CHFI: Computer Hacking Forensic Investigator

Course Code: CHFI
Duration: 5 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

The ***CHFI: Computer Hacking Forensic Investigator*** certification includes all the essentials of digital forensics analysis and evaluation required for today's digital world. From identifying the footprints of a breach to collecting evidence for a prosecution, CHFI v10 walks students through every step of the process with experiential learning. This course has been tested and approved by veterans and top practitioners of the cyber forensics industry.

CHFI v10 is engineered by industry practitioners for both professionals and aspiring professionals alike from careers including forensic analysts, cybercrime investigators, cyber defense forensic analysts, incident responders, information technology auditors, malware analysts, security consultants, and chief security officers

SKILLS COVERED

After taking this course, you should be able to:

- Includes critical modules in Dark Web Forensics and IoT Forensics
- Extensive coverage of Malware Forensics (latest malware samples such as Emotet and EternalBlue)
- Significant coverage of forensic methodologies for public cloud infrastructure, including Amazon AWS and Microsoft Azure
- More than 50GB of crafted evidence files for investigation purposes
- More than 50% of new and advanced forensic labs
- Latest forensic tools including Splunk, DNSQuerySniffer, etc.
- In-depth focus on Volatile and Non-volatile data acquisition and examination process (RAM Forensics, Tor Forensics, etc.)
- New techniques such as Defeating Anti-forensic technique, Windows ShellBags including analyzing LNK files and Jump Lists
- Massive updates on all modules in CHFI
- Accepted and trusted by cybersecurity practitioners across the Fortune 500 globally

WHO SHOULD ATTEND?

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

- Police and other law enforcement personnel
- Defense and Security personnel
- e-Business Security professionals
- Legal professionals
- Banking, Insurance and other professionals
- Government agencies
- IT managers
- Digital forensics Service providers

PREREQUISITES

There are no prerequisites required to attend this course

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 Forensics

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 Crimes

Module 14: Malware Forensics

Module 15: Mobile Forensics

Module 16: IoT Forensics

END OF PAGE