

CHFI Certification - Computer Hacking Forensic Investigator Training CHFI v10

Course: **00059**

Filter: **Beginner**

Duration: **20 hours**

Category:: **Gouvernance, Risk and Compliance**

Price: **2500,00 €**

About Course

This EC-Council Computer Hacking Forensic Investigator (CHFI) certification course will prepare you to achieve this in-demand certification. Learn a detailed, methodological approach to computer forensic and evidence analysis, including searching and seizing, chain-of-custody, acquisition, preservation, analysis, and reporting of digital evidence. This CHFI certification course provides the necessary skills to perform effective digital forensic investigations and covers the primary tools and theories used by cyber forensic experts today. Passing the CHFI Certification Exam meets U.S. DoD Directive 8140/8570.01 CSSP Incident Responder and CSSP Infrastructure Support requirements.

What you'll learn

- Perform electronic evidence collections.
- Perform digital forensic acquisitions.
- Conduct thorough examinations of computer hard disk drives and other electronic data storage media.
- Utilize forensic tools and investigative methods to find electronic data, including Internet use history, word processing documents, images, and other files.
- Perform anti-forensics detection
- Apply advanced forensic tools and techniques for attack reconstruction.

Pre-requisites

- Prior completion of the Learning Tree course 2031, Certified Ethical Hacker (CEH) Training, would be an advantage.

Curriculum

Module 1: CHFI Certification

- Computer Forensics in Today's World
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems
- Operating System Forensics
- Defeating Anti-Forensics Techniques
- Data Acquisition and Duplication
- Network Forensics
- Investigating Web Attacks
- Database Forensics
- Cloud Forensics
- Malware Forensics
- Investigating Email Crimes
- Mobile Forensics
- Investigative Reports

Module 2: CHFI On-Demand

- Computer Forensics in Today's World
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems
- Operating System Forensics
- Defeating Anti-Forensics Techniques
- Data Acquisition and Duplication
- Network Forensics
- Investigating Web Attacks
- Database Forensics
- Cloud Forensics
- Malware Forensics

- Investigating Email Crimes
- Mobile Forensics
- Investigative Reports