CHFI: Computer Hacking Forensic Investigator

EC-Council

Com certificação

- **Nível:** Avançado
- **Duração:** 40h

Sobre o curso

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/triage incidents and point the 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 brings a company to its knees.

This intense hands-on digital forensics program immerses students in over 68 forensic labs, working on crafted evidence files utilizing the tools of the world's top digital forensics professionals. Students will go beyond traditional hardware and memory forensics, covering current topics in cloud forensics, mobile and IoT, and investigating web application attacks and malware forensics. The C|HFI presents a methodological approach to computer forensics, including searching and seizing, 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 through various operating environments, students also learn the chain of custody and legal procedures required to preserve evidence and ensure it is admissible in court, enabling the eventual prosecution of cyber criminals and containing liability on the victim organization.

The program provides credible professional knowledge with globally recognized certification required for a successful digital forensics and DFIR career, thus increasing your employability.

Digital Forensics—The Need of the Hour Amidst Escalating Threats

As per Statista, In 2022, phishing topped cybercrimes reported to the US Internet Crime Complaint Center, affecting about 300k individuals, with nearly 59k personal data breaches reported.

In 2022, investment fraud led to the highest financial losses for individuals in the US, totaling over $3 billion. Business email compromise (BEC) followed with reported losses of around $2.7 billion, while victims of tech support fraud reported losses of $806 million.

Dark web statistics show that in 2020, cyber criminals added over 22 billion new records to the dark web.

The global average cost of a data breach in 2023 was $4.45 million, a 15% increase over three years (IBM).

According to the source, approximately 52 percent of respondents in the United States stated that their company had in place a dark web threat intelligence policy in 2022.

Over 90% of all crime is recognized as having a digital element, highlighting the movement of present-day policing towards having technology at its core.

Why is Digital Forensics crucial for Organizations and Professionals?

No cybersecurity team is complete without digital forensics. Digital forensics and investigations are critical to successfully handling a cyber incident when it occurs.

A breach can be brutal; investing in building an expert in-house forensics team with C|HFI training is a strategic move for enterprises looking to safeguard their stakeholder's interests as well as theirs. The C|HFI empowers the existing team by applying the latest investigation practices.

The C|HFI boosts investigational forensics skills and helps build forensic readiness in their organization

Demand for Digital Forensics Professionals:

Over 90% of all crime is recognized as having a digital element, highlighting the movement of present-day policing towards having technology at its core.
The U.S. Bureau of Labor Statistics projects that the employment of forensic science technicians is projected to grow 13% from 2022 to 2032, much faster than the average for all occupations.

CHFI Course Benefits

- Master a methodological forensics framework approach for performing digital forensics investigation;
- Build skills for investigating diverse types of digital forensic investigations;
- 70+ GB of crafted evidence files fo investigation purpose;
- Learn In-depth focus on volatile and non-volatile data acquisition and examination of Mac Operating Systems and also RAM Forensics, Tor Forensics, etc
- Become proficient in Malware Forensics process and Malware analysis, including the latest analysis: BlackCat (ALPHV)
- Learn Social Media Forensics and Wireless Network Forensics
- Learn Electron Application and Web Browser Forensics
- Gain In-depth skill in Mobile Forensics Analysis
- Learn a critical skill of performing Digital Forensics Investigation through Python Scripting
- Master a Unique skill set: C|HFI-The first Certification to offer Dark Web & IoT Forensics
- Become skilled in Forensic Methodologies for Cloud Infrastructure (AWS, Azure and GCP)
- Learn techniques such as Defeating Anti-forensic technique, Windows ShellBags, including analyzing LNK

files and Jump Lists
- Learn the latest digital forensics tools/platforms and framework
- 40% of training time on labs that simulate real-life networks and platforms
- The C|HFI is designed by SMEs and digital forensics practitioners worldwide after a rigorous job task analysis (JTA) of the job roles involved in the field of digital forensics, which also increases your employability

Download the brochure >

Destinatários

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

- 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

Condições

O exame EC-Council incluido no valor do curso deve ser obrigatoriamente realizado presencialmente, num dos centros de Exames GALILEU. Caso não tenha disponibilidade ou não pretenda realizar o exame de forma presencial e prefira uma solução remota acresce uma taxa de 89€ ao valor do curso.

Pré-requisitos

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

Metodologia

Presencial ou Live Training **About the CHFI Exam** The CHFI certification is awarded after successfully passing exam EC0 312-49. CHFI EC0 312-49 exams are available at ECC exam centers around the world.

- Number of Questions: 150
- Test Duration: 4 hours
- Test Format: Multiple Choice

Programa

- Computer Forensics in Today’s World
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems
- Data Acquisition and Duplication
- Defeating Anti-forensics Techniques
- Windows Forensics
- Linux and Mac Forensics
- Network Forensics
- Malware Forensics
- Investigating Web Attacks
- Dark Web Forensics
- Cloud Forensics
- Email and Social Media Forensics
- Mobile Forensics
- IoT Forensics