Windows Forensics and Advanced NTFS Investigation Course

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Windows Forensics and Advanced NTFS Investigation Course

Course Overview:

The **Windows Forensic Analysis and Advanced NTFS Investigation Course** develops the practical skills required to investigate Windows systems, reconstruct user activity, and support incident response. Participants examine Windows forensic evidence from the Registry, Event Logs, Prefetch, AmCache, Shimcache, UserAssist, ShellBags, LNK files, Jump Lists, SRUM, browsers, email, USB devices, and cloud applications.

The course strengthens standard Windows Forensics Training with dedicated NTFS Forensics, including Master File Table Analysis, USN Journal Analysis, $LogFile, deleted-file examination, timestamps, and Windows Timeline Analysis. Participants learn how to correlate multiple artifacts rather than depend on a single source.

Realistic investigation scenarios cover insider threats, data leakage, malware activity, unauthorized access, renamed files, deleted evidence, removable media, and anti-forensic behavior. The NIST data-leakage case demonstrates how email, browsers, Windows Search, cloud storage, NTFS, and USB evidence can be combined into one investigative timeline.

Target Audience:

- Digital Forensic Analysts
- Incident Response and DFIR Specialists
- SOC and Cybersecurity Analysts
- Computer Forensic Examiners
- Cybercrime Investigators
- Threat Hunters
- Endpoint Security Professionals
- Internal Audit and Corporate Investigation Teams
- IT Security Professionals

AGILE LEADERS
Training Center

Targeted Organizational Departments:

- Digital Forensics and Incident Response
- Cybersecurity and SOC Operations
- Corporate Security and Investigations
- Internal Audit and Compliance
- Legal and e-Discovery
- Fraud and Insider-Risk Management
- IT Infrastructure and Endpoint Security

Targeted Industries:

- Banking and Financial Services
- Government and Defense
- Oil, Gas, and Energy
- Telecommunications
- Healthcare
- Critical Infrastructure
- Technology and Cloud Services
- Manufacturing

Course Offerings:

By the end of this course, participants will be able to:

- Conduct structured Windows Forensic Analysis.
- Perform rapid forensic triage of Windows endpoints.
- Examine NTFS architecture and metadata.
- Analyze $MFT, USN Journal, and $LogFile.
- Investigate deleted, renamed, and moved files.
- Perform Windows Registry Forensics.
- Examine program-execution artifacts.
- Analyze LNK files, Jump Lists, and ShellBags.
- Profile USB devices and removable-media usage.
- Conduct Windows Event Log Analysis.

AGILE LEADERS
Training Center

Training Methodology:

The course combines instructor-led sessions, practical demonstrations, guided investigations, group exercises, and case-study analysis. Participants learn the purpose, location, forensic value, and limitations of each Windows artifact.

Exercises focus on NTFS Forensic Analysis, Registry examination, program execution, Event Logs, Browser Forensics, Email Forensics, USB activity, and Windows Timeline Analysis. The NIST data-leakage case provides a realistic scenario involving confidential files, cloud uploads, removable media, renamed extensions, deleted evidence, and anti-forensic activity.

Participants work individually and in groups to identify evidence, test investigative hypotheses, reconstruct events, and present findings. Tool examples are introduced where relevant, but the course remains focused on investigative methods rather than one software platform.

Course Toolbox:

- Windows artifact reference
- NTFS metadata guide
- MFT Analysis checklist
- USN Journal and $LogFile guide
- Windows timestamp matrix
- Registry investigation reference
- Program-execution artifact comparison

Tool clarification: Software and licensed forensic tools are **not** provided. Participants receive insights, demonstrations, and examples of tools relevant to the course.

AGILE LEADERS
Training Center

Course Agenda:

Day 1: Windows Forensic Investigation and Evidence Triage

- **Topic 1:** Understanding the Windows forensic investigation process
- **Topic 2:** Identifying key Windows evidence and artifact locations
- **Topic 3:** Collecting and prioritizing evidence during forensic triage
- **Topic 4:** Mounting and examining Windows forensic images
- **Topic 5:** Analyzing file metadata, signatures, and deleted data
- **Topic 6:** Correlating evidence during Windows Incident Response
- **Reflection & Review:** Select the most relevant evidence for a Windows security incident

Day 2: NTFS File-System and Deleted-File Investigation

- **Topic 1:** Understanding NTFS structure and system metadata
- **Topic 2:** Examining files and directories through the Master File Table
- **Topic 3:** Using MFT records to identify deleted, moved, and renamed files
- **Topic 4:** Tracking file changes through the USN Journal
- **Topic 5:** Investigating $LogFile, Recycle Bin, and alternate data streams
- **Topic 6:** Reconstructing file activity through NTFS timestamps
- **Reflection & Review:** Build a timeline of file creation, modification, movement, and deletion

Day 3: Windows Registry and Program-Execution Analysis

- **Topic 1:** Examining Windows Registry hives and forensic evidence
- **Topic 2:** Identifying user accounts, profiles, and system settings
- **Topic 3:** Using Prefetch to investigate program execution
- **Topic 4:** Interpreting AmCache and Shimcache evidence correctly
- **Topic 5:** Tracking application activity through UserAssist, BAM, and SRUM
- **Topic 6:** Analyzing LNK files, Jump Lists, and ShellBags
- **Reflection & Review:** Determine which user accessed or executed a program

AGILE LEADERS
Training Center

Day 4: Event Logs, USB Devices, Browsers, and Email

- **Topic 1:** Investigating security activity through Windows Event Logs
- **Topic 2:** Identifying logons, remote sessions, and authentication events
- **Topic 3:** Tracing connected USB devices and removable-media activity
- **Topic 4:** Recovering browsing activity from Chrome, Edge, and Firefox
- **Topic 5:** Examining browser history, cache, cookies, and downloads
- **Topic 6:** Analyzing email messages, attachments, and communication records
- **Reflection & Review:** Connect user logons, USB activity, browsing, and email evidence

Day 5: Integrated Windows Forensic Case Investigation

- **Topic 1:** Planning insider-threat and data-leakage investigations
- **Topic 2:** Correlating NTFS, Registry, Event Log, and browser artifacts
- **Topic 3:** Detecting deleted evidence and anti-forensic activity
- **Topic 4:** Building and validating a complete Windows activity timeline
- **Topic 5:** Preparing clear forensic findings and investigation reports
- **Topic 6:** Completing an integrated Windows forensic case challenge
- **Reflection & Review:** Present and evaluate the final investigative conclusions

FAQ:

What specific qualifications or prerequisites are needed for participants before enrolling in the course?

Participants should understand Windows operating systems, file structures, user accounts, networking, and basic cybersecurity concepts. Previous experience in incident response, system administration, SOC operations, or digital forensics is beneficial.

How long is each day's session, and is there a total number of hours required for the entire course?

Each day's session is generally structured to last around 4–5 hours, with breaks and interactive activities included. The total course duration spans five days, approximately 20–25 hours of instruction.

Can one Windows artifact prove that a user executed a program?

Usually not. Investigators should correlate several artifacts, such as Prefetch, UserAssist, SRUM, Event Logs, AmCache, Shimcache, and Registry data. Some artifacts indicate only that a file existed, while others provide stronger evidence of execution.

AGILE LEADERS
Training Center

How This Course is Different from Other Windows Forensic Analysis Courses:

This course gives NTFS Forensics a central role rather than treating it as a brief file-system overview. Participants examine $MFT, USN Journal, $LogFile, timestamps, deleted records, and alternate data streams in detail.

It also connects NTFS evidence with Windows Registry Forensics, Event Logs, Prefetch, AmCache, Shimcache, UserAssist, SRUM, ShellBags, Browser Forensics, Email Forensics, and USB activity.

The course is tool-independent and focuses on evidence interpretation, artifact correlation, timeline reconstruction, and defensible conclusions. A realistic data-leakage case connects technical analysis to corporate risks such as insider threats, intellectual-property theft, unauthorized cloud transfers, and removable-media misuse

AGILE LEADERS
Training Center

Training Course Categories

- Agile PM and Project Management Training Courses
- Certified Courses By International Bodies
- Communication and Public Relations Training Courses
- Data Analytics Training and Data Science Courses
- Environment & Sustainability Training Courses
- Finance and Accounting Training Courses
- Governance, Risk and Compliance Training Courses
- Human Resources Training and Development Courses
- IT Security Training & IT Training Courses
- Leadership and Management Training Courses
- Legal Training, Procurement and Contracting Courses
- Maintenance Training and Engineering Training Courses
- Marketing, Customer Relations, and Sales Courses
- Occupational Health, Safety and Security Training Courses
- Personal & Self-Development Training Courses
- Quality and Operations Management Training Courses
- Secretarial and Administration Training Courses

AGILE LEADERS
Training Center

Training Cities

Accra Ghana	**Al Jubail** Saudi Arabia	**Amman** Jordan
Amsterdam Netherlands	**Athens** Greece	**Baku** Azerbaijan
Bangkok Thailand	**Barcelona** Spain	**Berlin** Germany
Cairo Egypt	**Cape town** South Africa	**Casablanca** Morocco
Chicago USA	**Doha** Qatar	**Dubai** UAE
Frankfurt Germany	**Geneva** Switzerland	**Istanbul** Turkey
Jakarta Indonesia	**Johannesburg** South Africa	**Kuala Lumpur** Malaysia
Kuwait Kuwait	**Langkawi** Malaysia	**Lisbon** Portugal
London UK	**Madrid** Spain	**Manama** Bahrain
Marbella Spain	**Milan** Italy	**Montreux** Switzerland
Munich Germany	**Muscat** Oman	**Nairobi** Kenya
New York USA	**Paris** France	**Phuket** Thailand

AGILE LEADERS
Training Center

Training Cities

Porto Portugal	**Prague** Czech Republic	**Riyadh** Saudi Arabia
Rome Italy	**San Diego** USA	**Seoul** South Korea
Sharm El-Sheikh Egypt	**Singapore** Singapore	**Tashkent** Uzbekistan
Tbilisi Georgia	**Tokyo** Japan	**Toronto** Canada
Trabzon Turkey	**Vienna** Austria	**Zanzibar** Tanzania
Zoom Online Training		