Volatile Artifact Snapshot Triage (VAST): User Manual

Overview

VAST (Volatile Artifact Snapshot Triage) is a lightweight digital forensics triage tool designed to quickly extract, parse, and analyse volatile artifacts from memory dumps and VM snapshots. It enables investigators to reconstruct system state, identify suspicious processes, inspect network connections, and extract system-level indicators with minimal setup.

Unlike traditional full-scale forensics analysis suites, VAST focuses on rapid triage, allowing analysts to quickly assess whether a host shows signs of compromise before performing deeper analysis.

Key Capabilities

- Identify suspicious or malicious processes
- Extract command-line history, system information, and registry artifacts
- Analyse network activity from volatile memory
- Extract handles, loaded DLLs, user sessions, etc.
- Visualize event timelines for faster investigation
- Provide automated triage scoring based on heuristics

System Requirements

Frontend Requirements:

- A modern web browser (Google Chrome, Mozilla Firefox, Safari, or Microsoft Edge).
- A stable network connection to the host machine (if accessing remotely).

Backend Requirements:

- **OS**: Linux, macOS, or Windows 10/11.
- **Python**: Version 3.8 or higher.
- **Package Manager**: pip (Python package installer).
- **Dependencies**: All required Python libraries are listed in requirements.txt.
- **Disk Space**: Sufficient space to store memory dump files and extracted artifact data.

Installation & Setup

Prerequisites

1. Ensure Python 3.8+ and pip are installed on your system. You can verify this by running python3 --version and pip3 --version in your terminal.
2. Obtain a memory dump (e.g., .mem, .raw, .dmp) from a Windows system for analysis.

Installation Steps

Open the terminal and run the following:

```
# Clone the VAST repository from GitHub
git clone https://github.com/khrnrn/VAST.git

# Navigate into the project directory
cd VAST

# Install dependencies
pip install -r requirements.txt
```

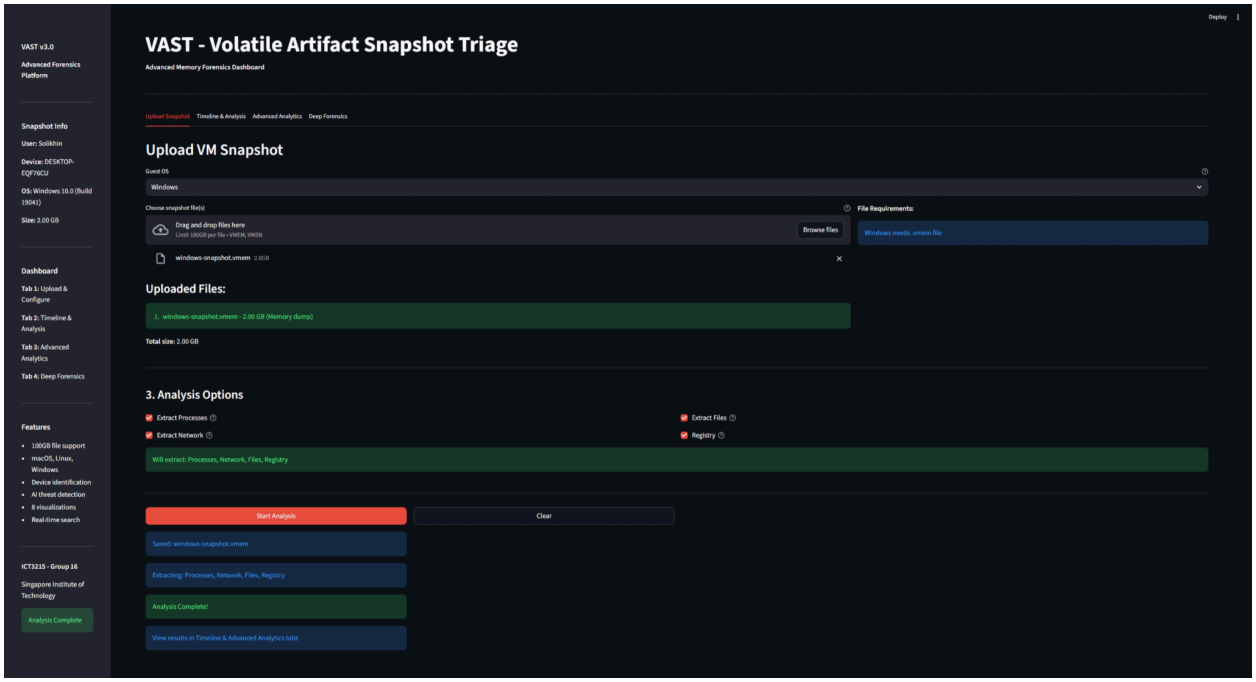
To run the application:

```
streamlit run dashboard.py
```

Once started, VAST can be accessed locally at: https://localhost:8501.

Accessing VAST

1. Open your browser.
2. Go to https://localhost:8501
3. You will see the dashboard's interface.



Interface Overview

The VAST dashboard consists of four main tabs that provide a comprehensive workflow for investigating a volatile system snapshot:

1. **Upload Snapshot** – Upload a memory dump or VM snapshot file (e.g., .vmem, .vmsn, .sav) from a system for analysis.
2. **Timeline & Analysis** – View a chronological timeline of system events and conduct initial triage of artifacts.
3. **Advanced Analytics** – Utilize AI-driven threat detection and other analytical tools to identify suspicious patterns.
4. **Deep Forensics** – Perform a detailed, low-level forensic examination of the memory dump for advanced evidence collection.

The dashboard also has a consistent sidebar that displays the dashboard tabs, key features, and snapshot information once analysed.

Upload Snapshot

The logical workflow is:

1. Upload File:
    - The user drags and drops a memory dump file or uses the "Browse files" button.

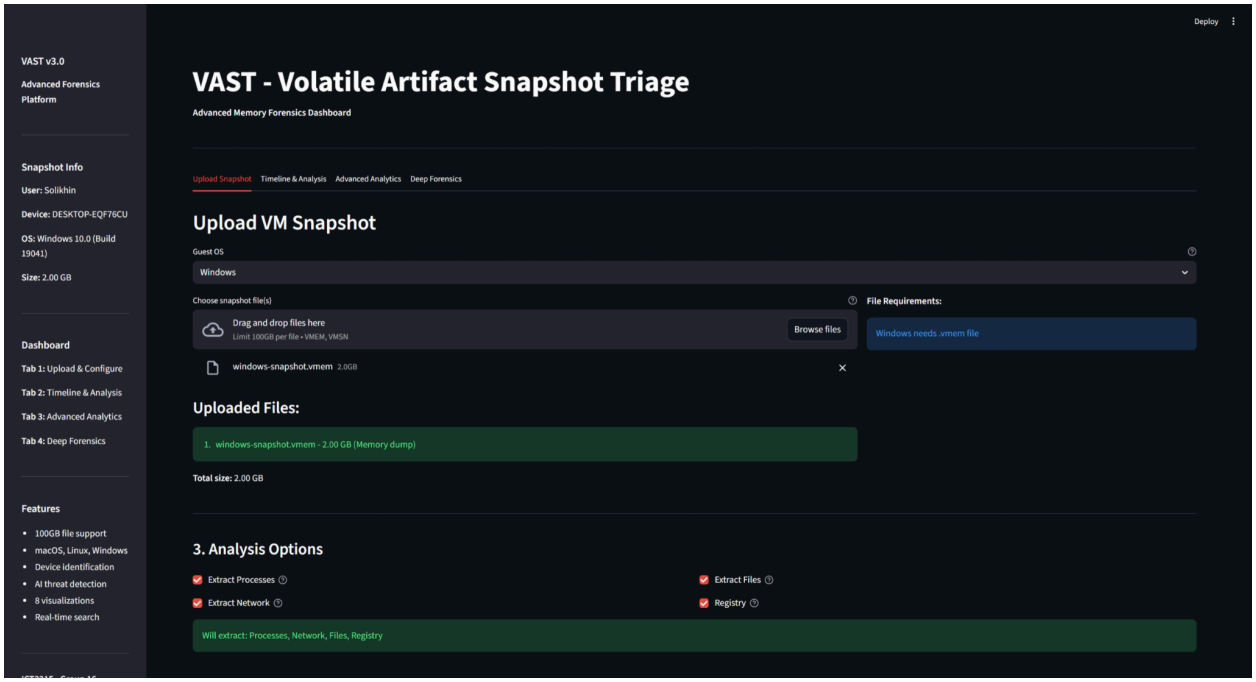
- The system validates the file type and size (supporting files like .vmem, .raw up to 100GB).

2. Review Snapshot Info:
    - Once uploaded, basic system information is automatically parsed and displayed from the memory dump in the "Snapshot Info" panel (e.g., User, Device, OS Version, File Size).

3. Configure Analysis Options:
    - This is a critical step. The user selects which types of artifacts to extract from the memory dump.
    - The options include:
        - Extract Processes
        - Extract Network connections
        - Extract Files
        - Extract Registry (specific to Windows analysis)
    - Selecting these options dictates what data will be available for investigation in the subsequent tabs.

4. Initiate Analysis
    - The user clicks the "Start Analysis" button.
    - The backend processing begins, extracting the selected artifacts (Processes, Network, Files, Registry) from the memory dump.
    - A status message ("Analysis Complete") confirms the process is finished.

5. Proceed to Results
    - Once analysis is complete, the user is instructed to "View results in Timeline & Advanced Analytics tabs" to begin the actual investigation.



Timeline and Analysis

Upon navigating to this tab, the user is presented with a consolidated dashboard for initial triage. The logical workflow within this tab would be:

1. **Review the Snapshot Information**: First, the user checks the Snapshot Information panel to confirm basic details about the uploaded memory dump, such as the OS Type and File Size.

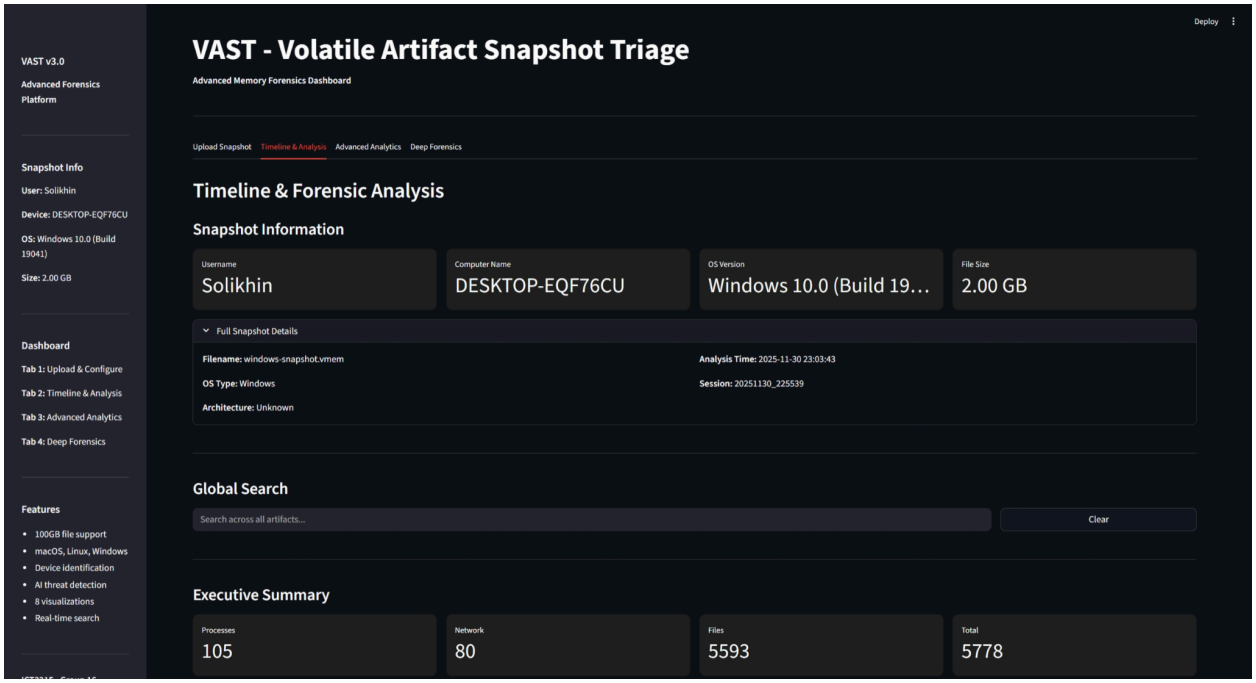
2. **Use Global Search**: At any point, the user can utilize the Global Search bar to look for specific indicators of compromise (IoCs) like a particular process name, IP address, or filename across all extracted artifacts.

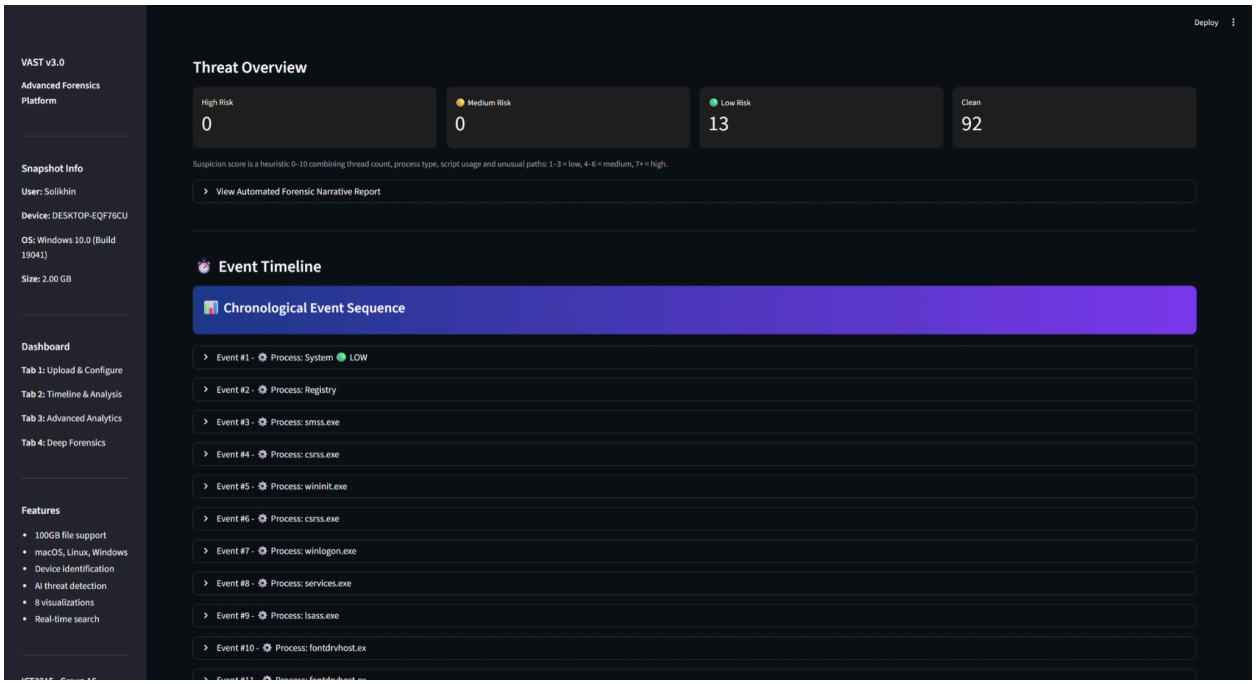
3. **Scan the Executive Summary**: Next, they look at the Executive Summary to grasp the scale of the data, seeing the total counts of Processes, Network Connections, Files, and the overall total artifacts.

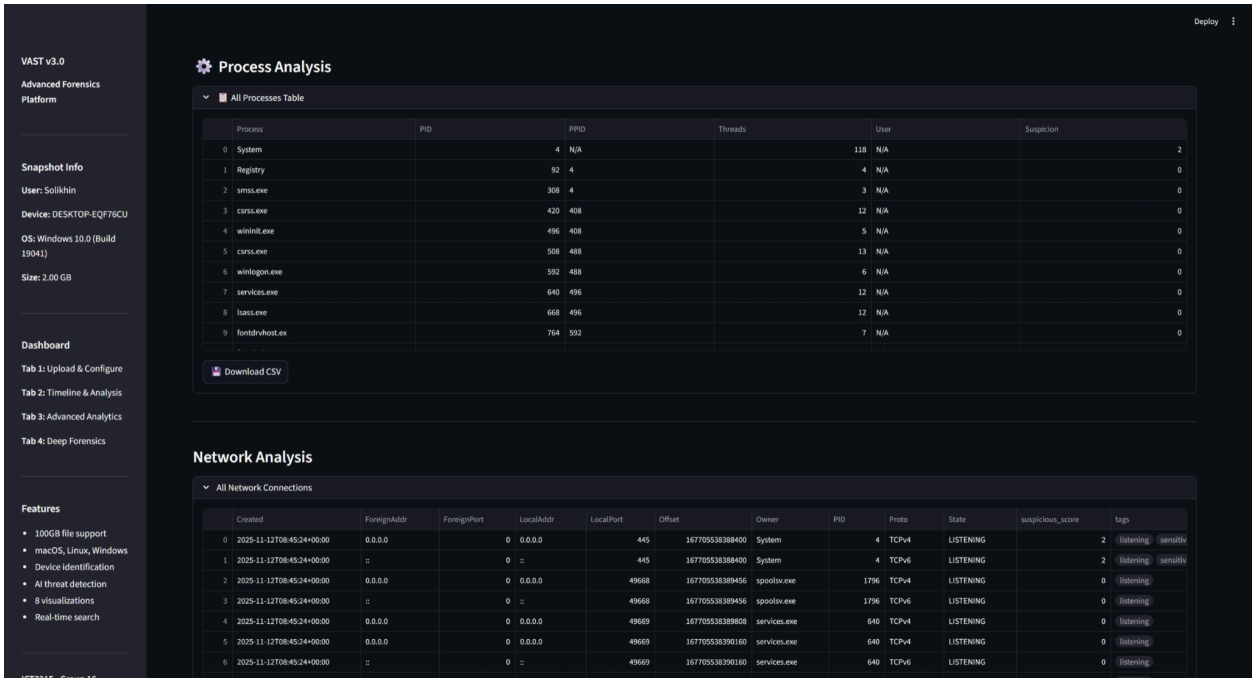
4. **Assess the Threat Overview**: The user then immediately checks the Threat Overview widget to understand the severity distribution. In this case, they see that 3 processes have been flagged as "Low Risk" and 341 are "Clear." This quickly tells them there is no major active compromise, but a few items need checking.

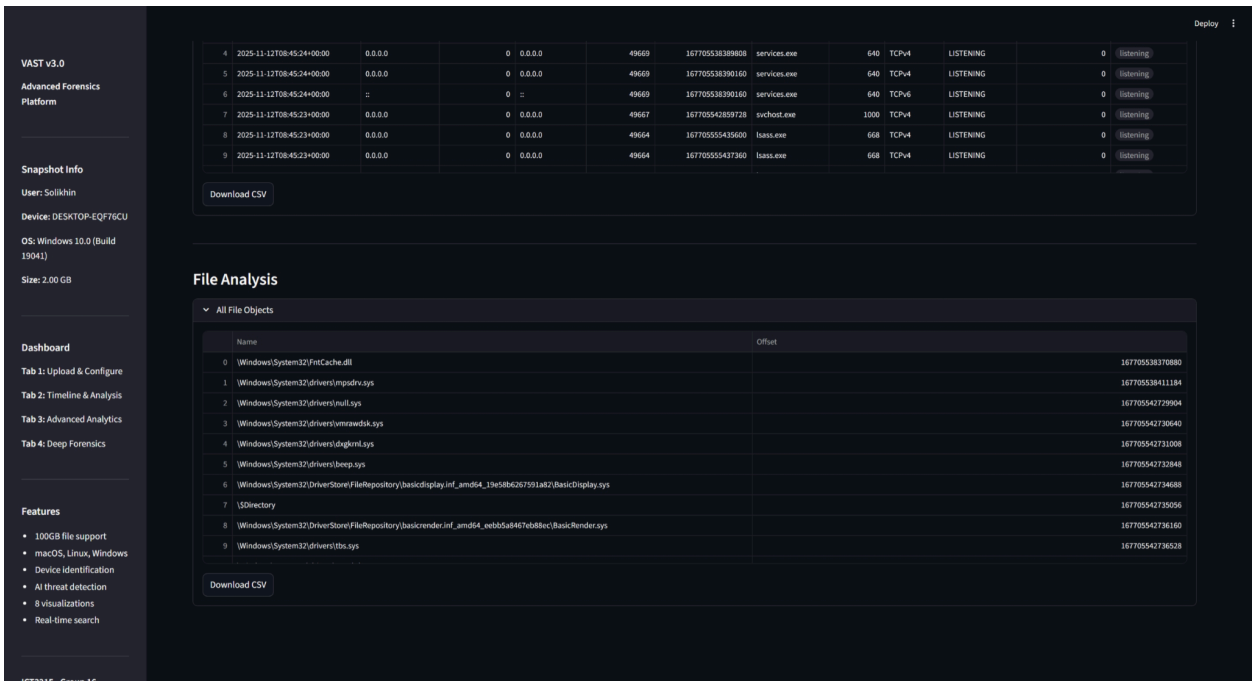
5. **Investigate the Event Timeline**: The user clicks into the Chronological Event Sequence to see the order of process events. Here, they can scrutinize the processes that were assigned a "Low Risk" score to understand why they were flagged based on their tags and the context of their execution.

6. **Drill Down into Specific Artifacts**: Using the tabs for Process Analysis, Network Analysis, and File Analysis, the user can dive deeper into each category.









Advanced Analytics

After triaging the snapshot in the "Timeline & Analysis" tab, proceed to the "Advanced Analytics" tab to perform a deeper, data-driven investigation. This tab provides advanced visualizations and scoring to help you understand the "why" behind the alerts and correlate evidence into a coherent attack narrative.

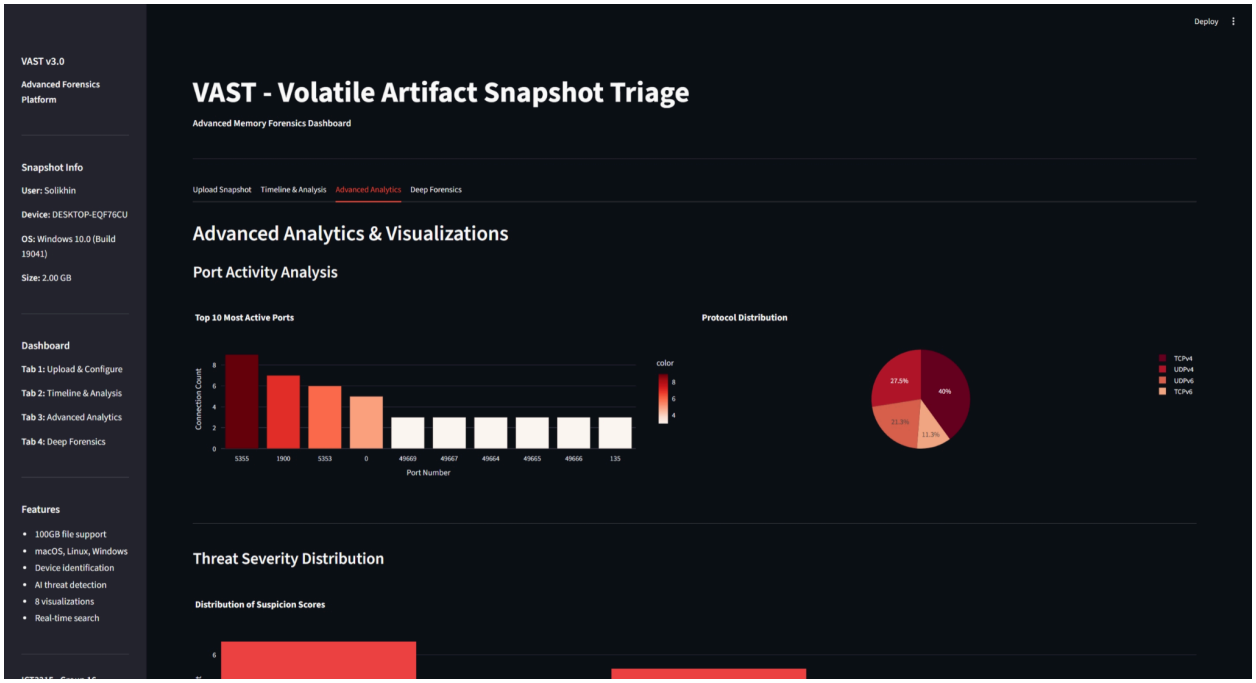
The logical workflow within this tab is:

1. **Review the Threat Severity Distribution**: Begin by examining the "Distribution of Suspicious Scores" chart. This provides a high-level view of the risk landscape across all analyzed artifacts, showing how many items fall into high, medium, and low-risk categories.

2. **Identify Key Suspects**: Consult the "Top 10 Most Suspicious Processes" list. This ranked list, based on heuristic scores, immediately directs your attention to the most likely malicious processes for further investigation.

3. **Analyze Resource Consumption**: Examine the "Memory Usage Distribution" and "Top 10 Thread Consumers" visualizations. Legitimate system processes often consume significant resources, but an unknown or suspicious process with high resource usage is a major red flag and potential indicator of payload execution or data exfiltration.

4. **Correlate Network Activity**: Use the "Connection State Analysis" to view the states (e.g., ESTABLISHED, LISTENING) of network connections. Cross-reference the "Top 10 External Connections" with the suspicious processes list. A suspicious process making external connections strongly indicates potential command-and-control (C2) activity or data theft.



Deploy

VAST v3.0

Advanced Forensics Platform

Snapshot Info

User: Solikhin

Device: DESKTOP-EQF76CU

OS: Windows 10.0 (Build 19041)

Size: 2.00 GB

Dashboard

Tab 1: Upload & Configure

Tab 2: Timeline & Analysis

Tab 3: Advanced Analytics

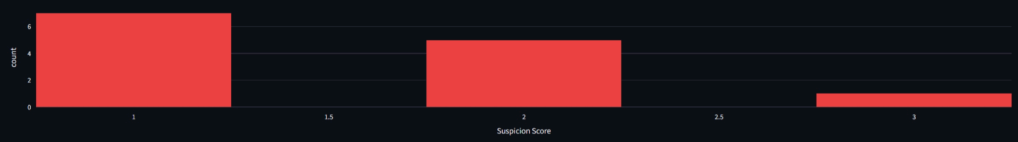
Tab 4: Deep Forensics

Features

- 100GB file support
- macOS, Linux, Windows
- Device identification
- AI threat detection
- 8 visualizations
- Real-time search

Threat Severity Distribution

Distribution of Suspicion Scores



Top 10 Most Suspicious Processes

	ImageFileName	MITRE	PID	suspicious_score	tags
101	cmd.exe	T1059 - Command & Scripting Interpreter	6300	3	script_or_shell
0	System		4	2	high_thread_count
13	svchost.exe	T1543 - Create or Modify System Process	1000	2	high_thread_count
21	MemCompression		1432	2	high_thread_count
53	explorer.exe		3780	2	high_thread_count
62	SearchApp.exe		4808	2	high_thread_count
37	MicrosoftEdgeU		2444	1	wow64_process
48	MicrosoftEdgeU		3356	1	wow64_process
80	OneDrive.exe		6576	1	wow64_process

Memory Usage Distribution

Top 10 Thread Consumers

Deploy

VAST v3.0

Advanced Forensics Platform

Snapshot Info

User: Solikhin

Device: DESKTOP-EQF76CU

OS: Windows 10.0 (Build 19041)

Size: 2.00 GB

Dashboard

Tab 1: Upload & Configure

Tab 2: Timeline & Analysis

Tab 3: Advanced Analytics

Tab 4: Deep Forensics

Features

- 100GB file support
- macOS, Linux, Windows
- Device identification
- AI threat detection
- 8 visualizations
- Real-time search

Memory Usage Distribution

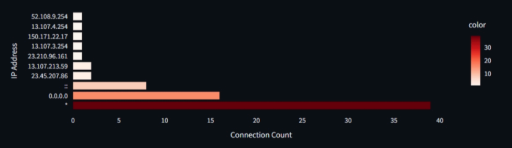
Top 10 Thread Consumers

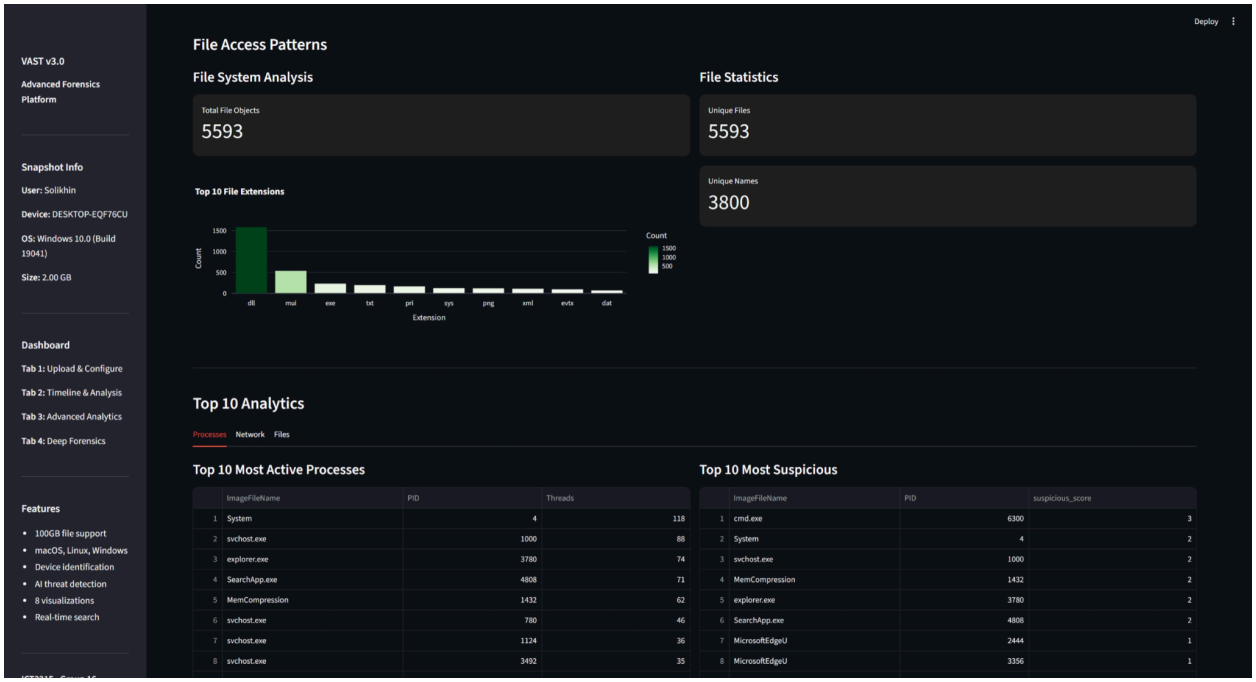
	ImageFileName	PID	Threads
1	System	4	118
2	svchost.exe	1000	88
3	explorer.exe	3780	74
4	SearchApp.exe	4808	71
5	MemCompression	1432	62
6	svchost.exe	780	46
7	svchost.exe	1124	36
8	svchost.exe	3492	35
9	svchost.exe	1288	28
10	MsMpEng.exe	2348	27

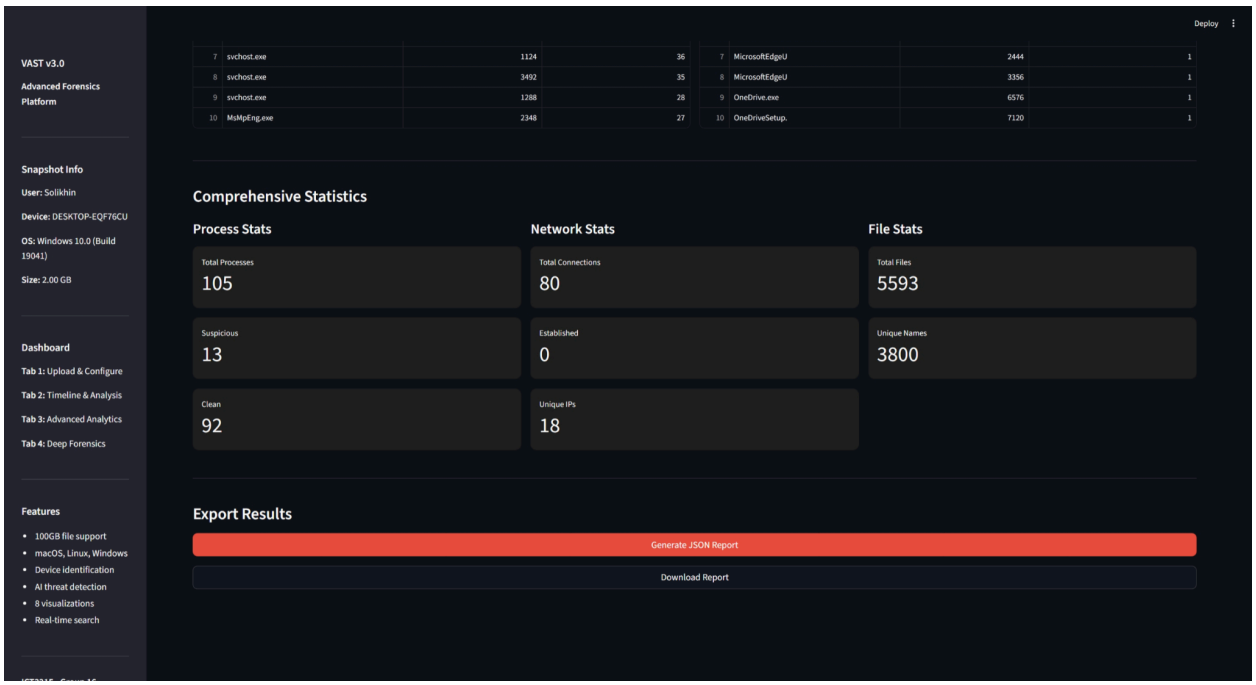
Connection State Analysis

Connection States

Top 10 External Connections



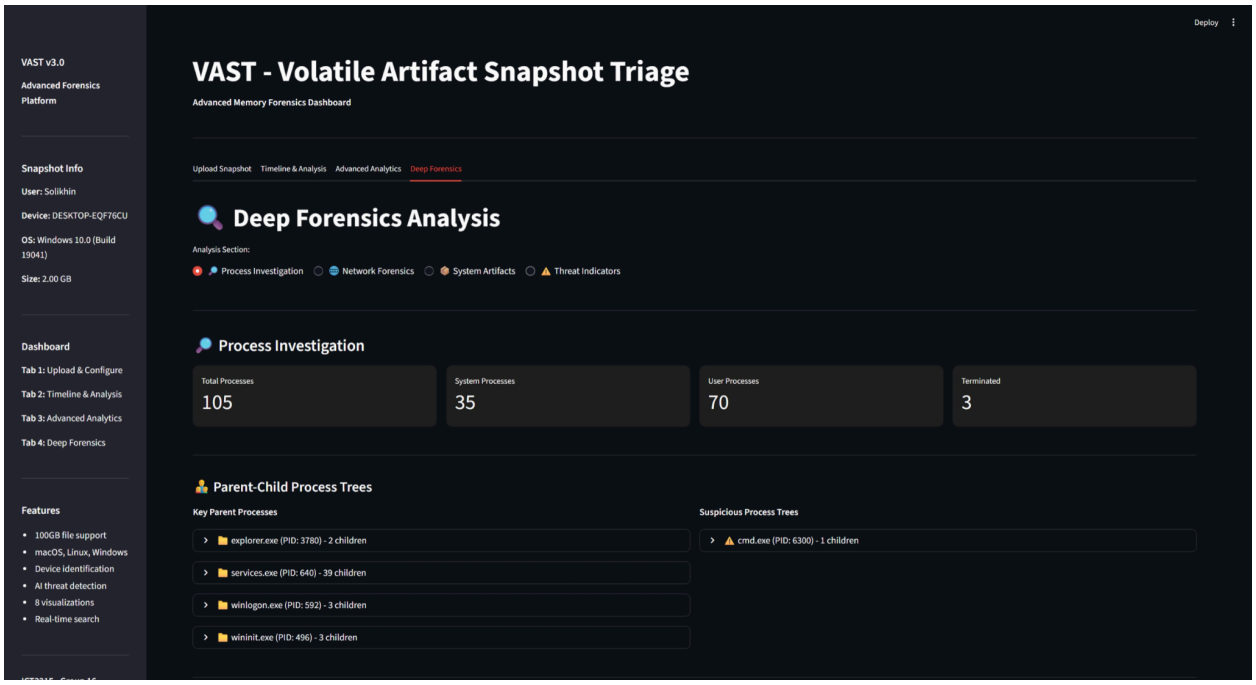


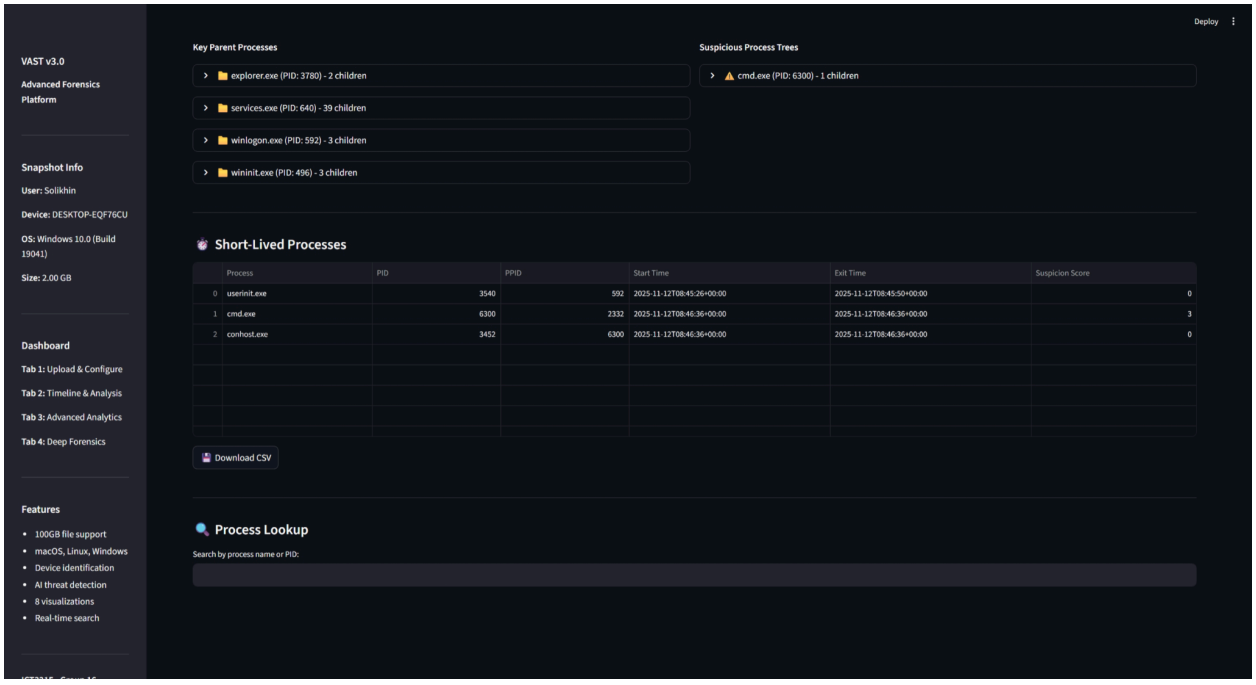


Deep Forensics

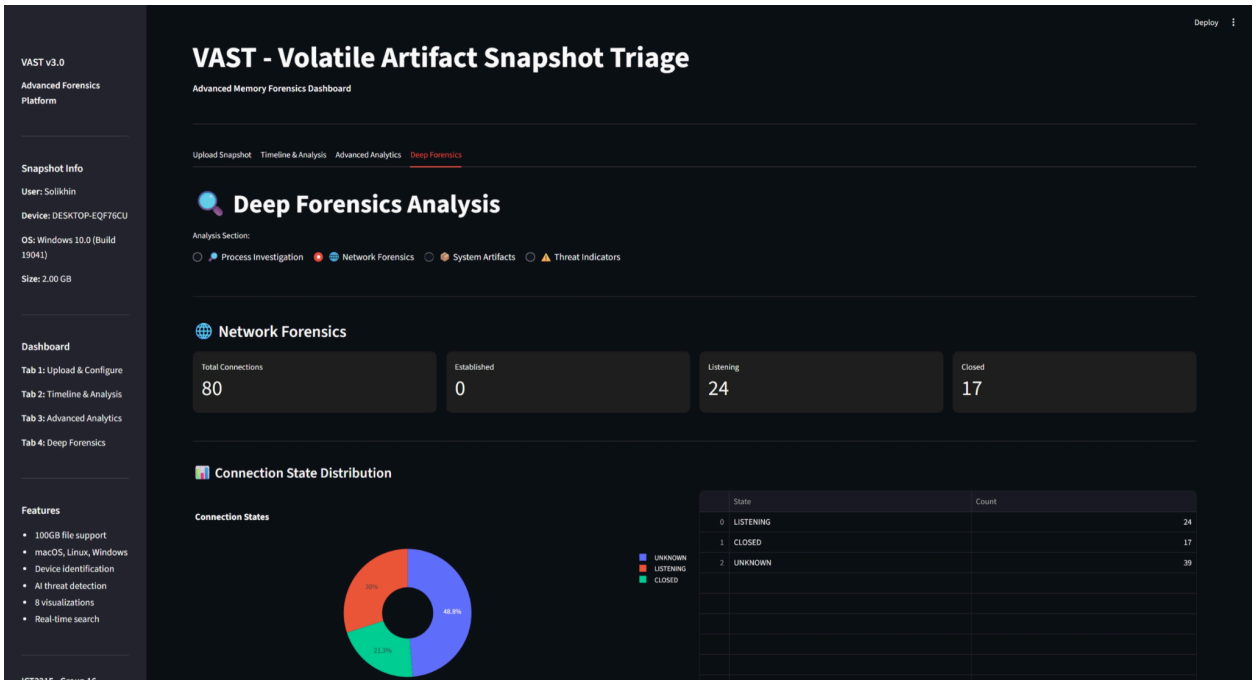
The "Deep Forensics" tab is your platform for a granular, low-level examination of the memory dump. Use this tab to gather definitive evidence, investigate specific indicators of compromise (IOCs), and uncover stealthy artifacts that may evade automated detection.
The logical workflow within this tab is:

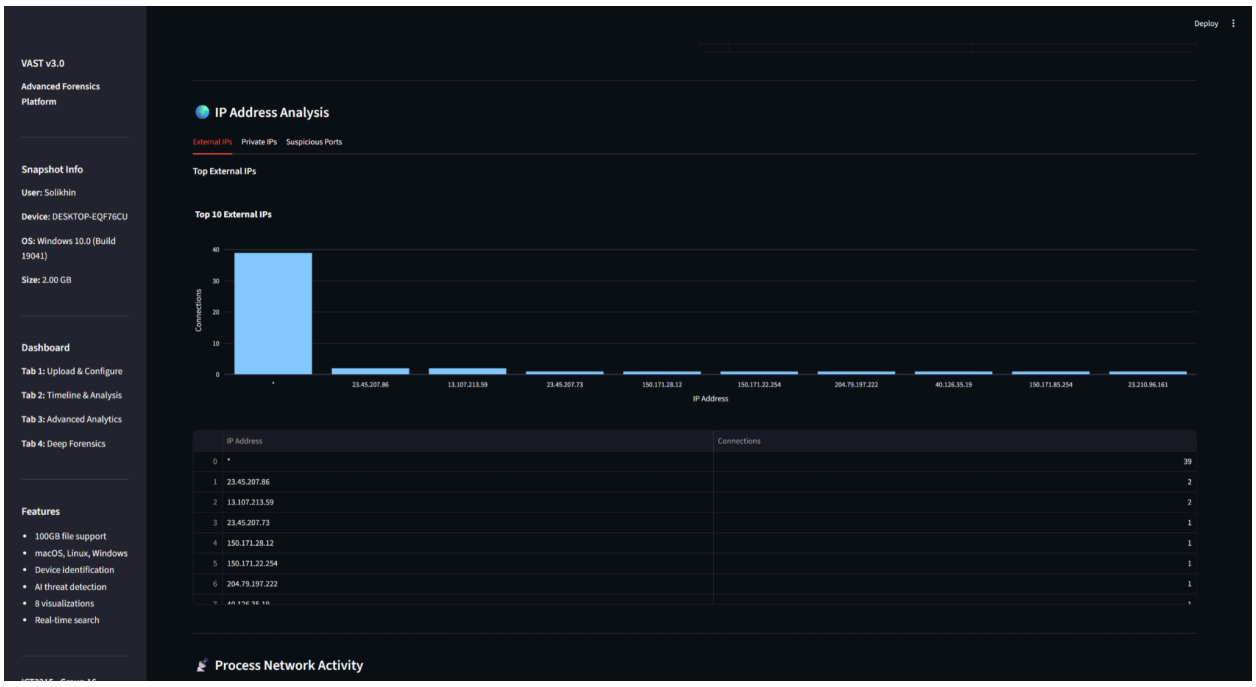
1. **Initiate a Targeted Process Investigation**:
    - Select a specific suspicious process identified in earlier tabs.
    - Perform a deep memory scan to extract detailed information such as its full command line arguments, loaded DLLs, open handles, and network sockets. This is crucial for understanding the full scope of its execution.

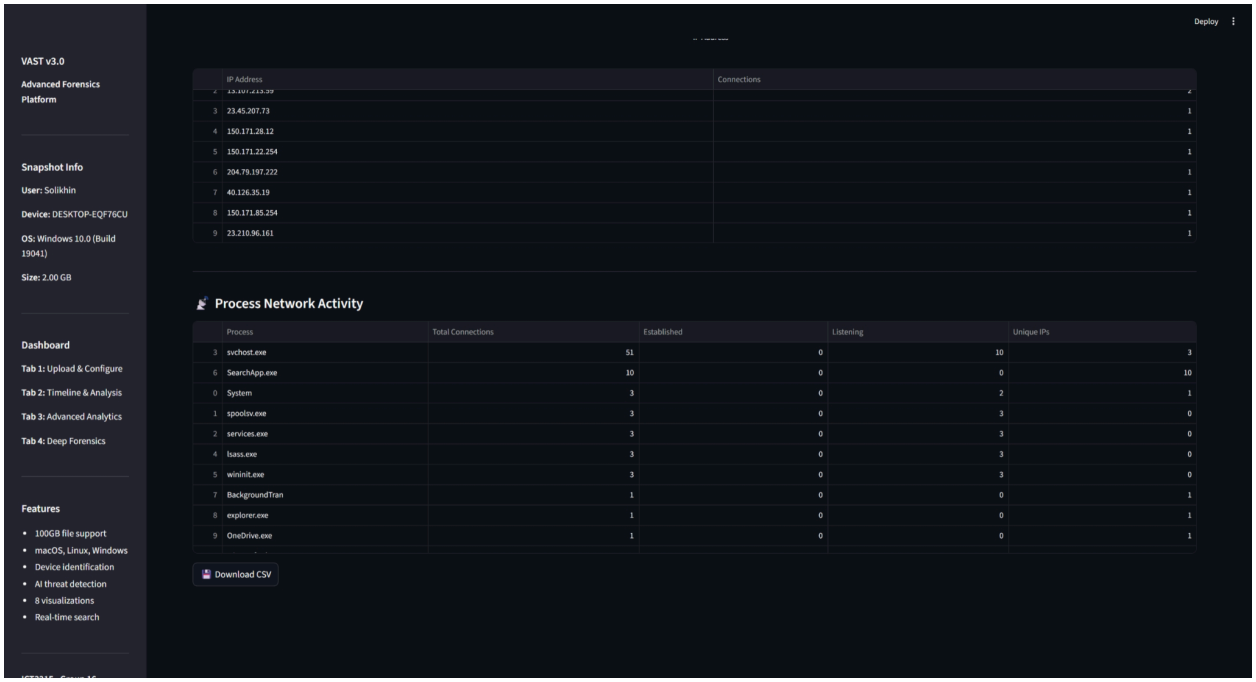




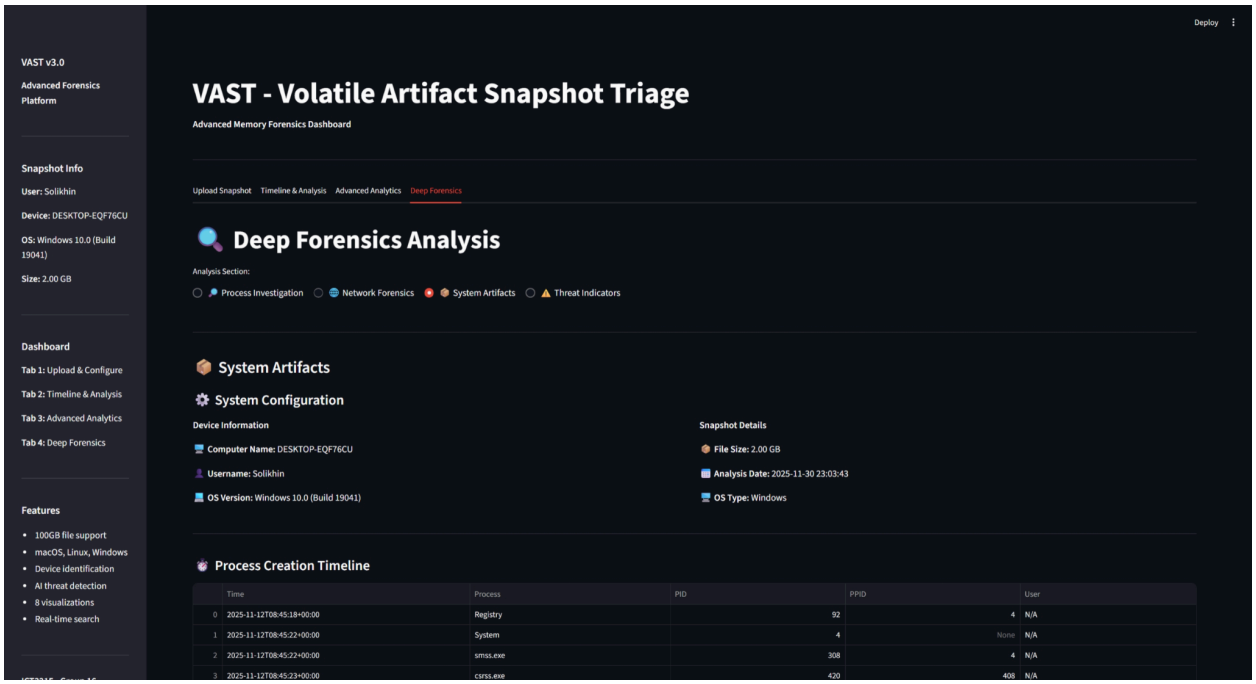
2. **Perform Detailed Network Forensics**:
    - Go beyond simple connection lists. Analyze the "Connection State Distribution" in detail.
    - Reconstruct network conversations and extract raw packet data from memory where possible, to identify patterns of communication and potential data exfiltration.

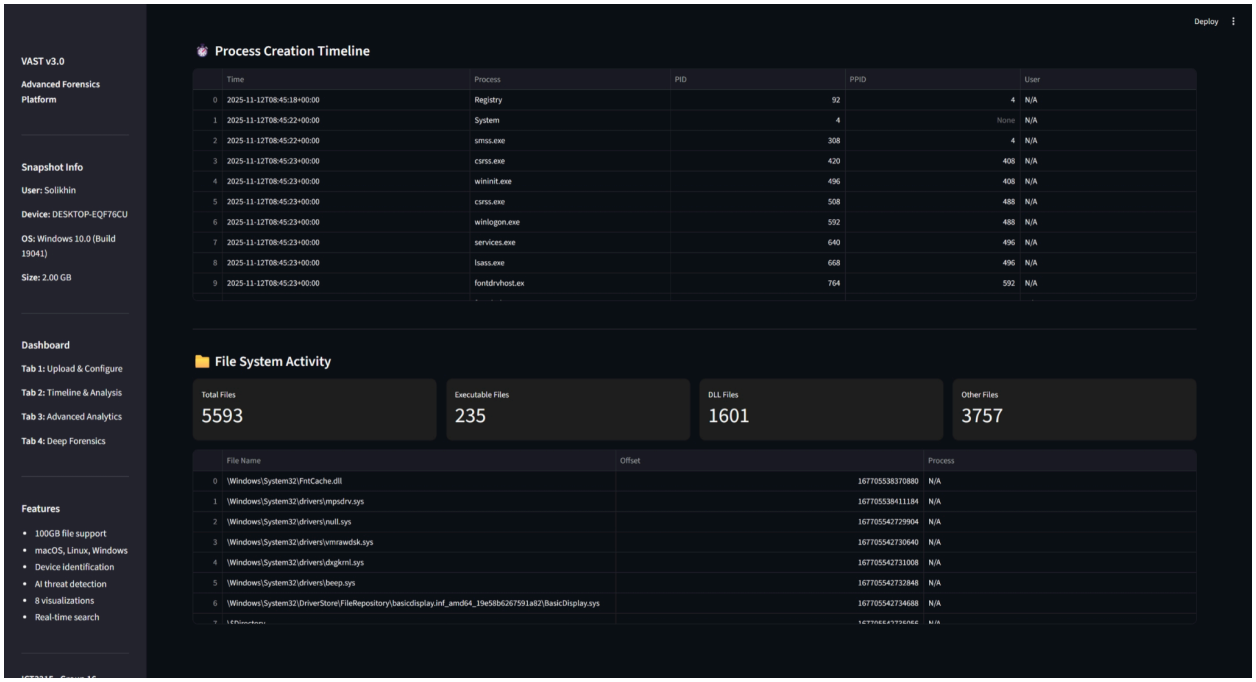




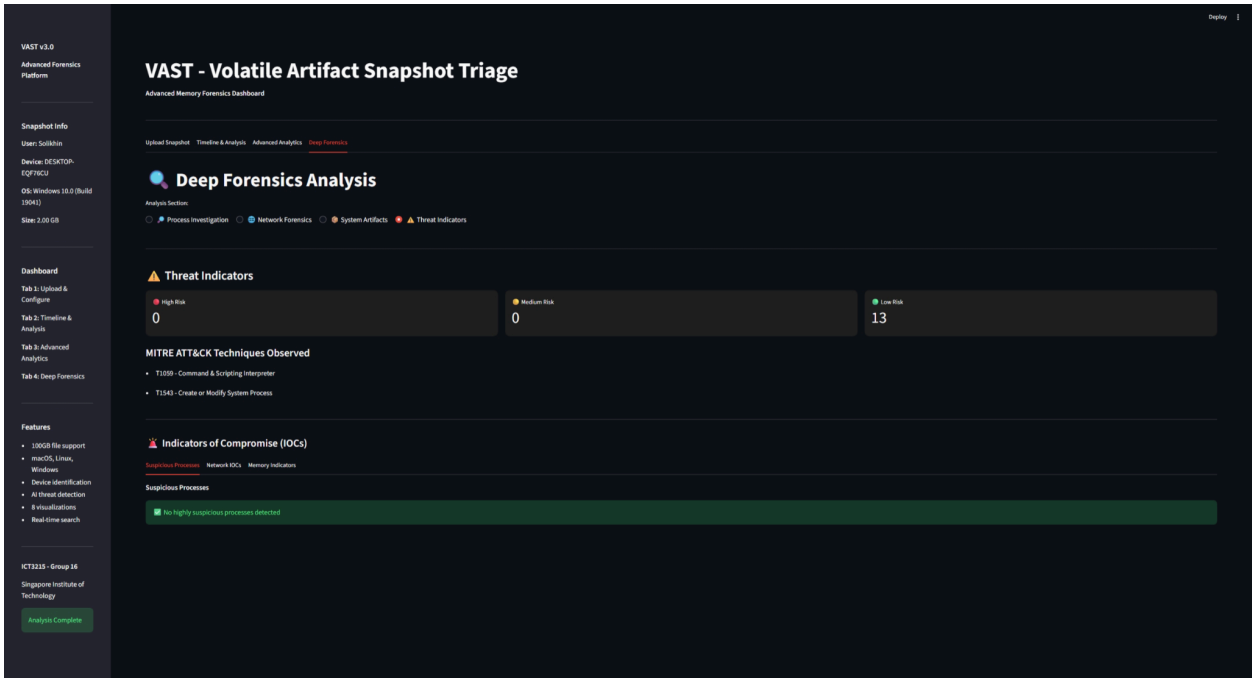


3. **Extract and Analyze System Artifacts**:
    - Review the "System Configuration" and "Device Information" for signs of system manipulation.
    - Examine the "Process Creation Timeline" to build a precise sequence of events, which is critical for understanding the initial infection vector and the progression of an attack.





4. **Hunt for Threat Indicators**:
    - Use the "Threat Indicators" section to review a consolidated list of all IOCs automatically detected by the system.
    - Manually hunt for IOCs not caught by automated rules by scanning for known malicious strings, code patterns, or rootkit signatures within the memory dump itself.



Logical User Workflow

1. Upload a dump file. Supported formats are: .vmem, .vmsn, .sav, .raw and .gz.
2. Click “Start Analysis” & VAST will extract the Processes, Handles, DLLs, Network artifacts & System metadata.
3. View Suspicious execution order, Odd parent/child chains, Processes running after shutdown in the “Timeline & Analysis” tab
4. Check the Threat severity distribution, Network connections, Suspicious processes in the “Advanced Analytics” tab
5. Investigate the DLL injections, Memory-resident malware, Rogue handles or hidden processes in the “Deep Forensics” tab

Troubleshooting

Issue: Streamlit doesn’t launch

→ Do a `pip install streamlit`