

Kapabilities - 1

Write up by:

John Antone

835 COS

854 CPT

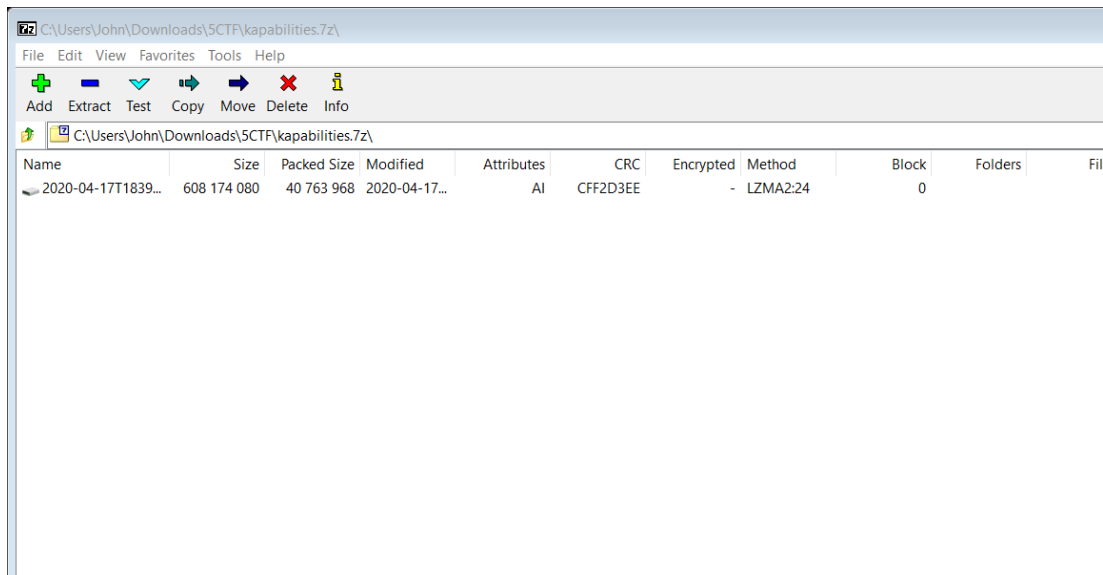
Kapabilities 1

50

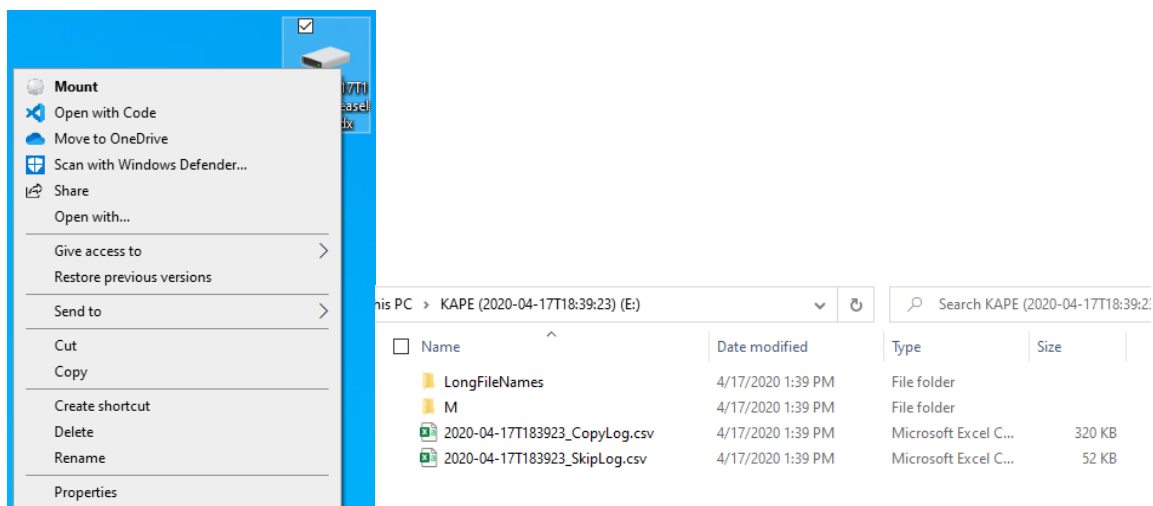
You can solve these challenges by downloading the Kape forensic capture at [this link](#).

What is the hostname of the machine?

After getting the file the first thing, we need to do is to extract it with 7zip or WinRAR.



Once the File is extracted on a windows system we can right click and mount the drive to browse the contents.



In this drive we have the M folder which contains basically the C drive of a windows pc. The excel files are created from the KAPE tool and the long file names contains a list of files that are over a certain number of characters (most likely 256).

Let's start off by jumping into the Event logs in the following location:

E:\M\Windows\system32\winevt\logs

Open up the System logs to get the first flag.

> Windows > system32 > winevt > logs

□ Name

- Microsoft-Windows-Health%4Operational.evtx
- Microsoft-Windows-WER-PayloadHealth%4Operational.evtx
- Microsoft-Windows-WFP%4Operational.evtx
- Microsoft-Windows-Windows Defender%4Operational.evtx
- Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx
- Microsoft-Windows-WindowsUpdateClient%4Operational.evtx
- Microsoft-Windows-WinNet-Config%4ProxyConfigChanged.evtx
- Microsoft-Windows-Winlogon%4Operational.evtx
- Microsoft-Windows-WinRM%4Operational.evtx
- Microsoft-Windows-WMI-Activity%4Operational.evtx
- OpenSSH%4Operational.evtx
- Security.evtx
- SMSApi.evtx
- ☒ System.evtx
- Windows PowerShell.evtx

Log Name:	System		
Source:	DistributedCOM	Logged:	12/30/2019 9:17:22 AM
Event ID:	10016	Task Category:	None
Level:	Warning	Keywords:	Classic
User:	S-1-5-21-2593535590-357514	Computer:	DESKTOP-COM08SK
OpCode:	Info		

All the events have the computer name at the bottom. Answer: Desktop-COM08SK

Kapabilities 2

50

There are three local administrators on this system. Besides assessor and Administrator, what is the name of the third account?

For this one go back to File Explorer and go to the following location: E:\M\users

C > KAPE (2020-04-17T18:39:23) (E:) > M > users			Search use
□ Name	Date modified	Type	
assessor	4/17/2020 1:39 PM	File folder	
Default	4/17/2020 1:39 PM	File folder	
Silver Smurfer	4/17/2020 1:39 PM	File folder	

We will see three accounts here:

Answer: Silver Smurfer

Kapabilities 3

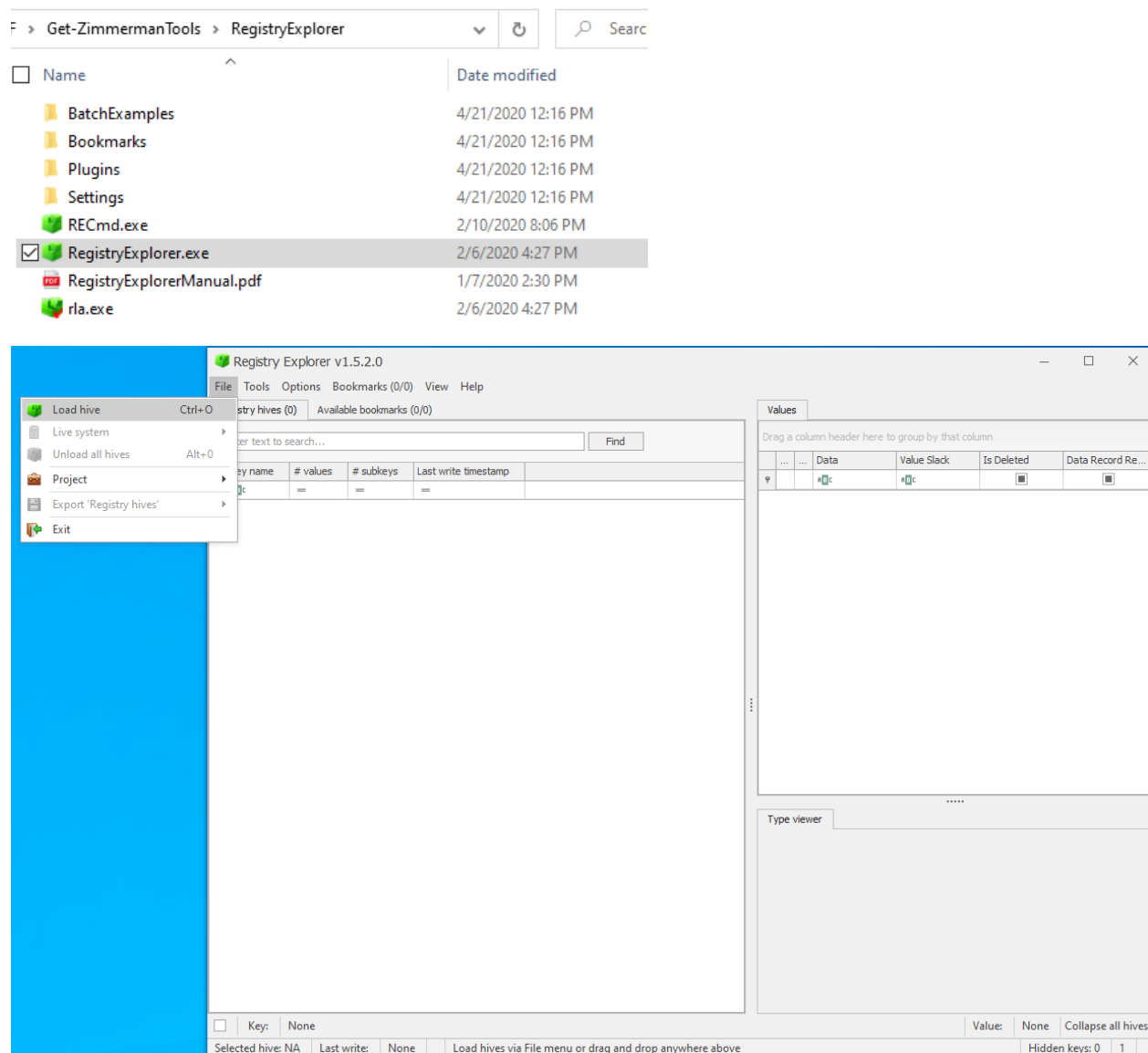
100

Silver Smurfer accessed a suspicious website. What is the website URL?

For this next one we are going to look at the ntuser.dat file for Silver Smurfer, to do this we need a tool from Eric Zimmerman: <https://ericzimmerman.github.io/#!index.md>

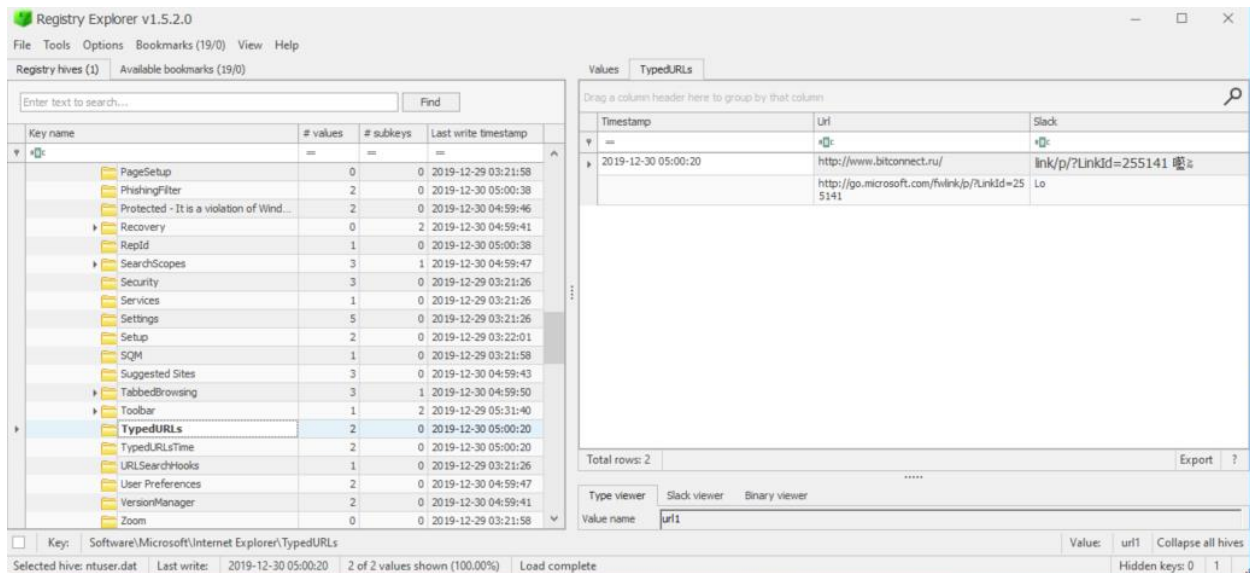
I would grab the script to install the tools as we will need a few others for later questions.

For this one in particular we are going to run the RegistryExplorer



We will load the ntuser.dat file which is the HKUser hive for Silver Smurfer.

The registry key we are looking for is under ROOT\Software\Microsoft\Internet Explorer\TypedURLs



We see that since they used Internet Explorer, we have their history and the answer to this question.

Answer: <http://www.bitconnect.ru>

Kapabilities 4

79

A malicious executable was executed on this system and appears to be attempting to masquerade as a legitimate Windows component. What is the name of the malicious process?

For this one we will go back to the event logs. For this we will use Zimmermans EvtxECmd.exe command.

This will read all the event logs and put it into a CSV file that will make it easier to parse the results.

From the folder of EvtxECmd.exe run the following command: `.\EvtxECmd.exe -d E:\M\Windows\system32\winevt\logs\ --csv c:\temp\zimmerman`

This will read all the log files from the drive and output to `c:\temp\zimmerman\<date>_EvtxECmd_Output.csv`

RecordNu	EventID	Time	Created	Level	Provider	Channel	ProcessId	ThreadId	Computer	UserId	MapDescr	ChunkNur	UserNam	RemoteH	PayloadDi	PayloadDi	PayloadDi	PayloadDi	PayloadDi	Executabl	SourceFil	Payload
1	357	557	17:38.6	6000	4 Microsoft-Windows-Winlogon	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
2	558	558	17:39.0	6000	4 Microsoft-Windows-Winlogon	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
3	559	559	17:39.4	1532	4 Microsoft-Windows-User Profiles Service	Application	1200	1292	DESKTOP-5-1-5-18	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
4	560	560	17:57.7	1531	4 Microsoft-Windows-User Profiles Service	Application	1092	1128	DESKTOP-5-1-5-18	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
5	561	561	17:58.4	4625	4 Microsoft-Windows-EventSystem	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
6	562	562	18:01.0	5615	4 Microsoft-Windows-WMI	Application	1636	2132	DESKTOP-5-1-5-18	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
7	563	563	18:02.2	5617	4 Microsoft-Windows-WMI	Application	1636	2180	DESKTOP-5-1-5-18	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
8	564	564	18:05.1	6003	4 Microsoft-Windows-Winlogon	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
9	565	565	18:06.7	6000	4 Microsoft-Windows-Winlogon	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
10	566	566	18:12.8	102	4 ESENT	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
11	567	567	18:12.9	105	4 ESENT	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
12	568	568	18:13.6	330	4 ESENT	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
13	569	569	18:13.6	641	4 ESENT	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
14	570	570	18:13.7	326	4 ESENT	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
15	571	571	18:14.5	1003	4 Microsoft-Windows-Search	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
16	572	572	18:15.9	900	4 Microsoft-Windows-Security-SP	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
17	573	573	18:16.1	16394	4 Microsoft-Windows-Security-SP	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
18	574	574	18:16.3	1066	4 Microsoft-Windows-Security-SP	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
19	575	575	18:17.1	1003	4 Microsoft-Windows-Security-SP	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
20	576	576	18:17.3	902	0 Microsoft-Windows-Security-SP	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
21	577	577	18:50.2	1003	4 Microsoft-Windows-Security-SP	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
22	578	578	18:50.8	1003	4 Microsoft-Windows-Security-SP	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
23	579	579	18:50.9	8198	2 Microsoft-Windows-Security-SP	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
24	580	580	27:16.9	4625	4 Microsoft-Windows-EventSystem	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
25	581	581	27:16.8	1531	4 Microsoft-Windows-User Profiles Service	Application	1036	1108	DESKTOP-5-1-5-18	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
26	582	582	27:18.7	5615	4 Microsoft-Windows-WMI	Application	2080	2188	DESKTOP-5-1-5-18	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
27	583	583	27:21.2	5611	4 Microsoft-Windows-WMI	Application	2080	2276	DESKTOP-5-1-5-18	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
28	584	584	27:22.2	5617	4 Microsoft-Windows-WMI	Application	2080	2276	DESKTOP-5-1-5-18	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
29	585	585	27:24.6	900	4 Microsoft-Windows-Security-SP	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
30	586	586	27:25.4	6003	4 Microsoft-Windows-Winlogon	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
31	587	587	27:25.6	16394	4 Microsoft-Windows-Security-SP	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
32	588	588	27:25.7	1066	4 Microsoft-Windows-Security-SP	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
33	589	589	27:25.7	8225	3 Microsoft-Windows-Security-SP	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
34	590	590	27:26.1	6000	4 Microsoft-Windows-Winlogon	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
35	591	591	27:26.6	1034	4 Microsoft-Windows-Security-SP	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
36	592	592	27:26.7	1034	4 Microsoft-Windows-Security-SP	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		
37	593	593	27:26.8	1034	4 Microsoft-Windows-Security-SP	Application	0	0	DESKTOP-COM0B8SK	0	0	0	0	0	0	0	0	0	0	E:\M\Win ("Even		

From here click on a cell and do Control + A to select all and go to insert Table with headers. This will make filter take no time at all.

First Filter Channel -> deselect all and select only Security

Next Filter EventID -> deselect all and select 4688 or New Process Creation

Next we will go to Column V: ExecutableInfo Click on V to highlight the whole column -> Insert -> Pivot Table -> Dump the column into a new sheet. This will give us a unique list of all processes started.

Row Labels
4 \SystemRoot\System32\drivers\e1i65x64.sys
5 C:\Program Files\WindowsApps\Microsoft.SkypeApp_14.35.152.0_x64__kzf8qxf38zg5c\SkypeBackgroundHost.exe
6 C:\Program Files\WindowsApps\Microsoft.WindowsStore_11811.1001.18.0_x64__8wekyb3d8bbwe\WinStore.App.exe
7 C:\Program Files\WindowsApps\Microsoft.XboxGamingOverlay_2.26.14003.0_x64__8wekyb3d8bbwe\GameBar.exe
8 C:\Users\Silver Smurfer\AppData\Local\Microsoft\OneDrive\OneDrive.exe
9 C:\Users\Silver Smurfer\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe
10 C:\Users\Silver Smurfer\AppData\Local\Temp\Issas.exe
11 C:\Users\Silver Smurfer\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\FirefoxAnalyzer.exe
12 C:\Windows\explorer.exe
13 C:\Windows\ImmersiveControlPanel\SystemSettings.exe
14 C:\Windows\regedit.exe
15 C:\Windows\System32\ApplicationFrameHost.exe
16 C:\Windows\System32\audiogd.exe
17 C:\Windows\System32\autochk.exe
18 C:\Windows\System32\backgroundTaskHost.exe
19 C:\Windows\System32\browser_broker.exe
20 C:\Windows\System32\ClipRenew.exe
21 C:\Windows\System32\cmd.exe
22 C:\Windows\System32\CompatTelRunner.exe
23 C:\Windows\System32\conhost.exe
24 C:\Windows\System32\consent.exe
25 C:\Windows\System32\control.exe
26 C:\Windows\System32\csrss.exe
27 C:\Windows\System32\ctfmon.exe
28 C:\Windows\System32\dasHost.exe
29 C:\Windows\System32\DeviceCensus.exe
30 C:\Windows\System32\dllhost.exe
31 C:\Windows\System32\drvinst.exe
32 C:\Windows\System32\dwm.exe
33 C:\Windows\System32\dxgiadaptercache.exe
34 C:\Windows\System32\find.exe
35 C:\Windows\System32\fontdrvhost.exe
36 C:\Windows\System32\ipconfig.exe
37 C:\Windows\System32\LogonUI.exe
38 C:\Windows\System32\lsass.exe

We look at Silver Smurfer we can see that there is an odd looking Issas.exe file launched from there.

Answer: Issas.exe

Kapabilities 5

50

What is the full path to Issas.exe's parent process?

For this one we will go back to the main sheet in our event log dump.

We will filter out the Column V for Issas.exe executable that we found and the answer jumps out.

PayloadData1	ExecutableInfo
Parent process: C:\Windows\System32\cmd.exe	C:\Users\Silver Smurfer\AppData\Local\Temp\Issas.exe
Parent process: C:\Windows\System32\cmd.exe	C:\Users\Silver Smurfer\AppData\Local\Temp\Issas.exe
Parent process: C:\Windows\System32\cmd.exe	C:\Users\Silver Smurfer\AppData\Local\Temp\Issas.exe
Parent process: C:\Windows\System32\cmd.exe	C:\Users\Silver Smurfer\AppData\Local\Temp\Issas.exe
Parent process: C:\Windows\System32\cmd.exe	C:\Users\Silver Smurfer\AppData\Local\Temp\Issas.exe
Parent process: C:\Windows\System32\cmd.exe	C:\Users\Silver Smurfer\AppData\Local\Temp\Issas.exe
Parent process: C:\Windows\System32\cmd.exe	C:\Users\Silver Smurfer\AppData\Local\Temp\Issas.exe
Parent process: C:\Windows\System32\cmd.exe	C:\Users\Silver Smurfer\AppData\Local\Temp\Issas.exe

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

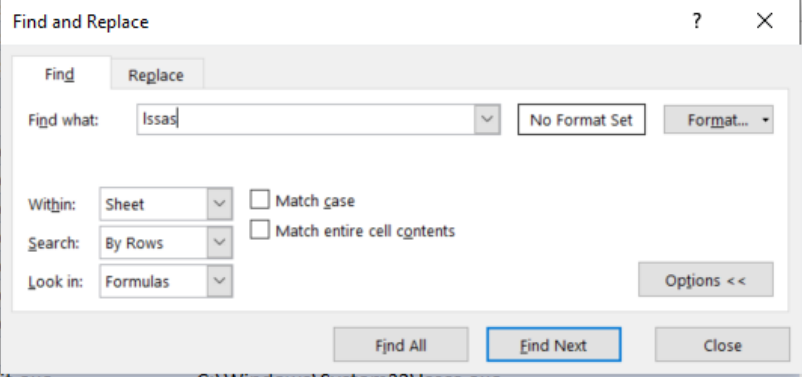
Kapabilities 6

50

What two processes were launched by cmd.exe immediately before Issas.exe? (format: file.exe,file.exe)

For this remove the filter for Issas.exe from question 5. Do a search for Issas and look at the events surrounding the search.

Parent process: C:\windows\system32\control.exe	C:\windows\system32\inetplwiz.exe
Parent process: C:\Windows\System32\services.exe	C:\Windows\System32\svchost.exe
Parent process: C:\Windows\System32\svchost.exe	C:\Windows\System32\consent.exe
Parent process: C:\Windows\System32\control.exe	C:\Windows\System32\Netplwiz.exe
Parent process: C:\Windows\System32\cmd.exe	C:\Windows\System32\tasklist.exe
Parent process: C:\Windows\System32\cmd.exe	C:\Windows\System32\find.exe
Parent process: C:\Windows\System32\cmd.exe	C:\Users\Silver Smurfer\AppData\Local\Temp\Issas.exe
Parent process: C:\Windows\System32\winlogon.exe	C:\Windows\System32\wlrmr.exe
Parent process: C:\Windows\System32\svchost.exe	C:\Windows\System32\taskhostw.exe
Parent process: C:\Windows\System32\svcho	
Parent process: C:\Windows\System32\svcho	
Parent process: C:\Windows\System32\svcho	
Parent process:	
Parent process:	
Parent process: C:\Windows\System32\smss.	
Parent process: C:\Windows\System32\smss.	
Parent process: C:\Windows\System32\smss.	
Parent process: C:\Windows\System32\smss.	
Parent process: C:\Windows\System32\smss.	
Parent process: C:\Windows\System32\smss.	
Parent process: C:\Windows\System32\smss.	
Parent process: C:\Windows\System32\smss.	
Parent process: C:\Windows\System32\winin	
Parent process: C:\Windows\System32\winin	



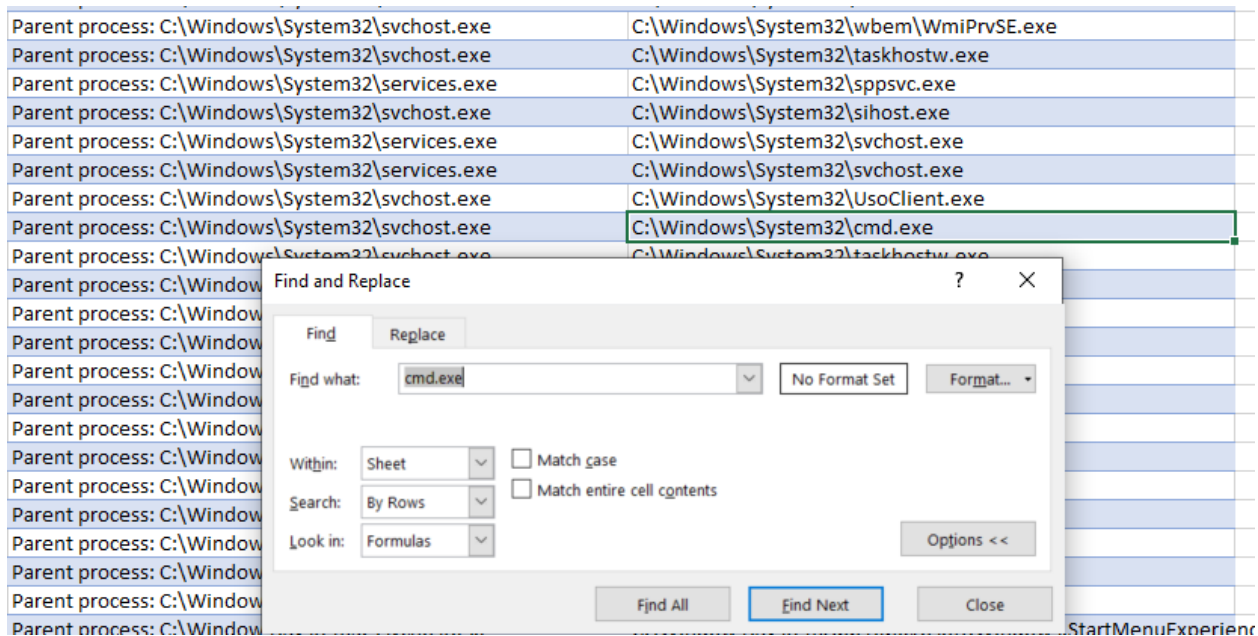
Answer: find.exe,tasklist.exe

Kapabilities 7

50

What is the full path to Issas.exe's grandparent process? (the parent of the cmd.exe process that spawned Issas.exe)

For this we will do the same as question 6, only we will look for the next instance of cmd.exe in the executable info (not the parent process).



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

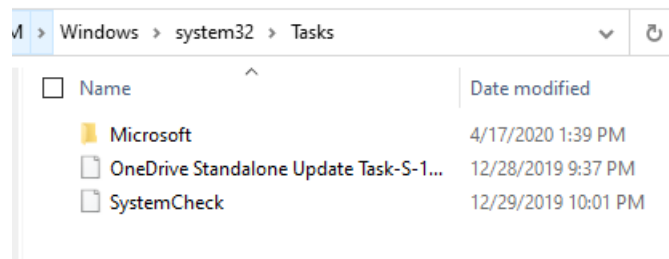
Kapabilities 8

80

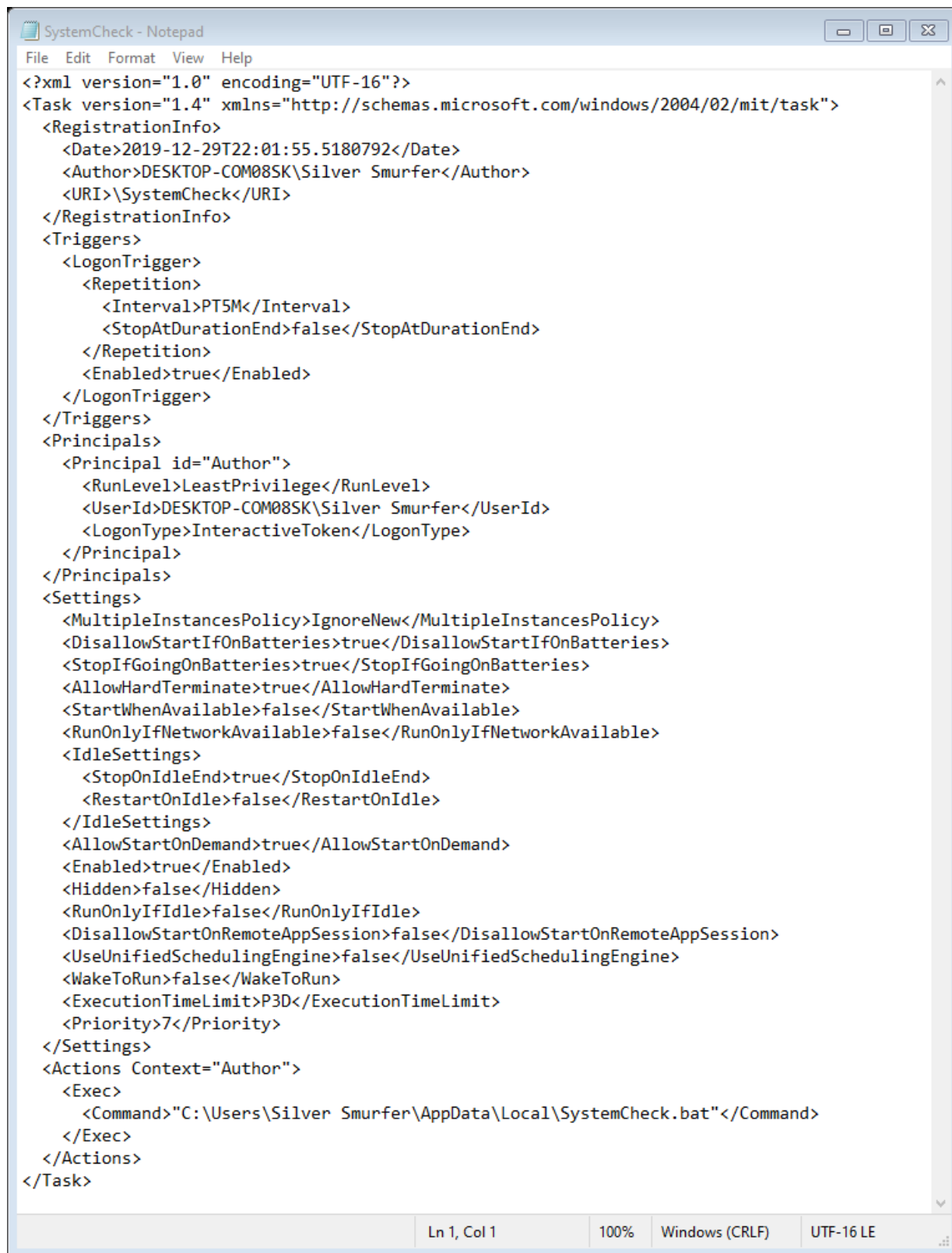
What is the name of the scheduled task Issas.exe is using for persistence? This may require a logical leap - make an educated guess.

For this question we will go back to the M drive and go to the Tasks Folder:
E:\M\Windows\system32\Tasks

Here we see a task called SystemCheck that we need to look at.



Open this up in Notepad:



```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.4" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Date>2019-12-29T22:01:55.5180792</Date>
    <Author>DESKTOP-COM08SK\Silver Smurfer</Author>
    <URI>\SystemCheck</URI>
  </RegistrationInfo>
  <Triggers>
    <LogonTrigger>
      <Repetition>
        <Interval>PT5M</Interval>
        <StopAtDurationEnd>>false</StopAtDurationEnd>
      </Repetition>
      <Enabled>>true</Enabled>
    </LogonTrigger>
  </Triggers>
  <Principals>
    <Principal id="Author">
      <RunLevel>LeastPrivilege</RunLevel>
      <UserId>DESKTOP-COM08SK\Silver Smurfer</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>
    <DisallowStartOnRemoteAppSession>>false</DisallowStartOnRemoteAppSession>
    <UseUnifiedSchedulingEngine>>false</UseUnifiedSchedulingEngine>
    <WakeToRun>>false</WakeToRun>
    <ExecutionTimeLimit>P3D</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>"C:\Users\Silver Smurfer\AppData\Local\SystemCheck.bat"</Command>
    </Exec>
  </Actions>
</Task>
```

We see that this is calling a bat file. There is a repetition check enabled so this is persistence.

Answer: SystemCheck

Kapabilities 9

79

What is the name of the network share hosted on this workstation?

For this question we will be using Zimmerman's MFTExplorer program to look at the MFT table located: E:\M

Load the \$MFT table on the M drive.

MFT Explorer v0.5.1.0

File Tools Help

Name

E:\M\SMFT

\$Extend

\$Recycle.Bin

Documents and Settings

PerfLogs

Program Files

Program Files (x86)

ProgramData

Recovery

System Volume Information

Users

Windows

Drag a column header here to group by that column

Image Icon	Name	Parent Path	Is Dir	Is Deleted	SI_Created On	FN_Created On	SI_Modified On	FN_Modified On	SI_Last Accessed	FN_La
No image data	\$Extend	.	✓	□	2019-12-29 05:...	2019-12-29 05:...	2019-12-29 05:...	2019-12-29 05:...	2019-12-29 05:02...	20
	\$Recycle.Bin	.	✓	□	2019-03-19 04:...	2019-12-29 05:...	2019-12-30 05:...	2019-12-29 05:...	2019-12-30 14:57...	20
	Documents and Settings	.	✓	□	2019-12-29 05:...	2019-12-29 05:...	2019-12-29 05:...	2019-12-29 05:...	2019-12-29 05:15...	20
	PerfLogs	.	✓	□	2019-03-19 04:...	2019-12-29 05:...	2019-03-19 04:...	2019-12-29 05:...	2019-03-19 04:52...	20
	Program Files	.	✓	□	2019-03-19 04:...	2019-12-29 05:...	2019-12-29 05:...	2019-12-29 05:...	2019-12-30 15:13...	20
	Program Files (x86)	.	✓	□	2019-03-19 04:...	2019-12-29 05:...	2019-10-07 02:...	2019-12-29 05:...	2019-12-30 15:13...	20
	ProgramData	.	✓	□	2019-03-19 04:...	2019-12-29 05:...	2019-12-30 14:...	2019-12-29 05:...	2019-12-30 15:14...	20
	Recovery	.	✓	□	2019-12-29 05:...	2019-12-29 05:...	2019-12-29 05:...	2019-12-29 05:...	2019-12-29 05:15...	20

Properties

Copied

Has ADS

Is deleted

Is directory

Possible Timestamped

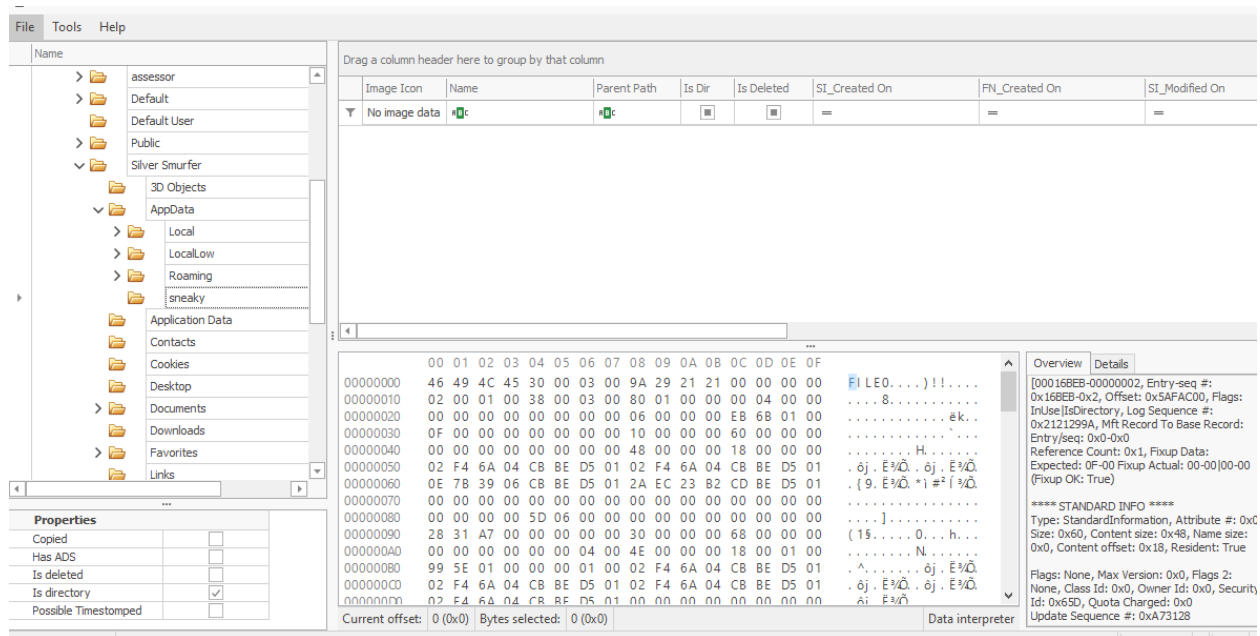
Current offset: 0 (0x0) Bytes selected: 0 (0x0)

Data interpreter

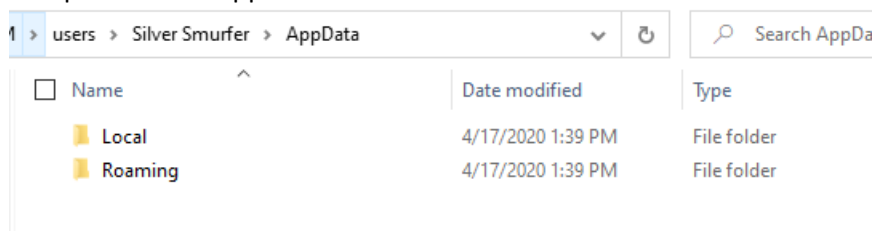
Created On: 2019-03-19

Directories 11 Files 13

Since we know that Silver Smurfer is the user we want to focus on from all the previous questions, and we have a bat file coming from their appdata folder, let's start our search there.



Compared to the appdata folder on the M drive



We see that there is a sneaky folder in there.

Answer: sneaky

Kapabilities 10 50

What is the full path to the sneaky share folder?

Sticking with question 9 we can say that the following is the path

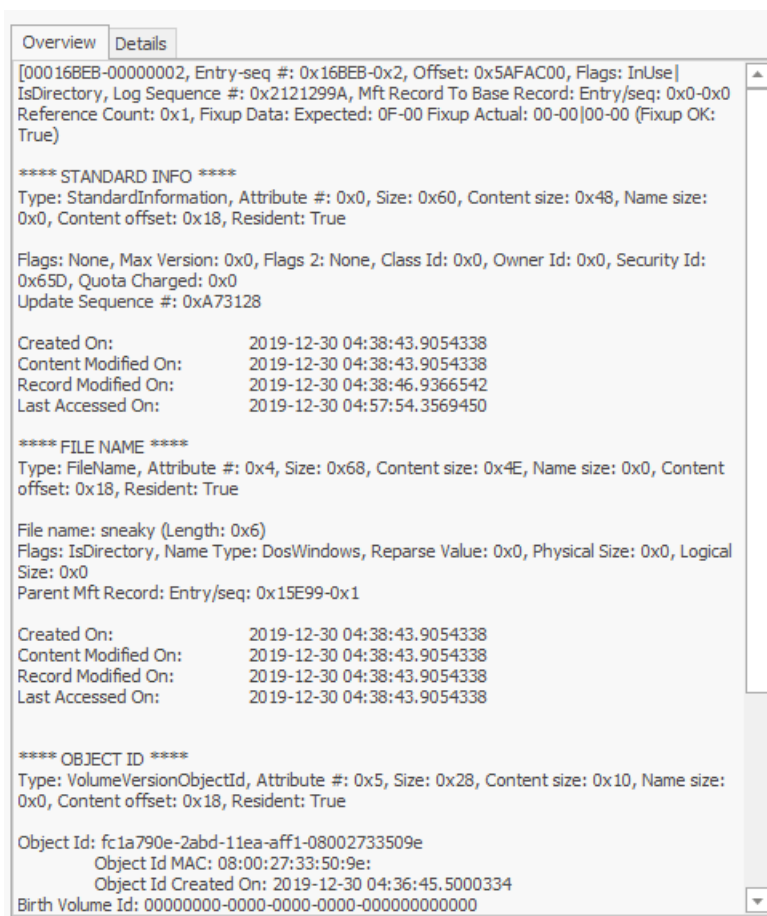
Answer: C:\users\Silver Smurfer\AppData\sneaky

Kapabilities 11

50

On what day was the C:\Users\Silver Smurfer\sneaky directory created? (format: YYYY-MM-DD)

We look on the bottom right corner to of the MFTExplorer to find this info.



Answer: 2019-12-30

Kapabilities 12

80

There is another unusual binary (besides lssas.exe) set to run automatically on this system. What is the full path to the executable?

For this one we will go back to the event log spreadsheet we had made earlier. If we look at our pivot table, we made we see there is another file running out of Silver Smurfer's Folder.

Row Labels
\SystemRoot\System32\drivers\ei165x64.sys
C:\Program Files\WindowsApps\Microsoft.SkypeApp_14.35.152.0_x64__kzf8qxf38zg5c\SkypeBackgroundHost.exe
C:\Program Files\WindowsApps\Microsoft.WindowsStore_11811.1001.18.0_x64__8wekyb3d8bbwe\WinStore.App.exe
C:\Program Files\WindowsApps\Microsoft.XboxGamingOverlay_2.26.14003.0_x64__8wekyb3d8bbwe\GameBar.exe
C:\Users\Silver Smurfer\AppData\Local\Microsoft\OneDrive\OneDrive.exe
C:\Users\Silver Smurfer\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe
C:\Users\Silver Smurfer\AppData\Local\Temp\lssas.exe
C:\Users\Silver Smurfer\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\FirefoxAnalyzer.exe
C:\Windows\explorer.exe
C:\Windows\ImmersiveControlPanel\SystemSettings.exe
C:\Windows\regedit.exe
C:\Windows\System32\ApplicationFrameHost.exe
C:\Windows\System32\audiodg.exe
C:\Windows\System32\autochk.exe
C:\Windows\System32\backgroundTaskHost.exe

Answer: C:\Users\Silver Smurfer\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\FirefoxAnalyzer.exe

Kapabilities 13

100

What is the full path to the system utility someone used to examine FireFoxAnalyzer.exe?

For this we will move to another Zimmerman tool PECmd.exe.

Run this command to dump the contents to a csv in the c:\temp location

.\PECmd.exe -d e:\M --csv c:\temp\prefetch

```
s> .\PECmd.exe -d e:\M --csv c:\temp\prefetch
```

PC > Local Disk (C:) > temp > prefetch

Name

20200421231135_PECmd_Output.csv
20200421231135_PECmd_Output_Timeline.csv

Open the Output CSV and put it into a table: Control + A -> Insert -> Table

Next we will search on Firefox and see what accessed the file.

We have two items that opened the file, Certutil.exe and firfoxanalyzer.exe

The screenshot shows a Windows File Explorer window with the address bar set to 'Local Disk (C:) > temp > prefetch'. The file list shows two CSV files. A red box highlights the file 'FIREFOXANALYZER.EXE' in the file list. Below the file list, a 'Find and Replace' dialog box is open, showing the search term 'firefox'.

SourceFilename	ExecutableName	FilesLoaded
e:\M\Windows\prefetch\AUDIODG.EXE-BDFD3029.pf	AUDIODG.EXE	\VOLUME{01d5be0528ae8f8c-1628d43c}\WINDOWS\SYS
e:\M\Windows\prefetch\BACKGROUNDTASKHOST.EXE-0C002D5C.pf	BACKGROUNDTASKHOST.EXE	\VOLUME{01d5be0528ae8f8c-1628d43c}\WINDC
e:\M\Windows\prefetch\BACKGROUNDTASKHOST.EXE-2B8811BF.pf	BACKGROUNDTASKHOST.EXE	\VOLUME{01d5be0528ae8f8c-1628d43c}\WINDC
e:\M\Windows\prefetch\BACKGROUNDTASKHOST.EXE-2BFC3AB0.pf	BACKGROUNDTASKHOST.EXE	\VOLUME{01d5be0528ae8f8c-1628d43c}\WINDC
e:\M\Windows\prefetch\BACKGROUNDTASKHOST.EXE-37866894.pf	BACKGROUNDTASKHOST.EXE	\VOLUME{01d5be0528ae8f8c-1628d43c}\WINDC
e:\M\Windows\prefetch\BACKGROUNDTASKHOST.EXE-591BEDB7.pf	BACKGROUNDTASKHOST.EXE	\VOLUME{01d5be0528ae8f8c-1628d43c}\WINDC
e:\M\Windows\prefetch\BACKGROUNDTASKHOST.EXE-654F4811.pf	BACKGROUNDTASKHOST.EXE	\VOLUME{01d5be0528ae8f8c-1628d43c}\WINDC
e:\M\Windows\prefetch\BACKGROUNDTASKHOST.EXE-70603A0C.pf	BACKGROUNDTASKHOST.EXE	\VOLUME{01d5be0528ae8f8c-1628d43c}\WINDC
e:\M\Windows\prefetch\BACKGROUNDTASKHOST.EXE-858A19DE.pf	BACKGROUNDTASKHOST.EXE	\VOLUME{01d5be0528ae8f8c-1628d43c}\WINDC
e:\M\Windows\prefetch\BACKGROUNDTASKHOST.EXE-A471C84E.pf	BACKGROUNDTASKHOST.EXE	\VOLUME{01d5be0528ae8f8c-1628d43c}\WINDC
e:\M\Windows\prefetch\BACKGROUNDTASKHOST.EXE-A4F5A8B5.pf	BACKGROUNDTASKHOST.EXE	\VOLUME{01d5be0528ae8f8c-1628d43c}\WINDC
e:\M\Windows\prefetch\BACKGROUNDTASKHOST.EXE-B866D1B4.pf	BACKGROUNDTASKHOST.EXE	\VOLUME{01d5be0528ae8f8c-1628d43c}\WINDC
e:\M\Windows\prefetch\BACKGROUNDTASKHOST.EXE-BC47CCB1.pf	BACKGROUNDTASKHOST.EXE	\VOLUME{01d5be0528ae8f8c-1628d43c}\WINDC
e:\M\Windows\prefetch\BACKGROUNDTASKHOST.EXE-C03F8FFD.pf	BACKGROUNDTASKHOST.EXE	\VOLUME{01d5be0528ae8f8c-1628d43c}\WINDC
e:\M\Windows\prefetch\BACKGROUNDTASKHOST.EXE-CBD68A6D.pf	BACKGROUNDTASKHOST.EXE	\VOLUME{01d5be0528ae8f8c-1628d43c}\WINDC
e:\M\Windows\prefetch\BACKGROUNDTASKHOST.EXE-CF0D8E31.pf	BACKGROUNDTASKHOST.EXE	\VOLUME{01d5be0528ae8f8c-1628d43c}\WINDC
e:\M\Windows\prefetch\BACKGROUNDTRANSFERHOST.EXE-5FF6C1FF.pf	BACKGROUNDTRANSFERHOST.EXE	\VOLUME{01d5be0528ae8f8c-1628d43c}\WINDC
e:\M\Windows\prefetch\BACKGROUNDTRANSFERHOST.EXE-F28781DE.pf	BACKGROUNDTRANSFERHOST.EXE	\VOLUME{01d5be0528ae8f8c-1628d43c}\WINDC
e:\M\Windows\prefetch\BYTECODEGENERATOR.EXE-C1E9BCE6.pf	BYTECODEGENERATOR.EXE	\VOLUME{01d5be0528ae8f8c-1628d43c}\WINDC
e:\M\Windows\prefetch\CERTUTIL.EXE-FA34F34C.pf	CERTUTIL.EXE	\VOLUME{01d5be0528ae8f8c-1628d43c}\WINDC
e:\M\Windows\prefetch\CHXSMARTS...		
e:\M\Windows\prefetch\CLOUDEXPER...		
e:\M\Windows\prefetch\CMD.EXE-4A...		
e:\M\Windows\prefetch\COMPATTEL...		
e:\M\Windows\prefetch\CONHOST.EX...		
e:\M\Windows\prefetch\CONSENT.EX...		
e:\M\Windows\prefetch\CONTROL.EX...		
e:\M\Windows\prefetch\DASHOST.EX...		
e:\M\Windows\prefetch\DEFRAG.EXE...		
e:\M\Windows\prefetch\DLLHOST.EX...		
e:\M\Windows\prefetch\DLLHOST.EX...		
e:\M\Windows\prefetch\DLLHOST.EX...		
e:\M\Windows\prefetch\DLLHOST.EX...		

Find and Replace dialog box:

- Find what: firefox
- Within: Sheet
- Search: By Rows
- Look in: Formulas
- Buttons: Find All, Find Next, Close

This file is located at: \VOLUME{01d5be0528ae8f8c-1628d43c}\WINDOWS\SYSTEM32\CERTUTIL.EXE

AKA Answer: c:\WINDOWS\SYSTEM32\CERTUTIL.EXE