WISEMAN CYBERSEC
BE WISE , BE SECURE

MODULE 1 : INTRODUCTION TO DIGITAL FORENSICS

1.1 Introduction
1.2 Fundamentals
1.3 Digital Evidence
1.4 Analysis Steps
1.5 Investigation Scope
1.6 Reconstructing Of The Crime Scene
1.7 Challenges Of Digital Evidence
1.8 Major Concept

MODULE 2 : DATA ACQUISITION

2.1 Introduction
2.2 Storage Formats
2.3 Acquisition Method
2.4 Write Blocker
2.5 Live Data Acquisition
2.6 Tools
2.7 Validating the Evidence
2.8 Exploring the Evidence
2.9 Time & Timestamps

MODULE 3 : DEFEATING ANTI-FORENSICS TECHNIQUES

3.1 Understanding Anti-Forensics Techniques
3.2 Data Deletion
3.3 Finding Hidden Data
3.4 Understanding Anti-Forensics Countermeasures

MODULE 4 : DATA RECOVERY & FILE CARVING

4.1 Understanding How Data Is Stored
4.2 Logical Data Recovery
4.3 Recovering Data From Recycle Bin
4.4 File Carving
4.5 Raw Data Recovery

MODULE 5: UNDERSTANDING HARD DISKS

5.1 Different Types of Disk Drives & Their Characteristics
5.2 Understanding Logical Structure of a Disk
5.3 Booting Process of Linux, Windows & macOS
5.4 File System Analysis with Autopsy
5.5 Understanding Storage Systems (RAID & NAS)

WISEMAN CYBERSEC
BE WISE , BE SECURE

MODULE 6: UNDERSTANDING FILE SYSTEM

6.1 New Technology File System (NTFS)
6.2 File Allocation Table (FAT)
6.3 Extended File System
6.4 Extensible File Allocation Table (exFAT)
6.5 Hierarchical File System (HFS)
6.6 Apple File System (APFS)

MODULE 7 : WINDOWS FORENSICS

7.1 Collecting Evidence
7.2 Windows Registry Forensics
7.3 Examine Cache, Cookies and History Stored in Web Browsers
7.4 Examine Windows Files and Metadata Analysis
7.5 Investigating Windows Logs
7.6 File Signature Analysis

MODULE 8 : LINUX FORENSICS

8.1 Understanding Volatile & Non-Volatile Data in Linux
8.2 Linux File System & Analysis
8.3 Linux Memory Acquisition

MODULE 9 : MEMORY FORENSICS

9.1 Memory Acquisition
9.2 Volatility: Introduction
9.3 MemProcFS: Introduction
9.4 Windows Memory Analysis
9.5 Linux Memory Analysis
9.6 Analysis of Malware-Affected System Memory

MODULE 10 : DARK WEB FORENSICS

10.1 Understanding Dark Web
10.2 Identifying Traces of Tor Browser During Investigation
10.3 Performing Tor Browser Forensics

MODULE 11 : ANDROID FORENSICS

11.1 Importance of Android Device Forensics
11.2 Steps Involved in Android Device Forensics
11.3 Performing Logical Data Acquisition
11.4 Rooting
11.5 Performing Physical Data Acquisition
11.6 Analyzing Android with Autopsy
11.7 Challenges Faced During Android Device Forensics

WISEMAN CYBERSEC
BE WISE , BE SECURE

MODULE 12 : IOS FORENSICS

12.1 Importance of iOS Device Forensics
12.2 Steps Involved in iOS Device Forensics
12.3 Performing Logical Data Acquisition
12.4 Jailbreaking
12.5 Performing Physical Data Acquisition
12.6 Analyzing iOS with Autopsy
12.7 Challenges Faced During iOS Device Forensics

MODULE 13 : NETWORK FORENSICS

13.1 Understanding Network Forensics
13.2 Indicators of Compromise (IOCs)
13.3 Investigating Network Traffic
13.4 Analyzing Network Logs

MODULE 14 : ADVANCED FORENSICS TOOLS

14.1 PassMark: OSForensics
14.2 Magnet AXIOM
14.3 Cellebrite UFED
14.4 Internet Evidence Finder
14.5 Oxygen Detective
14.6 Cellebrite Physical Analyzer
14.7 MD-NEXT, MD-RED
14.8 Amped FIVE

BONUS MODULES

MODULE 15: Cloud Forensic
MODULE 16: Database Forensic
MODULE 17: Linux-Based Forensic OS
MODULE 18: Introduction to Professional Data Recovery

MODULE 19 : CCTV & VIDEO EVIDENCE FORENSICS

19.1 DVR Extraction
19.2 Proprietary Video Format Conversion
19.3 Video Evidence Enhancements
19.4 Data Carving from DVR Disk

Module 20: Final Exam

PRACTICAL CHALLENGE