Certified Hacking Forensic Investigator v10

Duration: 5 days; /35 hours; Instructor-led/ remote online training
Time: 9.00am – 5.00pm
Break: 10.15am – 10.30am /3.15pm – 3.30pm
Lunch: 1.00pm – 2.00pm

WHAT YOU WILL LEARN

EC-Council's Certified Hacking Forensic Investigator (CHFI) is the only comprehensive ANSI accredited, lab-focused program in the market that gives organizations vendor-neutral training in digital forensics. CHFI provides its attendees with a firm grasp of digital forensics, presenting a detailed and methodological approach to digital forensics and evidence analysis that also pivots around Dark Web, IoT, and Cloud Forensics. The tools and techniques covered in this program will prepare the learner for conducting digital investigations using ground-breaking digital forensics technologies.

The program is designed for IT professionals involved with information system security, computer forensics, and incident response. It will help fortify the application knowledge in digital forensics for forensic analysts, cybercrime investigators, cyber defense forensic analysts, incident responders, information technology auditors, malware analysts, security consultants, and chief security officers.

The program equips candidates with the necessary skills to proactively investigate complex security threats, allowing them to investigate, record, and report cybercrimes to prevent future attacks

Why CHFI v10?

- EC-Council is one of the few ANSI 17024 accredited institutions globally that specializes in Information Security. The Computer Hacking Forensic Investigator (CHFI) credential is an ANSI 17024 accredited certification.
- The CHFI v10 program has been redesigned and updated after a thorough investigation into current market requirements, job tasks analysis, and the recent industry focuses on forensic skills.
- It is designed and developed by experienced subject matter experts and digital forensics practitioners.
    - CHFI v10 program includes extensive coverage of Malware Forensics processes, along with new modules such as Dark Web Forensics and IoT Forensics.
    - It also covers detailed forensic methodologies for public cloud infrastructure, including Amazon AWS and Azure.
    - The program is developed with an in-depth focus on Volatile data acquisition and examination processes (RAM Forensics, Tor Forensics, etc.).
- CHFI v10 is a complete vendor-neutral course covering all major forensics investigation technologies and solutions.
- CHFI has detailed labs for a hands-on learning experience. On average, 50% of training time is dedicated to labs, loaded on EC-Council's CyberQ (Cyber Ranges). It covers all the relevant knowledge bases and skills to meet regulatory compliance standards such as ISO 27001, PCI DSS, SOX, HIPPA, etc.
- It comes with an extensive number of white papers for additional reading.
- The program presents a repeatable forensics investigation methodology from a versatile digital forensic professional, increasing employability.

- The courseware is packed with forensics investigation templates for evidence collection, the chain of custody, final investigation reports, etc.
- The program comes with cloud-based virtual labs, loaded on advanced Cyber Ranges, enabling students to practice various investigation techniques in real-time and realistically simulated environments.

AUDIENCE

The CHFI program is designed for all IT professionals involved with information system security, computer forensics, and incident response.

- Police and other law enforcement personnel
- Defense and Military personnel
- e-Business Security professionals
- Systems administrators
- Legal professionals
- Banking, Insurance and other professionals
- Government agencies
- IT managers
- Digital Forensics Service Providers

PREREQUISITES

- IT/forensics professionals with basic knowledge of IT/cybersecurity, computer forensics, and incident response.
- Has knowledge of Threat Vectors.

METHODOLOGY

This program will be conducted with interactive lectures, PowerPoint presentation, discussion, and practical exercise.

COURSE OBJECTIVES

A BREACH can be BRUTAL. Investing in building an expert in-house forensics team with CHFI training and certification is a strategic move for enterprises looking to safeguard their stakeholders' interests as well as their own. CHFI empowers their existing team with learning the latest investigation practices.

The course aligns with all the crucial forensic job roles across the globe.

It is an ANSI 17024 accredited Certification Program, mapped to the NICE 2.0 framework.

The course focuses on the latest technologies including IoT Forensics, Dark Web Forensics, Cloud Forensics (including Azure and AWS), Network Forensics, Database Forensics, Mobile Forensics, Malware Forensics (including Emotet and Eternal Blue), OS Forensics, RAM forensics and Tor Forensics, CHFI v10 covers the latest tools, techniques, and methodologies along with ample crafted evidence files.

COURSE OUTLINES

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 ad Duplication

Module 5: Defeating Anti-Forensics Techniques

Module 6: Windows Forensics

Module 7: Linux and Mac Forensics

Module 8: Network Forensics

Module 9: Investigation 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

Module 17: About the Exam

Module 18: CHFI Exam Details