******

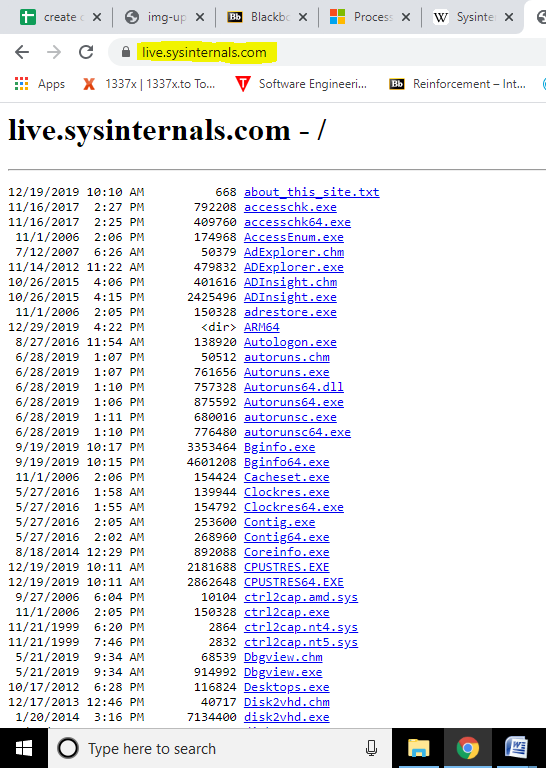
**Digital Forensics II LAB**

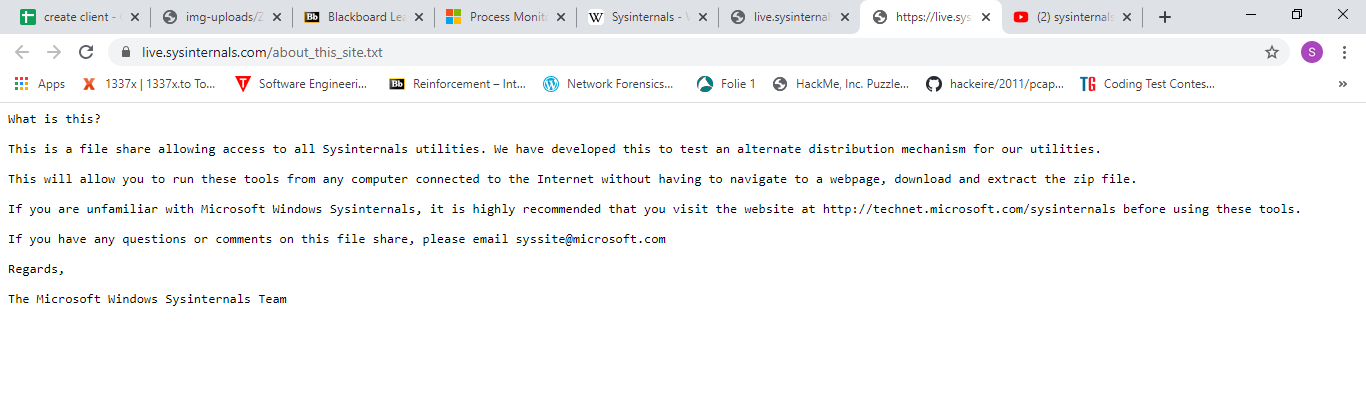
**Experiment-7**

**Windows Sys-Internals Suite**

***AIM: Forensics Using Sys-internals tools***

**Windows Sys-internals** is a suite of more than 70 freeware utilities that was initially developed by Mark Russinovich and Bryce Cogswell that is used to monitor, manage and troubleshoot the Windows operating system, and which Microsoft now owns and hosts on its TechNet site. It offers technical resources and utilities to manage, diagnose, troubleshoot, and monitor a Microsoft Windows environment. The tools include utilities such as Process Explorer, which is a lot like Task Manager with a plethora of extra features, or Process Monitor, which monitors your PC for file-system, registry, or even network activity from almost any process on your system. Most of these tools are going to require administrator access on your computer, so you’d be wise to test them out in a virtual machine or a test computer if you aren’t sure what you are doing — these are some heavy duty tools.

* **Check Sys-internals tools :** To check sys-internals tool, browse on the google and go to the website: **https://live.sysinternals.com/ ,** there we can see all the tools:

The details about the about this site is shown below :

**Here is the list of all the sys-internal tool with the description of their job:**

Process   
v16.21 (May 16, 2017)  
Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.

Process   
v3.50 (February 13, 2018)  
Monitor file system, Registry, process, thread and DLL activity in real-time.

[PsExec](https://docs.microsoft.com/en-us/sysinternals/downloads/psexec)  
v2.2 (June 29, 2016)  
Execute processes on remote systems.

[PsFile](https://docs.microsoft.com/en-us/sysinternals/downloads/psfile)  
v1.03 (June 29, 2016)  
See what files are opened remotely.

[AccessChk](https://docs.microsoft.com/en-us/sysinternals/downloads/accesschk)  
v6.20 (November 19, 2017)  
AccessChk is a command-line tool for viewing the effective permissions on files, registry keys, services, processes, kernel objects, and more.

[AccessEnum](https://docs.microsoft.com/en-us/sysinternals/downloads/accessenum)  
v1.32 (November 1, 2006)  
This simple yet powerful security tool shows you who has what access to directories, files and Registry keys on your systems. Use it to find holes in your permissions.

[AdRestore](https://docs.microsoft.com/en-us/sysinternals/downloads/adrestore)  
v1.1 (November 1, 2006)  
Undelete Server 2003 Active Directory objects.

[Autologon](https://docs.microsoft.com/en-us/sysinternals/downloads/autologon)  
v3.10 (August 29, 2016)  
Bypass password screen during logon.

[Autoruns](https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns)  
v13.95 (June 11, 2019)  
See what programs are configured to startup automatically when your system boots and you login. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.

[CacheSet](https://docs.microsoft.com/en-us/sysinternals/downloads/cacheset)  
v1.0 (November 1, 2006)  
CacheSet is a program that allows you to control the Cache Manager's working set size using functions provided by NT. It's compatible with all versions of NT.

[ClockRes](https://docs.microsoft.com/en-us/sysinternals/downloads/clockres)  
v2.1 (July 4, 2016)  
View the resolution of the system clock, which is also the maximum timer resolution.

[Hex2dec](https://docs.microsoft.com/en-us/sysinternals/downloads/hex2dec)  
v1.1 (July 4, 2016)  
Convert hex numbers to decimal and vice versa.

[Junction](https://docs.microsoft.com/en-us/sysinternals/downloads/junction)  
v1.07 (July 4, 2016)  
Create Win2K NTFS symbolic links.

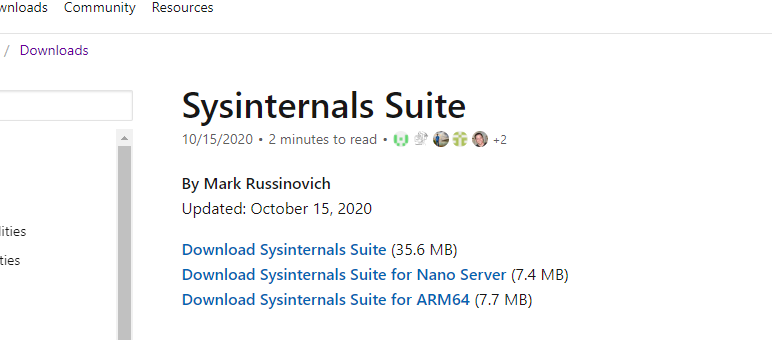
[LDMDump](https://docs.microsoft.com/en-us/sysinternals/downloads/ldmdump)  
v1.02 (November 1, 2006)  
Dump the contents of the Logical Disk Manager's on-disk database, which describes the partitioning of Windows 2000 Dynamic disks.

[ListDLLs](https://docs.microsoft.com/en-us/sysinternals/downloads/listdlls)  
v3.2 (July 4, 2016)  
List all the DLLs that are currently loaded, including where they are loaded and their version numbers.

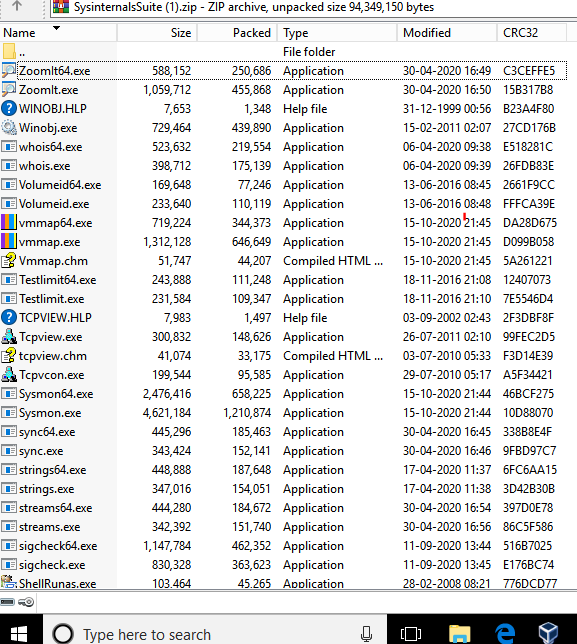
[ProcDump](https://docs.microsoft.com/en-us/sysinternals/downloads/procdump)  
v9.0 (May 16, 2017)  
This command-line utility is aimed at capturing process dumps of otherwise difficult to isolate and reproduce CPU spikes.

**Installation**

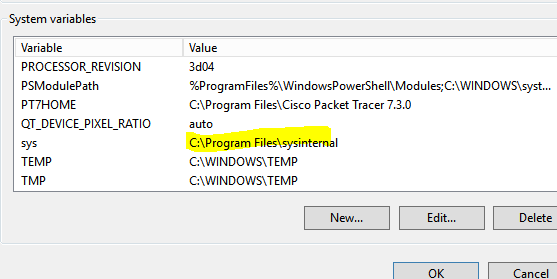
1. The Sys-internals Suite can be downloaded from   
   <https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite>



1. After downloading extract, the zip file in a folder.
2. After extracting you can use the various tools provided in the Sys-internals Suite.



Setting path

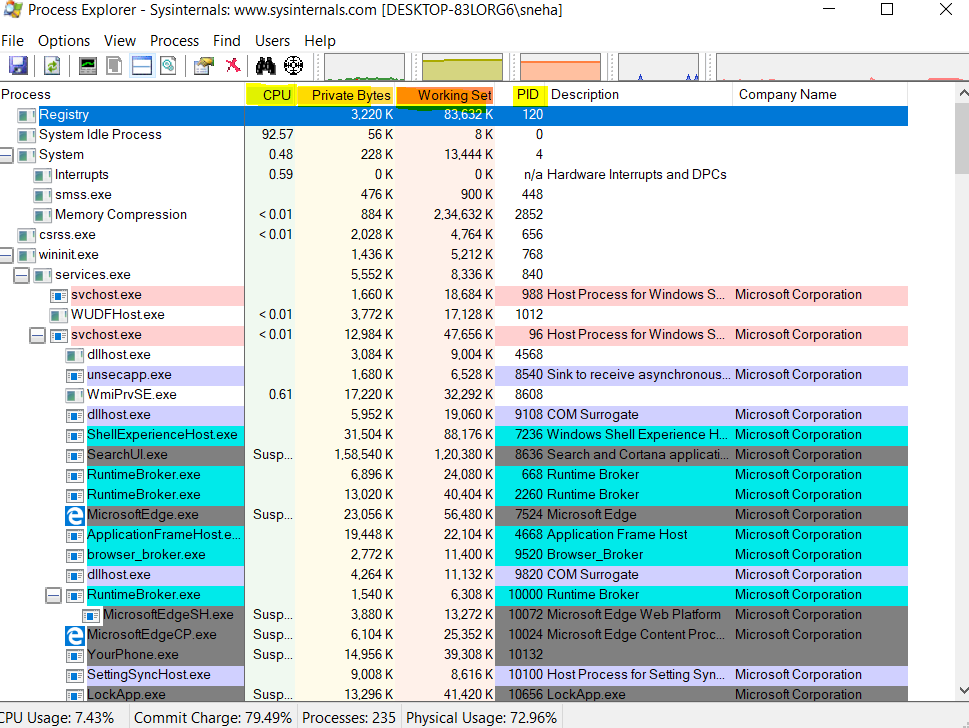
****

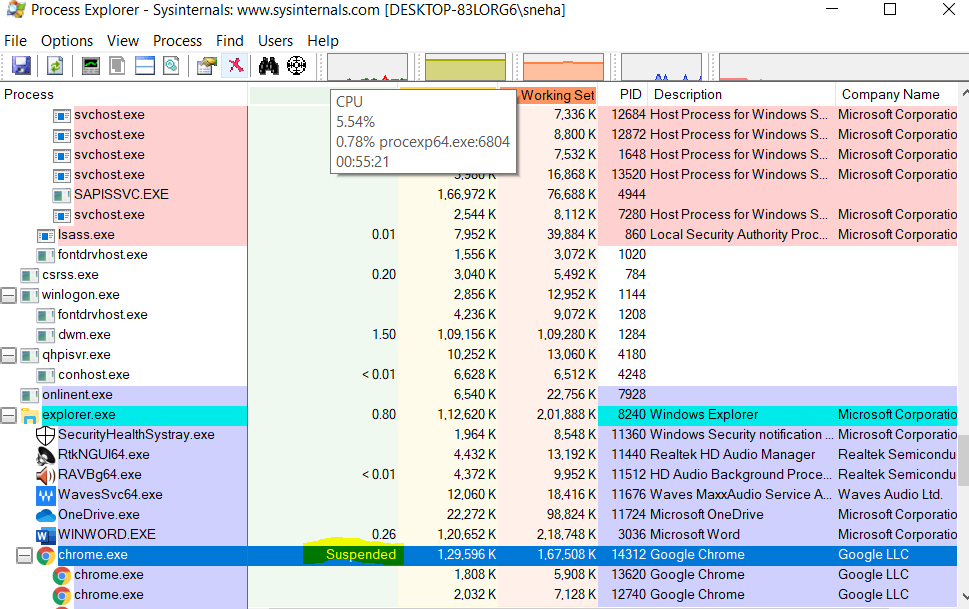
**Tools in Sys-internal Suite**

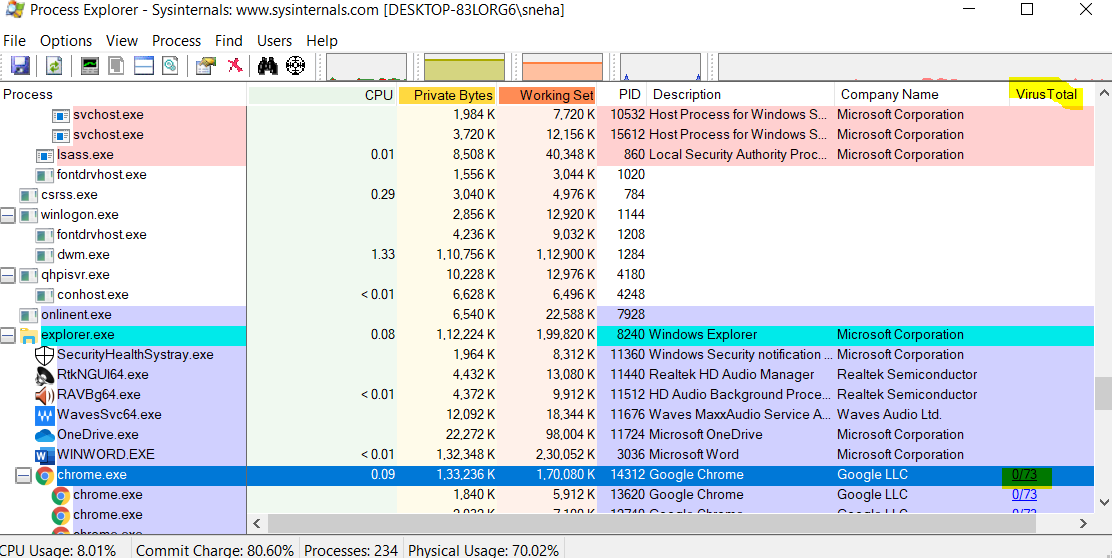
* **Monitor Live Processes :** Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such 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.

**Procexp64.exe**

The Process Explorer display consists of two sub-windows. The top window always shows a list of the currently active processes, including the names of their owning accounts, whereas the information displayed in the bottom window depends on the mode that Process Explorer is in: if it is in handle mode you'll see the handles that the process selected in the top window has opened; if Process Explorer is in DLL mode you'll see the DLLs and memory-mapped files that the process has loaded. Process Explorer also has a powerful search capability that will quickly show you which processes have particular handles opened or DLLs loaded.

1) Suspendthe process to diagnose it by right click select the option suspend it will be shown as

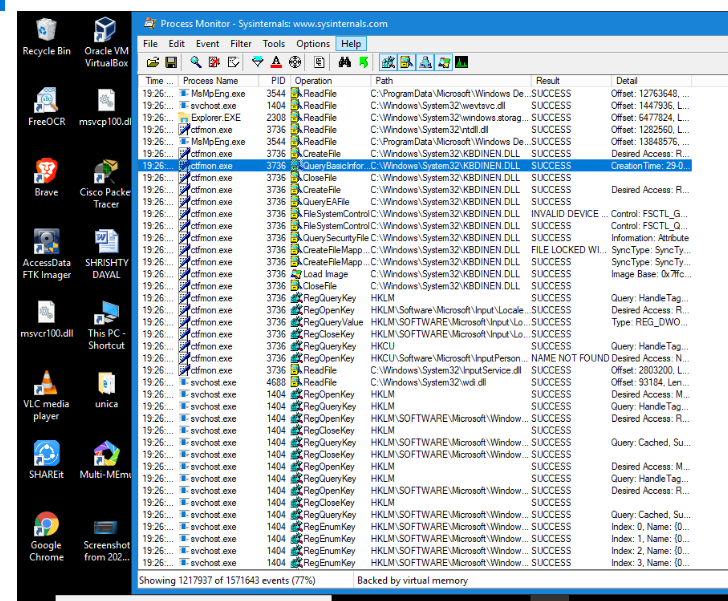


2) Again right click and select the option **virus total**. This will help you know whether that process contain virus or not. Virus total contain 73 companies so we can see the progress.

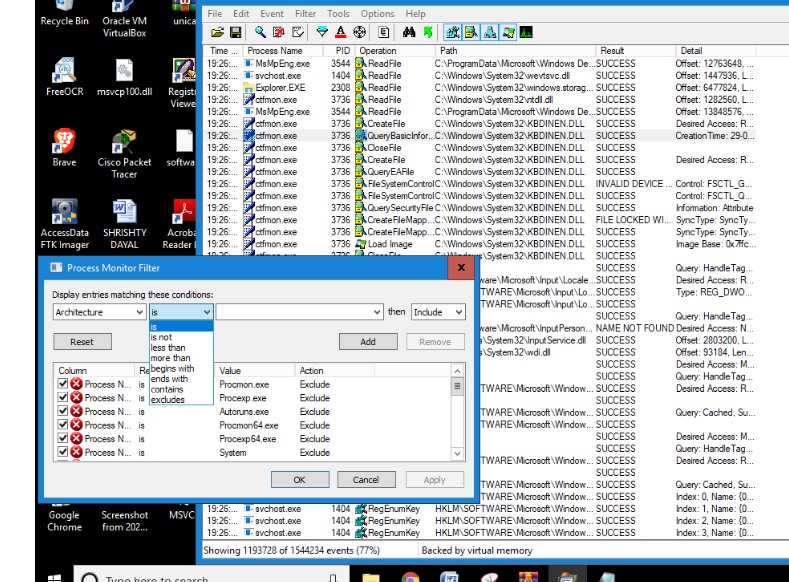
**Observation: Chrome does not contain any virus as it is showing 0/73.**

1. On right click we can select the option of “**set priority**” of the process. Best option is the “high” as “real time” will freeze your system.
2. We can replace task manager with sys-internals if we don’t like task manager. We can monitor CPU

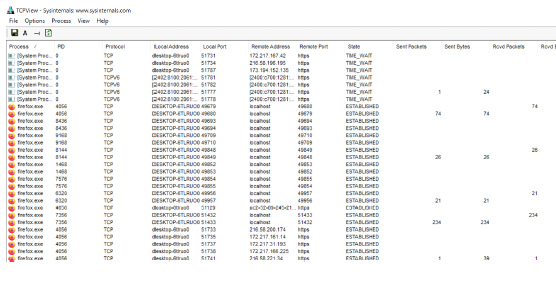
time, private bytes etc.

** Process Monitor**

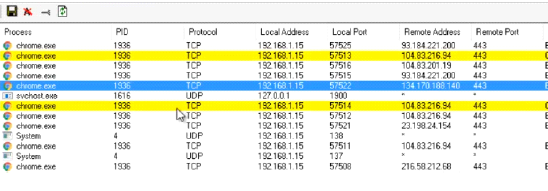
**Description about the process monitor interface**: When I first load up the Process Monitor interface, it was presented with an enormous number of rows of data, with more data flying in quickly. The first thing that I noticed was that to try filter those rows down to the much smaller subset of data .

**Observation** : We can also remove or edit filters by selecting them in the list and then modifying or removing them:

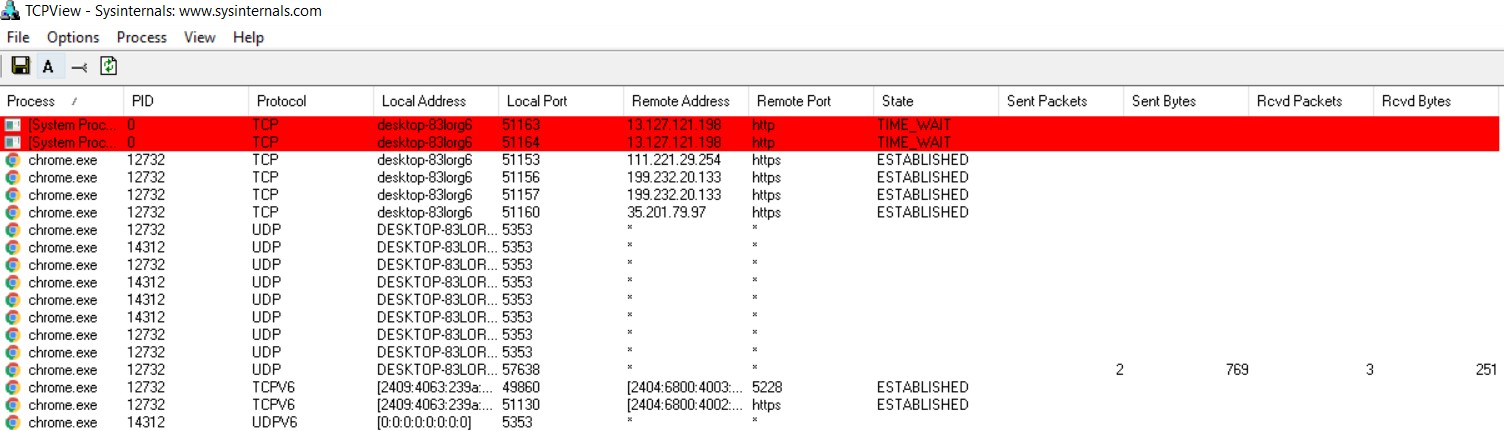
* **MONITOR TCP/UDP PACKETS**: Open TCP View from the suite tools. TCP View is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections.

When you start TCP View it will enumerate all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions. 

By default, TCP View updates every second, but you can use the Options>Refresh Rate menu item to change the rate. Endpoints that change state from one update to the next are highlighted in yellow; those that are deleted are shown in red, and new endpoints are shown in green.







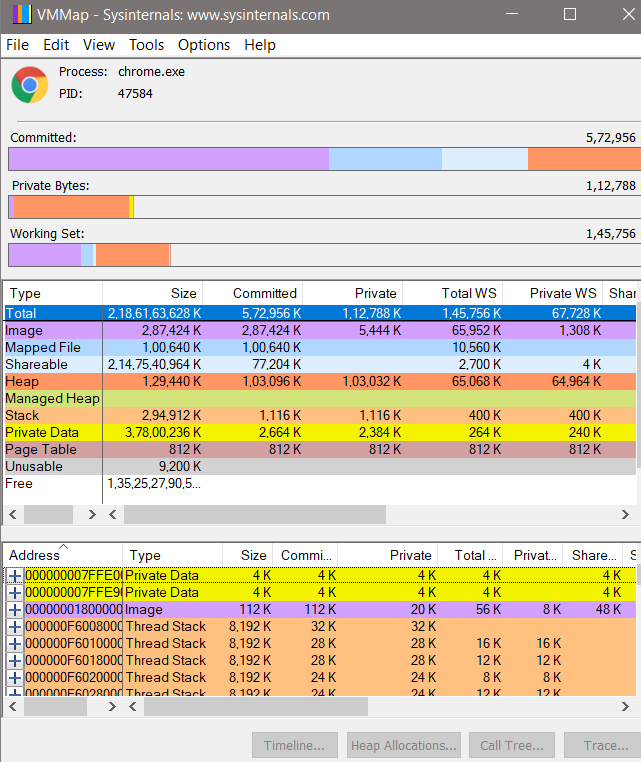
Observation:

* **Red color** - New opened connections.
* **Yellow color** – Closed connections
* **Green color** – Connection in state changing.
* **Monitor Virtual Memory:** To Monitor Virtual Memory using a Sys-Internals tool, we have to use VM-Map. We can find this in the Sys-Internals Suite package. Once we double click on the application we will be greeted by the major live processes of the system as we can see in the picture above and to take a look about their memory, we need to select a process and click *‘Okay’*.

**VM-MAP**

VM-Map 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.

VM-Map is the ideal tool for developers wanting to understand and optimize their application's memory resource usage.



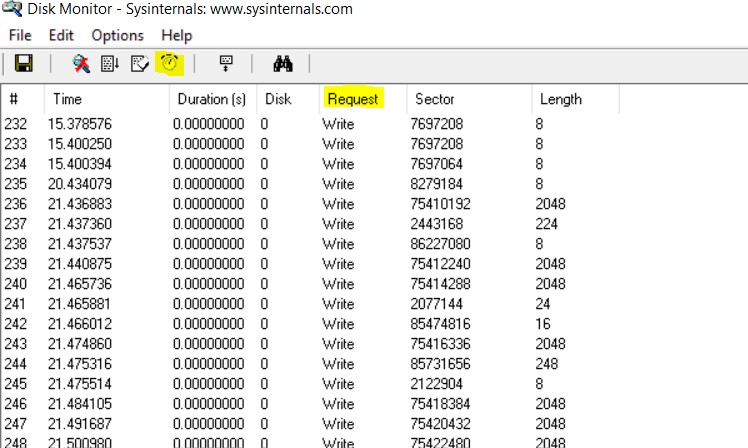
Observation: Besides flexible views for analyzing live processes, VM-Map supports the export of data in multiple forms, including a native format that preserves all the information so that you can load back in. It also includes command-line options that enable scripting scenarios.

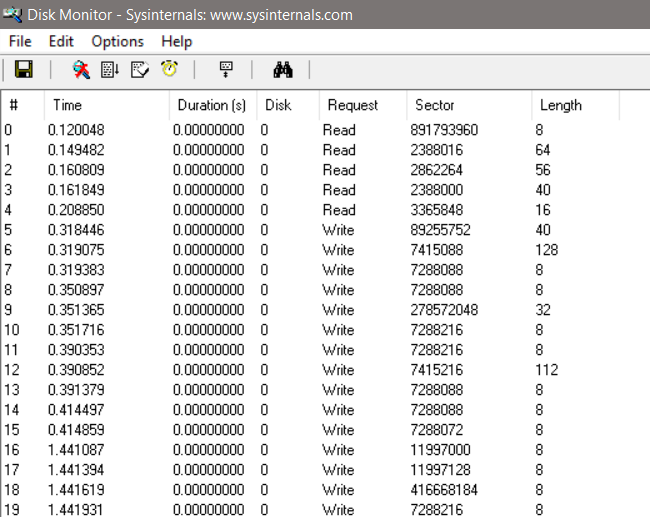
* **Monitor Hard Disk**

To monitor the activity inside the Hard Disk we need to use an application in Sys-Internals Suite package known as Disk Monitor. We can find it as Disk-mon in the package. We need to open this application as an Administrator because a guest cannot access such sensitive information.

**Disk-Mon**

Disk-Mon is an application that logs and displays all hard disk activity on a Windows system. You can also minimize Disk-Mon 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

* Read and write offsets are presented in terms of sectors (512 bytes).
* Events can be either timed for their duration (in microseconds), or stamped with the absolute time that they were initiated.
* The History Depth dialog can be used to specify the maximum number of records that will be kept in the GUI (0 signifies no limit)

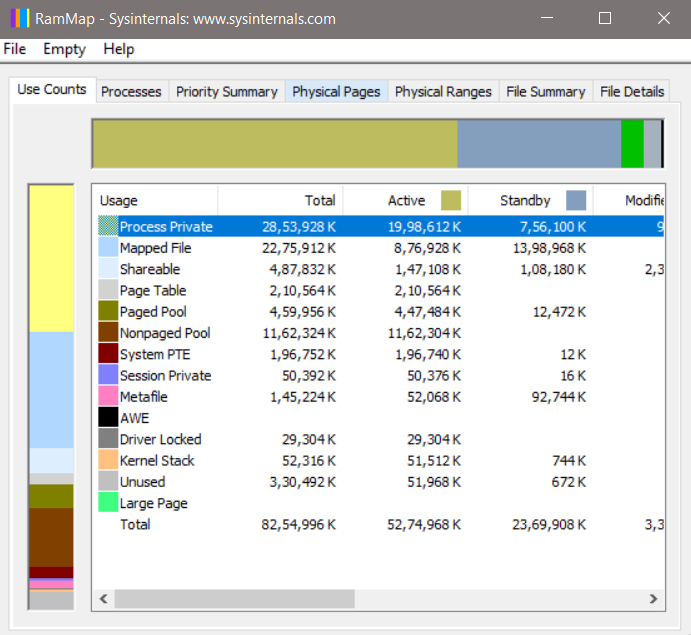


**Observation: Clock represent history depth and request are displayed .**

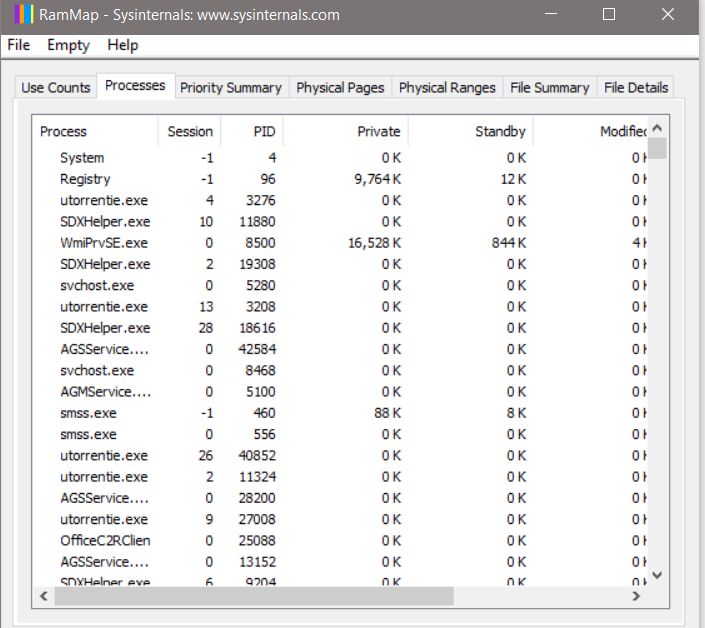
* **Monitor Cache Memory**

**Ram-map**

We know that cache memory is stored in RAM. Therefore, we need to use RAM-Map to monitor Cache Memory. We can find this in the Sys-Internals Suite package.



The above image shows the different portions of the RAM. To access the Cache processes we need to select the ‘Processes’ tab.

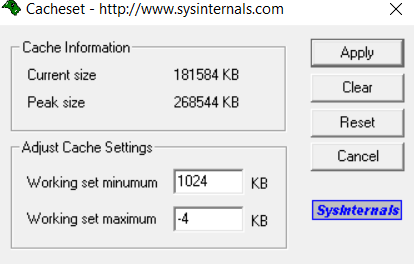


The picture above shows the processes stored in the RAM.

**Cache Set**

Cache-Set is an applet that allows you to manipulate the working-set parameters of the system file cache. Unlike Cache Man, Cache Set runs on all versions of NT and will work without modifications on new Service Pack releases. In addition to providing you the ability to control the minimum and maximum working set sizes, it also allows you to reset the Cache's working set, forcing it to grow as necessary from a minimal starting point. Also unlike Cache Man, changes made with Cache Set have an immediate effect on the size of the Cache.

Use Cache Set to performance tune the system. Cache size in a way is not possible without tweaking internal variables the way Cache Man does.



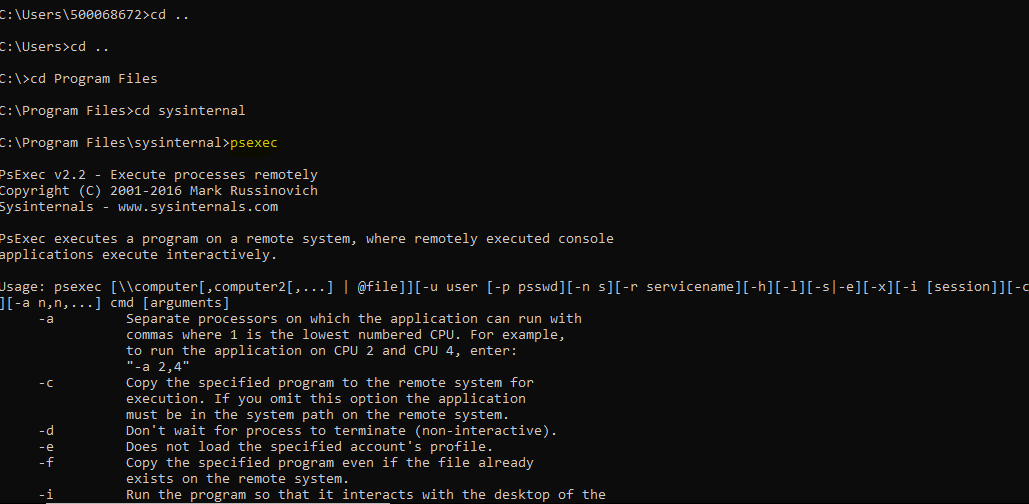
Uses are

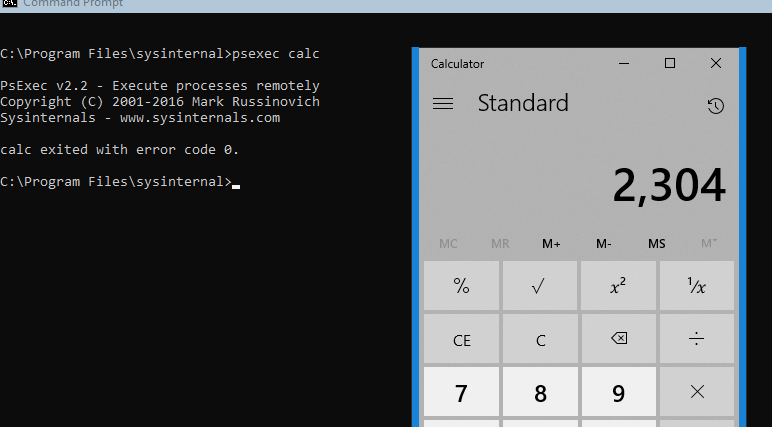
* Setting New Sizes
* Resetting Previous Values
* Clearing the Cache's Working Set

## Ps-Toolkit

## Ps-Exec

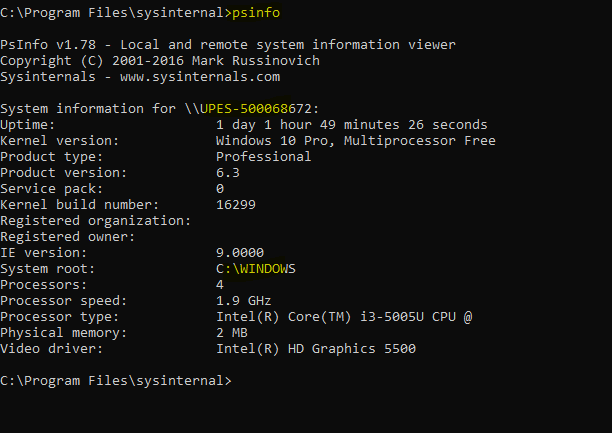
Ps-Exec is a light-weight telnet-replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software. Ps-Exec's most powerful uses include launching interactive command-prompts on remote systems and remote-enabling tools like Ip-Config that otherwise do not have the ability to show information about remote systems.





## Ps-Info

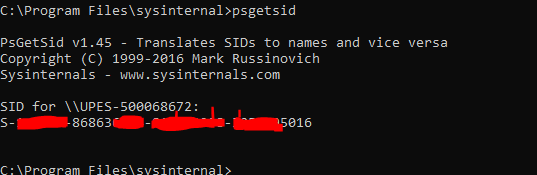
Ps-Info is a command-line tool that gathers key information about the local or remote system, including the type of installation, kernel build, registered organization and owner, number of processors and their type, memory size, the install date of the system, and if it's a trial version, the expiration date. PsInfo command-line switches also let you view installed hotfixes and software applications.



## Ps-Get-Sid

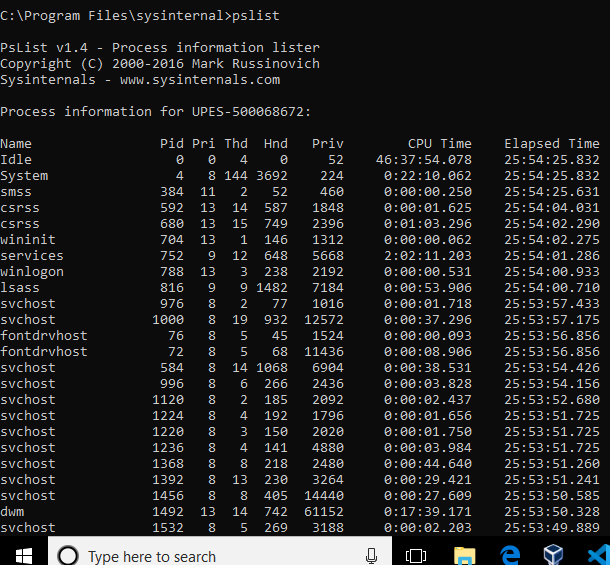
Ps Get Sid makes reading a computer's SID easy, and works across the network so that you can query SIDs remotely.

**Ps-Get-Sid also lets you see the SIDs of user accounts**



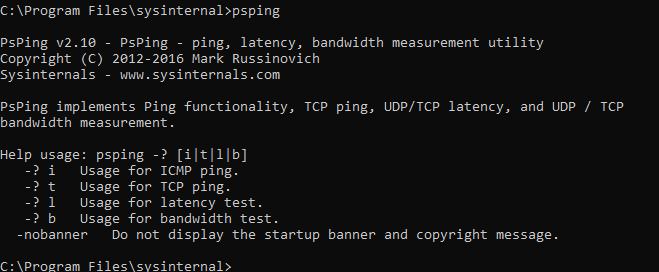
## Ps-List

Ps List is utility that shows you a combination of the information obtainable individually with pmon and pstat. You can view process CPU and memory information, or thread statistics. What makes PsList more powerful than the Resource Kit tools is that you can view process and thread statistics on a remote computer.



## Ps-Ping

PsPing is a command-line utility for measuring network performance. In addition to standard ICMP ping functionality, it can report the latency of connecting to TCP ports, the latency of TCP round-trip communication between systems, and the TCP bandwidth available to a connection between systems. Besides obtaining min, max, and average values in 0.01ms resolution, you can also use Ps-Ping to generate histograms of the results that are easy to import into spreadsheets.



## Ps-Service

Ps-Service is a service viewer and controller for Windows NT/2K. Like the SC utility that's included in the Windows NT and Windows 2000 Resource Kits and Windows XP, PsService displays the status, configuration, and dependencies of a service, and allows you to start, stop, pause, resume and restart them. Unlike the SC utility, PsService enables you to logon to a remote system using a different account, for cases when the account from which you run it doesn't have required permissions on the remote system. PsService includes a unique service-search capability, which identifies active instances of a service on your network. You would use the search feature if you wanted to locate systems running DHCP servers, for instance.

