CyberHunt

DIGITAL FORENSICS / INCIDENT INVESTIGATION

Computer Hacking Forensic Investigator

Master digital forensics and cybercrime investigation — from evidence acquisition and disk analysis to malware forensics and court-ready reporting. Designed for security professionals pursuing forensic investigation roles.

- Digital Evidence Acquisition
- Disk & Memory Forensics
- Malware & Network Analysis
- Forensic Reporting & Chain of Custody

5000+	95%	100+	24/7
Students Trained	Success Rate	Hiring Partners	Support

CyberHunt

Program Highlights

- 40-Hour Instructor-Led Training
- EC-Council Authorized Partner
- Practical Training on Latest Tools
- Telegram Group for Exam Support
- Learn from CEI Certified Trainers
- 98% Exam Pass Rate
- Post Training Support till Exam
- Access to Recorded Sessions
- Career Guidance & Mentorship

https://cyberhuntit.com/

CyberHunt

ABOUT COURSE

CHFI – Computer Hacking Forensic Investigator

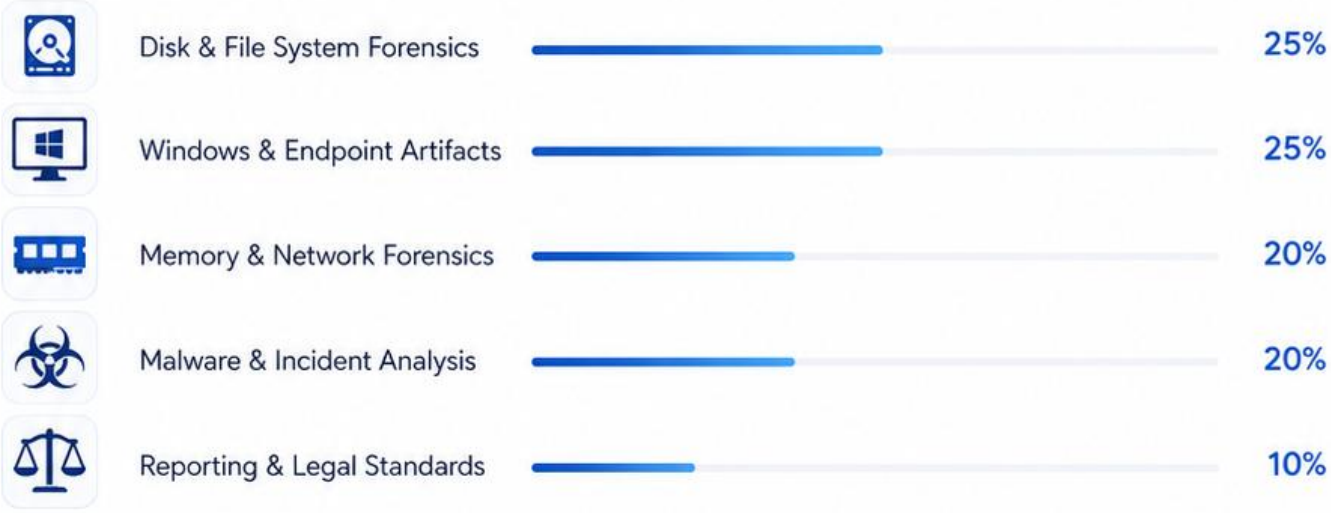
The CHFI – Computer Hacking Forensic Investigator program is a comprehensive digital forensics training focused on identifying, preserving, analyzing, and presenting digital evidence in cybercrime investigations.

This course prepares candidates to conduct forensic investigations on compromised systems, acquire and preserve digital evidence, perform disk and memory analysis, and investigate email and network-based attacks.

You will learn how to analyze malware artifacts, maintain proper chain of custody, and prepare legally acceptable forensic reports using investigation methodologies used by enterprise security teams, law enforcement, and incident response units.

This program bridges the gap between SOC operations and professional-grade digital forensics and incident investigation roles.

Forensic Skill Coverage



CyberHunt

Target Audience

- Security Analysts
- Ethical Hackers
- System Administrators
- Network Administrators
- Network and Security Engineers
- Cyber Security Managers
- Information Security Auditors
- Security Professionals

Pre-Requisites

- Basic understanding of network essentials and core concepts, including server and network components.

CyberHunt

Course Curriculum

Comprehensive digital forensics training covering evidence acquisition, analysis, and court-ready reporting

01 Digital Forensics Fundamentals

- Introduction to Digital Forensics
- Types of Cybercrimes
- Forensic Investigation Process
- Evidence Identification & Classification
- Forensic Readiness
- Legal & Compliance Considerations
- Chain of Custody Procedures

Practical: Understanding evidence handling workflow.

02 Forensic Lab Setup & Evidence Acquisition

- Forensic Workstation Setup
- Write Blockers & Forensic Imaging
- Bit-by-Bit Disk Imaging
- Hashing (MD5, SHA) & Integrity Verification
- Live vs Dead Acquisition
- Evidence Preservation Techniques

Practical: Create and verify forensic disk image.

03 Disk & File System Forensics

- File System Basics (NTFS, FAT, EXT)
- File Carving Techniques
- Deleted File Recovery
- Master File Table (MFT) Analysis
- Timestamp Analysis
- Hidden Data & Steganography
- USB Artifact Analysis

Practical: Recover deleted files and analyze file metadata.

04 Windows Forensics & Artifact Analysis

- Windows Registry Analysis
- Event Log Investigation
- User Activity Analysis
- Prefetch Analysis
- Browser History Investigation
- Startup & Persistence Artifacts
- Logon & Authentication Artifacts

Practical: Investigate compromised Windows machine artifacts.

05 Linux & Mac Forensics

- Linux Log Analysis
- User Activity Tracking
- Bash History Analysis
- System Logs Investigation
- MacOS Artifacts Overview

Practical: Investigate Linux-based attack case.

06 Memory Forensics

- Importance of Memory Analysis
- RAM Acquisition
- Volatile Data Analysis
- Process Enumeration
- Detecting Malware in Memory
- Rootkit Detection
- Credential Extraction Indicators

Practical: Analyze memory dump for suspicious processes.

07 Network Forensics

- Network Traffic Analysis
- Packet Capture Analysis
- Detecting Data Exfiltration
- DNS & HTTP Traffic Investigation
- Identifying C2 Communication
- Firewall & Proxy Log Analysis

Practical: Investigate network breach using packet capture file.

08 Email & Web Forensics

- Email Header Analysis
- Phishing Investigation
- Email Artifact Extraction
- Web Browser Artifacts
- Download & Upload Activity Analysis

Practical: Investigate phishing email case study.

09 Malware Forensics & Incident Investigation

- Malware Behavior Basics
- Static vs Dynamic Analysis
- Persistence Mechanisms
- Attack Timeline Reconstruction
- Root Cause Analysis

Practical: Analyze infected system artifacts and reconstruct attack timeline.

10 Mobile & Cloud Forensics (Overview Level)

- Mobile Device Evidence Handling
- Android & iOS Forensic Basics
- Cloud Log Investigation
- SaaS Forensics Overview

Practical: Case study-based cloud investigation scenario.

11 Forensic Reporting & Court Presentation

- Writing Forensic Reports
- Evidence Documentation
- Presenting Technical Findings to Non-Technical Audience
- Legal Admissibility Standards
- Expert Witness Basics

Practical: Prepare complete forensic investigation report.

CyberHunt

TRAINING ENQUIRIES

Have questions or need more information about our training programs? We're here to help!

For Training
+91 99599 06195
+91 93156 97737

Email
trainings@cyberhuntit.com

Website
www.cyberhuntit.com

Empowering Your Future
Industry-relevant training designed to upskill and empower you.

Follow us on