Course Outline

Computer Hacking Forensic Investigator
Course CHFI: 5 days Instructor Led

About this course
EC-Council released the most advanced computer forensic investigation program in the world. This course covers major forensic investigation scenarios that enable you to acquire hands-on experience on various forensic investigation techniques and standard tools necessary to successfully carry out a computer forensic investigation.

Battles between corporations, governments, and countries are no longer fought using physical force. Cyber war has begun, and the consequences can be seen in everyday life. With the onset of sophisticated cyber-attacks, the need for advanced cybersecurity and investigation training is critical. If you or your organization requires the knowledge or skills to identify, track, and prosecute cyber criminals, then this is the course for you. You will learn how to excel in digital evidence acquisition, handling, and forensically sound analysis. These skills will lead to successful prosecutions in various types of security incidents such as data breaches, corporate espionage, insider threats, and other intricate cases involving computer systems.

This course includes one exam voucher for CHFI.

Audience profile
IT professionals involved with information system security, computer forensics, and incident response.

At course completion
After completing this course, students will be able to:

- The computer forensic investigation process and the various legal issues involved
- Evidence searching, seizing and acquisition methodologies in a legal and forensically sound manner
- Types of digital evidence, rules of evidence, digital evidence examination process, and electronic crime and digital evidence consideration by crime category
- Roles of the first responder, first responder toolkit, securing and evaluating electronic crime scene, conducting preliminary interviews, documenting electronic crime scene, collecting and preserving electronic evidence, packaging and transporting electronic evidence, and reporting the crime scene
- Setting up a computer forensics lab and the tools involved in it
- Various file systems and how to boot a disk
- Gathering volatile and non-volatile information from Windows
- Data acquisition and duplication rules
- Validation methods and tools required
- Recovering deleted files and deleted partitions in Windows, Mac OS X, and Linux
- Forensic investigation using AccessData FTK and EnCase
- Steganography and its techniques
- Steganalysis and image file forensics
- Password cracking concepts, tools, and types of password attacks
- Investigating password protected files
- Types of log capturing, log management, time synchronization, and log capturing tools
- Investigating logs, network traffic, wireless attacks, and web attacks
- Tracking emails and investigate email crimes
- Mobile forensics and mobile forensics software and hardware tools
- Writing investigative reports
- Dark Web Forensics and IOT Forensics

Course Outline

Course Outline

Module 01: Computer Forensics in Today's World
Module 02: Computer Forensics Investigation Process
Module 03: Understanding Hard Disks and File Systems
Module 04: Data Acquisition and Duplication
Module 05: Defeating Anti-Forensics Techniques
Module 06: Windows Forensics
Module 07: Linux and Mac Forensics
Module 08: Network Forensics
Module 09: Investigating Web Attacks
Module 10: Dark Web Forensics
Module 11: Database Forensics
Module 12: Cloud Forensics
Module 13: Investigating Email Crimes
Module 14: Malware Forensics
Module 15: Mobile Forensics
Module 16: IoT Forensics