EC-Council Computer Hacking Forensic Investigator (CHFI) + Voucher d'examen

Durée: 5 Jours **Réf de cours: CHFI**

Résumé:

Computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud. CHFI investigators can draw on an array of methods for discovering data that resides in a computer system, or recovering deleted, encrypted, or damaged file information known as computer data recovery.

EC-Council's Certified Hacking Forensic Investigator (CHFI) is the only comprehensive ANSI accredited, lab-focused program in the market that gives organizations vendor-neutral training in digital forensics. CHFI provides its attendees with a firm grasp of digital forensics, presenting a detailed and methodological approach to digital forensics and evidence analysis that also pivots around Dark Web, IoT, and Cloud Forensics. The tools and techniques covered in this program will prepare the learner for conducting digital investigations using ground-breaking digital forensics technologies.
The program is designed for IT professionals involved with information system security, computer forensics, and incident response. It will help fortify the application knowledge in digital forensics for forensic analysts, cybercrime investigators, cyber defense forensic analysts, incident responders, information technology auditors, malware analysts, security consultants, and chief security officers.
The program equips candidates with the necessary skills to proactively investigate complex security threats, allowing them to investigate, record, and report cybercrimes to prevent future attacks.

Please note an exam voucher is included with this course
Mise à jour : 28.02.2023

Public visé:

The CHFI program is designed for all IT professionals involved with information system security, computer forensics, and incident response. Individuals in industries such as Banking, Defense and Law Enforcement.

Objectifs pédagogiques:

- **After completing this course you should be able to:**
- Perform electronic evidence collections
- Perform digital forensic acquisitions
- Conduct thorough examinations of computer hard disk drives and other electronic data storage media
- Utilise forensic tools and investigative methods to find electronic data, including Internet use history, word processing documents, images and other files
- Perform anti-forensics detection
- Apply advanced forensic tools and techniques for attack reconstruction

Pré-requis:

Attendees should meet the following prerequisites:

- IT/forensics professionals with basic knowledge on IT/cyber security, computer forensics, and incident response
- Prior completion of Certified Ethical Hacker (CEH) training would be an advantage
- CEH - EC-Council Certified Ethical Hacker (CEH) + Voucher d'examen

Test et certification

Recommended as preparation for the following exams:

- **ECO 312-49 - CHFI Exam**

Contenu:

Computer Forensics in Today's World

- Understand the Fundamentals of Computer Forensics
- Understand Cybercrimes and their Investigation Procedures
- Understand Digital Evidence
- Understand Forensic Readiness, Incident Response and the Role of SOC (Security Operations Center) in Computer Forensics
- Identify the Roles and Responsibilities of a Forensic Investigator
- Understand the Challenges Faced in Investigating Cybercrimes
- Understand Legal Compliance in Computer Forensics

Computer Forensics Investigation Process

- Understand the Forensic Investigation Process and its Importance
- Understand the Pre-investigation Phase
- Understand First Response
- Understand the Investigation Phase
- Understand the Post-investigation Phase

Understanding Hard Disks and File Systems

- Describe Different Types of Disk Drives and their Characteristics
- Explain the Logical Structure of a Disk
- Understand Booting Process of Windows, Linux and Mac Operating Systems
- Understand Various File Systems of Windows, Linux and Mac Operating Systems
- Examine File System Using Autopsy and The Sleuth Kit Tools
- Understand Storage Systems
- Understand Encoding Standards and Hex Editors
- Analyze Popular File Formats Using Hex Editor

Data Acquisition and Duplication

- Understand Data Acquisition Fundamentals
- Understand Data Acquisition Methodology
- Prepare an Image File for Examination

Defeating Anti-forensics Techniques

- Understand Anti-forensics Techniques
- Discuss Data Deletion and Recycle Bin Forensics
- Illustrate File Carving Techniques and Ways to Recover Evidence from Deleted Partitions
- Explore Password Cracking/Bypassing Techniques
- Detect Steganography, Hidden Data in File System Structures, Trail Obfuscation, and File Extension Mismatch
- Understand Techniques of Artifact Wiping,

Linux and Mac Forensics

- Understand Volatile and Non-volatile Data in Linux
- Analyze Filesystem Images Using The Sleuth Kit
- Demonstrate Memory Forensics Using Volatility ; PhotoRec
- Understand Mac Forensics

Network Forensics

- Understand Network Forensics
- Explain Logging Fundamentals and Network Forensic Readiness
- Summarize Event Correlation Concepts
- Identify Indicators of Compromise (IoCs) from Network Logs
- Investigate Network Traffic
- Perform Incident Detection and Examination with SIEM Tools
- Monitor and Detect Wireless Network Attacks

Investigating Web Attacks

- Understand Web Application Forensics
- Understand Internet Information Services (IIS) Logs
- Understand Apache Web Server Logs
- Understand the Functionality of Intrusion Detection System (IDS)
- Understand the Functionality of Web Application Firewall (WAF)
- Investigate Web Attacks on Windows-based Servers
- Detect and Investigate Various Attacks on Web Applications

Dark Web Forensics

- Understand the Dark Web
- Determine How to Identify the Traces of Tor Browser during Investigation
- Perform Tor Browser Forensics

Database Forensics

- Understand Database Forensics and its Importance
- Determine Data Storage and Database Evidence Repositories in MSSQL Server
- Collect Evidence Files on MSSQL Server
- Perform MSSQL Forensics
- Understand Internal Architecture of MySQL and Structure of Data Directory
- Understand Information Schema and List MySQL Utilities for Performing Forensic Analysis
- Perform MySQL Forensics on WordPress Web Application Database

Cloud Forensics

Investigating Email Crimes

- Understand Email Basics
- Understand Email Crime Investigation and its Steps
- U.S. Laws Against Email Crime

Malware Forensics

- Define Malware and Identify the Common Techniques Attackers Use to Spread Malware
- Understand Malware Forensics Fundamentals and Recognize Types of Malware Analysis
- Understand and Perform Static Analysis of Malware
- Analyze Suspicious Word and PDF Documents
- Understand Dynamic Malware Analysis Fundamentals and Approaches
- Analyze Malware Behavior on System Properties in Real-time
- Analyze Malware Behavior on Network in Real-time
- Describe Fileless Malware Attacks and How they Happen
- Perform Fileless Malware Analysis - Emotet

Mobile Forensics

- Understand the Importance of Mobile Device Forensics
- Illustrate Architectural Layers and Boot Processes of Android and iOS Devices
- Explain the Steps Involved in Mobile Forensics Process
- Investigate Cellular Network Data
- Understand SIM File System and its Data Acquisition Method
- Illustrate Phone Locks and Discuss Rooting of Android and Jailbreaking of iOS Devices
- Perform Logical Acquisition on Android and iOS Devices
- Perform Physical Acquisition on Android and iOS Devices
- Discuss Mobile Forensics Challenges and Prepare Investigation Report

IOT Forensics

- Understand IoT and IoT Security Problems
- Recognize Different Types of IoT Threats
- Understand IoT Forensics
- Perform Forensics on IoT Devices

Overwritten Data/Metadata Detection, and Encryption

- Detect Program Packers and Footprint Minimizing Techniques
- Understand Anti-forensics Countermeasures
- Anti-Forensics techniques

Windows Forensics

- Collect Volatile and Non-volatile Information
- Perform Windows Memory and Registry Analysis
- Examine the Cache, Cookie and History Recorded in Web Browsers
- Examine Windows Files and Metadata
- Understand ShellBags, LNK Files, and Jump Lists
- Understand Text-based Logs and Windows Event Logs

- Understand the Basic Cloud Computing Concepts
- Understand Cloud Forensics
- Understand the Fundamentals of Amazon Web Services (AWS)
- Determine How to Investigate Security Incidents in AWS
- Understand the Fundamentals of Microsoft Azure
- Determine How to Investigate Security Incidents in Azure
- Understand Forensic Methodologies for Containers and Microservices

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• Modalités d'évaluation : le participant est invité à s'auto-évaluer par rapport aux objectifs énoncés.
• Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

•Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
•Votre place sera confirmée à la réception d'un devis ou ""booking form"" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
•Attention, si vous utilisez votre Compte Personnel de Formation pour financer votre inscription, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés.