# Computer Hacking Forensic Investigator (CHFI)

## Duration: 5 Days

## Method: Instructor-Led Training (ILT)

***Certification:*** *Computer Hacking Forensic Investigator*

## Course Description

Digital technologies are changing the face of business. As organizations are rapidly embracing digital technologies such as cloud, mobile, big data and IoT, the context of digital forensics is more relevant than before. The growing number of cyber crimes has changed the role of forensics from DNA to Digital.

CHFI v9, the latest version of the program, has been designed for professionals handling digital evidence while investigating cybercrime. It covers the detailed methodological approach to computer forensics and evidence analysis. It provides the necessary skill set for identification of intruder's footprints and gathering the necessary evidence for use in prosecution. All major tools and theories used by the cyber forensic industry in the curriculum, which includes searching and seizing, chain-of-custody, acquisition, preservation, analysis and reporting of digital evidence. The certification can fortify the applied knowledge level of the target audience.

This is a comprehensive course, covering major forensic investigation scenarios, that enables participants to acquire necessary hands-on experience on various forensic investigation techniques and standard forensic tools necessary to successfully carry out computer forensic investigation leading to the prosecution of perpetrators. It covers all the relevant knowledge-bases and skills to meet with regulatory compliance standards such as ISO 27001, PCI DSS, SOX, HIPPA, etc. In addition, it also aims at elevating the knowledge, understanding, and skill levels of cybersecurity and forensic practitioners.

## Target Audience

This course is intended for:

- IT Professionals, IT Directors/Managers
- Information Security Managers
- Incident Response Team Members
- Network Defenders
- System/Network Engineers
- Security Analyst/Architect/Auditors/Consultants
- e-Business Security Professionals
- Attorneys, Legal Consultants, and Lawyers
- Banking and Insurance Professionals
- Police Officers and Other Law Enforcement Officers
- Detectives/Investigators
- Federal/Government Agents
- Defence and Military Personnel
- Anyone interested in cyber forensics/investigations

## Prerequisites

To attend this course, attendees must have:

- Basic knowledge of information technology, cybersecurity, computer forensics, and incident response.
  **NOTE:** Prior completion of CEH training would be an advantage.

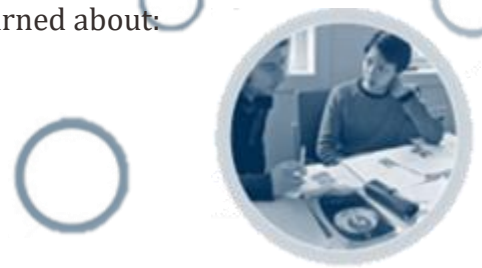
## Exam Details

| | |
|---|---|
| Exam Code: | • 312-49 |
| Length of Exam: | • 4 Hours |
| Number of Questions: | • 150 |
| Passing Score: | • 60% – 78% |
| Question Format: | • Multiple Choice |

## Course Objectives

Upon successful completion of this course, attendees will have learned about:

- How to set up a computer forensics lab.
- Password cracking.
- How to recover deleted files.
- How to write investigative reports.
- The roles of a first responder such as:
  - Securing and evaluating an electronic crime scene.
  - Conducting preliminary interviews.
  - Documenting electronic crime scenes.
  - Collecting and preserving electronic evidence.



REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
"Training You Can Really Use"

## Course Topics

- **Module 1.** Computer Forensics in Today's World
- **Module 2.** Computer Forensics Investigation Process
- **Module 3.** Understanding Hard Disks and File Systems
- **Module 4.** Data Acquisition and Duplication
- **Module 5.** Defeating Anti-Forensics Techniques
- **Module 6.** Operating System Forensics
- **Module 7.** Network Forensics
- **Module 8.** Investigating Web Attacks
- **Module 9.** Database Forensics
- **Module 10.** Cloud Forensics
- **Module 11.** Malware Forensics
- **Module 12.** Investigating Email Crimes
- **Module 13.** Mobile Forensics
- **Module 14.** Forensics Report Writing and Presentation

## LABS INCLUDED

Microsoft Partner
Silver Learning

EC-Council
Accredited
Training Center