Certified Hacking Forensic Investigator (CHFI) Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The rapid rise of cybercrime and sophisticated Advanced Persistent Threats (APTs) has created a critical demand for specialists who can meticulously investigate security breaches. The Certified Hacking Forensic Investigator (CHFI) course is a comprehensive, vendor-neutral program designed to equip cybersecurity and IT professionals with the essential skills to conduct professional, legally-sound digital forensics investigations. You will master a systematic methodology encompassing evidence acquisition, preservation of the chain of custody, in-depth forensic analysis across various operating systems and platforms, and the crucial skill of presenting findings as a credible expert witness. Certified Hacking Forensic Investigator (CHFI) Training Course focuses on the practical application of cutting-edge forensic tools and techniques to identify, track, and prosecute cybercriminals, ensuring your organization achieves and maintains forensic readiness against both internal and external threats.

This program goes beyond traditional disk forensics to cover modern, complex areas like Cloud Forensics, Mobile Device Forensics, IoT Forensics, and Malware Reverse Engineering. By integrating theoretical knowledge with extensive hands-on labs and real-world case studies, the CHFI course provides an invaluable, career-defining expertise for incident response teams, law enforcement, and security consultants. Graduates will be prepared to decisively respond to incidents, recover deleted or encrypted data, defeat anti-forensics techniques, and ultimately safeguard digital assets while ensuring all collected evidence is admissible in court, closing the loop on the entire cyber incident lifecycle.

Programme Curriculum

Certified Hacking Forensic Investigator (CHFI) Training Course

Introduction

The rapid rise of cybercrime and sophisticated Advanced Persistent Threats (APTs) has created a critical demand for specialists who can meticulously investigate security breaches. The Certified Hacking Forensic Investigator (CHFI) course is a comprehensive, vendor-neutral program designed to equip cybersecurity and IT professionals with the essential skills to conduct professional, legally-sound digital forensics investigations. You will master a systematic methodology encompassing evidence acquisition, preservation of the chain of custody, in-depth forensic analysis across various operating systems and platforms, and the crucial skill of presenting findings as a credible expert witness. Certified Hacking Forensic Investigator (CHFI) Training Course focuses on the practical application of cutting-edge forensic tools and techniques to identify, track, and prosecute cybercriminals, ensuring your organization achieves and maintains forensic readiness against both internal and external threats.

This program goes beyond traditional disk forensics to cover modern, complex areas like Cloud Forensics, Mobile Device Forensics, IoT Forensics, and Malware Reverse Engineering. By integrating theoretical knowledge with extensive hands-on labs and real-world case studies, the CHFI course provides an invaluable, career-defining expertise for incident response teams, law enforcement, and security consultants. Graduates will be prepared to decisively respond to incidents, recover deleted or encrypted data, defeat anti-forensics techniques, and ultimately safeguard digital assets while ensuring all collected evidence is admissible in court, closing the loop on the entire cyber incident lifecycle.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Master the Digital Forensics Methodology and Chain of Custody protocols.
2. Conduct advanced Volatile Data Acquisition and Non-Volatile Data collection.
3. Perform comprehensive Windows Forensics and File System Analysis
4. Implement techniques to Defeat Anti-Forensics and recover hidden/wiped data.
5. Execute specialized Network Forensics for incident detection and event correlation.
6. Analyze compromised systems using Memory Forensics and live acquisition tools.
7. Investigate data breaches and evidence across major Cloud Platforms
8. Perform effective Malware Analysis and Reverse Engineering of suspicious code.
9. Conduct Mobile Device Forensics on both Android and iOS operating systems.
10. Explore and forensically analyze activities on the Dark Web
11. Collect and analyze evidence from IoT Devices and embedded systems.
12. Generate professional, Legally Admissible Forensic Reports for litigation.
13. Apply the principles of Forensic Readiness and proactive threat hunting.

Target Audience

1. Digital Forensics Investigators
2. Incident Response Team Members
3. Cybercrime and Law Enforcement Personnel
4. IT Security Managers and SOC Analysts
5. eDiscovery Professionals and Legal Consultants
6. Information Security Auditors and Consultants
7. System and Network Administrators
8. Threat Intelligence Analysts

Course Modules

Module 1: Forensic Foundations & Legal Procedures

- Digital Evidence standards, rules, and types.
- The Forensic Investigation Process and first responder roles.
- Establishing and maintaining the strict Chain of Custody.
- Setting up a fully equipped Forensic Lab environment.
- Legal Compliance and serving as an Expert Witness.
- Case Study: The Enron Email Scandal.

Module 2: Data Acquisition and Anti-Forensics

- Hard Disk and File System Analysis
- Data Acquisition methodologies
- Forensically sound Disk Imaging and Hashing/Verification.
- Techniques to Defeat Anti-Forensics
- File Carving and recovering data from deleted partitions.
- Case Study: Defeating File Shredding.

Module 3: Operating System Forensics

- In-depth Windows Artifacts analysis.
- Memory Forensics for live system artifacts.
- Linux/Mac Forensics.
- Investigating user activity.
- Password Cracking and bypassing techniques for operating systems.
- Case Study: The Stuxnet Attack Analysis.

Module 4: Network and Web Application Forensics

- Network Forensics fundamentals and data capture
- Analyzing Network Traffic using tools like Wireshark and TCPDump.
- Event Correlation and investigating Indicators of Compromise
- Web Application Forensics.
- Investigating Wireless and Router Forensics for breach analysis.
- Case Study: Investigating a DDoS Botnet Attack.

Module 5: Malware, Email, and Dark Web Forensics

- Malware Forensics.
- Investigating Email Crimes and message headers.
- Dark Web Forensics.
- Analyzing Ransomware infection markers and communication channels.
- Understanding and analyzing Fileless Malware techniques.
- Case Study: The WannaCry Global Outbreak.

Module 6: Mobile, IoT, and Cloud Forensics

- Mobile Device Forensics.
- Analyzing app data, location services, and call logs from mobile devices.
- Cloud Forensics.

- Investigating IoT Devices and embedded systems.
- Addressing legal and privacy challenges in Cross-Border Forensics.
- Case Study: Insider Data Leak via Personal Device.

Module 7: Database and Advanced Forensics

- Database Forensics.
- Investigating Virtual Machine disk images and snapshots.
- Advanced techniques in Timeline Analysis and data reconstruction.
- Forensic analysis of Encryption and disk volume protection.
- Report generation and Expert Witness Testimony best practices.
- Case Study: Financial Fraud in an SQL Database.

Module 8: Incident Response and Threat Hunting

- Integrating Digital Forensics with Incident Response.
- Threat Hunting using forensic artifacts and indicators.
- Implementing Forensic Readiness and documentation for business continuity.
- Utilizing Security Information and Event Management for log analysis.
- Simulating an end-to-end Cyber Incident Lifecycle response.
- Case Study: Incident Response Simulation.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com