



National Forensic
Sciences University

Knowledge | Wisdom | Fulfilment

An Institution of National Importance
(Ministry of Home Affairs, Government of India)



DIGITAL FORENSICS - TA2 ASSIGNMENT

JUN 2022

Under the Guidance of Prof. Sarang Rajvansh

PREPARED BY

Sagar Shah

ENROLLMENT NUMBER:

101CTMTCS2122040



Introduction & Background

The Sysinternals web site was created in 1996 by Mark Russinovich to host his advanced system utilities and technical information. Whether you're an IT Pro or a developer, you'll find Sysinternals utilities to help you manage, troubleshoot and diagnose your Windows systems and applications.

1. Read the official guide to the Sysinternals tools, [Troubleshooting with the Windows Sysinternals Tools](#)
2. Read the Sysinternals Blog for a detailed change feed of tool updates
3. Watch Mark's Sysinternals Update videos on YouTube
4. Watch Mark's top-rated Case-of-the-Unexplained troubleshooting presentations and other webcasts
5. Read Mark's Blog which highlight use of the tools to solve real problems
6. Check out the Sysinternals Learning Resources page
7. Post your questions in the Sysinternals Forum



Submission Guidelines & Requirements

1. To be submitted before 7-Jun-2022.
2. The following practical is given to test our investigation skills.



AUTORUN

INTRODUCTION

This utility, which has the most far reaching information on auto-beginning areas of any startup screen, shows you what projects are arranged to run during framework bootup or login, and when you start different inherent Windows applications like Internet Explorer, Explorer and media players. These projects and drivers remember ones for your startup organiser, Run, RunOnce, and other Registry keys. Autoruns reports Explorer shell augmentations, toolbars, program partner objects, Winlogon notices, auto-start administrations, and significantly more. Autoruns go far past other autostart utilities.

Autoruns' Hide Signed Microsoft Entries choice assists you with focusing in on outsider auto-beginning pictures that have been added to your framework and it has support for taking a gander at the auto-beginning pictures designed for different records designed on a framework. Likewise remembered for the download bundle is an order line identical that can yield in CSV design, Autorunsc.

You'll most likely be amazed at the number of executables that are sent off naturally!

SCREENSHOT

[illegible]

USAGE

Basically run Autoruns and it shows you the presently arranged auto-start applications as well as the full rundown of Registry and document framework areas accessible for auto-start setup. Autostart areas showed via Autoruns incorporate logon sections, Explorer additional items, Internet Explorer additional items including Browser Helper Objects (BHOs), Appinit_dlls, picture commandeers, boot execute pictures, Winlogon notice DLLs, Windows Services and Winsock Layered Service Providers, media codecs, and then some. Change tabs to see autostarts from various classes.

To see the properties of an executable arranged to run naturally, select it and utilise the Properties menu thing or toolbar button. Assuming Process Explorer is running and there is a functioning cycle executing the chosen executable then the Process Explorer menu thing in the Entry menu will open the cycle properties exchange box for the cycle executing the chosen picture.

Explore the Registry or document framework area shown or the arrangement of an auto-start thing by choosing the thing and utilising the Jump to Entry menu thing or toolbar button, and explore to the area of an autostart picture.

To incapacitate an auto-start section uncheck its really take a look at the box. To erase an auto-start design section utilise the Delete menu thing or toolbar button.

The Options menu incorporates a few showcase sifting choices, for example, just appearance non-Windows sections, as well as admittance to an output choices discourse from where you can empower signature check and VirusTotal hash and record accommodation.

Select sections in the User menu to see auto-beginning pictures for various client accounts.

More data in plain view choices and extra data is accessible in the on-line help.

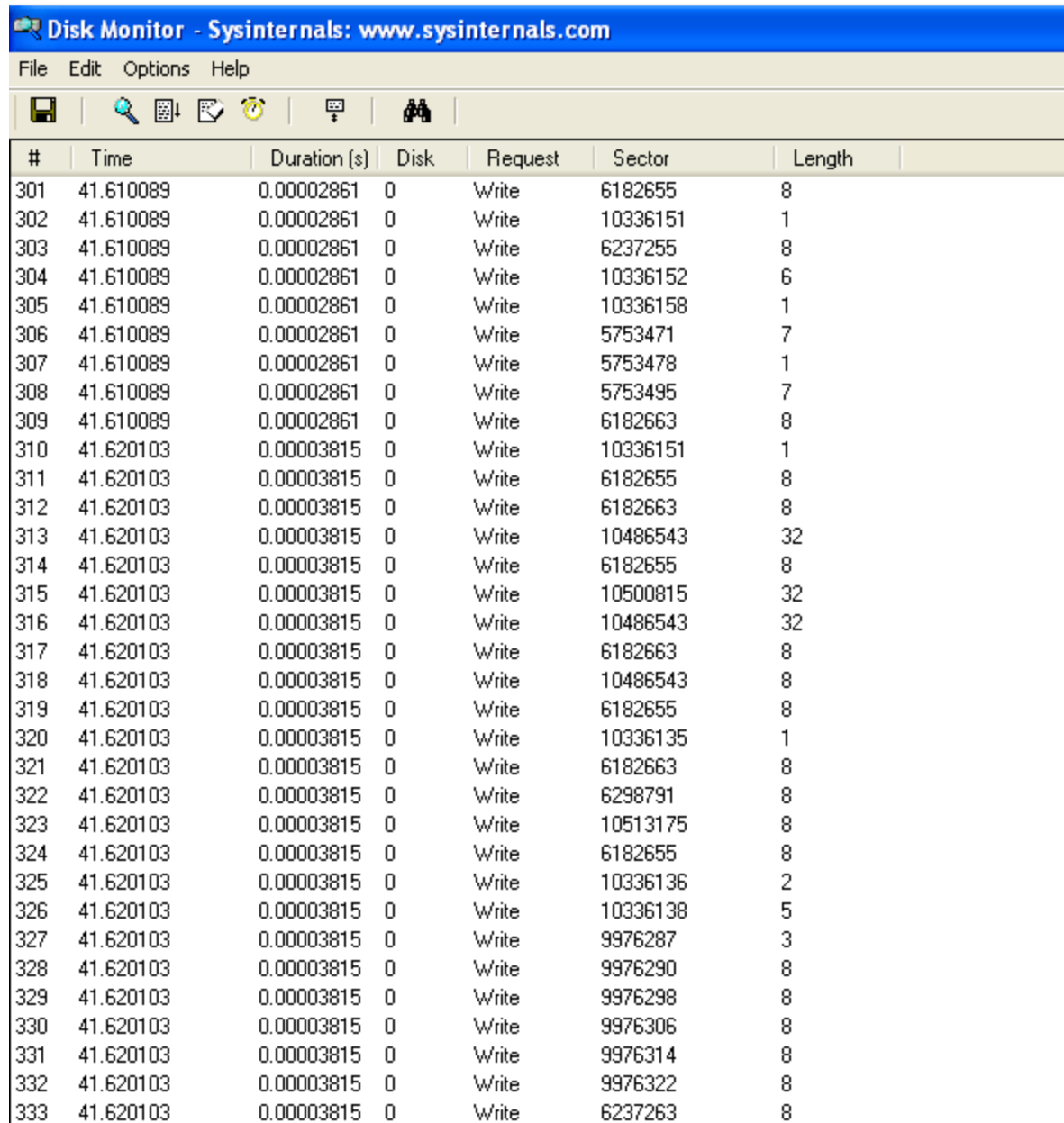


DISKMON

INTRODUCTION

DiskMon is an application that logs and displays all hard disk activity on a Windows system. You can also minimise DiskMon to your system tray where it acts as a disk light, presenting a green icon when there is disk-read activity and a red icon when there is disk-write activity.

SCREENSHOT



The screenshot shows the Disk Monitor application window. The title bar reads "Disk Monitor - Sysinternals: www.sysinternals.com". The menu bar includes "File", "Edit", "Options", and "Help". The toolbar contains icons for saving, finding, printing, pausing, and other functions. The main display area is a table with the following columns: #, Time, Duration (s), Disk, Request, Sector, and Length. The table contains 33 rows of data, all showing "Write" requests to disk 0.

#	Time	Duration (s)	Disk	Request	Sector	Length
301	41.610089	0.00002861	0	Write	6182655	8
302	41.610089	0.00002861	0	Write	10336151	1
303	41.610089	0.00002861	0	Write	6237255	8
304	41.610089	0.00002861	0	Write	10336152	6
305	41.610089	0.00002861	0	Write	10336158	1
306	41.610089	0.00002861	0	Write	5753471	7
307	41.610089	0.00002861	0	Write	5753478	1
308	41.610089	0.00002861	0	Write	5753495	7
309	41.610089	0.00002861	0	Write	6182663	8
310	41.620103	0.00003815	0	Write	10336151	1
311	41.620103	0.00003815	0	Write	6182655	8
312	41.620103	0.00003815	0	Write	6182663	8
313	41.620103	0.00003815	0	Write	10486543	32
314	41.620103	0.00003815	0	Write	6182655	8
315	41.620103	0.00003815	0	Write	10500815	32
316	41.620103	0.00003815	0	Write	10486543	32
317	41.620103	0.00003815	0	Write	6182663	8
318	41.620103	0.00003815	0	Write	10486543	8
319	41.620103	0.00003815	0	Write	6182655	8
320	41.620103	0.00003815	0	Write	10336135	1
321	41.620103	0.00003815	0	Write	6182663	8
322	41.620103	0.00003815	0	Write	6298791	8
323	41.620103	0.00003815	0	Write	10513175	8
324	41.620103	0.00003815	0	Write	6182655	8
325	41.620103	0.00003815	0	Write	10336136	2
326	41.620103	0.00003815	0	Write	10336138	5
327	41.620103	0.00003815	0	Write	9976287	3
328	41.620103	0.00003815	0	Write	9976290	8
329	41.620103	0.00003815	0	Write	9976298	8
330	41.620103	0.00003815	0	Write	9976306	8
331	41.620103	0.00003815	0	Write	9976314	8
332	41.620103	0.00003815	0	Write	9976322	8
333	41.620103	0.00003815	0	Write	6237263	8



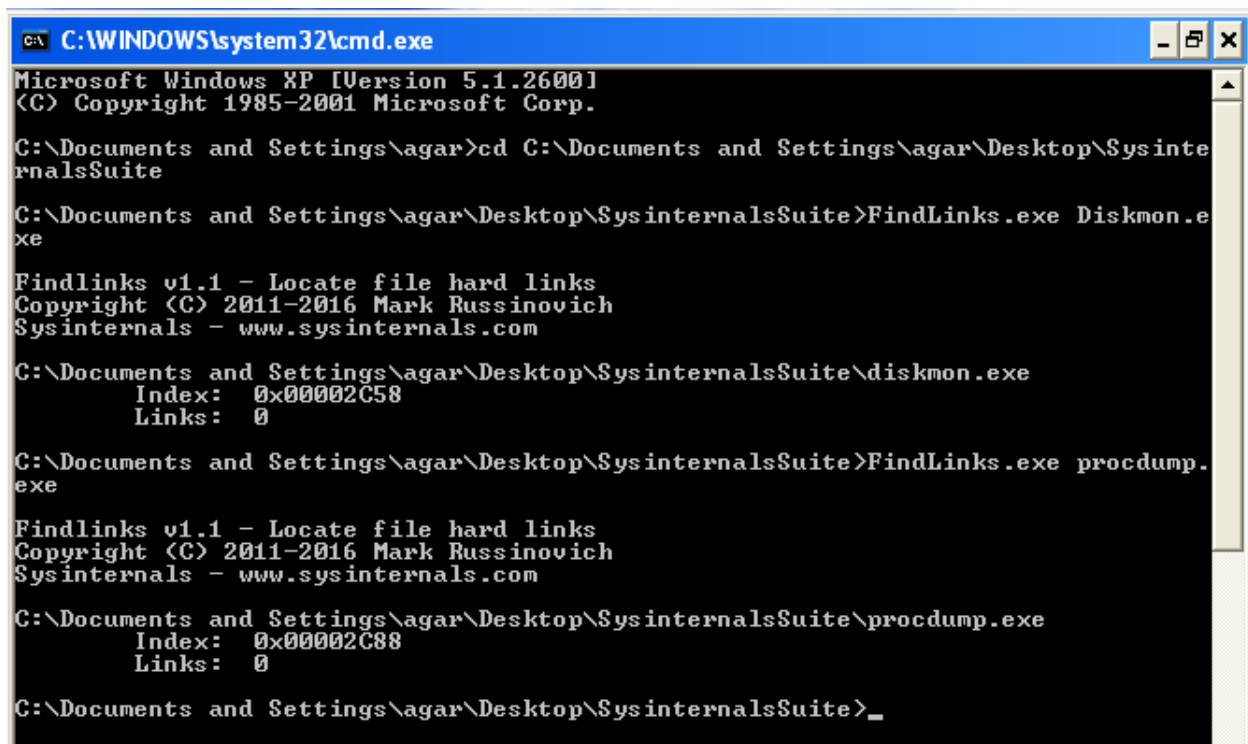
FINDLINKS

INTRODUCTION

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 it has at least one file name referencing it.

USAGE findlinks <filename>

SCREENSHOT



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\agar>cd C:\Documents and Settings\agar\Desktop\SysinternalsSuite

C:\Documents and Settings\agar\Desktop\SysinternalsSuite>FindLinks.exe Diskmon.exe

Findlinks v1.1 - Locate file hard links
Copyright (C) 2011-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Documents and Settings\agar\Desktop\SysinternalsSuite\diskmon.exe
      Index: 0x00002C58
      Links: 0

C:\Documents and Settings\agar\Desktop\SysinternalsSuite>FindLinks.exe procdump.exe

Findlinks v1.1 - Locate file hard links
Copyright (C) 2011-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Documents and Settings\agar\Desktop\SysinternalsSuite\procdump.exe
      Index: 0x00002C88
      Links: 0

C:\Documents and Settings\agar\Desktop\SysinternalsSuite>_
```



PROCESS EXPLORER

INTRODUCTION

Ever wondered which program has a particular file or directory open? Now you can find out. Process Explorer shows you information about which handles and DLLs processes have opened or loaded.

The Process Explorer display consists of two sub-windows. The top window always shows a list of the currently active processes, including the names of their owning accounts, whereas the information displayed in the bottom window depends on the mode that Process Explorer is in: if it is in handle mode you'll see the handles that the process selected in the top window has opened; if Process Explorer is in DLL mode you'll see the DLLs and memory-mapped files that the process has loaded. Process Explorer also has a powerful search capability that will quickly show you which processes have particular handles opened or DLLs loaded.

The unique capabilities of Process Explorer make it useful for tracking down DLL-version problems or handle leaks, and provide insight into the way Windows and applications work.

SCREENSHOT

Process Explorer - Sysinternals: www.sysinternals.com [SAGAR-4E577FD72\agar]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
csrss.exe		1,716 K	1,436 K	588	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		6,184 K	4,688 K	612	Windows NT Logon Applicat...	Microsoft Corporation
services.exe		1,576 K	3,204 K	656	Services and Controller app	Microsoft Corporation
VBoxService.exe		3,148 K	3,932 K	824	VirtualBox Guest Additions S...	Oracle Corporation
svchost.exe		2,984 K	4,640 K	872	Generic Host Process for Wi...	Microsoft Corporation
wmiprivse.exe		2,120 K	6,096 K	408	WMI	Microsoft Corporation
wmiprivse.exe		1,788 K	4,656 K	2688	WMI	Microsoft Corporation
svchost.exe		1,908 K	4,260 K	964	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe					Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe					Windows Security Center No...	Microsoft Corporation
wuauclt.exe					Automatic Updates	Microsoft Corporation
svchost.exe					Generic Host Process for Wi...	Microsoft Corporation
svchost.exe					Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe					Spooler SubSystem App	Microsoft Corporation
alg.exe					Application Layer Gateway S...	Microsoft Corporation
lsass.exe		3,756 K	5,928 K	668	LSA Shell (Export Version)	Microsoft Corporation
explorer.exe	0.81	15,096 K	23,792 K	1488	Windows Explorer	Microsoft Corporation
VBoxTray.exe		1,924 K	3,508 K	564	VirtualBox Guest Additions Tr...	Oracle Corporation
apateDNS.exe		22,516 K	23,780 K	1268	Mandiant	Mandiant
cmd.exe		1,876 K	108 K	2196	Windows Command Processor	Microsoft Corporation
procexp.exe		16,536 K	21,740 K	1536	Sysinternals Process Explorer	Sysinternals - www.sysinter...
Procmon.exe		9,524 K	652 K	3256	Process Monitor	Sysinternals - www.sysinter...
svchost.exe		828 K	2,212 K	2860	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		828 K	2,216 K	2008	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		828 K	2,216 K	3880	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		828 K	2,220 K	3916	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		828 K	2,220 K	3776	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		828 K	2,216 K	932	Generic Host Process for Wi...	Microsoft Corporation

Command Line:
C:\WINDOWS\system32\wbem\wmiprivse.exe
Path:
C:\WINDOWS\system32\wbem\wmiprivse.exe
WMI Providers:
[WMIProv]
Namespace: Root\WMI
DLL: C:\WINDOWS\system32\wbem\wmiprov.dll

CPU Usage: 0.81% Commit Charge: 4.88% Processes: 31 Physical Usage: 9.76%



PROCESS MONITOR

INTRODUCTION

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such as session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.

OVERVIEW

Process Monitor includes powerful monitoring and filtering capabilities, including:

1. More data captured for operation input and output parameters
2. Non-destructive filters allow you to set filters without losing data
3. Capture of thread stacks for each operation make it possible in many cases to identify the root cause of an operation
4. Reliable capture of process details, including image path, command line, user and session ID
5. Configurable and moveable columns for any event property
6. Filters can be set for any data field, including fields not configured as columns
7. Advanced logging architecture scales to tens of millions of captured events and gigabytes of log data
8. Process tree tool shows relationship of all processes referenced in a trace
9. Native log format preserves all data for loading in a different Process Monitor instance
10. Process tooltip for easy viewing of process image information
11. Detail tooltip allows convenient access to formatted data that doesn't fit in the column
12. Cancellable search
13. Boot time logging of all operations
14. The best way to become familiar with Process Monitor's features is to read through the help file and then visit each of its menu items and options on a live system.

SCREENSHOT

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Process Monitor - Sysinternals: www.sysinternals.com

Time...	Process Name	PID	Operation	Path	Result	Detail
10:41:...	svchost.exe	964	RegCloseKey	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	SUCCESS	
10:41:...	svchost.exe	964	RegCloseKey	HKCU\Software\Classes	SUCCESS	
10:41:...	svchost.exe	964	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
10:41:...	svchost.exe	964	RegOpenKey	HKCU\Software\Classes\ApplID\{8BC3...	NAME NOT FOUND	Desired Access: R...
10:41:...	svchost.exe	964	RegOpenKey	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	SUCCESS	Desired Access: R...
10:41:...	svchost.exe	964	RegQueryKey	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	SUCCESS	Query: Name
10:41:...	svchost.exe	964	RegOpenKey	HKCU\Software\Classes\ApplID\{8BC3...	NAME NOT FOUND	Desired Access: M...
10:41:...	svchost.exe	964	RegQueryValue	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	NAME NOT FOUND	Length: 144
10:41:...	svchost.exe	964	RegCloseKey	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	SUCCESS	
10:41:...	svchost.exe	964	RegOpenKey	HKCU\Software\Classes	SUCCESS	Desired Access: R...
10:41:...	svchost.exe	964	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
10:41:...	svchost.exe	964	RegOpenKey	HKCU\Software\Classes\ApplID\{8BC3...	NAME NOT FOUND	Desired Access: R...
10:41:...	svchost.exe	964	RegOpenKey	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	SUCCESS	Desired Access: R...
10:41:...	svchost.exe	964	RegQueryKey	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	SUCCESS	Query: Name
10:41:...	svchost.exe	964	RegOpenKey	HKCU\Software\Classes\ApplID\{8BC3...	NAME NOT FOUND	Desired Access: M...
10:41:...	svchost.exe	964	RegQueryValue	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	SUCCESS	Type: REG_SZ, Le...
10:41:...	svchost.exe	964	RegQueryKey	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	SUCCESS	Query: Name
10:41:...	svchost.exe	964	RegOpenKey	HKCU\Software\Classes\ApplID\{8BC3...	NAME NOT FOUND	Desired Access: M...
10:41:...	svchost.exe	964	RegQueryValue	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	SUCCESS	Type: REG_SZ, Le...
10:41:...	svchost.exe	964	RegQueryKey	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	SUCCESS	Query: Name
10:41:...	svchost.exe	964	RegOpenKey	HKCU\Software\Classes\ApplID\{8BC3...	NAME NOT FOUND	Desired Access: M...
10:41:...	svchost.exe	964	RegQueryValue	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	NAME NOT FOUND	Length: 144
10:41:...	svchost.exe	964	RegQueryKey	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	SUCCESS	Query: Name
10:41:...	svchost.exe	964	RegOpenKey	HKCU\Software\Classes\ApplID\{8BC3...	NAME NOT FOUND	Desired Access: M...
10:41:...	svchost.exe	964	RegQueryValue	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	NAME NOT FOUND	Length: 144
10:41:...	svchost.exe	964	RegQueryKey	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	SUCCESS	Query: Name
10:41:...	svchost.exe	964	RegOpenKey	HKCU\Software\Classes\ApplID\{8BC3...	NAME NOT FOUND	Desired Access: M...
10:41:...	svchost.exe	964	RegQueryValue	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	BUFFER OVERFL...	Length: 144
10:41:...	svchost.exe	964	RegQueryKey	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	SUCCESS	Query: Name
10:41:...	svchost.exe	964	RegOpenKey	HKCU\Software\Classes\ApplID\{8BC3...	NAME NOT FOUND	Desired Access: M...
10:41:...	svchost.exe	964	RegQueryValue	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	BUFFER OVERFL...	Length: 144
10:41:...	svchost.exe	964	RegQueryValue	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	SUCCESS	Type: REG_BINA...
10:41:...	svchost.exe	964	RegOpenKey	HKLM\Software\Microsoft\OLE	SUCCESS	Desired Access: M...
10:41:...	svchost.exe	964	RegQueryValue	HKLM\SOFTWARE\Microsoft\Ole\Leg...	NAME NOT FOUND	Length: 144
10:41:...	svchost.exe	964	RegQueryValue	HKLM\SOFTWARE\Microsoft\Ole\Leg...	NAME NOT FOUND	Length: 144
10:41:...	svchost.exe	964	RegCloseKey	HKLM\SOFTWARE\Microsoft\Ole	SUCCESS	
10:41:...	svchost.exe	964	RegQueryKey	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	SUCCESS	Query: Name
10:41:...	svchost.exe	964	RegOpenKey	HKCU\Software\Classes\ApplID\{8BC3...	NAME NOT FOUND	Desired Access: M...
10:41:...	svchost.exe	964	RegQueryValue	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	NAME NOT FOUND	Length: 144
10:41:...	svchost.exe	964	RegQueryKey	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	SUCCESS	Query: Name
10:41:...	svchost.exe	964	RegOpenKey	HKCU\Software\Classes\ApplID\{8BC3...	NAME NOT FOUND	Desired Access: M...
10:41:...	svchost.exe	964	RegQueryValue	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	NAME NOT FOUND	Length: 144
10:41:...	svchost.exe	964	RegOpenKey	HKCU\Software\Classes\ApplID\{8BC3...	NAME NOT FOUND	Desired Access: M...
10:41:...	svchost.exe	964	RegQueryValue	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	NAME NOT FOUND	Length: 144
10:41:...	svchost.exe	964	RegCloseKey	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	SUCCESS	
10:41:...	svchost.exe	964	RegCloseKey	HKCU\Software\Classes	SUCCESS	
10:41:...	svchost.exe	964	RegOpenKey	HKCU\Software\Classes	SUCCESS	Desired Access: R...
10:41:...	svchost.exe	964	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
10:41:...	svchost.exe	964	RegOpenKey	HKCU\Software\Classes\ApplID\{8BC3...	NAME NOT FOUND	Desired Access: R...
10:41:...	svchost.exe	964	RegOpenKey	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	SUCCESS	Desired Access: R...
10:41:...	svchost.exe	964	RegQueryKey	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	SUCCESS	Query: Name
10:41:...	svchost.exe	964	RegOpenKey	HKCU\Software\Classes\ApplID\{8BC3...	NAME NOT FOUND	Desired Access: M...
10:41:...	svchost.exe	964	RegQueryValue	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	SUCCESS	Type: REG_SZ, Le...
10:41:...	svchost.exe	964	RegQueryKey	HKCR\ApplID\{8BC3F05E-D86B-11D0-...	SUCCESS	Query: Name

Showing 17,086 of 48,490 events (35%) Backed by virtual memory

start SysinternalsSuite Process Monitor - Sys...



TCPVIEW

INTRODUCTION

TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. On Windows Server 2008, Vista, and XP, TCPView also reports the name of the process that owns the endpoint. TCPView provides a more informative and conveniently presented subset of the Netstat program that ships with Windows. The TCPView download includes Tcpcvcon, a command-line version with the same functionality.

USING TCPVIEW

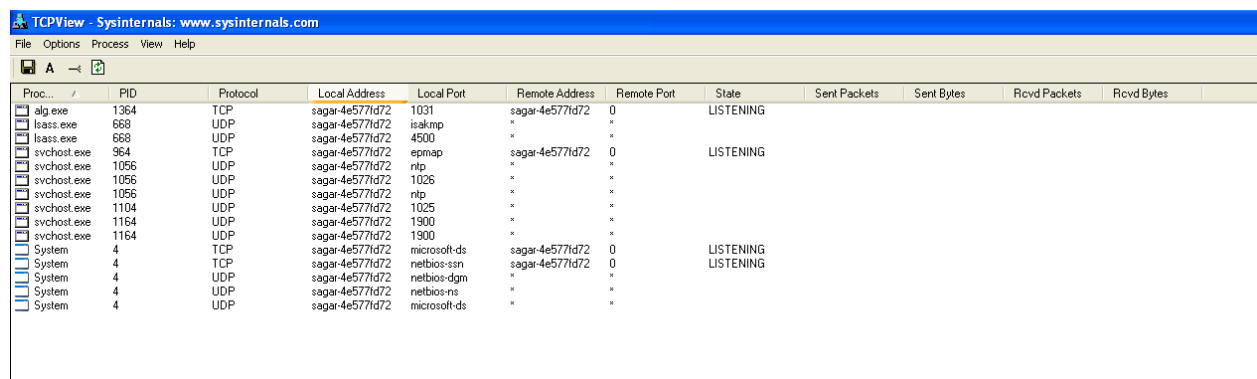
When you start TCPView it will enumerate all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions. You can use a toolbar button or menu item to toggle the display of resolved names. TCPView shows the name of the process that owns each endpoint, including the service name (if any).

By default, TCPView updates every second, but you can use the Options|Refresh Rate menu item to change the rate. Endpoints that change state from one update to the next are highlighted in yellow; those that are deleted are shown in red, and new endpoints are shown in green.

You can close established TCP/IP connections (those labelled with a state of ESTABLISHED) by selecting File|Close Connections, or by right-clicking on a connection and choosing Close Connections from the resulting context menu.

You can save TCPView's output window to a file using the Save menu item.

SCREENSHOT



The screenshot shows the TCPView application window with the title bar 'TCPView - Sysinternals: www.sysinternals.com'. The menu bar includes 'File', 'Options', 'Process', 'View', and 'Help'. The toolbar contains icons for saving, refreshing, and other functions. The main display is a table with the following columns: Proc., PID, Protocol, Local Address, Local Port, Remote Address, Remote Port, State, Sent Packets, Sent Bytes, Rcvd Packets, and Rcvd Bytes. The table lists several endpoints, including those for 'alg.exe', 'lsass.exe', 'svchost.exe', and 'System'. The 'State' column shows 'LISTENING' for several entries. The 'Remote Address' column shows 'sagar-4e5771d72' for several entries.

Proc.	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
alg.exe	1364	TCP	sagar-4e5771d72	1031	sagar-4e5771d72	0	LISTENING				
lsass.exe	668	UDP	sagar-4e5771d72	isakmp	*	*					
lsass.exe	668	UDP	sagar-4e5771d72	4500	*	*					
svchost.exe	964	TCP	sagar-4e5771d72	epmap	sagar-4e5771d72	0	LISTENING				
svchost.exe	1056	UDP	sagar-4e5771d72	ntp	*	*					
svchost.exe	1056	UDP	sagar-4e5771d72	1026	*	*					
svchost.exe	1056	UDP	sagar-4e5771d72	ntp	*	*					
svchost.exe	1104	UDP	sagar-4e5771d72	1025	*	*					
svchost.exe	1164	UDP	sagar-4e5771d72	1900	*	*					
svchost.exe	1164	UDP	sagar-4e5771d72	1900	*	*					
System	4	TCP	sagar-4e5771d72	microsoft-ds	sagar-4e5771d72	0	LISTENING				
System	4	TCP	sagar-4e5771d72	netbios-ssn	sagar-4e5771d72	0	LISTENING				
System	4	UDP	sagar-4e5771d72	netbios-dgm	*	*					
System	4	UDP	sagar-4e5771d72	netbios-ns	*	*					
System	4	UDP	sagar-4e5771d72	microsoft-ds	*	*					

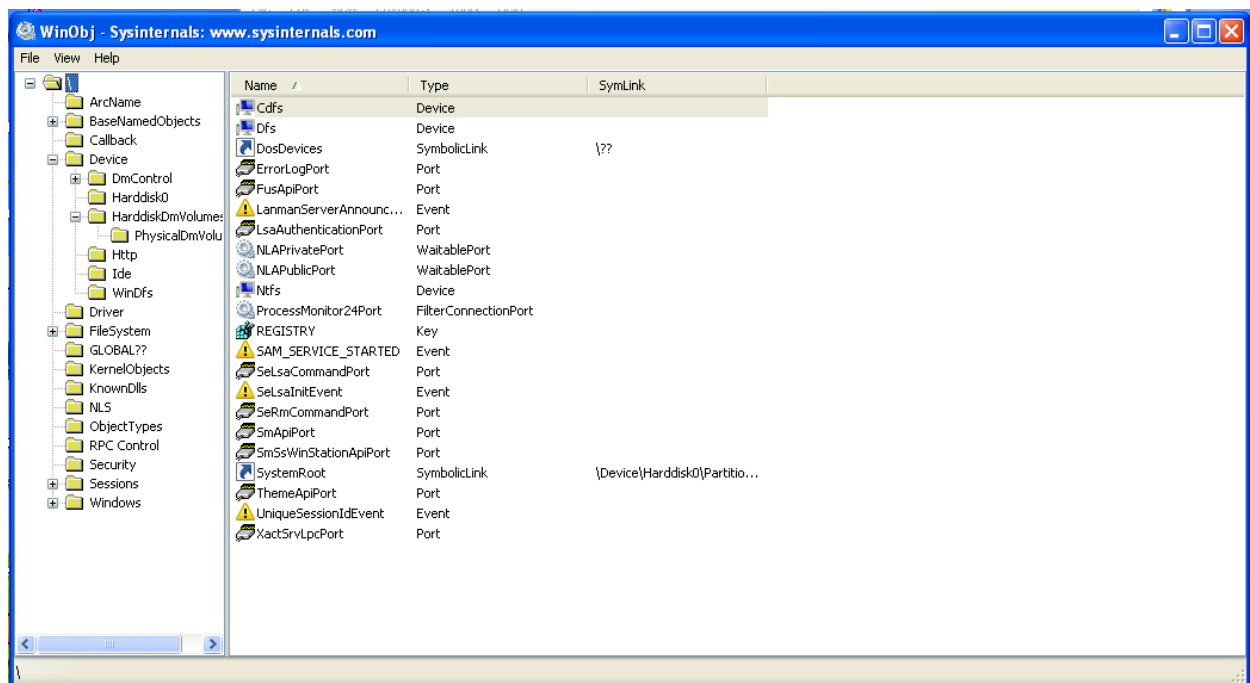


INTRODUCTION

WinObj is a must-have tool if you are a system administrator concerned about security, a developer tracking down object-related problems, or just curious about the Object Manager namespace.

WinObj is a 32-bit Windows NT program that uses the native Windows NT API (provided by NTDLL.DLL) to access and display information on the NT Object Manager's namespace. Winobj may seem similar to the Microsoft SDK's program of the same name, but the SDK version suffers from numerous significant bugs that prevent it from displaying accurate information (e.g. its handle and reference counting information are totally broken). In addition, our WinObj understands many more object types. Finally, Version 3.0 of our WinObj has user-interface enhancements (including a dark theme), knows how to open device objects, provides dynamic updates when objects are created/destroyed, and allows searching and filtering.

SCREENSHOT





INTRODUCTION

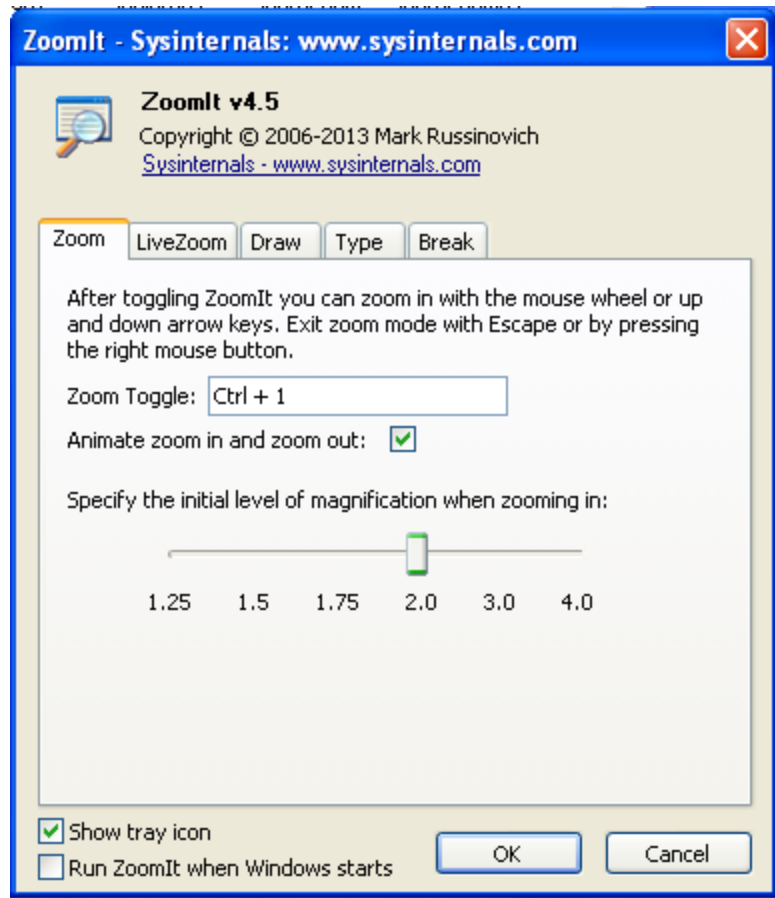
ZoomIt is a screen zoom and annotation tool for technical presentations that include application demonstrations. ZoomIt runs unobtrusively in the tray and activates with customizable hotkeys to zoom in on an area of the screen, move around while zoomed, and draw on the zoomed image. I wrote ZoomIt to fit my specific needs and use it in all my presentations.

ZoomIt works on all versions of Windows and you can use pen input for ZoomIt drawing on tablet PCs.

USAGE

The first time you run ZoomIt it presents a configuration dialog that describes ZoomIt's behaviour, lets you specify alternate hotkeys for zooming and for entering drawing mode without zooming, and customise the drawing pen colour and size. I use the draw-without-zoom option to annotate the screen at its native resolution, for example. ZoomIt also includes a break timer feature that remains active even when you tab away from the timer window and allows you to return to the timer window by clicking on the ZoomIt tray icon.

SCREENSHOT





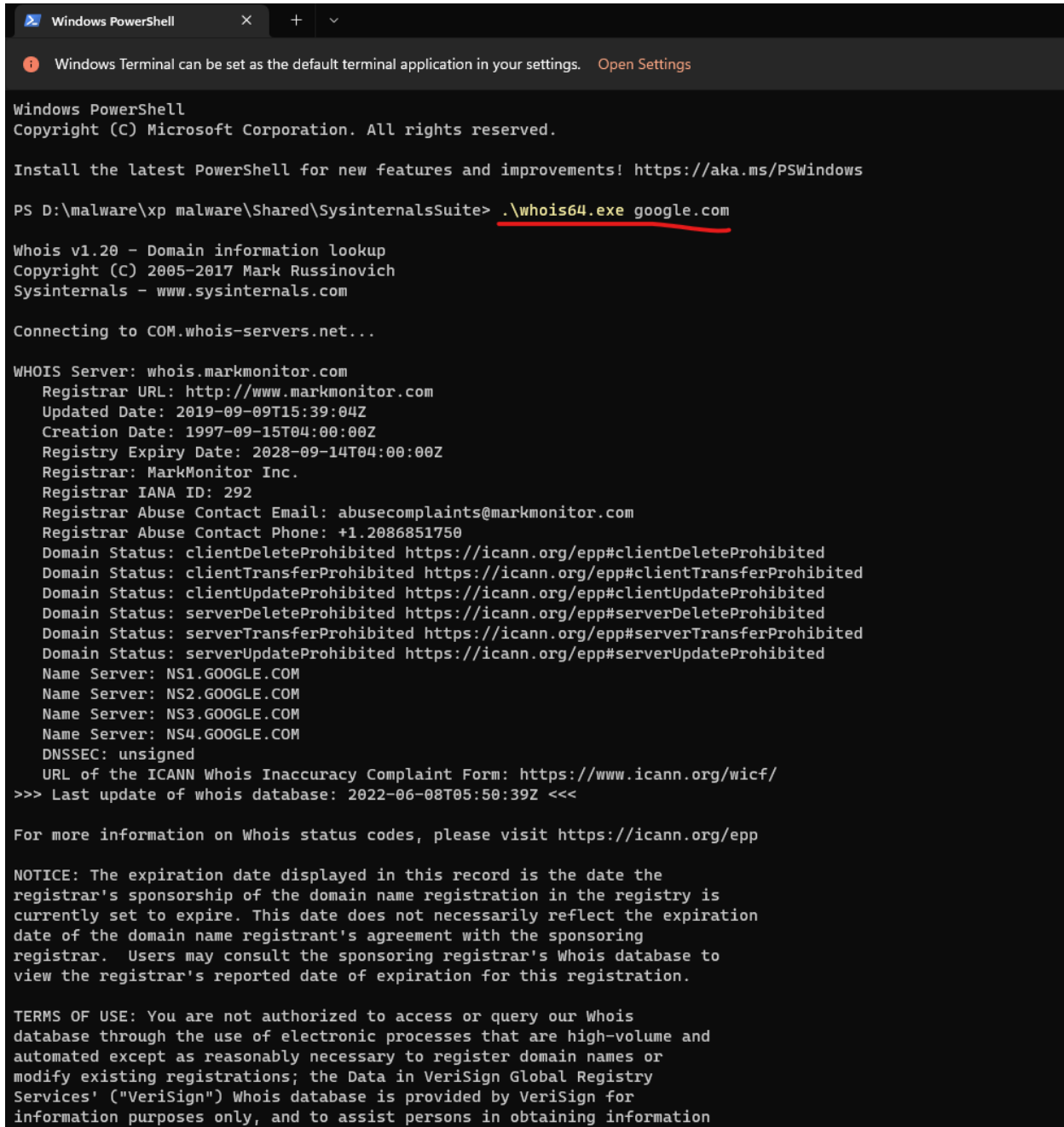
INTRODUCTION

Whois performs the registration record for the domain name or IP address that you specify.

USAGE

Usage: whois [-v] domainname [whois.server]

SCREENSHOT



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS D:\malware\xp malware\Shared\SysinternalsSuite> .\whois64.exe google.com

Whois v1.20 - Domain information lookup
Copyright (C) 2005-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to COM.whois-servers.net...

WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2028-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-06-08T05:50:39Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
```



DESKTOP

INTRODUCTION

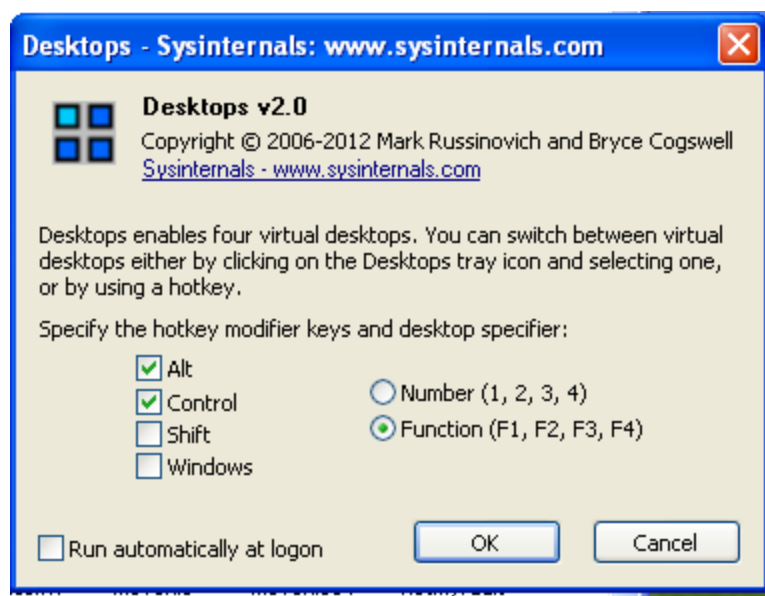
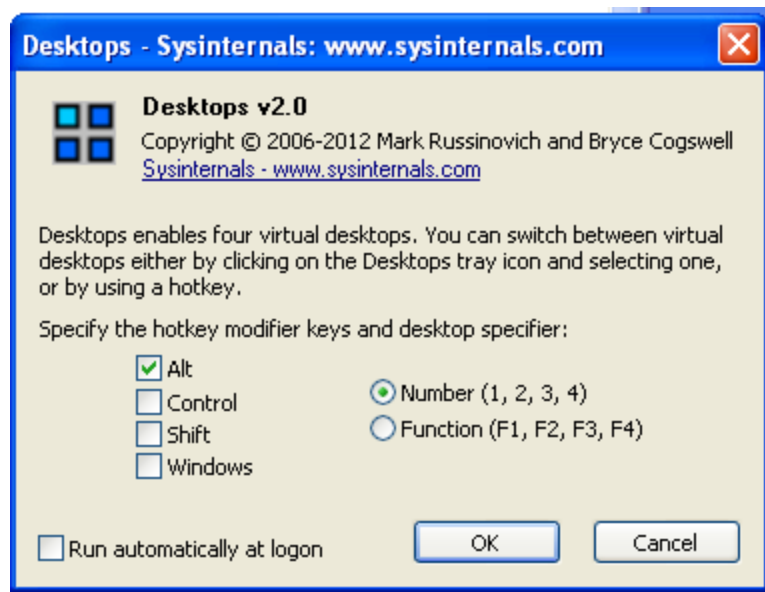
Desktops allows you to organise your applications on up to four virtual desktops. Read email on one, browse the web on the second, and do work in your productivity software on the third, without the clutter of the windows you're not using. After you configure hotkeys for switching desktops, you can create and switch desktops either by clicking on the tray icon to open a desktop preview and switching window, or by using the hotkeys.

USAGE

Unlike other virtual desktop utilities that implement their desktops by showing the windows that are active on a desktop and hiding the rest, Sysinternals Desktops uses a Windows desktop object for each desktop. Application windows are bound to a desktop object when they are created, so Windows maintains the connection between windows and desktops and knows which ones to show when you switch a desktop. That making Sysinternals Desktops very lightweight and free from bugs that the other approach is prone to where their view of active windows becomes inconsistent with the visible windows.

Desktop's reliance on Windows desktop objects means that it cannot provide some of the functionality of other virtual desktop utilities, however. For example, Windows doesn't provide a way to move a window from one desktop object to another, and because a separate Explorer process must run on each desktop to provide a taskbar and start menu, most tray applications are only visible on the first desktop. Further, there is no way to delete a desktop object, so Desktops does not provide a way to close a desktop, because that would result in orphaned windows and processes. The recommended way to exit Desktops is therefore to log off.

SCREENSHOT





THANK YOU