SYSINTERNALS LAB EXERCISE

Explore the tools and complete the exercises

Objective: Upon completion you will have gained a hands-on overview of a collection of advanced diagnostic and troubleshooting tools that can also be used for malware detection, analysis, and removal.

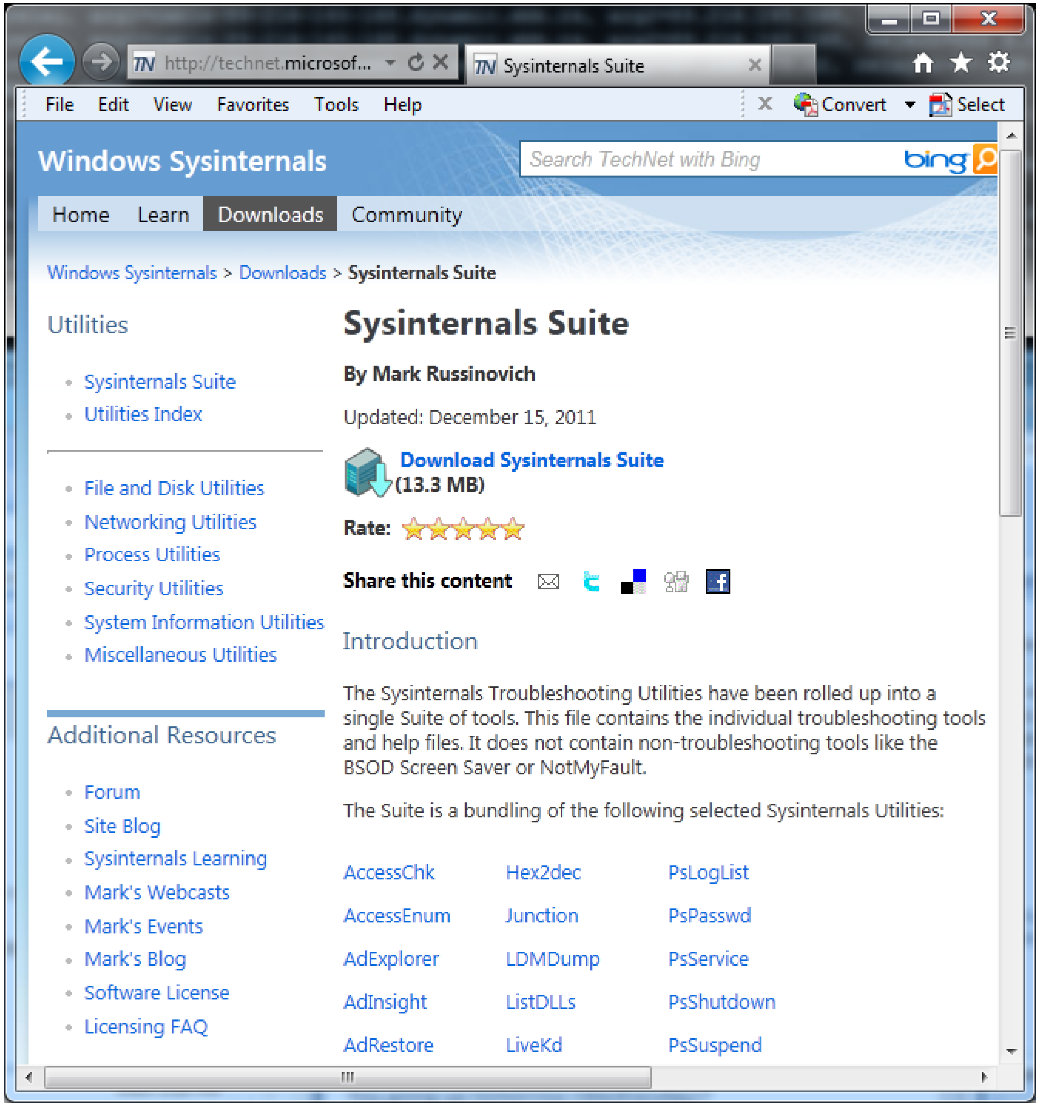
Some of the Sysinternals tools are Windows version specific, administrator privilege typically is required.

Sysinternals Lab

Sysinternals are free technical tools utilities to manage, diagnose, troubleshoot, and monitor a Microsoft Windows environment. The individual tools can be downloaded, ran live from the site, or downloaded as a suite.

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

To install or update the suite of tools:
Download SysinternalsSuite.zip file
Right-click | Properties | Unblock
Double-click | Extract all files
Select destination folder
    c:\bin\sysinternals or
    c:\tools\sysinternals
    c:\ProgramFiles\sysinternals   *
  * Prevents modification by non-administrative users
Optional: Add the location to the system Path variable



Windows Sysinternals

Home | Learn | Downloads | Community

Windows Sysinternals > Downloads > Sysinternals Suite

Utilities

- Sysinternals Suite
- Utilities Index

- File and Disk Utilities
- Networking Utilities
- Process Utilities
- Security Utilities
- System Information Utilities
- Miscellaneous Utilities

Additional Resources

- Forum
- Site Blog
- Sysinternals Learning
- Mark's Webcasts
- Mark's Events
- Mark's Blog
- Software License
- Licensing FAQ

Sysinternals Suite

By Mark Russinovich

Updated: December 15, 2011

Download Sysinternals Suite
(13.3 MB)

Rate: ★★★★★

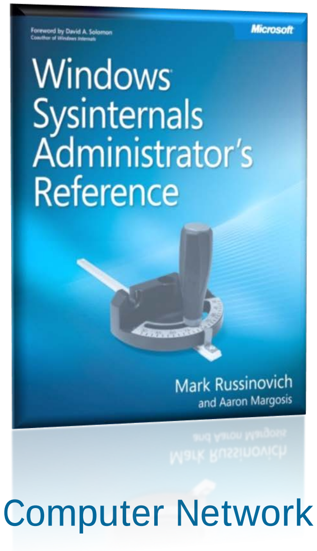
Share this content

Introduction

The Sysinternals Troubleshooting Utilities have been rolled up into a single Suite of tools. This file contains the individual troubleshooting tools and help files. It does not contain non-troubleshooting tools like the BSOD Screen Saver or NotMyFault.

The Suite is a bundling of the following selected Sysinternals Utilities:

AccessChk	Hex2dec	PsLogList
AccessEnum	Junction	PsPasswd
AdExplorer	LDMDump	PsService
AdInsight	ListDLLs	PsShutdown
AdRestore	LiveKd	PsSuspend


Foreword by David A. Solomon
Microsoft
Windows Sysinternals Administrator's Reference
Mark Russinovich
and Aaron Margosis

Reference Book
Published July 2011

Sysinternals Lab

Examples of the Sysinternals tools: (there are many more)

- AccessEnum shows access to directories, files and Registry keys
- Autoruns shows all the registry and file autostart settings
- Disk2vhd simplifies migrations of physical to virtual machines
- Diskmon shows all hard disk activity
- DiskView graphical disk sector utility
- Filemon shows file system activity
- Handle shows open files and processes using them
- Listdlls shows DLLs in use
- Process Explorer see what keys and files processes have opened
- Process Monitor see file, Registry, process, DLL activity in real-time
- RAMMap physical memory usage analysis utility
- RegMon shows Registry data in real time
- RootkitRevealer scan for rootkit-based malware
- SDelete DoD compliant file overwrite tool
- TCPView active socket command-line viewer
- VMMap process virtual and physical memory analysis tool

- PSTools collection of CLI tools (see next page)

Sysinternals Lab

PsTools CLI included in Sysinternals

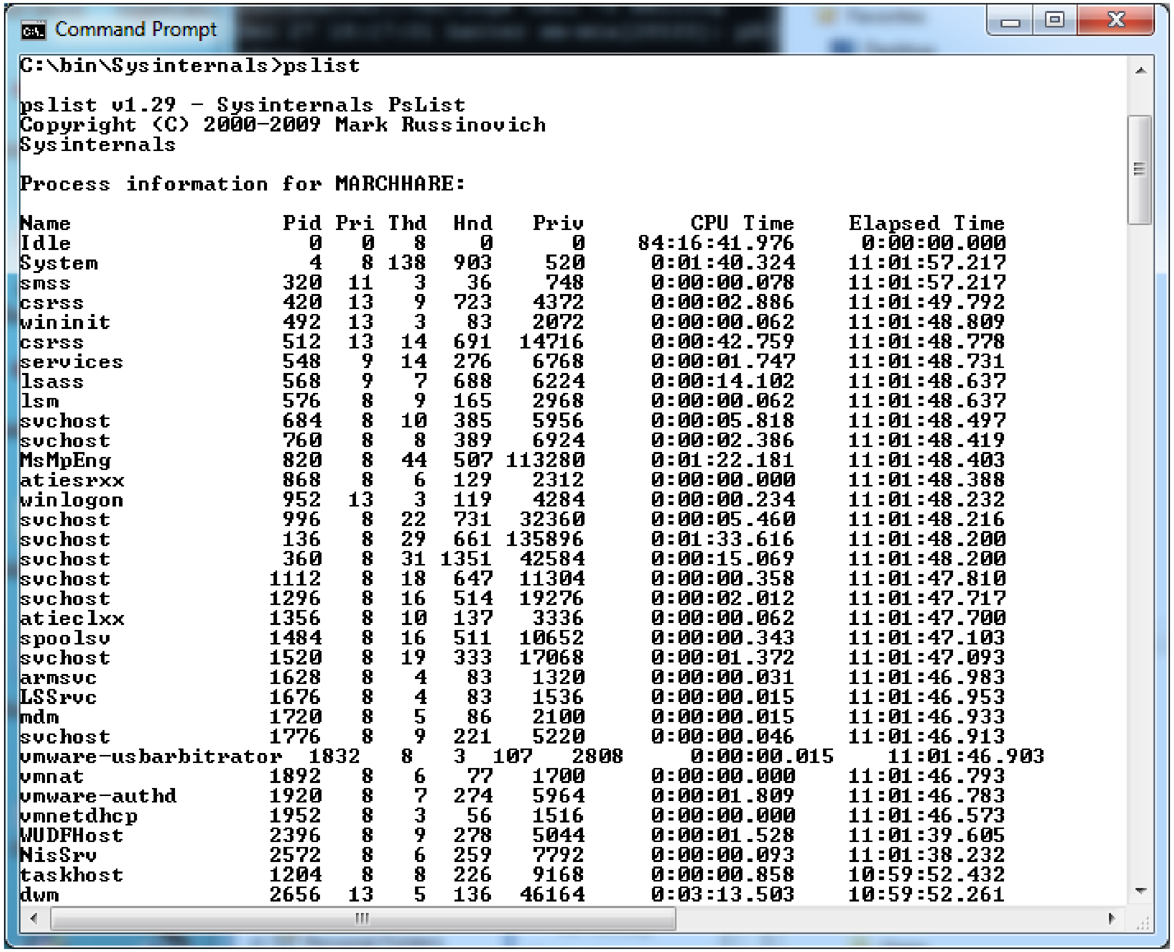
- PsExec runs processes remotely
- PSFile see what files are opened remotely
- PsGetSid displays security identifier (SID)
- PsInfo displays system information
- PsKill kills process by name or ID
- PsList lists details about a process
- PsLoggedon shows who’s logged locally
- PsLogList dump event log records
- PsPasswd changes account passwords
- PsService controls and views services
- PsShutdown shuts down and restarts PCs
- PsSuspend suspends processes

Pstools.chm is an HTML help file with usage information for all the tools.
All work locally and remotely, no manual remote software installation needed.
Note: For remote use - /accepteula

pslist

Similar to the Unix ps utility. Lists running processes and their memory and CPU usage. PsList can optionally show process parent-child relationships, list per-thread information, or continually self-update in task manager mode. PsList can report on local or remote processes.

pslist options include:
-? Show help
-d Show thread detail
-m Show memory detail
-t Show process tree
-x Show processes, memory information and threads



```
C:\bin\Sysinternals>pslist

pslist v1.29 - Sysinternals PsList
Copyright (C) 2000-2009 Mark Russinovich
Sysinternals

Process information for MARCHHARE:

Name                Pid Pri Thd  Hnd   Priv        CPU Time    Elapsed Time
Idle                  0   0   8    0      0    84:16:41.976     0:00:00.000
System                4   8 138  903    520     0:01:40.324    11:01:57.217
smss                320  11   3   36    748     0:00:00.078    11:01:57.217
csrss               420  13   9  723   4372     0:00:02.886    11:01:49.792
wininit             492  13   3   83   2072     0:00:00.062    11:01:48.809
csrss               512  13  14  691  14716     0:00:42.759    11:01:48.778
services            548   9  14  276   6768     0:00:01.747    11:01:48.731
lsass               568   9   7  688   6224     0:00:14.102    11:01:48.637
lsm                 576   8   9  165   2968     0:00:00.062    11:01:48.637
svchost             684   8  10  385   5956     0:00:05.818    11:01:48.497
svchost             760   8   8  389   6924     0:00:02.386    11:01:48.419
MsMpEng             820   8  44  507 113280     0:01:22.181    11:01:48.403
atiesrxx            868   8   6  129   2312     0:00:00.000    11:01:48.388
winlogon            952  13   3  119   4284     0:00:00.234    11:01:48.232
svchost             996   8  22  731  32360     0:00:05.460    11:01:48.216
svchost             136   8  29  661 135896     0:01:33.616    11:01:48.200
svchost             360   8  31 1351  42584     0:00:15.069    11:01:48.200
svchost            1112   8  18  647  11304     0:00:00.358    11:01:47.810
svchost            1296   8  16  514  19276     0:00:02.012    11:01:47.717
atieclxx           1356   8  10  137   3336     0:00:00.062    11:01:47.700
spoolsv            1484   8  16  511  10652     0:00:00.343    11:01:47.103
svchost            1520   8  19  333  17068     0:00:01.372    11:01:47.093
armsvc             1628   8   4   83   1320     0:00:00.031    11:01:46.983
LSSrvc             1676   8   4   83   1536     0:00:00.015    11:01:46.953
mdm                1720   8   5   86   2100     0:00:00.015    11:01:46.933
svchost            1776   8   9  221   5220     0:00:00.046    11:01:46.913
vmware-usbarbitrator  1832   8   3  107   2808     0:00:00.015    11:01:46.903
vmnat              1892   8   6   77   1700     0:00:00.000    11:01:46.793
vmware-authd       1920   8   7  274   5964     0:00:01.809    11:01:46.783
vmnetdhcp          1952   8   3   56   1516     0:00:00.000    11:01:46.573
WUDFHost           2396   8   9  278   5044     0:00:01.528    11:01:39.605
NisSrv             2572   8   6  259   7792     0:00:00.093    11:01:38.232
taskhost           1204   8   8  226   9168     0:00:00.858    10:59:52.432
dwm                2656  13   5  136  46164     0:03:13.503    10:59:52.261
```

All memory values are displayed in KB.
Abbreviation key:

Pri	Priority
Thd	Number of Threads
Hnd	Number of Handles
VM	Virtual Memory
WS	Working Set
Priv	Private Virtual Memory

pslist output

PsExec

- psexec execute processes on remote computers
- Uses redirected console I/O
  - e.g. remote-enable console applications
- Execute processes as System

- psexec \\computer   also   @file
- psexec \\computer –u username –p password

- -s Run process in system account
- -l   Run the process as a limited user
- -h Use the accounts elevated context

Redirected Console Tips

- Don’t forget /accepteula !
  - Remoted Sysinternals utilities will hang

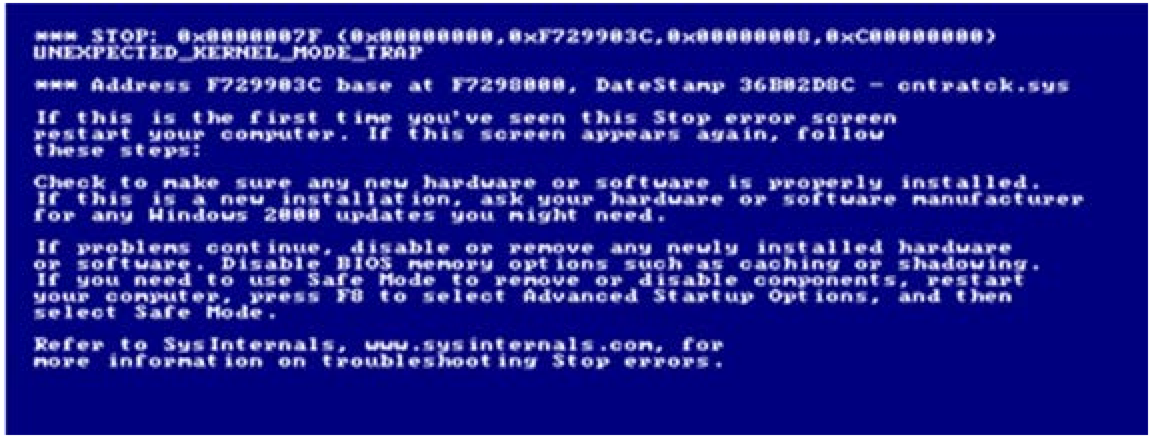
- Things you can’t do in a redirected console:
  - CLS
  - MORE
  - Text coloring
  - Tab completion
  - PowerShell v1

Misc. Tools

- du – Report directory disk usage
- streams – view alternate data streams
- strings – see ASCII strings
- Disk and cache utilities

Tools for:

- Active Directory
  - Adexplorer – AD viewer and editor
  - AdInsight – LDAP monitoring tool
- Defragmentation
  - Contig
- File links
- Migration
- Encryption
- Conversion



```
*** STOP: 0x0000007F (0x00000000,0xF729903C,0x00000008,0xC0000000)
UNEXPECTED_KERNEL_MODE_TRAP

*** Address F729903C base at F7290000, DateStamp 36B02D8C - cntratck.sys

If this is the first time you've seen this Stop error screen
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows 2000 updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Refer to SysInternals, www.sysinternals.com, for
more information on troubleshooting Stop errors.
```

Available at the website: Bluescreen (BSOD) Screen Saver

Lab Exercise

From a Command Prompt, CD to sysinternals folder:

```
Run: psinfo                        # default output
Run: psinfo -?                     # to see the built-in help
Run: psinfo -s                     # show installed software
Run: psinfo -d                     # show disk volume info
Run: psinfo -s and -d  on a remote lab computer

Run: pslist                        # default output
Run: pslist -?                     # to see the built-in help
Run: pslist -t                     # show process tree
Run: pslist -m                     # show memory info
Run: pslist -t and -m  on a remote lab computer

Run: du –v / | more                # enumerate file system
```

ProcessExplorer

- A process is a container for a set of resources, including one or more threads, virtual memory address space, open handles, security tokens, etc.
- Threads – not processes – do the work and consume CPU, memory, etc.
- ProcessExplorer works on all Windows platforms
- ProcessExplorer starts where Task Manager ends:
  - Detailed information about running processes, including paths and command-lines
  - Description of EXE
  - SID from process security token
  - View DLLs loaded by processes
    - Including version numbers
  - See what handles processes have opened
  - Examine services running within service processes

ProcessExplorer

Process Explorer can be used to:

- Detect DLL versioning problems
- Compare output from *good* system with output from *broken* system
- Use search feature to determine what process is holding a file or directory open
- View the state of synchronization objects (mutexes, semaphores, events)
- Detect handle leaks using refresh difference highlighting
- Uses undocumented functions for enumeration
- Provides performance graphs for CPU(total or by core), memory, I/O, and GPU. Moving the mouse over part of a graph results in the time of the corresponding data point being shown in the graph as a popup.

ProcessExplorer

CPU, Memory, IO, & GPU Utilization Graphs

Click to sort on key

Selected (clicked on)

Application Icon

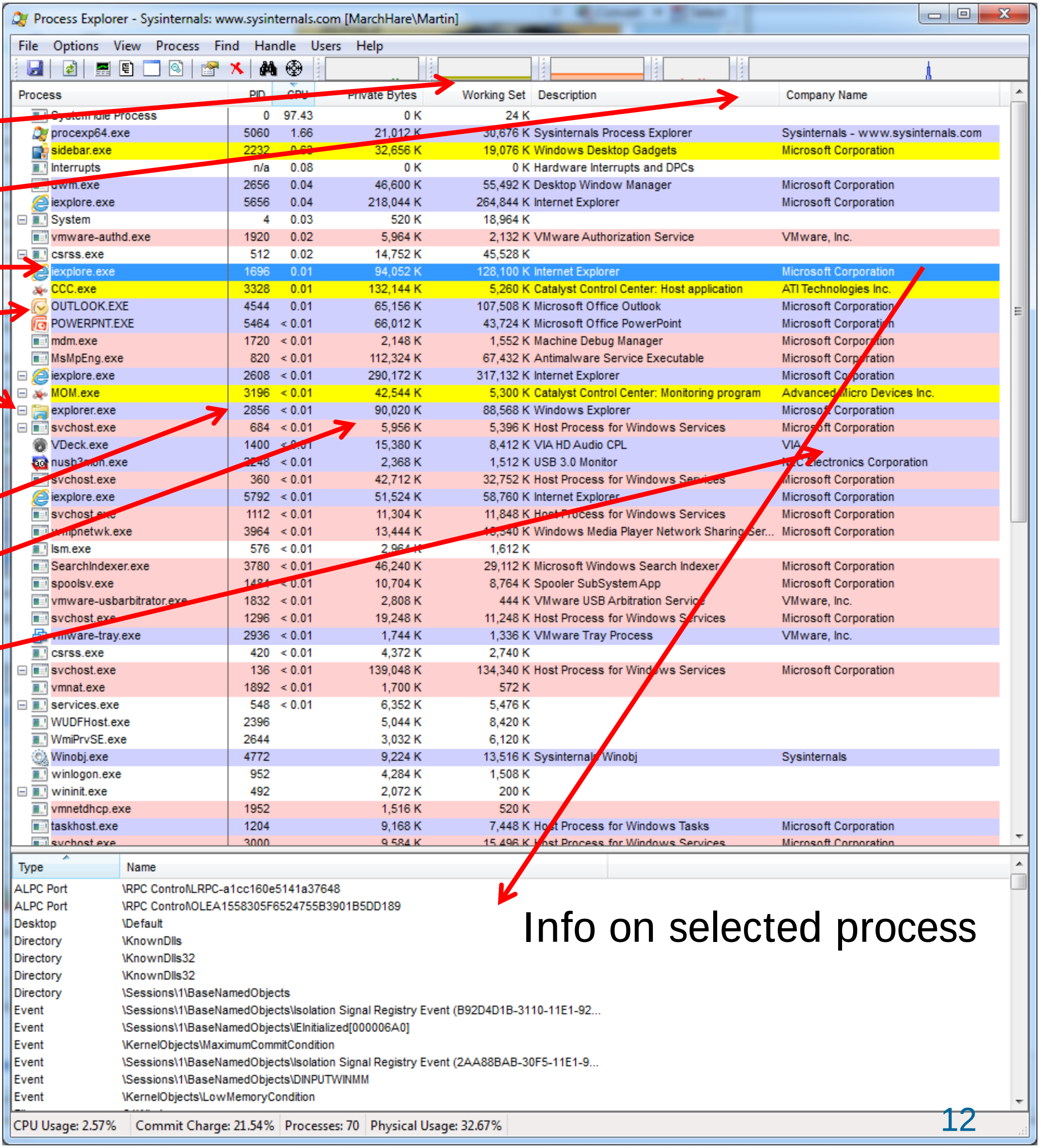
PID

Memory

Company name

Violet - Packed Images
Pink - Services
Yellow - .NET processes
Dark gray - Suspended
Light gray - lacks focus

Process Explorer shows information about which handles and DLLs processes have opened or loaded



Process Explorer - Sysinternals: www.sysinternals.com [MarchHare\Martin]
File Options View Process Find Handle Users Help

Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
System Idle Process	0	97.43	0 K	24 K		
procexp64.exe	5060	1.66	21,012 K	30,676 K	Sysinternals Process Explorer	Sysinternals - www.sysinternals.com
sidebar.exe	2232	0.63	32,656 K	19,076 K	Windows Desktop Gadgets	Microsoft Corporation
Interrupts	n/a	0.08	0 K	0 K	Hardware Interrupts and DPCs	
dwm.exe	2656	0.04	46,600 K	55,492 K	Desktop Window Manager	Microsoft Corporation
iexplore.exe	5656	0.04	218,044 K	264,844 K	Internet Explorer	Microsoft Corporation
System	4	0.03	520 K	18,964 K		
vmware-authd.exe	1920	0.02	5,964 K	2,132 K	VMware Authorization Service	VMware, Inc.
csrss.exe	512	0.02	14,752 K	45,528 K		
iexplore.exe	1696	0.01	94,052 K	128,100 K	Internet Explorer	Microsoft Corporation
CCC.exe	3328	0.01	132,144 K	5,260 K	Catalyst Control Center: Host application	ATI Technologies Inc.
OUTLOOK.EXE	4544	0.01	65,156 K	107,508 K	Microsoft Office Outlook	Microsoft Corporation
POWERPNT.EXE	5464	< 0.01	66,012 K	43,724 K	Microsoft Office PowerPoint	Microsoft Corporation
mdm.exe	1720	< 0.01	2,148 K	1,552 K	Machine Debug Manager	Microsoft Corporation
MsMpEng.exe	820	< 0.01	112,324 K	67,432 K	Antimalware Service Executable	Microsoft Corporation
iexplore.exe	2608	< 0.01	290,172 K	317,132 K	Internet Explorer	Microsoft Corporation
MOM.exe	3196	< 0.01	42,544 K	5,300 K	Catalyst Control Center: Monitoring program	Advanced Micro Devices Inc.
explorer.exe	2856	< 0.01	90,020 K	88,568 K	Windows Explorer	Microsoft Corporation
svchost.exe	684	< 0.01	5,956 K	5,396 K	Host Process for Windows Services	Microsoft Corporation
VDeck.exe	1400	< 0.01	15,380 K	8,412 K	VIA HD Audio CPL	VIA
nusb3mon.exe	2248	< 0.01	2,368 K	1,512 K	USB 3.0 Monitor	NEC Electronics Corporation
svchost.exe	360	< 0.01	42,712 K	32,752 K	Host Process for Windows Services	Microsoft Corporation
iexplore.exe	5792	< 0.01	51,524 K	58,760 K	Internet Explorer	Microsoft Corporation
svchost.exe	1112	< 0.01	11,304 K	11,848 K	Host Process for Windows Services	Microsoft Corporation
wmpnetwk.exe	3964	< 0.01	13,444 K	10,540 K	Windows Media Player Network Sharing Ser...	Microsoft Corporation
lsm.exe	576	< 0.01	2,964 K	1,612 K		
SearchIndexer.exe	3780	< 0.01	46,240 K	29,112 K	Microsoft Windows Search Indexer	Microsoft Corporation
spoolsv.exe	1484	< 0.01	10,704 K	8,764 K	Spooler SubSystem App	Microsoft Corporation
vmware-usbarbitrator.exe	1832	< 0.01	2,808 K	444 K	VMware USB Arbitration Service	VMware, Inc.
svchost.exe	1296	< 0.01	19,248 K	11,248 K	Host Process for Windows Services	Microsoft Corporation
vmware-tray.exe	2936	< 0.01	1,744 K	1,336 K	VMware Tray Process	VMware, Inc.
csrss.exe	420	< 0.01	4,372 K	2,740 K		
svchost.exe	136	< 0.01	139,048 K	134,340 K	Host Process for Windows Services	Microsoft Corporation
vmnat.exe	1892	< 0.01	1,700 K	572 K		
services.exe	548	< 0.01	6,352 K	5,476 K		
WUDFHost.exe	2396		5,044 K	8,420 K		
WmiPrvSE.exe	2644		3,032 K	6,120 K		
Winobj.exe	4772		9,224 K	13,516 K	Sysinternals Winobj	Sysinternals
winlogon.exe	952		4,284 K	1,508 K		
wininit.exe	492		2,072 K	200 K		
vmnetdhcp.exe	1952		1,516 K	520 K		
taskhost.exe	1204		9,168 K	7,448 K	Host Process for Windows Tasks	Microsoft Corporation
svchost.exe	3000		9,584 K	15,496 K	Host Process for Windows Services	Microsoft Corporation

Type	Name
ALPC Port	\RPC Control\LRPC-a1cc160e5141a37648
ALPC Port	\RPC Control\OLEA1558305F6524755B3901B5DD189
Desktop	\Default
Directory	\KnownDlls
Directory	\KnownDlls32
Directory	\KnownDlls32
Directory	\Sessions\1\BaseNamedObjects
Event	\Sessions\1\BaseNamedObjects\Isolation Signal Registry Event (B92D4D1B-3110-11E1-92...
Event	\Sessions\1\BaseNamedObjects\IEInitialized[000006A0]
Event	\KernelObjects\MaximumCommitCondition
Event	\Sessions\1\BaseNamedObjects\Isolation Signal Registry Event (2AA88BAB-30F5-11E1-9...
Event	\Sessions\1\BaseNamedObjects\DINPUTWINMM
Event	\KernelObjects\LowMemoryCondition

CPU Usage: 2.57% | Commit Charge: 21.54% | Processes: 70 | Physical Usage: 32.67%

Info on selected process

Process Explorer

Shortcut Keys

Ctrl+C	Copy current row
Ctrl+D	Display DLL view
Ctrl+H	Display handle view
Ctrl+I	Display SystemInformation view
Ctrl+L	Display/Hide lower panel view
Ctrl+M	Search online
Ctrl+R	Start a new process (File|Run)
Ctrl+S	Saved displayed data to file (File|Save
Ctrl+T	Show process list in tree view
Space	Pause|Resume automatic updating

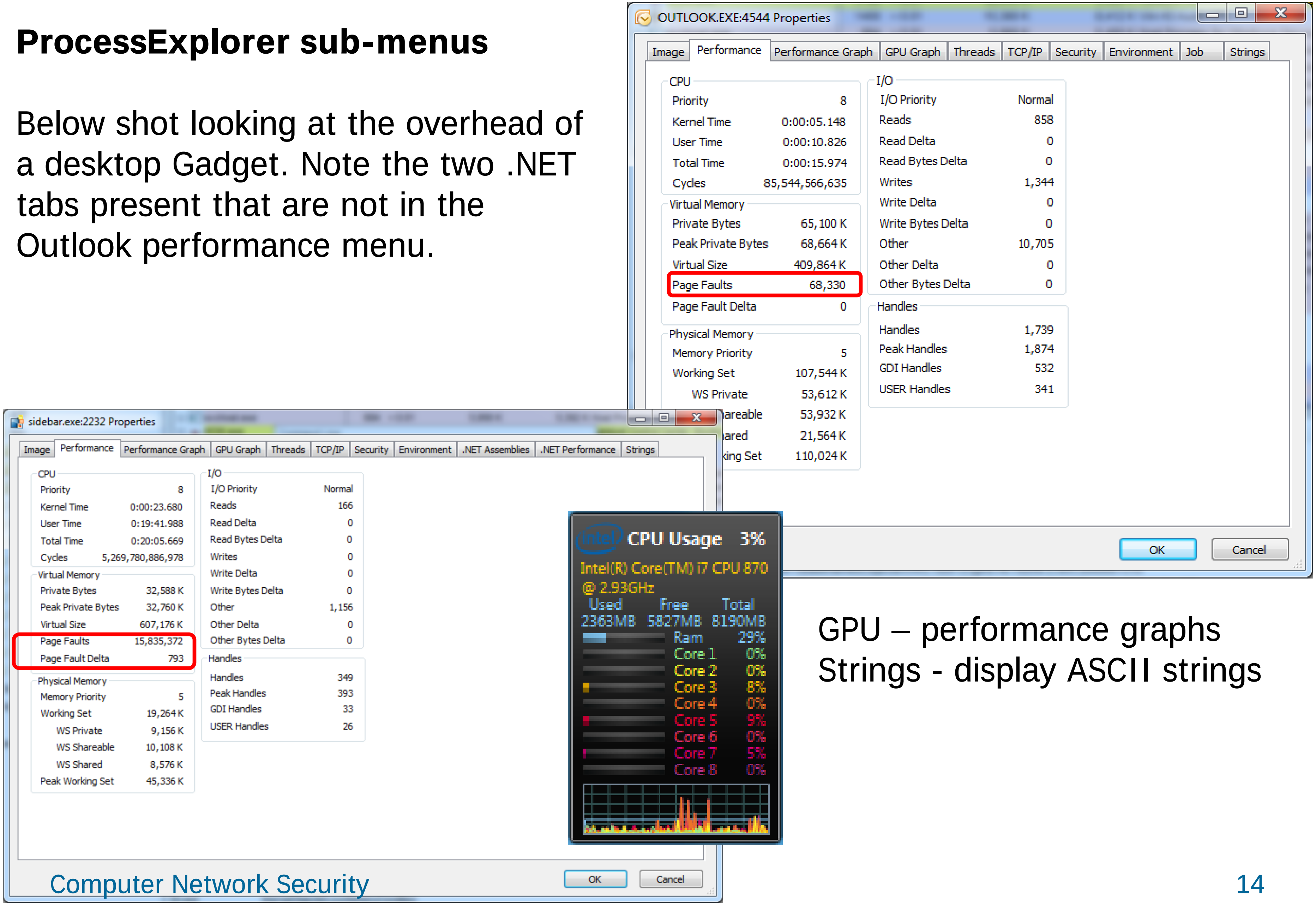
Startup Options

- /t Start Procexp minimized in system tray
- /s:PID Selects process (e.g. Procexp.exe /s:520)
- /e On Vista, 7 – requests UAC elevation

ProcessExplorer

ProcessExplorer sub-menus

Below shot looking at the overhead of a desktop Gadget. Note the two .NET tabs present that are not in the Outlook performance menu.



OUTLOOK.EXE:4544 Properties

CPU	
Priority	8
Kernel Time	0:00:05.148
User Time	0:00:10.826
Total Time	0:00:15.974
Cycles	85,544,566,635

Virtual Memory	
Private Bytes	65,100 K
Peak Private Bytes	68,664 K
Virtual Size	409,864 K
Page Faults	68,330
Page Fault Delta	0

Physical Memory	
Memory Priority	5
Working Set	107,544 K
WS Private	53,612 K
areable	53,932 K
ared	21,564 K
king Set	110,024 K

I/O	
I/O Priority	Normal
Reads	858
Read Delta	0
Read Bytes Delta	0
Writes	1,344
Write Delta	0
Write Bytes Delta	0
Other	10,705
Other Delta	0
Other Bytes Delta	0

Handles	
Handles	1,739
Peak Handles	1,874
GDI Handles	532
USER Handles	341

sidebar.exe:2232 Properties

CPU	
Priority	8
Kernel Time	0:00:23.680
User Time	0:19:41.988
Total Time	0:20:05.669
Cycles	5,269,780,886,978

Virtual Memory	
Private Bytes	32,588 K
Peak Private Bytes	32,760 K
Virtual Size	607,176 K
Page Faults	15,835,372
Page Fault Delta	793

Physical Memory	
Memory Priority	5
Working Set	19,264 K
WS Private	9,156 K
WS Shareable	10,108 K
WS Shared	8,576 K
Peak Working Set	45,336 K

I/O	
I/O Priority	Normal
Reads	166
Read Delta	0
Read Bytes Delta	0
Writes	0
Write Delta	0
Write Bytes Delta	0
Other	1,156
Other Delta	0
Other Bytes Delta	0

Handles	
Handles	349
Peak Handles	393
GDI Handles	33
USER Handles	26

intel CPU Usage 3%

Intel(R) Core(TM) i7 CPU 870 @ 2.93GHz

Used	Free	Total
2363MB	5827MB	8190MB

Ram	29%
Core 1	0%
Core 2	0%
Core 3	8%
Core 4	0%
Core 5	9%
Core 6	0%
Core 7	5%
Core 8	0%

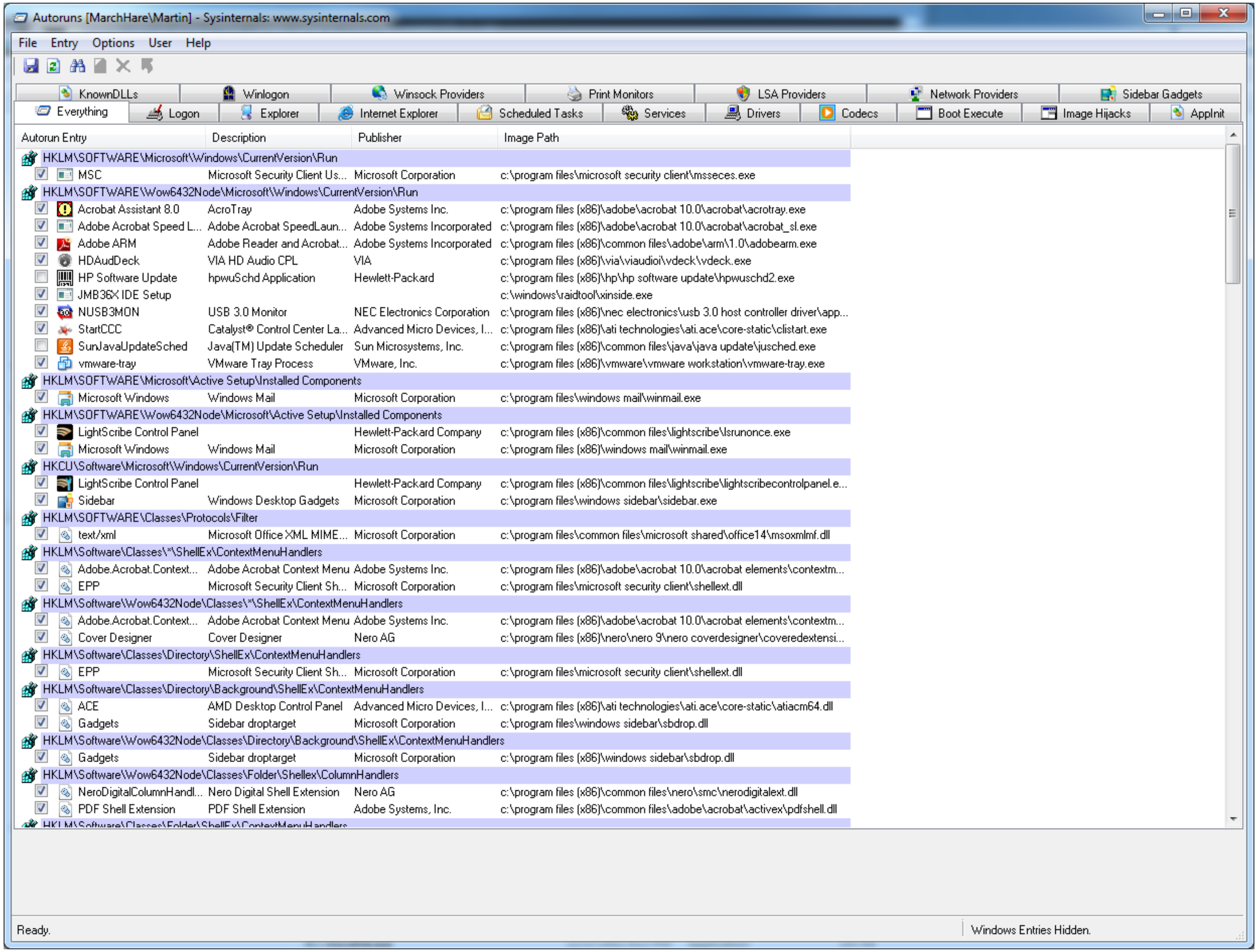
GPU – performance graphs
Strings - display ASCII strings

ProcessExplorer

- Suspend Process: useful when dealing with malware where two or more processes watch for each other’s termination, with the non-terminated process restarting the other if it dies. Defeat this by suspending the processes first and then terminate them.
- Search Online will launch a search for the selected executable name using the default browser and search engine. Useful when researching malware or identifying the source of an unrecognized process.
- Change which columns are displayed by right-clicking the column header row and selecting Select Columns, or by choosing Select Columns from the View menu.
- Identify the process that owns any visible window on desktop by clicking and holding the toolbar crosshairs icon. Drag it over the window of interest, release the mouse button, and ProcessExplorer will reappear with the owning process selected in the main window. This can identify the source of an unexpected error message or window (such as a fake Anti-Virus window).
- ProcessExplorer can be configured to replace the TaskManager.

AutoRuns

Shows what programs are configured to run during system bootup or login, in the order Windows processes them. Includes programs in the startup folder, Run, RunOnce, and other Registry keys. Most startup malware, adware, and junk-ware can be stopped using this tool.



Autorun Entry	Description	Publisher	Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ MSC	Microsoft Security Client Us...	Microsoft Corporation	c:\program files\microsoft security client\msseces.exe
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run			
☑ Acrobat Assistant 8.0	AcroTray	Adobe Systems Inc.	c:\program files (x86)\adobe\acrobat 10.0\acrobat\acrotray.exe
☑ Adobe Acrobat Speed L...	Adobe Acrobat SpeedLaun...	Adobe Systems Incorporated	c:\program files (x86)\adobe\acrobat 10.0\acrobat\acrobat_sl.exe
☑ Adobe ARM	Adobe Reader and Acrobat...	Adobe Systems Incorporated	c:\program files (x86)\common files\adobe\arm\1.0\adobearm.exe
☑ HDAudDeck	VIA HD Audio CPL	VIA	c:\program files (x86)\via\viaudioi\vdeck\vdeck.exe
☐ HP Software Update	hpwuSchd Application	Hewlett-Packard	c:\program files (x86)\hp\hp software update\hpwuschd2.exe
☑ JMB36X IDE Setup			c:\windows\raidtool\xinside.exe
☑ NUSB3MON	USB 3.0 Monitor	NEC Electronics Corporation	c:\program files (x86)\nec electronics\usb 3.0 host controller driver\app...
☑ StartCCC	Catalyst® Control Center La...	Advanced Micro Devices, I...	c:\program files (x86)\ati technologies\ati.ace\core-static\clistart.exe
☐ SunJavaUpdateSched	Java(TM) Update Scheduler	Sun Microsystems, Inc.	c:\program files (x86)\common files\java\java update\jusched.exe
☑ vmware-tray	VMware Tray Process	VMware, Inc.	c:\program files (x86)\vmware\vmware workstation\vmware-tray.exe
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components			
☑ Microsoft Windows	Windows Mail	Microsoft Corporation	c:\program files\windows mail\winmail.exe
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components			
☑ LightScribe Control Panel		Hewlett-Packard Company	c:\program files (x86)\common files\lightscribe\lsrunonce.exe
☑ Microsoft Windows	Windows Mail	Microsoft Corporation	c:\program files (x86)\windows mail\winmail.exe
HKCU\Software\Microsoft\Windows\CurrentVersion\Run			
☑ LightScribe Control Panel		Hewlett-Packard Company	c:\program files (x86)\common files\lightscribe\lightscribecontrolpanel.e...
☑ Sidebar	Windows Desktop Gadgets	Microsoft Corporation	c:\program files\windows sidebar\sidebar.exe
HKLM\SOFTWARE\Classes\Protocols\Filter			
☑ text/xml	Microsoft Office XML MIME...	Microsoft Corporation	c:\program files\common files\microsoft shared\office14\msoxmlmf.dll
HKLM\Software\Classes\*\ShellEx\ContextMenuHandlers			
☑ Adobe.Acrobat.Context...	Adobe Acrobat Context Menu	Adobe Systems Inc.	c:\program files (x86)\adobe\acrobat 10.0\acrobat elements\contextm...
☑ EPP	Microsoft Security Client Sh...	Microsoft Corporation	c:\program files\microsoft security client\shellext.dll
HKLM\Software\Wow6432Node\Classes\*\ShellEx\ContextMenuHandlers			
☑ Adobe.Acrobat.Context...	Adobe Acrobat Context Menu	Adobe Systems Inc.	c:\program files (x86)\adobe\acrobat 10.0\acrobat elements\contextm...
☑ Cover Designer	Cover Designer	Nero AG	c:\program files (x86)\nero\nero 9\nero coverdesigner\coveredextensi...
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers			
☑ EPP	Microsoft Security Client Sh...	Microsoft Corporation	c:\program files\microsoft security client\shellext.dll
HKLM\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers			
☑ ACE	AMD Desktop Control Panel	Advanced Micro Devices, I...	c:\program files (x86)\ati technologies\ati.ace\core-static\atiacm64.dll
☑ Gadgets	Sidebar droptarget	Microsoft Corporation	c:\program files\windows sidebar\sbdrop.dll
HKLM\Software\Wow6432Node\Classes\Directory\Background\ShellEx\ContextMenuHandlers			
☑ Gadgets	Sidebar droptarget	Microsoft Corporation	c:\program files (x86)\windows sidebar\sbdrop.dll
HKLM\Software\Wow6432Node\Classes\Folder\Shellex\ColumnHandlers			
☑ NeroDigitalColumnHandl...	Nero Digital Shell Extension	Nero AG	c:\program files (x86)\common files\nero\smc\nerodigitalext.dll
☑ PDF Shell Extension	PDF Shell Extension	Adobe Systems, Inc.	c:\program files (x86)\common files\adobe\acrobat\activex\pdfshell.dll
HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers			

Ready.　Windows Entries Hidden.

Step through each of the tabs – note the various startup methods/locations

AutoRuns

- Autoruns allows you to disable or delete autostart entries.
- AutoRuns can reduce assorted bloatware loaded found on new computers. Use it to remove various free/trial programs, semi-hidden startup programs, unwanted toolbars, and browser helper objects (BHO's) from IE.
- AutorunsC is the command-line version, which provides a way to capture the same information via scripts.
- Each row includes the name of the autostart entry, description and publisher of the item, path to the executable, and an icon for that file.
- A check box in each row can be used to temporarily disable the entry.
- Autostarts using a hosting process (e.g. Cmd.exe, Rundll32.exe, Regsvr32.exe, or Svchost.exe) are exposed by the image path showing the target script or DLL on the command line.
- A "File not found" in the Image Path column indicates the target file cannot be found in the expected location (e.g. safe to remove).

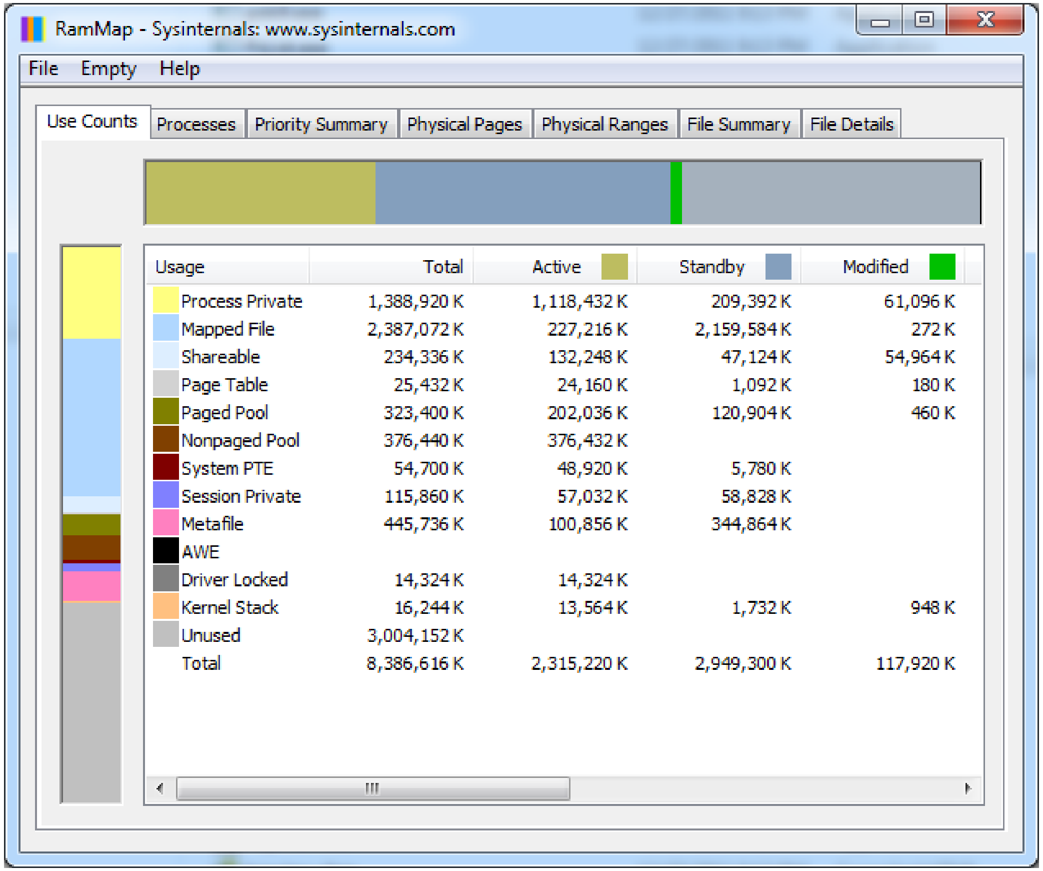
- Caveats:
  - AutoRuns does not stop any existing processes
  - Don't disable a critical service or application
  - Don't disable anything needed during the boot process

RAMMap

RAMMap displays how Windows uses physical memory

Widen the window to see all the columns

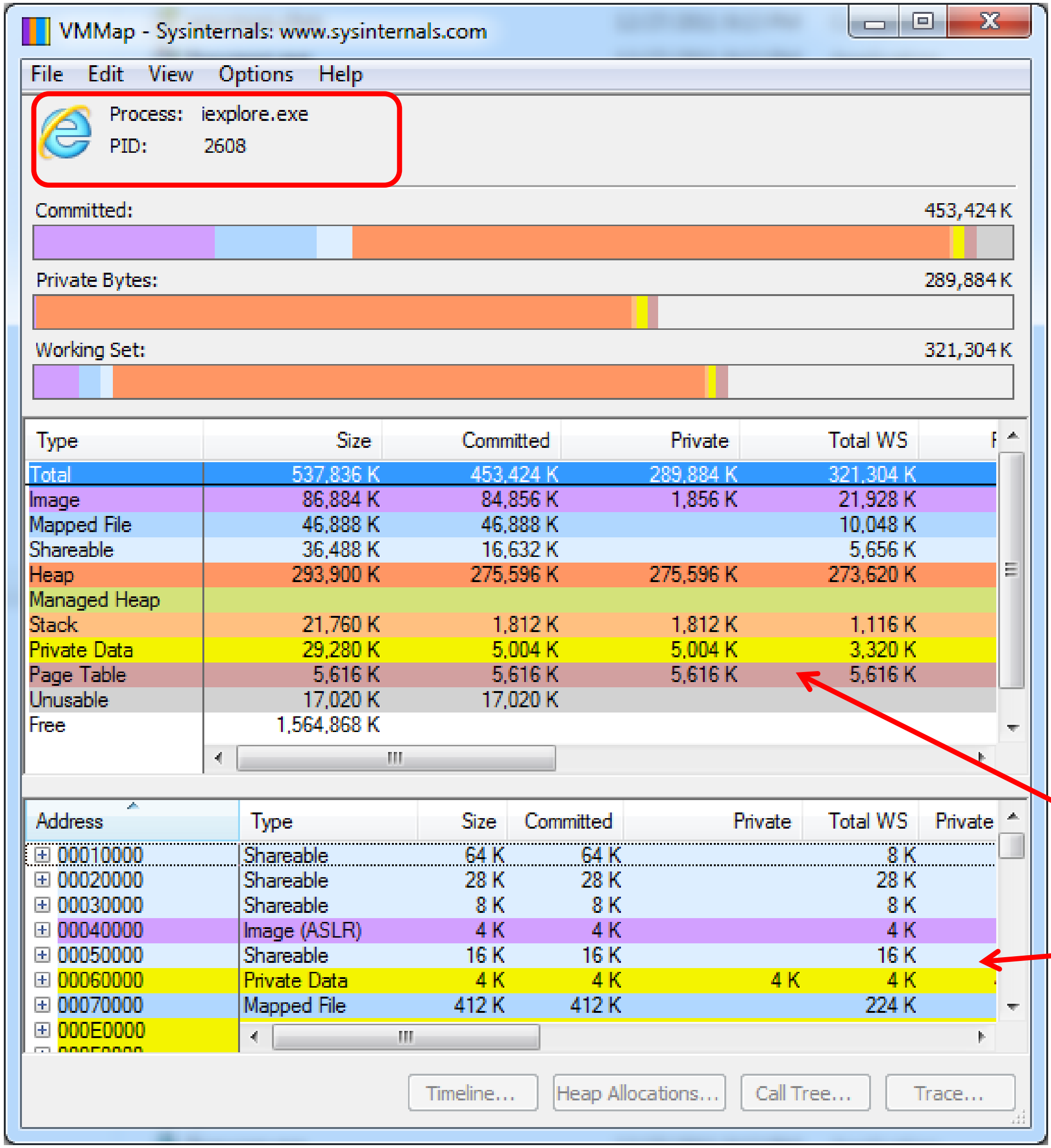
- Use Counts: usage summary by type and paging list
- Processes: working set sizes
- Priority Summary: prioritized standby list sizes
- Physical Pages: per-page use for all physical memory
- Physical Ranges: physical memory addresses
- File Summary: RAM data by file
- File Details: individual physical pages by file



Usage	Total	Active	Standby	Modified
Process Private	1,388,920 K	1,118,432 K	209,392 K	61,096 K
Mapped File	2,387,072 K	227,216 K	2,159,584 K	272 K
Shareable	234,336 K	132,248 K	47,124 K	54,964 K
Page Table	25,432 K	24,160 K	1,092 K	180 K
Paged Pool	323,400 K	202,036 K	120,904 K	460 K
Nonpaged Pool	376,440 K	376,432 K		
System PTE	54,700 K	48,920 K	5,780 K	
Session Private	115,860 K	57,032 K	58,828 K	
Metafile	445,736 K	100,856 K	344,864 K	
AWE				
Driver Locked	14,324 K	14,324 K		
Kernel Stack	16,244 K	13,564 K	1,732 K	948 K
Unused	3,004,152 K			
Total	8,386,616 K	2,315,220 K	2,949,300 K	117,920 K

Step through all of the tabs.
On the File Summary tab – could non-active files be on the standby page list?
Empty the standby list and click the refresh tab to find out.

VMMap



VMMap - Sysinternals: www.sysinternals.com
File Edit View Options Help

Process: iexplore.exe
PID: 2608

Committed: 453,424 K

Private Bytes: 289,884 K

Working Set: 321,304 K

Type	Size	Committed	Private	Total WS
Total	537,836 K	453,424 K	289,884 K	321,304 K
Image	86,884 K	84,856 K	1,856 K	21,928 K
Mapped File	46,888 K	46,888 K		10,048 K
Shareable	36,488 K	16,632 K		5,656 K
Heap	293,900 K	275,596 K	275,596 K	273,620 K
Managed Heap				
Stack	21,760 K	1,812 K	1,812 K	1,116 K
Private Data	29,280 K	5,004 K	5,004 K	3,320 K
Page Table	5,616 K	5,616 K	5,616 K	5,616 K
Unusable	17,020 K	17,020 K		
Free	1,564,868 K			

Address	Type	Size	Committed	Private	Total WS	Private
⊞ 00010000	Shareable	64 K	64 K		8 K	
⊞ 00020000	Shareable	28 K	28 K		28 K	
⊞ 00030000	Shareable	8 K	8 K		8 K	
⊞ 00040000	Image (ASLR)	4 K	4 K		4 K	
⊞ 00050000	Shareable	16 K	16 K		16 K	
⊞ 00060000	Private Data	4 K	4 K	4 K	4 K	
⊞ 00070000	Mapped File	412 K	412 K		224 K	
⊞ 000E0000						

VMMap 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. In addition to graphical representations of memory usage, VMMap also shows summary information and a detailed process memory map.

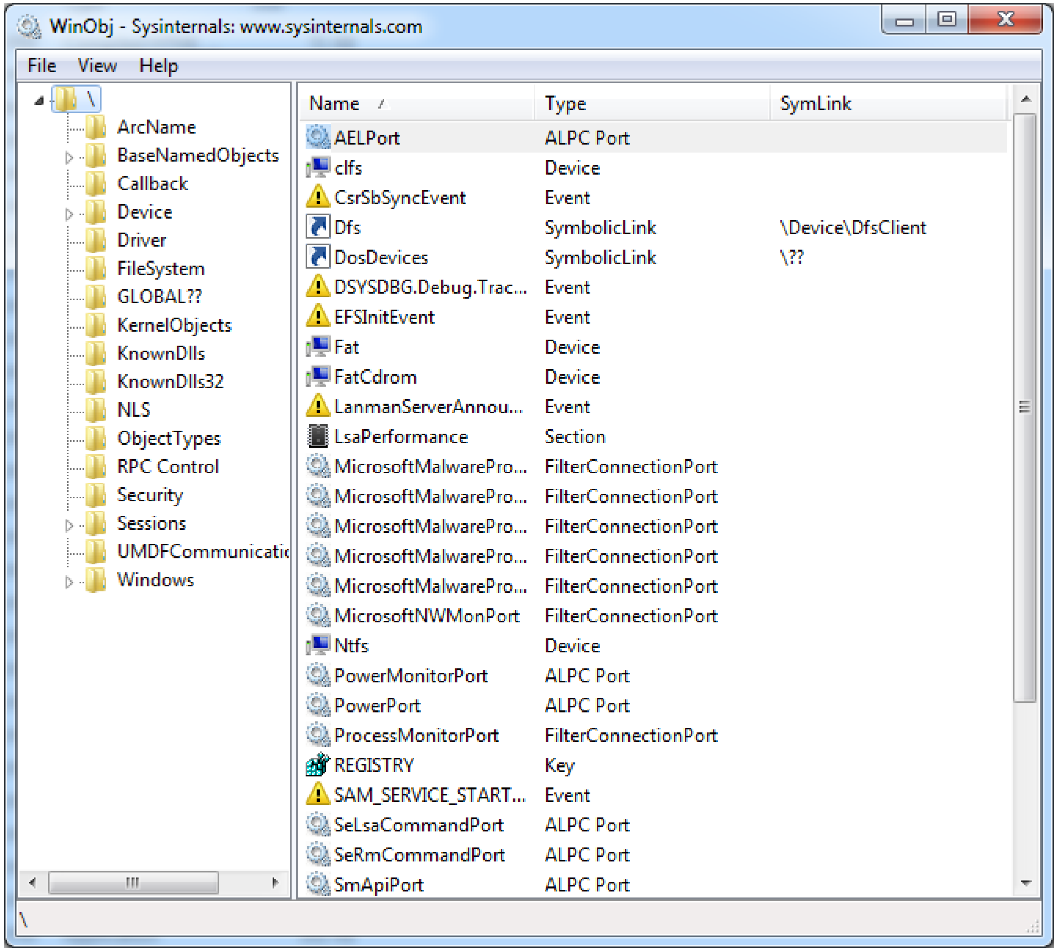
Clicking on type updates the lower window

Use VMMap to explore the memory used by an application.

WinObj

WinObj - uses the native Windows NT API (provided by NTDLL.DLL) to access and display information on the NT Object Manager's name space.

- Mutexes (mutants) – padlock
- Sections (file-mapping) – chip
- Events - exclamation triangle
- KeyedEvents – a key overlaid
- Semaphores - traffic signal
- Symbolic links - a curved arrow
- Devices - desktop computer icon
- Drivers - gears on a page
- Window Stations - video monitor
- Timers - clock



WinObj - Sysinternals: www.sysinternals.com

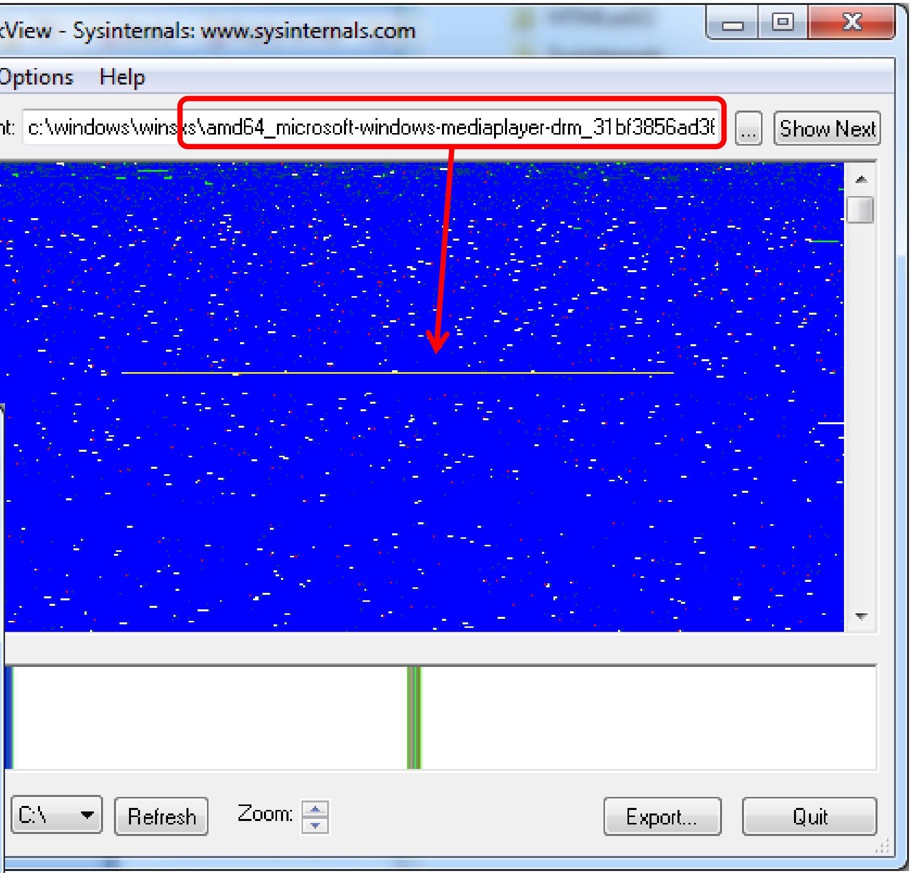
- \
  - ArcName
  - BaseNamedObjects
  - Callback
  - Device
  - Driver
  - FileSystem
  - GLOBAL??
  - KernelObjects
  - KnownDlls
  - KnownDlls32
  - NLS
  - ObjectTypes
  - RPC Control
  - Security
  - Sessions
  - UMDFCommunicati
  - Windows

Name	Type	SymLink
AELPort	ALPC Port	
clfs	Device	
CsrSbSyncEvent	Event	
Dfs	SymbolicLink	\Device\DfsClient
DosDevices	SymbolicLink	\??
DSYSDBG.Debug.Trac...	Event	
EFSInitEvent	Event	
Fat	Device	
FatCdrom	Device	
LanmanServerAnnou...	Event	
LsaPerformance	Section	
MicrosoftMalwarePro...	FilterConnectionPort	
MicrosoftMalwarePro...	FilterConnectionPort	
MicrosoftMalwarePro...	FilterConnectionPort	
MicrosoftMalwarePro...	FilterConnectionPort	
MicrosoftMalwarePro...	FilterConnectionPort	
MicrosoftNWMonPort	FilterConnectionPort	
Ntfs	Device	
PowerMonitorPort	ALPC Port	
PowerPort	ALPC Port	
ProcessMonitorPort	FilterConnectionPort	
REGISTRY	Key	
SAM_SERVICE_START...	Event	
SeLsaCommandPort	ALPC Port	
SeRmCommandPort	ALPC Port	
SmApiPort	ALPC Port	

\

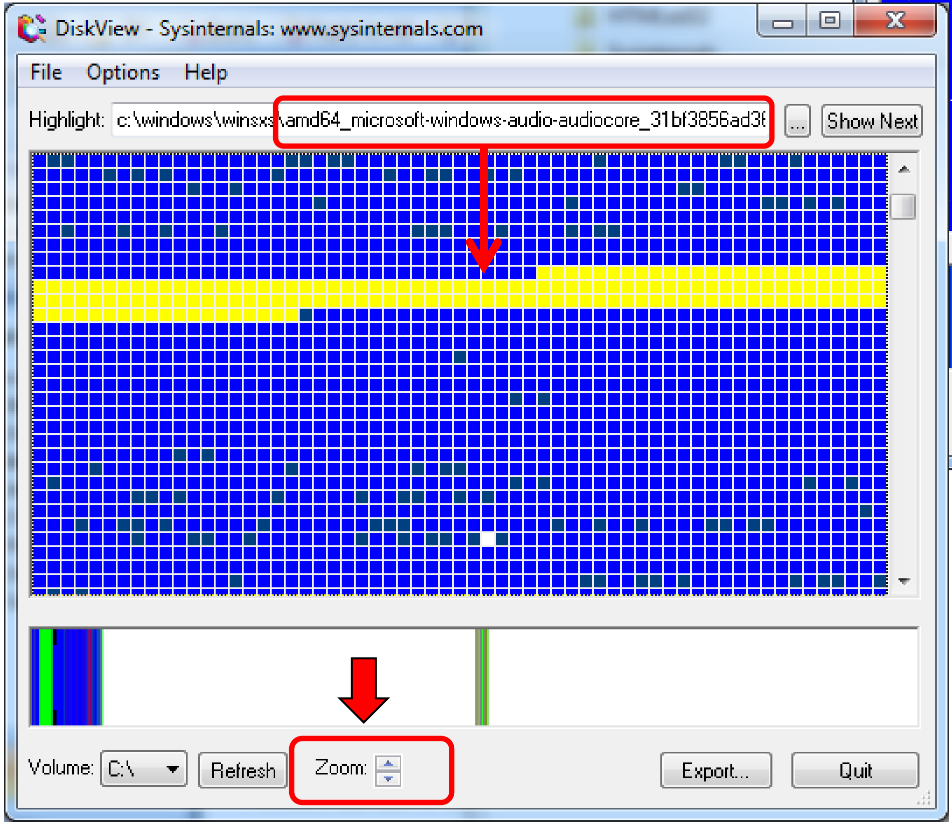
DiskView

DiskView presents a graphical map of the disk, showing where a file is located or, by clicking on a cluster, seeing which file occupies it. Double-clicking provides additional file information on the allocated cluster.



Highlight: c:\windows\winsxs\amd64_microsoft-windows-mediaplayer-drm_31bf3856ad3

Volume: C:\



Highlight: c:\windows\winsxs\amd64_microsoft-windows-audio-audiocore_31bf3856ad3

Volume: C:\

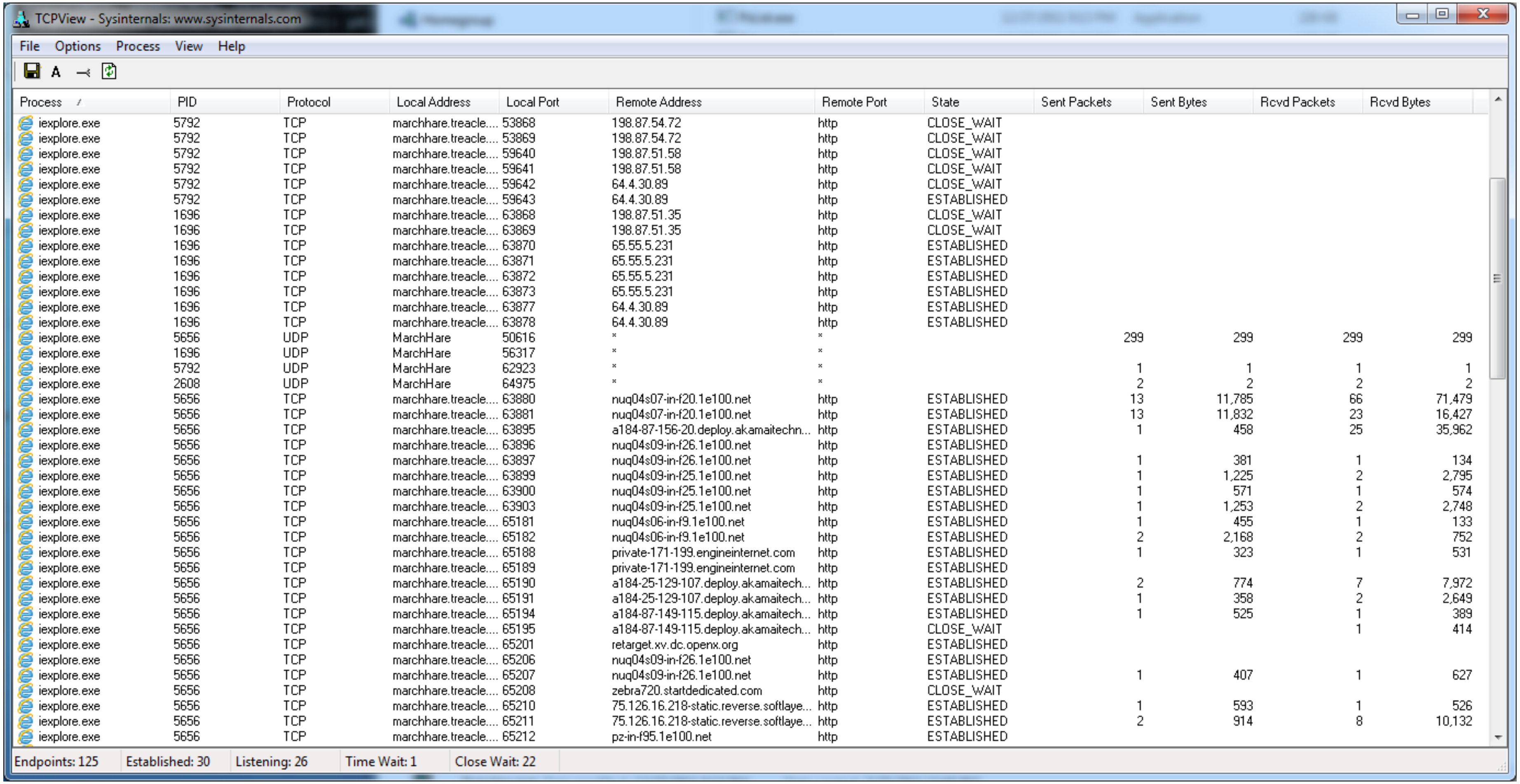
TCPView

- GUI version of Netstat
- Works on all Windows platforms
- Lists active TCP and UDP endpoints in real-time
- Shows endpoint owner
- Includes auto-refresh and difference highlighting
- Can close established TCP/IP connections
- Works using documented and undocumented IPHelper library functions

- Find broken and misconfigured applications
- Use to find adware, malware, spyware, and keyloggers
  - Find malware sending SPAM
- Find applications connecting without your knowledge
- Monitor system while downloading, shopping, and banking online, while on Facebook or 4Chan

TCPView

Shows detailed listings of all TCP and UDP endpoints on the system, including the local and remote addresses, bytes/packets sent/received and state of TCP connections. Detect, monitor, and kill processes with hidden communication features.

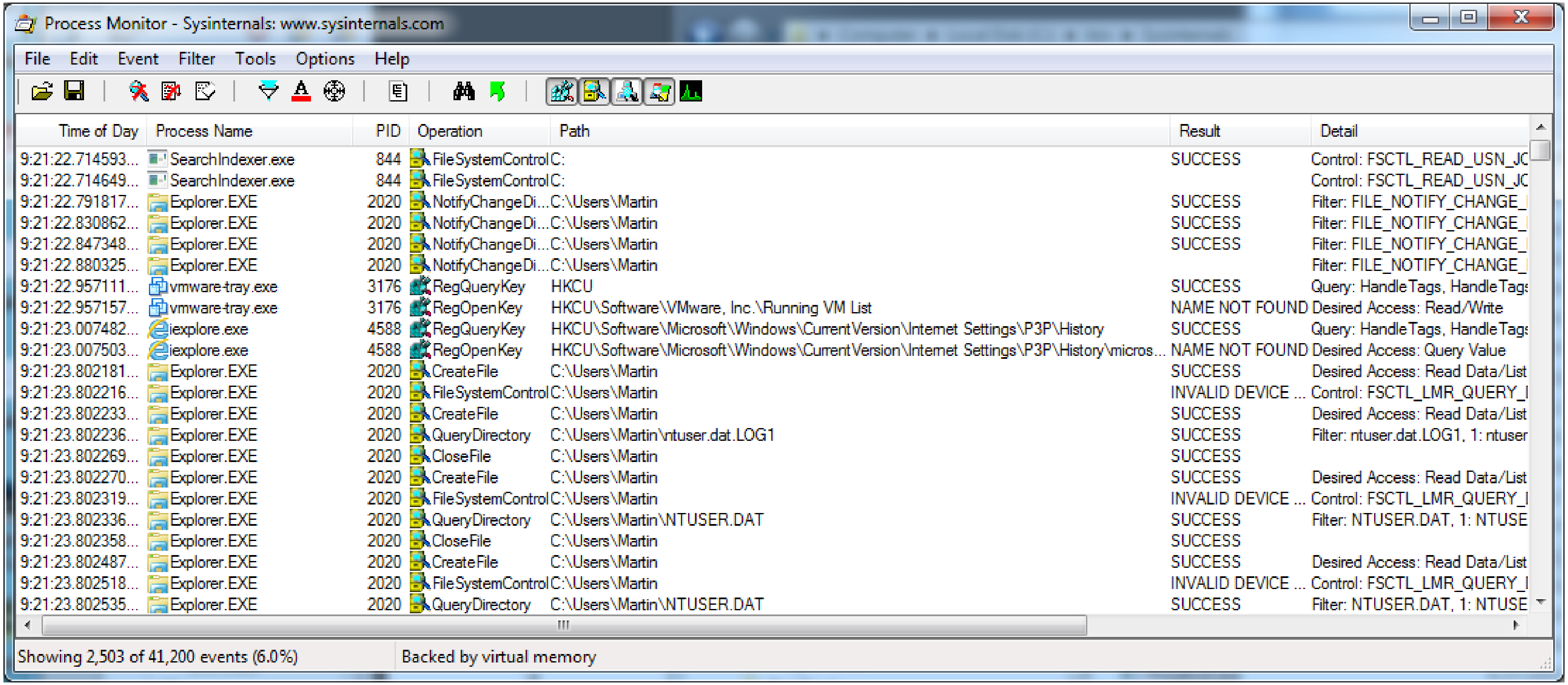


Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
iexplore.exe	5792	TCP	marchhare.treacle....	53868	198.87.54.72	http	CLOSE_WAIT				
iexplore.exe	5792	TCP	marchhare.treacle....	53869	198.87.54.72	http	CLOSE_WAIT				
iexplore.exe	5792	TCP	marchhare.treacle....	59640	198.87.51.58	http	CLOSE_WAIT				
iexplore.exe	5792	TCP	marchhare.treacle....	59641	198.87.51.58	http	CLOSE_WAIT				
iexplore.exe	5792	TCP	marchhare.treacle....	59642	64.4.30.89	http	CLOSE_WAIT				
iexplore.exe	5792	TCP	marchhare.treacle....	59643	64.4.30.89	http	ESTABLISHED				
iexplore.exe	1696	TCP	marchhare.treacle....	63868	198.87.51.35	http	CLOSE_WAIT				
iexplore.exe	1696	TCP	marchhare.treacle....	63869	198.87.51.35	http	CLOSE_WAIT				
iexplore.exe	1696	TCP	marchhare.treacle....	63870	65.55.5.231	http	ESTABLISHED				
iexplore.exe	1696	TCP	marchhare.treacle....	63871	65.55.5.231	http	ESTABLISHED				
iexplore.exe	1696	TCP	marchhare.treacle....	63872	65.55.5.231	http	ESTABLISHED				
iexplore.exe	1696	TCP	marchhare.treacle....	63873	65.55.5.231	http	ESTABLISHED				
iexplore.exe	1696	TCP	marchhare.treacle....	63877	64.4.30.89	http	ESTABLISHED				
iexplore.exe	1696	TCP	marchhare.treacle....	63878	64.4.30.89	http	ESTABLISHED				
iexplore.exe	5656	UDP	MarchHare	50616	*	*		299	299	299	299
iexplore.exe	1696	UDP	MarchHare	56317	*	*					
iexplore.exe	5792	UDP	MarchHare	62923	*	*		1	1	1	1
iexplore.exe	2608	UDP	MarchHare	64975	*	*		2	2	2	2
iexplore.exe	5656	TCP	marchhare.treacle....	63880	nuq04s07-in-f20.1e100.net	http	ESTABLISHED	13	11,785	66	71,479
iexplore.exe	5656	TCP	marchhare.treacle....	63881	nuq04s07-in-f20.1e100.net	http	ESTABLISHED	13	11,832	23	16,427
iexplore.exe	5656	TCP	marchhare.treacle....	63895	a184-87-156-20.deploy.akamaitechn...	http	ESTABLISHED	1	458	25	35,962
iexplore.exe	5656	TCP	marchhare.treacle....	63896	nuq04s09-in-f26.1e100.net	http	ESTABLISHED				
iexplore.exe	5656	TCP	marchhare.treacle....	63897	nuq04s09-in-f26.1e100.net	http	ESTABLISHED	1	381	1	134
iexplore.exe	5656	TCP	marchhare.treacle....	63899	nuq04s09-in-f25.1e100.net	http	ESTABLISHED	1	1,225	2	2,795
iexplore.exe	5656	TCP	marchhare.treacle....	63900	nuq04s09-in-f25.1e100.net	http	ESTABLISHED	1	571	1	574
iexplore.exe	5656	TCP	marchhare.treacle....	63903	nuq04s09-in-f25.1e100.net	http	ESTABLISHED	1	1,253	2	2,748
iexplore.exe	5656	TCP	marchhare.treacle....	65181	nuq04s06-in-f9.1e100.net	http	ESTABLISHED	1	455	1	133
iexplore.exe	5656	TCP	marchhare.treacle....	65182	nuq04s06-in-f9.1e100.net	http	ESTABLISHED	2	2,168	2	752
iexplore.exe	5656	TCP	marchhare.treacle....	65188	private-171-199.engineinternet.com	http	ESTABLISHED	1	323	1	531
iexplore.exe	5656	TCP	marchhare.treacle....	65189	private-171-199.engineinternet.com	http	ESTABLISHED				
iexplore.exe	5656	TCP	marchhare.treacle....	65190	a184-25-129-107.deploy.akamaitech...	http	ESTABLISHED	2	774	7	7,972
iexplore.exe	5656	TCP	marchhare.treacle....	65191	a184-25-129-107.deploy.akamaitech...	http	ESTABLISHED	1	358	2	2,649
iexplore.exe	5656	TCP	marchhare.treacle....	65194	a184-87-149-115.deploy.akamaitech...	http	ESTABLISHED	1	525	1	389
iexplore.exe	5656	TCP	marchhare.treacle....	65195	a184-87-149-115.deploy.akamaitech...	http	CLOSE_WAIT			1	414
iexplore.exe	5656	TCP	marchhare.treacle....	65201	retarget.xv.dc.openx.org	http	ESTABLISHED				
iexplore.exe	5656	TCP	marchhare.treacle....	65206	nuq04s09-in-f26.1e100.net	http	ESTABLISHED				
iexplore.exe	5656	TCP	marchhare.treacle....	65207	nuq04s09-in-f26.1e100.net	http	ESTABLISHED	1	407	1	627
iexplore.exe	5656	TCP	marchhare.treacle....	65208	zebra720.startdedicated.com	http	CLOSE_WAIT				
iexplore.exe	5656	TCP	marchhare.treacle....	65210	75.126.16.218-static.reverse.softlaye...	http	ESTABLISHED	1	593	1	526
iexplore.exe	5656	TCP	marchhare.treacle....	65211	75.126.16.218-static.reverse.softlaye...	http	ESTABLISHED	2	914	8	10,132
iexplore.exe	5656	TCP	marchhare.treacle....	65212	pz-in-f95.1e100.net	http	ESTABLISHED				

Endpoints: 125 | Established: 30 | Listening: 26 | Time Wait: 1 | Close Wait: 22

ProcessMonitor

ProcessMonitor is an advanced logging tool that captures detailed information about registry, file, process/thread, and network activity as well as showing the information in real-time.



Process Monitor - Sysinternals: www.sysinternals.com

Time of Day	Process Name	PID	Operation	Path	Result	Detail
9:21:22.714593...	SearchIndexer.exe	844	FileSystemControl	C:	SUCCESS	Control: FSCTL_READ_USN_JC
9:21:22.714649...	SearchIndexer.exe	844	FileSystemControl	C:		Control: FSCTL_READ_USN_JC
9:21:22.791817...	Explorer.EXE	2020	NotifyChangeDi...	C:\Users\Martin	SUCCESS	Filter: FILE_NOTIFY_CHANGE_
9:21:22.830862...	Explorer.EXE	2020	NotifyChangeDi...	C:\Users\Martin	SUCCESS	Filter: FILE_NOTIFY_CHANGE_
9:21:22.847348...	Explorer.EXE	2020	NotifyChangeDi...	C:\Users\Martin	SUCCESS	Filter: FILE_NOTIFY_CHANGE_
9:21:22.880325...	Explorer.EXE	2020	NotifyChangeDi...	C:\Users\Martin		Filter: FILE_NOTIFY_CHANGE_
9:21:22.957111...	vmware-tray.exe	3176	RegQueryKey	HKCU	SUCCESS	Query: HandleTags, HandleTags
9:21:22.957157...	vmware-tray.exe	3176	RegOpenKey	HKCU\Software\VMware, Inc.\Running VM List	NAME NOT FOUND	Desired Access: Read/Write
9:21:23.007482...	iexplore.exe	4588	RegQueryKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\P3P\History	SUCCESS	Query: HandleTags, HandleTags
9:21:23.007503...	iexplore.exe	4588	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\P3P\History\micros...	NAME NOT FOUND	Desired Access: Query Value
9:21:23.802181...	Explorer.EXE	2020	CreateFile	C:\Users\Martin	SUCCESS	Desired Access: Read Data/List
9:21:23.802216...	Explorer.EXE	2020	FileSystemControl	C:\Users\Martin	INVALID DEVICE ...	Control: FSCTL_LMR_QUERY_I
9:21:23.802233...	Explorer.EXE	2020	CreateFile	C:\Users\Martin	SUCCESS	Desired Access: Read Data/List
9:21:23.802236...	Explorer.EXE	2020	QueryDirectory	C:\Users\Martin\ntuser.dat.LOG1	SUCCESS	Filter: ntuser.dat.LOG1, 1: ntuser
9:21:23.802269...	Explorer.EXE	2020	CloseFile	C:\Users\Martin	SUCCESS	
9:21:23.802270...	Explorer.EXE	2020	CreateFile	C:\Users\Martin	SUCCESS	Desired Access: Read Data/List
9:21:23.802319...	Explorer.EXE	2020	FileSystemControl	C:\Users\Martin	INVALID DEVICE ...	Control: FSCTL_LMR_QUERY_I
9:21:23.802336...	Explorer.EXE	2020	QueryDirectory	C:\Users\Martin\NTUSER.DAT	SUCCESS	Filter: NTUSER.DAT, 1: NTUSE
9:21:23.802358...	Explorer.EXE	2020	CloseFile	C:\Users\Martin	SUCCESS	
9:21:23.802487...	Explorer.EXE	2020	CreateFile	C:\Users\Martin	SUCCESS	Desired Access: Read Data/List
9:21:23.802518...	Explorer.EXE	2020	FileSystemControl	C:\Users\Martin	INVALID DEVICE ...	Control: FSCTL_LMR_QUERY_I
9:21:23.802535...	Explorer.EXE	2020	QueryDirectory	C:\Users\Martin\NTUSER.DAT	SUCCESS	Filter: NTUSER.DAT, 1: NTUSE

Showing 2,503 of 41,200 events (6.0%)   Backed by virtual memory

ProcessMonitor

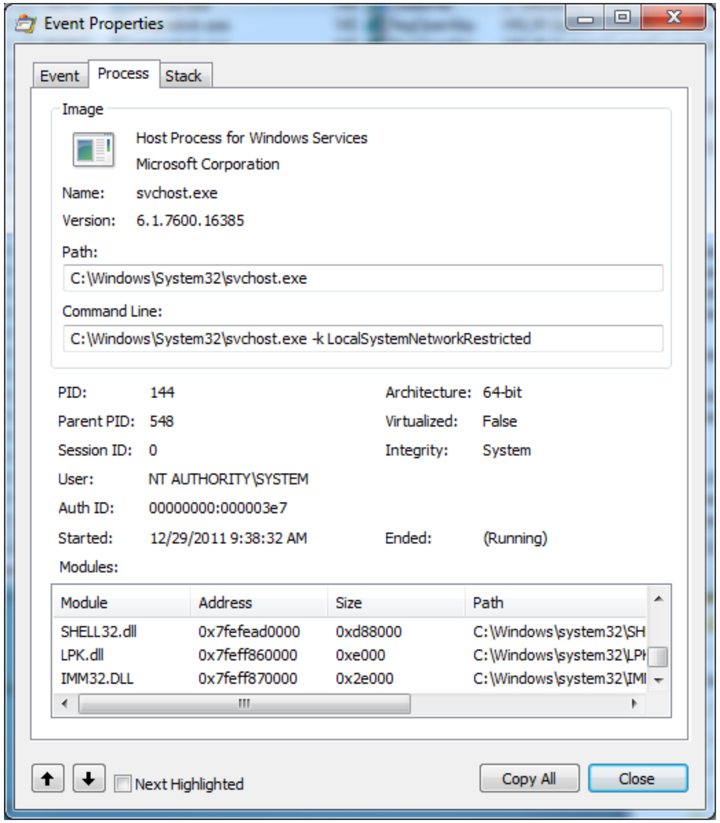
Common Result Codes

- BUFFER OVERLOW occurs when a program requests variable-length information, such as data from a registry value, but doesn't provide a large enough buffer to receive it because it doesn't know the actual data size in advance. The system will tell the program how large a buffer is required and might copy as much data as it can into the buffer, but it will not actually overflow the buffer. Typically after a BUFFER OVERLOW result is received, the program then allocates a large enough buffer and requests the same data again—this time resulting in SUCCESS.
- NAME NOT FOUND|PATH NOT FOUND|NO SUCH FILE - Caller tried to open an object that doesn't exist. This result code often is the result of a DLL load routine looking in various directories as part of the DLL search process.
- NO MORE ENTRIES|NO MORE FILES Caller has finished enumerating the contents of a folder or registry key.
- REPARSE Caller requested an object that links to another object. (e.g. CurrentControlSet redirects to ControlSet001).
- FILE LOCKED WITH ONLY READERS a file or file mapping was locked and all users of the file can only read from it.
- FILE LOCKED WITH WRITERS a file or file mapping was locked and that at least one user of the file can write to it
- INVALID DEVICE REQUEST The specified request is not a valid operation for the target device.
- INVALID PARAMETER An invalid parameter was passed to a service or function.

ProcessMonitor

Process tab for a selected event includes:

- Application (or default) icon from image
- Description, company name, and file version extracted from the version information resource
- Process name
- File path to the executable image
- Command line used to start this process
- Process ID for this process and for the parent process that started it
- Terminal services session ID process running in
- User account under which process is running
- Authentication ID for the process token
- Process start time, when it ended (if it has)
- Architecture (32-bit or 64-bit executable code)
- If UAC file and registry virtualization
- Process integrity level
- List of modules (executable images) loaded into the process’ address space at time event occurred



Image

Host Process for Windows Services
Microsoft Corporation
Name: svchost.exe
Version: 6.1.7600.16385

Path:
C:\Windows\System32\svchost.exe

Command Line:
C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted

PID: 144
Architecture: 64-bit
Parent PID: 548
Virtualized: False
Session ID: 0
Integrity: System
User: NT AUTHORITY\SYSTEM
Auth ID: 00000000:000003e7
Started: 12/29/2011 9:38:32 AM
Ended: (Running)

Modules:

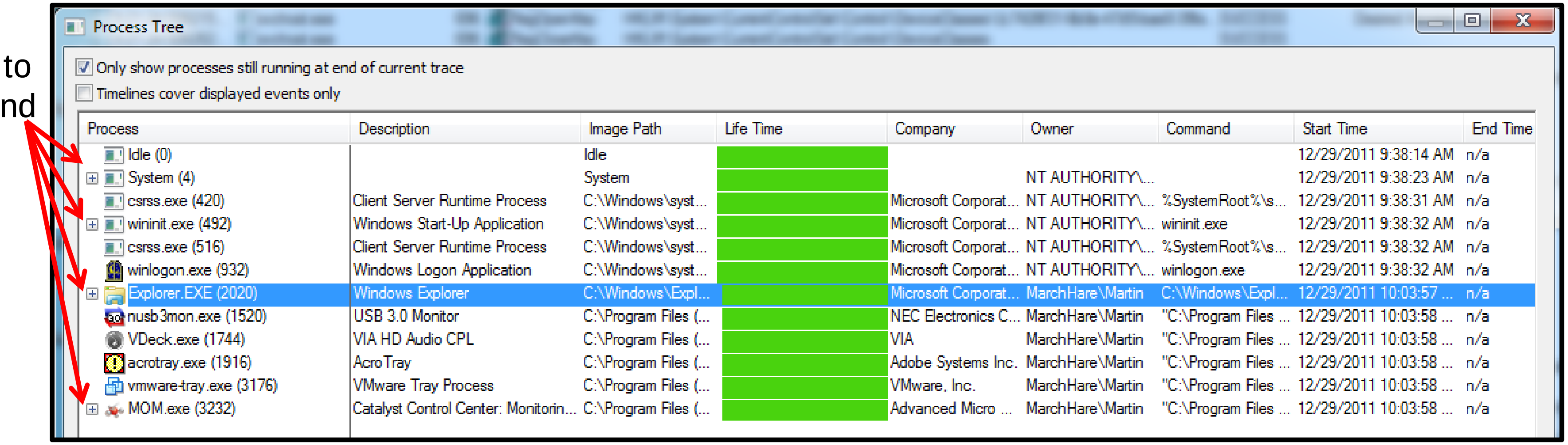
Module	Address	Size	Path
SHELL32.dll	0x7fefead0000	0xd88000	C:\Windows\system32\SH
LPK.dll	0x7feff860000	0xe000	C:\Windows\system32\LPK
IMM32.DLL	0x7feff870000	0x2e000	C:\Windows\system32\IMI

ProcessMonitor

- Filtering and Highlighting - Procmon can log millions of events in a short amount of time, initiated from dozens of different processes. To help isolate events filtering options limit what displays.
- Similar options are provided for highlighting particular events.
- Filtered entries are removed only from the display, not from the underlying data. They can be displayed again by changing or removing the filter.
- By default, Procmon hides (filters) events typically not relevant.
- Complex custom filters can be saved and exported.

- Process Tree Tool shows relationship of processes referenced in a trace capture, making it possible to identify root cause of an operation.

click to expand



Process Tree

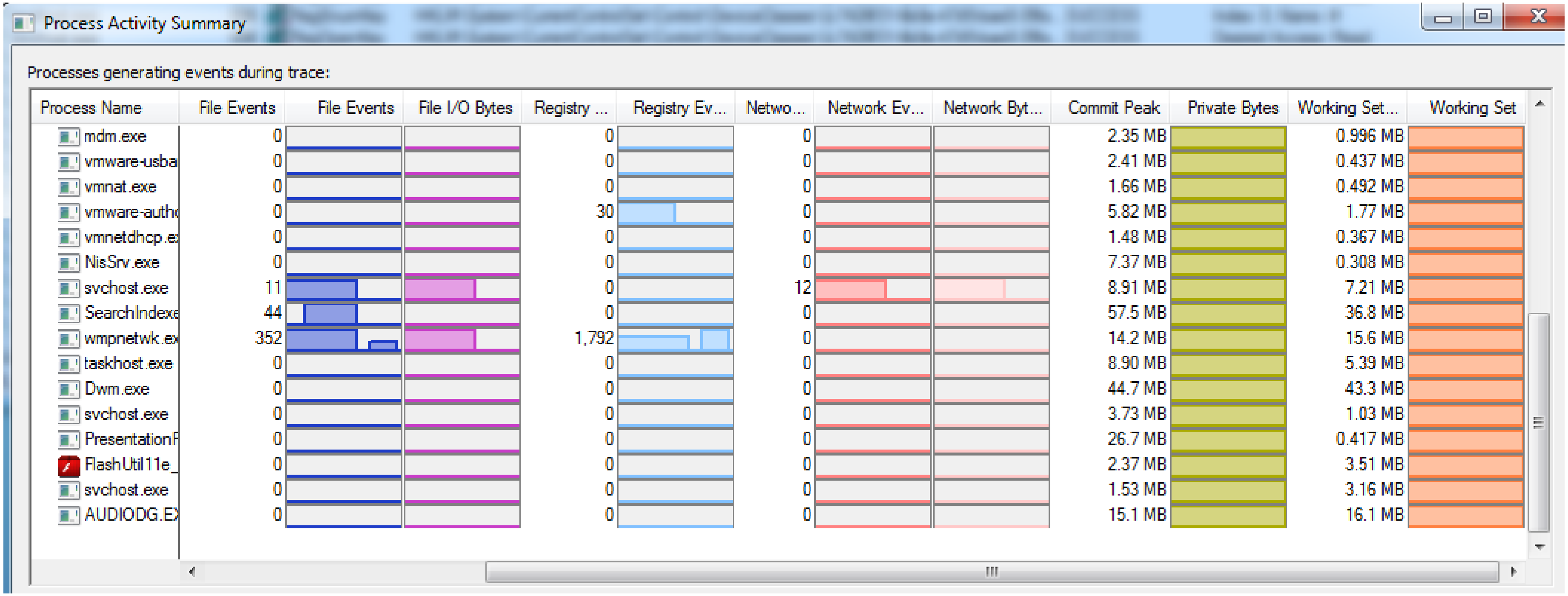
☑ Only show processes still running at end of current trace

□ Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Owner	Command	Start Time	End Time
Idle (0)		Idle	🟩				12/29/2011 9:38:14 AM	n/a
⊞ System (4)		System	🟩		NT AUTHORITY\...		12/29/2011 9:38:23 AM	n/a
csrss.exe (420)	Client Server Runtime Process	C:\Windows\syst...	🟩	Microsoft Corporat...	NT AUTHORITY\...	%SystemRoot%\s...	12/29/2011 9:38:31 AM	n/a
⊞ wininit.exe (492)	Windows Start-Up Application	C:\Windows\syst...	🟩	Microsoft Corporat...	NT AUTHORITY\...	wininit.exe	12/29/2011 9:38:32 AM	n/a
csrss.exe (516)	Client Server Runtime Process	C:\Windows\syst...	🟩	Microsoft Corporat...	NT AUTHORITY\...	%SystemRoot%\s...	12/29/2011 9:38:32 AM	n/a
winlogon.exe (932)	Windows Logon Application	C:\Windows\syst...	🟩	Microsoft Corporat...	NT AUTHORITY\...	winlogon.exe	12/29/2011 9:38:32 AM	n/a
⊞ Explorer.EXE (2020)	Windows Explorer	C:\Windows\Expl...	🟩	Microsoft Corporat...	MarchHare\Martin	C:\Windows\Expl...	12/29/2011 10:03:57 ...	n/a
nusb3mon.exe (1520)	USB 3.0 Monitor	C:\Program Files (...	🟩	NEC Electronics C...	MarchHare\Martin	"C:\Program Files ...	12/29/2011 10:03:58 ...	n/a
VDeck.exe (1744)	VIA HD Audio CPL	C:\Program Files (...	🟩	VIA	MarchHare\Martin	"C:\Program Files ...	12/29/2011 10:03:58 ...	n/a
acrotray.exe (1916)	AcroTray	C:\Program Files (...	🟩	Adobe Systems Inc.	MarchHare\Martin	"C:\Program Files ...	12/29/2011 10:03:58 ...	n/a
vmware-tray.exe (3176)	VMware Tray Process	C:\Program Files (...	🟩	VMware, Inc.	MarchHare\Martin	"C:\Program Files ...	12/29/2011 10:03:58 ...	n/a
⊞ MOM.exe (3232)	Catalyst Control Center: Monitorin...	C:\Program Files (...	🟩	Advanced Micro ...	MarchHare\Martin	"C:\Program Files ...	12/29/2011 10:03:58 ...	n/a

ProcessMonitor

- ProcessMonitor traces can be saved and reloaded.
- The internal PML files are different between 32 and 64-bit systems, 64-bit Windows logs can only be read on 64-bit systems.
- Event|JumpTo will open Regedit to the selected operation.
- Tools|Process Activity Summary produces the below output:



Process Activity Summary

Processes generating events during trace:

Process Name	File Events	File Events	File I/O Bytes	Registry ...	Registry Ev...	Netwo...	Network Ev...	Network Byt...	Commit Peak	Private Bytes	Working Set...	Working Set
mdm.exe	0			0		0			2.35 MB		0.996 MB	
vmware-usba	0			0		0			2.41 MB		0.437 MB	
vmnat.exe	0			0		0			1.66 MB		0.492 MB	
vmware-auth	0			30		0			5.82 MB		1.77 MB	
vmnetdhcp.e	0			0		0			1.48 MB		0.367 MB	
NisSrv.exe	0			0		0			7.37 MB		0.308 MB	
svchost.exe	11			0		12			8.91 MB		7.21 MB	
SearchIndexe	44			0		0			57.5 MB		36.8 MB	
wmpnetwk.ex	352			1,792		0			14.2 MB		15.6 MB	
taskhost.exe	0			0		0			8.90 MB		5.39 MB	
Dwm.exe	0			0		0			44.7 MB		43.3 MB	
svchost.exe	0			0		0			3.73 MB		1.03 MB	
PresentationF	0			0		0			26.7 MB		0.417 MB	
FlashUtil11e_	0			0		0			2.37 MB		3.51 MB	
svchost.exe	0			0		0			1.53 MB		3.16 MB	
AUDIODG.EX	0			0		0			15.1 MB		16.1 MB	

Lab Exercise

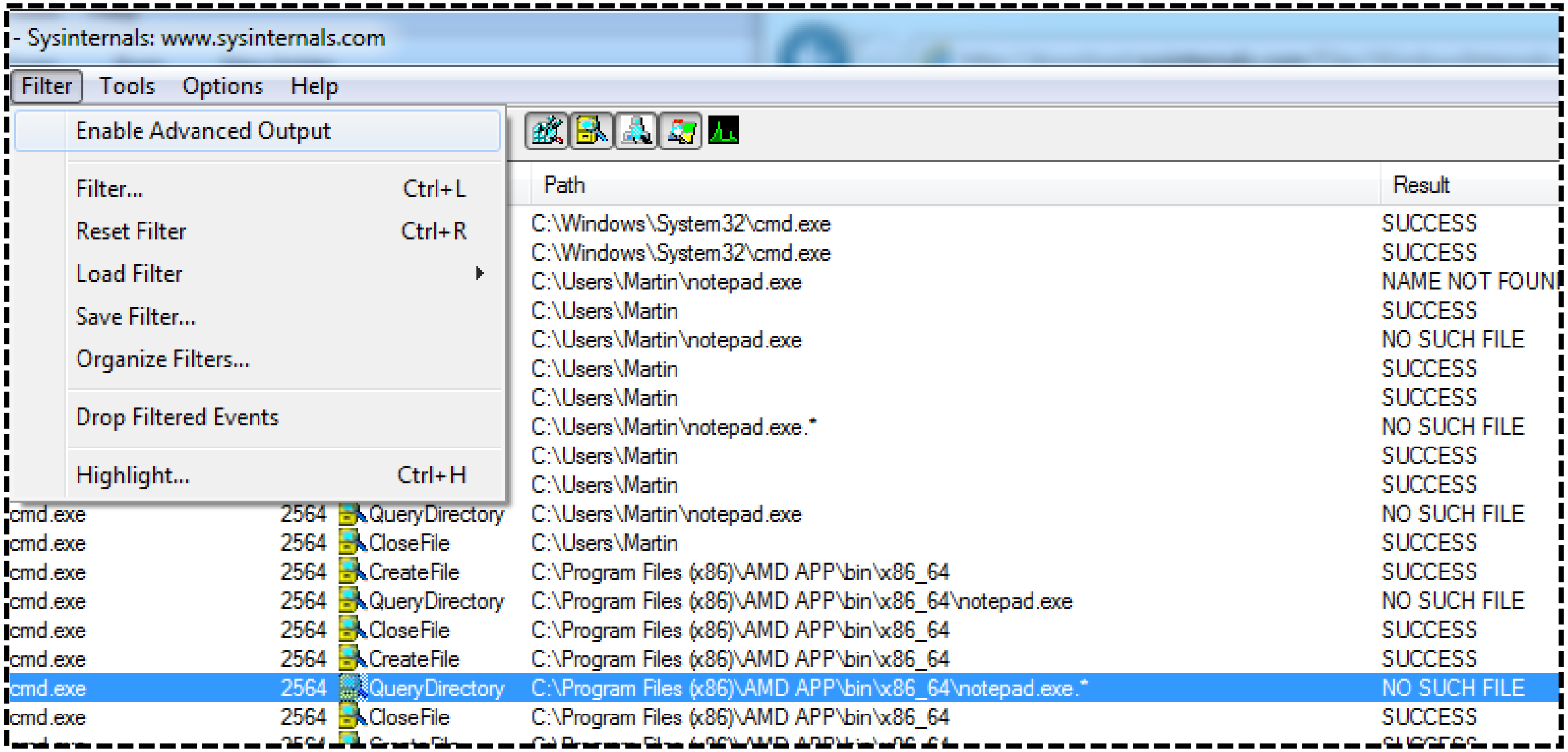
- ProcessMonitor can be used to look at the file I/O and registry keys accessed when executing an application.

- Start ProcessMonitor
  - The Ctrl+E hotkey toggles (start/stop) monitoring
  - Control+A toggles (on/off) the autoscroll feature
  - Ctrl+X will clear the display

- For the lab exercise, add two filters:
  - One for Process Name is Cmd.exe
  - One for Process Name is Notepad.exe
    - These are the only two processes to be included
- Ensure neither Cmd or Notepad is currently running
- Start up the command prompt
- Start the monitoring with Ctrl+E
- In the Cmd box type: Notepad.exe [Enter]
- Once the Showing value slows/stops, press Ctrl+E to stop monitoring

Lab Exercise

- Select a line where the result is No Such File
- Click on the Filter menu, select Highlight, and filter for that result
- Right click on a No Such File line – note the options available
- From the tools menu, select Count
- Use the Count Value Occurrences Column pulldown to count occurrences
- Look at: Tools | Process Summary



			Path	Result
			C:\Windows\System32\cmd.exe	SUCCESS
			C:\Windows\System32\cmd.exe	SUCCESS
			C:\Users\Martin\notepad.exe	NAME NOT FOUN
			C:\Users\Martin	SUCCESS
			C:\Users\Martin\notepad.exe	NO SUCH FILE
			C:\Users\Martin	SUCCESS
			C:\Users\Martin	SUCCESS
			C:\Users\Martin\notepad.exe.*	NO SUCH FILE
			C:\Users\Martin	SUCCESS
			C:\Users\Martin	SUCCESS
cmd.exe	2564	QueryDirectory	C:\Users\Martin\notepad.exe	NO SUCH FILE
cmd.exe	2564	CloseFile	C:\Users\Martin	SUCCESS
cmd.exe	2564	CreateFile	C:\Program Files (x86)\AMD APP\bin\x86_64	SUCCESS
cmd.exe	2564	QueryDirectory	C:\Program Files (x86)\AMD APP\bin\x86_64\notepad.exe	NO SUCH FILE
cmd.exe	2564	CloseFile	C:\Program Files (x86)\AMD APP\bin\x86_64	SUCCESS
cmd.exe	2564	CreateFile	C:\Program Files (x86)\AMD APP\bin\x86_64	SUCCESS
cmd.exe	2564	QueryDirectory	C:\Program Files (x86)\AMD APP\bin\x86_64\notepad.exe.*	NO SUCH FILE
cmd.exe	2564	CloseFile	C:\Program Files (x86)\AMD APP\bin\x86_64	SUCCESS

Lab Exercise Results

Complete the following and turn in to the lab assistant.

Name: ______________________________ Date: ________________

What was the count of:

1. _____ Total events
2. _____ Filtered events
3. _____ Notepad.exe
4. _____ Cmd.exe
5. _____ Event class: File system
6. _____ Event class: Process
7. _____ Event class: Registry
8. _____ Result: Buffer Overflow
9. _____ Result: Name Not Found
10. _____ What was the Total Kernel CPU time for Notepad

Malware Detection & Removal

Antivirus software primarily uses signature-based detection methods - searching for known patterns of data within executable code. Polymorphic viruses encrypt or modify parts of their code to avoid matching virus signatures in the database. Antivirus software can use heuristic analysis to identify new malware, as well as variants of known malware, by using generic non-contiguous signatures. However, it is possible for a computer to be infected by zero-day threats, e.g. new malware for which no signature is yet known. Several of the Sysinternals tools can be used to detect and remove malware. Caution: Malware can spread via USB sticks, use "read only" media (such as a CD-R disc) to move any tools to a computer that may be infected.

Malware Cleaning Steps

- Disconnect the computer from the network (wired or wireless)
- Identify malicious processes and drivers
- Suspend and terminate any identified processes
- Identify and delete malware related applications that auto start
- Delete malware related files
- Reboot and repeat
- Repair any damage

Identify Malicious Processes

Use ProcessExplorer to look for files that:

Lack a description or company name

Are in a Windows directory

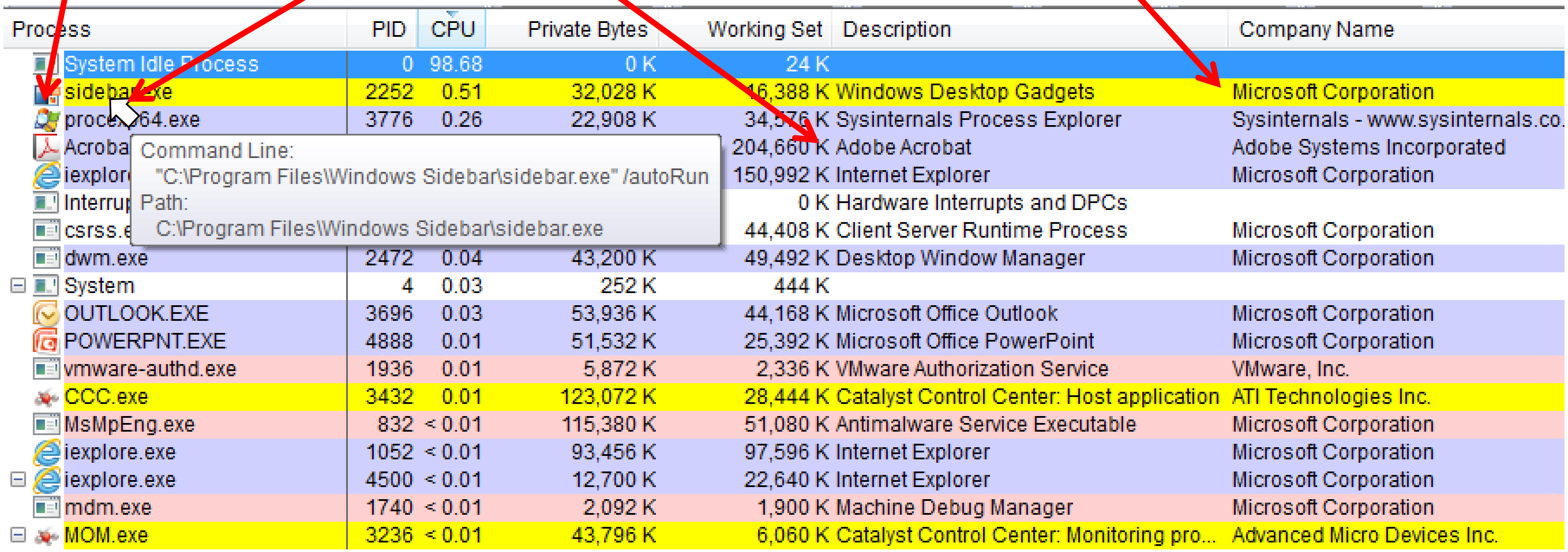
Are in a user profile

Are packed

Lack an icon

Violet - Packed Images
Pink - Services
Yellow - .NET processes
Dark gray - Suspended
Light gray - lacks focus

Tooltip



Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
System Idle Process	0	98.68	0 K	24 K		
sidebar.exe	2252	0.51	32,028 K	16,388 K	Windows Desktop Gadgets	Microsoft Corporation
procexp64.exe	3776	0.26	22,908 K	34,576 K	Sysinternals Process Explorer	Sysinternals - www.sysinternals.co...
Acroba				204,660 K	Adobe Acrobat	Adobe Systems Incorporated
iexplor				150,992 K	Internet Explorer	Microsoft Corporation
Interrup				0 K	Hardware Interrupts and DPCs	
csrss.e				44,408 K	Client Server Runtime Process	Microsoft Corporation
dwm.exe	2472	0.04	43,200 K	49,492 K	Desktop Window Manager	Microsoft Corporation
System	4	0.03	252 K	444 K		
OUTLOOK.EXE	3696	0.03	53,936 K	44,168 K	Microsoft Office Outlook	Microsoft Corporation
POWERPNT.EXE	4888	0.01	51,532 K	25,392 K	Microsoft Office PowerPoint	Microsoft Corporation
vmware-authd.exe	1936	0.01	5,872 K	2,336 K	VMware Authorization Service	VMware, Inc.
CCC.exe	3432	0.01	123,072 K	28,444 K	Catalyst Control Center: Host application	ATI Technologies Inc.
MsMpEng.exe	832	< 0.01	115,380 K	51,080 K	Antimalware Service Executable	Microsoft Corporation
iexplore.exe	1052	< 0.01	93,456 K	97,596 K	Internet Explorer	Microsoft Corporation
iexplore.exe	4500	< 0.01	12,700 K	22,640 K	Internet Explorer	Microsoft Corporation
mdm.exe	1740	< 0.01	2,092 K	1,900 K	Machine Debug Manager	Microsoft Corporation
MOM.exe	3236	< 0.01	43,796 K	6,060 K	Catalyst Control Center: Monitoring pro...	Advanced Micro Devices Inc.

```
Command Line:
  "C:\Program Files\Windows Sidebar\sidebar.exe" /autoRun
Path:
  C:\Program Files\Windows Sidebar\sidebar.exe
```

Identify Malicious Processes

- Refresh Highlighting - highlights changes
  - Red: process exited
  - Green: new process
- Change duration (default is 1 second) in Options
- Press the space bar to pause and F5 to refresh
- Show New Processes option
  - Display scrolls to make new processes visible
- Blue - running in same security context as ProcessExplorer
- Pink - host Windows services
- Purple – software image is packed (see UPX)
  - Compressed or encrypted
  - Malware uses packing (e.g. UPX)
  - Makes antivirus signature matching more difficult
  - Hides any ASCII strings (such as URL's, names)

Identify Malicious Processes

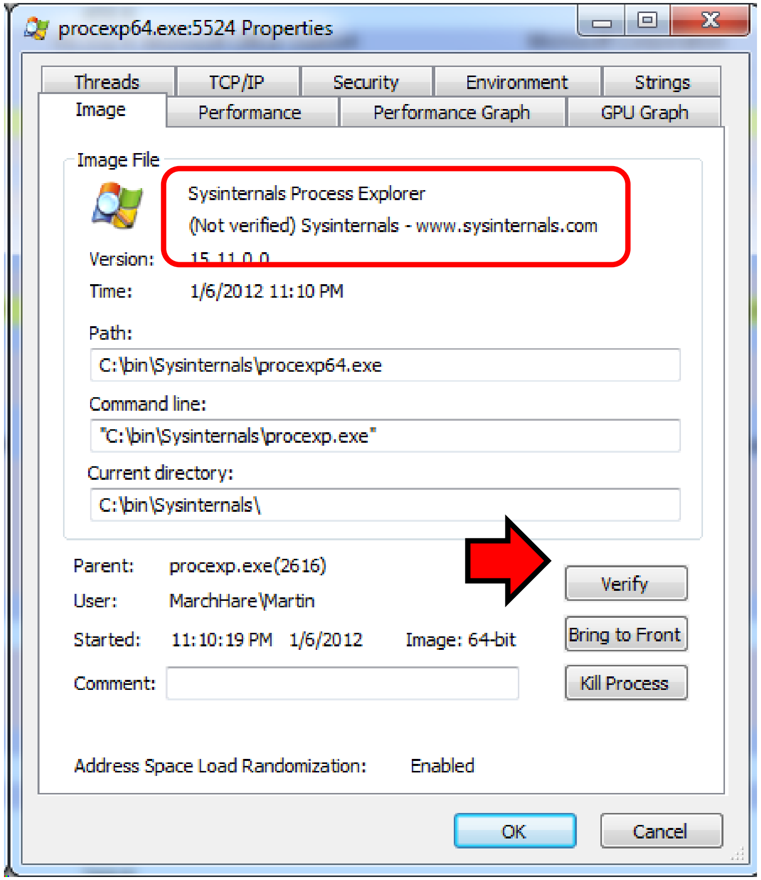
Windows Services

- Can start at system boot and run independently of the logged-on user
- Examples include IIS, Themes, Server, Workstation, …
- Can run as their own process or a service DLL inside an Svchost.exe
- Services tab shows service information details:
  - Registry name (HKLM\System\CurrentControlSet\Services\...)
  - Display name
  - Description (optional)
  - DLL path (for Svchost DLLs)

Software Image Verification

- Almost all Microsoft code is digitally signed
- Check specific signatures via the Verify button
- Check all via Verify Image Signatures option

Verification uses the Internet to query the Certificate Revocation List servers (CRL)



Sysinternals Process Explorer
(Not verified) Sysinternals - www.sysinternals.com

Version: 15.11.0.0

Time: 1/6/2012 11:10 PM

Path:
C:\bin\Sysinternals\procexp64.exe

Command line:
"C:\bin\Sysinternals\procexp.exe"

Current directory:
C:\bin\Sysinternals\

Parent: procexp.exe(2616)

User: MarchHare\Martin

Started: 11:10:19 PM 1/6/2012 Image: 64-bit

Comment:

Address Space Load Randomization: Enabled

Identify Malicious Processes

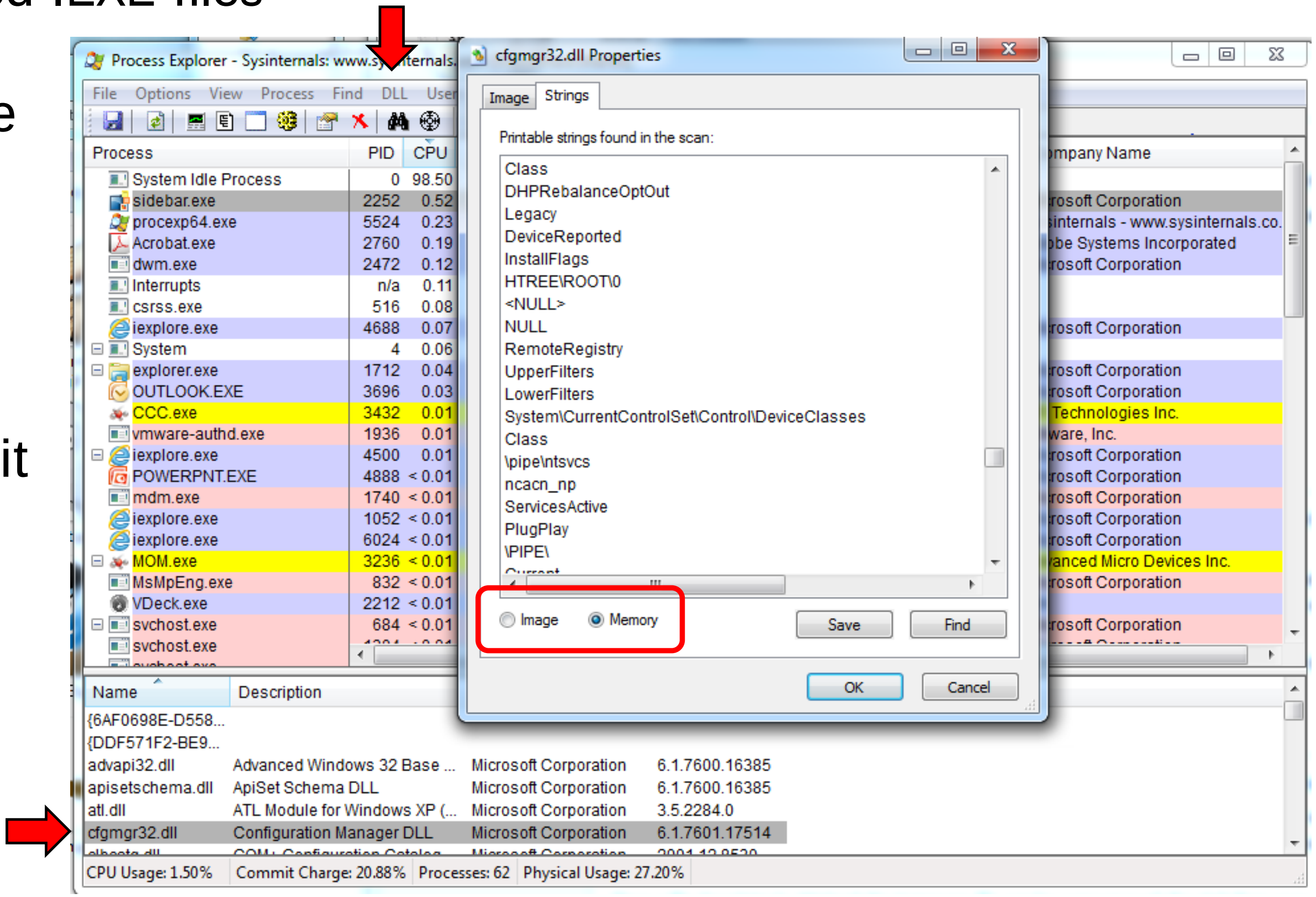
Malware can hide as a DLL inside a valid process (such as svchost)

- Typically loads through an autostart
- Can load through DLL injection (driveby)

Select DLL then click on DLL Icon

- Shows any included .EXE files
- Compare:
  - Software Image
  - In memory

Check Strings: Use Find to search for “www” or “http” and the address used, is it reasonable? If it’s a packed process, select the Memory button and do the same search.


Process Explorer - Sysinternals: www.sysinternals.
File Options View Process Find DLL User

Process	PID	CPU	ompany Name
System Idle Process	0	98.50	
sidebar.exe	2252	0.52	rosoft Corporation
procexp64.exe	5524	0.23	sinternals - www.sysinternals.co.
Acrobat.exe	2760	0.19	bbe Systems Incorporated
dwm.exe	2472	0.12	rosoft Corporation
Interrupts	n/a	0.11	
csrss.exe	516	0.08	
iexplore.exe	4688	0.07	rosoft Corporation
System	4	0.06	
explorer.exe	1712	0.04	rosoft Corporation
OUTLOOK.EXE	3696	0.03	rosoft Corporation
CCC.exe	3432	0.01	Technologies Inc.
vmware-authd.exe	1936	0.01	ware, Inc.
iexplore.exe	4500	0.01	rosoft Corporation
POWERPNT.EXE	4888	< 0.01	rosoft Corporation
mdm.exe	1740	< 0.01	rosoft Corporation
iexplore.exe	1052	< 0.01	rosoft Corporation
iexplore.exe	6024	< 0.01	rosoft Corporation
MOM.exe	3236	< 0.01	anced Micro Devices Inc.
MsMpEng.exe	832	< 0.01	rosoft Corporation
VDeck.exe	2212	< 0.01	
svchost.exe	684	< 0.01	rosoft Corporation
svchost.exe			

Name	Description		
{6AF0698E-D558...			
{DDF571F2-BE9...			
advapi32.dll	Advanced Windows 32 Base ...	Microsoft Corporation	6.1.7600.16385
apisetschema.dll	ApiSet Schema DLL	Microsoft Corporation	6.1.7600.16385
atl.dll	ATL Module for Windows XP (...	Microsoft Corporation	3.5.2284.0
cfgmgr32.dll	Configuration Manager DLL	Microsoft Corporation	6.1.7601.17514

CPU Usage: 1.50% | Commit Charge: 20.88% | Processes: 62 | Physical Usage: 27.20%

Printable strings found in the scan:

```
Class
DHPRebalanceOptOut
Legacy
DeviceReported
InstallFlags
HTREE\ROOT\0
<NULL>
NULL
RemoteRegistry
UpperFilters
LowerFilters
System\CurrentControlSet\Control\DeviceClasses
Class
\pipe\ntsvcs
ncacn_np
ServicesActive
PlugPlay
\PIPE\
```

○ Image ● Memory

Identify Malicious Processes

- Don't kill a malicious process
  - Often are restarted by watchdog or buddy process
- First – try to suspend it
  - Caution: May hang system if an Svchost process
  - Write down absolute path for each malicious EXE, DLL
- After all are suspended – kill them all
- Monitor for restarting – possibly with new names

Use AutoRuns against malware autostarts

- Reduce clutter
  - Verify code signatures
  - Hide Microsoft entries
- Double click on an item to see the configuration
- Disable malicious autostarts – delete when confirmed

Avoid False Positives

- Make reversible changes – just in case
- False positives can have unintended side-effects
  - In April 2010, McAfee VirusScan detected svchost.exe, a normal Windows binary, as a virus on machines running Windows XP with Service Pack 3, causing a reboot loop and loss of all network access. The impact on typical Enterprise monoculture environments was non-trivial.
  - In December 2010, a faulty update on the AVG anti-virus suite damaged 64-bit versions of Windows 7, rendering it unable to boot, due to an endless boot loop created.
  - In October 2011, Microsoft Security Essentials removed (quarantined) the Google Chrome browser, flagging the rival Chrome as a Zbot banking trojan.

- Malware detection is a combination of research, aptitude, attitude, experience, etc. The only 100% guarantee for removal is reimaging, including rewriting the Master Boot Record (MBR).

Memory

Memory Terms used in the tools

Private Bytes is memory that's private to that process; generally it's the amount of RAM the process has asked for in order to store runtime data. In general, doesn't include any DLLs loaded by the process.

Working Set is the portion of the processes' address space ("Private Bytes" plus memory mapped files) that is currently resident in RAM and can be referenced without a page fault. Should always be a multiple of the 4,096 byte page size.

Virtual Bytes is the total virtual address space of the process, includes both private bytes and anything memory-mapped.

Commit Charge is the combination of both the actual pagefile usage, and any memory used in every process's VM to store things actually written to memory.

System Cache is actually Cache Bytes plus the standby page list. The standby page list is also included in the "Available" physical memory.

Paging File, % In Use is the measure of how much of the page file is actually being used.

Page Fault when a process asks for some of its memory that isn't currently in its working set.

Standby Page List When a page of memory is dropped from a process's working set, rather that disappear into the "free memory" block, its put on the end of the standby page list. When a process needs new memory in its working set, the standby page list is the last place the OS looks. First, it looks in the zero page list, or the free page list, both of which are "free memory". One list is initialized to zeroes, one's not -- and they're accessed depending on the process request. Only when both of those are empty does the system look to the standby page list. The standby page list is raided last because, in the meantime, if a process has released a page from its working set, then later asks for it back (via a page fault), the system can check the standby page list to see if it is still available. If it is, the OS can retrieve it and return it back to the process without having to go to disk for it. A large majority of page faults are resolved from the standby page list, which is much faster than going to disk.

References

- http://technet.microsoft.com/en-us/sysinternals/bb963890
- Sysinternals Technical Blog
  - Hunting down and killing ransomware
  - The case of the very slow logons
  - The case of the unusable system

- http://technet.microsoft.com/en-us/sysinternals/bb963887
- Sysinternals videos

- http://technet.microsoft.com/en-us/sysinternals/bb469930
- Sysinternals Resources