

A dark blue vertical bar runs down the left side of the page. A blue arrow-shaped banner points to the right from this bar, containing the date. Below the banner, several thin, curved lines in dark blue and light grey sweep upwards from the bottom left corner.

3/17/2021

# PROCESS MONITOR

Gaganpreet Singh

## Contents

1. Introduction .....	2
2. For This activity, we are going to examine Spotify software. ....	2
3. References .....	20

## 1. Introduction

Process Monitor is a monitoring tool for Windows OS which provide data of registry, real time file system, Network activity and process/thread activity.

Process Monitor can capture Input/Output operations happening through file system, registry or the network. Other types of operations it can detect are process and profiling.

Powerful features of process monitor tool provide a huge help in system troubleshooting and malware hunting.

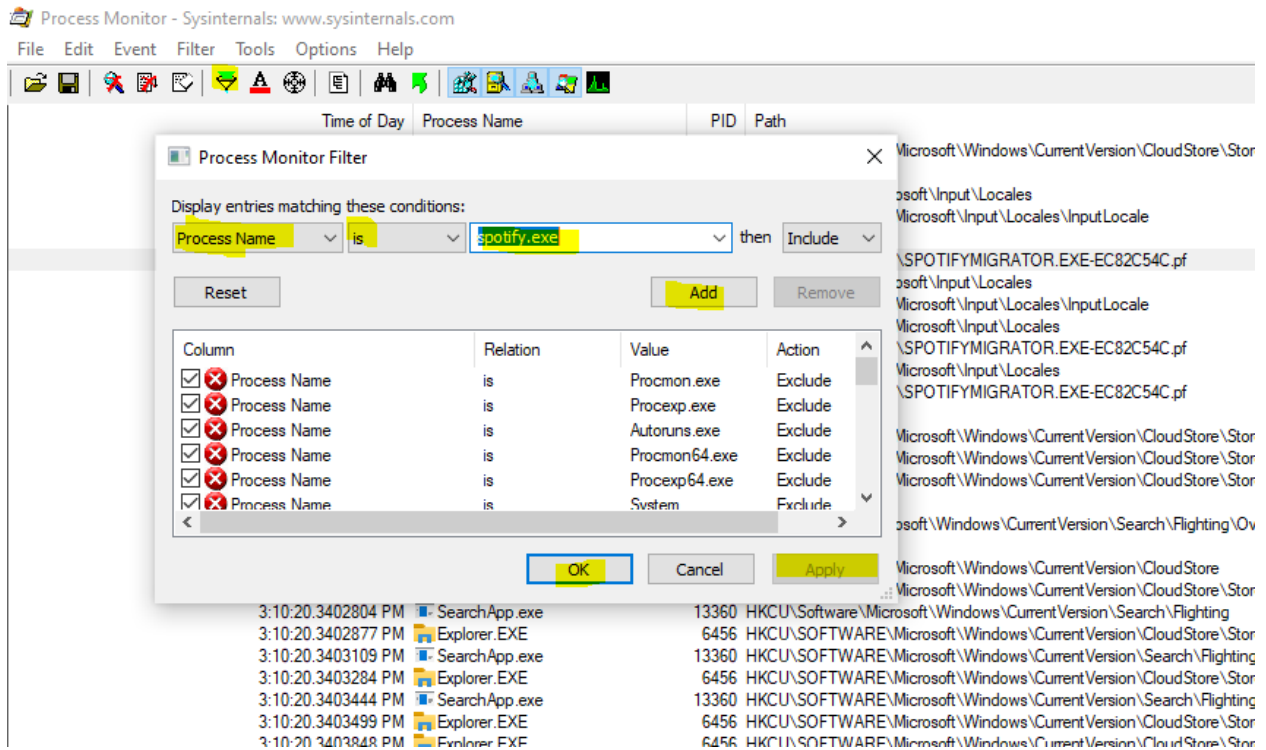
## 2. For This activity, we are going to examine Spotify software.

We need to follow the below steps for the analysis:

Step 1: Run the Application and navigate to Process monitor application-> File-> Capture Events.

Step 2: Run the Spotify Software and do certain UI actions and let Process Monitor capture events.

Step 3: Stop capturing events to analyze the operations and processes performed by the software. Filter the Processes according to "Process Name" attribute as shown in the image below. Click on Add and click Ok then apply.



**Step 4: Below is the screenshot of all the processes under Spotify.exe name after applying filter.**

Time of Day	Process Name	PID	Path	Result	Detail
3:10:20.3807847 PM	Spotify.exe	18580		SUCCESS	Parent P
3:10:20.3807898 PM	Spotify.exe	18580		SUCCESS	Thread I
3:10:20.3829546 PM	Spotify.exe	18580	C:\Program Files\WindowsApps\SpotifyAB.SpotifyMusic_1.154.592.0_x-ww_zpnekdzrea0\Spotify.exe	SUCCESS	Image B
3:10:20.3830079 PM	Spotify.exe	18580	C:\Windows\System32\ntdll.dll	SUCCESS	Image B
3:10:20.3830636 PM	Spotify.exe	18580	C:\Windows\System32\kernel32.dll	SUCCESS	Image B
3:10:20.3831248 PM	Spotify.exe	18580	C:\Windows\prefetch\SPOTIFY.EXE-46D44F43.pf	SUCCESS	Desired /
3:10:20.3831538 PM	Spotify.exe	18580	C:\Windows\prefetch\SPOTIFY.EXE-46D44F43.pf	SUCCESS	Allocator
3:10:20.3831638 PM	Spotify.exe	18580	C:\Windows\prefetch\SPOTIFY.EXE-46D44F43.pf	SUCCESS	Offset: 0.
3:10:20.3835025 PM	Spotify.exe	18580	C:\Windows\prefetch\SPOTIFY.EXE-46D44F43.pf	SUCCESS	
3:10:20.3975439 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired /
3:10:20.3975615 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired /
3:10:20.3975766 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadlock	NAME NOT FOUND	Length: 1
3:10:20.3975956 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
3:10:20.3975947 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	REPARSE	Desired /
3:10:20.3976057 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	NAME NOT FOUND	Desired /
3:10:20.3976309 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired /
3:10:20.3976405 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
3:10:20.3976510 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 2
3:10:20.3976592 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
3:10:20.3976903 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired /
3:10:20.3977010 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired /
3:10:20.3977109 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 2
3:10:20.3977246 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
3:10:20.3979436 PM	Spotify.exe	18580	C:\Windows	SUCCESS	Desired /
3:10:20.3981152 PM	Spotify.exe	18580	C:\Windows\System32\wow64.dll	SUCCESS	Image B
3:10:20.3982239 PM	Spotify.exe	18580	C:\Windows\System32\wow64win.dll	SUCCESS	Image B
3:10:20.3984660 PM	Spotify.exe	18580	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired /
3:10:20.3986586 PM	Spotify.exe	18580	C:\Windows	SUCCESS	Desired /
3:10:20.3987000 PM	Spotify.exe	18580	C:\Windows	SUCCESS	Name: \
3:10:20.3987187 PM	Spotify.exe	18580	C:\Windows	SUCCESS	
3:10:20.3987574 PM	Spotify.exe	18580	HKLM\Software\Microsoft\Wow64\Wow64	SUCCESS	Desired /
3:10:20.3987814 PM	Spotify.exe	18580	HKLM\Software\Microsoft\Wow64\Wow64\Spotify.exe	SUCCESS	Desired /
3:10:20.3988004 PM	Spotify.exe	18580	HKLM\Software\Microsoft\Wow64\Wow64\Spotify.exe	NAME NOT FOUND	Length: 1
3:10:20.3988101 PM	Spotify.exe	18580	HKLM\Software\Microsoft\Wow64\Wow64\Spotify.exe	SUCCESS	Type: RE
3:10:20.3989059 PM	Spotify.exe	18580	C:\Windows\System32\wow64cpu.dll	SUCCESS	
3:10:20.3990426 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Image B
3:10:20.3990570 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired /
3:10:20.3990700 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	KeySetIn
3:10:20.3990772 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadlock	NAME NOT FOUND	Length: 1
3:10:20.3990860 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
3:10:20.3990905 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired /

Step 5: As mentioned above a process can have File System, Registry, Network event class which we can filter after selecting the highlighted icons as shown in the image below:

- Show Registry activity button show processes under Registry event class.

Process Monitor - Sysinternals: www.sysinternals.com

Time of Day	Process Name	PID	Path	Result	Detail	Event Class
3:10:20.3926433 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value	Registry
3:10:20.3975615 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value	Registry
3:10:20.3978566 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadlock	NAME NOT FOUND	Length: 80	Registry
3:10:20.3979547 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value	Registry
3:10:20.3979657 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	REPARSE	Desired Access: Query Value	Registry
3:10:20.3976309 PM	Spotify.exe	18580	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	NAME NOT FOUND	Desired Access: Query Value	Registry
3:10:20.3976405 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value, Enumerate Sub Keys	Registry
3:10:20.3976510 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	SUCCESS	Desired Access: Query Value, Enumerate Sub Keys	Registry
3:10:20.3976592 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	NAME NOT FOUND	Length: 24	Registry
3:10:20.3976903 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value, Enumerate Sub Keys	Registry
3:10:20.3977010 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value, Enumerate Sub Keys	Registry
3:10:20.3977109 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 24	Registry
3:10:20.3977246 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Read	Registry
3:10:20.3987574 PM	Spotify.exe	18580	HKLM\Software\Microsoft\Wow64\86	SUCCESS	Desired Access: Read	Registry
3:10:20.3987814 PM	Spotify.exe	18580	HKLM\SOFTWARE\Microsoft\Wow64\86	SUCCESS	Length: 520	Registry
3:10:20.3987934 PM	Spotify.exe	18580	HKLM\SOFTWARE\Microsoft\Wow64\86\Spotify.exe	NAME NOT FOUND	Type: REG_SZ, Length: 26, Data: wow64cpu.dll	Registry
3:10:20.3988004 PM	Spotify.exe	18580	HKLM\SOFTWARE\Microsoft\Wow64\86	SUCCESS	Desired Access: Read	Registry
3:10:20.3988101 PM	Spotify.exe	18580	HKLM\SOFTWARE\Microsoft\Wow64\86	SUCCESS	Length: 520	Registry
3:10:20.3990426 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value	Registry
3:10:20.3990570 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value	Registry
3:10:20.3990700 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	KeySetInformationClass: KeySetHandleTagInformation, Length: 0	Registry
3:10:20.3990777 PM	Spotify.exe	18580	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadlock	NAME NOT FOUND	Length: 80	Registry

- Show File System activity button show processes under File System event class.

Process Monitor - Sysinternals: www.sysinternals.com

Time of Day	Process Name	PID	Path	Result	Detail	Event Class
3:10:20.3831248 PM	Spotify.exe	18580	C:\Windows\prefetch\SPOTIFY.EXE-46D44F43.pf	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Sync	File System
3:10:20.3831538 PM	Spotify.exe	18580	C:\Windows\prefetch\SPOTIFY.EXE-46D44F43.pf	SUCCESS	AllocationSize: 40,960, EndOfFile: 38,260, NumberOfLinks: 1, De...	File System
3:10:20.3831638 PM	Spotify.exe	18580	C:\Windows\prefetch\SPOTIFY.EXE-46D44F43.pf	SUCCESS	Offset: 0, Length: 38,260, Priority: Normal	File System
3:10:20.3832525 PM	Spotify.exe	18580	C:\Windows\prefetch\SPOTIFY.EXE-46D44F43.pf	SUCCESS	Desired Access: Read Attributes, Synchronize, Disposition: Open...	File System
3:10:20.3979436 PM	Spotify.exe	18580	C:\Windows	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Op...	File System
3:10:20.3984660 PM	Spotify.exe	18580	C:\Windows\System32\wow64cpu.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Op...	File System
3:10:20.3985056 PM	Spotify.exe	18580	C:\Windows	SUCCESS	Desired Access: Read Attributes, Synchronize, Disposition: Open...	File System
3:10:20.3987000 PM	Spotify.exe	18580	C:\Windows	SUCCESS	Name: \Windows	File System
3:10:20.3987187 PM	Spotify.exe	18580	C:\Windows	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Op...	File System
3:10:20.3994195 PM	Spotify.exe	18580	C:\Windows\SysWOW64	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Op...	File System
3:10:20.4000584 PM	Spotify.exe	18580	C:\Windows\SysWOW64\KernelBase.dll	NAME NOT FOUND	Name: \Windows\SysWOW64\KernelBase.dll	File System
3:10:20.4001512 PM	Spotify.exe	18580	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Name: \Windows\SysWOW64\KernelBase.dll	File System
3:10:20.4007353 PM	Spotify.exe	18580	C:\Program Files\WindowsApps\SpotifyAB.SpotifyMusic_1154.592.0_x-ww...	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Op...	File System
3:10:20.4008192 PM	Spotify.exe	18580	C:\Windows\WinSxS\x-ww...	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Op...	File System
3:10:20.4010309 PM	Spotify.exe	18580	C:\Windows\WinSxS\x-ww...	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Op...	File System
3:10:20.4010418 PM	Spotify.exe	18580	C:\Program Files\WindowsApps\SpotifyAB.SpotifyMusic_1154.592.0_x-ww...	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Op...	File System
3:10:20.4010520 PM	Spotify.exe	18580	C:\Windows\WinSxS\x-ww...	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Op...	File System
3:10:20.4010596 PM	Spotify.exe	18580	C:\Windows\WinSxS\x-ww...	SUCCESS	Creation Time: 2/4/2021 6:57:18 PM, Last Access Time: 3/15/202...	File System
3:10:20.4011200 PM	Spotify.exe	18580	C:\Windows\WinSxS\x-ww...	SUCCESS	Desired Access: Read Data/List Directory, Execute/Traverse, Sy...	File System
3:10:20.4011279 PM	Spotify.exe	18580	C:\Windows\WinSxS\x-ww...	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Op...	File System
3:10:20.4011502 PM	Spotify.exe	18580	C:\Windows\WinSxS\x-ww...	SUCCESS	SynchType: SynchTypeCreateSection, PageProtection: PAGE_EXECUTE...	File System
3:10:20.4013778 PM	Spotify.exe	18580	C:\Windows\WinSxS\x-ww...	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Op...	File System

- Show Network activity button show processes under Network event class. Show File System activity button show processes under File System event class.

Process Monitor - Sysinternals: www.sysinternals.com

Time of Day	Process Name	PID	Path	Result	Detail	Event Class
3:10:22.1974853 PM	Spotify.exe	18580	LAPTOP-09P15T96.55804 -> 239.255.255.250:wsdp	SUCCESS	Length: 168, sequence: 0, connid: 0	Network
3:10:22.1977575 PM	Spotify.exe	18580	LAPTOP-09P15T96.55805 -> 239.255.255.250:wsdp	SUCCESS	Length: 168, sequence: 0, connid: 0	Network
3:10:22.1978905 PM	Spotify.exe	18580	LAPTOP-09P15T96.55806 -> 239.255.255.250:wsdp	SUCCESS	Length: 168, sequence: 0, connid: 0	Network
3:10:22.1980106 PM	Spotify.exe	18580	LAPTOP-09P15T96.55807 -> 239.255.255.250:wsdp	SUCCESS	Length: 168, sequence: 0, connid: 0	Network
3:10:22.2054246 PM	Spotify.exe	18580	LAPTOP-09P15T96.55807 -> 192.168.29.95:wsdp	SUCCESS	Length: 232, sequence: 0, connid: 0	Network
3:10:22.2189132 PM	Spotify.exe	18580	LAPTOP-09P15T96.5353 -> 224.0.0.251:5353	SUCCESS	Length: 40, sequence: 0, connid: 0	Network
3:10:22.2193205 PM	Spotify.exe	18580	LAPTOP-09P15T96.5353 -> 224.0.0.251:5353	SUCCESS	Length: 40, sequence: 0, connid: 0	Network
3:10:22.2193804 PM	Spotify.exe	18580	LAPTOP-09P15T96.5353 -> 224.0.0.251:5353	SUCCESS	Length: 40, sequence: 0, connid: 0	Network
3:10:22.2200194 PM	Spotify.exe	18580	LAPTOP-09P15T96.5353 -> 224.0.0.251:5353	SUCCESS	Length: 40, sequence: 0, connid: 0	Network
3:10:22.2200787 PM	Spotify.exe	18580	LAPTOP-09P15T96.5353 -> 224.0.0.251:5353	SUCCESS	Length: 40, sequence: 0, connid: 0	Network
3:10:22.2202371 PM	Spotify.exe	18580	LAPTOP-09P15T96.5353 -> 224.0.0.251:5353	SUCCESS	Length: 40, sequence: 0, connid: 0	Network
3:10:22.2203395 PM	Spotify.exe	18580	LAPTOP-09P15T96.5353 -> 224.0.0.251:5353	SUCCESS	Length: 40, sequence: 0, connid: 0	Network
3:10:22.2205581 PM	Spotify.exe	18580	LAPTOP-09P15T96.5353 -> 224.0.0.251:5353	SUCCESS	Length: 40, sequence: 0, connid: 0	Network
3:10:22.2206003 PM	Spotify.exe	18580	LAPTOP-09P15T96.5353 -> 224.0.0.251:5353	SUCCESS	Length: 40, sequence: 0, connid: 0	Network
3:10:22.2206079 PM	Spotify.exe	18580	LAPTOP-09P15T96.5353 -> 224.0.0.251:5353	SUCCESS	Length: 40, sequence: 0, connid: 0	Network
3:10:22.2209121 PM	Spotify.exe	18580	LAPTOP-09P15T96.5353 -> 224.0.0.251:5353	SUCCESS	Length: 40, sequence: 0, connid: 0	Network
3:10:22.2217173 PM	Spotify.exe	18580	LAPTOP-09P15T96.5353 -> 224.0.0.251:5353	SUCCESS	Length: 40, sequence: 0, connid: 0	Network
3:10:22.2212209 PM	Spotify.exe	18580	LAPTOP-09P15T96.5353 -> 224.0.0.251:5353	SUCCESS	Length: 40, sequence: 0, connid: 0	Network
3:10:22.2215529 PM	Spotify.exe	18580	LAPTOP-09P15T96.5353 -> 224.0.0.251:5353	SUCCESS	Length: 40, sequence: 0, connid: 0	Network
3:10:22.2216679 PM	Spotify.exe	18580	LAPTOP-09P15T96.5353 -> 224.0.0.251:5353	SUCCESS	Length: 40, sequence: 0, connid: 0	Network

- Show Process and Thread Activity show processes under Process event class.

Process Monitor - Sysinternals: www.sysinternals.com

Time of Day	Process Name	PID	Path	Result	Detail	Event Class
3:10:20.3807847 PM	Spotify.exe	18580		SUCCESS	Parent PID: 11304, Command Line: Spotify.exe, Current Directory: ...	Process
3:10:20.3807968 PM	Spotify.exe	18580		SUCCESS	Thread ID: 21576	Process
3:10:20.3826846 PM	Spotify.exe	18580	C:\Program Files\WindowsApps\SpotifyAB.SpotifyMusic_1154.592.0_x-ww...	SUCCESS	Image Base: 0x4050000, Image Size: 0x1707000	Process
3:10:20.3830079 PM	Spotify.exe	18580	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x77c7a950000, Image Size: 0x15000	Process
3:10:20.3830636 PM	Spotify.exe	18580	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77c7a950000, Image Size: 0x1a3000	Process
3:10:20.3881152 PM	Spotify.exe	18580	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x77c7a950000, Image Size: 0x59000	Process
3:10:20.3882239 PM	Spotify.exe	18580	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x77c7a950000, Image Size: 0x83000	Process

## Step 6: Now we will analyze what changes are made by network event class processes.

A total of 1214 events related to network were collected dealing with operation UDP Send, TCP send, TCP receive and UDP Receive.

Process Monitor - Sysinternals: www.sysinternals.com

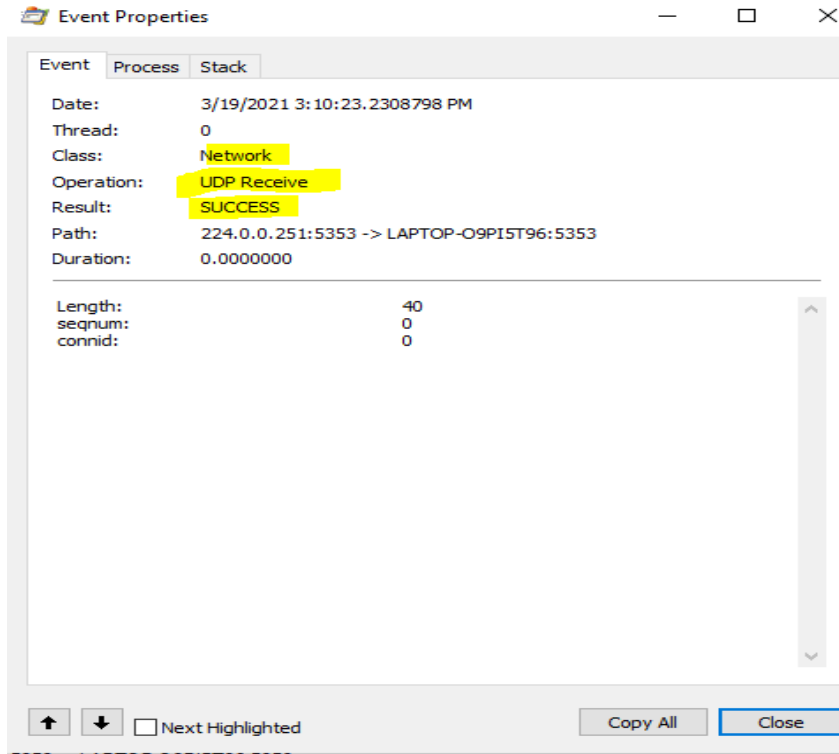
File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Path	Result	Detail	Event Class	Operation
3:10:22.1974933 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.55804 -> 239.255.255.250:udp	SUCCESS	Length: 169, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.1978759 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.55805 -> 239.255.255.250:udp	SUCCESS	Length: 169, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.1979055 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.55806 -> 239.255.255.250:udp	SUCCESS	Length: 169, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.1980106 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.55807 -> 239.255.255.250:udp	SUCCESS	Length: 169, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.2054246 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.55807 -> 192.168.29.55:udp	SUCCESS	Length: 232, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.2169132 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.5383 -> 224.0.0.251:5383	SUCCESS	Length: 40, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.2193026 PM	Spotify.exe	18500	224.0.0.251:5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 40, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.2193984 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.5383 -> R02-Rb.5383	SUCCESS	Length: 40, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.2200194 PM	Spotify.exe	18500	R02-Rb.5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 40, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.2200787 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.5383 -> 224.0.0.251:5383	SUCCESS	Length: 40, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.2202871 PM	Spotify.exe	18500	224.0.0.251:5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 40, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.2203395 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.5383 -> R02-Rb.5383	SUCCESS	Length: 40, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.2205581 PM	Spotify.exe	18500	R02-Rb.5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 40, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.2206008 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.5383 -> 224.0.0.251:5383	SUCCESS	Length: 40, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.2208079 PM	Spotify.exe	18500	224.0.0.251:5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 40, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.2209121 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.5383 -> R02-Rb.5383	SUCCESS	Length: 40, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.2211713 PM	Spotify.exe	18500	R02-Rb.5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 40, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.2212289 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.5383 -> 224.0.0.251:5383	SUCCESS	Length: 40, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.2215529 PM	Spotify.exe	18500	224.0.0.251:5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 40, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.2216679 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.5383 -> R02-Rb.5383	SUCCESS	Length: 40, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.2221539 PM	Spotify.exe	18500	R02-Rb.5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 40, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.5301555 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.5383 -> 224.0.0.251:5383	SUCCESS	Length: 45, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.5302977 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.54434 -> 239.255.255.250:udp	SUCCESS	Length: 125, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.5304142 PM	Spotify.exe	18500	224.0.0.251:5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 45, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.5304707 PM	Spotify.exe	18500	239.255.255.250:udp -> LAPTOP-ORP1ST96.54434	SUCCESS	Length: 125, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.5304858 PM	Spotify.exe	18500	224.0.0.251:5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 45, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.5306384 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.5383 -> 224.0.0.251:5383	SUCCESS	Length: 45, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.5307620 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.54435 -> 239.255.255.250:udp	SUCCESS	Length: 125, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.5307854 PM	Spotify.exe	18500	224.0.0.251:5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 45, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.5308643 PM	Spotify.exe	18500	224.0.0.251:5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 45, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.5309264 PM	Spotify.exe	18500	239.255.255.250:udp -> LAPTOP-ORP1ST96.54435	SUCCESS	Length: 125, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.5311025 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.5383 -> 224.0.0.251:5383	SUCCESS	Length: 45, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.5311432 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.54436 -> 239.255.255.250:udp	SUCCESS	Length: 125, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.5315074 PM	Spotify.exe	18500	224.0.0.251:5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 45, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.5316077 PM	Spotify.exe	18500	239.255.255.250:udp -> LAPTOP-ORP1ST96.54436	SUCCESS	Length: 125, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.5316546 PM	Spotify.exe	18500	224.0.0.251:5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 45, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.5318071 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.5383 -> 224.0.0.251:5383	SUCCESS	Length: 45, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.5319318 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.54437 -> 239.255.255.250:udp	SUCCESS	Length: 125, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.5320151 PM	Spotify.exe	18500	224.0.0.251:5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 45, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.5320757 PM	Spotify.exe	18500	224.0.0.251:5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 45, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.5321409 PM	Spotify.exe	18500	239.255.255.250:udp -> LAPTOP-ORP1ST96.54437	SUCCESS	Length: 125, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.5368533 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.54456 -> 239.255.255.250:udp	SUCCESS	Length: 125, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.5369242 PM	Spotify.exe	18500	239.255.255.250:udp -> LAPTOP-ORP1ST96.54456	SUCCESS	Length: 125, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.53691975 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.54457 -> 239.255.255.250:udp	SUCCESS	Length: 125, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.53693535 PM	Spotify.exe	18500	239.255.255.250:udp -> LAPTOP-ORP1ST96.54457	SUCCESS	Length: 125, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.53696006 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.54458 -> 239.255.255.250:udp	SUCCESS	Length: 125, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.53697352 PM	Spotify.exe	18500	239.255.255.250:udp -> LAPTOP-ORP1ST96.54458	SUCCESS	Length: 125, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.7001149 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.54459 -> 239.255.255.250:udp	SUCCESS	Length: 125, seqnum: 0, connid: 0	Network	UDP Send
3:10:22.7003006 PM	Spotify.exe	18500	239.255.255.250:udp -> LAPTOP-ORP1ST96.54459	SUCCESS	Length: 125, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.7024742 PM	Spotify.exe	18500	239.255.255.250:udp -> 10.10.241.52:54458	SUCCESS	Length: 125, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.7065519 PM	Spotify.exe	18500	LAPTOP-ORP1ST96.54458 -> 192.168.29.55:udp	SUCCESS	Length: 232, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.7245864 PM	Spotify.exe	18500	224.0.0.251:5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 28, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.7247867 PM	Spotify.exe	18500	224.0.0.251:5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 28, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.7248848 PM	Spotify.exe	18500	224.0.0.251:5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 28, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.7251528 PM	Spotify.exe	18500	224.0.0.251:5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 28, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.7253677 PM	Spotify.exe	18500	R02-Rb.5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 28, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.7255571 PM	Spotify.exe	18500	R02-Rb.5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 28, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.7258826 PM	Spotify.exe	18500	R02-Rb.5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 28, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.7260884 PM	Spotify.exe	18500	R02-Rb.5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 28, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.7264088 PM	Spotify.exe	18500	224.0.0.251:5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 28, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.7265385 PM	Spotify.exe	18500	224.0.0.251:5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 28, seqnum: 0, connid: 0	Network	UDP Receive
3:10:22.7266514 PM	Spotify.exe	18500	224.0.0.251:5383 -> LAPTOP-ORP1ST96.5383	SUCCESS	Length: 28, seqnum: 0, connid: 0	Network	UDP Receive

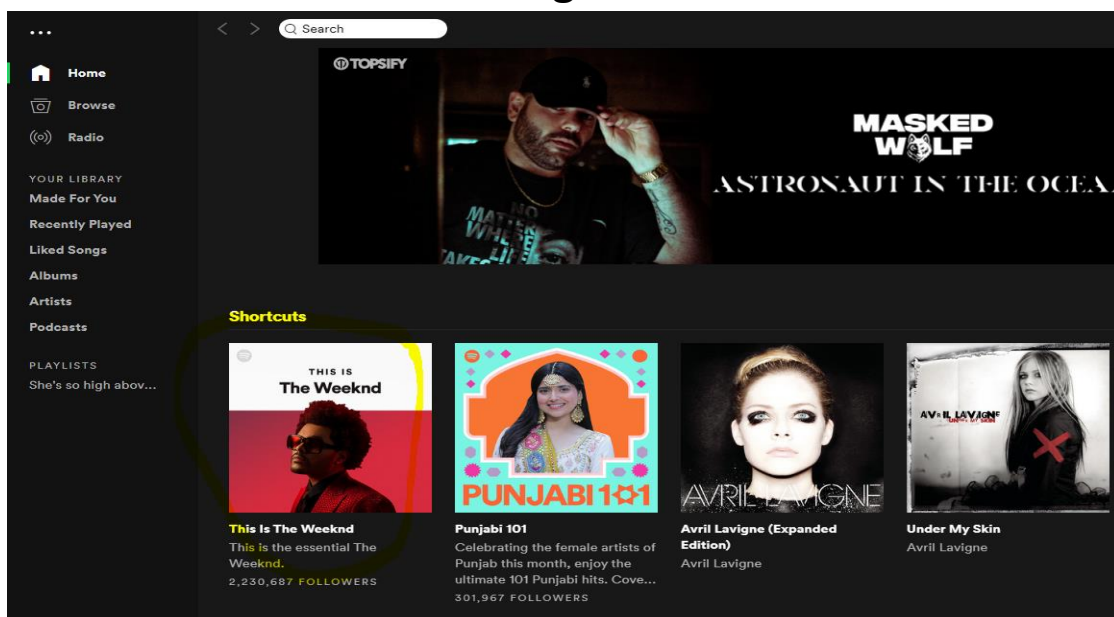
Showing 1,214 of 995,667 events (0.12%) Backed by virtual memory

Step 6.1: Now, Let's analyze in details what is being changed by a specific process name and their sequence number. Right Click on an event-> Properties, Event properties tab will open.





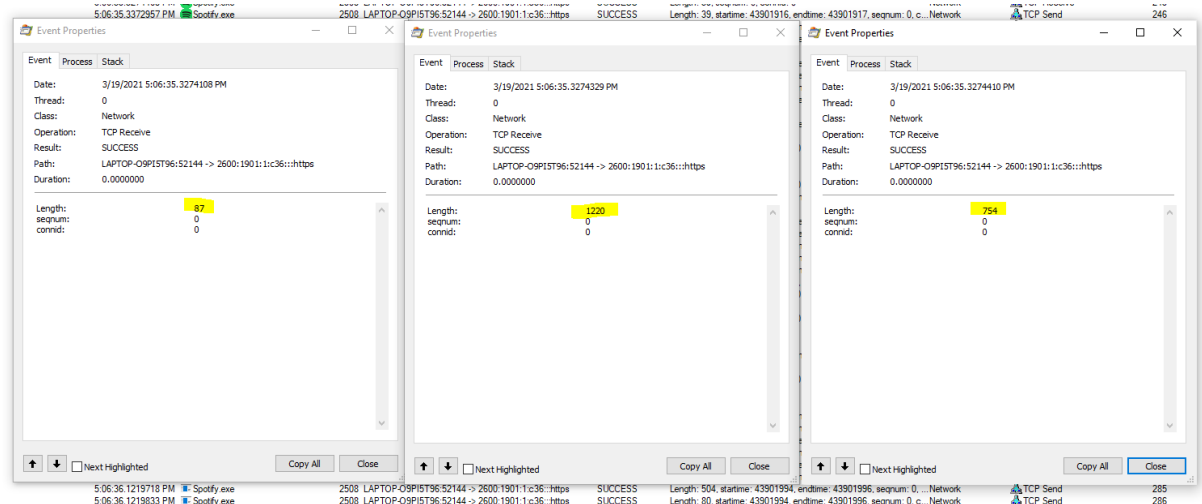
- Clicking a particular song in the Spotify application at 5:06:35 pm to play the song raised the events as shown in the images below.





5:06:35.1918070 PM	Spotify.exe	2508	LAPTOP-O9PI5T96:52144 -> 2600:1901:1:c36::https	SUCCESS	Length: 114, starttime: 43901901, endtime: 43901903, seqnum: 0, ...Network	TCP Send	240
5:06:35.1918380 PM	Spotify.exe	2508	LAPTOP-O9PI5T96:52144 -> 2600:1901:1:c36::https	SUCCESS	Length: 175, starttime: 43901901, endtime: 43901903, seqnum: 0, ...Network	TCP Send	241
5:06:35.3274108 PM	Spotify.exe	2508	LAPTOP-O9PI5T96:52144 -> 2600:1901:1:c36::https	SUCCESS	Length: 87, seqnum: 0, connid: 0	TCP Receive	242
5:06:35.3274329 PM	Spotify.exe	2508	LAPTOP-O9PI5T96:52144 -> 2600:1901:1:c36::https	SUCCESS	Length: 1220, seqnum: 0, connid: 0	TCP Receive	243
5:06:35.3274410 PM	Spotify.exe	2508	LAPTOP-O9PI5T96:52144 -> 2600:1901:1:c36::https	SUCCESS	Length: 754, seqnum: 0, connid: 0	TCP Receive	244
5:06:35.3274468 PM	Spotify.exe	2508	LAPTOP-O9PI5T96:52144 -> 2600:1901:1:c36::https	SUCCESS	Length: 39, seqnum: 0, connid: 0	TCP Receive	245
5:06:35.3372957 PM	Spotify.exe	2508	LAPTOP-O9PI5T96:52144 -> 2600:1901:1:c36::https	SUCCESS	Length: 39, starttime: 43901916, endtime: 43901917, seqnum: 0, ...Network	TCP Send	246
5:06:35.3417459 PM	Spotify.exe	2508	LAPTOP-O9PI5T96:52144 -> 2600:1901:1:c36::https	SUCCESS	Length: 80, starttime: 43901917, endtime: 43901918, seqnum: 0, ...Network	TCP Send	247
5:06:35.3417807 PM	Spotify.exe	2508	LAPTOP-O9PI5T96:52144 -> 2600:1901:1:c36::https	SUCCESS	Length: 548, starttime: 43901917, endtime: 43901918, seqnum: 0, ...Network	TCP Send	248
5:06:35.5040959 PM	Spotify.exe	2508	LAPTOP-O9PI5T96:52144 -> 2600:1901:1:c36::https	SUCCESS	Length: 98, seqnum: 0, connid: 0	TCP Receive	249
5:06:35.5083272 PM	Spotify.exe	2508	LAPTOP-O9PI5T96:52144 -> 2600:1901:1:c36::https	SUCCESS	Length: 144, starttime: 43901933, endtime: 43901934, seqnum: 0, ...Network	TCP Send	250
5:06:35.5190106 PM	Spotify.exe	26616	LAPTOP-O9PI5T96:52145 -> 2600:1901:1:c36::https	SUCCESS	Length: 942, starttime: 43901933, endtime: 43901935, seqnum: 0, ...Network	TCP Send	251
5:06:35.5190463 PM	Spotify.exe	2508	LAPTOP-O9PI5T96:52144 -> 2600:1901:1:c36::https	SUCCESS	Length: 39, starttime: 43901934, endtime: 43901935, seqnum: 0, ...Network	TCP Send	252
5:06:35.5634417 PM	Spotify.exe	26616	LAPTOP-O9PI5T96:52136 -> 26.240.199.104.bc.googleus...	SUCCESS	Length: 254, starttime: 43901925, endtime: 43901940, seqnum: 0, ...Network	TCP Send	253
5:06:35.5634800 PM	Spotify.exe	26616	LAPTOP-O9PI5T96:52136 -> 26.240.199.104.bc.googleus...	SUCCESS	Length: 55, seqnum: 0, connid: 0	TCP Receive	254
5:06:35.6126387 PM	Spotify.exe	26616	LAPTOP-O9PI5T96:52136 -> 26.240.199.104.bc.googleus...	SUCCESS	Length: 176, starttime: 43901931, endtime: 43901945, seqnum: 0, ...Network	TCP Send	255
5:06:35.6495476 PM	Spotify.exe	2508	LAPTOP-O9PI5T96:52144 -> 2600:1901:1:c36::https	SUCCESS	Length: 83, seqnum: 0, connid: 0	TCP Receive	256
5:06:35.6495778 PM	Spotify.exe	2508	LAPTOP-O9PI5T96:52144 -> 2600:1901:1:c36::https	SUCCESS	Length: 279, seqnum: 0, connid: 0	TCP Receive	257
5:06:35.6495938 PM	Spotify.exe	2508	LAPTOP-O9PI5T96:52144 -> 2600:1901:1:c36::https	SUCCESS	Length: 53, seqnum: 0, connid: 0	TCP Receive	258
5:06:35.6496068 PM	Spotify.exe	2508	LAPTOP-O9PI5T96:52144 -> 2600:1901:1:c36::https	SUCCESS	Length: 39, seqnum: 0, connid: 0	TCP Receive	259
5:06:35.6496259 PM	Spotify.exe	26616	LAPTOP-O9PI5T96:52145 -> 2600:1901:1:c36::https	SUCCESS	Length: 738, seqnum: 0, connid: 0	TCP Receive	260
5:06:35.6650647 PM	Spotify.exe	2508	LAPTOP-O9PI5T96:52144 -> 2600:1901:1:c36::https	SUCCESS	Length: 39, starttime: 43901949, endtime: 43901950, seqnum: 0, c...Network	TCP Send	261
5:06:35.7587770 PM	Spotify.exe	26616	LAPTOP-O9PI5T96:52136 -> 26.240.199.104.bc.googleus...	SUCCESS	Length: 55, seqnum: 0, connid: 0	TCP Receive	262

- Several TCP send/receive operations were performed having various lengths.

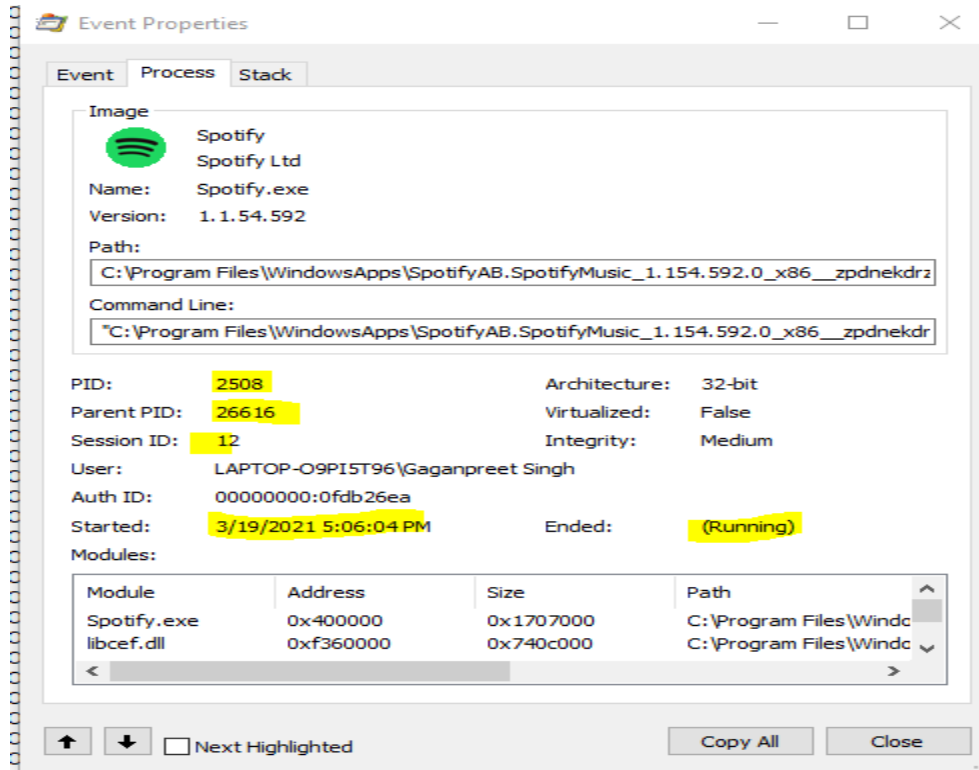


- Process tab provides information about the process that generated the event. Process Tab is useful to get information about the specific process that generated a specific event like PID, Parent PID, Session ID, Auth ID etcetera and the time when event started especially if it is something that happened very quickly and then disappeared from the process list. This way the

data

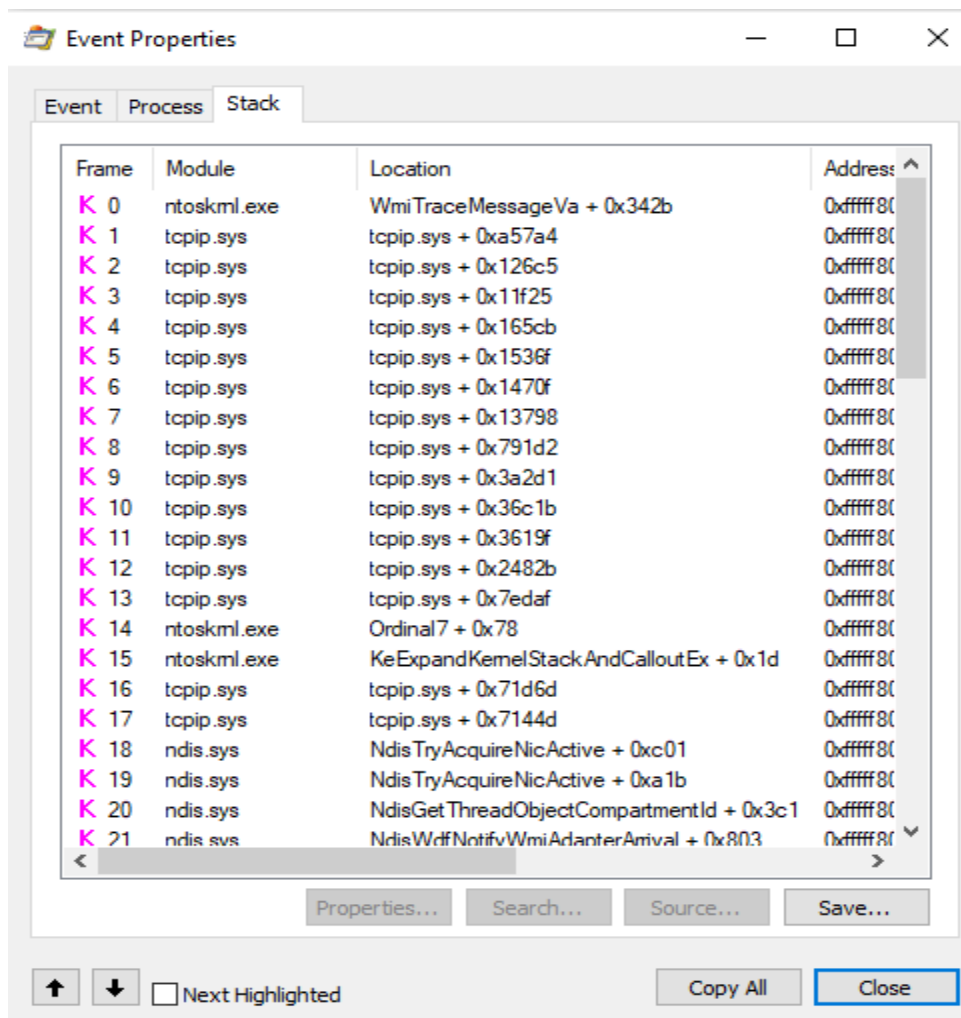
is

captured.

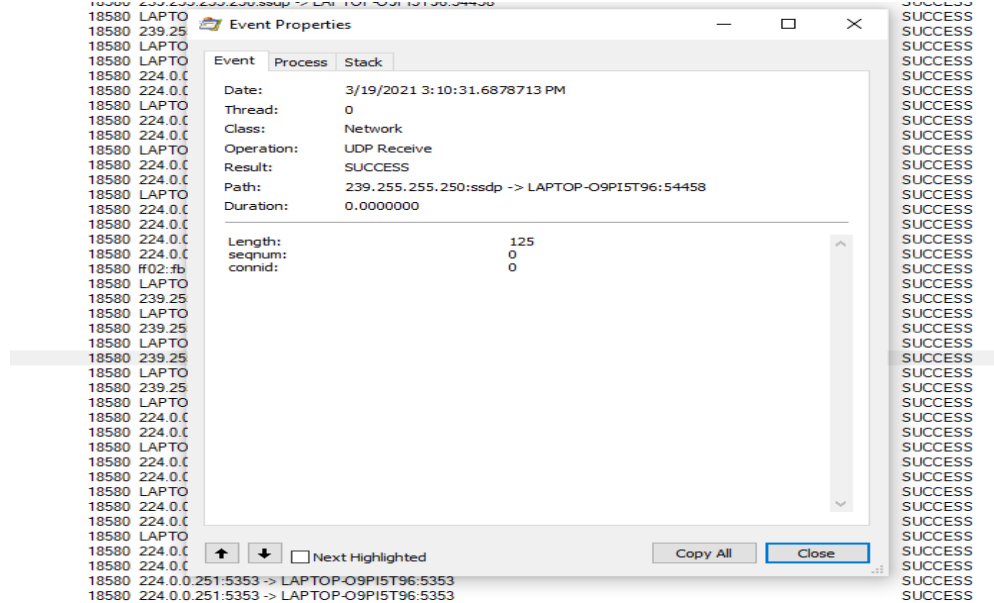


- Now Navigate to Stack tab, which can be useful, because we can troubleshoot events by examining the Module column for anything that doesn't look quite right.

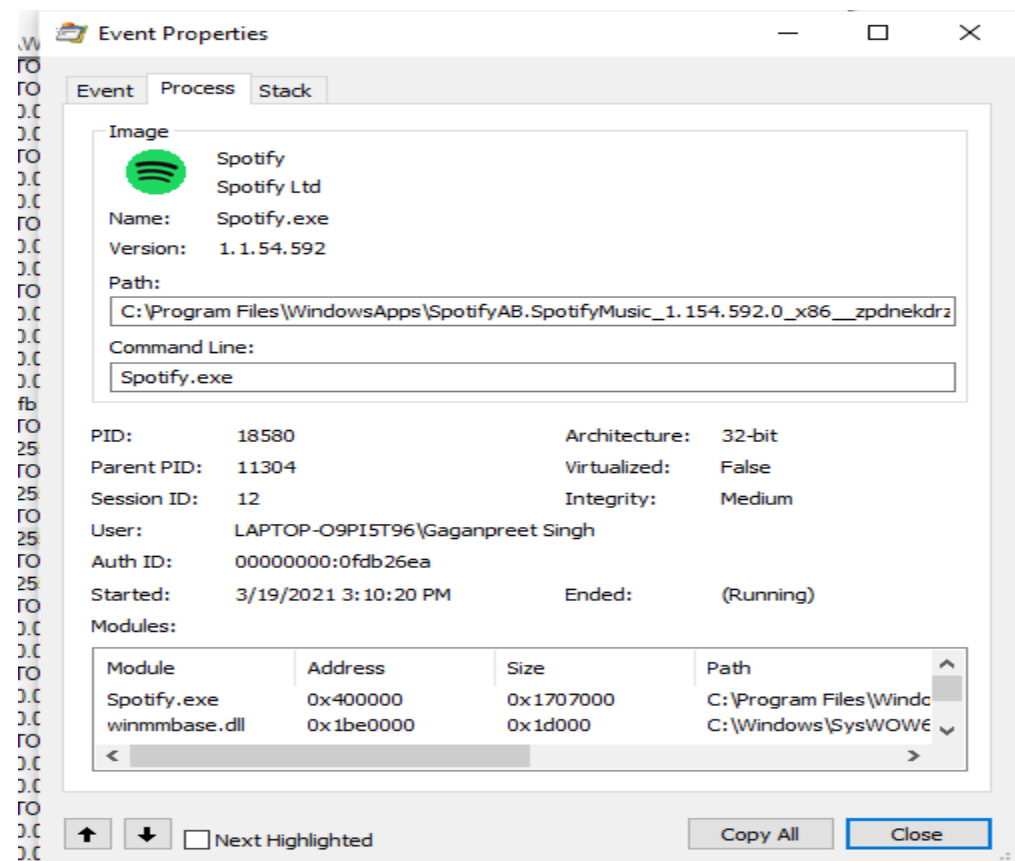
As an example, imagine that a process was constantly trying to question or access a file that doesn't exists. For this, you can look into the Stack tab and see if there were any modules that doesn't look right, and then research them. You might find an out-of-date component, or even malware, which is causing the problem.



- Let's analyze another Network event naming 18580 and sequence number 658. The operation performed in this event was successful and operation was UDP receive.



- The Process tab provide information in more details as explained in the above event.

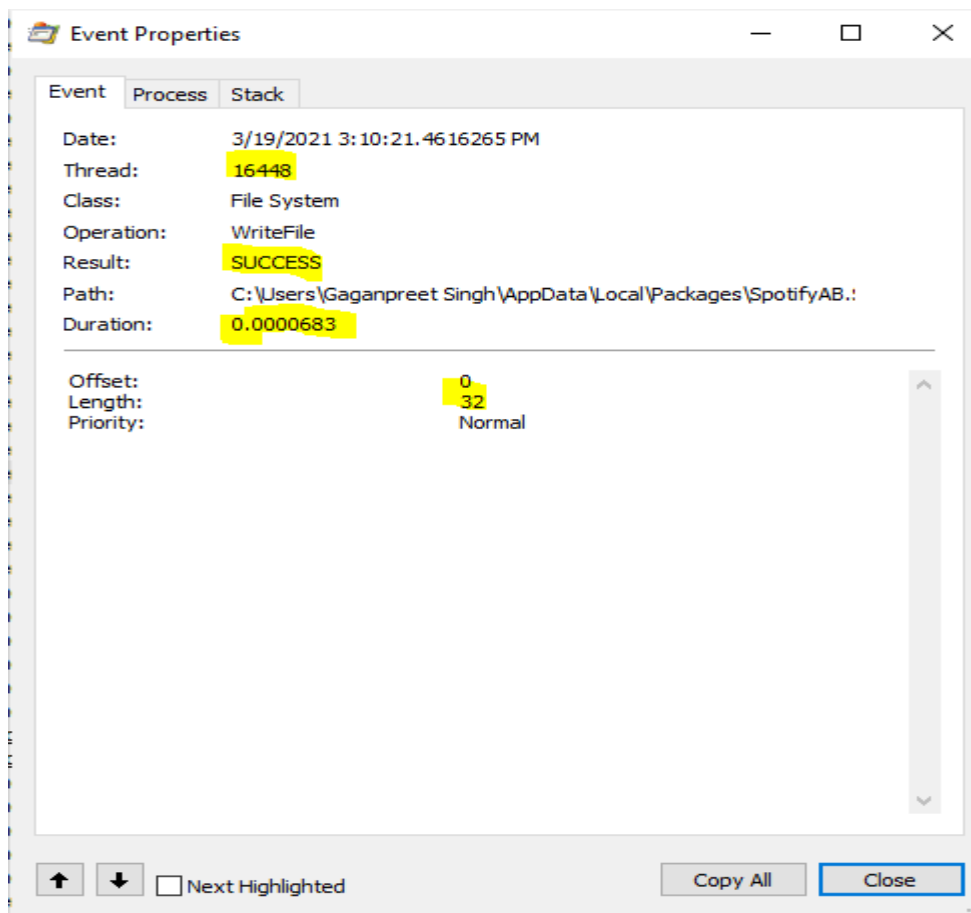


Step 7: Now we will analyze what changes are made by **File System** event class processes.

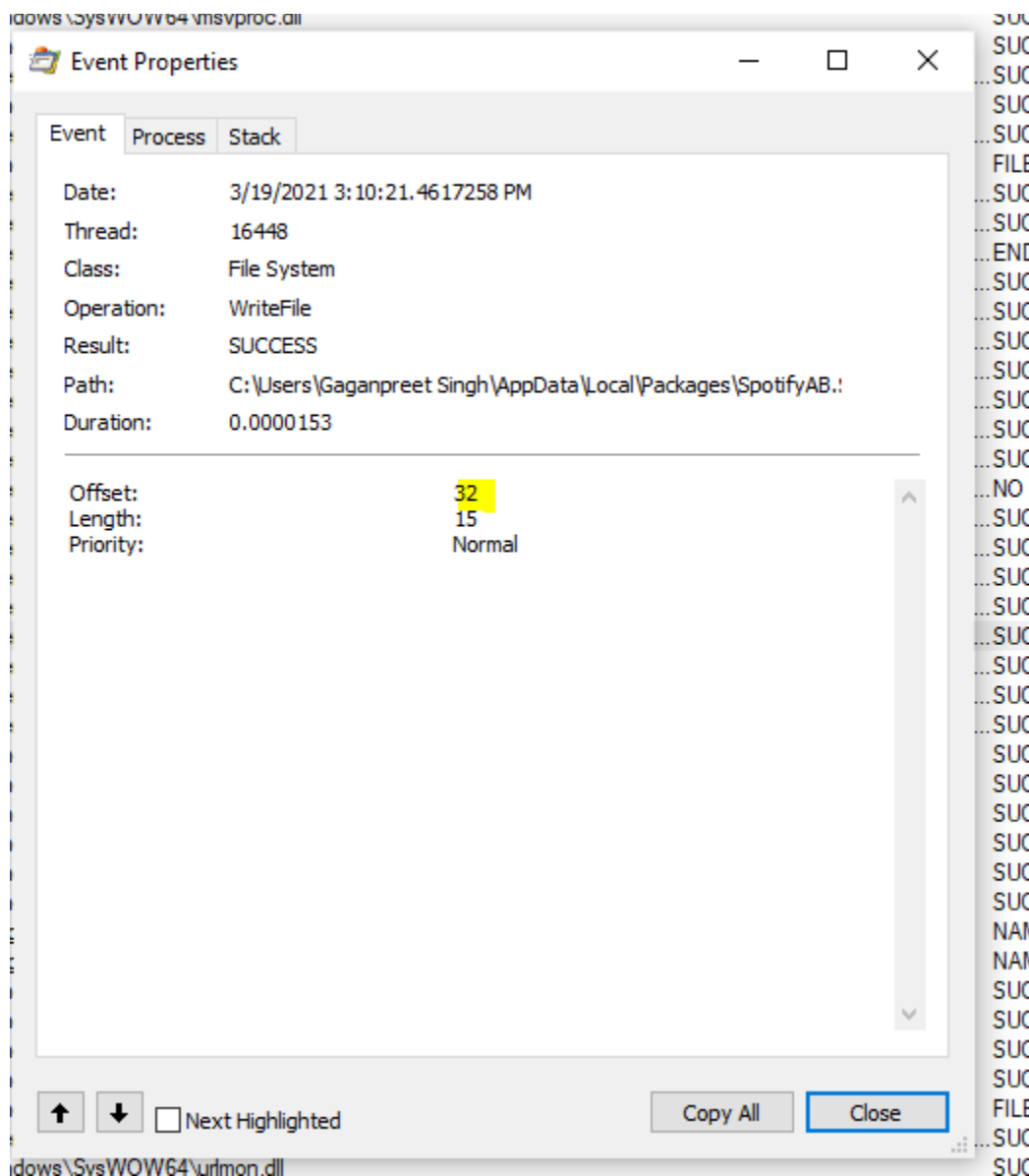
A total of 29518 events sequence were captured for file system event class. 26163 events were resulting as success where other remaining had problems like buffer overflow, end of file, privilege not found, path not found, name not found etcetera.

The events which were successful had operations like Create file, read file, close file, create file mapping, query basic information, write file etcetera.

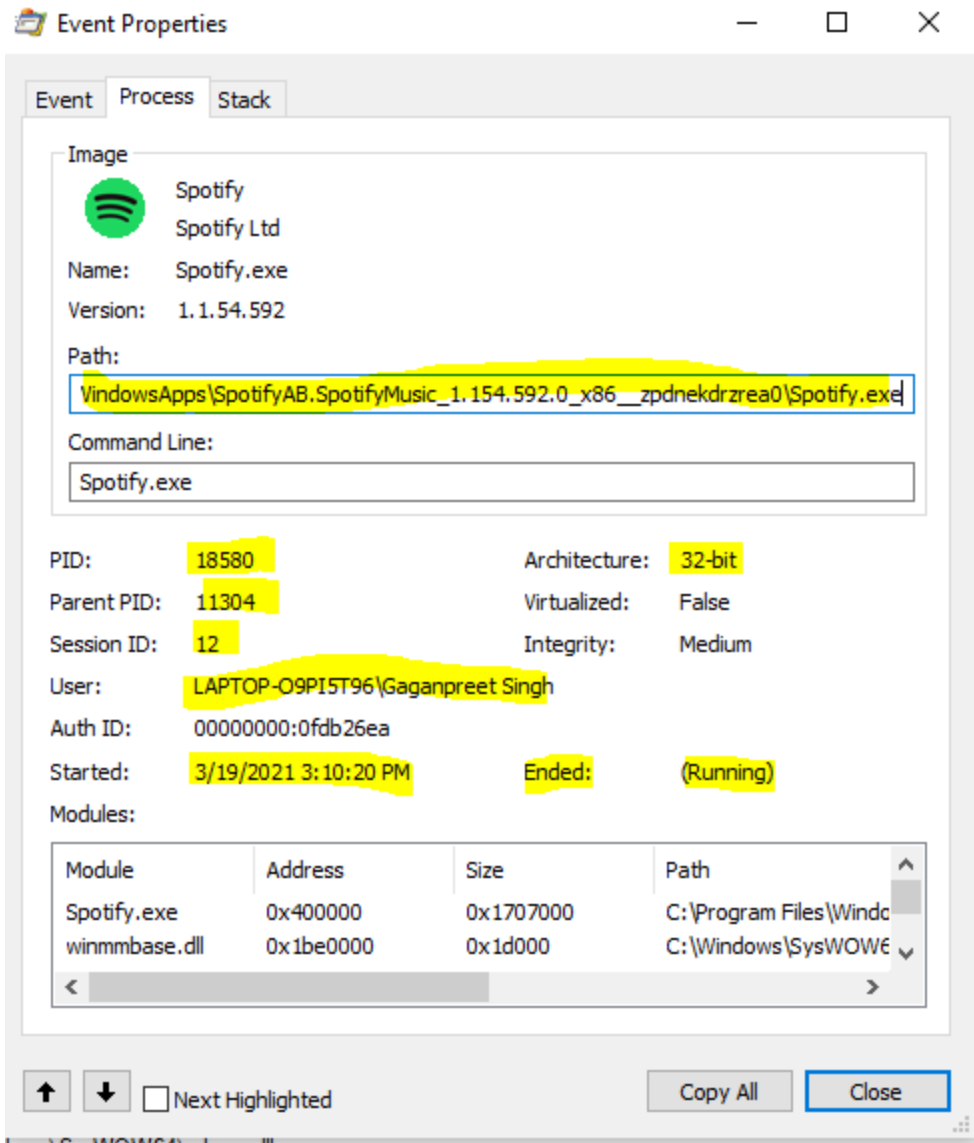
- Now we will have a look at an event with Write file operation and what changes it does to the system. The event tab shows the thread number is 16448 for the event, the duration of the file is shown and operation performed is WriteFile for the file in the location **C:\Users\Gaganpreet Singh\AppData\Local\Packages\SpotifyAB.SpotifyMusic\_zpdnekdrzrea0\LocalState\Spotify\public ldb\MANIFEST-000002**.



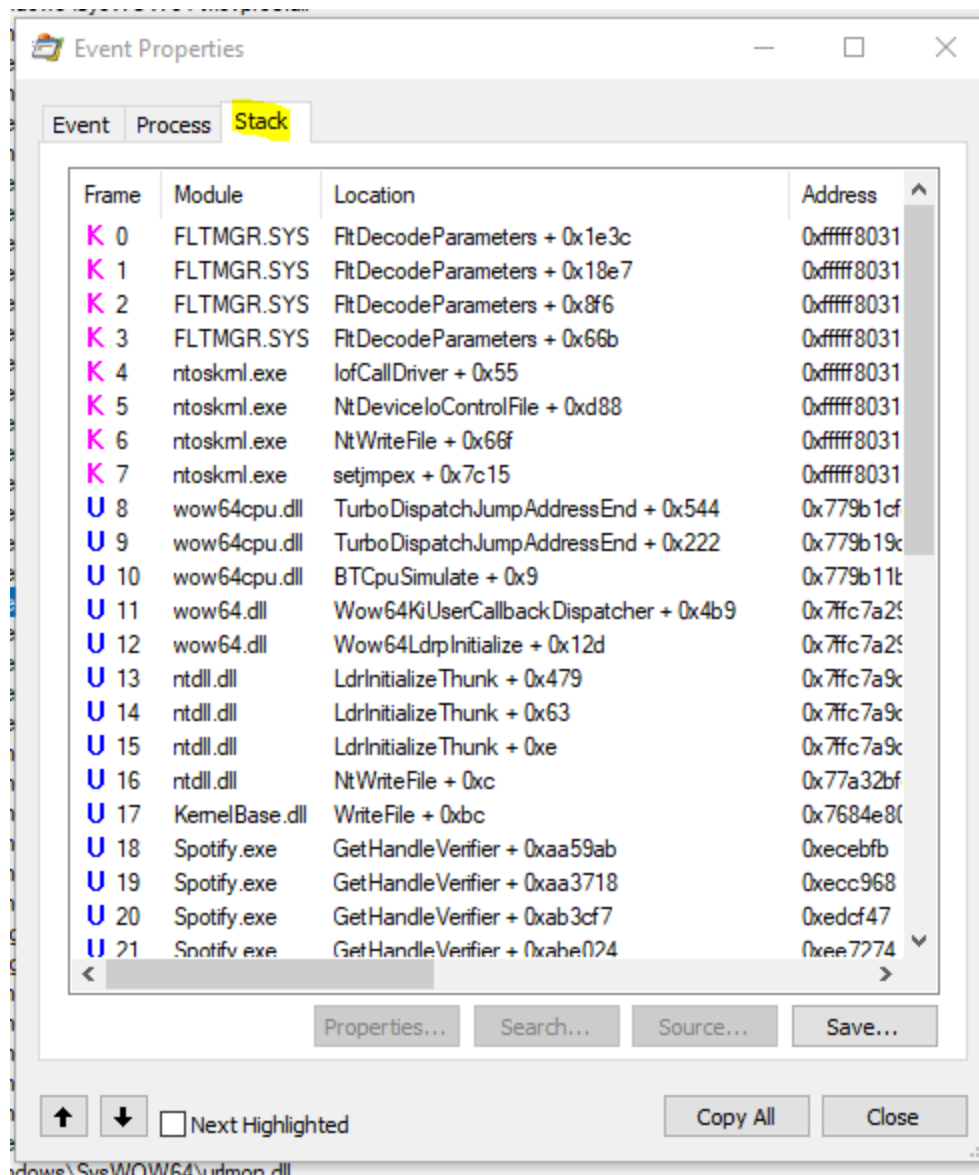
Offset means the file before writing was empty and length means the number of characters that are added in the file during the write operation. The priority of the file here is normal. In the next event write operation we can see the offset begins from 32 which means the write operation starts after 32 characters.



- Similarly Process Tab provide more detailed information for the running event like PID, Path of the file for which operation is performed and the status of the event with other important information.

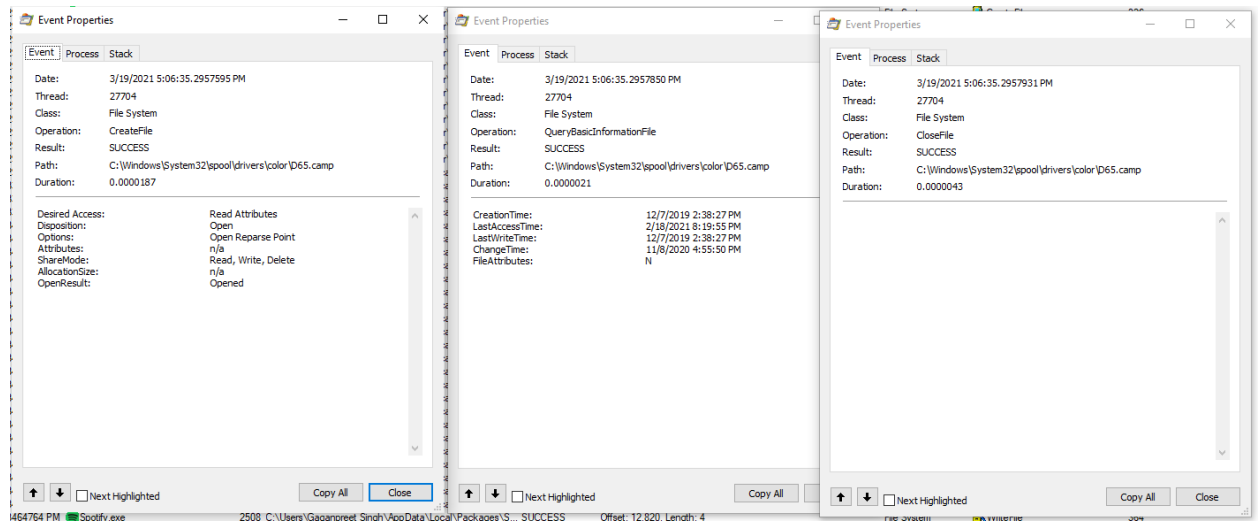


- Now Navigate to Stack tab, which can be useful, because we can troubleshoot events by examining the Module column for anything that doesn't look quite right.





**Clicking in the Spotify application at 5:06:35 pm to play the song raised the events related to FILE SYSTEM as shown in the images below.**



We will study process 26616 with sequence number 320, 321 and 322.

**Operations performed were CreateFile, QueryBasicInformationFile and CloseFile and all were successful.**

- **CreateFile Event created file with read attributes having read, write and delete sharing mode with the file location "C:\Windows\System32\spool\drivers\color\D65.camp".**
- **QueryBasicInformationFile event tell about creation time, lastAccess time, Last write time and change time of the file stored in the location "C:\Windows\System32\spool\drivers\color\D65.camp".**
- **CloseFile event explains the file was closed successfully.**

Step 8: Now we will analyze what changes are made by **Registry** event class processes.

Registry events deals with operations related to profiles of user, applications installed on the computer and deals with events related to settings, options of software installed on the windows operating system.

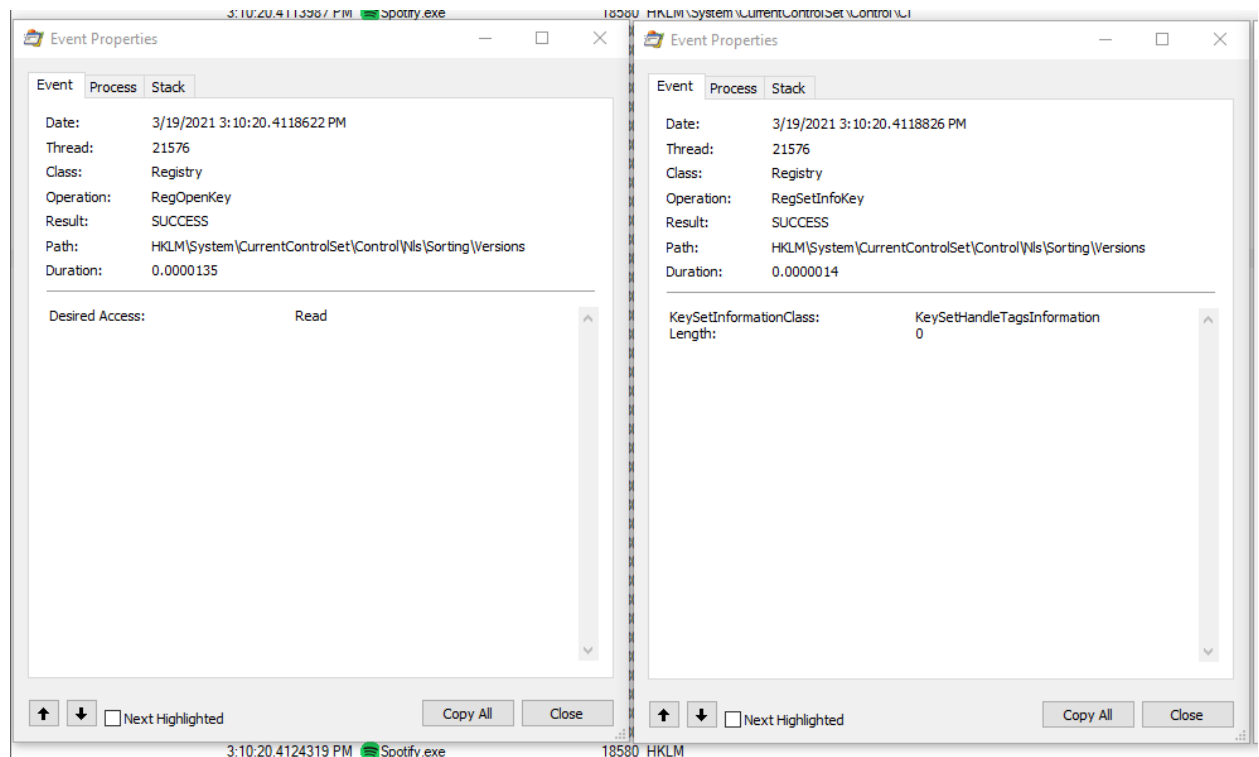
A total of 17986 events sequence were captured for registry event class. 16963 events were resulting as success where other remaining had problems like buffer overflow, buffer too small, name not found, access denied, rephrase etcetera.

The events which were successful had operations like RegOpenKey, RegCloseKey, RegQueryValue, RegSetValue etcetera.

Now, we will have a look at event sequence 205 to 209.

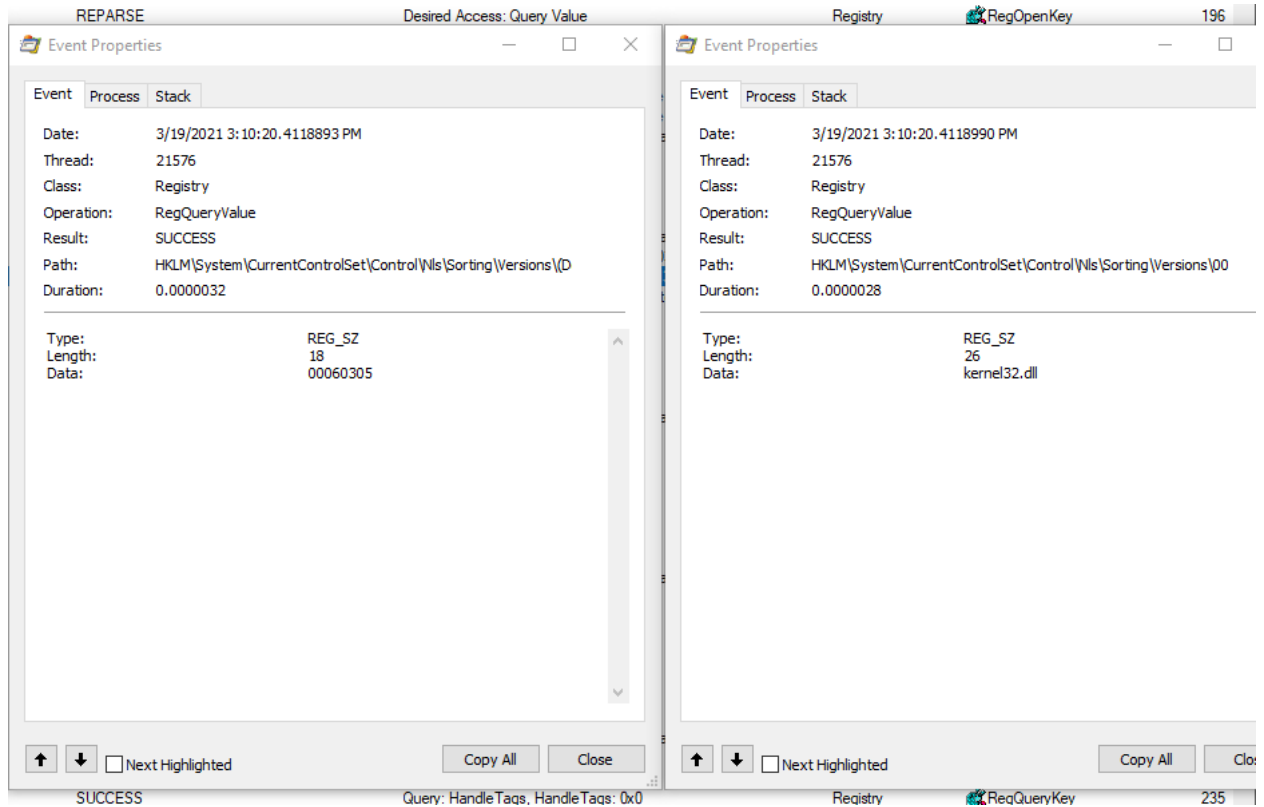
In These events we can see the operation was RegOpenKey whose Desired access was read for event sequence 205 which was successful.

For event 206 Operation was RegSetInfoKey which was also a success.



For event 208 and 209, operation was RegQueryValue and both were successful and the type of operation was REG\_SZ and length of the queryValue was 18 and 26. REG\_SZ is a windows header file and a null terminated string which can either be a UNICODE or an ANSI string.

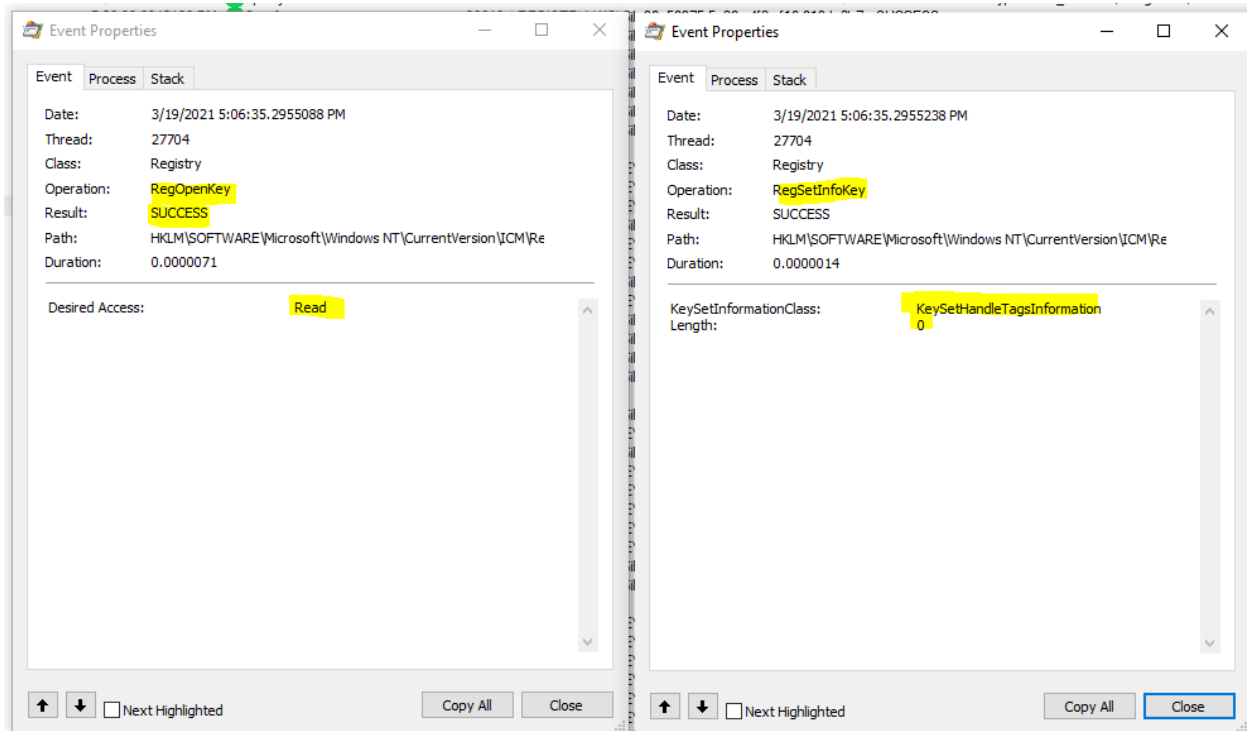
Both Operations were successful.



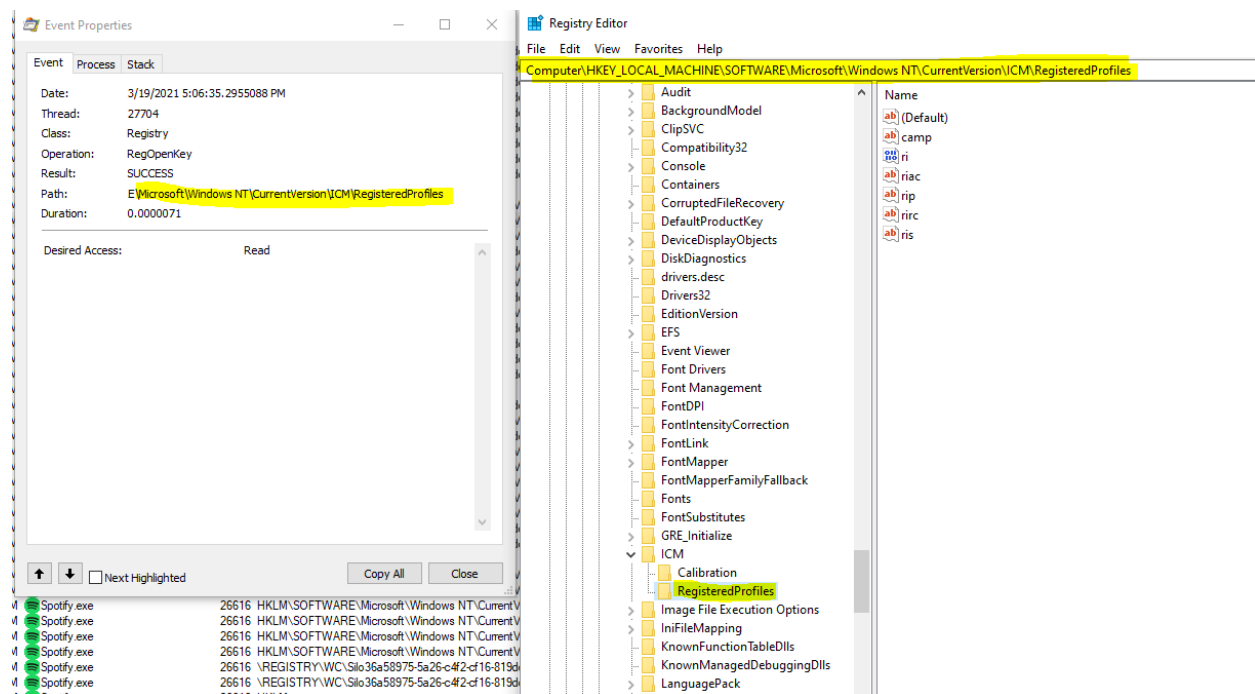
**Clicking in the Spotify application at 5:06:35 pm to play the song raised the registry events as shown in the images below.**

5:06:35.2954404 PM	Spotify.exe	26616	\REGISTRY\WC\Silo36a58975-5a26-c42d-16-819dc0b7...	SUCCESS	Query: HandleTags, HandleTags: 0x0	Registry	1RegQueryKey	900
5:06:35.2954530 PM	Spotify.exe	26616	\REGISTRY\WC\Silo36a58975-5a26-c42d-16-819dc0b7...	NAME NOT FO...	Desired Access: Read	Registry	1RegOpenKey	901
5:06:35.2954747 PM	Spotify.exe	26616	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0	Registry	1RegQueryKey	902
5:06:35.2954835 PM	Spotify.exe	26616	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersio...	0x368	Desired Access: Read	Registry	1RegOpenKey	903
5:06:35.2955088 PM	Spotify.exe	26616	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersio...	SUCCESS	Desired Access: Read	Registry	1RegOpenKey	904
5:06:35.2955238 PM	Spotify.exe	26616	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersio...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	Registry	1RegSetInfoKey	905
5:06:35.2955320 PM	Spotify.exe	26616	\REGISTRY\WC\Silo36a58975-5a26-c42d-16-819dc0b7...	SUCCESS	Query: HandleTags, HandleTags: 0x0	Registry	1RegQueryKey	906
5:06:35.2955326 PM	Spotify.exe	26616	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersio...	BUFFER OVERF...	Length: 12	Registry	1RegQueryValue	907
5:06:35.2955415 PM	Spotify.exe	26616	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersio...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0	Registry	1RegQueryValue	908
5:06:35.2955438 PM	Spotify.exe	26616	\REGISTRY\WC\Silo36a58975-5a26-c42d-16-819dc0b7...	SUCCESS	Query: Name	Registry	1RegQueryKey	909
5:06:35.2955516 PM	Spotify.exe	26616	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersio...	SUCCESS	Query: HandleTags, HandleTags: 0x0	Registry	1RegCloseKey	910
5:06:35.2955561 PM	Spotify.exe	26616	\REGISTRY\WC\Silo36a58975-5a26-c42d-16-819dc0b7...	SUCCESS	Query: HandleTags, HandleTags: 0x0	Registry	1RegQueryKey	911
5:06:35.2955687 PM	Spotify.exe	26616	\REGISTRY\WC\Silo36a58975-5a26-c42d-16-819dc0b7...	SUCCESS	Desired Access: Read	Registry	1RegOpenKey	912
5:06:35.2955755 PM	Spotify.exe	26616	\REGISTRY\WC\Silo36a58975-5a26-c42d-16-819dc0b7...	NAME NOT FO...	Desired Access: Read	Registry	1RegOpenKey	913
5:06:35.2955889 PM	Spotify.exe	26616	\REGISTRY\WC\Silo36a58975-5a26-c42d-16-819dc0b7...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	Registry	1RegSetInfoKey	914
5:06:35.2955918 PM	Spotify.exe	26616	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0	Registry	1RegQueryKey	915
5:06:35.2955994 PM	Spotify.exe	26616	\REGISTRY\WC\Silo36a58975-5a26-c42d-16-819dc0b7...	NAME NOT FO...	Length: 16	Registry	1RegQueryValue	916
5:06:35.2956033 PM	Spotify.exe	26616	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersio...	0x368	Desired Access: Read	Registry	1RegOpenKey	917
5:06:35.2956116 PM	Spotify.exe	26616	\REGISTRY\WC\Silo36a58975-5a26-c42d-16-819dc0b7...	SUCCESS	Desired Access: Read	Registry	1RegCloseKey	918
5:06:35.2956216 PM	Spotify.exe	26616	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersio...	SUCCESS	Desired Access: Read	Registry	1RegOpenKey	919
5:06:35.2956321 PM	Spotify.exe	26616	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersio...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0	Registry	1RegSetInfoKey	920
5:06:35.2956386 PM	Spotify.exe	26616	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersio...	BUFFER OVERF...	Length: 12	Registry	1RegQueryValue	921

Process number 26616 with event sequence 903 and 904 performed below functions, in the **local machine registry** under software tab which performed successful read operation and KeySetHandleTagsInformation operation of length 0.



Below show the location for which read operation was performed..



### 3. References

- <https://www.howtogeek.com/school/sysinternals-pro/lesson4/>
- [https://en.wikipedia.org/wiki/Process\\_Monitor](https://en.wikipedia.org/wiki/Process_Monitor)