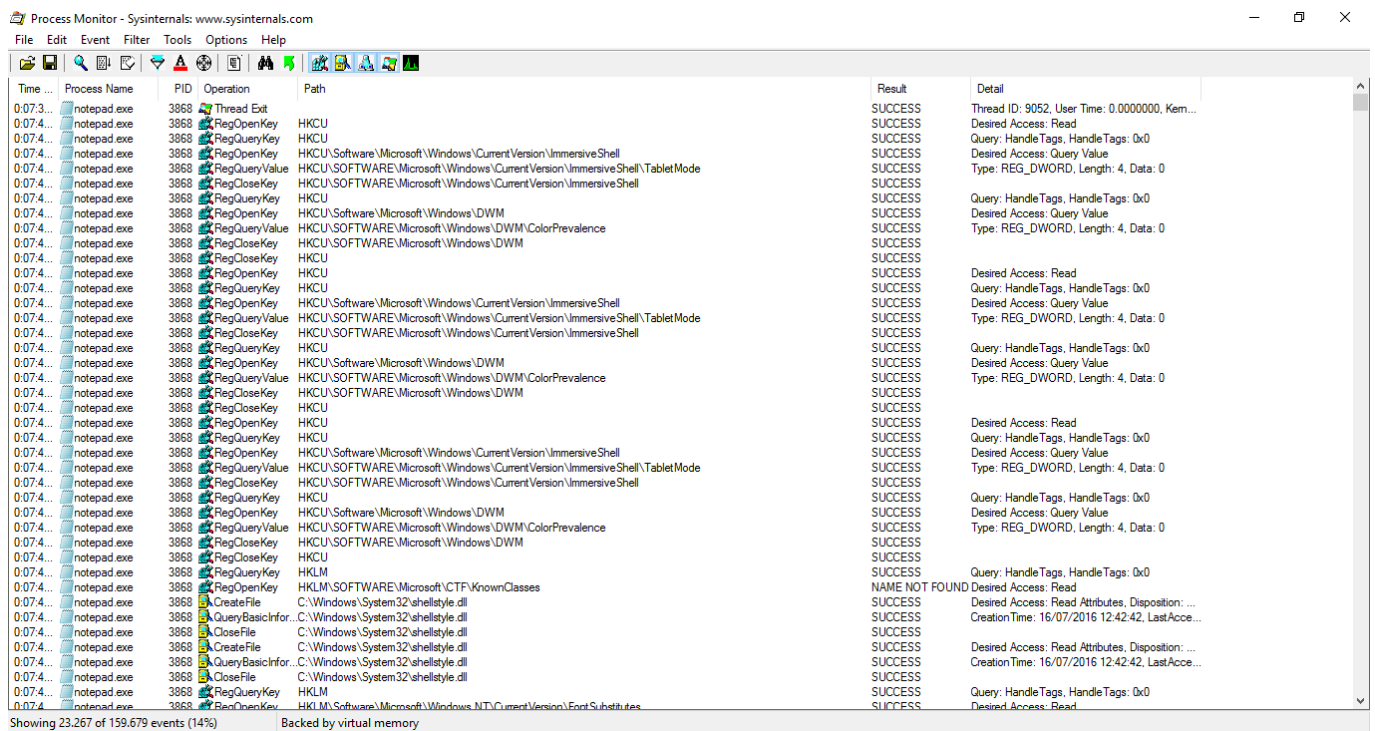


Process Monitor v3.32

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.



Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result	Detail
0:07.3...	notepad.exe	3868	Thread Exit		SUCCESS	Thread ID: 9052, User Time: 0.0000000, Kem...
0:07.4...	notepad.exe	3868	RegOpenKey	HKCU	SUCCESS	Desired Access: Read
0:07.4...	notepad.exe	3868	RegQueryValue	HKCU	SUCCESS	Query: HandleTags, HandleTags: 0x0
0:07.4...	notepad.exe	3868	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\ImmersiveShell	SUCCESS	Desired Access: Query Value
0:07.4...	notepad.exe	3868	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\ImmersiveShell\TabletMode	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
0:07.4...	notepad.exe	3868	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\ImmersiveShell	SUCCESS	
0:07.4...	notepad.exe	3868	RegQueryValue	HKCU	SUCCESS	Query: HandleTags, HandleTags: 0x0
0:07.4...	notepad.exe	3868	RegOpenKey	HKCU\Software\Microsoft\Windows\DWM	SUCCESS	Desired Access: Query Value
0:07.4...	notepad.exe	3868	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\DWM\ColorPrevalence	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
0:07.4...	notepad.exe	3868	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\DWM	SUCCESS	
0:07.4...	notepad.exe	3868	RegOpenKey	HKCU	SUCCESS	Desired Access: Read
0:07.4...	notepad.exe	3868	RegQueryValue	HKCU	SUCCESS	Query: HandleTags, HandleTags: 0x0
0:07.4...	notepad.exe	3868	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\ImmersiveShell	SUCCESS	Desired Access: Query Value
0:07.4...	notepad.exe	3868	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\ImmersiveShell\TabletMode	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
0:07.4...	notepad.exe	3868	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\ImmersiveShell	SUCCESS	
0:07.4...	notepad.exe	3868	RegQueryValue	HKCU	SUCCESS	Query: HandleTags, HandleTags: 0x0
0:07.4...	notepad.exe	3868	RegOpenKey	HKCU\Software\Microsoft\Windows\DWM	SUCCESS	Desired Access: Query Value
0:07.4...	notepad.exe	3868	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\DWM\ColorPrevalence	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
0:07.4...	notepad.exe	3868	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\DWM	SUCCESS	
0:07.4...	notepad.exe	3868	RegCloseKey	HKCU	SUCCESS	
0:07.4...	notepad.exe	3868	RegOpenKey	HKCU	SUCCESS	Desired Access: Read
0:07.4...	notepad.exe	3868	RegQueryValue	HKCU	SUCCESS	Query: HandleTags, HandleTags: 0x0
0:07.4...	notepad.exe	3868	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\ImmersiveShell	SUCCESS	Desired Access: Query Value
0:07.4...	notepad.exe	3868	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\ImmersiveShell\TabletMode	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
0:07.4...	notepad.exe	3868	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\ImmersiveShell	SUCCESS	
0:07.4...	notepad.exe	3868	RegOpenKey	HKCU	SUCCESS	Query: HandleTags, HandleTags: 0x0
0:07.4...	notepad.exe	3868	RegQueryValue	HKCU\Software\Microsoft\Windows\DWM	SUCCESS	Desired Access: Query Value
0:07.4...	notepad.exe	3868	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\DWM\ColorPrevalence	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
0:07.4...	notepad.exe	3868	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\DWM	SUCCESS	
0:07.4...	notepad.exe	3868	RegCloseKey	HKCU	SUCCESS	
0:07.4...	notepad.exe	3868	RegOpenKey	HKCU	SUCCESS	Desired Access: Read
0:07.4...	notepad.exe	3868	RegQueryValue	HKCU	SUCCESS	Query: HandleTags, HandleTags: 0x0
0:07.4...	notepad.exe	3868	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\ImmersiveShell	SUCCESS	Desired Access: Query Value
0:07.4...	notepad.exe	3868	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\ImmersiveShell\TabletMode	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
0:07.4...	notepad.exe	3868	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\ImmersiveShell	SUCCESS	
0:07.4...	notepad.exe	3868	RegOpenKey	HKCU	SUCCESS	Query: HandleTags, HandleTags: 0x0
0:07.4...	notepad.exe	3868	RegQueryValue	HKCU\Software\Microsoft\Windows\DWM	SUCCESS	Desired Access: Query Value
0:07.4...	notepad.exe	3868	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\DWM\ColorPrevalence	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
0:07.4...	notepad.exe	3868	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\DWM	SUCCESS	
0:07.4...	notepad.exe	3868	RegCloseKey	HKCU	SUCCESS	
0:07.4...	notepad.exe	3868	RegOpenKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
0:07.4...	notepad.exe	3868	RegOpenKey	HKLM\Software\Microsoft\CTF\KnownClasses	NAME NOT FOUND	Desired Access: Read
0:07.4...	notepad.exe	3868	CreateFile	C:\Windows\System32\shellstyle.dll	SUCCESS	Desired Access: Read Attributes, Disposition: ...
0:07.4...	notepad.exe	3868	QueryBasicInfor...	C:\Windows\System32\shellstyle.dll	SUCCESS	CreationTime: 16/07/2016 12:42:42, LastAcce...
0:07.4...	notepad.exe	3868	CloseFile	C:\Windows\System32\shellstyle.dll	SUCCESS	
0:07.4...	notepad.exe	3868	CreateFile	C:\Windows\System32\shellstyle.dll	SUCCESS	Desired Access: Read Attributes, Disposition: ...
0:07.4...	notepad.exe	3868	QueryBasicInfor...	C:\Windows\System32\shellstyle.dll	SUCCESS	CreationTime: 16/07/2016 12:42:42, LastAcce...
0:07.4...	notepad.exe	3868	CloseFile	C:\Windows\System32\shellstyle.dll	SUCCESS	
0:07.4...	notepad.exe	3868	RegQueryValue	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
0:07.4...	notepad.exe	3868	RegOpenKey	HKLM\Software\Microsoft\Windows\NT\CurrentVersion\FontSubstitutes	SUCCESS	Desired Access: Read

Showing 23,267 of 159,679 events (14%) Backed by virtual memory

For more information

<https://technet.microsoft.com/en-us/sysinternals/processmonitor.aspx>