Date-28/10 /2023

Roll No. - 25

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 is a suite of utilities designed to help IT professionals and power users manage, diagnose, troubleshoot, and monitor Windows systems and applications. It was originally developed by Mark Russinovich and Bryce Cogswell and was acquired by Microsoft in 2006.

Windows Sysinternals has been developed with the aim of offering IT professionals a range of technical resources and utilities for efficiently managing, diagnosing, troubleshooting, and monitoring Windows systems. This comprehensive suite has gained significant recognition and appreciation within the IT professional community for its wide array of capabilities.

## ****Categories of Sysinternals Suite****

1. **File and Disk:** This category offers utilities that monitor file usage and disk status. Notably, Process Monitor is a highly regarded tool in this section as it provides real-time monitoring of activities in the file system, registry, and processes.
2. **Networking**: Here, you can find applications designed to troubleshoot and monitor connections on both desktop and server systems. TCPView, a tool for checking TCP and UDP endpoints, and PS Tools, a set of command-line utilities facilitating remote system monitoring and management, are among the popular choices in this category.
3. **Process:** This section contains utilities that aid in monitoring and troubleshooting running applications. Process Explorer, a well-known tool within this category, allows users to track the files and directories accessed by a specific process.
4. **Security:** The Security category hosts utilities focused on security-related tasks. For instance, Autoruns is a valuable tool that reveals the applications configured to start automatically during system boot-up, assisting in identifying potential security risks.
5. **System Information:** Applications in this category provide general information about workstations or servers, aiding in understanding system configurations and capabilities.
6. **Miscellaneous:** This section encompasses utilities that do not fit neatly into the other categories and typically offer limited diagnostic or troubleshooting capabilities. BgInfo is an example of a popular download in this category, which creates a background image displaying essential system configuration details like the IP address and computer name.

**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.

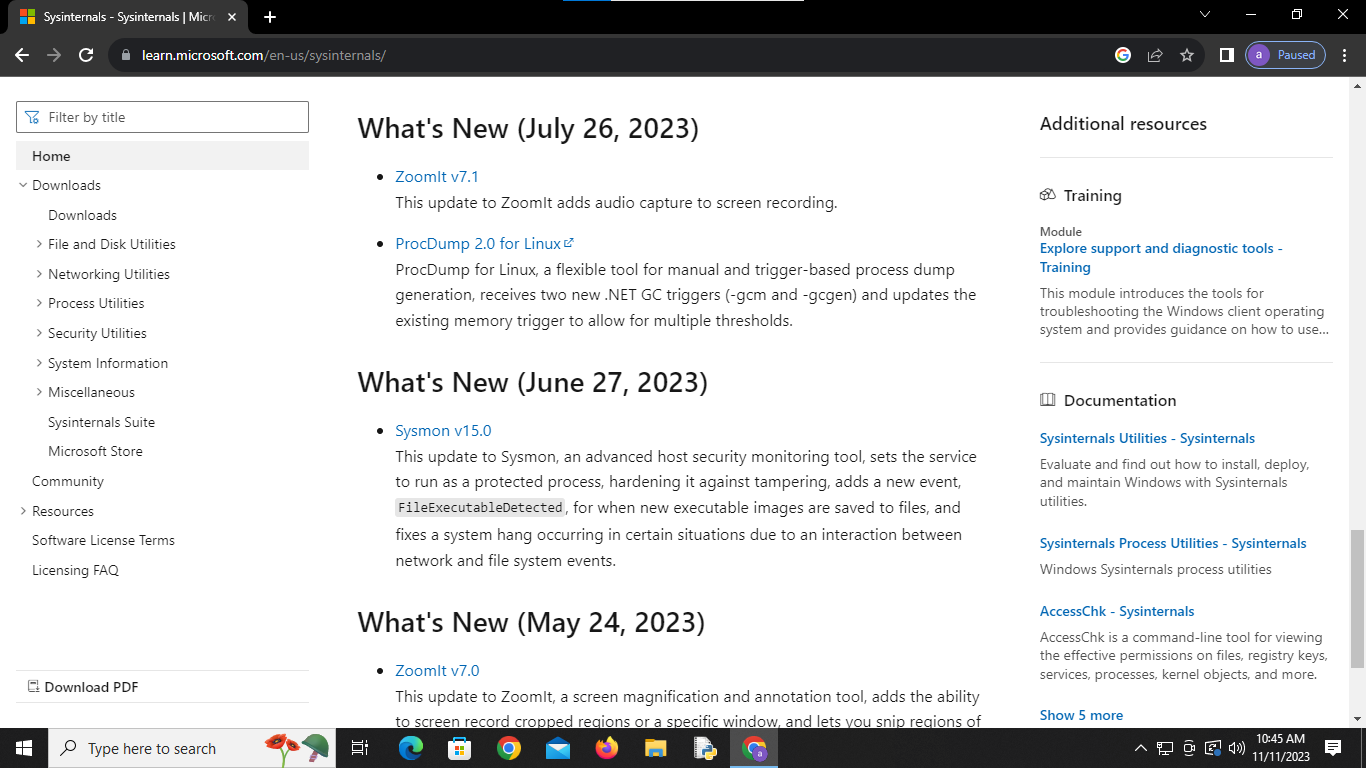
**TCP View**

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.

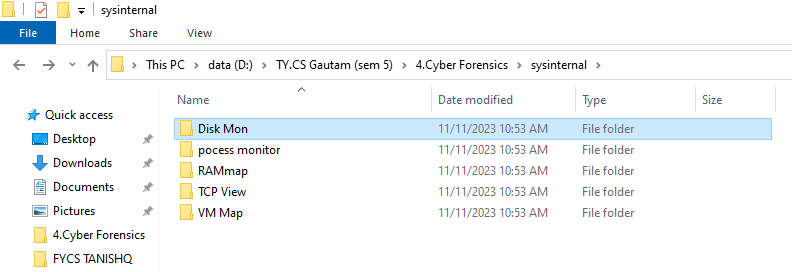
**VM Map**

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.

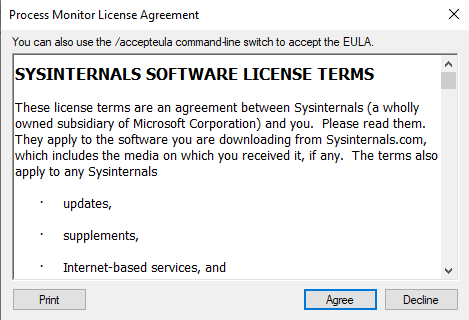
**Sysinternals tools Download**



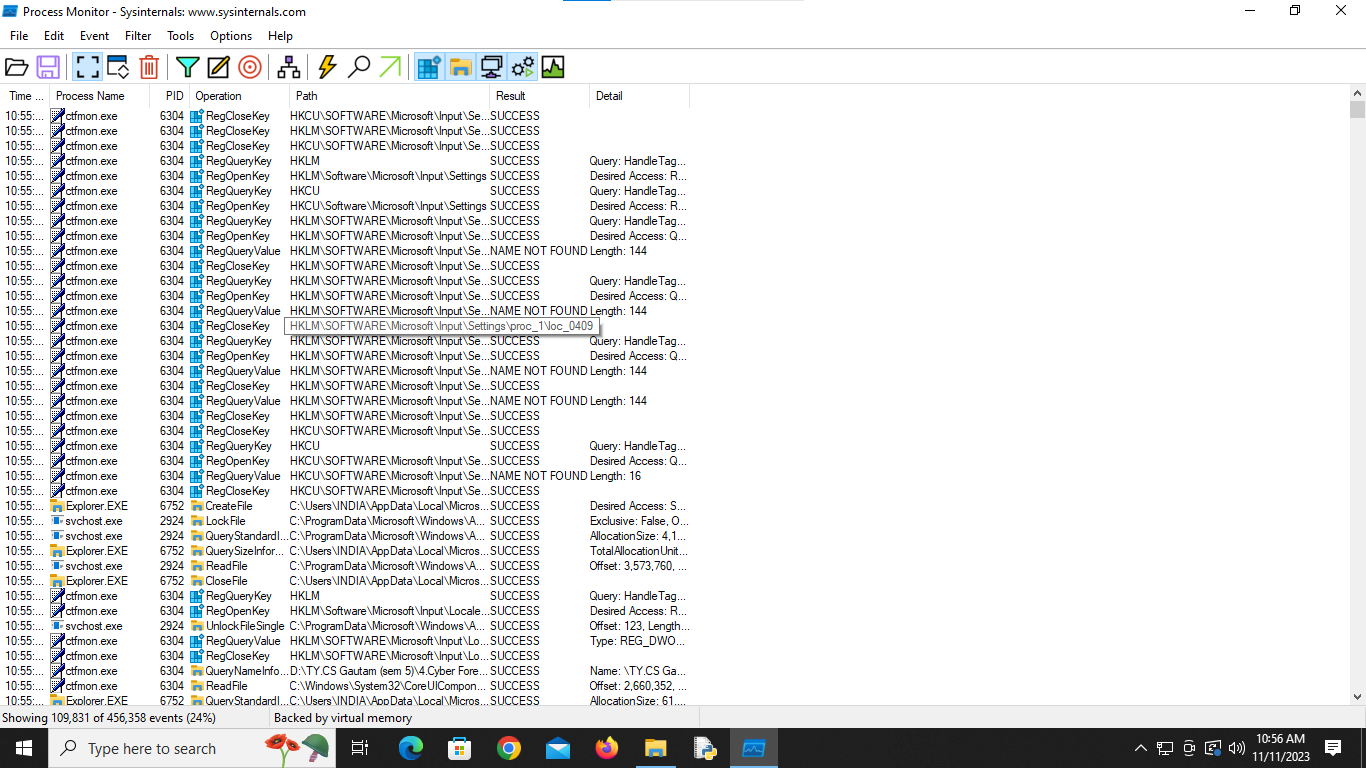
**Download Tools**



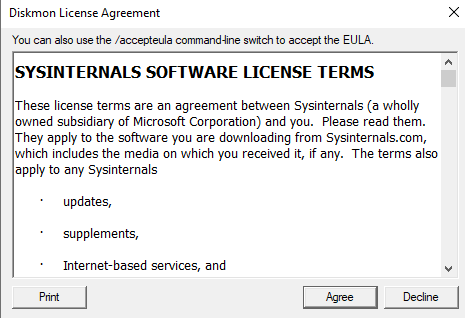
**Process Monitor**



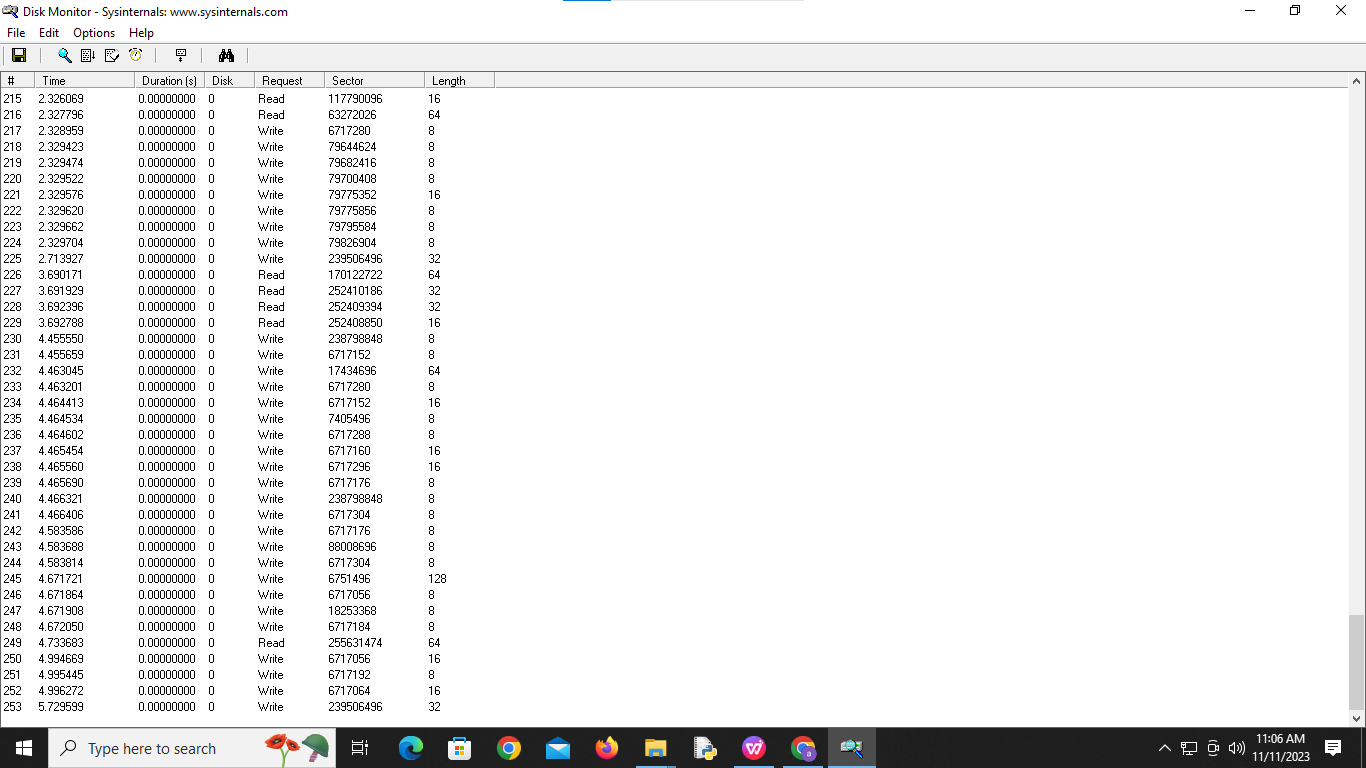
**Analysis of Process monitor**



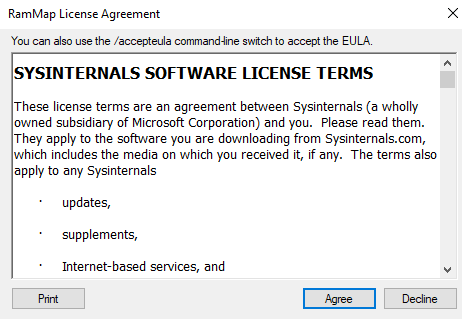
**Disk Monitor**



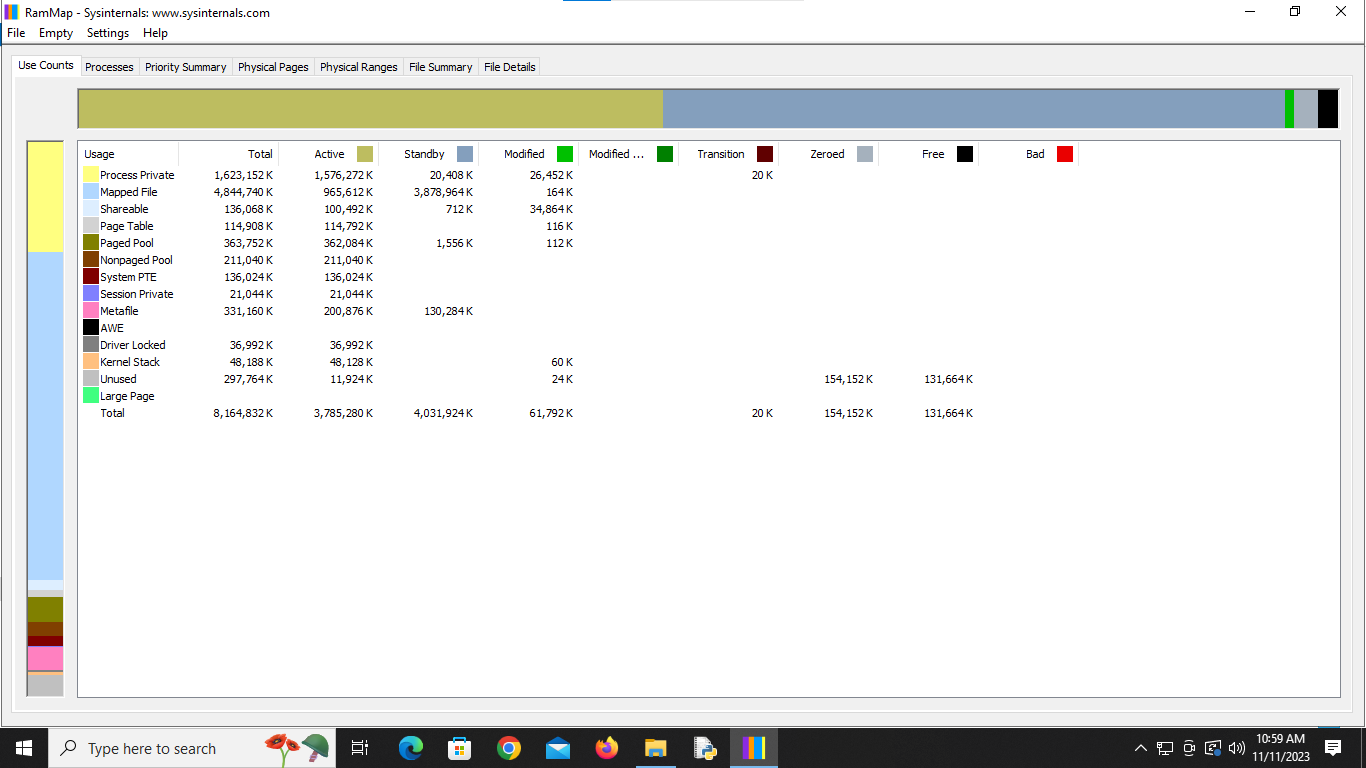
**Disk Mon**



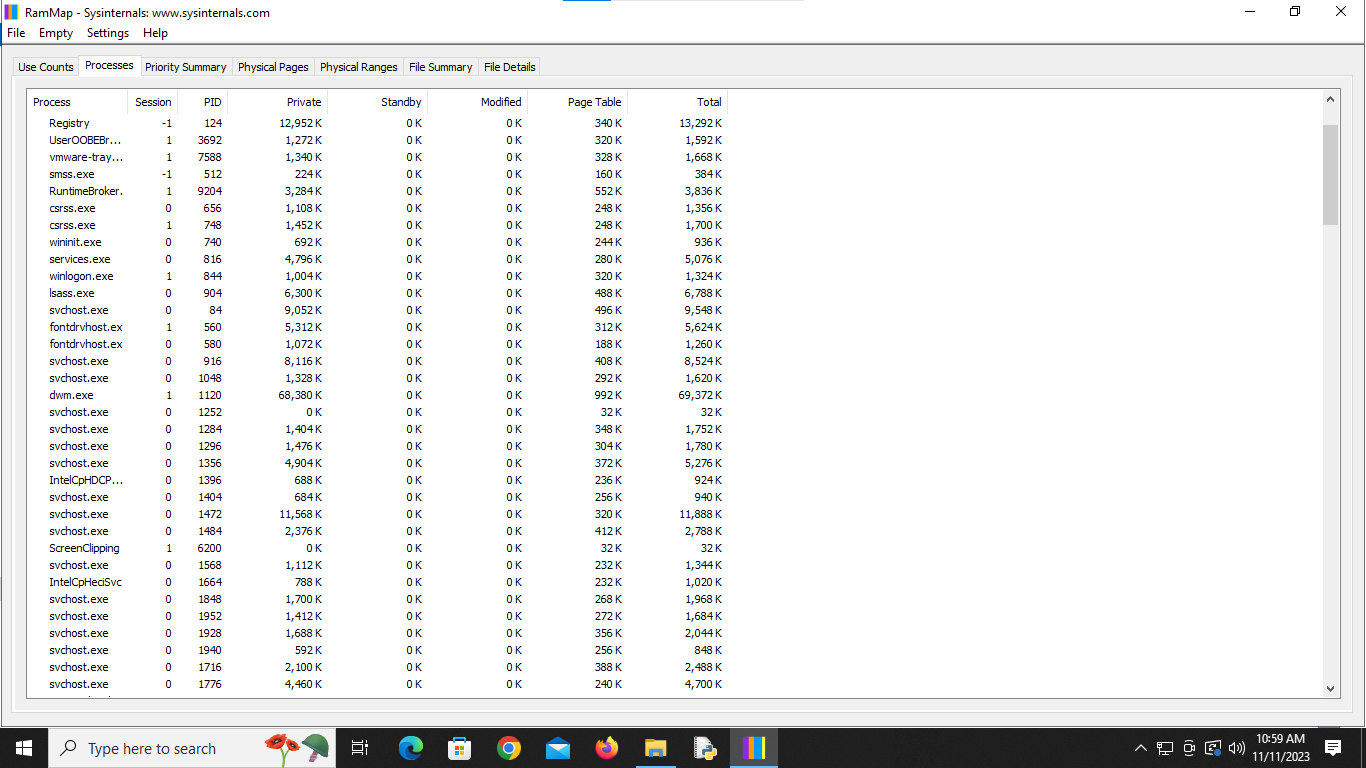
**RAM Map**



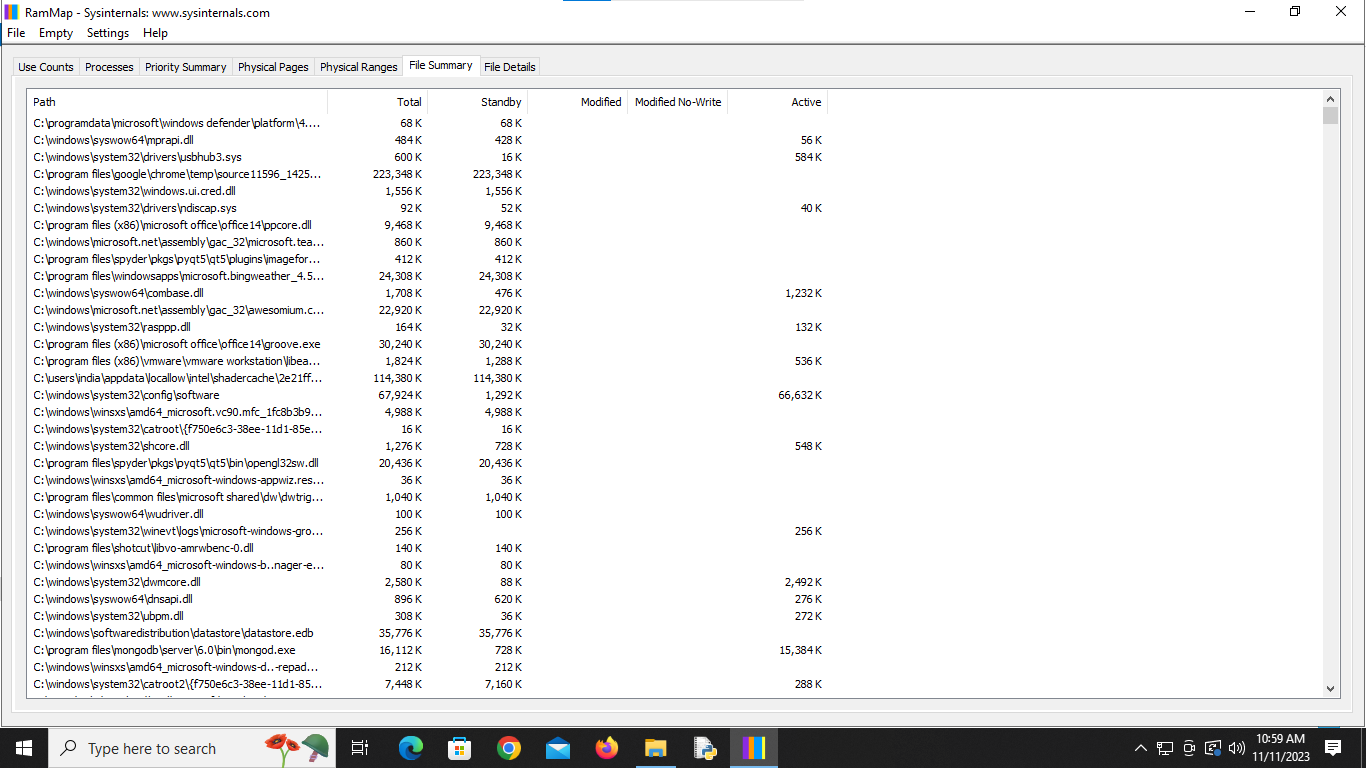
**Analysis RAM Map**



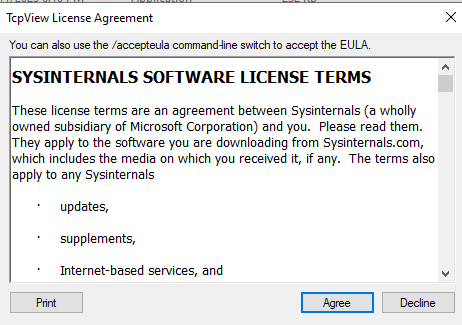
**RAM Map process**



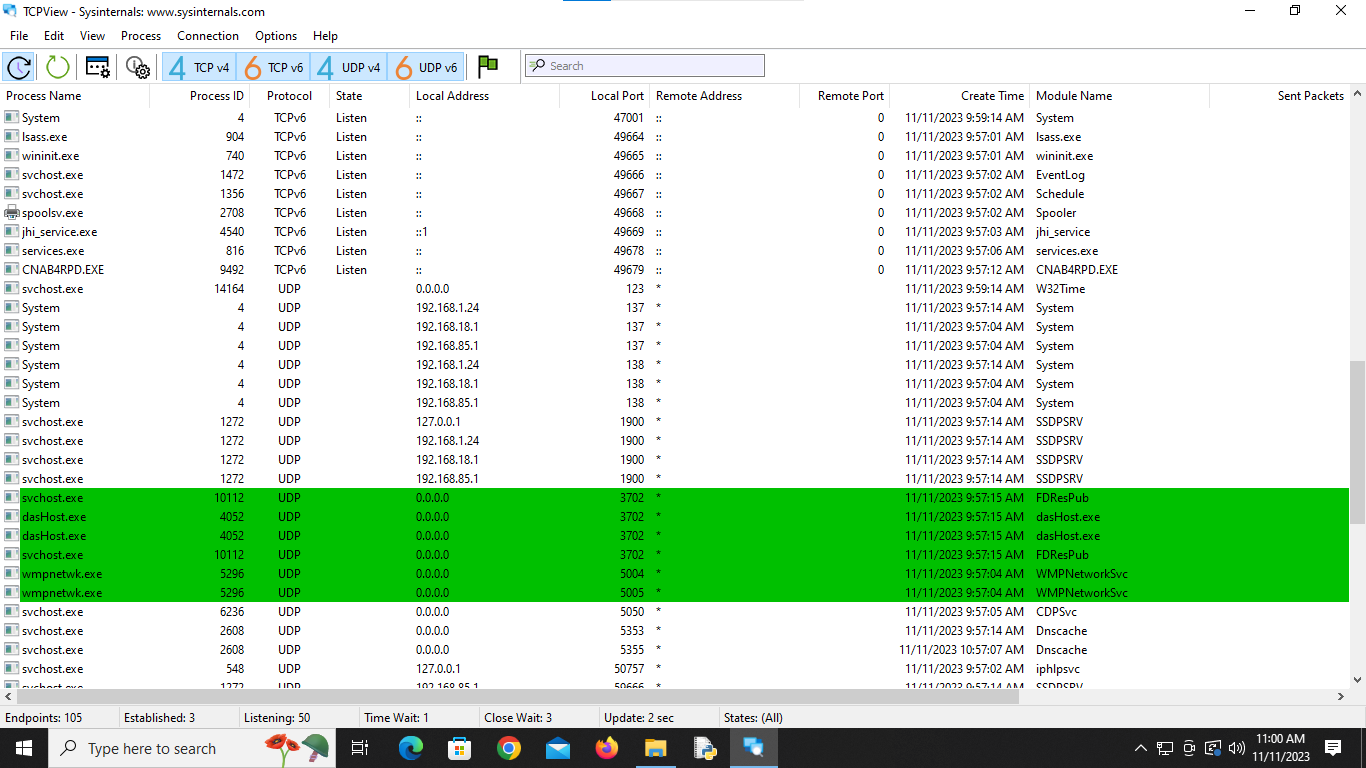
RAM Map file summary



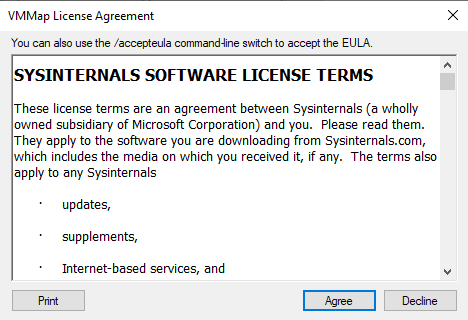
**TCP View**



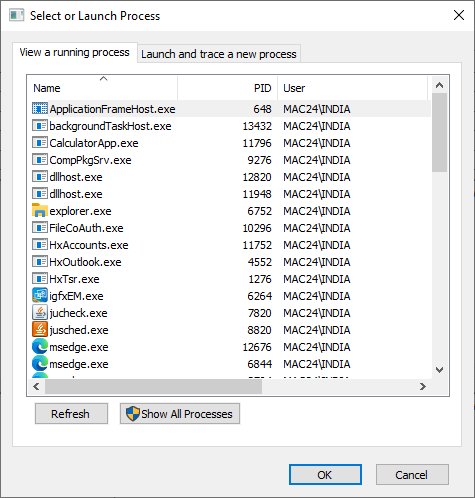
**Analysis TCP View**



**VM Map**



**Launch Process**



Analysis VM Map

