The Credential That Sets the Global Benchmark for Job-Ready Forensic Skills with the Latest Advanced Strategies.

C|HFI Computer Hacking Forensic INVESTIGATOR

EC-Council Building A Culture Of Security

C|HFI Program Overview

EC-Council's **C|HFI** program prepares cybersecurity professionals with the knowledge and skills to perform effective digital forensics investigations and bring their organization into a state of forensic readiness. This includes establishing the forensics process, lab, evidence handling procedures, as well as the investigation procedures required to validate/triage incidents and point the incident response teams in the right direction. Forensic readiness could be the difference between a minor incident and a major cyber-attack that brings a company to its knees.

C|HFI Course Modules:

- Computer Forensics in Today's World
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems
- Data Acquisition and Duplication
- Defeating Anti-forensics Techniques
- Windows Forensics
- Linux and Mac Forensics
- Network Forensics
- Malware Forensics
- Investigating Web Attacks
- Dark Web Forensics
- Cloud Forensics
- Email and Social Media Forensics
- Mobile Forensics
- IoT Forensics

Key Features and Critical Components

- 2100+ pages of the comprehensive student manual
- 1550+ pages of lab manual
- 600+ digital forensics tools
- 68 hands-on labs
- 70+ GB of crafted evidence files for investigation purposes
- Approved and Accredited by US Department of Defense (DoD) 8570/8140 and ANAB (ANSI) ISO/IEC 17024
- Understand regulatory compliance standards such as ISO 27001, PCI DSS, SOX, HIPPA, etc.
- EC-Council C|HFI is mapped to 30+ job roles.

Exam Title: Computer Hacking Forensic Investigator

Exam Code: 312-49
Number of Questions: 150
Duration: 4 hours

Availability: ECC EXAM Portal
Training: 5 Days

What Will You Learn from the C|HFI:

1. **Master a methodological forensics framework:**
   - Documenting the Crime Scene
   - Search and Seizure
   - Evidence Preservation
   - Data Acquisition
   - Data Examination
   - Reporting
3. Learn diverse types of digital forensic investigation and investigation through Python Scripting.

And more…

2. **Gain in-depth skills in**
   - Social Media Forensics
   - Mobile Forensics Analysis
   - Wireless Network Forensics
   - RAM forensics and Tor forensics
   - Electron Application and Web Browser Forensics
   - Malware Forensics Process and Malware Analysis
   - Forensic Methodologies for Cloud Infrastructure (AWS, Azure, and GCP)
   - Dark Web and IoT Forensics