Understanding Process Monitor

Version 3

Created by <u>Will Coffey</u> on Sep 20, 2016 3:12 PM. Last modified by <u>David Holland</u> on Nov 13, 2016 1:23 PM.

Overview

Process Monitor (procmon) is an advanced monitoring/logging utility that provides visibility into the who, what, when, where and how behind the events executed on the Windows OS. It's free and provided by Windows Sysinternals. With insight into what low-level operation a process is performing, the user privilege the operation is being executed under, when it occurred, how long it took and the result of the event, you'll find root causing a difficult issue much easier. A procmon capture will record real-time file system, registry, process/thread activity and minimal network operations. This tool requires administrative rights, including the Load and Unload Device Drivers privilege (assigned via Local Security Policy or Group Policy). This document will outline some of the features offered as well as a few tips and tricks I've found to be useful.

- ٠
- <u>Toolbar Options and Shortcuts</u>
- <u>Events Classes</u>
- <u>Capturing Events</u>
- Saving Captured Events
- <u>Customizing the Captured Events</u>
- Filtering and Highlighting
- <u>Filtering</u>
- <u>Highlighting</u>
- <u>Common Result Codes</u>
- Boot Logging
- <u>Tips and Tricks</u>
- <u>Troubleshooting with Process Monitor Video</u>

Toolbar Options and Shortcuts

🖙 🖬 | 💸 🕸 🙄 | 🗢 🔺 🌚 | 🗉 | 🚧 🦐 | 🔐 🛃 🚑 🌆

	Toolbar Options	and Shortcuts
	Save (ctrl + s)	Filter (ctrl + l) (ctrl + r) I = load r = reset
M	Open (ctrl + o)	Highlight (ctrl + h)
×	Capture (ctrl + e)	Show Process Tree (ctrl + t)
*	Autoscroll (ctrl + a)	Find (ctrl + f)
Ń	Clear (ctrl + x)	Jump to Object (ctrl + j)

Events Classes

Registry – This could be creating keys, reading them, deleting them, or querying them. You'll be surprised just how often this happens.

File System – This could be file creation, writing, deleting, etc, and it can be for both local hard drives and network drives.

Network – This will show the source and destination of TCP/UDP traffic. It doesn't show the data traffic.

Process and Thread – These are events for processes and threads where a process is started, a thread starts or exits, etc. This can be useful information in certain instances, but is often something you'd want to look at in Process Explorer instead.

Profiling – These events are captured by Process Monitor to check the amount of processor time used by each process, and the memory use. Again, you would probably want to use Process Explorer for tracking these things most of the time, but it's useful here if you need it.

Capturing Events

In order to analyze the actions of an event, you must first capture those events while procmon is running. To access.download procmon.exe, navigate to the following location:

SysInternalsTools

Procmon does not have to be downloaded to capture events, however, I recommend downloading it. Once you have access to promon, launch the application on the device to view the operations being performed. Here's an example of how a procmon trace looks:



As you can see, there's a lot of data collected and at first glance can be a bit overwhelming. Later we'll go over options we have to isolate the captured events.

Saving Captured Events

To save a capture you can select File | Save from the menu bar or use the ctrl+s keyboard shortcut.

The default trace file will be in a Native Process Monitor (PML) format.

Events to save:		
Events displayed using current filter		
Also include profiling events		
Format:		
Native Process Monitor Format (PML)		
O Comma-Separated Values (CSV)		
O Extensible Markup Language (XML)		
Indude stack traces (will increas	e file size)	
Resolve stack symbols (will be sl	ow)	
Path: C:\Users\Will Coffey\Downloads\Logfile	PML	

Customizing the Captured Events

The data captured is customizable in the sense of column order and font type. To adjust the order in which the columns appear simply drag them to your desired location. The below listed columns are included by default.

Columns:

- Time of Day this column is fairly self-explanatory; it shows the exact time that an event occurred
- **Process Name** the name of the process performing the operation along with an icon identifying the event class
- **PID** the process ID of the process that generated the event.
- **Operation** this is the name of the operation that is being logged, and there is an icon that matches up with one of the event types (registry, file, network, process).
- **Path** this is not the path of the process; it is the path to whatever was being worked on by this event. For instance, if there was a WriteFile event, this field will show the name of the file or folder being touched. If this was a registry event, it would show the full key being accessed.
- **Result** This shows the result of the operation, which codes like SUCCESS or ACCESS DENIED, NAME NOT FOUND, END OF FILE, BUFFER OVERFLOW etc. Buffer Over Flow: This occurs when a program copies more data into a memory buffer than the program was designed to accommodate. When looking at the Windows NTSTATUS result code, Status_Buffer_Overflow "The data was too large to fit into the specified buffer."

Don't confuse this with the malicious buffer_overflow in the sense of exploiting computer security. When contained in a procmon trace think of this result as "Buffer Too Small".

• **Detail** - additional information related to the operation of the event.

The below image (Process Monitor Column Selection) outlines all of the available column options. To include the additional column options, right-click on any column header and *select columns*. You will then be presented with the following interface allowing you to enable more items:

cess Monitor Column Se	lection	
elect columns to appear in t	ne Process Monitor w	indow
Application Details		
Process Name	Description	
🗹 Image Path	Version	
Command Line	Architecture	
Company Name		
Event Details		
Sequence Number	Path	
Event Class	Detail	
Operation	Result	
Date &Time	Relative Time	e
Time of Day	Duration	
Category	Completion T	īme
Process Management		
User Name	Process ID	
Session ID	Thread ID	
Authentication ID	Parent PID	
	Virtualized	
	OK Ca	ancel

Application Details - static info determined at process startup, this info won't change

Event Details - dynamic info specific to the event

Process Management – RunTime info about the process

Filtering and Highlighting

When performing a capture, a ton of events will be loaded in a relatively short period of time. In efforts to isolate the events and only show items you deem important, filtering and highlighting options can be specified. Filtering these events do not drop them from the capture, it simply removes them from the display. Highlighting works the same as filtering from a configuration standpoint but also adds a visual distinction to the selected events.

Filtering

To view the filter options you can select **Filter** | **Filter** from the menu or use the **ctrl**-I keyboard shortcut:

File Edit Event	Filter Tools Options Help	
🗃 🖬 🕴 💸 🛙	Enable Advanced Output	
Time Process Na	Filter	Ctrl+L
9:04:4 smss.exe 9:04:4	Reset Filter	Ctrl+R
9:04:4 Smss.exe	Load Filter	*
9:04:4 smss.exe	Save Filter	
9:04:4 smss.exe	Organize Filters	
9:04:4 Smss.exe 9:04:4 Smss.exe	Drop Filtered Events	
9:04:4 Smss.exe	Highlight	Ctrl+H

There are (4) configurable sections under *Display entries matching these conditions*:

Architecture	✓ is	-	∼ then Inc	lude 🗸
Reset			Add	emove
Column	Relation	Value	Action	^
🗹 🚱 Process	is	Procmon.exe	Exclude	
🗹 🔇 Process	is	Procexp.exe	Exclude	
🗹 🔇 Process	is	Autoruns.exe	Exclude	
🗹 🔇 Process	is	Procmon64.exe	Exclude	
🗹 🔇 Process	is	Procexp64.exe	Exclude	
🗹 🔇 Process	is	System	Exclude	
🗹 🔇 Operation	begins with	IRP_MJ_	Exclude	
🗹 🔇 Operation	begins with	FASTIO_	Exclude	
🗹 🔇 Result	begins with	FAST IO	Exclude	
🗹 🔇 Path	ends with	pagefile.sys	Exclude	
🗹 🔇 Path	ends with	\$Mft	Exclude	
🗹 🔇 Path	ends with	\$MftMirr	Exclude	
🛛 😢 Path	ends with	\$LogFile	Exclude	~

- The first field includes all of the available **columns**, the first entry in this list is *Architecture*. There are a total of (27) columns to choose from. Keep in mind that you can filter by these columns even if they are not enabled in the display.
- The second field has a list of **expressions** you can choose from. This list includes the following options:
- \circ ls
- o Is not
- \circ Less than
- \circ More than
- Begins with
- o Ends with
- Contains
- $_{\circ}$ Excludes
- The third field contains a "drop down" of objects for you to choose from. These are dependent on the column type you specified in the first field. In some cases, the drop down list will be blank. In this case you will need to type in the condition you wish to filter off of.
- The fourth field allows an Include/Exclude option for the conditions you configured. The specified condition has to be **included** if you want the filter to apply.

Highlighting

To view the highlight option you can select **Filter | Highlight** from the menu or use the **ctrl-h** keyboard shortcut:

File Edit Event Fi	ilter Tools Options	Help	Process Mon	itor Highlighting		
	Fachle Advanced O		Highlight entries r	matching these cond	litions:	
	Enable Advanced O	utput	Architecture	∽ is	~	
Time Process Na 9:04:4 • smss.exe 9:04:4 • smss.exe	Filter Reset Filter	Ctrl+L Ctrl+R	Reset			
9:04:4 • smss.exe 9:04:4 • smss.exe 9:04:4 • smss.exe 9:04:4 • smss.exe 9:04:4 • smss.exe 9:04:4 • smss.exe	Load Filter Save Filter Organize Filters Drop Filtered Events	• 5	Column	Relation	Value	
9:04:4 smss.exe 9:04:4 smss.exe	Highlight	Ctrl+H	Make Filter			<u>о</u> к
Process Monitor Highlight	ing	×				
Highlight entries matching these	conditions:					
Path \checkmark contain	ns 🗸 .sys	✓ then Include ✓				
Reset		Add Remove				
Column Relation Path contains	Value Ac .sys In	tion clude				
Make Filter	<u>O</u> K	<u>C</u> ancel Apply				

Preview

ОК

●FG ○BG

Cancel

Select

<u>A</u>dd <u>R</u>emove ction Cancel Apply

 \times

By default, the highlight color is bright blue, this can be modified by navigating to the menu and selecting **Options** | **Highlight Colors**.

9:29:0 A SearchIndexer	3260 🛃 ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 2,193,408, Lengtl
9:29:0 🔽 MsMpEng.exe	3276 🔜 ReadFile	C:\Program Files\Windows Defender\MpClient.dll	SUCCESS	Offset: 779,776, Length:
9:29:0 A SearchIndexer	3260 🗟 File System Contr	olC:	SUCCESS	Control: FSCTL READ
9:29:0 🖉 Search Indexer	3260 Sile SystemContr	olC:	SUCCESS	Control: FSCTL READ
9:29:0 MsMpEng.exe	3276 QueryEAFile	C:\Windows\System32\drivers\PROCMON23.SYS	NO EAS ON FILE	
9:29:0 📧 MsMpEng.exe	3276 🗟 Create File	C:\Windows\System32\drivers\PROCMON23.SYS	SUCCESS	Desired Access: Read A
9:29:0 T MsMpEng.exe	3276 🗟 QueryInformatio	C:\Windows\System32\drivers\PROCMON23.SYS	BUFFER OVERFL	VolumeCreationTime: 2/1
9:29:0 T MsMpEng.exe	3276 🗟 Query All Informa	C:\Windows\System32\drivers\PROCMON23.SYS	BUFFER OVERFL	Creation Time: 7/13/2010
9:29:0 🔳 MsMpEng.exe	3276 🗟 QueryInformatio	C:\Windows\System32\drivers\PROCMON23.SYS	BUFFER OVERFL	VolumeCreation Time: 2/1
9:29:0 🔳 MsMpEng.exe	3276 🗟 Query All Informa	C:\Windows\System32\drivers\PROCMON23.SYS	BUFFER OVERFL	Creation Time: 7/13/2010
9:29:0 📧 MsMpEng.exe	3276 🗟 Close File	C:\Windows\System32\drivers\PROCMON23.SYS	SUCCESS	
9:29:0 📧 MsMpEng.exe	3276 🗟 CloseFile	C:\Windows\System32\drivers\PROCMON23.SYS	SUCCESS	
9:29:0 📧 MsMpEng.exe	3276 🗟 Create File	C:\Windows\System32\drivers\PROCMON23.SYS	SUCCESS	Desired Access: Read A
9:29:0 📧 MsMpEng.exe	3276 🗟 Query Stream Inf.	C:\Windows\System32\drivers\PROCMON23.SYS	SUCCESS	
9:29:0 📧 MsMpEng.exe	3276 🗟 CloseFile	C:\Windows\System32\drivers\PROCMON23.SYS	SUCCESS	
9:29:0 📧 MsMpEng.exe	3276 🛃 File System Contr	olC:	SUCCESS	Control: FSCTL_QUERY
9:29:0 📧 MsMpEng.exe	3276 🗟 CreateFile	C:\Windows\System32\drivers\PROCMON23.SYS	SUCCESS	Desired Access: Read A
9:29:0 📧 MsMpEng.exe	3276 🗟 File System Contr	oIC:\Windows\System32\drivers\PROCMON23.SYS	SUCCESS	Control: FSCTL_READ_I
9:29:0 📧 MsMpEng.exe	3276 🔂 CloseFile	C:\Windows\System32\drivers\PROCMON23.SYS	SUCCESS	
9:29:0 📧 MsMpEng.exe	3276 🌋 RegClose Key	HKU\.DEFAULT	SUCCESS	
9:29:0 📧 MsMpEng.exe	3276 🧟 Thread Exit		SUCCESS	Thread ID: 8264, User Ti
9:29:0 📧 csrss.exe	1824 🛃 ReadFile	C:\Windows\System32\sxssrv.dll	SUCCESS	Offset: 31,232, Length: 1
			0100500	07 - 10 000 1 - 4 - 6
	Choose High			
	Color choices:			

Common Result Codes

The below listed table outlines the known results and their descriptions. Most of them are selfexplanatory but this will hopefully bring understanding to all of the results.

Result Code	Description
Success	The operation succeeded
Access Denied	The operation failed due to insufficient permissions from the requester.
	The operation failed because the object is already opened and doesn't
Sharing Violation	allow sharing mode
Name Collision	An attempt to create an object that already exist.
Name Not Found /	An attempt was made to open an object that doesn't exist was made.
Path Not Found / No	Routinely DLL files are compiled to search recursively or for specific
Such File	directories.
Name Invalid	A request was attempted for an object with an invalid name
No More Entries / No	The caller has finished enumerating the contents of a folder or registry
More Files	key
End of File	The caller has read to the end of a file
Buffer Too Small	Essentially the same as Buffer Overflow
	The caller has requested an object that links to another object. Ex:
D	HKLM/System/CurrentControlSet might redirect to
Re-parse	HKLM/System/ControlSet001
Not Re-parse Point	I ne requested object does not link to another object
EAST IO Dicallowod	Indicates a low-level optimized mechanism is not available for the
File Locked with	Indicates that a file or file mapping was locked and that all users of the
Only Readers	file can only read from it
File Locked with	Indicates that a file or file mapping was locked and that at least one
Writers	user of the file can write to it
File Locked with Only Readers Indicates that a file or file mapping was locked and that all users of th file can only read from it. File Locked with Writers Indicates that a file or file mapping was locked and that at least one user of the file can write to it. IS Directory The requested object is a file system folder Invalid Device Indicates that a file or file mapping was locked and that at least one	
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
Not Granted	A requested file lock cannot be granted because of other existing locks.
	An I/O request was cancelled – ex: the monitoring of a file system
Cancelled	folder for changes
Bad Network Path	The network pat cannot be located.
Bad Network Name	The specified share name cannot be found on the remote server
Media Write	
Protected	The disk cannot be written to because it's write protected
	Illegal operation attempted on a registry key that has been marked for
Key Deleted	deletion.
Not Implemented	The requested operation is not implemented

Boot Logging

Procmon is capable of motoring system activity when no one is logged on and after users have logged off. You are also able to capture events occurring during system shutdown. The following activity can be captured before, during or when no user has logged into the device:

- Boot-start device drivers
- Auto-start services
- Logon sequence

Boot logging does not run during safe mode. If the system crashes early in the boot process, logging can be deactivated by selecting the Last Known Good option from the Windows boot menu. To access this option press F8 during startup.

To enable Boot logging select **Options | Enable Boot Logging** can from the menu and select **OK**. Selecting Generate thread profiling events will provide more data to the boot log regarding the state of the applications running at during the capture.

Enable Boot Logging						
Process Monitor can generate thread profiling events that capture the state of all running applications at a regular interval.						
Generate thread profiling events						
• Every second						
○ Every 100 milliseconds						
OK Cancel						

When boot logging is enabled it's only for the next boot process. You must explicitly enable boot logging for each subsequent boot process. Once enabled, logging will continue until you launch procmon again and the captured activity will be contained in a PMB file in the following location:

%windir%\Procmon.pmb

Boot logging should only be enabled for troubleshooting purposes. The procmon.pmb file will continue to capture data until procmon.exe is re-ran.

Once boot logging is enabled you will be ready to capture events occurring during the boot process. After you log off and log back on to the device or restart the device and log back in, open procmon. An auto-detection will sense boot logging was enabled and the below listed prompt will appear:

Process Monitor x	
A log of boot-time activity was created by a previous instance of Process Monitor. Do you wish to save the collected data now?	
Yes No	

After selecting **Yes**, the boot time data will be converted into a PML file you can filter and use for troubleshooting.

Converting boot-time event data
19% - 0:42 remaining (10/10/2016 9:17:07 AM)
Cancel

Tips and Tricks

In order to effectively troubleshoot issues it's very beneficial to understand what the sequence of events look like when things are successful. Knowing the expected behavior and what process are involved as well as the processing order, will allow you to pinpoint the failure quicker. Sometime you may not want to focus too much on the error message you are being presented. As we all have come to realize, the root issue may be stemming from another underlying process or dll file. To have insight on the processes included and the order of operations during the life of a job you can capture the activity and review the process tree. This will show you the parent-child relationship of the running processes.

To view the process tree select **Tools | Process Tree** from the menu bar or use the **ctrl+t** keyboard shortcut.

	Description	image Path	Life Tine	Company	Owner	Corwand	Stat Time	End Time	
Ide 0:		He.		1000000			10/13/2016/8/45	n/a	
 Supera (d) 		Setters	_		NT AUTHORITY.		10/13/2016 2 49	1.1	
area ana (256)	Nedews Session		-	Mcroash Corporat.	NT AUTHORITYS.	SpatenRoat Spatien 32 areas and	10/13/2016 3 45	n/a	
MenConpression (3504)		MenConpresson			NT AUTHORITIN.		10/13/2015-8.49	. 6/8	
Carea ann (554)	Dert Sever Rurt.	Chill/hDOWSlay		Moreaft Corporat.	NT AUTHORITY'.	1.SystemPoot Visystem32/came are ObjectDirectory=VWindows SharedSection=1024.20480.708 Wind	10/13/2016 8 49	n/e	
Wining one (600)	Mindows Stat-Co.	C'INNDOWS'wy		Moreaft Corporat.	INT AUTHORITY'.	which and	10/13/2016 0.49.		
E Manufaces asia (700)	Sensoes and Cort.	C'INNDOWS're		Mcreart Copone	NT AUTHORITY.	C13WNDOWS water/32 venices exe	15/13/2016 8:45	. m/a	
10 sychost ever (\$24)	Host Process for	C.WINDOWS'ay		Monerft Corporat.	NT AUTHORITY.	C1/WNDOWS1aysten32/ovchost.exe & DoomLaunch	10/13/2016 8.49.	. m/a	
Winterverse and CB42	616 Provider Host	C-WINDOWS'er		Moreeft Corporat.	NT AUTHORITY.	C10W800W31apten321wben1wmpnee.exe	10/13/2016 8 49		
 Runtmettroker ava (703)8 	Runtime Boker	C:\Illindows\Syst		Moreaft Corporat.	CAPTAINAMERIC.	. C \Windows\System32-RuntmeBroker.exe Enbedding	10/13/2016 8.50.	n/a	
Shellipetenceilost esel	Nindows Shell Ex.	C-UNNDOWSIS		Monest Corporat	CAPTAINAMERIC.	"C:\WINDOWS' SystemApps' Shell ExperienceFloat, cw5n1h2byewy' ShellExperienceFloat.exs" -Server	10/13/2016 8:51	0.18	
EsearchUllace (5712)	Search and Cota	C'\Illedows\Syst		Monard Corporat.	CAPTANAMERIC.	. "C: \Wedove\SystexAppe\MoreeOf\WedoveCostana_cov5rlh2byevy\Search\Lese" -ServeName	10/13/2016 8.51	- 10/8	
Skypelfost.exe (7940)	Moosot Sope P.	C:/Pogan Resl.		Moneaft Corporat.	CAPTABLAMERIC.	. 'C:/Program Files/28Indows/apps/Monsoft.Skype/app_11.8.190.0_x64kc/Skpd28apSc/Skype/inst.ex.	10/13/2016 8:51	. 6/8	
ApplicationFrameHoat.ex/	Ipplication Frame .	C/WINDOWS ay		Mcreath Corporat.	CAPTAMAMERIC.	C \WNDOWS water 32 ApplicationFrameHost ever Embedding	10/13/2016 9 02	. n/a	
SystemSettings.exe (721)	Settings	C1877DOWS1am		Moneaft Corporat.	CAPTAPAMERE.	. "C: WIRECOWS' ImmensiveControl Panel' SystemSettings eve." - ServerName microsoft windows immensiv	10/13/2016 9-02	. 16/16	
SetzgSyncHost ave (42)	Host Process for	C\WNDOWSlag_		Mcroarit Corporat.	CAPTAMAMERIC.	C:\WNDOWS\aystee32\SettingSyncHist.exe Embedding	10/13/2016 9 12	. m/a	
Calynohmiconv exe (4390)		C1Program Files (-		CAPTARIAMERIC.	. "C: Program Files \$95? Moreant Office' Root Office 15 \ynchtmiconv ever" -Embedding	10/13/2016 9:12	0.2	
Lock/IppHost.exe (2284)	Lock/lepHeet	C \Illedows \Syst	-	Morearit Corporat.	CAPTAPAAMERIC.	. C/Windows/System32/Lock/aphilest evel Embedding	10/13/2016 10:0.	0.14	
DiHosteve (3568)	COM Sunogate	C'INNDOWS'wy		Moreaft Corporat.	CAPTAPAAMERIC.	C \WINDOWS wytee 32 Dillost eve /Processid SABS90284-09CA-4885-878D ABF59079A8D50	10/13/2016 10.5.	m/a	
amatacreen exe (5200)	SmatScreen	C \illindows \Syst		Microardt Corporat.	CAPTANAMERIC.	. C1/Windows/System32 americaneen.exx -Enbedding	10/13/2016 10-5	n/a	
(00Host eve (3076)	COM Surrogate	C:WINDOWSW		Morosoft Corporat.	NT AUTHORITY'.	C \WINDOWS water 32 Dilliost eve (Processid (E10F9C3A/FTAE-4ADC AASD 2FE65525666E)	10/13/2016 10 5.	10/13/2016 10.5.	
EleHost ave (\$800)	20H Surrogate	C\IIINDOWS'wy-		Morearit Carponat.	INT AUTHORITY'.	 CAWINDOWS'system32/DEHost are /Processed (E10F6C3A/F1AE-4ADC AASD-2/FE65525666E) 	10/13/2016 10.5.	10/13/2016 10.5.	
Winiprise and (4542)	ATE Provider Host	C'INNDOWS W.	1000	Moreaft Corporat.	NT AUTHORITY	C1WNDOWS'system32'wben'wmprise.exe -Enbedding	10/13/2016 10.5.	n/a	
sychest ans (1004)	Host Process for	C.WINDOWS m	1.00	Monard Corporat.	NT AUTHORITY'.	C\WINDOWS\ayatem32'unchoat.exe & RPCSS	10/13/2016.8.49.	in la	
Southest.eve (756)	Host Process for	C:\WNDOWS\5_		Moreart Corporat.	NT AUTHORITY'.	C1WINDOWS1System32'svohost.exe # NetworkService	10/13/2016 8.49.	. n/a	
E sychod ass (440)	Host Process for	C:WNDOWSing	-	Moreart Corporat	NT AUTHORITY	C:\WNDOWS\system32'ovchost.exe & LocalSystemNetwork/Restricted	10/13/2016 8.45	- cola	
WUDFHost.exe (1252)	Windows Driver F	C'\Illindows\Syst		Moreart Corporat.	NT AUTHORITY'.	. "C:\Windows\System32\WUDFHost.exe" HostGUID (193e1620d3ec-4997-8c55be817523/6aa) 4eE	10/13/2016 8:49.	. 0.2	
WUDFHoat.exe (1544)	Nindows Driver F	C \Illedows\Syst		Moneth Corporat.	NT AUTHORITYS.	. "C:\Wedows\System32\WUDFHost.exe" -HostGUID (190a1820-d3ac-4997-8c55-ball17529Haa) -IoE	10/13/2016.0.45	- mie	
ashost.exe (1872)	Device Associatio	C:\WINDOWS by_		Morosoft Corporat.	NT AUTHORITY	. dashost.exe (4c8d376c-28b4-44c8-85d2e8c91eda1724)	10/13/2016-8.49	. m/a	
WUDFHost axe (1964)	Nindows Driver F	C:\/IIIndows\Syst		Moreaft Corporat.	NT AUTHORITYS.	. "C: \Wedows\System12\WUDFHost exe" HostGUID (153s1820-d3sc-4997-3c55-bel17529Has) -IcE	10/13/2016-8-45	- m/a	
Li IIII Tab-Tax eve (7512)	Tauch Keyboard	C\Program Files\		Morseaft Corporat.	CAPTARIAMERIC.	. /Q.#Hr/s 000000000000000000000000000000000000	10/13/2016/0.51	- 0/8	
Tab Tp 32 even (7552)	Touch Keyboard	C:/Pogran Files [Moneaft Corporat.	CAPTABIAMERIC.	. Asadhaska /Parent 00000000001c58	10/13/2016/8:51	n/a	
TabTip ave (1512)	Fouch Keyboard	C\Pegan Res_		Morperft Corporat.	NT AUTHORITYL.	. /Q.XH/h: 00000000000E24.0000000000E2E	10/13/2016 10:5.	10/13/2016 10.5	
Weinhoet.min (370)	Nott Process for	CAMMDOWS'S		Moreart Carporat.	NT AUTHORITY.	C10WNDOWS1System32'sschoat.exe & LocalSensoeNetwork/Restricted	10/13/2016-0.49	- mia	
svchost.exe (432)	Holt Process for	C:WNDOWS'ay_		Moreart Corporat.	NT AUTHORITYL.	. C1/WINDOWS/aystem32/avcheat.exe ik LocalSenvice	10/13/2016-8.49	- n/a	
evchost.exe (1006)	Nost Procees for	C::III/NDOWS'ry		Moreaft Corporat.	NT AUTHORITYS.	C \WWDOWS wystem\22 anchost.exe + Local SeniceNetwork/Restricted	10/13/2016 8:45	n/a	
svchost.exe (1340)	Host Process for	C\WNDOWS\wy		Moneaft Carporat.	NT AUTHORITY'L	C \WINDOWS wystem 32 wysheat.exe & Local Senvice NoNetwork	10/13/2016 8.49.	- m/a	
avchost.exe (1352)	Host Process for	C:sWhDOWS'ry_		Moreatt Corporat.	NT AUTHORITY.	C13WNDOWS'upstein32'avohost.exe ik LocalSeniosAndNoimpersonation	10/13/2016 0.45	. m/a	
10 svchost.exe (1484) (*	Host Process for	C:///NDOWSiey_		Moreadit Corporat.	NT AUTHORITY.	. C/WINDOWS/ayatem32-ovchost.exe ik netavca	10/13/2016 8.49.	. n/a	
	Stell Intreductur	C-WINDOWS'ry	1.00	Moreart Corporat.	CAPTARIAMERIC	who there	10/13/2016 8.50.	. n/a	
Shost exe (2116)				Moreaft Corporat	CAPTAMAMERIC.	. laskhostiv isos (222A2458-EE37-4AE9-AS9F-A59CA119A75E)	10/13/2016/8:50.	- 1/4	

Another option I've found extremely helpful is the ability to filter by event classes.



The event classes have been covered above and toggling these options allows you to immediately filter out non-pertinent data.

Include Process from Windows. This is also referred to as a Bulls-eye. This feature allows you to drag and drop the Bulls-eye onto any application, automatically including it as a filtered event.

Troubleshooting with Process Monitor Video

The purpose of this video is to outline how you can use filtering in process monitor to isolate events for a more focused troubleshooting approach.

For additional information regarding uses for Procmon please reference the following articles: