Computer Hacking Forensic Investigator (CHFI) (v10)

Duration: 5 Days
Method: Instructor-Led Training (ILT) | Live Online Training

Certification: *Computer Hacking Forensic Investigator (CHFI V10)*
*— **Exam:** Computer Hacking Forensic Investigator ((312-49)*

Course Description

CHFI v10 includes all the essentials of digital forensics analysis and evaluation required for today's digital world. From identifying the footprints of a breach to collecting evidence for a prosecution, CHFI v10 walks participants through every step of the process with experiential learning. The course focuses on the latest technologies including IoT Forensics, Dark Web Forensics, Cloud Forensics (including Azure and AWS), Network Forensics, Database Forensics, Mobile Forensics, Malware Forensics (including Emotet and Eternal Blue), OS Forensics, RAM forensics and Tor Forensics, CHFI v10 covers the latest tools, techniques, and methodologies along with ample crafted evidence files.

Target Audience

This course is intended for:

- 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

Prerequisites

To attend this course, candidates must have:

- IT/forensics professionals with basic knowledge of IT/cybersecurity, computer forensics, and incident response.
- Knowledge of Threat Vectors.

Exam Details

Exam Code:	• CHFI EC0 312-49
Length of Exam:	• 4 Hours
Number of Questions:	• 150
Passing Score:	• 70%
Question Format:	• Multiple Choice

Course Objectives

Upon successful completion of this course, attendees will be able to:

- Pursuing the same will help you get a proper understanding of threat intelligence and a crucial understanding of the points that support and scenario modeling pro-active profiling.
- Work on an anti-forensic process for the purpose of detection.
- Learn to execute post-intrusion analysis of digital and electronic media to assess who, where, what, when, and how the intrusion happened in the CHFI training.
- Assess and extract logs from different devices in the form of firewall, IPS, IDS, laptop, desktop, servers, SIM tool, firewall, DHCP logs, switches AD server, Access Control Logs & conclude as part of the investigation procedure.
- Learn how to Assess and check incident source and origin.
- Learn how to recover deleted files in different operating systems.
- Learn how to work on reverse engineering for suspected and known malware files.
- Learn how to the process of collecting data for the purpose of forensic technology priced in accordance with the evidence handling process.

Course Topics

Module 1: 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

Module 2: 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

Module 3: 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

Module 4: Data Acquisition and Duplication

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

Module 5: 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, Overwritten Data/Metadata Detection, and Encryption
- Detect Program Packers and Footprint Minimizing Techniques
- Understand Anti-forensics Countermeasures

Course Topics *Continued*

Module 6: 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

Module 7: 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

Module 8: 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

Module 9: 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

Module 10: Dark Web Forensics

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

Module 11: 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

Course Topics *Continued*

Module 12: Cloud Forensics

- 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

Module 13: Investigating Email Crimes

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

Module 14: 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

Module 15: 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

Module 16: IoT Forensics

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

LABS INCLUDED