EC-Council Computer Hacking Forensic Investigator Certification v9 (CHFI)

Course Summary

Description

Digital technologies are changing the face of business. As organizations 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 cybercrimes has changed the role of forensics from DNA to Digital. According to the market research report published by IndustryARC, by 2020, the digital forensics market will reach 4.8 billion USD. IndustryARC also predicts that the maximum use of digital forensics is from the federal sector and this will grow from $1,097.2 million in 2015 to $2,060.5 million by 2020. The major drivers for this are increasing threats from cybercrime and terrorist attacks. Foote Partners, which tracks information technology (IT) jobs across all skill levels, projects the global demand for cyber security talent to rise to six million by 2019, with an expected shortfall of 1.5 million professionals. Over the last many years, EC-Council's CHFI certification has gained massive traction and recognition amongst Fortune 500 enterprises globally. It has immensely benefited professionals from law enforcement, criminal investigation, defense, and security field. CHF v9, the latest version of the program has been designed for professionals handling digital evidence while investigating cybercrimes. It is developed by an experienced panel of subject matter experts and industry specialists, and also has set global standards for computer forensics best practices. In addition, it also aims at elevating the knowledge, understanding, and skill levels of in cyber security and forensics practitioners.

CHFI v9 covers detailed methodological approach to computer forensic and evidence analysis. It provides the necessary skillset for identification of intruder's footprints and gathering necessary evidence for its prosecution. All major tools and theories used by cyber forensic industry are covered in the curriculum. The certification can fortify the applied knowledge level of law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, computer and network security professionals, and anyone who is concerned about the integrity of the network and digital investigations.

CHFI provides necessary skills to perform effective digital forensic investigation. It is a comprehensive course covering major forensic investigation scenarios that enables students to acquire necessary hands-on experience on various forensic investigation techniques and standard forensic tools necessary to successfully carryout computer forensic investigation leading to prosecution of perpetrators. CHFI presents a methodological approach to computer forensic including searching and seizing, chain-of-custody, acquisition, preservation, analysis and reporting of digital evidence.

Exam details:

- Number of Questions: 150
- Passing Score: 70%
- Test Duration: 4 hours
- Test Format: MCQ
- Test Delivery: Exam portal

Objectives

By the end of this course, students will be able to:

- 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.

EC-Council Computer Hacking Forensic Investigator Certification v9 (CHFI)

Course Summary (cont'd)

- 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

EC-Council Computer Hacking Forensic Investigator Certification v9 (CHFI)

Course Summary (cont'd)

- 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

Topics

- Computer Forensics in Today's World
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems
- Operating System Forensics
- Defeating Anti-Forensics Techniques
- Data Acquisition and Duplication
- Network Forensics
- Investigating Web Attacks
- Database Forensics
- Cloud Forensics
- Malware Forensics
- Investigating Email Crimes
- Mobile Forensics
- Investigative Reports

Audience

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

- 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

Prerequisites

Prior to taking this course, students should be IT/forensics professionals with basic knowledge on IT/cyber security, computer forensics, and incident response. Prior completion of CEH training would be an advantage.

Duration

Five days