

Computer Forensics

InfoSecInstitute.com | 866-471-0059

Learn to discover the source of computer crime!

In This Brochure:



Page 1

InfoSec Institute's Compute Forensics Program.

Pages 2-3

Detailed Syllabus

Computer crimes happen. The rate of fraud, abuse and downright criminal activity on IT systems by hackers, contractors and even employees are reaching alarming rates. Corporate IT, Law Enforcement and Information Security Pros are often required to perform computer forensics duties on their jobs. In terms of job growth, nothing beats computer forensics as a career, and no one can beat InfoSec Institute as the best place to learn from a computer forensics training expert.

During InfoSec Institute's Computer Forensics Training course you will:

- **See the dark side of how computer crimes are committed.**
- **Learn how to find traces of illegal or illicit activities left on disk with computer forensics tools and manual techniques.**
- **Learn how to recover data intentionally hidden or encrypted by perpetrators.**



Learn how to fight computer crime by finding the trace elements left behind by computer criminals and IT System Abusers.

InfoSec Institute 505 N. Lake Shore Dr. Suite 221, Chicago, IL 60611 USA
(866) 471-0059 www.InfoSecInstitute.com

Detailed 5 Day Syllabus

In this hands on course, you will gain real world experience in the core computer forensic procedures that apply to examining any operating system or file system.

Day 1:

The first day of the course introduces you to the theory of computer forensics as well as the legal, privacy and ethical considerations to make during a real world case. You spend the rest of the day learning the foundations of computer forensics and file recovery on Windows operating systems.

- Overview of Computer Crime
- Preparing sterile examination media
- Acquisition, collection and seizure of magnetic media.
- Documenting a Chain of Custody
- Understanding Microsoft Windows from a forensics point of view
- Recovering deleted files
- Determining creation/modification date on files
- Dealing with Windows long file names
- Introduction to the Forensic Tool Kit (FTK) program
- Understanding the uses of EnCase
- Understanding how directories are stored, deleted and recovered
- Recovering files, sub-directories and metadata from formatted disks
- Determining the deletion state of files prior to a disk format
- File slack space/Recovering data from slack space
- Forensics on FAT file systems

Day 2:

The second day delves deep into file recovery and the disk imaging process. You will learn tasks such as how to create a forensics boot disk with forensics utilities built in, the recovery of various Windows file metadata, and the ever important recovery of internet usage data. Modules include:

- Working with NTFS Partition table and boot record
- The Master File Table (MFT)
- Resident versus Non-Resident Files
- Investigating data streams
- File storage dates and times
- File deletion/recovery
- Dealing with the storage of directories
- Tracing files/directories
- Examining the Registry hive
- Examining NTFS drives
- Making a Forensics Boot Disk
- Disk Imaging Methods
- Recovering Internet Usage Data
- Recovering: Swap Files/Temporary Files/Cache Files
- Recovering Email Files
- Determining Internet usage via resident Cookies and Browser History with FTK

Student Testimonials



See what previous students have to say:

■ *"The instructor knew the material extremely well and was very articulate. I liked the way he threw in his real world experiences to the class!!!"*

Thomas Davis, Independent Contractor

■ *"This was the best course that I have ever attended. The content was perfect for keeping me interested. I've attended many courses where I didn't feel like the first few days were worth my time, but not here. I was constantly learning new things."*

**Mike Kempa, Centre of Criminology
University of Toronto**

Detailed 5 Day Syllabus Continued

Day 3:

The third day of the course prepares you to present your findings to your customer or in a court of law. You will also learn how to make exact copies of media, an essential preparatory step to a sound investigation.

- Preparing sterile examination media with Forensic Tool Kit (FTK)
- Preservation and safe handling of original media with EnCase
- Making bitstream copies of original media
- Common data hiding techniques
- "Carving" Data from unused space
- Determining skin tone Percentages in Images
- Analyzing media formats (.bmp, .jpg, .gif, .png, etc.)
- Finding data in unallocated space.
- Determining Printer information forensically
- Finding the location of hidden data.

Day 4:

In the fourth day of the course you will deal with situations where people have attempted to hide files and subvert a computer forensics investigation. We will also cover forensics for various mobile digital devices, such as Cell Phones, PDAs and Digital Cameras. Modules include:

- Text Searching with EnCase
- Recovering data from formatted drives
- Recovering data from defragged drives
- Stenography and file hiding
- Circumventing password protection in Microsoft Office Documents
- Accessing metadata in Microsoft Office documents
- Breaking Windows OS Passwords
- Circumventing Microsoft EFS (Encrypted File System)
- Digital Camera Forensics
- Cell Phone Forensics
- PDA Forensics
- P2P (Peer to Peer) File Sharing forensics
- KaZaa Forensics
- Experienced Computer Forensics Examiner Review

Day 5:

The final day of the course focuses on Linux Forensics. Students have the option of taking the CHFI at course completion. The CHFI is an accredited certification administered by the EC Council. The Modules include:

- Linux Bootable Disk Forensics
- SleuthKit
- TCT
- Linux File System Forensics
- Analyzing Ext2 file systems
- Analyzing Ext3 File Systems
- Using Linux to process forensic data
- Managing data.
- Presenting the data to the client in a useful format.
- The basic use of automated forensic suites
- CHFI Online Examination

CHFI Certification



The CHFI certification:

■ The CHFI is a multiple choice, true/false and situational question exam. Students have 2 hours to complete a 50 question exam. Most questions are "case questions" that involve understanding the details of a particular computer forensics exam.

■ The CHFI is proctored in-class on the last day of InfoSec Institute's computer forensic exam.

■ You can register for the exam outside of InfoSec Institute at any Prometric Testing center world wide.