

FINDING PRIVESC WITH PROCMON

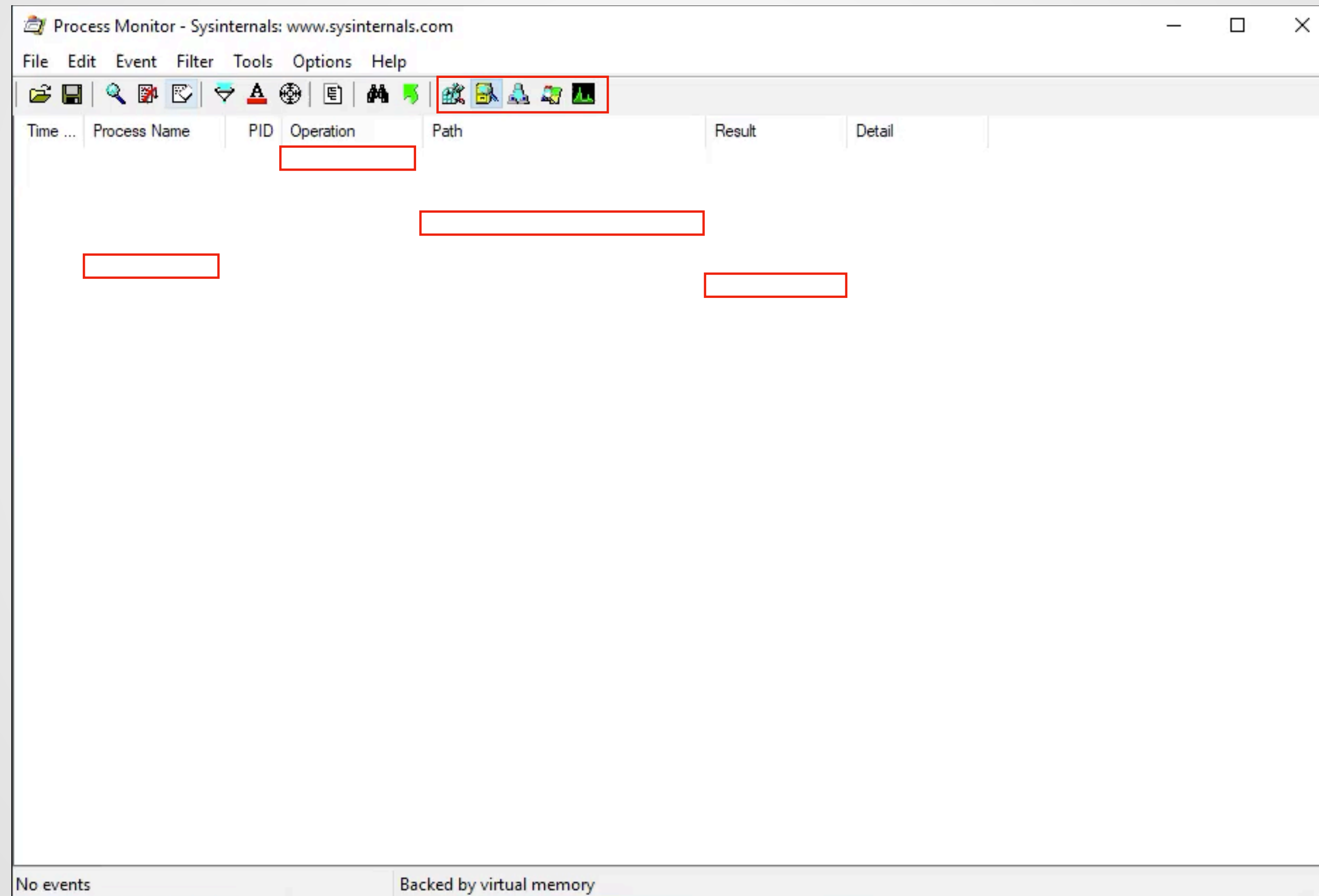
VETLE ØKLAND

::1

- Pentester @ Nagarro
- Live here in Oslo
- Too young to understand why Windows does anything
- Twitter: @bordplate
- Blog: <https://bordplate.no/blog/en>

What is Procmon?

PROCESS MONITOR



Event Properties

EventProcessStack

Frame	Module	Location	Addr
U 11	ntdll.dll	RtlDosSearchPath_Ustr + 0x641	0x7ff
U 12	ntdll.dll	RtlDosSearchPath_Ustr + 0x131	0x7ff
U 13	KERNELBASE.dll	SearchPathW + 0x148	0x7ff
U 14	USER32.dll	PrivateExtractIconsW + 0x143	0x7ff
U 15	SHELL32.dll	ExtractIconExW + 0x374	0x7ff
U 16	SHELL32.dll	SHDefExtractIconW + 0x200	0x7ff
U 17	SHELL32.dll	SHGetImageList + 0x267b	0x7ff
U 18	SHELL32.dll	SHDefExtractIconW + 0x1ce0	0x7ff
U 19	comctl32.dll	DSA_Create + 0x4b7	0x7ff
U 20	comctl32.dll	DSA_Create + 0x3d1	0x7ff
U 21	comctl32.dll	DPA_Sort + 0x1437	0x7ff
U 22	Explorer.EXE	Explorer.EXE + 0x2c969	0x7ff
U 23	Explorer.EXE	Explorer.EXE + 0x2c7c9	0x7ff
U 24	SHELL32.dll	SHGetSetSettings + 0xd79	0x7ff
U 25	SHELL32.dll	SHGetItemFromDataObject + 0x701	0x7ff
U 26	windows.storage.dll	ILLoadFromStreamEx + 0x88dc	0x7ff
U 27	windows.storage.dll	ILLoadFromStreamEx + 0x8595	0x7ff
U 28	windows.storage.dll	ILLoadFromStreamEx + 0x8475	0x7ff
U 29	shcore.dll	Ordinal246 + 0x1a6	0x7ff
U 30	ntdll.dll	TpSetPoolStackInformation + 0x195	0x7ff
U 31	ntdll.dll	RtlReleaseSRWLockExclusive + 0x694	0x7ff
U 32	KERNFI 32 DI I	BaseThreadInitThunk + 0x14	0x7ff

<

>

Properties...

Search...

Source...

Save...

↑

↓

☐ Next Highlighted

Copy All

Close

Boot Logging

- Consider disabling anti-virus scanning for smaller log files

What are we looking for?

9:28:0...	3720	CloseFile	C:\Program Files\	.Shim.dll	SUCCESS	
9:28:0...	3720	CreateFile	C:\OpenSSL\openssl.cnf		PATH NOT FOUND	Desired Access: G...
9:28:0...	3720	CreateFile	C:\OpenSSL\openssl.cnf		PATH NOT FOUND	Desired Access: G...
9:28:0...	3720	CreateFile	C:\Program Files\	Service.exe	SUCCESS	Desired Access: G...

2:09:2...	svchost.exe	2964	CreateFile	C:\Windows\System32\System Interrupts.DLL	NAME NOT FOUND	Desired Access: R...
2:09:2...	svchost.exe	2964	CreateFile	C:\Windows\System32\System Interrupts.DLL	NAME NOT FOUND	Desired Access: R...
2:09:2...	svchost.exe	2964	CreateFile	C:\Windows\System32\System Interrupts.DLL	NAME NOT FOUND	Desired Access: R...
2:09:2...	svchost.exe	2964	CreateFile	C:\Windows\System32\System Interrupts.DLL	NAME NOT FOUND	Desired Access: R...
2:09:2...	svchost.exe	2964	CreateFile	C:\Windows\System32\System.DLL	NAME NOT FOUND	Desired Access: R...
2:09:2...	svchost.exe	2964	CreateFile	C:\Windows\System32\System.DLL	NAME NOT FOUND	Desired Access: R...
2:09:2...	svchost.exe	2964	CreateFile	C:\Windows\System32\System.DLL	NAME NOT FOUND	Desired Access: R...
2:09:2...	svchost.exe	2964	CreateFile	C:\Windows\System32\System.DLL	NAME NOT FOUND	Desired Access: R...

Process Name	PID	Operation	Path	Result	Detail
svchost.exe	4184	CreateFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Desired Access: Read Attributes, Read Control, Write DAC, Write Owner
svchost.exe	4184	QueryBasicInformationFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	CreationTime: 1/18/2019 7:57:37 AM, LastAccessTime: 1/25/2019 6:4
svchost.exe	4184	QueryRemoteProtocolInformation	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	INVALID PARAMETER	
svchost.exe	4184	QuerySecurityFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Information: Owner, Group, DACL, SACL, Label, SACL Protected, DACL
svchost.exe	4184	QuerySecurityFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Information: SACL
svchost.exe	4184	SetSecurityFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Information: DACL, SACL, Label, SACL Protected, DACL Unprotected
svchost.exe	4184	CloseFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	
svchost.exe	4184	CreateFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Rep
svchost.exe	4184	QueryBasicInformationFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	CreationTime: 1/18/2019 7:57:37 AM, LastAccessTime: 1/25/2019 6:4
svchost.exe	4184	CloseFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	
svchost.exe	4184	CreateFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Desired Access: Read Control, Disposition: Open, Options: Sequential A
svchost.exe	4184	FileSystemControl	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Control: FSCTL_SET_COMPRESSION
svchost.exe	4184	QueryStandardInformationFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	AllocationSize: 73,728, EndOfFile: 71,680, NumberOfLinks: 2, DeletePe
svchost.exe	4184	QuerySecurityFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	BUFFER OVERFLOW	Information: DACL
svchost.exe	4184	QuerySecurityFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Information: DACL
svchost.exe	4184	CloseFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	
svchost.exe	4184	CreateFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Desired Access: Read Data/List Directory, Write Data/Add File, Read C
svchost.exe	4184	SetBasicInformationFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTime: -1, ChangeTime:
svchost.exe	4184	FileSystemControl	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Control: FSCTL_SET_COMPRESSION
svchost.exe	4184	QueryStandardInformationFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	AllocationSize: 73,728, EndOfFile: 71,680, NumberOfLinks: 2, DeletePe
svchost.exe	4184	QuerySizeInformationVolume	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	TotalAllocationUnits: 10,324,479, AvailableAllocationUnits: 5,850,797, S
svchost.exe	4184	QuerySecurityFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	BUFFER OVERFLOW	Information: DACL
svchost.exe	4184	QuerySecurityFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Information: DACL
svchost.exe	4184	FlushBuffersFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	
svchost.exe	4184	ReadFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Offset: 0, Length: 512, Priority: Normal
svchost.exe	4184	ReadFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Offset: 4,096, Length: 512
svchost.exe	4184	QueryBasicInformationFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	CreationTime: 1/18/2019 7:57:37 AM, LastAccessTime: 1/25/2019 6:4
svchost.exe	4184	SetBasicInformationFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	CreationTime: 1/18/2019 7:57:37 AM, LastAccessTime: 1/25/2019 6:4
svchost.exe	4184	CloseFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	
svchost.exe	4184	CreateFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Desired Access: Read Attributes, Delete, Disposition: Open, Options: N
svchost.exe	4184	QueryAttributeTagFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Attributes: AT, ReparseTag: 0x0
svchost.exe	4184	SetDispositionInformationFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Delete: True
svchost.exe	4184	CloseFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	
svchost.exe	4184	CreateFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Sequential
svchost.exe	4184	QueryEAFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	
svchost.exe	4184	QueryAttributeTagFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Attributes: A, ReparseTag: 0x0
svchost.exe	4184	QueryStandardInformationFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	AllocationSize: 8,192, EndOfFile: 8,192, NumberOfLinks: 3, DeletePend
svchost.exe	4184	QueryBasicInformationFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	CreationTime: 4/11/2018 3:34:39 PM, LastAccessTime: 1/25/2019 6:3
svchost.exe	4184	QueryStreamInformationFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	0:::\$DATA
svchost.exe	4184	QueryBasicInformationFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	CreationTime: 4/11/2018 3:34:39 PM, LastAccessTime: 1/25/2019 6:3
svchost.exe	4184	QueryEaInformationFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	EaSize: 0
svchost.exe	4184	CreateFile	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	Desired Access: Generic Read/Write, Delete, Write DAC, Disposition: C
svchost.exe	4184	QueryAttributeInformationVolume	C:\Users\testuser\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\Settings\settings.dat	SUCCESS	FileSystemAttributes: Case Preserved, Case Sensitive, Unicode, ACLs, C

Image from:
<https://krbtgt.pw/dacl-permissions-overwrite-privilege-escalation-cve-2019-0841/>
 DACL Permissions Overwrite Privilege Escalation (CVE-2019-0841)
 by Nabeel Ahmed

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
10:39:...	services.exe	604	CreateFile	C:\Custom	NAME NOT FOUND	Desired Access: R...
10:39:...	services.exe	604	CreateFile	C:\Custom.exe	NAME NOT FOUND	Desired Access: R...
10:39:...	services.exe	604	CreateFile	C:\Custom Services\Permission	NAME NOT FOUND	Desired Access: R...
10:39:...	services.exe	604	CreateFile	C:\Custom Services\Permission.exe	NAME NOT FOUND	Desired Access: R...
10:39:...	services.exe	604	CreateFile	C:\Custom Services\Permission Checker\perm	NAME NOT FOUND	Desired Access: R...
10:39:...	services.exe	604	CreateFile	C:\Custom Services\Permission Checker\perm.exe	NAME NOT FOUND	Desired Access: R...
10:39:...	services.exe	604	CreateFile	C:\Custom Services\Permission Checker\perm check.exe	SUCCESS	Desired Access: R...
10:39:...	services.exe	604	QueryBasicInfor...	C:\Custom Services\Permission Checker\perm check.exe	SUCCESS	CreationTime: 4/23...
10:39:...	services.exe	604	CloseFile	C:\Custom Services\Permission Checker\perm check.exe	SUCCESS	
10:39:...	services.exe	604	CreateFile	C:\Custom Services\Permission Checker\perm check.exe	SUCCESS	Desired Access: R...
10:39:...	services.exe	604	QueryBasicInfor...	C:\Custom Services\Permission Checker\perm check.exe	SUCCESS	CreationTime: 4/23...
10:39:...	services.exe	604	CloseFile	C:\Custom Services\Permission Checker\perm check.exe	SUCCESS	
10:39:...	services.exe	604	CreateFile	C:\Custom Services\Permission Checker\perm check.exe	SUCCESS	Desired Access: R...
10:39:...	services.exe	604	QueryEAFile	C:\Custom Services\Permission Checker\perm check.exe	SUCCESS	
10:39:...	MsMpEng.exe	2876	CreateFile Mapp...	C:\Custom Services\Permission Checker\perm check.exe	FILE LOCKED WI...	SyncType: SyncTy...
10:39:...	MsMpEng.exe	2876	QueryStandardI...	C:\Custom Services\Permission Checker\perm check.exe	SUCCESS	AllocationSize: 28,...
10:39:...	services.exe	604	CreateFile Mapp...	C:\Custom Services\Permission Checker\perm check.exe	FILE LOCKED WI...	SyncType: SyncTy...
10:39:...	services.exe	604	CreateFile Mapp...	C:\Custom Services\Permission Checker\perm check.exe	SUCCESS	SyncType: SyncTy...
10:39:...	services.exe	604	QueryNameInfo...	C:\Custom Services\Permission Checker\perm check.exe	SUCCESS	Name: \Custom Se...
10:39:...	MsMpEng.exe	2876	CreateFile	C:\Custom Services\Permission Checker\perm check.exe	SUCCESS	Desired Access: R...
10:39:...	MsMpEng.exe	2876	QueryInformatio...	C:\Custom Services\Permission Checker\perm check.exe	SUCCESS	VolumeCreationTim...
10:39:...	MsMpEng.exe	2876	QueryAllInfoma...	C:\Custom Services\Permission Checker\perm check.exe	BUFFER OVERFL...	CreationTime: 4/23...
10:39:...	MsMpEng.exe	2876	QueryInformatio...	C:\Custom Services\Permission Checker\perm check.exe	SUCCESS	VolumeCreationTim...
10:39:...	MsMpEng.exe	2876	QueryAllInfoma...	C:\Custom Services\Permission Checker\perm check.exe	BUFFER OVERFL...	CreationTime: 4/23...
10:39:...	MsMpEng.exe	2876	FileSystemControl	C:\Custom Services\Permission Checker\perm check.exe	SUCCESS	Control: FSCTL_R...
10:39:...	MsMpEng.exe	2876	CloseFile	C:\Custom Services\Permission Checker\perm check.exe	SUCCESS	
Showing 91 of 312,927 events (0.029%)			Backed by virtual memory			

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents	SUCCESS	Desired Access: Execute/T...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents\Important.rtf	SUCCESS	Desired Access: Generic R...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents\Important.rtf	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents\Important.rtf	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents\MAPI32.DLL	NAME NOT FOUND	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents	SUCCESS	Desired Access: Read Data...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents\Important.rtf	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents	IS DIRECTORY	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents	IS DIRECTORY	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents\Important.rtf	SUCCESS	Desired Access: Generic R...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents\Important.rtf	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents\Important.rtf	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents\Important.rtf	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents\Important.rtf	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents\Important.rtf	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents	SUCCESS	Desired Access: Read Data...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents\Important.rtf	SUCCESS	Desired Access: Generic R...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents\Important.rtf	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\Some Documents\Important.rtf	SUCCESS	Desired Access: Read Attrib...

Showing 29 of 87,146 events (0.033%)
Backed by virtual memory

Paths and Files

- PATH NOT FOUND
- NAME NOT FOUND

Both of these in a user-writable folder indicate you can influence the program.

Will vary based on file type and the program handling the files.

9:30:1...	CrashPlanService.exe	2704	ReadFile	C:\Program Files\CrashPlan\lib\log4j-slf4j-impl-2.1.jar	SUCCESS	Offset: 21,418, Len...
9:30:1...	CrashPlanService.exe	2704	ReadFile	C:\Program Files\CrashPlan\lib\log4j-slf4j-impl-2.1.jar	SUCCESS	Offset: 11,514, Len...
9:30:1...	CrashPlanService.exe	2704	ReadFile	C:\Program Files\CrashPlan\lib\log4j-slf4j-impl-2.1.jar	SUCCESS	Offset: 11,586, Len...
9:30:1...	CrashPlanService.exe	2704	CreateFile	C:\ProgramData\CrashPlan\lang\org\slf4j\ext\EventData.class	PATH NOT FOUND	Desired Access: R...
9:30:1...	CrashPlanService.exe	2704	CreateFile	C:\Program Files\CrashPlan\lang\org\slf4j\ext\EventData.class	PATH NOT FOUND	Desired Access: R...
9:30:1...	CrashPlanService.exe	2704	CreateFile	C:\Program Files\CrashPlan\org\slf4j\ext\EventData.class	PATH NOT FOUND	Desired Access: R...
9:30:1...	CrashPlanService.exe	2704	ReadFile	C:\Program Files\CrashPlan\lib\com.backup42.desktop.jar	SUCCESS	Offset: 7,372,053, ...
9:30:1...	CrashPlanService.exe	2704	CreateFile	C:\ProgramData\CrashPlan\lang\org\apache\logging\log4j\web\...	PATH NOT FOUND	Desired Access: R...

Image from a vulnerability found by Florian Bogner at bogner.sh:
<https://bogner.sh/2018/02/local-privilege-escalation-in-crashplans-windows-client/>

9:28:0...	3720	CloseFile	C:\Program Files\	.Shim.dll	SUCCESS	
9:28:0...	3720	CreateFile	C:\OpenSSL\openssl.cnf		PATH NOT FOUND	Desired Access: G...
9:28:0...	3720	CreateFile	C:\OpenSSL\openssl.cnf		PATH NOT FOUND	Desired Access: G...
9:28:0...	3720	CreateFile	C:\Program Files\	Service.exe	SUCCESS	Desired Access: G...

SetSecurityFile / Permission Overwrite

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
3:03:3...	TracSrvWrapp...	9180	SetSecurityFile	C:\Windows\Internet Logs\fwdbglog.txt	SUCCESS	Information: DACL
3:03:3...	TracSrvWrapp...	9180	SetSecurityFile	C:\Windows\Internet Logs\fwpktlog.txt	SUCCESS	Information: DACL
3:03:3...	TracSrvWrapp...	9180	SetSecurityFile	C:\Windows\Internet Logs\trDebug.log	SUCCESS	Information: DACL
3:03:3...	TracSrvWrapp...	9180	SetSecurityFile	C:\Windows\Internet Logs\user-created-file.txt	SUCCESS	Information: DACL

user-created-file Properties

General Security Details Previous Versions

Object name: C:\Windows\Internet Logs\user-created-file.txt

Group or user names:

Authenticated Users

To change permissions, click Edit.

Permissions for Authenticated Users

	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.

Advanced

Internet Logs

File Home Share View

Search Internet Logs

Name	Date modified	Type	Size
fwdbglog	2/15/2019 2:35 PM	Text Document	
fwpktlog	2/15/2019 2:35 PM	Text Document	
trDebug	4/22/2019 3:03 PM	Text Document	
user-created-file	4/22/2019 3:02 PM	Text Document	

CVE-2019-8452 – Permission Overwrite

Internet Logs Properties

General Sharing Security Previous Versions Customize

Object name: C:\Windows\Internet Logs

Group or user names:

Authenticated Users

To change permissions, click Edit.

Permissions for Authenticated Users

	Allow	Deny
Modify		
Read & execute		
List folder contents		
Read		
Write		
Special permissions	✓	

For special permissions or advanced settings, click Advanced.

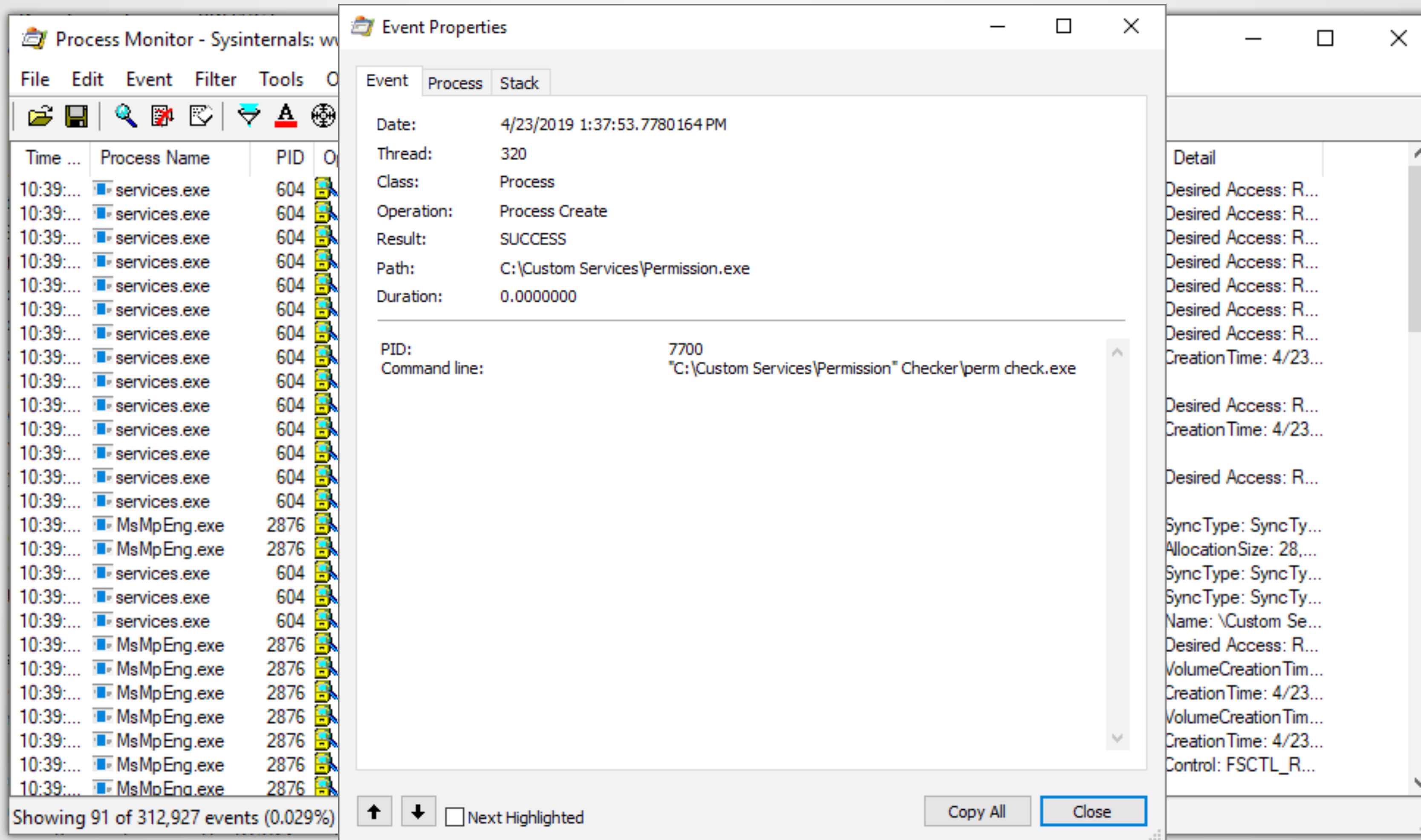
Advanced

OK Cancel Apply

Hard links to any file

- Courtesy of James Forshaw from Google's Project Zero
- Normal `mkLink` tool does not allow hard links to files you don't have write-access to
- `ZwSetInformationFile` does not enforce that check
 - `CreateHardLinkW` does however
- `Native-HardLink.ps1` from <https://github.com/FuzzySecurity/PowerShell-Suite/blob/master/Native-HardLink.ps1> by @fuzzysec (Ruben Boonen)

Unquoted service paths



DLL search order hijacking

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments	SUCCESS	Desired Access: Execute/T...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments\Important.rtf	SUCCESS	Desired Access: Generic R...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments\Important.rtf	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments\Important.rtf	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments\MAPI32.DLL	NAME NOT FOUND	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments	SUCCESS	Desired Access: Read Data...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments\Important.rtf	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments	IS DIRECTORY	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments	IS DIRECTORY	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments\Important.rtf	SUCCESS	Desired Access: Generic R...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments\Important.rtf	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments\Important.rtf	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments\Important.rtf	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments\Important.rtf	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments\Important.rtf	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments	SUCCESS	Desired Access: Read Data...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments\Important.rtf	SUCCESS	Desired Access: Generic R...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments\Important.rtf	SUCCESS	Desired Access: Read Attrib...
11:04:...	WORDPAD.EXE	5132	CreateFile	C:\SomeDocuments\Important.rtf	SUCCESS	Desired Access: Read Attrib...

Showing 29 of 87,146 events (0.033%) Backed by virtual memory

Configuration

- Need to have local admin

Useful filters

Process Monitor Filter

Display entries matching these conditions:

Event Class is then Exclude

Reset Add Remove

Column	Relation	Value	Action
<input checked="" type="checkbox"/> Result	is	PATH NOT FOUND	Include
<input checked="" type="checkbox"/> Result	is	NAME NOT FOUND	Include
<input checked="" type="checkbox"/> User	contains	SYSTEM	Include
<input checked="" type="checkbox"/> Path	begins with	C:\Windows	Exclude
<input checked="" type="checkbox"/> Path	begins with	C:\Program Files	Exclude
<input checked="" type="checkbox"/> Path	excludes	C:\	Exclude
<input checked="" type="checkbox"/> Path	begins with	C:\ProgramData\Microsoft\	Exclude

OK Cancel Apply

Process Monitor Filter

Display entries matching these conditions:

User contains SYSTEM then Include

Reset Add Remove

Column	Relation	Value	Action
<input checked="" type="checkbox"/> Result	is	NAME INVALID	Include
<input checked="" type="checkbox"/> User	contains	SYSTEM	Include

OK Cancel Apply

Process Monitor Filter

Display entries matching these conditions:

Operation is SetSecurityFile then Include

Reset Add Remove



















Column	Relation	Value	Action
<input checked="" type="checkbox"/> Operation	is	SetSecurityFile	Include
<input checked="" type="checkbox"/> User	contains	SYSTEM	Include

OK Cancel Apply

Exporting for other tools

- Exports to CSV and XML
 - Exporting for XML with stack traces can create *really* big files

Exploring in Procmon

										
Time ...	Process Name	PID	Operation	Path					Result	User
11:17:...	.exe	2448	 CreateFile	C:\ProgramData\	\	tools.conf			NAME NOT FOUND	NT AUTHORITY\SYSTEM
11:17:...	 Service...	2664	 CreateFile	C:\ProgramData\	\	msgCatalogs\messages\en_US...			PATH NOT FOUND	NT AUTHORITY\SYSTEM
11:17:...	 Service...	2664	 CreateFile	C:\ProgramData\	\	aliasStore\mapping.xml			NAME NOT FOUND	NT AUTHORITY\SYSTEM
11:17:...	 Service...	2664	 CreateFile	C:\Program%20Files\	\	%20	etc\catalog		PATH NOT FOUND	NT AUTHORITY\SYSTEM
11:17:...	 Service...	2664	 CreateFile	C:\Program%20Files\	\	%20	etc\catalog		PATH NOT FOUND	NT AUTHORITY\SYSTEM
11:17:...	 Service...	2664	 CreateFile	C:\Program%20Files\	\	%20	\	%20\sche...	PATH NOT FOUND	NT AUTHORITY\SYSTEM
11:17:...	 Service...	2664	 CreateFile	C:\Program%20Files\	\	%20	\	%20\sche...	PATH NOT FOUND	NT AUTHORITY\SYSTEM
11:17:...	 Service...	2664	 CreateFile	C:\Program%20Files\	\	%20	\	%20\sche...	PATH NOT FOUND	NT AUTHORITY\SYSTEM
11:17:...	 Service...	2664	 CreateFile	C:\Program%20Files\	\	%20	\	%20\sche...	PATH NOT FOUND	NT AUTHORITY\SYSTEM

```
C:\Windows\system32\cmd.exe
C:\Program%20Files\... %20 \etc\catalog>
```


Process Monitor Filter

Display entries matching these conditions:

Path

begins with

C:\Program%20Files

then

Include

Reset

Add





















Remove

Column	Relation	Value	Action
<input checked="" type="checkbox"/>	Process N...	is exe	Include
<input checked="" type="checkbox"/>	Path	begins with C:\Program%20Files	Include
<input checked="" type="checkbox"/>	Process N...	is Procmon.exe	Exclude
<input checked="" type="checkbox"/>	Process N...	is Procexp.exe	Exclude
<input checked="" type="checkbox"/>	Process N...	is Autoruns.exe	Exclude
<input checked="" type="checkbox"/>	Process N...	is Procmon64.exe	Exclude
<input checked="" type="checkbox"/>	Process N...	is Procexp64.exe	Exclude
<input checked="" type="checkbox"/>	Process N...	is System	Exclude
<input checked="" type="checkbox"/>	Operation	begins with IRP_MJ_	Exclude
<input checked="" type="checkbox"/>	Operation	begins with FASTIO_	Exclude
<input checked="" type="checkbox"/>	Result	begins with FAST IO	Exclude
<input checked="" type="checkbox"/>	Path	ends with pagefile.sys	Exclude
<input checked="" type="checkbox"/>	Path	ends with \$Mft	Exclude
<input checked="" type="checkbox"/>	Path	ends with \$MftMirr	Exclude
<input checked="" type="checkbox"/>	Path	ends with \$LogFile	Exclude
<input checked="" type="checkbox"/>	Path	ends with \$Volume	Exclude

OK

Cancel

Apply

Time ...	Process Name	PID	Operation	Path					Result	User
12:16:...	 Service...	2580	 CreateFile	C:\Program%20Files\	\	%20	\etc\catalog		SUCCESS	NT AUTHORITY\SYSTEM
12:16:...	 Service...	2580	 QueryInformationVolume	C:\Program%20Files\	\	%20	\etc\catalog		SUCCESS	NT AUTHORITY\SYSTEM
12:16:...	 Service...	2580	 QueryAllInformationFile	C:\Program%20Files\	\	%20	\etc\catalog		BUFFER OVERFL...	NT AUTHORITY\SYSTEM
12:16:...	 Service...	2580	 CloseFile	C:\Program%20Files\	\	%20	\etc\catalog		SUCCESS	NT AUTHORITY\SYSTEM
12:16:...	 Service...	2580	 CreateFile	C:\Program%20Files\	\	%20	\etc\catalog		IS DIRECTORY	NT AUTHORITY\SYSTEM
12:16:...	 Service...	2580	 CreateFile	C:\Program%20Files\	\	%20	\etc\catalog		IS DIRECTORY	NT AUTHORITY\SYSTEM
12:16:...	 Service...	2580	 CreateFile	C:\Program%20Files\	\	%20	\ %20V...		PATH NOT FOUND	NT AUTHORITY\SYSTEM
12:16:...	 Service...	2580	 CreateFile	C:\Program%20Files\	\	%20	\ %20V...		PATH NOT FOUND	NT AUTHORITY\SYSTEM
12:16:...	 Service...	2580	 CreateFile	C:\Program%20Files\	\	%20	\ %20V...		PATH NOT FOUND	NT AUTHORITY\SYSTEM
12:16:...	 Service...	2580	 CreateFile	C:\Program%20Files\	\	%20	\ %20V...		PATH NOT FOUND	NT AUTHORITY\SYSTEM

Event Properties

EventProcessStack

Frame	Module	Location	Address	Path
K 6	ntoskml.exe	ObOpenObjectByNameEx + 0x1bd9	0xffff80554e28ed9	C:\Windows\system32
K 7	ntoskml.exe	ObOpenObjectByNameEx + 0x1df	0xffff80554e274df	C:\Windows\system32
K 8	ntoskml.exe	NtCreateFile + 0x494	0xffff80554e9b8c4	C:\Windows\system32
K 9	ntoskml.exe	NtCreateFile + 0x79	0xffff80554e9b4a9	C:\Windows\system32
K 10	ntoskml.exe	setjmpex + 0x7805	0xffff805549d0085	C:\Windows\system32
U 11	ntdll.dll	NtCreateFile + 0x14	0x7ffa8b050204	C:\Windows\System32
U 12	KernelBase.dll	CreateFileW + 0x376	0x7ffa877ee5d6	C:\Windows\System32
U 13	KernelBase.dll	CreateFileW + 0x66	0x7ffa877ee2c6	C:\Windows\System32
U 14	ucrtbase.dll	initialize_narrow_environment + 0x1ff	0x7ffa87c6f05f	C:\Windows\System32
U 15	ucrtbase.dll	wsopen_s + 0x9d	0x7ffa87c7026d	C:\Windows\System32
U 16	ucrtbase.dll	wsopen_s + 0x2d	0x7ffa87c701fd	C:\Windows\System32
U 17	ucrtbase.dll	wfsopen + 0x12c	0x7ffa87c6783c	C:\Windows\System32
U 18	ucrtbase.dll	wfsopen + 0x7c	0x7ffa87c6778c	C:\Windows\System32
U 19	libxml2.dll	xmlFileOpen + 0x252	0x7ffa7d0d66b2	C:\Program Files\
U 20	libxml2.dll	xmlFileOpen + 0x12	0x7ffa7d0d6472	C:\Program Files\
U 21	libxml2.dll	xlLink.SetDefaultHandler + 0x96c	0x7ffa7d0d5a5c	C:\Program Files\
U 22	libxml2.dll	xmlParseCatalogFile + 0x6c	0x7ffa7d05a20c	C:\Program Files\
U 23	libxml2.dll	xmlParseCatalogFile + 0xc03	0x7ffa7d05ada3	C:\Program Files\
U 24	libxml2.dll	xmlConvertSGMLCatalog + 0x905	0x7ffa7d058f15	C:\Program Files\
U 25	libxml2.dll	xmlCatalogIsEmpty + 0x2cc	0x7ffa7d0573ac	C:\Program Files\
U 26	libxml2.dll	xmlACatalogResolve + 0xb9	0x7ffa7d056169	C:\Program Files\
U 27	libxml2.dll	xmlRegisterOutputCallbacks + 0xd6	0x7ffa7d0d85e6	C:\Program Files\
U 28	libxml2.dll	xlLink.SetDefaultHandler + 0x5e	0x7ffa7d0d514e	C:\Program Files\
U 29	libxml2.dll	xmlLoadExternalEntity + 0x9e	0x7ffa7d0d6e5e	C:\Program Files\
U 30	libxml2.dll	xmlCtxtReadFile + 0x4b	0x7ffa7d082edb	C:\Program Files\
U 31	libxml2.dll	xmlSaveTree + 0x2c7f	0x7ffa7d0f2bff	C:\Program Files\
U 32	libxml2.dll	xmlSchemaParse + 0x4df2	0x7ffa7d10b2a2	C:\Program Files\
U 33	libxml2.dll	xmlSchemaParse + 0x9176	0x7ffa7d10f626	C:\Program Files\
U 34	libxml2.dll	xmlSchemaParse + 0x7c28	0x7ffa7d10e0d8	C:\Program Files\
U 35	libxml2.dll	xmlSchemaParse + 0x1ba	0x7ffa7d10666a	C:\Program Files\
U 36	.exe	.exe + 0x10829	0x7ff750540829	C:\Program Files\
U 37	.exe	.exe + 0x10a1b	0x7ff750540a1b	C:\Program Files\
U 38	.exe	.exe + 0x1fd8	0x7ff750531fd8	C:\Program Files\
U 39	kemsel32.dll	BaseThreadInitThunk + 0x14	0x7ffa89957974	C:\Windows\System32
U 40	ntdll.dll	RtlUserThreadStart + 0x21	0x7ffa8b01a271	C:\Windows\System32

Properties...

Search...

Source...

Save...

↑

↓

☐ Next Highlighted

Copy All

Close

Task Scheduler

File Action View Help

Task Scheduler (Local)

Task Scheduler Library

Name	Status	Triggers
OneDrive St...	Ready	At 10:00 AM on 5/1/1992 - After triggered, rep

Actions

Task Scheduler Library

- Create Basic Task...
- Create Task...
- Import Task...
- Display All Running Tasks
- Enable All Tasks History
- New Folder...
- View
- Refresh
- Help

test

File Home Share View

This PC > Local Disk (C:) > Users > test

Search test

Name	Date modified	Type	Size
3D Objects	5/22/2019 10:25 AM	File folder	
Contacts	5/22/2019 10:25 AM	File folder	
Desktop	5/22/2019 10:25 AM	File folder	
Documents	5/22/2019 10:33 AM	File folder	
Downloads	5/22/2019 10:25 AM	File folder	
Favorites	5/22/2019 10:25 AM	File folder	
Links	5/22/2019 10:25 AM	File folder	
Music	5/22/2019 10:25 AM	File folder	
OneDrive	5/22/2019 10:30 AM	File folder	
Pictures	5/22/2019 10:28 AM	File folder	
Saved Games	5/22/2019 10:25 AM	File folder	
Searches	5/22/2019 10:25 AM	File folder	
Videos	5/22/2019 10:25 AM	File folder	

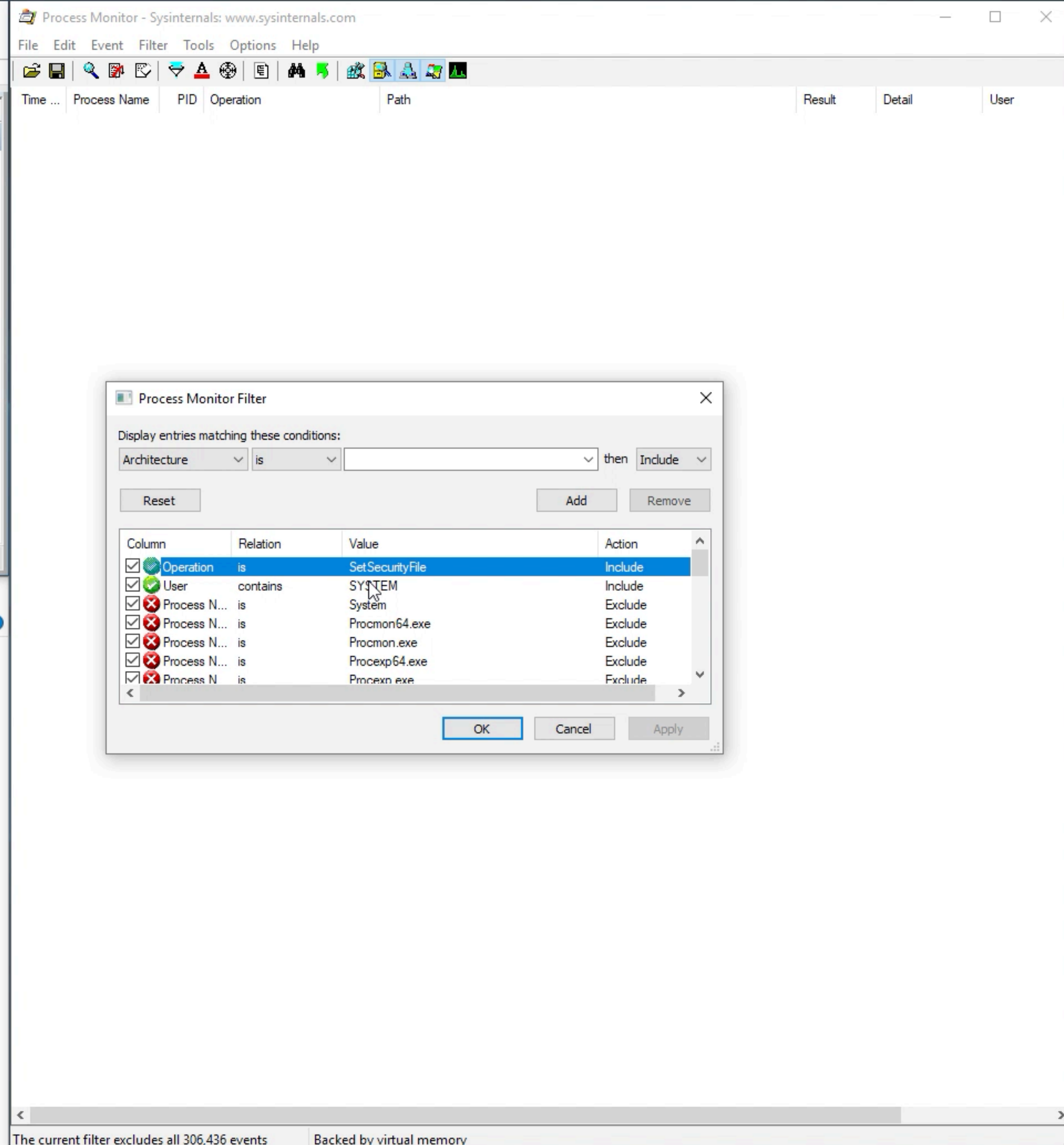
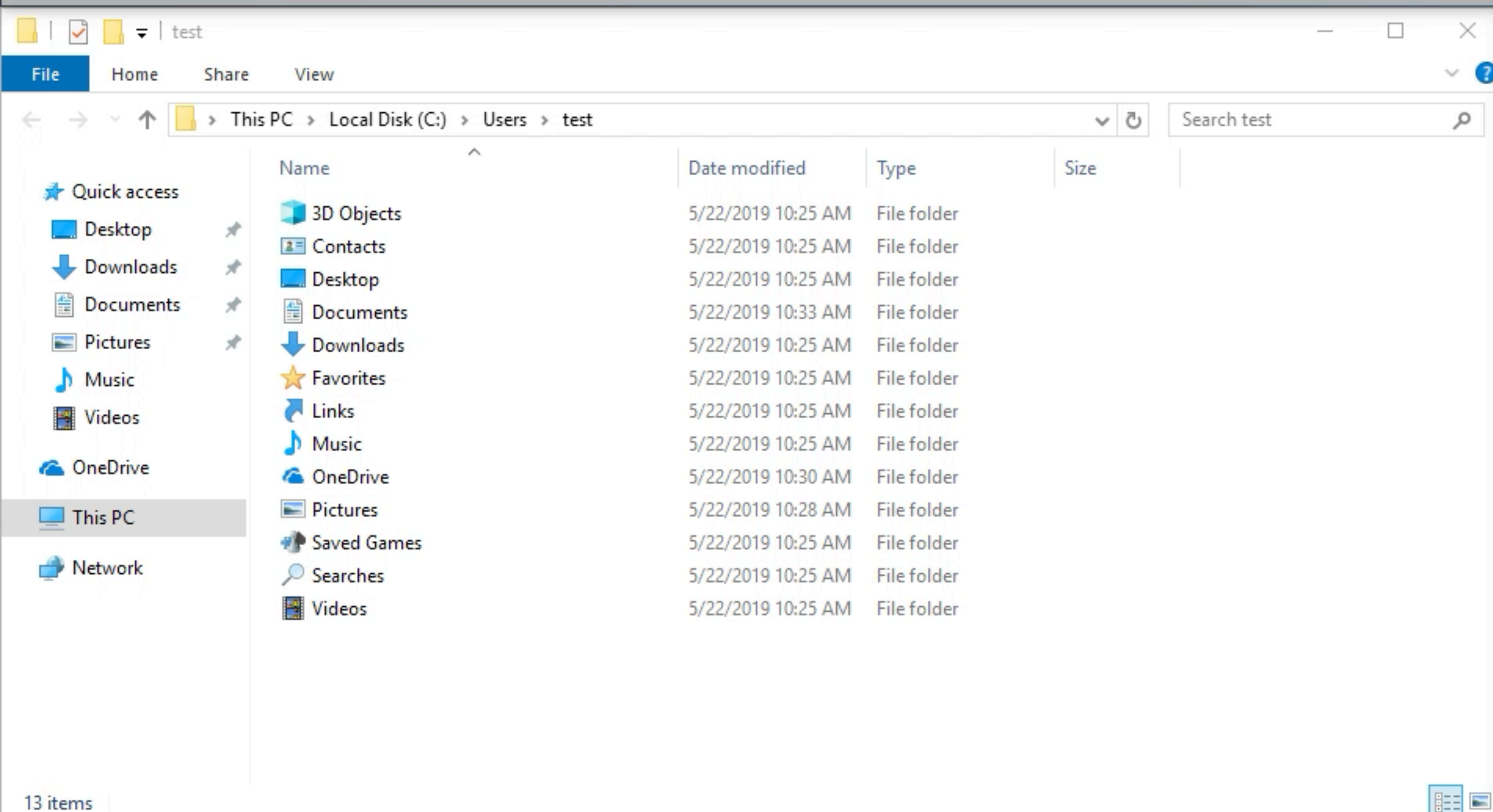
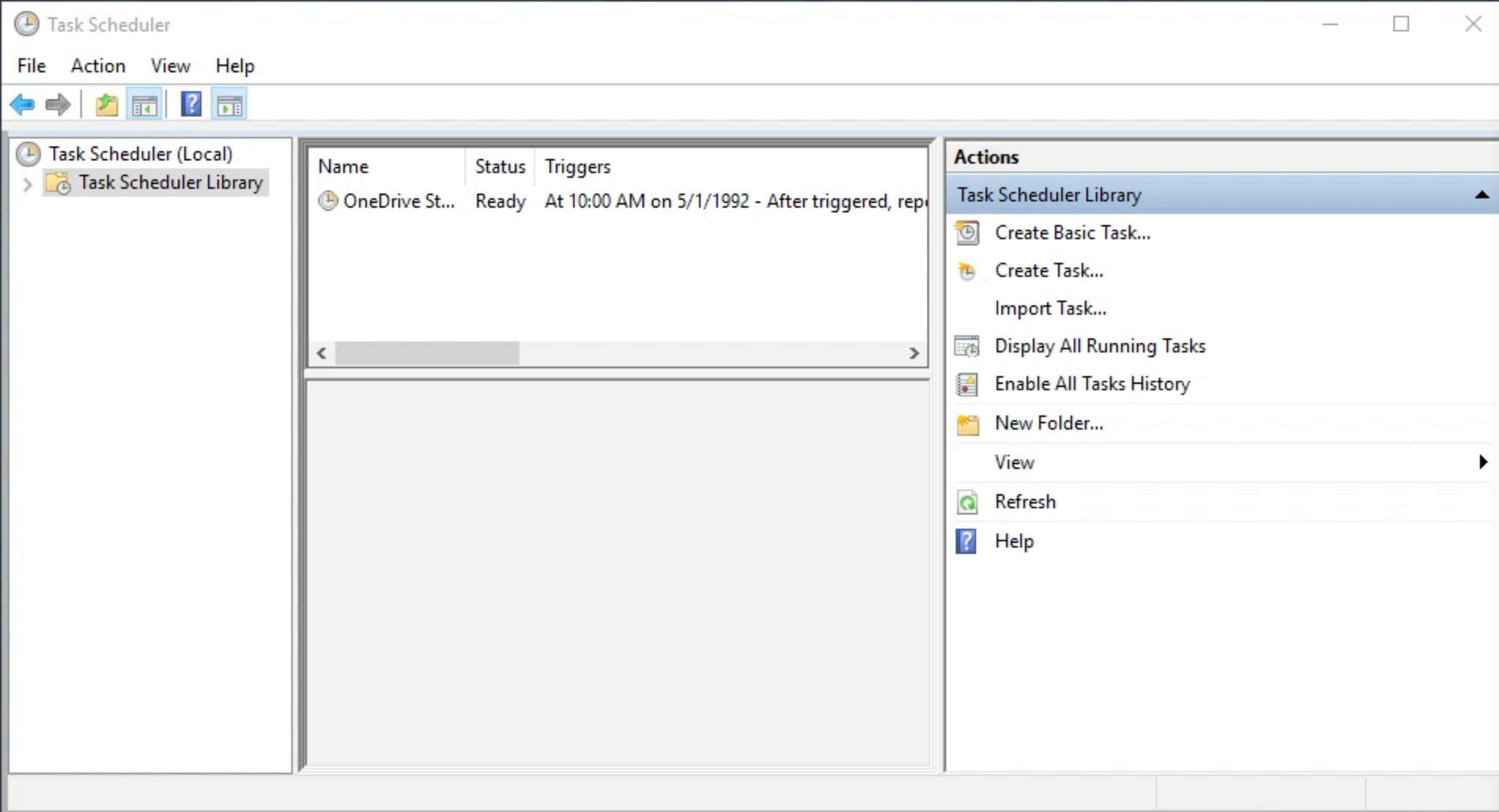
13 items

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail	User
----------	--------------	-----	-----------	------	--------	--------	------

The current filter excludes all 228,857 events Backed by virtual memory



Task Scheduler

File Action View Help

Task Scheduler (Local)

Task Scheduler Library

Name	Status	Triggers
OneDrive St...	Ready	At 10:00 AM on 5/1/1992 - After triggered, rep
Testing	Ready	

General Triggers Actions Conditions Settings History (disabled)

Name: Testing

Location: \

Author: DESKTOP-O3SRU5F\test

Description:

Security options

Actions

Task Scheduler Library

- Create Basic Task...
- Create Task...
- Import Task...
- Display All Running Tasks
- Enable All Tasks History
- New Folder...
- View
- Refresh
- Help

Selected Item

- Run
- End
- Disable
- Export...

test

File Home Share View

This PC > Local Disk (C:) > Users > test

Name	Date modified	Type	Size
3D Objects	5/22/2019 10:25 AM	File folder	
Contacts	5/22/2019 10:25 AM	File folder	
Desktop	5/22/2019 10:25 AM	File folder	
Documents	5/22/2019 10:33 AM	File folder	
Downloads	5/22/2019 10:25 AM	File folder	
Favorites	5/22/2019 10:25 AM	File folder	
Links	5/22/2019 10:25 AM	File folder	
Music	5/22/2019 10:25 AM	File folder	
OneDrive	5/22/2019 10:30 AM	File folder	
Pictures	5/22/2019 10:28 AM	File folder	
Saved Games	5/22/2019 10:25 AM	File folder	
Searches	5/22/2019 10:25 AM	File folder	
Videos	5/22/2019 10:25 AM	File folder	

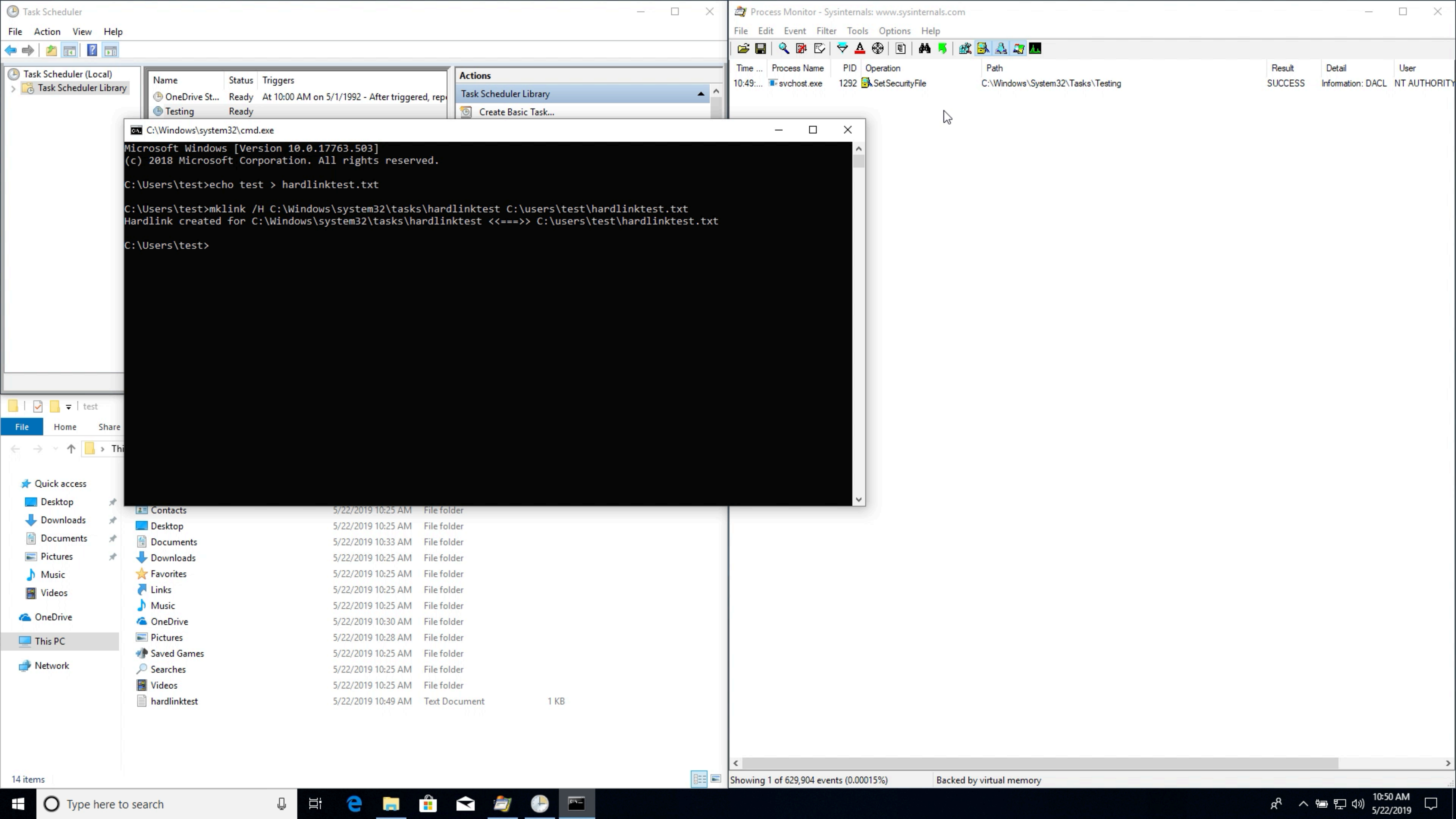
13 items

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail	User
10:49:...	svchost.exe	1292	SetSecurityFile	C:\Windows\System32\Tasks\Testing	SUCCESS	Information: DACL	NT AUTHORITY

Showing 1 of 483,275 events (0.00020%) Backed by virtual memory



Task Scheduler

File Action View Help

Task Scheduler (Local)

Task Scheduler Library

Name	Status	Triggers
OneDrive St...	Ready	At 10:00 AM on 5/1/1992 - After triggered, rep
Testing	Ready	

Actions

Task Scheduler Library

Create Basic Task...

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail	User
10:49:...	svchost.exe	1292	SetSecurityFile	C:\Windows\System32\Tasks\Testing	SUCCESS	Information: DACL	NT AUTHORITY

C:\Windows\system32\cmd.exe

Microsoft Windows [Version 10.0.17763.503]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\test>echo test > hardlinktest.txt

C:\Users\test>mklink /H C:\Windows\system32\tasks\hardlinktest C:\users\test\hardlinktest.txt

Hardlink created for C:\Windows\system32\tasks\hardlinktest <==> C:\users\test\hardlinktest.txt

C:\Users\test>

test

File Home Share

Quick access

Desktop

Downloads

Documents

Pictures

Music

Videos

OneDrive

This PC

Network

Contacts	5/22/2019 10:25 AM	File folder
Desktop	5/22/2019 10:25 AM	File folder
Documents	5/22/2019 10:33 AM	File folder
Downloads	5/22/2019 10:25 AM	File folder
Favorites	5/22/2019 10:25 AM	File folder
Links	5/22/2019 10:25 AM	File folder
Music	5/22/2019 10:25 AM	File folder
OneDrive	5/22/2019 10:30 AM	File folder
Pictures	5/22/2019 10:28 AM	File folder
Saved Games	5/22/2019 10:25 AM	File folder
Searches	5/22/2019 10:25 AM	File folder
Videos	5/22/2019 10:25 AM	File folder
hardlinktest	5/22/2019 10:49 AM	Text Document 1 KB

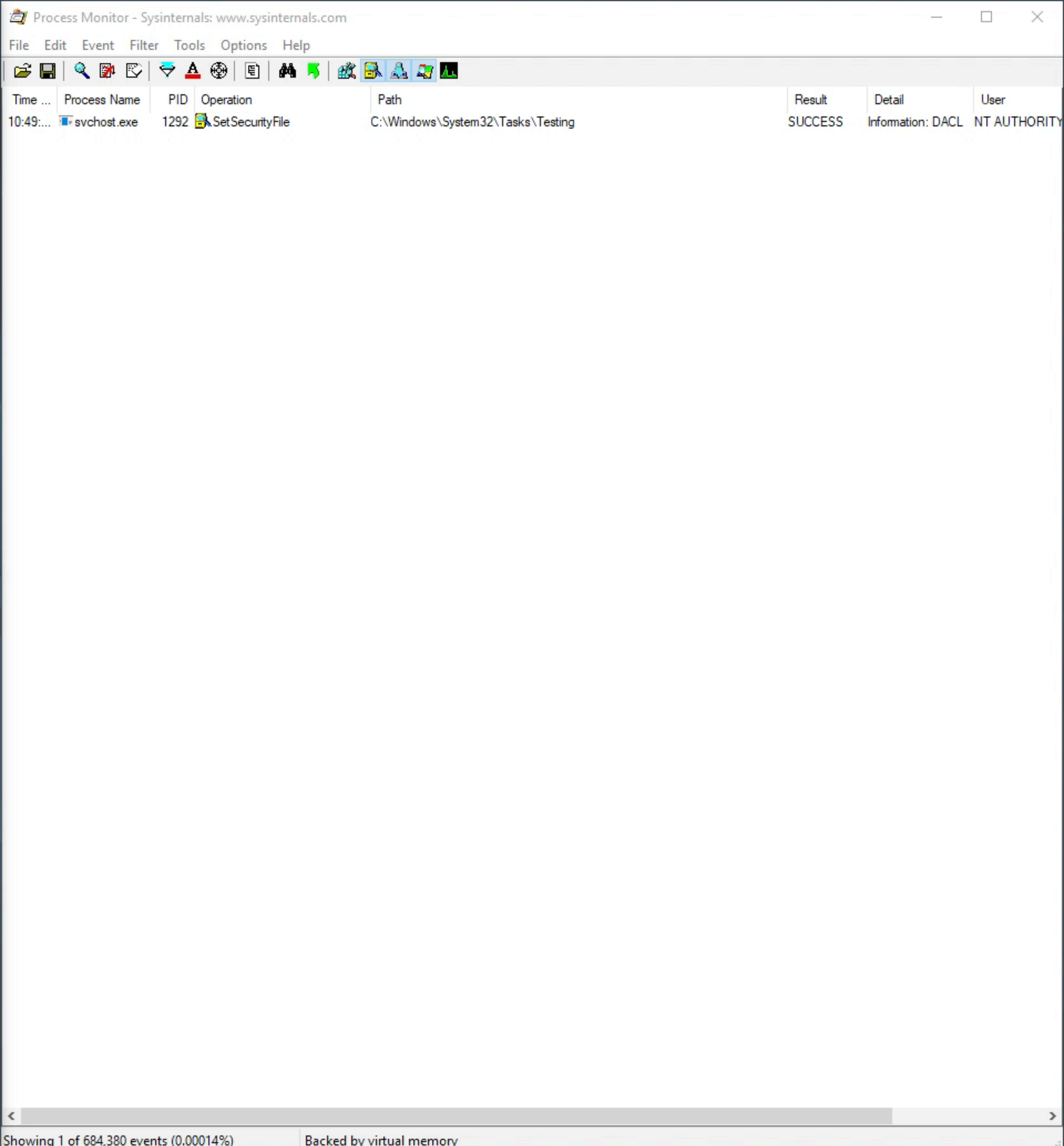
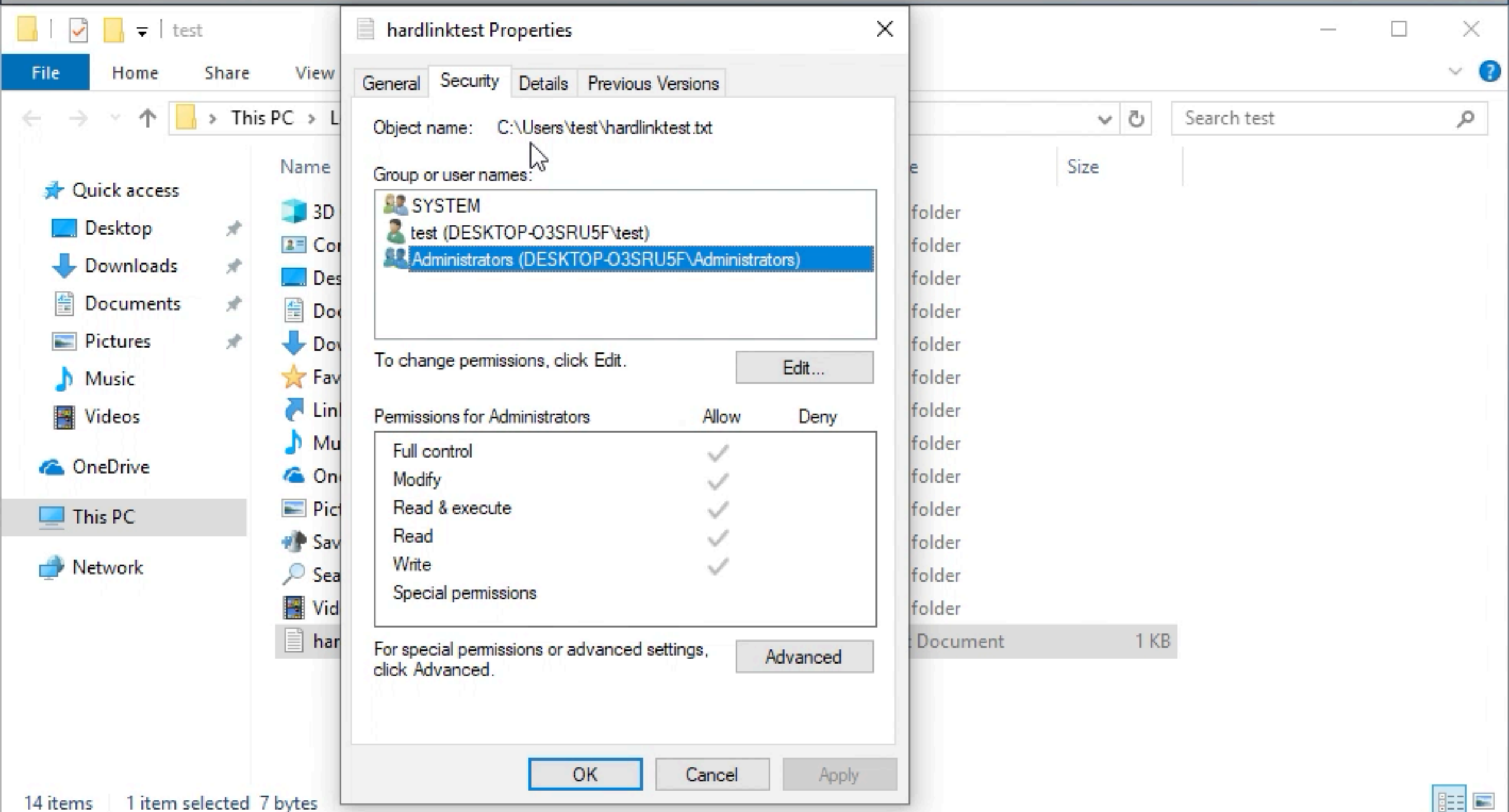
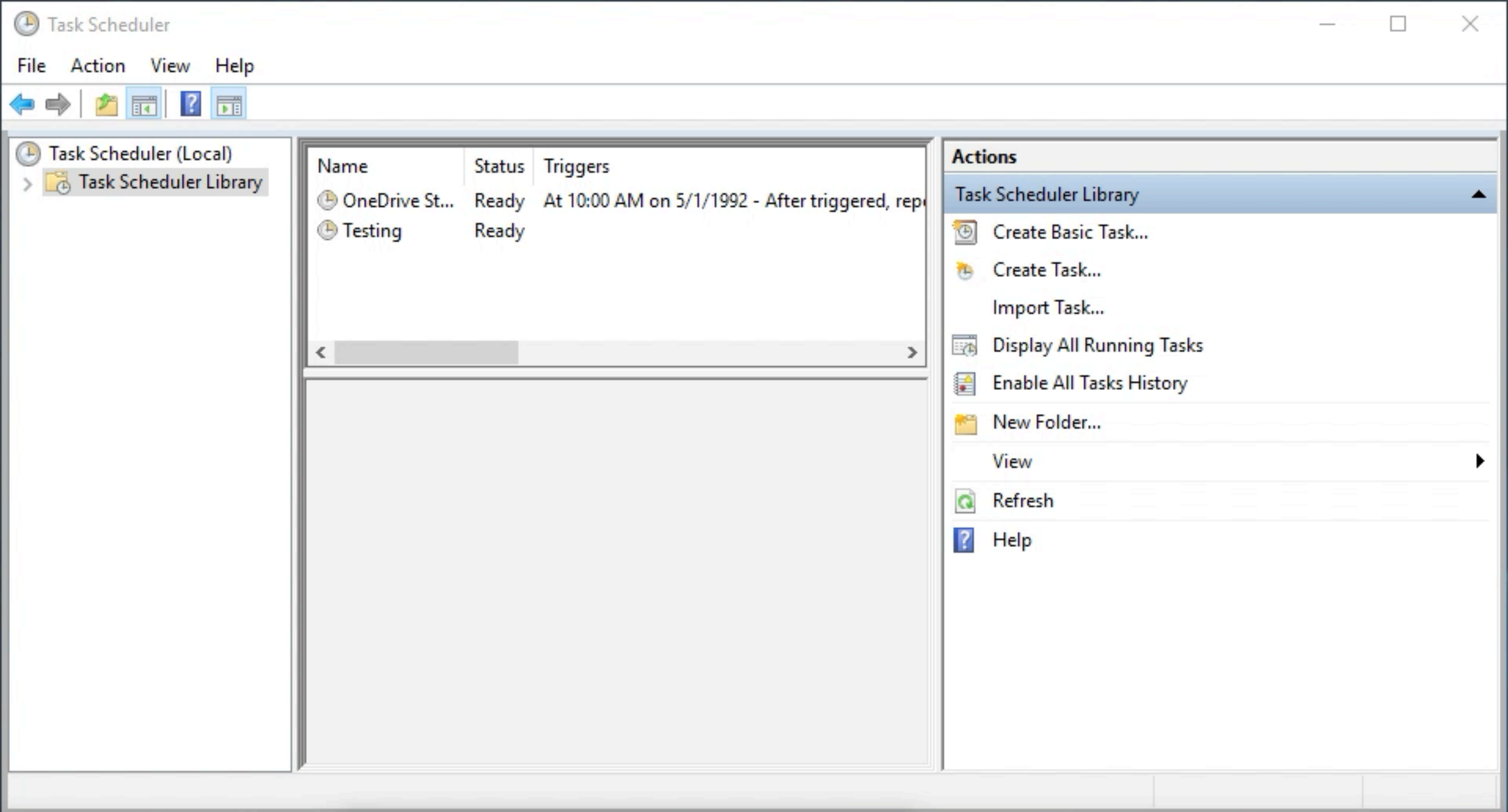
14 items

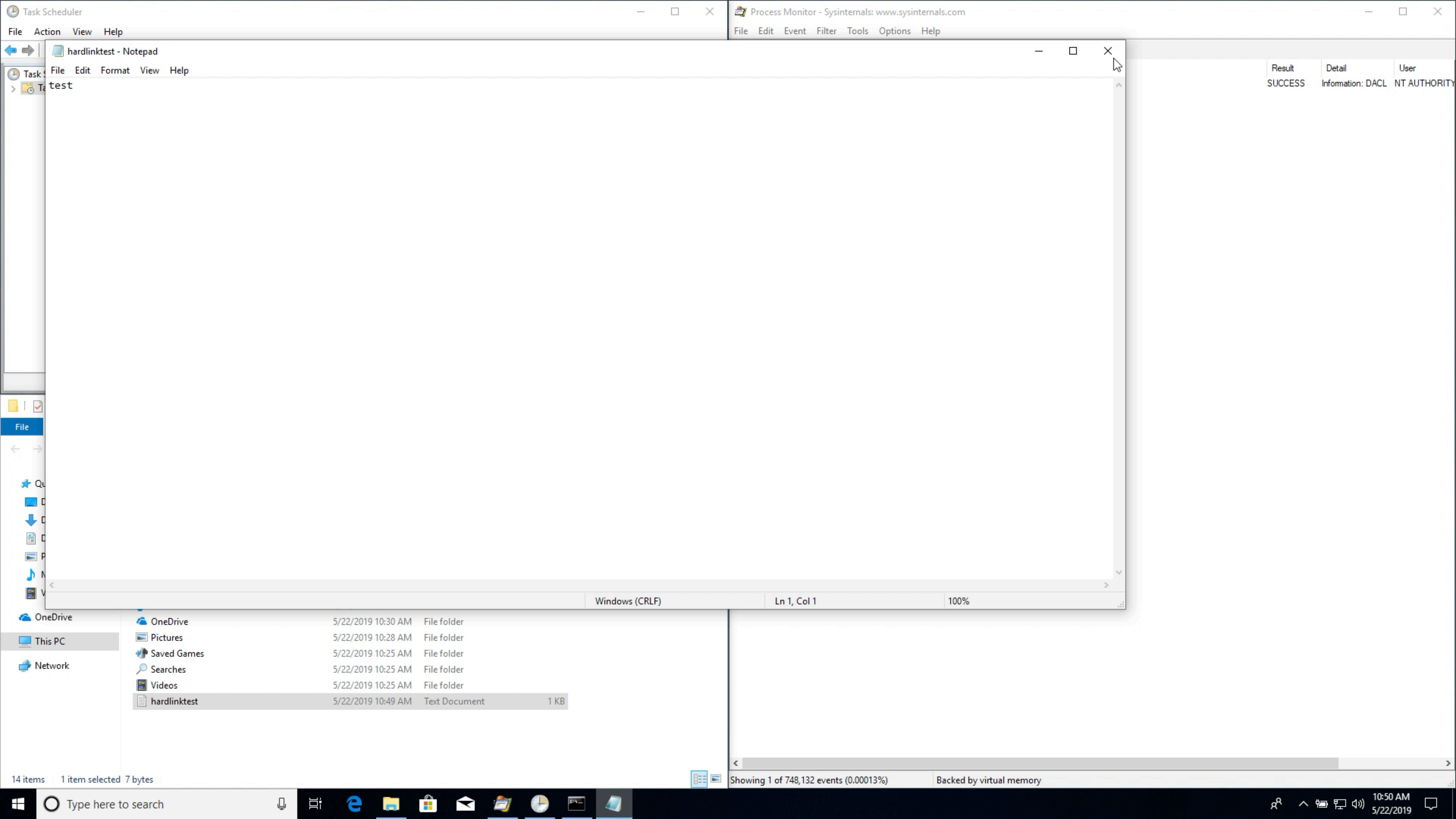
Showing 1 of 629,904 events (0.00015%)

Backed by virtual memory

Type here to search

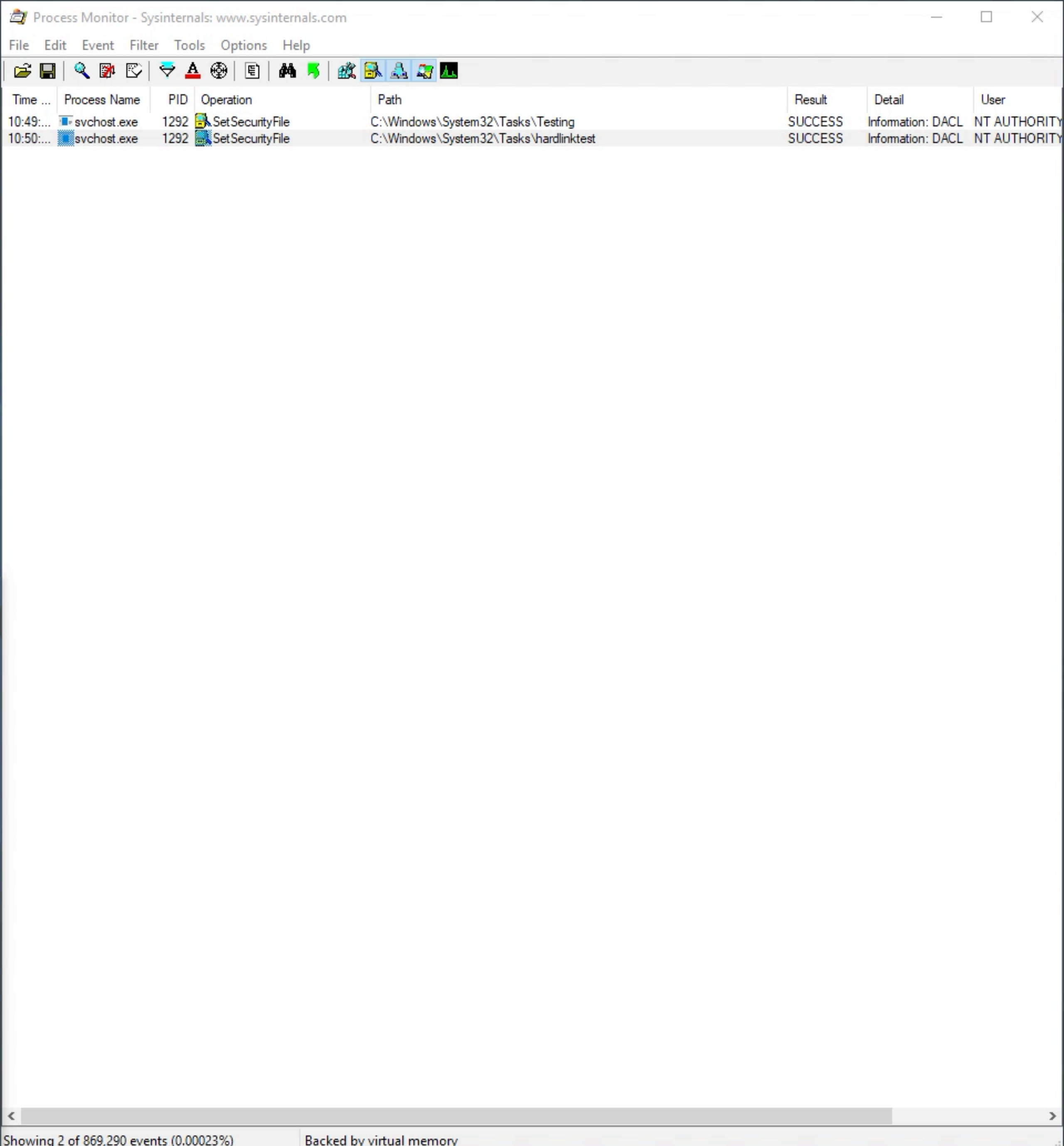
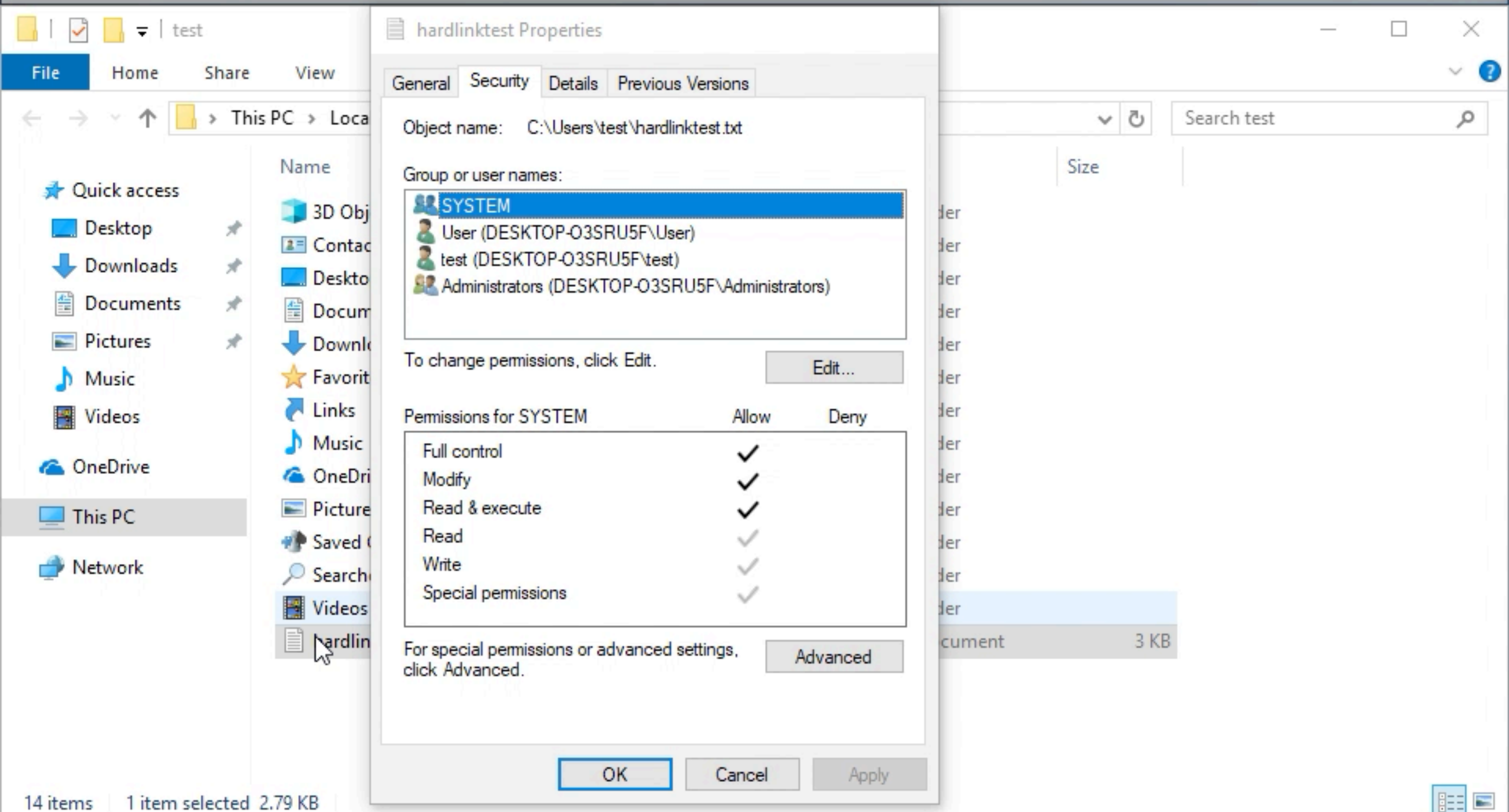
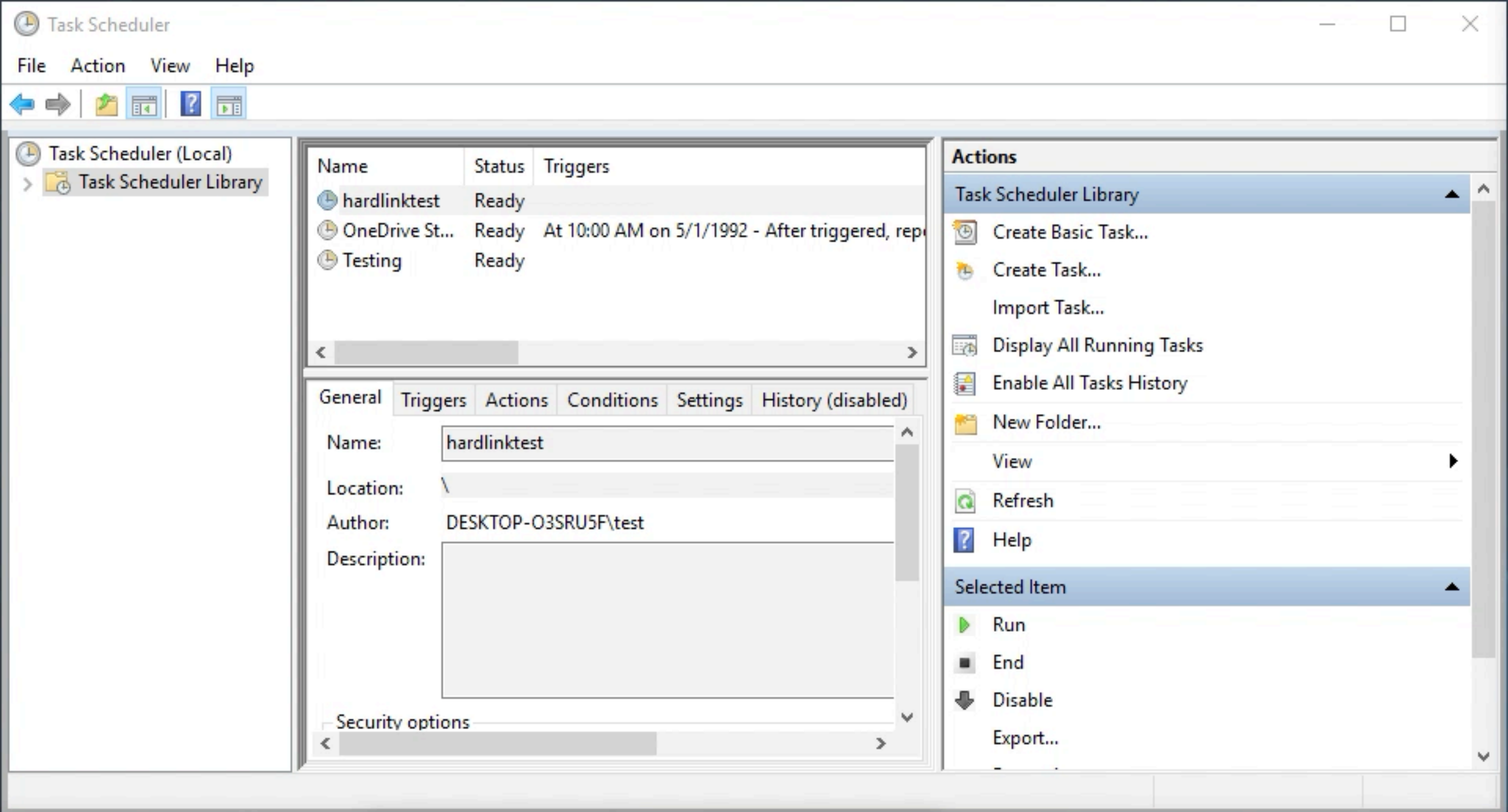
10:50 AM 5/22/2019

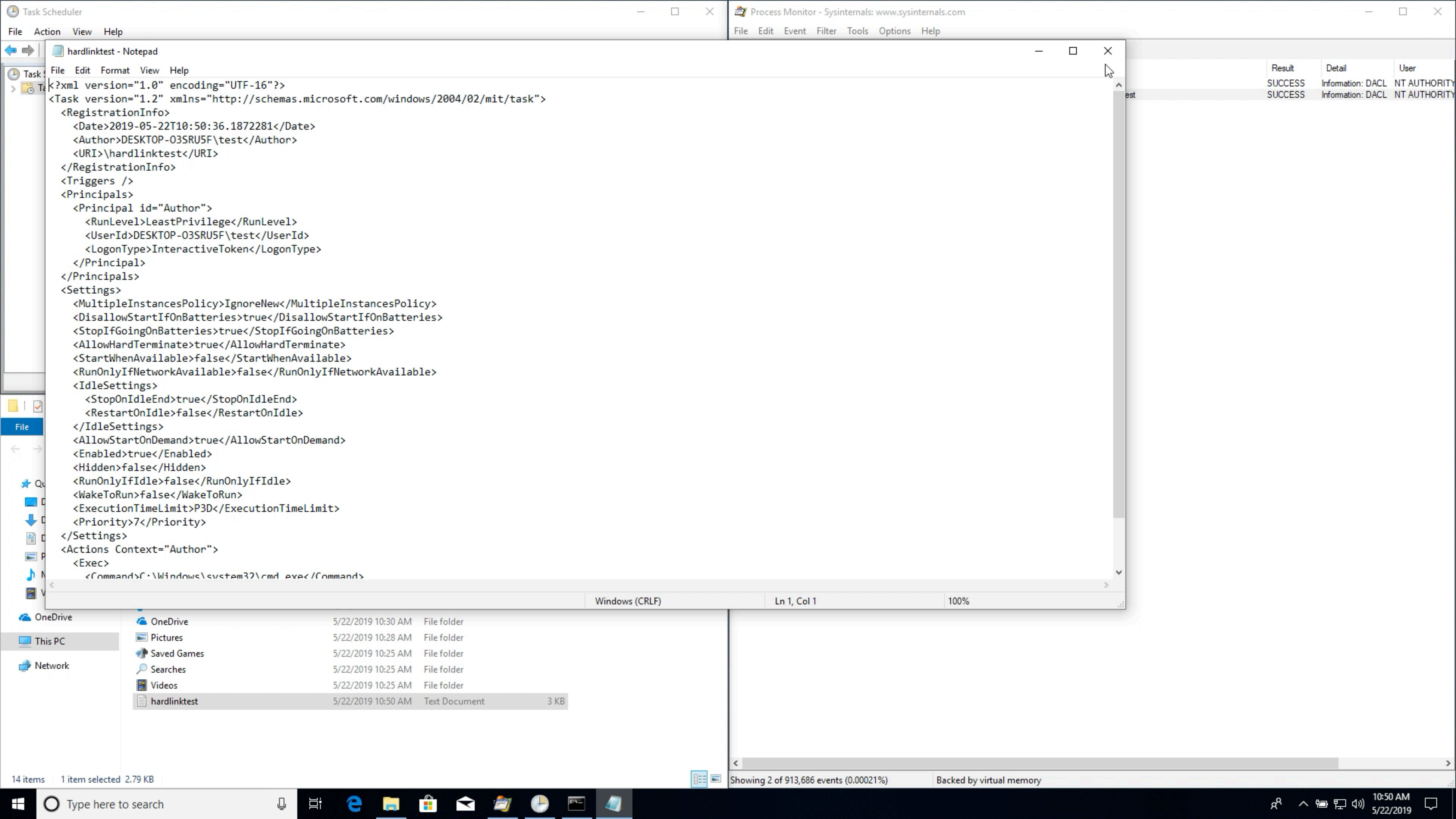




Result	Detail	User
SUCCESS	Information: DACL	NT AUTHORITY\SYSTEM

OneDrive	5/22/2019 10:30 AM	File folder	
Pictures	5/22/2019 10:28 AM	File folder	
Saved Games	5/22/2019 10:25 AM	File folder	
Searches	5/22/2019 10:25 AM	File folder	
Videos	5/22/2019 10:25 AM	File folder	
hardlinktest	5/22/2019 10:49 AM	Text Document	1 KB





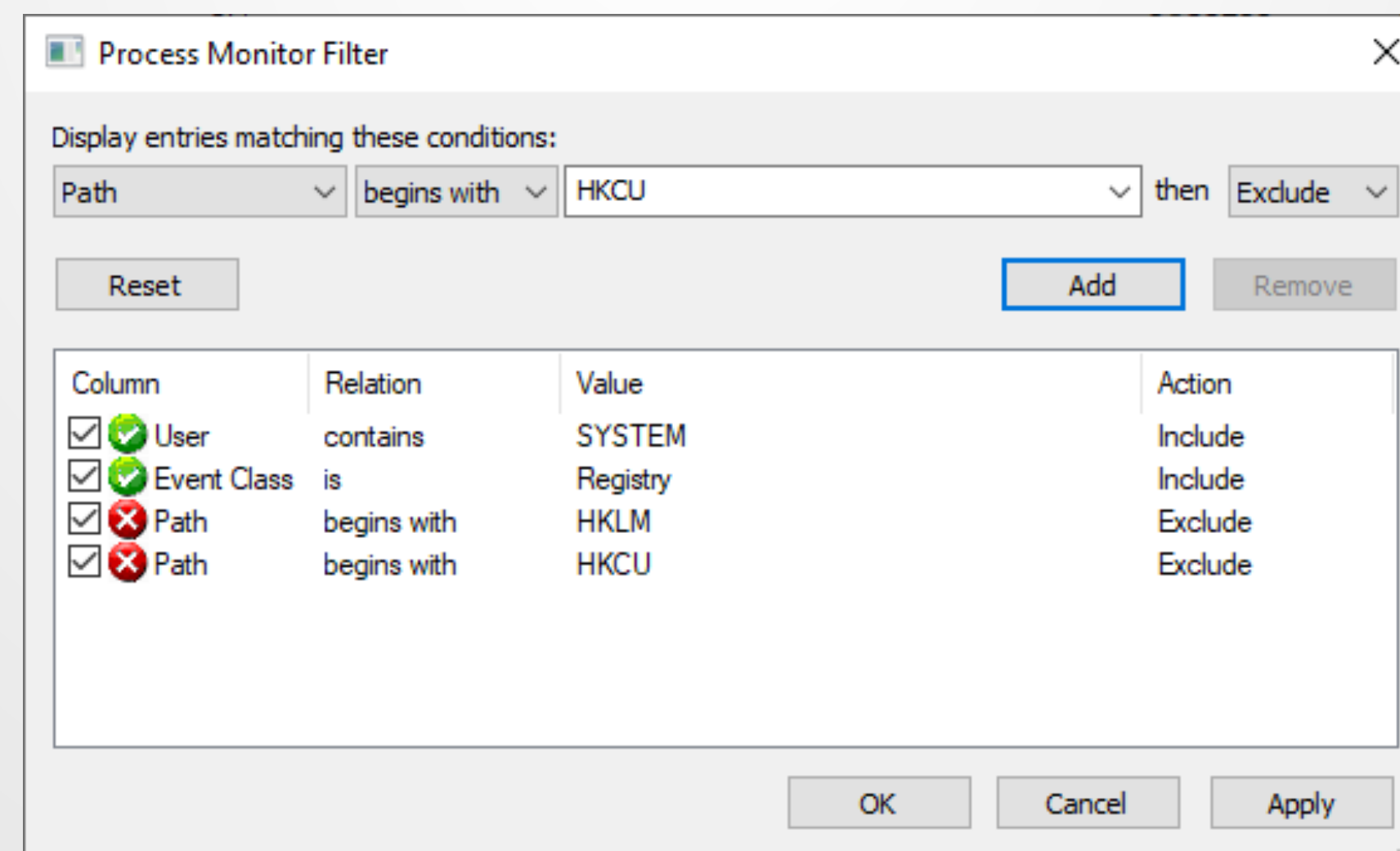
```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Date>2019-05-22T10:50:36.1872281</Date>
    <Author>DESKTOP-03SRU5F\test</Author>
    <URI>\hardlinktest</URI>
  </RegistrationInfo>
  <Triggers />
  <Principals>
    <Principal id="Author">
      <RunLevel>LeastPrivilege</RunLevel>
      <UserId>DESKTOP-03SRU5F\test</UserId>
      <LogonType>InteractiveToken</LogonType>
    </Principal>
  </Principals>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <AllowHardTerminate>true</AllowHardTerminate>
    <StartWhenAvailable>false</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>false</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>P3D</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>C:\Windows\system32\cmd.exe</Command>
    </Exec>
  </Actions>
</Task>
```

Result	Detail	User
SUCCESS	Information: DACL	NT AUTHORITY\SYSTEM
SUCCESS	Information: DACL	NT AUTHORITY\SYSTEM

OneDrive	OneDrive	5/22/2019 10:30 AM	File folder	
This PC	Pictures	5/22/2019 10:28 AM	File folder	
Network	Saved Games	5/22/2019 10:25 AM	File folder	
	Searches	5/22/2019 10:25 AM	File folder	
	Videos	5/22/2019 10:25 AM	File folder	
	hardlinktest	5/22/2019 10:50 AM	Text Document	3 KB

Hunting in registry

- Not seen any potential for abuse
- Include SYSTEM user
- Exclude starting with HKLM and HKCU



AccessEnum

