C|HFI™
Computer Hacking Forensic INVESTIGATOR

Blitz Academy

COMPUTER HACKING FORENSIC INVESTIGATOR

Build Ultimate Investigative Skills And Organizational Forensic Readiness With Advanced Strategies

Master Skills of Forensic Investigation

Decode Compile Defend Legal Action

What is the Computer Hacking Forensic Investigator (C|HFI) Program?

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. This includes establishing the forensics process, lab and evidence handling procedures, as well as the investigation procedures 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, enabling them to work on crafted evidence files and utilize the tools employed by the world's top digital forensics professionals. Students will go beyond traditional hardware and memory forensics and learn current topics such as cloud forensics, mobile and IoT, investigating web application attacks, and malware forensics. C|HFI presents a methodological approach to computer forensics, including searching and seizing, chain-of-custody, acquisition, preservation, analysis, and reporting of digital evidence.

Key Features and Critical Components of the C|HFI Program

- Master a methodological forensics framework approach for performing digital forensics investigation:

1. Documenting the crime Scene
2 . Search and Seizure
3 . Evidence Preservation
4 . Data Acquisition
5 . Data Examination
6 . Reporting

- 15 modules covering core domains of digital forensics
- 2100+ pages of the comprehensive student manual
- 1550+ pages of lab manual covering detailed lab scenarios and instructions
- 600+ digital forensics tools
- 100% compliance with NICE Special publication 800-181 cyber security workforce framework
- 70+ GB of crafted evidence files for investigation purposes
- 68 hands on labs

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

What Skills You'll Learn

- Computer forensics fundamentals, different types of cybercrimes and their investigation procedures, along with 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, and 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.
- Malware forensics concepts, static and dynamic malware analysis, system and network behavior analysis, and ransomware analysis.

Exam Details

- **Exam Title** : Computer Hacking Forensic Investigator
- **Exam Code** : 312-49
- **Number of Questions** : 150
- **Duration** : 4 Hours
- **Availability** : EC-Council Exam Portal

Key Benefits of the C|HFI Program

- Build skills for investigating diverse types of digital forensic investigation.
- Gain in-depth knoweldge of volatile and non-volatile data acquisition and examination of Mac Operating Systems, RAM forensics, Tor forensics, etc. .
- Become proficient in malware forensics process and malware analysis, including the latest analysis: BlackCat (ALPHV) .
- Learn social media forensics and wireless network forensics.
- Emphasis on electron application and web browser forensics.
- Gain in-depth skills in mobile forensics analysis.

- Learn how to perform digital forensics investigation through Python scripting.
- Master a unique skill set: the C|HFI is the first certification to offer dark web and IoT forensics.
- Become skilled in forensic methodologies for Cloud Infrastructure (AWS, Azure and GCP).
- Learn techniques such as defeating anti-forensic techniques and Windows ShellBags, including analyzing LNK files and jump lists. .
- Learn the latest digital forensics tools/platforms and frameworks .
- Lab setup simulates real-life networks and platforms .
- C|HFI is designed and developed by subject matter experts and digital forensics practitioners worldwide after a rigorous job task analysis (JTA) of the job roles involved in the field of digital forensics, which also increases your employability .

Career Opportunities with the C|HFI

Job Roles With C|HFI

C|HFI captures all the essentials of digital forensics analysis and evaluation required for the modern world — tested and approved by veterans and top practitioners in the cyber forensics industry. From identifying the footprints of a breach to collecting evidence for prosecution, C|HFI guides students through every step of the process with experiential learning. Industry practitioners have engineered C|HFI for professionals to delve into 30+ lucrative job roles.

- Digital Forensics Analyst.
- Computer Forensic Analyst/Practitioner/ Examiner/Specialist/Technician/ Criminal Investigator/Lab Project Manager.

- Digital Forensics Analyst.
- Cybercrime Investigator.
- Computer Crime Investigator.
- Cyber Defense Forensics Analyst.
- Law Enforcement/Counterintelligence Forensics Analyst.
- Data Forensic Investigator.
- Digital Crime Specialist.
- Computer Security Forensic Investigator.
- Network/Technology Forensic Analyst/ Specialist.
- Digital Forensics and Incident Response Engineer.
- Forensic Imaging Specialist.
- Forensics and eDiscovery Analyst.
- Computer Forensics and Intrusion Analyst.
- Intrusions Forensics Lead.
- Security Engineer – Forensics.
- Malware Analyst.
- Mobile Forensic Analyst/Expert.
- Mobile Exploitation Analyst.
- Information Systems Security Professional/Analyst.

Contact Us

Blitz Academy, Corporate office

📍 No.48, I star building, 100 feet Road Near Sony Signal, 4th Stage Koramangala,
Bangalore, Karnataka, India-560034

☎ +91 9513513007, +91 9061106007

✉ info@blitzacademy.org

Blitz Academy, Registered office

📍 41/2553-D, 2nd Floor,
Metro Palace, Opp.North Railway Station
Ernakulam,Kerala - 602018

☎ +91 9061106007, +91 9061903007

✉ info@blitzacademy.org

Blitz Academy, MG Road, Kochi

📍 62/5197, 1st floor Perumpillil Building,
Near Maharajas Metro Station,MG Road,
Ernakulam, Kerala, India-682011

☎ +91 9061106007, +91 9061903007

✉ info@blitzacademy.org