**Networking Tracking and Process Monitoring**

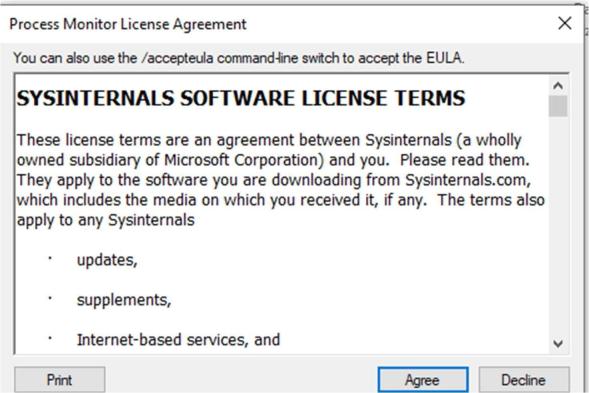
**Sysinternals** is a set of advanced system utilities and tools developed by Microsoft. It provides comprehensive insights into the internal workings of the Windows operating system.

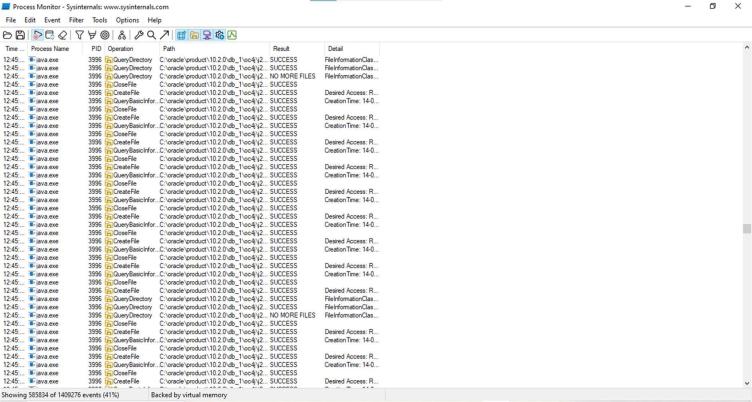
# **Installation**

*Unzip the folder*

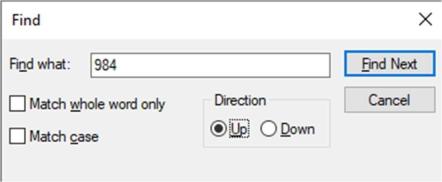
## **Procmon – Process Monitor**

Procmon - Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity.

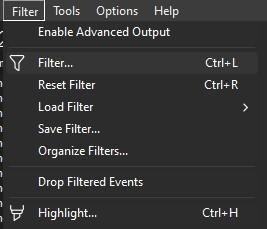


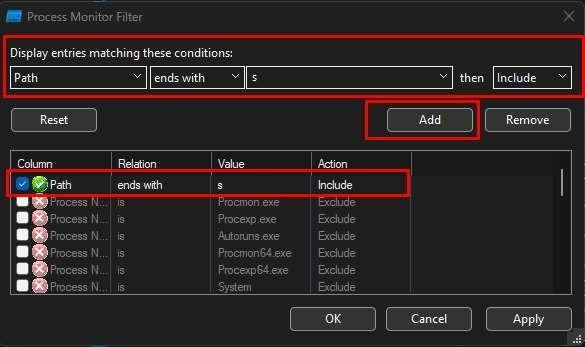


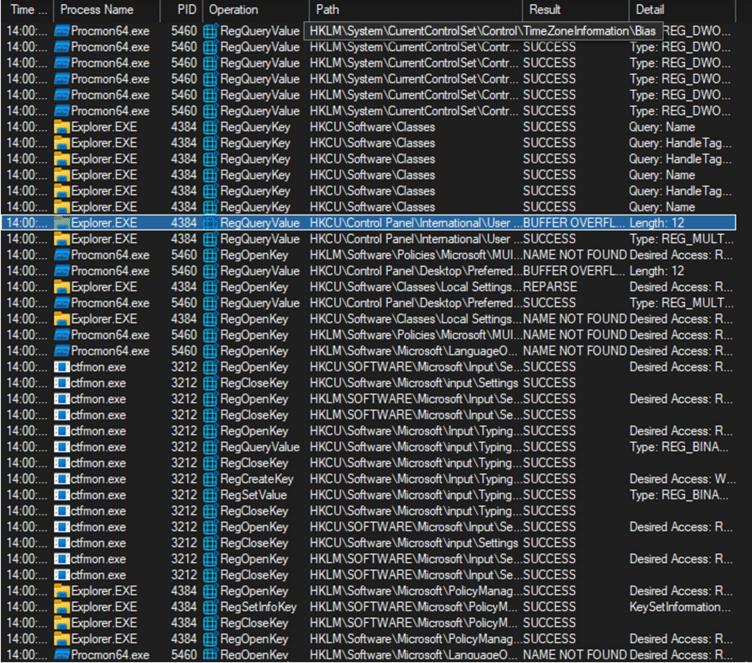
1. **Filtering by Process ID (PID)** in Procmon is useful for isolating the activity of a particular process, especially when investigating malware or specific software behavior. By applying a filter for **Process ID**, you can view the related file, registry, and network operations, making it easier to track and analyze specific actions.



## **Listing processes whose path ends with ‘s’**



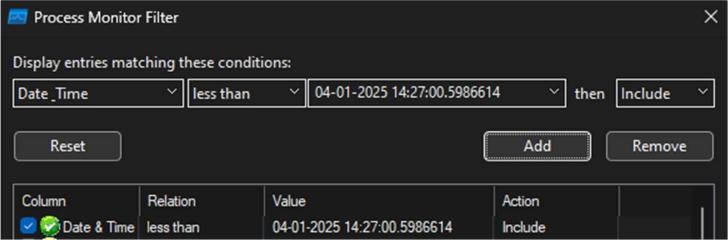




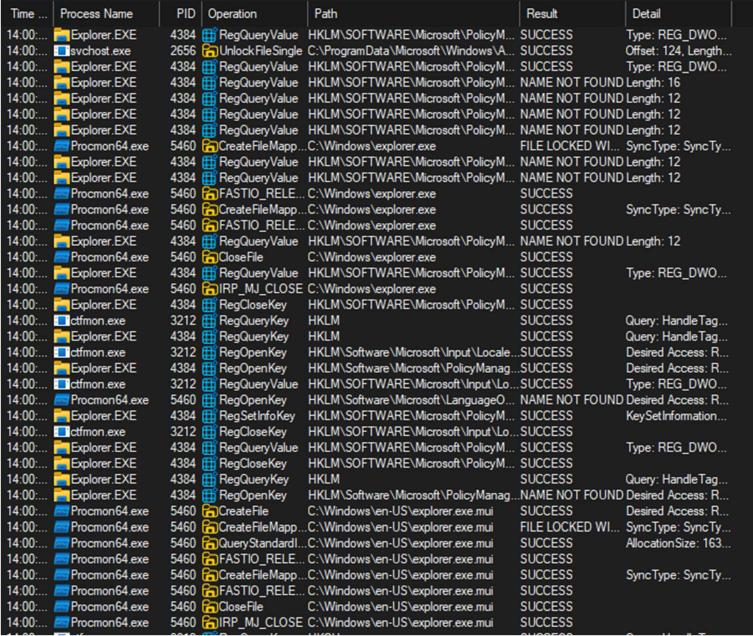
*Processes whose path ends with 's'*

## **Show all processes captured before 4/1/2025 14:27:00**

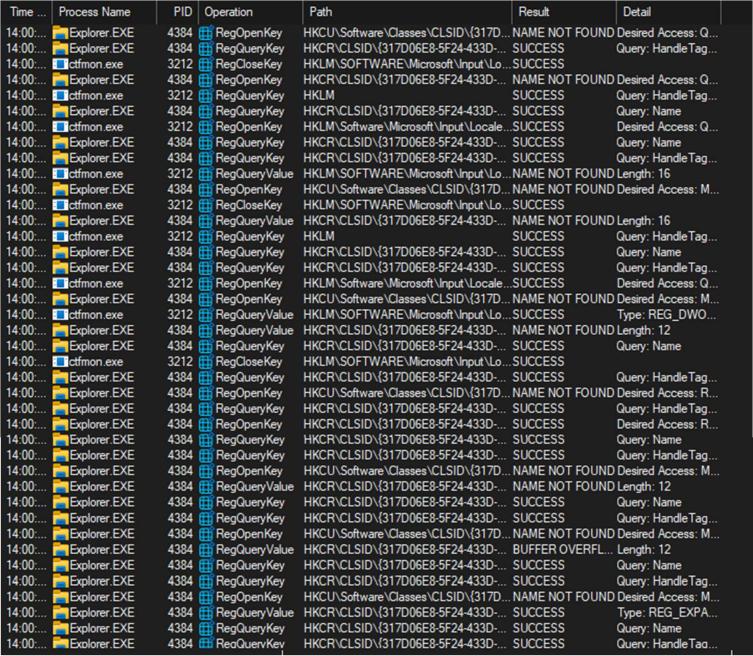
Right click on the time and select Edit Filter…..



You **cannot** directly get data from yesterday if you were not actively capturing it with **Procmon** during that time. If you did capture logs during yesterday, you can filter those logs by applying a **date/time filter** for that specific day.



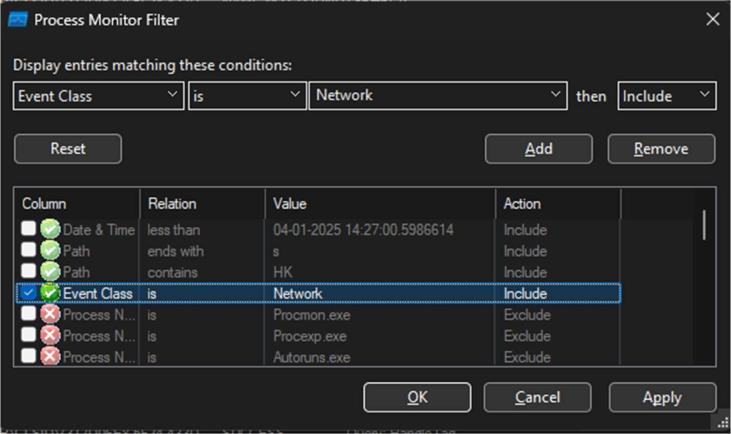
## **List process relate RegEdit operation (path contains HK)**

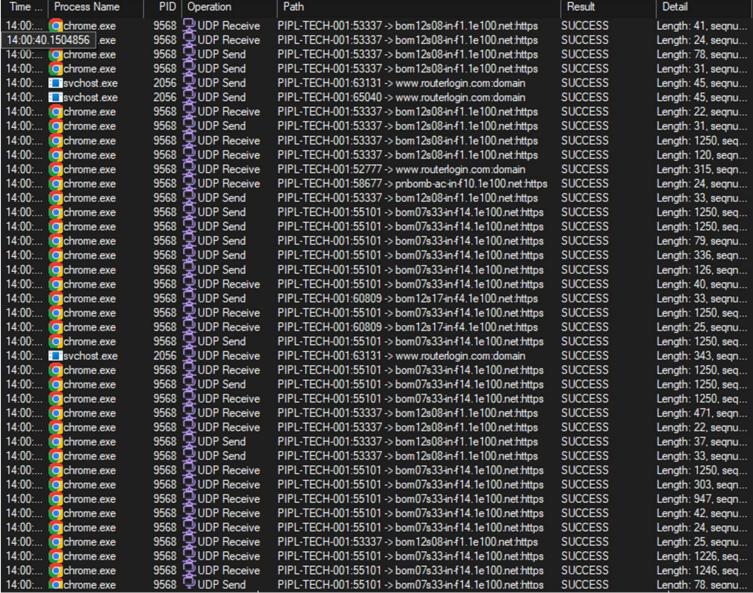


1. **Display network, registry, file system, process and thread activity separately**

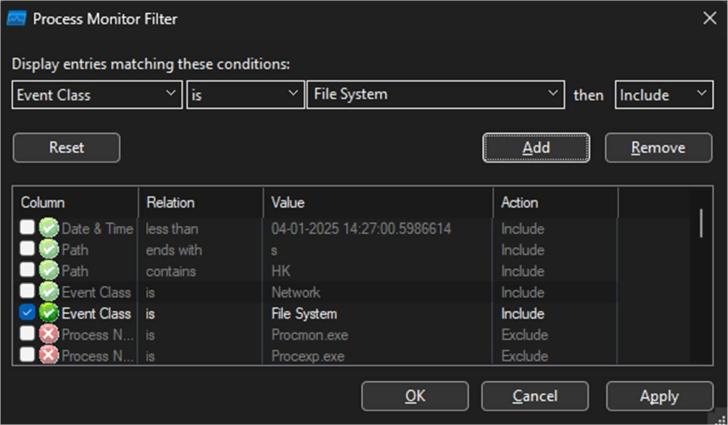
An **Event Class** refers to the **category** or **type of system activity** being logged.

* 1. **Network** - The **Network** event class in **Procmon** captures events related to network activity on the system



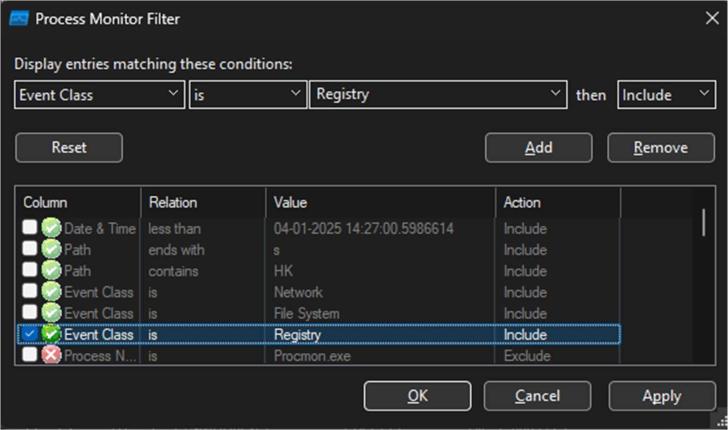


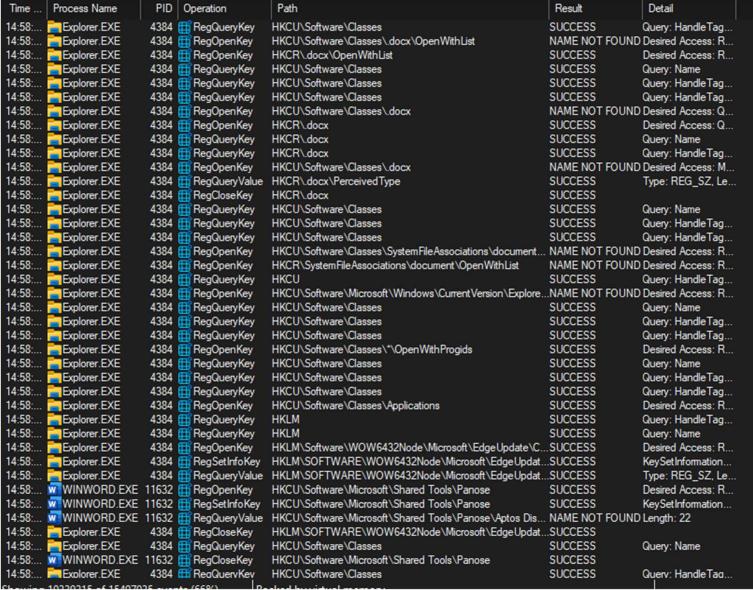
* 1. **File System**





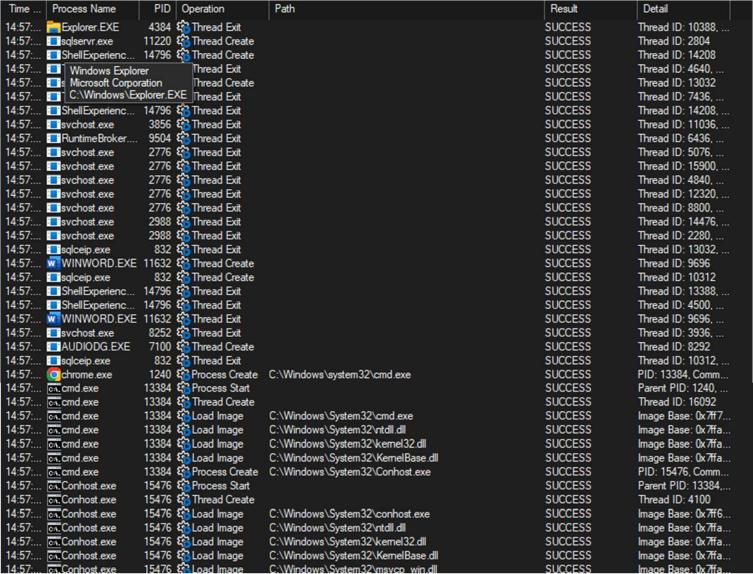
* 1. **Registry**

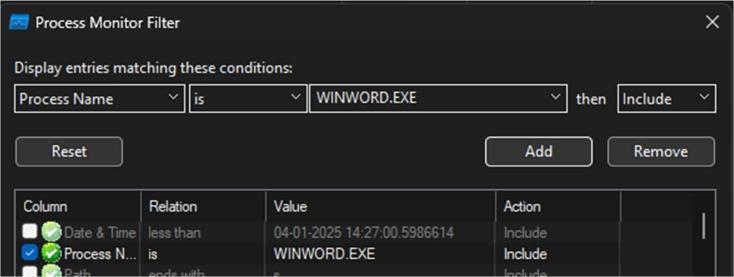


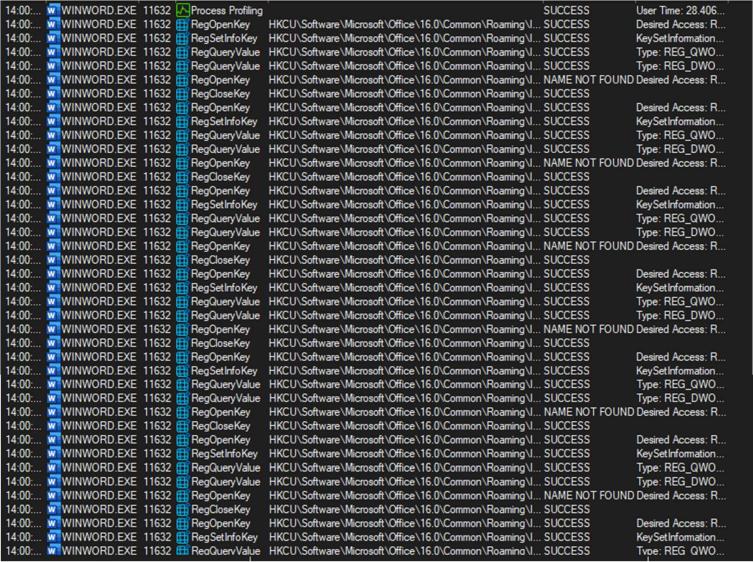


* 1. **Process**

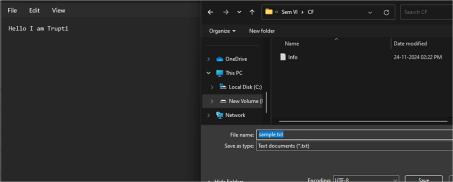




1. **Filter by process name**



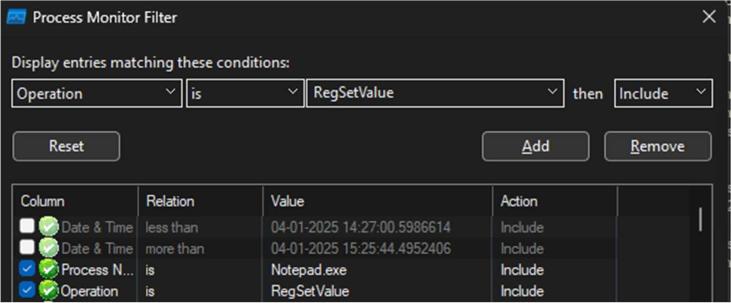
**Monitoring Notepad.exe process**



*Create a file & write some text and save the file*



*Change the font*

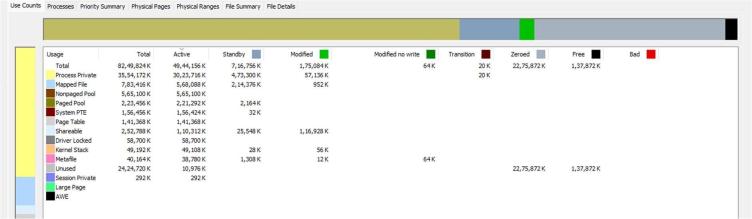


# **RAMMap**

## **Description**

**RAMMap** is a tool that helps forensic investigators analyze how a computer’s physical memory (RAM) is being used. It shows what files, processes, and system components are loaded into memory.

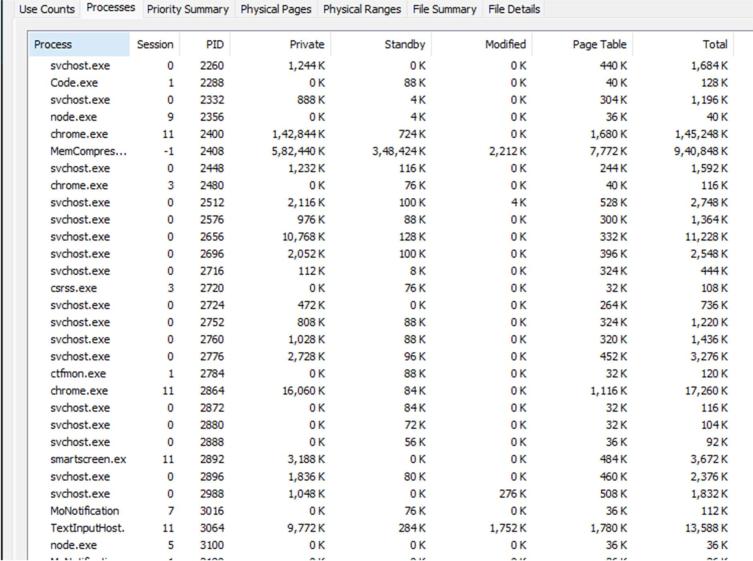
1. **Use Counts -** Shows how your computer’s memory is divided.



Active memory: What’s being used right now. Standby memory: Ready to use if needed (cached). Modified memory: Changed but not saved to disk yet. Free memory: Not being used at all.

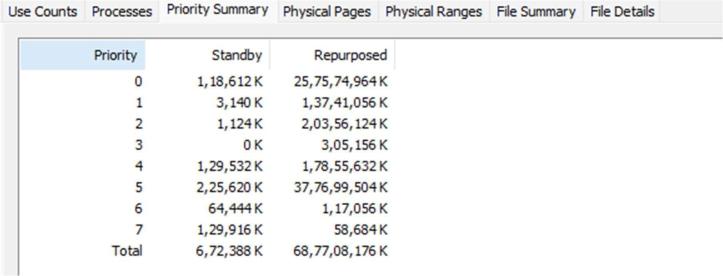
Why it’s useful: Helps you see how much memory is free, used, or ready for immediate use.

## **Processes**



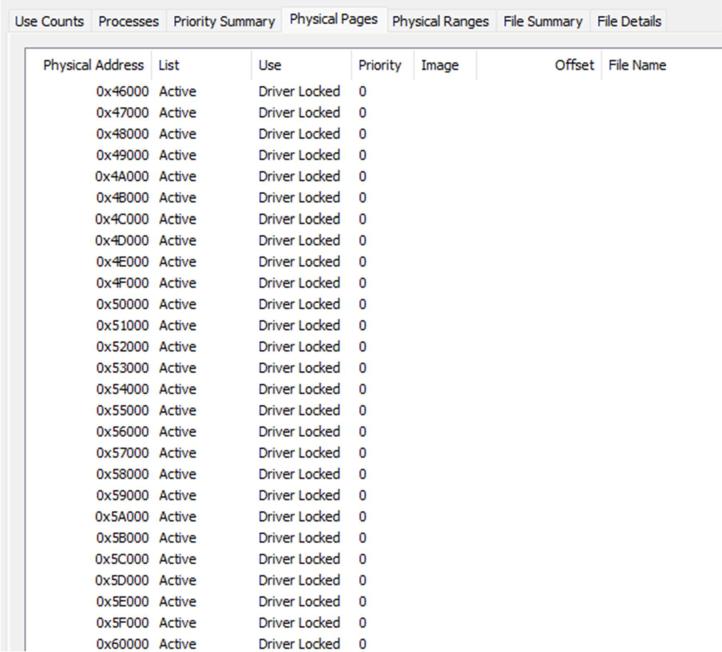
* + **What it does**: Lists all the programs and processes running on your computer and shows how much memory each one uses.
  + **Why it’s useful**: Helps you find programs that are using too much memory or behaving abnormally.

## **Priority Summary**



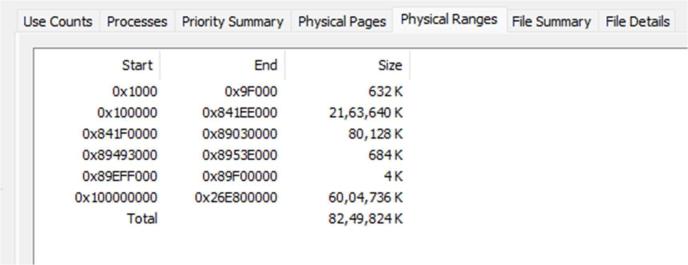
* + **What it does**: Shows how the system decides which data to keep in memory (important vs. less important).
  + **Why it’s useful**: Lets you see if critical processes are prioritized properly or if low-priority ones are hogging memory.

## **Physical Pages**



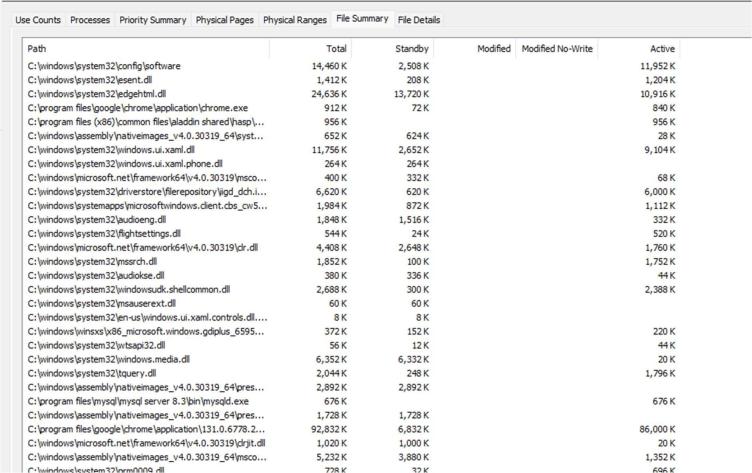
* + **What it does**: Displays the actual memory blocks (pages) in your computer and what each one is used for.
  + **Why it’s useful**: For deep troubleshooting when you need to analyze memory usage at the hardware level.

## **Physical Ranges**



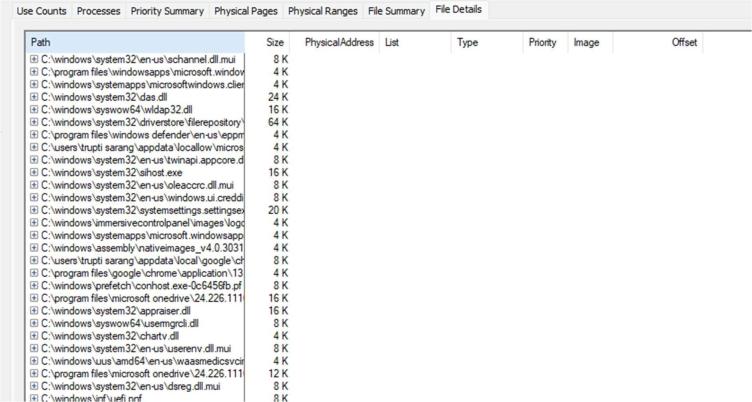
* + **What it does**: Shows the memory usage based on physical memory addresses (like sections of a bookshelf).
  + **Why it’s useful**: Helps analyze how memory is physically divided on your computer.

## **File Summary**



* + **What it does**: Lists all the files stored in memory (e.g., files you opened or cached files).
  + **Why it’s useful**: Helps forensic investigators find files loaded into memory, even if they aren’t saved to the disk.

## **File Details**



* + **What it does**: Provides a super-detailed view of memory usage for each file, like the exact parts of memory a file is using.
  + **Why it’s useful**: Tracks suspicious or specific files in memory, especially in forensic cases.

# **TCPView**

## **Description**

TCPView is designed to provide real-time information about the TCP and UDP activity on a Windows system. With TCPView, users can monitor and analyze the network connections established by various processes running on their computer.

**TCPView** is a useful tool in forensic investigations, especially for tracking network activity and identifying suspicious or malicious connections. It provides real-time monitoring of TCP and UDP connections, showing details such as local and remote addresses, ports, and associated processes. Key ways it supports forensic investigations include:

Green means “just opened,” yellow “ready to open,” red “ready to close,” and blue represents a user-selected entry.



* + - **Indicates "ESTABLISHED" connections**: A green line highlights a connection that is **established** and actively transmitting data between the local and remote systems.
    - **Meaning**: When you see a green line, it means the TCP handshake was successful, and the connection is open and operational, with data flowing between the two systems. This is the normal state for a working network connection.

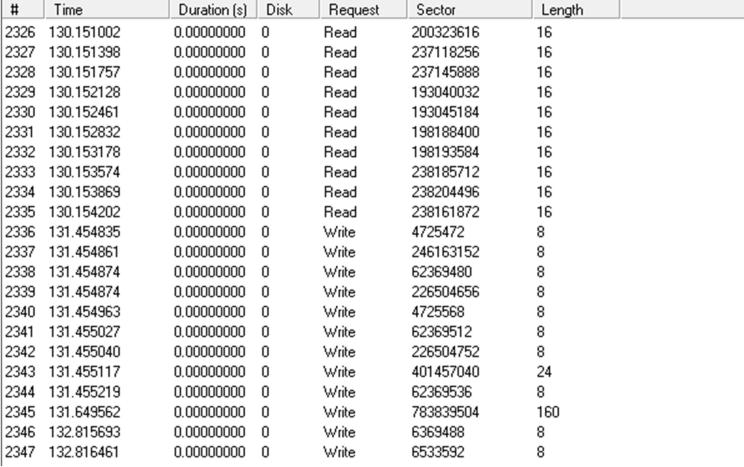
## **Yellow Line:**



* + - **Indicates "LISTENING" connections**: A yellow line typically represents a connection that is in the **LISTENING** state, meaning the local system is waiting for incoming connections on a specific port.
    - **Meaning**: This state is common for servers or applications that are waiting for connections from clients. The yellow line draws attention to ports that are open and ready to accept new incoming connections.

# **DiskMon**

**DiskMon** is a monitoring tool from Sysinternals (now part of Microsoft) that provides real-time monitoring of disk activity on a system. It helps track all disk input/output (I/O) operations and displays detailed information about every read and write request made to the disk.



**Time**: The timestamp when the disk operation occurred.

**Duration (s)**: The time taken for the disk operation. **Disk**: Which disk was accessed (e.g., Disk 0, Disk 1, etc.). **Request**: The type of I/O operation (Read/Write).

**Sector**: The disk sector being accessed (which may correlate to file locations).

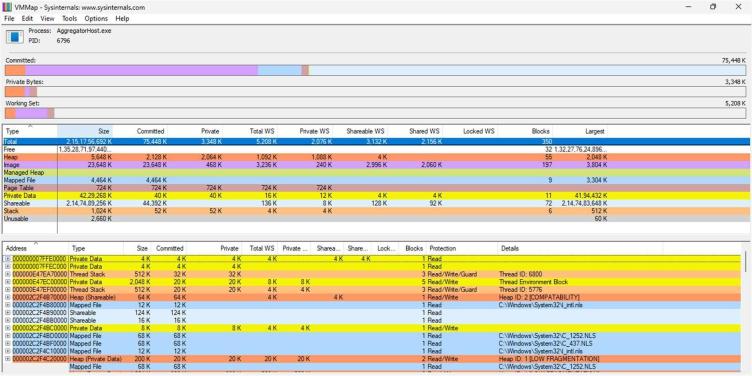
**Length**: The number of bytes involved in the read or write operation.

# **VMMap**

## **Description & formula**

VMMap is a process virtual and physical memory analysis utility. It shows a breakdown of a process's committed virtual memory types as well as the amount of physical memory (working set) assigned by the operating system to those types.

**VMMap** provides a detailed map of how a program is using memory, including which data is currently in **RAM** and which is in **virtual memory (disk)**.



**Committed memory** is the amount of memory that the OS has set aside for the program to use, either in RAM or on the paging file (disk). This memory is guaranteed to be available for the program, but it doesn't necessarily have to be physically in RAM; if needed, it could be moved to virtual memory (on disk).

# **6.Cacheset tool**

The **System File Cache** is a mechanism in operating systems (such as Windows) that temporarily stores data from disk files in memory (RAM). Its purpose is to improve system performance by reducing the time it takes to access frequently used files and data.

The **System File Cache** does not have a specific physical location on disk; instead, it resides in the system's **RAM (Random Access Memory)**. It is a portion of memory dynamically allocated by the operating system to temporarily store recently accessed file data, including file contents and metadata.

