Sysinternals

Task 1 Introduction

What are the tools known as **Sysinternals**?

The Sysinternals tools is a compilation of over 70+ Windows-based tools. Each of the tools falls into one of the following categories:

- File and Disk Utilities
- Networking Utilities
- Process Utilities
- Security Utilities
- System Information
- Miscellaneous

The Sysinternals tools and its website (sysinternals.com) were created by Mark Russinovich in the late '90s, along Bryce Cogswell under the company Wininternals Software.

In 2006, Microsoft acquired Wininternals Software, and Mark Russinovich joined Microsoft. Today he is the CTO of Microsoft Azure.

Mark Russinovich made headlines when he reported that Sony embedded rootkits into their music CDs back in 2005. This discovery was made known thanks to one of the Sysinternals tools he was testing. You can read more about that here.

He also discovered in 2006 that Symantec was using rootkit-like technology. You can read more about that here.

The Sysinternals tools are extremely popular among IT professionals who manage Windows systems. These tools are so popular that even red teamers and adversaries alike use them. Throughout this room, I'll note which tools MITRE has identified to have been used by adversaries.

The goal of this room is to introduce you to a handful of Sysinternals tools with the hopes that you will expand on this knowledge with your own research and curiosity.

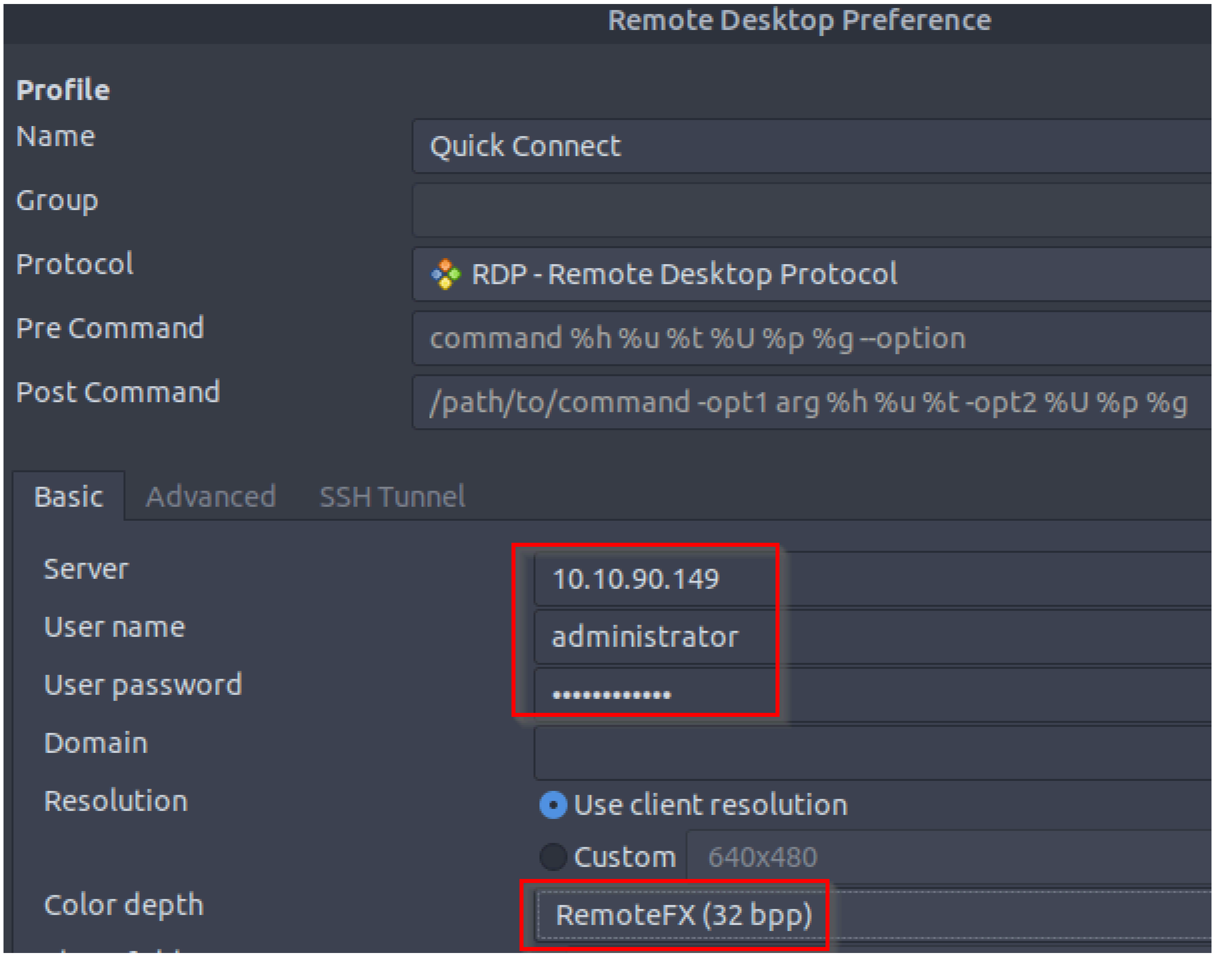
Hopefully, you can add Sysinternals to your toolkit, as many already have.

If you want to access the virtual machine via Remote Desktop, use the credentials below.

Machine IP:

User:

Password:



Remote Desktop Preference

Profile

Name: Quick Connect

Group:

Protocol: RDP - Remote Desktop Protocol

Pre Command: command %h %u %t %U %p %g --option

Post Command: /path/to/command -opt1 arg %h %u %t -opt2 %U %p %g

Server: 10.10.90.149

User name: administrator

User password: ••••••••••••

Domain:

Resolution: ● Use client resolution ○ Custom 640x480

Color depth: RemoteFX (32 bpp)

Accept the Certificate when prompted, and you should be logged into the remote system now.

Note: The virtual machine may take up to 3 minutes to load.

Answer the questions below
When did Microsoft acquire the Sysinternals tools?
2006

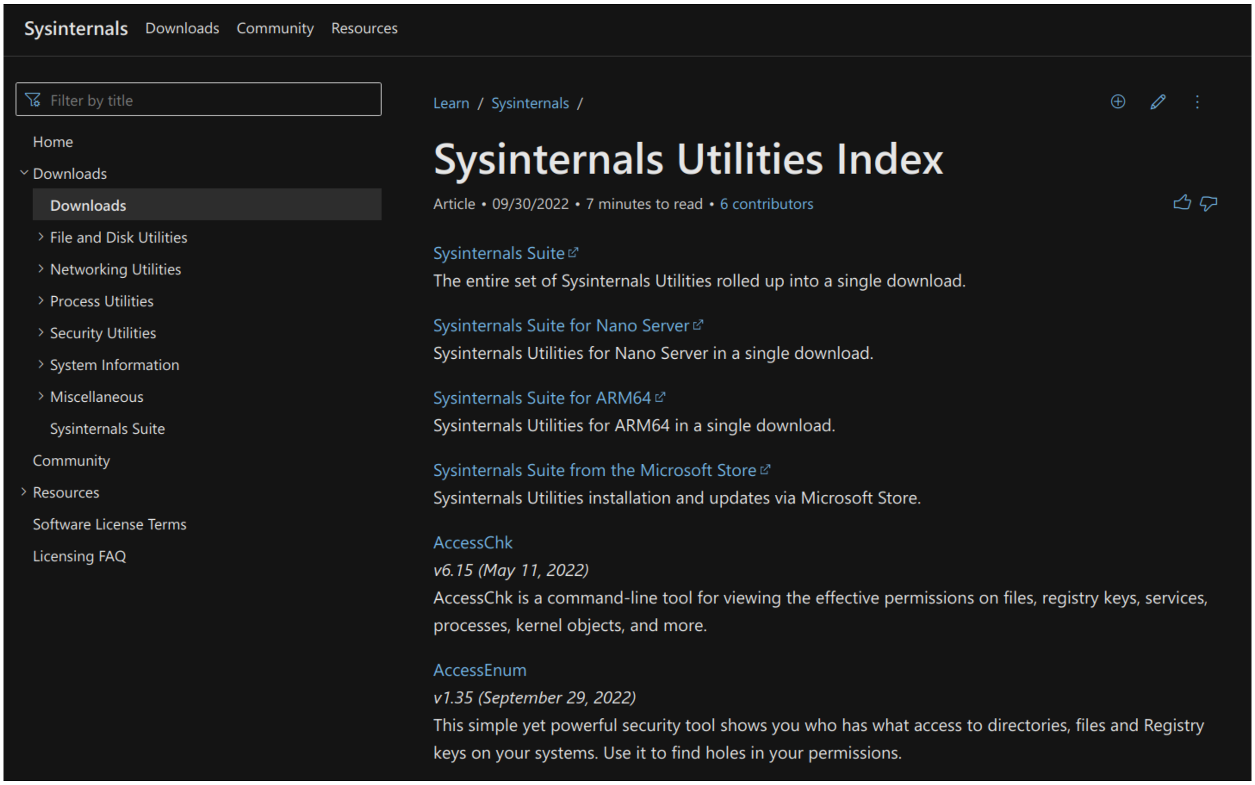
<u>Task 2</u> Install the Sysinternals Suite

Time to get our hands dirty with Sysinternals.

The Sysinternals tool(s) can be downloaded and run from the local system, or the tool(s) can be run from the web.

Note: machines started via "Start Machine" do not have Internet access, but you can practice this task on your own system!

If you wish to download a tool or two but not the entire suite, you can navigate to the **Sysinternals Utilities Index** page, https://docs.microsoft.com/en-us/sysinternals/downloads/, and download the tool(s). If you know which tool you want to download, then this is fine. The tools are listed in alphabetical order are not separated by categories.



Sysinternals Utilities Index

Article • 09/30/2022 • 7 minutes to read • 6 contributors

Sysinternals Suite
The entire set of Sysinternals Utilities rolled up into a single download.

Sysinternals Suite for Nano Server
Sysinternals Utilities for Nano Server in a single download.

Sysinternals Suite for ARM64
Sysinternals Utilities for ARM64 in a single download.

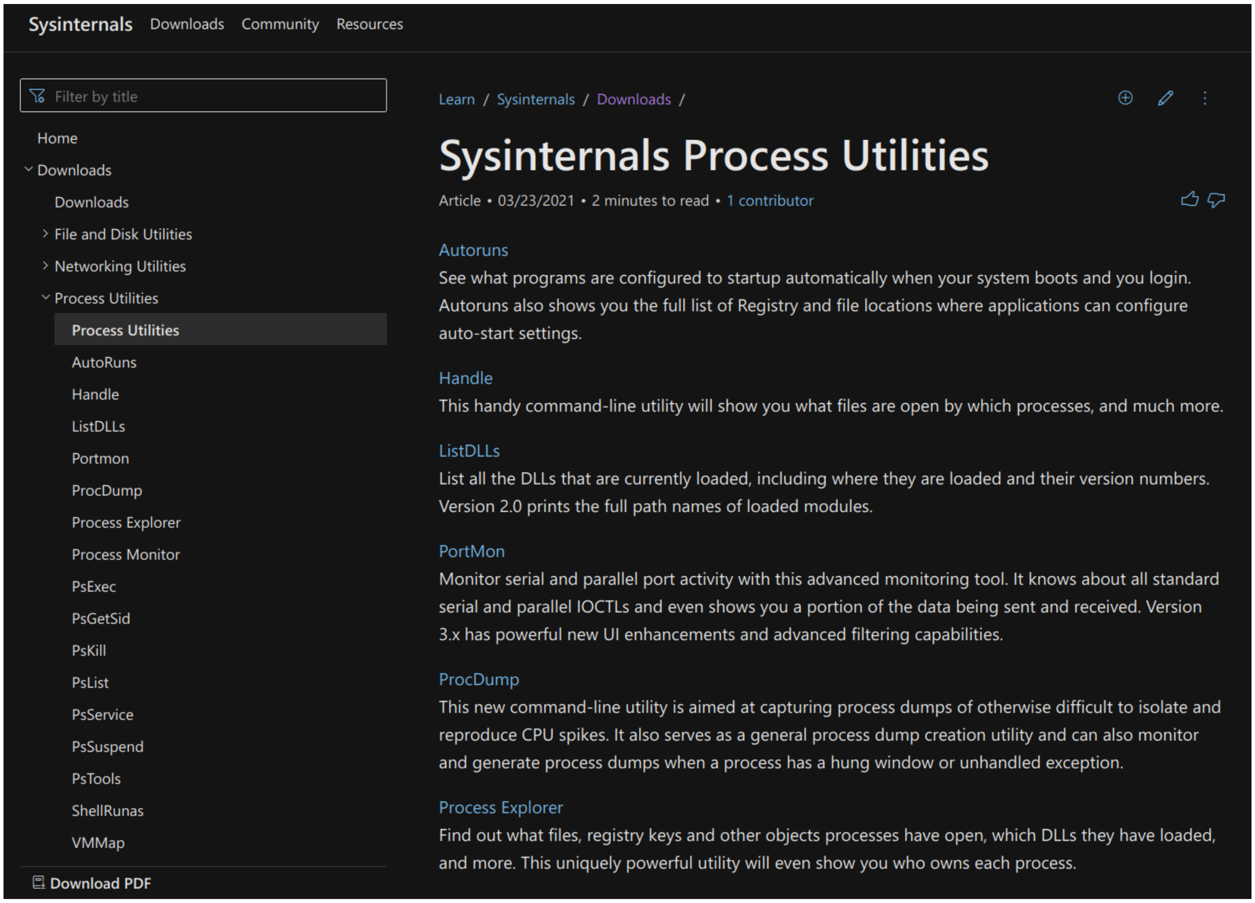
Sysinternals Suite from the Microsoft Store
Sysinternals Utilities installation and updates via Microsoft Store.

AccessChk
v6.15 (May 11, 2022)
AccessChk is a command-line tool for viewing the effective permissions on files, registry keys, services, processes, kernel objects, and more.

AccessEnum
v1.35 (September 29, 2022)
This simple yet powerful security tool shows you who has what access to directories, files and Registry keys on your systems. Use it to find holes in your permissions.

Alternatively, you can use the category links to find and download the tool(s). This route is better since there are so many tools you can focus on all the tools of interest instead of the entire index.

For example, let's say you need tools to inspect Windows processes; then, you can navigate to the **Process Utilities** page, https://docs.microsoft.com/en-us/sysinternals/downloads/process-utilities/, for all the tools that fall under this category.



Sysinternals Process Utilities

Article • 03/23/2021 • 2 minutes to read • 1 contributor

Autoruns
See what programs are configured to startup automatically when your system boots and you login. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.

Handle
This handy command-line utility will show you what files are open by which processes, and much more.

ListDLLs
List all the DLLs that are currently loaded, including where they are loaded and their version numbers. Version 2.0 prints the full path names of loaded modules.

PortMon
Monitor serial and parallel port activity with this advanced monitoring tool. It knows about all standard serial and parallel IOCTLs and even shows you a portion of the data being sent and received. Version 3.x has powerful new UI enhancements and advanced filtering capabilities.

ProcDump
This new command-line utility is aimed at capturing process dumps of otherwise difficult to isolate and reproduce CPU spikes. It also serves as a general process dump creation utility and can also monitor and generate process dumps when a process has a hung window or unhandled exception.

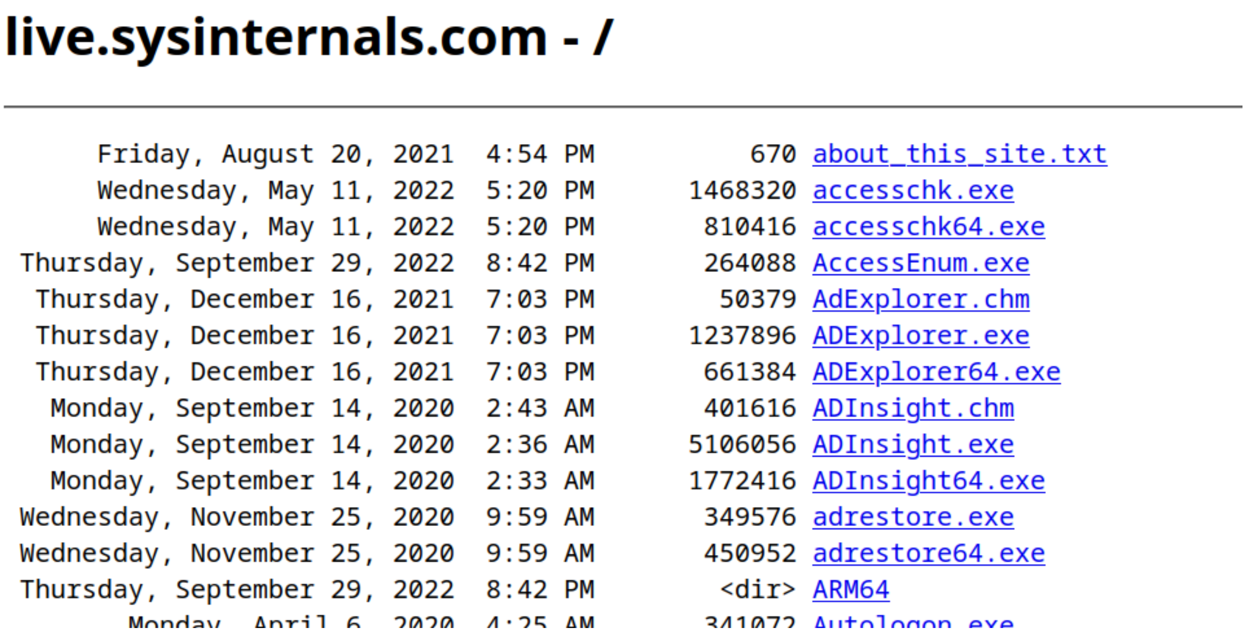
Process Explorer
Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.

Notice that you are conveniently supplied with a brief explanation for each tool.

Lastly, you can do the same from the Sysinternals Live URL, https://live.sysinternals.com/. This is the same URL to use if you wish to run the tool from the web. We will look at how to accomplish this in the next section.

If you chose to download from this page, it is similar to the Sysinternals Utilities Index page. The tools are listed in alphabetical order and are not separated by categories.

Image

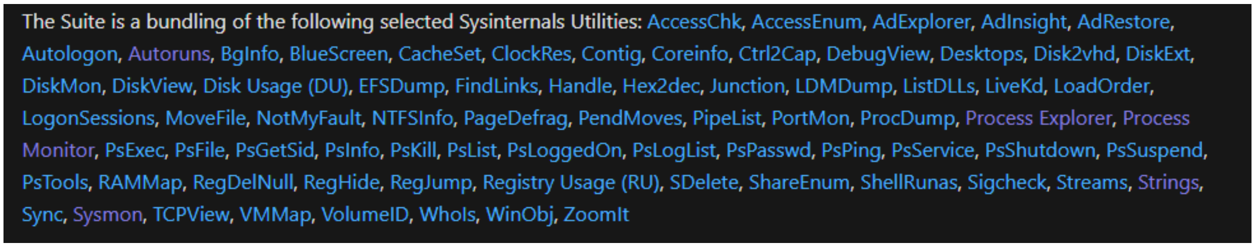


live.sysinternals.com - /

```
      Friday, August 20, 2021  4:54 PM        670 about_this_site.txt
      Wednesday, May 11, 2022  5:20 PM    1468320 accesschk.exe
      Wednesday, May 11, 2022  5:20 PM     810416 accesschk64.exe
 Thursday, September 29, 2022  8:42 PM     264088 AccessEnum.exe
  Thursday, December 16, 2021  7:03 PM      50379 AdExplorer.chm
  Thursday, December 16, 2021  7:03 PM    1237896 ADExplorer.exe
  Thursday, December 16, 2021  7:03 PM     661384 ADExplorer64.exe
   Monday, September 14, 2020  2:43 AM     401616 ADInsight.chm
   Monday, September 14, 2020  2:36 AM    5106056 ADInsight.exe
   Monday, September 14, 2020  2:33 AM    1772416 ADInsight64.exe
 Wednesday, November 25, 2020  9:59 AM     349576 adrestore.exe
 Wednesday, November 25, 2020  9:59 AM     450952 adrestore64.exe
 Thursday, September 29, 2022  8:42 PM      <dir> ARM64
        Monday, April 6, 2020  4:25 AM     341072 Autologon.exe
```

If you wish to download the Sysinternals Suite, you can download the zip file from here.

The suite has a select number of Sysinternal tools. See below for a rundown of the tools included in the suite.

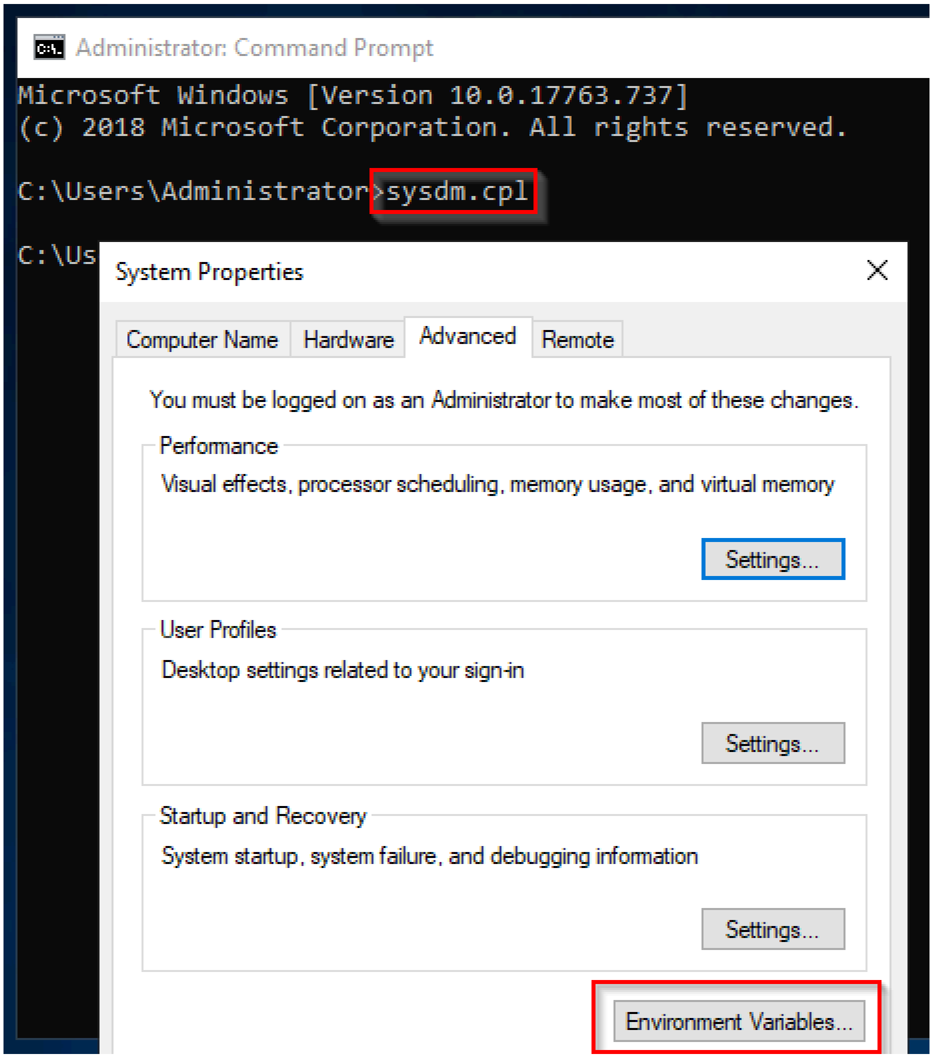


The Suite is a bundling of the following selected Sysinternals Utilities: AccessChk, AccessEnum, AdExplorer, AdInsight, AdRestore, Autologon, Autoruns, BgInfo, BlueScreen, CacheSet, ClockRes, Contig, Coreinfo, Ctrl2Cap, DebugView, Desktops, Disk2vhd, DiskExt, DiskMon, DiskView, Disk Usage (DU), EFSDump, FindLinks, Handle, Hex2dec, Junction, LDMDump, ListDLLs, LiveKd, LoadOrder, LogonSessions, MoveFile, NotMyFault, NTFSInfo, PageDefrag, PendMoves, PipeList, PortMon, ProcDump, Process Explorer, Process Monitor, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsList, PsLoggedOn, PsLogList, PsPasswd, PsPing, PsService, PsShutdown, PsSuspend, PsTools, RAMMap, RegDelNull, RegHide, RegJump, Registry Usage (RU), SDelete, ShareEnum, ShellRunas, Sigcheck, Streams, Strings, Sync, Sysmon, TCPView, VMMap, VolumeID, WhoIs, WinObj, ZoomIt

After you download the zip file, you need to extract the files. After the files are extracted, the extra step, which is by choice, is to add the folder path to the environment variables. By doing so, you can launch the tools via the command line without navigating to the directory the tools reside in.

Environment Variables can be edited from **System Properties**.

The System Properties can be launched via the command line by running . Click on the tab.



```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>sysdm.cpl

C:\Us
```

You must be logged on as an Administrator to make most of these changes.

Performance

Visual effects, processor scheduling, memory usage, and virtual memory

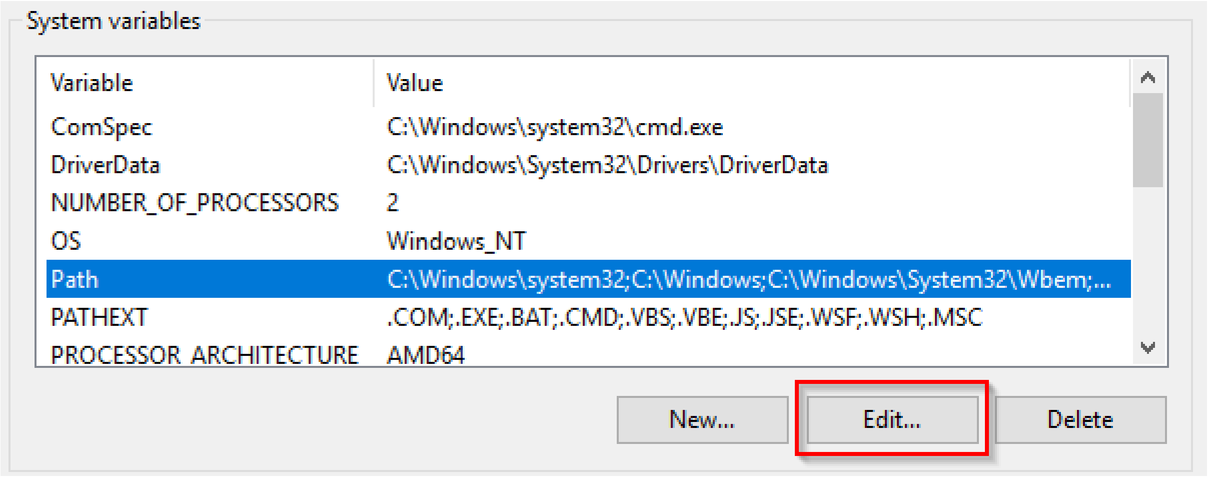
User Profiles

Desktop settings related to your sign-in

Startup and Recovery

System startup, system failure, and debugging information

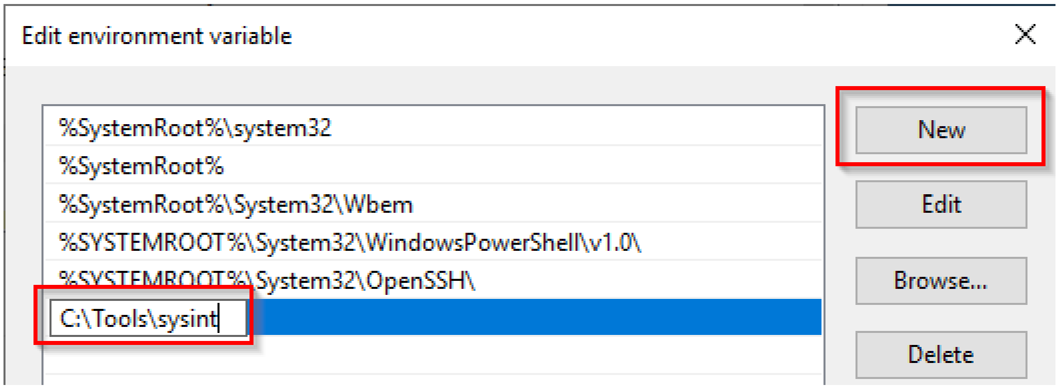
Select under and select Edit... then OK.



System variables

Variable	Value
ComSpec	C:\Windows\system32\cmd.exe
DriverData	C:\Windows\System32\Drivers\DriverData
NUMBER_OF_PROCESSORS	2
OS	Windows_NT
Path	C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;...
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE	AMD64

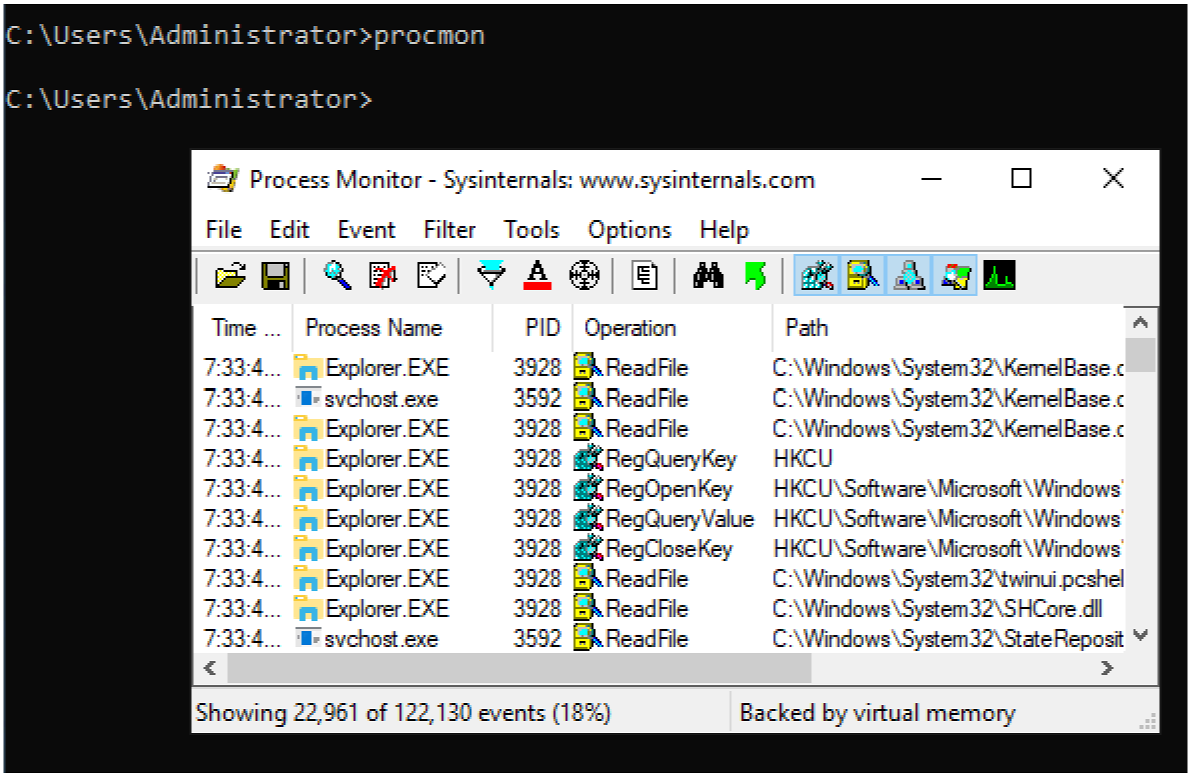
In the next screen select and enter the folder path where the Sysinternals Suite was extracted to. Press OK to confirm the changes.



Edit environment variable

%SystemRoot%\system32
%SystemRoot%
%SystemRoot%\System32\Wbem
%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\
%SYSTEMROOT%\System32\OpenSSH\
C:\Tools\sysint

Open a new command prompt (elevated) to confirm that the Sysinternals Suite can be executed from any location.



```
C:\Users\Administrator>procmon

C:\Users\Administrator>
```

Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path
7:33:4...	Explorer.EXE	3928	ReadFile	C:\Windows\System32\KernelBase.c
7:33:4...	svchost.exe	3592	ReadFile	C:\Windows\System32\KernelBase.c
7:33:4...	Explorer.EXE	3928	ReadFile	C:\Windows\System32\KernelBase.c
7:33:4...	Explorer.EXE	3928	RegQueryKey	HKCU
7:33:4...	Explorer.EXE	3928	RegOpenKey	HKCU\Software\Microsoft\Windows\
7:33:4...	Explorer.EXE	3928	RegQueryValue	HKCU\Software\Microsoft\Windows\
7:33:4...	Explorer.EXE	3928	RegCloseKey	HKCU\Software\Microsoft\Windows\
7:33:4...	Explorer.EXE	3928	ReadFile	C:\Windows\System32\twinui.pcshel
7:33:4...	Explorer.EXE	3928	ReadFile	C:\Windows\System32\SHCore.dll
7:33:4...	svchost.exe	3592	ReadFile	C:\Windows\System32\StateReposit

Showing 22,961 of 122,130 events (18%) Backed by virtual memory

A local copy of the Sysinternals Suite is located in .

Alternatively, a PowerShell module can download and install all of the Sysinternals tools.

- PowerShell command:

Now let's look at how to run the Sysinternals tools from the web.

Answer the questions below
What is the last tool listed within the Sysinternals Suite?
ZoomIt

Task 3 Using Sysinternals Live

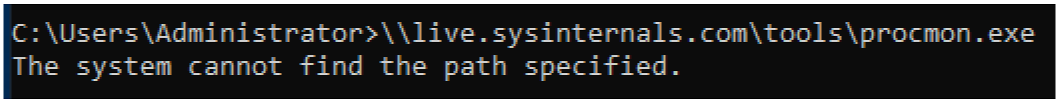
Per the Sysinternals website, "Sysinternals Live is a service that enables you to execute Sysinternals tools directly from the Web without hunting for and manually downloading them. Simply enter a tool's Sysinternals Live path into Windows Explorer or a command prompt as **live.sysinternals.com/<toolname>** or **\\live.sysinternals.com\tools\<toolname>**."

Note: machines started via "Start Machine" do not have Internet access, but you can practice this task on your own system! Let's take a look at how we can do this.

Based on the instructions, to launch Process Monitor from the web the syntax is

.

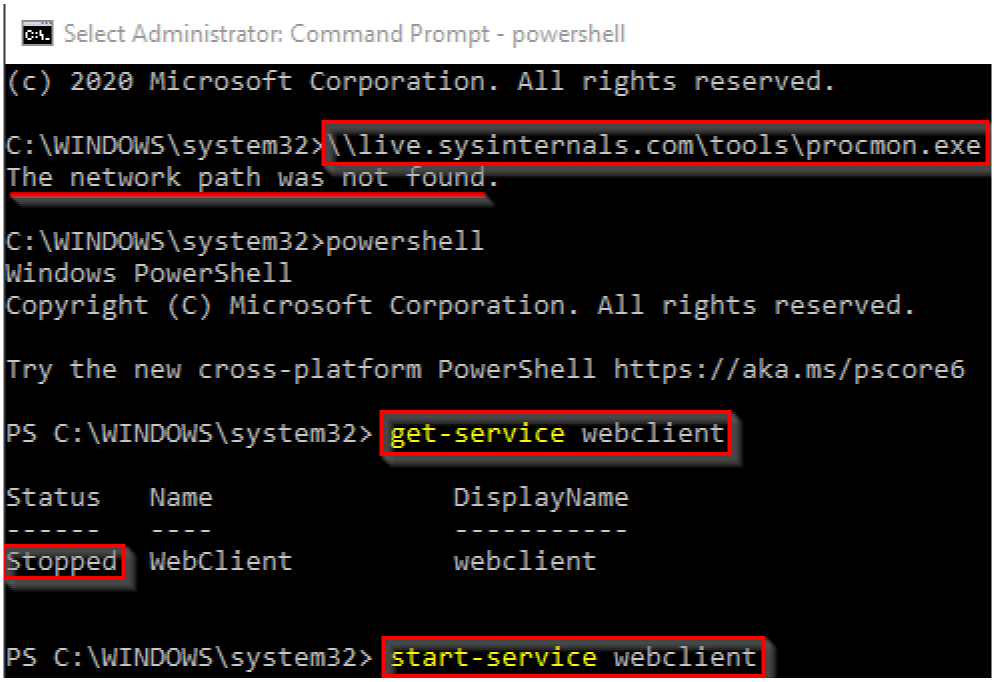
And it fails.



```
C:\Users\Administrator>\\live.sysinternals.com\tools\procmon.exe
The system cannot find the path specified.
```

To resolve this issue the WebDAV client must be installed and running on the machine. The WebDAV protocol is what allows a local machine to access a remote machine running a WebDAV share and perform actions in it.

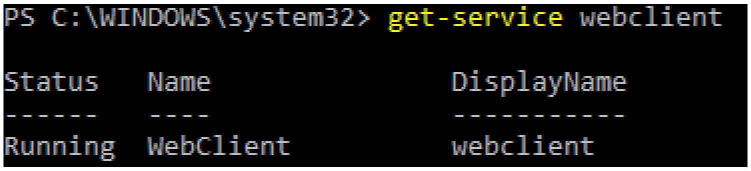
On a Windows 10 client, the WebDAV client is installed but the client is most likely not running. If you try to run a Sysinternals tool it will fail with a message "The network path was not found."



Select Administrator: Command Prompt - powershell

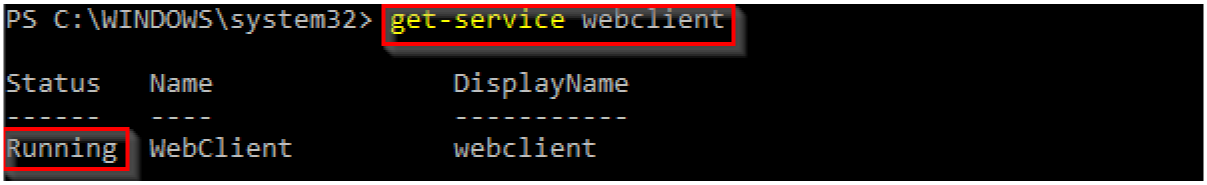
```
(c) 2020 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>\\live.sysinternals.com\tools\procmon.exe
The network path was not found.

C:\WINDOWS\system32>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> get-service webclient

Status   Name               DisplayName
------   ----               -----------
Stopped  WebClient          webclient


PS C:\WINDOWS\system32> start-service webclient
```

The service needs to be started before attempting to call any Sysinternals tool in this fashion.



```
PS C:\WINDOWS\system32> get-service webclient

Status   Name               DisplayName
------   ----               -----------
Running  WebClient          webclient
```

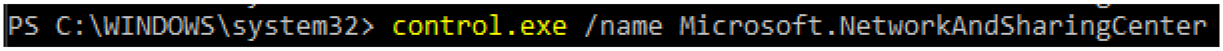
Verify it's running before proceeding.



```
PS C:\WINDOWS\system32> get-service webclient

Status   Name               DisplayName
------   ----               -----------
Running  WebClient          webclient
```

Also, **Network Discovery** needs to be enabled as well. This setting can be enabled in the **Network and Sharing Center**.

There are a few ways to open the Network and Sharing Center. Here is a neat command line to launch it.



```
PS C:\WINDOWS\system32> control.exe /name Microsoft.NetworkAndSharingCenter
```

Click on and select
for your current network profile.

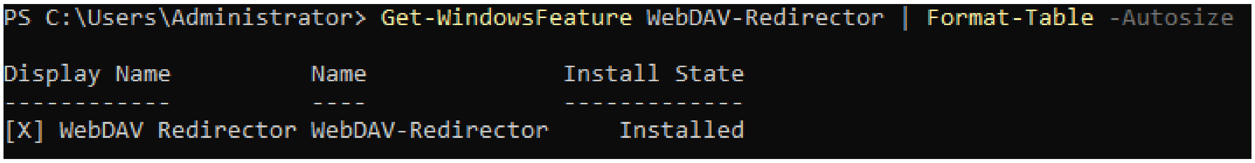
The attached VM is a Windows Server 2019 edition. The WebDAV client is not installed by default.

The feature to install on Windows Server is **WebDAV Redirector**. This feature can be installed via **Server Manager** or using **PowerShell**.

To install with PowerShell, .
The server needs to reboot for the installation to complete.

After reboot, the installation can be verified with the following PowerShell command,

.



```
PS C:\Users\Administrator> Get-WindowsFeature WebDAV-Redirector | Format-Table -Autosize

Display Name          Name              Install State
------------          ----              -------------
[X] WebDAV Redirector WebDAV-Redirector     Installed
```

The same process as with a Windows 10 client applies from this point:

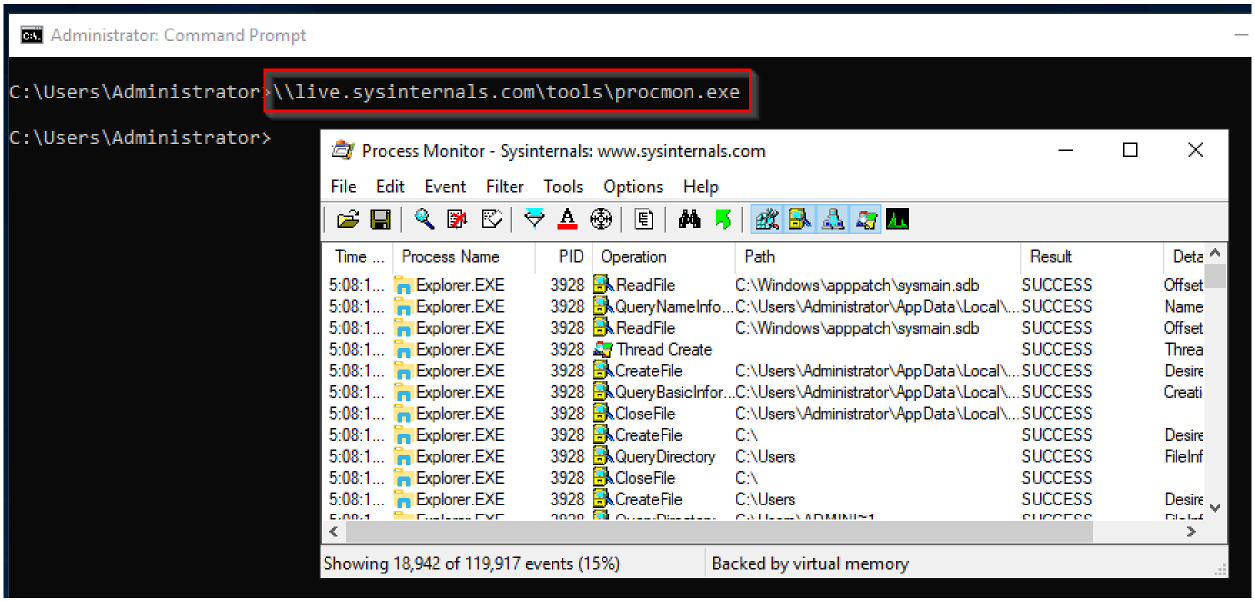
- Make sure the WebClient service is running
- Make sure Network Discovery is enabled

Now with all the necessary components installed and enabled the local machine is ready to run Sysinternals tools from the web.

There are 2 ways the tools can be run:

- Run the tool from the command line (as shown above from the Windows 10 machine)
- Create a network drive and run the tool from the mapped drive

Method 1 - Run tool from command line



Administrator: Command Prompt

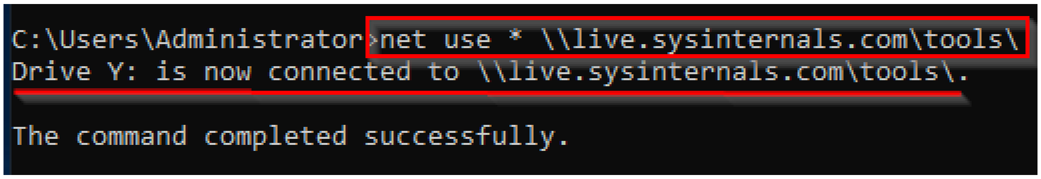
```
C:\Users\Administrator>\\live.sysinternals.com\tools\procmon.exe

C:\Users\Administrator>
```

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Deta
5:08:1...	Explorer.EXE	3928	ReadFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	Offset
5:08:1...	Explorer.EXE	3928	QueryNameInfo...	C:\Users\Administrator\AppData\Local\...	SUCCESS	Name
5:08:1...	Explorer.EXE	3928	ReadFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	Offset
5:08:1...	Explorer.EXE	3928	Thread Create		SUCCESS	Threa
5:08:1...	Explorer.EXE	3928	CreateFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	Desire
5:08:1...	Explorer.EXE	3928	QueryBasicInfor...	C:\Users\Administrator\AppData\Local\...	SUCCESS	Creati
5:08:1...	Explorer.EXE	3928	CloseFile	C:\Users\Administrator\AppData\Local\...	SUCCESS	
5:08:1...	Explorer.EXE	3928	CreateFile	C:\	SUCCESS	Desire
5:08:1...	Explorer.EXE	3928	QueryDirectory	C:\Users	SUCCESS	FileInf
5:08:1...	Explorer.EXE	3928	CloseFile	C:\	SUCCESS	
5:08:1...	Explorer.EXE	3928	CreateFile	C:\Users	SUCCESS	Desire

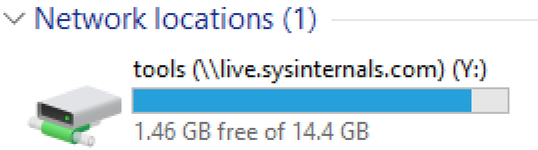
Showing 18,942 of 119,917 events (15%) Backed by virtual memory

Method 2 - Run tool from a mapped drive



```
C:\Users\Administrator>net use * \\live.sysinternals.com\tools\
Drive Y: is now connected to \\live.sysinternals.com\tools\.

The command completed successfully.
```

Note: The asterisk will auto-assign a drive letter. The asterick can be replaced with an actual drive letter instead.

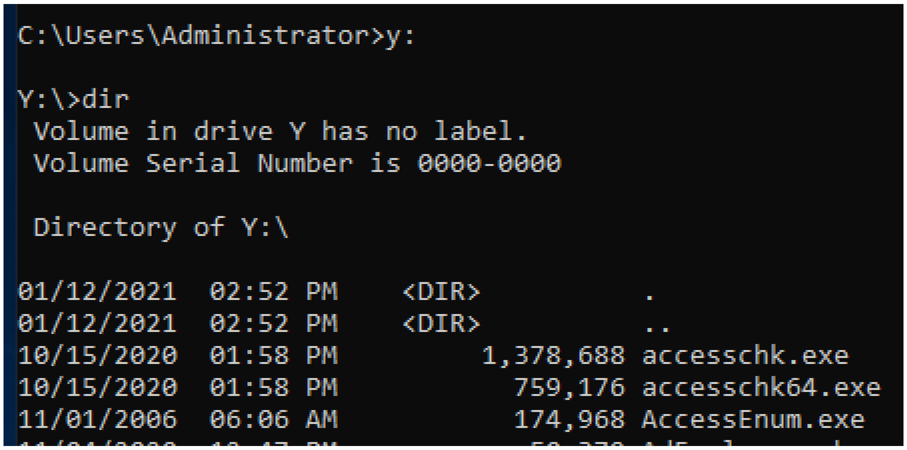


Network locations (1)

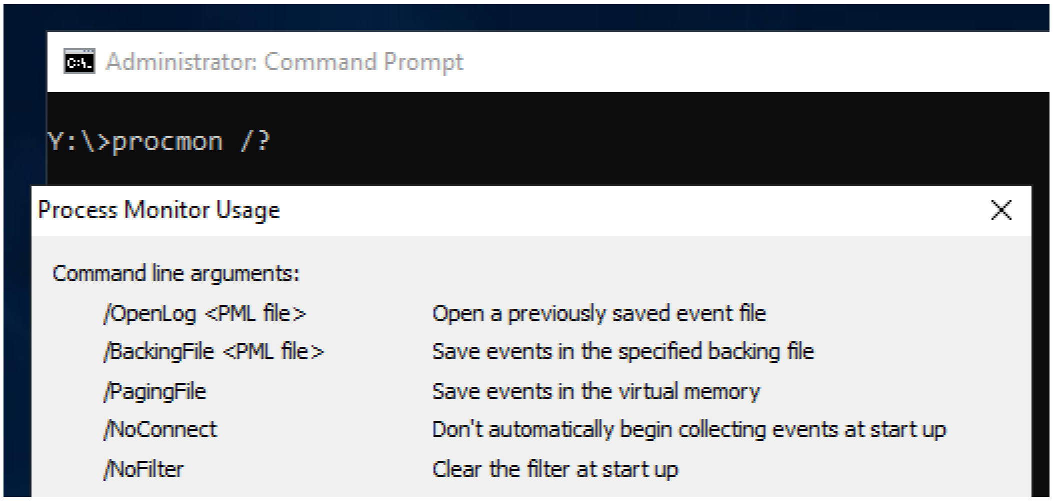
tools (\\live.sysinternals.com) (Y:)

1.46 GB free of 14.4 GB

The website is now browsable within the local machine.



```
C:\Users\Administrator>y:

Y:\>dir
 Volume in drive Y has no label.
 Volume Serial Number is 0000-0000

 Directory of Y:\

01/12/2021  02:52 PM    <DIR>          .
01/12/2021  02:52 PM    <DIR>          ..
10/15/2020  01:58 PM         1,378,688 accesschk.exe
10/15/2020  01:58 PM           759,176 accesschk64.exe
11/01/2006  06:06 AM           174,968 AccessEnum.exe
```



Administrator: Command Prompt

```
Y:\>procmon /?
```

Process Monitor Usage

Command line arguments:

/OpenLog <PML file>	Open a previously saved event file
/BackingFile <PML file>	Save events in the specified backing file
/PagingFile	Save events in the virtual memory
/NoConnect	Don't automatically begin collecting events at start up
/NoFilter	Clear the filter at start up

Now that we got that out of the way time to start exploring some of these tools.

Answer the questions below
What service needs to be enabled on the local host to interact with live.sysinternals.com?
WebClient

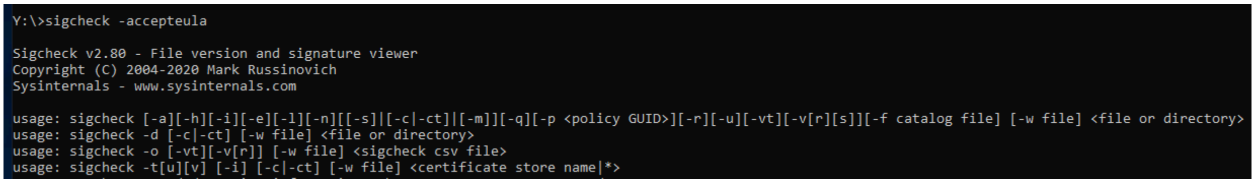
Task 4 File and Disk Utilities

Each task within this room will focus on 1 or 2 tools per section (maybe more).

Again, the goal is to introduce you to the Sysinternals tools, but there are far too many tools to go into each tool in depth.

Sigcheck

"**Sigcheck** is a command-line utility that shows file version number, timestamp information, and digital signature details, including certificate chains. It also includes an option to check a file's status on VirusTotal, a site that performs automated file scanning against over 40 antivirus engines, and an option to upload a file for scanning." (**official definition**)



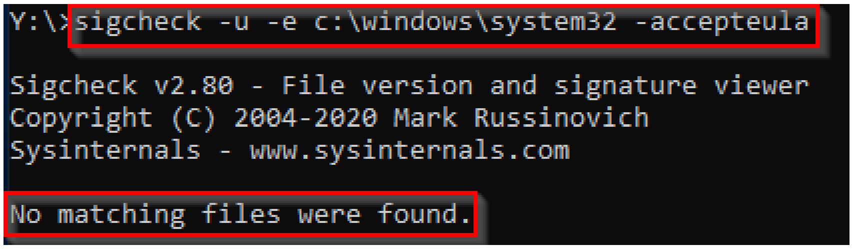
```
Y:\>sigcheck -accepteula

Sigcheck v2.80 - File version and signature viewer
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

usage: sigcheck [-a][-h][-i][-e][-l][-n][[-s]|[-c|-ct]|[-m]][-q][-p <policy GUID>][-r][-u][-vt][-v[r][s]][-f catalog file] [-w file] <file or directory>
usage: sigcheck -d [-c|-ct] [-w file] <file or directory>
usage: sigcheck -o [-vt][-v[r]] [-w file] <sigcheck csv file>
usage: sigcheck -t[u][v] [-i] [-c|-ct] [-w file] <certificate store name|*>
```

From the official Sigcheck page, a use case is identified towards the bottom of the page.

If you completed the Core Windows Processes room you should be aware that the location of all the executables is , except for **Explorer.exe** (which is).

Use Case: Check for unsigned files in C:\Windows\System32.

Command:



```
Y:\>sigcheck -u -e c:\windows\system32 -accepteula

Sigcheck v2.80 - File version and signature viewer
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

No matching files were found.
```

Parameter usage:

- "If VirusTotal check is enabled, show files that are unknown by VirusTotal or have non-zero detection, otherwise show only unsigned files."
- "Scan executable images only (regardless of their extension)"

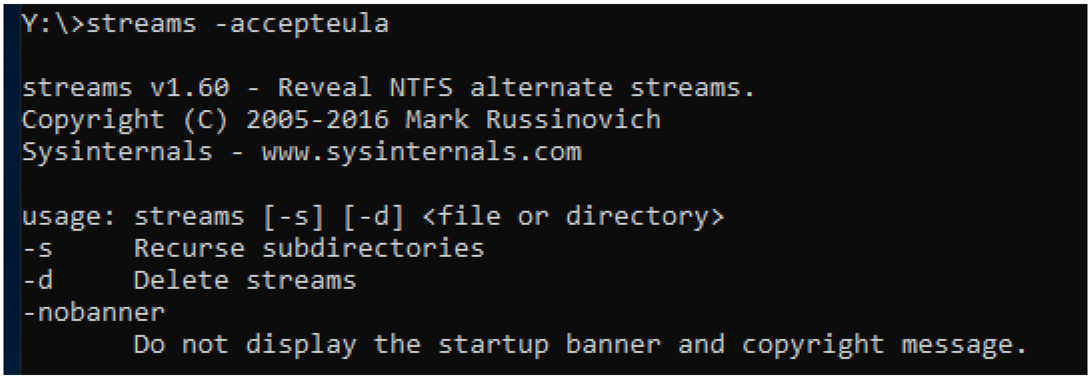
Note: If the results were different it would warrant an investigation into any listed executables.

Streams

"The NTFS file system provides applications the ability to create alternate data streams of information. By default, all data is stored in a file's main unnamed data stream, but by using the syntax 'file:stream', you are able to read and write to alternates." (**official definition**)

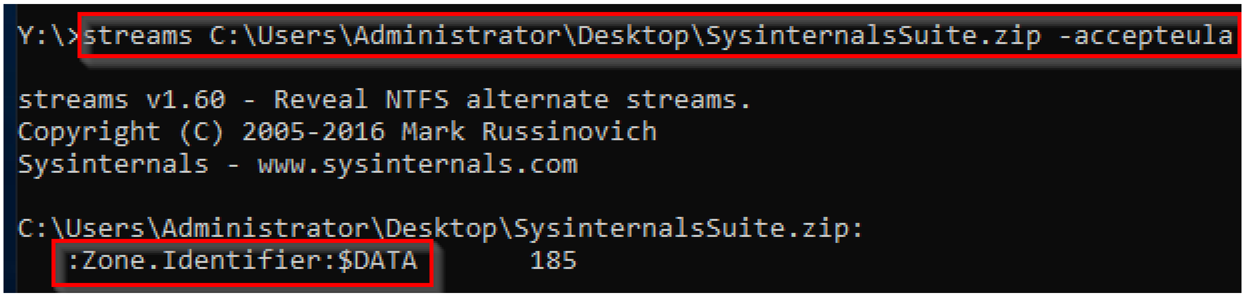
Alternate Data Streams (ADS) is a file attribute specific to Windows NTFS (New Technology File System). Every file has at least one data stream ($DATA) and ADS allows files to contain more than one stream of data. Natively Window Explorer doesn't display ADS to the user. There are 3rd party executables that can be used to view this data, but Powershell gives you the ability to view ADS for files.

Malware writers have used ADS to hide data in an endpoint, but not all its uses are malicious. When you download a file from the Internet unto an endpoint, there are identifiers written to ADS to identify that it was downloaded from the Internet.



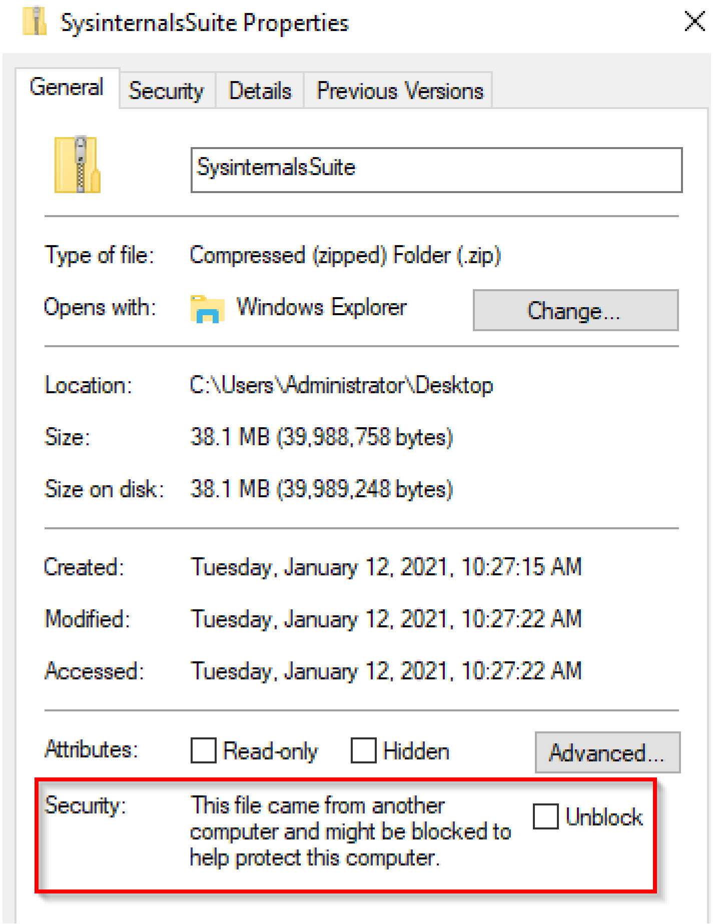
```
Y:\>streams -accepteula

streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

usage: streams [-s] [-d] <file or directory>
-s     Recurse subdirectories
-d     Delete streams
-nobanner
       Do not display the startup banner and copyright message.
```

Example: A file downloaded from the Internet.



```
Y:\>streams C:\Users\Administrator\Desktop\SysinternalsSuite.zip -accepteula

streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users\Administrator\Desktop\SysinternalsSuite.zip:
   :Zone.Identifier:$DATA       185
```

Since the file has this identifier, additional security measures are added to its properties.



SysinternalsSuite

Type of file: Compressed (zipped) Folder (.zip)

Opens with: Windows Explorer

Location: C:\Users\Administrator\Desktop

Size: 38.1 MB (39,988,758 bytes)

Size on disk: 38.1 MB (39,989,248 bytes)

Created: Tuesday, January 12, 2021, 10:27:15 AM

Modified: Tuesday, January 12, 2021, 10:27:22 AM

Accessed: Tuesday, January 12, 2021, 10:27:22 AM

Attributes: □ Read-only □ Hidden

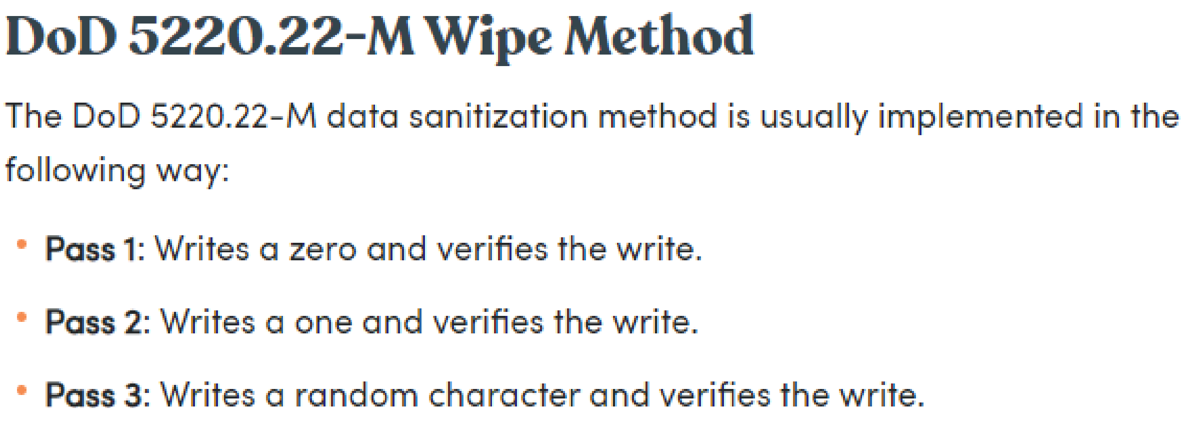
Security: This file came from another computer and might be blocked to help protect this computer. □ Unblock

You can read more on streams here.

SDelete

"**SDelete** is a command line utility that takes a number of options. In any given use, it allows you to delete one or more files and/or directories, or to cleanse the free space on a logical disk."

As per the official documentation page, SDelete (**Secure Delete**) implemented the **DOD 5220.22-M** (Department of Defense clearing and sanitizing protocol).



DoD 5220.22-M Wipe Method

The DoD 5220.22-M data sanitization method is usually implemented in the following way:

- **Pass 1**: Writes a zero and verifies the write.
- **Pass 2**: Writes a one and verifies the write.
- **Pass 3**: Writes a random character and verifies the write.

Source: https://www.lifewire.com/dod-5220-22-m-2625856

SDelete has been used by adversaries and is associated with MITRE techniques T1485 (**Data Destruction**) and T1070.004 (**Indicator Removal on Host: File Deletion**). It's MITRE ID S0195.

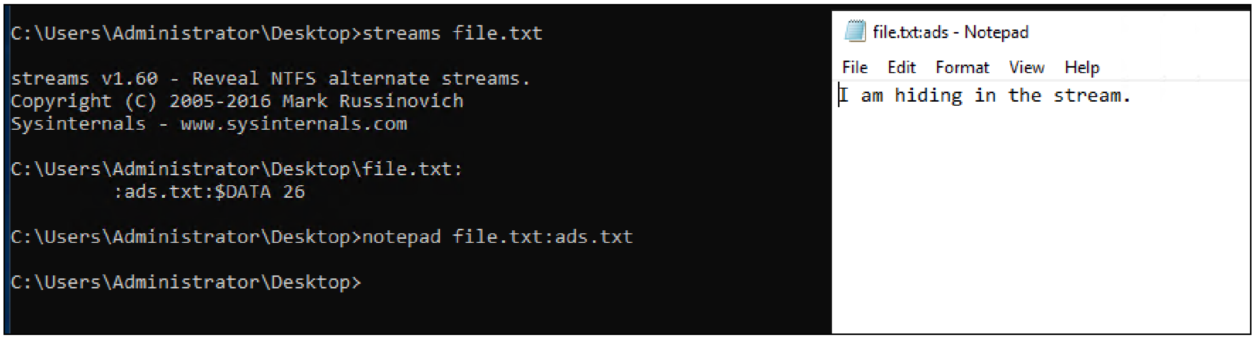
You can review this tool more in-depth by visiting its Sysinternals SDelete page.

Other tools fall under the **File and Disk Utilities** category. I encourage you to explore these tools at your own leisure.

Link: https://docs.microsoft.com/en-us/sysinternals/downloads/file-and-disk-utilities

Answer the questions below

There is a txt file on the desktop named Using one of the three discussed tools in this task, what is the text within the ADS?



```
C:\Users\Administrator\Desktop>streams file.txt

streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users\Administrator\Desktop\file.txt:
         :ads.txt:$DATA 26

C:\Users\Administrator\Desktop>notepad file.txt:ads.txt

C:\Users\Administrator\Desktop>
```

```
I am hiding in the stream.
```

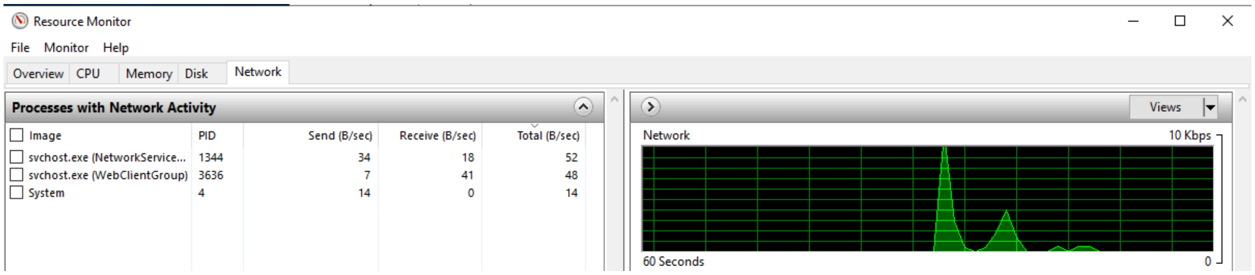
I am hiding in the stream.

Task 5 Networking Utilities

TCPView

"**TCPView** is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. On Windows Server 2008, Vista, and XP, TCPView also reports the name of the process that owns the endpoint. TCPView provides a more informative and conveniently presented subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality." (**official definition**)

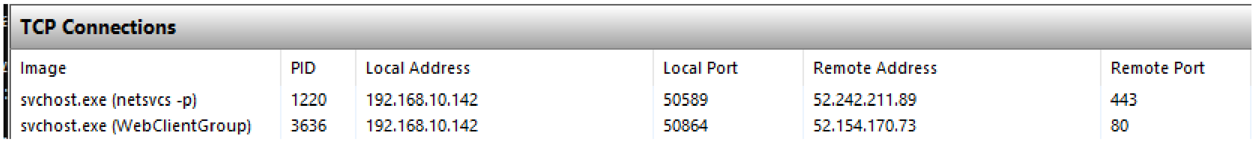
This is a good time to mention that Windows has a built-in utility that provides the same functionality. This tool is called **Resource Monitor**. There are many ways to open this tool. From the command line use .



Processes with Network Activity

□ Image	PID	Send (B/sec)	Receive (B/sec)	Total (B/sec)
□ svchost.exe (NetworkService...	1344	34	18	52
□ svchost.exe (WebClientGroup)	3636	7	41	48
□ System	4	14	0	14

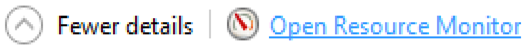
Expand **TCP Connections** to view the **Remote Address** for each **Process** with an outbound connection.



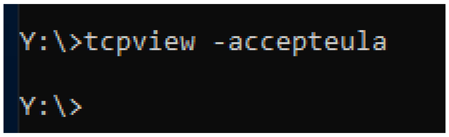
TCP Connections

Image	PID	Local Address	Local Port	Remote Address	Remote Port
svchost.exe (netsvcs -p)	1220	192.168.10.142	50589	52.242.211.89	443
svchost.exe (WebClientGroup)	3636	192.168.10.142	50864	52.154.170.73	80

This tool can also be called from the Performance tab within Task Manager. Look at the bottom left for the link to open Resource Monitor.

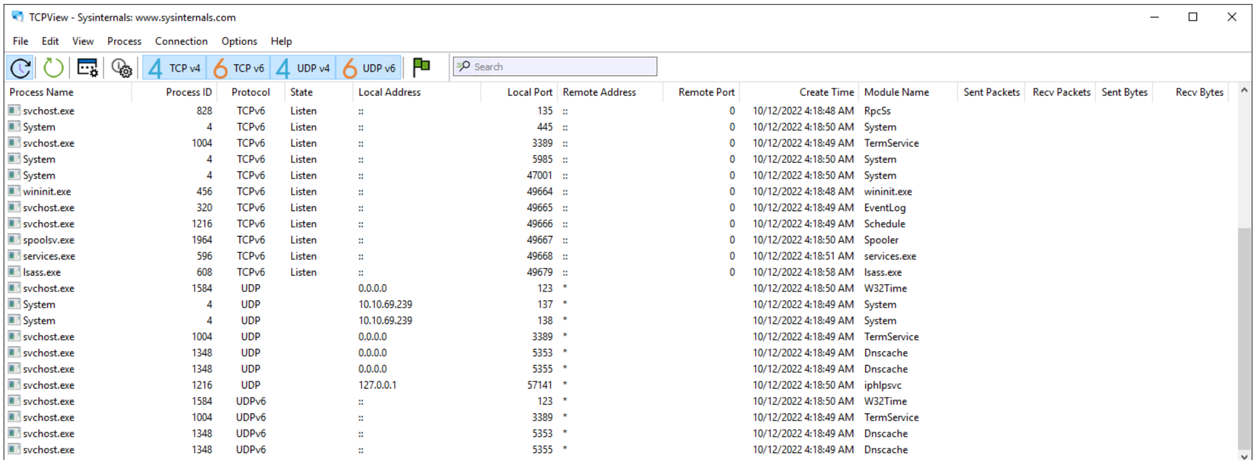


Now back to TCPView.



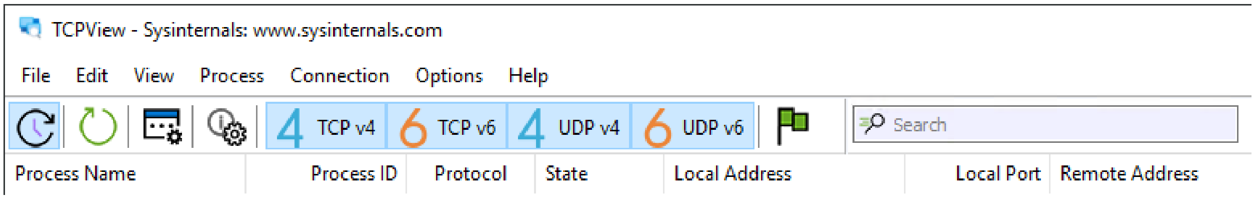
```
Y:\>tcpview -accepteula

Y:\>
```

The below image shows the default view for TCPView.

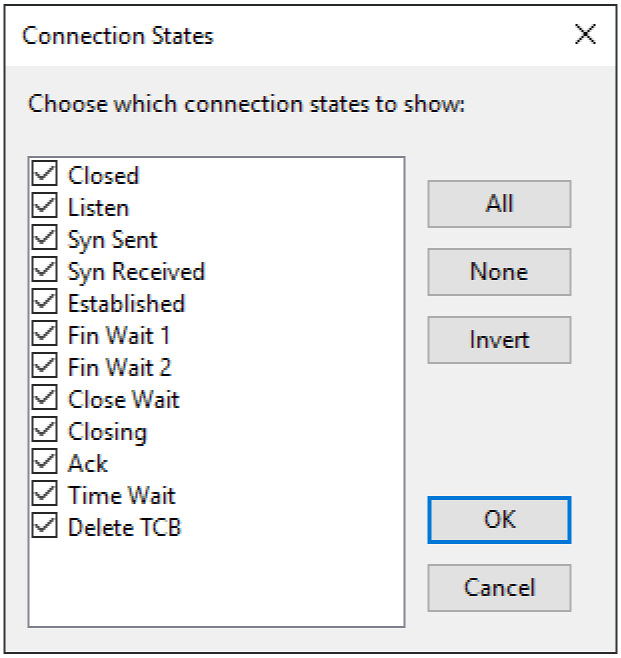


Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets	Recv Packets	Sent Bytes	Recv Bytes
svchost.exe	828	TCPv6	Listen	::	135	::	0	10/12/2022 4:18:48 AM	RpcSs				
System	4	TCPv6	Listen	::	445	::	0	10/12/2022 4:18:50 AM	System				
svchost.exe	1004	TCPv6	Listen	::	3389	::	0	10/12/2022 4:18:49 AM	TermService				
System	4	TCPv6	Listen	::	5985	::	0	10/12/2022 4:18:50 AM	System				
System	4	TCPv6	Listen	::	47001	::	0	10/12/2022 4:18:50 AM	System				
wininit.exe	456	TCPv6	Listen	::	49664	::	0	10/12/2022 4:18:48 AM	wininit.exe				
svchost.exe	320	TCPv6	Listen	::	49665	::	0	10/12/2022 4:18:49 AM	EventLog				
svchost.exe	1216	TCPv6	Listen	::	49666	::	0	10/12/2022 4:18:49 AM	Schedule				
spoolsv.exe	1964	TCPv6	Listen	::	49667	::	0	10/12/2022 4:18:50 AM	Spooler				
services.exe	596	TCPv6	Listen	::	49668	::	0	10/12/2022 4:18:51 AM	services.exe				
lsass.exe	608	TCPv6	Listen	::	49679	::	0	10/12/2022 4:18:58 AM	lsass.exe				
svchost.exe	1584	UDP		0.0.0.0	123	*		10/12/2022 4:18:50 AM	W32Time				
System	4	UDP		10.10.69.239	137	*		10/12/2022 4:18:49 AM	System				
System	4	UDP		10.10.69.239	138	*		10/12/2022 4:18:49 AM	System				
svchost.exe	1004	UDP		0.0.0.0	3389	*		10/12/2022 4:18:49 AM	TermService				
svchost.exe	1348	UDP		0.0.0.0	5353	*		10/12/2022 4:18:49 AM	Dnscache				
svchost.exe	1348	UDP		0.0.0.0	5355	*		10/12/2022 4:18:49 AM	Dnscache				
svchost.exe	1216	UDP		127.0.0.1	57141	*		10/12/2022 4:18:50 AM	iphlpsvc				
svchost.exe	1584	UDPv6		::	123	*		10/12/2022 4:18:50 AM	W32Time				
svchost.exe	1004	UDPv6		::	3389	*		10/12/2022 4:18:49 AM	TermService				
svchost.exe	1348	UDPv6		::	5353	*		10/12/2022 4:18:49 AM	Dnscache				
svchost.exe	1348	UDPv6		::	5355	*		10/12/2022 4:18:49 AM	Dnscache				

We can apply additional filtering by turning off TCP v4, TCP v6, UDP v4, and UDP v6 at the top toolbar, depending on which protocols we want to display. Moreover, we can click on the green flag to use the States Filter.



Clicking the green flag opens the **States Filter**, which provides an extensive list of options to select which connection states we want to display. Most of the connection states available apply only to TCP connections. (UDP, being a connectionless protocol, cannot offer this flexibility in filtering.)



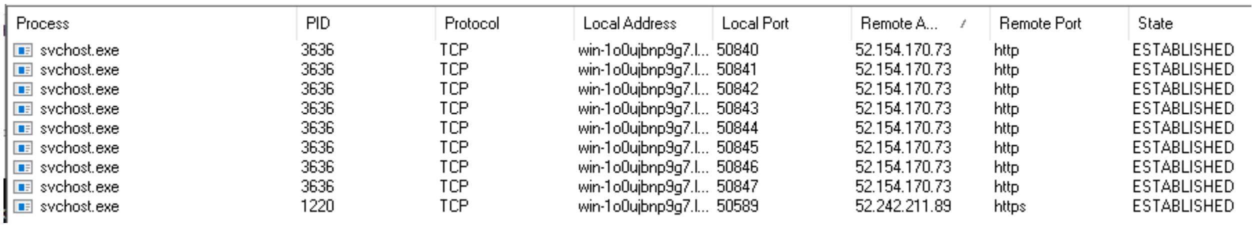
Connection States

Choose which connection states to show:

☑ Closed
☑ Listen
☑ Syn Sent
☑ Syn Received
☑ Established
☑ Fin Wait 1
☑ Fin Wait 2
☑ Close Wait
☑ Closing
☑ Ack
☑ Time Wait
☑ Delete TCB

The list below shows all TCP v4 and TCP v6 connections in any state except in the "Listen" state. For instance, we notice that we have one TCP connection in an *Established* state and another connection in a *Close Wait* state.

In the below image, I unselected Listen in the Connection States from the States Filter and turned off UDP v4 and UDP v6 from the top toolbar.



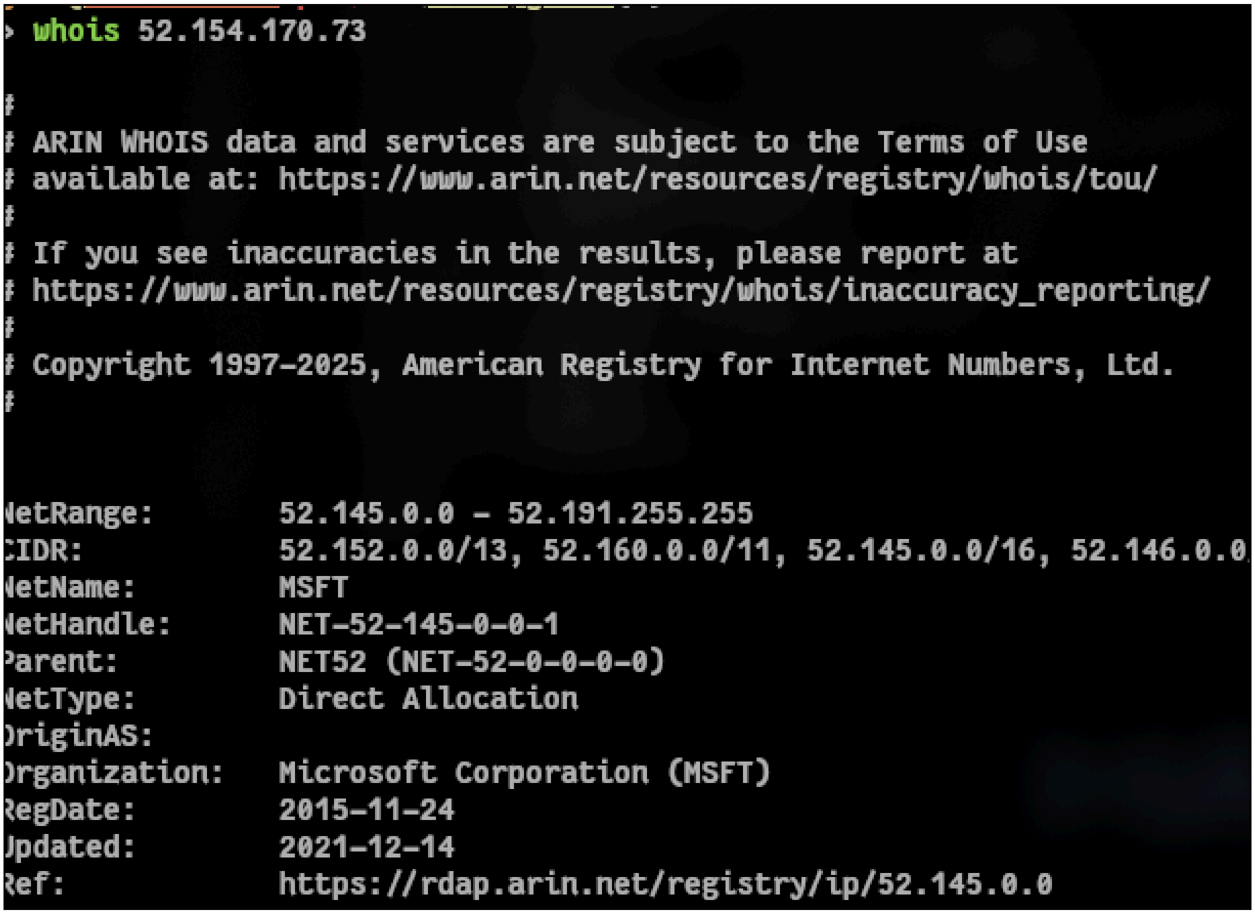
Process	PID	Protocol	Local Address	Local Port	Remote A...	Remote Port	State
svchost.exe	3636	TCP	win-1o0ujbnp9g7.l...	50840	52.154.170.73	http	ESTABLISHED
svchost.exe	3636	TCP	win-1o0ujbnp9g7.l...	50841	52.154.170.73	http	ESTABLISHED
svchost.exe	3636	TCP	win-1o0ujbnp9g7.l...	50842	52.154.170.73	http	ESTABLISHED
svchost.exe	3636	TCP	win-1o0ujbnp9g7.l...	50843	52.154.170.73	http	ESTABLISHED
svchost.exe	3636	TCP	win-1o0ujbnp9g7.l...	50844	52.154.170.73	http	ESTABLISHED
svchost.exe	3636	TCP	win-1o0ujbnp9g7.l...	50845	52.154.170.73	http	ESTABLISHED
svchost.exe	3636	TCP	win-1o0ujbnp9g7.l...	50846	52.154.170.73	http	ESTABLISHED
svchost.exe	3636	TCP	win-1o0ujbnp9g7.l...	50847	52.154.170.73	http	ESTABLISHED
svchost.exe	1220	TCP	win-1o0ujbnp9g7.l...	50589	52.242.211.89	https	ESTABLISHED

Now the output only displays processes with an established outbound connection.

Other tools fall under the Networking Utilities category. I encourage you to explore these tools at your own leisure.

Link: https://docs.microsoft.com/en-us/sysinternals/downloads/networking-utilities

Answer the questions below
Using WHOIS tools, what is the ISP/Organization for the remote address in the screenshots above?



```
> whois 52.154.170.73

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#


letRange:       52.145.0.0 - 52.191.255.255
:IDR:           52.152.0.0/13, 52.160.0.0/11, 52.145.0.0/16, 52.146.0.0
letName:        MSFT
letHandle:      NET-52-145-0-0-1
'arent:         NET52 (NET-52-0-0-0-0)
letType:        Direct Allocation
)riginAS:
)rganization:   Microsoft Corporation (MSFT)
legDate:        2015-11-24
Jpdated:        2021-12-14
lef:            https://rdap.arin.net/registry/ip/52.145.0.0
```

Microsoft Corporation

Task 6 Process Utilities

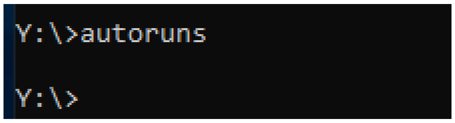
Note: Some of these tools require you to run as an administrator.

Autoruns

"This utility, which has the most comprehensive knowledge of auto-starting locations of any startup monitor, shows you what programs are configured to run during system bootup or login, and when you start various built-in Windows applications like Internet Explorer, Explorer and media players. These programs and drivers include ones in your startup folder, Run, RunOnce, and other Registry keys. **Autoruns** reports Explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, auto-start services, and much more. Autoruns goes way beyond other autostart utilities." (official definition)

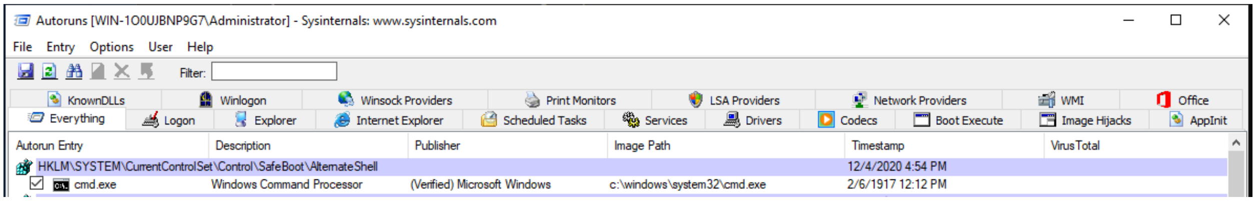
Note: This is a good tool to search for any malicious entries created in the local machine to establish **Persistence**.

Launch Autoruns.



```
Y:\>autoruns

Y:\>
```

Below is a snapshot of Autoruns, showing the first couple of items from the **Everything** tab. Normally there are a lot of entries within this tab.

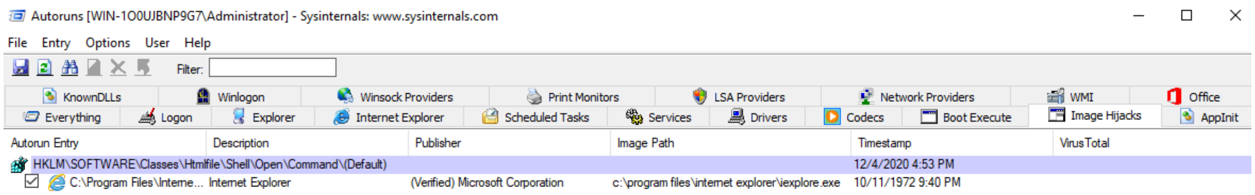


Autoruns [WIN-1O0UJBNP9G7\Administrator] - Sysinternals: www.sysinternals.com

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				12/4/2020 4:54 PM	
☑ cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	2/6/1917 12:12 PM	

Notice all the tabs within the application. Click on each tab to inspect the items associated with each.

The below image is a snapshot of the **Image Hijacks** tab. (At this time there is only 1 item listed)

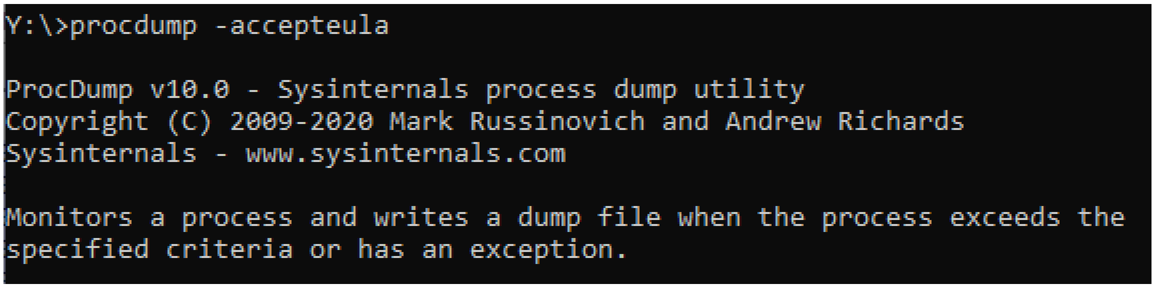


Autoruns [WIN-1O0UJBNP9G7\Administrator] - Sysinternals: www.sysinternals.com

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SOFTWARE\Classes\Htmlfile\Shell\Open\Command\(Default)				12/4/2020 4:53 PM	
☑ C:\Program Files\Interne...	Internet Explorer	(Verified) Microsoft Corporation	c:\program files\internet explorer\iexplore.exe	10/11/1972 9:40 PM	

ProcDump

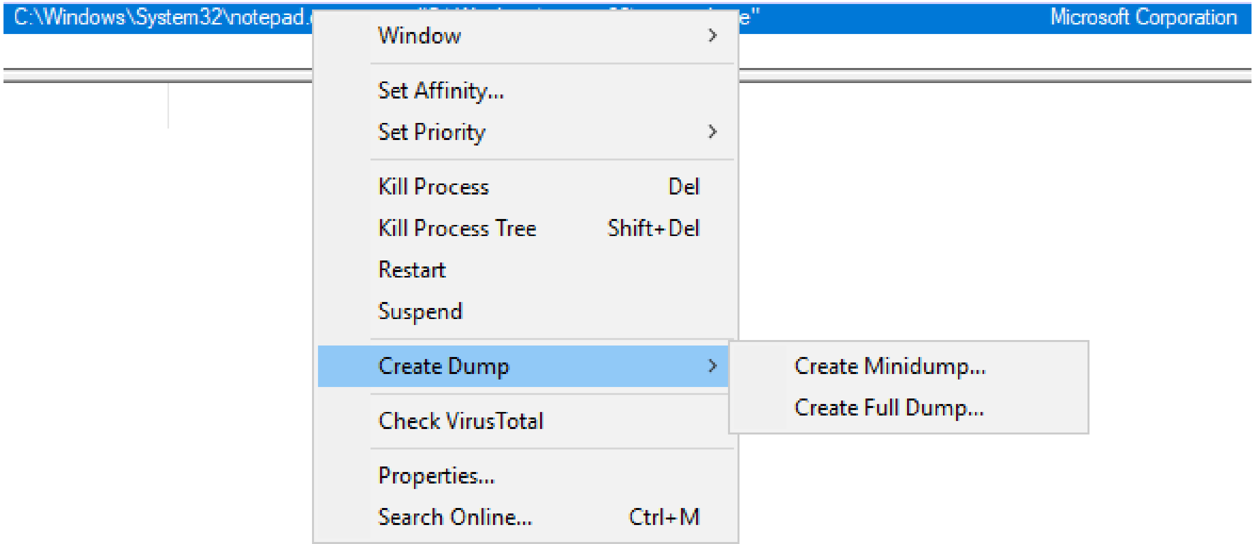
"**ProcDump** is a command-line utility whose primary purpose is monitoring an application for CPU spikes and generating crash dumps during a spike that an administrator or developer can use to determine the cause of the spike." (official definition)



```
Y:\>procdump -accepteula

ProcDump v10.0 - Sysinternals process dump utility
Copyright (C) 2009-2020 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

Monitors a process and writes a dump file when the process exceeds the
specified criteria or has an exception.
```

Alternatively, you can use **Process Explorer** to do the same.

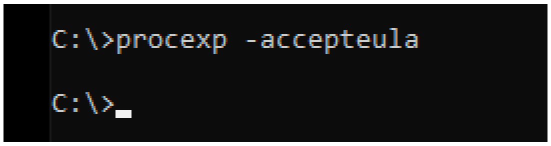
Right-click on the process to create a **Minidump** or **Full Dump** of the process.



Please refer to the examples listed on the ProcDump page to learn about all the available options with running this tool.

Process Explorer

"The **Process Explorer** display consists of two sub-windows. The top window always shows a list of the currently active processes, including the names of their owning accounts, whereas the information displayed in the bottom window depends on the mode that Process Explorer is in: if it is in handle mode you'll see the handles that the process selected in the top window has opened; if Process Explorer is in DLL mode you'll see the DLLs and memory-mapped files that the process has loaded." (official definition)

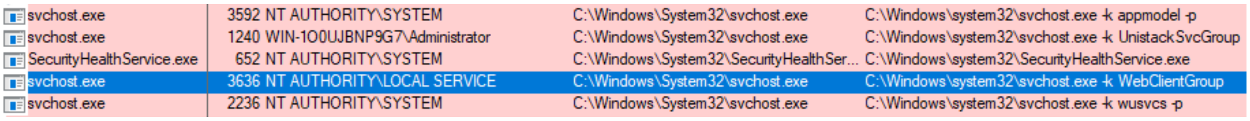


```
C:\>procexp -accepteula

C:\>
```

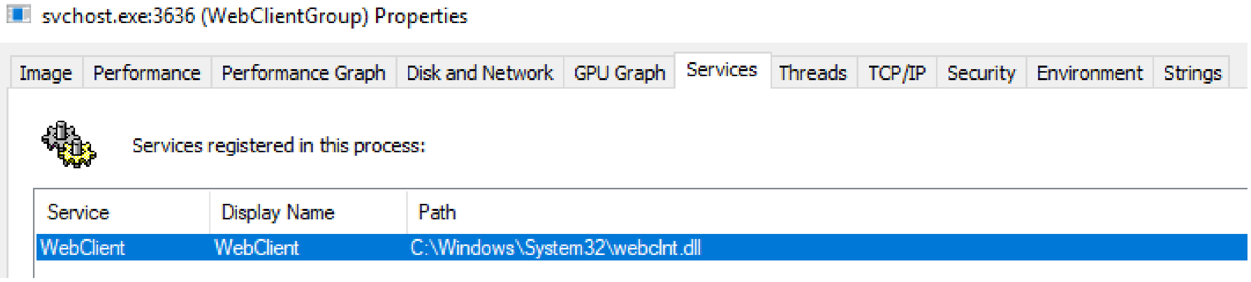
This tool was touched on slightly within the **Core Windows Processes** room. **Process Hacker** was intentionally used in that room to broaden your exposure to various tools that essentially perform the same tasks with subtle differences.

Since much of the basic foundational information was discussed in the **Core Windows Processes** room, Process Explorer will be briefly touched.

In the following images, let's look at svchost.exe PID 3636 more closely.



svchost.exe	3592 NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k appmodel -p
svchost.exe	1240 WIN-1O0UJBNP9G7\Administrator	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k UnistackSvcGroup
SecurityHealthService.exe	652 NT AUTHORITY\SYSTEM	C:\Windows\System32\SecurityHealthSer...	C:\Windows\system32\SecurityHealthService.exe
svchost.exe	3636 NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k WebClientGroup
svchost.exe	2236 NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k wusvcs -p



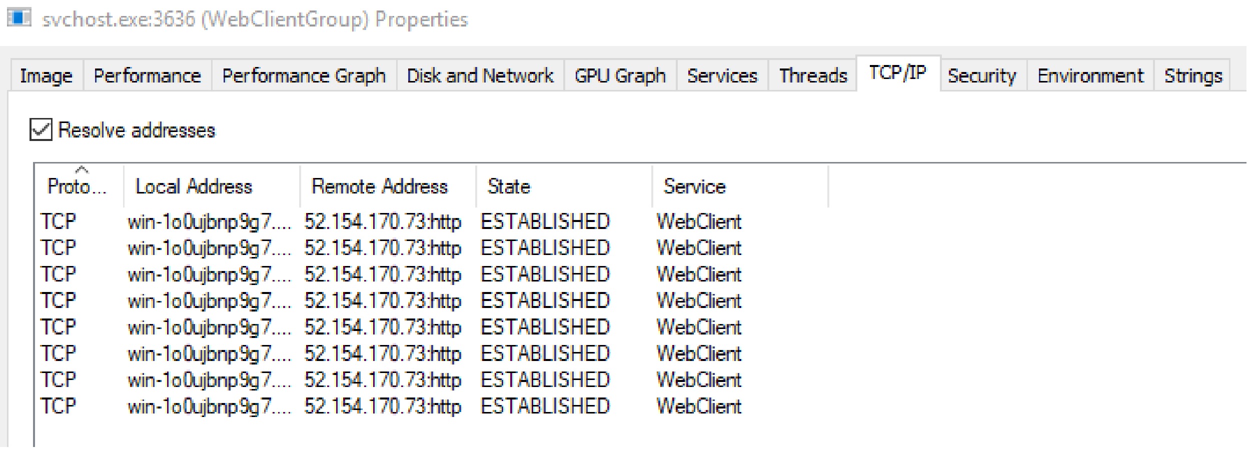
svchost.exe:3636 (WebClientGroup) Properties

Services registered in this process:

Service	Display Name	Path
WebClient	WebClient	C:\Windows\System32\webclnt.dll

This process is associated with the WebClient service that is needed to connect to live.sysinternals.com (WebDAV).

There should be web traffic listed in the TCP/IP tab.

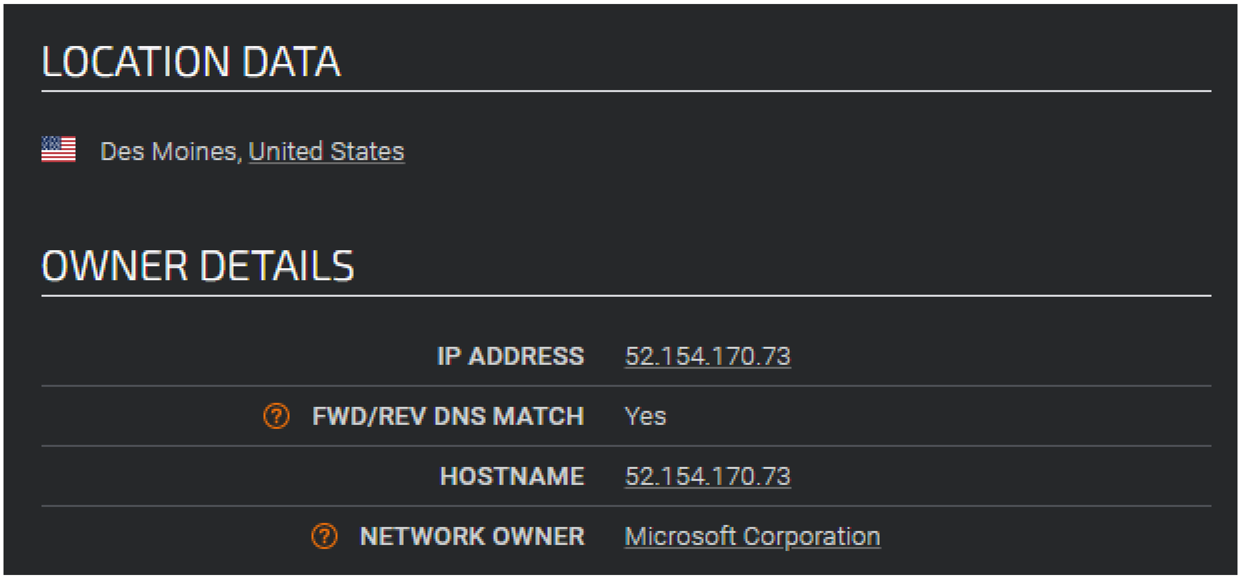


☑ Resolve addresses

Proto...	Local Address	Remote Address	State	Service
TCP	win-1o0ujbnp9g7....	52.154.170.73:http	ESTABLISHED	WebClient
TCP	win-1o0ujbnp9g7....	52.154.170.73:http	ESTABLISHED	WebClient
TCP	win-1o0ujbnp9g7....	52.154.170.73:http	ESTABLISHED	WebClient
TCP	win-1o0ujbnp9g7....	52.154.170.73:http	ESTABLISHED	WebClient
TCP	win-1o0ujbnp9g7....	52.154.170.73:http	ESTABLISHED	WebClient
TCP	win-1o0ujbnp9g7....	52.154.170.73:http	ESTABLISHED	WebClient
TCP	win-1o0ujbnp9g7....	52.154.170.73:http	ESTABLISHED	WebClient
TCP	win-1o0ujbnp9g7....	52.154.170.73:http	ESTABLISHED	WebClient

Ideally, it would be wise to check if that IP is what we assume it is.

Various online tools can be utilized to verify the authenticity of an IP address. For this demonstration, I'll use **Talos Reputation Center**.



LOCATION DATA

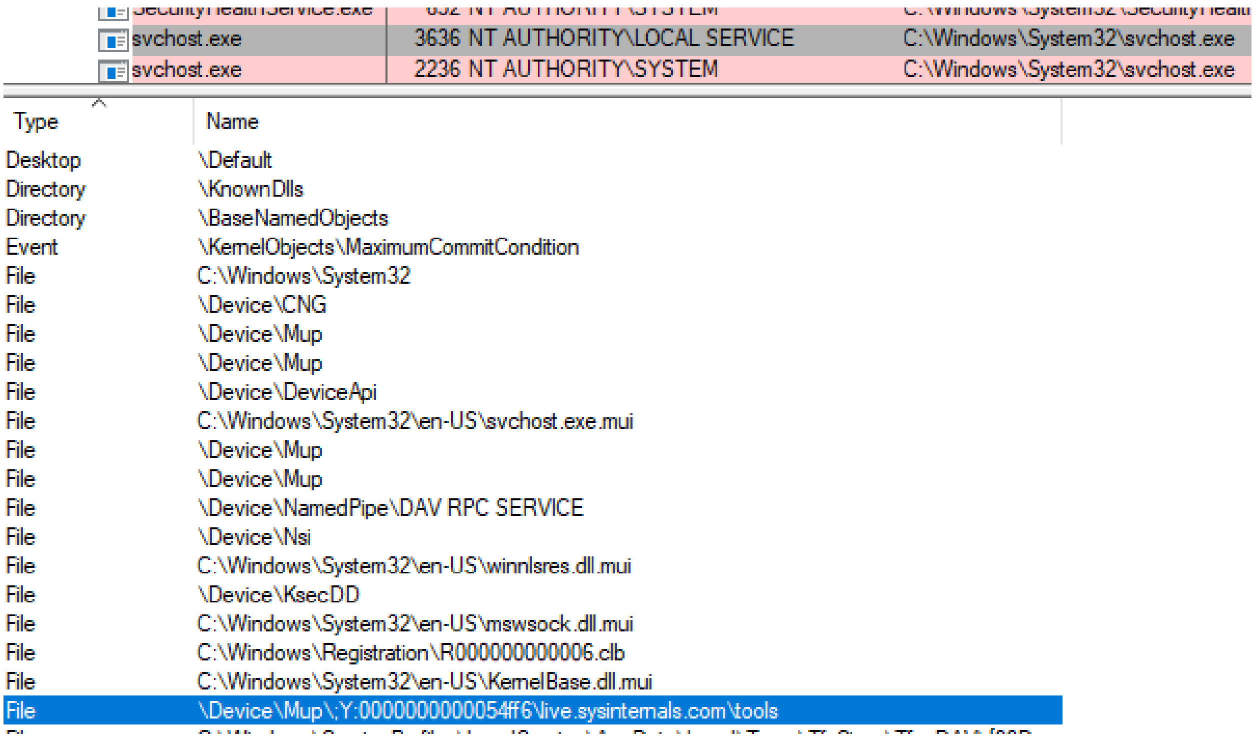
Des Moines, United States

OWNER DETAILS

IP ADDRESS	52.154.170.73
FWD/REV DNS MATCH	Yes
HOSTNAME	52.154.170.73
NETWORK OWNER	Microsoft Corporation

https://talosintelligence.com/reputation_center/lookup?search=52.154.170.73

As mentioned in the **ProcExp** description, we can see open handles associated with the process within the bottom window.

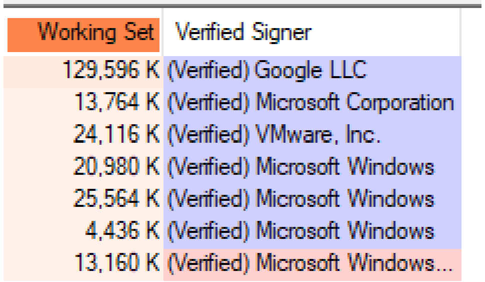


svchost.exe	3636 NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
svchost.exe	2236 NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe

Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\BaseNamedObjects
Event	\KernelObjects\MaximumCommitCondition
File	C:\Windows\System32
File	\Device\CNG
File	\Device\Mup
File	\Device\Mup
File	\Device\DeviceApi
File	C:\Windows\System32\en-US\svchost.exe.mui
File	\Device\Mup
File	\Device\Mup
File	\Device\NamedPipe\DAV RPC SERVICE
File	\Device\Nsi
File	C:\Windows\System32\en-US\winnlsres.dll.mui
File	\Device\KsecDD
File	C:\Windows\System32\en-US\mswsock.dll.mui
File	C:\Windows\Registration\R000000000006.clb
File	C:\Windows\System32\en-US\KernelBase.dll.mui
File	\Device\Mup\;Y:0000000000054ff6\live.sysinternals.com\tools

Listed as an open handle is the connection to the remote WebDAV folder.

There is an option within ProcExp to **Verify Signatures**. Once enabled, it shows up as a column within the Process view.

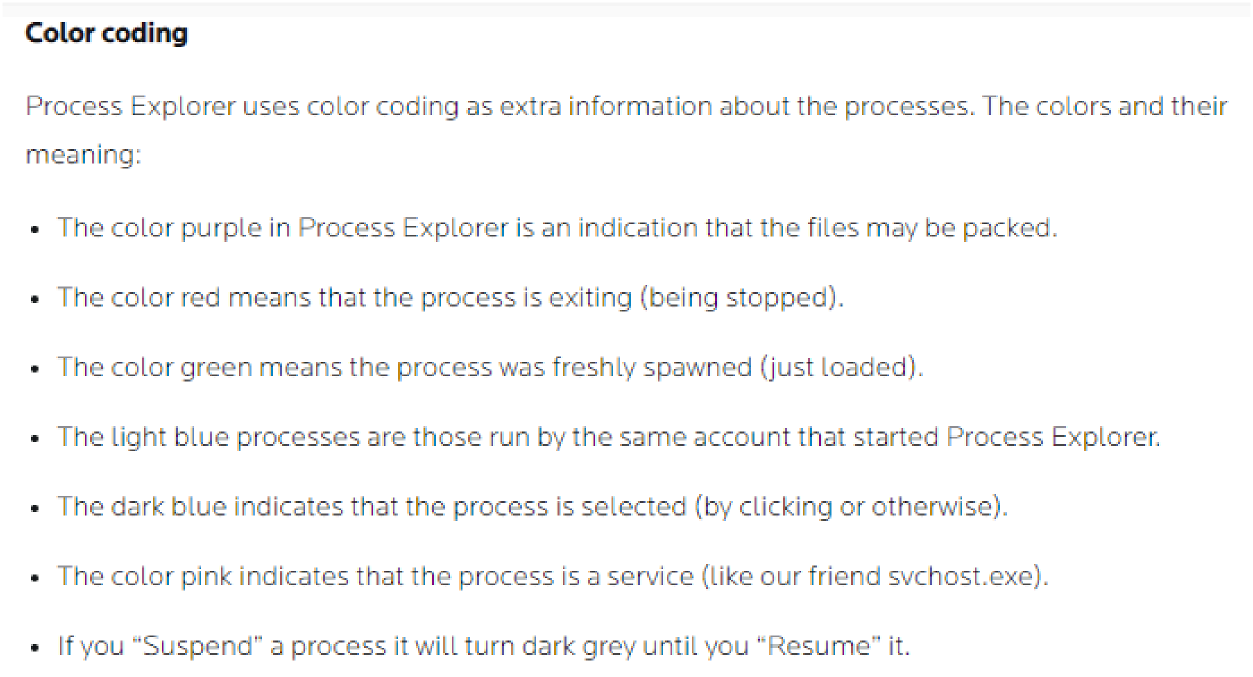


Working Set	Verified Signer
129,596 K	(Verified) Google LLC
13,764 K	(Verified) Microsoft Corporation
24,116 K	(Verified) VMware, Inc.
20,980 K	(Verified) Microsoft Windows
25,564 K	(Verified) Microsoft Windows
4,436 K	(Verified) Microsoft Windows
13,160 K	(Verified) Microsoft Windows...

Other options to note include **Run at Logon** and **Replace Task Manager**.

You may have noticed that some of the processes within Process Explorer have different colors. Those colors have meaning.

Below is a snippet from MalwareBytes explaining what each of those colors means.



Color coding

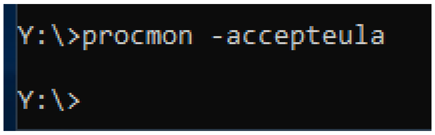
Process Explorer uses color coding as extra information about the processes. The colors and their meaning:

- The color purple in Process Explorer is an indication that the files may be packed.
- The color red means that the process is exiting (being stopped).
- The color green means the process was freshly spawned (just loaded).
- The light blue processes are those run by the same account that started Process Explorer.
- The dark blue indicates that the process is selected (by clicking or otherwise).
- The color pink indicates that the process is a service (like our friend svchost.exe).
- If you "Suspend" a process it will turn dark grey until you "Resume" it.

Process Monitor

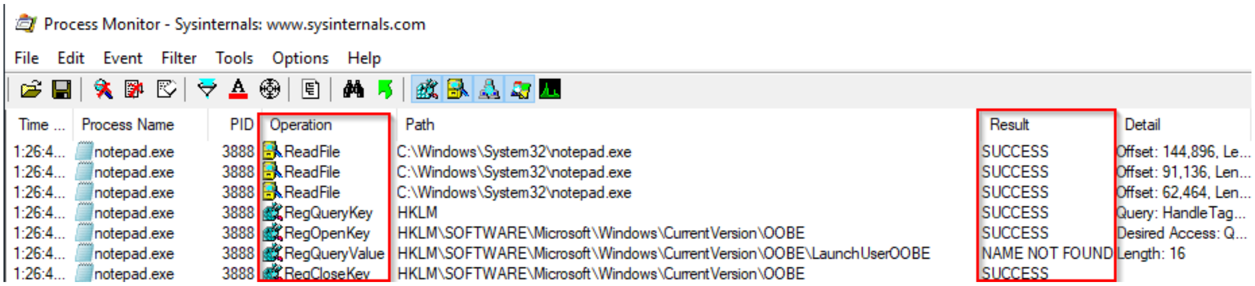
"Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such as session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit." (**official definition**)

Launch ProcMon.



```
Y:\>procmon -accepteula

Y:\>
```

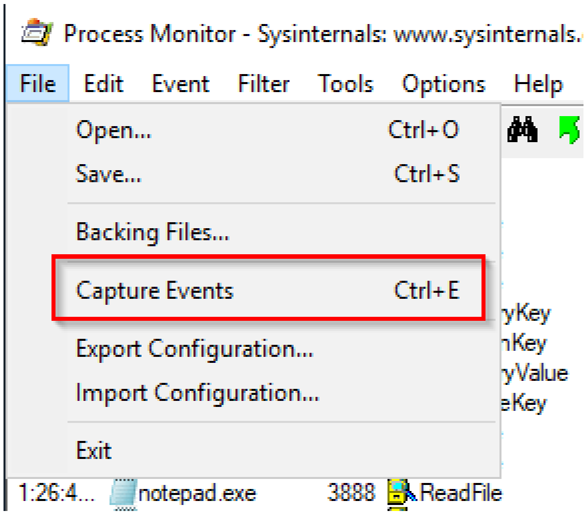
In the below snapshot, I set a filter to capture all the events related to PID 3888, notepad.exe. You can see some of the file operations that were captured and the file path or registry path/key the action occurred on, and the operation result.


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

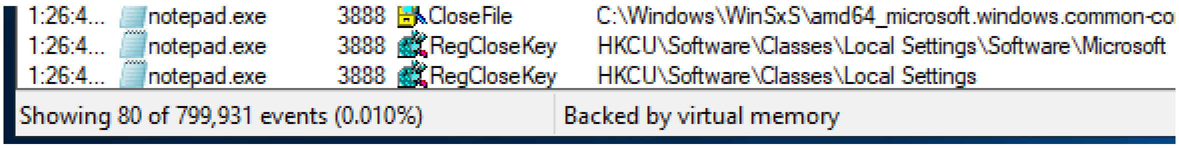
Time ...	Process Name	PID	Operation	Path	Result	Detail
1:26:4...	notepad.exe	3888	ReadFile	C:\Windows\System32\notepad.exe	SUCCESS	Offset: 144,896, Le...
1:26:4...	notepad.exe	3888	ReadFile	C:\Windows\System32\notepad.exe	SUCCESS	Offset: 91,136, Len...
1:26:4...	notepad.exe	3888	ReadFile	C:\Windows\System32\notepad.exe	SUCCESS	Offset: 62,464, Len...
1:26:4...	notepad.exe	3888	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
1:26:4...	notepad.exe	3888	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\OOBE	SUCCESS	Desired Access: Q...
1:26:4...	notepad.exe	3888	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\OOBE\LaunchUserOOBE	NAME NOT FOUND	Length: 16
1:26:4...	notepad.exe	3888	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\OOBE	SUCCESS	

ProcMon will capture thousands upon thousands of events occurring within the operating system.

The option to capture events can be toggled on and off.



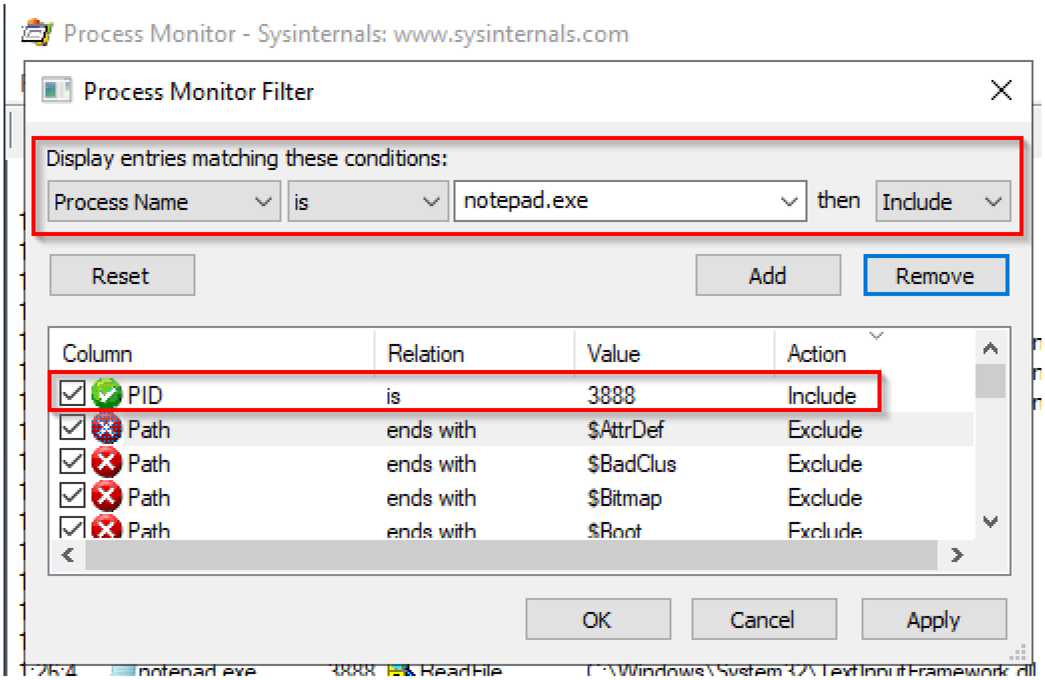
In this ProcMon example, the session captured events only for a few seconds. Look at how many events were captured in that short space of time!



1:26:4...	notepad.exe	3888	CloseFile	C:\Windows\WinSxS\amd64_microsoft.windows.common-co
1:26:4...	notepad.exe	3888	RegCloseKey	HKCU\Software\Classes\Local Settings\Software\Microsoft
1:26:4...	notepad.exe	3888	RegCloseKey	HKCU\Software\Classes\Local Settings

Showing 80 of 799,931 events (0.010%) Backed by virtual memory

To use ProcMon effectively you **must** use the Filter and **must** configure it properly.



Process Monitor - Sysinternals: www.sysinternals.com

Process Monitor Filter

Display entries matching these conditions:

Process Name | is | notepad.exe | then | Include

Column	Relation	Value	Action
☑ PID	is	3888	Include
☑ Path	ends with	$AttrDef	Exclude
☑ Path	ends with	$BadClus	Exclude
☑ Path	ends with	$Bitmap	Exclude
☑ Path	ends with	$Boot	Exclude

1:26:4 notepad.exe 3888 ReadFile C:\Windows\System32\TextInputFramework.dll

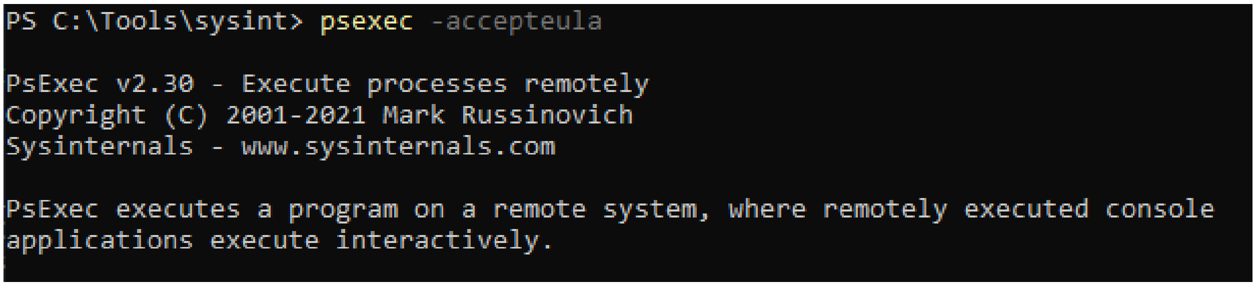
In the above image, a filter was already set to capture events associated with **PID** 3888. Alternatively, a filter could have been set to capture events with the **Process Name** = notepad.exe.

Here is a useful guide on configuring ProcMon.

Note: To fully understand the output from some of these tools you need to understand some Windows concepts, such as Processes and Threads and Windows API calls.

PsExec

"**PsExec** is a light-weight telnet-replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software. PsExec's most powerful uses include launching interactive command-prompts on remote systems and remote-enabling tools like IpConfig that otherwise do not have the ability to show information about remote systems." (official definition)



```
PS C:\Tools\sysint> psexec -accepteula

PsExec v2.30 - Execute processes remotely
Copyright (C) 2001-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

PsExec executes a program on a remote system, where remotely executed console
applications execute interactively.
```

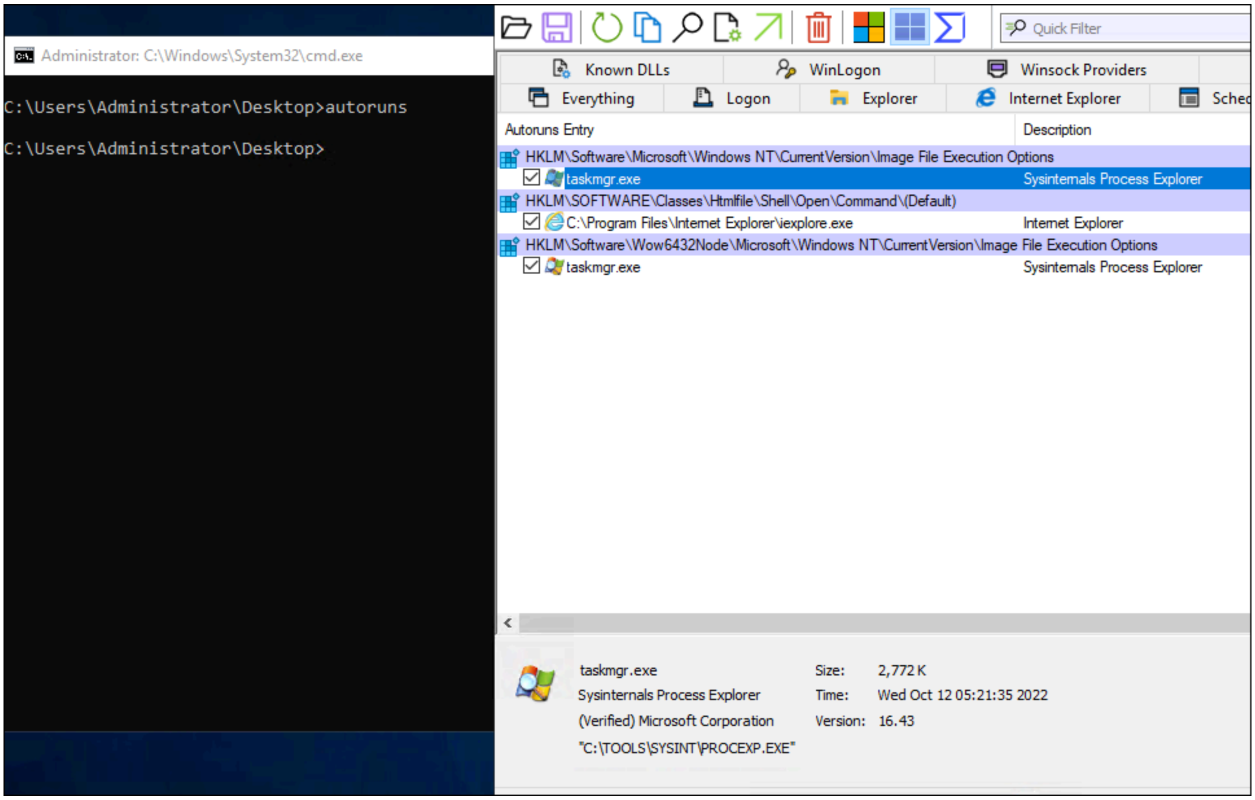
PsExec is another tool that is utilized by adversaries. This tool is associated with MITRE techniques T1570 (**Lateral Tool Transfer**), T1021.002 (**Remote Services: SMB/Windows Admin Shares**), and T1569.002 (**System Services: Service Execution**). It's MITRE ID is S0029.

You can review this tool more in-depth by visiting its Sysinternals PsExec page. You can also check out this resource page.

Other tools fall under the Process Utilities category. I encourage you to explore these tools at your own leisure.

Link: https://docs.microsoft.com/en-us/sysinternals/downloads/process-utilities

Answer the questions below



```
C:\Users\Administrator\Desktop>autoruns

C:\Users\Administrator\Desktop>
```

Autoruns Entry	Description
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	
☑ taskmgr.exe	Sysinternals Process Explorer
HKLM\SOFTWARE\Classes\Htmlfile\Shell\Open\Command\(Default)	
☑ C:\Program Files\Internet Explorer\iexplore.exe	Internet Explorer
HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	
☑ taskmgr.exe	Sysinternals Process Explorer

taskmgr.exe
Sysinternals Process Explorer
(Verified) Microsoft Corporation
"C:\TOOLS\SYSINT\PROCEXP.EXE"

Size: 2,772 K
Time: Wed Oct 12 05:21:35 2022
Version: 16.43

What entry was updated?

taskmgr.exe

What is the updated value?

C:\tools\sysint\procexp.exe

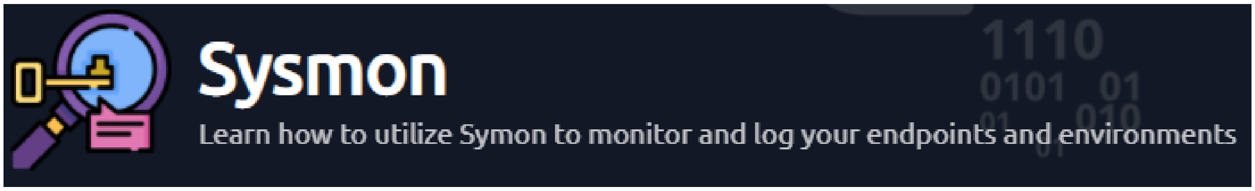
Task 7 Security Utilities

Sysmon

"System Monitor (Sysmon) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network." (**official definition**)

Sysmon is a comprehensive tool, and it can't be summarized in just one section.

Check out the Sysmon room to further learn what Sysmon is and how to use it.


Sysmon
Learn how to utilize Symon to monitor and log your endpoints and environments
1110
0101 01
01 010
01

Other tools fall under the Security Utilities category. I encourage you to explore these tools at your own leisure.

Link: https://docs.microsoft.com/en-us/sysinternals/downloads/security-utilities

Task 8 System Information

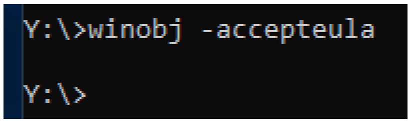
WinObj

"**WinObj** is a 32-bit Windows NT program that uses the native Windows NT API (provided by NTDLL.DLL) to access and display information on the NT Object Manager's name space." (**official definition**)

To showcase this tool, let's look into the concept of **Session 0** and **Session 1** that was mentioned in the Core Windows Processes room.

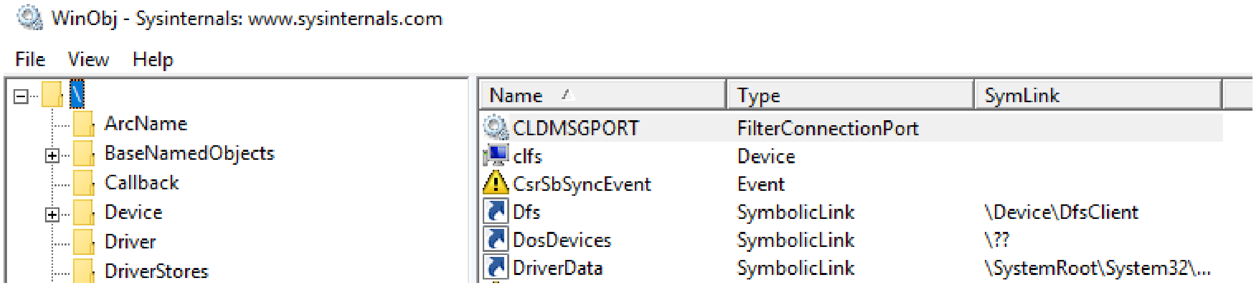
Remember that Session 0 is the OS session and Session 1 is the User session. Also recall that there will be at least 2 csrss.exe processes running, one for each session. **Note Session 1 will be for the first user logged into the system**.

Launch WinObj.



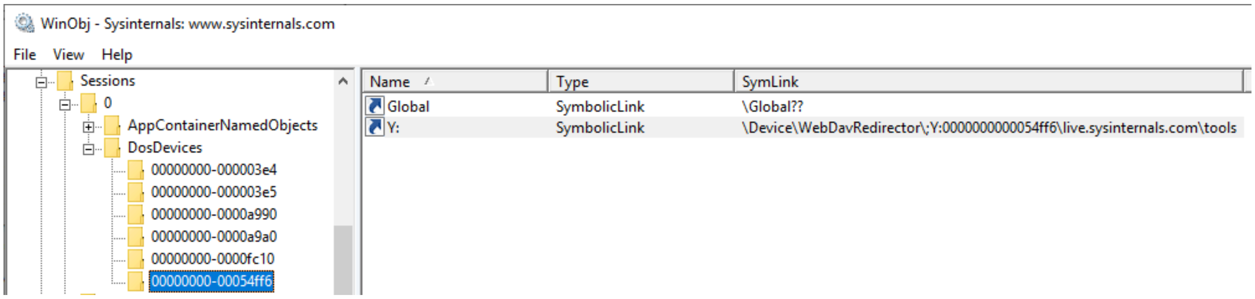
```
Y:\>winobj -accepteula

Y:\>
```

The below image shows the default view for WinObj.



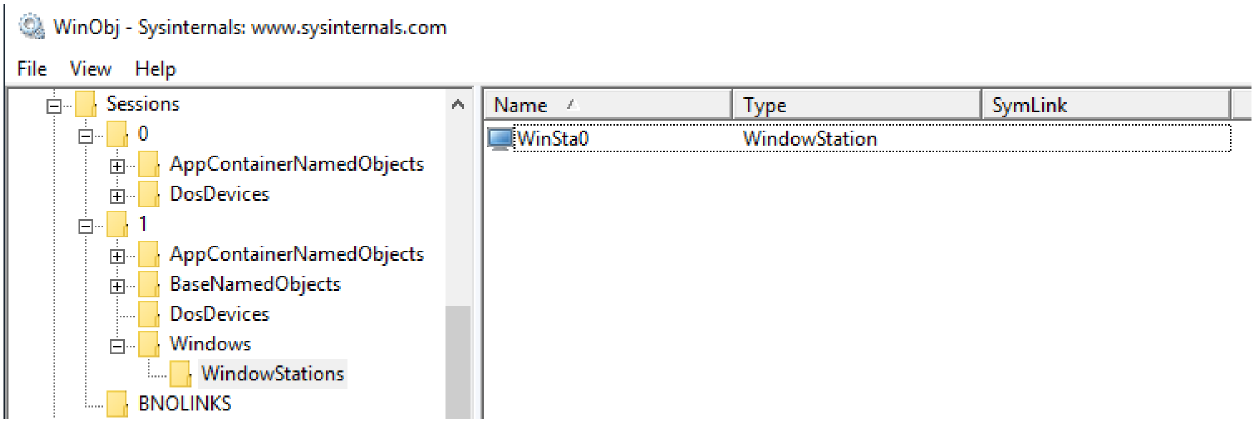
Name	Type	SymLink
CLDMSGPORT	FilterConnectionPort	
clfs	Device	
CsrSbSyncEvent	Event	
Dfs	SymbolicLink	\Device\DfsClient
DosDevices	SymbolicLink	\??
DriverData	SymbolicLink	\SystemRoot\System32\...

Within Session 0, under , there is an entry for the network drive I mounted in my local machine.



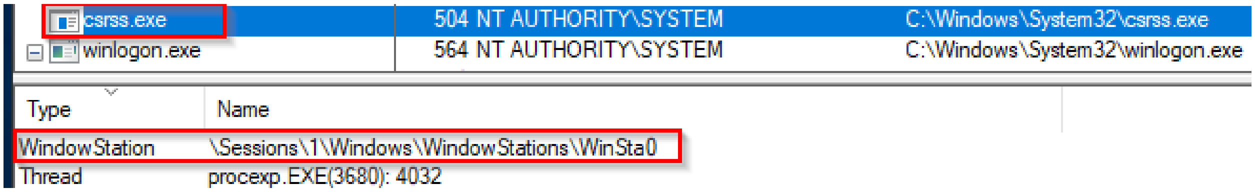
Name	Type	SymLink
Global	SymbolicLink	\Global??
Y:	SymbolicLink	\Device\WebDavRedirector\;Y:0000000000054ff6\live.sysinternals.com\tools

Let's look at value for Session 1.



Name	Type	SymLink
WinSta0	WindowStation	

Let's compare this information with Process Explorer. The below image is for **csrss.exe**, which was launched along with **winlogon.exe** by **smss.exe**.



```
csrss.exe          504 NT AUTHORITY\SYSTEM      C:\Windows\System32\csrss.exe
winlogon.exe       564 NT AUTHORITY\SYSTEM      C:\Windows\System32\winlogon.exe

Type               Name
WindowStation      \Sessions\1\Windows\WindowStations\WinSta0
Thread             procexp.EXE(3680): 4032
```

Note: This is a high-level exposure for this tool.

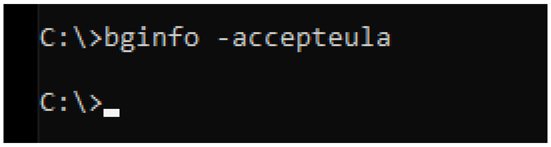
Other tools fall under the **System** Information category. I encourage you to explore these tools at your own leisure.

Link: https://docs.microsoft.com/en-us/sysinternals/downloads/system-information

Task 9   **Miscellaneous**

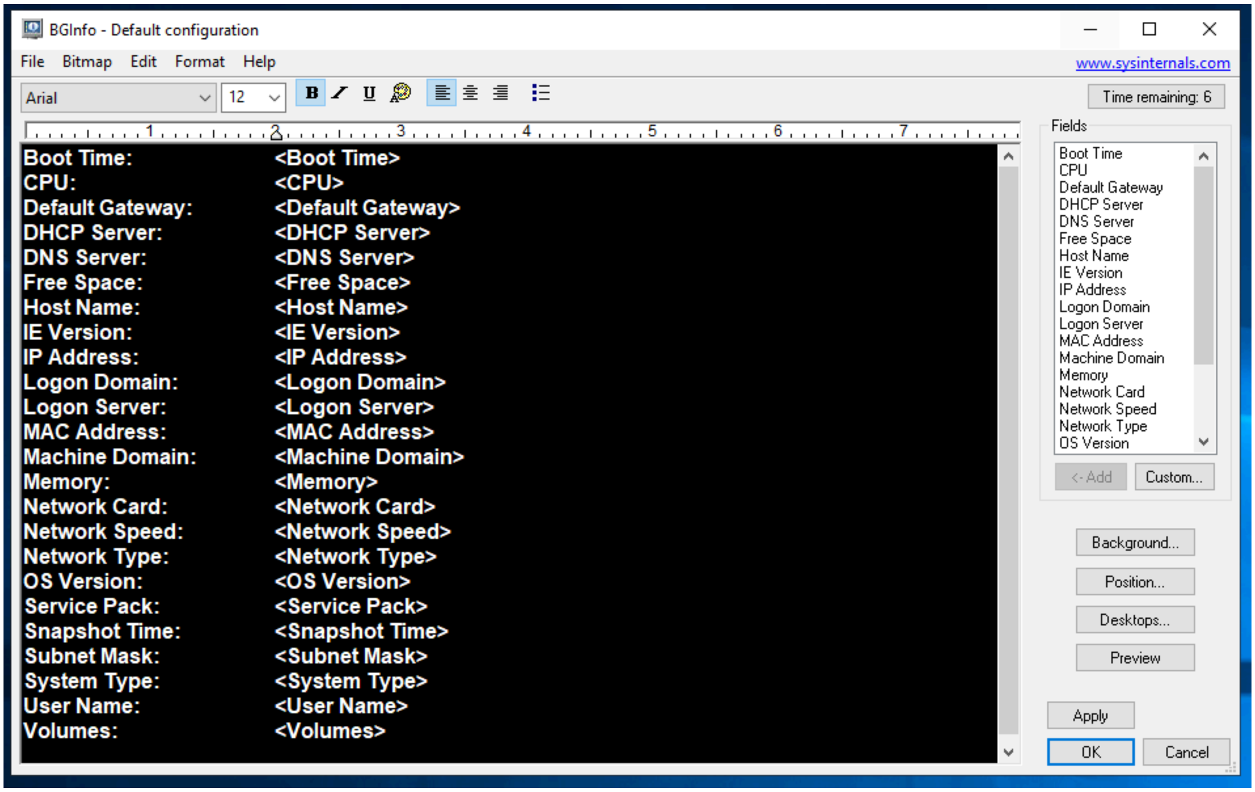
BgInfo

"It automatically displays relevant information about a Windows computer on the desktop's background, such as the computer name, IP address, service pack version, and more." (**official definition**)



```
C:\>bginfo -accepteula

C:\>_
```

This is a handy utility if you manage multiple machines. This tool, or similar tools, are typically utilized on servers. When a user RDPs into a server, the system information is displayed on the wallpaper to provide quick information about the server, such as the server's name.



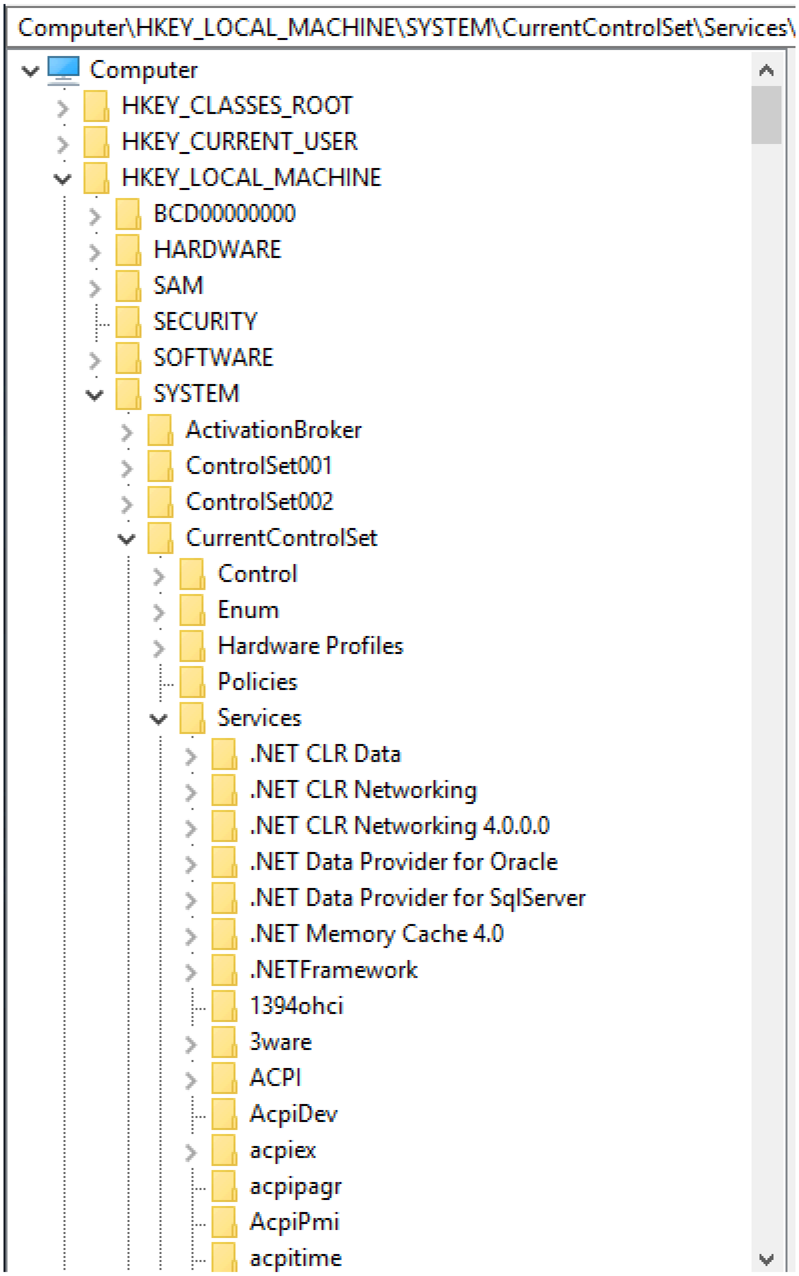
```
Boot Time:          <Boot Time>
CPU:                <CPU>
Default Gateway:    <Default Gateway>
DHCP Server:        <DHCP Server>
DNS Server:         <DNS Server>
Free Space:         <Free Space>
Host Name:          <Host Name>
IE Version:         <IE Version>
IP Address:         <IP Address>
Logon Domain:       <Logon Domain>
Logon Server:       <Logon Server>
MAC Address:        <MAC Address>
Machine Domain:     <Machine Domain>
Memory:             <Memory>
Network Card:       <Network Card>
Network Speed:      <Network Speed>
Network Type:       <Network Type>
OS Version:         <OS Version>
Service Pack:       <Service Pack>
Snapshot Time:      <Snapshot Time>
Subnet Mask:        <Subnet Mask>
System Type:        <System Type>
User Name:          <User Name>
Volumes:            <Volumes>
```

Refer to the Sysinternals BgInfo page for more information on installation and usage.

RegJump

"This little command-line applet takes a registry path and makes Regedit open to that path. It accepts root keys in standard (e.g. HKEY_LOCAL_MACHINE) and abbreviated form (e.g. HKLM)." (official definition)

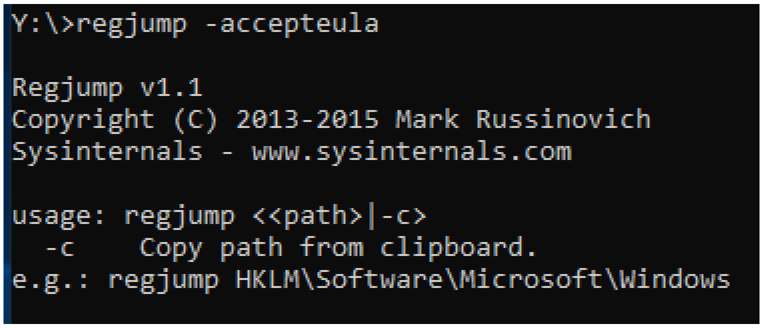
When navigating through the registry using the Registry Editor, one must manually drill down to the key you wish to inspect.



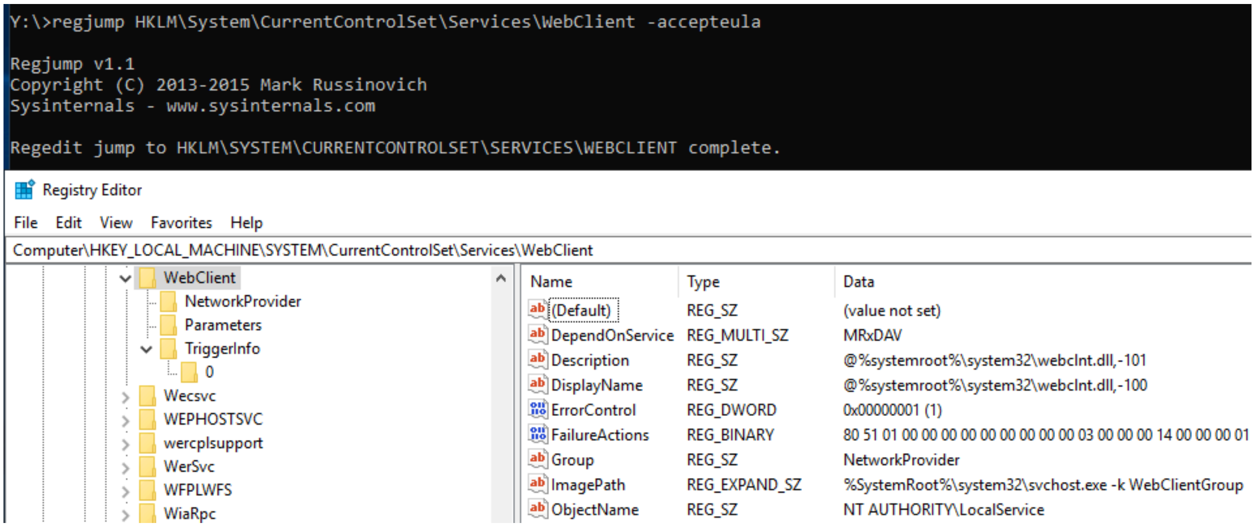
```
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
  HKEY_LOCAL_MACHINE
    BCD00000000
    HARDWARE
    SAM
    SECURITY
    SOFTWARE
    SYSTEM
      ActivationBroker
      ControlSet001
      ControlSet002
      CurrentControlSet
        Control
        Enum
        Hardware Profiles
        Policies
        Services
          .NET CLR Data
          .NET CLR Networking
          .NET CLR Networking 4.0.0.0
          .NET Data Provider for Oracle
          .NET Data Provider for SqlServer
          .NET Memory Cache 4.0
          .NETFramework
          1394ohci
          3ware
          ACPI
          AcpiDev
          acpiex
          acpipagr
          AcpiPmi
          acpitime
```

There are multiple ways to query the Windows Registry without using the Registry Editor, such as via the command line (   ) and PowerShell (/   ).

Using Regjump will open the Registry Editor and automatically open the editor directly at the path, so one doesn't need to navigate it manually.



```
Y:\>regjump -accepteula

Regjump v1.1
Copyright (C) 2013-2015 Mark Russinovich
Sysinternals - www.sysinternals.com

usage: regjump <<path>|-c>
  -c    Copy path from clipboard.
e.g.: regjump HKLM\Software\Microsoft\Windows
```



```
Y:\>regjump HKLM\System\CurrentControlSet\Services\WebClient -accepteula

Regjump v1.1
Copyright (C) 2013-2015 Mark Russinovich
Sysinternals - www.sysinternals.com

Regedit jump to HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\WEBCLIENT complete.
```

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient

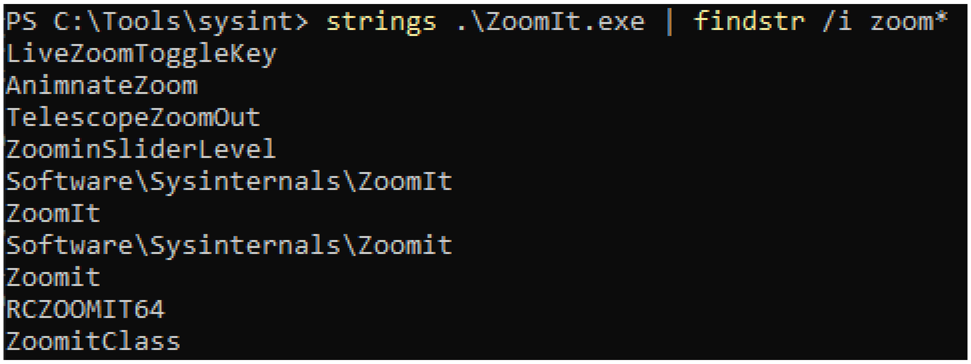
Name	Type	Data
(Default)	REG_SZ	(value not set)
DependOnService	REG_MULTI_SZ	MRxDAV
Description	REG_SZ	@%systemroot%\system32\webclnt.dll,-101
DisplayName	REG_SZ	@%systemroot%\system32\webclnt.dll,-100
ErrorControl	REG_DWORD	0x00000001 (1)
FailureActions	REG_BINARY	80 51 01 00 00 00 00 00 00 00 00 00 03 00 00 00 14 00 00 00 01
Group	REG_SZ	NetworkProvider
ImagePath	REG_EXPAND_SZ	%SystemRoot%\system32\svchost.exe -k WebClientGroup
ObjectName	REG_SZ	NT AUTHORITY\LocalService

Strings

"Strings just scans the file you pass it for UNICODE (or ASCII) strings of a default length of 3 or more UNICODE (or ASCII) characters. Note that it works under Windows 95 as well." (official definition)

This is the tool that was used on Day 21 of AoC2 to inspect a mysterious binary.

The example below **strings** is used to search within the ZoomIt binary for any string containing the word 'zoom'.



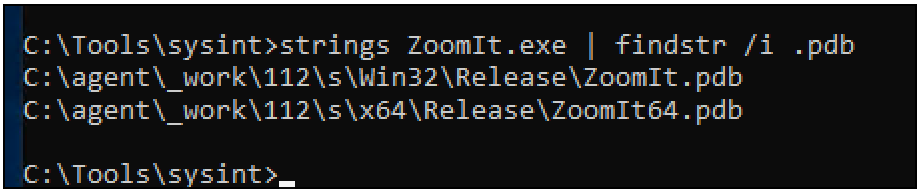
```
PS C:\Tools\sysint> strings .\ZoomIt.exe | findstr /i zoom*
LiveZoomToggleKey
AnimnateZoom
TelescopeZoomOut
ZoominSliderLevel
Software\Sysinternals\ZoomIt
ZoomIt
Software\Sysinternals\Zoomit
Zoomit
RCZOOMIT64
ZoomitClass
```

Other tools fall under the **Miscellaneous** category. I encourage you to explore these tools at your own leisure.

Link: https://docs.microsoft.com/en-us/sysinternals/downloads/misc-utilities

Answer the questions below

Run the Strings tool on ZoomIt.exe. What is the full path to the .pdb file?



```
C:\Tools\sysint>strings ZoomIt.exe | findstr /i .pdb
C:\agent\_work\112\s\Win32\Release\ZoomIt.pdb
C:\agent\_work\112\s\x64\Release\ZoomIt64.pdb

C:\Tools\sysint>_
```

C:\agent_work\112\s\Win32\Release\ZoomIt.pdb

Task 10 Conclusion

When you read the Sysinternals documentation, it might hint these tools are for troubleshooting purposes only, but that is not entirely the case.

You should know or be familiar with the Sysinternals tools whether you're a Desktop Engineer, Systems Analyst, or Security Engineer.

Real-world scenario: As a security engineer, I had to work with vendors to troubleshoot why an agent wasn't responding on an endpoint—the tools used were **ProcExp**, **ProcMon**, and **ProcDump**.

- ProcExp = to inspect the agent process, its properties, and associated threads and handles.
- ProcMon = to investigate if there were any indicators on why the agent was not operating as it should.

- ProcDump = to create a dump of the agent process to send to the vendor for further analysis.

And guess what? Asking questions about Sysinternals became part of the interview questions when hiring additional staff.

Remember, red teamers and adversaries even use these tools.

Below are some additional links to further your knowledge on how to use these tools as a Security Analyst, Security Engineer, or even an Incident Responder:

- Mark's Blog - https://docs.microsoft.com/en-us/archive/blogs/markrussinovich/
- Windows Blog Archive - https://techcommunity.microsoft.com/t5/windows-blog-archive/bg-p/Windows-Blog-Archive/label-name/Mark%20Russinovich
- License to Kill: Malware Hunting with Sysinternals Tools - https://www.youtube.com/watch?v=A_TPZxuTzBU

- Malware Hunting with Mark Russinovich and the Sysinternals Tools - https://www.youtube.com/watch?v=vW8eAqZyWeo

Note: Some of the videos/blogs are a bit outdated, but they're still good to review as it showcases how to use these tools extensively. This will build your foundation on the tools covered, along with the tools that weren't covered in this room.