TEL: +971 4 246 2843
Office 3832, 38th Fl.
The One Tower
Sheikh Zayed Road
Barsha Heights
Dubai - UAE

Computer Hacking Forensic Investigator CHFI

Computer Hacking Forensic Investigator (CHFI) v10 is a complete training program designed to assist IT professionals and Law Enforcement personnel in understanding the security aspects and forensic investigation related to various informatics and digital evidence. The CHFI course focuses on the development of skills related to acquisition, analysis, investigation, and security incident response. It also covers topics related to network security, cloud forensics, malware, computer forensics, and digital evidence. It provides a comprehensive overview of the different types of evidence that might be obtained from digital devices and the various methods used to investigate such evidence. The CHFI course covers topics such as basic computer forensics, data acquisition and analysis, e-mail investigations, computer forensics investigation tools and procedures, website investigations, and mobile device forensics. It is an essential part of any IT security and forensics program.

Duration:

- 5 Days (40 hours)

Course Prerequisites

The prerequisites for CHFI V10 training are:

- Proficiency in computer and networking fundamentals.
- Experience in installing, configuring, and troubleshooting computers and networks.
- Experience with analyzing system and/or application logs.
- Experience or knowledge of basic incident response techniques.
- Familiarity with forensic tools such as EnCase, FTK, Helix, and Autopsy.
- Basic understanding of the incident response process.

TEL: +971 4 246 2843
Office 3832, 38th Fl.
The One Tower
Sheikh Zayed Road
Barsha Heights
Dubai - UAE

Target Audience:

- Information security professionals
- Security officers
- System administrators
- Legal professionals, banking
- Insurance and government personnel
- Defense and military personnel
- IT Managers
- Network Professional

Learning Objectives:

- Describe and explain the core forensic investigation processes and procedures.
- Explain computer crime and the applicable laws associated with it.
- Describe digital evidence types and explain how each can be used in an investigation.
- Explain various forensic techniques used to acquire evidence from various digital media.
- Describe different types of networks and explain the artifacts that can be forensically collected from it.
- Discuss the challenges related to digital investigations and explain various solutions to solve them.
- Explain the fundamentals of computer systems, networks, and storage media.
- Describe different mobile and wireless devices and the artifacts that can be forensically collected from them.
- Explain cloud computing and its challenges in the forensic investigation.
- Identify and explain the legal, ethical and professional practices in computer forensics investigations.

TEL: +971 4 246 2843
Office 3832, 38th Fl.
The One Tower
Sheikh Zayed Road
Barsha Heights
Dubai - UAE

Learning Modules:

- Module 1: Computer Forensics in Today's World
- Module 2: Computer Forensics Investigation Process
- Module 3: Understanding Hard Disks and File Systems
- Module 4: Data Acquisition and Duplication
- Module 5: Defeating Anti-Forensics Techniques
- Module 6: Windows Forensic
- Module 7: Linux and Mac Forensics
- Module 8: Network Forensics
- Module 9: Investigating Web Attacks
- Module 10: Dark Web Forensics
- Module 11: Database Forensics
- Module 12: Cloud Forensics
- Module 13: Investigating Email
- Module 14: Malware Forensics
- Module 14: Malware Forensics
- Module 16: IoT Forensics