

# Monitoring Your Computer's Performance

## A computer performance primer

By: William P. Flinn – May, 2007

### Introduction:

You got a new computer last Christmas, or maybe you just got one as a graduation present. Perhaps during your spring computer cleaning you got some upgrade parts to make that old computer seem like new, and make it perform a little better. Whatever the case, it is nice to know how to determine when that old computer needs new parts, or when that new computer is suffering from performance problems due to software or configuration issues. It is also a good idea to know which part of the system is having problems, and how to identify what may be causing those performance problems. It could be a hardware performance problem, it could be improperly configured software, a patch could have caused a problem, or it could be some malicious software (malware) causing your computer to act sluggishly and slow.

Just like you would keep an eye on your own physical health by seeing a doctor regularly, and monitoring things like blood pressure and overall feelings of wellness, monitoring your computer's performance can tell you a lot about its health and ability to quickly access your data. Computer performance issues can quickly evolve into computer security issues as well. If you can't access your data, then that is an availability problem, availability being one of the three information security tenets. If you have issues caused by malware, then that is a security issue which will possibly have drastic consequences. Performance certainly affects the availability of your data, but as will be discussed later in this article, poor performance could very well be due to a virus or other malicious problem, leading to other security issues as well.

For those of you using Microsoft Windows, there are a number of built-in tools that you can use to measure and monitor your computer's performance, and determine which subsystems are in need of attention. Not only will these tools help you quantify performance metrics, but they will also help you determine what processes or programs are consuming the most of your system's resources. There are also additional and freely available tools that you can use to diagnose performance as well. A few of the Sysinternals (now Microsoft) tools will be discussed later in this article.

Although much of what is discussed in this article is usually used by people who maintain network servers, the tools discussed and methods used for diagnosing system problems and performance apply to everyone with a computer. There are a number of ways that you can use the tools built in to your operating system to determine what types of upgrades to perform or what processes are causing performance problems.

### Some Basic Terminology - Computer Subsystems:

First things first – let's make sure we are all on the same page, terminologically speaking. There are a number of misconceptions and misunderstandings about parts of the computer and what they do. For example, to many people, the terms "memory" and "storage" are interchangeable. I have often heard people complain that their computer is running out of "memory," when what they mean to say is that their hard drive is getting full, and they are actually running out of "storage." A full hard drive can cause performance issues, as the hard drive is actually used by the memory sub-system in an operation discussed later called "page swapping." See my article about [memory and storage](#) for a more in-depth explanation of both memory and storage.

So let's take a moment to talk about and define the important sub-systems in your computer. For the purposes of this article, we only need to focus on three main sub-systems: processor (CPU),

memory (RAM and swap file), and hard disk (read/write and swap file). There are others that can affect the main three, such as the video sub-system that will be mentioned briefly as well. But the three sub-systems mentioned here are the ones that do most of the work of processing, storing, reading, and writing data. Especially the disk drives, as those components involve mechanical movement of drive motors and read/write heads, and interface closely with the memory subsystem.

**Processor:** This is the part of the computer, often called the central processing unit (CPU), that does all the processing and calculations to give you a desired result when you input data. There is the CPU itself, along with a number of supporting circuits. There may be one or more CPUs in your computer, and some processors may be the duo-core type that has recently come out. The speed rating of the CPU is the rating given to the speed of the processor in performing its internal calculations.

**Memory:** When we speak of the memory sub-system, we are mainly discussing the random access memory (RAM) contained in your computer. This is the part of the system that works directly with the CPU to store program variables, information about the various pieces of hardware in your computer, and of course the data itself while it is being used by the active application. This memory is what is known as “volatile” memory, which means that as soon as you turn your computer off, everything in memory is erased. In some systems, the RAM often shares its space with the video system, hence the term “shared memory” when the video system for your computer is described in the specifications. In this case, the total memory specified for your system is not the total of the memory that is available for applications because some of it is solely dedicated to the video system. Video requires its own memory, and the more memory available to the video system, the better performance you will have for graphics. The problem with that is that in systems with shared memory, this takes away from memory that is needed by the CPU and can actually degrade overall system performance.

**Disk Drives:** These are the physical disks in your system that permanently store the operating system, hardware drivers, application software, and most importantly, all of your files and important data. Unlike the RAM, this component is referred to as “storage” as opposed to being called memory. This storage is “non-volatile” which means that as soon as you turn off your computer, the data does not get erased – it is kept there until you delete it, unless some other process such as a failure or malware erases it inadvertently. One important aspect of the disk system is that it interacts with RAM in an important way. Whenever your computer needs more memory (RAM), it can “swap” pages of information between the RAM and the hard drive. This is what is known as “virtual memory.” The more RAM you have, the less that your computer needs to swap with virtual memory. This is an important concept to remember because later when we talk about disk performance factors, it will be important to see if your computer has to do a lot of page swapping, which may be due to inadequate amounts of RAM in the computer. Also important is the factor that hard drives are mechanical devices, which means that interactions between memory and the hard drive requires a read/write head to move – taking much longer than the purely electronic operations performed by memory, the CPU, and other circuitry.

## Monitoring Utilities - Performance Monitor:

Now that we have covered the three basic computer sub-systems with which we will be most concerned, let's take a look at some ways that we can use to find out exactly how they are performing, and whether or not we need to address any issues. Two of the tools that will be discussed in this article are two tools that come free to you, as they are built right in to your Windows operating system: **Performance Monitor** and **Task Monitor**. Let's take a look at Performance Monitor first – you can do this by clicking on your Start button, clicking on run, and then typing “**perfmon**” into the run window command line. The System Monitor tool within Performance Monitor will then appear. If you are using Windows XP, Windows 2003, or Windows

Vista, three “performance counters” will be automatically selected for you – “% Processor Time,” “Avg. Disk Queue Length,” and “Pages/sec

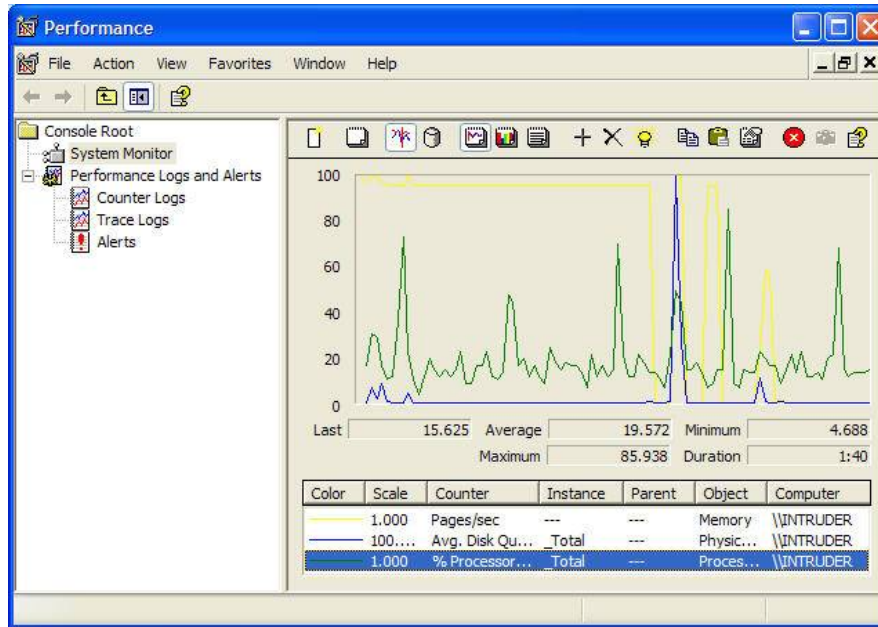


Figure 1: System Monitor Graphical Representations

**% Processor Time:** This is the counter that will give you real-time indications of how much work your CPU is doing. It is perfectly normal to see the processor occasionally spike at 100% usage. It is important to monitor this counter over long periods so that you can look at averages and sustained performance levels. When the computer is just sitting there, it is normal to see levels of around 2% - 15% usage. When the computer is doing a lot of processing, it is common to see sustained levels of anywhere between 40% and 70%. In fact, one common misperception is that a CPU that is always running at 50% is working too hard. In fact, a CPU that is always running at around 50% would be considered to be an underutilized CPU if it were in a file or application server. If it is always running above 70%, however, then it is time to look at what processes are causing the CPU to do too much work, or perhaps offload some of that work to another machine if it is a server. A common remedy for a CPU that is working too hard is to add another CPU if your motherboard supports it. If your motherboard does not support it, try to find a more powerful CPU that the motherboard will support. Depending on the age and abilities of your current motherboard, you may end up having to replace the entire mother board with one that will support a more powerful CPU or even multiple CPUs. See my related article about replacing the motherboard.

**Avg. Disk Queue Length:** This particular counter takes a look at the average number of read or write operations that are waiting their turn. Average disk queue length is a relative measurement of the disk drive and controller speed and ability to read and write data. An average disk queue length of “2,” for example, means that two things are waiting in line, either to be written to or read from the disk. A value less than 2 is desirable – that means that access to the disk is fast and that data requests are not backing up. If you have a high number, say greater than “5,” then that means that your disk drive(s) can’t keep up with requests. To fix this, you might consider getting faster disk drives, or even using multiple disk drives in a redundant (RAID) configuration. The newer SATA disk drives will provide a much needed performance boost. A RAID configuration will allow multiple disk controllers and disk drives to service the request, resulting in less time for the data to be written to or read from the disk drives. Hardware RAID will provide better performance boosts than software RAID. Keep in mind that if your current motherboard does not

support RAID or SATA drives, then you will need to either purchase adapters for the current motherboard, or a new motherboard that includes support for these components.

**Pages/sec:** As mentioned previously, your computer can overcome shortages in RAM by using virtual memory, which is simply a process whereby the contents of memory are swapped back and forth between the RAM and the hard disk. Related to this is a process whereby the CPU is looking for data in memory. When it doesn't find it in memory, it goes to the hard drive to retrieve the data. When data is not found in memory, this is what is known as a "page fault." The pages/sec counter is a measure of hard page faults, with values over "10" indicating a condition called "thrashing", or excessive paging. This actually results in a disk bottleneck, caused by a shortage of memory. There are other conditions that cause excessive paging, however, that are not necessarily due to memory shortages.

But generally speaking, if you see a lot of paging going on, then that is a good indication that you don't have enough physical RAM installed. Spikes in paging counters are fairly normal, but constantly high paging activity means that your memory has to write to and read from the disk sub-system a great deal, and this can affect the burden placed on the hard drive(s). Two things to keep in mind here. 1) Since RAM is an electronic component, it is able to take data from and give data back to the CPU very fast. If the contents needed exist on the hard drive, then the mechanical operation involved in moving read/write heads on the hard drive tends to be quite a bit slower. Thus it is simply a matter of fact that if as little active data as possible has to reside on a disk drive, then processing will be much faster. The more RAM you have, the less paging that has to take place.

**Additional Counters:** You are not limited to the three default counters in perfmon. Additional counters can be added in case you are interested in tracking the performance of different parts of the computer, such as the network card, database processes, or even Windows Management Instrumentation (WMI) processes. Within each performance object, there are many different counters that can be selected for specific information.



Figure 2: Performance Monitor – Adding counters

One exciting new technology available in Windows Vista is a performance feature known as "SpeedBoost." This feature allows you to use a jump drive (flash drive / thumb drive) to house the paging file. Since jump drives are also purely electronic (with no moving parts), then the paging activities can occur much more quickly. See my article about [Windows Vista](#) for more information.

## Counter Logs:

Monitoring performance using perfmon will give you a good snapshot of how your computer is performing at a given time. But it is often necessary to monitor a computer for longer periods, say twenty four hours or even a few days, to get an idea how it is performing under varying circumstances and workloads. Windows Performance Monitor allows you to monitor a computer's performance over time and collect more data that can be used to get a better idea of trends and performance loading during different periods. Within the Performance Logs and Alerts section of perfmon, you can schedule a performance monitoring session, selecting the counters you want to monitor, specifying a sampling interval, and even specifying a log format. If you suspect a performance issue, but can't identify anything when you first open perfmon (and after watching it for a few minutes), then go ahead and schedule a logging session, and let it run while you perform various tasks such as web browsing, word processing, or using any other application that you would normally use. Once you collect the logs, you can view them within perfmon, or if you save them as a CSV file, you can load into a program like Excel and create your own trend graphs and perform a custom analysis.

One thing that may prove extremely useful is to take a baseline of your computer performance when you first get the computer set up with all of your applications and configuration settings finalized. Run the baseline for about twenty four hours, and try to use the computer as you normally would. Keep track of the general times when you used applications, the Internet, and particularly any programs that tend to drive the system a little harder.

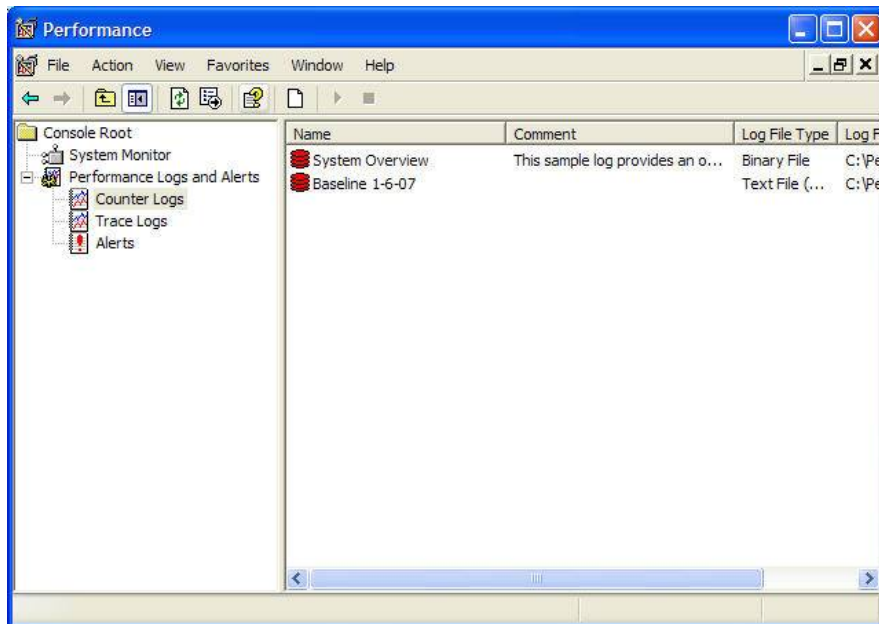


Figure 3: Performance Monitor – Counter Logs

## Task Manager:

Another built in Windows tool is a tool called Task Manager. You can get to Task Monitor by hitting the Ctrl-Alt-Del key sequence and clicking on the Task Manager button. Task Manager has graphing functions for looking at graphic representations of CPU, Page File, and network card activity. And another important function that Task Manager provides is a listing of applications and processes that are running. The process monitoring function will provide information about process name, an identification number, and how much CPU usage that particular process is taking.

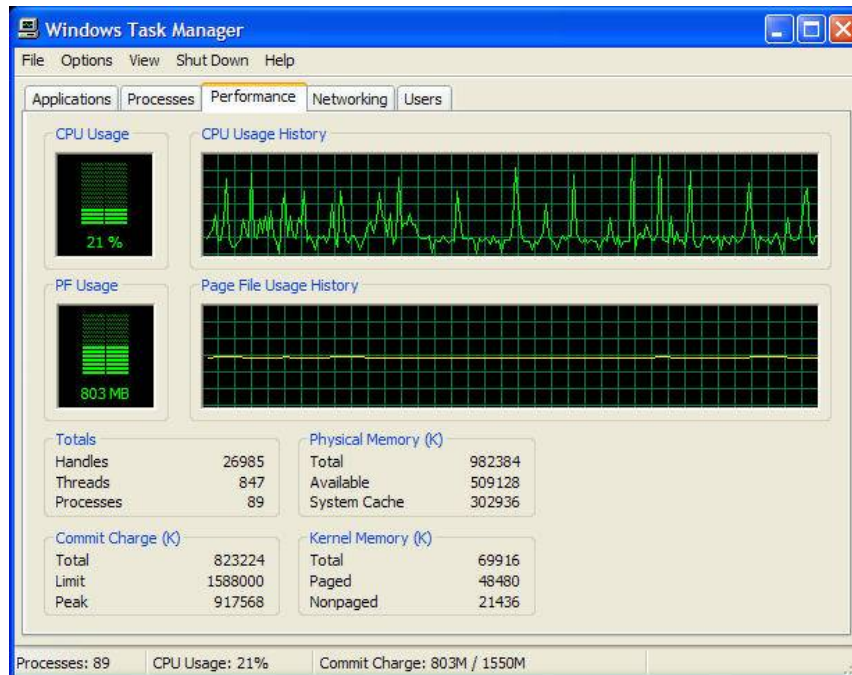


Figure 4: Task Manager – Performance tab showing graphical view

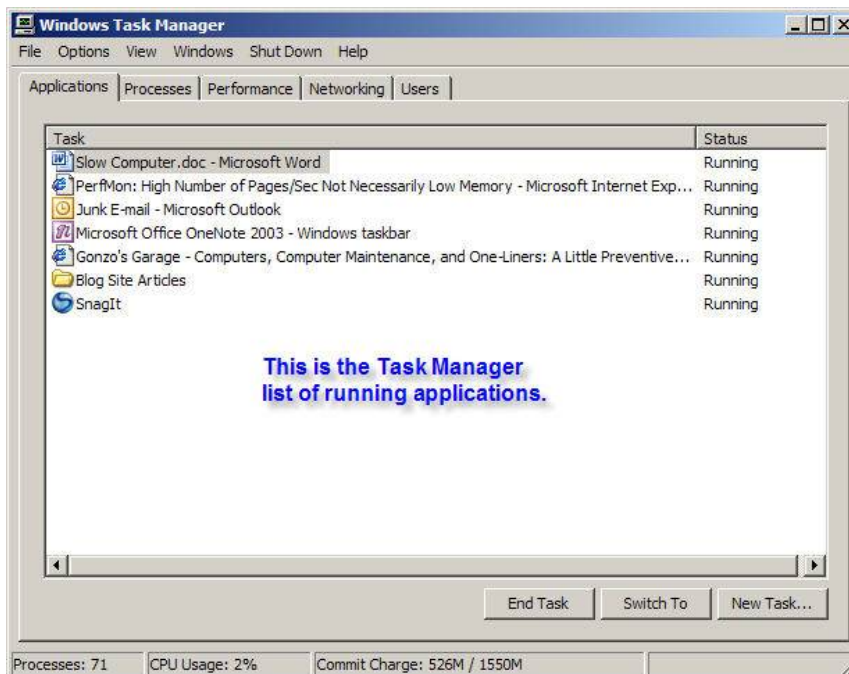


Figure 5: Task Manager – Applications tab showing applications list

The processes tab is particularly useful because perfmon and Task Manager graphs will tell you that the CPU usage is high, for example, but the graphs don't tell you the "what" about the high usage. By clicking on the CPU column header in the Processes tab, you can arrange the processes from highest CPU usage to lowest, and identify which process is taking up most of your CPU's time. There is a process called the "System Idle Process" that will be listed also. If this particular process is listed first and taking up a great deal of CPU usage – don't worry. That simply means that the CPU isn't working on much else, and that its resources are available for use. Additionally, make sure to check the box in the lower left corner labeled "Show processes from all users." This is important because you are not the only "user" logged in to your computer. There are various processes running as a "SYSTEM" or "LOCAL SERVICE" or "NETWORK SERVICE" account, and it will be important to show these to identify which processes are using all the resources. If you don't select to see processes from all users, it is possible to see your CPU being used at a high percentage, but yet very few processes listed.

You can use the process list to troubleshoot a certain process by selecting the process and clicking the "End Process button." Try ending a process you suspect and watch your CPU usage in perfmon simultaneously. Be careful, however, as some processes, if ended, may crash your computer or cause it to operate abnormally. If this happens, rebooting should fix this. Another thing you may notice, is that when you end a process, it will re-spawn itself. This is normal; some applications will automatically re-start a process if it shuts down to prevent abnormal operation. An interesting thing to note here, though, is that if you end a process, even though it re-spawns itself, you may notice that the CPU usage still stays low. Sometimes a process runs away and continues to use more and more resources, and ending that process easily corrects the problem. Once you have identified such a situation, keep an eye on it to see if that same process runs away again, how often it occurs, and what seems to be happening when it does occur.

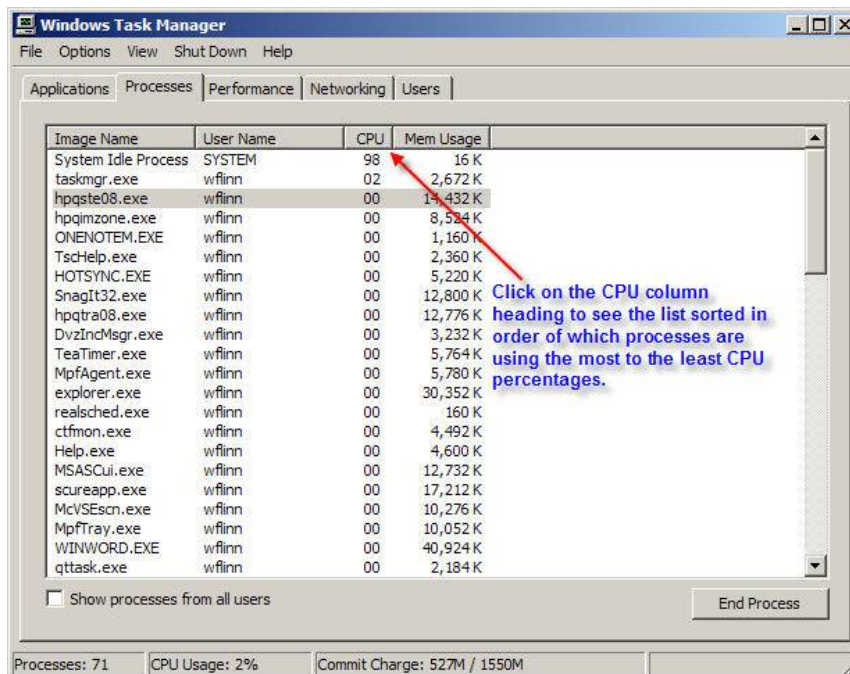


Figure 6: Task Manager – Processes tab showing list of running processes

Some of these processes have pretty cryptic names. When you find a process that seems to be causing a problem, and you don't know what it is, research it before doing anything else. Use Google or another search engine, and type in the name of the process. You will typically find a number of sources that can tell you what the process is, what application is usually responsible for it, and if there are any known issues or fixes for that process. Here is a [web site](#) that will give you a lot of good information on common processes.

This tool provides a good way to find out if you have a malicious process running as well. If you see a process running that is consuming a great deal of resources, and you don't recognize it, research it as previously mentioned. If it is a known malicious process, your search results will often return that information right away. In fact, many resources on the web for finding information about processes will tell you what applications use them under normal circumstances, and if there are any viruses or other malicious processes associated with a process by the same name. Once you have this information, you can dig deeper to find out what file names and versions should be associated with this process, and compare that to the files for that process that exist on your computer.

However, one of the weaknesses in using the built in Windows Task Manager utility is that it may not give you enough information about the processes that are running. For example, there is a commonly appearing process called SVCHOST.EXE that may be running, and you may see several instances of it, but no other information about what exactly is using that process. For help with this, there is a free set of tools from the web site formally known as "Sysinternals" and now available on the Microsoft web site (see link here). While the scope of this article cannot possibly go into depth on the many Sysinternals tools available, I would like to concentrate on one of the tools known as "Process Explorer."

## Sysinternals Process Explorer:

The Sysinternals tools were written by Mark Russinovich, who is now working for Microsoft, and presents various topics at Microsoft's annual TechEd conference. Process Explorer gives a much better breakdown of the running processes, what they are, and how much CPU time each is consuming. For example, the SVCHOST.EXE process is used by various applications. The built-in Windows Task Manager tool will simply list SVCHOST multiple times, and will tell you which ones are using high CPU usage amounts, but will not necessarily tell you what application is using the particular instance that is causing high CPU usage. Additionally, Process Explorer gives a breakdown of the running processes in a hierarchical and color coded list, as well as listing process IDs, to assist in analyzing running processes.

Process explorer gives the ability to pop up graphic representations of the computer's performance metrics as well. Once the graphs are visible, mousing over a particular point on the graph will allow you to see what process caused that particular resource usage. For example, you notice on the CPU usage graph a large spike. By simply running the mouse pointer over that point, another pop up box will state which process caused that spike.

Process	PID	CPU	Description	Company Name
System Idle Process	0	95.38		
Interrupts	n/a		Hardware Interrupts	
DPCs	n/a		Deferred Procedure Calls	
System	4	1.54		
smss.exe	1408		Windows NT Session Manager	Microsoft Corporation
csrss.exe	1592		Client Server Runtime Process	Microsoft Corporation
winlogon.exe	1616		Windows NT Logon Application	Microsoft Corporation
services.exe	1668	1.54	Services and Controller app	Microsoft Corporation
nlservice.exe	1864		IBM Lotus Notes/Domino	IBM Corp
nsl.exe	1880		IBM Lotus Notes/Domino	IBM Corp
ati2evco.exe	1900		ATI External Event Utility EXE Module	ATI Technologies Inc.
svchost.exe	1920		Generic Host Process for Win32 Services	Microsoft Corporation
wmiprvse.exe	3524		WMI	Microsoft Corporation
cscontrol.exe	2036		CSA Service Control	Cisco Systems, Inc.
leventmgr.exe	136		Cisco Security Agent component	Cisco Systems, Inc.
okclient.exe	2228		Cisco Security Agent component	Cisco Systems, Inc.
svchost.exe	396		Generic Host Process for Win32 Services	Microsoft Corporation
svchost.exe	440		Generic Host Process for Win32 Services	Microsoft Corporation
EvtEng.exe	524		EvtEng Module	Intel Corporation
S24EvMon.exe	584		Event Monitor - Supports driver extensions to NIC Driver for wirele...	Intel Corporation
WLKEEPER.exe	616		WLKEEPER	Intel Corporation
svchost.exe	820		Generic Host Process for Win32 Services	Microsoft Corporation
svchost.exe	860		Generic Host Process for Win32 Services	Microsoft Corporation
ccEvtMgr.exe	1176		Symantec Event Manager Service	Symantec Corporation
ccSetMgr.exe	1192		Symantec Settings Manager Service	Symantec Corporation
spoolsv.exe	1360		Spooler SubSystem App	Microsoft Corporation
AMBroker.exe	956			
svchost.exe	988		Generic Host Process for Win32 Services	Microsoft Corporation
cvpnd.exe	1008		Cisco Systems VPN Client	Cisco Systems, Inc.
DefWatch.exe	1040		Virus Definition Daemon	Symantec Corporation
LpsSearchSvc.exe	1000		Local Search Service	Microsoft Corporation

CPU Usage: 4.62% Commit Charge: 14.93% Processes: 61

Figure 7: Process Explorer – Hierarchical and color-coded process listing

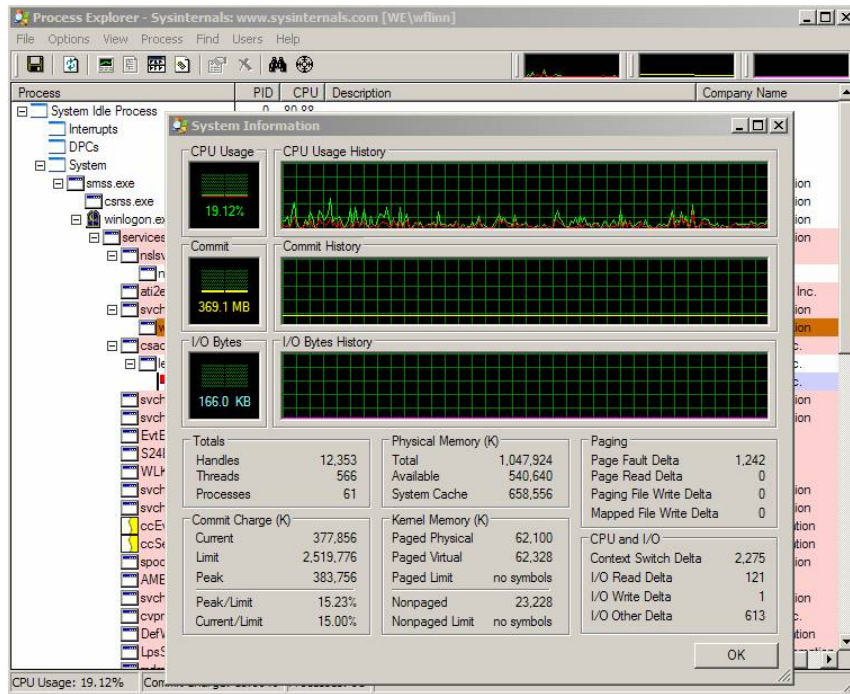


Figure 8: Process Explorer – Pop-up System Information graphs

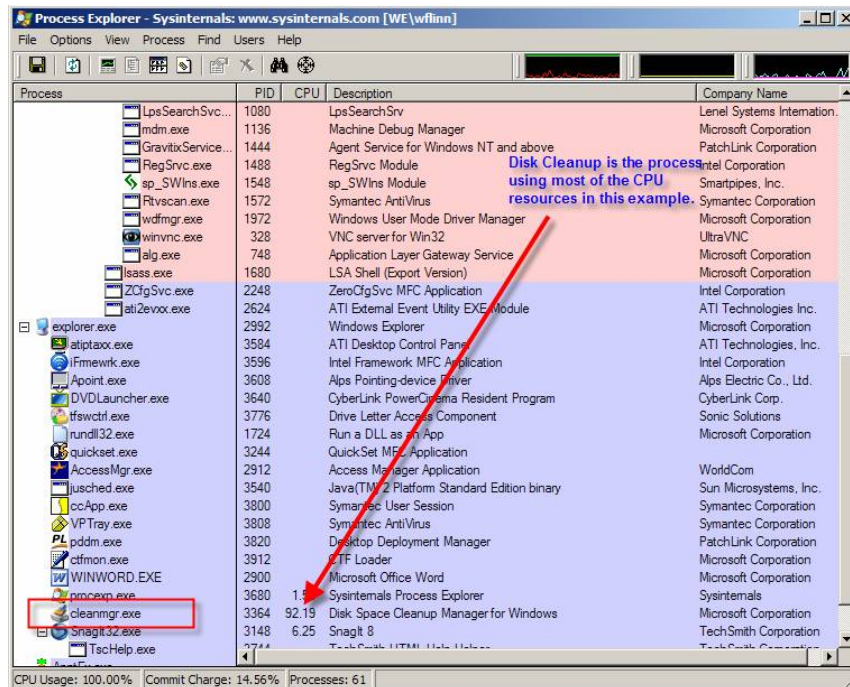


Figure 9: Process Explorer – CPU usage and process listing example

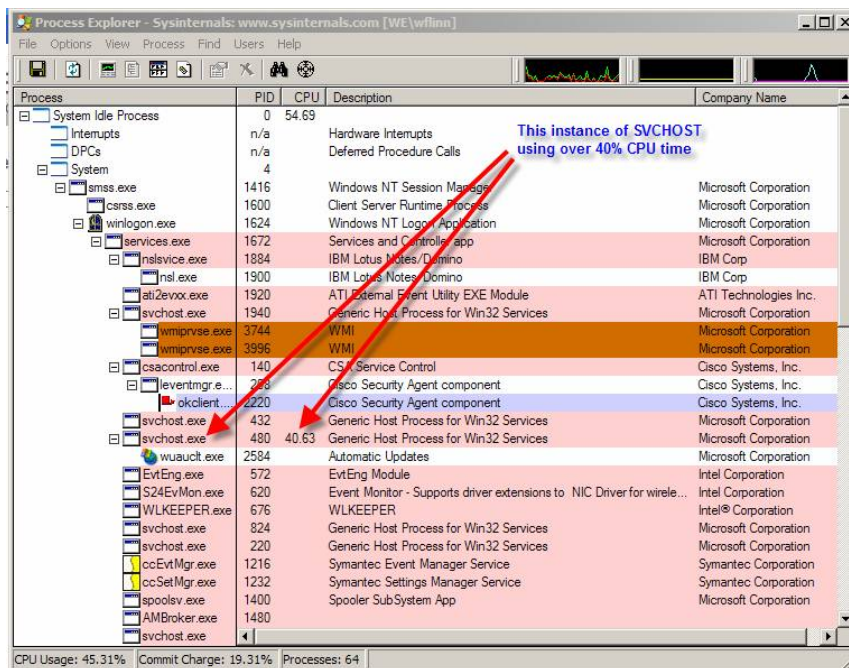


Figure 10: Process Explorer – SVCHOST.EXE and the specific program that spawned it – in this case Automatic Updates

This tool is particularly useful for finding malware because it gives a much more descriptive listing of the running processes, and what applications are spawning them. Sometimes malware authors will write their program so as to hide its activity within a normally recognized process. SVCHOST.EXE is an example – which, as mentioned previously, is a commonly used process, and is often seen running under multiple instances. It would be very easy to hide malware when it uses this process. Viewing Task Manager, the only information about it is the fact that SVCHOST is running, but no further information about what particular program spawned that process. Process Explorer, on the other hand, gives more information about these processes, so that you can tell if a valid piece of software is causing a process to run, or whether or not it is a piece of malware. As mentioned previously, if you notice a process running, but do not recognize the name, there are a number of [web sites](#) that will list each process and what it does, and whether or not it is commonly associated with malware. Just “Google” it!

## Summary of Performance Indicators and Corrective Action:

Using the information from the performance monitoring tools, we can now take a look at what can be done to improve performance. By taking a look at what sub-systems are suffering performance problems, you can decide which actions to take next:

**General Performance Checks and Improvements:** Eliminate the basics first. Make sure that you have scanned for viruses, spyware, and other malicious processes. Then make sure your hard drive is cleaned up using the built in Disk Cleanup and Defrag tools built into Windows. You may also want to explore using some of the Sysinternals or other third-party tools for defragmenting the page file and the registry. These are regular maintenance tasks that should be part of an ongoing [preventive maintenance routine](#). Do the following in order:

- Scan for viruses
- Scan for spyware
- Check for other malicious processes such as rootkits

- Remove all malware
- Ensure your computer's patches are up to date
- Run Disk Cleanup
- Run Defrag. Defragment the hard drive, but also defragment the paging file. To defrag the paging file, you need a free tool from Sysinternals (now Microsoft) called PageDefrag to do this. You can find this tool [here](#).
- What was the last thing you installed? If your computer is suddenly running sluggishly, eliminate a recent patch, new software, or updated hardware drivers from the equation.

**High % Processor (CPU) Usage:** Now that the basics are taken care of, go back to your performance analysis and take a look at which ones were showing high or abnormal values. If the CPU is being consumed at high levels on a consistent basis, take a look at the following:

- Are there too many start-up applications or processes? If so, use MSCONFIG to disable a few of them and see which ones are causing the problems.
- Is it an older system? If so, the CPU may not be robust enough to handle the workload of the applications you are using now. It might be time for a CPU upgrade. This often involves upgrading (replacing) the motherboard as well.
- Is this a server? If so, consider offloading some of the workload to another existing server or build dedicated servers for the applications and services that are the most needy.

**High Avg. Disk Queue Length:** Anything above "2" means that there are a lot of read/write operations waiting their turn. Try the following:

- Disk cleanup and defrag to help the disk drive(s) operate more efficiently.
- Is the hard drive getting too full? Try removing applications that are no longer needed or archiving some data that is no longer needed to CDs or other storage. Try adding additional hard drives.
- Is the disk drive old? Maybe time to upgrade to a newer and faster type of drive. The original hard drive may also be starting to fail – run CHKDSK or other hard drive diagnostics to determine if this is the problem.
- Is RAID a possibility? If your motherboard supports RAID, add hard drives and configure RAID 0, for example, to make read/write operations faster. If your motherboard doesn't support RAID, there are inexpensive third-party disk drive adapters available that do support RAID. RAID configurations can add performance and redundancy benefits.

**High Pages/Sec values:** This is simple – look at the amount of RAM you have installed, and install more. You may also have RAM that is starting to malfunction as well. Try the following:

- Run a memory diagnostic. A [free memory diagnostic](#) can be obtained from Microsoft at this link.
- If the installed RAM in the machine is 512MB or less, install more. 1GB of RAM can make a huge difference.
- If you OS is Windows Vista – Get a compatible USB flash drive and implement SpeedBoost to use the faster flash drive for storage instead of the slower hard drives.

## Wrapping It All Up:

Computer performance is just as much a matter of security as anti-virus, firewalls, or other security measures. For one thing, performance directly affects the availability of your data (remember the C-I-A triad of information security?). After all, if you can't get to your data because of a poorly performing computer, then availability suffers, and you get frustrated by slow

performance. Especially if this is a server, then many users are being affected, and data availability suffers.

In looking for performance issues, you may very well find a process that is the culprit, and your research may reveal that this errant process is actually a malicious process caused by a virus or other malware. Task Manager can give you a good idea of which processes are consuming large amounts of resources, but Sysinternals Process Explorer can give you a much more descriptive and detailed listing of these processes. This is especially helpful if there are several instances of the same process listed, and you need to know which one is causing the problem.

It is a good idea to find out how your computer is performing normally, then monitor it periodically to see if any performance trends can be identified, and particularly to notice if any degradations are beginning to occur. When diagnosing performance problems, it is important to try to narrow down when the performance problem started. For instance, did the problem start right after "Patch Tuesday?" A patch may be causing the problem. Did the problem start after downloading and installing some files on the Internet or opening an email attachment? Malware be the culprit in this case. Did the problem start after installing some software that you just purchased? The software possibly has some inefficient code, or is possibly conflicting with another part of the OS. Know how your computer performs normally, and keep an eye on performance after major events such as installing software or security patches.

There are so many factors that can affect computer performance, but there are some easy ways to diagnose potential performance issues. Use the Windows built-in tools, and explore some of the other free tools offered for download by Microsoft. These can be a big help in keeping computer performance at peak levels and keep your data secure from an availability point of view.