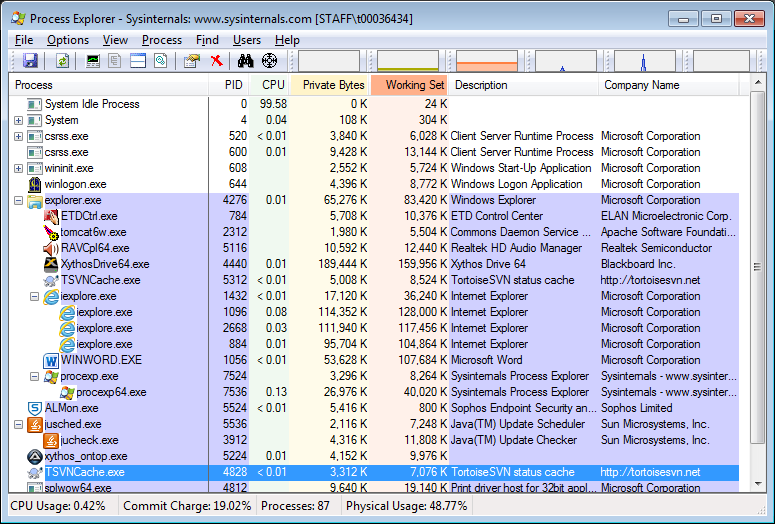
Process Explorer

[Windows Sysinternals](http://www.microsoft.com/technet/sysinternals) has some useful downloads to help you manage, troubleshoot and diagnose your Windows systems and applications.

The [Process Explorer](http://www.microsoft.com/technet/sysinternals/utilitiesindex.mspx) utility procexp is up on Xythos.

This utility allows you see more accurate and detailed CPU usage of a process than you can see with Task Manager.



Above we can see System Idle at 99.58% CPU usage and WINWORD.exe at <0.01% CPU usage.

Copy procexp to your desktop and run it.

Pink processes are services. Light blue processes are running in your user account.

Name any service running on your system. \_\_\_svchost.exe\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name any user process that is currently running on your system. \_\_\_nvtray.exe\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is its process id (PID)\_\_\_\_1988\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What percentage CPU is it using? \_\_\_none\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the Working Set (RAM assigned to this process)?\_\_\_\_19444K\_\_\_\_\_\_\_

What is the description? \_\_\_\_NVIDIA Settings\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the company name? \_\_\_\_\_NVIDIA Corporation\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The description and company name help in identifying processes that are not malware.

Choose View, then Update Speed. How often is Process Explorer updated?\_1 second\_\_\_\_\_\_\_\_\_\_\_

Run Notepad. Hover over the process in Process Explorer. What is it’s path? \_C:\Windows\System32\notepad.exe\_\_\_\_\_\_\_\_\_\_

Pink processes are services. Light blue processes are running in your user account. Choose Options, then Configure Colors to see the colour selections. What is the colour green used for?

\_\_New Objects\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This colour appears for one second.

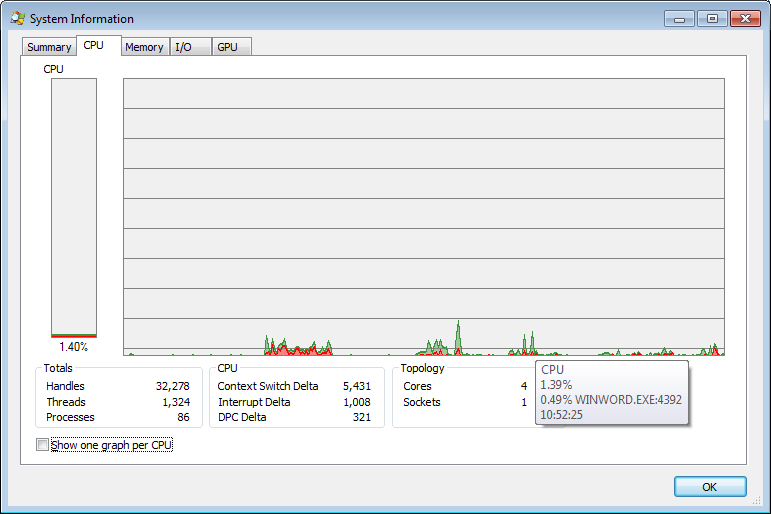
**Choose Options, then Difference Highlight Duration.** Set the Duration to 5 or more seconds. This will help you see processes starting and stopping. Every process which starts is associated a green color and every process that stops gets a red. The processes will exist in the Process Explorer for at least 5 seconds with the same color code, so that you can see them starting and stopping.

Run Notepad. You should now be able to see it in red as it starts. How much CPU time does it take to open it? \_<0.01 seconds\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

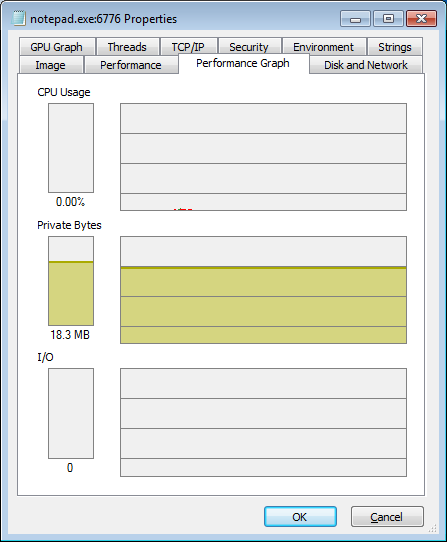
Exit Notepad and you should see it in red.

You can also see CPU usage history for a process in a few ways.

Choose View from menu and then System Information. Choose CPU tab. Hover the mouse over a spike in the graph to see the process. You will see the following:



Or you can right-click on the process on the main Procexp window and choose Properties, then choose Performance Graph tab.



Now start a new program, e.g. Microsoft Word. You should see WINWORD.EXE at the bottom of the Process Explorer screen.

Have both the Microsoft Word window and Process Explorer window visible on the screen.

Enter some data into Word and save the data to a file.

Describe how CPU usage changes when you start Microsoft Word, a minute after you have started this program, when you enter and save the data, and when you terminate this program. Click on System Information button (Ctrl+I) or choose View from menu and then System Information to see this information in detail. Provide an explanation for this CPU usage pattern.

When I start Microsoft Word the CPU usage jumped up to 3% . when I start entering data the

CPU usage hikes up and down from 2% to 4%. When I tried to save the document, the CPU

usage hikes up to 8% and upon closing the program cpu usage declines to 2%. Every time the program needs to access to the memory, kernel, the system, or I/O, the cpu usage increases.

There are many extra columns that can be added to the main screen. One useful column is Page Fault Delta. A page fault occurs when a chunk of referenced virtual storage is on the hard drive rather than in memory. Page faults are perfectly normal but an excessive number can slow up your system. Page Fault Delta is the number of page faults since the last Procexp refresh.

Specify the process experiencing the most page faults. Porcexp64.exe\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_