



Certified Computer Examiner (CCE)[®] BOOTCAMP

Offered in partnership by [Trial Solutions](#) and [Acquisition Data](#)

The Certified Computer Examiner (CCE)[®] BootCamp is an intensive hands on 4 ½ day training course in computer forensics that will teach you how to perform forensically sound computer examinations and prepare you to take the CCE certification examination. We are an Authorized Certified Computer Examiner (CCE)[®] Training and Testing Center. Calendar of upcoming courses: <http://www.regonline.com/?customer=248012>

Why should you attend our course?

With the new Federal Rules of Civil Procedures (FRCP) now in affect, law firms and corporate clients alike are looking for reliable sources of information on how to collect and analyze Electronically Stored Information (ESI) in a forensically sound manner.

Our highly qualified and experienced instructors are Certified Computer Examiners (CCE)[®], have real world forensic experience, and many are former or current special agents or law enforcement officers.

Our intensive training course in computer forensics is hardware-and-software independent and as such we utilize the best forensic tools for the job.

Real world computer forensic examples will be reinforced by hands on practical exercises and exams.

You will be provided with a course binder that contains detailed handouts of all course material.

CCE BootCamp Highlights are below: <http://www.cce-bootcamp.com/details.htm>

- Overview of what types of crimes computer evidence might be used in
- Forensic examinations scoping, first steps, and procedures
- Preparing and verifying forensically wiped examination media
- Establishing a sound chain of custody
- Safe handling, labeling, and preservation of original media
- Labeling, storage and transmittal of evidence
- Reporting and detailed notes
- Overview of several operating systems including:
 - Windows NT/2000
 - Novell
 - Unix/Linux
 - DOS

- Windows 95/98
- Legal and privacy issues
- How files and folders are created, stored, and deleted
- What happens when a diskette or hard disk drive is formatted
- Simple and complex deleted files recovery as well as file “carving”
 - Recover files, sub-directories and data from formatted disks
 - Determine which files had been deleted prior to formatting
 - Recover data from file slack space
- Password cracking and file decryption
- An in-depth exploration of the NTFS file system
- The significance and determination of the created, modified, and last accessed date and time as well as compound "metadata" in MS Office documents.
- Various bit-stream imaging methods
- Write blocker usage to prevent inadvertent writes to the original media
- Boot disk creation
- Significance and location of temporary, cache and various types of email data
- Common situations an examiner may encounter during a forensic examination
- Commonly data hiding techniques and how to find hidden data
- Presenting data to the client
- Presenting data in court or other proceedings

Our lab computers will have all of the forensic software necessary for the course, including:

- A wiping program
- A checksum program
- A file documentation program
- A program that will allow examination of unallocated space
- A program that will make exact forensic copies of floppy diskettes
- A forensic "carving" utility
- Passware Kit from Lost Password.com
- Norton Utilities
- Norton Ghost
- QuickView Plus
- Virus scanning utility
- The demo version of Access Data's Forensic Tool Kit (FTK)

Course binders containing sample reports, practical exercises and other useful information will also be provided on day one of the course.

Please note that the course material is constantly being updated and is subject to change.