Digital Forensics Essentials

(Version 1)

Course Outline

Module 01: Computer Forensics Fundamentals

- **Understand the Fundamentals of Computer Forensics**
  - Understanding Computer Forensics
  - Objectives of Computer Forensics
  - Need for Computer Forensics
  - When Do You Use Computer Forensics?
  - Types of Cybercrimes
    - Examples of Cybercrimes
  - Impact of Cybercrimes at the Organizational Level
- **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

- **Understand Forensic Readiness**
  - Forensic Readiness
  - Forensic Readiness and Business Continuity
  - Forensics Readiness Planning
- **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?
- **Understand Legal Compliance in Computer Forensics**
  - 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**
  - Forensic Investigation Process
  - Importance of the Forensic Investigation Process
  - Phases Involved in the Forensics Investigation Process
- **Forensic Investigation Process - Pre-investigation Phase**
  - Setting Up a Computer Forensics Lab
  - Building the Investigation Team
  - Understanding the Hardware and Software Requirements of a Forensic Lab
- **Forensic Investigation Process - Investigation Phase**
  - Computer Forensics Investigation Methodology
    - Documenting the Electronic Crime Scene
    - Search and Seizure
    - Planning the Search and Seizure
    - Evidence Preservation
    - Data Acquisition

- Data Analysis
- Case Analysis

- **Forensic Investigation Process - Post-investigation Phase**
  - Gathering and Organizing Information
  - Writing the Investigation Report
  - Forensics Investigation Report Template
  - Testifying as an Expert Witness

Lab Exercise

- Performing Hash or HMAC Calculations
- Comparing Hash Values of Files to Check their Integrity
- Viewing Files of Various Formats
- Creating a Disk Image File of a Hard Disk Partition

Module 03: Understanding Hard Disks and File Systems

- **Describe Different Types of Disk Drives and their Characteristics**
  - Understanding Hard Disk Drive
    - Tracks
    - Track Numbering
    - Sector
    - Sector Addressing
    - 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

- **Explain the Logical Structure of a Disk**
  - Logical Structure of Disk
  - Clusters
  - Cluster Size
  - 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 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
- **Understand Various File Systems of Windows, Linux, and Mac Operating Systems**
  - Windows File Systems

- File Allocation Table (FAT)
- New Technology File System (NTFS)
  - NTFS Architecture
  - NTFS System Files
- Encrypting File Systems (EFS)
- 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)
- macOS File Systems
  - Hierarchical File System Plus (HFS+)
  - Apple File System (APFS)

- **Examine the File System**
  - File System Analysis using Autopsy
  - File System Analysis using The Sleuth Kit (TSK)
  - Recovering Deleted Files from Hard Disks using WinHex

Lab Exercise

- Analyzing File System of a Linux Image
- Recovering Deleted Files from Hard Disks

Module 04: Data Acquisition and Duplication

- **Understand Data Acquisition Fundamentals**
  - Data Acquisition

- Live Acquisition
- Order of Volatility
- Dead Acquisition
- Rules of Thumb for Data Acquisition

- **Discuss Different Types of Data Acquisition**
  - Types of Data Acquisition
    - Logical Acquisition
    - Sparse Acquisition
    - Bit-Stream Imaging
      - Bit-stream disk-to-image file
      - Bit-stream disk-to-disk

Lab Exercise

- Creating a dd Image of a System Drive

- **Determine the Data Acquisition Format**
  - Raw Format
  - Proprietary Format
  - Advanced Forensics Format (AFF)
  - Advanced Forensic Framework 4 (AFF4)

- **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
    - Step 5: Enable Write Protection on the Evidence Media
    - Step 6: Acquire Non-Volatile Data
      - Acquire Non-volatile Data (Using a Windows Forensic Workstation)
    - Step 7: Plan for Contingency

- Step 8: Validate Data Acquisition
  - Validate Data Acquisition – Windows Validation Methods

Lab Exercise

- Converting Acquired Image File to a Bootable Virtual Machine
- Acquiring RAM from Windows Workstations
- Viewing Contents of Forensic Image File

Module 05: Defeating Anti-forensics Techniques

- **Understand Anti-forensics and its Techniques**
  - What is Anti-forensics?
  - Anti-forensics Techniques
    - Data/File Deletion
      - What Happens When a File is Deleted in Windows?
      - Recycle Bin in Windows
      - Recycle Bin Forensics
    - File Carving
      - File Carving on Windows
      - File Recovery Tools: Windows
      - File Carving on Linux
      - SSD File Carving on Linux File System
    - Recovering Deleted Partitions
      - Recovering Deleted Partitions: Using EaseUS Data Recovery Wizard
    - Password Protection
      - Password Types
      - Password Cracking Techniques
      - Password Cracking Tools
    - Steganography
      - Steganography Detection Tools

- Alternate Data Streams
- Trail Obfuscation
- Artifact Wiping
- Overwriting Data/Metadata
- Encryption

Lab Exercise

- SSD File Carving on a Windows File System
- Recovering Data from Lost / Deleted Disk Partition
- Cracking Application Passwords
- Detecting Steganography

- **Discuss Anti-forensics Countermeasures**
  - Anti-forensics Countermeasures
  - Anti-forensics Tools

Module 06: Windows Forensics

- **Collect Volatile and Non-Volatile Information**
  - Introduction to OS Forensics
  - Collecting Volatile Information
    - Collecting System Time
    - Collecting Logged-On Users
    - 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

- 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

Lab Exercise

- Acquiring Volatile Information from a Live Windows System

- **Perform Windows Memory and Registry Analysis**
  - Windows Memory Analysis
    - Windows Crash Dump
    - Collecting Process Memory
    - Random Access Memory (RAM) Acquisition
    - Memory Forensics: Malware Analysis Using Redline
  - Windows Registry Analysis
    - Windows Registry
    - Registry Structure within a Hive File
    - Windows Registry: Forensic Analysis

Lab Exercise

- Investigating Forensic Image of Windows RAM

- **Examine Cache, Cookie, and History Recorded in Web Browsers**
  - Cache, Cookie, and History Analysis
    - Google Chrome
      - Analysis Tool: ChromeCacheView
      - Analysis Tool: ChromeCookiesView
      - Analysis Tool: ChromeHistoryView

- Mozilla Firefox
- Microsoft Edge

Lab Exercise

- Examining Web Browser Artifacts

- **Examine Windows Files and Metadata**
  - Windows File Analysis
    - System Restore Points (Rp.log Files)
    - System Restore Points (Change.log.x Files)
    - Prefetch Files
    - Image Files
  - Metadata Investigation
    - Understanding Metadata
    - Metadata in Different File Systems
    - Metadata in PDF Files
    - Metadata in Word Documents
    - Metadata Analysis Tool: Metashield Analyzer

Lab Exercise

- Extracting Information about Loaded Processes on a Computer

Module 07: Linux and Mac Forensics

- **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
- Viewing Running Processes in the System

o 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

▪ **Analyze Filesystem Images Using The Sleuth Kit**

o File System Analysis Using The Sleuth Kit: fsstat

o System Analysis Using The Sleuth Kit: fls and istat

▪ **Demonstrate Memory Forensics**

o Memory Forensics: Introduction

o Memory Forensics Using Volatility Framework

o Carving Memory Dumps Using PhotoRec Tool

Lab Exercise

o Forensic Investigation on a Linux Memory Dump

o Recovering Data from a Linux Memory Dump

▪ **Understand Mac Forensics**

o Introduction to Mac Forensics

o Mac Forensics Data

o Mac Log Files

o Mac Directories

o APFS Analysis: Biskus APFS Capture

o Parsing Metadata on Spotlight

o Mac Forensics Tools

Module 08: Network Forensics

- **Understand Network Forensics Fundamentals**
  - 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
- **Understand Event Correlation Concepts and Types**
  - Event Correlation
  - Types of Event Correlation
  - Prerequisites of Event Correlation
  - Event Correlation Approaches
- **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: Check Point
  - Analyzing Honeypot Logs
  - Analyzing Router Logs
    - Analyzing Router Logs: Cisco
  - Analyzing DHCP Logs
- **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

Lab Exercise

- Identifying and Investigating Various Network Attacks using Wireshark

Module 09: Investigating Web Attacks

- **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
- **Understand IIS and Apache Web Server Logs**
  - IIS Logs
    - IIS Web Server Architecture
    - IIS Logs
    - Analyzing IIS Logs
  - 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

- **Investigating Web Attacks on Windows-based Servers**
- **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 Snort Alert Logs for XSS Attack
    - Examining SIEM Logs for XSS Attack
  - Investigating SQL Injection Attack
    - Investigating SQL Injection Attack: Using Regex
    - Examining IIS Logs for SQL Injection Attack
    - Examining Snort Alert Logs for SQL Injection Attack
    - Examining SIEM Logs for SQL Injection Attack

Lab Exercise

- Identifying and Investigating Web Application Attacks Using Splunk

Module 10: Dark Web Forensics

- **Understand the Dark Web**
  - Understanding the Dark Web
  - Tor Relays
  - Working of the Tor Browser
  - Tor Bridge Node
- **Understand Dark Web Forensics**
  - Dark Web Forensics
  - Identifying Tor Browser Artifacts: Command Prompt

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

Lab Exercise

- Detecting TOR Browser on a Machine

- **Perform Tor Browser Forensics**
  - Memory Acquisition
  - Collecting Memory Dumps
  - Memory Dump Analysis: Bulk Extractor

Lab Exercise

- Analyzing RAM Dumps to Retrieve TOR Browser Artifacts

Module 11: Investigating Email Crimes

- **Understand Email Basics**
  - Introduction to an Email System
  - Components Involved in Email Communication
  - How Email Communication Works?
  - Understanding the Parts of an Email Message
- **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
      - Acquiring Thunderbird Local Email Files via SysTools MailPro+
    - 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 Gmail

- Step 5: Analyzing Email Headers
  - Checking Email Authenticity
  - Investigating a Suspicious Email
- Step 6: Recovering Deleted Email Messages
  - Recovering Deleted Email Messages from Outlook .pst Files Using Paraben's Electronic Evidence Examiner

Lab Exercise

- Investigating a Suspicious Email

Module 12: Malware Forensics

- **Understand Malware, its Components and Distribution Methods**
  - Introduction to Malware
  - Components of Malware
  - Common Techniques Attackers Use to Distribute Malware across Web
- **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
  - Types of Malware Analysis
- **Perform Static Malware Analysis**

- Malware Analysis: Static
- File Fingerprinting
- Online Malware Scanning
- Performing Strings Search
- Identifying Packing/Obfuscation Methods
- Finding the Portable Executables (PE) Information
- Identifying File Dependencies
- Malware Disassembly

Lab Exercise

- Performing Static Analysis on a Suspicious File

- **Analyze Suspicious Word Documents**
  - Analyzing Suspicious MS Office Document
    - Finding Suspicious Components
    - Finding Macro Streams
    - Dumping Macro Streams
    - Identifying Suspicious VBA Keywords

Lab Exercise

- Forensic Examination of a Suspicious Microsoft Office Document

- **Perform Dynamic Malware Analysis**
  - Malware Analysis: Dynamic
  - Pre-Execution Preparation
  - Monitoring Host Integrity
  - Observing Runtime Behavior
- **Perform System Behavior Analysis**
  - Monitoring Registry Artifacts
    - Windows AutoStart Registry Keys
    - Analyzing Windows AutoStart Registry Keys
  - Monitoring Processes

- Monitoring Windows Services
- Monitoring Startup Programs
  - Startup Programs Monitoring Tool: AutoRuns for Windows
- Monitoring Windows Event Logs
- Monitoring API Calls
- Monitoring Device Drivers
  - Device Drivers Monitoring Tool: DriverView
- Monitoring Files and Folders
  - File and Folder Monitoring Tool: PA File Sight
  - File and Folder Integrity Checkers: FastSum and WinMD5

Lab Exercise

- Performing System Behaviour Analysis

- **Perform Network Behavior Analysis**
  - Monitoring Network Activities
    - Monitoring IP Addresses
  - Monitoring Port
    - Port Monitoring Tools: TCPView and CurrPorts
  - Monitoring DNS
    - DNS Monitoring Tool: DNSQuerySniffer