Day 1: Introduction to Digital & Forensic Data Analysis

- Fundamentals of Digital Forensics
- Types of Digital Evidence (Disk, Memory, Network, Cloud)
- Forensic Investigation Lifecycle
    - Identification
    - Preservation
    - Collection
    - Examination
    - Analysis
    - Reporting
- Legal & Compliance Aspects
    - Chain of Custody
    - Evidence Handling Procedures
- Overview of Forensic Tools
    - FTK Imager
    - Autopsy
    - EnCase
- Lab: Evidence Acquisition using FTK Imager

Day 2: Disk & File System Forensics

- Disk Structures and Storage Concepts
- File Systems Deep Dive
    - NTFS, FAT, exFAT
- File Metadata Analysis
- Deleted File Recovery Techniques
- File Carving Methods
- Timeline Analysis (MAC times)
- Identifying Suspicious Files & Hidden Data
- Lab:
    - Disk Image Analysis
    - Recover Deleted Files
    - Timeline Creation

Day 3: Memory & Malware Forensics

- Memory Forensics Fundamentals
- RAM Acquisition Techniques
- Analyzing Memory Dumps
- Detecting Malware Artifacts in Memory
- Process & DLL Analysis
- Registry Forensics
- Indicators of Compromise (IOCs)

- Lab:
    - Memory Analysis using Volatility
    - Detecting Suspicious Processes

Day 4: Network & Log Forensics

- Network Forensics Fundamentals
- Packet Capture Analysis (PCAP)
- Protocol Analysis (HTTP, DNS, TCP/IP)
- Log Analysis Techniques
    - Windows Event Logs
    - Firewall & IDS Logs
- SIEM Basics for Forensics
- Correlating Logs & Network Data
- Lab:
    - Wireshark Analysis
    - Log Correlation & Attack Detection

Day 5: Advanced Forensic Analysis & Reporting

- Cloud & Email Forensics Basics
- Insider Threat Investigations
- Data Exfiltration Detection Techniques
- Anti-Forensics & Evasion Techniques
- Automation in Forensic Analysis (Python basics)
- Forensic Reporting & Documentation
    - Structuring Reports
    - Presenting Evidence in Court
- Case Study: End-to-End Incident Investigation
- Final Lab:
    - Full Forensic Investigation Scenario
    - Report Preparation & Presentation