**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**

**Steps:**

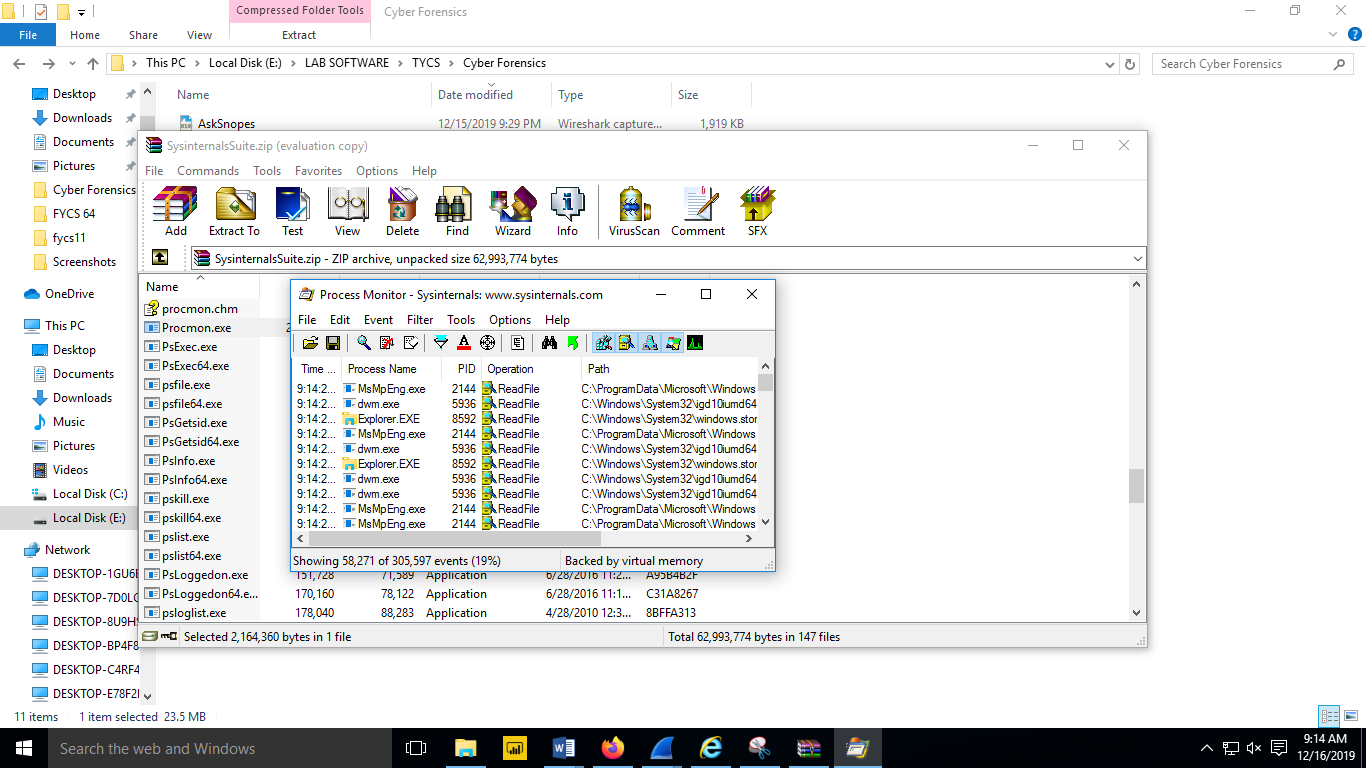
**1) Check Sysinternals tools**

**Windows Sysinternals tools are utilities to manage, diagnose, troubleshoot, and monitor a**

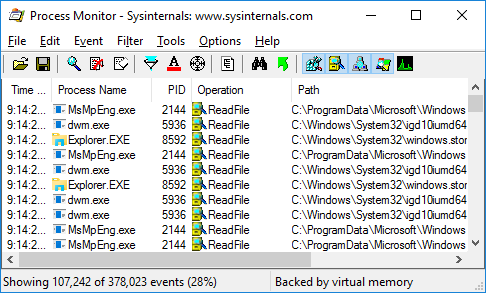
**Microsoft Windows environment**

**The following are the categories of Sysinternals Tools:**

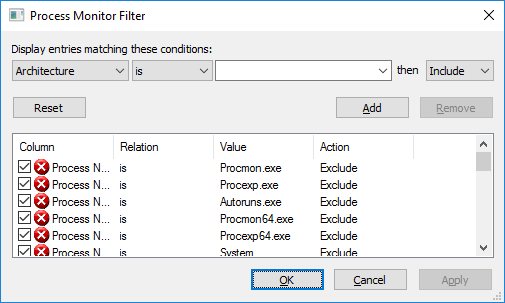
* **File and Disk Utilities**
* **Networking Utilities**
* **Process Utilities**
* **Security Utilities**
* **System Information Utilities**
* **Miscellaneous Utilities**



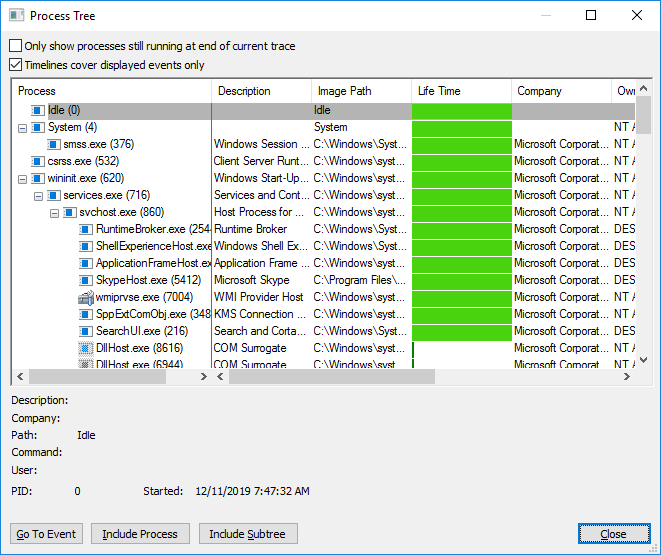
**2) Monitor Live Processes (Tool: ProcMon)**



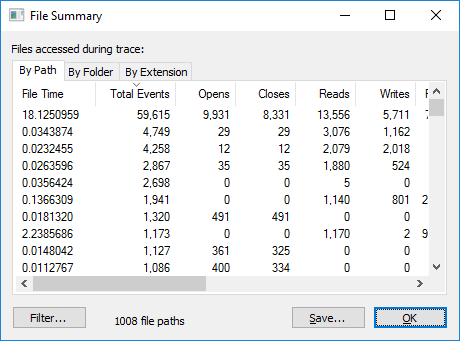
**Click on filter > Process monitor filter**



**Click on tools > Process tree**

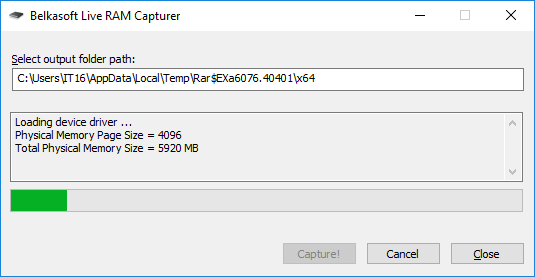


**Click on tools > File summary**

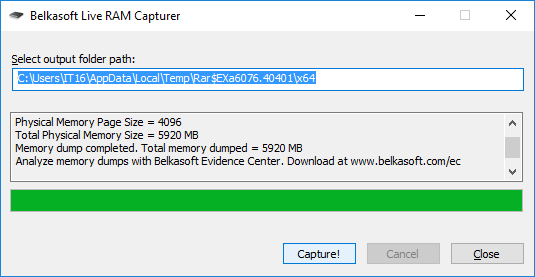


**3) Capture RAM (Tool: RAMCapture)**

**Open the Ramcapture tool.**

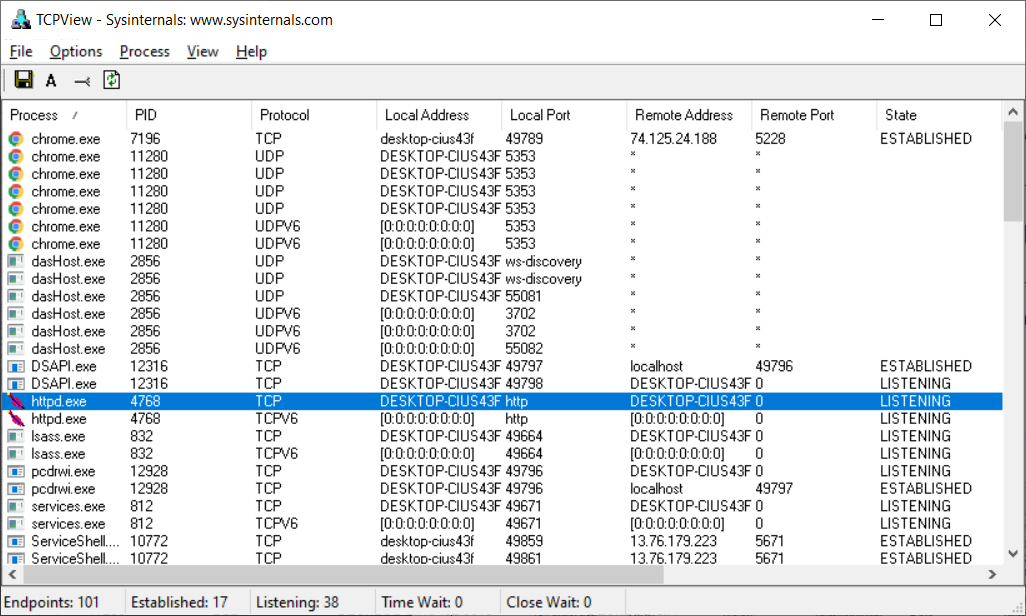


**Click on capture.**

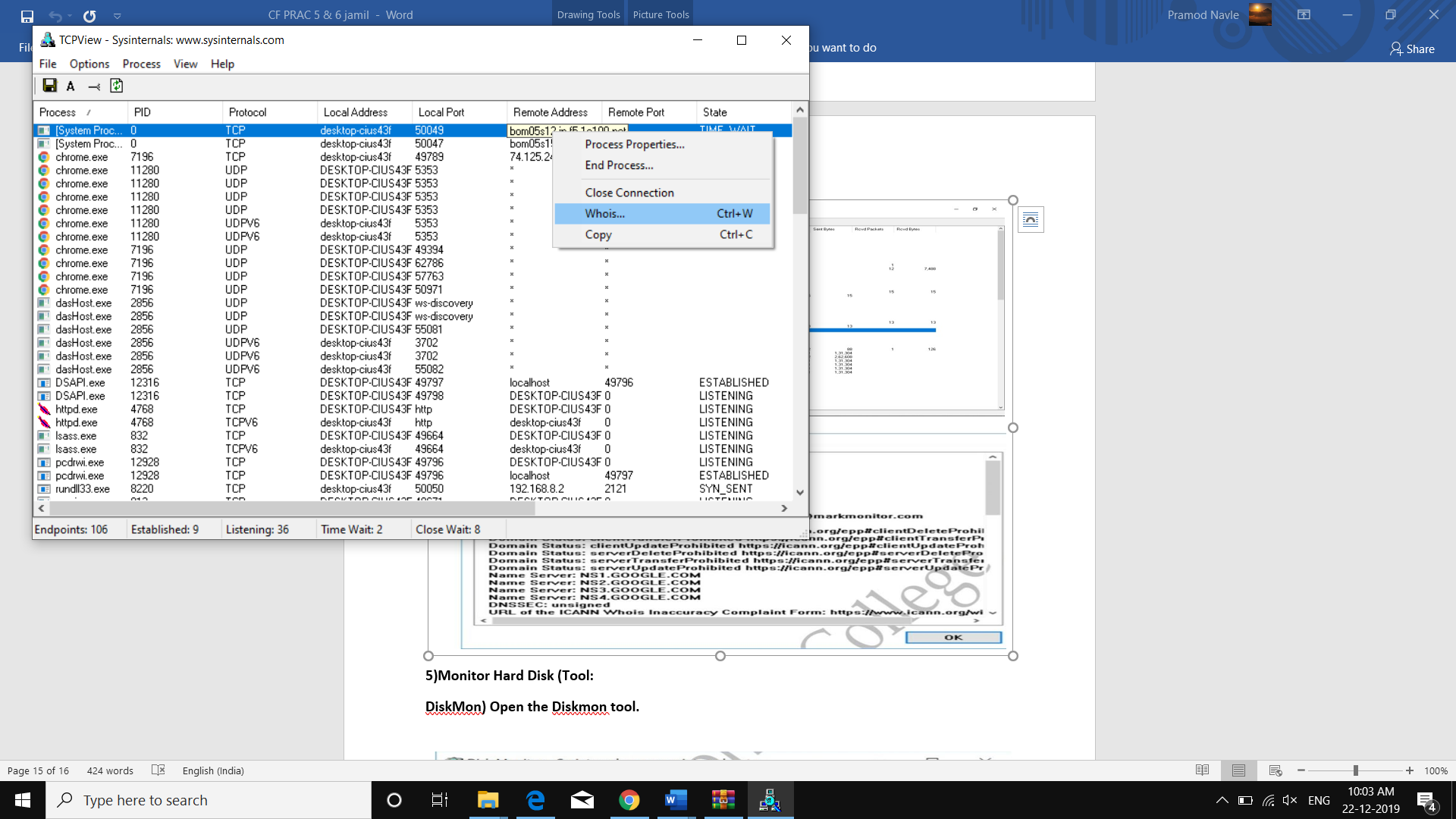


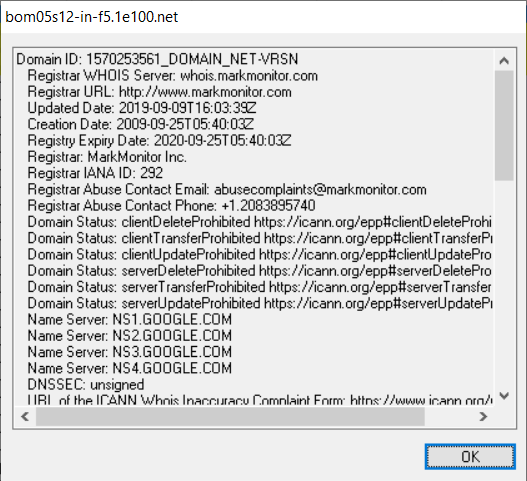
**4) Capture TCP/UDP packets (Tool: TcpView)**

**Open the Tcpview tool.**



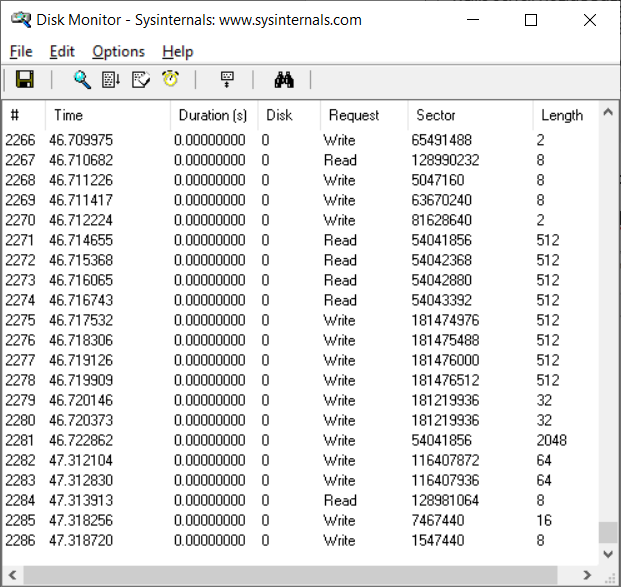
**Right click on any packet> Whois**





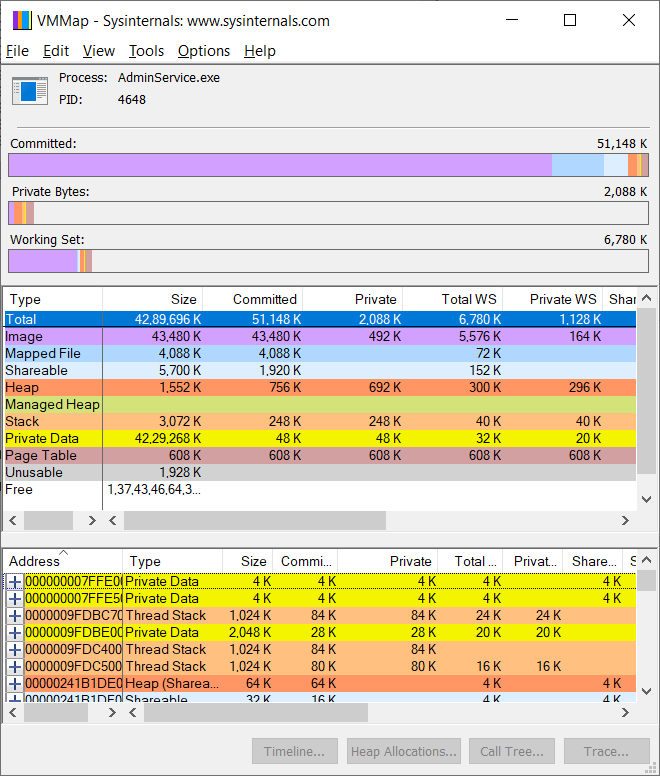
5) Monitor Hard Disk (Tool: DiskMon)

Open the Diskmon tool.



1. Monitor Virtual Memory (Tool: VMMap)

Open the VMMap tool.



**7) Monitor Cache Memory (Tool: RAMMap)**

**Open the RAMMap tool.**

