Computer Hacking Forensic Investigator (CHFI)

Modality: Virtual Classroom

Duration: 5 Days

What's Included:

- *Official EC Council Invitation to the virtual class*
- *Official EC Council Print or e-courseware included*
- *EC Council Exam Voucher included*

About this Course:

Computer hacking forensic investigation is the process of detecting hacking attacks and properly extracting evidence to report the crime and conduct audits to prevent future attacks.

Computer crime in today's cyber world is on the rise. Computer Investigation techniques are being used by police, government and corporate entities globally and many of them turn to EC-Council for Computer Hacking Forensic Investigator CHFI Certification Program.

Computer Security and Computer investigations are changing terms. More tools are invented daily for conducting Computer Investigations, be it computer crime, digital forensics, computer investigations, or even standard computer data recovery. The tools and techniques covered in EC-Council's CHFI program will prepare the student to conduct computer investigations using groundbreaking digital forensics technologies.

Computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud. CHFI investigators can draw on an array of methods for discovering data that resides in a computer system, or recovering deleted, encrypted, or damaged file information known as computer data recovery.

Course Objectives:

- 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
- Perform detailed evaluation of the data and any evidence of activity in order to analyze the full circumstances and implications of the event
- Identify data, images and/or activity which may be the target of an internal investigation.
- 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

Audience:

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

Course 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