Windows Endpoint Investigation

FOR501

Investigate Windows systems from the evidence up. Answer the questions that matter: What ran? Who was here? How did the attacker move? What did they install? What data left? Work through real forensic artifacts, build timelines across multiple hosts, detect anti-forensics, and complete two full capstone investigations.

Modules	21
Lessons	150
Phases	4
Free preview	Course Orientation (6 lessons)

The method

This course is organized around the questions an investigation actually asks, rather than around the artifacts that happen to answer them. Each module is a question and the loop inside it is the same.

1. Ask the question before choosing the artifact. What ran, who was here, how did they get in, what did they install. Starting from the question stops an investigation becoming a tour of a forensic toolkit.

2. Collect once, correctly. Acquisition and triage decide everything downstream, and a host that has been rebuilt cannot be re-collected.

3. Corroborate across at least two artifacts. Execution evidence in Prefetch alone is a lead. The same execution in Prefetch, Amcache and an event log, with times that agree, is a finding.

4. Notice what is missing. Cleared logs, wiped artifacts and timestamps that disagree are evidence in themselves, and an absence with a mechanism named is a finding rather than a gap.

5. Assemble the picture last. The timeline is built from artifacts already understood. Building it first inherits every parsing error into the narrative.

The course closes with two full investigations, an insider case and a ransomware case, worked end to end.

What this course assumes

No minimum experience and no prerequisite course. Every artifact is introduced with what it records, why Windows writes it and what it cannot tell you.

What makes it go faster: a Windows machine to examine and the tooling installed. Neither is required, and every artifact in the course is shown parsed with its output.

What this course does not cover: memory forensics, network investigation and malware reverse engineering. Each is a separate course, and this one is the disk and the operating system.

Full syllabus

Phase 1: Foundations

Course Orientation FREE PREVIEW

What Windows Endpoint Investigation teaches: how to reconstruct an attack from the evidence a Windows system leaves behind.

1. WF0.1 What Forensic Analysis Is
2. WF0.2 How This Course Is Structured
3. WF0.3 The Forensic Toolstack
4. WF0.4 What Windows Records Without Being Asked
5. WF0.5 Best Practices
6. WF0 Module Summary

Evidence Acquisition and Triage

How to collect and preserve Windows forensic evidence in the correct order, with the correct tools, producing an analysis-ready evidence package.

1. WF1.1 Order of Volatility and Collection Decisions
2. WF1.2 Encryption Before You Image
3. WF1.3 Memory Acquisition and Extraction
4. WF1.4 KAPE Triage and Processing
5. WF1.5 Velociraptor for Remote Collection
6. WF1.6 Full Disk Imaging and Verification
7. WF1.7 Processing Collected Evidence
8. WF1.8 Fleet-Wide Collection at Scale
9. WF1.9 Proving the Collection Is Complete
10. WF1.10 The Collection You Cannot Repeat
11. WF1.11 See It Done: A Soldered Laptop, Four Hundred Hosts, and a Ticket Nobody Mentioned
12. WF1 Check My Knowledge

Phase 2: Investigation Questions

What Ran on This System?

Finding execution evidence from Prefetch, Amcache, Shimcache, BAM, SRUM, and event logs.

1. WF2.1 The Execution Evidence Hierarchy
2. WF2.2 Prefetch
3. WF2.3 Amcache
4. WF2.4 BAM, DAM and SRUM
5. WF2.5 Process Creation Events
6. WF2.6 PowerShell Execution
7. WF2.7 Credential Tool Identification
8. WF2.8 C2 and Lateral Movement Tools
9. WF2.9 Anti-Forensics and Execution Evidence
10. WF2.10 Building a Cross-Source Execution Timeline
11. WF2.11 See It Done: Seventy-One Minutes, Found Nine Days Later
12. Check My Knowledge

Who Was Here and What Did They Do?

Account forensics, authentication analysis, folder and file access artifacts, application usage, search history, geolocation, document tracking, and user attribution.

1. WF3.1 Account Forensics
2. WF3.2 Authentication and Session Analysis
3. WF3.3 Folder and File Access
4. WF3.4 Application Usage
5. WF3.5 Search History
6. WF3.6 Location and Network History
7. WF3.7 Document Access and Metadata
8. WF3.8 Attribution
9. WF3.9 See It Done: The Client List
10. WF3 Check My Knowledge

How Did They Get In, and How Far Did They Get?

Patient zero and retention horizons, origin markings and what removes them, delivery chains that carry no file, following an account across a boundary, the one technique whose evidence sits on the source, and the three kinds of gap in a chain.

1. WF4.1 Initial Access and Patient Zero
2. WF4.2 Mark of the Web
3. WF4.3 The Delivery Chain
4. WF4.4 Following the Account Across the Boundary
5. WF4.5 Remote Desktop and What It Records
6. WF4.6 What Each Technique Leaves, and Where
7. WF4.7 Stolen Credentials and What They Do to Attribution
8. WF4.8 Choosing the Next Host
9. WF4.9 Collecting While the Estate Is Running
10. WF4.10 A Chain With a Gap, and When to Stop
11. WF4.11 See It Done: The Contractor's Second Tuesday
12. WF4 Check My Knowledge

What Did They Install to Stay?

Persistence mechanism forensics: registry Run keys, services, scheduled tasks, WMI subscriptions, COM hijacking, PowerShell-based persistence, user-level persistence, Autoruns triage, multi-layer patterns, and persistence timeline reconstruction.

1. WF5.1 The Persistence Landscape
2. WF5.2 Registry Persistence Across Hives
3. WF5.3 Scheduled Tasks and Services From Event Logs
4. WF5.4 WMI Subscriptions and the Mechanisms Most Analysts Miss
5. WF5.5 PowerShell and Script-Based Persistence
6. WF5.6 NTUSER.DAT and User-Level Persistence
7. WF5.7 The Autoruns Triage Workflow
8. WF5.8 Multi-Layer Persistence
9. WF5.9 Reconstructing the Persistence Timeline
10. WF5.10 See It Done: Six Mechanisms, Two Rebuilds, One Account
11. WF5 Check My Knowledge

What Data Left the Network?

Data exfiltration forensics: SRUM application network usage, USB device history, browser uploads and downloads, cloud storage sync evidence, email artifacts, staging and compression patterns, and quantifying the exfiltration narrative.

1. WF6.1 SRUM and the Volume Question
2. WF6.2 USB Devices and Removable Media
3. WF6.3 Browser Downloads, and the Uploads Nobody Logged
4. WF6.4 Cloud Storage on the Endpoint
5. WF6.5 Email Artifacts and the Export That Was a Decision
6. WF6.6 Staging and Compression
7. WF6.7 Quantifying What Left
8. WF6.8 See It Done: Six Routes, One Employee, Two Reports
9. WF6 Check My Knowledge

What Happened on the Filesystem?

NTFS filesystem forensics: MFT architecture, MFTECmd parsing, USN Journal analysis, ransomware pattern detection, $LogFile transactions, deleted file recovery, timestomping detection, Alternate Data Streams, document metadata, INDX directory analysis, and unified timeline construction.

1. WF7.1 NTFS Architecture for Investigators
2. WF7.2 Reading a Parsed MFT
3. WF7.3 The Change Journal
4. WF7.4 Mass Operations and Ransomware
5. WF7.5 The Transaction Log
6. WF7.6 Deleted File Recovery
7. WF7.7 Timestomping Detection
8. WF7.8 Alternate Data Streams
9. WF7.9 File and Document Metadata
10. WF7.10 Directory Index Analysis
11. WF7.11 Building the Filesystem Timeline
12. WF7.12 See It Done: Eleven Days Later
13. WF7 Check My Knowledge

What Did They Try to Hide?

Anti-forensic detection and evidence recovery: anti-forensics threat model, Volume Shadow Copy recovery, event log clearing detection, secure deletion tool artifacts, data hiding techniques, pagefile and hibernation analysis, and evidence integrity for court admissibility.

1. WF8.1 The Anti-Forensics Threat Model
2. WF8.2 Volume Shadow Copies
3. WF8.3 Event Log Clearing and Recovery
4. WF8.4 Secure Deletion and Wiping Tool Detection
5. WF8.5 Data Hiding
6. WF8.6 Memory, Pagefile and Hibernation File Analysis
7. WF8.7 Evidence Integrity and Admissibility
8. WF8.8 See It Done: Forty-Five Minutes of Cleanup
9. Check My Knowledge

Phase 3: Integration

Building the Complete Picture

Constructing super timelines with Plaso, analyzing with Timeline Explorer, correlating across multiple hosts, assessing confidence levels, and producing defensible findings and reports.

1. WF9.1 Why Timelines Change Everything
2. WF9.2 Building Targeted Timelines With Plaso
3. WF9.3 Timeline Explorer for Analysis
4. WF9.4 Multi-Host Timeline Correlation
5. WF9.5 Confidence Assessment and Writing Findings
6. WF9.6 Reporting and Testimony Preparation
7. WF9 Module Summary
8. Check My Knowledge

Communication & Application Forensics

What browsers and communication applications leave behind: Chromium and Firefox artifacts, cross-browser analysis, private browsing recovery, and the messaging and email application traces that place a user at a keyboard.

1. WF10.1 Chromium Browser Forensics
2. WF10.2 Firefox and Cross-Browser Analysis
3. WF10.3 Private Browsing and Artifact Recovery
4. WF10.4 Electron and WebView2 Application Forensics
5. WF10.5 The Windows Search Database
6. WF10.6 Email Forensics
7. WF10.7 Cloud Application Artifacts on the Endpoint
8. Module Summary
9. Knowledge Check

Phase 4: Capstone Investigations

Investigation: Insider Threat

A full insider threat investigation worked end to end: case briefing and evidence inventory, account and session analysis, execution evidence, and the findings package somebody else reads.

1. INV1.01 Case Briefing and Evidence Inventory
2. INV1.02 Account and Session Analysis
3. INV1.03 Execution Evidence
4. INV1.04 Data Staging and USB Transfer
5. INV1.05 Cloud and Browser Evidence
6. INV1.06 Anti-Forensic Cleanup
7. INV1.07 Timeline Construction
8. INV1.08 Findings and Report
9. Module Summary
10. Knowledge Check

Investigation: Ransomware

A full ransomware investigation worked end to end: initial triage, the phishing vector, credential theft and escalation, and a classification that separates the encrypted hosts from the compromised ones.

1. INV2.01 Case Briefing and Initial Triage
2. INV2.02 The Phishing Vector
3. INV2.03 Credential Theft
4. INV2.04 Lateral Movement
5. INV2.05 Persistence
6. INV2.06 Defense Evasion
7. INV2.07 Encryption Timeline
8. INV2.08 Blast Radius
9. Module Summary
10. Knowledge Check

Phase 0: Course Resources

Cheatsheets
The lookup layer: every command the course teaches, grouped by what you are trying to establish.
1. Cheatsheet

Cookbooks
Procedures: what you do, in what order, and what each step must produce.
1. Cookbook

Lab Setup
Build the environment that produces the evidence this course analyzes.
1. Lab Setup

Walkthroughs
Complete investigations worked end to end, including the wrong turns.
1. A Binary That Is No Longer On Disk
2. The Account That Was Not The Person
3. Files That Left On A USB Stick
4. Persistence Nobody Installed Deliberately
5. Timestamps That Disagree
6. Evidence Somebody Tried To Remove
7. Triage: A Disk Image And No Context
8. The Artifact That Was Not There

Playbooks
Artifact generation and analysis procedures.
1. Execution Evidence
2. Logon and Session Evidence
3. Folder and File Access
4. Removable Media
5. Persistence Mechanisms
6. Filesystem and Timestamps
7. Anti-Forensic Traces

Playground
Resources for practicing endpoint investigation and using it at work: the forensic lab, an open-source DFIR toolkit, the detection library, guided investigations, and response playbooks.

References
External sources this course draws on: tooling documentation, research, standards and community Windows forensics material.

Course Completion

Course Exam
Windows Endpoint Investigation end-of-course exam: a simulation-based assessment testing your ability to reconstruct attacker activity from forensic evidence across multiple hosts.
1. Course Completion. Windows Endpoint Investigation

Generated 2026-09-04 from the published course. The current syllabus is always at ridgelinecyber.com/training/courses/windows-endpoint-investigation/