Operating Systems Lab Sheet 4

Jack Carroll

T00194823

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

Name any service running on your system. AdobeUpdateService.exe

Name any user process that is currently running on your system. XythosDrive.exe

What is its process id (PID)? 4836

What percentage CPU is it using? 0.01%

What is the Working Set (RAM assigned to this process)? 123,372 K

What is the description? Xythos Drive

What is the company name? Blackboard.Inc

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

Choose View, then Update Speed. How often is Process Explorer updated? 0.5,1,2,5 and 10 seconds

Run Notepad. Hover over the process in Process Explorer. What is its 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?

Green is used for new objects which represents the launch of different processes.

This colour appears for one second.

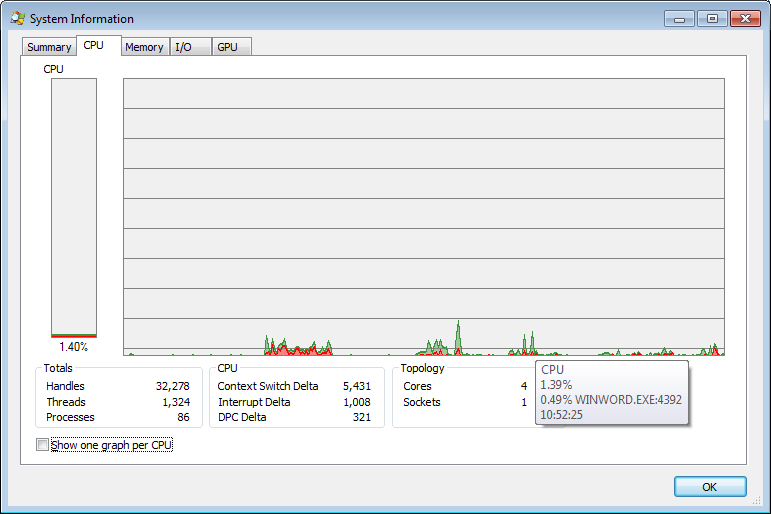
**Choose Options, then Difference Highlight Duration.** Set the Duration to 5 or more seconds. This will help you see processes starting and stopping. Every process which starts is associated a green color and every process that stops gets a red. The processes will exist in the Process Explorer for at 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? 6 seconds

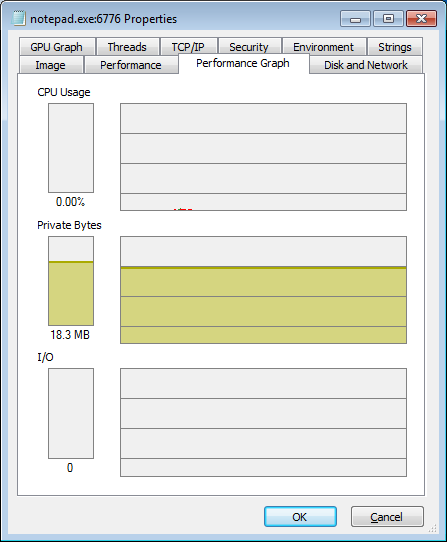
Exit Notepad and you should see it in red.

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.

The CPU increases rapidly as the processor runs the program and the new Word file is being set up with a new blank sheet. Then the CPU decreases after the new document is loaded up because the Word file is awaiting input/output completion. As Word runs idle for about a minute, the CPU usage is idle as the WINWORD.EXE process is in its blocked state awaiting some input from the keyboard.

Before typing the data, the process is in the ready state as it awaits the data to be executed when typed on Microsoft Word. When the data is being entered, the CPU usage rises up gradually due to the input being entered where the process is running after the writing is executed. When the input is typed, the CPU usage gradually falls since the process returns to ready after it is in its running state.

As the data is being saved, there is a substantial rise in CPU usage as the computer runs the WINWORD.EXE program to activate the Windows Explorer to save the file once the save button is pressed. This leads to the CPU running even though no input is entered here as the save process is being carried out. When the Word application is terminated, the CPU usage falls as the program stops running and enters the blocked phase where it awaits the I/O completion or Word activation to restart the program.

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. Procexp64.exe