# Triager

## An Open-Source Platform for Automated Forensic Triage and Investigation

**Cristian Souza**, Eduardo Ovalle and Daniel Batista

DFIR Specialist, Ph.D. Candidate

# Agenda

# Introduction

- DFIR investigations depend on the correct collection, parsing, and analysis of several operating system artifacts.
- However, parsing these artifacts manually is time-consuming.
- Each artifact usually requires a specific parser, generates a specific output format, and needs to be interpreted in the context of the investigation.

# Introduction

- This work introduces `Triager`, a Python-based DFIR automation platform.
- It is designed to automatically process Windows forensic artifacts collected during incident response and post-incident investigations.

# Introduction

**Main features:**

- Parsing and analysis orchestration.
- Post-processing activities.
- IOC hunting.
- AI-assisted analysis and report generation.

# Background and related tools

**Relevant Windows forensics artifacts:**

- Event Logs (EVTX)
- Prefetch, Amcache, Shimcache, BAM/DAM, SRUM
- EDR logs
- MFT, USN Journal, and $LogFile
- User artifacts

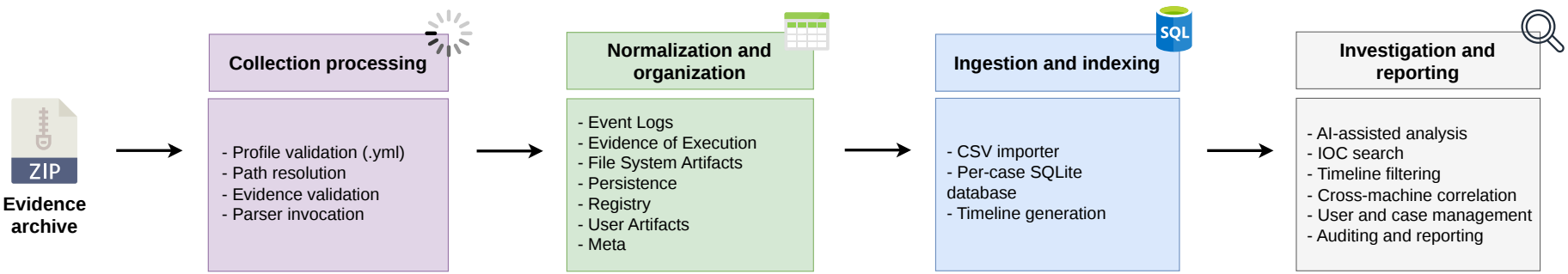
# Background and related tools

**Several specialized tools already exist for parsing Windows forensic artifacts, including:**

- `PECmd`, `AppCompatCacheParser`, `AmcacheParser`, `UserAssistReport`
- `MFTECmd`
- `SBECmd`, `JLECmd`
- `SrumECmd`
- `EvtxECmd`
- `Hayabusa`, `Chainsaw`, `APT-Hunter`

# Architecture and implementation

Figure: Triager architecture.



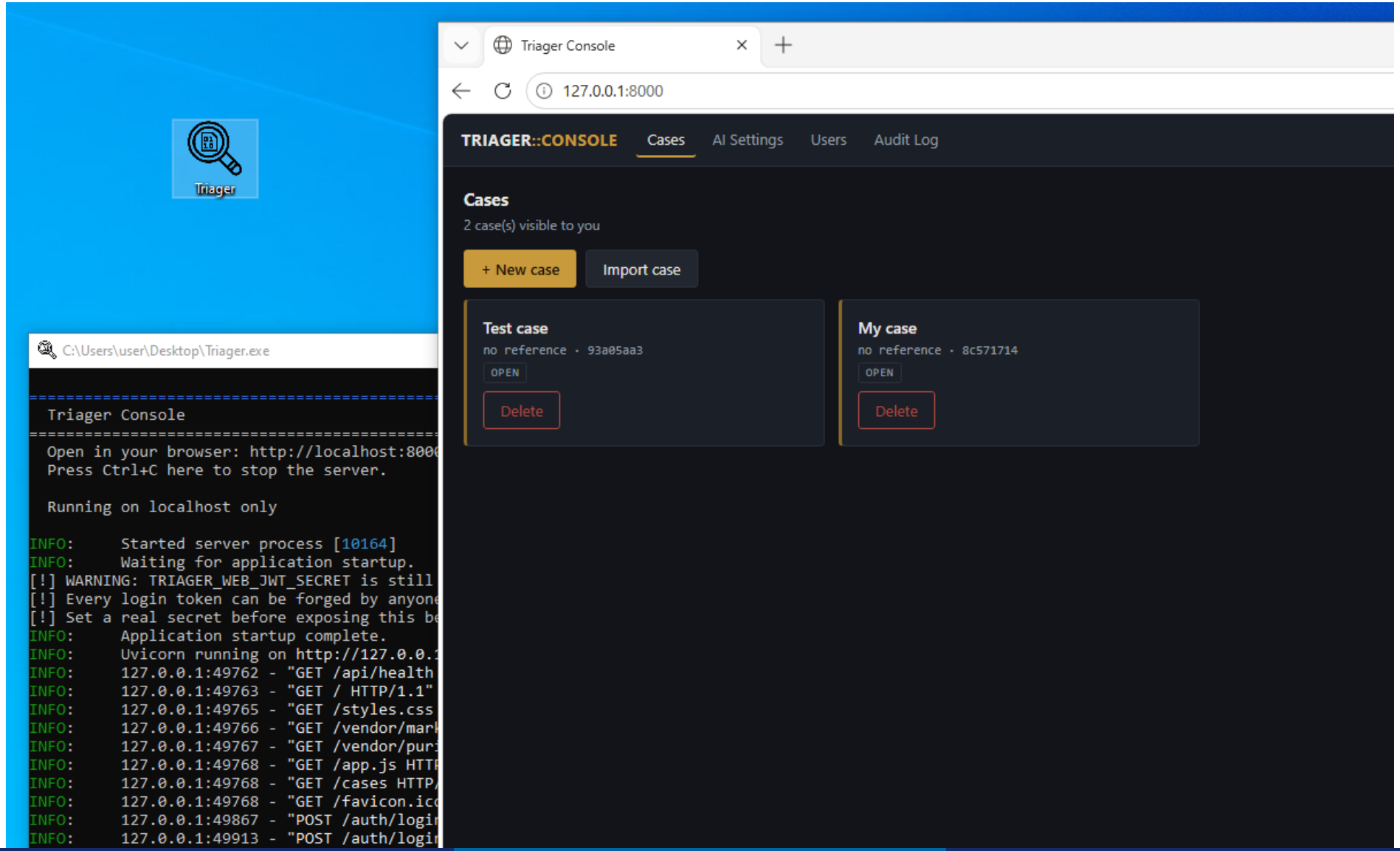
# Architecture and implementation

- `Triager` requires Python 3.10 or newer.
- Its main dependencies are: `PyYAML`, `python-registry`, `FastAPI`, `SQLAlchemy`, and `Uvicorn`.
- External forensic utilities are placed under the `tools/` directory.

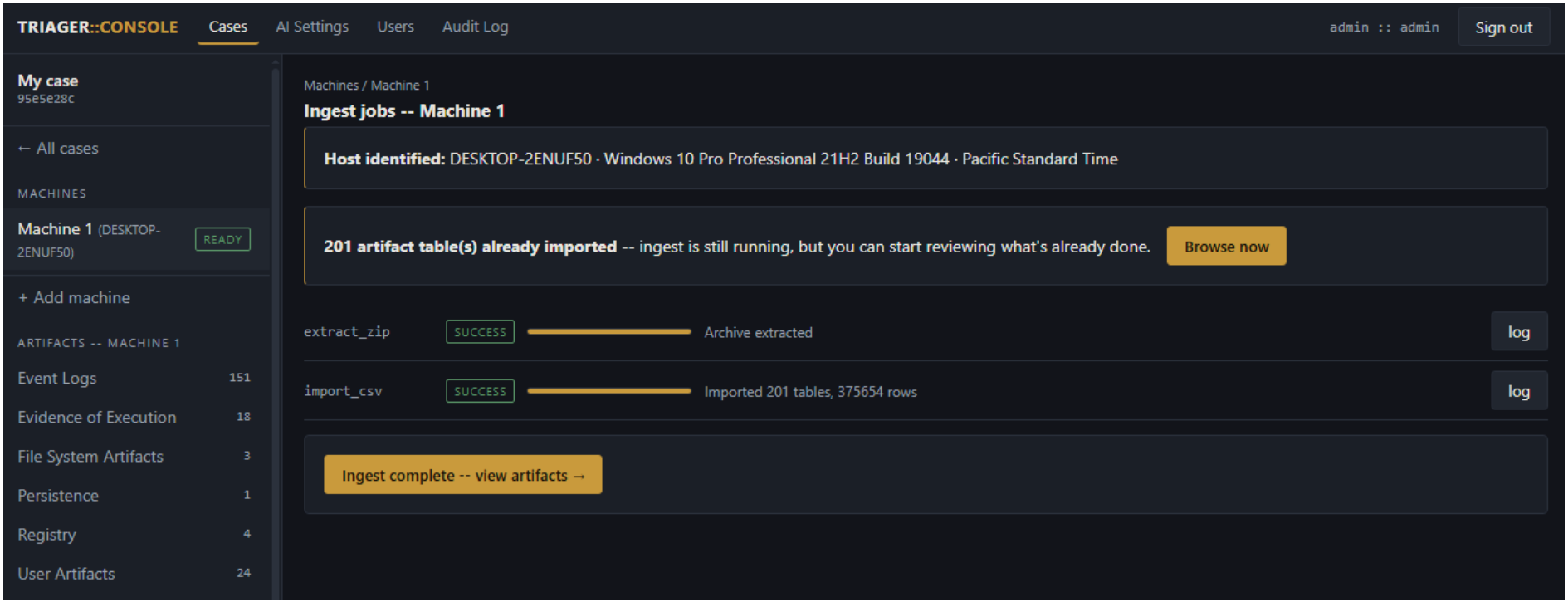
# Architecture and implementation

- The Web Console exposes a structured correlation query language.
- Example: `amcache.publisher not_contains microsoft`
- Processed evidence, table data, and timeline or correlation results can all be exported as CSV.
- A full Word (`.docx`) investigation report can be generated directly from the web interface.

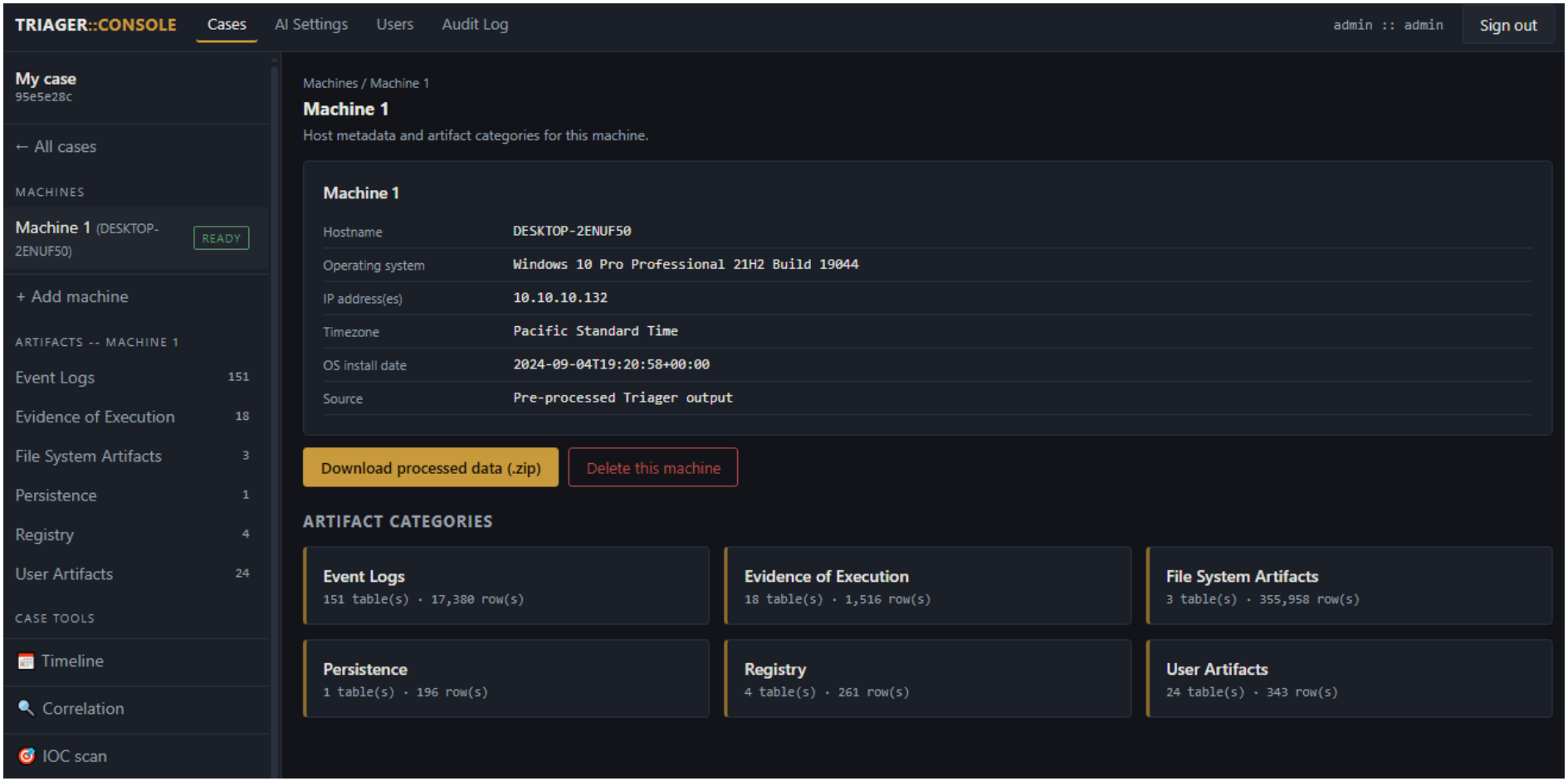
# Usage


Triager
C:\Users\user\Desktop\Triager.exe
Triager Console
Open in your browser: http://localhost:8000
Press Ctrl+C here to stop the server.
Running on localhost only
INFO: Started server process [10164]
INFO: Waiting for application startup.
[!] WARNING: TRIAGER_WEB_JWT_SECRET is still
[!] Every login token can be forged by anyone
[!] Set a real secret before exposing this be
INFO: Application startup complete.
INFO: Uvicorn running on http://127.0.0.1
INFO: 127.0.0.1:49762 - "GET /api/health
INFO: 127.0.0.1:49763 - "GET / HTTP/1.1"
INFO: 127.0.0.1:49765 - "GET /styles.css
INFO: 127.0.0.1:49766 - "GET /vendor/mark
INFO: 127.0.0.1:49767 - "GET /vendor/puri
INFO: 127.0.0.1:49768 - "GET /app.js HTTP
INFO: 127.0.0.1:49768 - "GET /cases HTTP/
INFO: 127.0.0.1:49768 - "GET /favicon.ico
INFO: 127.0.0.1:49867 - "POST /auth/login
INFO: 127.0.0.1:49913 - "POST /auth/login
Triager Console
127.0.0.1:8000
TRIAGER::CONSOLE
Cases
AI Settings
Users
Audit Log
Cases
2 case(s) visible to you
+ New case
Import case
Test case
no reference · 93a05aa3
OPEN
Delete
My case
no reference · 8c571714
OPEN
Delete

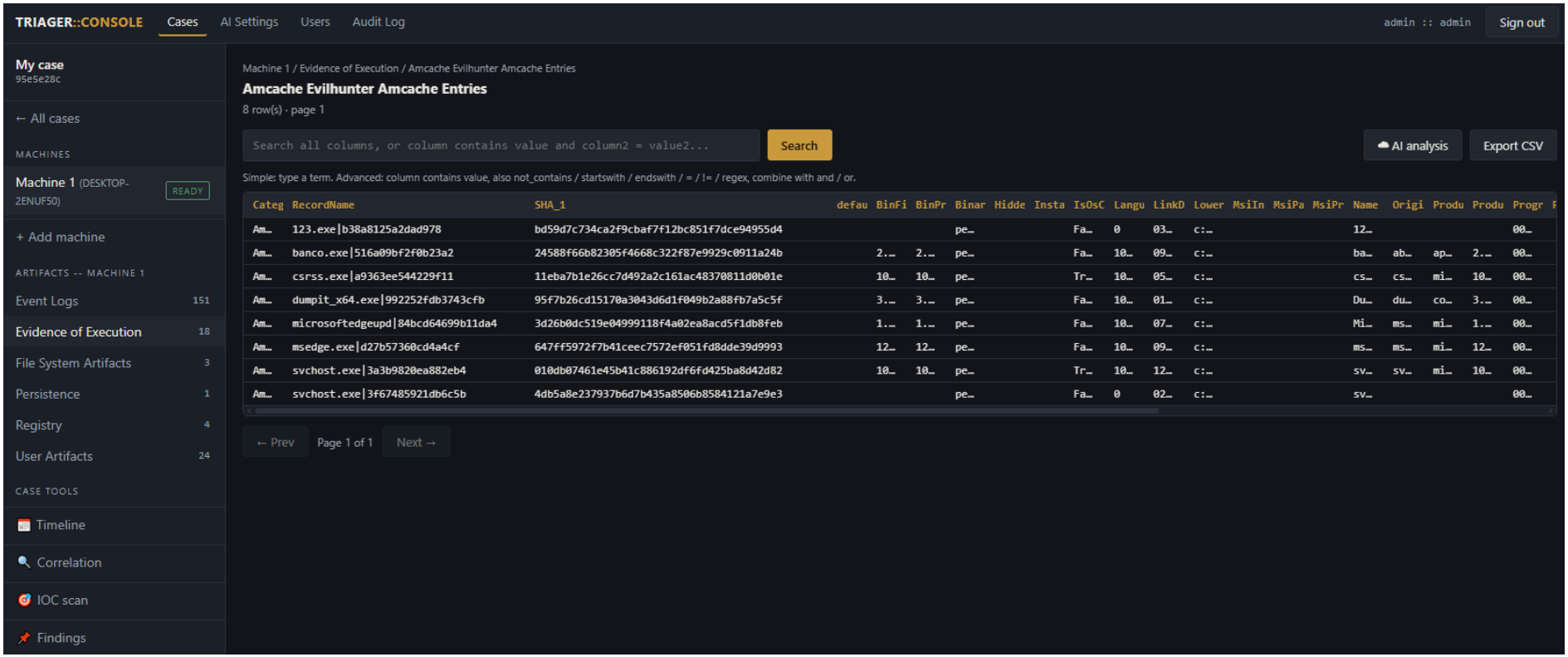
# Usage


TRIAGER::CONSOLE
Cases
AI Settings
Users
Audit Log
admin :: admin
Sign out
My case
95e5e28c
← All cases
MACHINES
Machine 1 (DESKTOP-2ENUF50)
READY
+ Add machine
ARTIFACTS -- MACHINE 1
Event Logs 151
Evidence of Execution 18
File System Artifacts 3
Persistence 1
Registry 4
User Artifacts 24
Machines / Machine 1
Ingest jobs -- Machine 1
Host identified: DESKTOP-2ENUF50 · Windows 10 Pro Professional 21H2 Build 19044 · Pacific Standard Time
201 artifact table(s) already imported -- ingest is still running, but you can start reviewing what's already done.
Browse now
extract_zip
SUCCESS
Archive extracted
log
import_csv
SUCCESS
Imported 201 tables, 375654 rows
log
Ingest complete -- view artifacts →

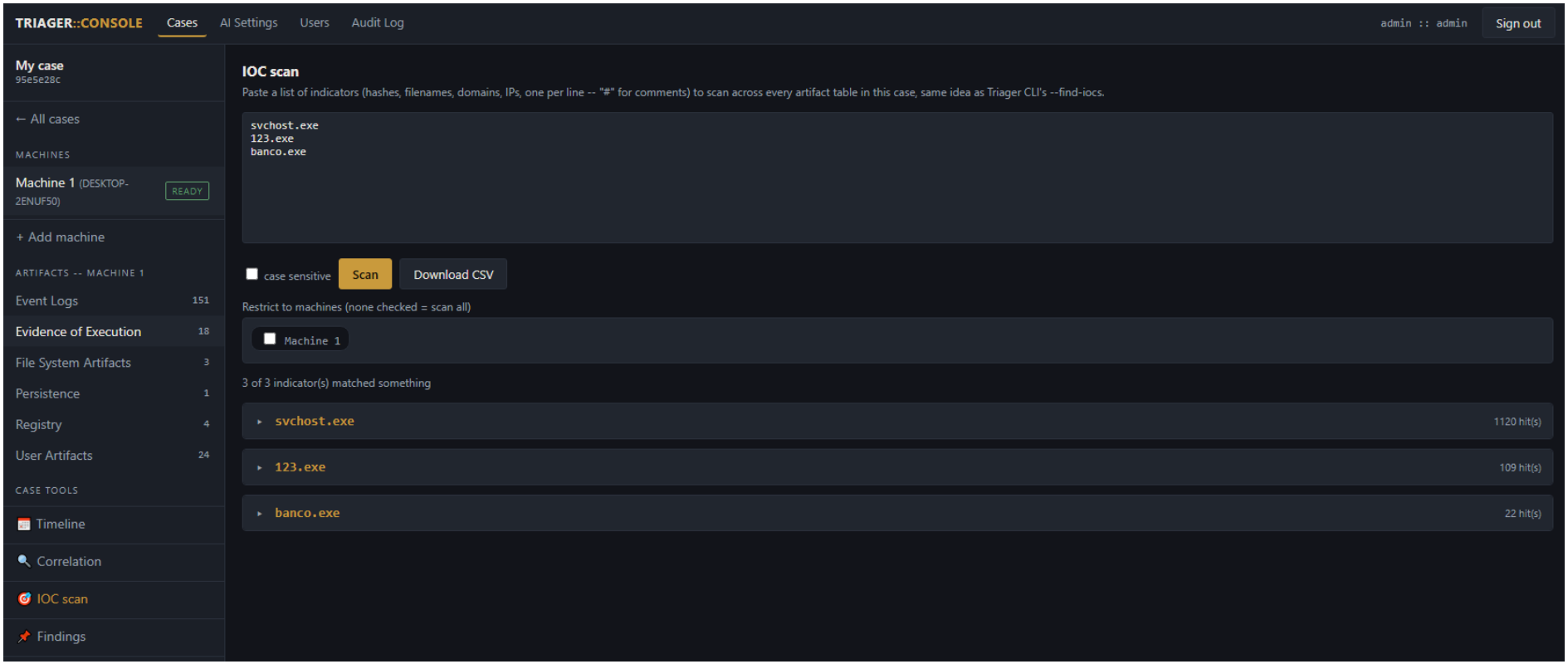
# Usage


TRIAGER::CONSOLE
Cases
AI Settings
Users
Audit Log
admin :: admin
Sign out
My case
95e5e28c
← All cases
MACHINES
Machine 1 (DESKTOP-2ENUF50)
READY
+ Add machine
ARTIFACTS -- MACHINE 1
Event Logs 151
Evidence of Execution 18
File System Artifacts 3
Persistence 1
Registry 4
User Artifacts 24
CASE TOOLS
Timeline
Correlation
IOC scan
Machines / Machine 1
Machine 1
Host metadata and artifact categories for this machine.
Machine 1
Hostname DESKTOP-2ENUF50
Operating system Windows 10 Pro Professional 21H2 Build 19044
IP address(es) 10.10.10.132
Timezone Pacific Standard Time
OS install date 2024-09-04T19:20:58+00:00
Source Pre-processed Triager output
Download processed data (.zip)
Delete this machine
ARTIFACT CATEGORIES
Event Logs
151 table(s) · 17,380 row(s)
Evidence of Execution
18 table(s) · 1,516 row(s)
File System Artifacts
3 table(s) · 355,958 row(s)
Persistence
1 table(s) · 196 row(s)
Registry
4 table(s) · 261 row(s)
User Artifacts
24 table(s) · 343 row(s)

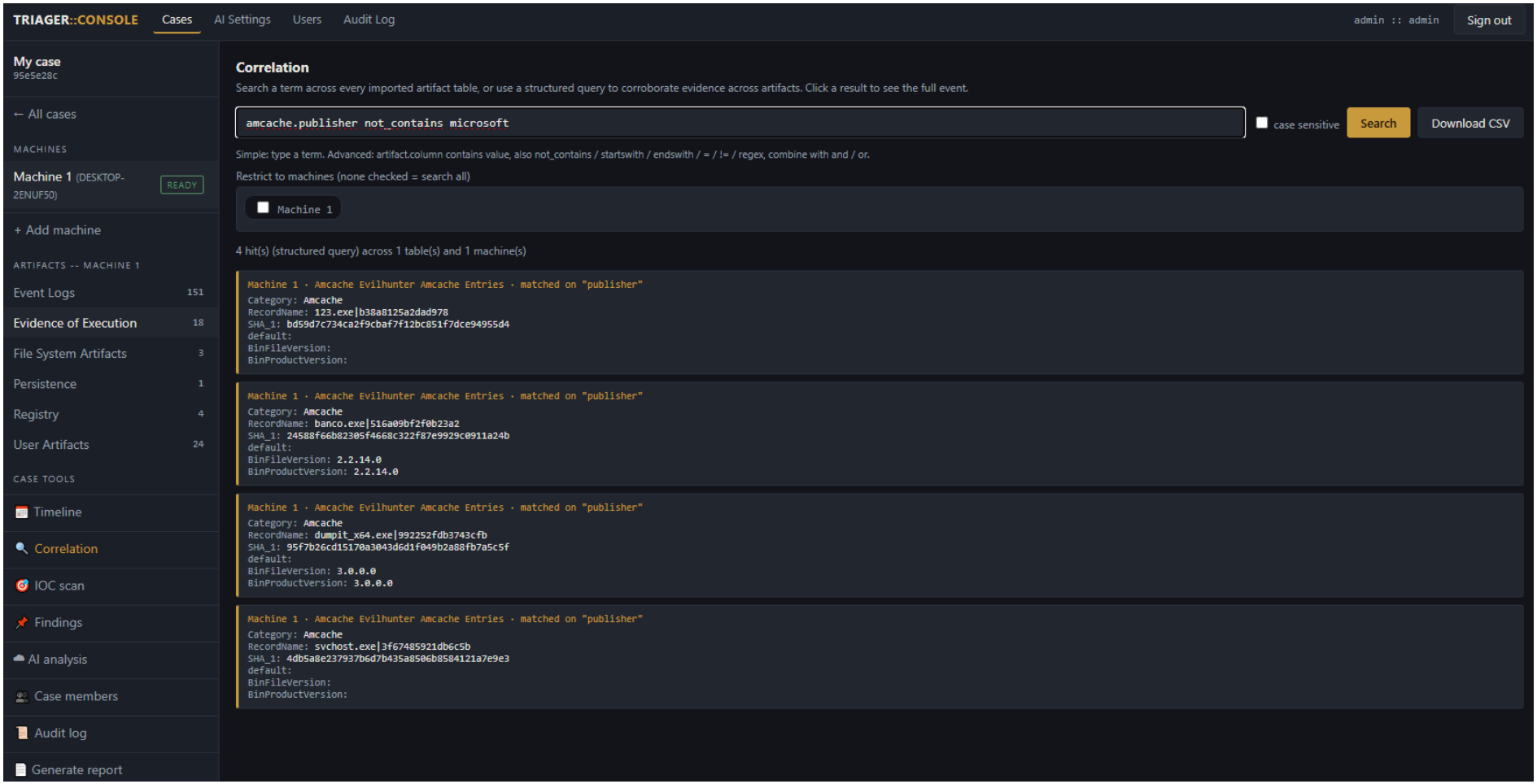
# Usage


TRIAGER::CONSOLE
Cases
AI Settings
Users
Audit Log
admin :: admin
Sign out
My case
95e5e28c
← All cases
MACHINES
Machine 1 (DESKTOP-2ENUF50)
READY
+ Add machine
ARTIFACTS -- MACHINE 1
Event Logs 151
Evidence of Execution 18
File System Artifacts 3
Persistence 1
Registry 4
User Artifacts 24
CASE TOOLS
Timeline
Correlation
IOC scan
Findings
Machine 1 / Evidence of Execution / Amcache Evilhunter Amcache Entries
Amcache Evilhunter Amcache Entries
8 row(s) · page 1
Search all columns, or column contains value and column2 = value2...
Search
AI analysis
Export CSV
Simple: type a term. Advanced: column contains value, also not_contains / startswith / endswith / = / != / regex, combine with and / or.
Categ RecordName SHA_1 defau BinFi BinPr Binar Hidde Insta IsOsC Langu LinkD Lower MsiIn MsiPa MsiPr Name Origi Produ Produ Progr
Am… 123.exe|b38a8125a2dad978 bd59d7c734ca2f9cbaf7f12bc851f7dce94955d4 pe… Fa… 0 03… c:… 12… 00…
Am… banco.exe|516a09bf2f0b23a2 24588f66b82305f4668c322f87e9929c0911a24b 2.… 2.… pe… Fa… 10… 09… c:… ba… ab… ap… 2.… 00…
Am… csrss.exe|a9363ee544229f11 11eba7b1e26cc7d492a2c161ac48370811d0b01e 10… 10… pe… Tr… 10… 05… c:… cs… cs… mi… 10… 00…
Am… dumpit_x64.exe|992252fdb3743cfb 95f7b26cd15170a3043d6d1f049b2a88fb7a5c5f 3.… 3.… pe… Fa… 10… 01… c:… Du… du… co… 3.… 00…
Am… microsoftedgeupd|84bcd64699b11da4 3d26b0dc519e04999118f4a02ea8acd5f1db8feb 1.… 1.… pe… Fa… 10… 07… c:… Mi… ms… mi… 1.… 00…
Am… msedge.exe|d27b57360cd4a4cf 647ff5972f7b41ceec7572ef051fd8dde39d9993 12… 12… pe… Fa… 10… 09… c:… ms… ms… mi… 12… 00…
Am… svchost.exe|3a3b9820ea882eb4 010db07461e45b41c886192df6fd425ba8d42d82 10… 10… pe… Tr… 10… 12… c:… sv… sv… mi… 10… 00…
Am… svchost.exe|3f67485921db6c5b 4db5a8e237937b6d7b435a8506b8584121a7e9e3 pe… Fa… 0 02… c:… sv… 00…
← Prev
Page 1 of 1
Next →

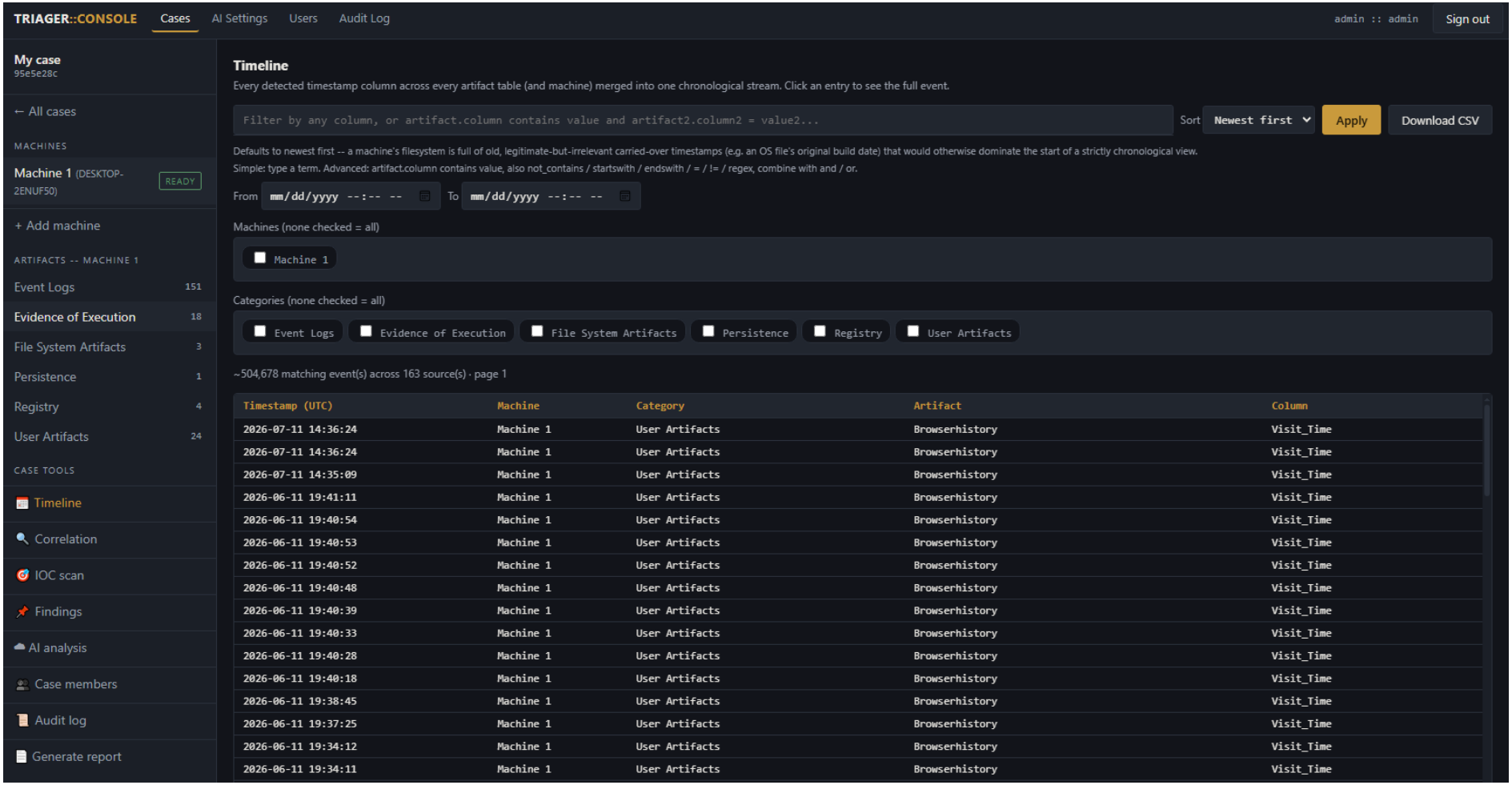
# Usage


TRIAGER::CONSOLE
Cases
AI Settings
Users
Audit Log
admin :: admin
Sign out
My case
95e5e28c
← All cases
MACHINES
Machine 1 (DESKTOP-2ENUF50)
READY
+ Add machine
ARTIFACTS -- MACHINE 1
Event Logs 151
Evidence of Execution 18
File System Artifacts 3
Persistence 1
Registry 4
User Artifacts 24
CASE TOOLS
Timeline
Correlation
IOC scan
Findings
IOC scan
Paste a list of indicators (hashes, filenames, domains, IPs, one per line -- "#" for comments) to scan across every artifact table in this case, same idea as Triager CLI's --find-iocs.
svchost.exe
123.exe
banco.exe
case sensitive
Scan
Download CSV
Restrict to machines (none checked = scan all)
Machine 1
3 of 3 indicator(s) matched something
svchost.exe 1120 hit(s)
123.exe 109 hit(s)
banco.exe 22 hit(s)

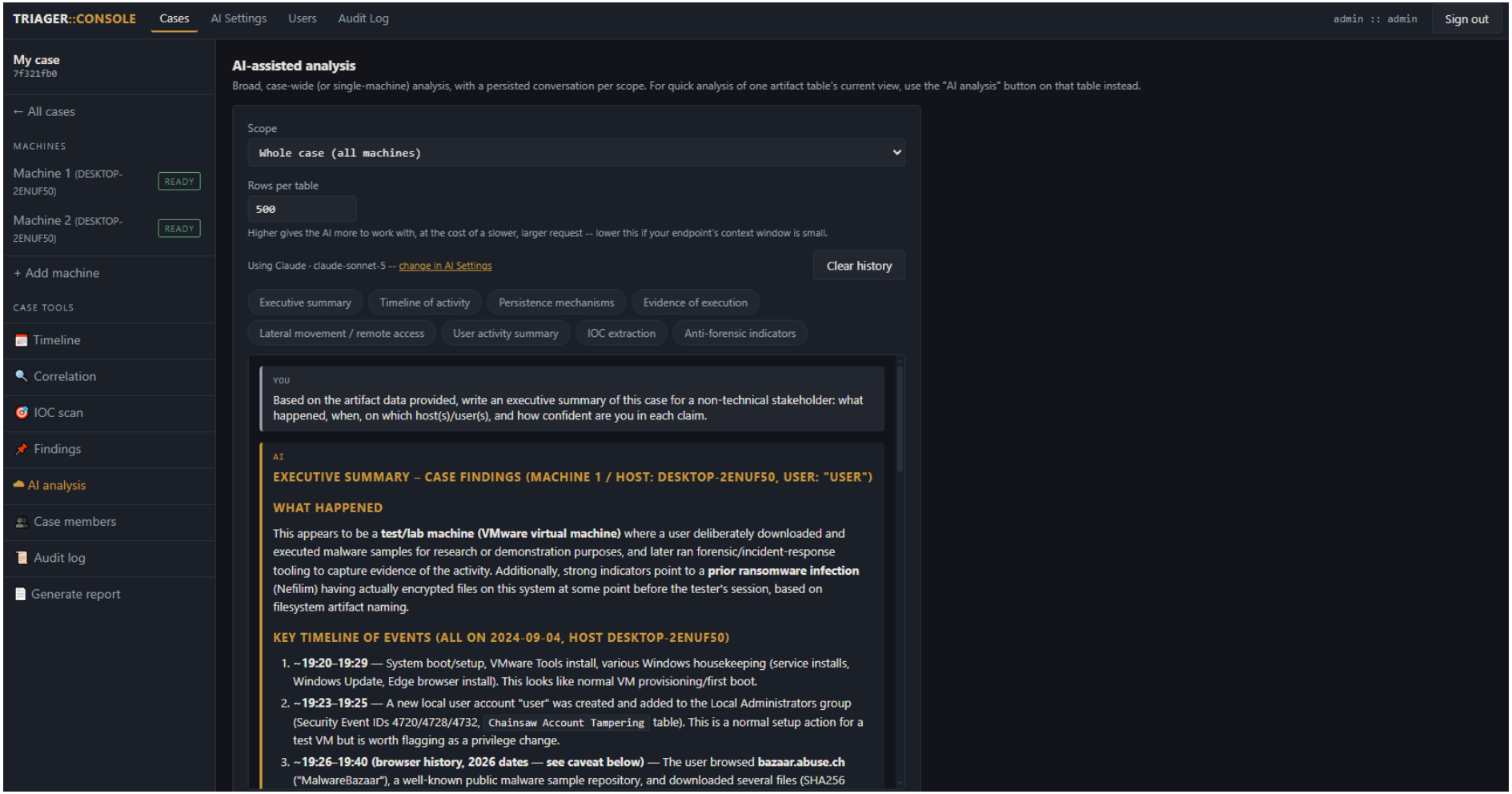
# Usage


TRIAGER::CONSOLE
Cases
AI Settings
Users
Audit Log
admin :: admin
Sign out
My case
95e5e28c
← All cases
MACHINES
Machine 1 (DESKTOP-2ENUF50)
READY
+ Add machine
ARTIFACTS -- MACHINE 1
Event Logs 151
Evidence of Execution 18
File System Artifacts 3
Persistence 1
Registry 4
User Artifacts 24
CASE TOOLS
Timeline
Correlation
IOC scan
Findings
AI analysis
Case members
Audit log
Generate report
Correlation
Search a term across every imported artifact table, or use a structured query to corroborate evidence across artifacts. Click a result to see the full event.
amcache.publisher not_contains microsoft
case sensitive
Search
Download CSV
Simple: type a term. Advanced: artifact.column contains value, also not_contains / startswith / endswith / = / != / regex, combine with and / or.
Restrict to machines (none checked = search all)
Machine 1
4 hit(s) (structured query) across 1 table(s) and 1 machine(s)
Machine 1 · Amcache Evilhunter Amcache Entries · matched on "publisher"
Category: Amcache
RecordName: 123.exe|b38a8125a2dad978
SHA_1: bd59d7c734ca2f9cbaf7f12bc851f7dce94955d4
default:
BinFileVersion:
BinProductVersion:
Machine 1 · Amcache Evilhunter Amcache Entries · matched on "publisher"
Category: Amcache
RecordName: banco.exe|516a09bf2f0b23a2
SHA_1: 24588f66b82305f4668c322f87e9929c0911a24b
default:
BinFileVersion: 2.2.14.0
BinProductVersion: 2.2.14.0
Machine 1 · Amcache Evilhunter Amcache Entries · matched on "publisher"
Category: Amcache
RecordName: dumpit_x64.exe|992252fdb3743cfb
SHA_1: 95f7b26cd15170a3043d6d1f049b2a88fb7a5c5f
default:
BinFileVersion: 3.0.0.0
BinProductVersion: 3.0.0.0
Machine 1 · Amcache Evilhunter Amcache Entries · matched on "publisher"
Category: Amcache
RecordName: svchost.exe|3f67485921db6c5b
SHA_1: 4db5a8e237937b6d7b435a8506b8584121a7e9e3
default:
BinFileVersion:
BinProductVersion:

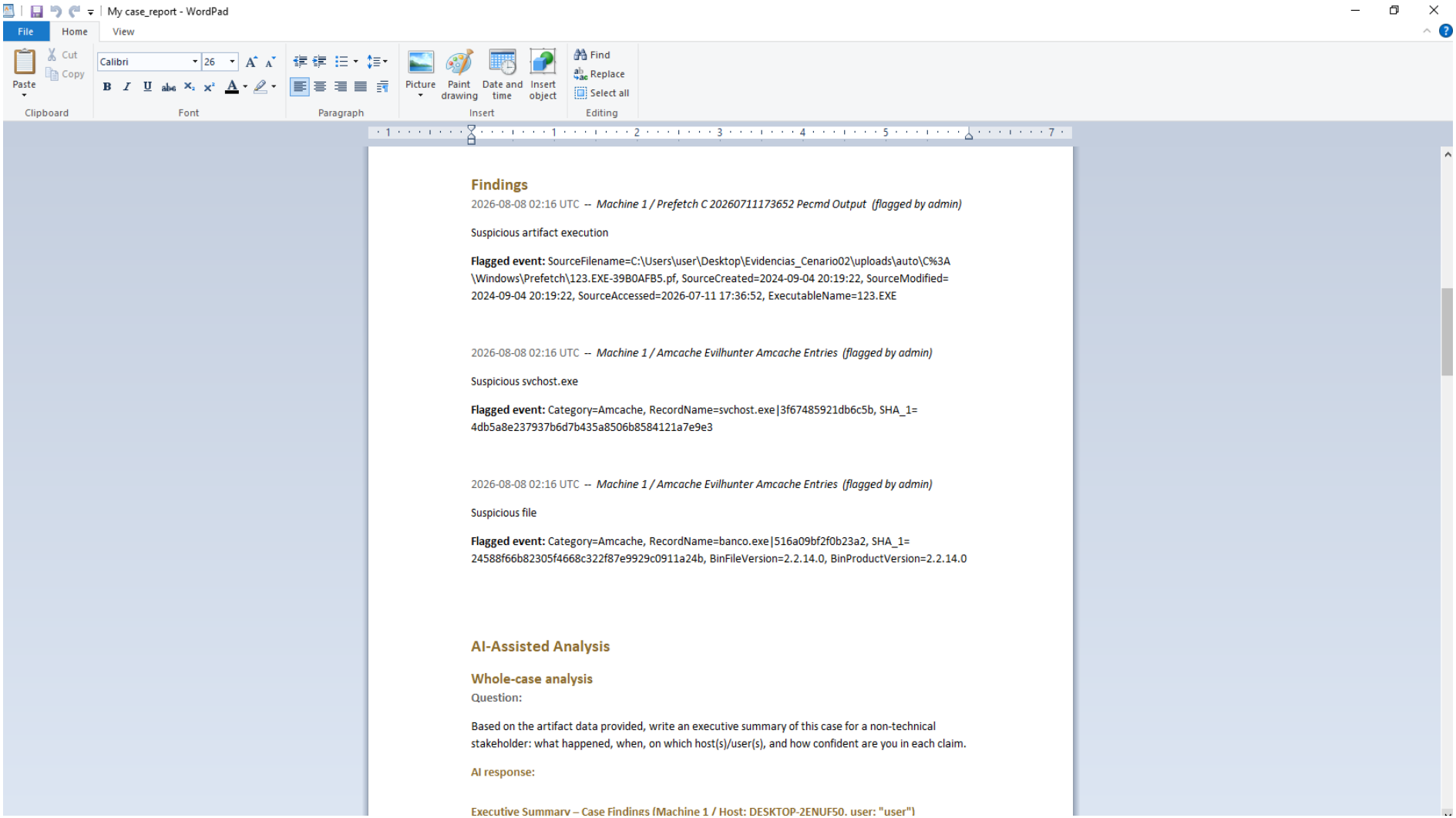
# Usage


TRIAGER::CONSOLE
Cases
AI Settings
Users
Audit Log
admin :: admin
Sign out
My case
95e5e28c
← All cases
MACHINES
Machine 1 (DESKTOP-2ENUF50)
READY
+ Add machine
ARTIFACTS -- MACHINE 1
Event Logs 151
Evidence of Execution 18
File System Artifacts 3
Persistence 1
Registry 4
User Artifacts 24
CASE TOOLS
Timeline
Correlation
IOC scan
Findings
AI analysis
Case members
Audit log
Generate report
Timeline
Every detected timestamp column across every artifact table (and machine) merged into one chronological stream. Click an entry to see the full event.
Filter by any column, or artifact.column contains value and artifact2.column2 = value2...
Sort
Newest first
Apply
Download CSV
Defaults to newest first -- a machine's filesystem is full of old, legitimate-but-irrelevant carried-over timestamps (e.g. an OS file's original build date) that would otherwise dominate the start of a strictly chronological view.
Simple: type a term. Advanced: artifact.column contains value, also not_contains / startswith / endswith / = / != / regex, combine with and / or.
From
mm/dd/yyyy --:-- --
To
mm/dd/yyyy --:-- --
Machines (none checked = all)
Machine 1
Categories (none checked = all)
Event Logs
Evidence of Execution
File System Artifacts
Persistence
Registry
User Artifacts
~504,678 matching event(s) across 163 source(s) · page 1
Timestamp (UTC) Machine Category Artifact Column
2026-07-11 14:36:24 Machine 1 User Artifacts Browserhistory Visit_Time
2026-07-11 14:36:24 Machine 1 User Artifacts Browserhistory Visit_Time
2026-07-11 14:35:09 Machine 1 User Artifacts Browserhistory Visit_Time
2026-06-11 19:41:11 Machine 1 User Artifacts Browserhistory Visit_Time
2026-06-11 19:40:54 Machine 1 User Artifacts Browserhistory Visit_Time
2026-06-11 19:40:53 Machine 1 User Artifacts Browserhistory Visit_Time
2026-06-11 19:40:52 Machine 1 User Artifacts Browserhistory Visit_Time
2026-06-11 19:40:48 Machine 1 User Artifacts Browserhistory Visit_Time
2026-06-11 19:40:39 Machine 1 User Artifacts Browserhistory Visit_Time
2026-06-11 19:40:33 Machine 1 User Artifacts Browserhistory Visit_Time
2026-06-11 19:40:28 Machine 1 User Artifacts Browserhistory Visit_Time
2026-06-11 19:40:18 Machine 1 User Artifacts Browserhistory Visit_Time
2026-06-11 19:38:45 Machine 1 User Artifacts Browserhistory Visit_Time
2026-06-11 19:37:25 Machine 1 User Artifacts Browserhistory Visit_Time
2026-06-11 19:34:12 Machine 1 User Artifacts Browserhistory Visit_Time
2026-06-11 19:34:11 Machine 1 User Artifacts Browserhistory Visit_Time

# Usage


TRIAGER::CONSOLE
Cases
AI Settings
Users
Audit Log
admin :: admin
Sign out
My case
7f321fb0
← All cases
MACHINES
Machine 1 (DESKTOP-2ENUF50)
READY
Machine 2 (DESKTOP-2ENUF50)
READY
+ Add machine
CASE TOOLS
Timeline
Correlation
IOC scan
Findings
AI analysis
Case members
Audit log
Generate report
AI-assisted analysis
Broad, case-wide (or single-machine) analysis, with a persisted conversation per scope. For quick analysis of one artifact table's current view, use the "AI analysis" button on that table instead.
Scope
Whole case (all machines)
Rows per table
500
Higher gives the AI more to work with, at the cost of a slower, larger request -- lower this if your endpoint's context window is small.
Using Claude · claude-sonnet-5 -- change in AI Settings
Clear history
Executive summary
Timeline of activity
Persistence mechanisms
Evidence of execution
Lateral movement / remote access
User activity summary
IOC extraction
Anti-forensic indicators
YOU
Based on the artifact data provided, write an executive summary of this case for a non-technical stakeholder: what happened, when, on which host(s)/user(s), and how confident are you in each claim.
AI
EXECUTIVE SUMMARY – CASE FINDINGS (MACHINE 1 / HOST: DESKTOP-2ENUF50, USER: "USER")
WHAT HAPPENED
This appears to be a test/lab machine (VMware virtual machine) where a user deliberately downloaded and executed malware samples for research or demonstration purposes, and later ran forensic/incident-response tooling to capture evidence of the activity. Additionally, strong indicators point to a prior ransomware infection (Nefilim) having actually encrypted files on this system at some point before the tester's session, based on filesystem artifact naming.
KEY TIMELINE OF EVENTS (ALL ON 2024-09-04, HOST DESKTOP-2ENUF50)
1. ~19:20–19:29 — System boot/setup, VMware Tools install, various Windows housekeeping (service installs, Windows Update, Edge browser install). This looks like normal VM provisioning/first boot.
2. ~19:23–19:25 — A new local user account "user" was created and added to the Local Administrators group (Security Event IDs 4720/4728/4732, Chainsaw Account Tampering table). This is a normal setup action for a test VM but is worth flagging as a privilege change.
3. ~19:26–19:40 (browser history, 2026 dates — see caveat below) — The user browsed bazaar.abuse.ch ("MalwareBazaar"), a well-known public malware sample repository, and downloaded several files (SHA256

# Usage


My case_report - WordPad
File
Home
View
Paste
Cut
Copy
Clipboard
Calibri
26
Font
Paragraph
Picture
Paint drawing
Date and time
Insert object
Insert
Find
Replace
Select all
Editing
Findings
2026-08-08 02:16 UTC -- Machine 1 / Prefetch C 20260711173652 Pecmd Output (flagged by admin)
Suspicious artifact execution
Flagged event: SourceFilename=C:\Users\user\Desktop\Evidencias_Cenario02\uploads\auto\C%3A\Windows\Prefetch\123.EXE-39B0AFB5.pf, SourceCreated=2024-09-04 20:19:22, SourceModified=2024-09-04 20:19:22, SourceAccessed=2026-07-11 17:36:52, ExecutableName=123.EXE
2026-08-08 02:16 UTC -- Machine 1 / Amcache Evilhunter Amcache Entries (flagged by admin)
Suspicious svchost.exe
Flagged event: Category=Amcache, RecordName=svchost.exe|3f67485921db6c5b, SHA_1=4db5a8e237937b6d7b435a8506b8584121a7e9e3
2026-08-08 02:16 UTC -- Machine 1 / Amcache Evilhunter Amcache Entries (flagged by admin)
Suspicious file
Flagged event: Category=Amcache, RecordName=banco.exe|516a09bf2f0b23a2, SHA_1=24588f66b82305f4668c322f87e9929c0911a24b, BinFileVersion=2.2.14.0, BinProductVersion=2.2.14.0
AI-Assisted Analysis
Whole-case analysis
Question:
Based on the artifact data provided, write an executive summary of this case for a non-technical stakeholder: what happened, when, on which host(s)/user(s), and how confident are you in each claim.
AI response:
Executive Summary – Case Findings (Machine 1 / Host: DESKTOP-2ENUF50, user: "user")

# Conclusion

- `Triager`: open-source DFIR automation and investigation platform for Windows triage collections.
- Processing engine: orchestrates parsers, extracts host data from registry hives, normalizes outputs, and supports CLI search and IOC hunting.
- Web Console: multi-case and multi-machine management, cross-machine correlation, unified timeline, IOC scanning, AI-assisted analysis, and automated reporting.
- Distributed as a single binary.

# Triager

## An Open-Source Platform for Automated Forensic Triage and Investigation

**Cristian Souza**, Eduardo Ovalle and Daniel Batista

DFIR Specialist, Ph.D. Candidate