

Malware Triage

FOR203

Reach a defensible verdict on a suspicious file under time pressure: what its structure says, what it is equipped to do, what a clean reputation result is worth, what one run establishes, and how to say all of it without claiming more than the evidence supports.

Modules	15
Lessons	83
Phases	4
Free preview	Course Orientation (7 lessons)

The method

Triage is not analysis. The question is whether this file needs a reverse engineer, answered in minutes with a verdict somebody can act on. This course runs the same loop for every sample it examines.

1. Establish what the file is before what it does. Format, size, signing state, packing. Half of triage verdicts are reachable without running anything.
2. Read capability from the structure. Imports, strings, sections and resources describe what the file is equipped to do, which bounds what it could have done.
3. Check reputation, and know what a miss means. An unknown hash is not a clean hash. It is a file nobody has submitted, which for a targeted sample is expected.
4. Detonate only when static triage has run out. Detonation is slow, evadable and produces the most convincing wrong answer available. It is the last step, not the first.
5. Produce indicators and a verdict together. A verdict with no indicators cannot be actioned. Indicators with no verdict get ignored in a queue.

What this course assumes

No minimum experience and no prerequisite course. File formats, the PE structure, packing and the sandbox model are explained where they first matter.

What makes it go faster: an isolated virtual machine you are willing to break. Not required for most of the course, and every sample is examined with its output shown.

What this course does not cover: reverse engineering, debugging and unpacking as disciplines. This course is about deciding whether a sample needs those, quickly and defensibly, which is a different job.

Full syllabus

Phase 1: The Discipline

Course Orientation [FREE PREVIEW](#)

What Malware Triage teaches: taking an unknown file and producing a verdict somebody can act on, under time pressure, without reverse engineering it.

1. 0.1 What Triage Actually Is
2. 0.2 How This Course Is Structured
3. 0.3 The Environment You Will Build
4. 0.4 Where This Shows Up
5. 0.5 What It Cannot Do
6. 0.6 Following Along
7. Module Summary

The Triage Discipline

What a triage verdict is answering, how long you actually have and what that buys, the classes of thing that arrive in a queue, evidence integrity applied rather than described, and the first pass that decides whether a sample deserves the next twenty minutes.

1. 1.1 The Verdict You Are Producing
2. 1.2 What the Clock Buys You
3. 1.3 What Arrives, and What Each Class Implies
4. 1.4 Provenance and Integrity
5. 1.5 The First Pass
6. 1.6 Writing the Disposition
7. Module Summary
8. Check My Knowledge

Phase 2: Reading the File

Static Examination

Everything a file will tell you about itself before it runs: what it actually is, how it was compiled and prepared, whether it is packed, what a signature is worth, and the strings it did and did not intend you to see.

1. 2.1 Identification, Properly
2. 2.2 Reading the Structure
3. 2.3 Packing and Entropy
4. 2.4 Signatures and Trust
5. 2.5 Strings
6. 2.6 Putting the Static Picture Together
7. Module Summary
8. Check My Knowledge

Capability

What a program can do, named and mapped to ATT&CK, from code that has never run.

1. 3.1 The Question Imports Could Not Answer
2. 3.2 Running capa and Reading the Output
3. 3.3 ATT&CK and the Malware Behavior Catalog
4. 3.4 Reading a Profile
5. 3.5 Where Capability Analysis Stops
6. 3.6 Capability in the Verdict
7. Module Summary
8. Check My Knowledge

Phase 3: Outside and Running It

Reputation and Intelligence

What other people already know: hash lookups, detection counts and what they establish, sample repositories, the submission decision, and the arithmetic of a clean result.

1. 4.1 What a Lookup Establishes
2. 4.2 Reading a Detection Count
3. 4.3 The Clean Result
4. 4.4 Submission Is a Disclosure
5. 4.5 Beyond the Multi-Scanner
6. 4.6 Reputation in the Verdict
7. Module Summary
8. Check My Knowledge

Detonation

Running the sample yourself: the environment, what to capture, reading a behavioral report, and separating a sample that did nothing from one that decided not to.

1. 5.1 What Detonation Actually Establishes
2. 5.2 The Environment
3. 5.3 Running It
4. 5.4 Reading the Report
5. 5.5 The Sample That Decided Not to Run
6. 5.6 Detonation in the Verdict
7. Module Summary
8. Check My Knowledge

Phase 4: Output and Practice

Indicators and Detection

Turning a verdict into something deployable: what to extract, which values survive the next build, writing a rule that holds, and handing over indicators somebody can actually use.

1. 6.1 What an Indicator Is For
2. 6.2 The Durability Ordering
3. 6.3 Extracting From What You Have
4. 6.4 Writing a Rule That Holds
5. 6.5 What a Negative Result Establishes
6. 6.6 Indicators in the Verdict and the Handoff
7. Module Summary
8. Check My Knowledge

The Verdict and the Queue

Running triage as a function rather than performing it once: the queue, the handoff, the boundary where triage stops, and what a triage practice looks like when it is working.

1. 7.1 The Verdict, Assembled
2. 7.2 Running a Queue
3. 7.3 Where Triage Stops
4. 7.4 The Handoff
5. 7.5 Auditing Your Own Queue
6. 7.6 A Triage Function That Works
7. Module Summary
8. Check My Knowledge

Phase 0: Course Resources

Cheatsheets

Six lookup pages for the commands that decide a triage item: identification, static reading, capability, reputation, detonation and indicators, each with what the result carries and what it does not.

1. Identification and Preparation
2. Reading the Structure
3. Strings and Capability
4. Reputation
5. Detonation
6. Indicators and Rules

Cookbooks

Six runbooks for the procedures this work repeats: the four-minute pass, a novel sample, a packed one, an item feeding an incident, a sample that will not run, and the escalation.

1. The Four-Minute Pass
2. A Sample Nobody Has Seen
3. A Packed Sample
4. An Item Feeding an Incident
5. A Sample That Will Not Run
6. Writing the Escalation

Walkthroughs

Triage items reasoned end to end, including the ones that finish with a weaker verdict than the evidence first suggested and the one where the tooling was working perfectly and the reading was wrong.

1. The File That Was Clean
2. The Profile That Described a Stub
3. The Sample That Did Nothing
4. The Process That Was Still Running
5. The Hunt That Covered Eight Hundred
6. The Item That Should Have Been Escalated

Playground

Every practice surface available for this course, what each one gives you, where the gaps are, and the exercises worth building yourself.

Operational Reference

Every command, verdict field, format and check from the Malware Triage course in one place, organized by task and linked back to the section that explains when not to use it.

1. Operational Reference

References and Further Reading

The tools, documentation, sample sources and standards this course draws on, with what each is good for and where it goes stale.

Course Completion

Course Exam

Malware Triage end-of-course exam: a sample where every automated check is clean, testing whether you can establish capability statically, explain why four honest results were all wrong, and produce a verdict somebody else can evaluate.

1. Course Completion. Malware Triage

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