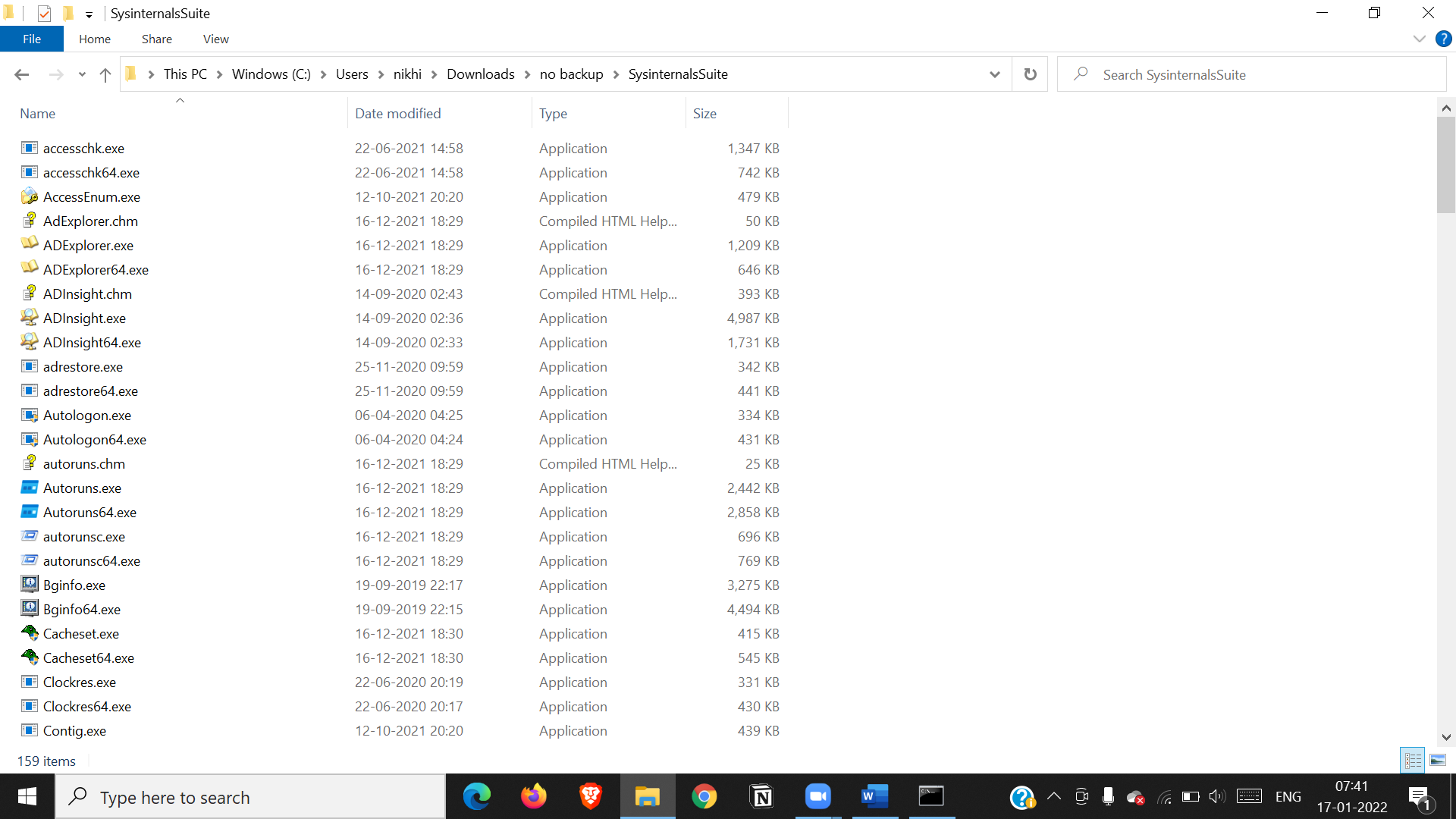
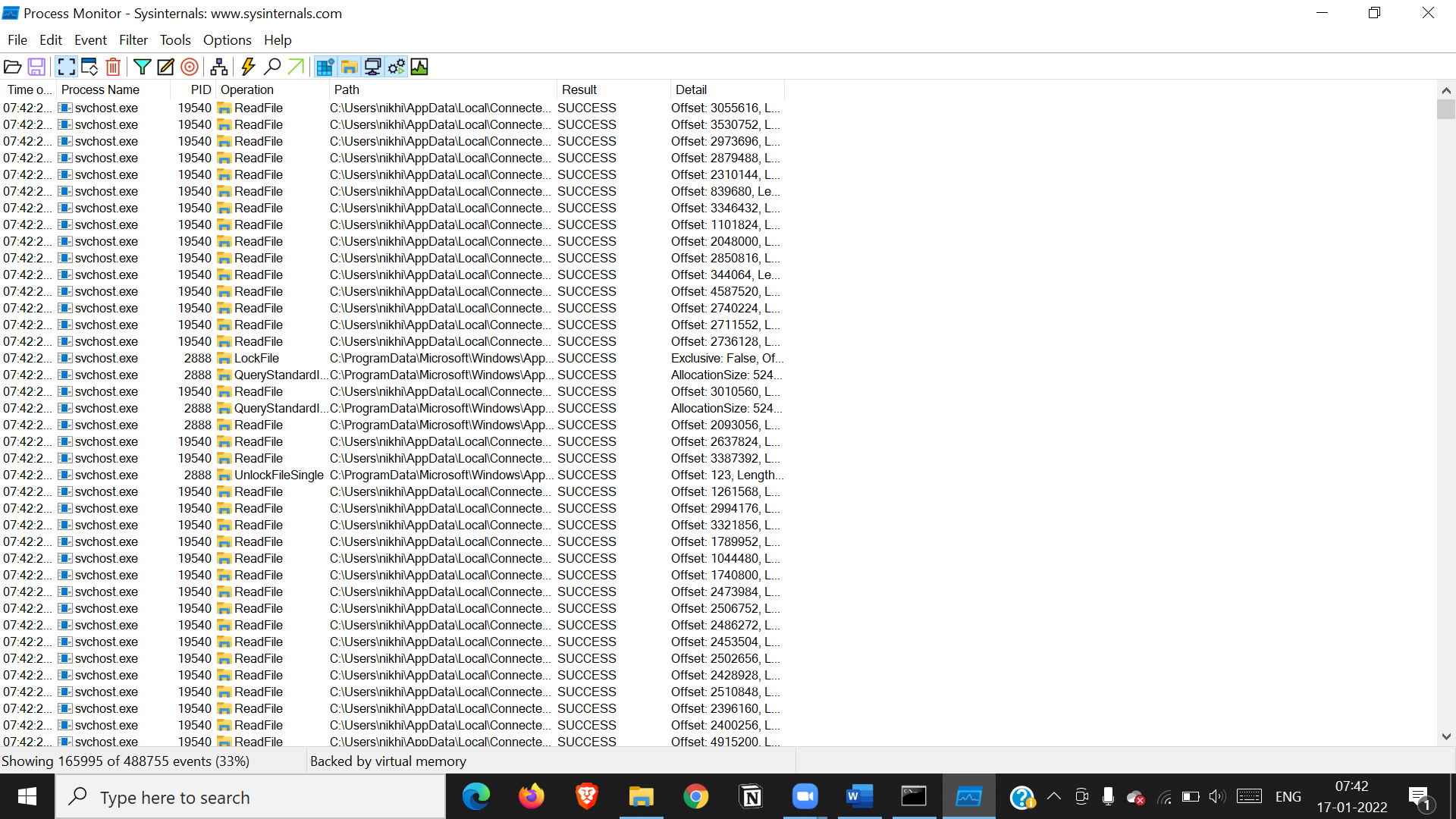
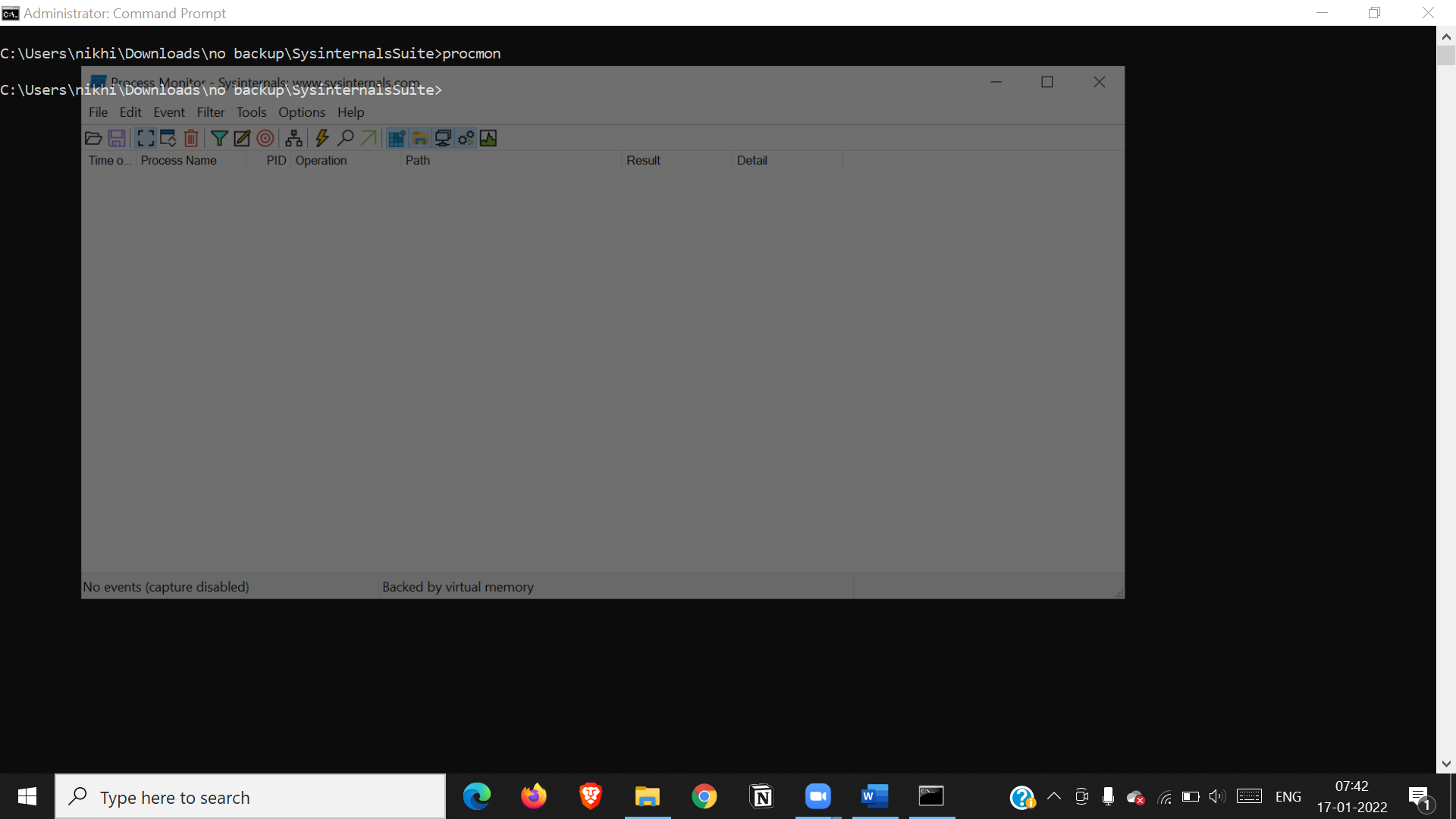
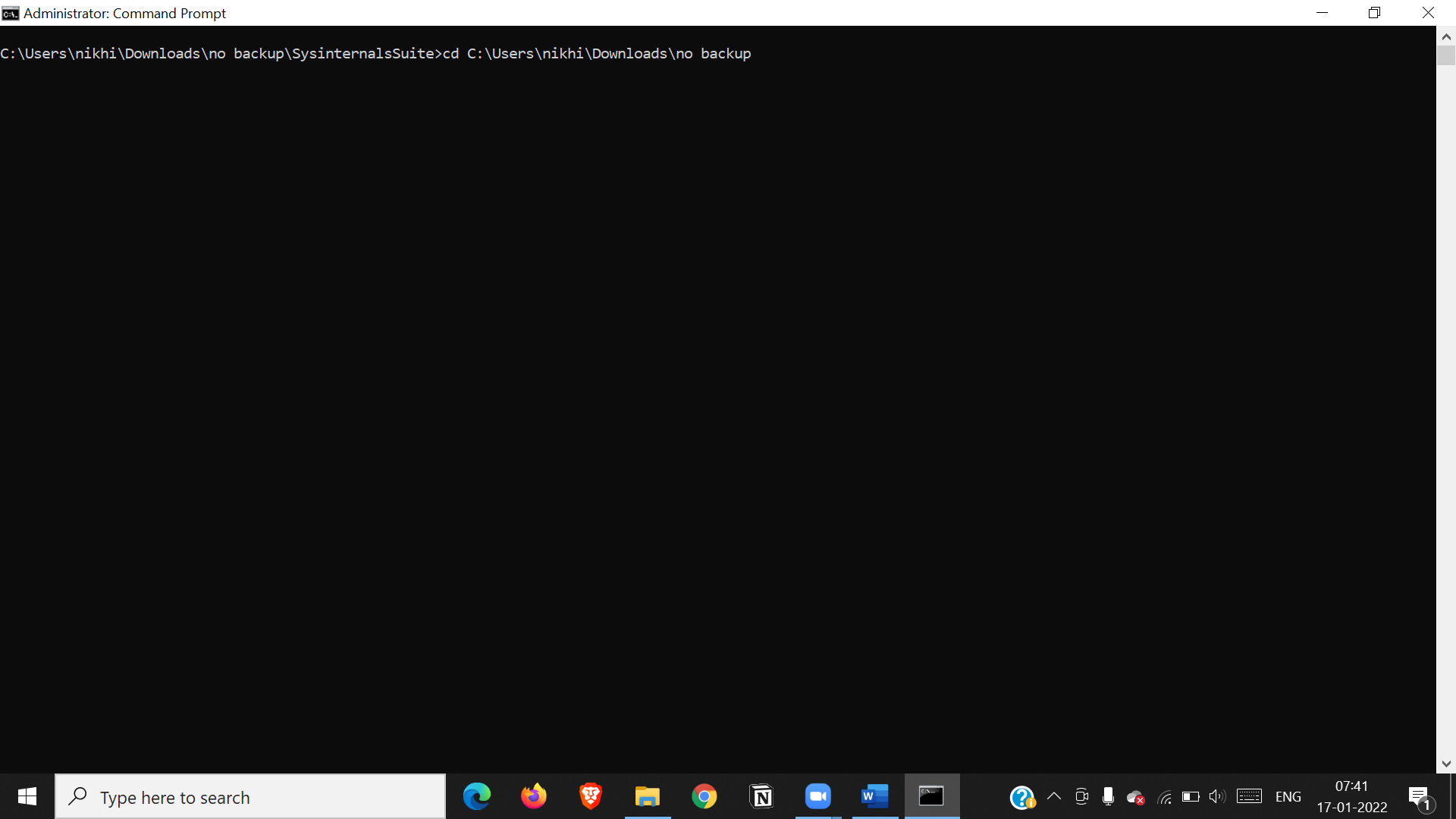
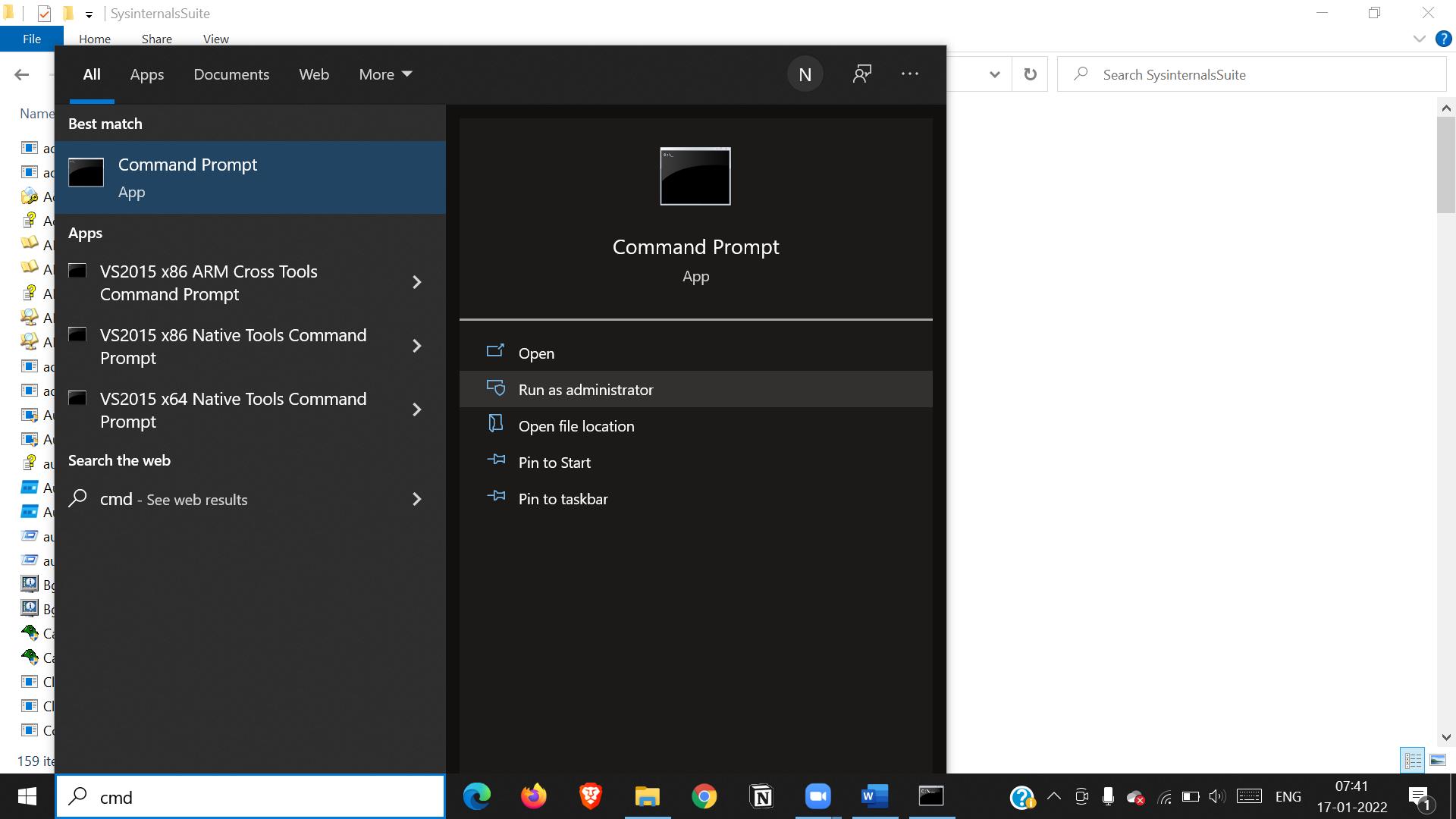
**AIM: Using Sysinternals tools for Network Tracking and Process Monitoring : - Check Sysinternals tools - Monitor Live Processes - Capture RAM - Capture TCP/UDP packets - Monitor Hard Disk - Monitor Virtual Memory - Monitor Cache Memory**

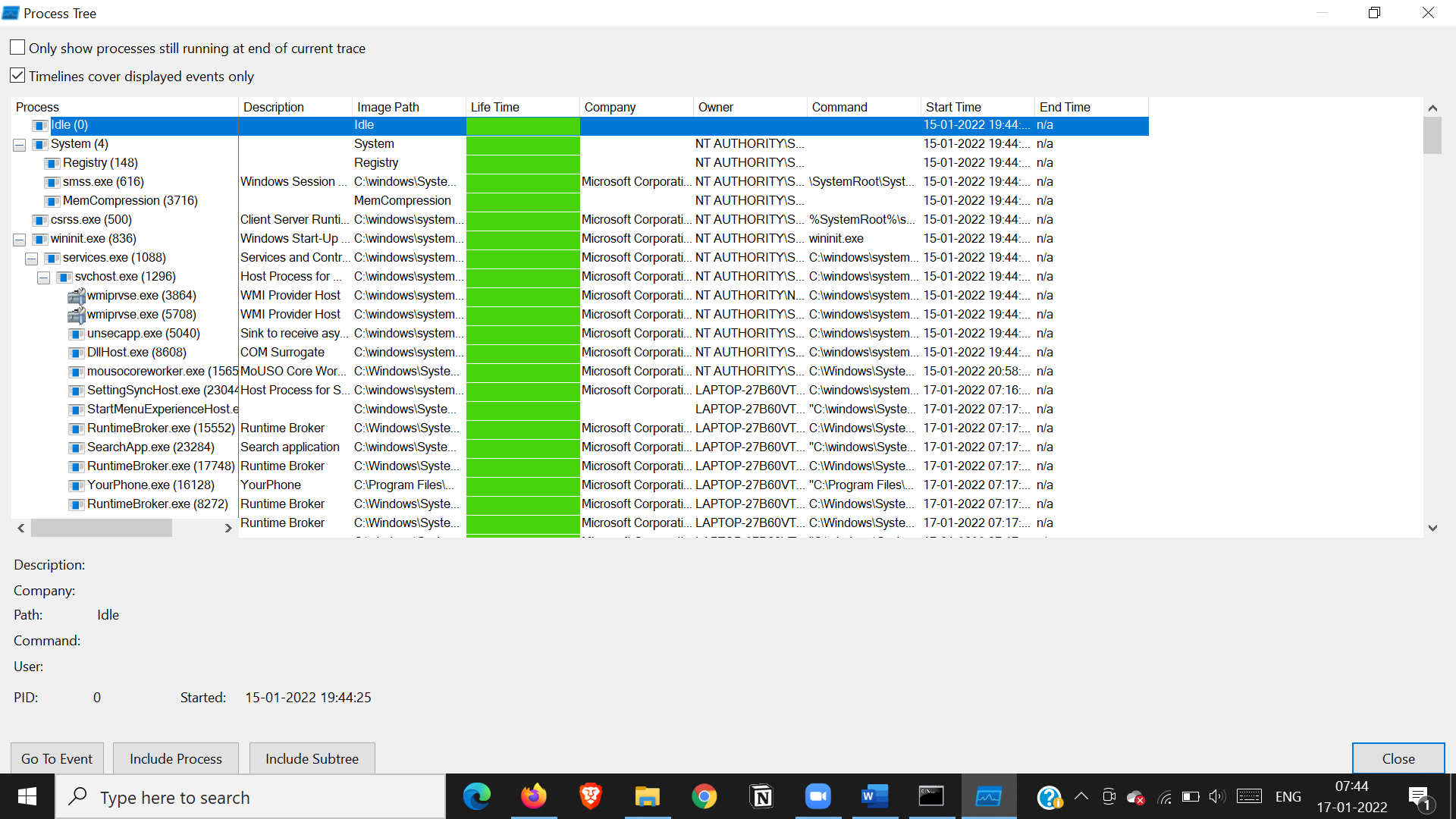
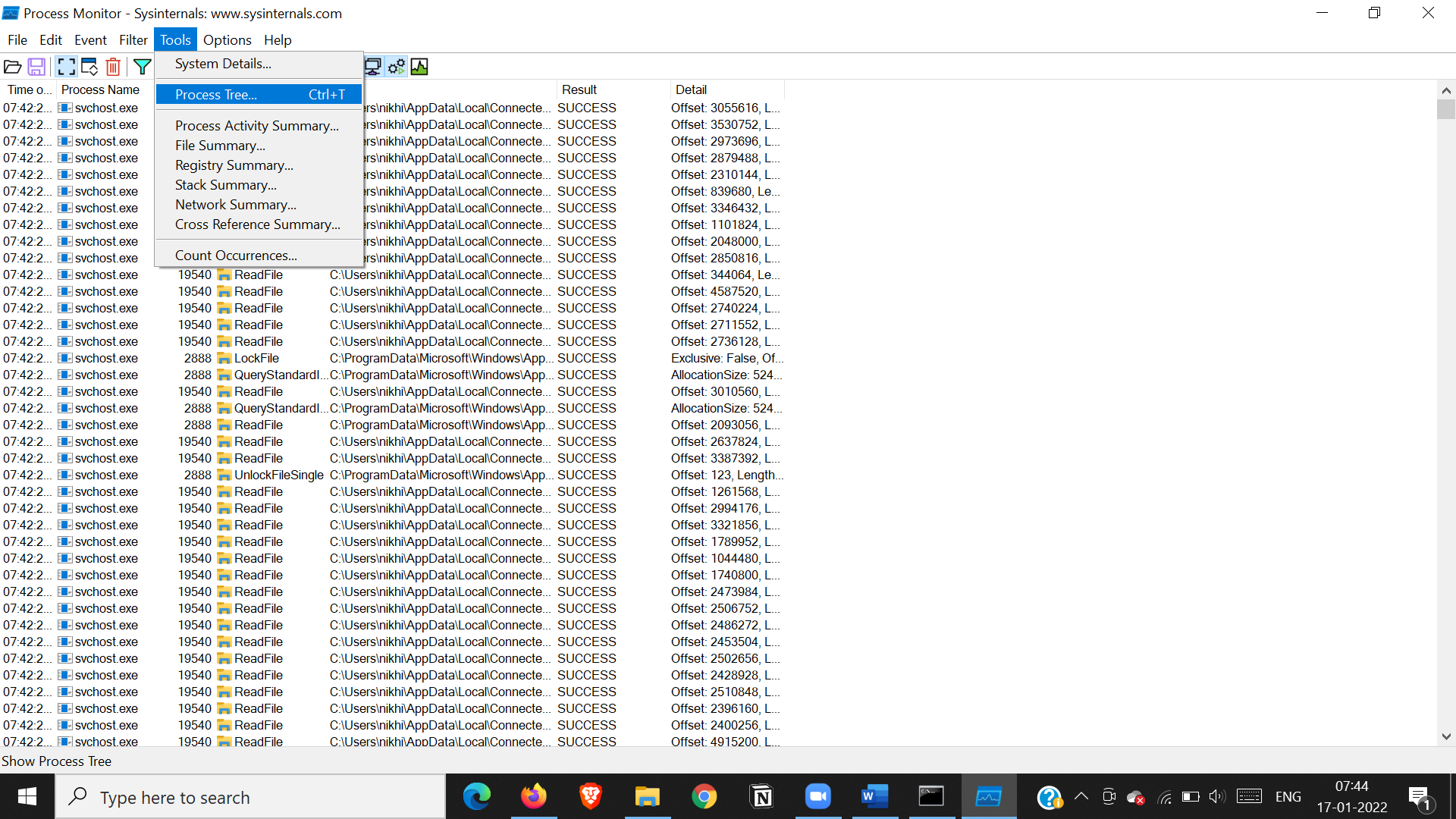
Sysinternal tools

The SysInternals suite of tools is simply a set of Windows applications that can be downloaded for free from their section of the Microsoft Technet web site. They are all portable, which means that not only do you not have to install them, you can stick them on a flash drive and use them from any PC

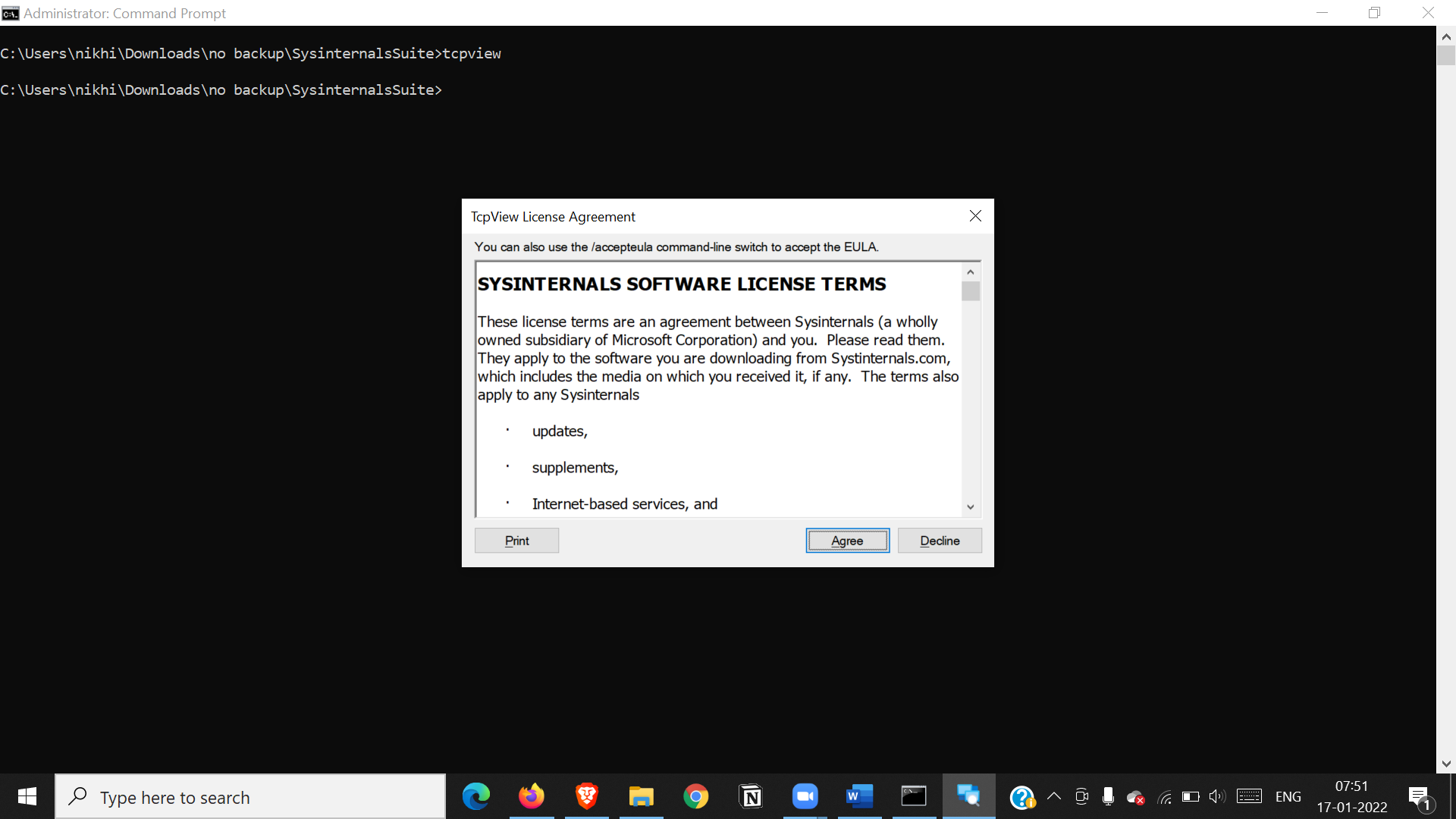
The Sysinternals tools are divided into six categories: File and Disk Utilities, Networking Utilities, Processes Utilities, Security Utilities, System Information and Miscellaneous Utilities. There are many tools, but the widely known are AutoRuns, Process Monitor, Process Explorer, TCPView and RootkitRevealer.

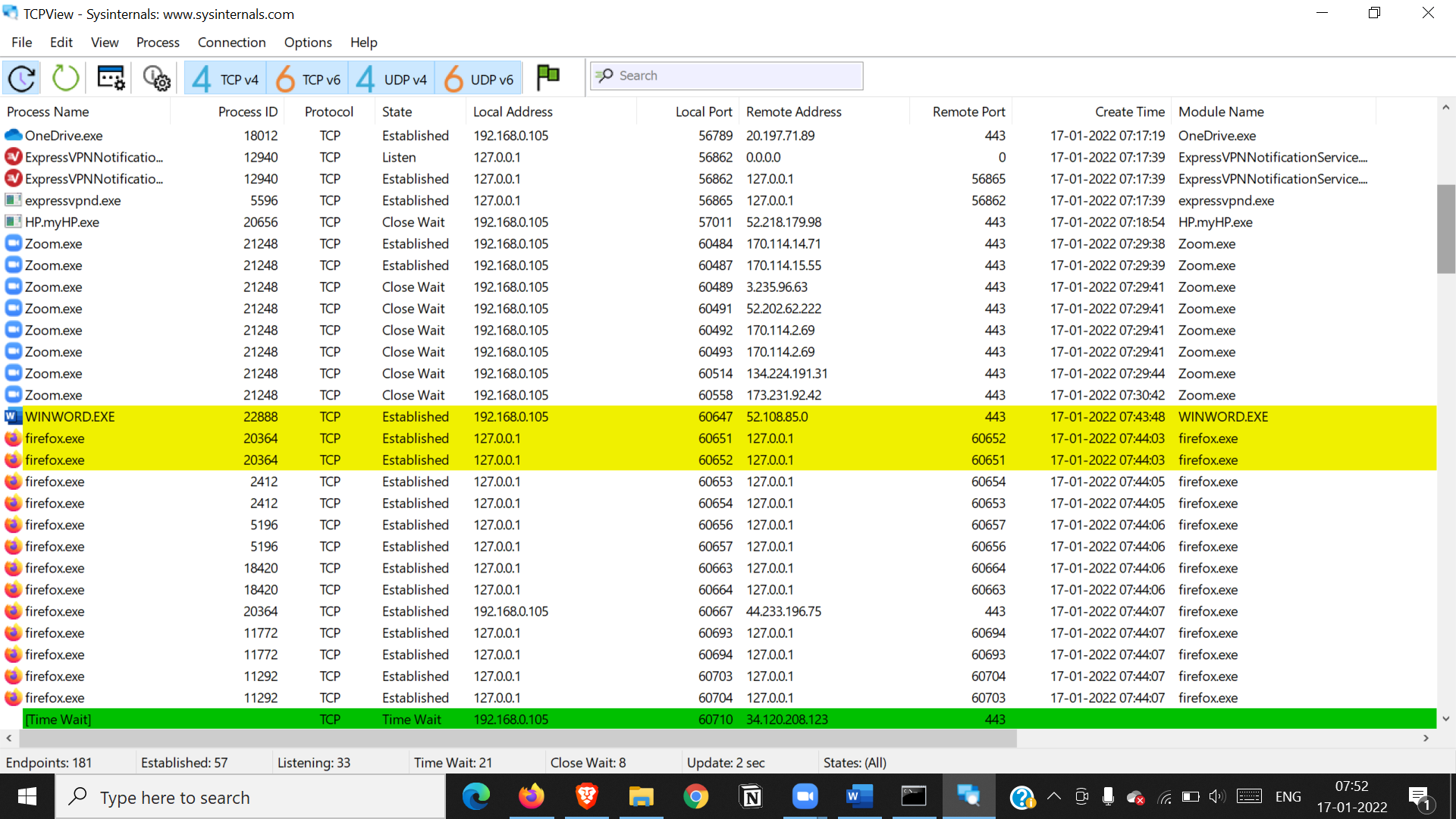




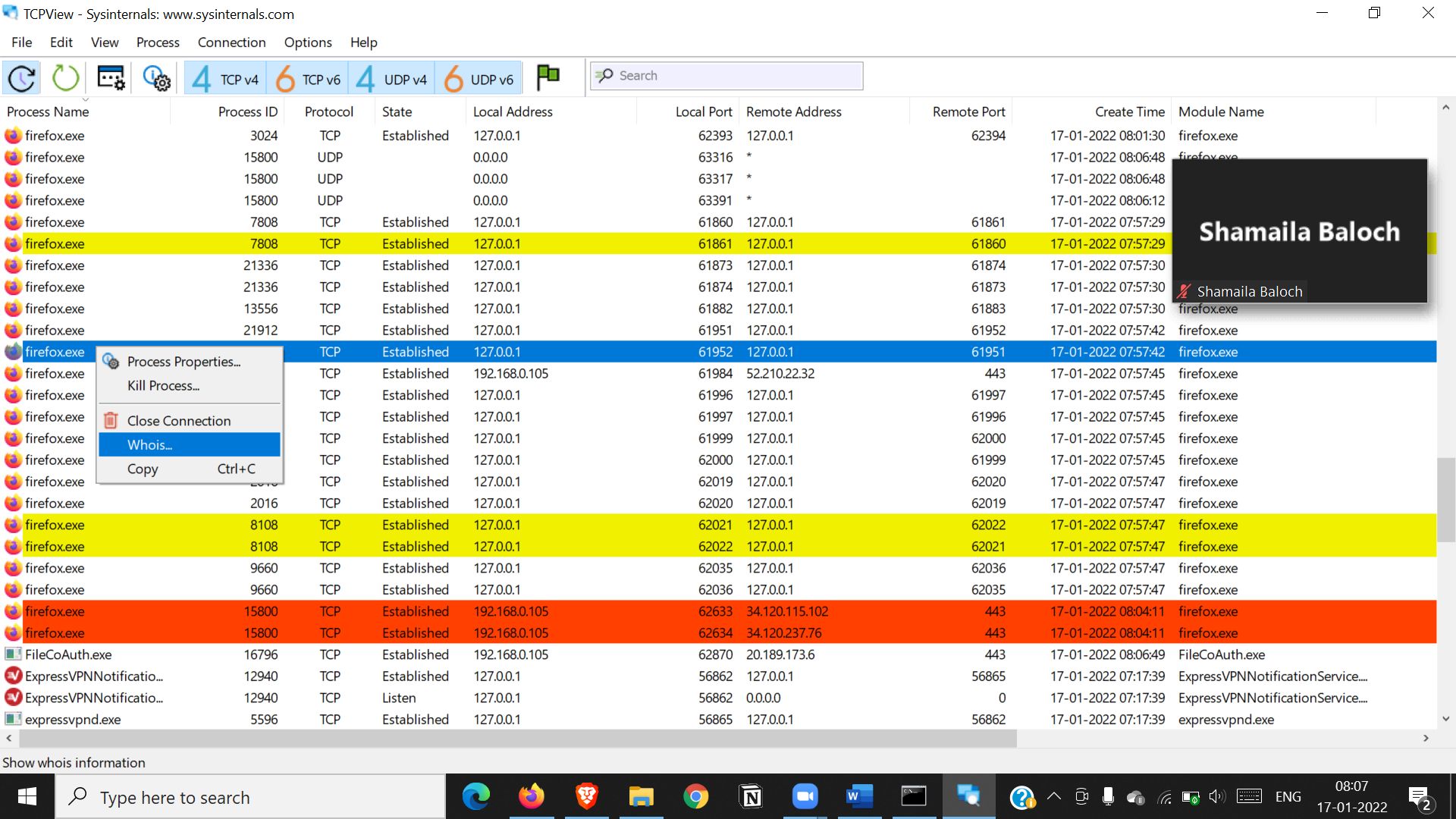


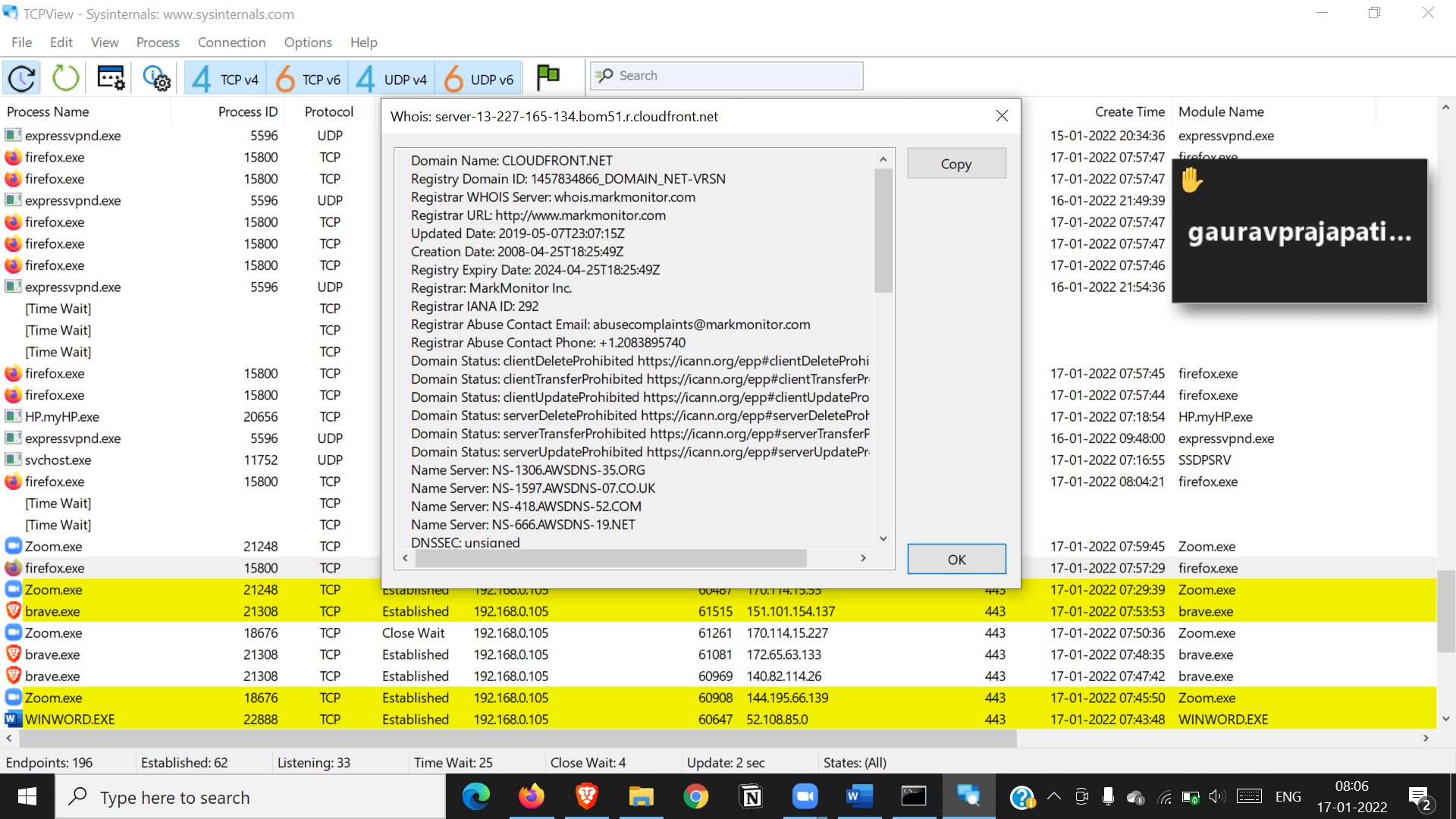
Tcp -udp packets



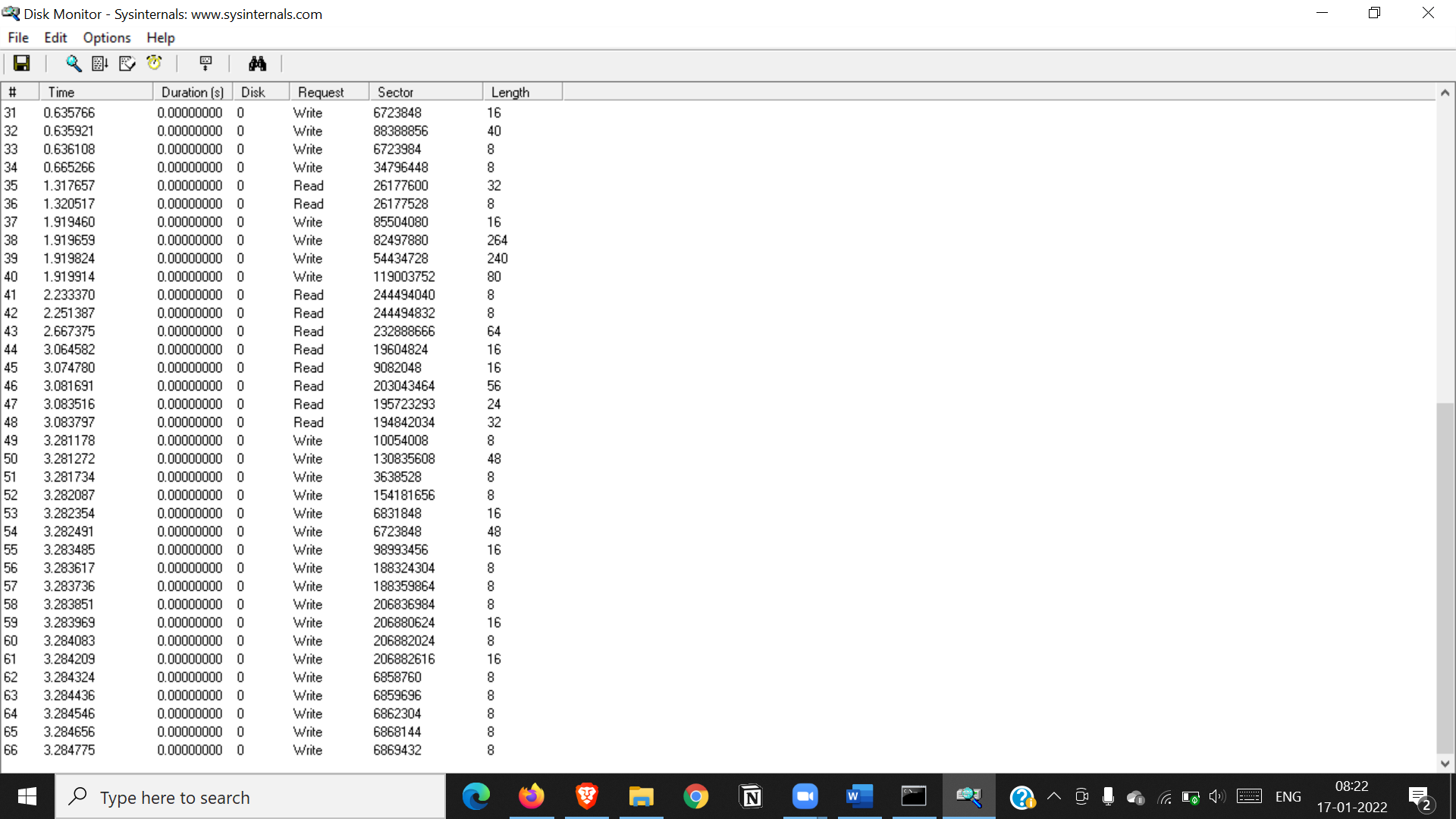
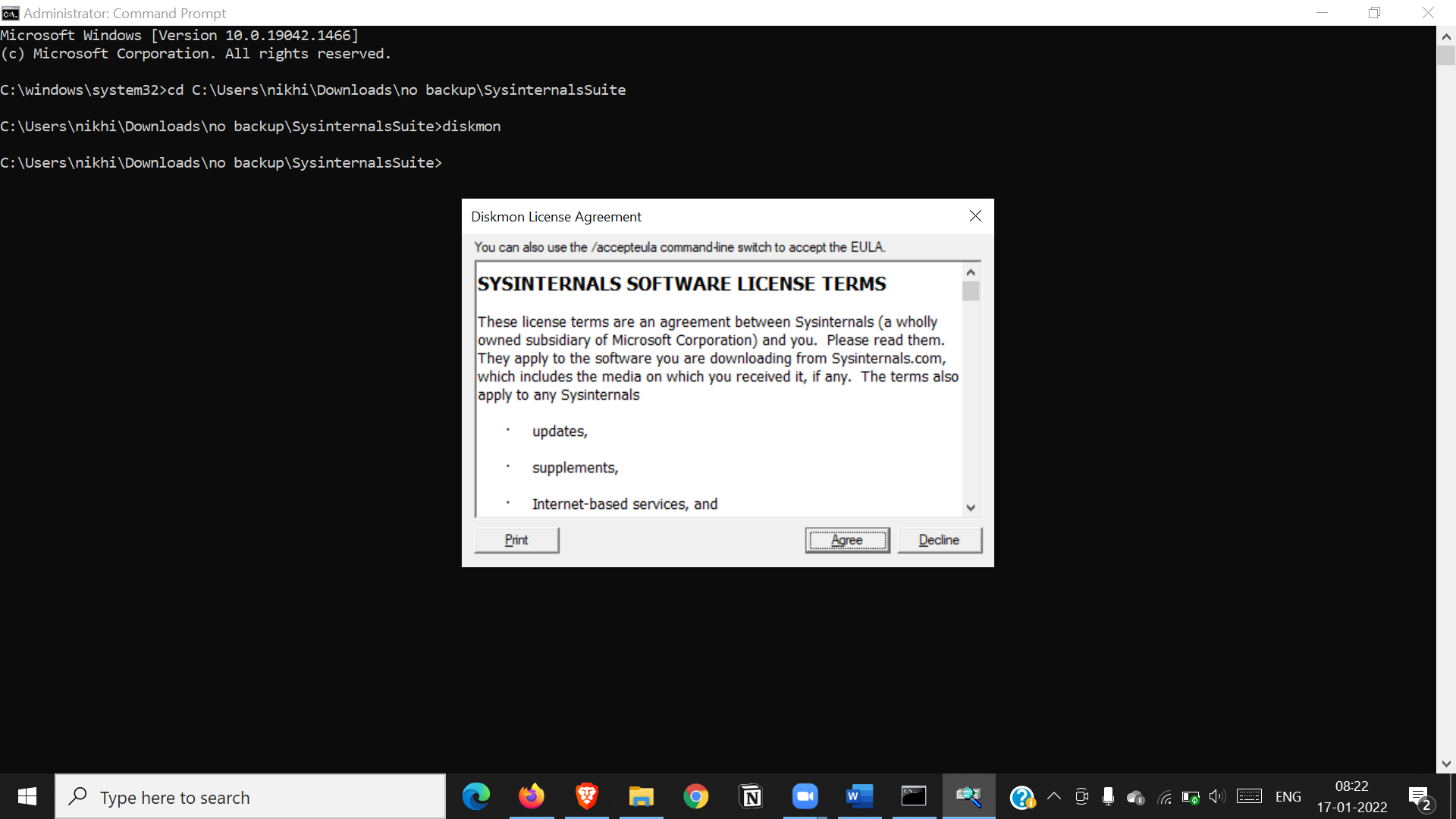


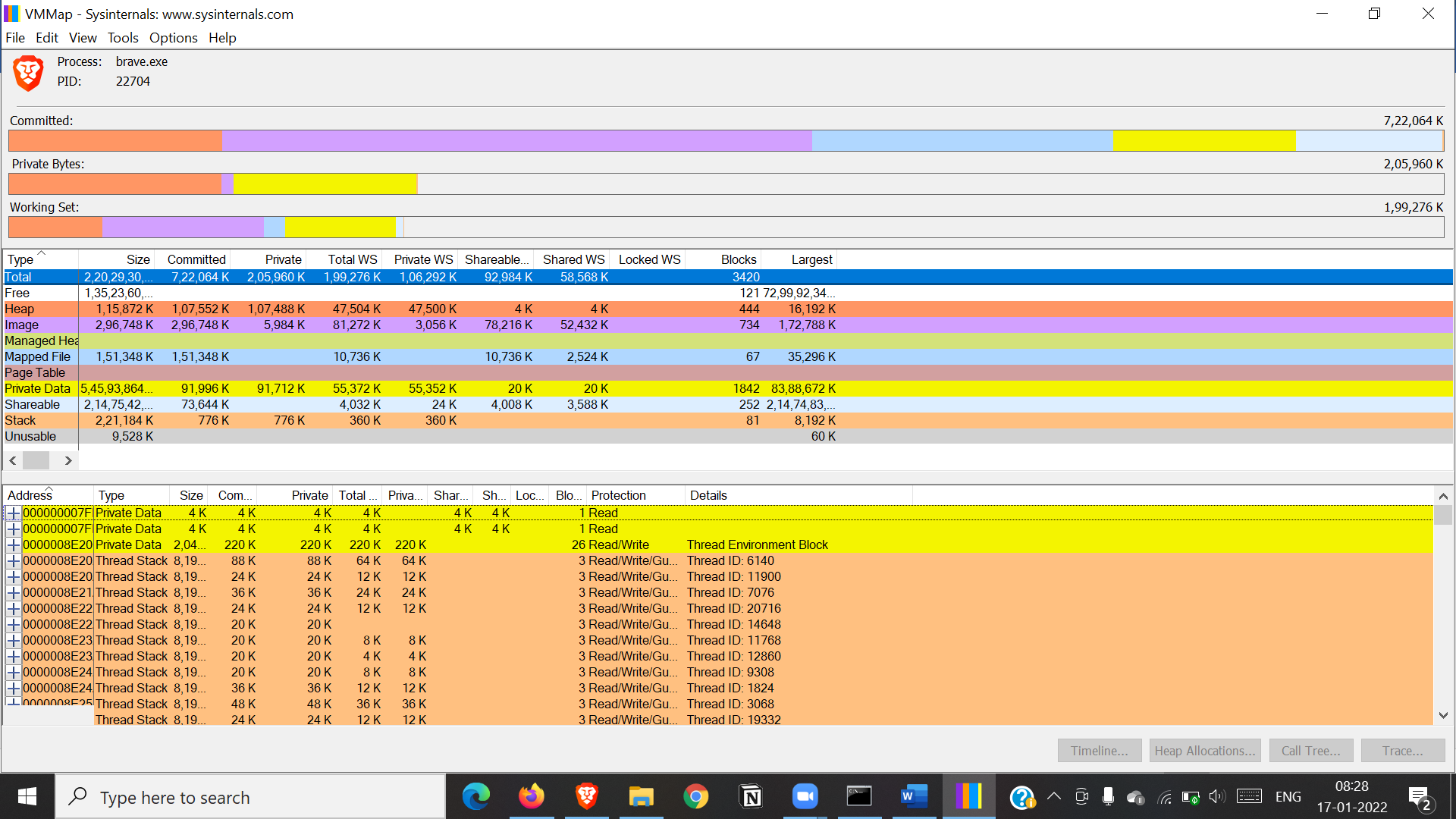
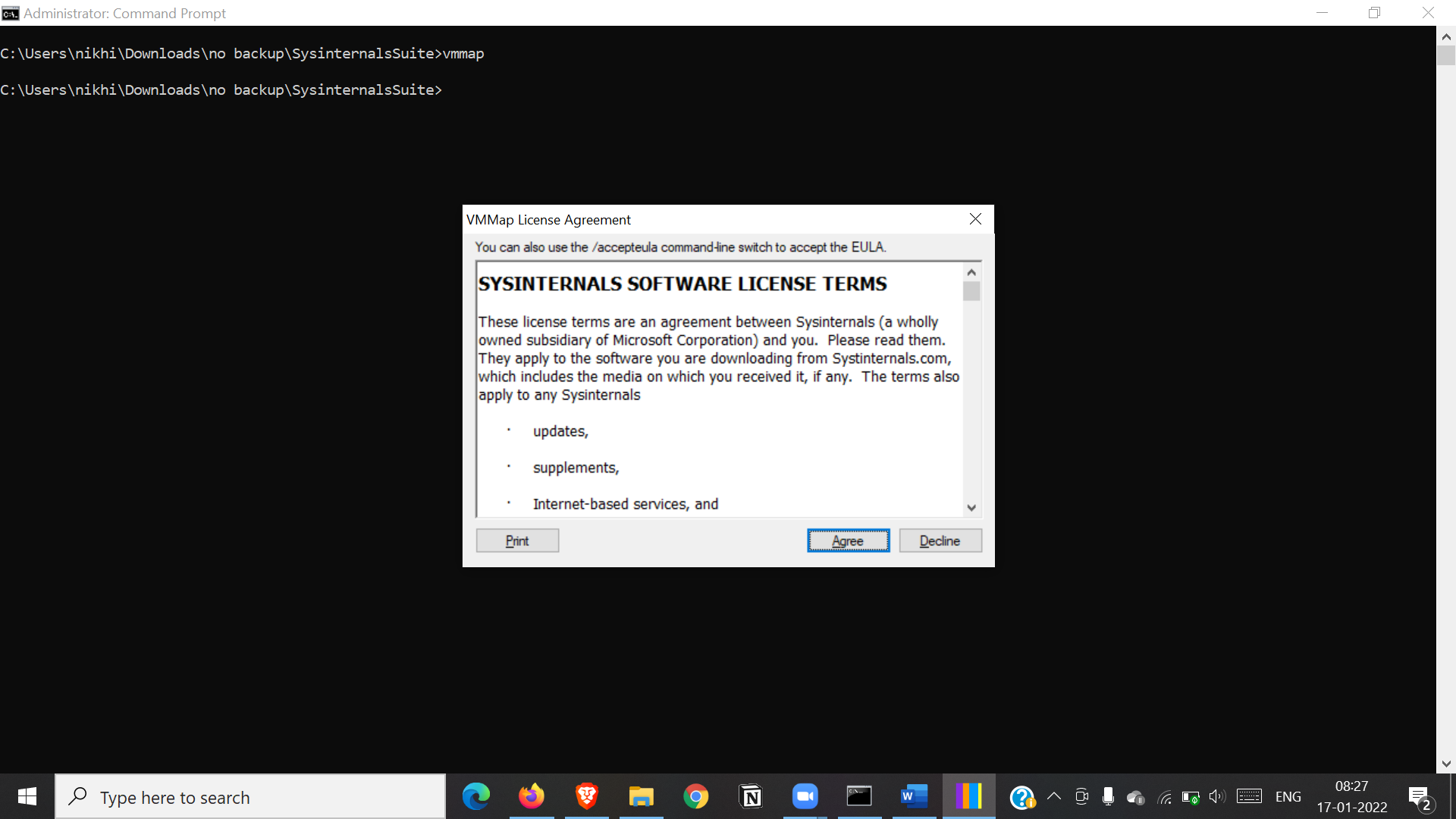




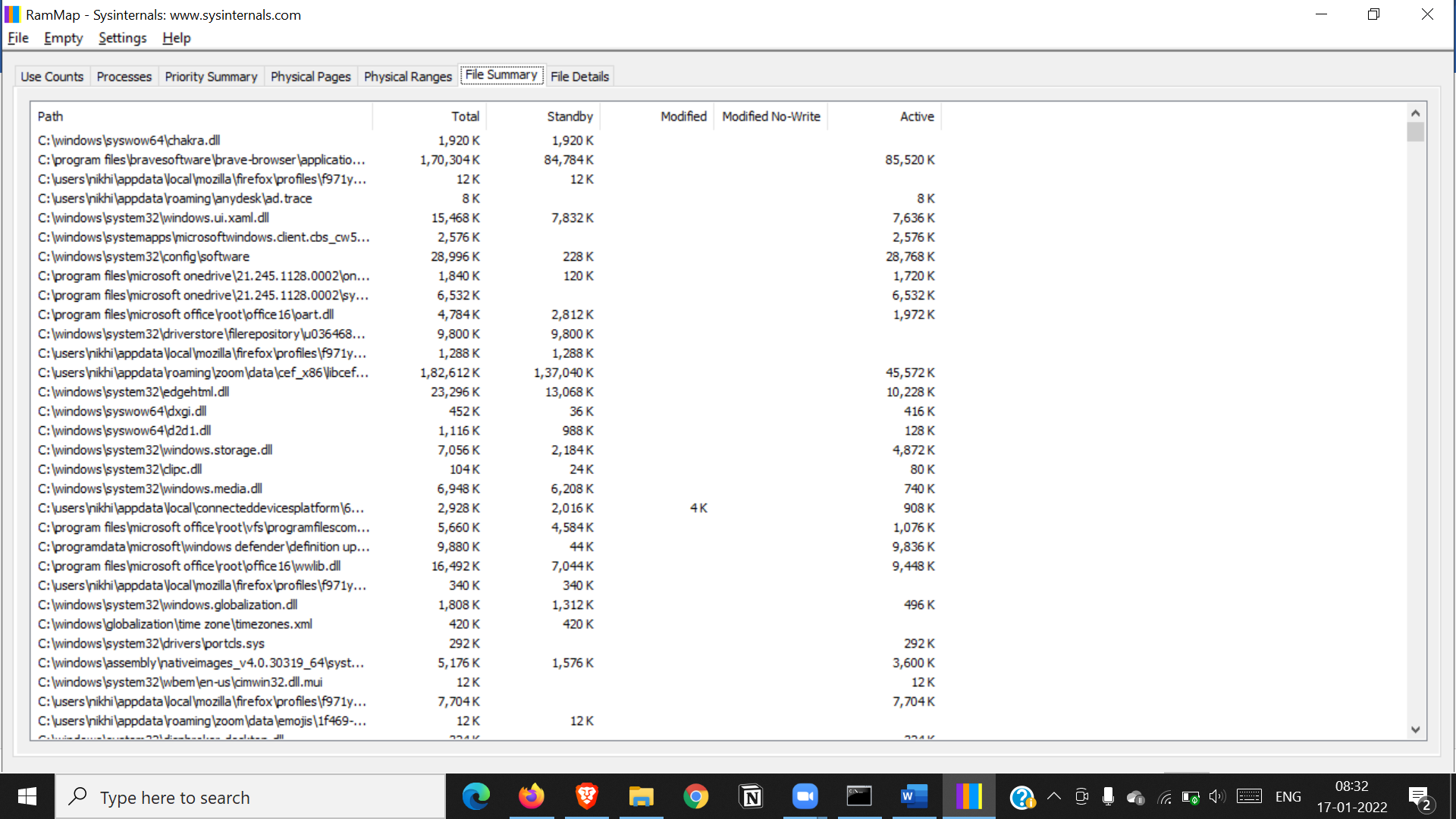
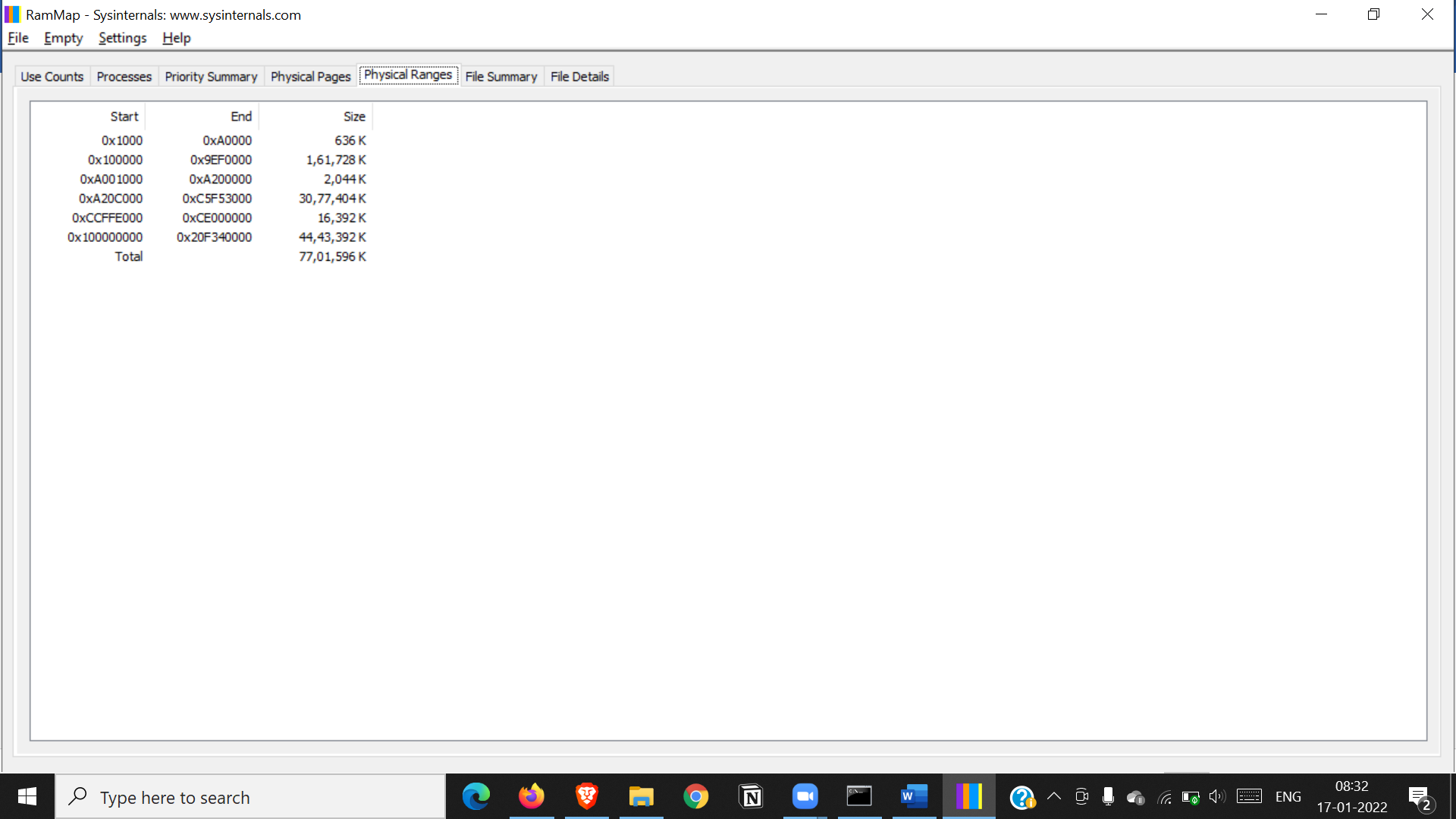
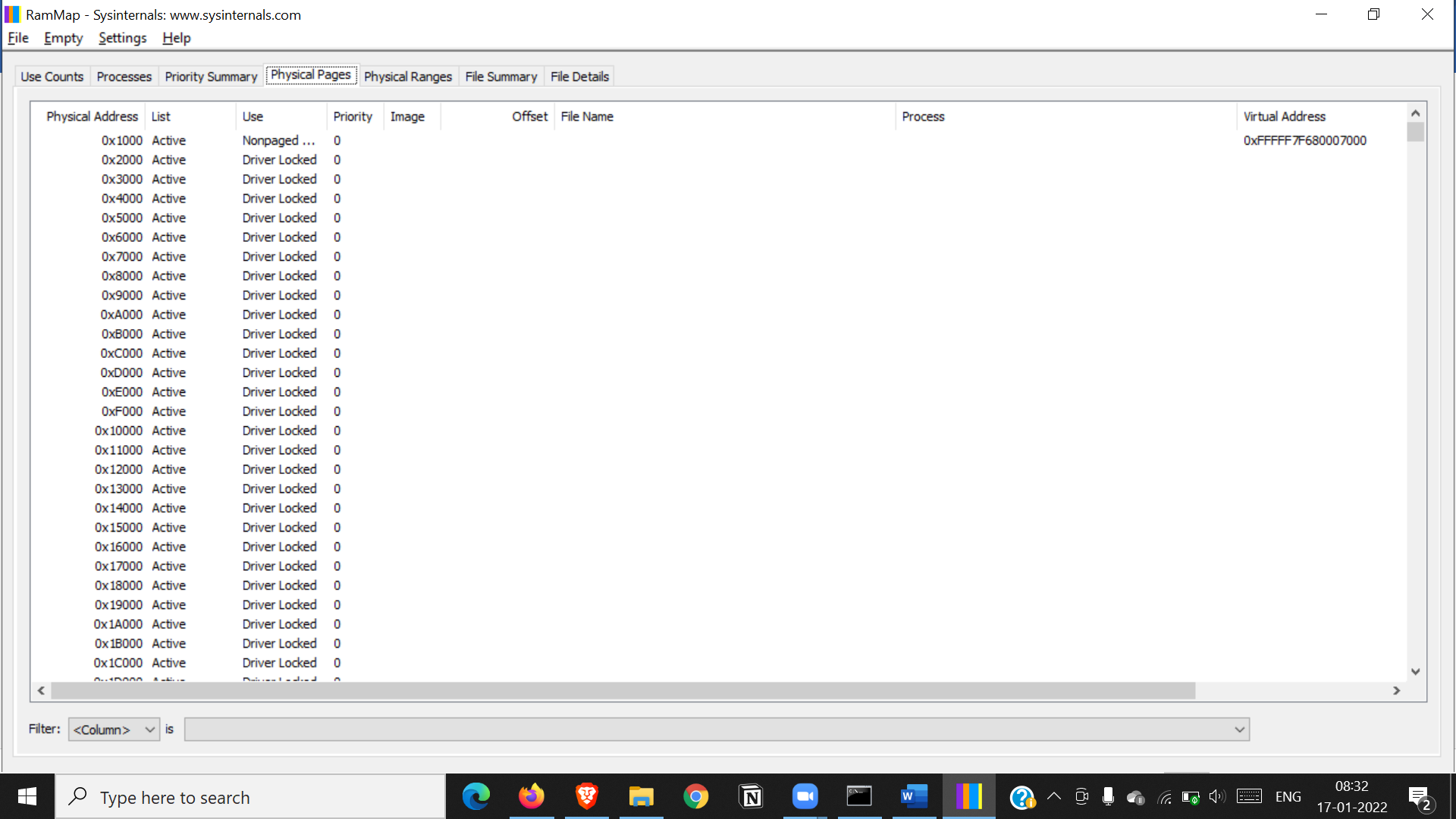
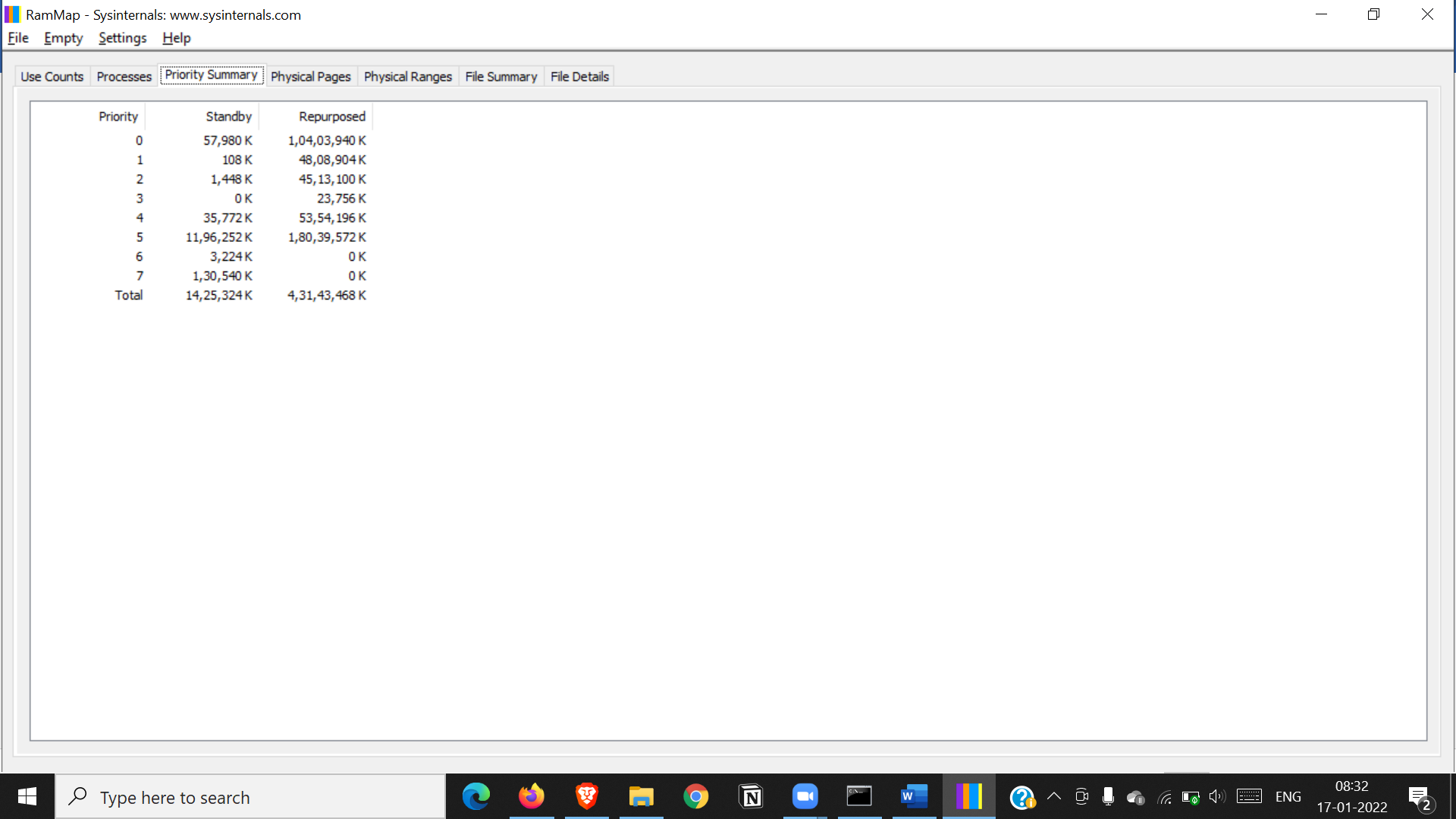
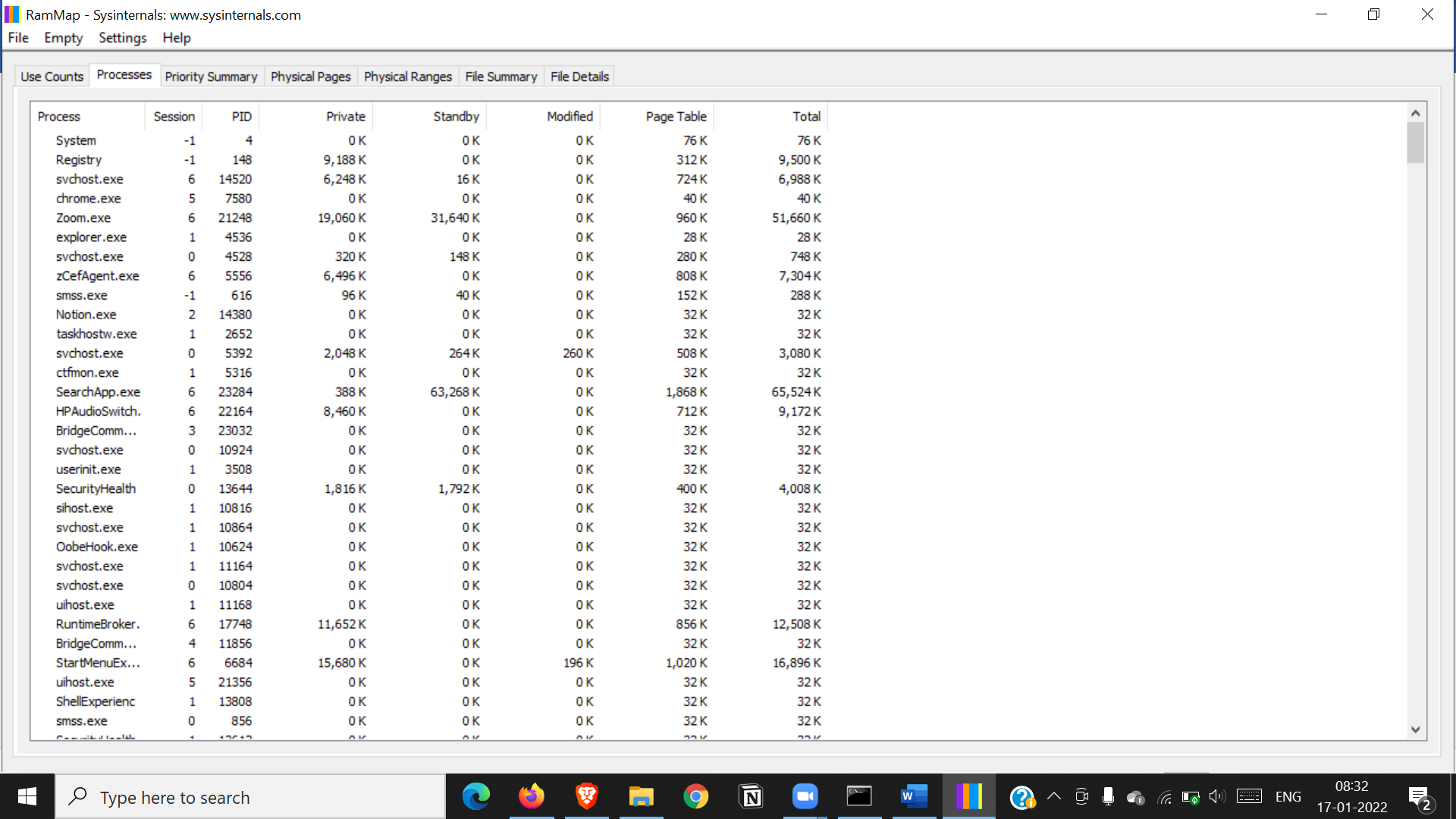
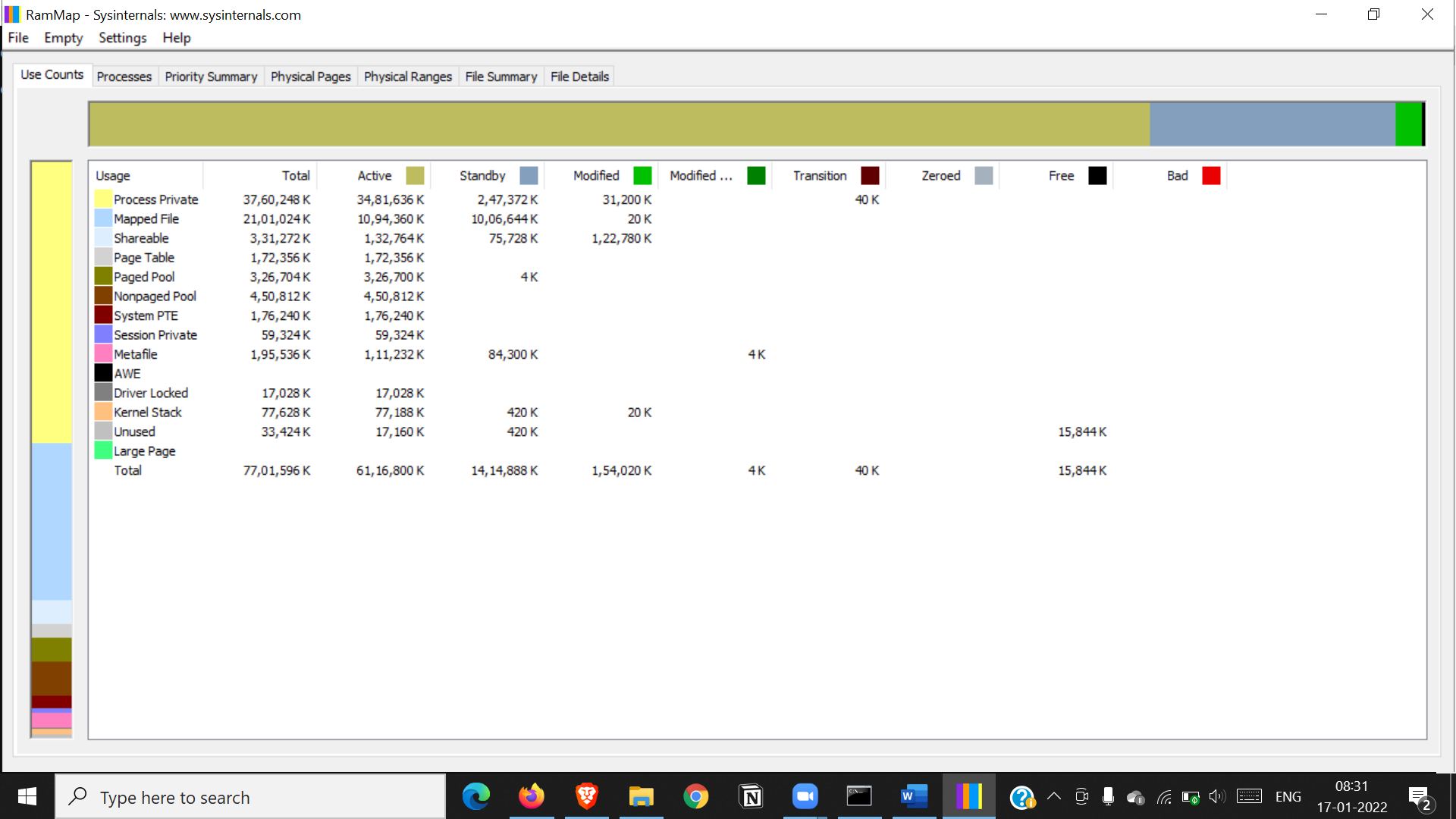
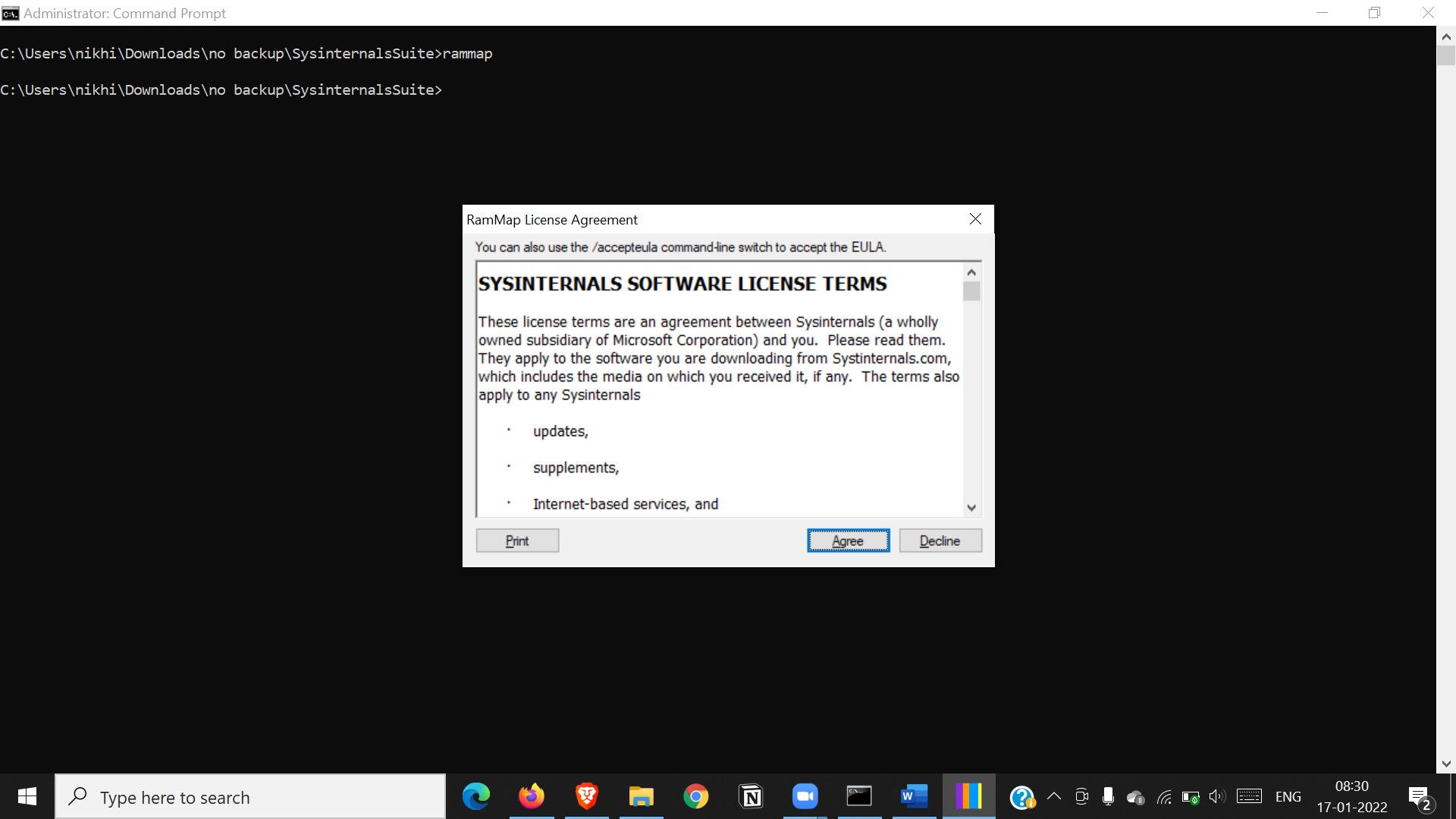


Diskmonitoring



Virtual memory map

Rammap



Ram capture

