Certified Hacking Forensic Investigator (CHFI)

Why CHFI Certifications ?

EC-Council's Certified Hacking Forensic Investigator (CHFI) is the only comprehensive ANSI accredited, lab-focused program in the market that gives organizations vendor-neutral training in digital forensics. CHFI provides its attendees with a firm grasp of digital forensics, presenting a detailed and methodological approach to digital forensics and evidence analysis that also pivots around Dark Web, IoT, and Cloud Forensics. The tools and techniques covered in this program will prepare the learner for conducting digital investigations using ground-breaking digital forensics technologies.

Training Solutions:

√ Offline Classroom Instructor-Led Training in our labs or onsite Locations.

√ Virtual Instructor-Led Training Via Virtual Video Conferencing Tools.

Why Learners Prefer CLS as their Training Services provider ?

■ Premuim Training Services Accredited from Global Technology Vendors.

■ Best Rated Experts & Certified Trainers in Egypt.

■ Official Training Hours, Practice Labs, Hands-on Learning.

■ CLS Training Classrooms are designed with High Edge PCs and Training Facilities.

■ Return on Training Investment is Guaranteed to boost performance.

Overview:

The Certified Ethical Hacker term was initially used to describe someone who possessed the skills necessary to be a hacker but whose moral code constrains them to stay within the bounds of legal activity. Over the years, the term ethical hacker has come to include all security professionals that provide offensive services, whether red team, pentester, or freelance offensive consultant.

The EC-Council organization certifies professionals in various e-business and security skills and knowledge. Their stated mission is to validate information security professionals who are equipped with the necessary skills and knowledge required in a specialized information security domain that will help them avert a cyber conflict, should the need ever arise.

CHFI 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

Course Objectives:

- Finding out about various kinds of cyber laws for investigating cyber-crimes.
- Analyzing digital evidence through rules of evidence by considering crime category.
- Roles of the first responder, first responder toolkit, securing and assessing electronic crime scene, directing preliminary interviews.
- Setting up the computer forensics lab and creating investigation reports.
- Steganography, Steganalysis and image forensics.
- Learn about Malware Forensics processes, along with new modules such as Dark Web Forensics and IoT Forensics.
- Skills to meet regulatory compliance standards such as ISO 27001, PCI DSS, SOX, HIPPA, etc.
- Kinds of log capturing, log management, Investigation logs, network traffic, wireless attacks, and web assaults.

Audience Profile :

Who Needs CHFI Certification?

CHFI program is designed for all IT professionals involved with information system security, computer forensics, and incident response.

- Police and other law enforcement personnel
- Defense and Security personnel
- e-Business Security professionals
- Legal professionals
- Banking, Insurance, and other professionals
- Government agencies
- IT managers

Prerequisities:

- IT/forensics professionals with basic knowledge of IT/cybersecurity, computer forensics, and incident response.
- Knowledge of Threat Vectors.