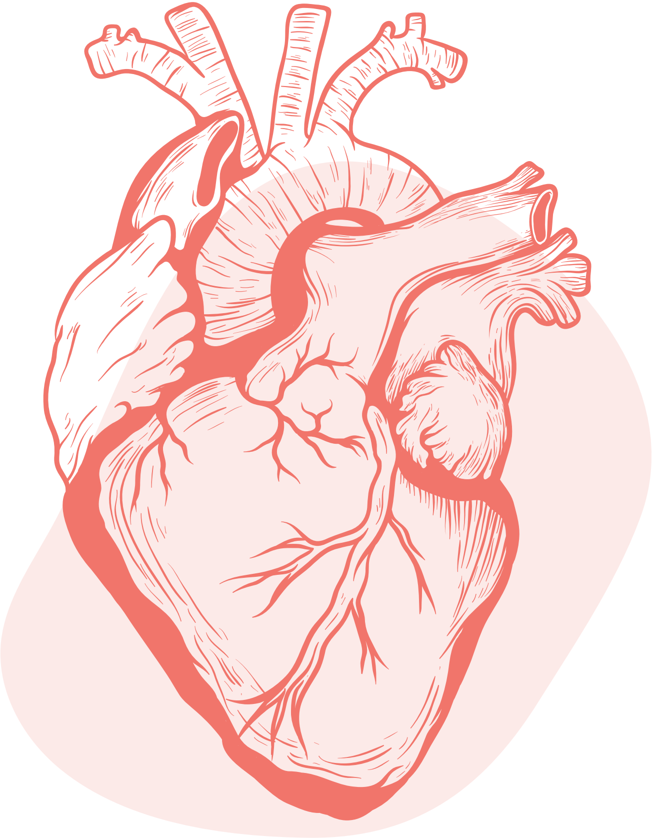
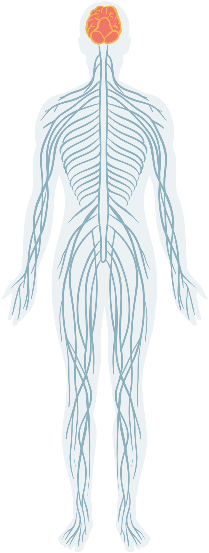
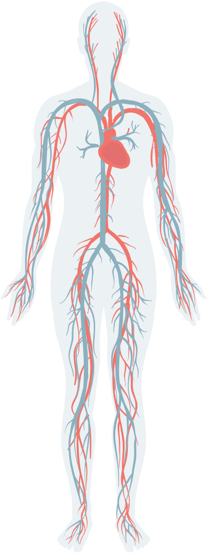


Windows Sysinternals

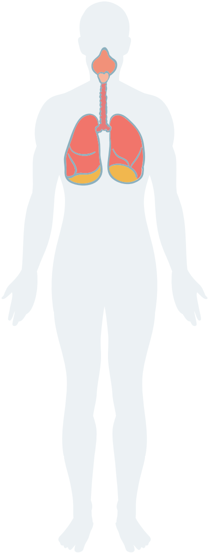
Utilities for...



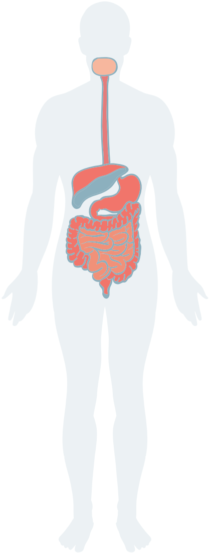
Networking



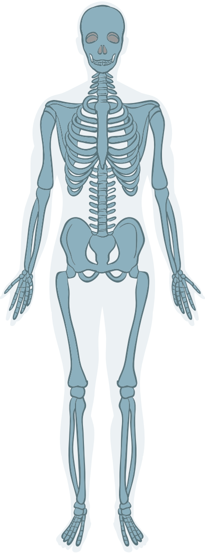
File/Disk



Other



Processing



Security

Networking

A

ShareEnum

Show file shares and their security

B

TCPview

Show all persistent connections

C

PStools

On remote systems, list/start/suspend/kill processes, passwords, users, open files, logs. Reboot. Check performance

D

Whois

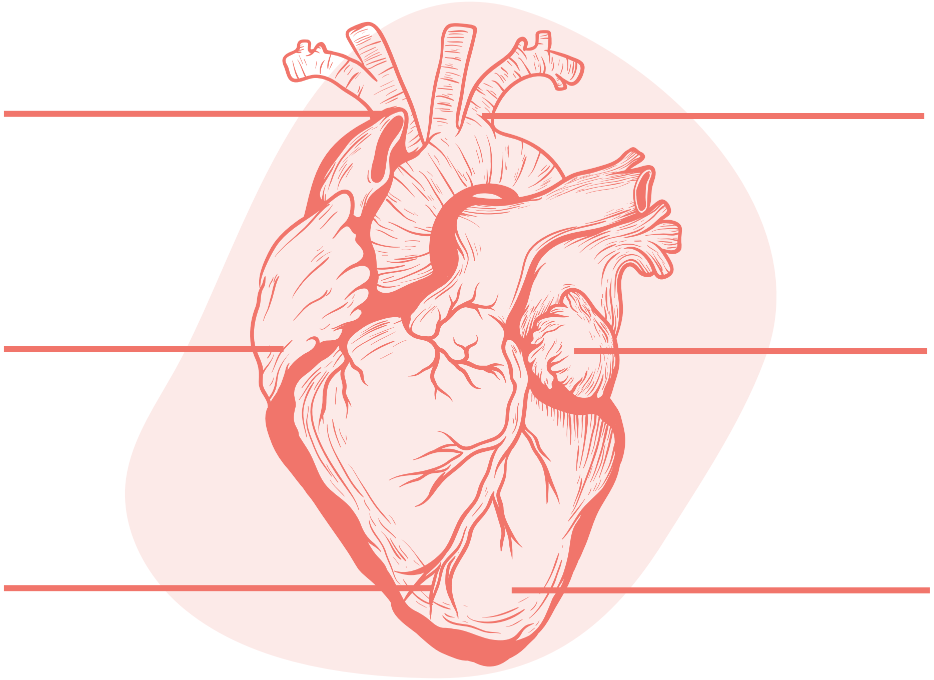
See who owns an Internet address

E

Pipelist

Show named pipes, max, and active instances

File/Disk utilities



Contig

Make a file contiguous – speeds access on HDs

Diskmon

Monitor all Disk activity; System try disk activity lite

MoveFile

Schedule file actions for boot. Good for some malware

DU - DiskUsage

Shows disk space usage for directories and sub-directories

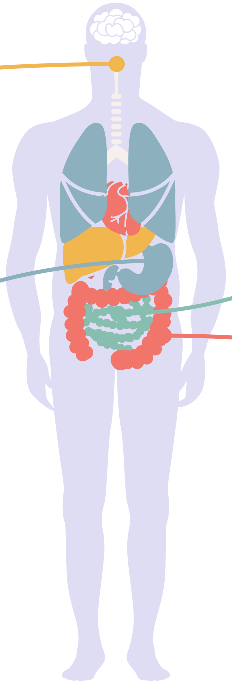
CacheSet

Control file access caching

Sync

Flush cache data to storage

Processing



01 **Autoruns**

Show/Edit boot/login programs

02 **Process Explorer**

Show/edit processes (Task manager on steroids)

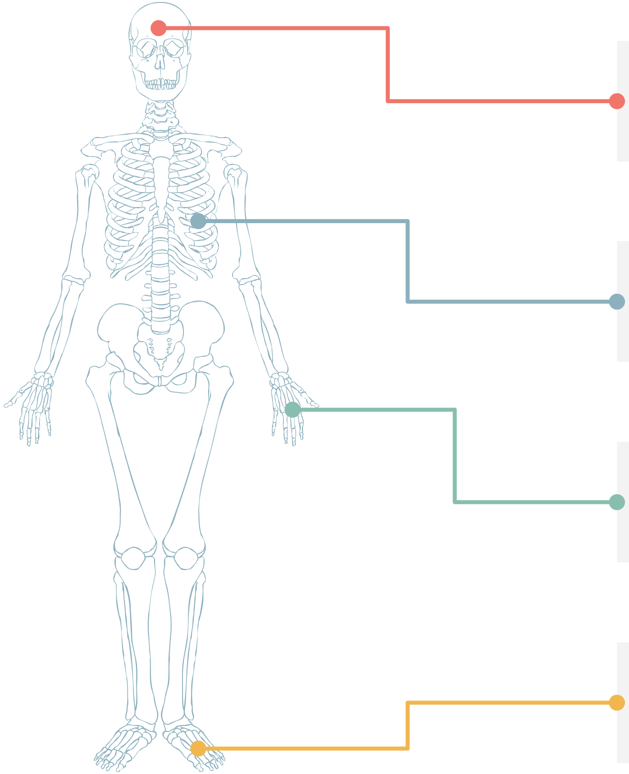
Process Monitor 03

View file, registry, thread, event activity. Can filter

ShellRunAs 04

Run a program as a different user

Security



AccessChk / AccessEnum

Check access authorities by
user / directory / registry key / service

Rootkit Revealer

Advanced rootkit detection utility

SDelete

Securely delete and overwrite
files / free space

ShareEnum

Show file shares & security settings
on your network

Process utilities

Autoruns
See what programs are configured to startup automatically when your system boots and you login. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.

Handle
This handy command-line utility will show you what files are open by which processes, and much more.

ListDLLs
List all the DLLs that are currently loaded, including where they are loaded and their version numbers. Version 2.0 prints the full path names of loaded modules.

PortMon
Monitor serial and parallel port activity with this advanced monitoring tool. It knows about all standard serial and parallel IOCTLs and even shows you a portion of the data being sent and received. Version 3.x has powerful new UI enhancements and advanced filtering capabilities.

ProcDump
This new command-line utility is aimed at capturing process dumps of otherwise difficult to isolate and reproduce CPU spikes. It also serves as a general process dump creation utility and can also monitor and generate process dumps when a process has a hung window or unhandled exception.

Process Explorer
Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.

Process Monitor
Monitor file system, Registry, process, thread and DLL activity in real-time.

PsExec
Execute processes remotely.

PsGetSid
Displays the SID of a computer or a user.

PsKill
Terminate local or remote processes.

PsList
Show information about processes and threads.

PsService
View and control services.

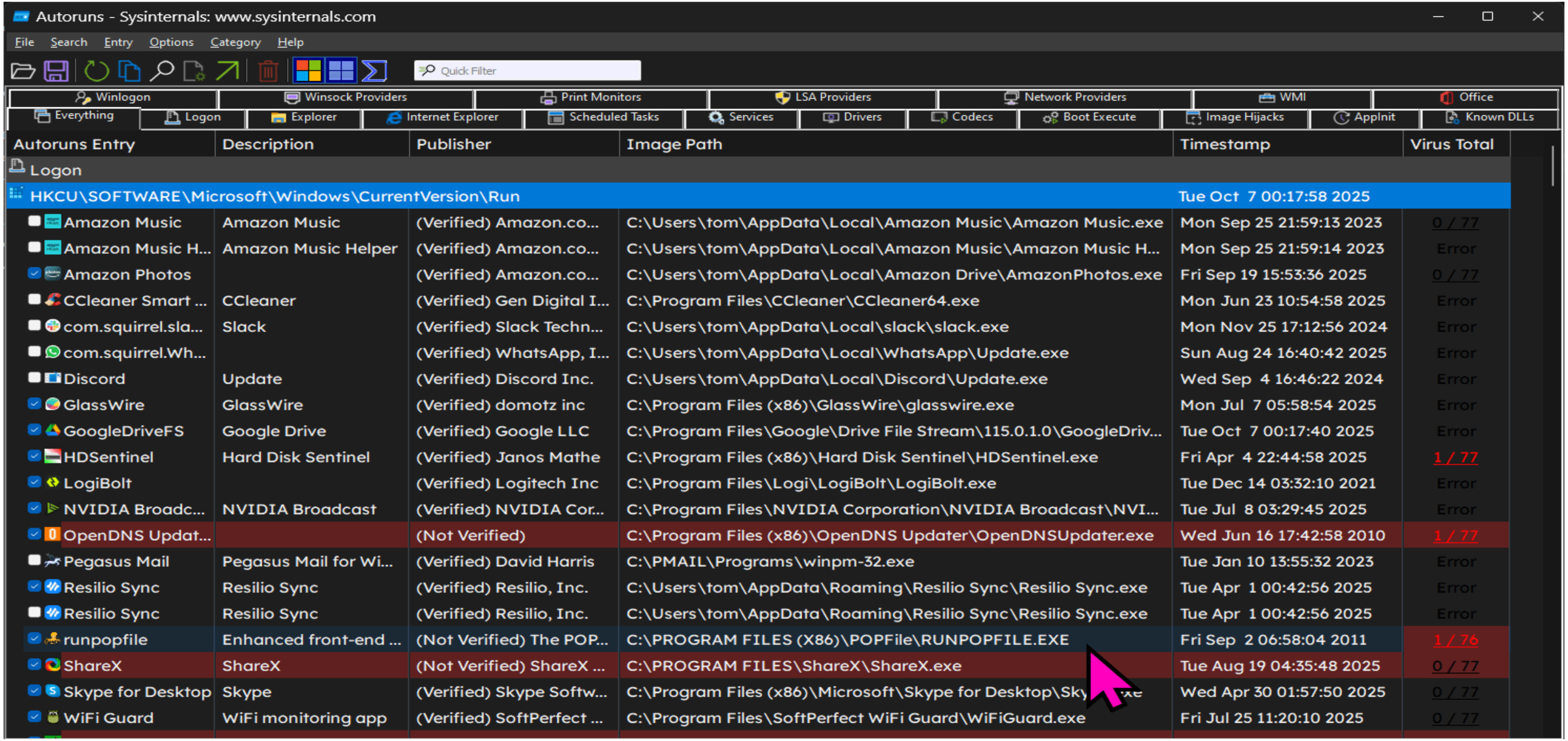
PsSuspend
Suspend and resume processes.

PsTools
The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

ShellRunas
Launch programs as a different user via a convenient shell context-menu entry.

VMMap
See 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. Identify the sources of process memory usage and the memory cost of application features.

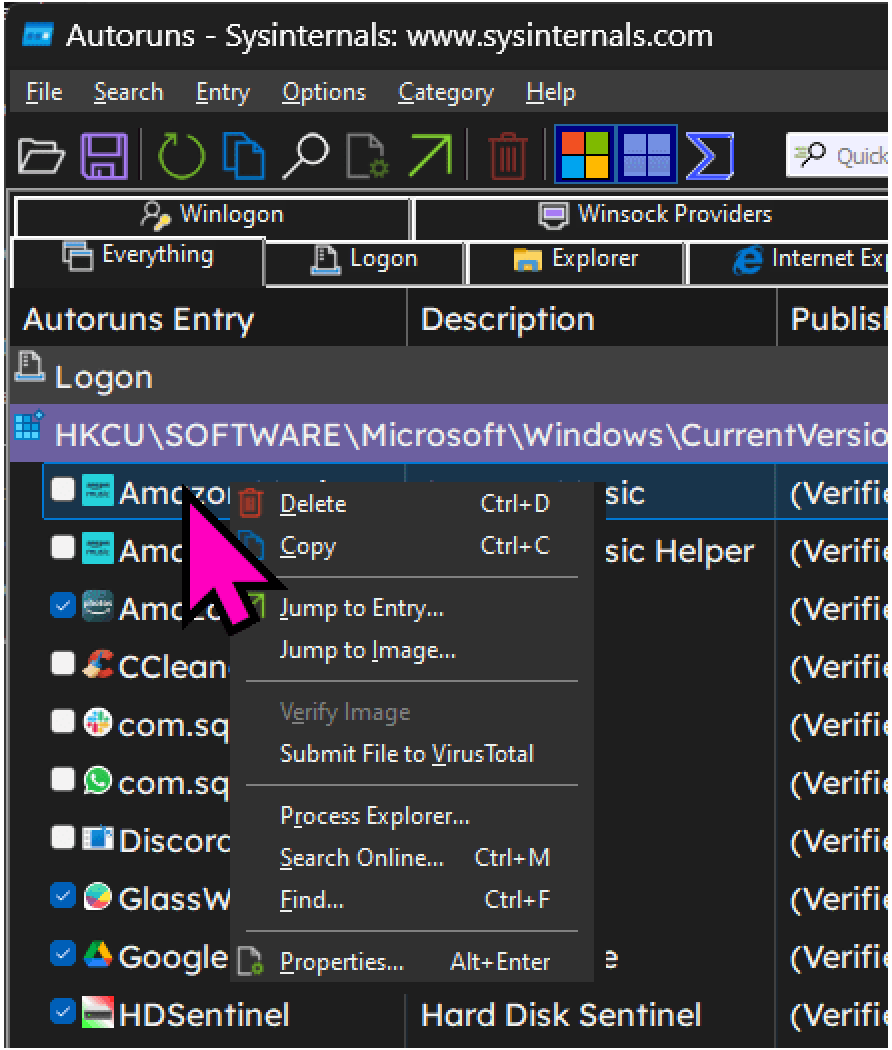
Autoruns – programs that run automatically



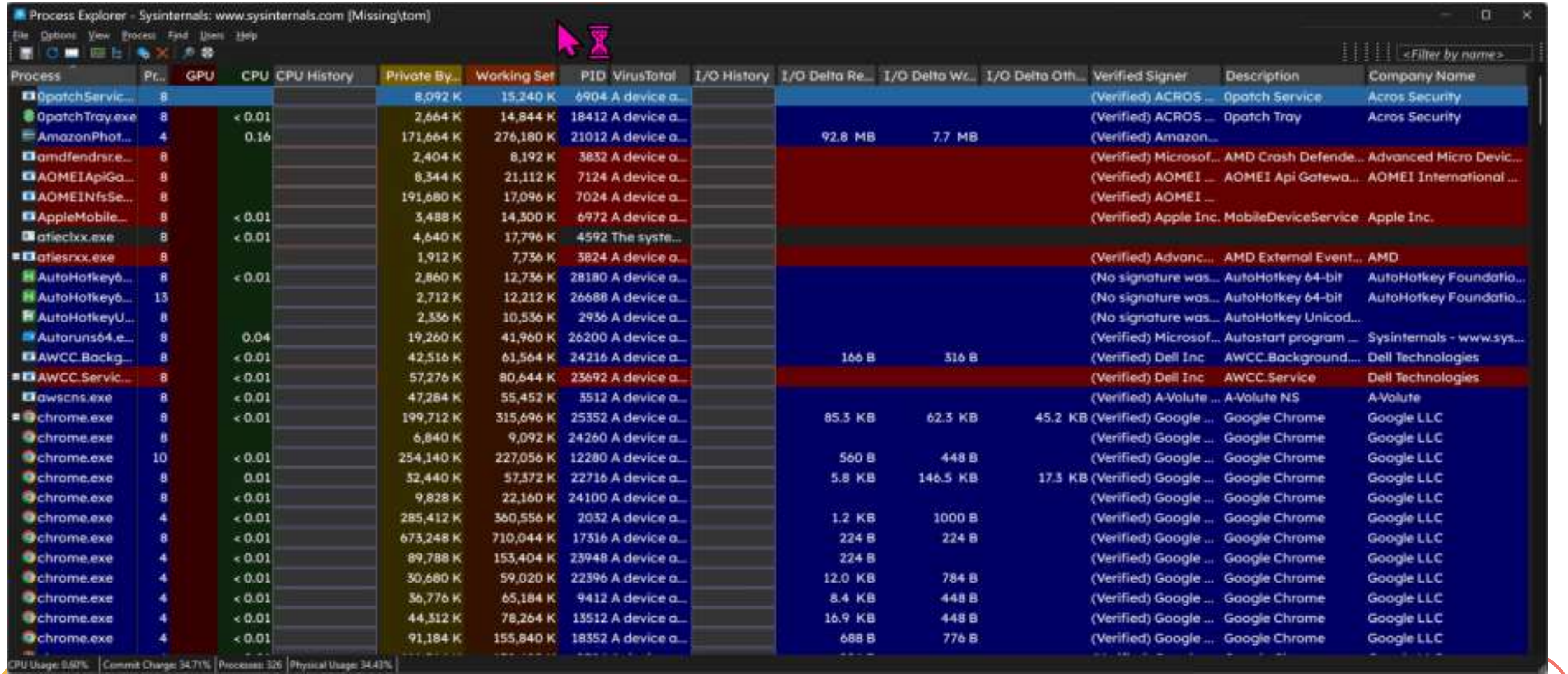
Autoruns Entry	Description	Publisher	Image Path	Timestamp	Virus Total
Logon					
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Tue Oct 7 00:17:58 2025	
□ Amazon Music	Amazon Music	(Verified) Amazon.co...	C:\Users\tom\AppData\Local\Amazon Music\Amazon Music.exe	Mon Sep 25 21:59:13 2023	0 / 77
□ Amazon Music H...	Amazon Music Helper	(Verified) Amazon.co...	C:\Users\tom\AppData\Local\Amazon Music\Amazon Music H...	Mon Sep 25 21:59:14 2023	Error
☑ Amazon Photos		(Verified) Amazon.co...	C:\Users\tom\AppData\Local\Amazon Drive\AmazonPhotos.exe	Fri Sep 19 15:53:36 2025	0 / 77
□ CCleaner Smart ...	CCleaner	(Verified) Gen Digital I...	C:\Program Files\CCleaner\CCleaner64.exe	Mon Jun 23 10:54:58 2025	Error
□ com.squirrel.sla...	Slack	(Verified) Slack Techn...	C:\Users\tom\AppData\Local\slack\slack.exe	Mon Nov 25 17:12:56 2024	Error
□ com.squirrel.Wh...		(Verified) WhatsApp, I...	C:\Users\tom\AppData\Local\WhatsApp\Update.exe	Sun Aug 24 16:40:42 2025	Error
□ Discord	Update	(Verified) Discord Inc.	C:\Users\tom\AppData\Local\Discord\Update.exe	Wed Sep 4 16:46:22 2024	Error
☑ GlassWire	GlassWire	(Verified) domotz inc	C:\Program Files (x86)\GlassWire\glasswire.exe	Mon Jul 7 05:58:54 2025	Error
☑ GoogleDriveFS	Google Drive	(Verified) Google LLC	C:\Program Files\Google\Drive File Stream\115.0.1.0\GoogleDriv...	Tue Oct 7 00:17:40 2025	Error
☑ HDSentinel	Hard Disk Sentinel	(Verified) Janos Mathe	C:\Program Files (x86)\Hard Disk Sentinel\HDSentinel.exe	Fri Apr 4 22:44:58 2025	1 / 77
☑ LogiBolt		(Verified) Logitech Inc	C:\Program Files\Logi\LogiBolt\LogiBolt.exe	Tue Dec 14 03:32:10 2021	Error
☑ NVIDIA Broadc...	NVIDIA Broadcast	(Verified) NVIDIA Cor...	C:\Program Files\NVIDIA Corporation\NVIDIA Broadcast\NVI...	Tue Jul 8 03:29:45 2025	Error
☑ OpenDNS Updat...		(Not Verified)	C:\Program Files (x86)\OpenDNS Updater\OpenDNSUpdater.exe	Wed Jun 16 17:42:58 2010	1 / 77
□ Pegasus Mail	Pegasus Mail for Wi...	(Verified) David Harris	C:\PMAIL\Programs\winpm-32.exe	Tue Jan 10 13:55:32 2023	Error
☑ Resilio Sync	Resilio Sync	(Verified) Resilio, Inc.	C:\Users\tom\AppData\Roaming\Resilio Sync\Resilio Sync.exe	Tue Apr 1 00:42:56 2025	Error
□ Resilio Sync	Resilio Sync	(Verified) Resilio, Inc.	C:\Users\tom\AppData\Roaming\Resilio Sync\Resilio Sync.exe	Tue Apr 1 00:42:56 2025	Error
☑ runpopfile	Enhanced front-end ...	(Not Verified) The POP...	C:\PROGRAM FILES (X86)\POPFile\RUNPOPFILE.EXE	Fri Sep 2 06:58:04 2011	1 / 76
☑ ShareX	ShareX	(Not Verified) ShareX ...	C:\PROGRAM FILES\ShareX\ShareX.exe	Tue Aug 19 04:35:48 2025	0 / 77
☑ Skype for Desktop	Skype	(Verified) Skype Softw...	C:\Program Files (x86)\Microsoft\Skype for Desktop\Sky xe	Wed Apr 30 01:57:50 2025	0 / 77
☑ WiFi Guard	WiFi monitoring app	(Verified) SoftPerfect ...	C:\Program Files\SoftPerfect WiFi Guard\WiFiGuard.exe	Fri Jul 25 11:20:10 2025	0 / 77

Autoruns actions
(as administrator)

- Uncheck entry to disable
- Delete entry
- Jump to other entries
- Submit to VirusTotal
- Open Process Explorer for the process
- Search Online
- Find among entries
- Properties



Process Explorer



Process Explorer - Sysinternals: www.sysinternals.com [Missing\tom]

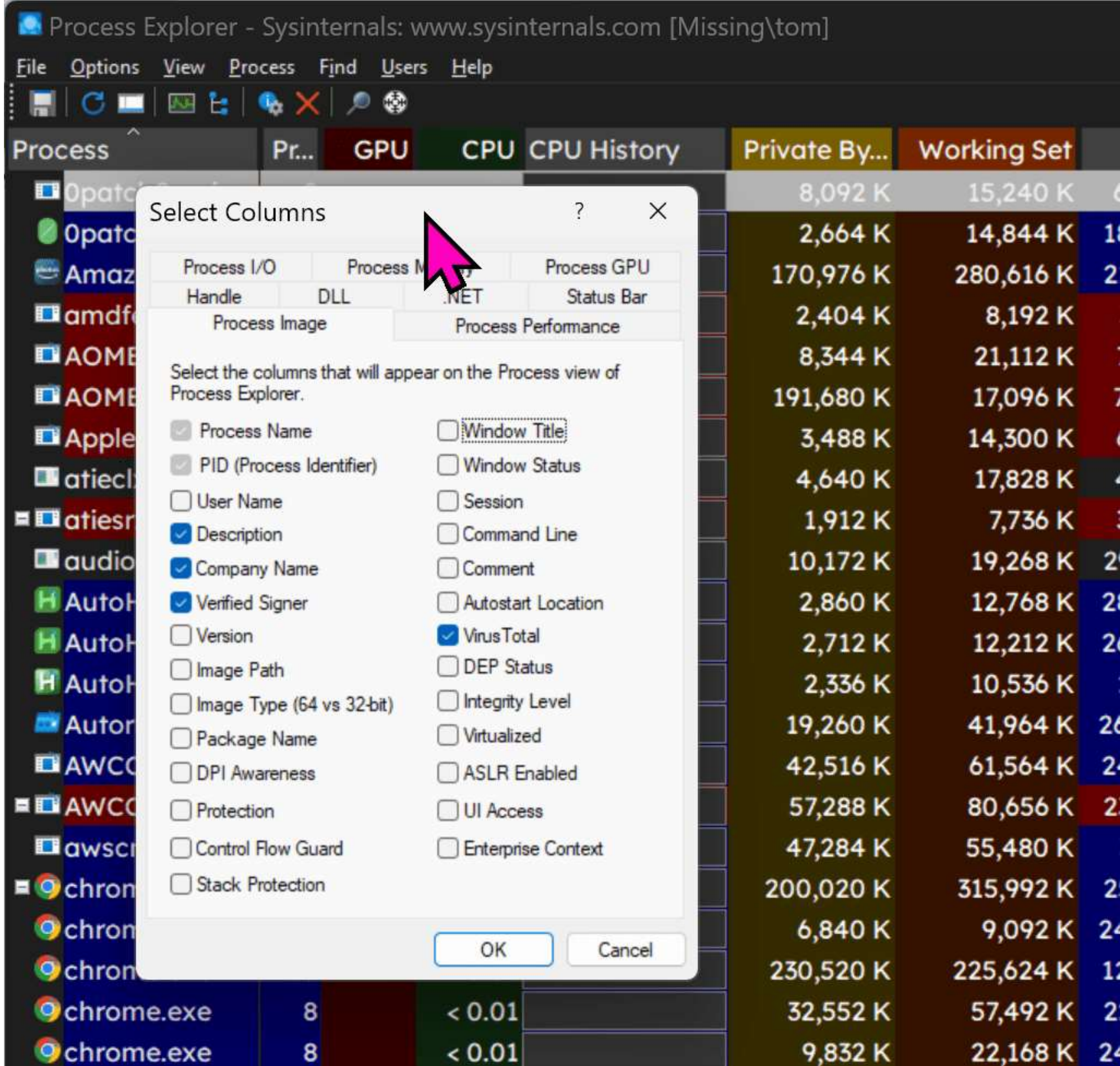
Process	Pr...	GPU	CPU	CPU History	Private By...	Working Set	PID	VirusTotal	I/O History	I/O Delta Re...	I/O Delta Wr...	I/O Delta Oth...	Verified Signer	Description	Company Name
0patchServic...	8				8,092 K	15,240 K	6904	A device a...					(Verified) ACROS ...	0patch Service	Acros Security
0patchTray.exe	8		< 0.01		2,664 K	14,844 K	18412	A device a...					(Verified) ACROS ...	0patch Tray	Acros Security
AmazonPhot...	4		0.16		171,664 K	276,180 K	21012	A device a...		92.8 MB	7.7 MB		(Verified) Amazon...		
amdfendrsr.e...	8				2,404 K	8,192 K	3832	A device a...					(Verified) Microsof...	AMD Crash Defende...	Advanced Micro Devic...
AOMEIApiGa...	8				8,344 K	21,112 K	7124	A device a...					(Verified) AOMEI ...	AOMEI Api Gatewa...	AOMEI International ...
AOMEINfsSe...	8				191,680 K	17,096 K	7024	A device a...					(Verified) AOMEI ...		
AppleMobile...	8		< 0.01		3,488 K	14,300 K	6972	A device a...					(Verified) Apple Inc.	MobileDeviceService	Apple Inc.
atieclxx.exe	8		< 0.01		4,640 K	17,796 K	4592	The syste...							
atiesrxx.exe	8				1,912 K	7,736 K	3824	A device a...					(Verified) Advanc...	AMD External Event...	AMD
AutoHotkey6...	8		< 0.01		2,860 K	12,736 K	28180	A device a...					(No signature was...	AutoHotkey 64-bit	AutoHotkey Foundatio...
AutoHotkey6...	13				2,712 K	12,212 K	26688	A device a...					(No signature was...	AutoHotkey 64-bit	AutoHotkey Foundatio...
AutoHotkeyU...	8				2,336 K	10,536 K	2936	A device a...					(No signature was...	AutoHotkey Unicod...	
Autoruns64.e...	8		0.04		19,260 K	41,960 K	26200	A device a...					(Verified) Microsof...	Autostart program ...	Sysinternals - www.sys...
AWCC.Backg...	8		< 0.01		42,516 K	61,564 K	24216	A device a...		166 B	316 B		(Verified) Dell Inc	AWCC.Background....	Dell Technologies
AWCC.Servic...	8		< 0.01		57,276 K	80,644 K	23692	A device a...					(Verified) Dell Inc	AWCC.Service	Dell Technologies
awscns.exe	8		< 0.01		47,284 K	55,452 K	3512	A device a...					(Verified) A-Volute ...	A-Volute NS	A-Volute
chrome.exe	8		< 0.01		199,712 K	315,696 K	25352	A device a...		85.3 KB	62.3 KB	45.2 KB	(Verified) Google ...	Google Chrome	Google LLC
chrome.exe	8				6,840 K	9,092 K	24260	A device a...					(Verified) Google ...	Google Chrome	Google LLC
chrome.exe	10		< 0.01		254,140 K	227,056 K	12280	A device a...		560 B	448 B		(Verified) Google ...	Google Chrome	Google LLC
chrome.exe	8		0.01		32,440 K	57,372 K	22716	A device a...		5.8 KB	146.5 KB	17.3 KB	(Verified) Google ...	Google Chrome	Google LLC
chrome.exe	8		< 0.01		9,828 K	22,160 K	24100	A device a...					(Verified) Google ...	Google Chrome	Google LLC
chrome.exe	4		< 0.01		285,412 K	360,556 K	2032	A device a...		1.2 KB	1000 B		(Verified) Google ...	Google Chrome	Google LLC
chrome.exe	8		< 0.01		673,248 K	710,044 K	17316	A device a...		224 B	224 B		(Verified) Google ...	Google Chrome	Google LLC
chrome.exe	4		< 0.01		89,788 K	153,404 K	23948	A device a...		224 B			(Verified) Google ...	Google Chrome	Google LLC
chrome.exe	4		< 0.01		30,680 K	59,020 K	22396	A device a...		12.0 KB	784 B		(Verified) Google ...	Google Chrome	Google LLC
chrome.exe	4		< 0.01		36,776 K	65,184 K	9412	A device a...		8.4 KB	448 B		(Verified) Google ...	Google Chrome	Google LLC
chrome.exe	4		< 0.01		44,312 K	78,264 K	13512	A device a...		16.9 KB	448 B		(Verified) Google ...	Google Chrome	Google LLC
chrome.exe	4		< 0.01		91,184 K	155,840 K	18352	A device a...		688 B	776 B		(Verified) Google ...	Google Chrome	Google LLC

CPU Usage: 0.60% | Commit Charge: 34.71% | Processes: 326 | Physical Usage: 34.43%

Process Explorer - columns

Tabs at top to choose fields for:

- Image
- Performance
- Handles
- DLL
- .NET
- Status bar
- GPU
- Memory
- I/O



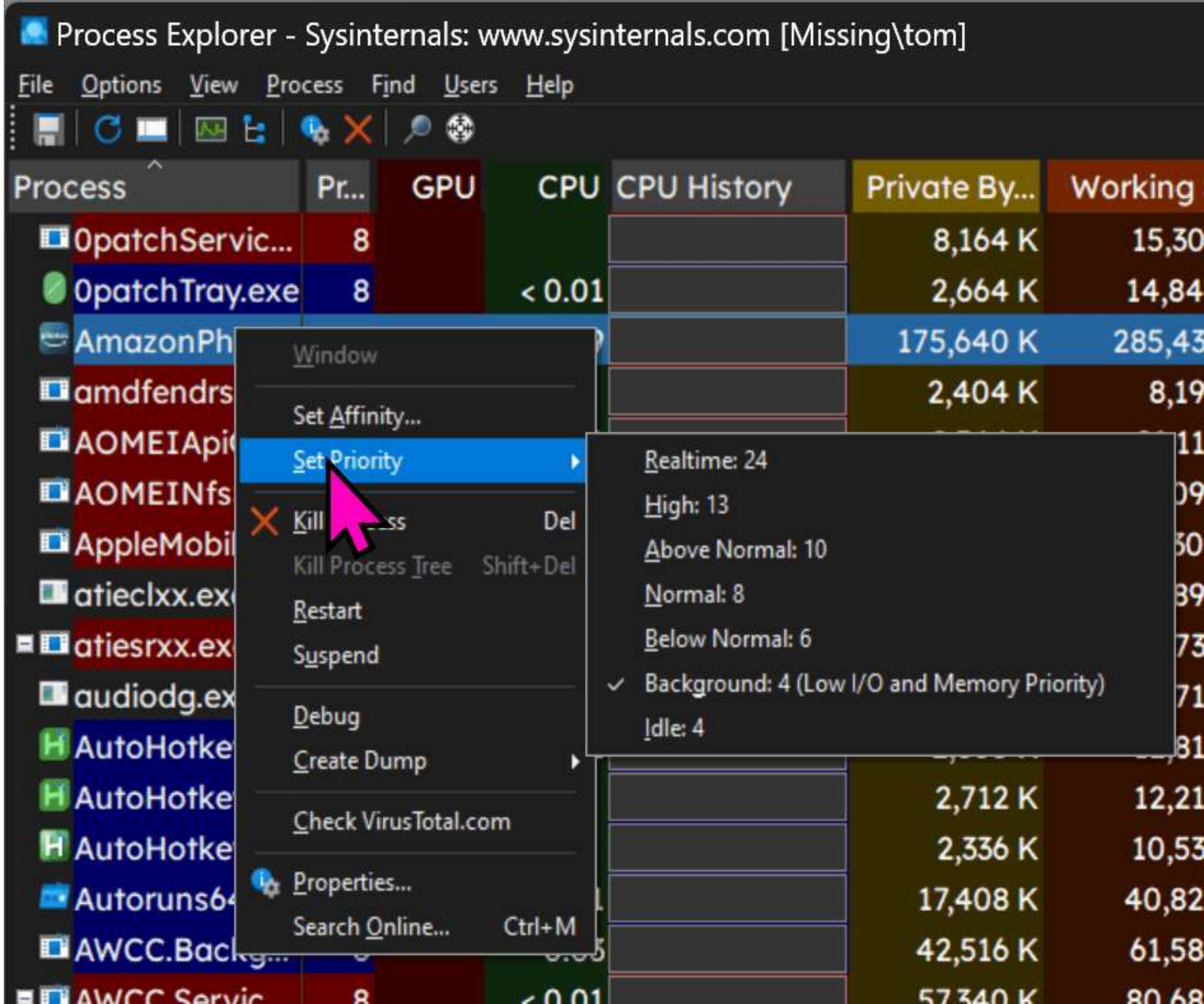
Select the columns that will appear on the Process view of Process Explorer.

☑ Process Name	☐ Window Title
☑ PID (Process Identifier)	☐ Window Status
☐ User Name	☐ Session
☑ Description	☐ Command Line
☑ Company Name	☐ Comment
☑ Verified Signer	☐ Autostart Location
☐ Version	☑ VirusTotal
☐ Image Path	☐ DEP Status
☐ Image Type (64 vs 32-bit)	☐ Integrity Level
☐ Package Name	☐ Virtualized
☐ DPI Awareness	☐ ASLR Enabled
☐ Protection	☐ UI Access
☐ Control Flow Guard	☐ Enterprise Context
☐ Stack Protection	

Process	Pr...	GPU	CPU	CPU History	Private By...	Working Set
0patc					8,092 K	15,240 K
0patc					2,664 K	14,844 K
Amaz					170,976 K	280,616 K
amdf					2,404 K	8,192 K
AOME					8,344 K	21,112 K
AOME					191,680 K	17,096 K
Apple					3,488 K	14,300 K
atiecl					4,640 K	17,828 K
atiesr					1,912 K	7,736 K
audio					10,172 K	19,268 K
AutoH					2,860 K	12,768 K
AutoH					2,712 K	12,212 K
AutoH					2,336 K	10,536 K
Autor					19,260 K	41,964 K
AWCC					42,516 K	61,564 K
AWCC					57,288 K	80,656 K
awscr					47,284 K	55,480 K
chron					200,020 K	315,992 K
chron					6,840 K	9,092 K
chron					230,520 K	225,624 K
chrome.exe	8		< 0.01		32,552 K	57,492 K
chrome.exe	8		< 0.01		9,832 K	22,168 K

Process Explorer actions

Set affinity (to a CPU core)
Set priority
Kill process
Restart
Suspen
Debug
Create dump
Check VirusTotal
Properties
Search online



Sysinternals File and Disk Utilities

AccessChk
This tool shows you the accesses the user or group you specify has to files, Registry keys or Windows services.

AccessEnum
This simple yet powerful security tool shows you who has what access to directories, files and Registry keys on your systems. Use it to find holes in your permissions.

CacheSet
CacheSet is a program that allows you to control the Cache Manager's working set size using functions provided by NT. It's compatible with all versions of NT.

Contig
Wish you could quickly defragment your frequently used files? Use Contig to optimize individual files, or to create new files that are contiguous.

Disk2vhd
Disk2vhd simplifies the migration of physical systems into virtual machines (p2v).

DiskExt
Display volume disk-mappings.

DiskMon
This utility captures all hard disk activity or acts like a software disk activity light in your system tray.

DiskView
Graphical disk sector utility.

Disk Usage (DU)
View disk usage by directory.

EFSDump
View information for encrypted files.

FindLinks
FindLinks reports the file index and any hard links (alternate file paths on the same volume) that exist for the specified file. A file's data remains allocated so long as at it has at least one file name referencing it.

jcd
jcd is a command-line tool that provides quick directory navigation with substring matching and smart selection for Linux and macOS.

Junction
Create Win2K NTFS symbolic links.

LDMDump
Dump the contents of the Logical Disk Manager"s on-disk database, which describes the partitioning of Windows 2000 Dynamic disks.

MoveFile
Schedule file rename and delete commands for the next reboot. This can be useful for cleaning stubborn or in-use malware files.

NTFSInfo
Use NTFSInfo to see detailed information about NTFS volumes, including the size and location of the Master File Table (MFT) and MFT-zone, as well as the sizes of the NTFS meta-data files.

PendMoves
See what files are scheduled for delete or rename the next time the system boots.

Process Monitor
Monitor file system, Registry, process, thread and DLL activity in real-time.

PsFile
See what files are opened remotely.

PsTools
The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

SDelete
Securely overwrite your sensitive files and cleanse your free space of previously deleted files using this DoD-compliant secure delete program.

ShareEnum
Scan file shares on your network and view their security settings to close security holes.

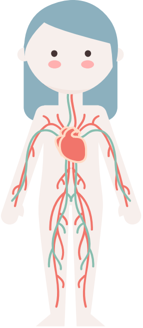
Sigcheck
Dump file version information and verify that images on your system are digitally signed.

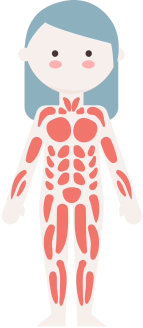
Streams
Reveal NTFS alternate streams.

Sync
Flush cached data to disk.

VolumeID
Set Volume ID of FAT or NTFS drives.

Security utilities





AccessChk

This tool shows you the level of access the user or group you specify has to files, Registry keys or Windows services.

AccessEnum

This simple yet powerful security tool shows you who has what access to directories, files and Registry keys on your systems. Use it to find holes in your permissions.

Autologon

Bypass password screen during logon.

Autoruns

See what programs are configured to startup automatically when your system boots and you log in. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.

LogonSessions

List active logon sessions

Process Explorer

Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.

PsExec

Execute processes with limited-user rights.

PsLoggedOn

Show users logged on to a system.

PsLogList

Dump event log records.

PsTools

The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

Rootkit Revealer

RootkitRevealer is an advanced rootkit detection utility.

SDelete

Securely overwrite your sensitive files and cleanse your free space of previously deleted files using this DoD-compliant secure delete program.

ShareEnum

Scan file shares on your network and view their security settings to close security holes.

ShellRunas

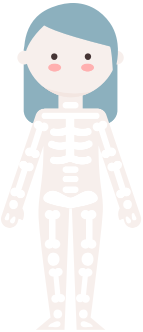
Launch programs as a different user via a convenient shell context-menu entry.

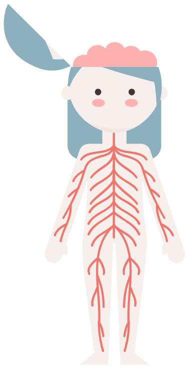
Sigcheck

Dump file version information and verify that images on your system are digitally signed.

Sysmon

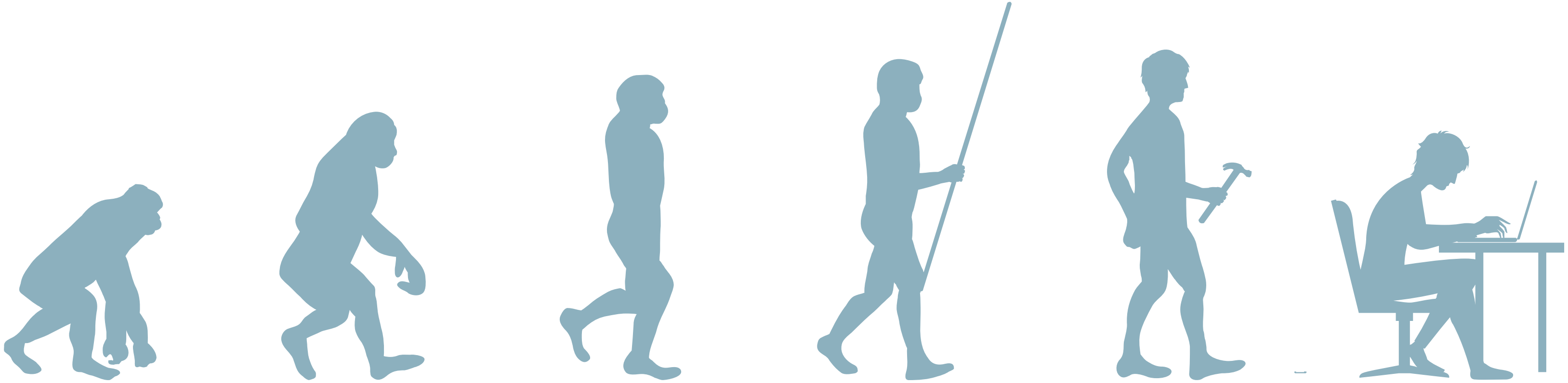
Monitors and reports key system activity via the Windows event log.





Other

Many tools: ADExplorer ADInsight adrestore Autologon Bginfo Clockres Coreinfo CPUSTRES ctrl2cap Dbgview Desktops disk2vhd diskext DiskView efsdump FindLinks handle hex2dec junction ldmdump Listdlls livekd LoadOrd logonsessions notmyfault notmyfaultc ntfsinfo pagedfrg pendmoves portmon procdump RAMMap RDCMan RegDelNull regjump ru sigcheck streams strings Sysmon tcpvcon Testlimit vmmap Volumeid Winobj ZoomIt



Sysinternals

Useful strong tools
for managing your computer
& diagnosing troubles.