Computer Hacking Forensic Investigator (CHFI)

Duration 5 Days

COURSE DESCRIPTION

EC-Council's C|HFI program prepares cybersecurity professionals with the knowledge and skills to perform effective digital forensics investigations and bring their organization into a state of forensic readiness. Establishing the forensics process, lab, evidence handling procedures, and investigation techniques are required to validate/triage incidents and point the incident response teams in the right direction. Forensic readiness is crucial as it can differentiate between a minor incident and a major cyber-attack that brings a company to its knees.

This intense hands-on digital forensics program immerses students in over 68 forensic labs, working on crafted evidence files utilizing the tools of the world's top digital forensics professionals. Students will go beyond traditional hardware and memory forensics, covering current topics in cloud forensics, mobile and IoT, and investigating web application attacks and malware forensics. The C|HFI presents a methodological approach to computer forensics, including searching and seizing, chain-of-custody, acquisition, preservation, analysis, and reporting of digital evidence. Students learn various forensic investigation techniques and standard forensic tools. As they learn how to acquire and manage evidence through various operating environments, students also learn the chain of custody and legal procedures required to preserve evidence and ensure it is admissible in court, enabling the eventual prosecution of cyber criminals and containing liability on the victim organization.

WHAT WILL YOU LEARN?

- Computer forensics fundamentals, different types of cybercrimes and their investigation procedures, and regulations and standards that influence computer forensics investigation
- Various phases involved in the computer forensics investigation process
- Different types of disk drives and their characteristics, booting process and file systems in Windows, Linux, and Mac operating systems, file system examination tools, RAID and NAS/SAN storage systems, various encoding standards, and file format analysis
- Data acquisition fundamentals and methodology, eDiscovery, and how to prepare image files for forensics examination
- Various anti-forensics techniques used by attackers, different ways to detect them and related tools, and countermeasures
- Volatile and non-volatile data acquisition in Windows-based operating systems, Windows memory and registry analysis, electron application analysis, web browser forensics,and examination of Windows files, ShellBags, LNK files, jump lists, and Windows event logs
- Volatile and non-volatile data acquisition and memory forensics in Linux and Mac operating systems
- Network forensics fundamentals, event correlation concepts, Indicators of Compromise (IOCs) and ways to identify them from network logs, techniques and tools related to network traffic investigation, incident detection and examination, and wireless attack detection and investigation

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

- Malware forensics concepts, static and dynamic malware analysis, system and network behavior analysis, and ransomware analysis
- Web application forensics and challenges, web application threats and attacks, web application logs (IIS logs, Apache web server logs, etc.), and how to detect and investigate various web application attacks
- Tor browser working methodology and steps involved in the Tor browser forensics process
- Cloud computing concepts, cloud forensics and challenges, fundamentals of AWS, Microsoft Azure, and Google Cloud and their investigation processes
- Components in email communication, steps involved in email crime investigation, and social media forensics
- Architectural layers and boot processes of Android and iOS devices, mobile forensics process, various cellular networks, SIM file system, and logical and physical acquisition of Android and iOS devices
- Different types of IoT threats, security problems, vulnerabilities and attack surfaces areas, and IoT forensics processes and challenges

OUTLINE

Module 1: Computer Forensics in Today's World

- Understand the Fundamentals of Computer Forensics
- Understand Cybercrimes and their Investigation Procedures
- Understand Digital Evidence and eDiscovery
- Understand Forensic Readiness
- Understand the Role of Various Processes and Technologies in Computer Forensics
- Identify the Roles and Responsibilities of a Forensic Investigator
- Understand the Challenges Faced in Investigating Cybercrimes
- Understand Various Standards and Best Practices Related to Computer Forensics
- Understand Laws and Legal Compliance in Computer Forensics

Module 2: Computer Forensics Investigation Process

- Understand the Forensic Investigation Process and its Importance
- Understand First Response
- Understand the Pre-investigation Phase
- Understand the Investigation Phase
- Understand the Post-investigation Phase

Module 3: Understanding Hard Disks and File Systems

- Describe Different Types of Disk Drives and their Characteristics
- Explain the Logical Structure of a Disk
- Understand the Booting Process of Windows, Linux, and macOS Operating Systems
- Understand Various File Systems of Windows, Linux and macOS Operating Systems
- Understand File System Analysis
- Understand Storage Systems
- Understand Encoding Standards and Hex Editors
- Analyze Popular File Formats Using Hex Editor

Module 4: Data Acquisition and Duplication

- Understand Data Acquisition Fundamentals
- Understand eDiscovery
- Understand Data Acquisition Methodology
- Prepare an Image File for Examination

Module 5: Defeating Anti-forensics Techniques

- Understand Anti-forensics Techniques
- Discuss Data Deletion and Recycle Bin Forensics
- Illustrate File Carving Techniques and Ways to Recover Evidence from Deleted Partitions
- Explore Password Cracking/Bypassing Techniques
- Detect Steganography, Hidden Data in File System Structures, Trail Obfuscation, and File Extension Mismatch
- Understand Techniques of Artifact Wiping, Overwritten Data/Metadata Detection, and Encryption
- Detect Program Packers and Footprint Minimizing Techniques

Module 6: Windows Forensics

- Understand Windows Forensics
- Collect Volatile Information
- Collect Non-volatile Information
- Perform Windows Memory Analysis
- Perform Windows Registry Analysis
- Perform Electron Application Analysis
- Perform Web Browser Forensics
- Examine Windows Files and Metadata
- Understand ShellBags, LNK Files, and Jump Lists
- Understand Text-based Logs and Windows Event Logs

Module 7: Linux and Mac Forensics

- Collect Volatile Information in Linux
- Collect Non-volatile Information in Linux
- Understand Linux Memory Forensics
- Understand Mac Forensics
- Collect Volatile Information in Mac
- Collect Non-volatile Information in Mac
- Understand Mac Memory Forensics and Mac Forensics Tools

Module 8: Network Forensics

- Understand Network Forensics
- Summarize Event Correlation Concepts
- Identify Indicators of Compromise (IoCs) from Network Logs
- Investigate Network Traffic
- Perform Incident Detection and Examination Using SIEM Tools
- Understand Wireless Network Forensics
- Detect and Investigate Wireless Network Attacks

Module 9: Malware Forensics

- Understand Malware Concepts
- Understand Malware Forensics
- Perform Static Malware Analysis
- Analyzing Suspicious Documents
- Perform System Behavior Analysis
- Perform Network Behavior Analysis
- Perform Ransomware Analysis

Module 10: Investigating Web Attacks

- Understand Web Application Forensics
- Understand Internet Information Services (IIS) Logs
- Understand Apache Web Server Logs
- Detect and Investigate Various Attacks on Web Applications

Module 11: Dark Web Forensics

- Understand the Dark Web and Dark Web Forensics
- Determine How to Identify the Traces of Tor Browser during Investigation
- Perform Tor Browser Forensics

Module 12: Cloud Forensics

- Understand Cloud Computing Concepts
- Understand Cloud Forensics
- Understand Amazon Web Services (AWS) Fundamentals
- Perform AWS Forensics
- Understand Microsoft Azure Fundamentals
- Perform Microsoft Azure Forensics
- Understand Google Cloud Fundamentals
- Perform Google Cloud Forensics

Module 13: Email and Social Media Forensics

- Understand Email Basics
- Explain Email Crime Investigation and its Steps
- Understand U.S. Laws Against Email Crime
- Explain Social Media Forensics

Module 14: Mobile Forensics

- Understand Mobile Device Forensics
- Understand Android and iOS Architecture, Boot Process, and File Systems
- Understand Mobile Forensics Process
- Investigate Cellular Network Data
- Perform File System Acquisition
- Understand Phone Locks, Rooting, and Jailbreaking of Mobile Devices
- Perform Logical Acquisition on Mobile Devices
- Perform Physical Acquisition on Mobile Devices
- Perform Android and iOS Forensic Analysis

Module 15: IoT Forensics

- Understand IoT Concepts
- Perform Forensics on IoT Devices

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

WHO CAN APPLY?

Recommended Prerequisites for the C|HFI:

IT/Forensics professionals with basic knowledge of IT/cybersecurity, computer forensics, incident response, and threat vectors.

PREREQUISITES

IT/forensics professionals with basic knowledge of IT/cybersecurity, computer forensics, incident response, and threat vectors.

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.

- **Number of Questions:** 150
- **Passing Score:** 70%
- **Test Duration:** 4 hours
- **Test Format:** Multiple choice

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th

Call us today 0-2634-7993-4

177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th