Date-28/10 /2023

Roll No. - 13

Expt. No. - 05

K.M.S.P. Mandal’s

Sant Rawool Maharaj Mahavidyalaya, Kudal

**Department of Computer Science**

Signature

Use Sysinternals tools for Network Tracking and Process Monitoring.

Title - \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Sysinternals tools are a set of advanced system utilities and troubleshooting tools originally created by Mark Russinovich and Bryce Cogswell. These tools are now owned by Microsoft and are freely available for download. They are designed to help users, system administrators, and IT professionals analyze, diagnose, and troubleshoot issues related to Microsoft Windows systems.

**Some key features of Sysinternals tools include:**

**1. Process and System Utilities:**

- Tools like Process Explorer, Process Monitor, and Autoruns provide in-depth information about running processes, system resource usage, and startup processes.

**2. File and Disk Utilities:**

- Tools like Disk2vhd, DiskView, and Streams help analyze and manage files, disks, and file systems.

**3. Networking Utilities:**

- TCPView, Wireshark, and PortMon assist in monitoring and troubleshooting network-related issues, displaying information about network connections, and monitoring network activity.

**4. Security Utilities:**

- Tools like RootkitRevealer and Sigcheck help in detecting and analyzing security-related issues, including rootkits and verifying file signatures.

**5. Memory Utilities:**

- RAMMap and VMMap provide insights into memory usage and help diagnose memory-related problems.

**6. Registry Utilities:**

- Regedit, Regmon, and Autoruns offer tools for analyzing and managing the Windows Registry.

These tools are widely used in the IT industry for system troubleshooting, performance monitoring, and security analysis. They are considered valuable resources for gaining a deep understanding of Windows internals and resolving complex system issues.

**Process Monitor**

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such as session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.

**Disk Mon**

DiskMon is an application that logs and displays all hard disk activity on a Windows system. You can also minimize DiskMon to your system tray where it acts as a disk light, presenting a green icon when there is disk-read activity and a red icon when there is disk-write activity.

**Ram Map**

Have you ever wondered exactly how Windows is assigning physical memory, how much file data is cached in RAM, or how much RAM is used by the kernel and device drivers? RAMMap makes answering those questions easy. RAMMap is an advanced physical memory usage analysis utility for Windows Vista and higher Use RAMMap to gain understanding of the way Windows manages memory, to analyze application memory usage, or to answer specific questions about how RAM is being allocated. RAMMap’s refresh feature enables you to update the display and it includes support for saving and loading memory snapshots.

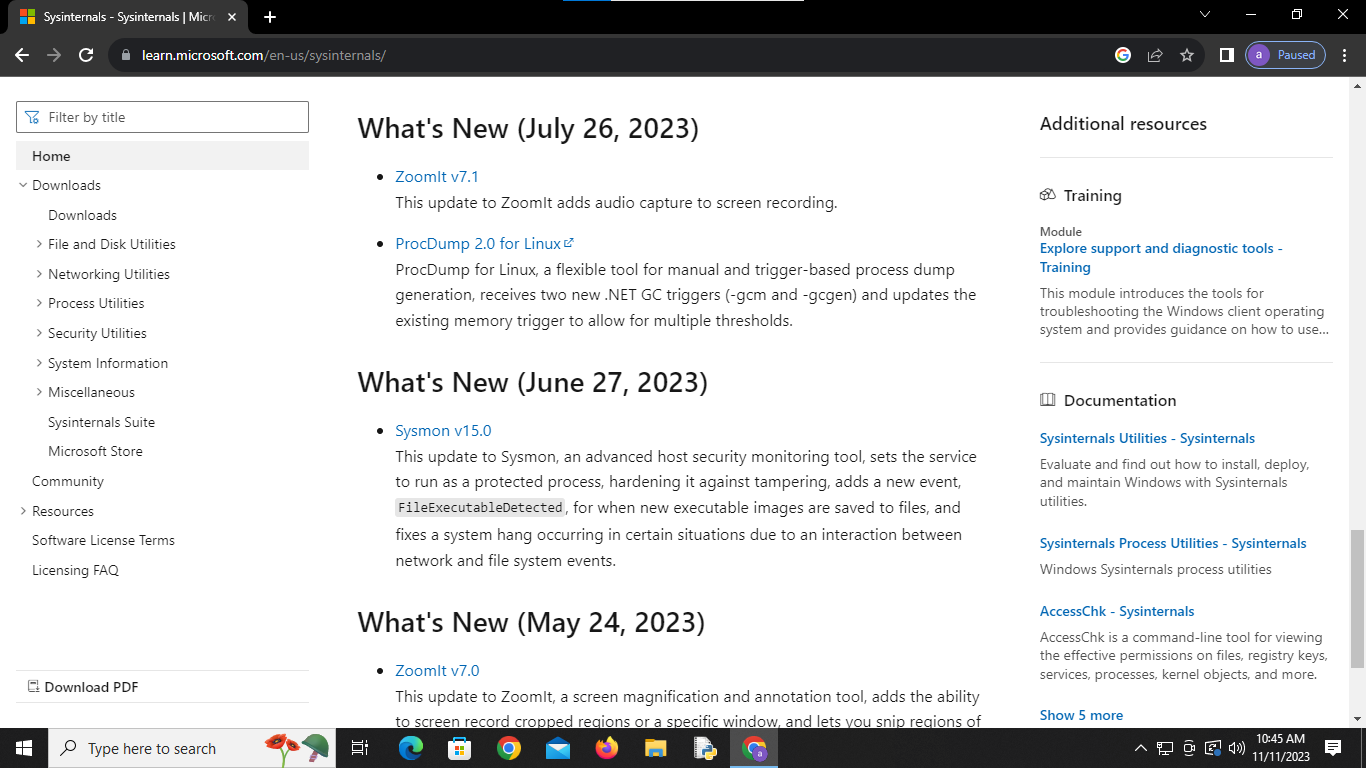
**TCP View**

TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. On Windows Server 2008, Vista, and XP, TCPView also reports the name of the process that owns the endpoint. TCPView provides a more informative and conveniently presented subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality.

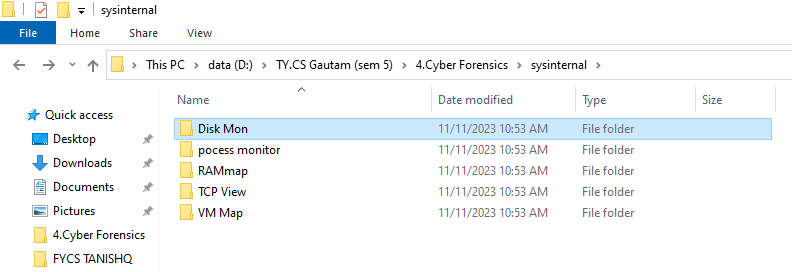
**VM Map**

VMMap is a process virtual and physical memory analysis utility. It shows a breakdown of a process's committed virtual memory types as well as the amount of physical memory (working set) assigned by the operating system to those types. Besides graphical representations of memory usage, VMMap also shows summary information and a detailed process memory map. Powerful filtering and refresh capabilities allow you to identify the sources of process memory usage and the memory cost of application features.

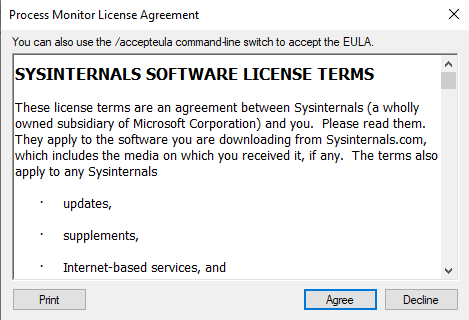
**Sysinternals tools Download**



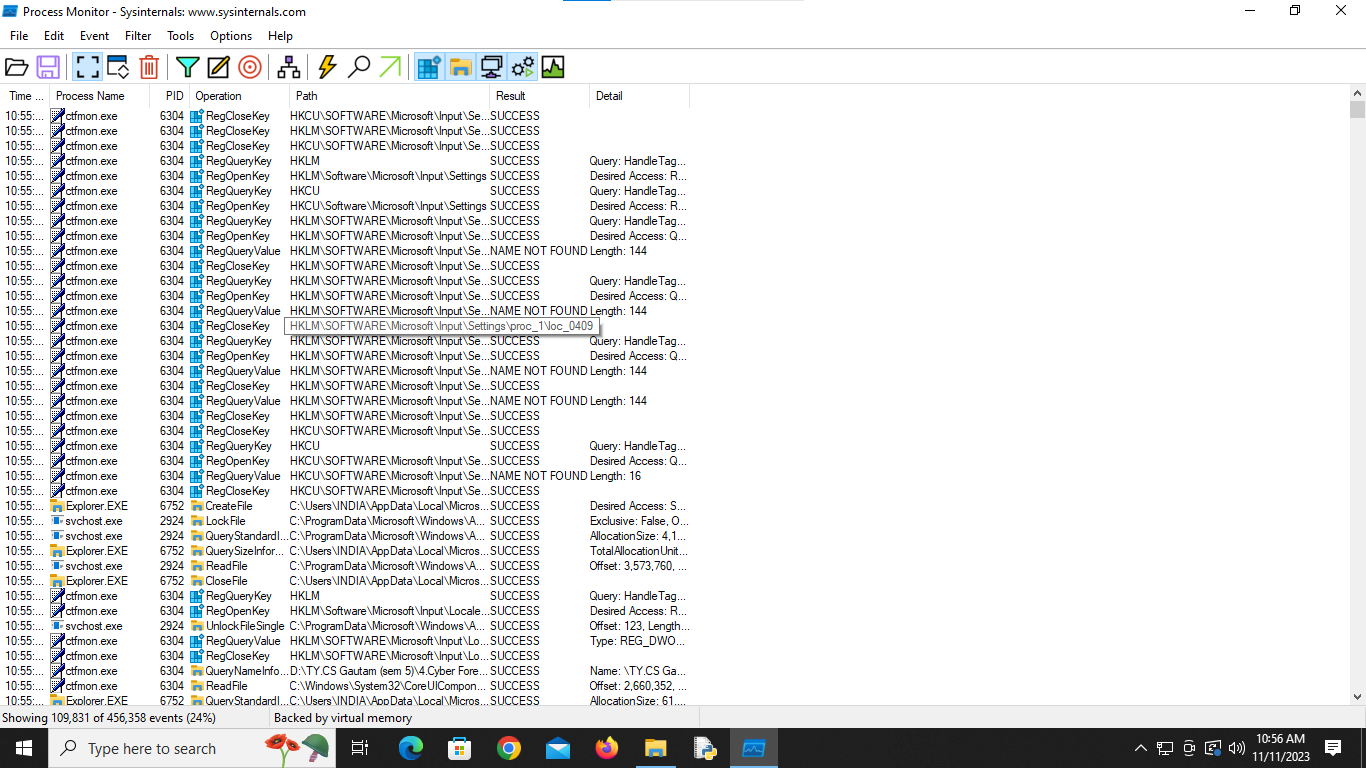
**Download Tools**



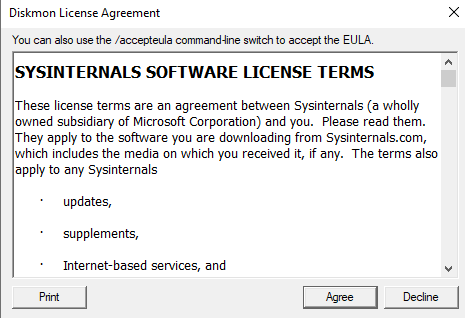
**Process Monitor**



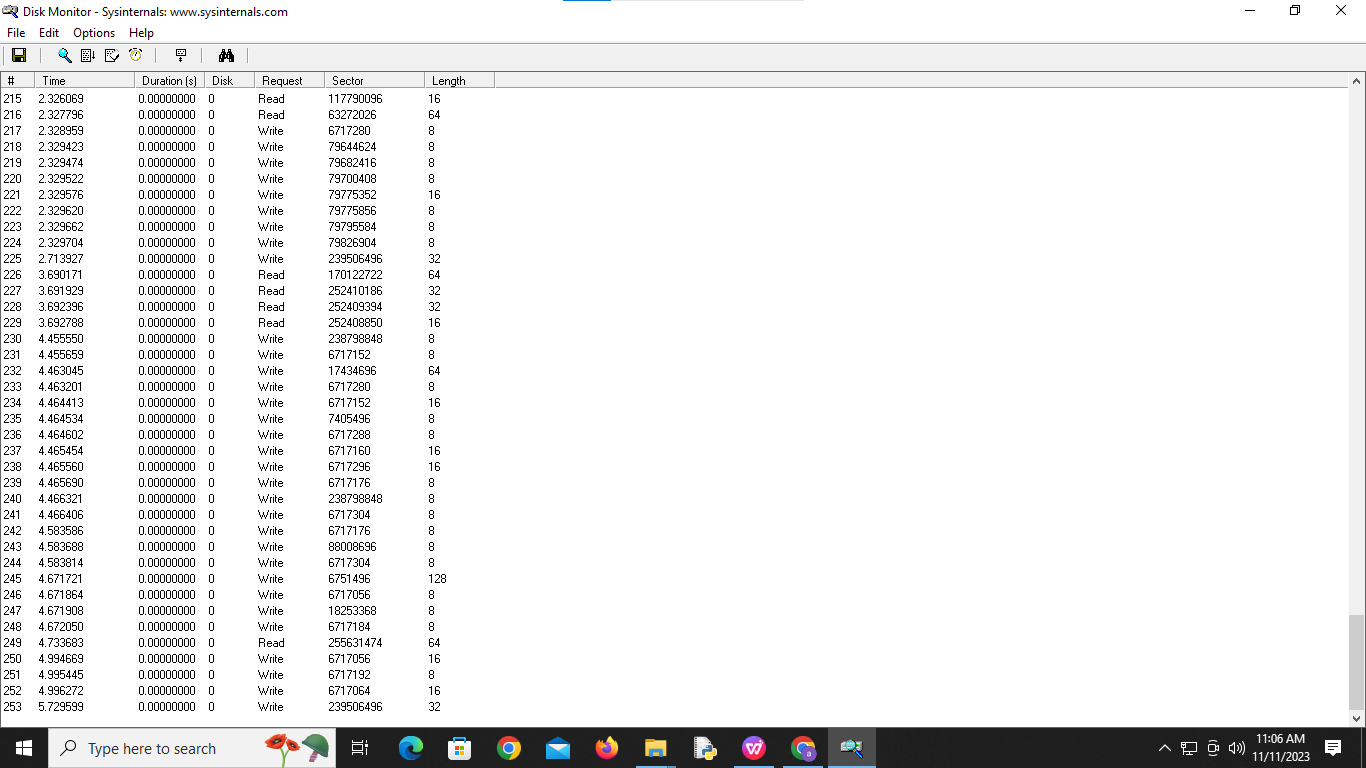
**Analysis of Process monitor**



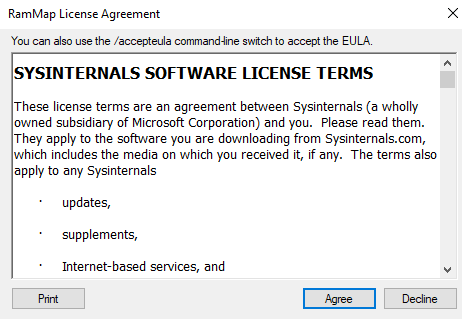
**Disk Monitor**



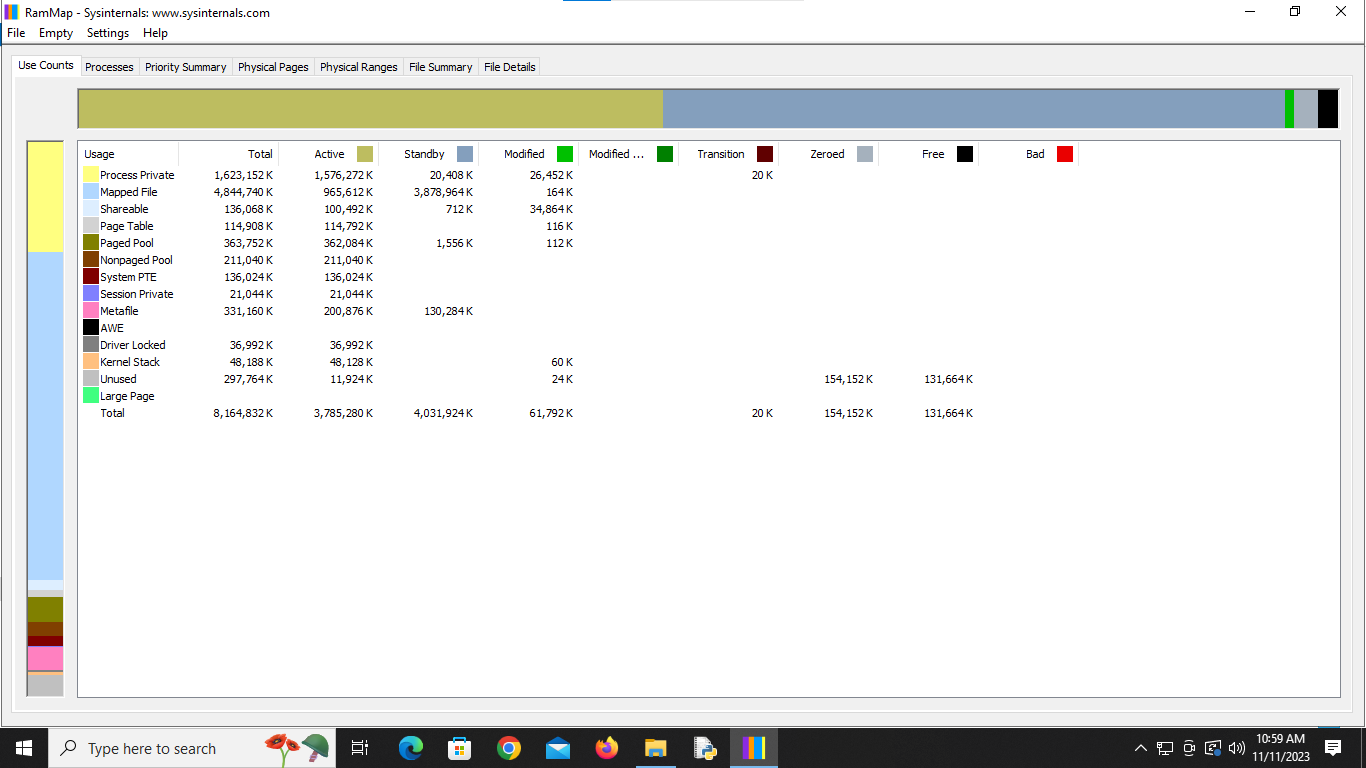
**Disk Mon**



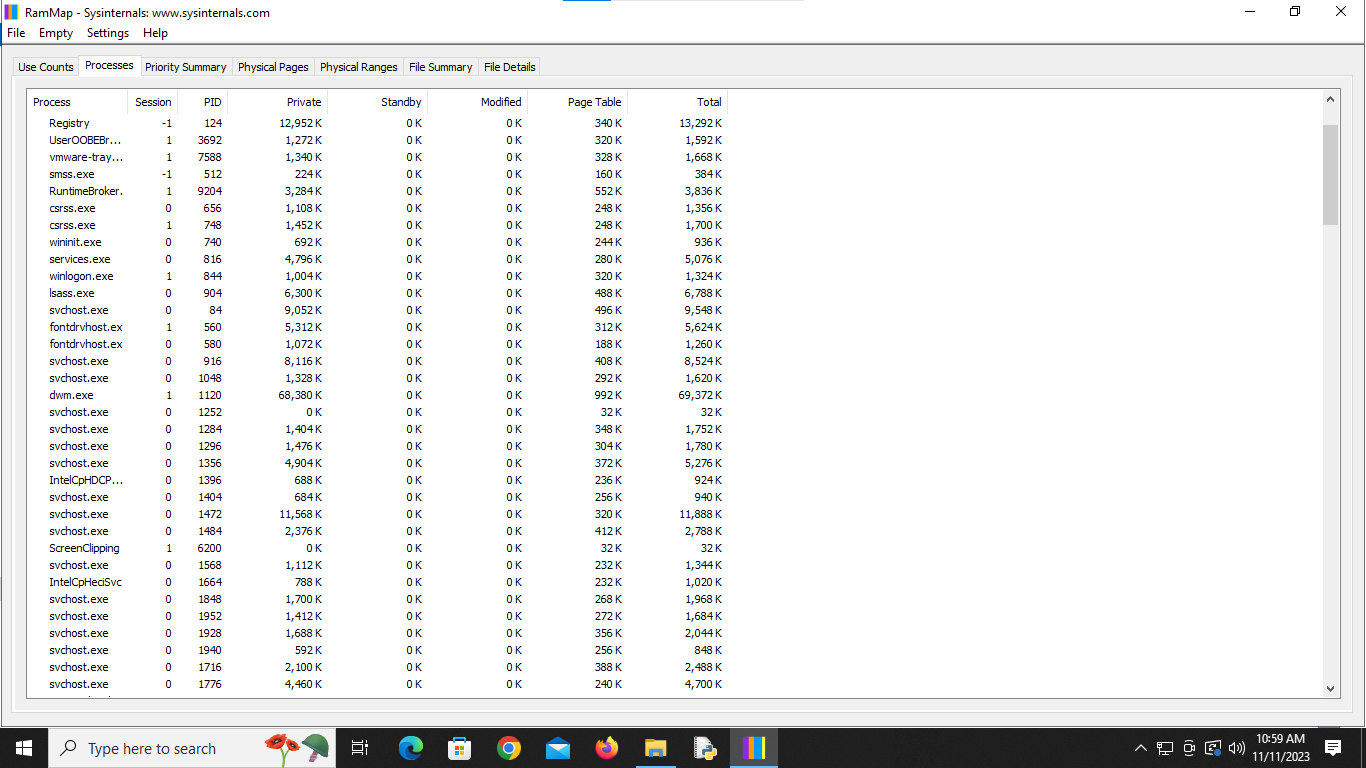
**RAM Map**



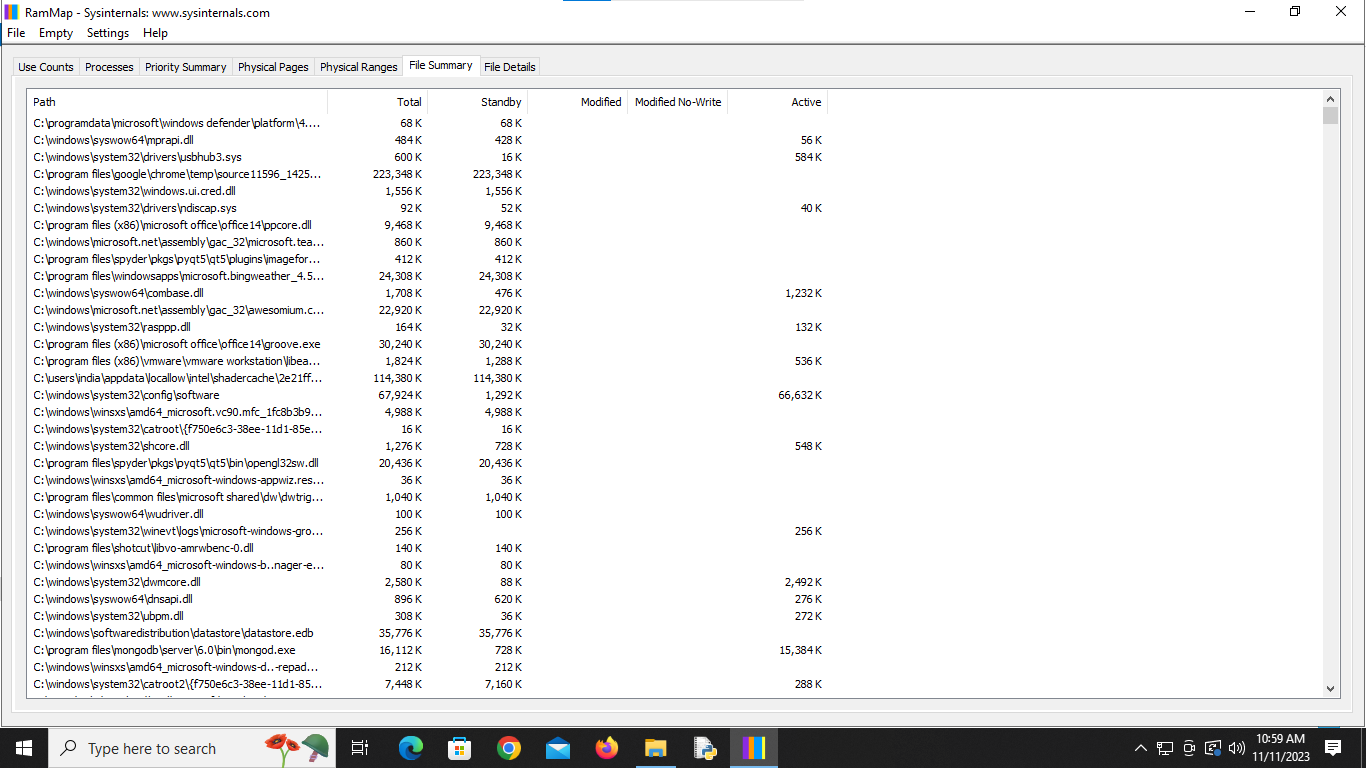
**Analysis RAM Map**



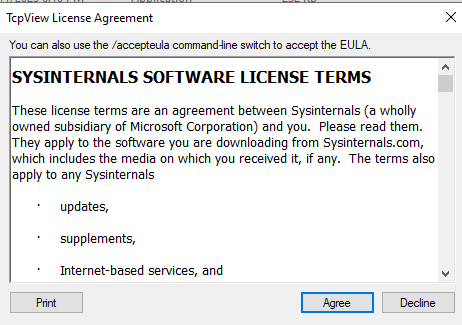
**RAM Map process**



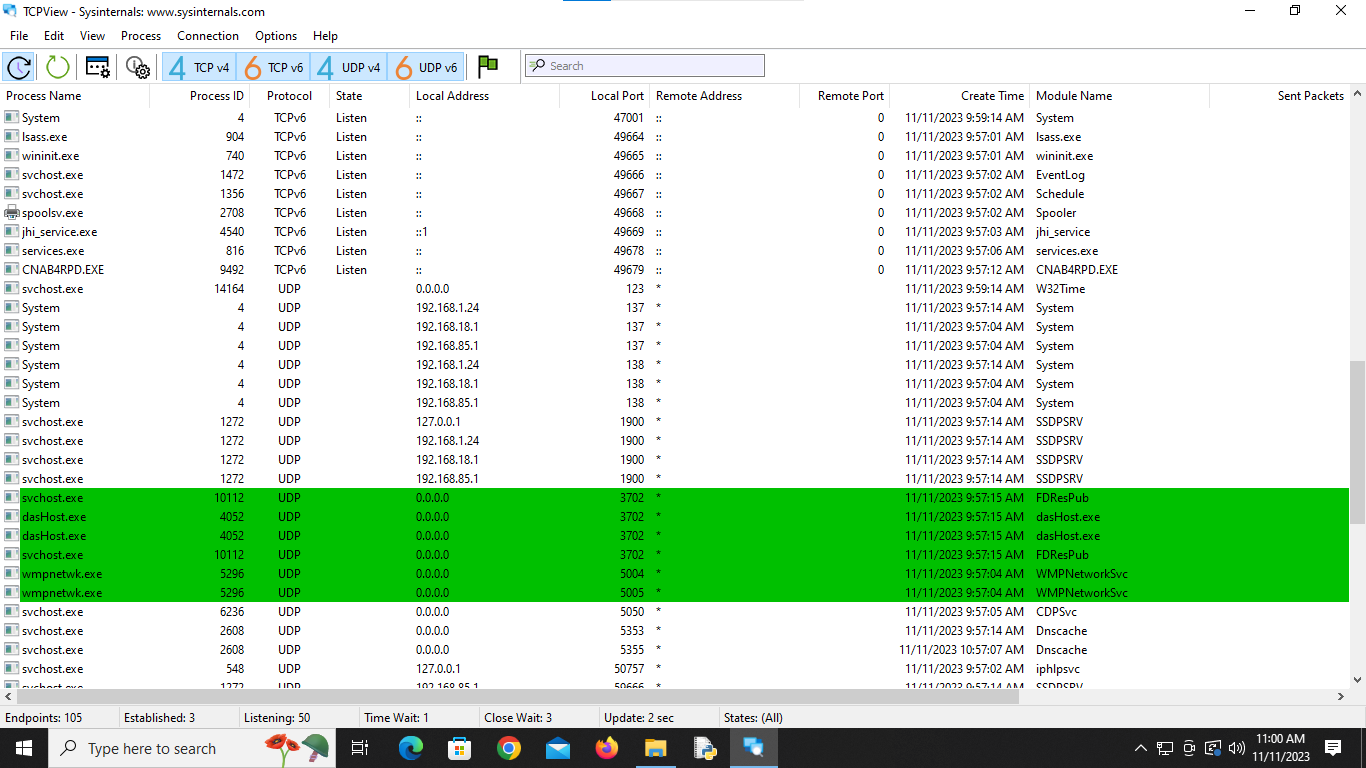
RAM Map file summary



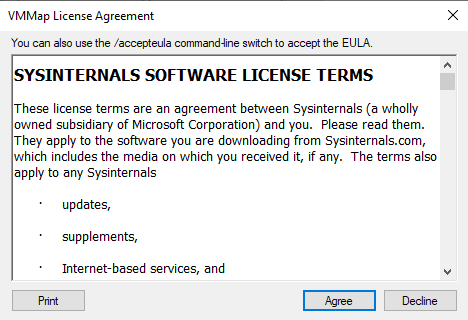
**TCP View**



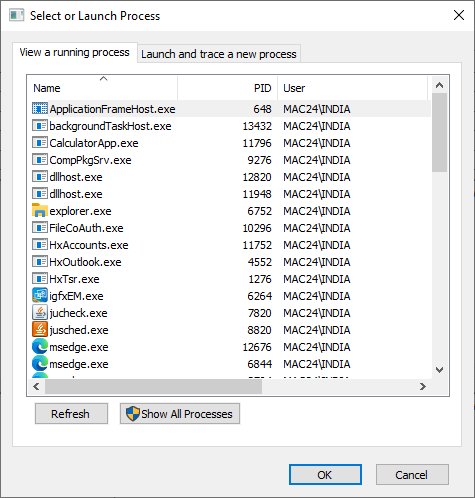
**Analysis TCP View**



**VM Map**



**Launch Process**



Analysis VM Map

