EC-Council Computer Hacking Forensic Investigator (CHFI) + Exam voucher

Varighed: 5 Days **Kursus Kode: CHFI** **Version: 11.0**

Beskrivelse:

EC-Council's C|HFI program prepares cybersecurity professionals with the knowledge and skills to perform effective digital forensics investigations and bring their organization into a state of forensic readiness. Establishing the forensics process, lab, evidence handling procedures, and investigation techniques are required to validate and triage incidents and guide incident response teams in the right direction. Forensic readiness is crucial as it can differentiate between a minor incident and a major cyber-attack that impacts an organization significantly. This hands-on digital forensics program immerses students in over 68 forensic labs, working on crafted evidence files using tools used by digital forensics professionals. Students go beyond traditional hardware and memory forensics, covering cloud forensics, mobile and IoT forensics, as well as investigations of web application attacks and malware forensics. The C|HFI presents a methodological approach to computer forensics, including searching and seizure, chain of custody, acquisition, preservation, analysis, and reporting of digital evidence. Students learn various forensic investigation techniques and standard forensic tools. As they learn how to acquire and manage evidence across different operating environments, they also learn chain of custody and legal procedures required to preserve evidence and ensure admissibility in court, supporting the prosecution of cybercriminals and reducing organizational liability.
The program provides credible professional knowledge with globally recognized certification required for a successful digital forensics and DFIR career, thereby increasing employability.
Updated 12/5/2026

Målgruppe:

IT/forensics professionals with basic knowledge of IT/cybersecurity, computer forensics, incident response, and threat vectors.

Agenda:

- **What will you learn?**
- Computer forensics fundamentals, different types of cybercrimes and their investigation procedures, and regulations and standards that influence computer forensics investigation
- Various phases involved in the computer forensics investigation process
- Different types of disk drives and their characteristics, booting process and file systems in Windows, Linux, and Mac operating systems, file system examination tools, RAID and NAS/SAN storage systems, various encoding standards, and file format analysis
- Data acquisition fundamentals and methodology, eDiscovery, and preparation of image files for forensic examination
- Various anti-forensics techniques used by attackers, methods to detect them, related tools, and countermeasures
- Volatile and non-volatile data acquisition in Windows-based operating systems, Windows memory and registry analysis, electron application analysis, web browser forensics, examination of Windows files, ShellBags, LNK files, Jump Lists, and Windows event logs
- Volatile and non-volatile data acquisition and memory forensics in Linux and Mac operating systems
- Network forensics fundamentals, event correlation concepts, Indicators of Compromise (IOCs), identification from network logs, network traffic investigation techniques and tools, incident detection and examination, and wireless attack detection and investigation
- Malware forensics concepts, static and dynamic malware analysis, system and network behavior analysis, and ransomware analysis
- Web application forensics and challenges, web application threats and attacks, web application logs (IIS logs, Apache web server logs, etc.), and detection and investigation of web application attacks
- Tor browser working methodology and steps involved in Tor browser forensics
- Cloud computing concepts, cloud forensics, and challenges, fundamentals of AWS, Microsoft Azure, and Google Cloud and their investigation processes
- Components in email communication, steps in email crime investigation, and social media forensics
- Architectural layers and boot processes of Android and iOS devices, mobile forensics process, cellular networks, SIM file system, and logical and physical acquisition of Android and iOS devices
- Different types of IoT threats, security problems, vulnerabilities and attack surface areas, and IoT forensics process and challenges

Forudsætninger:

Attendees should meet the following prerequisites:

- Basic knowledge of IT/cybersecurity, computer forensics, incident response, and threat vectors.
- CEH - EC-Council Certified Ethical Hacker (C|EH) + Exam voucher

Test og certificering

Recommended as preparation for the following exams:

- 312-49 - CHFI Exam

Examination

Number of Questions: 150

Duration: 4 hours

Availability: ECC Exam Portal

Indhold:

Module 01 Computer Forensics in Today's World

Module 02 Computer Forensics Investigation Process

Module 03 Understanding Hard Disks and File Systems

Module 04 Data Acquisition and Duplication

Module 05 Defeating Anti-forensics Techniques

Module 06 Windows Forensics

Module 07 Linux and Mac Forensics

Module 08 Network Forensics

Module 09 Malware Forensics

Module 10 Investigating Web Attacks

Module 11 Dark Web Forensics

Module 12 Cloud Forensics

Module 13 Email and Social Media Forensics

Module 14 Mobile Forensics

Module 15 IoT Forensics

Flere Informationer:

For yderligere informationer eller booking af kursus, kontakt os på tlf.nr.: 44 88 18 00

training@globalknowledge.dk

www.globalknowledge.com/da-dk/

Global Knowledge, Stamholmen 110, 2650 Hvidovre