

## Practical 6

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

- Check Sysinternals tools
- Monitor Live Processes
- Capture RAM
- Capture TCP/UDP packets
- Monitor Hard Disk
- Monitor Virtual Memory
- Monitor Cache Memory

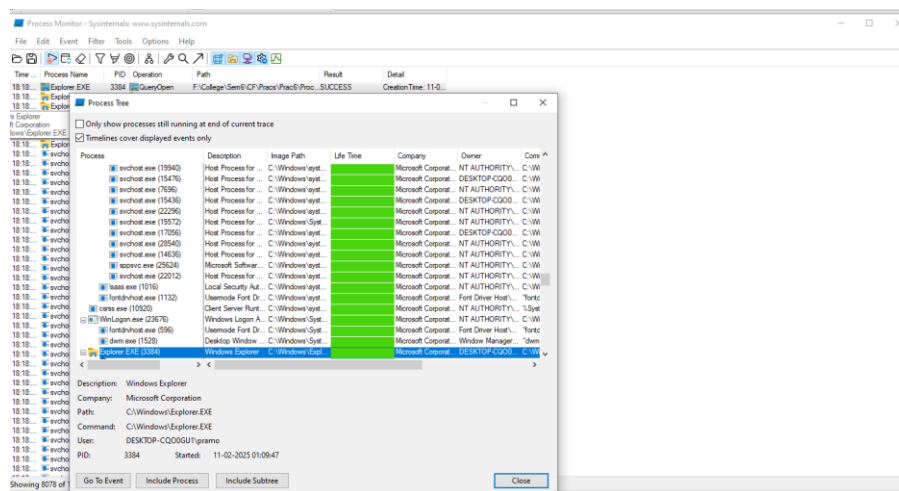
### 1. MONITOR LIVE PROCESSES (TOOL:-PROCMON)

**STEP 1:** Click on Filter -> Filter ☐ Process Monitor filter.

The screenshot shows the Process Monitor (Procmon) application window. The 'Filter' menu is open, and the 'Filter' option is selected. The 'Process Monitor Filter' dialog box is displayed, showing a list of filters. The 'Path' filter is selected, and the filter expression is 'msf\CP\Prac9\Prac9\Procmon.exe'. The 'Include' button is highlighted.

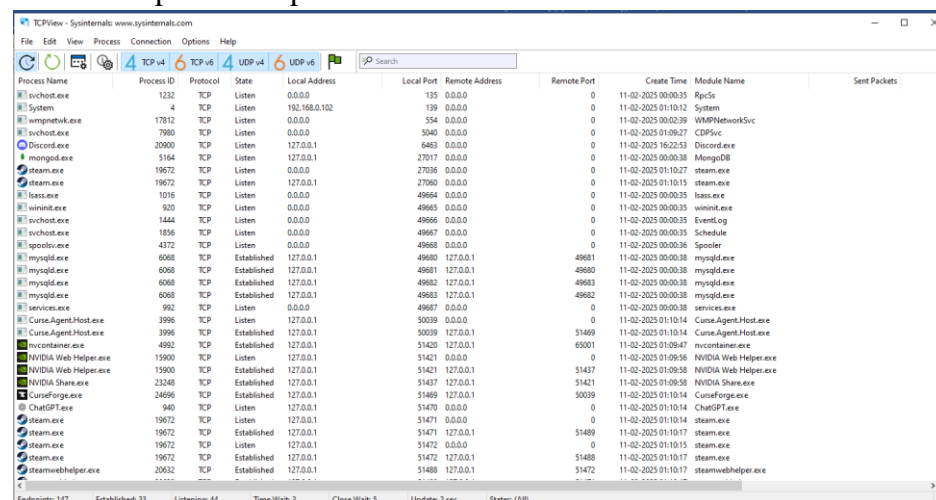
Column	Relation	Value	Action
<input checked="" type="checkbox"/> Path	is	F:\College\Sem6\CP\Prac9\Prac9\Procmon.exe	Include
<input checked="" type="checkbox"/> Process Name	is	Procmon.exe	Exclude
<input checked="" type="checkbox"/> Process Name	is	Process.exe	Exclude
<input checked="" type="checkbox"/> Process Name	is	Autounst.exe	Exclude
<input checked="" type="checkbox"/> Process Name	is	Procmon64.exe	Exclude
<input checked="" type="checkbox"/> Process Name	is	System	Exclude

**STEP 2:** Click On Tool ☐ Process Tree.

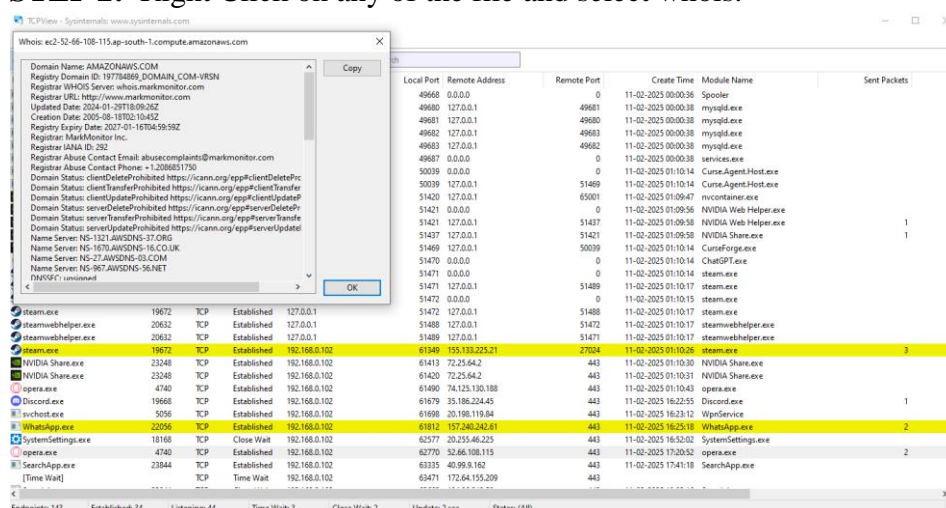


## 2. CAPTURE TCP/UDP PACKETS (TOOL:-Tcpcview):

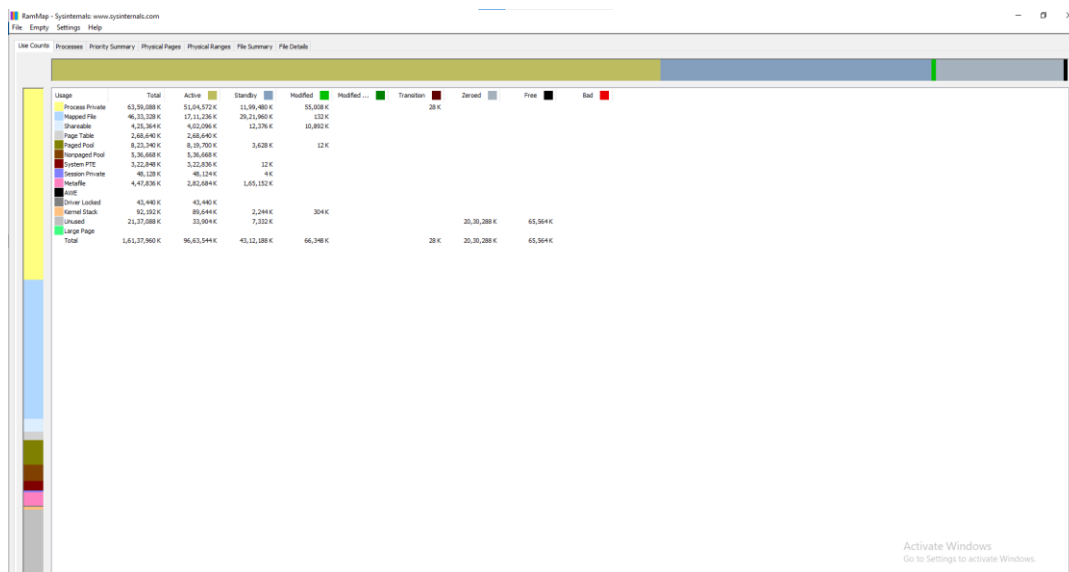
**STEP 1:** Open the Tcpcview tool.



**STEP 2:** Right Click on any of the file and select whois.

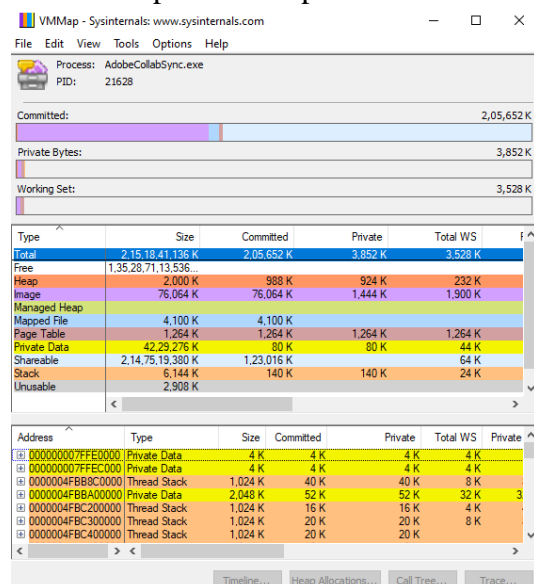


## 3. MONITOR HARD DISK (TOOL:-RAMMap) STEP 1: Open RAMMap tool.



#### 4. MONITOR VIRTUAL MEMORY (TOOL:-VMMMap):

##### STEP 1: Open VMMMap tool.



#### 5. MONITOR CACHE MEMORY (TOOL:-Cacheset):

##### STEP 1: Open Cacheset Tool.

