THE LEARNING CENTER
A TECHNICAL TRAINING INSTITUTION

C|HFI™

Computer Hacking Forensic INVESTIGATOR

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. The program is designed for IT professionals involved with information system security, computer forensics, and incident response. It will help fortify the application knowledge in digital forensics for forensic analysts, cybercrime investigators, cyber defense forensic analysts, incident responders, information technology auditors, malware analysts, security consultants, and chief security officers.

Course Goals:

- Play an active role in investigating and preserving digital and non-digital evidence of an attack.
- Counter to the series of compromises.
- Use threat intelligence to anticipate and alert cyber teams in case of future attacks.

EC-Council's CHFI is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements.

Our unique model follows a streamlined approach to workforce development and skills attainment

Assess: Assess each student to determine existing skill sets

Educate: Deliver goal-specific training utilizing all delivery modalities

Mentor: Expose students to instructors and mentors with front-line IT and cybersecurity experience

Certify: Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate: Validate student abilities through performance analytics and real-world exercises hosted on a cyber range

Exam Objectives: 312-49 CHFIv10

Forensic Science	18%
Regulations, Policies and Ethics	15%
Digital Evidence	17%
Procedures and Methodology	17%
Digital Forensics	17%
Tools/Systems/Programs	16%

Course Outline:

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: Windows Forensics
Module 7: Linux and Mac Forensics
Module 8: Network Forensics
Module 9: 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

Included

40 hours of instructor-led training sessions
Hands-on lab modules using industry tools
EC-Council authorized textbook/class materials