Computer Hacking Forensic Investigator (C|HFI) Training Course

The Computer Hacking Forensic Investigator (C|HFI) course equips you with the skills to detect hacking attacks, gather crucial evidence, and conduct thorough investigations to combat cybercrime.

SEC-204

Course Outcomes

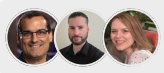
Professional, practical, & hands-on live instructor-led training

Further your skills and graduate as a certified professional, with the skills, experience, and job-search know how to get your career started.

Start Today

Potential Career Tracks

Digital Forensics Analyst | Computer Forensic Investigator | Cybersecurity Specialist | Information Security Analyst | Incident Responder | Network Security Engineer



Taught by Industry Veterans & World Class Instructors

Introduction to Computer Hacking Forensic Investigator (C|HFI)

Course Overview

Intellectual Point's Computer Hacking Forensic Investigator (C|HFI) Training Course equips you with the knowledge and skills needed to identify, track, and prosecute cybercriminals. This comprehensive program covers the essentials of digital forensics, giving you the tools and methodologies to conduct investigations across various environments and platforms. By integrating theory with practical training, the course prepares you to use cutting-edge technologies and processes to investigate cybercrimes efficiently.

Throughout the training, you will explore advanced topics such as computer crimes, digital evidence collection, forensics tools application, and report writing. The course includes hands-on experience in conducting network intrusion investigations, uncovering hidden data, and applying legal practices in evidence handling. By the end of the program, you'll be capable of implementing and managing enterprise-wide security and forensic strategies confidently.

Obtainable Skills

Digital Evidence Collection | Forensic Investigation Techniques | Data Recovery | Computer Network Forensics | Email Forensics | Cybercrime Incident Response | Malware Analysis | Legal Evidence Handling | Reporting and Documentation

Course Insights

Audience Profile

The Computer Hacking Forensic Investigator (C|HFI) course is targeted at professionals who are passionate about cybersecurity and eager to delve deeper into the realm of digital forensics. This course is ideal for IT professionals, law enforcement officers, legal professionals, system administrators, and security officers with a basic understanding of networks and security protocols. It is especially beneficial for those who wish to enhance their skills in identifying, responding to, and investigating cyber incidents. The program suits individuals interested in pursuing careers in digital forensic investigations or aiming to expand their cybersecurity expertise.

Course Outcomes

By the end of this course, participants will:

1. Gain expertise in conducting investigations of cyber incidents using advanced forensic tools.
2. Master the process of collecting, managing, and analyzing digital evidence.
3. Develop the ability to identify the footprints of hackers across various digital platforms.
4. Craft detailed investigation reports that stand up to legal scrutiny and aid in prosecution.
5. Be fully prepared for the C|HFI Certification exam, bolstering your credentials in the digital forensics.

Module by Module Learning *Outline*

6 Modules

Module 1: Introduction to Digital Forensics

Learning Objectives:

- Understand the fundamental principles of digital forensics.
- Recognize the role of a forensic investigator in the cybersecurity domain.

Topics Covered

Overview of Digital Forensics:

- Definition and importance of digital forensics.
- Key principles and objectives in forensic investigations.

Forensic Investigation Process:

- Steps in conducting a digital forensic investigation.
- Importance of maintaining integrity and chain of custody.

Module 2: Identifying and Collecting Digital Evidence

Learning Objectives:

- Learn how to identify and collect digital evidence from various sources.
- Understand the importance of proper evidence handling procedures.

Topics Covered

Sources of Digital Evidence:

- Types of digital evidence and their sources.
- Identifying potential evidence in cybercrime scenarios.

Evidence Handling and Preservation:

- Chain of custody and its significance.
- Techniques for preserving data integrity during collection.

Module 3: Forensic Investigation Techniques and Tools

Learning Objectives:

- Explore key forensic investigation techniques.
- Gain proficiency in using essential forensic tools.

Topics Covered

Forensic Techniques:

- Common investigation techniques for digital forensics.
- Techniques for extracting and analyzing data.

Application of Forensic Tools:

- Overview of popular forensic tools and software.
- Practical exercises in tool application for evidence analysis.

Module 4: Network and Email Forensics

Learning Objectives:

- Understand network forensics and its applications.
- Master techniques for conducting email forensic investigations.

Topics Covered

Network Forensics:

- Principles and methodologies in network forensics..
- Identifying and analyzing network-related evidence.

Email Forensics:

- Techniques for examining email headers and body.
- Identifying spoofed or phishing emails.

Module 5: Cybercrime and Incident Response

Learning Objectives:

- Acquire skills in responding to cybercrime incidents.
- Develop strategies for investigating cybercrimes.

Topics Covered

Introduction to Cybercrime:

- Types of cybercrimes and their impact.
- Methods used by cybercriminals and hacker footprints.

Incident Response Strategies:

- Steps in an effective incident response plan.
- Role of digital forensics in cyber incident management.

Module 6: Legal Aspects and Reporting

Learning Objectives:

- Gain insights into the legal aspects of digital forensics.
- Cultivate the ability to prepare professional investigation reports.

Topics Covered

Legal Considerations:

- Understanding the legal framework governing digital evidence.
- Regulations and compliance in digital forensics.

Reporting and Documentation:

- Crafting detailed investigation reports for legal proceedings.
- Best practices for documenting forensic findings and processes.