Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

# CHFI - Computer Hacking Forensics Investigator

## Course Description

SecureNinja's CHFI v11 (5) five-day training and certification boot camp in Washington, DC Metro, and San Diego, CA will provide participants with a detailed methodological approach to computer forensics and evidence analysis. CHFI is a comprehensive course covering all possible forensic investigation scenarios that enable students to acquire necessary hands-on experience on various forensic investigation techniques, and CHFI provides candidates with standard forensic tools necessary to successfully carry out a computer forensic investigation leading to the prosecution of proprietors.

Digital technologies are changing the face of business. As organizations rapidly embracing digital technologies such as cloud, mobile, big data and IoT, the context of digital forensics is more relevant than before. The growing number of cyber crimes has changed the role of forensics from DNA to Digital.

Over the last many years, EC-Council’s CHFI certification has gained massive traction and recognition among Fortune 500 enterprises globally. It has immensely benefited professionals from law enforcement, criminal investigation, defense, and security field. CHFI v11, the latest version of the program has been designed for professionals handling digital evidence while investigating cybercrimes. It is developed by an experienced panel of subject matter experts and industry specialists, and also has set global standards for computer forensics best practices. In addition, it aims at elevating the knowledge, understanding, and skill levels of cybersecurity and forensics practitioners.

*”Computer forensics graduates have been in high demand for jobs with law enforcement and that demand is growing. Starting salaries in the field can range as high as $85,000 to $120,000.”*

### Why CHFI v11

- The CHFI v11 program has been redesigned and updated after thorough investigation including current market requirements, job tasks analysis, and recent industry focus on forensic skills
- It is designed and developed by experienced subject matter experts and digital forensics practitioners
- CHFI is a complete vendor-neutral course covering all major forensics investigations technologies and solutions
- CHFI has detailed labs for a hands-on learning experience. On average, approximately 50% of training time is dedicated to labs
- It covers all the relevant knowledge-bases and skills to meets with regulatory compliance standards such as ISO 27001, PCI DSS, SOX, HIPPA, etc.

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- The student kit contains a large number of white papers for additional reading
- The program presents a repeatable forensics investigation methodology required from a versatile digital forensic professional which increases employability
- The student kit contains several forensics investigation templates for evidence collection, chain-of-custody, final investigation reports, etc.
- The program comes with cloud-based virtual labs enabling students to practice various investigation techniques in a real-time and simulated environment

## Topics Covered

- Computer Forensics in Today's World
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems
- Data Acquisition and Duplication
- Defeating Anti-forensics Techniques
- Operating System Forensics (Windows, Mac, Linux)
- Network Forensics
- Investigating Web Attacks
- Database Forensics
- Cloud Forensics
- Malware Forensics
- Investigating Email Crimes
- Mobile Forensics
- Forensics Report Writing and Presentation

## What’s New in CHFI v11?

The latest version of the **Computer Hacking Forensic Investigator (CHFI) v11** introduces cutting-edge advancements to keep up with the evolving field of digital forensics. Here’s what’s new:

- Expanded Module Coverage – New topics such as Dark Web Forensics and IoT Forensics provide deeper insights into emerging cyber threats.
- Latest Forensic Tools – Hands-on training with the newest forensic tools, including Splunk, DNSQuerySniffer, and advanced malware analysis techniques.
- Enhanced Investigation Techniques – Learn to defeat anti-forensic methods and conduct comprehensive malware forensics for more effective cybercrime investigations.
- Real-World Case Studies – Apply new methodologies in practical scenarios, ensuring readiness for real-life forensic challenges.
- Updated Industry-Relevant Content – Stay ahead with knowledge on the latest cyber threats, forensic methodologies, and legal compliance updates.

## Who Would Benefit

- Police and other law enforcement personnel
- Defense and Military personnel
- e-Business Security professionals
- Systems administrators

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- Legal professionals
- Banking
- Insurance and other professionals
- Government agencies
- IT managers

## Prerequisites

- IT/forensics professionals with basic knowledge of IT/cybersecurity, computer forensics, and incident response
- Prior completion of CEH training would be an advantage

## Exam Details

CHFI training at SecureNinja will properly prepare you for the following exam:

- CHFI 312-49
- Number of Questions: 150
- Passing score: 70%
- Test Duration: 4 hours
- Test Format: MCQ
- Test Delivery: ECC exam portal

This exam will be conducted on the last day of training.

## Course Length

- 5 Days
- 40 hours

## Career Track & Roles

- Computer Forensics Investigator
- Licensed Penetration Tester
- Systems Engineer
- Systems Architect
- Network Security Specialist

## Follow On Courses

- CISSP