EXCELSIOR COLLEGE

7 Columbia Circle, Albany, NY 12203-5159
Phone: **518.608.8211** | Toll Free: **888.647.2388** | Fax: 518.464.8777
WWW.EXCELSIOR.EDU/CPD

CENTER FOR PROFESSIONAL DEVELOPMENT

FORENSIC COMPUTER EXAMINER

80 Hours/12 Months/Instructor-Facilitated
Course Code: **CPD063** || Course Cost: **$3095**

OVERVIEW

Excelsior College has partnered with ed2go to bring you the Forensic Computer Examiner program.

As criminal defense attorneys and civil attorneys encountered law-enforcement examiners, the need for qualified civilian forensic computer examiners grew. Currently, there's a huge demand for certified, qualified forensic computer examiners. Some trained examiners have started their own businesses, some work for large companies, such as Deloitte and Touche, and others work for law-enforcement agencies.

This comprehensive online program prepares you for a career in this emerging field. You'll learn not only to thoroughly examine digital media, but also to clearly document, control, prepare, and present examination results that will stand up in a court of law. You'll be able to identify where and how data is stored and how to recover and interpret data and draw appropriate conclusions based on the data. Education on the ethics of computer forensics is also included. This program is hands-on and emphasizes learning by doing.

The primary certification for civilian forensic computer examiners is the Certified Computer Examiner (CCE) certification. The Forensic Computer Examiner Online Training Program is an authorized ISFCE training course that will thoroughly prepare you to take the CCE certification exam.

OBJECTIVES

Upon successful completion of the Forensic Computer Examiner Training Program, you'll:

- Know what a forensic examiner may expect to encounter during an examination
- Understand software licensing and how it affects forensic examiners
- Explore forensic ethical standards as they apply to forensic examiners
- Determine when a legal opinion may be necessary to prevent privacy issues from interfering with the examination or causing a valid lawsuit
- Understand how to properly establish and maintain the physical chain of custody of media and evidence
- Know the significance of, location of, and how to recover data from swap files, temporary files, Internet cache files, Internet cookies, mail files, and Internet sites visited
- Be able to prevent virus introduction and prevent activation of "booby traps"
- Understand how to find and document data, including hidden data and password-protected data
- Discover how to present recovered and evidence data to the client in a useful format
- Understand how to present data in court or other proceedings

- Be fully prepared to sit for the CCE Certification testing through the International Society of Forensic Computer Examiners

OUTLINE

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

- Recommended Machine Configurations
- 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 File System

- 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

- 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

COMPUTER REQUIREMENTS

This program is compatible with the Windows XP and later operating systems and IE 7 and later browsers.

Minimum Computer Requirements:

- PC with the latest updates and BIOS (Mac computers may not be used)
- XP, Vista or Windows 7 operating systems
- Internet access
- 1 GB (or more) memory
- 10 GB or larger hard-disk drive for examination purposes
- 2 (or more) open USB 2.0 ports

Recommended Configuration:

- PC with the latest updates and BIOS
- Windows 2000 or XP operating system
- High-speed Internet access
- 2 GB (or more) memory
- 15 GB or larger hard-disk drive for examination purposes
- Integrated PS/2 ports (not USB keyboard or mouse)
- 4 open USB 2.0 ports
- 1 open Firewire/IEEE 1394 port
- Read/Write blocking device such as the FireFly Read/Write device made by Digital Intelligence

You may use either a desktop or a laptop computer.

This program is based on the concept of teaching computer forensics from a vendor-neutral perspective, and you'll learn the low-level mechanics of commonly encountered file systems. If you can gain a solid understanding of one file system and how it functions at a low level, then you'll be prepared to learn other file systems as well.

This program material also teaches 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's 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.

Windows 98 and earlier versions are based on the FAT file system. A computer formatted with Windows 2000, XP, and Vista versions will typically be formatted with the NTFS file system.

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

INSTRUCTOR BIO

John Fretts retired from the Bureau of Alcohol, Tobacco, Firearms, and Explosives in 2005, after a distinguished thirty-year career with the Department of Justice, Bureau of Alcohol, Tobacco, and Firearms. John began his ATF career as a special agent in the Washington, DC, field division, where he led numerous federal investigations into violations of federal firearms and explosives laws. In 1991, John was promoted to the position of project manager at ATF Headquarters.

In 1994, John transferred to Connecticut with his appointment as supervisor of ATF's Hartford field office. While in Connecticut, John nurtured his technical interests, developing skills as a specialist in computer forensic investigations. He successfully completed the CIS 2000 Program at the Federal Law Enforcement Training Center in Brunswick, Georgia. He was also certified by the International Association of Computer Investigative Specialists as a Certified Forensic Computer Examiner (CFCE) in 2004. Because of his management experience and knowledge of computer investigations, John was named regional supervisor of ATF computer forensic operations for the northeast United States. While with the ATF, John testified in federal court and is qualified to appear as an expert in computer forensics and data recovery.

Upon retirement from federal service, John accepted a position as director of investigations with Security Services of Connecticut (SSC), a regional firm specializing in a full range of investigative services, particularly in computer forensics.

John had oversight of SSC's computer forensic operation and was regularly called upon to lecture on the topic of computer forensics and data recovery as it relates to fraud and computer misuse. In his presentations to corporate clients and at trade shows, John had an uncanny ability to explain the most complex aspects of computer forensics to those with the least understanding of the subject. With his law enforcement background, John was adept at explaining the necessity to respond rapidly to an incident involving fraud or criminal activity involving computers and the need to preserve electronic evidence.

In August of 2007, John resigned from his position with SSC to concentrate his time and skills on computer forensics investigation and education. John is a member of the University of New

Haven, criminal justice curriculum, student advisory board. He is a veteran of the United States Army and has a Bachelor's degree in criminal justice.

Steve Wisenburg is a 14-year veteran of the city of Atlanta police department. He's been a detective since 1999, and he started investigations in the physical abuse and sexual abuse of children. These investigations led to further investigation of child porn and other exploited children on the Internet. He's now assigned to the cybercrime unit, where he's a full-time computer forensic examiner.

Steve is the current president of the Atlanta chapter of the High Technology Investigation Association (HTCIA). He holds the Certified Computer Examiner (CCE) certification. He also is one of the founding directors of the Cybercrime Summit, a training conference held in metro Atlanta each year. Steve has attended several training classes, including the following: computer forensics boot camp, practical data forensics using Linux, access data forensic boot camp, EnCase intermediate analysis and reporting, basic data recovery and analysis, advanced data recovery and analysis, ILook, and Maresware Software Training.

Dave Good has served the U.S Department of Treasury and the U.S. Department of Justice for the past 18 years. He has over 21 years of experience in the management, design, and implementation of mainframe systems, local area networks, and virtual private networks.

His experience includes positions with Electronic Data Systems, Network Solutions, and Automation Research Systems. Dave completed the first seat-based Enterprise Systems Architecture for the Federal Government, where 300 sites were outfitted with new desktops, laptops, and servers, and he implemented the conversion of a packet-switched network to a frame relay network for all sites.

He's currently serving as a digital investigator and program manager of the computer forensics branch for a national law enforcement agency. He's been cited as a computer forensic expert witness in U.S. District Court, Charlotte, NC.

Dave is an active member of the National Technical Investigators Association, the High Technology Crime Investigation Association, and the International Society of Forensic Computer Examiners. He holds the following certifications: Novell Master Certified Network Engineer (MCNE), CCE, Comptia A+, Comptia Net+, and Comptia IT Project+.

Phil Harrold was employed by the Odessa, Texas, police department from 1979 to 1988. His assignments included patrol, narcotics, and crimes against property. From 1989 until 2000, Phil was employed by the Monroe County, Florida, sheriff's office. His assignments with that agency included patrol, general investigations, and homicide investigations, and he was also a bomb technician.

Phil has been employed since 2000 by the state attorney's office, 16th Judicial Circuit, and the state of Florida as an investigator. He specializes in computer-related investigations and performs forensic examinations for local, state, and federal agencies.
His education includes an A.A.S. in law enforcement from Odessa College, a Bachelor of Arts in

criminal justice from the University of Texas of the Permian Basin, and a Master of Science degree in management from Troy State University. He is a Certified Computer Examiner (CCE) and Electronic Evidence Collection Specialist (through IACIS).

Phil has completed numerous specialized trainings, including U.S. Army/FBI Hazardous Devices School, U.S. Army/FBI Weapons of Mass Destruction School, IACIS Basic, and training in computer crime investigation, basic data recovery and analysis, advanced analysis of Microsoft NTFS, advanced analysis of e-mail, Microsoft Access, online investigations, access data-intermediate forensic boot camp, homicide investigation, hostage negotiation, multi-disciplinary investigation of computer-facilitated child sexual exploitation, and racketeering Investigations.

Phil's professional affiliations include International Association of Computer Investigative Specialists, High Technology Crime Investigation Association, High Tech Crime Consortium, and the International Society of Forensic Computer Examiners.

Keith Barger is a director in KPMG's forensic practice in Houston, Texas. Keith specializes in electronic data discovery and investigative services in support of civil litigation, and he provides advisory services regarding technology-related matters. Keith joined KPMG in 2006 after six years as a special agent and digital forensics Western regional coordinator with the Department of Justice, Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF).

Keith has extensive experience in digital forensic investigations, forensic methodologies, computer evidence recovery, and data analysis. He's investigated and provided oversight for domestic investigations violating federal, state, and local laws. These investigations often included testimonies before grand juries, inquests, trials, and other hearings.

Keith is responsible for national direction and oversight for KPMG's hold-order management system. He leads a national team responsible for the collection of litigation preservation requests on behalf of KPMG and its clients and collaborates with others on his team in the identification of custodians, automation of the collection process, and the production of litigation requests to relevant parties.

Additionally, he's responsible for the assessment and review of network infrastructures and related record management systems, recommending improvements, and overseeing the implementation of those improvements.

William (Bill) Taylor is a computer investigative specialist/special agent with a federal law enforcement agency in Nashville, Tennessee. He has served as a full-time forensic computer examiner since 1994.

Bill is a Certified Forensic Computer Examiner (International Association of Computer Investigative Specialists) and a Certified Fraud Examiner (Association of Certified Fraud Examiners), and holds an Associate's degree in forensic computer science. In addition, he holds both Baccalaureate and Master's degrees in criminal justice and is a graduate of the FBI National Academy.

Bill has over 24 years of investigative law enforcement experience at the state, local, and federal level. He served on the IACIS Board of Directors for six years, was vice-president for one year, and was president and CEO for nearly three years.