EC-Council - CHFI - Computer Hacking Forensic Investigator (EC-CHFI)

Code:	3401
Length:	5 days
URL:	View Online

EC-Council released the most advanced computer forensic investigation program in the world. This course covers major forensic investigation scenarios that enable you to acquire hands-on experience on various forensic investigation techniques and standard tools necessary to successfully carry-out a computer forensic investigation.

Battles between corporations, governments, and countries are no longer fought using physical force. Cyber war has begun and the consequences can be seen in everyday life. With the onset of sophisticated cyber attacks, the need for advanced cybersecurity and investigation training is critical. If you or your organization requires the knowledge or skills to identify, track, and prosecute cyber criminals, then this is the course for you. You will learn how to excel in digital evidence acquisition, handling, and forensically sound analysis. These skills will lead to successful prosecutions in various types of security incidents such as data breaches, corporate espionage, insider threats, and other intricate cases involving computer systems.

This course includes one exam voucher for CHFI.

Skills Gained

- The computer forensic investigation process and the various legal issues involved
- Evidence searching, seizing and acquisition methodologies in a legal and forensically sound manner
- Types of digital evidence, rules of evidence, digital evidence examination process, and electronic crime and digital evidence consideration by crime category
- Roles of the first responder, first responder toolkit, securing and evaluating electronic crime scene, conducting preliminary interviews, documenting electronic crime scene, collecting and preserving electronic evidence, packaging and transporting electronic evidence, and reporting the crime scene
- Setting up a computer forensics lab and the tools involved in it
- Various file systems and how to boot a disk
- Gathering volatile and non-volatile information from Windows
- Data acquisition and duplication rules
- Validation methods and tools required
- Recovering deleted files and deleted partitions in Windows, Mac OS X, and Linux
- Forensic investigation using AccessData FTK and EnCase
- Steganography and its techniques
- Steganalysis and image file forensics
- Password cracking concepts, tools, and types of password attacks
- Investigating password protected files
- Types of log capturing, log management, time synchronization, and log capturing tools

- Investigating logs, network traffic, wireless attacks, and web attacks
- Tracking emails and investigate email crimes
- Mobile forensics and mobile forensics software and hardware tools
- Writing investigative reports
- Dark Web Forensics and IOT Forensics

Who Can Benefit

IT professionals involved with information system security, computer forensics, and incident response

Prerequisites

It is strongly recommended that you attend Certified Ethical Hacker before enrolling into CHFI program

Course Details

Lab 1: Computer Forensics in Today's World

Lab 2: Learning about Computer Crime Policies, Programs, and Computer Forensics Laws

Lab 3: Reporting a Cybercrime to the FBI

Lab 4: Case Study: Child Pornography

Lab 5: Additional Reading Material

Lab 6: Computer Forensics Investigation Process

Lab 7: Recovering Data Using the Recover My Files Tool

Lab 8: Performing Hash, Checksum, or HMAC Calculations Using the HashCalc Tool

Lab 9: Generating MD5 Hashes Using MD5 Calculator

Lab 10: Additional Reading Material

Lab 11: Searching and Seizing Computers with a Search Warrant

Lab 12: Understanding an Application for a Search Warrant (Exhibit A)

Lab 13: Additional Reading Material

Lab 14: Studying the Digital Evidence Examination Process - Case Study 1

Lab 15: Studying Digital Evidence Examination Process - Case Study 2

Lab 16: Additional Reading Material

Lab 17: Studying First Responder Procedures

Lab 18: Understanding the First Responder Toolkit

Lab 19: Additional Reading Material

Lab 20: Computer Forensics Lab

Lab 21: Gathering Evidence Using the Various Tools of DataLifter

Lab 22: Viewing Files of Various Formats Using the File Viewer Tool

Lab 23: Handling Evidence Data Using the P2 Commander Tool

Lab 24: Creating a Disk Image File of a Hard Disk Partition Using the R-Drive Image Tool

Lab 25: Additional Reading Material

Lab 26: Understanding Hard Disks and File Systems

Lab 27: Recovering Deleted Files from Hard Disks Using WinHex

Lab 28: Analyzing File System Types Using The Sleuth Kit (TSK)

Lab 29: Case Study: Corporate Espionage

Lab 30: Additional Reading Material

Lab 31: Performing Windows Forensics

Lab 32: Discovering and Extracting Hidden Forensic Material on Computers Using OSForensics

Lab 33: Extracting Information about Loaded Processes Using Process Explorer

Lab 34: Investigating Metadata Using Metadata Analyzer

Lab 35: Viewing, Monitoring, and Analyzing Events Using the Event Log

Explorer Tool

Lab 36: Performing a Computer Forensic Investigation Using the Helix Tool

Lab 37: Case Study: Terrorist Attack

Lab 38: Case Study: Brutal Murder

Lab 39: Forensics Challenge: Banking Troubles

Lab 40: Additional Reading Material

Lab 41: Data Acquisition and Duplication

Lab 42: Investigating NTFS Drive Using DiskExplorer for NTFS

Lab 43: Viewing Content of Forensic Image Using AccessData FTK Imager Tool

Lab 44: Searching Text Strings in the Hard Disk Partition Image Using DriveLook

Lab 45: Forensics Challenge: Forensic Analysis of a Compromised Server

Lab 46: Additional Reading Material

Lab 47: Recovering Deleted Files and Deleted Partitions

Lab 48: File Recovery Using EASEUS Data Recovery Wizard

Lab 49: File Recovery Using Quick Recovery Tool

Lab 50: Partition Recovery Using MiniTool Power Data Recovery Tool

Download Whitepaper: Accelerate Your Modernization Efforts with a Cloud-Native Strategy

Get Your Free Copy Now

ExitCertified® Corporation and iMVP® are registered trademarks of ExitCertified ULC and ExitCertified Corporation, respectively
Copyright ©2024 ExitCertified ULC & ExitCertified Corporation. All Rights Reserved.