SULFMAN TRAININGS

COURSE:

COMPUTER HACKING FORENSIC INVESTIGATOR (CHFI)

COMPUTER HACKING FORENSIC INVESTIGATOR (CHFI)

OVERVIEW

CHFI v10 provides essential digital forensics skills for today's digital world, guiding participants from identifying breach footprints to evidence collection. Tailored for professionals and aspiring individuals, it's endorsed by industry veterans. With a focus on decoding digital footprints, the course equips students to actively respond to cyber breaches. Given the global growth in the forensics market, projected at USD 9.7 billion by 2023, CHFI v10 meets the increasing demand in the face of rising cyber threats.

MODULES

- **Module 1:** Computers 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

COURSE OUTCOMES

- Includes critical modules in Dark Web Forensics and IoT Forensics
- More than 50% of new and advanced forensic labs
- Latest forensic tools including Splunk, DNSQuerySniffer, etc.
- Significant coverage of forensic methodologies for public cloud infrastructure, including Amazon AWS and Microsoft Azure
- In-depth focus on Volatile and Non-volatile data acquisition and examination process (RAM Forensics, Tor Forensics, etc.)
- More than 50GB of crafted evidence files for investigation purposes