



التحليل الجنائي لأنظمة Windows والتحقيق المتقدم في NTFS



AGILE LEADERS
Training Center

05 - 09 Oct 2026
لندن

التحليل الجنائي لأنظمة Windows والتحقيق المتقدم في NTFS

المرجع: 103600651_82913 التاريخ: 05 - 09 Oct 2026 الموقع: لندن الرسوم: Euro 5700

Course Overview:

develops the practical skills required to Windows Forensic Analysis and Advanced NTFS Investigation Course The 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

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.

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 •

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

Course Agenda:

Day 1: Windows Forensic Investigation and Evidence Triage

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

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

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

Day 3: Windows Registry and Program-Execution Analysis

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

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

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

Day 5: Integrated Windows Forensic Case Investigation

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

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.

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.

فئات الدورات التدريبية

الدورات التدريبية في مجال البيئة والاستدامة	دورات إدارة الجودة وتطوير العمليات
دورات إدارة و تحليل البيانات ودورات علم البيانات	دورات إدارة و تطوير الموارد البشرية
دورات الذهن السيرياني ودورات تقنية المعلومات	دورات الاتصال الجماهيري و السياسات والعلاقات العامة
دورات التدريب القانوني والهشتريات والتعاقدات	دورات التسويق وإدارة علاقات العملاء وإدارة المبيعات
دورات الحوكمة وإدارة المخاطر والامتثال	دورات السكرتارية و إدارة المكاتب
دورات الصحة والسلامة والذهن المهني	دورات الصيانة ودورات المجالات الهندسية المتنوعة
دورات المحاسبة و التهويل و دورات الإدارة المالية	دورات المهارات الشخصية وتطوير الذات
دورات في مجالات القيادة والإدارة	دورات معتمدة من قبل هيئات دولية
دورات مكتب إدارة المشاريع وإدارة المشاريع الرشيقية	



معدن التدريب

أكرا غانا	أثينا اليونان	أبوظبي الإمارات العربية المتحدة
الجبيل المملكة العربية السعودية	استنبول تركيا	أهستردام هولندا
الرياض المملكة العربية السعودية	الدوحة قطر	الدار البيضاء المغرب
المنامة مملكة البحرين	الكويت الكويت	القاهرة مصر
بانكوك تايلند	باكو أذربيجان	باريس فرنسا
برلين ألمانيا	برشلونة إسبانيا	براغ جمهورية التشيك
تيليسي جورجيا	بوكيت تايلاند	بورتو البرتغال
جنيف سويسرا	جاكارتا جمهورية إندونيسيا	تورنتو كندا
روما إيطاليا	حلي الإمارات العربية المتحدة	جوهانسبرغ جنوب أفريقيا
سنغافورة سنغافورة	سان دييغو الولايات المتحدة الأمريكية	زنجان تنزانيا
شيكاغو الولايات المتحدة الأمريكية	شرم الشيخ مصر	سيول كوريا الجنوبية
طوكيو اليابان	طشقند أوزبكستان	طرابزون تركيا
فرانكفورت ألمانيا	عن بعد منصة زووم	عمان المملكة الأردنية الهاشمية



مدن التدريب

كيب تاون جنوب افريقيا	كوالالمبور ماليزيا	فيينا النمسا
لندن المملكة المتحدة	لشبونة البرتغال	لانكاوي ماليزيا
مسقط سلطنة عمان	هدريد اسبانيا	ماربيا اسبانيا
ميونخ ألمانيا	ميلان إيطاليا	مونترو سويسرا
	نيويورك الولايات المتحدة الأمريكية	نيروبي كينيا