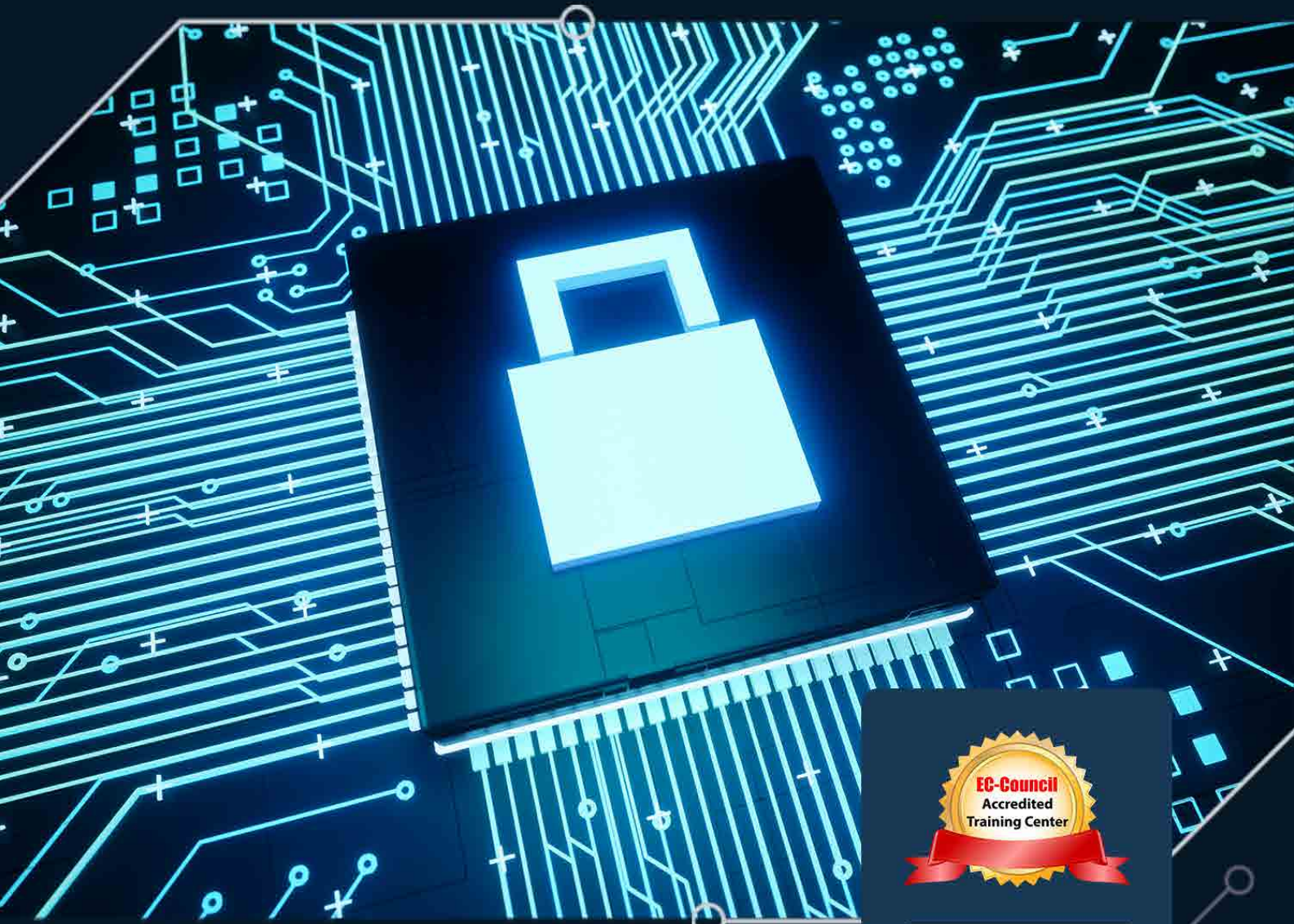
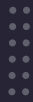


CHFI v10

Computer Hacking
Forensic Investigator

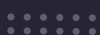


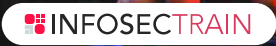


Overview

Computer Hacking Forensic Investigation (CHFI) is an all-encompassing certification training course devised by EC-council that helps security professionals stay ahead of the curve with extensive know-how of detecting and investigating the cyber-attacks and exploiting all crucial evidences to support the investigation reports. This certification also focuses to explain all vital components to perform security audits ensuring prevention from such attacks in the future. CHFI certification authenticates the expertise of security professionals in overall computer forensics including reporting the incidents of cyber-attacks and hacking attempts in the courts of law.

Computer Hacking Forensic Investigator (CHFI v10) is a vendor-neutral training certification that imbibes extensive understanding of diverse cyber forensic techniques, ultra-moderns forensic tools, footprints collection, and other essential components to conduct far-reaching hacking forensic investigations with hands-on exposure. This training has been exclusively designed to expertly train the professionals intending to advance their career as Forensic Investigators and execute their security roles with more proficiency. It focuses to practically explain miscellaneous foolproof methodologies to address digital forensics concerns in the organization, that constitute core fundamentals of security incidents including security infrastructure analysis tools and techniques to identify and capture legal evidence against the hackers and intruders. CHFI v10 certification enables the cyber investigators to detect incidents such as compromising of the confidential data, trade secret thefts, exploitation of the intellectual property, and digital frauds.





Target Audience

The CHFI v10 training and certification course have been developed to equip the security professionals accountable for various executing roles pertaining to the computer forensics, incident response, and information system security. It helps the workforce in the roles of:

- Digital Forensic Examiner
- Computer Crime Investigator
- Computer Forensic Analyst
- Network Forensic Examiner
- Computer Network Defense (CND) Forensic Analyst
- Forensic Analyst and technician
- Special Agent







Pre-Requisite

Basic understanding of IT, cybersecurity, computer forensics, and incident response CEH training and certification recommended





Why Infosec Train?

 <p>Certified & Experienced Instructor</p>	 <p>Flexible Schedule</p>	 <p>Access to the recorded sessions</p>
 <p>Post Training Support</p>	 <p>Tailor Made Training</p>	 <p>4 hrs/day in Weekend/ Weekday</p>

Exam Information

Certification Name	312-49 (ECC EXAM)
Test Format	Multiple choice questions
Number of Questions	150
Test Duration	4 Hours



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 focus 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.





Industries that prefer CHFI professionals



e-Businesses



Government Agencies



Legal Firms



Information Technology



Banking and Finance



Defense and Security



Law Enforcement



Digital Forensics
Service Providers



Course Outline

CHFI v9 curriculum is a comprehensive course with 14 training modules covering major forensic investigation scenarios



Module 1. Computer forensics in today's world



Module 9. Network forensics



Module 2. Computer forensics investigation process



Module 10. Investigating web attacks



Module 3. Understanding hard disks and file systems



Module 11. Database forensic



Module 4. Data acquisition and duplication



Module 12. Cloud forensic



Module 5. Defeating anti-forensics techniques



Module 13. Malware forensic



Module 6. Windows Forensics



Module 14. Investigating email crimes



Module 7. Linux and Mac Forensics



Module 15. Mobile forensic



Module 8. Operating system forensics



Module 16. Forensics report writing and presentation





www.infosectrain.com | sales@infosectrain.com