OVERVIEW

The Computer Hacking Forensic Investigator (CHFI) course delivers the security discipline of digital forensics from a vendor-neutral perspective. CHFI is a comprehensive course covering major forensic investigation scenarios and enabling students to acquire necessary hands-on experience with various forensic investigation techniques and standard forensic tools necessary to successfully carry out a computer forensic investigation leading to the prosecution of perpetrators.

The CHFI certification gives participants (Law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of the network infrastructure.) the necessary skills to perform an effective digital forensics investigation.

CHFI presents a methodological approach to computer forensics including searching and seizing, chain-of-custody, acquisition, preservation, analysis and reporting of digital evidence.

EC COUNCIL COMPUTER HACKING FORENSIC INVESTIGATOR (CHFI)

COURSE OBJECTIVES

- The course was designed and developed by experienced SMEs and digital forensics practitioners
- A complete vendor neutral course covering all major forensics investigations technologies and solutions
- Detailed labs for hands-on learning experience; 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.
- The program presents a repeatable forensics investigation methodology required from a versatile digital forensic professional which increases your employability.

Students going through CHFI training will learn:

- Establish threat intelligence and key learning points to support pro-active profiling and scenario modeling
- Perform anti-forensic methods detection
- Perform post-intrusion analysis of electronic and digital media to determine the who, where, what, when, and how the intrusion occurred
- Extract and analyze of logs from various devices like proxy, firewall, IPS, IDS, Desktop, laptop, servers, SIM tool, router, firewall, switches AD server, DHCP logs, Access Control Logs & conclude as part of investigation process.
- Identify & check the possible source / incident origin.
- Recover deleted files and partitions in Windows, Mac OS X, and Linux
- Conduct reverse engineering for known and suspected malware files
- Collect data using forensic technology methods in accordance with evidence handling procedures, including collection of hard copy and electronic documents

TARGET STUDENT

The CHFI program is designed for all IT professionals involved with information system security, computer forensics, and incident response.

Target Audience

- Police and other law enforcement personnel
- Defense and Military personnel
- e-Business Security professionals
- Systems administrators
- Legal professionals
- Banking, Insurance and other professionals
- Government agencies
- IT managers.

COURSE CONTENT

Lesson 1: Computer Forensics in Today's World

Lesson 2: Computer Forensics Investigation Process

Lesson 3: Understanding Hard Disks and File Systems

Lesson 4: Operating System Forensics

Lesson 5: Defeating Anti- forensics Techniques

Lesson 6: Data Acquisition and Duplication

Lesson 7: Network Forensics

Lesson 8: Investigating Web Attacks

Lesson 9: Database Forensics

Lesson 10: Cloud Forensics

Lesson 11: Malware Forensics

Lesson 12: Investigating Email Crimes

Lesson 13: Mobile Forensics

Lesson 14: Investigative Reports