EC-Council CHFI: Computer Hacking Forensic Investigator v10

Course Outline

1. Computer Forensics in Today's World

- Understand the Fundamentals of Computer Forensics
- Understand Cybercrimes and their Investigation Procedures
- Understand Digital Evidence
- Understand Forensic Readiness, Incident Response and the Role of SOC (Security Operations Center) in Computer Forensics
- Identify the Roles and Responsibilities of a Forensic Investigator
- Understand the Challenges Faced in Investigating Cybercrimes
- Understand Legal Compliance in Computer Forensics

2. Computer Forensics Investigation Process

- Understand the Forensic Investigation Process and its Importance
- Understand the Pre-investigation Phase
- Understand First Response
- Understand the Investigation Phase
- Understand the Post-investigation Phase

3. Understanding Hard Disks and File Systems

- Describe Different Types of Disk Drives and their Characteristics
- Explain the Logical Structure of a Disk
- Understand Booting Process of Windows, Linux and Mac Operating Systems
- Understand Various File Systems of Windows, Linux and Mac Operating Systems
- Examine File System Using Autopsy and The Sleuth Kit Tools
- Understand Storage Systems
- Understand Encoding Standards and Hex Editors
- Analyze Popular File Formats Using Hex Editor

4. Data Acquisition and Duplication

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

5. Defeating Anti-forensics Techniques

- Understand Anti-forensics Techniques
- Discuss Data Deletion and Recycle Bin Forensics
- Illustrate File Carving Techniques and Ways to Recover Evidence from Deleted Partitions
- Explore Password Cracking/Bypassing Techniques
- Detect Steganography, Hidden Data in File System Structures, Trail Obfuscation, and File Extension Mismatch
- Understand Techniques of Artifact Wiping, Overwritten Data/Metadata Detection, and Encryption
- Detect Program Packers and Footprint Minimizing Techniques

SpireTec Solutions

- Understand Anti-forensics Countermeasures

6. Windows Forensics

- Collect Volatile and Non-volatile Information
- Perform Windows Memory and Registry Analysis
- Examine the Cache, Cookie and History Recorded in Web Browsers
- Examine Windows Files and Metadata
- Understand ShellBags, LNK Files, and Jump Lists
- Understand Text-based Logs and Windows Event Logs

7. Linux and Mac Forensics

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

8. Network Forensics

- Understand Network Forensics
- Explain Logging Fundamentals and Network Forensic Readiness
- Summarize Event Correlation Concepts
- Identify Indicators of Compromise (IoCs) from Network Logs
- Investigate Network Traffic
- Perform Incident Detection and Examination with SIEM Tools
- Monitor and Detect Wireless Network Attacks

9. Investigating Web Attacks

- Understand Web Application Forensics
- Understand Internet Information Services (IIS) Logs
- Understand Apache Web Server Logs
- Understand the Functionality of Intrusion Detection System (IDS)
- Understand the Functionality of Web Application Firewall (WAF)
- Investigate Web Attacks on Windows-based Servers
- Detect and Investigate Various Attacks on Web Applications

10. Dark Web Forensics

- Understand the Dark Web
- Determine How to Identify the Traces of Tor Browser during Investigation
- Perform Tor Browser Forensics

11. Database Forensics

- Understand Database Forensics and its Importance
- Determine Data Storage and Database Evidence Repositories in MSSQL Server
- Collect Evidence Files on MSSQL Server
- Perform MSSQL Forensics
- Understand Internal Architecture of MySQL and Structure of Data Directory
- Understand Information Schema and List MySQL Utilities for Performing Forensic Analysis

SpireTec Solutions

12. Cloud Forensics

- Understand the Basic Cloud Computing Concepts
- Understand Cloud Forensics
- Understand the Fundamentals of Amazon Web Services (AWS)
- Determine How to Investigate Security Incidents in AWS
- Understand the Fundamentals of Microsoft Azure
- Determine How to Investigate Security Incidents in Azure
- Understand Forensic Methodologies for Containers and Microservices

13. Investigating Email Crimes

- Understand Email Basics
- Understand Email Crime Investigation and its Steps
- U.S. Laws Against Email Crime

14. Malware Forensics

- Define Malware and Identify the Common Techniques Attackers Use to Spread Malware
- Understand Malware Forensics Fundamentals and Recognize Types of Malware Analysis
- Understand and Perform Static Analysis of Malware
- Analyze Suspicious Word and PDF Documents
- Understand Dynamic Malware Analysis Fundamentals and Approaches
- Analyze Malware Behavior on System Properties in Real-time
- Analyze Malware Behavior on Network in Real-time
- Describe Fileless Malware Attacks and How they Happen
- Perform Fileless Malware Analysis – Emotet

15. Mobile Forensics

- Understand the Importance of Mobile Device Forensics
- Illustrate Architectural Layers and Boot Processes of Android and iOS Devices
- Explain the Steps Involved in Mobile Forensics Process
- Investigate Cellular Network Data
- Understand SIM File System and its Data Acquisition Method
- Illustrate Phone Locks and Discuss Rooting of Android and Jailbreaking of iOS Devices
- Perform Logical Acquisition on Android and iOS Devices
- Perform Physical Acquisition on Android and iOS Devices
- Discuss Mobile Forensics Challenges and Prepare Investigation Report

16. IoT Forensics

- Understand IoT and IoT Security Problems
- Recognize Different Types of IoT Threats
- Understand IoT Forensics
- Perform Forensics on IoT Devices

SpireTec Solutions