

# Forensics Analysis

From Incident Response to Digital Forensics

Ondřej Šrámek · Czechitas · 2026





Linktree

## Ondřej Šrámek

GMON, GNFA, GCTI

- Worked in the public sector and commercial sector
- 12+ years in the field, primarily Incident Response, DFIR, Threat Hunting and Threat Intelligence

# Agenda

# Agenda



Disclaimer



Environment Setup



Digital Forensics



Data Acquisition



Artifact Analysis



Memory Analysis



AI in Forensic Analysis



Forensics Challenge

# Disclaimer

*"With great power there must also come great responsibility!" — Spider-Man*

In the following lesson you will get a lot of useful information. Their misuse or use by the dark side could mean significant disruption to future forensic investigations.

Consider this lesson and presentation as **need to know, TLP:RED**

# Write Down Your Notes

Context matters!

- Paper vs. Flipchart vs. DFIR-IRIS
- MISP/OpenCTI/Case Management (The Hive)
- Map findings to MITRE ATT&CK TTPs
- (Super)Timeline!

# Environment

Windows vs. Linux vs. macOS

# Your (Forensic) Environment

Your analysis machine should be **isolated**

- **No AV** — extracted files vs. AV/EDR
- Watch out for malware execution
- Created for **Windows** → SIFT / macOS / WIN-FOR
- Created for **macOS** → WIN-FOR / macOS / Linux
- Collaboration
- Malware analysis / IR / CTI

# Our Setup

Tool	Purpose
<b>KAPE</b>	Artifact collection from Windows
<b>Dumplt</b>	Memory dump
<b>Splunk / Timeline Explorer</b>	Analyze collected artifacts
<b>Volatility</b>	Memory analysis
<b>Kali / Remnux / SIFT</b>	Analysis environment

# Digital Forensics

# This is NOT Forensics



# This is How It Works



# Evidence Gathering

## General Approach

- **Hash** of evidence (log, disc image, ...)
- Source (device) + Path (log/file gathered)
- Owner
- Timestamp (when gathered)
- Malware in archive with password **infected**
- Physical specifics
  - Handover protocol
  - Photography of evidence
  - Evidence bag (antistatic)

# What Are We Looking For?

Artifacts vs. Confirmation of Presence

# Goals / Tasks

## Following Incident Response

- Root Cause / Impact Analysis
- Confirm Hypothesis
  - Presence of specific files (Crime / Exfiltration)
  - Website visit (Crime / Hack)
  - Actions done (Crime / Hack)
- Root Cause
- Attacker's Path

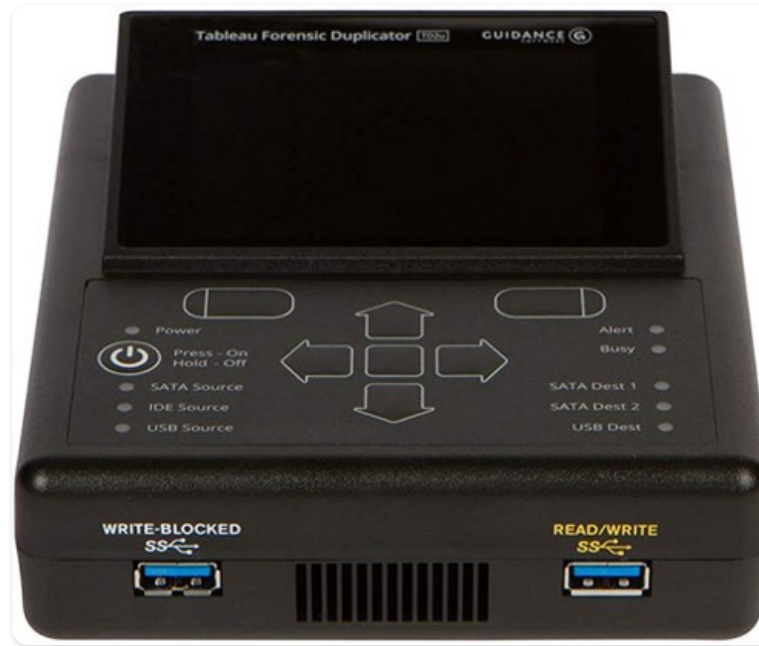
# Preparation

- OSINT
- CTI
- RFI (Request for Information)
- Files, Paths
- Timestamps
- Others

# Data Acquisition

Memory, disc, ...

# Disc Image



# Mobile Device Acquisition



# Full Scale vs. Artifact Extraction

Sometimes full scale is **not needed** (no lawsuit)

- Grab the necessary files
- Limited impact (blocked by AV/EDR)
  - Browser History, Downloaded Files, ...
  - Grab via KAPE, CyLR, Velociraptor or other agent
- **Always note path and hash**
- Context!

# **Artifact Collection**

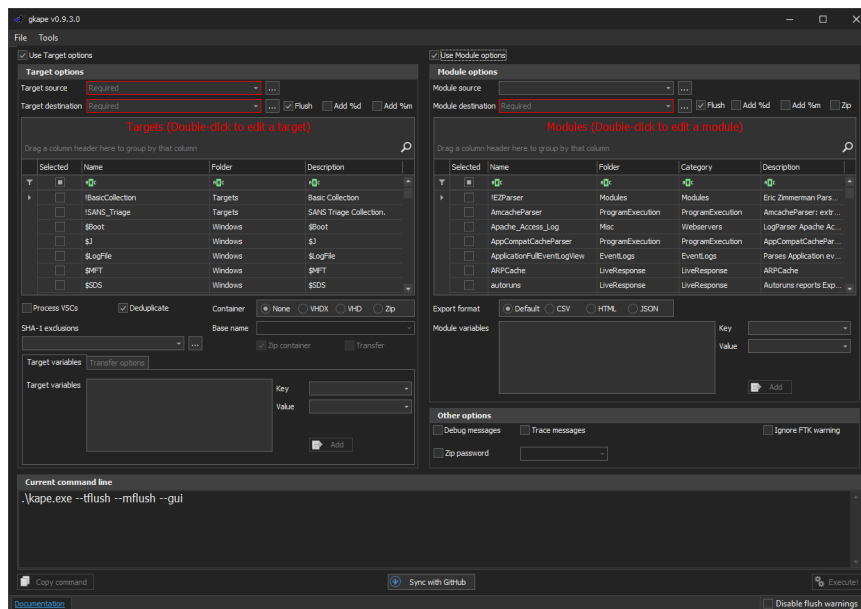
# KAPE

Artifact parser and Extractor — [official site](#)

**Targets** — what will be grabbed

- Virtual disc
- Mounted system
- Live

**Modules** — how to process data



# KAPE GUI

The screenshot displays the KAPE GUI interface, version v0.9.3.0. The interface is divided into several sections:

- File Tools:** Contains checkboxes for "Use Target options" and "Use Module options".
- Target options:** Includes fields for "Target source" and "Target destination", along with checkboxes for "Flush", "Add %d", and "Add %m".
- Targets (Double-click to edit a target):** A table listing various targets with columns for "Selected", "Name", "Folder", and "Description".
- Modules (Double-click to edit a module):** A table listing various modules with columns for "Select...", "Name", "Folder", "Category", and "Description".
- Process VSCs:** Includes a "Deduplicate" checkbox and radio buttons for "None", "VHDX", "VHD", and "Zip".
- SHA-1 exclusions:** A field for "Base name" and checkboxes for "Zip container" and "Transfer".
- Target variables:** A table for defining variables with "Key" and "Value" columns, and an "Add" button.
- Export format:** Radio buttons for "Default", "CSV", "HTML", and "JSON".
- Module variables:** A table for defining variables with "Key" and "Value" columns, and an "Add" button.
- Other options:** Checkboxes for "Debug messages", "Trace messages", and "Ignore FTK warning", along with a "Zip password" field.
- Current command line:** A text area showing the command `.\kape.exe --gui`.
- Footer:** Includes a "Copy command" button, a "Sync with GitHub" button, an "Execute" button, a "Documentation" link, and a "Disable flush warnings" checkbox.

# KAPE — Configuration

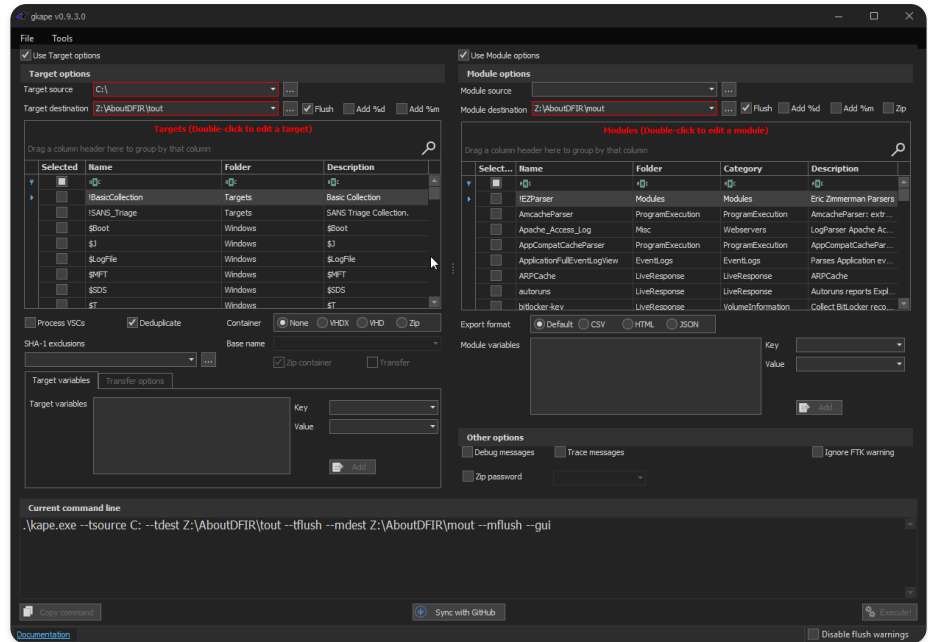
Run as **Admin**, sync with GitHub

## Target

- !SANS\_Triage
- !BasicCollection
- Container: **None**

## Module

- !EZParser
- Export format: **JSON**



# From KAPE to Splunk / Timeline Explorer

1. Take the output (JSON), zip and transfer to your Splunk (Kali)
2. Import → Create a separate index
3. **Splunk time!**

If you have CSV (as KAPE output), open it in **Timeline Explorer**

# Splunk / Timeline Explorer - Demo time

The screenshot displays the Splunk Timeline Explorer interface. On the left, a table lists event logs with columns for Row, Timestamp, Sourcefile, Channel, EventID, Provider, Computer, User, and Description. The right pane shows a 'New Search' configuration with the following search string: `index="wineventlog" sourcetype="WinEventLog:*" | stats count by _time, ComputerName, EventCode, Channel, Message | sort 0 + _time`. Below the search configuration, a table displays search results with columns for \_time, ComputerName, EventCode, Channel, and count.

Row	Timestamp	Sourcefile	Channel	EventID	Provider	Computer	User	Description
1	5/14/2024 07:59:58.123	Security.evtx	Security	4624	Microsoft-Windows-Security-Auditing	WIN10-CLIENT	SYSTEM	An account was successfully logged on.
2	5/14/2024 07:59:59.456	Security.evtx	Security	4634	Microsoft-Windows-Security-Auditing	WIN10-CLIENT	SYSTEM	An account was logged off.
3	5/14/2024 08:00:00.789	Security.evtx	Security	4672	Microsoft-Windows-Security-Auditing	WIN10-CLIENT	ADMINISTRATOR	Special privileges assigned to new logon.
4	5/14/2024 08:03:12.101	Security.evtx	Security	4688	Microsoft-Windows-Security-Auditing	WIN10-CLIENT	SYSTEM	A new process has been created.
5	5/14/2024 08:03:12.456	Security.evtx	Security	4688	Microsoft-Windows-Security-Auditing	WIN10-CLIENT	SYSTEM	A new process has been created.
6	5/14/2024 08:04:05.222	Security.evtx	Security	4720	Microsoft-Windows-Security-Auditing	WIN10-CLIENT	SYSTEM	A user account was created.
7	5/14/2024 08:04:05.223	Security.evtx	Security	4722	Microsoft-Windows-Security-Auditing	WIN10-CLIENT	SYSTEM	A user account was enabled.
8	5/14/2024 08:05:17.331	Security.evtx	Security	4719	Microsoft-Windows-Security-Auditing	WIN10-CLIENT	SYSTEM	System audit policy was changed.
9	5/14/2024 08:06:44.654	Security.evtx	Security	4688	Microsoft-Windows-Security-Auditing	WIN10-CLIENT	SYSTEM	A new process has been created.
10	5/14/2024 08:07:15.987	Security.evtx	Security	4663	Microsoft-Windows-Security-Auditing	WIN10-CLIENT	SYSTEM	An attempt was made to access an object.
11	5/14/2024 08:07:16.123	Security.evtx	Security	4656	Microsoft-Windows-Security-Auditing	WIN10-CLIENT	SYSTEM	A handle to an object was requested.
12	5/14/2024 08:10:22.456	Security.evtx	Security	1102	Microsoft-Windows-Eventlog	WIN10-CLIENT	SYSTEM	The audit log was cleared.
13	5/14/2024 08:12:31.789	System.evtx	System	7045	Microsoft-Windows-Service Control Manager	WIN10-CLIENT	SYSTEM	A service was installed in the system.
14	5/14/2024 08:12:32.001	System.evtx	System	7036	Microsoft-Windows-Service Control Manager	WIN10-CLIENT	SYSTEM	The service entered the running state.
15	5/14/2024 08:15:22.111	Security.evtx	Security	4624	Microsoft-Windows-Security-Auditing	WIN10-CLIENT	SYSTEM	An account was successfully logged on.
16	5/14/2024 08:15:27.222	Security.evtx	Security	4648	Microsoft-Windows-Security-Auditing	WIN10-CLIENT	SYSTEM	A logon was attempted using explicit credentials.
17	5/14/2024 08:16:03.333	Security.evtx	Security	4624	Microsoft-Windows-Security-Auditing	WIN10-CLIENT	SYSTEM	An account was successfully logged on.
18	5/14/2024 08:16:11.444	Security.evtx	Security	4625	Microsoft-Windows-Security-Auditing	WIN10-CLIENT	SYSTEM	An account failed to log on.
19	5/14/2024 08:18:45.555	Application.evtx	Application	1000	Application Error	WIN10-CLIENT	SYSTEM	Faulting application name: notepad.exe
20	5/14/2024 08:20:10.666	System.evtx	System	6005	Eventlog	WIN10-CLIENT	SYSTEM	The Event log service was started.
21	5/14/2024 08:21:33.777	Security.evtx	Security	4670	Microsoft-Windows-Security-Auditing	WIN10-CLIENT	SYSTEM	Permissions on an object were changed.

_time	ComputerName	EventCode	Channel	count
2024-05-14 07:59:58	WIN10-CLIENT	4624	Security	1
2024-05-14 07:59:59	WIN10-CLIENT	4634	Security	1
2024-05-14 08:00:00	WIN10-CLIENT	4672	Security	1
2024-05-14 08:03:12	WIN10-CLIENT	4688	Security	2
2024-05-14 08:04:05	WIN10-CLIENT	4720	Security	1
2024-05-14 08:04:05	WIN10-CLIENT	4722	Security	1
2024-05-14 08:05:17	WIN10-CLIENT	4719	Security	1
2024-05-14 08:06:44	WIN10-CLIENT	4688	Security	1
2024-05-14 08:07:15	WIN10-CLIENT	4663	Security	1
2024-05-14 08:07:16	WIN10-CLIENT	4656	Security	1
2024-05-14 08:10:22	WIN10-CLIENT	1102	Security	1
2024-05-14 08:12:31	WIN10-CLIENT	7045	System	1
2024-05-14 08:12:32	WIN10-CLIENT	7036	System	1
2024-05-14 08:15:22	WIN10-CLIENT	4624	Security	1
2024-05-14 08:15:27	WIN10-CLIENT	4648	Security	1
2024-05-14 08:16:03	WIN10-CLIENT	4624	Security	1
2024-05-14 08:16:11	WIN10-CLIENT	4625	Security	1
2024-05-14 08:18:45	WIN10-CLIENT	1000	Application	1
2024-05-14 08:20:10	WIN10-CLIENT	6005	System	1
2024-05-14 08:21:33	WIN10-CLIENT	4670	Security	1

# Artifact Analysis

From Data to CTI

# Gathering the Evidence

## Document everything

- Screenshot
- Copy line of the event
- IoCs (files, IPs, domains, URLs, ...)
- OSINT / CTI
- **Hash!** — MD5 + SHA1 + SHA256
  - `md5sum | sha1sum | sha256sum`
- From event to MITRE
  - Categorize each (attacker's) step to MITRE TTP

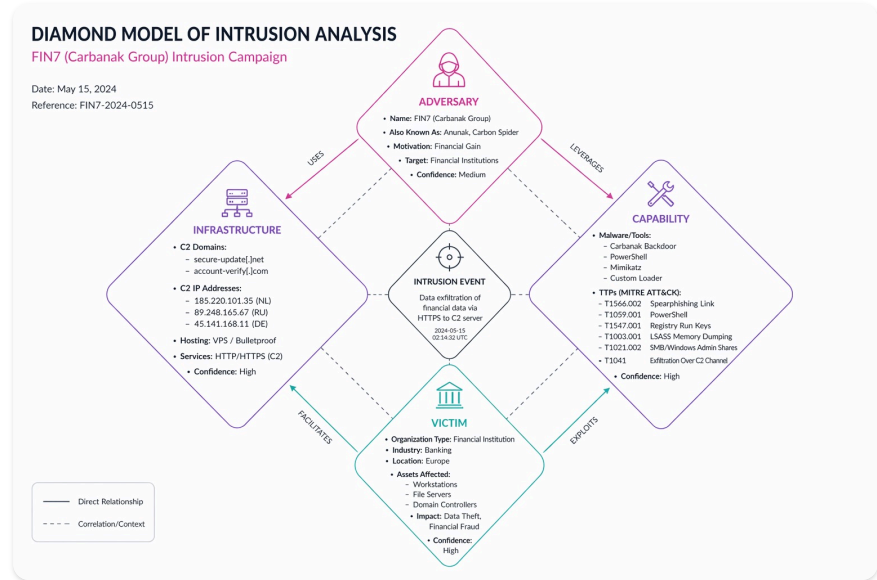
# Defanging

Defanging is a security practice that modifies potentially malicious indicators to make them **non-functional while still readable**.

Original	Defanged
<code>https://example.com</code>	<code>hxxps[://]example[.]com</code>
<code>https://example.com/login.php</code>	<code>hxxps[://]example[.]com/login[.]php</code>
<code>8.8.8.8</code>	<code>8[.]8[.]8[.]8</code>
<code>1.1.1.1:53</code>	<code>1[.]1[.]1[.]1[:]53</code>
<code>name.surname@example.com</code>	<code>name[.]surname@example[.]com</code>

# Diamond Model

Overlaps between attacks — two identical parts



# ACH — Analysis of Competing Hypotheses

Prepare information for CTI / attribution

1. Write down hypotheses
2. Confirm (support) / deny (refute) with gathered evidence

# Memory Analysis

# Volatility

App for memory analysis — **Python based**

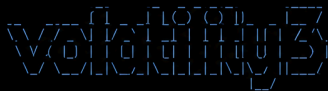
- [TryHackMe Room — Volatility](#)
- [TryHackMe Room — Memory Forensics](#)

# Memory Analysis — Key Plugins

Category	Plugin
<b>Processes</b>	<code>(windows linux mac).pslist</code> , <code>pstree</code> , <code>psxview</code>
<b>Connections</b>	<code>(windows linux mac).netstat</code> , <code>netscan</code>
<b>Commands (CLI)</b>	<code>(windows linux mac).cmdline</code> , <code>cmdscan</code>
<b>File Dump</b>	<code>(windows linux mac).pslist --pid XXXX --dump</code>
<b>Network traffic</b>	Via Network Miner Pro (Cap Loader)

# Volatility — Demo time

```
$ python3 vol.py -f memory.raw windows.pstree
```



```
Volatility 3 Framework 2.7.0
```

```
Progress: 100.00
```

```
PDB scanning finished
```

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime
4	0	System	0x9b2d8040	164	-	N/A	False	2024-05-14 08:15:22.000000
108	4	Registry	0x9b317330	4	-	N/A	False	2024-05-14 08:15:22.000000
372	4	smss.exe	0x9b31e6c0	2	-	N/A	False	2024-05-14 08:15:22.000000
452	556	csrss.exe	0x9b348080	11	-	0	False	2024-05-14 08:15:22.000000
500	556	wininit.exe	0x9b355a80	3	-	0	False	2024-05-14 08:15:22.000000
556	444	services.exe	0x9b35f0c0	9	-	0	False	2024-05-14 08:15:22.000000
564	444	lsass.exe	0x9b36b080	12	-	0	False	2024-05-14 08:15:23.000000
684	556	svchost.exe	0x9b377080	24	-	0	False	2024-05-14 08:15:23.000000
728	556	svchost.exe	0x9b3a8080	17	-	0	False	2024-05-14 08:15:24.000000
832	556	fontdrvhost.exe	0x9b3c2080	5	-	0	False	2024-05-14 08:15:24.000000
916	556	spoolsv.exe	0x9b3d5080	13	-	0	False	2024-05-14 08:15:24.000000
1072	1052	explorer.exe	0x9b456b80	48	1,201	1	False	2024-05-14 08:15:27.000000
├	2156	1072	cmd.exe	4	198	1	False	2024-05-14 08:16:03.000000
└	2892	2156	notepad.exe	2	87	1	False	2024-05-14 08:16:11.000000

```
... (output truncated) ...
```

# Forensics Challenge

section

# Information

- Alert triggered on **Windows 2008 R2 Server**
- Brute force attack detected
- Adversary has likely pentesting skills
- Gathered evidence can be found:
  - `Evidence\Windows2k8_KAPE_CSV.zip` (Timesketch)
  - `Evidence\Windows2k8_KAPE_JSON.zip` (Splunk)
  - `Evidence\Windows2k8_Mem_Dump.zip` (Volatility) — collected later than KAPE
  -
- Password is **infected**

# Find the Answers

## When? What? Where? Why? (Who?) and How?

Evidence may contain compromise of the server including persistence:

- Scanning
- Exploitation
- Persistence
- C2 communication

# It Is Not a Competition

- Try everything
- OSINT on the findings
- Defanging of IoCs
- Diamond Model
- Create a hypothesis → ACH
- Present your findings
- It is **not needed** to find everything the attacker did
- CTF

# Hints

## Find something 100% suspicious

- C2 Communication
- Weird process / binary

## Leverage the knowledge

- What happened before
- What happened after

**Document** → Create a big picture

# Feedback

## Executive Summary

- Prepare for the answers
- **Facts!** Not assumptions (evidence)
- Lessons Learned / Hardening if needed

**(Real World) Examples**

# Apple Watch

## **Police use Apple Watch health data as evidence in murder case**

Fitness data was submitted as evidence.

## **Husband buries wife alive, smashes Apple Watch to stop her calling for help**

# Browser History

## MURDER OF KARI BAKER

One of the earlier cases using digital evidence was the murder of **Kari Baker**. In 2010, Baker's husband, Matt Baker was convicted of his wife's murder and sentenced to 65 years in prison. In 2006, Texas elementary school teacher, Kari Baker was found dead from a supposed suicide by sleeping pills. Baker had forged a suicide note for police. When police searched his computer, the history revealed searches for "overdosing on sleeping pills". That, along with **physical evidence** of the pills was enough to convict Baker.

# Pacemaker

## ROSS COMPTON

One of the most interesting pieces of digital evidence was used in the Ross Compton case. In 2016, Compton set fire to his Middletown, Ohio home as a part of an insurance fraud scam. During the investigation of the fire, Compton, who has a pacemaker with an external pump, told police he was asleep when the fire started. He told police when he woke up and saw the fire, he packed a suitcase, broke his bedroom window with a cane, and escaped. During the investigation, police ordered the data from Compton's pacemaker and consulted with a cardiologist who found that Compton could not have escaped the fire based on data from his pacemaker. Compton also submitted forged medical records that did not match the pacemaker data. The pacemaker data included heart rate, pacer demand, and heart rhythms which were used as evidence to prove insurance fraud and arson.

# Serial Killer Sent a Floppy

Fast forward to 2004, when Rader made a fatal mistake. He sent a floppy disk to the police, believing it was untraceable. However, he was wrong.

Digital forensics experts were able to recover deleted data from the disk, which led them to a computer at a local church.

# GPS Data

In the days following April's disappearance, investigators turned to digital forensics to build their case against Bridger.

They discovered that he had attempted to destroy evidence by deleting files and wiping his computer's hard drive.

But digital forensics experts were able to recover critical data, including images of April and internet searches related to child abduction and murder.

Digital forensics also played a role in linking Bridger's vehicle to the crime scene. By analyzing GPS data from his car, investigators were able to place him at the scene of April's abduction and track his movements afterward.

# **AI in Forensic Analysis**

# AI in Forensic Analysis — Use Cases

- **Log parsing & timeline reconstruction** — processing large volumes of data in seconds
- **Anomaly detection** — spotting unusual patterns in network traffic or user behaviour
- **Malware classification** — clustering artifacts by behaviour or code similarity
- **MITRE ATT&CK mapping** — automatically tagging findings to tactics and techniques
- **Natural language queries** — ask questions over your data (Copilot for Security, Elastic AI Assistant)

# AI in Forensic Analysis — Limitations & Risks

- **Hallucinations** — AI output cannot be treated as evidence without verification
- **Chain of custody** — AI must not modify original evidence
- **Admissibility** — courts require reproducibility and full auditability
- **Training data bias** — may produce false positives or miss novel threats

Rule of thumb: AI is an analyst's assistant, not an expert witness.

# Summary

# Overview

- **Grab memory if possible!**
- Disc is big and takes time — consider grabbing only the artifacts
- **Do not rush, document!**
- **Defang!**
- Match findings to MITRE ATT&CK
- Diamond Model

# Other Courses

Course	Provider
Forensic Training	CESNET (FLAB)
Introduction to Memory Analysis	CZ.NIC
Digital Forensics	CIRCL
Practice rooms	TryHackMe · LetsDefend
Certifications	SANS (GIAC) · EC-Council
Mobile OS Images	Public Images

# Other Challenges

## General

- THM, [Case B4DM755](#)
- THM, [KAPE](#)
- THM, [Timeline Analysis](#)

## Windows

- THM, [Compromised Windows](#)
- THM, [Windows Forensics 1](#)

## macOS

- THM, [macOS Basics](#)

# Resources

Resource	Description
<a href="#">SIFT</a>	SANS Investigative Forensics Toolkit
<a href="#">Remnux</a>	Linux distro for malware analysis
<a href="#">WIN-FOR</a>	Windows forensics environment
<a href="#">EZ-Tools</a>	Eric Zimmerman's forensic tools
<a href="#">KAPE</a>	Artifact parser and extractor
<a href="#">Autopsy</a>	Open source digital forensics platform
<a href="#">SANS Cheat Sheet Booklet</a>	Quick reference for forensic analysts

**Q&A**

# Thank You for Your Attention!

Ondřej Šrámek

**Czechitas · DA Cybersecurity · 2026**

# Feedback



Feedback form