INFOSECTRAIN

EC-Council Accredited Training Center

CHFI (v11)

(Computer Hacking Forensic Investigator)

Certification Training

INFOSECTRAIN

Course Highlights

- 40-Hour Instructor-led Training
- Training Certificate
- Learn with Real-World Scenarios
- Highly Interactive and Dynamic Sessions
- 98% Exam Pass Rate
- Learn from Industry Experts
- Career Guidance and Mentorship
- Extended Post Training Support
- Access to Recorded Sessions

INFOSECTRAIN

About Course

Computer Hacking Forensic Investigator (C|HFI) certification validates the expertise of security professionals in comprehensive computer forensics, including reporting incidents of cyber attacks and hacking attempts in the courts of law. C|HFI certification provides an extensive understanding of diverse cyber forensic techniques, ultra-modern forensic tools, evidence collection, and other critical elements required to perform thorough forensic investigations of hacking incidents, all with practical, hands-on experience.

This training is meticulously designed to expertly train the professionals intending to advance their careers as Forensic Investigators and execute their security roles and responsibilities with greater expertise. It offers practical insights into diverse, robust methodologies for addressing digital forensics concerns in the organization, constituting core fundamentals of security incidents, including infrastructure analysis and tools and techniques to identify and capture legal evidence against hackers and intruders.

Course Objectives

- Understand the fundamentals of digital forensics and cybercrime investigation techniques.
- Master anti-forensics techniques and methods to counteract them.
- Develop malware analysis and network forensics skills to detect and investigate cyber threats.
- Gain expertise in mobile forensics for comprehensive investigations.
- Perform forensic investigations on Windows, Linux, and macOS environments, including memory analysis and file system examination.
- Develop expertise in investigating dark web activities and social media forensics.
- Learn how to analyze web application attacks and investigate email crimes.
- Learn the fundamentals of cloud and IoT forensics.
- Prepare for real-world forensic challenges through hands-on labs and practical scenarios.

INFOSECTRAIN

Target Audience

- Incident Responder
- Cybercrime Investigator
- Cyber Defense Forensic Analyst
- Forensic Analyst
- Malware Analyst
- Security Consultant
- Chief Security Officer
- Information Technology Auditor

Pre-Requisites

- Basic understanding of IT, cybersecurity, computer forensics, and incident response.
- It is recommended to have CEH training and certification.

INFOSECTRAIN

Exam Information

Name of the Certification	C|HFI
Exam Code	312-49
Exam Format	Multiple Choice Questions
Exam Duration	240 Minutes
No. of Questions	150 Questions
Passing Score	60-85%

INFOSECTRAIN

Course Content

Module 1: Computer Forensics in Today's World

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

Module 2: Computer Forensic Investigation Process

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

Labs: Create a Hard Disk Image File for Forensics Investigation and Recover the Data

Module 3: Understanding Hard Disks and File Systems

- Disk Drives and their Characteristics
- Logical Structure of a Disk
- Booting Process of Windows, Linux, and mac Operating Systems
- File Systems of Windows, Linux, and mac Operating Systems
- File System Analysis
- Storage Systems
- Encoding Standards and Hex Editors
- Analyze Popular File Formats

Labs:

- Analyze File Systems of Linux and Windows Evidence Images and Recover the Deleted Files
- Analyze File Formats

Module 4: Data Acquisition and Duplication

- Data Acquisition
- eDiscovery
- Data Acquisition Methodology
- Preparing an Image File for Examination

Labs:

- Create a Forensic Image for Examination and Convert it into Various Supportive Formats for Data Acquisition

Module 5: Defeating Anti-Forensics Techniques

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

Labs:

- Perform Solid-State Drive (SSD) File Carving on Windows and Linux File Systems
- Recover Lost/Deleted Partitions and their Contents
- Crack Passwords of Various Applications
- Detects Hidden Data Streams and Unpacks Program Packers

Module 6: Windows Forensics

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

Labs:

- Acquire and Investigate RAM and Windows Registry Contents
- Examine Forensic Artifacts from Web Browsers
- Identify and Extract Forensic Evidence from Computers

Module 7: Linux and Mac Forensics

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

Labs:

- Perform Volatile and Non-volatile Data Acquisition on Linux and Mac Computers
- Perform Memory Forensics on a Linux Machine

Module 8: Network Forensics

- Network Forensics
- Event Correlation
- Indicators of Compromise (IoCs) from Network Logs
- Investigate Network Traffic
- Incident Detection and Examination
- Wireless Network Forensics
- Detect and Investigate Wireless Network Attacks

Labs:

- Identify and Investigate Network Attacks
- Analyze Network Traffic for Artifacts

Module 9: Malware Forensics

- Malware
- Malware Forensics
- Static Malware Analysis
- Analyze Suspicious Documents
- System Behavior Analysis
- Network Behavior Analysis
- Ransomware Analysis

Labs:

- Perform Static Malware Analysis
- Analyze a Suspicious PDF File and Microsoft Office Document
- Emotet Malware Analysis

Module 10: Investigating Web Attacks

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

Labs:

- Identify and Investigate Web Application Attacks

Module 11: Dark Web Forensics

- Dark Web and Dark Web Forensics
- Identify the Traces of Tor Browser during Investigation
- Tor Browser Forensics

Labs:

- Detect Tor Browser Activity and Examine RAM Dumps to Discover Tor Browser Artifacts

Module 12: Cloud Forensics

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

Labs:

- Forensic Acquisition and Examination of an Amazon EC2 Instance, Azure VM, and GCP VM

Module 13: Email and Social Media Forensics

- Email Basics
- Email Crime Investigation and its steps
- U.S. Laws Against Email Crime
- Social Media Forensics

Labs:

- Investigate a Suspicious Email to Extract Forensic Evidence

Module 14: Mobile Forensics

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

Labs:

- Investigate a Suspicious Email to Extract Forensic Evidence

Module 15: IoT Forensics

- IoT Concepts
- IoT Devices Forensics

INFOSECTRAIN
Educate. Excel. Empower.

www.infosectrain.com | sales@infosectrain.com

Version 11.0