**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.

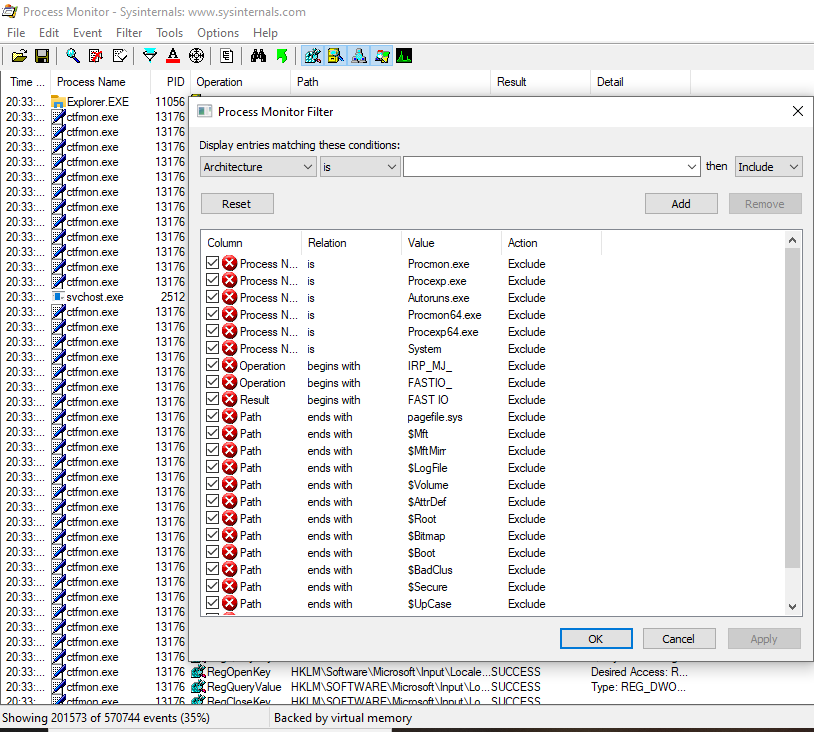
The following are the categories of Sysinternals Tools:

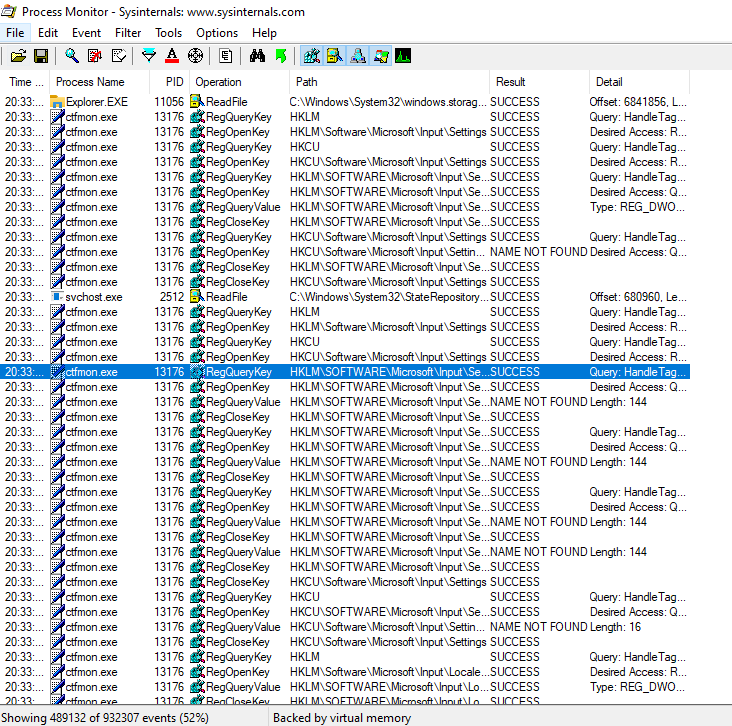
* 1. File and Disk Utilities
  2. Networking Utilities
  3. Process Utilities
  4. Security Utilities
  5. System Information Utilities
  6. Miscellaneous Utilities

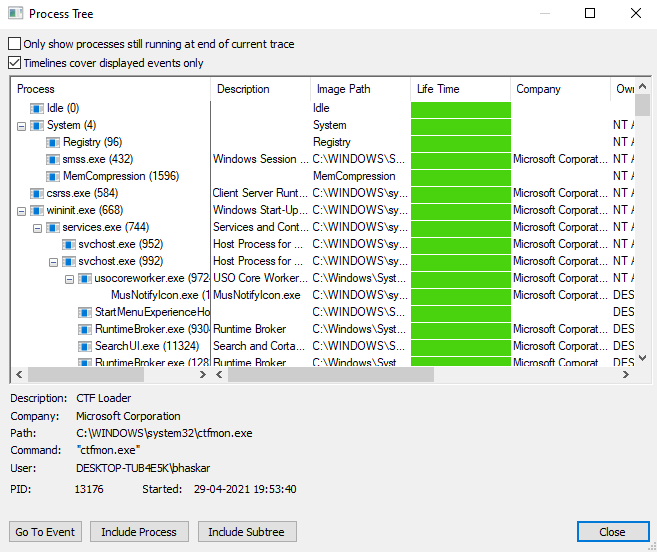
## Monitor Live Processes : (Tool: ProcMon) To Do:

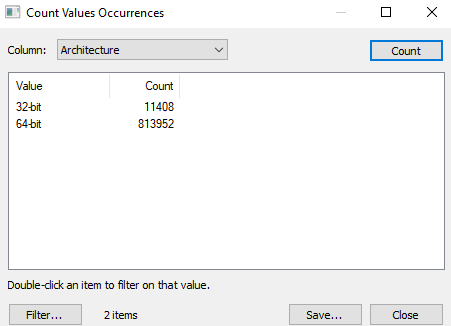
1. Filter (Process Name or PID or Architecture, etc)
2. Process Tree
3. Process Activity Summary
4. Count Occurrence

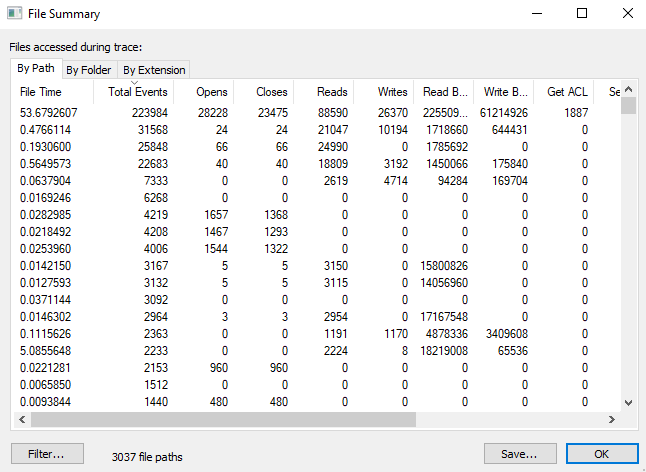
## Output:





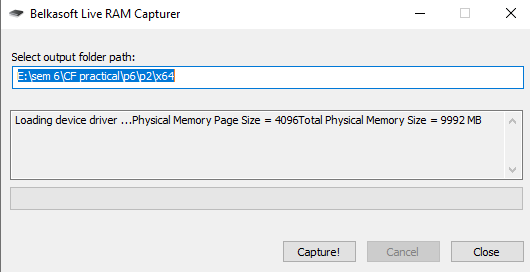


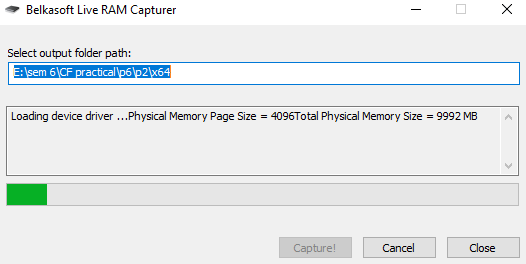


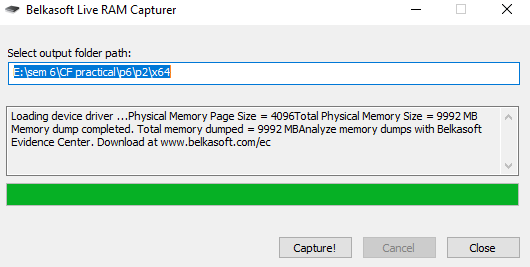


* + **Capture RAM (Tool: RAMCapture)**
  + **To Do:**
  1. Click Capture
  2. Creates a .mem file of the system memory (RAM) utilized.

## Output:







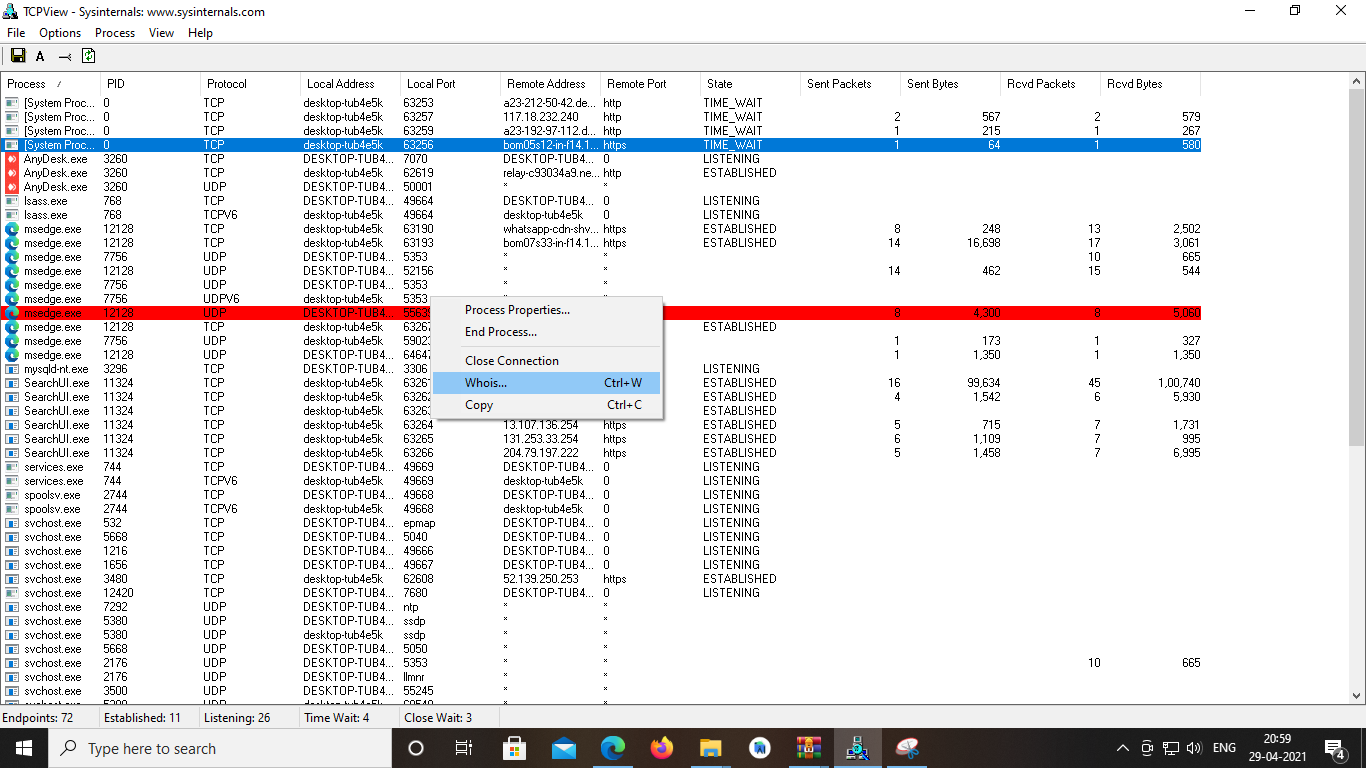
* + **Capture TCP/UDP packets (Tool: TcpView) :**

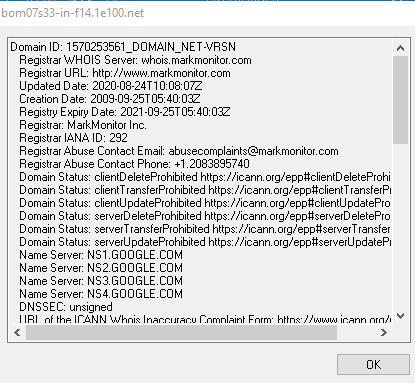
**To Do:**

1. Save to .txt file.

2. Whois

## Output:

****



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

**To Do:**

1. Save to .log file.
2. Check operations performed in the disk as per time and sectors affected.

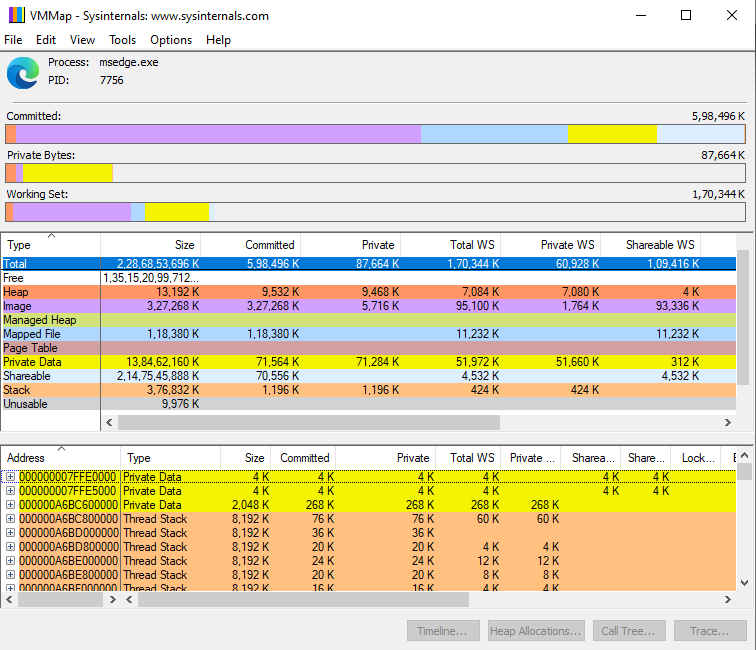
## Output :

* **Monitor Virtual Memory ( Tool : VMMAP) :**

**To Do:**

1. Options – Show Free & Unusable Regions
2. File-> Select Process e.g. chrome.exe
3. Save to .mmp file.

## Output :



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

**TO DO :**

* 1. Save to .RMP file.

## Output:

