**⚙Digisuraksha project 2025**

**Tool Name: Process Explorer Process Monitor**

### **History**

Born from Sysinternals (founded by Mark Russinovich), these tools were acquired by Microsoft in 2006. Process Explorer merged earlier tools in 2001, while Process Monitor succeeded others, unifying system activity logging.

### **Description: What Is This Tool About?**

* **Process Explorer:** An advanced task manager showing a **hierarchical view of processes** with details on threads, handles, DLLs, and performance.
* **Process Monitor:** A real-time monitor capturing **file system, Registry, and process/thread activity**, providing granular event logs.

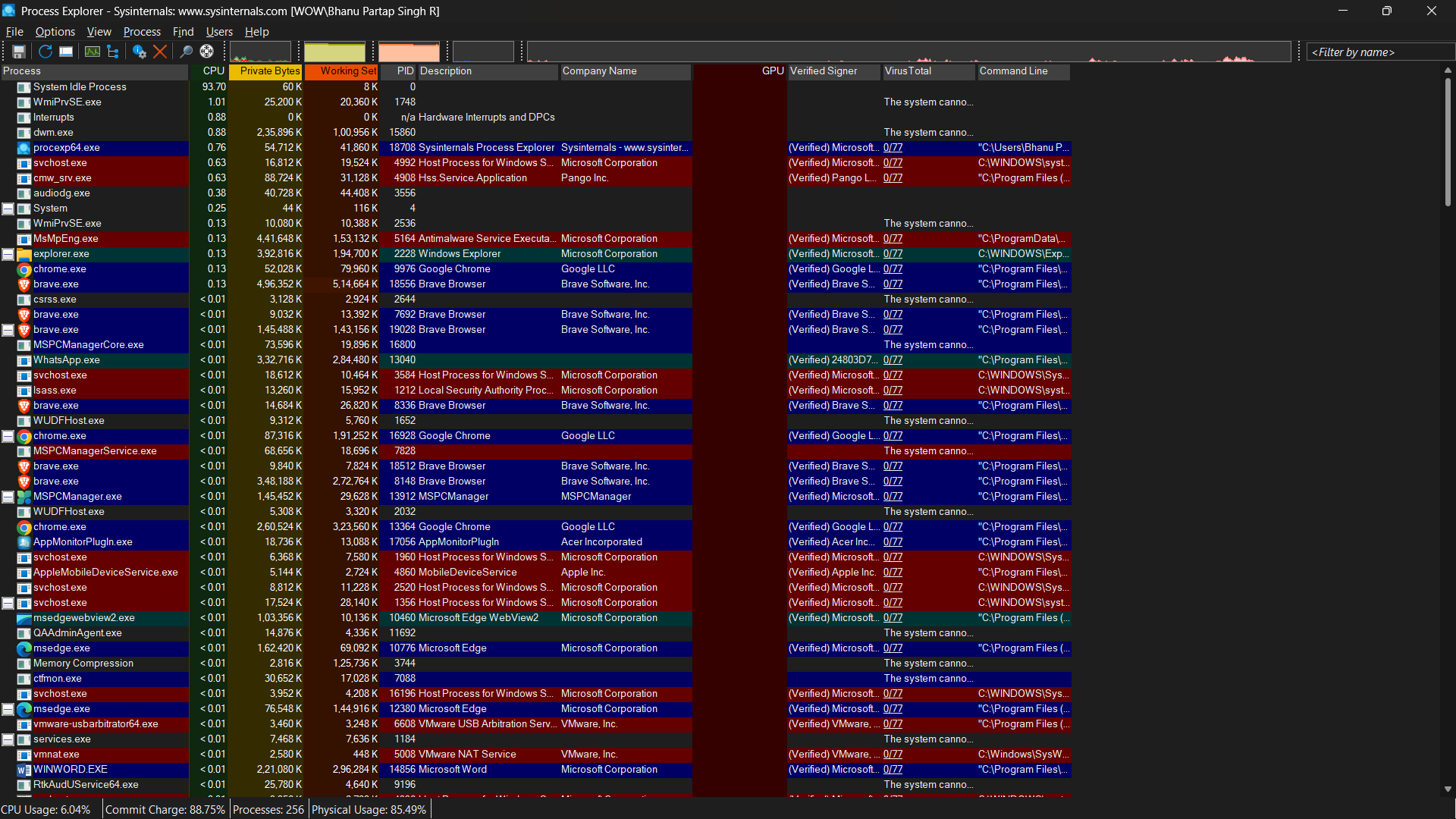
### **Key Characteristics / Features:**

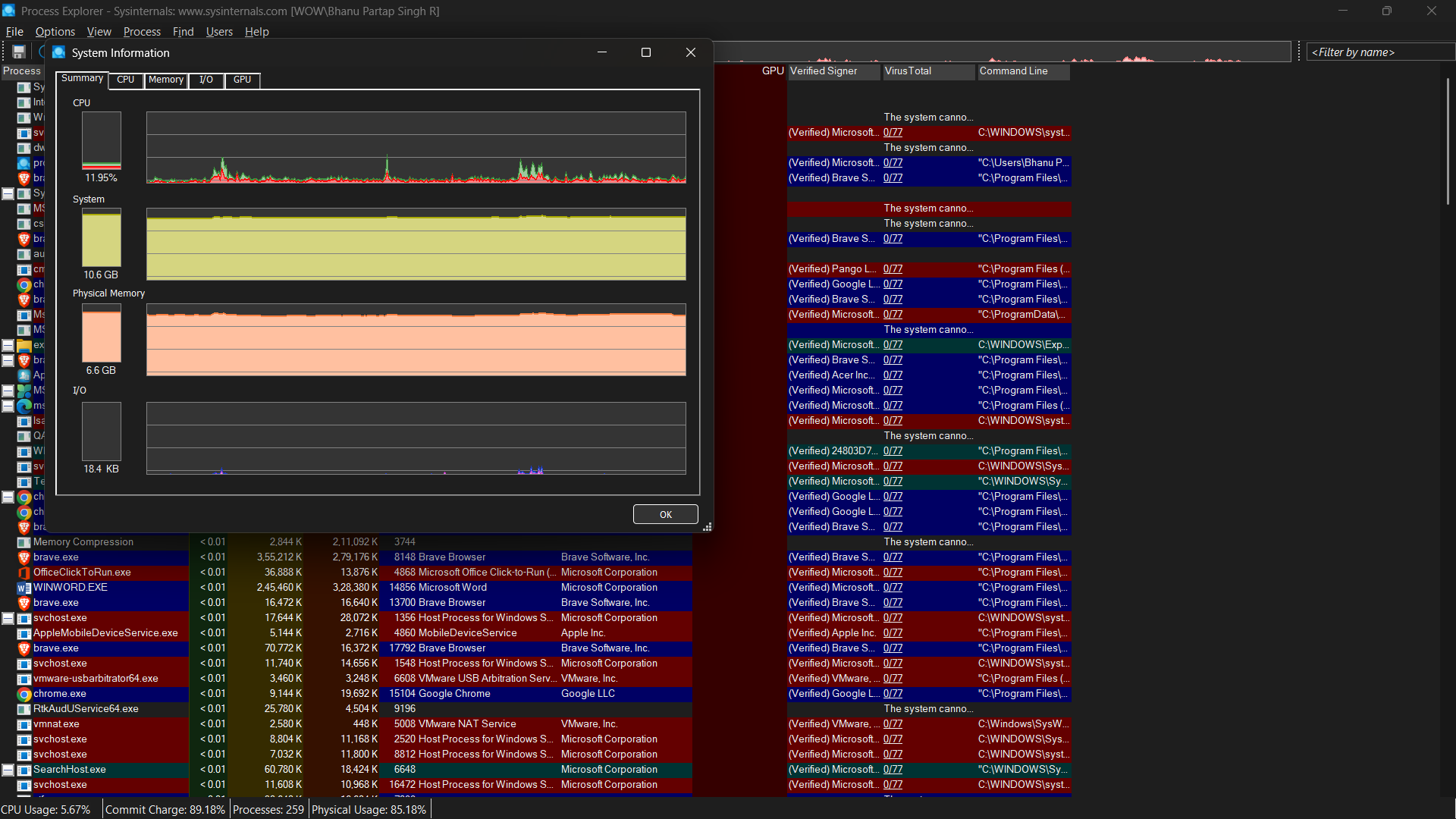
* **Process Explorer:** Detailed process info, handle/DLL inspection, process control, real-time graphs, VirusTotal integration.
* **Process Monitor:** Real-time event capture, powerful filtering, detailed event properties, boot logging, process tree view.

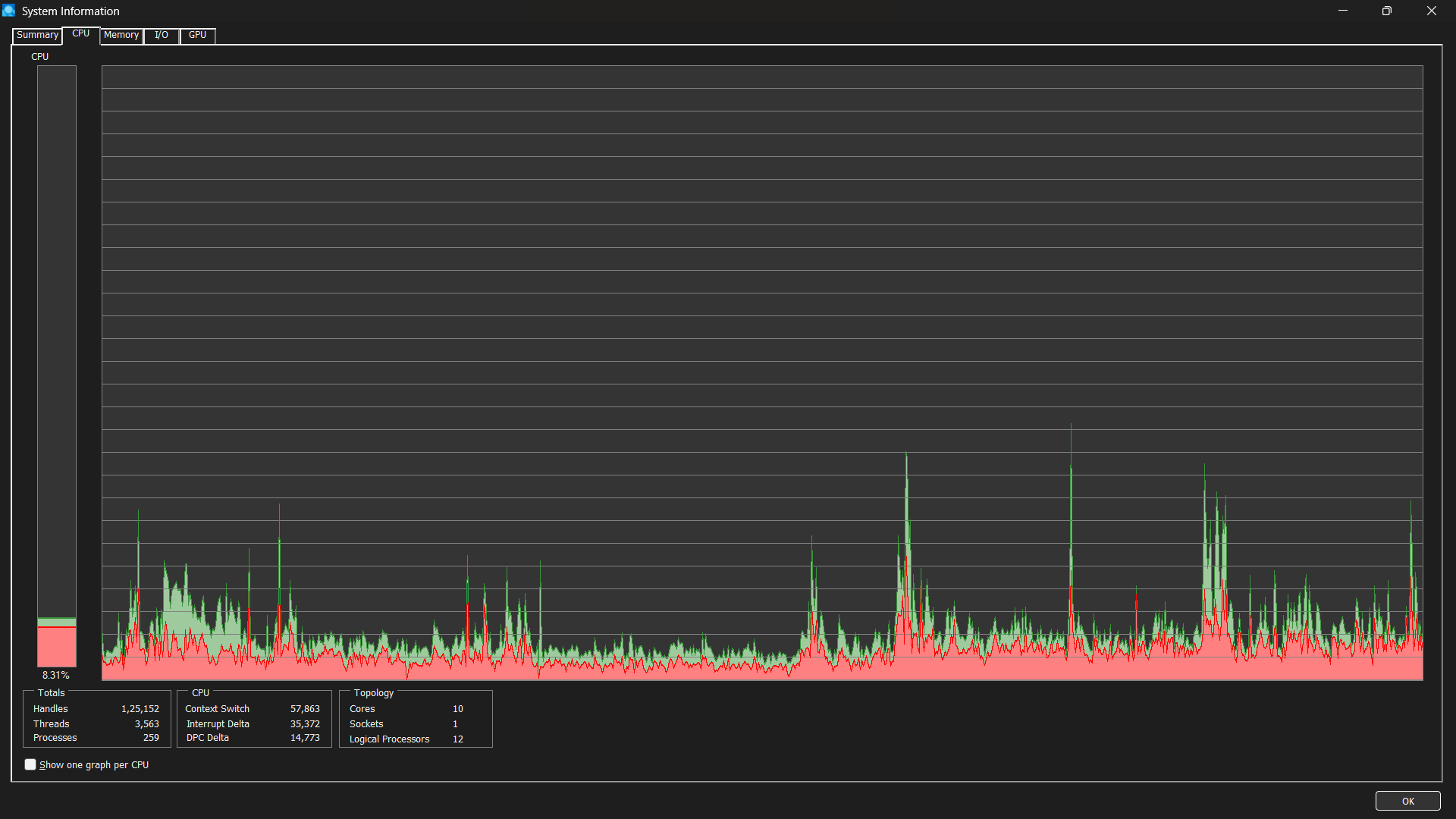
### **How Will This Tool Help?**

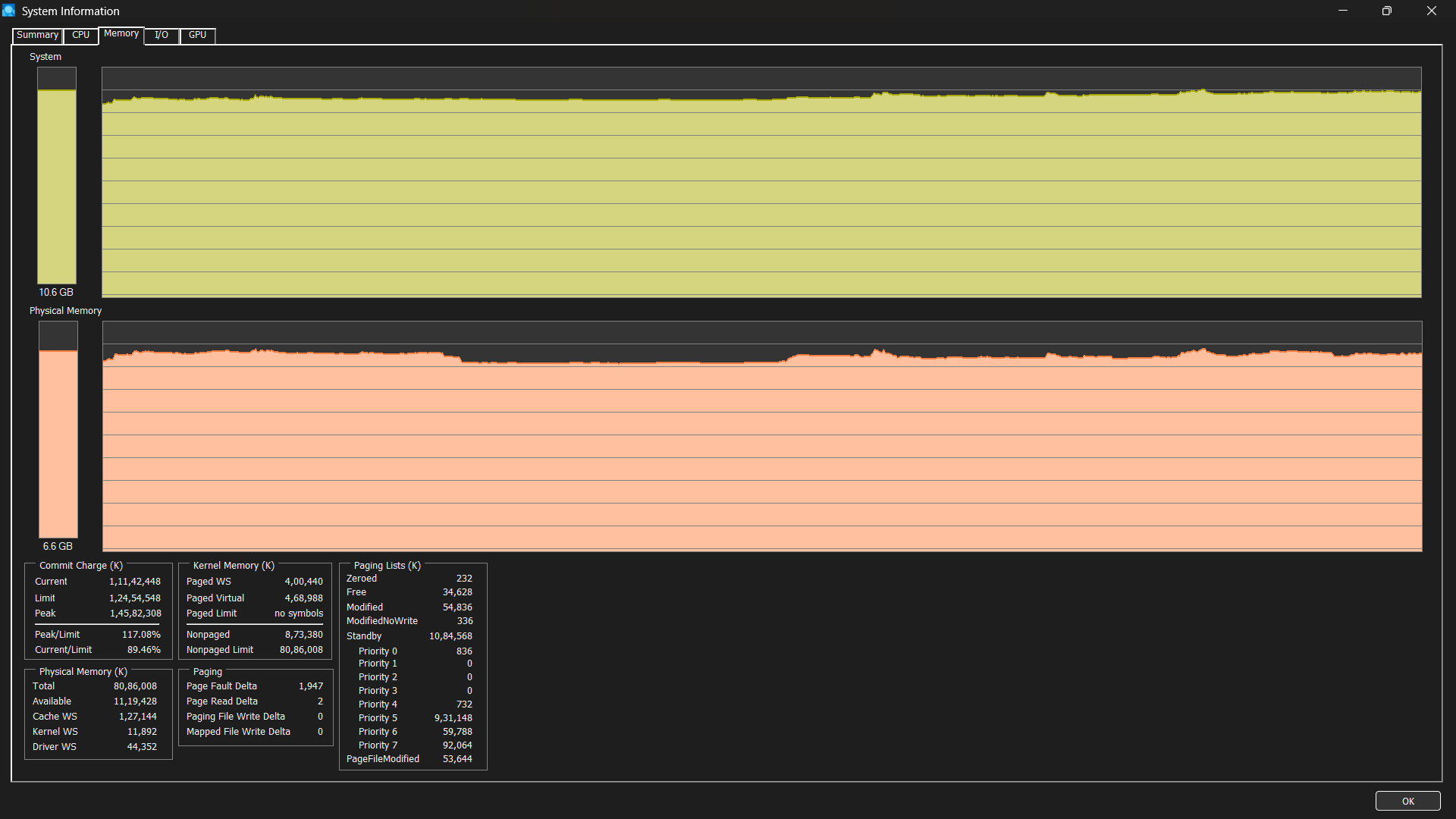
They help **troubleshoot system issues** (crashes, slowdowns, errors), **analyze malware** by observing suspicious activity, and **understand system interactions** for debugging and security auditing.

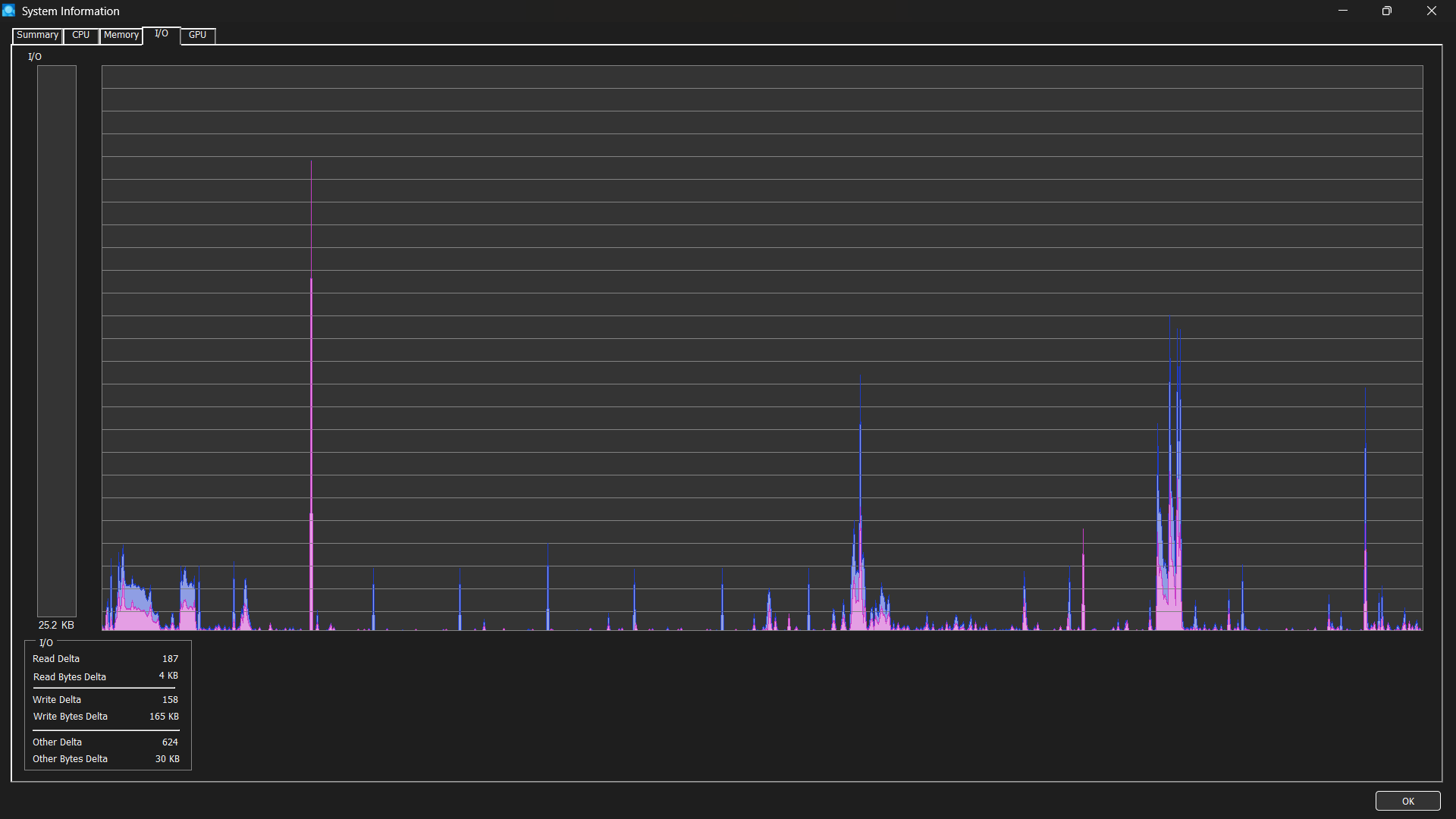
### **Proof of Concept (PoC) Images:**

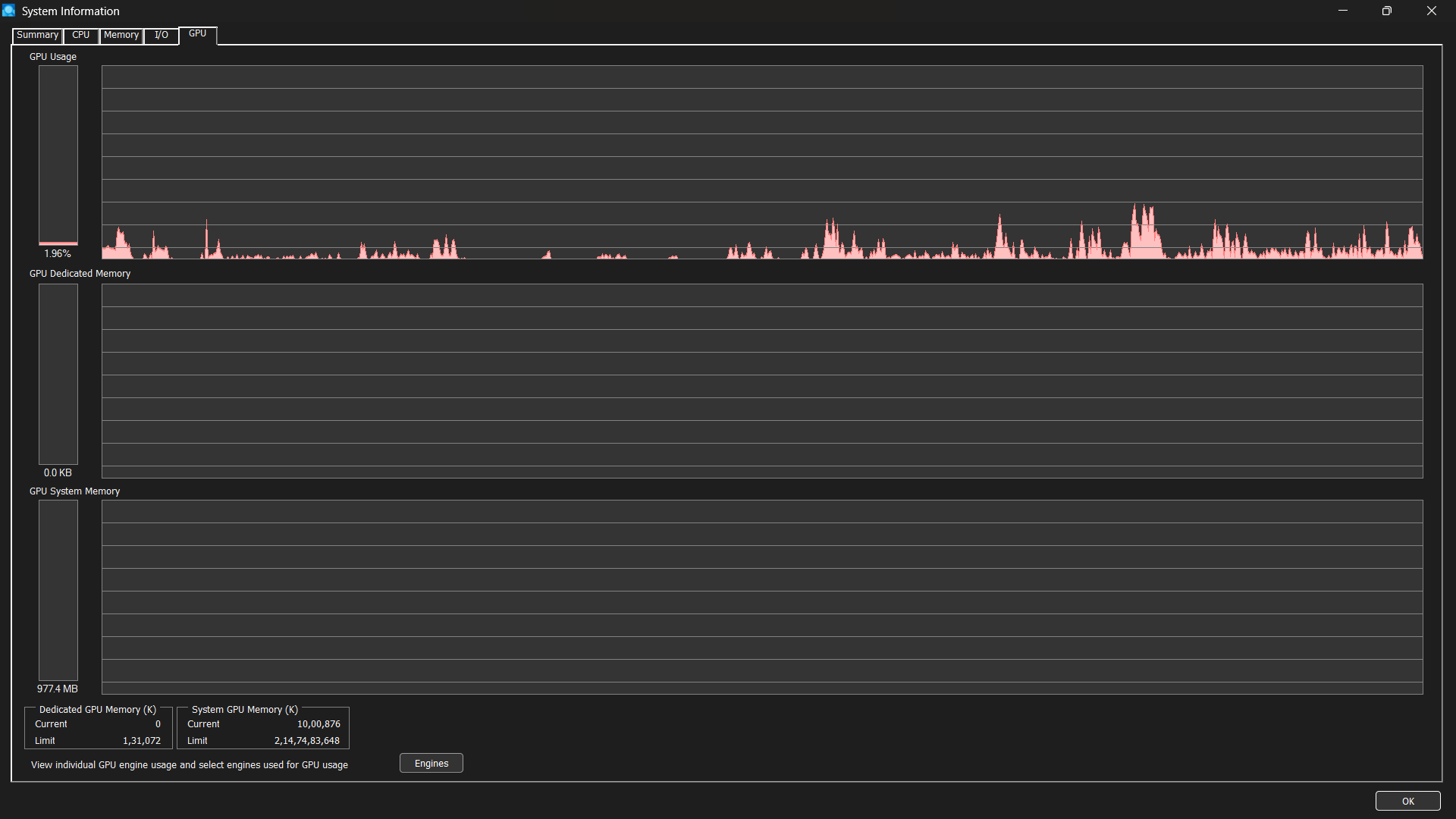


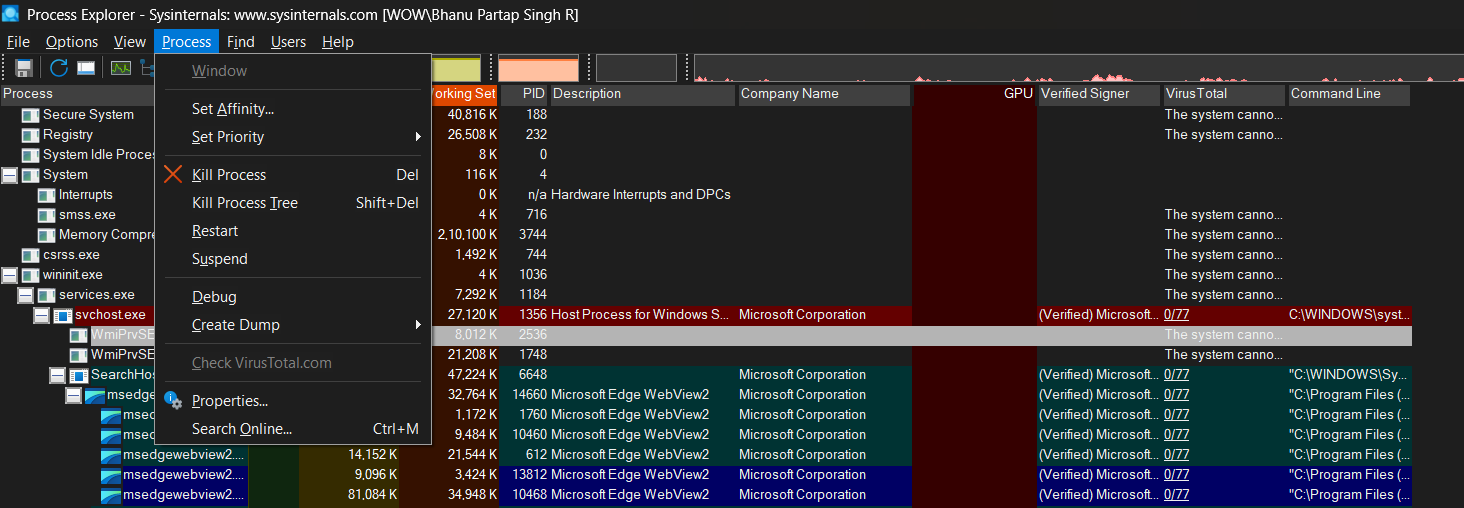


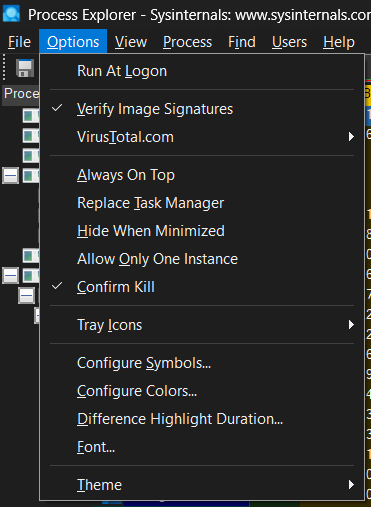


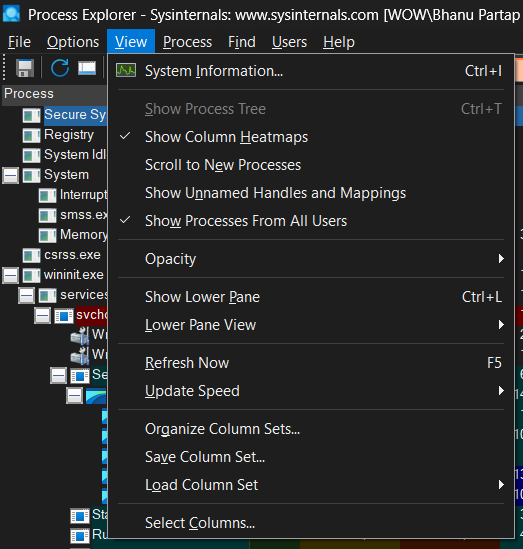


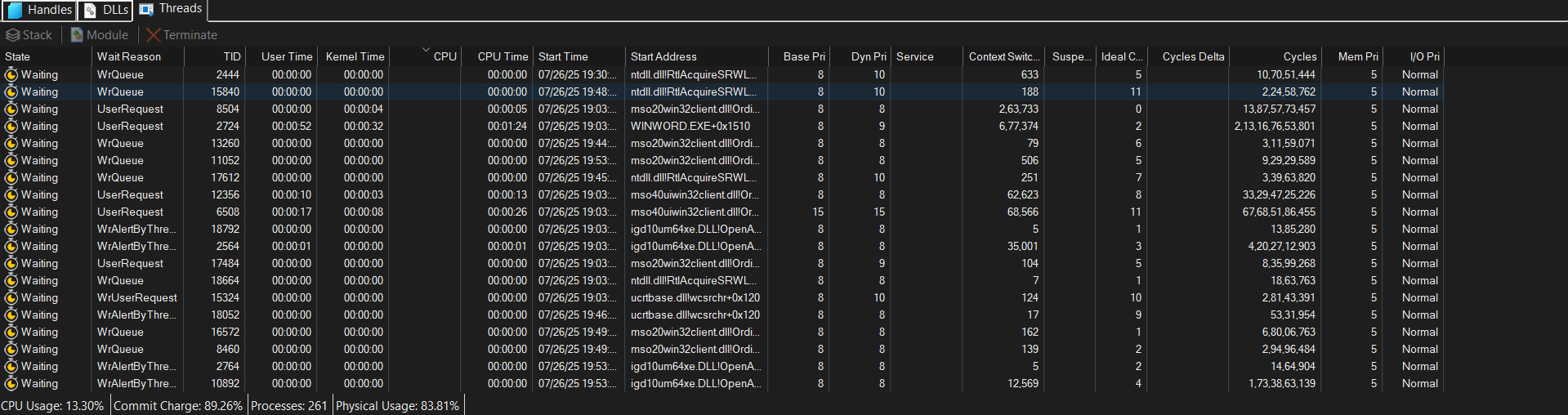












### **15-Liner Summary:**

 Process Explorer and Process Monitor are indispensable Windows utilities from Sysinternals.

 They are powerful, free, and portable, requiring no installation.

 **Process Explorer** functions as an enhanced task manager.

 It offers deep insights into running processes.

 Details include resource consumption (CPU, memory), open handles, and loaded DLLs.

 It's crucial for identifying performance bottlenecks.

 Its VirusTotal integration helps detect suspicious activity.

 **Process Monitor**, conversely, logs real-time system operations.

 It captures file, Registry, and process activity.

 This makes it invaluable for diagnosing application errors.

 It's excellent for tracking system changes.

 Its powerful filtering aids in observing malware behavior.

 Together, these tools provide unparalleled visibility into the Windows OS.

 They empower IT professionals, security analysts, and developers.

 They facilitate efficient troubleshooting, understanding interactions, and bolstering security posture.

### **Time to Use / Best Case Scenarios:**

* **Process Explorer:** When a system is slow (identify resource hogs), an app freezes (terminate/investigate), or to identify file locks or verify process legitimacy.
* **Process Monitor:** When apps fail (find "Access Denied" errors), track installer changes, monitor network connections, or observe malware actions.

### **When to Use During Investigation:**

Use them **early in an investigation** for performance issues, application malfunctions, security incidents (e.g., live malware analysis), and live system forensics.

### **Best person to use that tool and what skills required:**

* **Best Person:** System Administrators, Cybersecurity Analysts (malware analysts, incident responders), Developers, Advanced IT Support.
* **Skills:** Strong **Windows Internals knowledge**, analytical thinking, problem-solving, and basic security concepts.

### **Flaws / Suggestions to Improve in That Tool:**

* **Process Explorer:** Lacks robust historical logging and scripting. *Suggestion: Add logging and scripting APIs.*
* **Process Monitor:** Generates high data volume and can consume resources for long captures. *Suggestion: Improve intelligent filtering and optimize resource use for extended logging.* Both primarily monitor; they don't directly remediate.

### **Good About Tools:**

* **Free and Portable:** No installation needed.
* **Comprehensive Insight:** Deep visibility into Windows.
* **Real-time Visibility:** Instant feedback on system activity.
* **Powerful Filtering (ProcMon):** Essential for managing vast data.
* **VirusTotal Integration (ProcExp):** Critical for quick malware checks.
* **Reliable:** Developed by Microsoft (Sysinternals).
* **Lightweight:** Minimal performance impact.
* **Indispensable:** Go-to tools for complex Windows problems.