CHFI: Computer Hacking Forensic Investigator

Course ID #: 1275-200-ZZ-W

Hours: 35

Course Content

Course Description:

In this course, you will cover, you will cover 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 defense forensic analysts, incident responders, information technology auditors, malware analysts, security consultants, and chief security officers.

Course Objectives:

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

- Perform effective digital forensic investigation.

Prerequisites:

- IT/Forensics Professionals with basic knowledge on IT/Cyber Security, Computer Forensics, and Incident response.
- Knowledge of Threat Vectors
- Prior completion of CEH training would be an advantage.

Target Audience:

- Anyone interested in cyber forensics/investigations.
- Attorneys, Legal Consultants, and Lawyers
- Law Enforcement Officers
- Police Officers
- Federal/Government Agents
- Defense and Military
- Detectives/Investigators
- Incident Response Team Members
- Information Security Managers
- Network Defenders
- IT Professionals, IT Directors/Managers
- System/Network Engineers
- Security Analyst/Architect/Auditors/Consultants

CHFI: Computer Hacking Forensic Investigator

Course ID #: 1275-200-ZZ-W

Hours: 35

Topics:

Module 01: Computer Forensics in Today's World

Lesson 1: Understanding the Fundamentals of Computer Forensics

- Understanding Computer Forensics
- Need for Computer Forensics
- Why and When Do You Use Computer Forensics?

Lesson 2: Understand Cybercrimes and their Investigation Procedures

- Types of Cybercrimes
  - Examples of Cybercrimes
- Impact of Cybercrimes at the Organizational Level
- Cybercrime Investigation
  - Civil vs. Criminal Investigation
  - Administrative Investigation

Lesson 3: Understand Digital Evidence

- Introduction to Digital Evidence
- Types of Digital Evidence
- Roles of Digital Evidence
- Sources of Potential Evidence
- Rules of Evidence
- Best Evidence Rule
- Federal Rules of Evidence (United States)
- Scientific Working Group on Digital Evidence (SWGDE)
- The Association of Chief Police Officers (ACPO) Principles of Digital Evidence

Lesson 4: Understand Forensic Readiness, Incident Response and the Role of SOC (Security Operations Center) in Computer Forensics

- Forensic Readiness
- Forensic Readiness and Business Continuity
- Forensics Readiness Planning
- Incident Response
- Computer Forensics as a part of Incident Response Plan
- Overview of Incident Response Process Flow
- Role of SOC in Computer Forensics

Lesson 5: Identify the Roles and Responsibilities of a Forensic Investigator

- Need for a Forensic Investigator
- Roles and Responsibilities of a Forensics Investigator
- What Makes a Good Computer Forensics Investigator?
- Code of Ethics
- Accessing Computer Forensics Resources

Lesson 6: Understand the Challenges Faced in Investigating Cybercrimes

- Challenges Cybercrimes Pose to Investigators
- Other Factors That Influence Forensic Investigations
- Computer Forensics: Legal Issues
- Computer Forensics: Privacy Issues

Lesson 7: Understand Legal Compliance in Computer Forensics

- Computer Forensics and Legal Compliance
- Other Laws Relevant to Computer Forensics

CHFI: Computer Hacking Forensic Investigator

Course ID #: 1275-200-ZZ-W

Hours: 35

Module 02: Computer Forensics Investigation Process

Lesson 1: Understand the Forensic Investigation Process and Its Importance

- Forensic Investigation Process
- Importance of the Forensic Investigation Process

Lesson 2: Understand the Pre-investigation Phase

- Setting Up a Computer Forensics Lab
- Building the Investigation Team
- Understanding the Hardware and Software Requirements of a Forensic Lab
- Validating Laboratory Software and Hardware
- Ensuring Quality Assurance

Lesson 3: Understand First Response

- First Response Basics
- First Response by Non-forensics Staff
- First Response by System/Network Administrators
- First Response by Laboratory Forensics Staff

Lesson 4: Understand the Investigation Phase

- Documenting the Electronic Crime Scene
  - Documenting the Electronic Crime Scene
  - Photographing and Sketching the Scene
- Search and Seizure
  - Search and Seizure Process Flow
  - Planning the Search and Seizure
  - Seeking Consent
  - Obtaining Witness Signatures
  - Obtaining Warrant for Search and Seizure
  - Example of a Search Warrant
  - Searches Without a Warrant
  - Collecting Incident Information
  - Initial Search of the Scene
  - Securing and Evaluating the Crime Scene: A Checklist
  - Seizing Evidence at the Crime Scene
  - Dealing with Powered-On Computers
  - Dealing with Powered-Off Computers
  - Dealing with Networked Computers
  - Dealing with Open Files and Startup Files
  - Operating System Shutdown Procedure
  - Dealing with Smartphones or Other Handheld Devices
- Evidence Preservation
  - Preserving Evidence
  - Chain of Custody
  - Simple Format of the Chain of Custody Document
  - Chain of Custody Form
  - Chain of Custody on Property Evidence Envelope/Bag and Sign-out Sheet
  - Evidence Bag Contents List
  - Packaging Evidence
  - Exhibit Numbering
  - Determining the Location for Evidence Examination
  - Transporting and Storing Evidence
- Data Acquisition
  - Acquiring the Data
  - Duplicating the Data (Imaging)
- Data Analysis
  - Analyzing the Data
- Case Analysis
  - Analysis of the Case
  - Evidence Reconstruction
  - Collecting Evidence from Social Networks

Lesson 5: Understand the Post-investigation Phase

- Reporting
  - Gathering and Organizing Information
  - Writing the Investigation Report
  - Forensic Investigation Report Template
  - Guidelines for Writing a Report
- Testify as an Expert Witness
  - Who is an Expert Witness?
  - Roles of an Expert Witness
  - What Makes a Good Expert Witness?
  - Testifying in the Court
  - General Ethics while Testifying

CHFI: Computer Hacking Forensic Investigator

Course ID #: 1275-200-ZZ-W

Hours: 35

Module 03: Understanding Hard Disks and File Systems

Lesson 1: Describe Different Types of Disk Drives and their Characteristics

- Understanding Hard Disk Drive
  - Tracks
  - Sector
  - 4K Sectors
  - Data Density on a Hard Disk
  - CHS (Cylinder-Head-Sector) Data Addressing and Disk Capacity Calculation
  - Measuring the Hard Disk Performance
- Understanding Solid-State Drive (SSD)
- Disk Interfaces
  - ATA/PATA (IDE/EIDE)
  - Serial ATA/ SATA (AHCI)
  - Serial Attached SCSI
  - PCIe SSD
  - SCSI

Lesson 2: Explain the Logical Structure of a Disk

- Logical Structure of Disks
  - Clusters
  - Lost Clusters
  - Slack Space
  - Master Boot Record (MBR)
  - Structure of a Master Boot Record
  - Disk Partitions
  - BIOS Parameter Block (BPB)
  - Globally Unique Identifier (GUID)
- GUID Partition Table (GPT)

Lesson 3: Understand Booting Process of Windows, Linux and Mac Operating Systems

- What is the Booting Process?
- Essential Windows System Files
- Windows Boot Process: BIOS-MBR Method
  - Identifying the MBR Partition
- Windows Boot Process: UEFI-GPT
  - Identifying the GUID Partition Table (GPT)
  - Analyzing the GPT Header and Entries
  - GPT Artifacts
- Macintosh Boot Process
- Linux Boot Process

Lesson 4: Understand Various File Systems of Windows, Linux and Mac Operating Systems

- Windows File Systems
  - File Allocation Table (FAT)
- FAT File System Layout
- FAT Partition Boot Sector
- FAT Folder Structure
- Directory Entries and Cluster Chains
- Filenames on FAT Volumes
- FAT32
  - New Technology File System (NTFS)
- NTFS Architecture
- NTFS System Files
- NTFS Partition Boot Sector
- Cluster Sizes of NTFS Volume
- NTFS Master File Table (MFT)
  - Metadata Files Stored in the MFT
- NTFS Attributes
- NTFS Data Stream
- NTFS Compressed Files
- Encrypting File Systems (EFS)
  - Components of EFS
  - EFS Attribute
- Sparse Files
- Linux File Systems
- Linux File System Architecture
  - Filesystem Hierarchy Standard (FHS)
  - Extended File System (ext)
  - Second Extended File System (ext2)
  - Third Extended File System (ext3)

  - Journaling File System
  - Fourth Extended File System (ext4)
  - Understanding Superblocks, Inodes, and Data Blocks
- Mac OS X File Systems
  - Hierarchical File System Plus (HFS+)
- HFS Plus Volumes
- HFS Plus Journal
  - Apple File System (APFS)
- Major Components of APFS
- APFS vs. HFS Plus
- CD-ROM/DVD File System
- Virtual File System (VFS) and Universal Disk Format (UDF) File System

Lesson 5: Examine File System Using Autopsy and The Sleuth Kit Tools

- File System Analysis Using Autopsy
- File System Analysis Using The Sleuth Kit (TSK)
  - The Sleuth Kit (TSK): fsstat
  - The Sleuth Kit (TSK): istat
  - The Sleuth Kit (TSK): fls and img_stat

Lesson 6: Understand Storage Systems

- RAID Storage System
  - Levels of RAID Storage System
  - Just a Bunch of Drives/Disks (JBOD)
  - Host Protected Areas (HPA) and Device Configuration Overlays (DCO)
- NAS/SAN Storage
  - Network-Attached Storage (NAS)
  - Storage Area Network (SAN)
  - Differences between NAS and SAN

Lesson 7: Understand Encoding Standards and Hex Editors

- Character Encoding Standard: ASCII
- Character Encoding Standard: UNICODE
- OFFSET
- Understanding Hex Editors
- Understanding Hexadecimal Notation

Lesson 8: Analyze Popular File Formats Using Hex Editor

- Image File Analysis: JPEG
- Image File Analysis: BMP
- Hex View of Popular Image File Formats
- PDF File Analysis
- Word File Analysis
- PowerPoint File Analysis
- Excel File Analysis
- Hex View of Other Popular File Formats
- Hex View of Popular Video File Formats
- Hex View of Popular Audio File Formats

Module 04: Data Acquisition and Duplication

Lesson 1: Understand Data Acquisition Fundamentals

- Understanding Data Acquisition
- Live Acquisition
- Order of Volatility
- Dead Acquisition
- Rules of Thumb for Data Acquisition
- Types of Data Acquisition
  - Logical Acquisition
  - Sparse Acquisition
  - Bit-Stream Imaging
- Bit-stream disk-to-image file
- Bit-stream disk-to-disk
- Determine the Data Acquisition Format
  - Raw Format
  - Proprietary Format
  - Advanced Forensics Format (AFF)
  - Advanced Forensic Framework 4 (AFF4)

Lesson 2: Understand Data Acquisition Methodology

- Data Acquisition Methodology
- Step 1: Determine the Best Data Acquisition Method
- Step 2: Select the Data Acquisition Tool
- Step 3: Sanitize the Target Media
- Step 4: Acquire Volatile Data
  - Acquire Volatile Data from a Windows Machine
  - Acquire Volatile Data from a Linux Machine
- Acquire Volatile Data from a Linux Machine Using dd (Local Acquisition)
- Acquire Volatile Data from a Linux Machine Using dd and Netcat (Remote Acquisition)
- Acquire Volatile Data from a Linux Machine Using LiME (Local Acquisition)
- Acquire Volatile Data from a Linux Machine Using LiME and Netcat (Remote Acquisition)
  - Acquire Volatile Data from a Mac Machine Using
- Digital Collector
- OSXpmem
- Step 5: Enable Write Protection on the Evidence Media
- Step 6: Acquire Non-volatile Data
  - Using a Windows Forensic Workstation
  - Using a Linux Forensic Workstation
  - Using macOS - Single User Mode
  - Using macOS - Target Disk Mode
  - Using a Linux Bootable CD/USB
  - Using Digital Collector
  - Acquiring RAID Disks
- Step 7: Plan for Contingency
- Step 8: Validate Data Acquisition Using
  - Windows Validation Methods
  - Linux/Mac Validation Methods

Lesson 3: Prepare an Image File for Examination

- Preparing an Image for Examination
  - Scenario 1: The Acquired Evidence is in E01 Format and the Forensic Workstation is Linux
  - Scenario 2: The Acquired Evidence Needs to be Converted to a Bootable VM
  - Scenario 3: The Acquired Physical Hard Disk Contains Windows File System and the Forensic Workstation is Linux
  - Scenario 4: The Acquired Evidence Contains APFS file system and the Forensic Workstation is Linux
- Viewing an Image on a Windows, Linux and Mac Forensic Workstations

CHFI: Computer Hacking Forensic Investigator

Course ID #: 1275-200-ZZ-W

Hours: 35

Module 05: Defeating Anti-forensics Techniques

Lesson 1: Understand Anti-forensics Techniques

- What is Anti-forensics?
- Anti-forensics Techniques

Lesson 2: Discuss Data Deletion and Recycle Bin Forensics

- Anti-forensics Technique: Data/File Deletion
- What Happens When a File is Deleted in Windows?
- Recycle Bin in Windows
  - Recycle Bin Forensics

Lesson 3: Illustrate File Carving Techniques and Ways to Recover Evidence from Deleted Partitions

- File Carving
  - File Carving on Windows
- SSD File Carving on Windows File System
- HDD File Carving on Windows File System
- File Recovery Tools: Windows
  - File Carving on Linux
- File Carving on Linux File System
- File Recovery Tools: Linux
  - File Carving on macOS
- SSD File Carving on Apple File System
- File Recovery Tools: macOS
- Recovering Deleted Partitions
  - Recovering Deleted Partitions: Using R-Studio
  - Recovering Deleted Partitions: Using EaseUS Data Recovery Wizard
  - Partition Recovery Tools

Lesson 4: Explore Password Cracking/Bypassing Techniques

- Anti-forensics Technique: Password Protection
- Using Rainbow Tables to Crack Hashed Passwords
  - Tool to Create Rainbow Tables: Winrtgen
- Password Cracking: Using L0phtCrack and Ophcrack
- Password Cracking: Using Cain & Abel and RainbowCrack
- Password Cracking: Using PwDump7
- Password Cracking Tools
- Bypassing Passwords on Powered-off Computer
  - Bypassing BIOS Passwords
  - Bypassing BIOS Passwords by Resetting CMOS Using Jumpers
  - Bypassing BIOS Passwords by Removing CMOS Battery
- Tool to Reset Admin Password
  - Lazesoft Recover My Password
  - Bypassing Windows User Password: Lazesoft Recovery Suite
  - Bypassing Windows User Password by Booting Live CD/USB
  - Application Password Cracking Tools

Lesson 5: Detect Steganography, Hidden Data in File System Structures, Trail Obfuscation, and File Extension Mismatch

- Anti-forensics Technique: Steganography
  - Defeating Anti-forensics: Steganalysis
  - Steganalysis Methods/Attacks on Steganography
- Detecting Steganography (Text, Image, Audio, and Video Files)
  - Steganography Detection Tools
- Defeating Anti-forensics Technique: Detecting Data Hiding in File System Structures Using OSForensics
- Anti-forensics Technique: Alternate Data Streams
  - Defeating Anti-forensics Technique: Detecting Alternate Data Streams
  - Defeating Anti-forensics Technique: Detecting Alternate Data Streams Using Stream Detector
- Anti-forensics Technique: Trail Obfuscation
- Defeating Anti-forensics Technique: Detecting File Extension Mismatch Using Autopsy

Lesson 6: Understand Techniques of Artifact Wiping, Overwritten Data/Metadata Detection, and Encryption

- Anti-forensics Technique: Artifact Wiping
- Anti-forensics Technique: Overwriting Data/Metadata
  - Defeating Anti-forensics Technique: Detecting Overwritten Data/Metadata
- Anti-forensics Technique: Encryption
  - Recover Encrypted Files Using Advanced EFS Data Recovery Tool

Lesson 7: Detect Program Packers and Footprint Minimizing Techniques

- Anti-forensics Technique: Program Packers
  - Unpacking Program Packers
- Anti-forensics Techniques that Minimize Footprint
  - Defeating Anti-forensics Technique: Detecting USB Devices

Lesson 8: Understand Anti-forensics Countermeasures

CHFI: Computer Hacking Forensic Investigator

Course ID #: 1275-200-ZZ-W

Hours: 35

Module 06: Windows Forensics

Lesson 1: Collect Volatile and Non-volatile Information

- Collecting Volatile Information
  - Collecting System Time
  - Collecting Logged-On Users
- PsLoggedOn Tool
- net sessions Command
- LogonSessions Tool
- Collecting Open Files
- net file Command
- Using NetworkOpenedFiles
  - Collecting Network Information
  - Collecting Information about Network Connections
  - Process Information
  - Process-to-Port Mapping
  - Examining Process Memory
  - Collecting Network Status
  - Examining Print Spool files
  - Collecting Clipboard Contents and Service/Driver Information
  - Collecting Command History and Locally Shared Resource Information
- Collecting Non-volatile Information
  - Examining File Systems
  - ESE Database File
- Examining .edb File Using ESEDatabaseView
  - Windows Search Index Analysis
  - Detecting Externally Connected Devices to the System
  - Slack Space
  - Collecting Hidden Partition Information
  - Other Non-volatile Information
  - Analyzing Windows Thumbnail Cache

Lesson 2: Perform Windows Memory and Registry Analysis

- Windows Crash Dump
- Collecting Process Memory
- Random Access Memory (RAM) Acquisition
- Memory Forensics
  - Malware Analysis Using Redline
  - Malware Analysis Using Volatility Framework
  - Virtual Memory Acquisition Using FTK Imager
  - Page File
- Examining Pagefile Using Strings Command
  - Hibernate Files
- Windows Registry Analysis
  - Windows Registry
  - Registry Structure within a Hive File
  - Windows Registry: Forensic Analysis
  - The Registry as a Log File
  - Collecting System Information
  - Collecting Last Shutdown Time and Time Zone Information
  - Shares
  - Wireless SSIDs
  - Startup Locations
  - System Boot
  - Importance of Volume Shadow Copy Services
  - User Login
  - Microsoft Security ID
  - User Activity
  - Enumerating Autostart Registry Locations
  - Registry Settings
  - USB Removable Storage Devices
  - Mounted Devices
  - Tracking User Activity
  - The UserAssist Keys
  - MRU Lists
  - Connecting to Other Systems
  - Analyzing Restore Point Registry Settings
  - Determining the Startup Locations

Lesson 3: Examine the Cache, Cookie and History Recorded in Web Browsers

- Cache, Cookie, and History Analysis: Mozilla Firefox
  - Analysis Tool: MZCacheView
  - Analysis Tool: MZCookiesView
  - Analysis Tool: MZHistoryView
- Cache, Cookie, and History Analysis: Google Chrome
  - Analysis Tool: ChromeCacheView
  - Analysis Tool: ChromeCookiesView
  - Analysis Tool: ChromeHistoryView
- Cache, Cookie, and History Analysis: Microsoft Edge
  - Analysis Tool: IECacheView
  - Analysis Tool: EdgeCookiesView
  - Analysis Tool: BrowsingHistoryView

Lesson 4: Examine Windows Files and Metadata

- Windows File Analysis
  - System Restore Points (Rp.log Files)
  - System Restore Points (Change.log.x Files)
  - Prefetch Files
- Examining Prefetch Files Using WinPrefetchView
  - Image Files
  - Understanding EXIF Data
- Metadata Investigation
  - Understanding Metadata
  - Metadata in Different File Systems
  - Metadata in PDF Files
  - Metadata in Word Documents
  - Metadata Analysis Tool: Metashield Analyzer

Lesson 5: Understand ShellBags, LNK Files, and Jump Lists

- Windows ShellBags
  - Windows ShellBags: Forensic Analysis
  - Parsing ShellBags: Using ShellBags Explorer Tool
- Analyzing LNK Files
  - Analyzing LNK files: LECmd Tool
- Analyzing Jump Lists
  - Analyzing Jump Lists: JumpListExt Tool

Lesson 6: Understand Text-based Logs and Windows Event Logs

- Understanding Events
- Types of Logon Events
- Event Log File Format
- Organization of Event Records
- ELF_LOGFILE_HEADER Structure
- EventLogRecord Structure
- Windows 10 Event Logs
- Evaluating Account Management Events
- Event Logs
  - Examining System Log Entries
  - Examining Application Log Entries
  - Searching with Event Viewer
  - Using Event Log Explorer to Examine Log Files
  - Windows Event Log Files Internals
  - Examining Removable Storage Using Event Viewer
- Windows Forensics Tools
  - OSForensics
  - Kroll Artifact Parser and Extractor (KAPE)
- Hashing it Out in PowerShell: Using Get-FileHash

CHFI: Computer Hacking Forensic Investigator

Course ID #: 1275-200-ZZ-W

Hours: 35

Module 07: Linux and Mac Forensics

Lesson 1: Understand Volatile and Non-volatile Data in Linux

- Introduction to Linux Forensics
- Collecting Volatile Data
  - Collecting Hostname, Date, and Time
  - Collecting Uptime Data
  - Collecting Network Information
  - Viewing Network Routing Tables
  - Collecting Open Port Information
  - Finding Programs/Processes Associated with a Port
  - Collecting Data on Open Files
  - Collecting Mounted File System Information
  - Finding Loaded Kernel Modules
  - Collecting User Events and Reading ELF Files
  - Viewing Running Processes in the System
  - Collecting Swap Areas and Disk Partition Information
  - Collecting Kernel Messages
- Collecting Non-volatile Data
  - Collecting System Information
  - Collecting Kernel Information
  - Collecting User Account Information
  - Collecting Currently Logged-in Users and Login History Information
  - Collecting System Logs Data
  - Linux Log Files
  - Collecting User History File Information and Viewing Hidden Files and Directories
  - Collecting Suspicious Information
  - File Signature Analysis
  - Usage of File and Strings Command
  - Using find Command to Find Writable Files

Lesson 2: Analyze Filesystem Images Using The Sleuth Kit

- File System Analysis Using The Sleuth Kit
  - fsstat
  - fls
  - istat

Lesson 3: Demonstrate Memory Forensics Using Volatility & PhotoRec

- Memory Forensics
  - Introduction
  - Collecting Network Information
  - Listing Open Files
  - Collecting Bash Information
  - Collecting System Information
  - Collecting Kernel Memory Information
  - Malware Analysis Using Volatility Framework
  - Carving Memory Dumps Using PhotoRec Tool

Lesson 4: Understand Mac Forensics

- Introduction to Mac Forensics
- Mac Forensics Data
- Mac Log Files
- Mac Directories
- APFS Analysis: Biskus APFS Capture
- Parsing Metadata on Spotlight
- Mac Forensics Tools

CHFI: Computer Hacking Forensic Investigator

Course ID #: 1275-200-ZZ-W

Hours: 35

Module 08: Network Forensics

Lesson 1: Understand Network Forensics

- Introduction to Network Forensics
- Postmortem and Real-Time Analysis
- Network Attacks
- Indicators of Compromise (IOCs)
- Where to Look for Evidence
- Types of Network-based Evidence

Lesson 2: Explain Logging Fundamentals and Network Forensic Readiness

- Log Files as Evidence
- Legal Criteria for Admissibility of Logs as Evidence
- Records of Regularly Conducted Activity as Evidence
- Guidelines to Ensure Log File Credibility and Usability
- Ensure Log File Authenticity
- Maintain Log File Integrity
- Implement Centralized Log Management
  - Centralized Logging Best Practices
  - Centralized Log Management Challenges
  - Addressing the Challenges in Centralized Log Management

Lesson 3: Summarize Event Correlation Concepts

- ▪ Event Correlation
- ▪ Types of Event Correlation
- ▪ Prerequisites of Event Correlation
- ▪ Event Correlation Approaches

Lesson 4: Identify Indicators of Compromise (IoCs) from Network Logs

- Analyzing Firewall Logs
  - Analyzing Firewall Logs: Cisco
  - Analyzing Firewall Logs: Check Point
- Analyzing IDS Logs
  - Analyzing IDS Logs: Juniper
  - Analyzing IDS Logs: Check Point
- Analyzing Honeypot Logs
- Analyzing Router Logs
  - Analyzing Router Logs: Cisco
  - Analyzing Router Logs: Juniper
- Analyzing DHCP Logs

Lesson 5: Investigate Network Traffic

- Why Investigate Network Traffic?
- Gathering Evidence via Sniffers
- Sniffing Tool: Tcpdump
- Sniffing Tool: Wireshark
  - Display Filters in Wireshark
- Analyze Traffic for TCP SYN Flood DoS Attack
- Analyze Traffic for SYN-FIN Flood DoS Attack
- Analyze Traffic for FTP Password Cracking Attempts
- Analyze Traffic for SMB Password Cracking Attempts
- Analyze Traffic for Sniffing Attempts
  - Analyze Traffic for MAC Flooding Attempt
  - Analyze Traffic for ARP Poisoning Attempt
- Analyze Traffic to Detect Malware Activity

Lesson 6: Perform Incident Detection and Examination with SIEM Tools

- Centralized Logging Using SIEM Solutions
- SIEM Solutions: Splunk Enterprise Security (ES)
- SIEM Solutions: IBM QRadar
- Examine Brute-force Attacks
- Examine DoS Attack
- Examine Malware Activity
- Examine Data Exfiltration Attempts over FTP
- Examine Network Scanning Attempts
- Examine Ransomware Attack
- Detect Rogue DNS Server (DNS Hijacking/DNS Spoofing)

Lesson 7: Monitor and Detect Wireless Network Attacks

- Wireless Network Security Vulnerabilities
- Monitoring for Attacks and Vulnerabilities
- Detect Rogue Access Points
- Detect Access Point MAC Address Spoofing Attempts
- Detect Misconfigured Access Points
- Detect Honeypot Access Points
- Detect Signal Jamming Attack

CHFI: Computer Hacking Forensic Investigator

Course ID #: 1275-200-ZZ-W

Hours: 35

Module 09: Investigating Web Application Forensics

Lesson 1: Understand Web Application Forensics
- Introduction to Web Application Forensics
- Challenges in Web Application Forensics
- Indications of a Web Attack
- Web Application Threats
- Web Attack Investigation Methodology

Lesson 2: Understand Internet Information Services (IIS) Logs
- IIS Web Server Architecture
- IIS Logs
- Analyzing IIS Logs

Lesson 3: Understand Apache Web Server Logs
- Apache Web Server Architecture
- Apache Web Server Logs
- Apache Access Logs
  - Analyzing Apache Access Logs
- Apache Error Logs
  - Analyzing Apache Error Logs

Lesson 4: Understand the Functionality of Intrusion Detection System (IDS)
- Intrusion Detection System (IDS)
- How IDS Detects an Intrusion
- Intrusion Detection Tool: Snort
- Snort Rules

Lesson 5: Understand the Functionality of Web Application Firewall (WAF)
- Web Application Firewall (WAF)
- Benefits of WAF
- Limitations of WAF
- WAF Tool: ModSecurity
- Types of ModSecurity Data Formats
  - Analyzing ModSecurity Alerts
  - Analyzing ModSecurity Audit Logs

Lesson 6: Investigate Web Attacks on Windows-based Servers
- Investigating Web Attacks on Windows-based Servers

Lesson 7: Detect and Investigate Various Attacks on Web Applications
- Investigating Cross-Site Scripting (XSS) Attack
  - Investigating XSS: Using Regex to Search XSS Strings
  - Examining Apache Logs for XSS Attack
  - Examining IIS Logs for XSS Attack
  - Examining Snort Alert Logs for XSS Attack
  - Examining WAF Logs for XSS Attack
  - Examining SIEM Logs for XSS Attack
- Investigating SQL Injection Attack
  - Investigating SQL Injection Attack: Using Regex
  - Examining Apache Logs for SQL Injection Attack
  - Examining IIS Logs for SQL Injection Attack
  - Examining Snort Alert Logs for SQL Injection Attack
  - Examining WAF Logs for SQL Injection Attack
  - Examining SIEM Logs for SQL Injection Attack
- Investigating Path/Directory Traversal Attack
  - Examining Apache Logs for Path/Directory Traversal Attack
- Investigating Command Injection Attack
  - Examining Apache Logs for Command Injection Attack
- Investigating XML External Entity (XXE) Attack
  - Examining Apache Log File for XXE Attack
- Investigating Brute-force Attack
  - Examining Apache Log File for Brute-force Attack

Module 10: Dark Web Forensics

Lesson 1: Understand the Dark Web

- Understanding the Dark Web
- Tor Relays
- Working of the Tor Browser
- Tor Bridge Node

Lesson 2: Determine How to Identify the Traces of Tor Browser during Investigation

- Dark Web Forensics
- Identifying Tor Browser Artifacts: Command Prompt
- Identifying Tor Browser Artifacts: Windows Registry
- Identifying Tor Browser Artifacts: Prefetch Files

Lesson 3: Perform Tor Browser Forensics

- Tor Browser Forensics: Memory Acquisition
- Collecting Memory Dumps
- Memory Dump Analysis: Bulk Extractor
- Forensic Analysis of Memory Dumps to Examine Email Artifacts (Tor Browser Open)
- Forensic Analysis of Storage to Acquire Email Attachments (Tor Browser Open)
- Forensic Analysis of Memory Dumps to Examine Email Artifacts (Tor Browser Closed)
- Forensic Analysis of Storage to Acquire Email Attachments (Tor Browser Closed)
- Forensic Analysis: Tor Browser Uninstalled
- Dark Web Forensics Challenges

CHFI: Computer Hacking Forensic Investigator

Course ID #: 1275-200-ZZ-W

Hours: 35

Module 11: Database Forensics

Lesson 1: Understand Database Forensics and its Importance

▪ Database Forensics and its Importance

Lesson 2: Determine Data Storage and Database Evidence Repositories in MSSQL Server

- Data Storage in SQL Server
- Database Evidence Repositories

Lesson 3: Collect Evidence Files on MSSQL Server

- Collecting Volatile Database Data
- Collecting Primary Data File and Active Transaction Logs Using SQLCMD
- Collecting Primary Data File and Transaction Logs
- Collecting Active Transaction Logs Using SQL Server Management Studio
- Collecting Database Plan Cache
- Collecting Windows Logs
- Collecting SQL Server Trace Files
- Collecting SQL Server Error Logs

Lesson 4: Perform MSSQL Forensics

- Database Forensics Using SQL Server Management Studio
- Database Forensics Using ApexSQL DBA

Lesson 5: Understand Internal Architecture of MySQL and Structure of Data Directory

- Internal Architecture of MySQL
- Structure of Data Directory

Lesson 6: Understand Information Schema and List MySQL Utilities for Performing Forensic Analysis

- MySQL Forensics
- Viewing the Information Schema
- MySQL Utility Programs for Forensic Analysis

Lesson 7: Perform MySQL Forensics on WordPress Web Application Database

- Common Scenario for Reference
- MySQL Forensics for WordPress Website Database: Scenario 1
  - Collect the Evidence
  - Examine the Log Files
  - Analyze the General Log
  - Take Backup of the Database
  - Create Evidence Database
  - Select Database
  - View Tables in the Database
  - View Users in the Database
  - View Columns in the Table
  - Collect Posts Made by the User
  - Examine the Posts Made by the User
- MySQL Forensics for WordPress Website Database: Scenario 2
  - Collect the Database and All the Logs
  - Examine the Binary Logs
  - wp_users.ibd in WordPress Database
  - wp_posts.ibd in WordPress Database

CHFI: Computer Hacking Forensic Investigator

Course ID #: 1275-200-ZZ-W

Hours: 35

Module 12: Cloud Forensics

Lesson 1: Understand the Basic Cloud Computing Concepts

- Introduction to Cloud Computing
- Types of Cloud Computing Services
- Cloud Deployment Models
- Cloud Computing Threats
- Cloud Computing Attacks

Lesson 2: Understand Cloud Forensics

- Introduction to Cloud Forensics
- Usage of Cloud Forensics
- Cloud Crimes
- Cloud Forensics: Stakeholders and their Roles
- Cloud Forensics Challenges
  - Architecture and Identification
  - Data Collection
  - Logs
  - Legal
  - Analysis

Lesson 3: Understand the Fundamentals of Amazon Web Services (AWS)

- Introduction to Amazon Web Services
- Division of Responsibilities in AWS
  - Shared Responsibility Model for Infrastructure Services
  - Shared Responsibility Model for Container Services
  - Shared Responsibility Model for Abstracted Services
- Data Storage in AWS
- Logs in AWS

Lesson 4: Determine How to Investigate Security Incidents in AWS

- Forensic Acquisition of Amazon EC2 Instance: Methodology
  - Step 1: Isolate the Compromised EC2 Instance
  - Step 2: Take a Snapshot of the EC2 Instance
  - Step 3: Provision and Launch a Forensic Workstation
  - Step 4: Create Evidence Volume from the Snapshot
  - Step 5: Attach the Evidence Volume to the Forensic Workstation
  - Step 6: Mount the Evidence Volume on the Forensic Workstation
- Investigating Log Files: CloudWatch Logs and S3 Server Access Logs

Lesson 5: Understand the Fundamentals of Microsoft Azure

- Introduction to Microsoft Azure
- Division of Responsibilities in Azure
- Data Storage in Azure
- Logs in Azure

Lesson 6: Determine How to Investigate Security Incidents in Azure

- Forensic Acquisition of VMs in Azure: Methodology
  - Forensic Acquisition of VMs in Azure: The Scenario
  - Step 1: Create a Snapshot of the OS Disk of the Affected VM via Azure Portal and Azure CLI
  - Step 2: Copy the Snapshot to a Storage Account under a Different Resource Group
  - Step 3: Delete the Snapshot from the Source Resource Group and Create a Backup Copy
  - Step 4: Mount the Snapshot onto the Forensic Workstation
  - Analyze the Snapshot via Autopsy

Lesson 7: Understand Forensic Methodologies for Containers and Microservices

- What are Containers and Microservices?
- Challenges of Performing Forensics on Containers
- Container Forensics and Incident Response: Methodology
- Container Forensics Using Docker

Module 13: Investigating Email Crimes

Lesson 1: Understand Email Basics

- Introduction to an Email System
- Components Involved in Email Communication
- How Email Communication Works?
- Understanding the Parts of an Email Message

Lesson 2: Understand Email Crime Investigation and its Steps

- Introduction to Email Crime Investigation
- Steps to Investigate Email Crimes
  - Step 1: Seizing the Computer and Email Accounts
  - Step 2: Acquiring the Email Data
- Acquiring Email Data from Desktop-based Email Clients
  - Local Email Files in Microsoft Outlook
  - Local Email Files in Mozilla Thunderbird
  - Acquiring Thunderbird Local Email Files via SysTools MailPro+
  - Acquiring Outlook Email Files: .ost to .pst File Conversion
  - Acquiring Outlook .pst File via SysTools MailPro+
- Acquiring Email Data from Web-based Email Accounts
  - Step 3: Examining Email Messages
  - Step 4: Retrieving Email Headers
- Retrieving Email Headers in Microsoft Outlook
- Retrieving Email Headers in Microsoft Outlook.com
- Retrieving Email Headers in AOL
- Retrieving Email Headers in Apple Mail
- Retrieving Email Headers in Gmail
- Retrieving Email Headers in Yahoo Mail
  - Step 5: Analyzing Email Headers
- Analyzing Email Headers: X-Headers
- Analyzing Email Headers: Checking Email Authenticity
- Analyzing Email Headers: Examining the Originating IP Address
- Investigating a Suspicious Email
  - Step 6: Recovering Deleted Email Messages
- Recovering Deleted Email Messages from Outlook .pst Files Using Paraben's Electronic Evidence Examiner
- Recovering deleted Email Data from Thunderbird Using Paraben's Electronic Evidence Examiner

Lesson 3: U.S. Laws Against Email Crime

- U.S. Laws Against Email Crime: CAN-SPAM Act

CHFI: Computer Hacking Forensic Investigator

Course ID #: 1275-200-ZZ-W

Hours: 35

Module 14: Malware Forensics

Lesson 1: Define Malware and Identify the Common Techniques Attackers Use to Spread Malware

- Introduction to Malware
- Components of Malware
- Common Techniques Attackers Use to Distribute Malware across Web

Lesson 2: Understand Malware Forensics Fundamentals and Recognize Types of Malware Analysis

- Introduction to Malware Forensics
- Why Analyze Malware?
- Malware Analysis Challenges
- Identifying and Extracting Malware
- Prominence of Setting Up a Controlled Malware Analysis Lab
- Preparing Testbed for Malware Analysis
- Supporting Tools for Malware Analysis
- General Rules for Malware Analysis
- Documentation Before Analysis
- Types of Malware Analysis

Lesson 3: Understand and Perform Static Analysis of Malware

- Malware Analysis: Static
  - Static Malware Analysis: File Fingerprinting
  - Static Malware Analysis: Online Malware Scanning
  - Online Malware Analysis Services
  - Static Malware Analysis: Performing Strings Search
  - Static Malware Analysis: Identifying Packing/Obfuscation Methods
  - Static Malware Analysis: Finding the Portable Executables (PE) Information
- Analyzing Portable Executable File Using Pestudio
  - Static Malware Analysis: Identifying File Dependencies
  - Static Malware Analysis: Malware Disassembly
  - Malware Analysis Tool: IDA Pro

Lesson 4: Analyze Suspicious Word and PDF Documents

- Analyzing Suspicious MS Office Document
- Analyzing Suspicious PDF Document

Lesson 5: Understand Dynamic Malware Analysis Fundamentals and Approaches

- Malware Analysis: Dynamic
  - Dynamic Malware Analysis: Pre-Execution Preparation
  - Monitoring Host Integrity
  - Monitoring Host Integrity Using WhatChanged Portable
  - Observing Runtime Behavior

Lesson 6: Analyze Malware Behavior on System Properties in Real-time

- System Behavior Analysis: Monitoring Registry Artifacts
  - Windows AutoStart Registry Keys
  - Analyzing Windows AutoStart Registry Keys
- System Behavior Analysis: Monitoring Processes
- System Behavior Analysis: Monitoring Windows Services
- System Behavior Analysis: Monitoring Startup Programs
  - Startup Programs Monitoring Tool: AutoRuns for Windows
- System Behavior Analysis: Monitoring Windows Event Logs
  - Key Event IDs to Monitor
  - Examining Windows Event logs
- System Behavior Analysis: Monitoring API Calls
- System Behavior Analysis: Monitoring Device Drivers
  - Device Drivers Monitoring Tool: DriverView
- System Behavior Analysis: Monitoring Files and Folders
  - File and Folder Monitoring Tool: PA File Sight
  - File and Folder Integrity Checkers: FastSum and WinMD5

Lesson 7: Analyze Malware Behavior on Network in Real-time

- Network Behavior Analysis: Monitoring Network Activities
  - Monitoring IP Addresses
- Network Behavior Analysis: Monitoring Port
  - Examining Open Ports
  - Port Monitoring Tools: TCPView and CurrPorts
- Network Behavior Analysis: Monitoring DNS
  - Examining DNS Entries
  - DNS Monitoring Tool: DNSQuerySniffer

Lesson 8: Describe Fileless Malware Attacks and How they Happen

- Introduction to Fileless Malware
- Infection Chain of Fileless Malware
- How Fileless Attack Works via Memory Exploits
- How Fileless Attack Happens via Websites
- How Fileless Attack Happens via Documents

Lesson 9: Perform Fileless Malware Analysis - Emotet

- Fileless Malware Analysis: Emotet
- Emotet Malware Analysis
- Emotet Malware Analysis: Timeline of the Infection Chain

CHFI: Computer Hacking Forensic Investigator

Course ID #: 1275-200-ZZ-W

Hours: 35

Module 15: Mobile Forensics

Lesson 1: Understand the Importance of Mobile Device Forensics

- Mobile Device Forensics
- Why Mobile Forensics?
- Top Threats Targeting Mobile Devices
- Mobile Hardware and Forensics
- Mobile OS and Forensics

Lesson 2: Illustrate Architectural Layers and Boot Processes of Android and iOS Devices

- Architectural Layers of Mobile Device Environment
- Android Architecture Stack
- Android Boot Process
- iOS Architecture
- iOS Boot Process
  - Normal and DFU Mode Booting
  - Booting iPhone in DFU Mode
  - Booting iPhone in Recovery Mode

Lesson 3: Explain the Steps Involved in Mobile Forensics Process

- Mobile Forensics Process
  - Collect the Evidence
  - Document the Evidence
  - Preserve the Evidence
  - Mobile Storage and Evidence Locations
  - Data Acquisition Methods

Lesson 4: Investigate Cellular Network Data

- Components of Cellular Network
- Different Cellular Networks
- Cell Site Analysis: Analyzing Service Provider Data
- CDR Contents

Lesson 5: Understand SIM File System and its Data Acquisition Method

- Subscriber Identity Module (SIM)
  - SIM File System
  - Data Stored in a SIM
  - Integrated Circuit Card Identification (ICCID)
  - International Mobile Equipment Identifier (IMEI)
  - SIM Cloning
  - SIM Data Acquisition Using Oxygen Forensic Extractor
  - SIM Data Acquisition Tools

Lesson 6: Illustrate Phone Locks and Discuss Rooting of Android and Jailbreaking of iOS Devices

  - Phone Locking on Android
  - Phone Locking on iOS
  - Rooting of Android Devices
  - Jailbreaking of iOS Devices
  - Risks of Jailbreaking
  - Types of Jailbreaks
  - Semi-tethered Jailbreaking Using Checkra1n

Lesson 7: Perform Logical Acquisition on Android and iOS Devices

- Logical Acquisition
  - Android Debug Bridge (ADB)
  - Steps Involved in Android Forensics Process
  - Logical Acquisition of Android Devices: Using “adb pull” Command
  - Logical Acquisition of Android Devices: Using Commercial Tools
  - Logical Acquisition Tools
  - Steps Involved in iOS Forensics Process
  - Logical Acquisition of iOS Devices: Using iTunes Backup
  - Logical Acquisition of iOS Devices: Using Commercial Tools
- Cloud Data Acquisition on Android and iOS Devices
- Cloud Data Acquisition: Using Commercial Tools

Lesson 8: Perform Physical Acquisition on Android and iOS Devices

- Physical Acquisition
  - Physical Acquisition of Android Devices: Using DD Command
  - Physical Acquisition of Android Devices: Using ADB, Busybox, Netcat
  - Physical Acquisition of Android Devices: Using Commercial Tools
  - Android Forensic Analysis: Using Commercial Tools
  - Physical Acquisition of iOS Devices: Using SSH, Netcat
  - Physical Acquisition of iOS Devices: Using Commercial Tools
  - iOS Forensic Analysis: Using Commercial Tools
- SQLite Database Extraction
  - SQLite Database Browsing Tools: Oxygen Forensics SQLite Viewer
  - SQLite Database Browsing Tools
- JTAG Forensics
- Chip-off Forensics
  - Chip-off Forensics Process
  - Chip-off Forensic Equipment
- Flasher Boxes

Lesson 9: Discuss Mobile Forensics Challenges and Prepare Investigation Report

- Challenges in Mobile Forensics
- Generate Investigation Report
- Mobile Forensics Report Template
- Sample Mobile Forensic Analysis Worksheet
- Cellebrite UFED Touch Sample Mobile Forensics Report Snapshot

CHFI: Computer Hacking Forensic Investigator

Course ID #: 1275-200-ZZ-W

Hours: 35

Module 16: IoT Forensics

Lesson 1: Understand IoT and IoT Security Problems

- What is IoT?
- IoT Architecture
- IoT Security Problems
- OWASP Top 10 IoT Vulnerabilities
- IoT Attack Surface Areas

Lesson 2: Recognize Different Types of IoT Threats

- IoT Threats
- DDoS Attack
  - Attack on HVAC Systems
  - Rolling Code Attack
  - BlueBorne Attack
  - Jamming Attack
  - Hacking Smart Grid/Industrial Devices: Remote Access Using Backdoor
  - Other IoT Attacks

Lesson 3: Understand IoT Forensics

- Introduction to IoT Forensics
- IoT Forensics Process
- Case Study: Default Passwords Aid Satori IoT Botnet Attacks
- IoT Forensics Challenges

Lesson 4: Perform Forensics on IoT Devices

- Wearable IoT Device: Smartwatch
  - Wearable IoT Device Forensics: Smartwatch
  - Steps Involved in Data Acquisition and Analysis of Android Wear
  - Logical Acquisition of Android Wear
  - Physical Acquisition of Android Wear
  - Forensic Examination of Evidence File: Android Wear
  - Recovered Forensic Artifacts: Android Wear
- IoT Device Forensics: Smart Speaker—Amazon Echo
  - Amazon Alexa Forensics: Client-based Analysis
  - Amazon Alexa Forensics: Cloud-based Analysis
  - List of Amazon Alexa APIs
- Hardware Level Analysis: JTAG and Chip-off Forensics