**Practical No 8**

**Aim:** Using Sysinternal tools for network tracking and process monitoring **Introduction –**

Check Sysinternals tools:

Windows Sysinternals tools are utilities to manage, diagnose, troubleshoot,

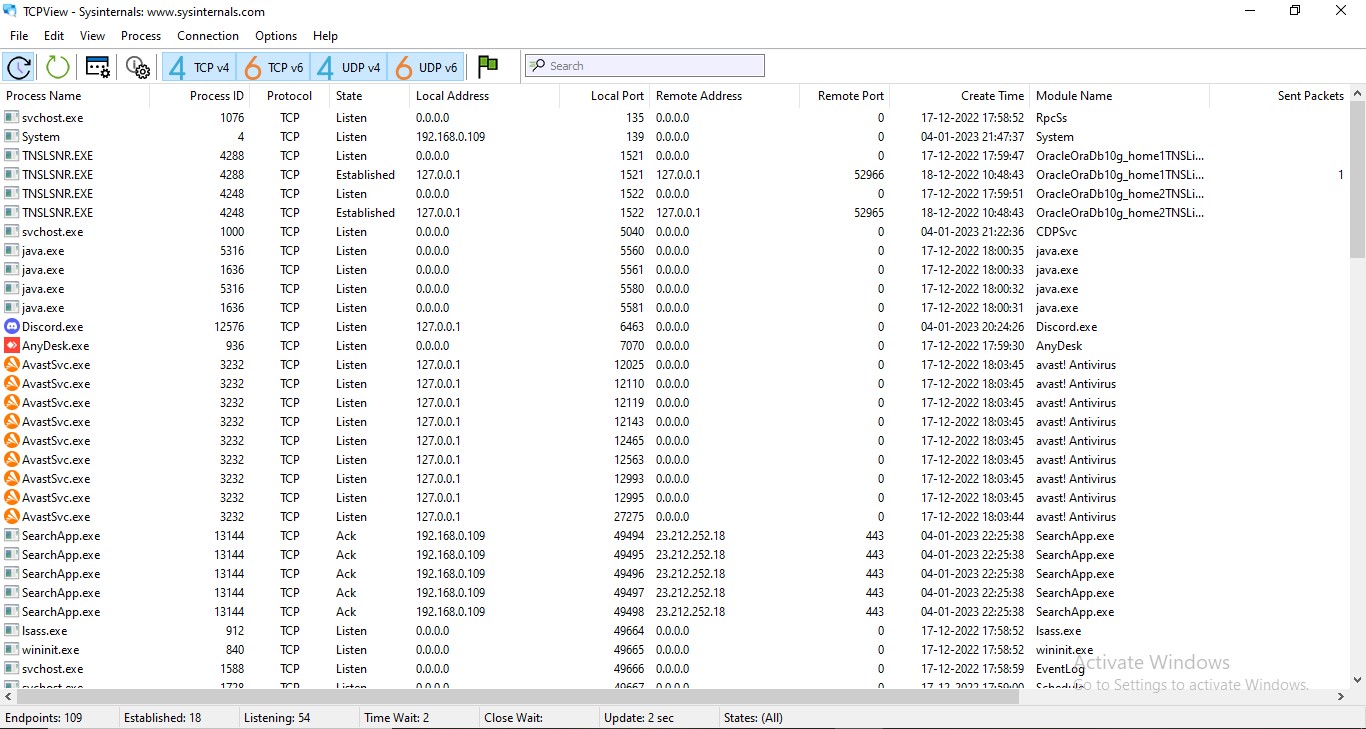
and monitor a

Microsoft Windows environment.

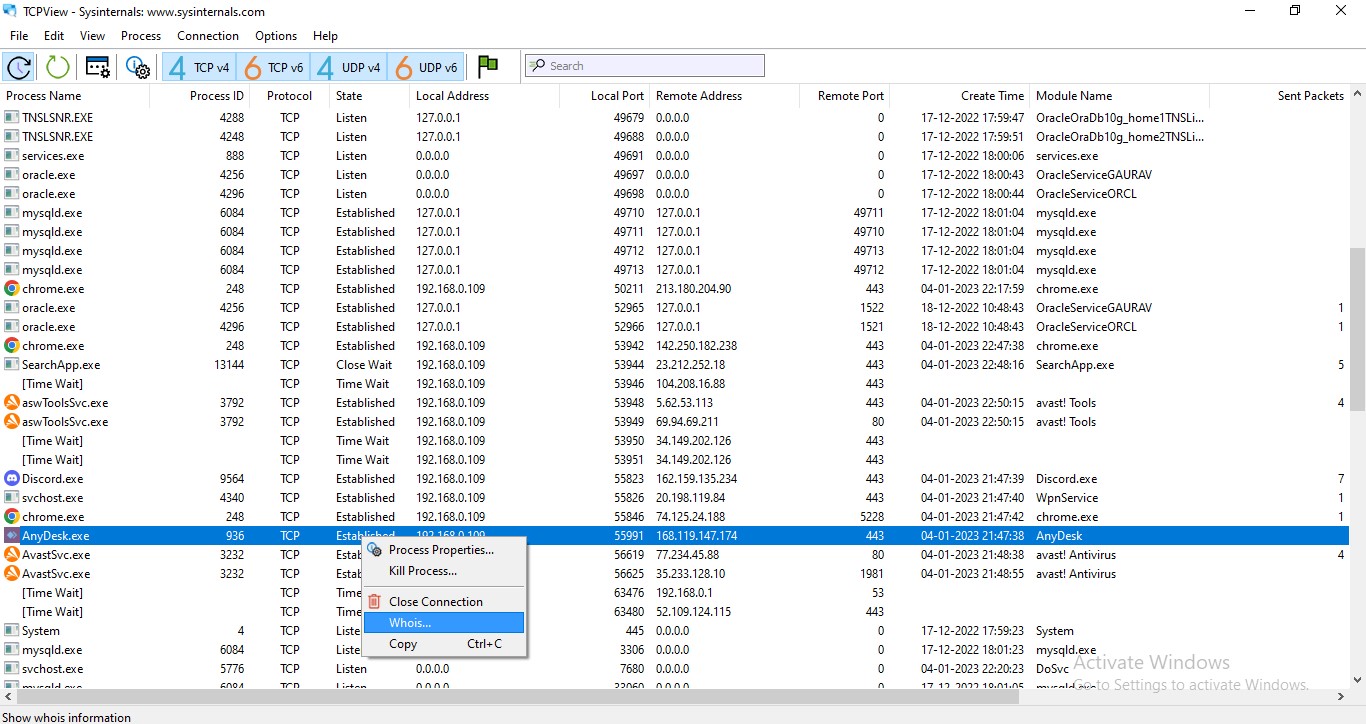
The following are the categories of Sysinternals Tools:

1. File and Disk Utilities
2. Networking Utilities
3. Process Utilities
4. Security Utilities
5. System Information Utilities
6. Miscellaneous Utilities
7. **Capture TCP/UDP packets (Tool: TcpView)**

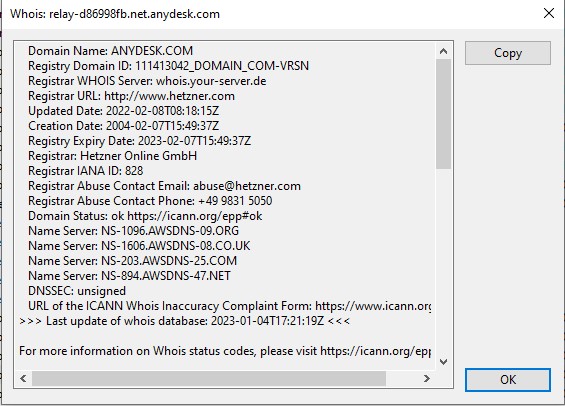
**Go to the SysinternalsSuite folder and double click on the TcpView.exe file. The following window appear on the screen.**



**Right click on any packet > Whois**

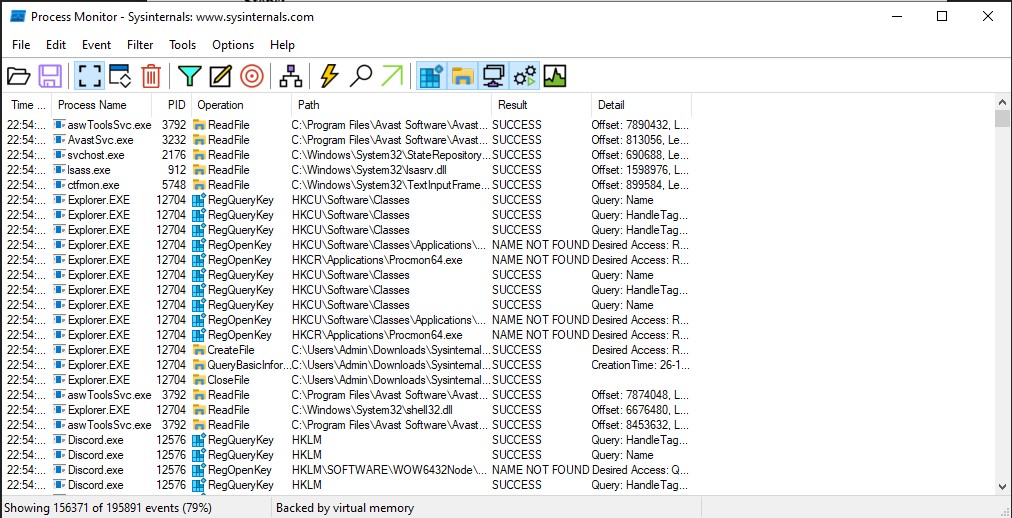


 **The following data is displayed:**

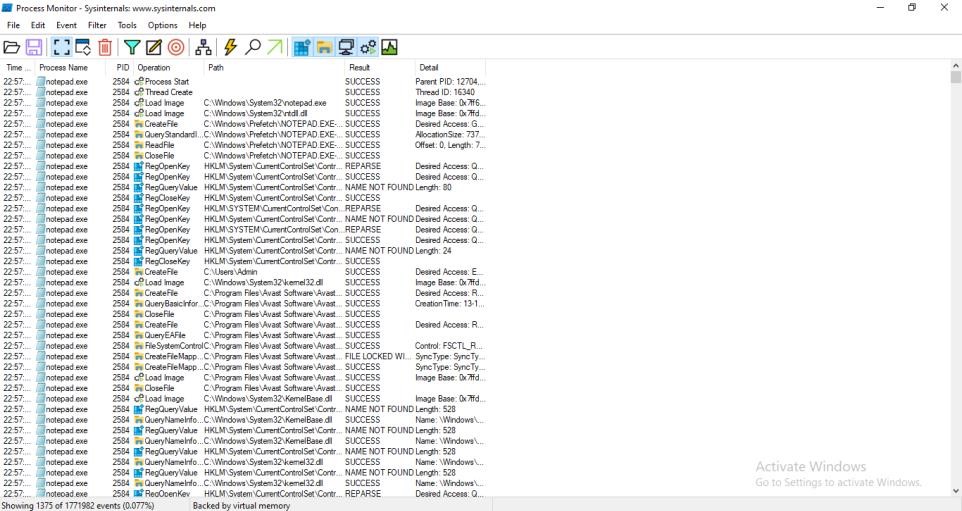
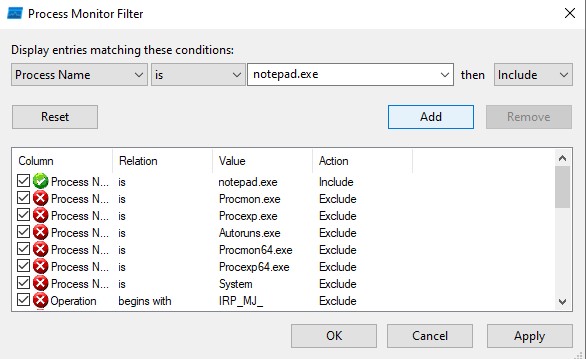


1. **Monitor Live Process (Tool: ProcMon)**

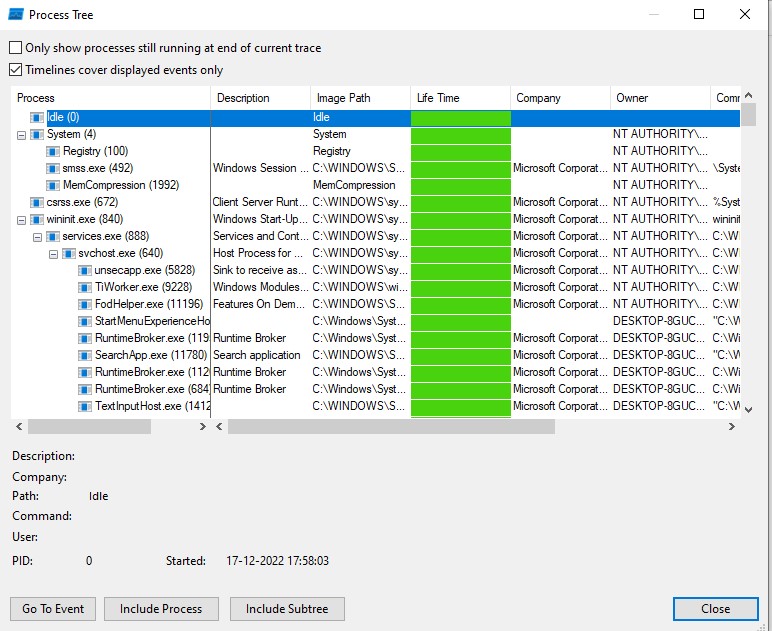
**a new window appears on your screen which displays all the ongoing processes of our system.**



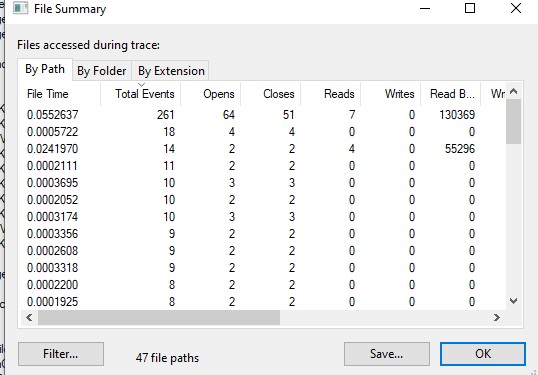
* **Click on filter > Process monitor filter**



**Click on tools > Process tree**

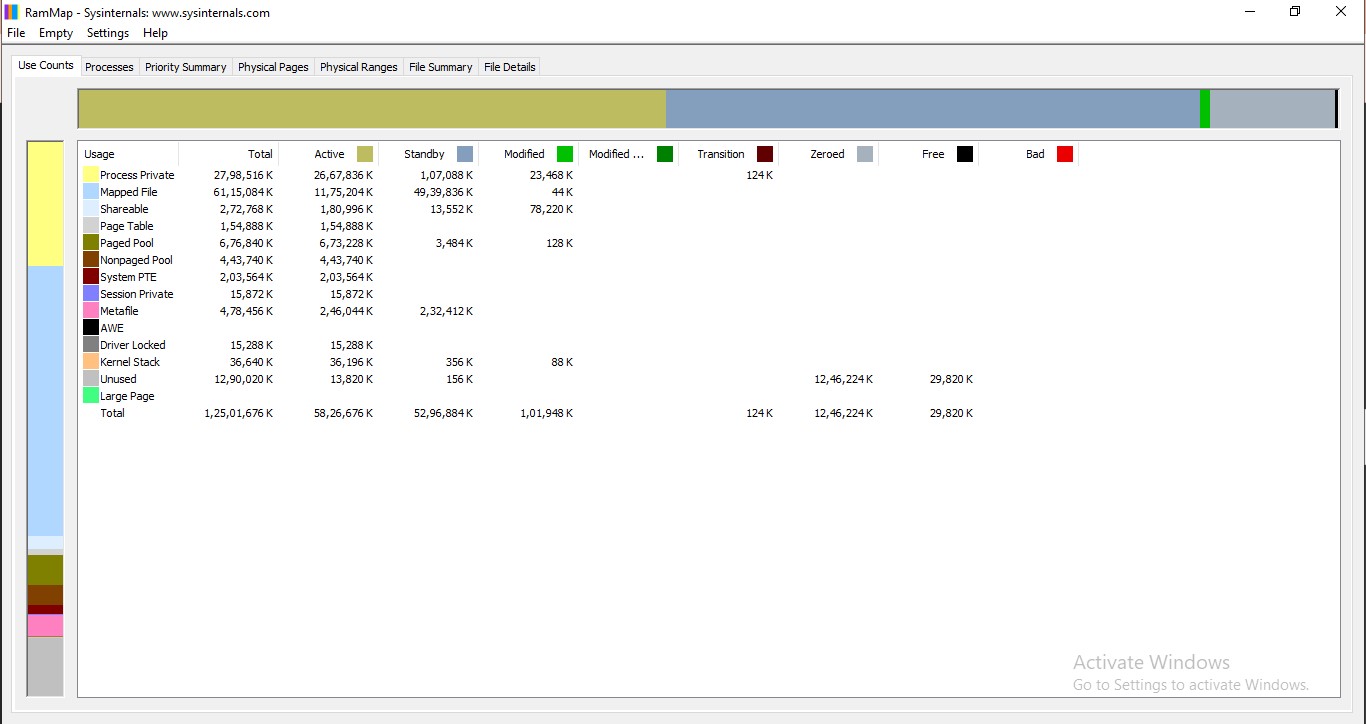


* **Click on tools > File summary**



1. **Monitor Cache Memory (Tool: RAMMap)**

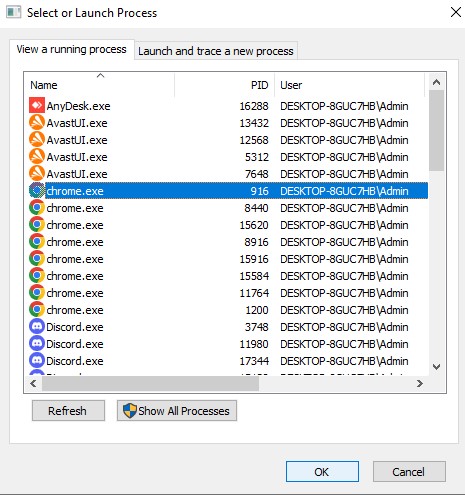
**Open the RAMMap tool. The following window will appear on the screen.**



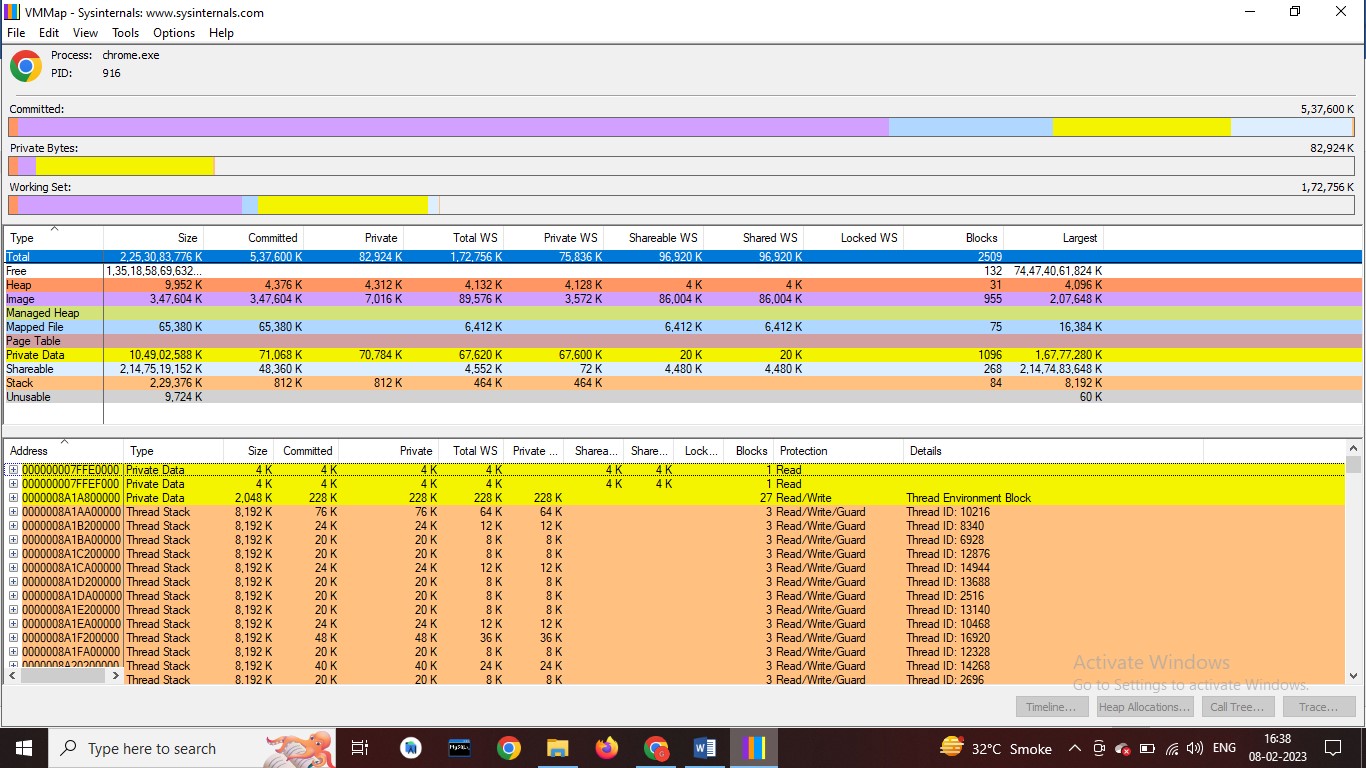
1. **Monitor Virtual Memory (Tool: VMMap)**

**Go to the SysinternalsSuite folder and double click on the VMMap.exe file.**

**The following window appears on the screen.**



**The following window displays the virtual memory accessed by the process selected by us.**



1. **Monitor Hard Disk (Tool: DiskMon)**

**1. Go to the SysinternalsSuite folder and double click on the DiskMon.exe file.(Note: While opening DiskMon.exe, you can’t open the .exe file on the same folder where you have saved the file. So, copy the file on any other local disk and then perform the steps mentioned above.)**

