EC-Council

Building A Culture Of Security

C|HFI

Computer Hacking Forensic INVESTIGATOR

Computer Hacking Forensic Investigator v11

COURSE OUTLINE

EC-Council Official Curricula

Computer Hacking Forensic Investigator

Course Outline

(Version 11)

Module 01: Computer Forensics in Today's World

Understand the Fundamentals of Computer Forensics

- Understanding Computer Forensics
  - Why and When Do You Use Computer Forensics?
- Scope of Computer Forensics

Understand Cybercrimes and their Investigation Procedures

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

Understand Digital Evidence and eDiscovery

- 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)
- The Association of Chief Police Officers (ACPO) (inherited into NPCC) Principles of Digital Evidence
- Computer Forensics vs. eDiscovery
- Legal and IT Team Considerations for eDiscovery
- Best Practices for Handling Digital Evidence

Understand Forensic Readiness

- Forensic Readiness
- Forensic Readiness and Business Continuity
- Forensics Readiness Planning
- Forensic Readiness Procedures
  - Forensic Policy
  - Forensics in the Information System Life Cycle
  - Creating an Investigation Team
  - Maintaining an Inventory
  - Host Monitoring
  - Network Monitoring

Understand the Role of Various Processes and Technologies in Computer Forensics

- Computer Forensics as a part of Incident Response Plan
  - Overview of Incident Response Process Flow
- Role of Computer Forensics in SOC Operations
- Role of Threat Intelligence in Computer Forensics
- Role of Artificial Intelligence in Computer Forensics
- Forensics Automation and Orchestration

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
- Managing Clients or Employers during Investigations
- Accessing Computer Forensics Resources

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

Understand Various Standards and Best Practices Related to Computer Forensics

- ISO Standards
  - ISO/IEC 27037
  - ISO/IEC 27041
  - ISO/IEC 27042
  - ISO/IEC 27043
  - ISO/IEC 27050
- ENFSI Best Practices for Forensic Examination of Digital Technology

Understand Laws and Legal Compliance in Computer Forensics

- Role of Local/International Agencies during Cybercrime Investigation
- Computer Forensics and Legal Compliance
- Other Laws Relevant to Computer Forensics

Module 02: Computer Forensics Investigation Process

Understand the Forensic Investigation Process and its Importance

- Importance of Computer Forensic Investigation Process
- Phases Involved in the Computer Forensics Investigation Process

Understand First Response

- First Response
- First Responder
- Roles of First Responder
- First Response Basics
- First Response: Different Situations
  - First Response by Non-forensic Staff
  - First Response by System/Network Administrators
  - First Response by Laboratory Forensics Staff

- First Responder Common Mistakes
- Health and Safety Issues

Understand the Pre-investigation Phase

- Setting Up a Computer Forensics Lab
- Building the Investigation Team
- Understanding Hardware and Software Requirements of Forensics Lab
- Validating Laboratory Software and Hardware
- Ensuring Quality Assurance
- Building Security Content, Scripts, Tools, or Methods to Enhance Forensic Processes

Understand the Investigation Phase

- Documenting the Electronic Crime Scene
  - Photographing and Sketching the Scene
- Search and Seizure
  - Search and Seizure Process Flow
  - Planning Search and Seizure
  - Seeking Consent
  - Obtaining Witness Signatures
  - Obtaining Warrant for Search and Seizure
    - Examples of a Search Warrant
  - Search Without Warrant
  - Collecting Incident Information
  - Initial Search of the Scene
  - Securing and Evaluating Crime Scene
  - Seizing Evidence at Crime Scene
  - Collecting Evidence
  - 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
  - Collecting Evidence from Social Networks

- Evidence Preservation
  - Chain of Custody
  - Simple Format of 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 Location for Evidence Examination
  - Transporting and Storing Evidence
- Data Acquisition
  - Duplicating the Data (Imaging)
- Data Analysis
- Case Analysis
  - Evidence Reconstruction

Understand the Post-investigation Phase

- Reporting
  - Audience of the Computer Forensic Report
  - Gathering and Organizing Information
  - Writing the Investigation Report
  - Forensic Investigation Report Template
  - Guidelines for Writing a Report
  - Visual Aids and Presentation Techniques in a Digital Forensic Report
  - Mock Case Presentations and Critiques
  - Data Visualization and Report Generation Tools
- Testifying as an Expert Witness
  - Who is an Expert Witness?
  - Roles of an Expert Witness
  - What Makes a Good Expert Witness?
  - Testifying in Court
  - General Ethics while Testifying

Module 03: Understanding Hard Disks and File Systems

Describe Different Types of Disk Drives and their Characteristics

- Understanding Hard Disk Drive
  - Tracks
  - Sectors
  - 4K Sectors
  - Data Density on a Hard Disk
  - Logical Block Addressing (LBA) and Disk Capacity Calculation
  - Measuring the Hard Disk Performance
- Understanding Solid-State Drive (SSD)
- Disk Interfaces
  - Serial ATA/SATA (AHCI)
    - mSATA III, SATA III
  - SCSI
  - Serial Attached SCSI
  - PCIe
  - NVMe

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)

Understand the Booting Process of Windows, Linux, and macOS Operating Systems

- What is the Booting Process?
- Essential Windows System Files and Components

- 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
- macOS Boot Process
- Linux Boot Process

Understand Various File Systems of Windows, Linux and macOS 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
  - exFAT
  - 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
    - NTFS Journals
      - Extracting information from USN Journal
    - Encrypting File Systems (EFS)
      - Components of EFS

- EFS Attribute
- Sparse Files

- Resilient File System (ReFS)

- Linux File Systems
  - Linux File System Architecture
  - Filesystem Hierarchy Standard (FHS)
  - Second Extended File System (ext2)
  - Third Extended File System (ext3)
  - Journaling File System
  - Fourth Extended File System (ext4)
  - Understanding Superblocks, Inodes, and Data Blocks
- macOS 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

Understand File System Analysis

- 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
  - The Sleuth Kit (TSK): img_stat
  - The Sleuth Kit (TSK): ffind
  - The Sleuth Kit (TSK): ils
- File System Timeline Creation and Analysis Using The Sleuth Kit (TSK)
  - MACB Timestamps
- NTFS Timestamp Rules in Windows and Linux
  - Windows NTFS Timestamp Rules

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)
- Network-Attached Storage (NAS)
- Storage Area Network (SAN)
- Differences between NAS and SAN

Understand Encoding Standards and Hex Editors

- Character Encoding Standards
  - ASCII
  - UNICODE
- OFFSET
- Understanding Hex Editors
- Understanding Hexadecimal Notation

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

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
  - Bitstream Image
    - Bitstream Disk-to-Image File
    - Bitstream Disk-to-Disk
- Determine Data Acquisition Format
  - Raw Format
  - Proprietary Format
  - Advanced Forensics Format (AFF)
  - Advanced Forensic Framework 4 (AFF4)

Understand eDiscovery

- eDiscovery
- Electronic Discovery Reference Model (EDRM) Cycle
- Monitor and Maintain Accurate Metrics and Detailed Tracking Information Related to eDiscovery
- eDiscovery Collection Methodologies
- Best Practices for eDiscovery
- eDiscovery Tools
  - Intella Pro
  - Logikcull
  - Nuix
  - Nextpoint
  - Relativity One
  - DISCO Ediscovery

Understand Data Acquisition Methodology

- Data Acquisition Methodology
- Step 1: Determine the Best Data Acquisition Method

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

Prepare an Image File for Examination

- Preparing an Image for Examination
  - Scenario 1: Examining Images on Linux Forensic Workstation
    - Scenario 1.1: Converting E01 Image File to dd Image File
    - Scenario 1.2: Converting E01 Image File to Raw Image File
    - Scenario 1.3: Converting dd Image File to VHDX File
    - Scenario 1.4: Examining a dd Image File
    - Scenario 1.5: Examining Physical Hard Disk
    - Scenario 1.6: Examining Mac APFS Image File
    - Scenario 1.7: Examining Disk Image Using PyTSK
  - Scenario 2: Examining Images on Windows Forensic Workstation
    - Examining Mac HFS+ Image File
  - Scenario 3: Examining Images on Mac Forensic Workstation
- Digital Forensic Imaging Tools
  - OSFClone

Module 05: Defeating Anti-forensics Techniques

Understand Anti-forensics Techniques

- What is Anti-forensics?
  - Anti-forensics Techniques
- Challenges to Forensics from Anti-forensics

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
  - Recycle Bin Forensics Using Python

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
  - SSD File Carving on Linux File System
  - File Recovery Tools: Linux
- File Carving on macOS
  - SSD File Carving on Apple File System
  - Recovering Deleted Files on Mac Machine
  - Recovering Deleted Files from USB on Mac Machine
  - File Recovery Tools: macOS
- Custom File Carving Signatures

- Recovering Deleted Partitions
  - Recovering Deleted Partitions: Using R-Studio
  - Partition Recovery Tools
  - Recovering ReFS Volumes Using ReFSUtil
  - RAID Recovery Tools

Explore Password Cracking/Bypassing Techniques

- Anti-forensics Technique: Password Protection
- Tools to Extract the Password Hashes
- 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 and Local User Password: PassFab 4WinKey
- Bypassing Windows User Password by Booting Live USB
- Application Password Cracking Tools

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

- Anti-forensics Technique: Steganography
  - Defeating Anti-forensics: Steganalysis

- Steganalysis Methods 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: Tools for Detecting Alternate Data Streams
- Anti-forensics Technique: Trail Obfuscation
- Defeating Anti-forensics Technique: Detecting File Extension Mismatch Using Autopsy

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 Elcomsoft Forensic Disk Decryptor

Detect Program Packers and Footprint Minimizing Techniques

- Anti-forensics Technique: Program Packers
  - Detecting and Unpacking Program Packers
    - Detecting Program Packers Using Detect it Easy (DiE)
    - Detecting Program Packers Using Exeinfo PE
    - Unpacking Program Packers Using Exeinfo PE
- Anti-forensics Techniques that Minimize Footprint
  - Defeating Anti-forensics Technique: Detecting USB Devices
- Anti-forensics Countermeasures

Module 06: Windows Forensics

Understand Windows Forensics

- Introduction to Windows Forensics
- Windows Forensics Methodology

Collect 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
  - Collecting Network Information
    - Collecting Information about Network Connections
    - Collecting Network Status
  - Process Information
  - Process-to-Port Mapping
  - Examining Process Memory
  - Examining Print Spool files
  - Collecting Clipboard Contents and Service/Driver Information
  - Collecting Command History and Locally Shared Resource Information

Collect Non-volatile Information

- Collecting Non-volatile Information
  - Examining File Systems
  - ESE Database File
    - Examining .edb Files Using ESEDatabaseView
  - Windows Search Index Analysis
  - Detecting Externally Connected Devices to the System
  - Slack Space
  - Collecting Hidden Partition Information
  - Collecting User Account Information
  - Extracting System Resource Usage Monitor (SRUM) Artifacts
  - Analyzing Windows Thumbnail Cache
  - Auditing Installed Applications

- Identifying System Updates

- Collecting Windows Domain Information
  - Collecting Information from Domain Controllers
- Examining Compressed Files
  - Analyzing ZIP Files in a Windows System
- Extracting Information from Sticky Notes Using Python

Perform Windows Memory Analysis

- Windows Memory Analysis
- Windows Crash Dump
- Collecting Process Memory
- Memory Forensics
  - Malware Analysis Using Redline
  - Malware Analysis Using Volatility Framework
  - Page File
    - Examining Pagefile Using Strings Command
  - Hibernate Files
  - Extracting Data from Hibernation Files Using Hibernation Recon
  - Advanced Memory Forensics Using MemProcFS
    - Remote Memory Analysis Using MemProcFS
  - Memory Analysis Tools
    - Velociraptor

Perform Windows Registry Analysis

- Windows Registry Analysis
  - Windows Registry
  - Windows Registry Data Types
  - Registry Structure within a Hive Files
  - Windows Registry: Forensic Analysis
  - Registry as Log File
  - Collecting System Information
  - Collecting Last Shutdown Time and Time Zone Information
  - Shares

- Wireless SSIDs
- Startup Locations
- Examining System Bootup and Enumerating Autostart Registry Locations
- Importance of Volume Shadow Copy Services
  - Accessing Historical Data from Volume Shadow Copies
- User Login
- Microsoft Security ID
- User Activity
- Registry Settings
- Registry Last Write Time
- Recovering Deleted Registry Keys
- USB Removable Storage Devices
  - Identifying Malicious HID USB Devices
- Mounted Devices
- Tracking User Activity
- UserAssist Keys
- MRU Lists
- Connecting to Other Systems
- Analyzing Restore Point Registry Settings
- Determining Startup Locations
- Analyzing Amcache and Shimcache
- Identifying Webcam and Microphone Usage by Illicit Applications

- Windows Registry Analysis Using Magnet AXIOM

Perform Electron Application Analysis

- Electron Application Forensics
  - Electron Application Architecture
  - Local Data storage for Electron
- Extracting Data from Microsoft Teams
- Extracting Data from WhatsApp
- Extracting Data from Skype

Perform Web Browser Forensics

- Web Browser Forensics
- Cache, Cookie, and History Analysis: Mozilla Firefox
  - SQLite Database Files Created by Mozilla Firefox
  - Examining Download History
  - Examining Form History
  - Examining Session Recovery Files
  - Examining Firefox Extensions
  - Examining Firefox Cross-device Synchronization Feature
  - Mozilla Firefox Analysis Tools
- Cache, Cookie, and History Analysis: Google Chrome
  - Examining URLs and Visits Tables
  - Examining History, Page Transition Types, and Preferences Files
  - Examining Web Data
  - Examining Shortcuts
  - Examining Network Action Predictor Databases
  - Examining Chrome Cache Files and Timestamps
  - Examining Download History
  - Examining Chrome Session Recovery
  - Examining Cross-device Chrome Synchronization
  - Google Chrome Analysis Tools
- Cache, Cookie, and History Analysis: Microsoft Edge
  - Examining Download History
  - Examining Session Recovery
  - Examining Microsoft Edge Collections
  - Examining Microsoft Edge Extensions
  - Examining Browser Data Synchronization
  - Examining Multiple User Profiles
  - Microsoft Edge Analysis Tools
- Recovering Private Browsing Data and Browser Artifacts
  - Recovering InPrivate Browser Data

- Mozilla Firefox Private Browsing
- Google Chrome Private Browsing
- Microsoft Edge Private Browsing

- Carving SQLite Database Files Using FTK® Imager
  - Extracting and Rebuilding Cached Web Pages Using FTK® Imager
  - Extracting and Analyzing Stored Browser Credentials Using FTK® Imager

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
  - Extracting Metadata from PDF Documents Using Python
  - Metadata in Word Documents
  - Extracting Metadata from Office Documents Using Python
  - Analyzing Zone.Identifier Streams
  - Metadata Analysis Tools

Understand ShellBags, LNK Files, and Jump Lists

- Windows ShellBags
  - Windows ShellBags: Forensic Analysis
  - Parsing ShellBags
- Analyzing LNK Files
  - Analyzing LNK files Using Belkasoft X
- Analyzing Jump Lists
  - Tools for Analyzing Jump Lists

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 11 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
  - Analyzing Microsoft Office Alert Logs
  - Examining Last Failed Login Attempts and Login Count
  - Auditing Windows Registry Using Security Audit Event
- Windows Forensics Tools
  - OSForensics
- Hashing it Out in PowerShell: Using Get-FileHash

Module 07: Linux and Mac Forensics

Collect Volatile Information in Linux

- Introduction to Linux Forensics
- Collecting Volatile Information
  - 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 Open Files
- Collecting Mounted File System Information
- Finding Loaded Kernel Modules
- Collecting User Events and Reading ELF Files
- Viewing Running Processes in the System
- Viewing Linux Services Using systemctl
- Collecting Swap Areas and Disk Partition Information
- Collecting Kernel Messages
- Collecting Volatile Information Using Freta
- Collecting Volatile Information Using Python

Collect Non-volatile Information in Linux

- Collecting Non-volatile Information
  - 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
  - Examining Cron Jobs for Linux
  - Performing Hash Calculations Using Python
  - Collecting System Reboot History Using Python
  - Viewing System Log Entries Using Python

Understand Linux Memory Forensics

- Linux Memory Forensics
  - Listing Open Files

- Collecting Bash Information
- Collecting System Information
- Collecting Kernel Memory Information
- Malware Analysis Using Volatility Framework

Understand Mac Forensics

- Introduction to Mac Forensics
- Mac Forensics Data
- Mac Log Files
- Mac Directories

Collect Volatile Information in Mac

- Collecting Volatile Information
  - Collecting System Date and Time
  - Collecting Process Information
  - Collecting Network information
  - Collecting Open Files
  - Collecting Clipboard Content Using Shell Script
  - Collecting Locally Shared Resource Information
  - Collecting Other Volatile Information
    - Collecting Loaded Kernel Modules
    - Collecting Logged-On Users
    - Collecting Command History

Collect Non-volatile Information in Mac

- Collecting Non-volatile Information
  - Collecting System Information and Configuration
  - Collecting Desktop Artifacts
  - Collecting Startup Files
  - Analyzing macOS Thumbnail Cache
  - Collecting User Home Folder and Activities Information
  - Identifying Last Accessed Files and Folders
  - Viewing Log Messages

Understand Mac Memory Forensics and Mac Forensics Tools

- Mac Memory Forensics
  - Collecting Swap Areas and Disk Partition Information
- APFS Analysis
- Parsing Metadata on Spotlight
- Mac Forensics Tools

Module 08: Network Forensics

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

Summarize Event Correlation Concepts

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

Identify Indicators of Compromise (IoCs) from Network Logs

- Log Files as Evidence
- Analyzing Firewall Logs
  - Analyzing Firewall Logs: Cisco
  - Analyzing Firewall Logs: Check Point
- Analyzing IDS Logs
  - Analyzing IDS Logs: OSSEC
  - Analyzing IDS Logs: Check Point
- Analyzing Honeypot Logs
- Analyzing Router Logs
  - Analyzing Router Logs: Cisco

- Analyzing Router Logs: Juniper
- Analyzing DHCP Logs
- Analyzing Cisco Switch Logs
- Analyzing VPN Logs
  - VPN Log Analysis Using Elastic Stack
- Analyzing SSH Logs
- Analyzing DNS Server Logs
- Network Log Analysis Tools
  - Security Onion
  - Logz.io

Investigate Network Traffic

- Why Investigate Network Traffic?
- Gathering Evidence via Sniffers
- Sniffing Tools
  - Tcpdump
  - Wireshark
  - Display Filters in Wireshark
  - Additional Wireshark Filters
- Analyze Traffic for TCP SYN Flood DoS Attack
- Analyze Traffic for SYN-FIN Flood DoS Attack
- Analyze Traffic for ICMP Flood Attack
- Analyze Traffic for UDP Flood Attack
- Analyze Traffic for HTTP Flood 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 for SMTP HELO Flood Attack
- Analyze Traffic to Detect Malware Activity
- Analyze Network Traffic through NetFlow

- Network Forensic Analysis Using Dshell
- Tools for Investigating Network Traffic
  - NetworkMiner
  - Arkime

Perform Incident Detection and Examination Using SIEM Tools

- Centralized Logging Using SIEM Solutions
- SIEM Solutions
  - Splunk Enterprise Security (ES)
  - IBM Security Qradar SIEM
- Examine Brute-force Attack
- 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)

Understand Wireless Network Forensics

- Introduction to Wireless Network Forensics
- Wireless Network Forensics Challenges and Risks
- Types of Wireless Evidence
- Wireless Network Forensics Process
  - Step 1: Discover Wireless Access Points
  - Step 2: Detect Rogue/Malicious Access Points
  - Step 3: Identify Active Connections
  - Step 4: Measure Signal Strength
  - Step 5: Connect to the Suspected Wireless Network
  - Step 6: Sniff and Analyze Packets

Detect and Investigate Wireless Network Attacks

- Detect Rogue Access Points
  - Wi-Fi Discovery Tools
- Detect Access Point MAC Address Spoofing Attempts

- Detect Misconfigured Access Points
- Detect Wi-Fi Jamming Attempts Using Wireshark
- Analyze Wireless Packet Captures
  - Examine Client Connections
  - Examine Deauthentication Attack
  - Examine Disassociation Attack
  - Decrypt and Analyze Encrypted Wi-Fi Traffic
- Analyze Wi-Fi Spectrum
- Analyze the Wireless Network Report
- Tools for Investigating Wireless Network Traffic

Module 09: Malware Forensics

Understand Malware Concepts

- Introduction to Malware
- Different Ways for Malware to Enter a System
- Common Techniques Attackers Use to Distribute Malware across Web
- Components of Malware

Understand Malware Forensics

- Introduction to Malware Forensics
- Why Analyze Malware?
- Malware Analysis Challenges
- Malware Forensic Artifacts
- Indicators of Malware
- Prominence of Setting Up a Controlled Malware Analysis Lab
- Preparing Testbed for Malware Analysis
- Malware Analysis Tools
- Documentation Before Analysis
- Types of Malware Analysis
- Static Malware Analysis
- Dynamic Malware Analysis
  - System Baselining
  - Host Integrity Monitoring

Perform Static Malware Analysis

- Static Malware Analysis: File Fingerprinting
  - File Fingerprinting Using Python
- Static Malware Analysis: Local and Online Malware Scanning
- Static Malware Analysis: Performing Strings Search
  - Performing Strings Search Using Python
- Static Malware Analysis: Identifying Packing/Obfuscation Methods
  - Identifying Packing/Obfuscation Method of ELF Malware
    - Detect It Easy (DIE)
- Static Malware Analysis: Finding the Portable Executables (PE) Information
  - Analyzing PE Files Using Python
- Static Malware Analysis: Identifying File Dependencies
  - Identifying File Dependencies Using Python
- Static Malware Analysis: Malware Disassembly
- Static Malware Analysis: Analyzing ELF Executable Files
- Static Malware Analysis: Analyzing Mach-O Executable Files

Analyzing Suspicious Documents

- Analyzing Suspicious MS Office Document
- Analyzing Suspicious MS Excel Document
- Analyzing Suspicious PDF Document
  - Analyzing Suspicious PDF Document Using YARA

Perform System Behavior Analysis

- System Behavior Analysis: Monitoring Registry Artifacts
  - Windows AutoStart Registry Keys
  - Analyzing Windows AutoStart Registry Keys
- System Behavior Analysis: Monitoring Processes
  - Analyzing Windows Processes Using Python
- System Behavior Analysis: Monitoring Windows Services
  - Analyzing Windows Services Using Python
- 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 Installation
- System Behavior Analysis: Monitoring System Calls
- System Behavior Analysis: Monitoring Scheduled Tasks
- System Behavior Analysis: Monitoring Files and Folders

Perform Network Behavior Analysis

- Network Behavior Analysis: Monitoring Network Activities
  - Monitoring IP Addresses
- Network Behavior Analysis: Monitoring Port
  - Examining Open Ports
  - Port Monitoring Tools
    - TCPView
- Network Behavior Analysis: Monitoring DNS
  - Examining DNS Entries
  - DNS Monitoring Tools
    - DNSQuerySniffer
- Network Behavior Analysis: Monitoring Browser Activity

Perform Ransomware Analysis

- Ransomware Analysis - BlackCat (ALPHV)
  - BlackCat (ALPHV) Malware Analysis
    - Initial Access
    - Discovery, Credential Access, and Privilege Escalation
    - Defense Evasion, Persistence, and Lateral Movement
    - Data Exfiltration and Covering Tracks
    - Encrypt and Create Ransom Note
  - BlackCat Toolkit Analysis

Module 10: Investigating Web Attacks

Understand Web Application Forensics

- Introduction to Web Application Forensics
- Challenges in Web Application Forensics
- Indicators of a Web Attack
- OWASP Top 10 Application Security Risks - 2021
- Web Application Threats
- Web Attack Investigation Methodology

Understand Internet Information Services (IIS) Logs

- IIS Web Server Architecture
- IIS Logs
- Analyzing IIS Logs
- Analyzing IIS HTTP Logs Using HttpLogBrowser
- IIS Log Analysis Tools

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
- Analyzing Apache Web Server Logs Using Python
- Apache Log Analysis Tools

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
  - Examining Web Server Logs for XSS Attack Using Python

- 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
  - Examining Web Server Logs for Path/Directory Traversal Attack Using Python
- Investigating Command Injection Attack
  - Examining Apache Logs for Command Injection Attack
  - Examining Web Server Logs for Command Injection Attack Using Python
- 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 11: Dark Web Forensics

Understand the Dark Web and Dark Web Forensics

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

Determine How to Identify the Traces of Tor Browser during Investigation

- Identifying Tor Browser Artifacts: Command Prompt
- Identifying Tor Browser Artifacts: Windows Registry
- Identifying Tor Browser Artifacts: Prefetch Files
- Identifying Tor Browser Artifacts: places.sqlite File

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

Module 12: Cloud Forensics

Understand Cloud Computing Concepts

- Introduction to Cloud Computing
- Types of Cloud Computing Services
- Separation of Responsibilities in Cloud
- OWASP Top 10 Cloud Security Risks
- Cloud Computing Threats
- Cloud Computing Attacks

Understand Cloud Forensics

- Introduction to Cloud Forensics
- Uses of Cloud Forensics
- Cyber Crime on Cloud Environment
- Cloud Forensics: Stakeholders and their Roles
- Cloud Forensics Challenges
    - Architecture and Identification
    - Data Collection
    - Logs
    - Analysis
    - Legal
    - Role Management
    - Standards

- Training
- Anti-forensics
- Incident First Responders

Understand Amazon Web Services (AWS) Fundamentals

- Introduction to Amazon Web Services
- Shared Responsibility Model for AWS
- Data Storage in AWS
  - AWS Cloud Storage Services
- Logs in AWS

Perform AWS Forensics

- 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
- Collecting Information Using AWS-CLI
- Investigating CloudWatch Logs
- Investigating S3 Server Access Logs
- Investigating AWS CloudTrail for IAM-based Incidents
- Investigating Amazon VPC Flow Logs Using AWS Management Console
- Analyzing AWS Security Incidents Using GuardDuty

Understand Microsoft Azure Fundamentals

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

Perform Microsoft Azure Forensics

- 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
- Analyzing Azure Monitor Logs
- Collecting and Analyzing Logs In Azure AD
- Investigating Security Incidents using Microsoft Azure Sentinel

Understand Google Cloud Fundamentals

- Introduction to Google Cloud
- Shared Responsibilities in Google Cloud
  - Google Kubernetes Engine (GKE) Shared Responsibility
- Data Storage in Google Cloud
  - Google Cloud Storage classes
  - Google Cloud Data Storage Services
- Logs in Google Cloud

Perform Google Cloud Forensics

- Forensic Acquisition of Persistent Disk Volumes in GCP: Methodology
  - Step 1: Create an Instant Snapshot of a Persistent Disk Volume
  - Step 2: View the Instant Snapshots for a Disk
  - Step 3: Copy an Instant Snapshot to a Different Location
  - Step 4: Delete an Instant Snapshot After Creating Long-term Snapshot
- Analyzing Google Workspace Logs
- Analyzing Log Data using Google Cloud Log Analytics
- Analyzing Google Cloud VPC Flow Logs
- Investigating Google Cloud Security Incidents
  - Analyzing Access Attempts from Anonymous Proxy

- Analyzing BigQuery Data Exfiltration
- Analyzing SSH Brute Force Attempts
- Analyzing Malware Incident
- Analyzing Persistent Anomalous IAM Grants

- Investigating Google Cloud Container Security Incidents
  - Analyzing Malicious Script Executed
  - Analyzing Reverse Shell
- Investigating Google Cloud VM-based Security Incidents
  - Analyzing Cryptocurrency Mining Hash Match
  - Analyzing Cryptocurrency Mining YARA Rule

Module 13: Email and Social Media Forensics

Understand Email Basics

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

Explain 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.live.com
- Retrieving Email Headers in AOL
- Retrieving Email Headers in Apple Mail
- Retrieving Email Headers in Gmail
- Retrieving Email Headers in Yahoo Mail

o Step 5: Analyzing Email Headers

- Analyzing Email Headers: X-Headers
- Analyzing Email Headers: Checking Email Authenticity
- Analyzing Email Headers: Examining the Originating IP Address
- Analyzing Email Headers: Tracing Email Origin
- Analyzing Email Headers: Tracing Back Web-based Email

o Step 6: Recovering Deleted Email Messages

- Recovering Deleted Email Messages from Outlook .pst Files Using Recover My eMail
- Recovering deleted Email Data from Thunderbird Using Thunderbird Forensics Wizard
- Recovering Deleted Emails from Gmail and Outlook
- Email Recovery Tools

Understand U.S. Laws Against Email Crime

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

Explain Social Media Forensics

- Introduction to Social Media Forensics
- Social Media Crimes
- Social Media Forensics Challenges
- Manually Collecting Data from Social Media Platforms
- Collecting Evidence from Social Media Platforms Using WebPreserver
- Extracting Footages from Social Media Platforms
- Tracking Social Media User Activities Using Social Searcher
- Constructing and Analyzing Social Network Graphs
- Social Media Forensics Tools

Module 14: Mobile Forensics

Understand Mobile Device Forensics

- Mobile Device Forensics
- OWASP Top 10 Mobile Risks - 2016
- Mobile Attacks
- Mobile Hardware and Forensics
- Mobile OS and Forensics
- Mobile Forensics Challenges

Understand Android and iOS Architecture, Boot Process, and File Systems

- Mobile Device Architecture
- Android OS Architecture
- Android Boot Process
- iOS Architecture
- iOS Boot Process
  - DFU Mode Booting
  - Booting iPhone in DFU Mode
  - Booting iPhone in Recovery Mode
- Android File System
- iOS File System

Understand Mobile Forensics Process

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

Investigate Cellular Network Data

- Components of Cellular Network
- Different Cellular Networks

- Cell Site Analysis: Analyzing Service Provider Data
- CDR Contents

Perform File System Acquisition

- 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

Understand Phone Locks, Rooting, and Jailbreaking of Mobile Devices

- Phone Locking on Android
  - Bypassing Locked Android Devices
- Phone Locking on iOS
- Rooting of Android Devices
  - Rooting Android Using KingoRoot
  - Accessing Root Files in Android
- Jailbreaking of iOS Devices
  - Risks of Jailbreaking
  - Jailbreaking Techniques
  - Jailbreaking iOS Using Hexxa Plus

Perform Logical Acquisition on Mobile Devices

- Logical Acquisition
  - Android Debug Bridge (ADB)
  - Logical Acquisition of Android Devices: Using “adb pull” Command
  - Logical Acquisition of Android Devices: Using Commercial Tools
  - Logical Acquisition of iOS Devices: Using Finder
  - Logical Acquisition of iOS Devices: Using Commercial Tools
- Extracting Data from Android Devices Using Magnet ACQUIRE
- Cloud Data Acquisition on Android and iOS Devices
- Cloud Data Acquisition: Using Commercial Tools

Perform Physical Acquisition on Mobile 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
  - Physical Acquisition of iOS Devices: Using SSH, Netcat
  - Physical Acquisition of iOS Devices: Using Commercial Tools
- SQLite Database Extraction
  - SQLite Database Browsing Tools
  - SQLite Forensics Using Belkasoft X
- JTAG Forensics
- Chip-off Forensics
  - Chip-off Forensics Process
  - Chip-off Forensic Equipment
- Flasher Boxes

Perform Android and iOS Forensic Analysis

- Static Analysis and Dynamic Analysis of Android Package Kit (APK)
- Android Logs
- Examining Android Logs Using Logcat
- Android Log Analysis Tools
- Collecting WhatsApp Artifacts from Android Devices
- Analyzing Android Chrome Artifacts
- Android Forensic Analysis: Using Commercial Tools
- Extracting iOS Signal Data Using Belkasoft Evidence Center
- Analyzing iOS Safari Artifacts
- Decrypting and Analyzing iOS Keychains
- iOS Forensic Analysis: Using Commercial Tools

Module 15: IoT Forensics

Understand IoT Concepts

- What is the IoT?

- IoT Architecture
- IoT Security Problems
- OWASP Top 10 IoT Threats
- OWASP IoT Attack Surface Areas
- IoT Attacks
  - DDoS Attack
  - Attack on HVAC Systems
  - Rolling Code Attack
  - BlueBorne Attack
  - Jamming Attack
  - Remote Access Using Backdoor
  - Other IoT Attacks

Perform Forensics on IoT Devices

- Introduction to IoT Forensics
- IoT Forensics Process
- IoT Forensics Challenges
- 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
  - Forensic Data Extraction of Apple Watch
- IoT Device Forensics: Smart Speaker—Amazon Echo
  - Amazon Alexa Forensics: Client-based Analysis
  - Amazon Alexa Forensics: Cloud-based Analysis
- Hardware Level Analysis: JTAG and Chip-off Forensics
- Extracting and Analyzing Data from Drone/UAVs
- IoT Forensics Tools