SANS FOR500: Windows Forensic Analysis Course

Course Duration: 40 Hrs. **Course Code: FOR500**

Course Overview

The **SANS FOR500: Windows Forensic Analysis** course is designed to provide in-depth, hands-on training in digital forensic analysis of Windows operating systems. This course focuses on identifying, collecting, and analyzing forensic artifacts from Windows systems to investigate security incidents, insider threats, and malware infections. Participants will develop practical skills to perform forensic examinations, reconstruct user activity, and present findings in a legally sound manner.

What You'll Learn?

By completing this course, you will be able to:

- Perform comprehensive Windows forensic investigations
- Identify and analyze key Windows forensic artifacts
- Reconstruct user and system activity timelines
- Analyze file systems, registry, and event logs
- Investigate malware and attacker persistence mechanisms
- Collect and preserve digital evidence properly
- Apply forensic methodologies in incident response cases

Target Audience

This course is ideal for:

- Digital Forensics Analysts
- Incident Response and SOC Professionals

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com

- Law Enforcement and Investigators
- Cybersecurity Analysts and Engineers
- IT and Security Professionals involved in investigations

Pre-Requisites

Participants should have:

- Basic understanding of Windows operating systems
- Familiarity with cybersecurity and incident response concepts
- Prior experience with forensic tools is helpful but not mandatory

Course Content

Module 1: Windows Forensics Fundamentals

- Forensic investigation process
- Evidence handling and chain of custody
- Windows architecture overview

Module 2: File System and Artifact Analysis

- NTFS structure and metadata
- File recovery and deleted file analysis
- Windows shortcut and prefetch files

Module 3: Windows Registry and Persistence

- Registry structure and analysis
- User activity artifacts
- Malware persistence mechanisms

Module 4: Event Logs and Timeline Analysis

- Windows event log analysis
- Timeline creation and correlation
- Identifying suspicious activity

Module 5: User Activity and Malware Investigation

- Browser artifacts and user behavior
- Malware execution traces
- Memory and process artifacts

Module 6: Reporting, Legal Considerations, and Best Practices

- Documentation and reporting findings
- Legal considerations in forensic investigations
- Best practices and exam preparation