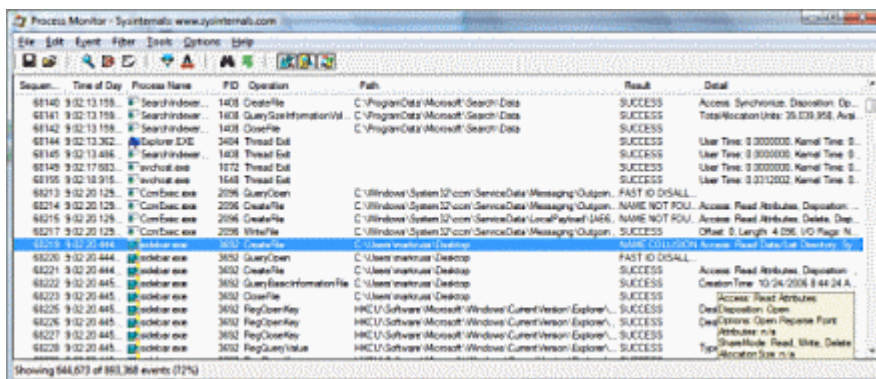


Process Monitor v3.40

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 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.



The screenshot shows the Process Monitor application window with a menu bar (File, Edit, Event Filter, Tools, Options, Help) and a toolbar. The main window displays a table of system events. The table has columns for Sequence, Time of Day, Process Name, PID, Operation, Path, Result, and Detail. The events listed include file operations like 'CreateFile', 'QuerySizeInformation', 'CloseFile', and 'Thread Exit' for processes like 'SearchIndexer.exe' and 'svchost.exe'. It also shows registry operations like 'QueryOpen', 'CreateFile', and 'WriteFile' for 'ConHost.exe'. The status bar at the bottom indicates 'Showing 644,677 of 883,368 events (72%)'.

Sequence	Time of Day	Process Name	PID	Operation	Path	Result	Detail
68140	9:02:13.158	SearchIndexer.exe	1408	CreateFile	C:\ProgramData\Microsoft\Search\Data	SUCCESS	Access: Synchronous, Disposition: Op...
68141	9:02:13.158	SearchIndexer.exe	1408	QuerySizeInformation	C:\ProgramData\Microsoft\Search\Data	SUCCESS	TotalAllocationUnits: 25,038,958, Avail...
68142	9:02:13.158	SearchIndexer.exe	1408	CloseFile	C:\ProgramData\Microsoft\Search\Data	SUCCESS	
68144	9:02:13.362	svchost.exe	3604	Thread Exit		SUCCESS	User Time: 0.0000000, Kernel Time: 0...
68145	9:02:13.406	SearchIndexer.exe	1408	Thread Exit		SUCCESS	User Time: 0.0000000, Kernel Time: 0...
68149	9:02:17.083	svchost.exe	1672	Thread Exit		SUCCESS	User Time: 0.0000000, Kernel Time: 0...
68155	9:02:18.915	svchost.exe	1648	Thread Exit		SUCCESS	User Time: 0.0010000, Kernel Time: 0...
68213	9:02:20.125	ConHost.exe	2096	QueryOpen	C:\Windows\System32\com\ServiceData\Messaging\Outgoing	FAST IO DISALL...	
68214	9:02:20.125	ConHost.exe	2096	CreateFile	C:\Windows\System32\com\ServiceData\Messaging\Outgoing	NAME NOT FOU...	Access: Read Attributes, Disposition...
68215	9:02:20.125	ConHost.exe	2096	CreateFile	C:\Windows\System32\com\ServiceData\LocalPayment\USER	NAME NOT FOU...	Access: Read Attributes, Delete, Disp...
68217	9:02:20.125	ConHost.exe	2096	WriteFile	C:\Windows\System32\com\ServiceData\Messaging\Outgoing	SUCCESS	Offset: 0, Length: 4,096, I/O Flags: N...
68219	9:02:20.914	svchost.exe	3652	CreateFile	C:\Users\markruss\Desktop	NAME COLLISION	Access: Read Data, List, Ownership, Sy...
68220	9:02:20.444	svchost.exe	3652	QueryOpen	C:\Users\markruss\Desktop	FAST IO DISALL...	
68221	9:02:20.444	svchost.exe	3652	CreateFile	C:\Users\markruss\Desktop	SUCCESS	Access: Read Attributes, Disposition...
68222	9:02:20.445	svchost.exe	3652	QueryBasicInformation	C:\Users\markruss\Desktop	SUCCESS	CreationTime: 10/24/2008 8:44:24 A...
68223	9:02:20.445	svchost.exe	3652	CloseFile	C:\Users\markruss\Desktop	SUCCESS	Access: Read Attributes
68225	9:02:20.445	svchost.exe	3652	RegOpenKey	HKEY\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	DealDisposition: Open
68226	9:02:20.445	svchost.exe	3652	RegOpenKey	HKEY\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	DealDisposition: Open
68227	9:02:20.445	svchost.exe	3652	RegOpenKey	HKEY\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	DealDisposition: Open
68228	9:02:20.445	svchost.exe	3652	RegQueryValue	HKEY\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	Attribute: n/a, ShareMode: Read, Write, Delete, Allocation Size: n/a

Download

<https://docs.microsoft.com/es-es/sysinternals/downloads/procm on>