and law enforcement, some working towards starting a forensic practice. Students in the IT, accounting, legal and other fields have successfully completed this training.

The CCE BootCamp will train you to not only thoroughly examine digital media, but also clearly document, control, prepare and present examination results.

The CCE BootCamp includes instruction on:

- Conducting thorough examinations

- Identifying where and how data is stored

- Recovering and interpreting data

- Drawing appropriate conclusions based on the data

A sound understanding of the FAT and NTFS file systems is critical to forensic examination. These file systems are important because they are the base of Windows operating systems, portable flash media, storage devices and other digital media in use everywhere today. USB drives, mobile phones, laptops, desktops and cameras are examples of common equipment that use these systems.

FAT file system logical structures are utilized by DOS and Windows 9.x. NTFS logical structures are utilized by Windows NT, 2000, XP and Vista.