COURSE OUTLINE

Course Code: EC-CHFI

Course Name: CHFI: Computer Hacking Forensic Investigator

DURATION	SKILL LEVEL	DELIVERY METHOD	TRAINING CREDITS	TECHNOLOGY
5 day (s)	Advanced	In Class	N/A	Ethical Hacking

Course Overview

Digital forensic practices stem from forensic science, the science of collecting and examining evidence or materials. Digital or computer forensics focuses on the digital domain including computer forensics, network forensics, and mobile forensics. As the cyber security profession evolves, organizations are learning the importance of employing digital forensic practices into their everyday activities. Computer forensic practices can help investigate attacks, system anomalies, or even help System administrators detect a problem by defining what is normal functional specifications and validating system information for irregular behaviours.

In the event of a cyber-attack or incident, it is critical investigations be carried out in a manner that is forensically sound to preserve evidence in the event of a breach of the law. Far too many cyber-attacks are occurring across the globe where laws are clearly broken and due to improper or non-existent forensic investigations, the cyber criminals go either unidentified, undetected, or are simply not prosecuted.

Cyber Security professionals who acquire a firm grasp on the principles of digital forensics can become invaluable members of Incident Handling and Incident response teams. The Computer Hacking Forensic Investigator course provides a strong baseline knowledge of key concepts and practices in the digital forensic domains relevant to today's organizations. CHFI provides its attendees a firm grasp on the domains of digital forensics.

Prerequisites

• IT/forensics professionals with basic knowledge on IT/cyber security, computer forensics, and incident response.

• Prior completion of CEH training would be an advantage.

Target Audience

• Anyone interested in cyber forensics/investigations

• Incident response team members

• Information security managers

• Network defenders

• IT professionals, IT directors/managers

• System/network engineers

• Security analyst/ architect/auditors/ consultants

Topics

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 Forensics

Module 10:   Cloud Forensics

Module 11:   Malware Forensics

Module 12:   Investigating email crimes

Module 13:   Mobile Forensics

Module 14:   Forensics report writing and presentation

Exams and Certifications

At course completion

Upon completing this course, the learner will be able to understand:

• 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.