[CHFI]: Computer Hacking Forensic Investigator (CHFI) v9

Length : 5 Days
Delivery Method : Instructor-led (Classroom)

Course Overview

EC-Council's CHFI certifies individuals in the specific security discipline of computer forensics from a vendor-neutral perspective. The CHFI certification will fortify the application knowledge of law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of the network infrastructure.

Audience Profile

- Anyone interested in cyber forensics/investigations
- Attorneys, legal consultants, and lawyers
- Law enforcement officers
- Police officers
- Federal/ government agents
- Defense and military
- Detectives/ investigators
- Incident response team members
- Information security managers
- Network defenders
- IT professionals, IT directors/ managers
- System/network engineers
- Security analyst/ architect/ auditors/ consultants

At Course Completion

- Perform incident response and forensics
- Perform electronic evidence collections
- Perform digital forensic acquisitions
- Perform bit-stream Imaging/acquiring of the digital media seized during the process of investigation.
- Examine and analyze text, graphics, multimedia, and digital images
- Conduct thorough examinations of computer hard disk drives, and other electronic data storage media
- Recover information and electronic data from computer hard drives and other data storage devices

- Follow strict data and evidence handling procedures
- Maintain audit trail (i.e., chain of custody) and evidence integrity
- Work on technical examination, analysis and reporting of computer-based evidence
- Prepare and maintain case files
- Utilize forensic tools and investigative methods to find electronic data, including Internet use history, word processing documents, images and other files
- Gather volatile and non-volatile information from Windows, MAC and Linux
- Recover deleted files and partitions in Windows, Mac OS X, and Linux
- Perform keyword searches including using target words or phrases
- Investigate events for evidence of insider threats or attacks
- Support the generation of incident reports and other collateral
- Investigate and analyze all response activities related to cyber incidents
- Plan, coordinate and direct recovery activities and incident analysis tasks
- Examine all available information and supporting evidence or artefacts related to an incident or event
- Collect data using forensic technology methods in accordance with evidence handling procedures, including collection of hard copy and electronic documents
- Conduct reverse engineering for known and suspected malware files
- Identify data, images and/or activity which may be the target of an internal investigation
- Perform detailed evaluation of the data and any evidence of activity in order to analyze the full circumstances and implications of the event
- Establish threat intelligence and key learning points to support pro-active profiling and scenario modelling
- Search file slack space where PC type technologies are employed
- File MAC times (Modified, Accessed, and Create dates and times) as evidence of access and event sequences
- Examine file type and file header information
- Review e-mail communications including web mail and Internet Instant Messaging programs
- Examine the Internet browsing history
- Generate reports which detail the approach, and an audit trail which documents actions taken to support the integrity of the internal investigation process
- Recover active, system and hidden files with date/time stamp information
- Crack (or attempt to crack) password protected files
- Perform anti-forensics detection
- Maintain awareness and follow laboratory evidence handling, evidence examination, laboratory safety, and laboratory security policy and procedures

- Play a role of first responder by securing and evaluating a cybercrime scene, conducting preliminary interviews, documenting crime scene, collecting and preserving electronic evidence, packaging and transporting electronic evidence, reporting of the crime scene
- Perform post-intrusion analysis of electronic and digital media to determine the who, where, what, when, and how the intrusion occurred
- Apply advanced forensic tools and techniques for attack reconstruction
- Perform fundamental forensic activities and form a base for advanced forensics
- Identify and check the possible source/incident origin
- Perform event co-relation
- Extract and analyze logs from various devices such as proxies, firewalls, IPSes, IDSes, Desktops, laptops, servers, SIM tools, routers, switches, AD servers, DHCP servers, Access Control Systems, etc.
- Ensure that reported incident or suspected weaknesses, malfunctions and deviations are handled with confidentiality
- Assist in the preparation of search and seizure warrants, court orders, and subpoenas
- Provide expert witness testimony in support of forensic examinations conducted by the examiner
- Cyber security as a profession has seen tremendous growth over the past 10 years and EC-Council has been on the leading edge of this profession. Practices in Network Defense, Ethical Hacking, and Penetration Testing have proven to be the pillars of cyber security teams across the globe and Digital Forensics is no exception. Whether you operate a team of 2 or 2,000 to tackle Cyber issues facing your organization, digital forensics must be a part of the equation as a critical skill and daily practice

Certification

The CHFI certification is awarded after successfully passing the exam EC0 312-49. CHFI EC0 312-49 exams are available at ECC exam center around the world.

Examination

Number of Questions	150
Passing Score	70%
Test Duration	4 Hours
Test Format	Multiple Choice
Test Delivery	ECC exam portal

Pre-Requisites

- IT/forensics professionals with basic knowledge on IT/cyber security,
- computer forensics, and incident response
- Prior completion of CEH training would be an advantage

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: Operating System Forensics

Module 7: Network Forensics

Module 8: Investigating Web Attacks

Module 9: Database Forensic

Module 10: Cloud Forensic

Module 11: Malware Forensic

Module 12: Investigating Email Crimes

Module 13: Mobile Forensic

Module 14: Forensics Report Writing and Presentation