

# Computer Forensics Course

**Length:** Three Day

**Summary:** You will also learn how to create an effective computer crime policy, and gain the hands on skills to implement it.

This 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.

After attending Computer Forensics Training, you will leave with a custom computer forensics toolkit that will enable you to perform a legally admissible forensics investigation and the skills to run the investigation properly.

This hands-on computer forensics training offers practical experience in a wide array of computer forensics situations that are applicable to the real world. Learn everything relating to computer forensics --- from how to establish a proper chain of custody that is admissible in a court of law to recovering files from intentionally damaged media

---

## Course Content

Run hacking attacks in our classroom labs, be a hacker for a week:  
Some of the hacking concepts you will learn to master during this hands on hacking course...

- Computer Forensics Training with open source tools
  - 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
  - Working with NTFS
  - Combing Partition table and boot record
  - Investigating The Master File Table (MFT)
  - Recovering Internet Usage Data
  - Recovering: Swap Files/Temporary Files/Cache Files
  - Digital Camera Computer Forensics
  - PDA and Mobile Computer Forensics
  - Linux/Unix computer forensics
  - Investigating data streams
  - File storage dates and times
  - File deletion/recovery
  - Preservation and safe handling of original media
  - Making bitstream copies of original media
  - Common data hiding techniques
  - Examining CD-ROM media
  - Carving out files "hidden" in unallocated disk space
  - Issues when presenting data in court
  - The marking, storage and transmittal of evidence.
  - Word document forensics and password cracking
  - Use tools such as Encase Forensic Edition, X-Ways Forensic Addition, Paraben, Forensic ToolKit (FTK), Linux dd, etc.
-