**Practical No 6.**

**Using Sysinternals tools for Network Tracking and Process Monitoring**

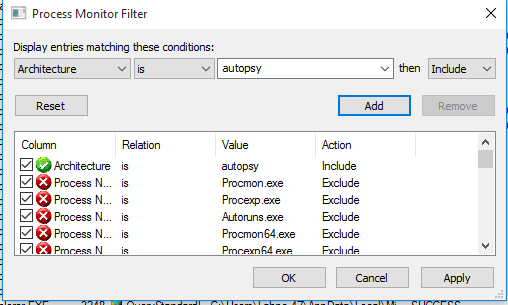
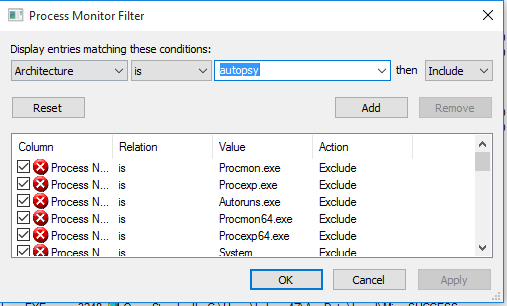
**1. Check Sysinternals tools**

Google🡪sysinternal tools

**2. Monitor Live Processes**

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.

Go to Process monitor 🡪 download 🡪 Open 🡪 Filter 🡪 any process name (autopsy)



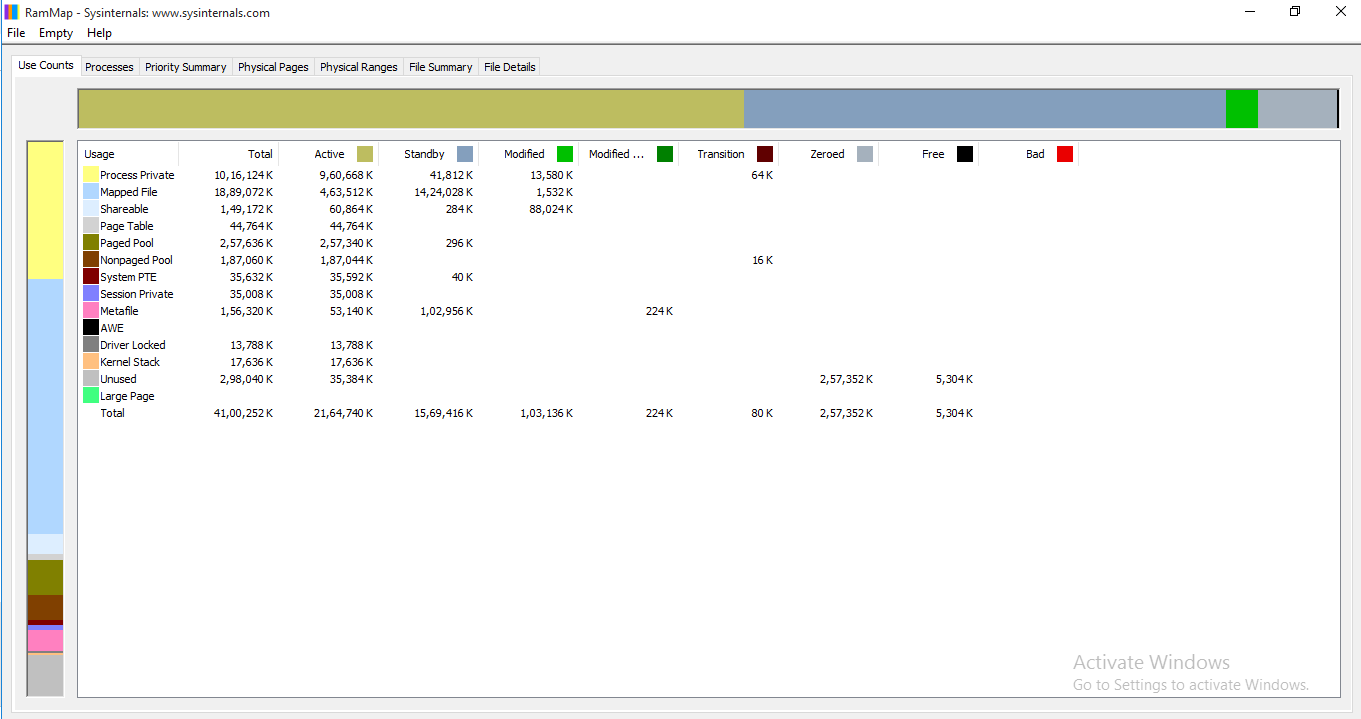
**3. Capture RAM**

RAMMap is an advanced physical memory usage analysis utility for Windows Vista and higher. It presents usage information in different ways on its several different tabs:

* *Use Counts:* usage summary by type and paging list
* *Processes:* process working set sizes
* *Priority Summary:* prioritized standby list sizes
* *Physical Pages:* per-page use for all physical memory
* *Physical Ranges:* physical memory addresses
* *File Summary:* file data in RAM by file
* *File Details:* individual physical pages by file

Use RAMMap to gain understanding of the way Windows manages memory, to analyze application memory usage, or to answer specific questions about how RAM is being allocated. RAMMap’s refresh feature enables you to update the display and it includes support for saving and loading memory snapshots.

**STEPS** Download 🡪 RAMMap



**4.Capture TCP/UDP packets**

TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. On Windows Server 2008, Vista, and XP, TCPView also reports the name of the process that owns the endpoint. TCPView provides a more informative and conveniently presented subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality.

**Using TCPView**

When you start TCPView it will enumerate all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions. You can use a toolbar button or menu item to toggle the display of resolved names. On Windows XP systems, TCPView shows the name of the process that owns each endpoint.By default, TCPView updates every second, but you can use the **Options|Refresh Rate** menu item to change the rate. Endpoints that change state from one update to the next are highlighted in yellow; those that are deleted are shown in red, and new endpoints are shown in green.You can close established TCP/IP connections (those labeled with a state of ESTABLISHED) by selecting **File|Close Connections**, or by right-clicking on a connection and choosing **Close Connections** from the resulting context menu.You can save TCPView's output window to a file using the **Save** menu item.

**Using Tcpvcon**

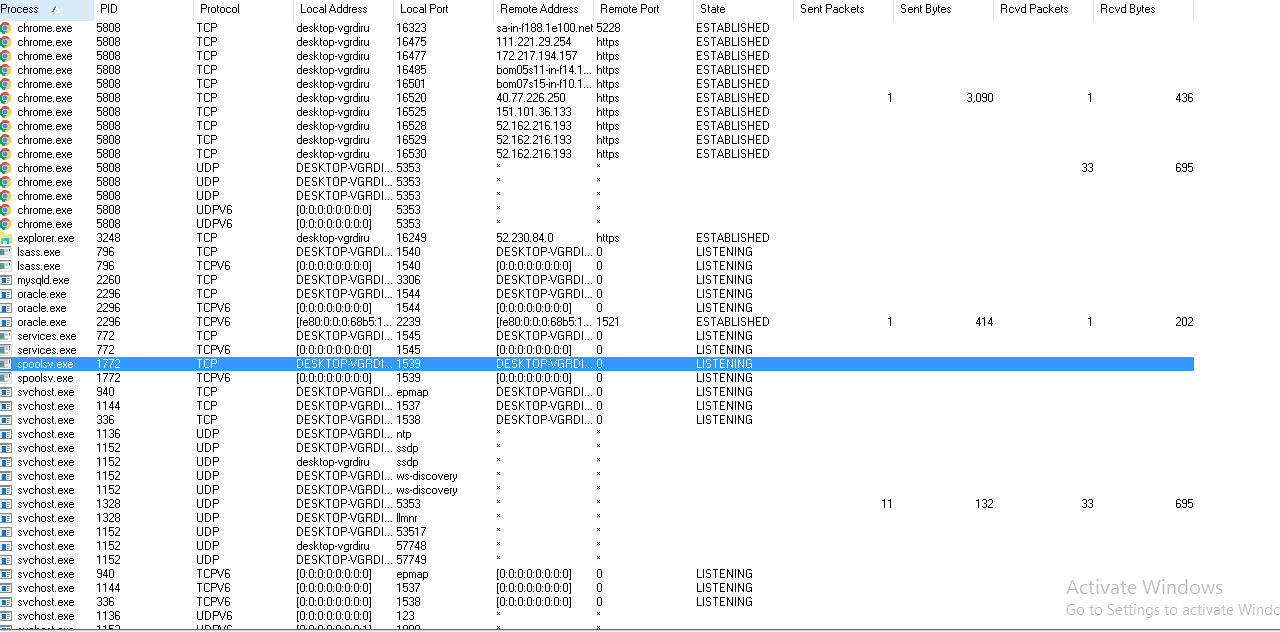
Tcpvcon usage is similar to that of the built-in Windows netstat utility:

**Usage: tcpvcon [-a] [-c] [-n] [process name or PID]**

| **Parameter** | **Description** |
| --- | --- |
| **-a** | Show all endpoints (default is to show established TCP connections). |
| **-c** | Print output as CSV. |
| **-n** | Don't resolve addresses. |

**STEPS**

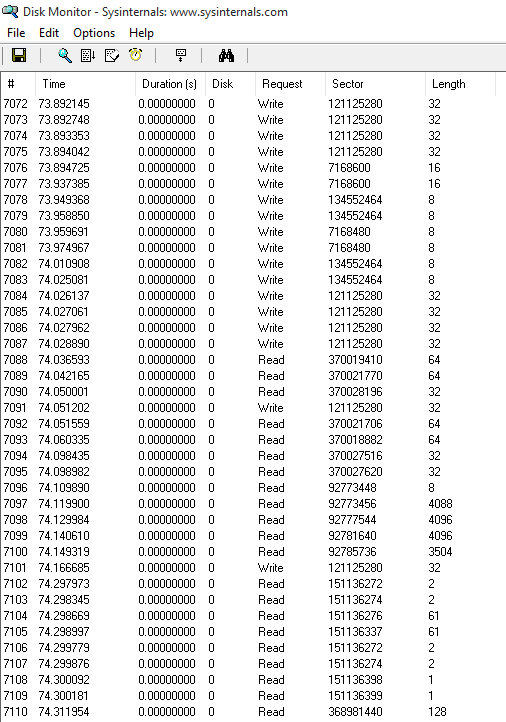
Download TCPView



**5. Monitor Hard Disk**

DiskMon is an application that logs and displays all hard disk activity on a Windows system. You can also minimize DiskMon to your system tray where it acts as a disk light, presenting a green icon when there is disk-read activity and a red icon when there is disk-write activity.

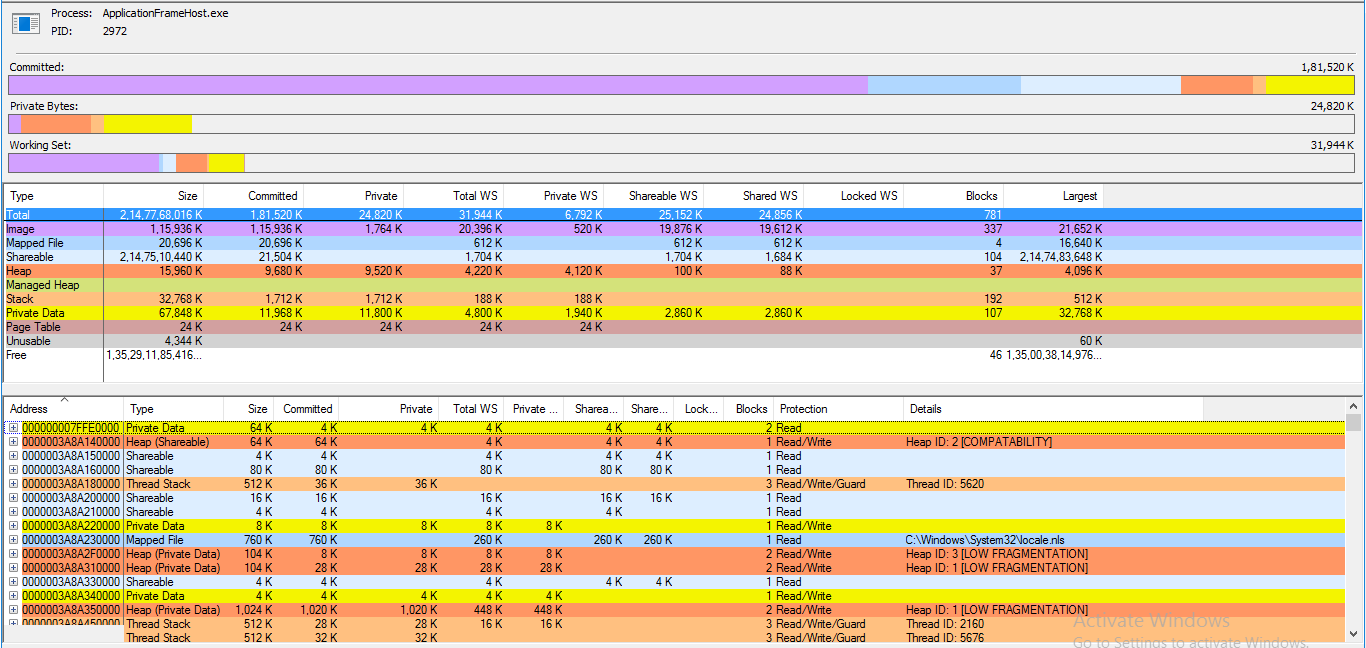
Download DiskMon 🡪 Run as administrator



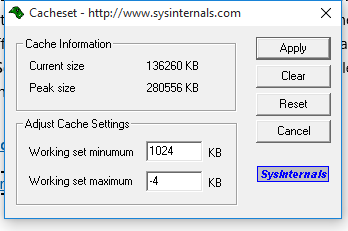
**6.Monitor Virtual Memory**

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. Besides graphical representations of memory usage, VMMap also shows summary information and a detailed process memory map. Powerful filtering and refresh capabilities allow you to identify the sources of process memory usage and the memory cost of application features

Download VMMap



**7.Monitor Cache Memory**

CacheSet is an applet that allows you to manipulate the working-set parameters of the system file cache. Unlike CacheMan, CacheSet runs on all versions of NT and will work without modifications on new Service Pack releases. In addition to providing you the ability to control the minimum and maximum working set sizes, it also allows you to reset the Cache's working set, forcing it to grow as necessary from a minimal starting point. Also unlike CacheMan, changes made with CacheSet have an immediate effect on the size of the Cache. ****