BOOST
THE LEADING TRAINING PROVIDER

Information Technology

FOR500 - Windows Forensic Analysis

Course Introduction

Every organization must be fully equipped against the cybercrime occurring on computer systems and within corporate networks. Government agencies increasingly require trained media exploitation specialists to recover vital intelligence from Windows systems, as well as law enforcement investigators to get to the root of a crime.

This FOR500: Windows Forensic Analysis provides an in-depth and comprehensive digital forensics knowledge of Microsoft Windows operating systems by analyzing and authenticating forensic data as well as track detailed user activity and organize findings. This will allow participants to apply digital forensic methodologies to a variety of case types and situations, allowing them to apply in the real world the right methodology to achieve the best outcome.

Target Audience

- Cloud Computing Engineer
- Computer Network Specialist
- Computer Support Specialist
- Database Administrator
- Information Technology Analyst
- Information Technology Leadership
- Information Security Specialist
- Software/Application Developer
- Web Developer
- Technology sales consultant

Learning Objectives

- Conduct proper Windows forensic analysis by applying key techniques focusing on Windows 7, Windows 8/8.1, and Windows10
- Identify and use forensic tools and analysis methods to detail nearly every action a suspect accomplished on a Windows system, including who placed an artifact on the system and how, program execution, file/folder opening, geolocation, browser history, profile USB device usage, cloud storage usage, and more
- Know the number of times files have been opened by a suspect through browser forensics, shortcut file analysis (LNK), email analysis, and Windows Registry parsing
- Identify keywords searched by a specific user on a Windows system to pinpoint the data and information that the suspect was interested in finding, and accomplish detailed damage assessments
- Discover the exact time that a specific user last executed a program through Registry and Windows artifact analysis, and understand how this information can be used to prove intent in cases such as intellectual property theft, hacker-breached systems, and traditional crimes
- Audit cloud storage usage, including detailed user activity, identifying deleted files and even documenting files available only in the cloud
- Use Windows Shellbag analysis tools to articulate every folder and directory a user or attacker interacted with while accessing local, removable, and network drives
- Determine each time a unique and specific USB device was attached to the Windows system, the files and folders accessed on it, and what user plugged it in by parsing Windows artifacts such as Registry hives and Event Log files
- Specifically determine how individuals used a system, who they communicated with, and files that were downloaded, modified, and deleted
- Use Event Log analysis techniques in determining when and how users logged into a Windows system, whether via a remote session, at the keyboard, or simply by unlocking a screensaver
- Determine where a crime was committed using Registry data and pinpoint the geolocation of a system by examining connected networks and wireless access points
- Use browser forensic tools to perform detailed web browser analysis, parse raw SQLite and ESE databases, and leverage session recovery artifacts to identify web activity, even if privacy cleaners and in-private browsing software are used

Course Outline

- **Day 01**

  Windows Operating Systems Focus (Windows 7, Windows 8/8.1, Windows 10, Server 2008/2012/2016/2019)

  - Windows File Systems (NTFS, FAT, exFAT)
  - Advanced Evidence Acquisition Tools and Techniques
  - Registry Forensics
  - Shell Item Forensics
  - Shortcut Files (LNK) - Evidence of File Opening
  - Shellbags - Evidence of Folder Opening
  - JumpLists - Evidence of File Opening and Program Execution
- **Day 02**

  Windows Artifact Analysis

  - Browser and Webmail Analysis
  - Microsoft Office Document Analysis
  - System Resource Usage Database
  - Windows 10 Timeline Database
  - Windows Recycle Bin Analysis
  - File and Picture Metadata Tracking and Examination
  - Myriad Application Execution Artifacts, including Several New to Windows 10
  - Cloud Storage File and Metadata Examinations
  - OneDrive and OneDrive for Business, Dropbox, Google Drive, Google Workspace, and Box
- **Day 03**

  Email Forensics (Host, Server, Web), including Microsoft 365 and G Suite

  - Microsoft Unified Audit Logging
  - Event Log Analysis
  - Chrome, Edge, Internet Explorer, and Firefox Browser Forensics
  - Microsoft 365 SharePoint, OneDrive, Teams, and Email
  - Google Workspace (G Suite) Applications and Logging
  - Deleted Registry Key and File Recovery
  - Recovering Missing Data from Registry and ESE Database .log Files
  - String Searching and File Carving

- Examination of Cases Involving Windows 7 through Windows 10

- **Day 04**

  Media Analysis and Exploitation to:

  - Track User Communications Using a Windows Device (Email, Chat, Webmail)
  - Identify If and How a Suspect Downloaded Specific Files to or from a Device
  - Determine the Exact Time and Number of Times a Suspect Executed a Program
  - Show When Any File Was First and Last Opened by a Suspect
  - Determine If a Suspect Had Knowledge of a Specific File

- **Day 05**

  Show the Exact Physical Location of the System

  - Track and Analyze Removable Media and USB Mass Storage Class Devices
  - Show How the Suspect Logged on to the Machine via the Console, RDP, or Network
  - Recover and Examine Browser Artifacts, including Those from Private Browsing Mode
  - Discover the Use of Anti-Forensics, including File Wiping, Time Manipulation, and Application Removal

Confirmed Sessions

FROM	TO	DURATION	FEES	LOCATION
June 1, 2025	June 5, 2025	5 days	4250.00 $	KSA - Al Khobar
Aug. 4, 2025	Aug. 8, 2025	5 days	4950.00 $	Netherlands - Amsterdam
Dec. 8, 2025	Dec. 12, 2025	5 days	4250.00 $	UAE - Abu Dhabi