FOR500: Windows Forensic Analysis

Duration: 5 Days

Course Overview:

This course provides a comprehensive deep dive into Windows forensic analysis, covering core forensic techniques, file system artifacts, registry analysis, event logs, memory forensics, and advanced analysis methodologies. Participants will learn how to investigate and extract evidence from Windows systems efficiently.

Day 1:

- Introduction to Windows Forensics & Core Concepts
- Understanding Digital Forensics & Incident Response
- Role of forensic analysis in investigations
- Key forensic methodologies and best practices
- Windows Operating System Fundamentals for Forensics
- File system overview (NTFS, FAT, ReFS)
- Core Windows components and their forensic relevance
- Disk & File System Forensics
- Understanding Master Boot Record (MBR) & GUID Partition Table (GPT)
- Analyzing file system structures and metadata
- Recovering deleted files and forensic imaging

Day 2:

- Windows Artifacts & Registry Analysis
- Windows Registry Forensics
- Key registry hives and forensic significance
- Tracking user activity via registry artifacts
- Recovering deleted and modified registry keys
- User Activity & System Artifacts
- Prefetch, Jump Lists, and Shellbags analysis
- USB device tracking and forensic examination
- Windows Search Index and Link File (LNK) forensics

Day 3:

- Event Log & Memory Analysis
- Windows Event Log Analysis
- Understanding Windows event logging
- Investigating security, system, and application logs
- Detecting anomalies and suspicious activities
- Memory Forensics & Live System Analysis
- Introduction to memory forensics techniques
- Using tools like Volatility for memory analysis
- Extracting evidence from RAM and investigating malware artifacts

Day 4:

- Advanced Windows Forensic Techniques
- Shadow Copies & Volume Snapshot Analysis
- Recovering previous versions of files
- Extracting hidden or deleted data
- Windows Artifact Correlation for Investigations
- Correlating different sources of evidence
- Case study: Timeline reconstruction using forensic artifacts
- Analyzing Modern Windows Features
- OneDrive and cloud-based artifacts
- BitLocker forensics and data recovery

Day 5:

- Case Study, Reporting, and Hands-on Exercises
- Real-World Forensic Investigation Scenario
- Step-by-step guided case study
- Investigating a compromised system
- Forensic Reporting & Documentation
- Best practices for forensic reports
- Presenting findings to stakeholders
- Final Practical Exam & Q&A Session