5 Days

CHFI v10 (Computer Hacking Forensic Investigator)

Criminal investigation isn't just limited to the physical world anymore. With Cybercrimes rising faster than the availability of competent professionals, and spanning geographies, it is almost compulsory to undergo CHFI Certification Training. This accreditation spans 16 modules, professionals as young as 2 years in the Information Security industry can enrich their knowledge, terms, tricks and most importantly technologies to upgrade their career and stand out from volumes of Cybersecurity workers.

What's new in CHFI Certification v10?

One of the updations in the CHFI v10 exam is the expansion of modules from 14 to 16, removal of modules like Forensics report writing and presentation, and addition of Operating Systems based Forensics which are Windows, Linux and Mac. Files in excess of 50GB are available as crafted evidence for investigation purposes, apart from the fact that more than half of forensic labs under EC-Council are new and advanced.

Certified Hacking Forensic Investigator is a Information Security certification and its tenth version has the following technologies:

- Fileless Malware Analysis like Emotet, EternalBlue
- Fresh tools like Anti-Malware, Windows ShellBags, Analyzing LNK files, Jump Lists
- JTAG and Chip-Off forensics
- Forensic tools like Splunk, Paraben's E3, PhotoRec, R-Studio, Bulk Extractor, KAPE
- Memory Forensic tools like Redline, Volatility Framework
- Internet of Things Forensics

Why CHFI Training?

A hacking forensic investigator is someone who is responsible for a digital criminal investigation, among other things. During CHFI Certification Training, it is important that learners come up to date, or revise the below concepts and technologies:

- Meet benchmarks such as ISO 27001, PCI DSS, SOX, HIPPA
- Learning about log capturing, log management, Investigation logs, network traffic, wireless attacks, and web assaults
- Extract and analyze logs, use proxy, firewall, IPS, IDS, Desktop, laptop, servers, SIM tool, router, firewall, switches, AD server, DHCP logs, AC Logs, Encase Steganography, Steganalysis & finalize them as part of the investigation process.
- Conducting incident response and forensics, bit-stream Imaging/disk imaging and analyzing .dd images, RAW, other formats and filing MAC times
- Updating tricks, and terms of EnVolatile & Non-volatile data acquisition, RAM Forensics, Tor Forensics
- Performing post-intrusion analysis to determine the who, where, what, when, and how the incision occurred.
- Investigate wireless attacks, different website attacks, and tracking emails from suspicious sources to keep a check on email crimes.

Course Details

Course Outline

This is the syllabus of version 10 of CHFI Certification Training:

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-Forensic Techniques

Module 6: Windows Forensics

Module 7: Linux and Mac Forensics

Module 8: Network Forensics

Module 9: 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

Who Should Attend

Certified Hacking Forensic Investigator from EC-Council is a hugely popular cybersecurity certification which attracts professionals from across the spectrum. Below is a list of designations who should pay CHFI Certification Cost. These are also those posts which learners may get post this prestigious accreditation.

- Manager- Information Security
- Manager- Information Security Risk
- Director, Information Technology Security
- Senior Information Technology Security Manager- Cloud & Digital
- Senior Network Security Engineering Specialist
- Senior Principal, Digital Forensics
- Senior Network Security Engineering Consultant
- Senior Cyber Security Consultant
- Senior Incident Response Consultant
- Senior Cyber Security Analyst
- Senior Cyber Threat Intel Analyst
- Senior Forensic Analyst
- Senior Information Assurance Analyst
- Senior Investigative Analyst
- Senior Network Security Engineer
- Team Lead
- Cyber Systems Administrator
- Cyber Systems Administrator
- Disaster Recovery Expert
- Mobile Forensics Expert
- Computer Forensic Specialist
- Security Specialist
- Information Security and Risk Assessment Specialist
- Security Consultant

- Application Security Analyst
- Computer Forensic Analyst
- Cyberspace Analyst
- Cryptanalyst
- Cyber Defense Forensic Analyst
- Cyber Risk Defense Analyst
- Cyber Security Analyst
- Cyber Security Analyst Advisor
- Cyber Security Intelligence Analyst
- Cyber Threat Analyst
- Cyber Threat Intelligence Analyst
- Forensic Analyst
- Junior Digital Forensics Analyst
- Information Security Analyst
- Intrusion Analyst
- Forensic Computer Analyst
- Information Security Analyst
- Intelligence Technology Analyst
- Malware Analyst
- Cybercrime Investigator
- Forensic Accountant
- Computer Forensics Technician
- Cybersecurity Auditor
- Information Technology Auditor
- Computer Forensics Examiner
- Incident Response Forensic Examiner
- Cyber Forensic Investigator
- Computer Crime Investigator
- Computer Forensics Criminal Investigator
- Cybersecurity Engineer
- Cybersecurity Systems Engineer
- Cyber Security Project Engineer
- Information Security Engineer
- Principal Cyber Security Engineer
- Security Operations Engineer
- Principal Cyber Operator
- Penetration Tester
- Security Control Assessor
- Cyber Security Associate
- Cryptographer

Pre Requisite

Official CHFI training is in the domain of Cybersecurity and requires professionals with more than 2 years of information security work experience.

Exams

Certified Hacking Forensic Investigator [CHFI] [ECO-312-49]

464, Udyog Vihar Phase V,Gurgaon (Delhi NCR)-122016,India

+91 8882 233 777

training@mercury.co.in

www.mercurysolutions.co

Date - Apr 24, 2025