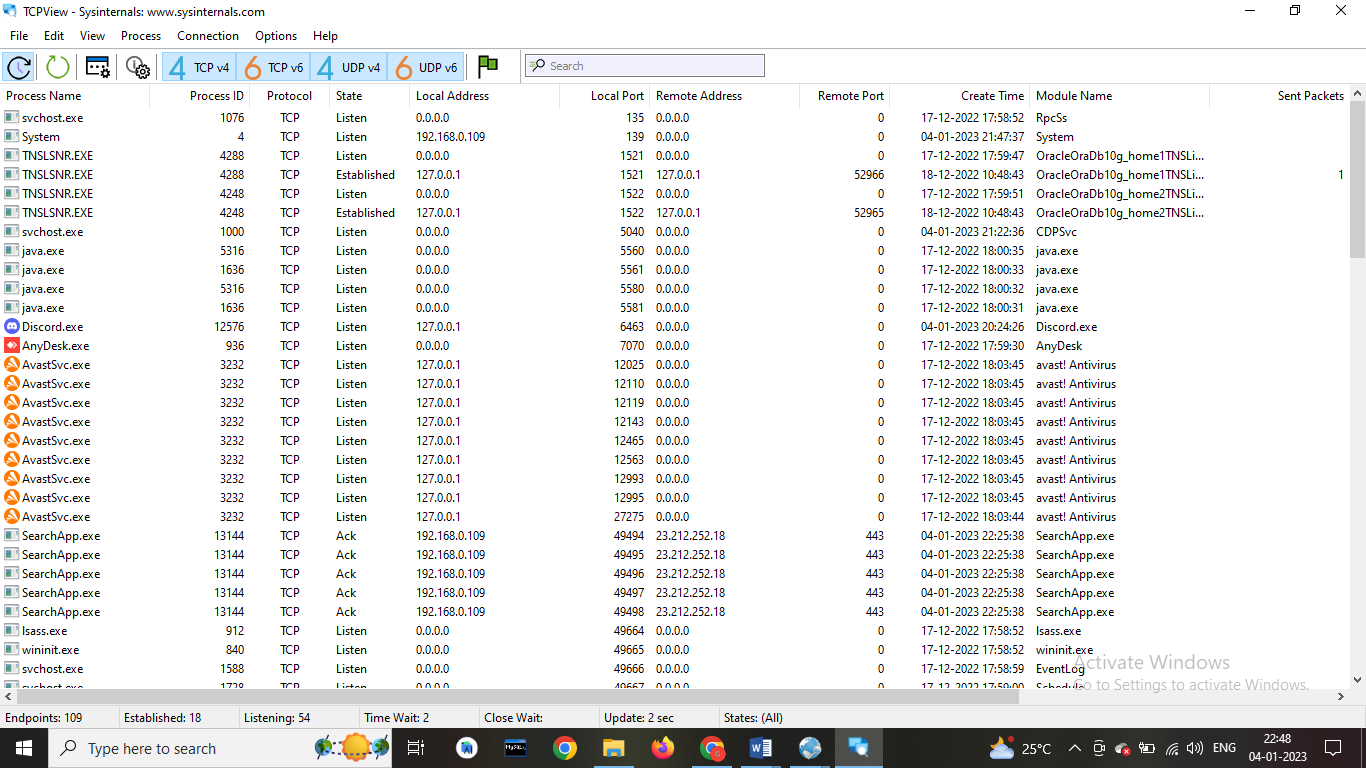
**Practical No 6**

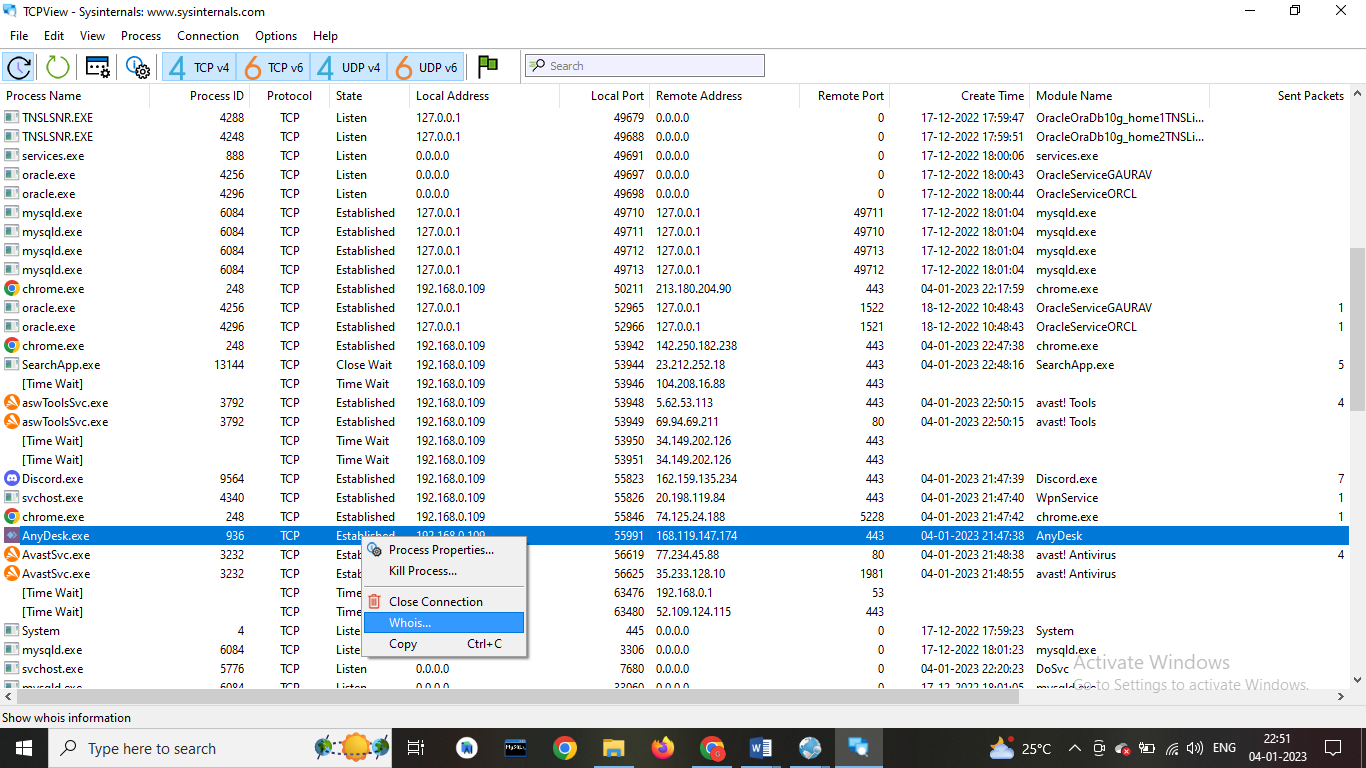
**Aim:**

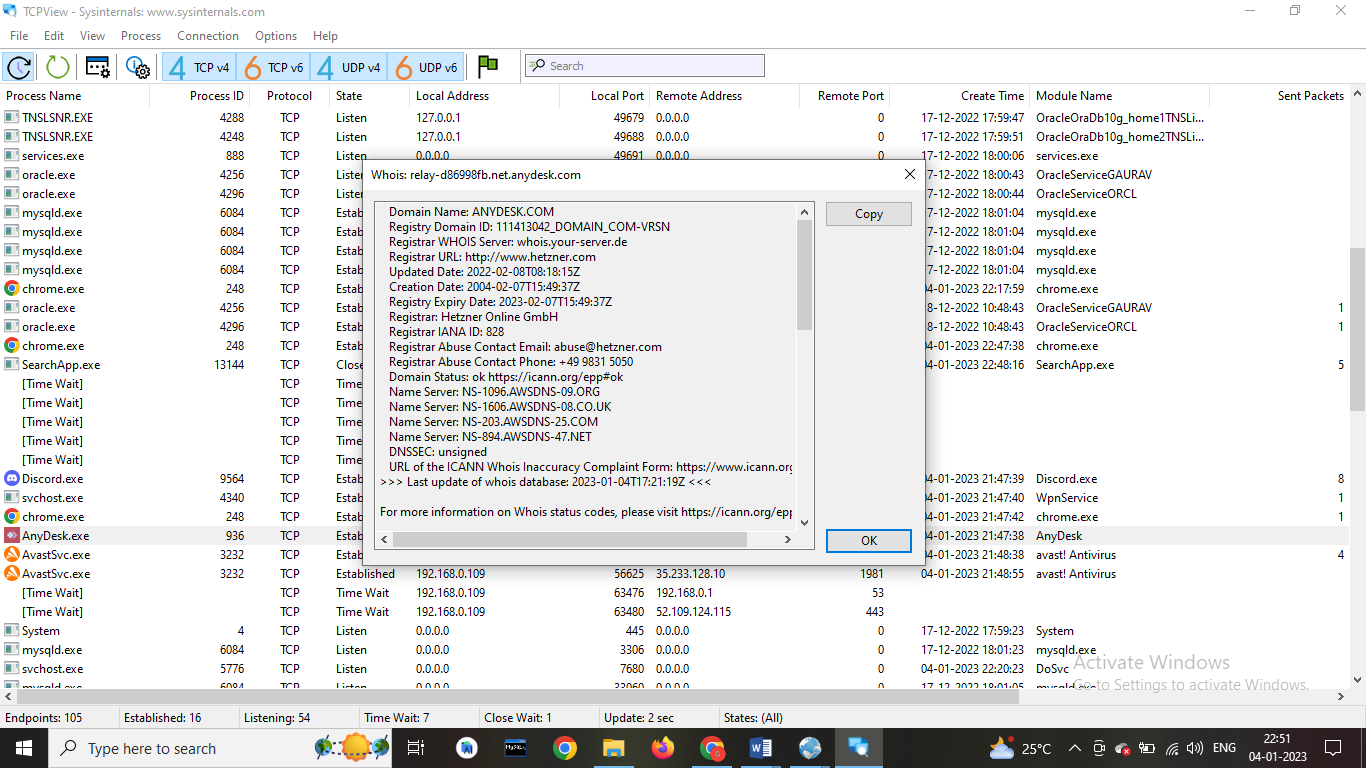
**1] Capture TCP/UDP packets (Tool: TcpView)**

* **Open the TCPView tool**

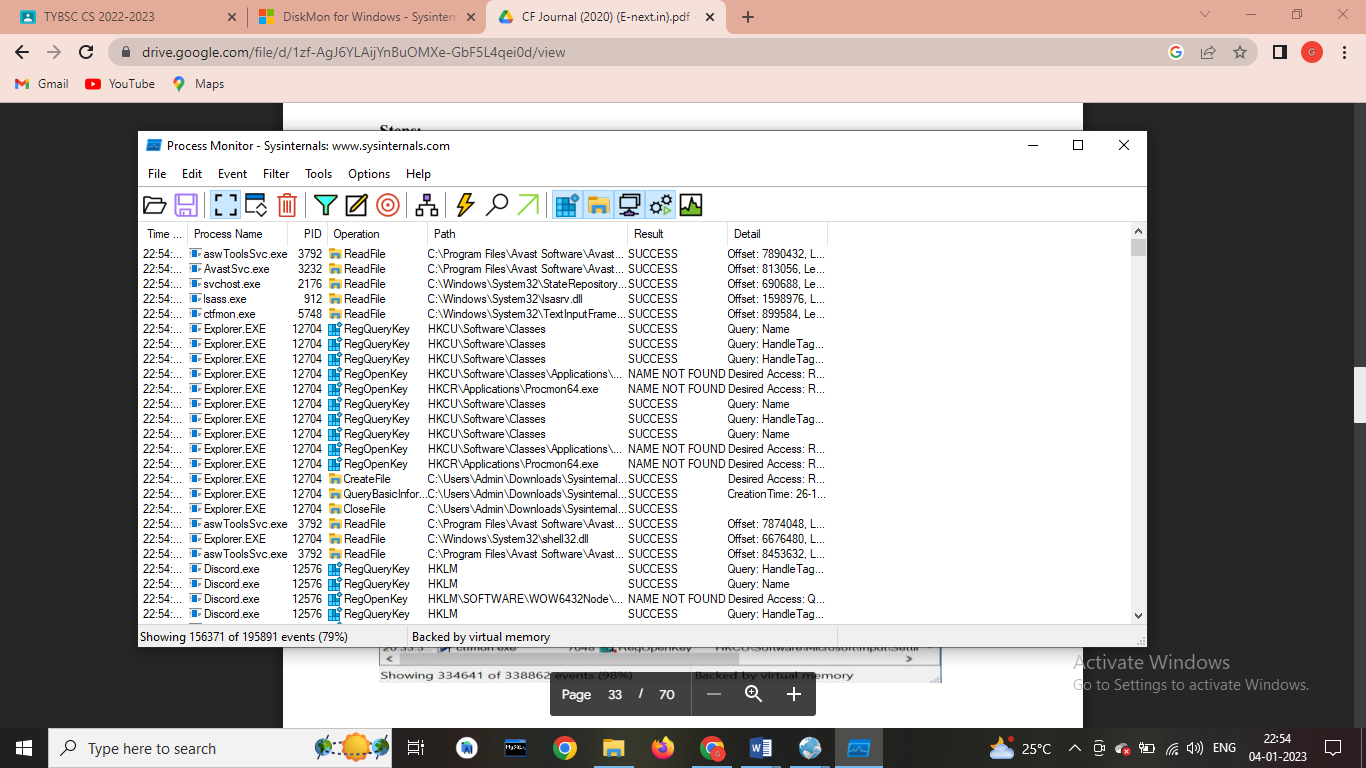


* **Right click on any packet > Whois**

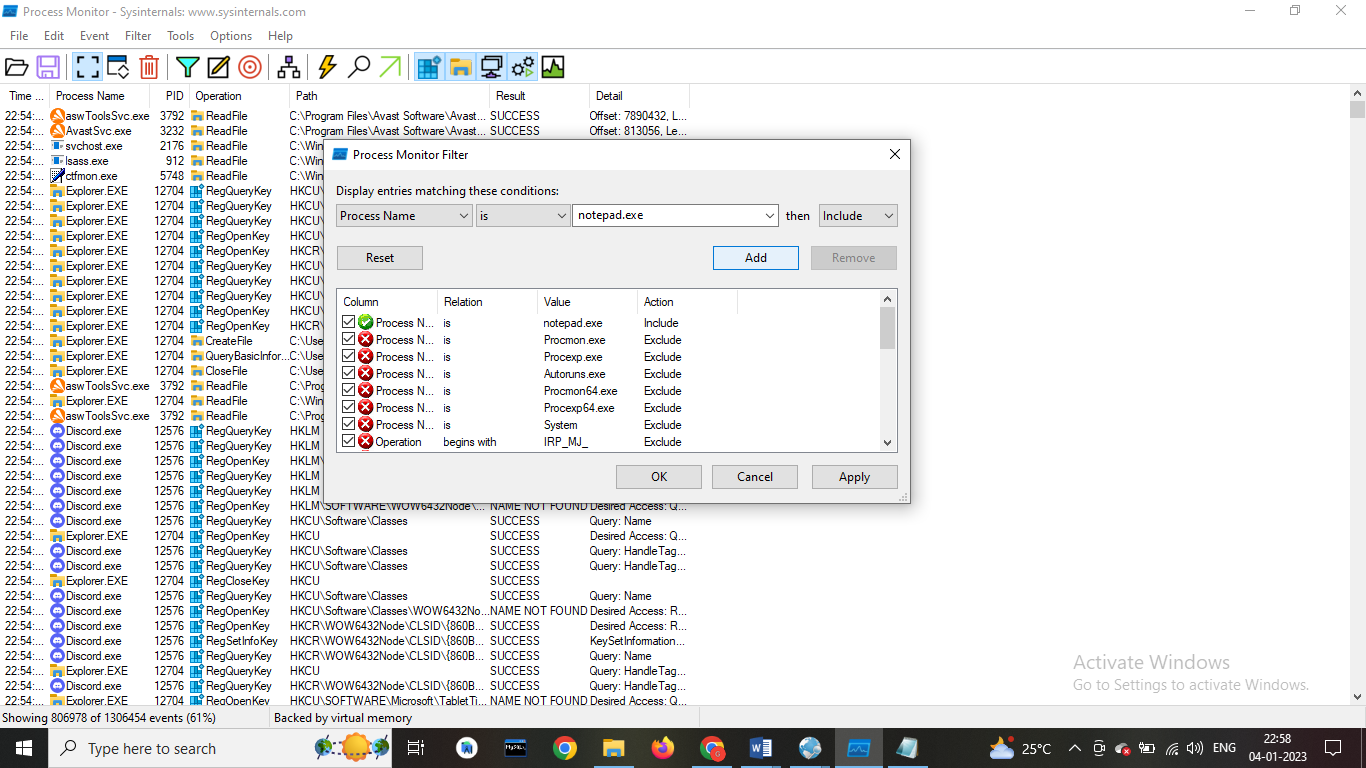


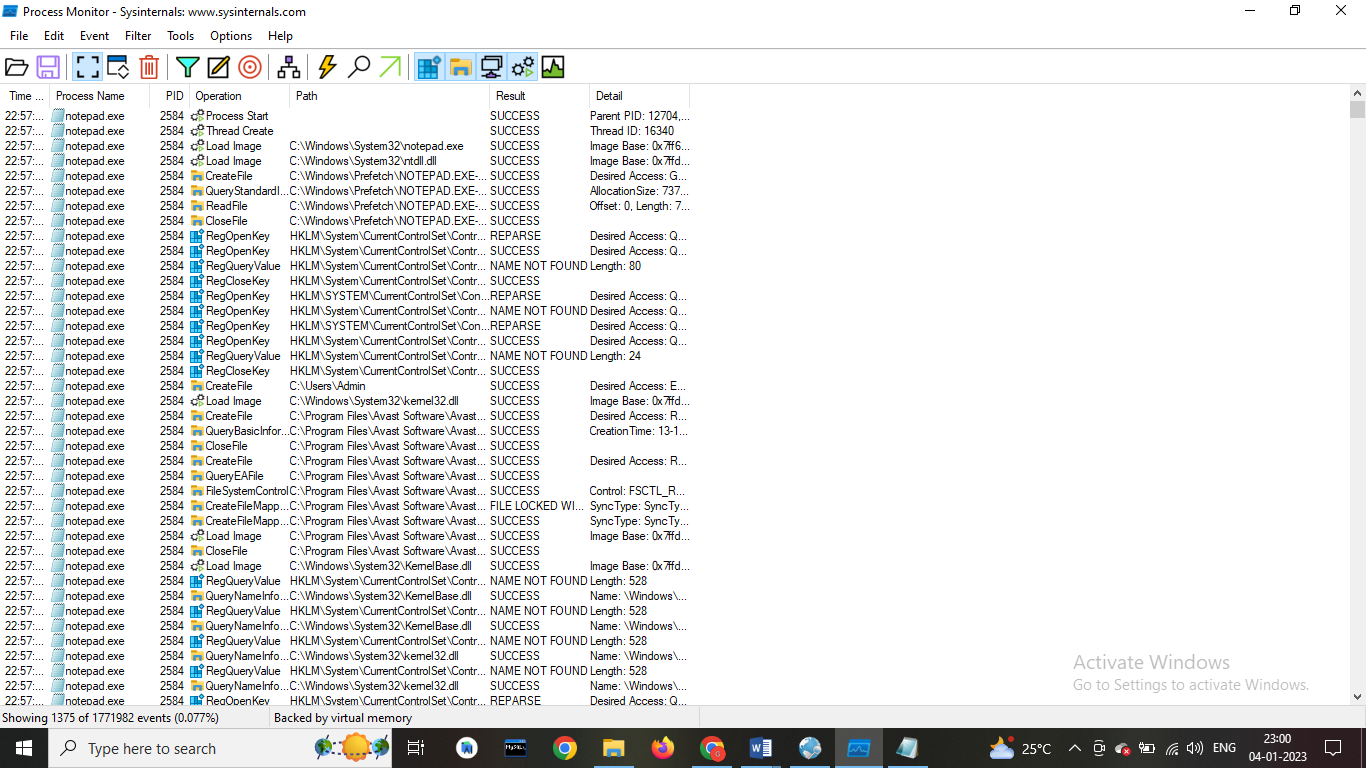


**2] Monitor Live Process (Tool: ProcMon)**

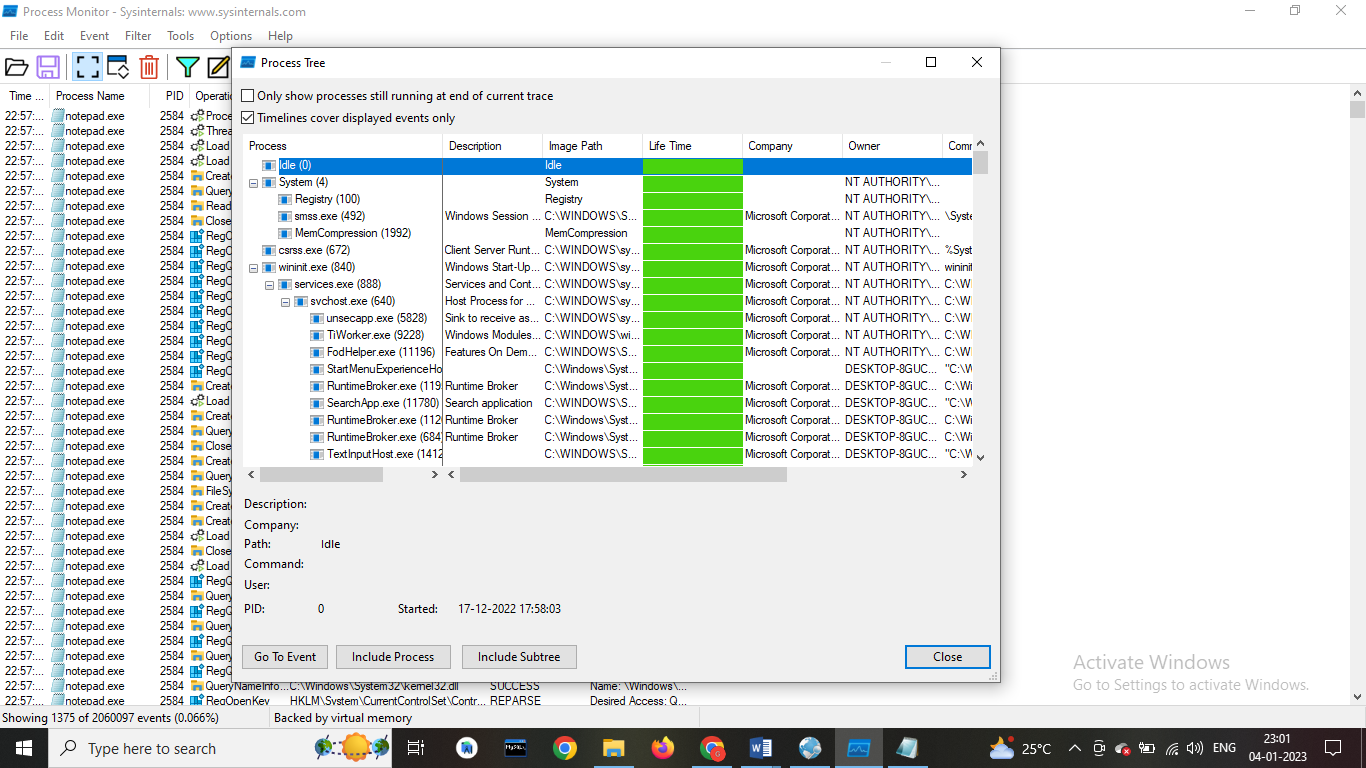


* **Click on filter > Process monitor filter**

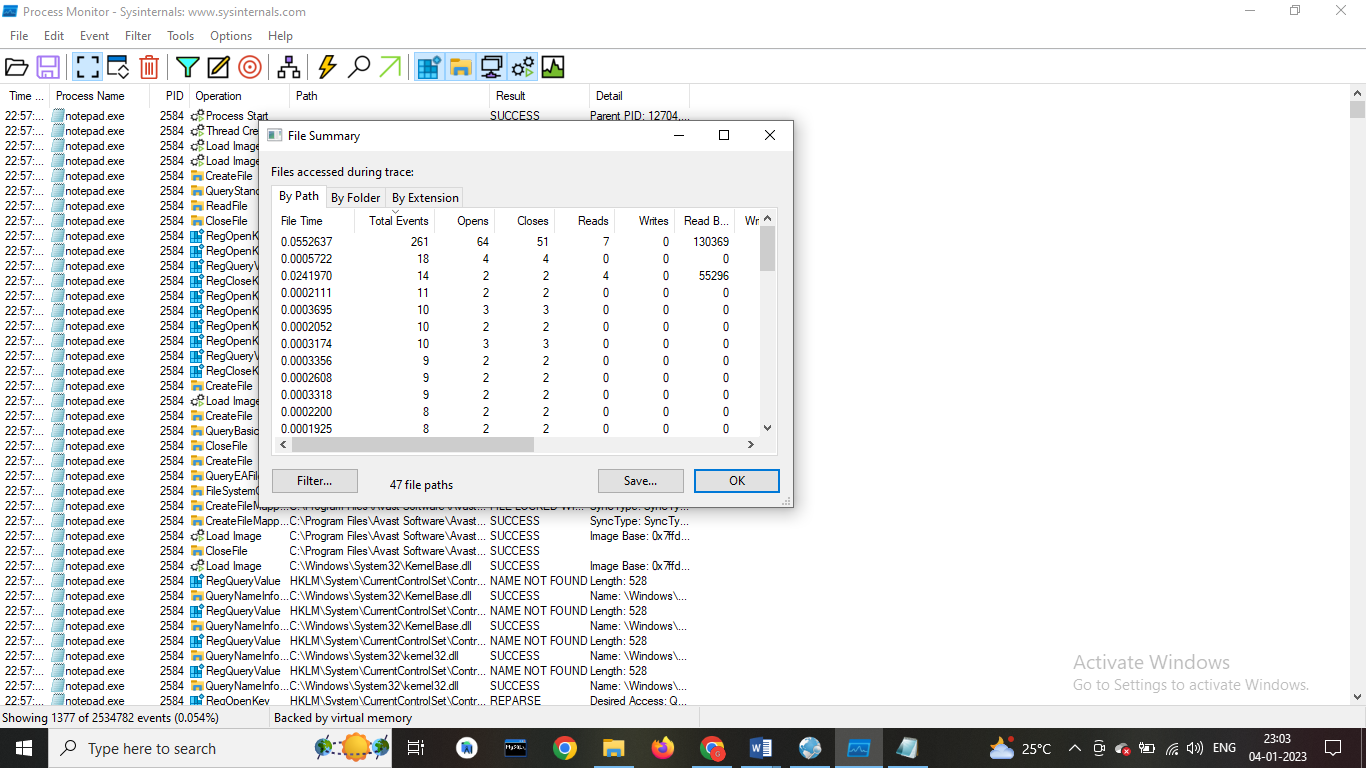




* **Click on tools > Process tree**

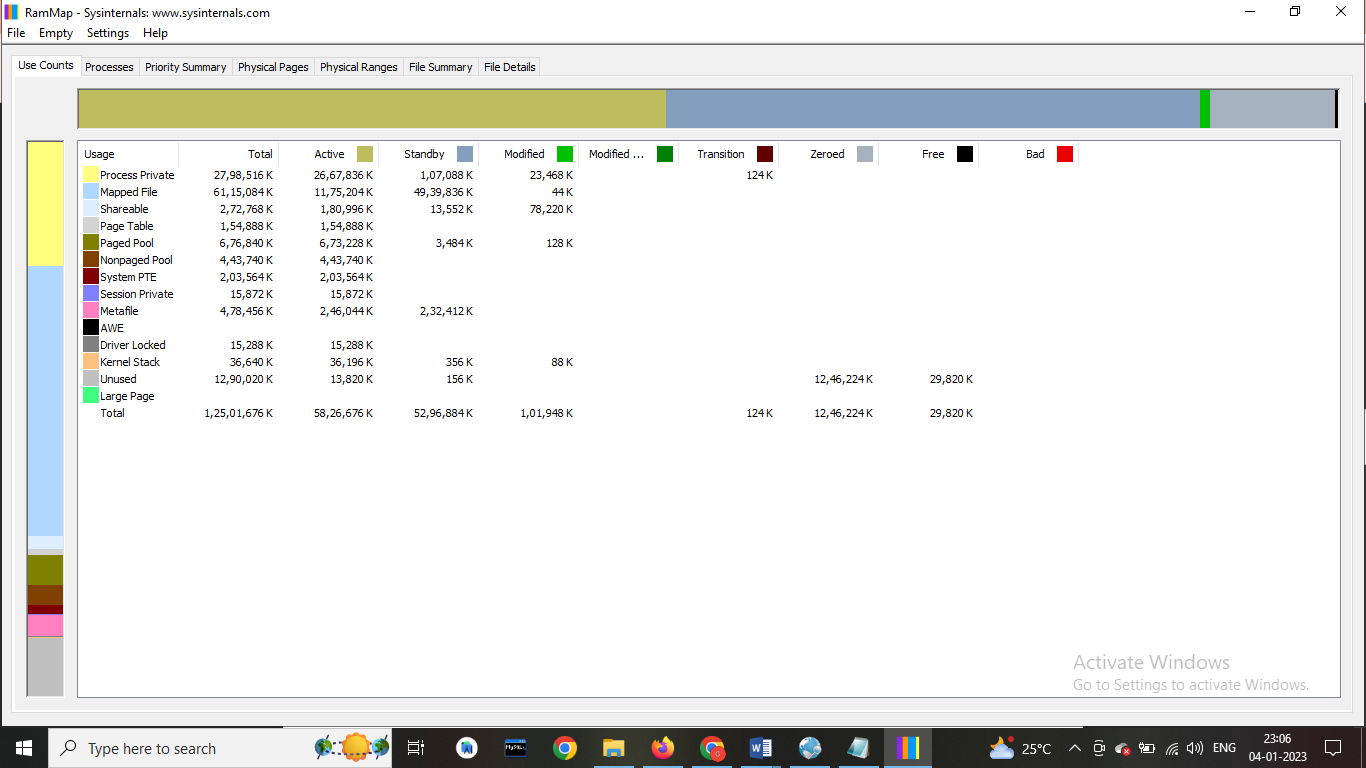


* **Click on tools > File summary**



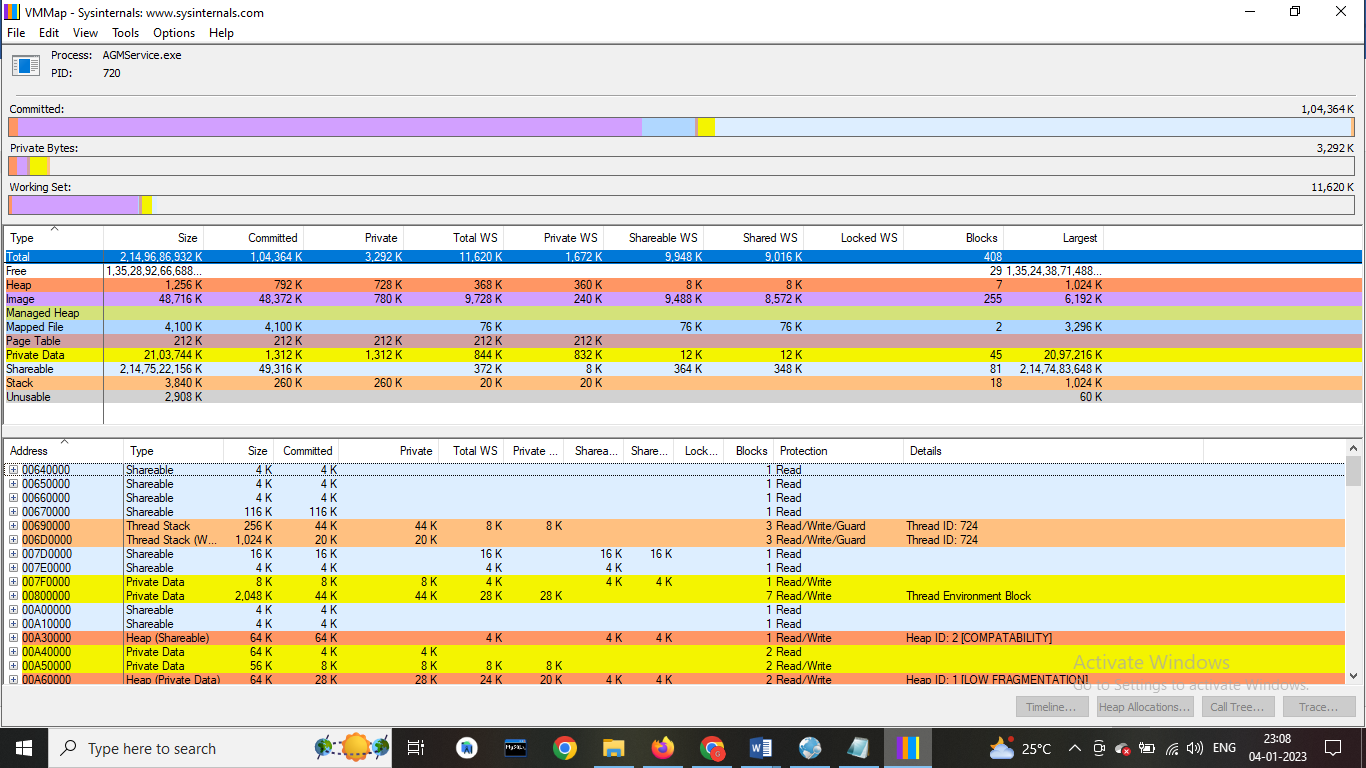
**3] Monitor Cache Memory (Tool: RAMMap)**

**Open the RAMMap tool.**



**4] Monitor Virtual Memory (Tool: VMMap)**

**Open the VMMap tool.**



**5] Monitor Hard Disk (Tool: DiskMon)**

**Open the DiskMon Tool**

