**Practical No: 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

**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

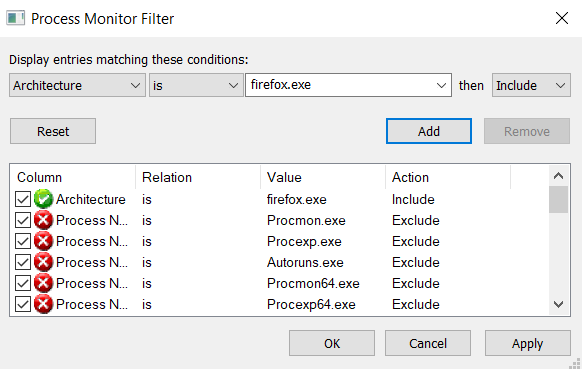
4. Security Utilities

5. System Information Utilities

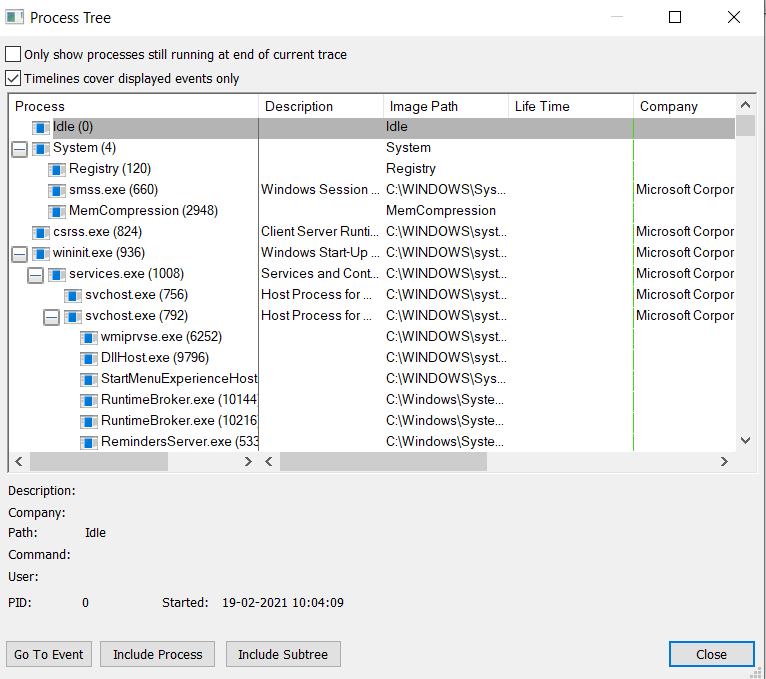
6. Miscellaneous Utilities

**Monitor Live Processes: (Tool: ProcMon)**

**Step1:** Click on Filter > Process Monitor filter.

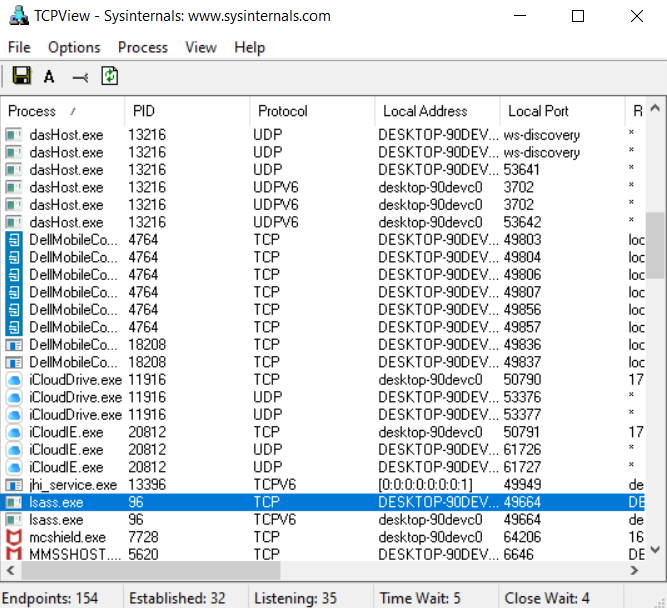


**Step2:** Click On Tool > Process Tree.

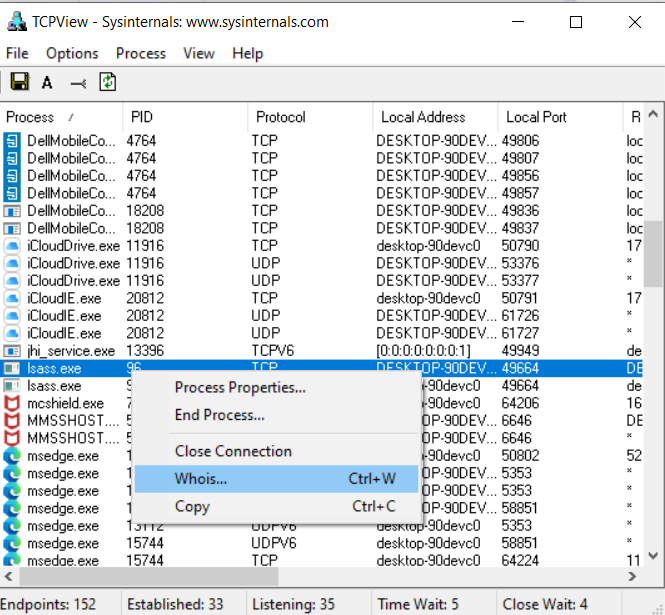


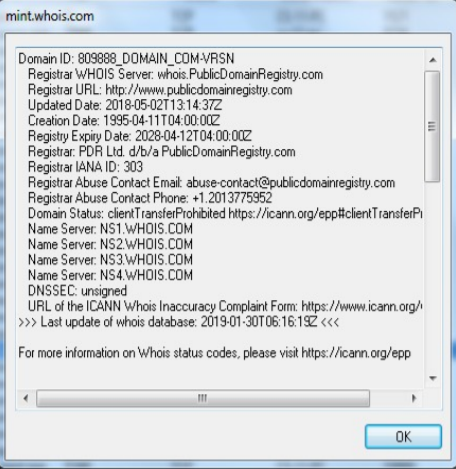
**Capture RAM - Capture TCP/UDP packets :**

**Step1:** Open the Tcpview tool.



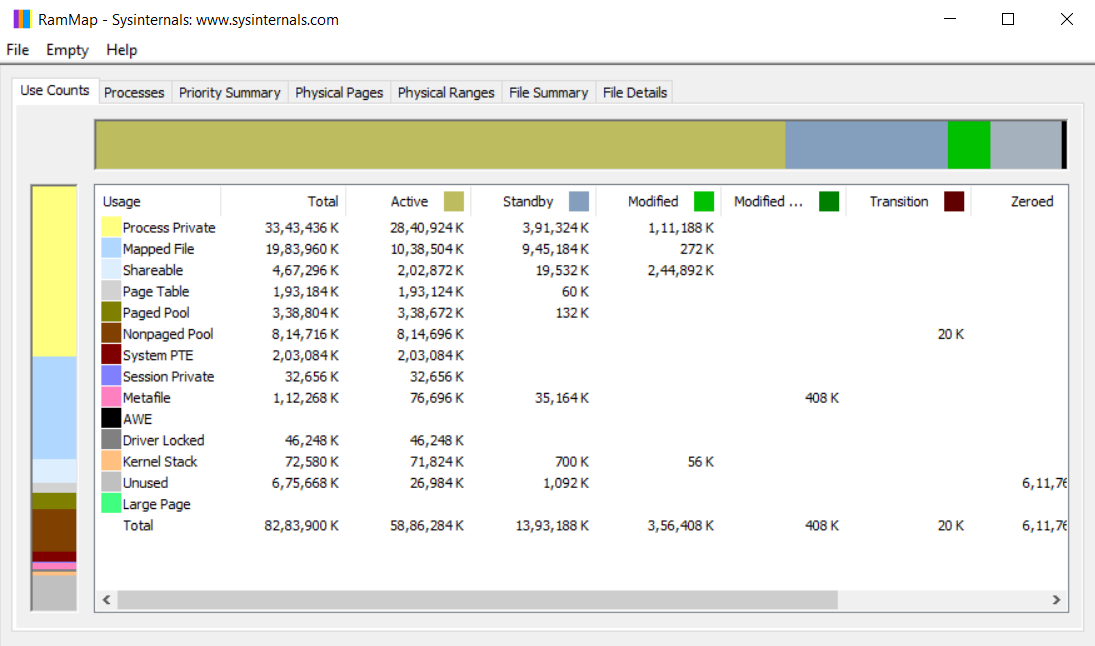
**Step2:** Right Click on any of the file and select whois.



****

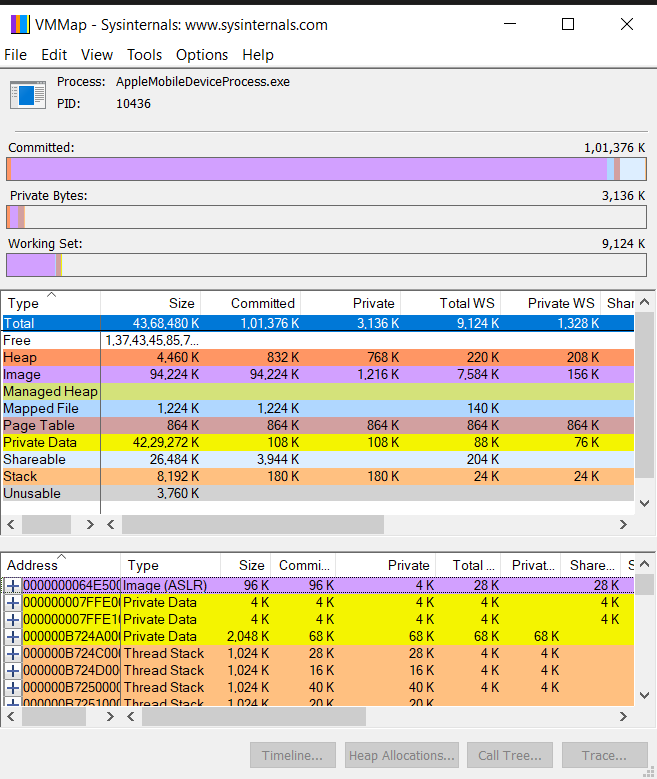
**Monitor Hard Disk**

**Step1:** Open RamMap tool.



**Monitor Virtual Memory**

**Step1:** Open VMMap tool.



**Monitor Cache Memory**

**Step1:** Open Cacheset Tool.

