

Computer Hacking Forensic Investigator (CHFI)

Duration 5 Days

Course Description

EC-Council releases the most advanced Computer Forensic Investigation program in the world. CHFIv8 presents a detailed methodological approach to computer forensics and evidence analysis. It is a comprehensive course covering major forensic investigation scenarios that enable students 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 every day life. With the onset of sophisticated cyber-attacks, the need for advanced cyber security and investigation training is a mandate in the present day. If you or your organization requires the knowledge or skills to identify, track, and prosecute the cybercriminals, then this is the course for you. This course helps students to excel in digital evidence acquisition, handling and analysis in a forensically sound manner. Acceptable in a court of law, 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.

Course Outline

- Module 01: Computer Forensics in Today's World
- Module 02: Computer Forensics Investigation Process
- Module 03: Searching and Seizing Computers
- Module 04: Digital Evidence
- Module 05: First Responder Procedures
- Module 06: Computer Forensics Lab
- Module 07: Understanding Hard Disks and File Systems
- Module 08: Windows Forensics
- Module 09: Data Acquisition and Duplication
- Module 10: Recovering Deleted Files and Deleted Partitions
- Module 11: Forensics Investigation using AccessData FTK
- Module 12: Forensics Investigation Using EnCase
- Module 13: Steganography and Image File Forensics
- Module 14: Application Password Crackers
- Module 15: Log Capturing and Event Correlation
- Module 16: Network Forensics, Investigating Logs and Investigating Network Traffic
- Module 17: Investigating Wireless Attacks
- Module 18: Investigating Web Attacks
- Module 19: Tracking Emails and Investigating Email Crimes
- Module 20: Mobile Forensics
- Module 21: Investigative Reports
- Module 22: Becoming an Expert Witness

Who Should Attend

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

Certification

The CHFI 312-49 exam will be conducted on the last day of training. Students need to pass the online Prometric exam to receive the CHFI certification.