Leveraging LLMs for Memory Forensics

A Comparative Analysis of Malware Detection

Key takeaway: Memory forensics with LLMs is feasible: reasoning boosts detection, false positives remain high, and the human analyst remains responsible.

Jan-Hendrik Lang & Thomas Schreck, September 16th - 17th, 2025

Motivation

Windows PowerShell

```
Progress:  100.00              PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

980     2924    AggregatorHost  0xa8800003c240  3       -       0       False   2025-02-24 10:40:21.000000 UTC  N/A     Disabled
7408    820     svchost.exe     0xa88000041080  4       -       0       False   2025-02-24 10:40:56.000000 UTC  N/A     Disabled
4       0       System  0xce09fc486040  169     -       N/A     False   2025-02-24 10:40:12.000000 UTC  N/A     Disabled
1716    820     svchost.exe     0xce09fc4d1080  10      -       0       False   2025-02-24 10:40:15.000000 UTC  N/A     Disabled
1900    820     svchost.exe     0xce09fc4f1080  10      -       0       False   2025-02-24 10:40:15.000000 UTC  N/A     Disabled
1728    820     svchost.exe     0xce09fc4f5080  6       -       0       False   2025-02-24 10:40:15.000000 UTC  N/A     Disabled
72      4       Registry        0xce09fc524080  4       -       N/A     False   2025-02-24 10:40:08.000000 UTC  N/A     Disabled
1848    820     svchost.exe     0xce09fc591080  2       -       0       False   2025-02-24 10:40:15.000000 UTC  N/A     Disabled
1860    820     svchost.exe     0xce09fc593080  5       -       0       False   2025-02-24 10:40:15.000000 UTC  N/A     Disabled
1808    4       MemCompression  0xce09fc599040  42      -       N/A     False   2025-02-24 10:40:15.000000 UTC  N/A     Disabled
1744    820     svchost.exe     0xce09fc5c8080  3       -       0       False   2025-02-24 10:40:15.000000 UTC  N/A     Disabled
528     4       smss.exe        0xce09ff4a9040  2       -       N/A     False   2025-02-24 10:40:12.000000 UTC  N/A     Disabled
5640    820     svchost.exe     0xce09ff662080  7       -       0       False   2025-02-24 10:40:39.000000 UTC  N/A     Disabled
2472    820     svchost.exe     0xce09ff6e1300  2       -       0       False   2025-02-24 10:40:16.000000 UTC  N/A     Disabled
632     624     csrss.exe       0xce09ff8c3140  10      -       0       False   2025-02-24 10:40:13.000000 UTC  N/A     Disabled
820     700     services.exe    0xce0a001c3080  7       -       0       False   2025-02-24 10:40:13.000000 UTC  N/A     Disabled
700     624     wininit.exe     0xce0a001ca080  1       -       0       False   2025-02-24 10:40:13.000000 UTC  N/A     Disabled
708     692     csrss.exe       0xce0a001cd140  12      -       1       False   2025-02-24 10:40:13.000000 UTC  N/A     Disabled
828     700     lsass.exe       0xce0a0081c080  9       -       0       False   2025-02-24 10:40:13.000000 UTC  N/A     Disabled
756     692     winlogon.exe    0xce0a0084f140  6       -       1       False   2025-02-24 10:40:13.000000 UTC  N/A     Disabled
912     756     fontdrvhost.ex  0xce0a0085a080  5       -       1       False   2025-02-24 10:40:13.000000 UTC  N/A     Disabled
904     700     fontdrvhost.ex  0xce0a0085f2c0  5       -       0       False   2025-02-24 10:40:13.000000 UTC  N/A     Disabled
972     820     svchost.exe     0xce0a008c7240  29      -       0       False   2025-02-24 10:40:13.000000 UTC  N/A     Disabled
1016    820     svchost.exe     0xce0a009112c0  18      -       0       False   2025-02-24 10:40:13.000000 UTC  N/A     Disabled
712     820     svchost.exe     0xce0a00968240  6       -       0       False   2025-02-24 10:40:13.000000 UTC  N/A     Disabled
560     756     dwm.exe 0xce0a009ed080  16      -       1       False   2025-02-24 10:40:14.000000 UTC  N/A     Disabled
1112    820     svchost.exe     0xce0a00a5a240  5       -       0       False   2025-02-24 10:40:14.000000 UTC  N/A     Disabled
7928    972     ApplicationFra  0xce0a00a5c080  9       -       1       False   2025-02-24 10:41:23.000000 UTC  N/A     Disabled
1128    820     svchost.exe     0xce0a00a662c0  2       -       0       False   2025-02-24 10:40:14.000000 UTC  N/A     Disabled
1168    820     svchost.exe     0xce0a00a7a300  3       -       0       False   2025-02-24 10:40:14.000000 UTC  N/A     Disabled
```

Motivation

Windows PowerShell

```
Progress:  100.00              PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0xa880000acaa0  TCPv4   192.168.241.129 49696   104.126.37.137  443     CLOSE_WAIT      6688    SearchApp.exe   2025-02-24 10:40:44.000000 UTC
0xce09fc48d050  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       2204    spoolsv.exe     2025-02-24 10:40:16.000000 UTC
0xce09fc48d470  TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  2025-02-24 10:40:16.000000 UTC
0xce09fc48d470  TCPv6   ::      445     ::      0       LISTENING       4       System  2025-02-24 10:40:16.000000 UTC
0xce09fc48db50  TCPv4   192.168.241.129 139     0.0.0.0 0       LISTENING       4       System  2025-02-24 10:40:15.000000 UTC
0xce09ff3fe730  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       2204    spoolsv.exe     2025-02-24 10:40:16.000000 UTC
0xce09ff3fe730  TCPv6   ::      49668   ::      0       LISTENING       2204    spoolsv.exe     2025-02-24 10:40:16.000000 UTC
0xce09ff5705c0  TCPv4   192.168.241.129 49698   204.79.197.222  443     CLOSED  6688    SearchApp.exe   2025-02-24 10:40:45.000000 UTC
0xce09ff7f05d0  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       1016    svchost.exe     2025-02-24 10:40:13.000000 UTC
0xce09ff7f05d0  TCPv6   ::      135     ::      0       LISTENING       1016    svchost.exe     2025-02-24 10:40:13.000000 UTC
0xce09ff7f0890  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       700     wininit.exe     2025-02-24 10:40:13.000000 UTC
0xce09ff7f0890  TCPv6   ::      49665   ::      0       LISTENING       700     wininit.exe     2025-02-24 10:40:13.000000 UTC
0xce09ff7f09f0  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       1340    svchost.exe     2025-02-24 10:40:14.000000 UTC
0xce09ff7f0b50  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       1340    svchost.exe     2025-02-24 10:40:14.000000 UTC
0xce09ff7f0b50  TCPv6   ::      49666   ::      0       LISTENING       1340    svchost.exe     2025-02-24 10:40:14.000000 UTC
0xce09ff7f1390  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       1332    svchost.exe     2025-02-24 10:40:14.000000 UTC
0xce09ff7f1650  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       1332    svchost.exe     2025-02-24 10:40:14.000000 UTC
0xce09ff7f1650  TCPv6   ::      49667   ::      0       LISTENING       1332    svchost.exe     2025-02-24 10:40:14.000000 UTC
0xce09ff7f17b0  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       700     wininit.exe     2025-02-24 10:40:13.000000 UTC
0xce09ff7f1bd0  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       1016    svchost.exe     2025-02-24 10:40:13.000000 UTC
0xce09ff7f1d30  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       828     lsass.exe       2025-02-24 10:40:13.000000 UTC
0xce09ff7f1e90  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       828     lsass.exe       2025-02-24 10:40:13.000000 UTC
0xce09ff7f1e90  TCPv6   ::      49664   ::      0       LISTENING       828     lsass.exe       2025-02-24 10:40:13.000000 UTC
0xce0a00cacd10  UDPv4   192.168.241.129 138     *       0               4       System  2025-02-24 10:40:15.000000 UTC
0xce0a00cad030  UDPv4   192.168.241.129 137     *       0               4       System  2025-02-24 10:40:15.000000 UTC
0xce0a00edb220  UDPv4   0.0.0.0 0       *       0               1096    svchost.exe     2025-02-24 10:40:16.000000 UTC
0xce0a00edb220  UDPv6   ::      0       *       0               1096    svchost.exe     2025-02-24 10:40:16.000000 UTC
0xce0a00edb860  UDPv4   0.0.0.0 5353    *       0               1096    svchost.exe     2025-02-24 10:40:16.000000 UTC
0xce0a00edb860  UDPv6   ::      5353    *       0               1096    svchost.exe     2025-02-24 10:40:16.000000 UTC
```

Motivation

Windows PowerShell

```
Volatility 3 Framework 2.8.0
Progress:  100.00               PDB scanning finished
Pid     Process Base    InLoad  InInit  InMem   MappedPath

4       System  0x77120000      False   False   False   \Windows\SysWOW64\ntdll.dll
4       System  0x7ff94c150000  False   False   False   \Windows\System32\vertdll.dll
4       System  0x7ff94c190000  False   False   False   \Windows\System32\ntdll.dll
528     smss.exe        0x7ff94c190000  True    True    True    \Windows\System32\ntdll.dll
528     smss.exe        0x7ff70d350000  True    False   True    \Windows\System32\smss.exe
632     csrss.exe       0x10e6ab80000   False   False   False   \Windows\System32\de-DE\csrss.exe.mui
632     csrss.exe       0x10e6ab90000   False   False   False   \Windows\System32\de-DE\winsrv.dll.mui
632     csrss.exe       0x7ff949810000  True    True    True    \Windows\System32\csrsrv.dll
632     csrss.exe       0x7ff74ff70000  True    False   True    \Windows\System32\csrss.exe
632     csrss.exe       0x7ff9497d0000  True    True    True    \Windows\System32\winsrv.dll
632     csrss.exe       0x7ff949790000  True    True    True    \Windows\System32\sxssrv.dll
632     csrss.exe       0x7ff949560000  True    True    True    \Windows\System32\sxs.dll
632     csrss.exe       0x7ff9497a0000  True    True    True    \Windows\System32\winsrvext.dll
632     csrss.exe       0x7ff9497f0000  True    True    True    \Windows\System32\basesrv.dll
632     csrss.exe       0x7ff94a330000  True    True    True    \Windows\System32\kernel32.dll
632     csrss.exe       0x7ff949c60000  True    True    True    \Windows\System32\cfgmgr32.dll
632     csrss.exe       0x7ff9499a0000  True    True    True    \Windows\System32\gdi32full.dll
632     csrss.exe       0x7ff949830000  True    True    True    \Windows\System32\ucrtbase.dll
632     csrss.exe       0x7ff949c30000  True    True    True    \Windows\System32\win32u.dll
632     csrss.exe       0x7ff949ba0000  True    True    True    \Windows\System32\bcryptprimitives.dll
632     csrss.exe       0x7ff949cb0000  True    True    True    \Windows\System32\KernelBase.dll
632     csrss.exe       0x7ff94a110000  True    True    True    \Windows\System32\msvcp_win.dll
632     csrss.exe       0x7ff94bf20000  True    True    True    \Windows\System32\user32.dll
632     csrss.exe       0x7ff94ba30000  True    True    True    \Windows\System32\combase.dll
632     csrss.exe       0x7ff94aac0000  True    True    True    \Windows\System32\rpcrt4.dll
632     csrss.exe       0x7ff94c190000  True    True    True    \Windows\System32\ntdll.dll
632     csrss.exe       0x7ff94c120000  True    True    True    \Windows\System32\gdi32.dll
700     wininit.exe     0x7ff61bb20000  True    False   True    \Windows\System32\wininit.exe
```

Motivation

- **Expertise-Intensive:** requires deep specialist knowledge & manual effort
- **Data Overload:** numerous plugin outputs, subtle IoCs to correlate
- **Steep Learning Curve:** difficult for less-experienced analysts
- **Memory Forensics Importance:** essential for detecting fileless malware & APTs
- **Analyst Fatigue:** overload increases errors and slows detection
- **Underexplored AI Potential:** unclear if LLMs can reduce effort while preserving accuracy

Research Questions

1. Detection Performance: How do different LLMs perform in detecting malware from Volatility3 data?

2. Impact of Reasoning: Do reasoning-enabled (“thinking mode”) configurations yield statistically significant improvements in detection quality?

3. Limitations & Error Sources: What drives false positives and false negatives, and can adding baseline system knowledge reduce these errors?

Methods: MemoryInvestigator

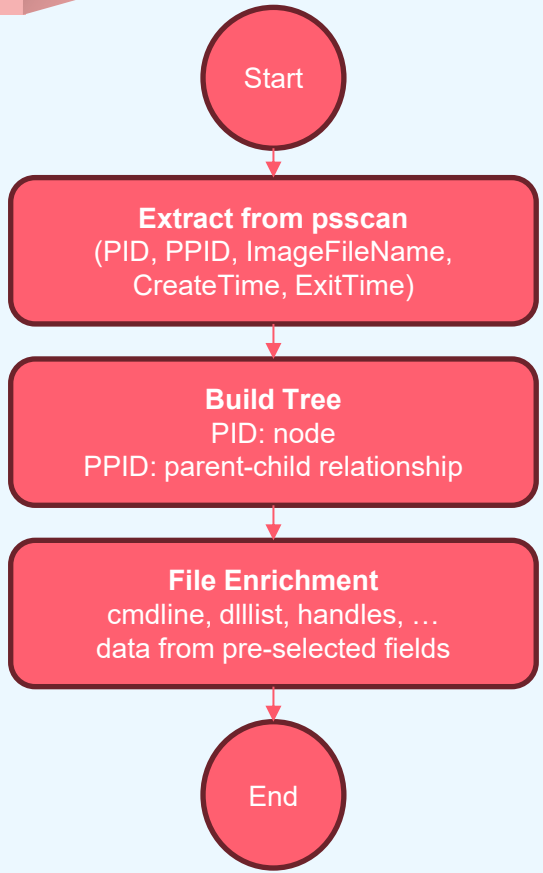
- **Proof-of-Concept Prototype Goals**
  - Volatility3 automated
  - Volatility3 output prepared for an LLM
  - forwarding the processed output to an LLM and displaying the results
  - to recognize anomalies on its own in the best case

- **Result**
  - Development of a Streamlit app
  - Available at: https://github.com/jan-hendrik-lang/MemoryInvestigator

- **Features**
  - Automation Volatility3 Version 2.8.0
  - Display and search of data as table and graph
  - Preparation of the data as a user-defined tree−of−table[1] for further use of the LLM
  - LLM-supported analysis of the tree-of-table
  - Dynamic creation of a RAG using PDF files or Malpedia Thread Reports

[1] D. Ji et al., “Tree-of-Table: Unleashing the Power of LLMs for Enhanced Large-Scale Table Understanding,” 2024, arXiv. doi: 10.48550/ARXIV.2411.08516.

Methods: Tree-of-Table



Volatility3 Modules:

- Process modules like *psscan, cmdline, dlllist*.
- Network modules like *netscan*.
- Malware-specific plugins like *malfind, processghosting, suspicious_threads*.
- Privilege and persistence indicators like *getsids* and *svcdiff*.

Processes
- **System (pid=4, ppid=0)**
  - SID: S-1-5-18, S-1-5-32-544, ...
  - ldrmodules: ntdll.dll [InInit=False, InLoad=False, InMem=False]
  - netscan: UDPv4, 192.168.10.210:137 → LISTENING
  - **Registry (pid=92)**
    - SID: S-1-5-18, S-1-5-32-544, ...
    - ldrmodules: ntdll.dll [InInit=False, InLoad=False, InMem=False]
    - netscan: UDPv4, 192.168.10.210:137 → LISTENING
  - **smss.exe (pid=328)**

System Message:

You are a forensic RAM analyst assistant specializing in Windows memory analysis. Analyze the JSON tree of Windows memory artifacts to detect intrusions or malicious activities. Cross-check your findings with known threats and provide clear, specific reasons for flagging any anomalies (e.g., unusual parentchild relationships, code injection, execution from nonstandard locations). If you are unsure, ask clarifying questions, and if you don't know, say so. Generate a structured forensic report highlighting confirmed threats while minimizing noise. Data: *"Tree-of-Table Data"*

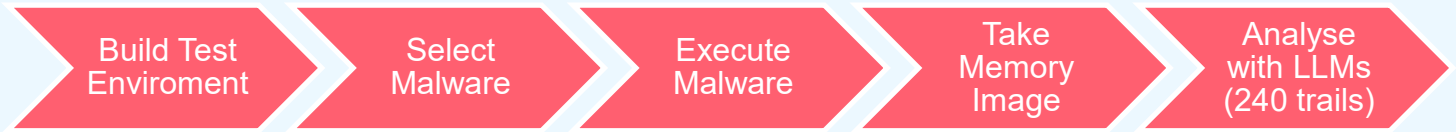
User Message: Analyze the data and determine whether there is an anomaly.

Evaluation and Results

- **Test Scenarios:**
  - Clean Image,
  - Process Injection (msfvenom),
  - PowerShell Empire,
  - QuasarRAT (Remote Access Trojan),
  - MassLogger (keylogger),
  - DarkCloud (trojan),
  - LockBit (ransomware),
  - LokiBot (stealer).

- **LLMs for Comparison:**
  - OpenAI GPT-4o,
  - OpenAI o1,
  - Google Gemini 2.0 Flash,
  - Google Gemini 2.0 Flash-Thinking,
  - Grok 3,
  - Grok 3 with enabled thinking mode.

Evaluation and Results



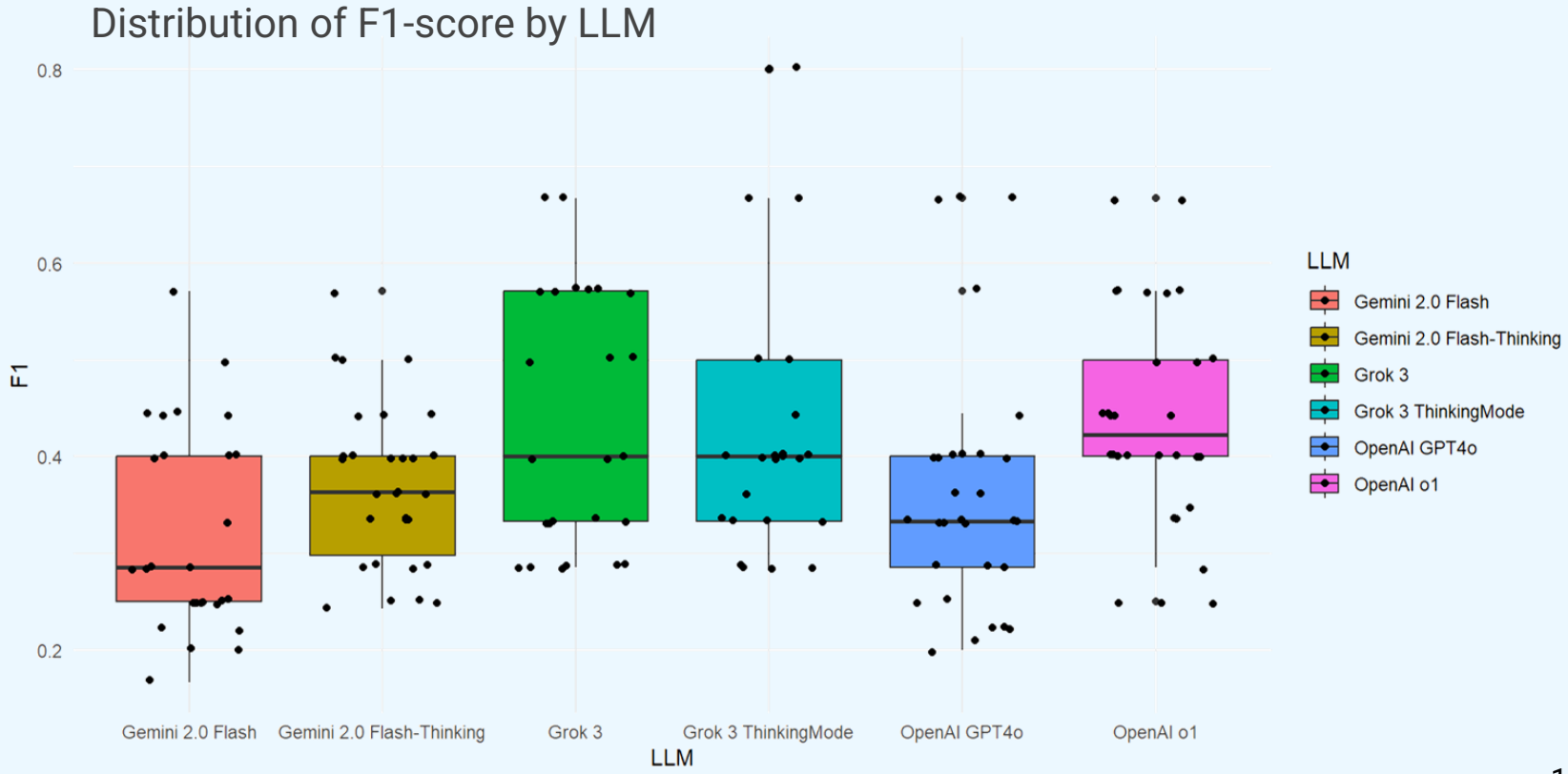
Performance Metrics:

- Accuracy,
- Precision,
- Recall,
- F1-score,
- ANOVA,
- t-tests.

Evaluation and Results

- **Experiment scale:** 240 trials (8 scenarios × 1 image × 6 LLMs × 5 runs)
- **Detection:** All LLMs found malicious evidence in most scenarios
- **Reasoning helps:** “Thinking” modes consistently outperformed standard modes
- **Different strengths:** Models excel at different artifact types (e.g., network vs. script decoding)
- **Performance pattern:** Very high recall (often ≈100%) — low precision (precision often <20%)
- **Blind spot:** LockBit IoCs were outside available inputs → missed detections
- **Common FP source:** malfind outputs (e.g., MsMpEng.exe) frequently mis-flagged

Evaluation and Results



Limitations

- **Dataset Scope:** one memory image per scenario; limited to Windows 10
- **Data Coverage:** only selected Volatility3 plugins; no registry hives, EVTX logs, or raw strings
- **Model Dependence:** results bound to specific LLM versions & modes (non-deterministic behavior)
- **Precision Gap:** high false positive rate; not suitable as a standalone detection system
- **Generalizability:** performance on other OS, larger datasets, or different attack techniques remains untested

Future Work

- **Broader Data Sources:** include registry hives, event logs, and memory strings
- **Improve Precision:** integrate baseline system[2] knowledge to filter benign processes
- **Advanced LLM Integration:** fine-tune models on forensic data; evaluate next-gen LLMs
- **User Studies & Deployment:** measure analyst time savings, detection gains, usability
- **Tool Enrichment:** expand from Volatility3 towards MemProcFS or Velociraptor
- **Protocol Experimentation:** test Model Context Protocol (MCP) as an alternative to tree-of-tables

[2] Gordon Fraser. 2021. Creating a Baseline of Process Activity for Memory Forensics.

Conclusion

- **Feasibility & Value:** LLMs can sift memory data and highlight likely IoCs
- **Recall vs. Precision:** strong recall, but very low precision (many false alarms)
- **Context Matters:** success depends on the breadth of forensic input data
- **Human Essential:** analysts remain critical due to false positives & blind spots
- **LLMs as Support:** assist in triage, improve interpretability, not a replacement

Contact Details

Jan-Hendrik Lang
jan-hendriklang@hotmail.de

Thomas Schreck
thomas.schreck@hm.edu

GitHub Repo:

https://github.com/jan-hendrik-lang/MemoryInvestigator