Processes

Patrick.j.rice@gmail.com

In computing, a process is an instance of a computer program that is being executed.

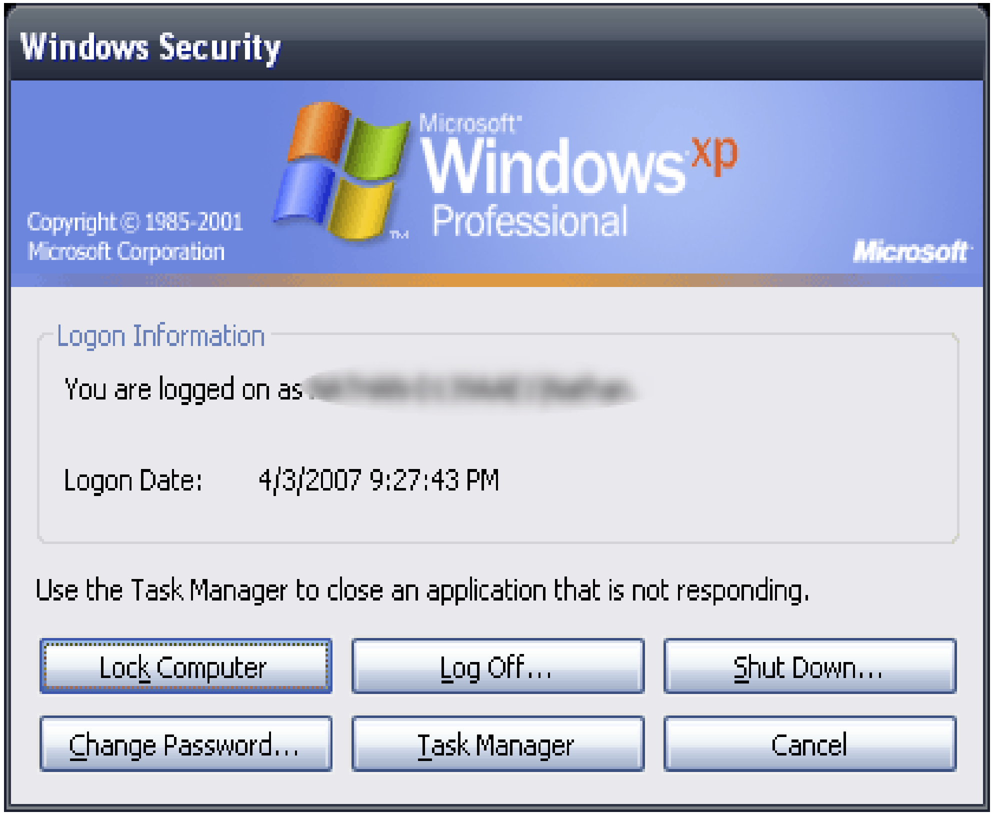
In simple English its a computer program running but it can run multiple versions of the same program

An Example would be internet explorer open twice.

Its the same program running but running twice.

•Ctrl-Alt-Del

- Ctrl-Alt-Del, also known as the "three-finger salute



Windows Security

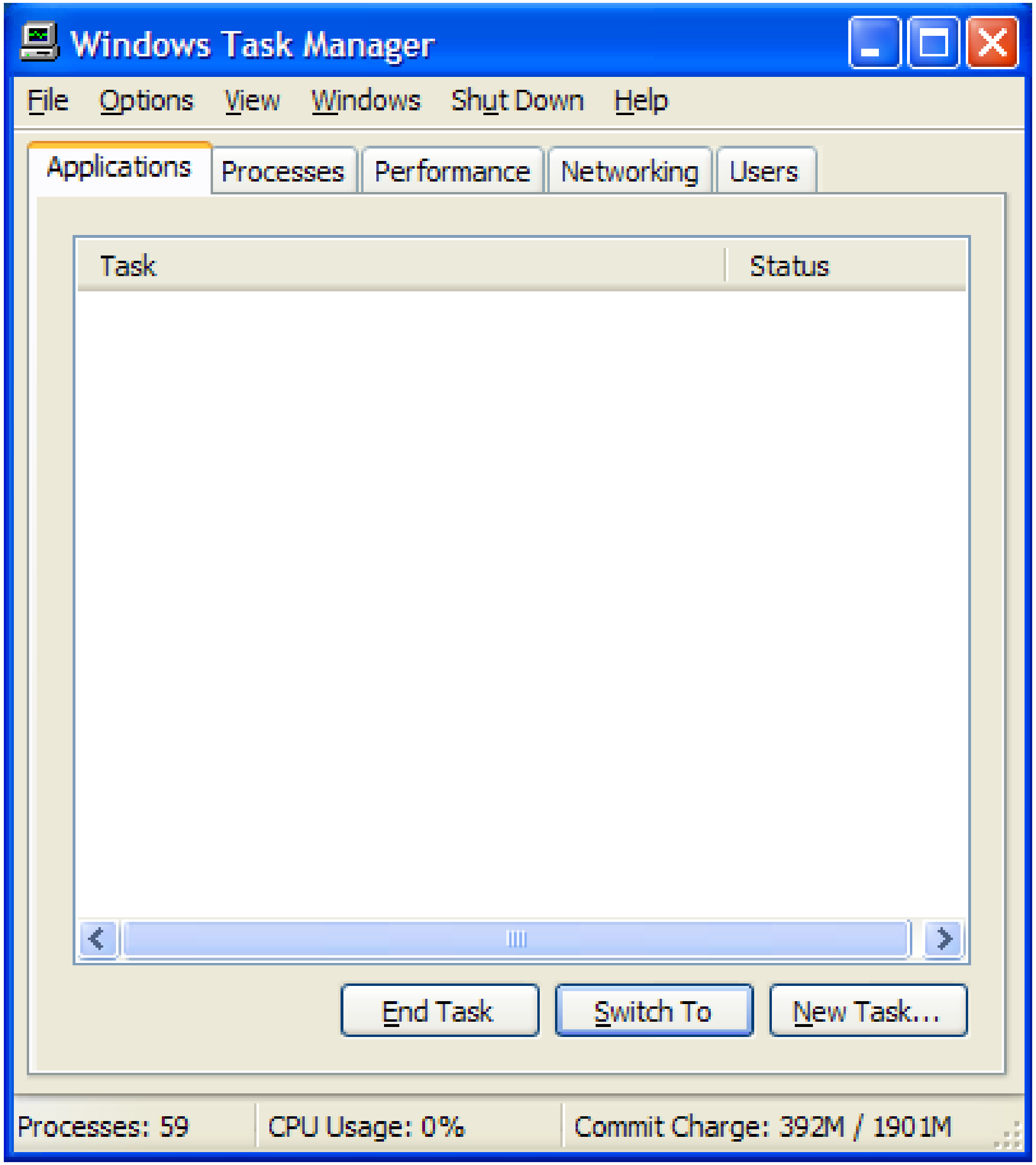
Copyright © 1985-2001
Microsoft Corporation

Logon Information

You are logged on as [redacted]

Logon Date: 4/3/2007 9:27:43 PM

Use the Task Manager to close an application that is not responding.



Processes: 59 CPU Usage: 0% Commit Charge: 392M / 1901M

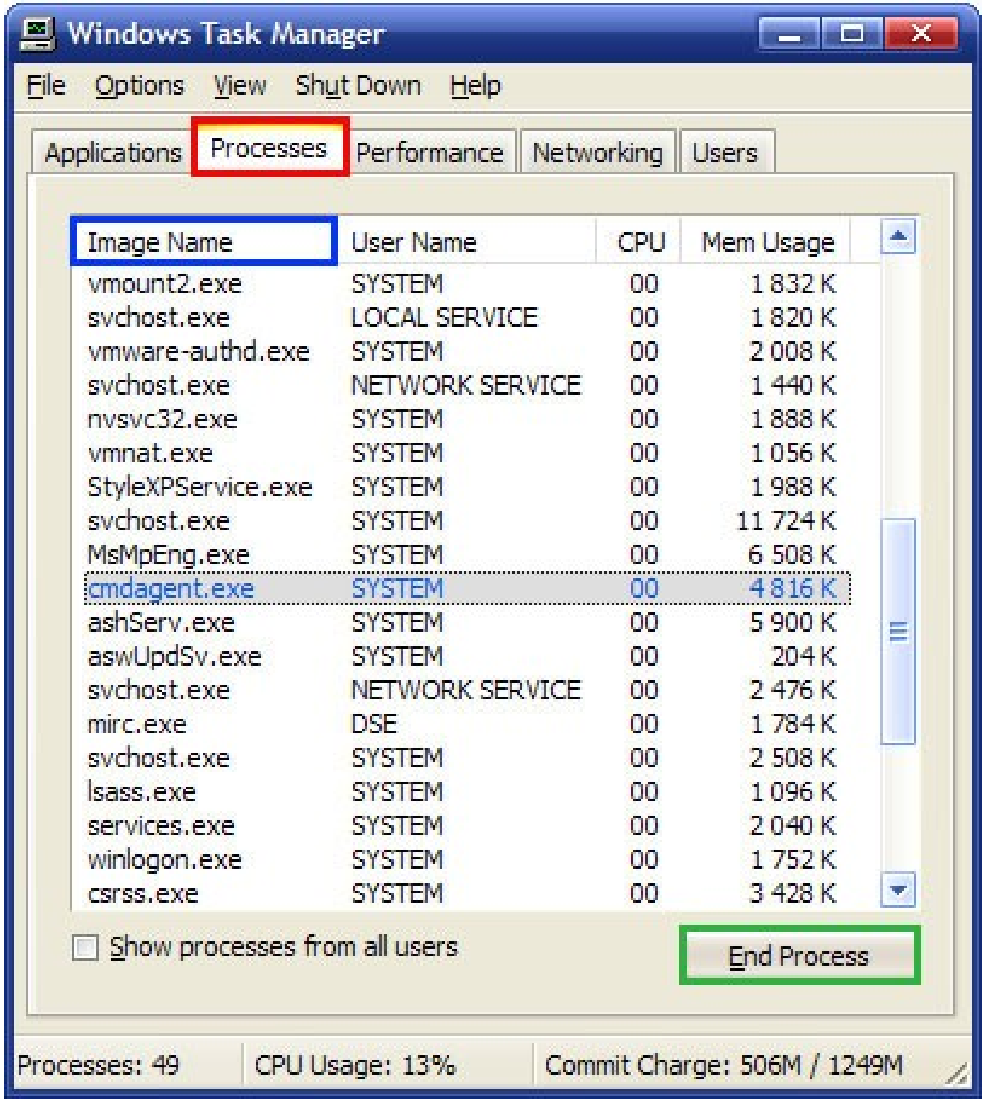


Image Name	User Name	CPU	Mem Usage
vmount2.exe	SYSTEM	00	1 832 K
svchost.exe	LOCAL SERVICE	00	1 820 K
vmware-authd.exe	SYSTEM	00	2 008 K
svchost.exe	NETWORK SERVICE	00	1 440 K
nvsvc32.exe	SYSTEM	00	1 888 K
vmnat.exe	SYSTEM	00	1 056 K
StyleXPService.exe	SYSTEM	00	1 988 K
svchost.exe	SYSTEM	00	11 724 K
MsMpEng.exe	SYSTEM	00	6 508 K
cmdagent.exe	SYSTEM	00	4 816 K
ashServ.exe	SYSTEM	00	5 900 K
aswUpdSv.exe	SYSTEM	00	204 K
svchost.exe	NETWORK SERVICE	00	2 476 K
mirc.exe	DSE	00	1 784 K
svchost.exe	SYSTEM	00	2 508 K
lsass.exe	SYSTEM	00	1 096 K
services.exe	SYSTEM	00	2 040 K
winlogon.exe	SYSTEM	00	1 752 K
csrss.exe	SYSTEM	00	3 428 K

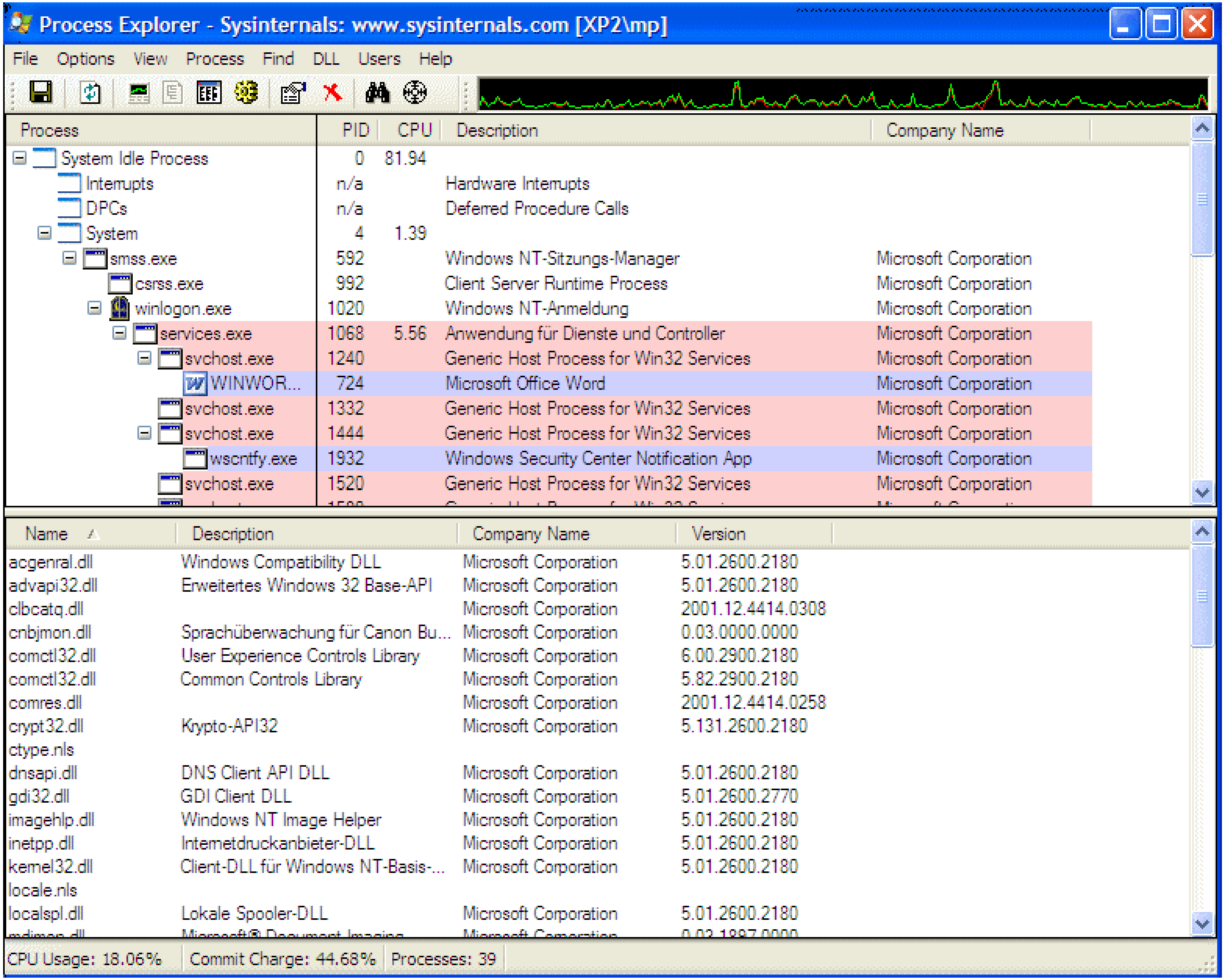
Processes: 49 CPU Usage: 13% Commit Charge: 506M / 1249M

The Columns

- The Mem Usage column on the Processes tab is actually the process' working set. A process has little or no control over its working set, which turns this column useless to determine how much memory a process is consuming.
- The VM Size column (not shown by default) is not the amount of virtual memory used by the process; it is actually the process' private bytes.
- The CPU column is calculated by trimming the CPU consumption to fit in a two-digit fashion, which can be inaccurate. A process consuming 0.9% of CPU will be reported as 00 in Task Manager.
- The System Idle Process is the first process that is created when Windows is loaded, and it always has a process ID of 0. When the CPU has no other work to do, the System Idle Process is run and it simply puts the CPU in a sleep state. There is actually one System Idle Process for each CPU in the system. Task Manager accounts interrupts and DPC time under the System Idle Processes CPU usage.

Process Explorer

- A tool to monitor processes
- Process Explorer shows you information about which handles and DLLs processes have opened or loaded.
- http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx


Process Explorer - Sysinternals: www.sysinternals.com [XP2\mp]
File
Options
View
Process
Find
DLL
Users
Help

Process	PID	CPU	Description	Company Name
System Idle Process	0	81.94		
Interrupts	n/a		Hardware Interrupts	
DPCs	n/a		Deferred Procedure Calls	
System	4	1.39		
smss.exe	592		Windows NT-Sitzungs-Manager	Microsoft Corporation
csrss.exe	992		Client Server Runtime Process	Microsoft Corporation
winlogon.exe	1020		Windows NT-Anmeldung	Microsoft Corporation
services.exe	1068	5.56	Anwendung für Dienste und Controller	Microsoft Corporation
svchost.exe	1240		Generic Host Process for Win32 Services	Microsoft Corporation
WINWOR...	724		Microsoft Office Word	Microsoft Corporation
svchost.exe	1332		Generic Host Process for Win32 Services	Microsoft Corporation
svchost.exe	1444		Generic Host Process for Win32 Services	Microsoft Corporation
wscntfy.exe	1932		Windows Security Center Notification App	Microsoft Corporation
svchost.exe	1520		Generic Host Process for Win32 Services	Microsoft Corporation

Name	Description	Company Name	Version
acgenral.dll	Windows Compatibility DLL	Microsoft Corporation	5.01.2600.2180
advapi32.dll	Erweitertes Windows 32 Base-API	Microsoft Corporation	5.01.2600.2180
clbcatq.dll		Microsoft Corporation	2001.12.4414.0308
cnbjmon.dll	Sprachüberwachung für Canon Bu...	Microsoft Corporation	0.03.0000.0000
comctl32.dll	User Experience Controls Library	Microsoft Corporation	6.00.2900.2180
comctl32.dll	Common Controls Library	Microsoft Corporation	5.82.2900.2180
comres.dll		Microsoft Corporation	2001.12.4414.0258
crypt32.dll	Krypto-API32	Microsoft Corporation	5.131.2600.2180
ctype.nls			
dnsapi.dll	DNS Client API DLL	Microsoft Corporation	5.01.2600.2180
gdi32.dll	GDI Client DLL	Microsoft Corporation	5.01.2600.2770
imagehlp.dll	Windows NT Image Helper	Microsoft Corporation	5.01.2600.2180
inetpp.dll	Internetdruckanbieter-DLL	Microsoft Corporation	5.01.2600.2180
kernel32.dll	Client-DLL für Windows NT-Basis-...	Microsoft Corporation	5.01.2600.2180
locale.nls			
localspl.dll	Lokale Spooler-DLL	Microsoft Corporation	5.01.2600.2180

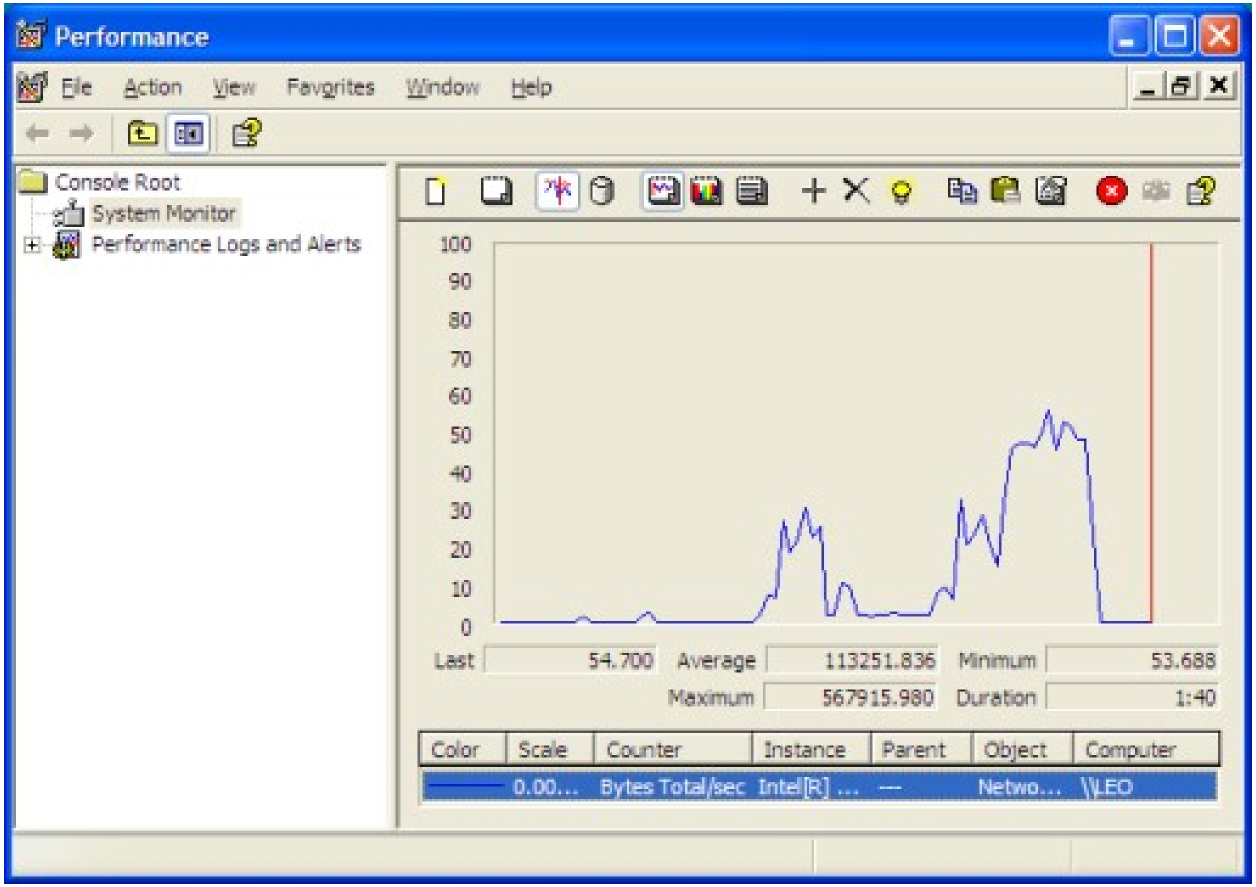
CPU Usage: 18.06% | Commit Charge: 44.68% | Processes: 39

SysInternals

- The Sysinternals web site was created in 1996 by Mark Russinovich and Bryce Cogswell to host their advanced system utilities and technical information. Microsoft acquired Sysinternals in July, 2006

http://technet.microsoft.com/en-us/sysinternals/default.aspx

Prefmon



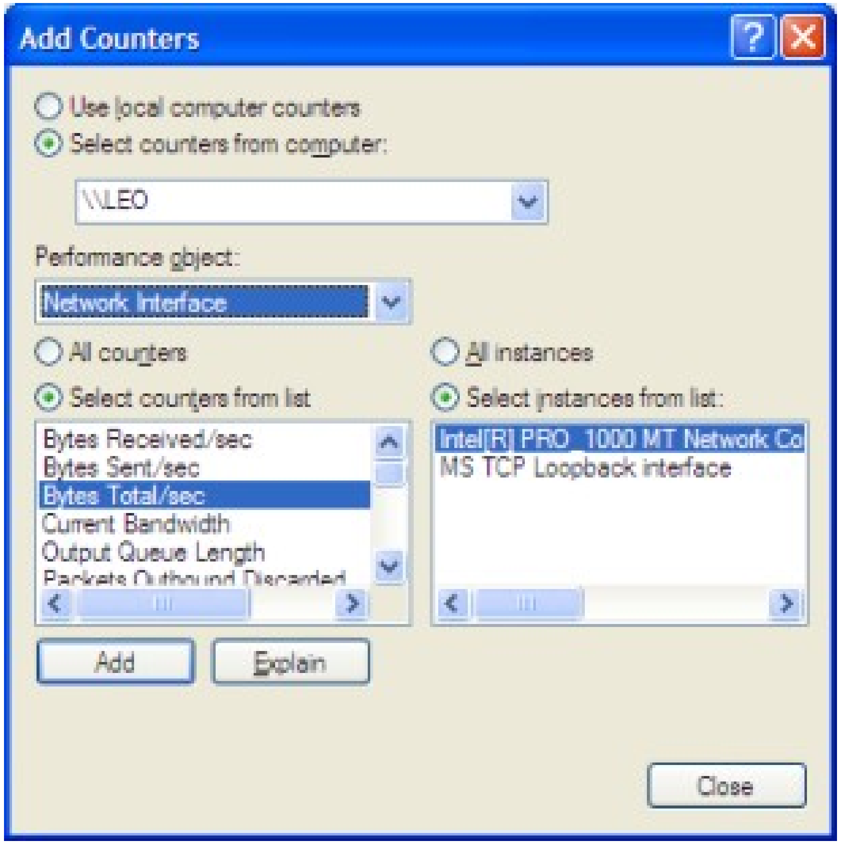
Last 54.700 Average 113251.836 Minimum 53.688
Maximum 567915.980 Duration 1:40

Color	Scale	Counter	Instance	Parent	Object	Computer
▬	0.00...	Bytes Total/sec	Intel[R] ...	---	Netwo...	\\LEO

- Monitors Performance over time

Prefmon

- Start, selecting Run, typing "perfmon" and pressing OK.
- select Add Counters
- The Performance Object dropdown lists several objects on your computer whose performance can be measured



Add Counters

○ Use local computer counters

● Select counters from computer:

\\LEO

Performance object:

Network Interface

○ All counters

● Select counters from list

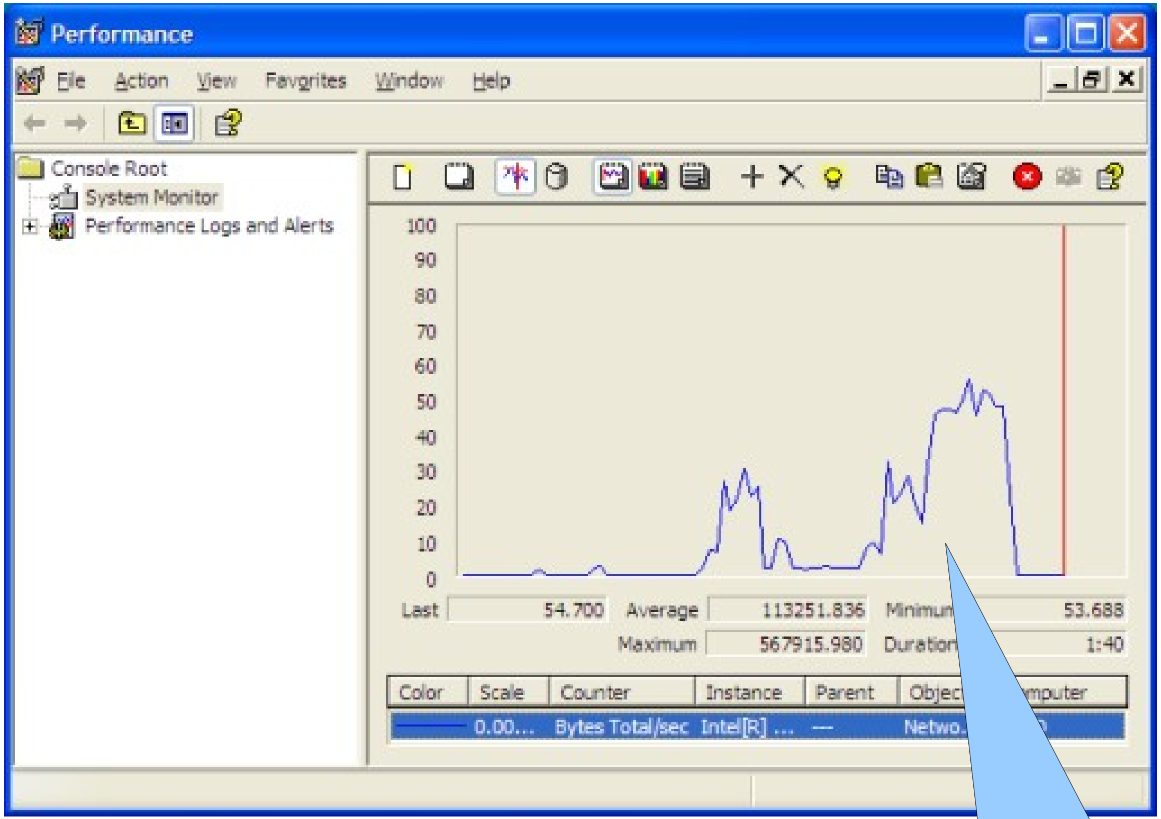
- Bytes Received/sec
- Bytes Sent/sec
- Bytes Total/sec
- Current Bandwidth
- Output Queue Length
- Packets Outbound Discarded

○ All instances

● Select instances from list:

- Intel[R] PRO_1000 MT Network Co
- MS TCP Loopback interface

Add your counter here e.g. network, Disk performance, Memory.


Performance
File Action View Favorites Window Help
Console Root
System Monitor
Performance Logs and Alerts
100
90
80
70
60
50
40
30
20
10
0

Last 54.700 Average 113251.836 Minimum 53.688

Maximum 567915.980 Duration 1:40

Color	Scale	Counter	Instance	Parent	Object	Computer
	0.00...	Bytes Total/sec	Intel[R] ...	---	Netwo...	

Produces a graph
Can analyse this to see
Performance issues

My Machine is Slow

- Is it
  - Memory
  - Disk
  - Cpu
- Use prefmon to analyse the problem
- Memory – Add Memory
- Disk – defrag
- Cpu – Remove processes

Task

- Get the Highest memory and Process load on the macnine by opening apps etc.
- Record it
- Kill off the proceses to reduce the load.