

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

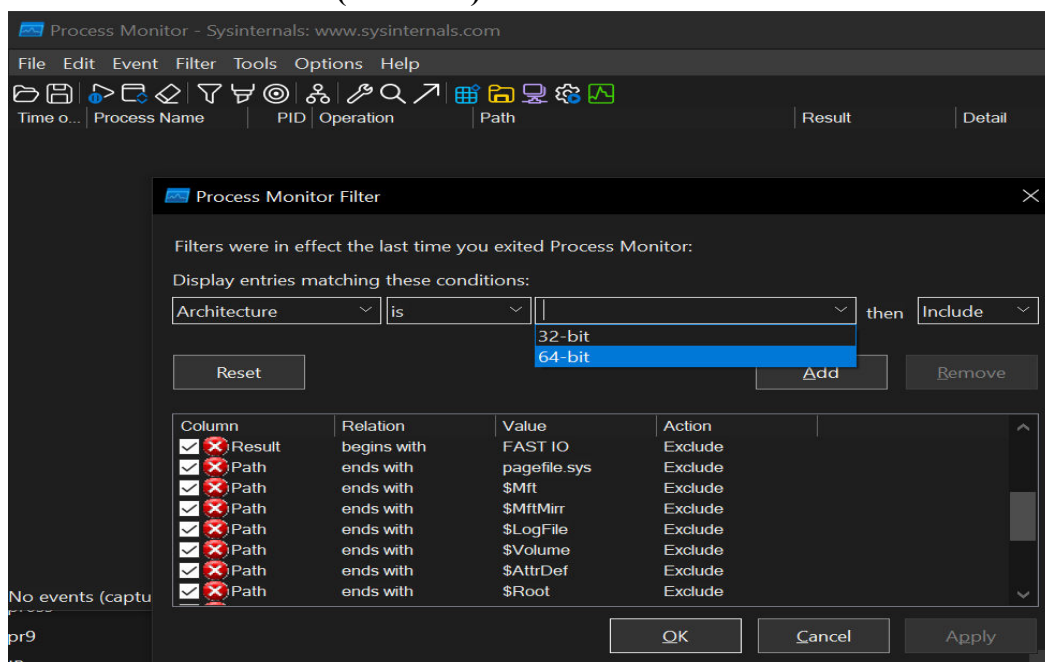
1. Check Sysinternals tools

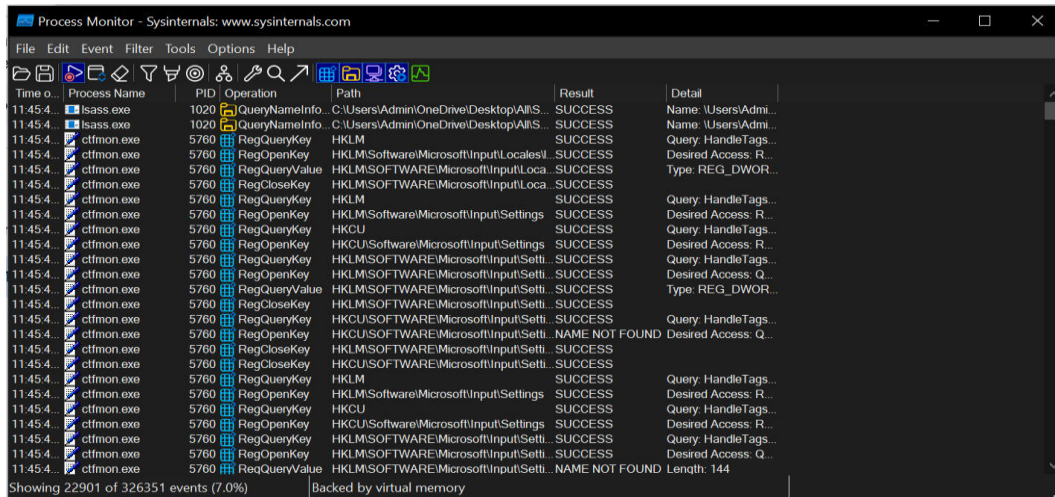
Step 1: Go to Chrome & search for Sysinternals tools

Step 2: Click on Sysinternals tools suite -> Download Sysinternals tools -> Unzip the zip file

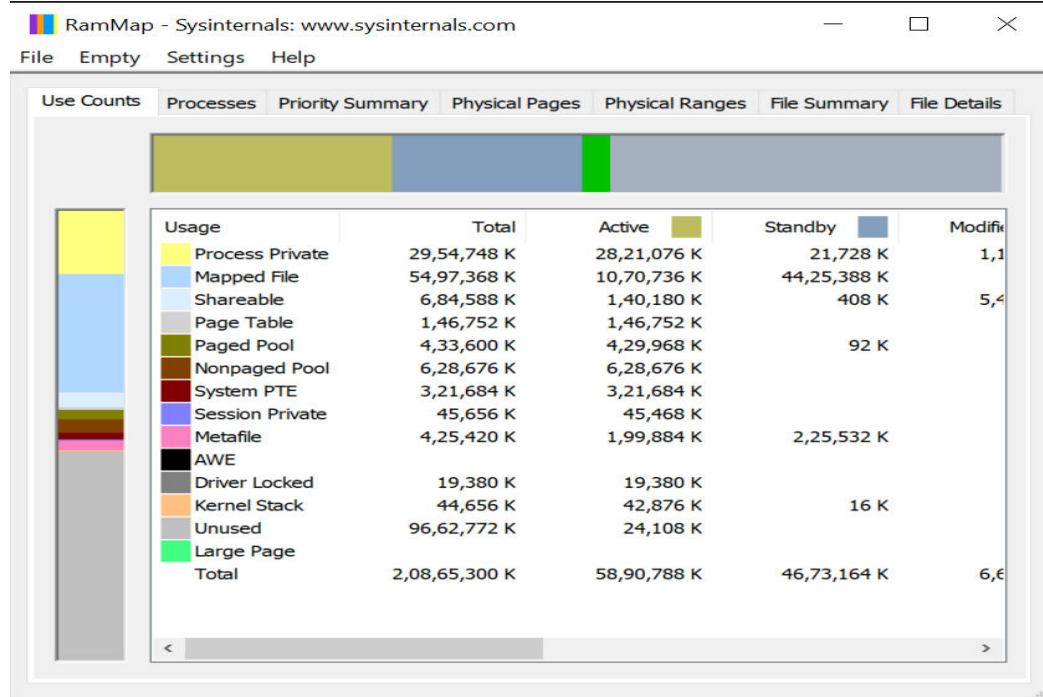
Name	Status	Date modified	Type	Size
autopsy		06-12-2024 20:57	File folder	
cf image		06-12-2024 20:59	File folder	
EnCase Forensic		06-12-2024 21:00	File folder	
FTK		06-12-2024 21:00	File folder	
ftk181		06-12-2024 21:00	File folder	
MOBILedit! Forensic		06-12-2024 21:00	File folder	
Sysinternals		06-12-2024 21:00	File folder	
wireshark		06-12-2024 21:00	File folder	
BrowserHistoryExaminer_v1.9.0_Installer.msi		11-03-2019 09:32	Windows Installer Pa...	43,067 KB

2. Monitor Live Processes (Procmon)





3. Capture RAM (RAMMap)



4. Capture TCP/UDP packets (tcpview)

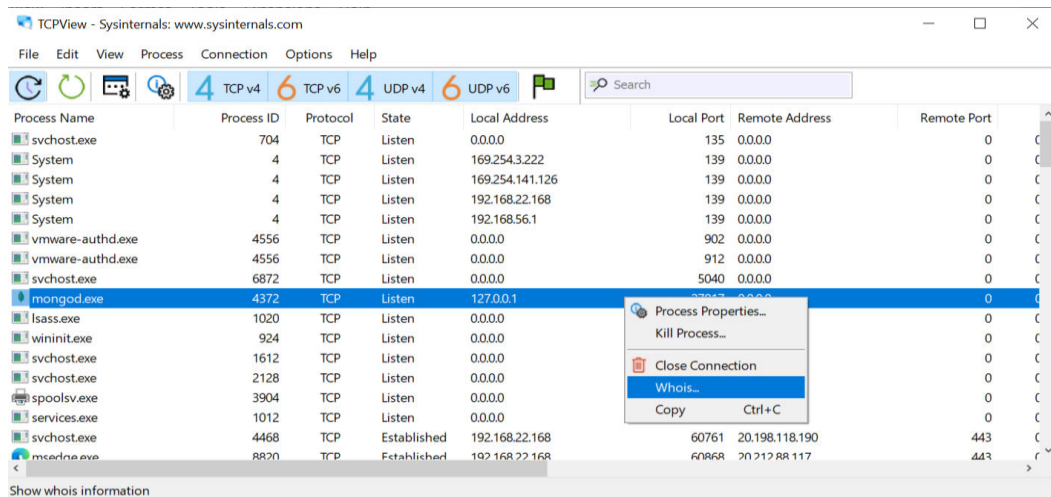
TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

Search

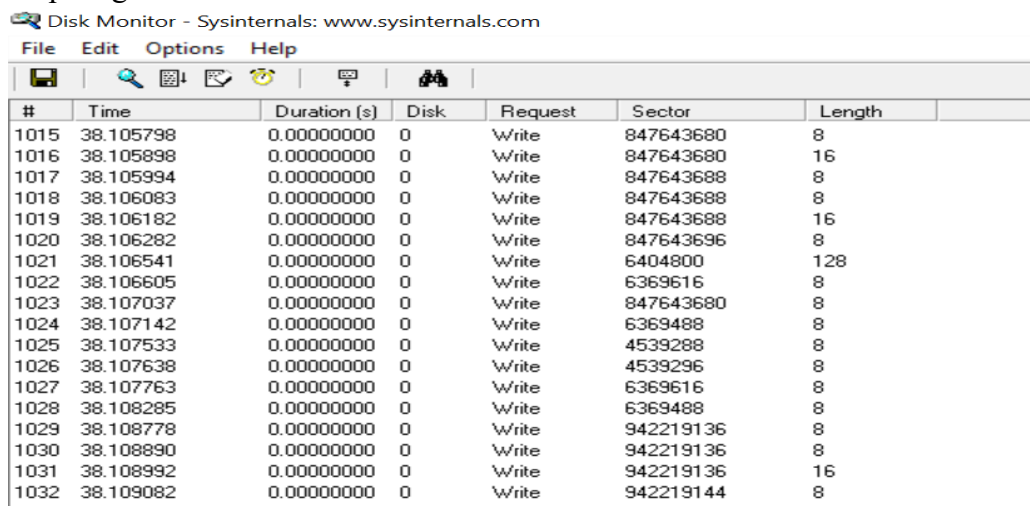
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port
svchost.exe	704	TCP	Listen	0.0.0	135	0.0.0	0
System	4	TCP	Listen	169.254.3.222	139	0.0.0	0
System	4	TCP	Listen	169.254.141.126	139	0.0.0	0
System	4	TCP	Listen	192.168.22.168	139	0.0.0	0
System	4	TCP	Listen	192.168.56.1	139	0.0.0	0
vmware-authd.exe	4556	TCP	Listen	0.0.0	902	0.0.0	0
vmware-authd.exe	4556	TCP	Listen	0.0.0	912	0.0.0	0
svchost.exe	6872	TCP	Listen	0.0.0	5040	0.0.0	0
mongod.exe	4372	TCP	Listen	127.0.0.1	27017	0.0.0	0
lsass.exe	1020	TCP	Listen	0.0.0	49664	0.0.0	0
wininit.exe	924	TCP	Listen	0.0.0	49665	0.0.0	0
svchost.exe	1612	TCP	Listen	0.0.0	49666	0.0.0	0
svchost.exe	2128	TCP	Listen	0.0.0	49667	0.0.0	0
spoolsv.exe	3904	TCP	Listen	0.0.0	49668	0.0.0	0
services.exe	1012	TCP	Listen	0.0.0	49672	0.0.0	0
svchost.exe	4468	TCP	Established	192.168.22.168	60761	20.198.118.190	443
svchost.exe	8820	TCP	Established	192.168.22.168	60868	20.212.188.117	443

Endpoints: 117 Established: 6 Listening: 26 Time Wait: 3 Close Wait: 2 Update: 2 sec States: (All)

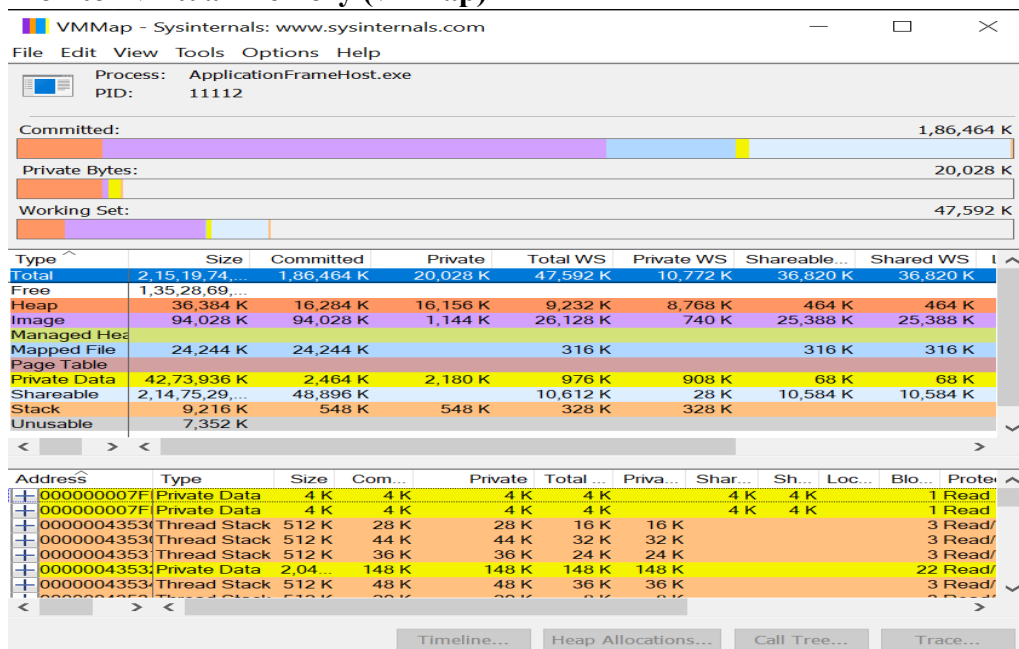


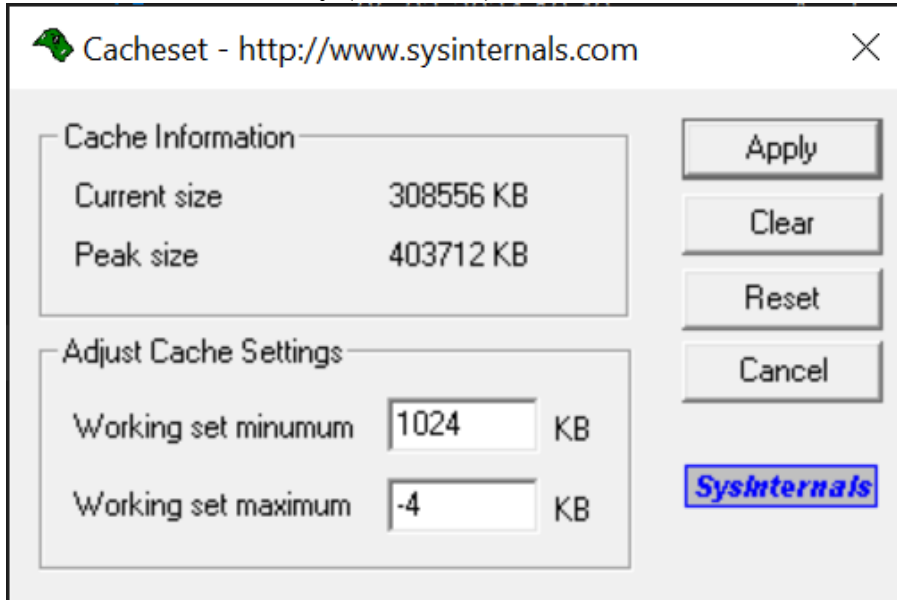
5. Monitor Hard disk (diskmon)

Step: Right click on diskmon.exe and Run as Administrator



6. Monitor Virtual Memory (vmmmap)



7. Monitor Cache memory (chacheset)

The screenshot shows the Cacheset utility window from Sysinternals. The window title is "Cacheset - http://www.sysinternals.com". It contains two main sections: "Cache Information" and "Adjust Cache Settings".

Cache Information:

Property	Value
Current size	308556 KB
Peak size	403712 KB

Adjust Cache Settings:

Setting	Value	Unit
Working set minimum	1024	KB
Working set maximum	-4	KB

On the right side of the window, there are four buttons: "Apply", "Clear", "Reset", and "Cancel". At the bottom right, there is a "Sysinternals" logo.