C|HFI

Computer Hacking Forensic Investigator

A Step By Step Guide To Level Up Your Career On CYBER SECURITY



Course Highlights & Exam Information

CHFI Computer Hacking Forensic INVESTIGATOR



Exam Information

Exam Name	CHFI Theory (MCQ)
Exam Format	MCQ Questions
No. Of Questions	150 Questions
Exam Duration	4 Hours

Introducing Computer Hacking Forensic Investigator CHFI

Computer Hacking Forensic INVESTIGATOR

- The Computer Hacking Forensic Investigator (CHFI) Course Is A Professional Certification Offered By Ec-council That Focuses On The Field Of Digital Forensics And Cybercrime Investigation. It Equips It Professionals, Law Enforcement Personnel, And Cybersecurity Experts With The Skills Necessary To Identify, Track, And Investigate Cybercriminal Activity, Using A Variety Of Forensic Tools And Techniques.

- This Course Is Ideal For Professionals Involved In Incident Response, Cybersecurity Operations, Law Enforcement, Or Anyone Looking To Specialize In Digital Forensics. Chfi Certification Is Globally Recognized And Demonstrates An Individual's Ability To Handle Computer-based Investigations And Support Legal And Corporate Security Processes. The Knowledge Gained From This Course Is Essential In Today's Digital World, Where Cybercrime Continues To Grow In Frequency And Sophistication



Computer Hacking Forensic Investigator

Modules C|HFI Computer Hacking Forensic INVESTIGATOR

Module 01 Computer Forensics in Today's World

- Introduction to Computer Forensics
- Importance in Cybercrime Investigation
- Digital Evidence Collection & Analysis
- Modern Tools and Techniques in Forensics
- Legal, Ethical & Future Challenges in Digital Forensics

Module 02 Computer Forensics Investigation Process

- Identification of Digital Evidence
- Evidence Collection and Preservation
- Data Examination and Analysis
- Documentation and Reporting
- Presentation in Legal Proceedings

Module 03 Understanding Hard Disks and File Systems

- Basics of Hard Disk Structure
- Types of Storage Devices
- Introduction to File Systems
- Data Storage and Organization
- Common File System Formats

Computer Hacking Forensic Investigator

Modules C|HFI Computer Hacking Forensic INVESTIGATOR

Module 04 Data Acquisition and Duplication

- Introduction to Data Acquisition
- Methods of Evidence Collection
- Disk Imaging and Cloning Techniques
- Data Integrity and Verification
- Challenges in Data Duplication

Module 05 Defeating Anti-Forensics Techniques

- Introduction to Anti-Forensics
- Common Anti-Forensics Methods
- Detecting Hidden or Deleted Data
- Techniques to Counter Anti-Forensics
- Challenges in Modern Investigations

Module 06 Windows Forensics

- Introduction to Windows Forensics
- Windows File System Analysis
- Registry and Event Log Investigation
- User Activity and Artifact Analysis
- Windows Forensic Tools and Techniques

Computer Hacking Forensic Investigator

Modules C|HFI Computer Hacking Forensic INVESTIGATOR

Module 07 Linux and Mac Forensics

- Introduction to Linux and Mac Forensics
- File System and Storage Analysis
- Log and User Activity Investigation
- Artifact Recovery and Examination
- Forensic Tools for Linux and macOS

Module 08 Network Forensics

- Introduction to Network Forensics
- Network Traffic Monitoring and Analysis
- Packet Capture and Log Investigation
- Detection of Network Attacks
- Network Forensic Tools and Techniques

Module 09 Malware Forensics

- Introduction to Malware Forensics
- Types of Malware and Threats
- Malware Detection and Analysis
- Reverse Engineering Techniques
- Malware Investigation Tools and Challenges

Computer Hacking Forensic Investigator

Modules C|HFI Computer Hacking Forensic INVESTIGATOR

Module 10 Investigating Web Attacks

- Introduction to Web Attacks
- Common Types of Web Attacks (SQL Injection, XSS, etc.)
- Log Analysis and Evidence Collection
- Tracing Attack Sources and Methods
- Web Forensics Tools and Mitigation Strategies

Module 11 Dark Web Forensics

- Introduction to the Dark Web and Tor Network
- Identifying Dark Web Activities and Threats
- Evidence Collection from Hidden Services
- Tracking Cybercriminal Behavior and Transactions
- Legal, Ethical, and Technical Challenges in Dark Web Investigations

Module 12 Cloud Forensics

- Introduction to Cloud Forensics
- Cloud Architecture and Evidence Sources
- Data Collection from Cloud Environments
- Investigation of Cloud-Based Incidents
- Challenges, Security, and Legal Issues in Cloud Forensics

Computer Hacking Forensic Investigator

Modules C|HFI Computer Hacking Forensic INVESTIGATOR

Module 13 Email and Social Media Forensics

- Introduction to Email and Social Media Forensics
- Email Header and Metadata Analysis
- Recovery and Examination of Deleted Messages
- Social Media Activity Tracking and Evidence Collection
- Challenges, Privacy Issues, and Legal Considerations

Module 14 Mobile Forensics

- Introduction to Mobile Forensics
- Mobile Device Data Acquisition
- Analysis of Call Logs, Messages, and Apps
- Recovery of Deleted and Hidden Data
- Challenges, Security, and Legal Aspects

Module 15 IoT Forensics

- Introduction to IoT Forensics
- IoT Device Architecture and Data Sources
- Evidence Collection from IoT Devices
- Analysis of IoT Logs and Communication Data
- Challenges, Security, and Legal Issues in IoT Forensics

Why Choose Us?

We provide the best CHFI training in india with expert instructors, official Ec-Council certification, and government-recognized training. our courses include flexible online and offline options, personal guidance, and special corporate programs to build real-world cybersecurity skills. join us to start your journey withthe best support and practical knowledge!

1. Online & Offline Lectures
2. Language : English & Hindi
3. Corporate Trainings
4. Certified Instructors
5. Live Interactive Classes
6. Access To Recorded Sessions
7. Ec-council's Authorized Training Partner

Follow us on:

Contact Us

+91 8448046612

www.cyberdefentech.com

D-12/ 77,78, 2nd Floor, Sector-08,
Rohini East, Delhi - 110085