VAIBHAV RATAN Intern ID- 441

🛠 Tool Name: RamMap

History

Developed by Microsoft Sysinternals, RamMap has been part of the Windows Sysinternals suite for years, offering deep insight into physical memory usage. It's widely used by system administrators, digital forensics analysts, and malware researchers.

📄 **Description:**

RamMap is a Windows-based forensic and performance analysis tool that provides detailed insight into physical memory usage. It reveals how Windows is allocating physical memory, down to the file, process, and page level.

📌 **What Is This Tool About?**

RamMap helps analysts visualize and dissect how physical memory is being used by the Windows operating system in real time and through snapshot-based views. It provides insight into memory segments that are often opaque, like driver-loaded memory, standby lists, and mapped file memory.

⭐ **Key Characteristics / Features:**

1. Displays usage by process, file, and memory type
2. Interactive GUI with sortable columns
3. Active, standby, and modified memory tracking
4. Breakdown by file summary and session usage
5. "Use Counts" tab to reveal actual allocation type

6. Show mapped files in RAM
7. Helps in identifying memory leaks
8. Supports save/load memory snapshots
9. Non-destructive – Read-only tool
10. Standalone executable (no installation needed)
11. Memory analysis at page level granularity
12. Differentiates between system, driver, and user memory
13. Helps in malware and rootkit memory investigation
14. Built-in support for Windows 10/11
15. Zero cost – freeware from Microsoft

🔧 **Types / Modules Available:**

- **Use Counts** – Summarizes allocation by type
- **Processes** – Shows memory usage per process
- **Priority Summary** – Displays memory distribution by priority
- **Physical Pages** – Detailed memory page data
- **File Summary** – Lists all memory-mapped files
- **File Details** – Breakdown of file-backed RAM pages
- **Session Use** – Session-level usage for Terminal Services

---

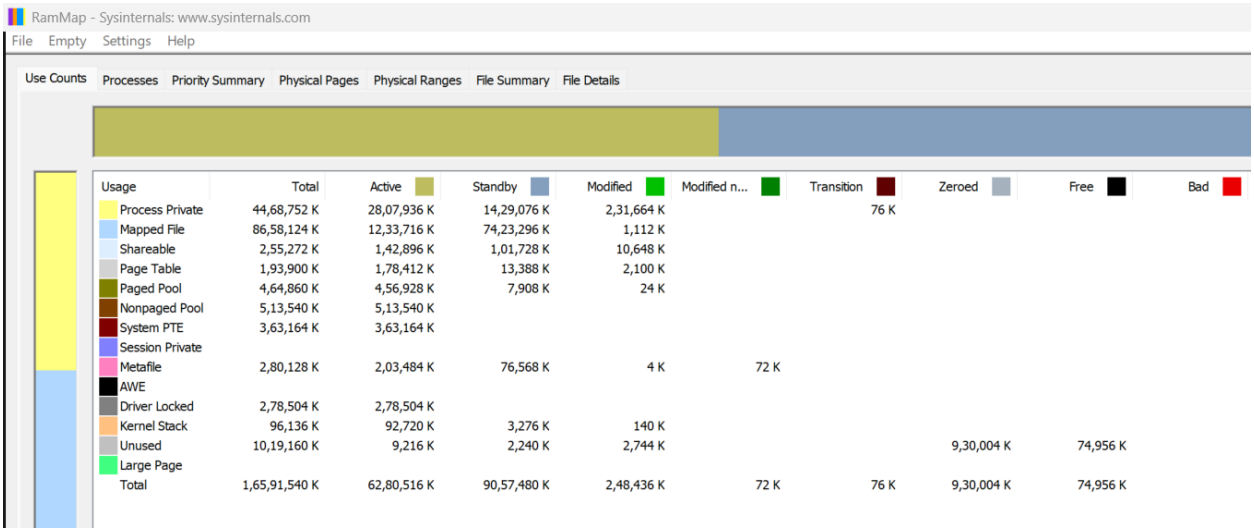
🎯 **How Will This Tool Help?**

- Identifies what files are consuming physical memory
- Locates hidden or injected memory sections used by malware
- Aids in triaging live memory during incident response
- Provides detailed forensic insight into RAM artifacts
- Detects memory-hogging processes or abnormal allocations

- Maps system internals for performance tuning or rootkit detection

---

🖼 Proof of Concept (PoC) Images:



📜 15-Liner Summary:

1. Maps real-time physical memory usage
2. Supports live system memory analysis
3. Provides insight into driver and system memory
4. Useful for detecting malicious in-memory artifacts
5. Non-intrusive, read-only memory parser
6. GUI with multiple views: Use Counts, Processes, etc.
7. Highlights memory leaks and resource hogs
8. Forensic triage for memory-resident malware
9. Standalone tool – no installation required
10. From trusted source (Microsoft Sysinternals)
11. Captures and saves memory snapshot states
12. Memory page-level analysis

13. Reveals hidden or injected memory sections
14. Works well in both IR and performance profiling
15. Ideal for both DFIR and memory optimization

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

- During live incident response
- Before memory gets swapped out or paged
- While investigating rootkits/memory-only malware
- For RAM-based IOC extraction
- During post-exploitation analysis
- Performance tuning on enterprise endpoints

🕵️ **When to Use During Investigation:**

- Live triage in malware incidents
- Volatile memory analysis
- Detection of fileless malware
- Rootkit or driver-level forensics
- Analyzing advanced persistent threats (APTs)
- Investigating large memory leaks or abnormal usage

👨‍💻 **Best Person to Use This Tool & Required Skills:**

Best User: Memory Forensics Analyst / Malware Researcher / IR Specialist

Required Skills:

- Understanding of Windows memory architecture
- Familiarity with system internals and page file usage
- Knowledge of malware memory behavior

- Basic forensic handling procedures (e.g., volatile data handling)
- Skill in interpreting memory segmentation and mapped files

🧩 **Flaws / Suggestions to Improve:**

- Lacks automation or scripting interface
- No CLI version for headless analysis
- No built-in export to volatile memory dump formats
- Limited filtering/sorting capabilities for large systems
- No integration with forensic suites like Volatility

✅ **Good About the Tool:**

- Highly detailed breakdown of memory usage
- Excellent for detecting fileless malware
- Lightweight and doesn’t alter memory state
- Maintained by a reputable source (Microsoft)
- Rapid memory inspection with user-friendly UI
- Portable and easy to deploy across systems