

EC Council Computer Hacking Forensic Investigator

Learn via: **Classroom/Virtual**

Duration: **5 Days**

Overview

Digital forensic practices stem from forensic science, the science of collecting and examining evidence or materials. Digital or computer forensics focuses on the digital domain including computer forensics, network forensics, and mobile forensics. As the cyber security profession evolves, organizations are learning the importance of employing digital forensic practices into their everyday activities. Computer forensic practices can help investigate attacks, system anomalies, or even help System administrators detect a problem by defining what is normal functional specifications and validating system information for irregular behaviors.

In the event of a cyber-attack or incident, it is critical investigations be carried out in a manner that is forensically sound to preserve evidence in the event of a breach of the law. Far too many cyber-attacks are occurring across the globe where laws are clearly broken and due to improper or non-existent forensic investigations, the cyber criminals go either unidentified, undetected, or are simply not prosecuted.

Cyber Security professionals who acquire a firm grasp on the principles of digital forensics can become invaluable members of Incident Handling and Incident response teams. The Computer Hacking Forensic Investigator course provides a strong baseline knowledge of key concepts and practices in the digital forensic domains relevant to today's organizations. CHFI provides its attendees a firm grasp on the domains of digital forensics.

Target Audience

The CHFI program is designed for all IT professionals involved with information system security, computer forensics, and incident response.

- Police and other law enforcement personnel
- Defense and Military personnel
- e-Business Security professionals
- Systems administrators
- Legal professionals
- Banking, Insurance and other professionals
- Government agencies
- IT managers

'For the most up-to-date and enriched knowledge of digital forensics, I chose Computer Hacking Forensic Investigator (CHFI), and it certainly paid off well. The training content, video streaming, and the hands-on labs, every learning method incorporated in the program were very interactive. I adored the real-time practice sessions as they left me with impressive technical skills. Getting to learn and practice hundreds of investigation tools was another exciting part of the program.'

Reuben Osilaja, Sr Security Compliance Specialist at Accenture Federal Services

Prerequisites

- IT/forensics professionals with basic knowledge on IT/cyber security, computer forensics, and incident response
- Prior completion of CEH training would be an advantage

Outline

Module 01: Computer Forensics in Today's World

- Understanding Computer Forensics
- Why and When Do You Use Computer Forensics?
- Cyber Crime (Types of Computer Crimes)
- Case Study
- Challenges Cyber Crimes Present For Investigators
- Cyber Crime Investigation
 - Civil versus Criminal Investigation
 - Case Study: Criminal Case

- Case Study: Civil Case
- Administrative Investigation
- Case Study: Administrative Case
- Rules of Forensics Investigation
 - Enterprise Theory of Investigation (ETI)
- Understanding Digital Evidence
- Types of Digital Evidence
- Characteristics of Digital Evidence
- Role of Digital Evidence
 - Digital Forensics Challenges
- Sources of Potential Evidence
- Rules of Evidence
 - Best Evidence Rule
 - "Hearsay" concept
 - Federal Rules of Evidence
 - Scientific Working Group on Digital Evidence (SWGDE)
- Forensics Readiness
 - Forensics Readiness Planning
- Computer Forensics as part of an Incident Response Plan
- Need for Forensic Investigator
- Roles and Responsibilities of Forensics Investigator
- What makes a Good Computer Forensics Investigator?
- Investigative Challenges
 - Computer Forensics: Legal Issues
 - Computer Forensics: Privacy Issues
- Legal and Privacy Issues
- Code of Ethics
- Accessing Computer Forensics Resources

Module 02: Computer Forensics Investigation Process

- Importance of Computer Forensics Process
- Phases Involved in the Computer Forensics Investigation Process
- **Pre-investigation Phase**
 - Setting Up a Computer Forensics Lab
 - Planning and Budgeting
 - Physical Location and Structural Design Considerations
 - Work Area Considerations
 - Physical Security Recommendations
 - Fire-Suppression Systems
 - Evidence Locker Recommendations
 - Auditing the Security of a Forensics Lab
 - Human Resource Considerations
 - Build a Forensics Workstation
 - Basic Workstation Requirements in a Forensics Lab
 - Build a Computer Forensics Toolkit
 - Forensics Hardware
 - Forensics Software (Cont'd)
 - Build the Investigation Team
 - Forensic Practitioner Certification and Licensing
 - Review Policies and Laws
 - Forensics Laws
 - Establish Quality Assurance Processes
 - Quality Assurance Practices in Digital Forensics
 - General Quality Assurance in the Digital Forensic Process
 - Quality Assurance Practices: Laboratory Software and Hardware
 - Laboratory Accreditation Programs
 - Data Destruction Industry Standards
 - Risk Assessment
 - Risk Assessment Matrix
- **Investigation Phase**
 - **Investigation Process**
 - Questions to Ask When a Client Calls the Forensic Investigator
 - Checklist to Prepare for a Computer Forensics Investigation
 - Notify Decision Makers and Acquire Authorization
 - Computer Forensics Investigation Methodology: First Response
 - First Responder
 - Roles of First Responder
 - First Response Basics
 - Incident Response: Different Situations

- First Response by System Administrators
 - First Response by Non-Forensic Staff
 - First Response by Laboratory Forensic Staff
 - First Responder Common Mistakes
 - Documenting the Electronic Crime Scene
 - Photographing the Scene
 - Sketching the Scene
 - Note Taking Checklist
- Computer Forensics Investigation Methodology: Search and Seizure
 - Consent
 - Sample of Consent Search Form
 - Witness Signatures
 - Witness Statement Checklist
 - Conducting Preliminary Interviews
 - Planning the Search and Seizure
 - Initial Search of the Scene
 - Warrant for Search and Seizure
 - Obtain Search Warrant
 - Example of Search Warrant
 - Searches Without a Warrant
 - Health and Safety Issues
 - Securing and Evaluating Electronic Crime Scene: A Checklist
- Computer Forensics Investigation Methodology: Collect the Evidence
 - Collect Physical Evidence
 - Evidence Collection Form
 - Collecting and Preserving Electronic Evidence
 - Dealing with Powered On Computers
 - Dealing with Powered Off Computers
 - Dealing with Networked Computer
 - Dealing with Open Files and Startup Files
 - Operating System Shutdown Procedure
 - Computers and Servers
 - Preserving Electronic Evidence
 - Seizing Portable Computers
 - Dealing with Switched On Portable Computers
- Computer Forensics Investigation Methodology: Secure the Evidence
 - Evidence Management
 - Chain of Custody
 - Simple Format of the Chain of Custody Document
 - Chain of Custody Forms
 - Chain of Custody on Property Evidence Envelope/Bag and Sign-out Sheet
 - Packaging and Transporting Electronic Evidence
 - Evidence Bag Contents List
 - Packaging Electronic Evidence
 - Exhibit Numbering
 - Transporting Electronic Evidence
 - Storing Electronic Evidence
- Computer Forensics Investigation Methodology: Data Acquisition
 - Guidelines for Acquiring Evidence
 - Duplicate the Data (Imaging)
 - Verify Image Integrity
 - MD5 Hash Calculators: HashCalc, MD5 Calculator and HashMyFiles
 - Recover Lost or Deleted Data
 - Data Recovery Software
- Computer Forensics Investigation Methodology: Data Analysis
 - Data Analysis
- **Post-investigation Phase**
 - Computer Forensics Investigation Methodology: Evidence Assessment
 - Evidence Assessment
 - Case Assessment
 - Processing Location Assessment
 - Collecting Evidence from Social Networks
 - Best Practices on how to Behave as an Investigator on Social Media
 - Best Practices to Assess the Evidence
 - Computer Forensics Investigation Methodology: Documentation and Reporting
 - Documentation in Each Phase
 - Gather and Organize Information
 - Writing the Investigation Report
 - Computer Forensics Investigation Methodology: Testify as an Expert Witness
 - Expert Witness
 - Testifying in the Court Room

- Closing the Case
- Maintaining Professional Conduct

Module 03: Understanding Hard Disks and File Systems

- Hard Disk Drive Overview
 - Disk Drive Overview
 - Hard Disk Drive (HDD)
 - Solid-State Drive (SSD)
 - Physical Structure of a Hard Disk
 - Logical Structure of Hard Disk
 - Types of Hard Disk Interfaces
 - Hard Disk Interfaces
 - ATA
 - SCSI
 - IDE/EIDE
 - USB
 - Fibre Channel
 - Tracks
 - Track Numbering
 - Sector
 - Sector Addressing
 - Advanced Format: Sectors
 - Cluster
 - Cluster Size
 - Slack Space
 - Lost Clusters
 - Bad Sectors
 - Understanding Bit, Byte, and Nibble
 - Hard Disk Data Addressing
 - Data Densities on a Hard Disk
 - Disk Capacity Calculation
 - Measuring the Performance of the Hard Disk
- Disk Partitions and Boot Process
 - Disk Partitions
 - BIOS Parameter Block (BPB) Partitioning utilities
 - Master Boot Record
 - Structure of a Master Boot Record
 - Globally Unique Identifier (GUID)
 - GUID Partition Table (GPT)
 - What is the Booting Process?
 - Essential Windows System Files
 - Windows Boot Process
 - Identifying GUID Partition Table (GPT)
 - Analyzing the GPT Header and Entries
 - GPT Artifacts
 - Macintosh Boot Process
 - Linux Boot Process
- Understanding File Systems
 - Understanding File Systems
 - Types of File 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
 - Setting the Compression State of a Volume
 - Encrypting File Systems (EFS)

- Components of EFS
 - EFS Attribute
 - Sparse Files
 - Linux File Systems
 - Linux File System Architecture
 - File System Hierarchy Standard (FHS)
 - Extensible File System (Ext)
 - Second Extensible File System (Ext2)
 - Third Extensible File System (Ext3)
 - Fourth Extensible File System (Ext4)
 - Mac OS X File Systems
 - HFS vs. HFS Plus
 - Hierarchical File System (HFS)
 - Hierarchical File System Plus (HFS+)
 - HFS Plus Volumes
 - HFS Plus Journal
 - Oracle Solaris 11 File System: ZFS
 - CD-ROM / DVD File System
 - Compact Disc File System (CDFS)
 - Virtual File System (VFS) and Universal Disk Format File System (UDF)
- RAID Storage System
 - Levels of RAID Storage System
 - Host Protected Areas (HPA) and Device Configuration Overlays (DCO)
- File System Analysis
 - File Carving
 - Image File Analysis: JPEG
 - Image File Analysis: BMP
 - Hex View of Popular Image File Formats
 - PDF File Analysis
 - Word File Analysis
 - PPT File Analysis
 - Excel File Analysis
 - Hex View of Other Popular File Formats
 - Video
 - Audio
 - 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

Module 04: Data Acquisition and Duplication

- Data Acquisition and Duplication Concepts
 - Understanding Data Acquisition
 - Types of Data Acquisition Systems
 - Live Data Acquisition
 - Order of Volatility
 - Common Mistakes in Volatile Data Collection
 - Volatile Data Collection Methodology
- Static Acquisition
 - Static Data Acquisition
 - Rules of Thumb
 - Why to Create a Duplicate Image?
 - Bit Stream Image Vs. Backups
 - Issues with Data Duplication
 - Data Acquisition and Duplication Steps
 - Prepare a Chain of Custody Document
 - Enable Write Protection on the Evidence Media
 - Sanitize the Target Media: NIST SP 800-88 Guidelines
 - Determine the Data Acquisition Format
 - Data Acquisition Methods
 - Determine the Best Acquisition Method
 - Select the Data Acquisition Tool
 - Mandatory Requirements
 - Optional Requirements
 - Data Acquisition and Duplication Tools: Hardware
 - Data Acquisition and Duplication Tools: Software
 - Linux Standard Tools
 - Acquiring Data on Linux: dd Command

- Acquiring Data on Linux: dcfldd Command
- Acquiring Data on Windows: AccessData FTK Imager
- Acquiring RAID Disks
- Remote Data Acquisition
- Data Acquisition Mistakes
- Plan for Contingency
- Validate Data Acquisitions
 - Linux Validation Methods
 - Windows Validation Methods
- Acquisition Best Practices

Module 05: Defeating Anti-forensics Techniques

- What is Anti-Forensics?
 - Goals of Anti-Forensics
- Anti-Forensics techniques
 - Data/File Deletion
 - What Happens When a File is Deleted in Windows?
 - Recycle Bin in Windows
 - Storage Locations of Recycle Bin in FAT and NTFS Systems
 - How the Recycle Bin Works
 - Damaged or Deleted INFO2 File
 - Damaged Files in Recycle Bin Folder
 - Damaged Recycle Bin Folder
 - File Recovery Tools: Windows
 - File Recovery in MAC OS X
 - File Recovery Tools: MAC
 - File Recovery in Linux
 - Recovering the Deleted Partitions
 - Partition Recovery Tools: Active@ Partition Recovery
 - Partition Recovery Tools (For Windows, MAC, & Linux all together)
 - Password Protection
 - Password Types
 - Password Cracker and its Working
 - Password Cracking Techniques
 - Default Passwords
 - Using Rainbow Tables to Crack Hashed Passwords
 - Tools to Create Rainbow Tables: rtgen and Winrtgen
 - Microsoft Authentication
 - How Hash Passwords Are Stored in Windows SAM?
 - System Software Password Cracking
 - Bypassing BIOS Passwords
 - Using Manufacturer's Backdoor Password to Access the BIOS
 - Using Password Cracking Software
 - CmosPwd
 - DaveGrohl
 - Resetting the CMOS using the Jumpers or Solder Beads
 - Removing CMOS Battery
 - Overloading the Keyboard Buffer and Using a Professional Service
 - Tool to Reset Admin Password
 - Active@ Password Changer
 - Windows Password Recovery Bootdisk
 - Windows Password Recovery Lastic
 - Application Password Cracking Tools
 - Word Password Recovery Tools
 - PowerPoint Password Recovery Tools
 - Excel Password Recovery Tools
 - PDF Password Recovery Tools
 - ZIP/RAR Password Recovery Tool: Advanced Archive Password Recovery
 - Other Application Software Password Cracking Tools
 - Other Password Cracking Tools
 - Steganography
 - Steganography
 - Steganography
 - Types of Steganography based on Cover Medium
 - Steganalysis
 - Steganalysis
 - Steganalysis Methods/Attacks on Steganography
 - Detecting Steganography
 - Steganography Detection Tool: Gargoyle Investigator™ Forensic Pro

- Steganography Detection Tools
- Data Hiding in File System Structures
- Trail Obfuscation
- Artifact Wiping
- Overwriting Data/Metadata
- Encryption
 - Encrypting File System (EFS): Recovery Certificate
 - Advanced EFS Data Recovery Tool
- Encrypted Network Protocols
- Program Packers
- Rootkits
 - Detecting Rootkits
 - Steps for Detecting Rootkits
- Minimize Footprint
- Exploiting Forensic Tools Bugs
- Detecting Forensic Tool Activities
- Anti-Forensics Countermeasures
- Anti-Forensics Challenges
- Anti-forensics Tools
 - Privacy Eraser
 - Azazel Rootkit
 - QuickCrypto
- Anti-forensics Tools

Module 06: Operating System Forensics (Windows, Mac, Linux)

Introduction to OS Forensics

Windows Forensics

- Collecting Volatile Information
 - Volatile Information
 - System Time
 - Logged-On Users
 - PsLoggedOn Tool
 - net sessions Command
 - LogonSessions Tool
 - Open Files
 - net file Command
 - PsFile Utility
 - Openfiles Command
 - Network Information
 - Network Connections
 - Process Information
 - Process-to-Port Mapping
 - Process Memory
 - Network Status
 - Print spool files
 - Other Important Information
- Collecting Non-Volatile Information
 - Non-Volatile Information
 - Examine File Systems
 - Registry Settings
 - Microsoft Security ID
 - Event Logs
 - ESE Database File
 - Connected Devices
 - Slack Space
 - Virtual Memory
 - Swap Space, hibernation, and Page Files
 - Windows Search Index
 - Collecting Hidden Partition Information
 - Hidden ADS Streams
 - Investigating ADS Streams: StreamArmor
 - Other Non-Volatile Information
- Analyze the Windows thumbcaches
- Windows Memory Analysis
 - Virtual Hard Disk (VHD)
 - Memory Dump
 - EProcess Structure
 - Process Creation Mechanism
 - Parsing Memory Contents

- Parsing Process Memory
- Extracting the Process Image
- Collecting Process Memory
- Windows Registry Analysis
 - Inside the Registry
 - Registry Structure within a Hive File
 - The Registry as a Log File
 - Registry Analysis
 - System Information
 - TimeZone Information
 - Shares
 - Wireless SSIDs
 - Startup Locations
 - Importance of volume shadow copy services
 - System Boot
 - User Login
 - User Activity
 - Enumerating Autostart Registry Locations
 - 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
- Cache, Cookie, and History Analysis
 - 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: ChromeCookiesView
 - Analysis Tool: ChromeCacheView
 - Analysis Tool: ChromeHistoryView
 - Cache, Cookie, and History Analysis: Microsoft Edge
 - Analysis Tool: IECookiesView
 - Analysis Tool: IECacheView
 - Analysis Tool: BrowsingHistoryView
- Windows File Analysis
 - System Restore Points (Rp.log Files)
 - System Restore Points (Change.log.x Files)
 - Prefetch Files
 - Shortcut Files
 - Image Files
- Metadata Investigation
 - Understanding Metadata
 - Types of Metadata
 - Metadata in Different File Systems
 - Metadata in PDF Files
 - Metadata in Word Documents
 - Tool: Metashield Analyzer
- Text Based 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
- Other Audit Events
 - Evaluating Account Management Events
 - Examining System Log Entries
 - Examining Application Log Entries
- Forensic Analysis of Event Logs
 - Searching with Event Viewer
 - Using Event Log explorer to Examine Windows Log Files
 - Windows Event Log Files Internals
- Windows Forensics Tools

- Shell Commands
- Linux Log files
- Collecting Volatile Data
- Collecting Non-Volatile Data

MAC Forensics

- Introduction to MAC Forensics
- MAC Forensics Data
- MAC Log Files
- MAC Directories
- MAC Forensics Tools

Module 07: Network Forensics

- Introduction to Network Forensics
 - Network Forensics
 - Postmortem and Real-Time Analysis
 - Network Vulnerabilities
 - Network Attacks
 - Where to Look for Evidence
- Fundamental Logging Concepts
 - Log Files as Evidence
 - Laws and Regulations
 - Legality of using Logs
 - Records of Regularly Conducted Activity as Evidence
- Event Correlation Concepts
 - Event Correlation
 - Types of Event Correlation
 - Prerequisites of Event Correlation
 - Event Correlation Approaches
- Network Forensic Readiness
 - Ensuring Log File Accuracy
 - Log Everything
 - Keeping Time
 - Why Synchronize Computer Times?
 - What is Network Time Protocol (NTP)?
 - Use Multiple Sensors
 - Avoid Missing Logs
 - Implement Log Management
 - Functions of Log Management Infrastructure
 - Challenges in Log Management
 - Meeting the Challenges in Log Management
 - Centralized Logging
 - Syslog
 - IIS Centralized Binary Logging
 - Ensure System's Integrity
 - Control Access to Logs
- Network Forensics Steps
 - Ensure Log File Authenticity
 - Use Signatures, Encryption, and Checksums
 - Work with Copies
 - Maintain Chain of Custody
 - Condensing Log File
 - Analyze Logs
 - Network Forensics Analysis Mechanism
 - Log Capturing and Analysis Tools: GFI EventsManager
 - Log Capturing and Analysis Tools: EventLog Analyzer
 - Log Capturing and Analysis Tools
 - Analyzing Router Logs
 - Evidence Gathering from ARP Table
 - Analyzing Router Logs (Cont'd)
 - Analyzing Router Logs: Cisco
 - Analyzing Router Logs: Juniper
 - Analyzing Firewall Logs
 - Analyzing Firewall Logs: Cisco
 - Analyzing Firewall Logs: Checkpoint
 - Analyzing IDS Logs
 - Analyzing IDS Logs: Juniper
 - Analyzing IDS Logs: Checkpoint

- Analyzing Honeypot Logs
 - DHCP Logging
 - Sample DHCP Audit Log File
 - Evidence Gathering at the Data-Link Layer: DHCP Database
 - ODBC Logging
- Network Traffic Investigation
 - Why Investigate Network Traffic
 - Evidence Gathering via Sniffing
 - Sniffing Tool: Wireshark
 - Display Filters in Wireshark
 - Additional Wireshark Filters
 - Sniffing Tool: SteelCentral Packet Analyzer
 - Sniffing Tool: Tcpdump/Windump
 - Packet Sniffing Tool: Capsa Network Analyzer
 - Network Packet Analyzer: OmniPeek Network Analyzer
 - Network Packet Analyzer: Observer
 - Network Packet Analyzer: Capsa Portable Network Analyzer
 - TCP/IP Packet Crafter: Colasoft Packet Builder
 - Network Packet Analyzer: RSA NetWitness Investigator
 - Additional Sniffing Tools
 - Gathering Evidence from an IDS
- Documenting the Evidence
- Evidence Reconstruction

Module 08: Investigating Web Attacks

- Introduction to Web Application Forensics
 - Introduction to Web Application Forensics
 - Web Application Architecture
 - Challenges in Web Application Forensics
- Web Attack Investigation
 - Indications of a Web Attack
 - Web Application Threats - 1
 - Web Application Threats - 2
 - Investigating a Web Attack
 - Investigating Web Attacks in Windows-Based Servers
- Investigating Web Server Logs
 - Internet Information Services (IIS) Logs
 - IIS Web Server Architecture
 - IIS Logs
 - Investigating IIS Logs
 - Maintaining Credible IIS Log Files
 - Investigating IIS Logs: Best Practices
 - UTC Time
 - Investigating Apache Logs
 - Apache Web Server Architecture
 - Apache Web Server Logs
 - Investigating Apache Logs
 - Investigating Cross-Site Scripting (XSS)
 - Investigating XSS: Using Regex to Search XSS Strings
 - Investigating SQL Injection Attacks
 - Pen-Testing CSRF Validation Fields
 - Investigating Code Injection Attack
 - Investigating Cookie Poisoning Attack
- Web Attack Detection Tools
 - Web Log Viewers
- Tools for Locating IP Address
 - IP Address Locating Tools
- WHOIS Lookup Tools

Module 09: Database Forensics

- Database Forensics and Its Importance
- MSSQL Forensics
 - Data Storage in SQL Server
 - Database Evidence Repositories
 - Collecting Volatile Database Data
 - Collecting Primary Data File and Active Transaction Logs Using SQLCMD

- Collecting Primary Data File & 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
- Database Forensics Using SQL Server Management Studio
- Database Forensics Using ApexSQL DBA
- MySQL Forensics
 - Internal Architecture of MySQL
 - Structure of the Data Directory
 - MySQL Forensics
 - Viewing the Information Schema
 - MySQL Utility Programs For Forensic Analysis
 - Common Scenario for Reference
 - MySQL Forensics for WordPress Website Database: Scenario 1
 - Collect the Evidences
 - Examine the Log Files
 - Analyze the General Log
 - Take a Backup of the Database
 - Create an Evidence Database
 - Select the Database
 - View the Tables in the Database
 - View the Users in the Databases
 - View Columns in the Table
 - Collect the 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 .frm Files
 - Examine the Binary Logs
 - Retrieve the Deleted User Account
 - ibdata1 in Data Directory

Module 10: Cloud Forensics

- Introduction to Cloud Computing
 - Types of Cloud Computing Services
 - Separation of Responsibilities in Cloud
 - Cloud Deployment Models
 - Cloud Computing Threats
 - Cloud Computing Attacks
- Cloud Forensics
 - Usage of Cloud Forensics
 - Cloud Crimes
 - Case Study: Cloud as a Subject
 - Case Study: Cloud as the Object
 - Case Study: Cloud as a Tool
 - Cloud Forensics: Stakeholders and their Roles
 - Cloud Forensics Challenges
 - Architecture and Identification
 - Data Collection
 - Legal
 - Analysis
 - Cloud Forensics Challenges
 - Investigating Cloud Storage Services
 - Investigating Dropbox Cloud Storage Service
 - Artifacts Left by Dropbox Web Portal
 - Artifacts Left by Dropbox Client on Windows
 - Investigating Google Drive Cloud Storage Service
 - Artifacts Left by Google Drive Web Portal
 - Artifacts Left by Google Drive Client on Windows
 - Cloud Forensics Tools: UFED Cloud Analyzer

Module 11: Malware Forensics

- Introduction to Malware
 - Different Ways a Malware can Get into a System

- Common Techniques Attackers Use to Distribute Malware on the Web
- Components of Malware
- Introduction to Malware Forensics
 - Why Analyze Malware
 - 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
 - Malware Analysis: Static
 - Static Malware Analysis: File Fingerprinting
 - Online Malware Testing: VirusTotal
 - Online Malware Analysis Services
 - Local and Online Malware Scanning
 - Performing Strings Search
 - Identifying Packing/Obfuscation Methods
 - Finding the Portable Executables (PE) Information
 - Identifying File Dependencies
 - Malware Disassembly
 - Malware Analysis Tool: IDA Pro
 - Malware Analysis: Dynamic
 - Installation Monitor
 - Process Monitor
 - Process Monitoring Tool: What's Running
 - Process Monitoring Tools
 - Files and Folder Monitor
 - Files and Folder Integrity Checkers: FastSum and WinMD5
 - Files and Folder Integrity Checkers
 - Registry Monitor
 - Registry Entry Monitoring Tool: RegScanner
 - Registry Entry Monitoring Tools
 - Network Activity Monitor
 - Detecting Trojans and Worms with Capsa Network Analyzer
 - Port Monitor
 - Port Monitoring Tools: TCPView and CurrPorts
 - DNS Monitoring/Resolution
 - API Calls Monitor
 - Device Drivers Monitor
 - Device Drivers Monitoring Tool: DriverView
 - Device Drivers Monitoring Tools
 - Startup Programs Monitor
 - Windows 10 Startup Registry Entries
 - Startup Programs Monitoring Tool: Security AutoRun
 - Startup Programs Monitoring Tools
 - Windows Services Monitor
 - Windows Service Manager (SrvMan)
 - Windows Services Monitoring Tools
 - Analysis of Malicious Documents
 - Malware Analysis Challenges

Module 12: Investigating Email Crimes

- Email System
 - Email Clients
 - Email Server
 - SMTP Server
 - POP3 Server
 - IMAP Server
 - Importance of Electronic Records Management
- Email Crimes (Email Spamming, Mail Bombing/Mail Storm, Phishing, Email Spoofing, Crime via Chat Room, Identity Fraud/Chain Letter)
 - Crime Via Chat Room
- Email Message
 - Sample of Email Header
 - List of Common Headers
 - List of Common X-Headers
- Steps to Investigate Email Crimes and Violation
 - Obtain a Search Warrant and Seize the Computer and Email Account
 - Examine E-mail Messages
 - Copy and Print the E-mail Message

- Viewing Email Headers in Microsoft Outlook
- Viewing Email Headers in Microsoft Outlook.com
- Viewing Email Headers in AOL
- Viewing Email Headers in Apple Mail
- Viewing Email Headers in Gmail
- Viewing Headers in Yahoo Mail
- Received Headers
- Analyzing Email Headers
- Examining Additional Files (.pst or .ost files)
- Checking the E-mail Validity
- Examine the Originating IP Address
- Trace the E-mail Origin
- Validating Header Information
- Tracing Back Web-based E-mail
- Acquire Email Archives
 - Email Archives
 - Content of Email Archives
 - Local Archive
 - Server Storage Archive
 - Forensic Acquisition of Email Archive
- Recover Deleted Emails
 - Deleted Email Recovery
- Examining Email Logs
 - Examining Linux E-mail Server Logs
 - Examining Microsoft Exchange E-mail Server Logs
 - Examining Novel Group-wise E-mail Server Logs
- Email Forensics Tools
 - Recover My Email
 - MailXaminer
 - Email Forensics Tools
- Laws and Acts against Email Crimes
 - U.S. Laws Against Email Crime: CAN-SPAM Act

Module 13: Mobile Phone Forensics

- Mobile Device Forensics
 - Why Mobile Forensics?
 - Top Threats Targeting Mobile Devices
 - Mobile Hardware and Forensics
 - Mobile OS and Forensics
 - 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
 - Mobile Storage and Evidence Locations
 - What Should You Do Before the Investigation?
 - Build a Forensics Workstation
 - Build the Investigation Team
 - Review Policies and Laws
 - Notify Decision Makers and Acquire Authorization
 - Risk Assessment
 - Build a Mobile forensics Toolkit
 - Mobile Phone Evidence Analysis
 - Mobile Forensics Process
 - Collecting the Evidence
 - Document the Scene
 - Document the Evidence
 - Evidence Preservation
 - Set of Rules for Switching ON/OFF Mobile Phone
 - Mobile Phone Signal Containment
 - Packing, Transporting, and Storing the Evidence
 - Forensics Imaging
 - Forensics Imaging of Android Device Using FTK Imager
 - Creating Disk Image of an iPhone Using SSH
 - Phone Locking
 - Bypassing Android Phone Lock Password Using ADB
 - iPhone Passcodes
 - Bypassing the iPhone Passcode Using IExplorer
 - Enabling USB Debugging
 - Platform Security Removal Techniques: Jailbreaking/Rooting

- Mobile Evidence Acquisition
 - Data Acquisition Methods
- Cellular Network
 - Components of Cellular Network
 - Different Cellular Networks
 - Cell Site Analysis: Analyzing Service Provider Data
 - CDR Contents
 - Sample CDR Log File
- Subscriber Identity Module (SIM)
 - SIM File System
 - Data Stored in a Subscriber Identity Module
 - Integrated Circuit Card Identification (ICCID)
 - International Mobile Equipment Identifier (IMEI)
 - Electronic Serial Number (ESN)
 - SIM Cloning
 - SIM Data Acquisition Tools
 - SIM Forensic Analysis Tools
- Logical Acquisition
 - Android Logical Acquisition Using MOBILedit
 - Additional Logical Acquisition Tools
- Physical Acquisition
 - Physical Acquisition Using Oxygen Forensic Suite
- File System Acquisition
 - File System Acquisition Using Oxygen Forensic Suite
- File Carving
 - File Carving Using Forensic Explorer
 - iPhone File Carving Using Scalpel Tool
 - File Carving Tools
- SQLite Database Extraction
 - Forensics Analysis of SQLite Database Using Andriller
 - SQLite Database Browsing Tools: Oxygen Forensics SQLite Viewer
 - SQLite Database Browsing Tools
- Android Forensics Analysis
- iPhone Data Extraction
 - iPhone Data Acquisition Tools
 - iPhone Forensics Analysis Using the Oxygen Forensics Suite
- Examination and Analysis
- Generating Investigation Report
- Mobile Forensics Report Template
 - Sample Mobile Forensics Analysis Worksheet
 - Cellebrite UFED Touch Sample Mobile Forensic Report Snapshot

Module 14: Forensics Report Writing and Presentation

- Writing Investigation Reports
 - Forensic Investigation Report
 - Important Aspects of a Good Report
 - Forensic Investigation Report Template
 - Report Classification
 - Guidelines for Writing a Report
 - Other Guidelines for Writing a Report
- Expert Witness Testimony
 - What is an Expert Witness?
 - Roles of an Expert Witness
 - Technical Witness Vs. Expert Witness
 - Daubert Standard
 - Frye Standard
 - What Makes a Good Expert Witness?
 - Importance of Curriculum Vitae
 - Professional Code of Conduct for an Expert Witness
 - Preparing for a Testimony
 - Testifying in the Court
 - General Order of Trial Proceedings
 - General Ethics While Testifying
 - Importance of Graphics in a Testimony
 - Helping your Attorney
 - Avoiding Testimony Issues
 - Testifying during Direct Examination
 - Testifying during Cross- Examination
 - Testifying during Cross- Examination: Best Practices

- Deposition
 - Guidelines to Testify at a Deposition
- Dealing with Media