COURSE OVERVIEW

Course Name:
EC-Council Certified Hacking Forensic Investigator - CHFI

COURSE DURATION: 5 Days

INTRODUCTION

The Certified Hacking Forensic Investigator (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 students through every step of the process with experiential learning.

This course has been tested and approved by veterans and top practitioners of the cyber forensics industry. CHFI v10 is engineered by industry practitioners for both professionals and aspiring professionals alike from careers including forensic analysts, cybercrime investigators, cyber defence forensic analysts, incident responders, information technology auditors, malware analysts, security consultants, and chief security officers.

Gauteng:
3rd Floor 34 Whitely Road
Melrose Arch
Johannesburg
2196
Tel: 087 941 5764
sales@impactful.co.za

Gauteng:
192 on Bram
192 Bram Fischer Drive
Ferndale, Randburg
Johannesburg
2160
sales@impactful.co.za

Cape Town:
3rd Floor Thomas Pattullo Building
19 Jan Smuts St
Cape Town
8000
sales@impactful.co.za

www.impactful.co.za

IMPACTFUL
Powered by LRMG

TARGET AUDIENCE

- Law Enforcement
- Defence & Military
- e-Business Security
- Systems Administrators
- Legal Professionals
- Banking & Insurance
- Government Agencies
- IT Managers

PREREQUISITES

Mid-Level to High-Level Cyber Security Professionals with a minimum of 3 years of experience. Information security professionals who want to enrich their skills and knowledge.

Knowledge of CND (Certified Network Defender), or CEH (Certified Ethical Hacker) and / or ECIH (Certified Incident Handler) is necessary.

COURSE Objectives

- How to set up a computer forensics lab
- Password Cracking
- How to recover deleted files, how to write investigative reports.
- Roles of first responder, securing & evaluating an electronic crime scene, conducting preliminary interviews, documenting electronic crime scene, & collecting & preserving electronic evidence

COURSE Topics

Module 01: 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 Centre) 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 02: 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 03: 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
- Analyse Popular File Formats Using Hex Editor

Module 04: Data Acquisition and Duplication

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

Module 05: 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

Module 06: 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 07: Linux and Mac Forensics

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

Module 08: 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 ▪ Why Investigate Network Traffic?
- Perform Incident Detection and Examination with SIEM Tools
- Monitor and Detect Wireless Network Attacks

Module 09: 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

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
- Understand Forensic Methodologies for Containers and Microservice

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
- Analyse Suspicious Word and PDF Documents
- Understand Dynamic Malware Analysis Fundamentals and Approaches
- Analyse Malware Behaviour on System Properties in Real-time
- Analyse Malware Behaviour 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
- Illustrate Architectural Layers and Boot Processes of Android and iOS
- 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
- Perform Forensics on IoT Devices