

# 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/khrnvn/VAST.git  
  
# Navigate into the project directory  
cd VAST  
  
# Install dependencies  
pip install -r requirements.txt
```

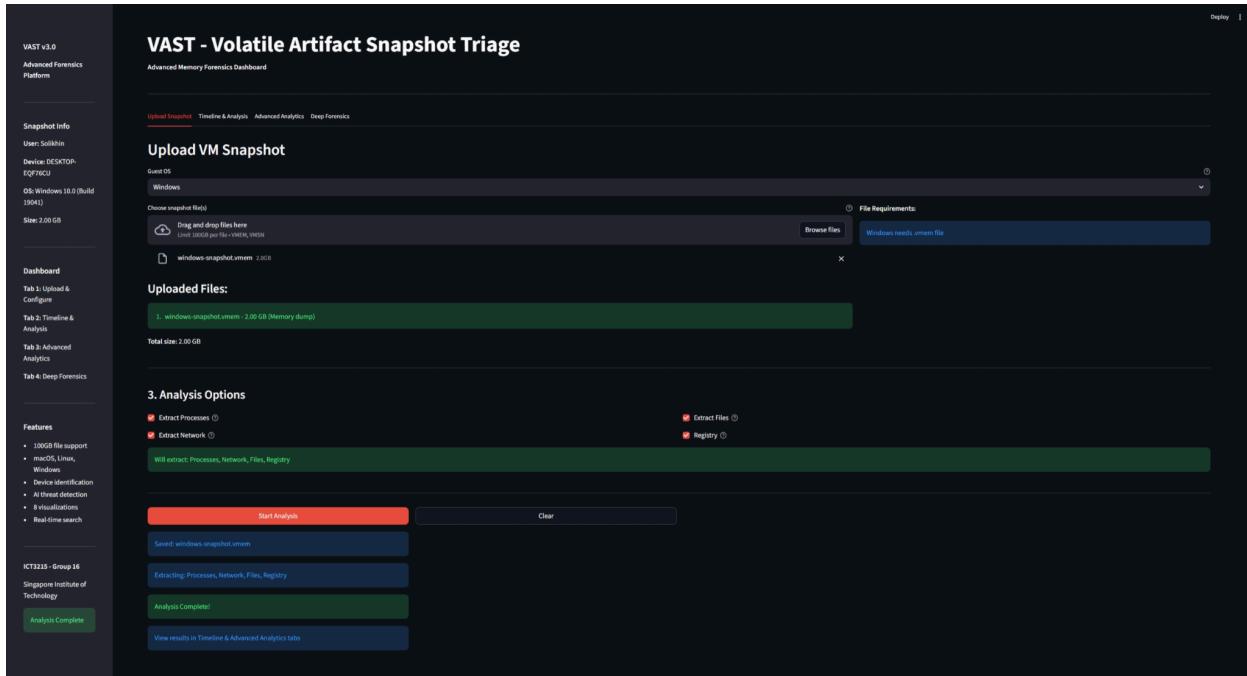
To run the application:

```
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:

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

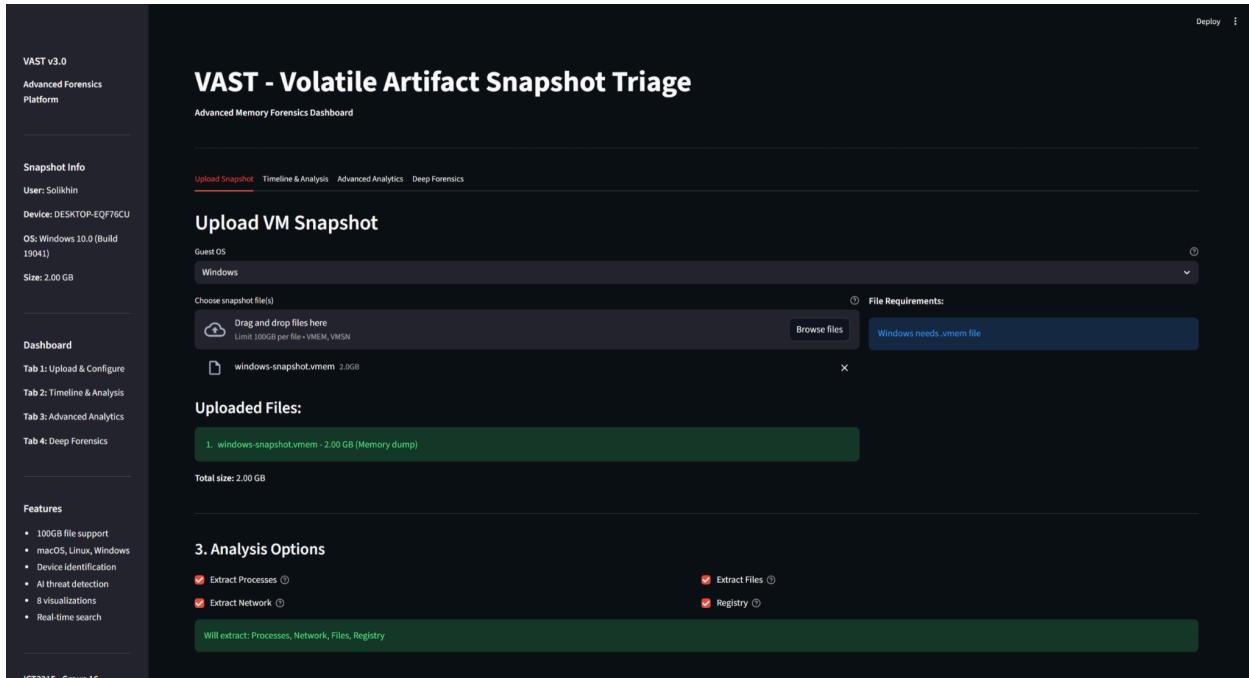
The dashboard also has a consistent sidebar that displays the dashboard tabs, key features, and snapshot information once analysed.

## Upload Snapshot

The logical workflow is:

- 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.

**VAST - Volatile Artifact Snapshot Triage**

Advanced Memory Forensics Dashboard

Upload Snapshot Timeline & Analysis Advanced Analytics Deep Forensics

### Timeline & Forensic Analysis

#### Snapshot Information

Username	Computer Name	OS Version	File Size
Solikhin	DESKTOP-EQF76CU	Windows 10.0 (Build 19041)	2.00 GB

Full Snapshot Details

Filename: windows-snapshot.vmem	Analysis Time: 2025-11-30 23:03:43
OS Type: Windows	Session: 20251130_225539
Architecture: Unknown	

#### Global Search

Search across all artifacts... Clear

#### Executive Summary

Processes	Network	Files	Total
105	80	5593	5778

---

### Threat Overview

High Risk	Medium Risk	Low Risk	Clean
0	0	13	92

Suspicion score is a heuristic 0-10 combining thread count, process type, script usage and unusual paths: 1-3 = low, 4-6 = medium, 7+ = high.

[View Automated Forensic Narrative Report](#)

#### Event Timeline

##### Chronological Event Sequence

- > Event #1 - ⚡ Process: System LOW
- > Event #2 - ⚡ Process: Registry
- > Event #3 - ⚡ Process: smss.exe
- > Event #4 - ⚡ Process: csrss.exe
- > Event #5 - ⚡ Process: wininit.exe
- > Event #6 - ⚡ Process: csrss.exe
- > Event #7 - ⚡ Process: winlogon.exe
- > Event #8 - ⚡ Process: services.exe
- > Event #9 - ⚡ Process: lsass.exe
- > Event #10 - ⚡ Process: fontdrvhost
- > Event #11 - ⚡ Process: fontdrvhost

**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

### Process Analysis

All Processes Table

Process	PID	PPID	Threads	User	Suspicion
System	4	N/A	118	N/A	2
Registry	92	4	4	N/A	0
sms.exe	308	4	3	N/A	0
csrss.exe	420	408	12	N/A	0
wininit.exe	496	408	5	N/A	0
cssrs.exe	508	488	13	N/A	0
winlogon.exe	592	488	6	N/A	0
services.exe	640	496	12	N/A	0
lsass.exe	668	496	12	N/A	0
fontdrvhost.exe	764	592	7	N/A	0

[Download CSV](#)

---

### Network Analysis

All Network Connections

Created	ForeignAddr	ForeignPort	LocalAddr	LocalPort	Offset	Owner	PID	Proto	State	suspicious_score	tags	
0	2025-11-12T08:45:24+00:00	0.0.0.0	0	0.0.0	445	16770538388400	System	4	TCPv4	LISTENING	2	listening sensitiv
1	2025-11-12T08:45:24+00:00	::	0	=	445	16770538388400	System	4	TCPv6	LISTENING	2	listening sensitiv
2	2025-11-12T08:45:24+00:00	0.0.0.0	0	0.0.0	49668	16770538389456	spoolsv.exe	1796	TCPv4	LISTENING	0	listening
3	2025-11-12T08:45:24+00:00	::	0	=	49668	16770538389456	spoolsv.exe	1796	TCPv6	LISTENING	0	listening
4	2025-11-12T08:45:24+00:00	0.0.0.0	0	0.0.0	49669	16770538389408	services.exe	640	TCPv4	LISTENING	0	listening
5	2025-11-12T08:45:24+00:00	0.0.0.0	0	0.0.0	49669	16770538390160	services.exe	640	TCPv4	LISTENING	0	listening
6	2025-11-12T08:45:24+00:00	::	0	=	49669	16770538390160	services.exe	640	TCPv6	LISTENING	0	listening

**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

### File Analysis

All File Objects

Name	Offset
0 \Windows\System32\FontCache.dll	16770538370680
1 \Windows\System32\drivers\pdps.sys	16770538311184
2 \Windows\System32\drivers\null.lys	167705542739954
3 \Windows\System32\drivers\vmrawdisk.sys	167705542730640
4 \Windows\System32\drivers\dxgkrnl.lys	167705542731008
5 \Windows\System32\drivers\beep.sys	167705542732648
6 \Windows\System32\DriverStore\FileRepository\basicdisplay.inf_amd64_19e58b6267591a82\BasicDisplay.sys	167705542734688
7 \\$Orkery	167705542735056
8 \Windows\System32\DriverStore\FileRepository\basicrender.inf_amd64_ebb5a8467eb88ec\BasicRender.sys	167705542736160
9 \Windows\System32\drivers\bbs.sys	167705542736528

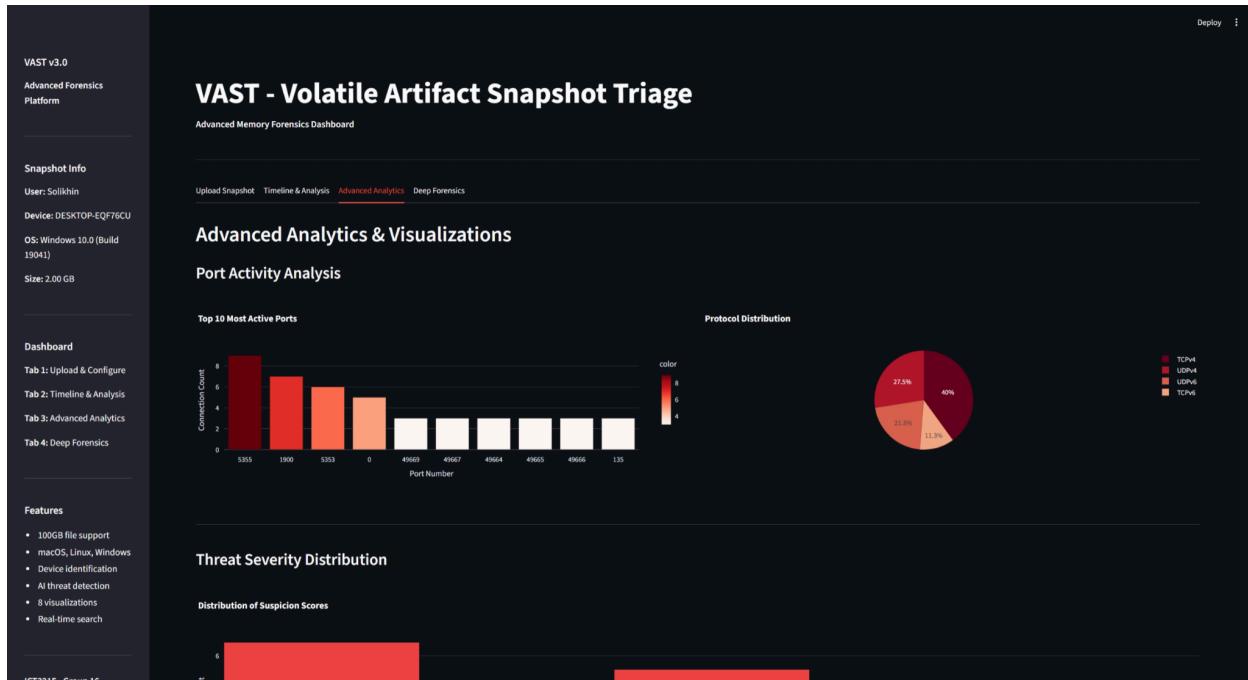
[Download CSV](#)

## 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.



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

Suspicion Score	Count
0.8	6
2.0	5
2.8	3

### Top 10 Most Suspicious Processes

ImageFileName	MITRE	PID	suspicious_score	tags
cmd.exe	T1059 - Command & Scripting Interpreter	6300	3	script_or_shell
System		4	2	high_thread_count
svchost.exe	T1541 - Create or Modify System Process	1000	2	high_thread_count
MemCompression		1432	2	high_thread_count
explorer.exe		3780	2	high_thread_count
SearchApp.exe		4808	2	high_thread_count
MicrosoftEdgeU		2444	1	wow64_process
MicrosoftEdgeU		3356	1	wow64_process
OneDrive.exe		6576	1	wow64_process

### Memory Usage Distribution

Top 10 Thread Consumers

ImageFileName	PID	Threads
System	4	118
svchost.exe	1000	88
explorer.exe	3780	74
SearchApp.exe	4808	71
MemCompression	1432	62
svchost.exe	780	46
svchost.exe	1124	36
svchost.exe	3492	35
svchost.exe	1288	28
MsMpEng.exe	2348	27

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
System	4	118
svchost.exe	1000	88
explorer.exe	3780	74
SearchApp.exe	4808	71
MemCompression	1432	62
svchost.exe	780	46
svchost.exe	1124	36
svchost.exe	3492	35
svchost.exe	1288	28
MsMpEng.exe	2348	27

### Connection State Analysis

Connection States

State	Count
LISTENING	38
CLOSED	18

Top 10 External Connections

IP Address	Connection Count
52.106.8.254	38
13.107.4.254	15
150.171.22.17	10
13.107.3.254	8
52.106.8.254	7
13.107.213.59	6
23.45.207.86	5
0.0.0.0	4

VAST v3.0  
Advanced Forensics Platform

**Snapshot Info**  
User: Solikhin  
Device: DESKTOP-EQF76CU  
OS: Windows 10.0 (Build 19041)  
Size: 2.00 GB

**File Access Patterns**

**File System Analysis**

Total File Objects: 5593

**File Statistics**

Unique Files: 5593  
Unique Names: 3800

**Top 10 File Extensions**

Extension	Count
dll	~1500
ini	~500
exe	~200
txt	~150
pri	~100
sys	~100
png	~100
xml	~100
extx	~100
dat	~100

**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

**Top 10 Analytics**

**Top 10 Most Active Processes**

ImageFileName	PID	Threads
System	4	118
svchost.exe	1000	88
explorer.exe	3780	74
SearchApp.exe	4808	71
MemCompression	1432	62
svchost.exe	780	46
svchost.exe	1124	36
svchost.exe	3492	35

**Top 10 Most Suspicious**

ImageFileName	PID	suspicious_score
cmd.exe	6300	3
System	4	2
svchost.exe	1000	2
MemCompression	1432	2
explorer.exe	3780	2
SearchApp.exe	4808	2
MicrosoftEdgeU	2444	1
MicrosoftEdge	3356	1

VAST v3.0  
Advanced Forensics Platform

**Snapshot Info**  
User: Solikhin  
Device: DESKTOP-EQF76CU  
OS: Windows 10.0 (Build 19041)  
Size: 2.00 GB

**Comprehensive Statistics**

**Process Stats**

Total Processes: 105

**Network Stats**

Total Connections: 80

**File Stats**

Total Files: 5593  
Unique Names: 3800

**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

**Export Results**

Generate JSON Report  
Download Report

## 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.

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

## VAST - Volatile Artifact Snapshot Triage

Advanced Memory Forensics Dashboard

Upload Snapshot   Timeline & Analysis   Advanced Analytics   Deep Forensics

### Deep Forensics Analysis

Analysis Section:  Process Investigation  Network Forensics  System Artifacts  Threat Indicators

#### Process Investigation

Total Processes	System Processes	User Processes	Terminated
105	35	70	3

#### Parent-Child Process Trees

Key Parent Processes

- > explorer.exe (PID: 3780) - 2 children
- > services.exe (PID: 640) - 39 children
- > winlogon.exe (PID: 592) - 3 children
- > wininit.exe (PID: 496) - 3 children

Suspicious Process Trees

- > cmd.exe (PID: 6300) - 1 children

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

#### Key Parent Processes

- > explorer.exe (PID: 3780) - 2 children
- > services.exe (PID: 640) - 39 children
- > winlogon.exe (PID: 592) - 3 children
- > wininit.exe (PID: 496) - 3 children

#### Suspicious Process Trees

- > cmd.exe (PID: 6300) - 1 children

#### Short-Lived Processes

Process	PID	PPID	Start Time	Exit Time	Suspicion Score
0 userinit.exe	3540	592	2025-11-12T08:45:26+00:00	2025-11-12T08:45:50+00:00	0
1 cmd.exe	6300	2332	2025-11-12T08:46:36+00:00	2025-11-12T08:46:36+00:00	3
2 conhost.exe	3452	6300	2025-11-12T08:46:36+00:00	2025-11-12T08:46:36+00:00	0

**Download CSV**

#### Process Lookup

Search by process name or PID:

## 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.

**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

### VAST - Volatile Artifact Snapshot Triage

Advanced Memory Forensics Dashboard

Upload Snapshot Timeline & Analysis Advanced Analytics Deep Forensics

**Deep Forensics Analysis**

Analysis Section:  Process Investigation  Network Forensics  System Artifacts  Threat Indicators

**Network Forensics**

Total Connections	Established	Listening	Closed
80	0	24	17

**Connection State Distribution**

Connection States

State	Count
LISTENING	24
CLOSED	17
UNKNOWN	39

---

**IP Address Analysis**

External IPs Private IPs Suspicious Ports

**Top External IPs**

Connections IP Address

IP Address	Connections
23.45.207.86	39
13.107.213.59	2
23.45.207.73	2
150.171.22.254	1
204.79.197.222	1
40.126.55.19	1
150.171.85.254	1
23.210.96.161	1

---

**Process Network Activity**

The screenshot shows the VAST v3.0 interface. On the left, there's a sidebar with 'Snapshot Info' (User: Solikhin, Device: DESKTOP-EQF76CU, OS: Windows 10.0 (Build 19041), Size: 2.00 GB) and a 'Features' section listing support for 100GB file support, macOS/Linux/Windows, Device identification, AI threat detection, 8 visualizations, and Real-time search. The main area has tabs for 'Process Network Activity' (which is active) and 'Process Creation Timeline'. The 'Process Network Activity' tab displays a table of connections with columns: Process, Total Connections, Established, Listening, and Unique IPs. A 'Download CSV' button is at the bottom.

### 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.

The screenshot shows the VAST - Volatile Artifact Snapshot Triage interface. It features a 'Deep Forensics Analysis' section with a 'System Artifacts' icon and a 'System Configuration' icon. Below these are sections for 'Device Information' (Computer Name: DESKTOP-EQF76CU, Username: Solikhin, OS Version: Windows 10.0 (Build 19041)) and 'Snapshot Details' (File Size: 2.00 GB, Analysis Date: 2025-11-30 23:03:43, OS Type: Windows). At the bottom, there's a 'Process Creation Timeline' table with columns: Time, Process, PID, PPID, and User.

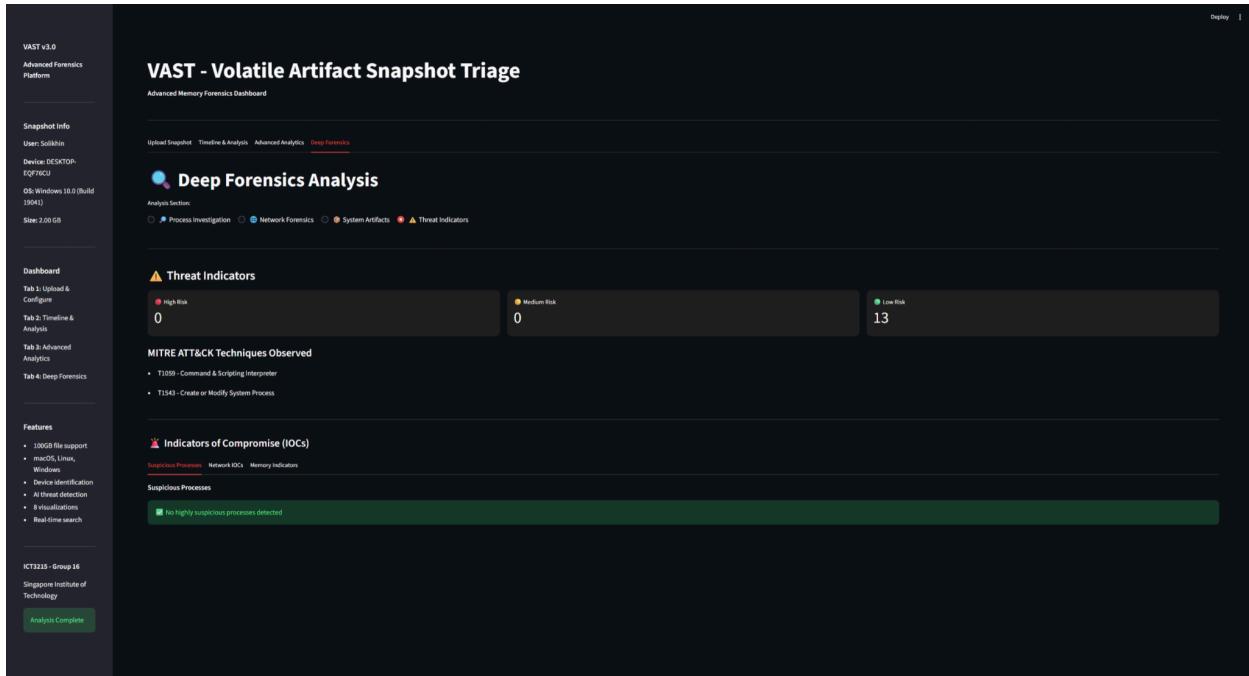
The screenshot displays the VAST v3.0 interface with the following sections:

- VAST v3.0** header.
- Advanced Forensics Platform** sidebar with "Snapshot Info" (User: Solikhin, Device: DESKTOP-EQF76CU, OS: Windows 10.0 (Build 19041), Size: 2.00 GB).
- Dashboard** sidebar with tabs: Tab 1: Upload & Configure, Tab 2: Timeline & Analysis, Tab 3: Advanced Analytics, Tab 4: Deep Forensics.
- Features** sidebar with a bulleted list: 100GB file support, macOS, Linux, Windows, Device Identification, AI threat detection, 8 visualizations, Real-time search.
- Process Creation Timeline** table showing processes from 0 to 9 with their corresponding Time, Process name, PID, PPID, and User.
- File System Activity** section with four counts: Total Files (5593), Executable Files (235), DLL Files (1601), and Other Files (3757). Below is a table of file details with columns: File Name, Offset, and Process.

File Name	Offset	Process
0 \Windows\System32\FltCache.dll	167705538370880	N/A
1 \Windows\System32\drivers\mpsdrv.sys	16770554211184	N/A
2 \Windows\System32\drivers\mult.sys	16770554272904	N/A
3 \Windows\System32\drivers\vmrawdsk.sys	167705542730640	N/A
4 \Windows\System32\drivers\dgkmlm.sys	167705542731008	N/A
5 \Windows\System32\drivers\beep.sys	167705542733848	N/A
6 \Windows\System32\DriverStore\FileRepository\basicdisplay.inf_amd64_19e5856207591a2\BasicDisplay.sys	167705542734688	N/A
7 \Windows\System32\DriverStore\FileRepository\basicdisplay.inf_amd64_19e5856207591a2\BasicDisplay.sys	167705542734688	N/A

#### 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: .vmmem, .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