



Computer Forensics Certification Online – IT105 150 hours

Computer Forensics Level I Training Online - 50 Hours

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.

This online program is designed for people interested in becoming Computer Forensics experts. Students move at their own pace through all **3 levels (7 modules)** and learn how to forensically Exam(s)ine and recover data from operating systems. Students learn core forensic procedures for any operating or file system, and how to conduct forensically sound Examinations to preserve evidence for admission and use in legal proceedings. Each module requires an Exam(s) and completion of practical exercises before you can move to the next module. Additionally, this course will help prepare you for the upcoming Certified Computer Examiner (CCE) Examination.



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 and Introduction to SMART

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

We will provide a detailed manual for each module covered. These manuals can be used later in your career for reference purposes. Sample reports, additional practical exercises, a DOS primer, Diskedit primer and other useful information and applications will also 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.



Computer Forensics Level II Training
Online - 50 Hours

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.

This online program is designed for people interested in becoming Computer Forensics experts. Students move at their own pace through all **3 levels (7 modules)** and learn how to forensically Exam(s)ine and recover data from operating systems. Students learn core forensic procedures for any operating or file system, and how to conduct forensically sound Examinations to preserve evidence for admission and use in legal proceedings. Each module requires an Exam(s) and completion of practical exercises before you can move to the next module. Additionally, this course will help prepare you for the upcoming Certified Computer Examiner (CCE) Examination.

Prerequisites - Successful completion of the Computer Forensics **Level I** training.

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

We will provide a detailed manual for each module covered. These manuals can be used later in your career for reference purposes. Sample reports, additional practical exercises, a DOS primer, Diskedit primer and other useful information and applications will also 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.

Computer Forensics Level III Training **Online - 50 Hours**

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.

This online program is designed for people interested in becoming Computer Forensics experts. Students move at their own pace through all **3 levels (7 modules)** and learn how to forensically Exam(s)ine and recover data from operating systems. Students learn core forensic procedures for any operating or file system, and how to conduct forensically sound Examinations to preserve evidence for admission and use in legal proceedings. Each module requires an Exam(s) and completion of practical exercises before you can move to the next module. Additionally, this course will help prepare you for the upcoming Certified Computer Examiner (CCE) Examination.

Prerequisites - Successful completion of the Computer Forensics **Level I and Level II** training.

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

We will provide a detailed manual for each module covered. These manuals can be used later in your career for reference purposes. Sample reports, additional practical exercises, a DOS primer, Diskedit primer and other useful information and applications will also 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.

Minimum Requirements:

- Newer PC with latest updates and BIOS
- Windows 2000 or XP Operating system (Vista is currently being tested for compatibility issues)
- Internet access
- 512 MB (or more) memory
- 2 GB or larger hard disk drive for examination purposes
- Integrated PS/2 ports (Not USB Keyboard or Mouse)
- 2 open USB 2.0 ports

Recommended Configuration:

- Newer PC with latest updates and BIOS
- Windows 2000 or XP Operating system (Vista is currently being tested for compatibility issues)
- Internet access
- 1 GB (or more) memory
- 2 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](#)

Software provided with the training course:

Alongside the training materials, we will also be providing all students one 1 GB USB Thumbdrive and a suite of licensed and shareware/freeware software. We provide fully licensed copies of the following software:

SMART - www.ASRData.com
Simple Carver - www.SimpleCarver.com
Passware Kit - www.LostPassword.com
Forensic Tool Kit (Demo version) - www.AccessData.com



The Certified Computer Examiner Certification

Computer forensics experts know how to preserve, identify, recover, and document computer data. Do you have what it takes to become a Certified Computer Examiner (CCE)?

Published January 19, 2004, By Michael C. Gregg

Part 1 - The Written Exam

The written exam is multiple choice. There are 75 questions and a 60-minute time limit. It covers a range of basic knowledge including:

- Acquisition, marking, handing, and storage of evidence procedures
- Chain of custody
- Basic PC hardware construction and theory
- Very basic networking theory
- Basic data recovery techniques
- Authenticating MS Word documents and accessing and interpreting metadata
- Basic CDR recording processes and accessing data on CDR media
- Basic password recovery techniques
- Basic Internet issues

If you are A+, Network+, and Security + certified, possess good hardware troubleshooting skills, and have a basic understanding of the rules of forensics you can successfully pass the written portion of the exam. If it's been a while since you've dealt with these types of issues, you might consider reviewing [Upgrading and Repairing PCs](#) by Scott Mueller, The IACIS® [Forensic Examination Procedures](#), and [DOJ Computer Crime Procedures](#). Even if you breeze through this portion of the certification process, don't become overconfident. The written exam only represents one-fourth of your grade. Three-fourths of your grade requires hands-on skills.

Part 2, 3, & 4 - Examination of Test Media

Once the written examination has been completed, you will be provided with the first test media. Your first challenge will be to examine and recover the information on a floppy disk. You will be expected to write a complete report on the examination of this disk. It's important to remember to take nothing for granted. You need to handle the media in a way that is forensically sound and that could be supported if you were called into a court of law. It's a good idea to purchase a cloth bound, page numbered notebook. Use this to record each step of the process, making sure to note the date and time of each action performed.

When you successfully complete the examination of the floppy disk, you'll be provided with a CD. This will raise the bar on the skills required to make a successful analysis. The CD will present you with several additional technical hurdles to overcome. Finally, you will be tasked with the examination of a hard drive. This will be the most technically challenging of the three.

Throughout the examination process, you may encounter deleted files, encrypted files, fragments of data, and other obscure artifacts. You will need to have a variety of tools at your disposal to be victorious. The most important of these tools is your brain. If you like puzzles and have some basic detective skills, you can be successful.



Tools of the Trade

There's a wide array of tools that are available for computer forensics. Some of these are rather expensive. The most well-known dedicated forensic software packages include Forensic Toolkit by AccessData and EnCase by Guidance Software. Fortunately, Access Data provides a demo version that will work for all three media examinations, however, you will still need other programs to complete the examination process. Most of these are not free and you'll need to budget for these if you are going to pursue a career in computer forensics. You would not want to explain to a judge or an attorney why you are using pirated or illegal versions of forensic software! This would lose the case and most likely, end your career in computer forensics. You will want to consider purchasing some of the following types of programs:

- Password Recovery Tools
 - [Cain](#)
 - [LOpht Crack](#)
 - [Passware](#)
- Data Viewers
 - [Quick View Plus](#)
- Disk Wiping Utilities
 - [Wipe Drive](#)
- Suitable Hashing Applications
 - [MD5sum](#)
- Utilities that make Forensic Copies of Media
 - [DD](#)
- CDR Examination Tools
- Email Extraction Utilities
- Internet History Viewers

Final Thoughts

Historically, computer forensics was the exclusive domain of the police and law enforcement, however, corporations are increasingly becoming concerned with security and computer forensics. More than ever, companies are tasked with the examination of attempted hacking attacks and allegations of employee computer misuse. Mishandling of these concerns can cost companies millions. Companies must handle each in a legal and defensible manner. This requires trained employees that possess computer forensic skills. If you are looking to gain this type of knowledge, the CCE is one certification to consider.

Michael C. Gregg (CISSP, MCSE, MCT, CTT+, A+, Network+, Security+, MCP+I, CNA, CCNA, TICSA, CIW SA, CEH, CEI, and CCE) is a consultant, trainer, and author. He is a contributing author to Computer Forensics: Handling Evidence of Cybercrime. His consulting firm, Superior Solutions, Inc., is based in Houston, Texas.