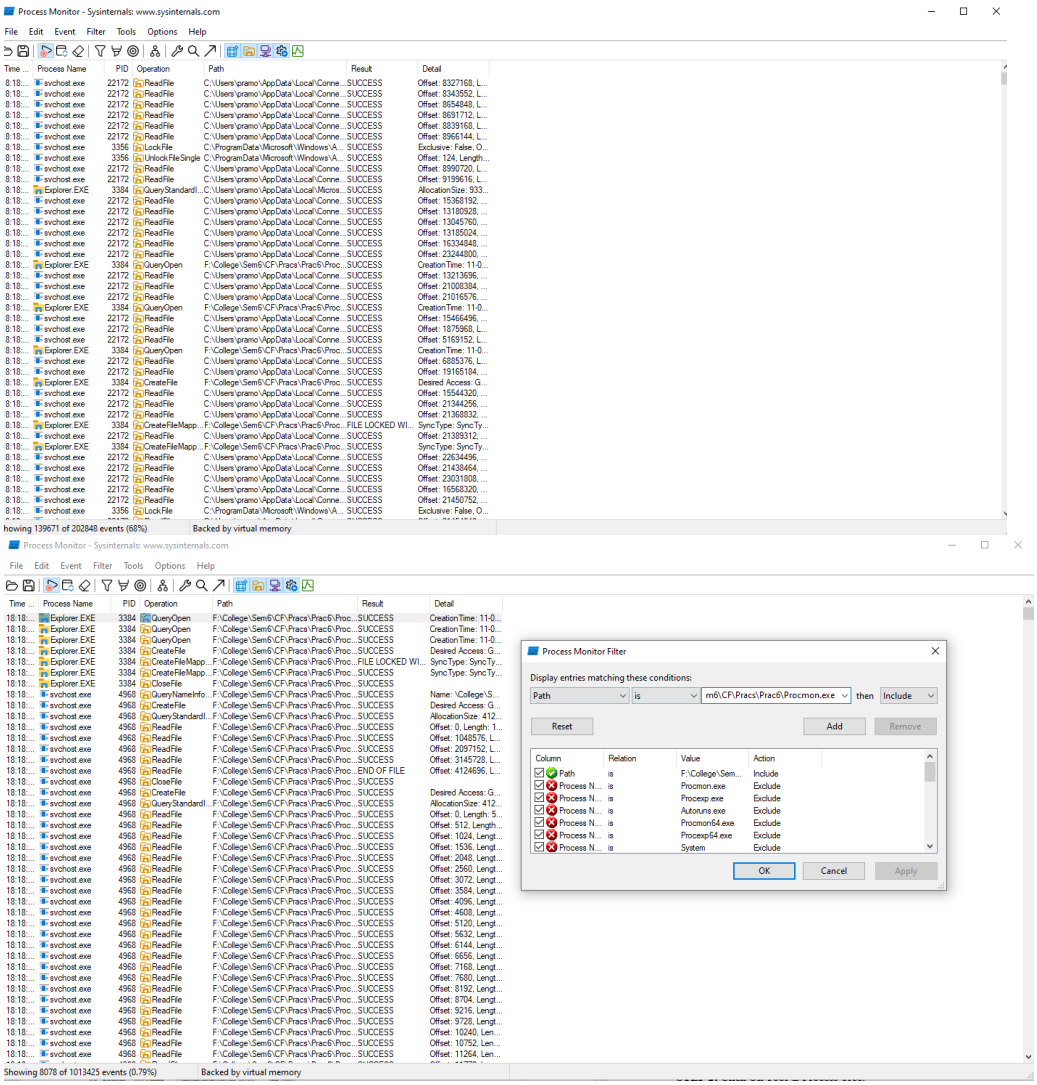
Practical 6

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

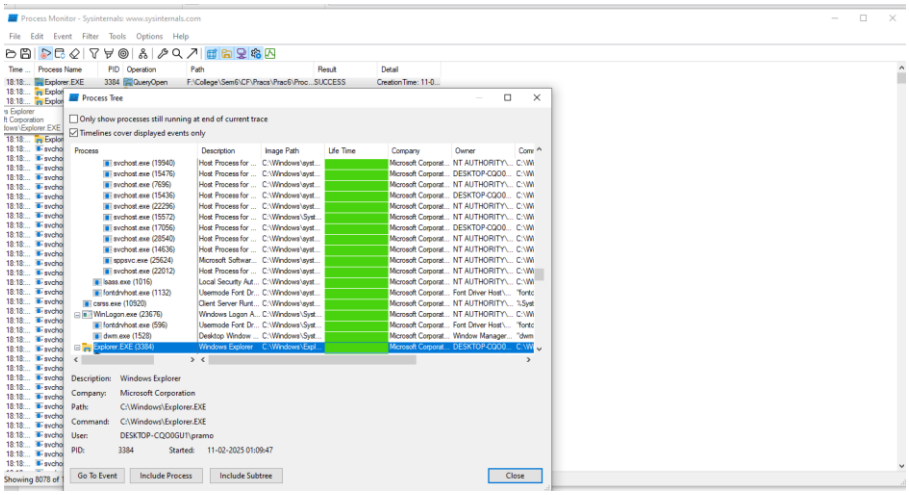
- Check Sysinternals tools
- Monitor Live Processes
- Capture RAM
- Capture TCP/UDP packets
- Monitor Hard Disk
- Monitor Virtual Memory
- Monitor Cache Memory

1. MONITOR LIVE PROCESSES (TOOL:-PROCMON)

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

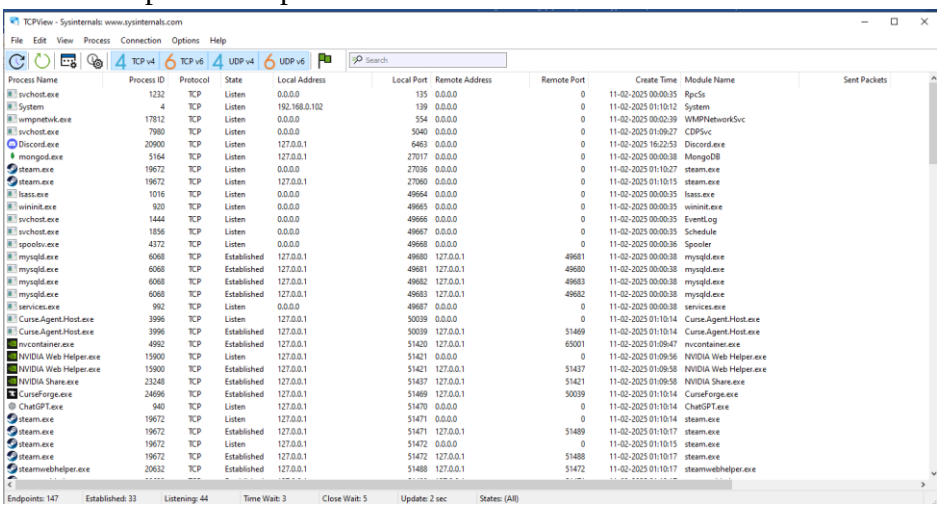


STEP 2: Click On Tool Process Tree.

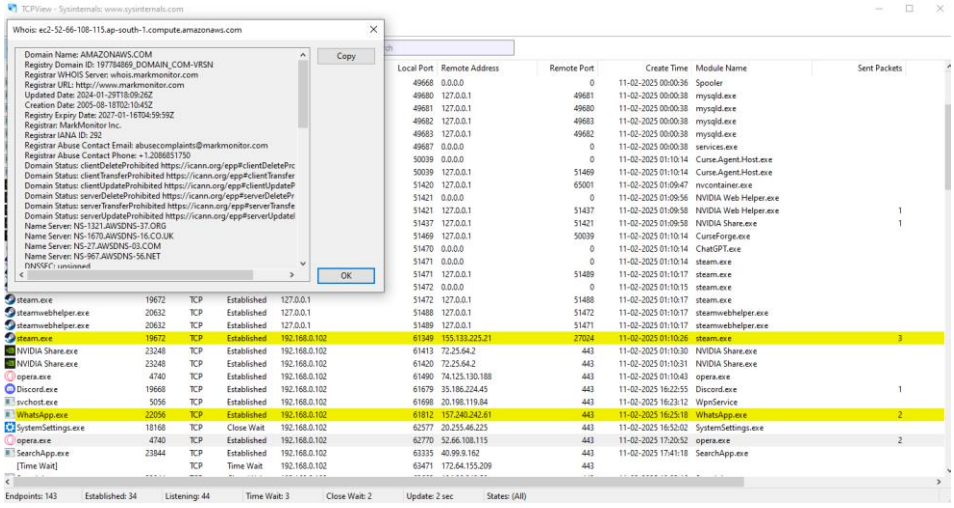


2. CAPTURE TCP/UDP PACKETS (TOOL:-Tcpview):

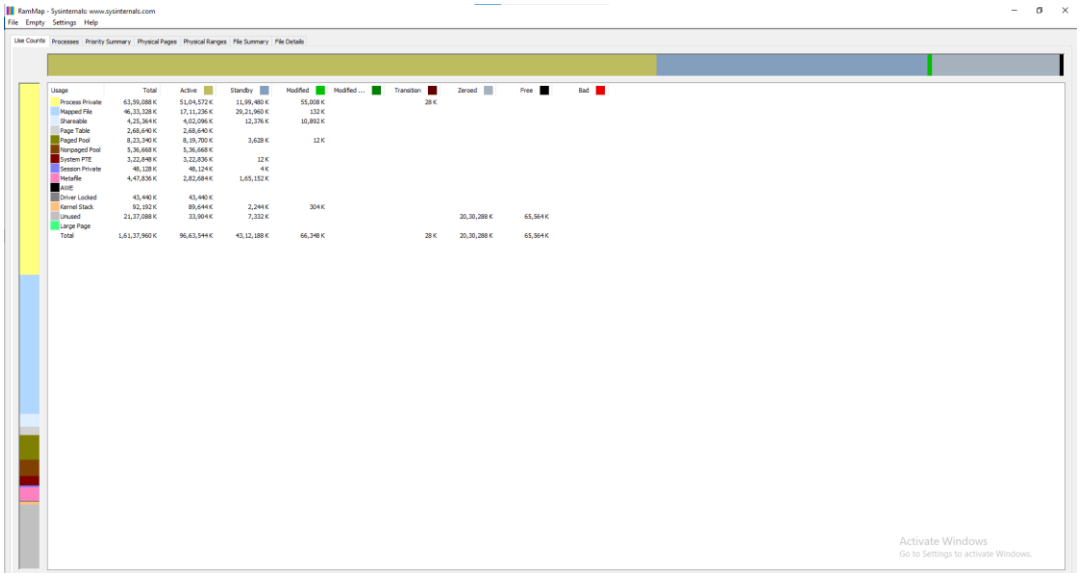
STEP 1: Open the Tcpview tool.



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

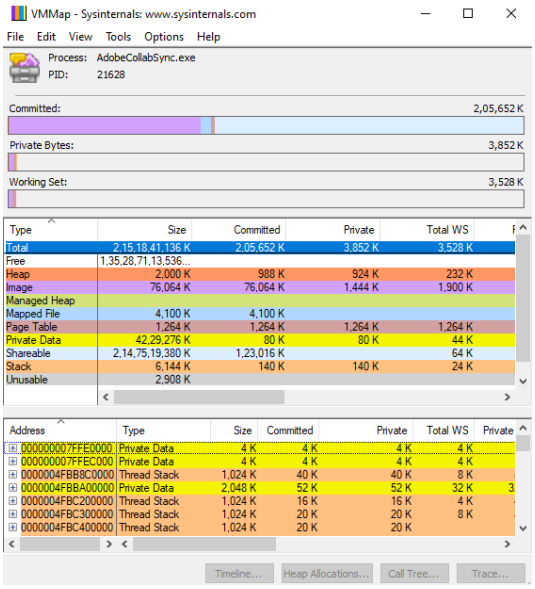


3. MONITOR HARD DISK (TOOL:-RAMMap) STEP 1: Open RAMMap tool.



4. MONITOR VIRTUAL MEMORY (TOOL:-VMMap):

STEP 1: Open VMMap tool.



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

STEP 1: Open Cacheset Tool.