macOS Endpoint Investigation

FOR503

Investigate Macs from the evidence up. Acquire an Apple Silicon machine correctly, read the stores macOS actually keeps, and build defensible findings across macOS Sequoia 15 and macOS 26 Tahoe. Work real artifacts, reason about what the platform does and does not record, and complete a full capstone investigation.

Modules	22
Lessons	177
Phases	4
Free preview	Course Orientation (7 lessons)

The method

macOS records a great deal and almost none of it where a Windows investigator would look. This course runs the same loop for every artifact class it covers.

1. Learn the architecture before the artifacts. APFS, the launchd model, SIP and the signed system volume decide where evidence can exist at all. An investigator who skips this looks in the wrong places confidently.

2. Acquire against what the platform allows. Apple Silicon, FileVault and SIP each constrain acquisition. Know the constraint before the incident rather than during it.

3. Read the unified log for what it actually kept. It is the richest source on the platform and the most aggressively rolled. Establishing the window is the first query, not an afterthought.

4. Prove execution from more than one artifact. Quarantine, Gatekeeper, launch services and the log each hold a fragment. The claim that a binary ran is only as good as the artifacts that agree.

5. State the platform limits in the finding. No live memory on Apple Silicon, a locked volume, reduced persistence surfaces on newer releases. A report that hides these is a report that fails on review.

The course closes with a full intrusion investigation worked end to end on a fresh case.

What this course assumes

No minimum experience and no prerequisite course, and no assumption that you use a Mac. Every subsystem is introduced with what it records and why Apple built it that way.

What makes it go faster: a Mac you can run commands on, ideally one you are willing to take apart. Not required, and every artifact in the course is shown with real output.

What this course does not cover: Windows and Linux forensics, iOS device extraction, and reverse engineering beyond static Mach-O triage. This course stays on the macOS endpoint and is honest about where the endpoint stops.

Full syllabus

Phase 1: Foundations

Course Orientation FREE PREVIEW

What macOS Endpoint Investigation teaches: how to reconstruct an incident from the evidence a Mac leaves behind.

1. MX0.1 What macOS Endpoint Investigation Is
2. MX0.2 How This Course Is Structured
3. MX0.3 The macOS Forensic Toolstack
4. MX0.4 Practical Applications
5. MX0.5 Evidence Handling and Honest Limits
6. MX0.6 Setting Up Your Analysis Environment
7. Module Summary

macOS in the Threat Landscape and the Security Model

What you are up against on a Mac and what macOS's own security machinery records.

1. MX1.1 Why macOS Endpoints Matter
2. MX1.2 Anatomy of a macOS Compromise
3. MX1.3 The macOS Security Model: Defenses as Recorders
4. MX1.4 SIP and System Integrity as a Baseline
5. MX1.5 Gatekeeper, Quarantine, and Notarization
6. MX1.6 XProtect, the Remediator, and the Behavior Service
7. MX1.7 TCC and Privacy as Evidence
8. MX1.8 Code Signing, the Sealed System Volume, and the Sandbox
9. MX1.9 FileVault, the Secure Enclave, and Lockdown Mode
10. MX1.10 Legal Foundations and Chain of Custody on macOS
11. Module Summary
12. Check My Knowledge

macOS Architecture for Investigators

The investigator's map of macOS. APFS containers and volumes, the System and Data split and the sealed system volume, the filesystem layout and where user, system, and application evidence each live, Mach-O binaries and application bundles, launchd as the service substrate, and the two storage...

1. MX2.1 APFS for Investigators
2. MX2.2 The Filesystem Layout and Key Locations
3. MX2.3 Mach-O Binaries
4. MX2.4 Application Bundles and Installer Packages on Disk
5. MX2.5 launchd, Daemons, and Agents
6. MX2.6 Property Lists and Extended Attributes
7. MX2.7 SQLite as a macOS Forensic Format
8. MX2.8 How Architecture Drives Artifact Location
9. Module Summary
10. Check My Knowledge

Phase 2: Acquisition and Logging

Acquisition and Triage

Getting analysis-ready macOS evidence off a machine you often cannot fully image.

1. MX3.1 Live vs Dead-Box on Modern Macs
2. MX3.2 Imaging a modern Mac: tools and formats
3. MX3.3 Reading What Live Response Collects
4. MX3.4 Live collection with Aftermath
5. MX3.5 Triage collection with mac_apt and AutoMacTC
6. MX3.6 FileVault, encryption, and the keybag
7. MX3.7 When you cannot image: account-side and escrowed evidence
8. MX3.8 Building the analysis-ready evidence package
9. Module Summary
10. Check My Knowledge

Unified Logging

Reading the single most detailed record of what a Mac and its processes actually did.

1. MX4.1 The Unified Logging system
2. MX4.2 The log store on disk
3. MX4.3 Reading the log with predicates
4. MX4.4 The predicate language in depth
5. MX4.5 Security-relevant log subsystems
6. MX4.6 Redaction and the private problem
7. MX4.7 Building timelines from the log
8. MX4.8 What the log does not capture
9. Module Summary
10. Check My Knowledge

Phase 3: Investigation Questions

Filesystem and Storage Artifacts

What the macOS file system remembers about file activity, often more than the current disk reveals.

1. MX5.1 What the filesystem remembers
2. MX5.2 FSEvents: the filesystem changelog
3. MX5.3 Spotlight metadata
4. MX5.4 APFS snapshots and local Time Machine
5. MX5.5 Time Machine backups
6. MX5.6 Document Versions and autosave
7. MX5.7 The Trash, deletion, and recovery realities on APFS
8. MX5.8 Reconstructing file activity
9. Module Summary
10. Check My Knowledge

Persistence

How an intruder makes code on a Mac survive a reboot and a login, and how to find it.

1. MX6.1 The macOS persistence landscape
2. MX6.2 LaunchAgents and LaunchDaemons: the plist contract
3. MX6.3 Normal vs malicious launchd jobs
4. MX6.4 Background Task Management
5. MX6.5 Login items, profiles, and MDM-delivered persistence
6. MX6.6 Legacy mechanisms: kexts and dylib hijacking
7. MX6.7 Scheduled and deprecated mechanisms
8. MX6.8 Detecting suspicious persistence
9. Module Summary
10. Check My Knowledge

Execution and Provenance

Module 7 of macOS Endpoint Investigation.

1. MX7.1 The execution-evidence problem on macOS
2. MX7.2 Quarantine and provenance
3. MX7.3 Gatekeeper and notarization as evidence
4. MX7.4 XProtect, XProtect Remediator, and MRT
5. MX7.5 Proving execution: KnowledgeC and Biome
6. MX7.6 Proving execution: ExecPolicy, logs, and the defensible claim
7. MX7.7 Install receipts and package history
8. MX7.8 Reconstructing the execution story
9. Module Summary
10. Check My Knowledge

User Activity and Application Artifacts

Module 8 of macOS Endpoint Investigation.

1. MX8.1 Browser artifacts
2. MX8.2 Communication apps
3. MX8.3 KnowledgeC and Biome pattern-of-life
4. MX8.4 The App.MenuItem Biome stream (Tahoe 26)
5. MX8.5 Clipboard History (Tahoe 26)
6. MX8.6 Recent items, MRU, and shared file lists
7. MX8.7 Keychain and credential artifacts
8. MX8.8 Reconstructing the user-activity timeline
9. Module Summary
10. Check My Knowledge

Network and Communication Artifacts

Module 9 of macOS Endpoint Investigation.

1. MX9.1 The endpoint network-evidence problem
2. MX9.2 Network configuration and connection history
3. MX9.3 Wi-Fi and known networks
4. MX9.4 Geolocation and movement from network artifacts
5. MX9.5 Bluetooth and paired devices
6. MX9.6 AirDrop and proximity transfer
7. MX9.7 Sharing services and remote access
8. MX9.8 Reconstructing the network picture
9. Module Summary
10. Check My Knowledge

macOS Malware and Mach-O Analysis

Module 10 of macOS Endpoint Investigation.

1. MX10.1 The macOS malware landscape
2. MX10.2 Mach-O for the analyst
3. MX10.3 The dynamic linker and load-command abuse
4. MX10.4 Code signing and the trust chain
5. MX10.5 Entitlements and notarization anomalies
6. MX10.6 Strings, symbols, and anti-analysis
7. MX10.7 Static triage to a verdict
8. MX10.8 Correlation and the malware finding
9. Module Summary
10. Check My Knowledge

Ecosystem and Cross-Device

Module 11 of macOS Endpoint Investigation.

1. MX11.1 The cross-device evidence problem
2. MX11.2 iCloud account and sync state
3. MX11.3 iCloud Drive and synced data on disk
4. MX11.4 Continuity, Handoff, and Universal Clipboard
5. MX11.5 MDM enrollment and supervision
6. MX11.6 Configuration profiles as evidence
7. MX11.7 iOS backups and connected-device history
8. MX11.8 Reconstructing the cross-device picture
9. Module Summary
10. Check My Knowledge

Phase 4: Integration and Capstone

Timeline Reconstruction and Anti-Forensics

Module 12 of macOS Endpoint Investigation.

1. MX12.1 The timeline problem
2. MX12.2 Building the macOS super timeline
3. MX12.3 Reading the timeline
4. MX12.4 Correlation and confidence
5. MX12.5 Anti-forensics: timestamp and log manipulation
6. MX12.6 Anti-forensics: artifact destruction and SIP
7. MX12.7 Findings and reporting
8. MX12.8 macOS caveats and the honest report
9. Module Summary
10. Check My Knowledge

Capstone: Full Intrusion Investigation

The FOR503 capstone. Work a complete compromised macOS endpoint end to end on a case you have not seen: acquisition, initial access and execution, persistence, malware triage, user activity and staging, the exfiltration channel, anti-forensics, the unified timeline, and the honest findings...

1. MX13.1 The case and the acquisition
2. MX13.2 Initial access and execution
3. MX13.3 Persistence and privilege
4. MX13.4 The malicious binary
5. MX13.5 User activity and staging
6. MX13.6 The exfiltration channel
7. MX13.7 Anti-forensics and the unified timeline
8. MX13.8 The findings package and the honest report
9. Module Summary
10. Check My Knowledge

Phase 0: Course Resources

Cheatsheets

macOS artifact commands by investigation area, each with the fields that carry the decision and what the output does not establish.

1. Security Model
2. Architecture and Formats
3. Acquisition and Triage
4. Unified Logging
5. Filesystem and Storage
6. Persistence
7. Execution and Timeline
8. User Activity
9. Network and Cross-Device
10. Malware and Mach-O
11. Paths, Schemas and Version Deltas

Cookbooks

Seven procedures a macOS examiner repeats: acquiring a machine you cannot image the old way, opening it without changing it, triaging in an hour, and proving something ran.

1. Acquiring a Modern Mac
2. Building the Analysis-Ready Evidence Package
3. The Sixty-Minute macOS Triage
4. Working the Unified Log
5. Sweeping for Persistence
6. Proving a Binary Executed
7. Recovering What Was Deleted

Lab Setup

Building a macOS environment that produces real artifacts to practice against, on hardware you probably already own, across both versions the course targets.

1. The Mac You Need
2. Turning On What Is Off By Default
3. The Toolchain
4. Generating Activity Worth Analyzing
5. Verify and Limits

Walkthroughs

Seven macOS examinations worked end to end, including the wrong turns, the bounded answers, and the cases where the evidence could not support the question asked.

1. Ten Minutes to a Defensible No
2. When the Sweep Does Not Clear It
3. The File That Claimed to Be a Year Old
4. The Binary Nobody Could Prove Ran
5. The Deletion That Was Recoverable
6. The Artifact That Never Existed
7. The Sixty Minutes

Playbooks

Seven macOS threats, each with the examination sequence that establishes what happened, the check that could end it, and what the handoff must carry.

1. Credential Harvesting Suspected
2. Unsigned Persistence Discovered
3. Unexpected Configuration Profile
4. Data Staging by a Departing User
5. Anti-Forensics Suspected
6. Compromised Developer Tooling
7. Cross-Device and Cloud Exposure

Playground
Where to practice macOS investigation and use it at work: your own Mac first, then the toolkit, the detection library, guided investigations and response playbooks.

References & Further Reading
Apple platform documentation, macOS forensic artifact resources, open-source tooling, vendor and community research, and forensic standards used throughout the macOS Endpoint Investigation course.

Course Completion

Course Exam
macOS Endpoint Investigation end-of-course exam: a simulation-based assessment testing your ability to acquire, investigate, and report on a macOS intrusion you have not seen before, using the artifacts and the method built across all fourteen modules.

1. Course Completion. macOS Endpoint Investigation

Generated 2026-09-01 from the published course. The current syllabus is always at ridgelinecyber.com/training/courses/macos-endpoint-investigation/