5 Days

CHFI v9 (Computer Hacking Forensic Investigator)

CHFI certification course is the world's most comprehensive computer hacking forensic program that delivers essential knowledge of digital forensic techniques and standard forensic tools accompanied by hands-on labs to identify intruder footprints and gather necessary evidence for its prosecution.

Thie CHFI Certification presents a methodological approach to digital forensics including searching and seizing, chain-of-custody, acquisition, preservation, analysis, and reporting of digital evidence.

It sets global standards for computer forensic best practices having set a recognition amongst Fortune 500 enterprises globally.

WHAT'S NEW IN CHFI V9?

- 14 comprehensive modules and 39 labs
- Coverage of latest forensics examination techniques, including Linux and MAC Forensics
- Courseware covers Digital Forensics Laws and Standards
- Labs on Defeating Anti-Forensics Techniques, Database Forensics, Cloud Forensics and Malware Forensics
- More than 40 percent new labs are added
- More than 300 new instructor slides
- More than 400 new/updated tools

WHY CHFI?

- The CHFI program has been redesigned and modified after thorough research and development analyzing current market requirements, job tasks, and recent industry emphasis on forensic skills.
- CHFI training includes exhaustive labs for hands-on labs experience. On an average, approximately 50% of training time is dedicated to labs.
- This training delivers relevant knowledge and skills required to meet with regulatory compliance standards such as ISO 27001, PCI DSS, SOX, HIPPA, etc.
- The program presents a repeatable forensics investigation methodology required from a versatile digital forensic professional which increases employability
- The training curriculum runs with cloud-based virtual labs enabling students to practice various investigation techniques in a real-time and simulated environment.

Course Details

Course Outline

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-forensics Techniques
Module 6. Operating system forensics
Module 7. Network forensics
Module 8. Investigating web attacks
Module 9. Database forensic
Module 10. Cloud forensic
Module 11. Malware forensic
Module 12. Investigating email crimes
Module 13. Mobile forensic

Who Should Attend

- E-Business Security professionals
- Defense and Military personnel
- Systems administrators
- T managers
- Police & law enforcement personnel
- Government agencies
- Legal professionals
- Banking, Insurance and other professionals

Pre Requisite

- IT/forensics professionals with basic knowledge on IT/cyber security,
- computer forensics, and incident response
- Prior completion of CEH training would be an advantage

Exams

CHFI v9 [EC0 312-49]

464, Udyog Vihar Phase V,Gurgaon (Delhi NCR)-122016,India | +91 8882 233 777 | training@mercury.co.in | www.mercurysolutions.co

Date - May 23, 2025