MedTech Programs

MedTech Mediterranean Institute of Technology

EC-COUNCIL | ACADEMIA PARTNER

Computer Hacking Forensic Invistigator

I. Program overview & Benefit:

The EC-Council's CHFI v10 (Computer Hacking Forensic Investigator version 10) is a cutting-edge program tailored for individuals keen on leading the digital forensics movement. Amid the rapid digital transformation and the escalating risk of cyberattacks, this program emerges as a critical solution for mastering digital forensics. CHFI v10 meticulously guides participants through the entire digital forensics process, from uncovering digital footprints left by cyber breaches to legally countering the perpetrators.

Structured with a blend of theory and practical sessions, the program is ideal for professionals aiming to excel as forensic analysts, cybercrime investigators, incident responders, IT auditors, among others. It boasts of an ANSI 17024 accreditation, aligning with the NICE 2.0 framework and recognized by the DoD under Directive 8570, ensuring its relevance and applicability in the real world.

Participants will delve into specialized modules like Dark Web and IoT Forensics, engage with over 50GB of crafted evidence files for hands-on investigation, and learn the latest in Malware Forensics, including handling contemporary malware threats like Emotet and EternalBlue. Furthermore, the curriculum covers forensic methodologies for cloud infrastructure, including Amazon AWS and Microsoft Azure, preparing students for challenges in today's cloud-centric operational environments.

CHFI v10 is not just a program but a gateway to becoming an indispensable part of the cybersecurity landscape, endorsed by top practitioners and trusted across the Fortune 500 companies globally.

II. Intended Participants:

The intended participants for the EC-Council's CHFI v10 (Computer Hacking Forensic Investigator version 10) program are professionals and aspiring professionals in various cybersecurity and digital forensics roles. This includes:

- Forensic analysts
- Cybercrime investigators
- Cyber defense analysts
- Incident responders
- Information technology auditors
- Malware analysts
- Security consultants
- Chief security officers

The program is engineered for individuals looking to deepen their expertise in digital forensics, aiming to address the growing need for skilled professionals capable of identifying, responding to, and investigating cyber breaches and cybercrimes.

III. Program Curriculum

The CHFI v10 program from EC-Council offers an in-depth journey into the world of digital forensics, tailored to the contemporary digital landscape. This comprehensive curriculum is designed to equip participants with the essential skills and knowledge required for excellence in digital forensics. Participants will engage in practical and theoretical learning, covering the critical aspects of digital forensics analysis and evaluation. From identifying digital footprints to collecting evidence for legal prosecution, the program walks students through every step of the forensic process with experiential learning. Crafted by industry veterans, this program is ideal for professionals aiming to navigate the complexities of cyber breaches and cybercrimes effectively.

IV. Core program curriculum:

The CHFI v10 curriculum includes a comprehensive set of 16 refreshed modules, designed to equip participants with advanced skills and knowledge in digital forensics. Here's a brief overview of the modules:

1. **Computer Forensics in Today's World:** An introduction to the field of digital forensics, highlighting its importance in the modern digital age.
2. **Computer Forensics Investigation Process:** Detailed processes involved in conducting forensic investigations from start to finish.
3. **Understanding Hard Disks and File Systems:** Fundamental knowledge of how data is stored and managed on digital devices.
4. **Data Acquisition and Duplication:** Techniques for securely collecting and duplicating data for analysis without tampering.
5. **Defeating Anti-Forensics Techniques:** Strategies to counteract methods used to obstruct forensic investigations.
6. **Windows Forensics:** Specialized techniques for investigating Windows operating systems.
7. **Linux and Mac Forensics:** Approaches for forensic investigations on Linux and Mac OS systems.
8. **Network Forensics:** Methods for analyzing network-related activities and uncovering digital evidence.
9. **Investigating Web Attacks:** Techniques for investigating attacks targeted at web applications and services.
10. **Dark Web Forensics:** Understanding and investigating activities on the dark web.
11. **Database Forensics:** Approaches for examining databases to extract and analyze evidence.
11. **Cloud Forensics:** Techniques for forensic investigations in cloud computing environments.
12. **Investigating Email Crimes:** Methods for analyzing emails to uncover evidence of crimes.
14. **Malware Forensics:** Techniques for analyzing and investigating malware.
15. **Mobile Forensics:** Strategies for extracting and analyzing data from mobile devices.
16. **IoT Forensics:** Approaches to investigate Internet of Things devices and gather digital evidence.

This curriculum is crafted to provide a thorough understanding of digital forensics, encompassing a wide range of topics essential for forensic analysts, cybercrime investigators, incident responders, and other cybersecurity professionals.

V. Schedule:

The certificate program entails a commitment of 40 hours, with sessions lasting 4 hours each week. Candidates have the flexibility to select their preferred schedule from the following options:

Evening classes
From 6:30 PM to 8:30 PM
Monday and Tuesday or Thursday and Friday

Weekend classes
From 10:00 AM to 12:00 PM:
Saturday and Sunday

VI. Enrollment requirements:

Enrollment requirements are straightforward: there are no specific prerequisites. However, participants are expected to have a basic understanding of networking, operating systems, and coding principles.

VII. The Benefits of the program:

- **Globally Recognized Certification:** ANSI 17024 accreditation and recognition by the DoD under Directive 8570.
- **Comprehensive Coverage:** Includes critical areas like Dark Web and IoT Forensics, and extensive labs in Malware Forensics.
- **Up-to-Date Content:** Massive updates across all modules to cover the latest forensic methodologies, especially for public cloud infrastructures like Amazon AWS and Microsoft Azure.
- **Practical Learning:** More than 50GB of evidence files for investigation purposes and exposure to the latest forensic tools including Splunk and DNSQuerySniffer.
- **Advanced Techniques:** In-depth focus on volatile and non-volatile data acquisition and examination, along with new techniques for defeating anti-forensic measures.
- **Industry Acceptance:** Trusted by cybersecurity practitioners across Fortune 500 companies globally.

These benefits collectively make the CHFI v10 program a valuable and comprehensive learning path for individuals aiming to excel in the field of digital forensics, offering the knowledge, skills, and credentials needed to advance in their careers.

Contacts :
cybersecuritycontact@medtech.tn
Les jardins du LAC 2, 1053, Tunis - Tunisie