7/31/2021

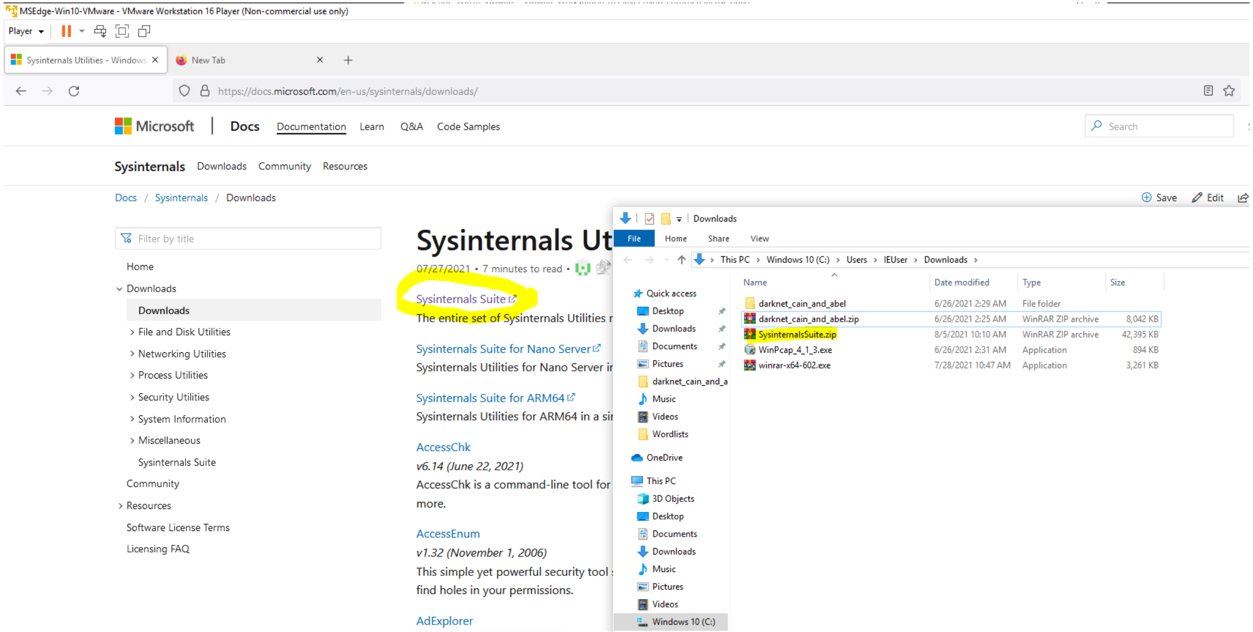
WINDOWS SYSINTERNALS

Table of Contents

Part 1: Sysinternals

PART 1.1 What Are the SysInternals Tools and How Do You Use Them?

1. Start your windows virtual machine.
2. Install Sysinternals, for this download the zip file and extract the file. All the applications in the package are ready to use no need to install them.



MSEdge-Win10-VMware - VMware Workstation 16 Player (Non-commercial use only)

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

Docs / Sysinternals / Downloads

Sysinternals Ut

07/27/2021 • 7 minutes to read

Sysinternals Suite

The entire set of Sysinternals Utilities r

Sysinternals Suite for Nano Server

Sysinternals Utilities for Nano Server ir

Sysinternals Suite for ARM64

Sysinternals Utilities for ARM64 in a si

AccessChk

v6.14 (June 22, 2021)

AccessChk is a command-line tool for more.

AccessEnum

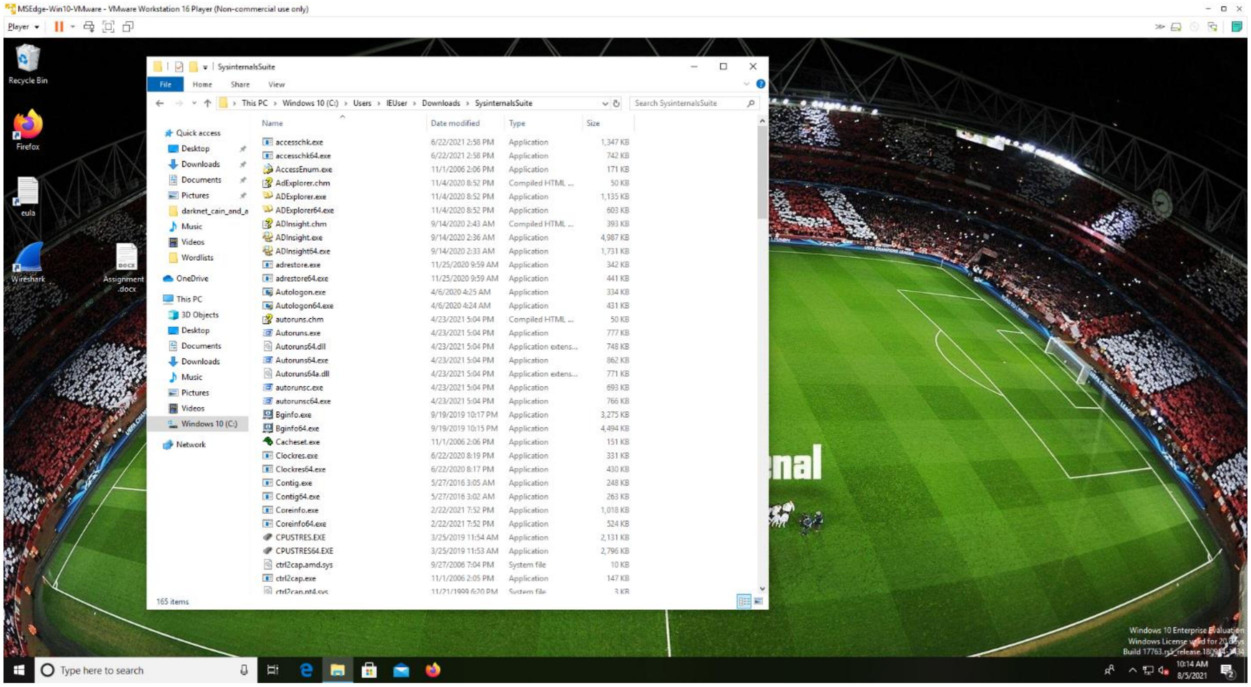
v1.32 (November 1, 2006)

This simple yet powerful security tool find holes in your permissions.

AdExplorer

This PC › Windows 10 (C:) › Users › IEUser › Downloads ›

Name	Date modified	Type	Size
darknet_cain_and_abel	6/26/2021 2:29 AM	File folder	
darknet_cain_and_abel.zip	6/26/2021 2:25 AM	WinRAR ZIP archive	8,042 KB
SysinternalsSuite.zip	8/5/2021 10:10 AM	WinRAR ZIP archive	42,395 KB
WinPcap_4_1_3.exe	6/26/2021 2:31 AM	Application	894 KB
winrar-x64-602.exe	7/28/2021 10:47 AM	Application	3,261 KB



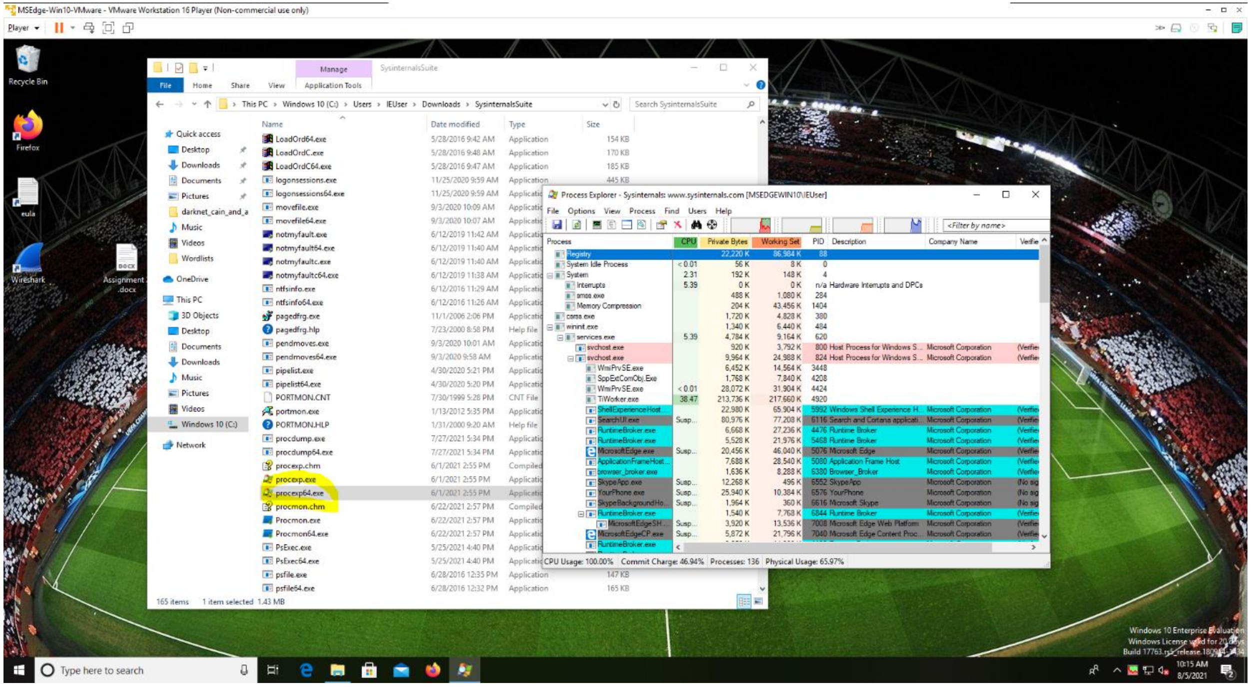
MSEdge-Win10-VMware - VMware Workstation 16 Player (Non-commercial use only)

This PC › Windows 10 (C:) › Users › IEUser › Downloads › SysinternalsSuite

Name	Date modified	Type	Size
accesschk.exe	6/22/2021 2:58 PM	Application	1,347 KB
accesschk64.exe	6/22/2021 2:58 PM	Application	742 KB
AccessEnum.exe	11/1/2006 2:06 PM	Application	171 KB
AdExplorer.chm	11/4/2020 8:52 PM	Compiled HTML ...	50 KB
ADExplorer.exe	11/4/2020 8:52 PM	Application	1,135 KB
ADExplorer64.exe	11/4/2020 8:52 PM	Application	603 KB
ADInsight.chm	9/14/2020 2:43 AM	Compiled HTML ...	393 KB
ADInsight.exe	9/14/2020 2:36 AM	Application	4,987 KB
ADInsight64.exe	9/14/2020 2:33 AM	Application	1,731 KB
adrestore.exe	11/25/2020 9:59 AM	Application	342 KB
adrestore64.exe	11/25/2020 9:59 AM	Application	441 KB
Autologon.exe	4/6/2020 4:25 AM	Application	334 KB
Autologon64.exe	4/6/2020 4:24 AM	Application	431 KB
autoruns.chm	4/23/2021 5:04 PM	Compiled HTML ...	50 KB
Autoruns.exe	4/23/2021 5:04 PM	Application	777 KB
Autoruns64.dll	4/23/2021 5:04 PM	Application extens...	748 KB
Autoruns64.exe	4/23/2021 5:04 PM	Application	862 KB
Autoruns64a.dll	4/23/2021 5:04 PM	Application extens...	771 KB
autorunsc.exe	4/23/2021 5:04 PM	Application	693 KB
autorunsc64.exe	4/23/2021 5:04 PM	Application	766 KB
Bginfo.exe	9/19/2019 10:17 PM	Application	3,275 KB
Bginfo64.exe	9/19/2019 10:15 PM	Application	4,494 KB
Cacheset.exe	11/1/2006 2:06 PM	Application	151 KB
Clockres.exe	6/22/2020 8:19 PM	Application	331 KB
Clockres64.exe	6/22/2020 8:17 PM	Application	430 KB
Contig.exe	5/27/2016 3:05 AM	Application	248 KB
Contig64.exe	5/27/2016 3:02 AM	Application	263 KB
Coreinfo.exe	2/22/2021 7:52 PM	Application	1,018 KB
Coreinfo64.exe	2/22/2021 7:52 PM	Application	524 KB
CPUSTRES.EXE	3/25/2019 11:54 AM	Application	2,131 KB
CPUSTRES64.EXE	3/25/2019 11:53 AM	Application	2,796 KB
ctrl2cap.amd.sys	9/27/2006 7:04 PM	System file	10 KB
ctrl2cap.exe	11/1/2006 2:05 PM	Application	147 KB
ctrl2cap.nt4.sys	11/21/1999 6:20 PM	System file	3 KB

165 items

3. Open the application procexp64.exe which is the application we are working on today.



MSEdge-Win10-VMware - VMware Workstation 16 Player (Non-commercial use only)

This PC › Windows 10 (C:) › Users › IEUser › Downloads › SysinternalsSuite

Name	Date modified	Type	Size
LoadOrd64.exe	5/28/2016 9:42 AM	Application	154 KB
LoadOrdC.exe	5/28/2016 9:48 AM	Application	170 KB
LoadOrdC64.exe	5/28/2016 9:47 AM	Application	185 KB
logonsessions.exe	11/25/2020 9:59 AM	Application	445 KB
logonsessions64.exe	11/25/2020 9:59 AM	Applicati	
movefile.exe	9/3/2020 10:09 AM	Applicati	
movefile64.exe	9/3/2020 10:07 AM	Applicati	
notmyfault.exe	6/12/2019 11:42 AM	Applicati	
notmyfault64.exe	6/12/2019 11:40 AM	Applicati	
notmyfaultc.exe	6/12/2019 11:40 AM	Applicati	
notmyfaultc64.exe	6/12/2019 11:38 AM	Applicati	
ntfsinfo.exe	6/12/2016 11:29 AM	Applicati	
ntfsinfo64.exe	6/12/2016 11:26 AM	Applicati	
pagedfrg.exe	11/1/2006 2:06 PM	Applicati	
pagedfrg.hlp	7/23/2000 8:58 PM	Help file	
pendmoves.exe	9/3/2020 10:01 AM	Applicati	
pendmoves64.exe	9/3/2020 9:58 AM	Applicati	
pipelist.exe	4/30/2020 5:21 PM	Applicati	
pipelist64.exe	4/30/2020 5:20 PM	Applicati	
PORTMON.CNT	7/30/1999 5:28 PM	CNT File	
portmon.exe	1/13/2012 5:35 PM	Applicati	
PORTMON.HLP	1/31/2000 9:20 AM	Help file	
procdump.exe	7/27/2021 5:34 PM	Applicati	
procdump64.exe	7/27/2021 5:34 PM	Applicati	
procexp.chm	6/1/2021 2:55 PM	Compiled	
procexp.exe	6/1/2021 2:55 PM	Applicati	
procexp64.exe	6/1/2021 2:55 PM	Applicati	
procmon.chm	6/22/2021 2:57 PM	Compiled	
Procmon.exe	6/22/2021 2:57 PM	Applicati	
Procmon64.exe	6/22/2021 2:57 PM	Applicati	
PsExec.exe	5/25/2021 4:40 PM	Applicati	
PsExec64.exe	5/25/2021 4:40 PM	Applicati	
psfile.exe	6/28/2016 12:35 PM	Application	147 KB
psfile64.exe	6/28/2016 12:32 PM	Application	165 KB

165 items 1 item selected 1.43 MB

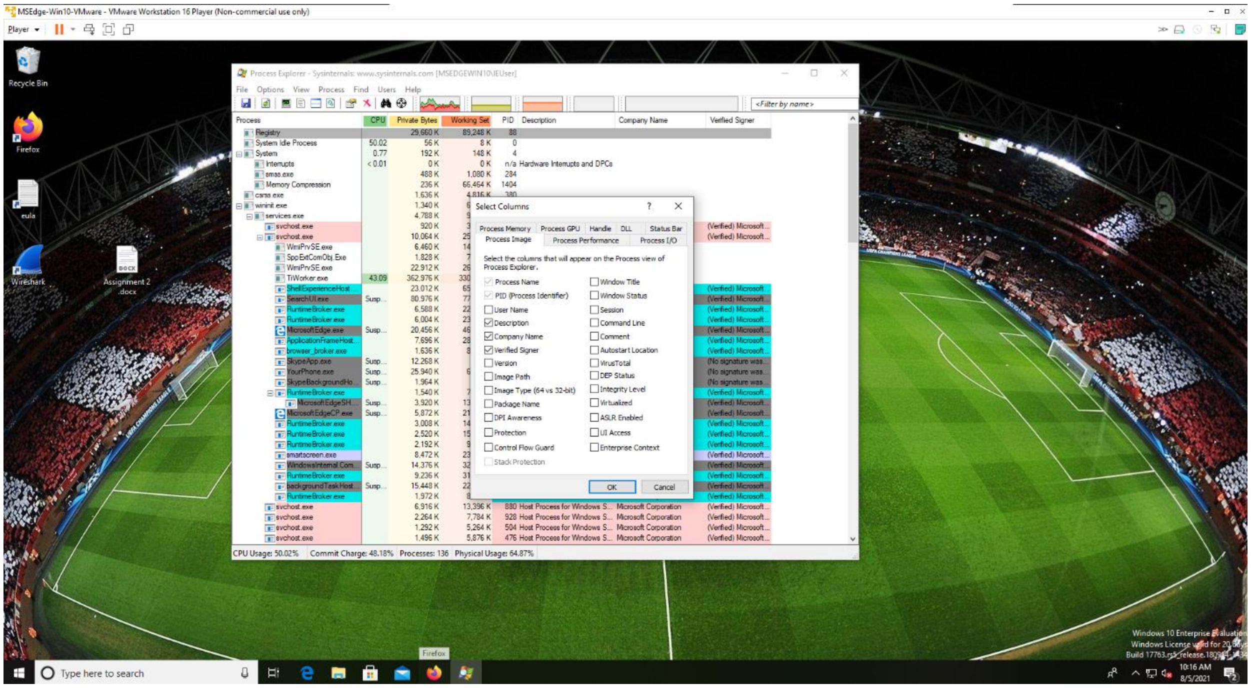
Process Explorer - Sysinternals: www.sysinternals.com [MSEDGEWIN10\IEUser]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verifie
Registry		22,220 K	86,984 K	88			
System Idle Process	< 0.01	56 K	8 K	0			
System	2.31	192 K	148 K	4			
Interrupts	5.39	0 K	0 K	n/a	Hardware Interrupts and DPCs		
smss.exe		488 K	1,080 K	284			
Memory Compression		204 K	43,456 K	1404			
csrss.exe		1,720 K	4,828 K	380			
wininit.exe		1,340 K	6,440 K	484			
services.exe	5.39	4,784 K	9,164 K	620			
svchost.exe		920 K	3,792 K	800	Host Process for Windows S...	Microsoft Corporation	(Verifie
svchost.exe		9,964 K	24,988 K	824	Host Process for Windows S...	Microsoft Corporation	(Verifie
WmiPrvSE.exe		6,452 K	14,564 K	3448			
SppExtComObj.Exe		1,768 K	7,840 K	4208			
WmiPrvSE.exe	< 0.01	28,072 K	31,904 K	4424			
TiWorker.exe	38.47	213,736 K	217,660 K	4920			
ShellExperienceHost...		22,980 K	65,904 K	5992	Windows Shell Experience H...	Microsoft Corporation	(Verifie
SearchUI.exe	Susp...	80,976 K	77,208 K	6116	Search and Cortana applicati...	Microsoft Corporation	(Verifie
RuntimeBroker.exe		6,668 K	27,236 K	4476	Runtime Broker	Microsoft Corporation	(Verifie
RuntimeBroker.exe		5,528 K	21,976 K	5468	Runtime Broker	Microsoft Corporation	(Verifie
MicrosoftEdge.exe	Susp...	20,456 K	46,040 K	5076	Microsoft Edge	Microsoft Corporation	(Verifie
ApplicationFrameHost...		7,688 K	28,540 K	5080	Application Frame Host	Microsoft Corporation	(Verifie
browser_broker.exe		1,636 K	8,288 K	6380	Browser_Broker	Microsoft Corporation	(Verifie
SkypeApp.exe	Susp...	12,268 K	496 K	6552	SkypeApp	Microsoft Corporation	(No sig
YourPhone.exe	Susp...	25,940 K	10,384 K	6576	YourPhone	Microsoft Corporation	(No sig
SkypeBackgroundHo...	Susp...	1,964 K	360 K	6616	Microsoft Skype	Microsoft Corporation	(No sig
RuntimeBroker.exe		1,540 K	7,768 K	6844	Runtime Broker	Microsoft Corporation	(Verifie
MicrosoftEdgeSH...	Susp...	3,920 K	13,536 K	7008	Microsoft Edge Web Platform	Microsoft Corporation	(Verifie
MicrosoftEdgeCP.exe	Susp...	5,872 K	21,796 K	7040	Microsoft Edge Content Proc...	Microsoft Corporation	(Verifie
RuntimeBroker.exe							

CPU Usage: 100.00% Commit Charge: 46.94% Processes: 136 Physical Usage: 65.97%

PART 1.2 UNDERSTANDING PROCESS EXPLORER

1. As Shown in the images above, the process explorer provides several columns of data like, Process, CPU, Private Bytes, Working Set, PID, Description and Company name. One can customize the columns as per the needs, several options available are listed in the screenshot below. To do this, Right click on columns and select the Columns u want to add in the list.


MSEdge-Win10-VMware - VMware Workstation 16 Player (Non-commercial use only)

Process Explorer - Sysinternals: www.sysinternals.com [MSEDGEWIN10\IEUser]

Select Columns

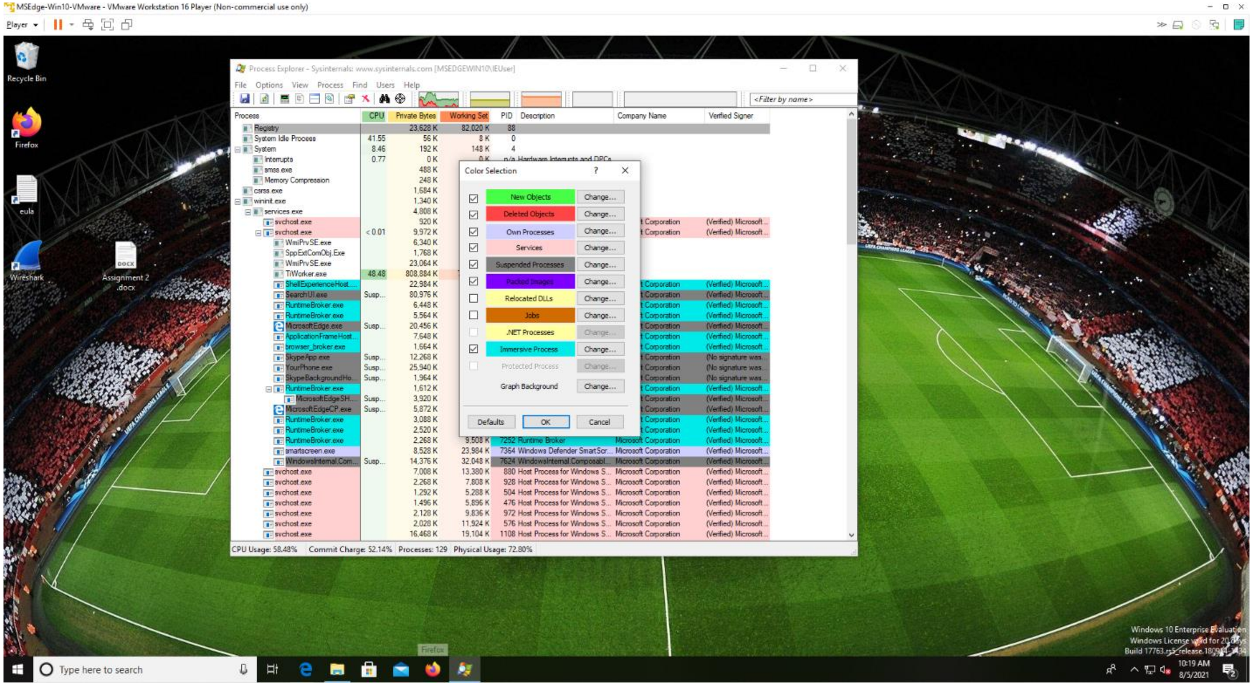
Process Memory | Process GPU | Handle | DLL | Status Bar
Process Image | Process Performance | Process I/O

Select the columns that will appear on the Process view of Process Explorer.

☑ Process Name
☑ PID (Process Identifier)
□ User Name
☑ Description
☑ Company Name
☑ Verified Signer
□ Version
□ Image Path
□ Image Type (64 vs 32-bit)
□ Package Name
□ DPI Awareness
□ Protection
□ Control Flow Guard
□ Stack Protection
□ Window Title
□ Window Status
□ Session
□ Command Line
□ Comment
□ Autostart Location
□ VirusTotal
□ DEP Status
□ Integrity Level
□ Virtualized
□ ASLR Enabled
□ UI Access
□ Enterprise Context

CPU Usage: 50.02% Commit Charge: 48.18% Processes: 136 Physical Usage: 64.87%

2. We can configure colors for the tasks, and if you don’t remember what a color defines simply click on options and select Configure colors. Color Selection tab will pop up to apply changes. These specific colors define specific types of processes like green color define new process or objects.


MSEdge-Win10-VMware - VMware Workstation 16 Player (Non-commercial use only)

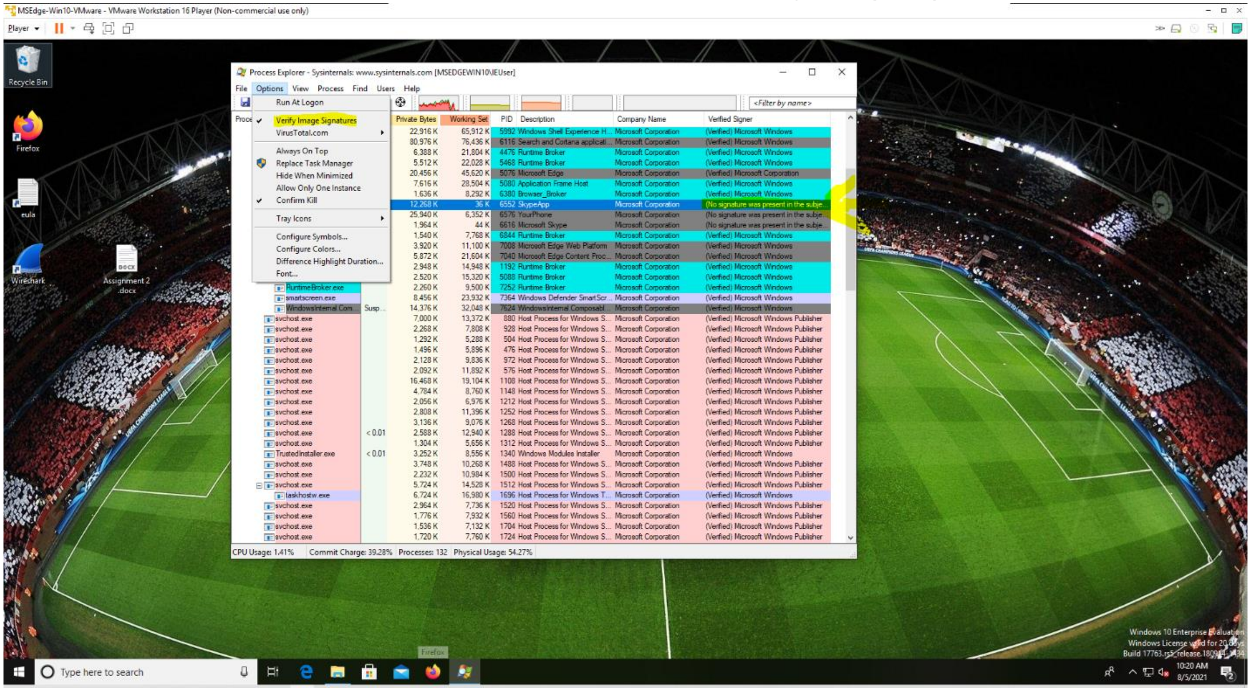
Process Explorer - Sysinternals: www.sysinternals.com [MSEDGEWIN10\IEUser]

Color Selection

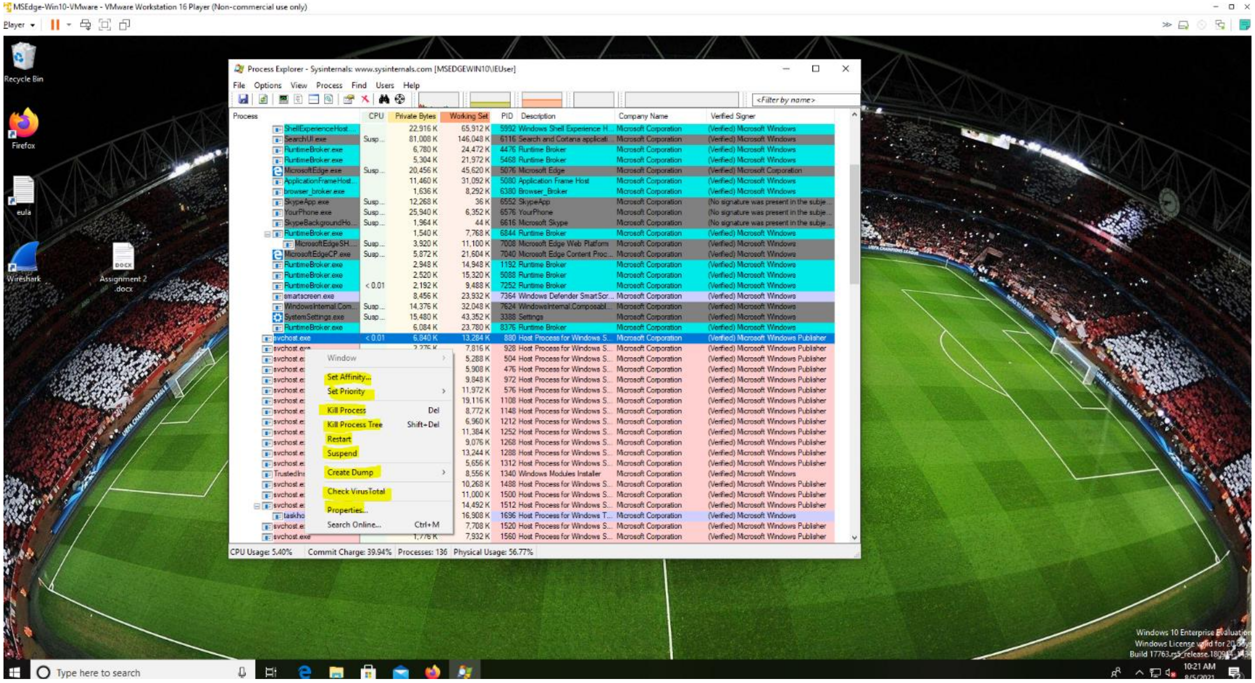
☑ New Objects
☑ Deleted Objects
☑ Own Processes
☑ Services
☑ Suspended Processes
☑ Packed Images
□ Relocated DLLs
□ Jobs
□ .NET Processes
☑ Immersive Process
□ Protected Process
Graph Background

CPU Usage: 58.48% Commit Charge: 52.14% Processes: 129 Physical Usage: 72.80%

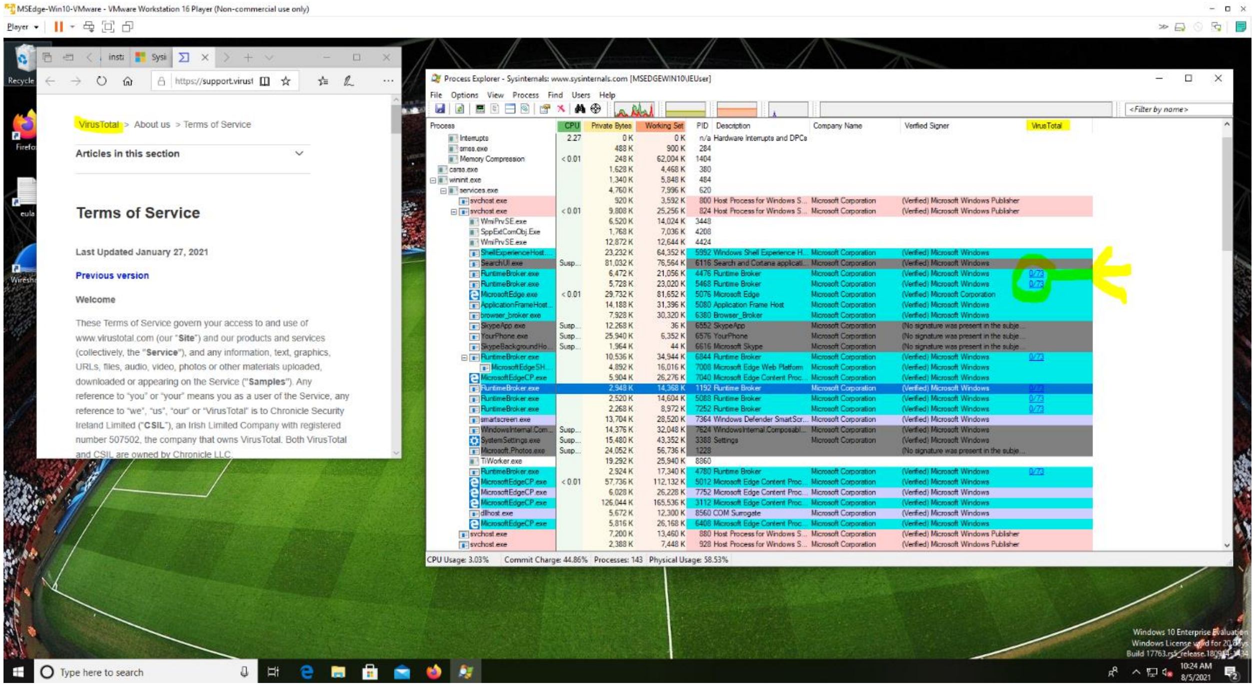
3. Next great feature is to verify image signatures, which check for the digital signature of every exe file appearing in the list, which helps in troubleshooting for some suspicious application. To Enable it, click options-> Verify Image signatures.



4. Other thing we can do is Taking action on a specific process. We can set priority for a process, kill a process, kill the whole process tree, restart a process, suspend the process. To do one of these tasks, right click on any process.



5. Using Process Explorer to quickly search VirusTotal which is very helpful to find a virus thread. You can check this by right clicking on any process and select Check VirusTotal. Accept the terms and the number of virus will be listed against every process.


MSEdge-Win10-VMware - VMware Workstation 16 Player (Non-commercial use only)
Player
Recycle
Firefox
eula
Wireshark
insti
Sysi
https://support.virust
Process Explorer - Sysinternals: www.sysinternals.com [MSEDGEWIN10\IEUser]
File
Options
View
Process
Find
Users
Help
<Filter by name>
Type here to search
Windows 10 Enterprise Evaluation
Windows License valid for 20 days
Build 17763.rs5_release.180914-1434
10:24 AM
8/5/2021

VirusTotal > About us > Terms of Service

Articles in this section

Terms of Service

Last Updated January 27, 2021

Previous version

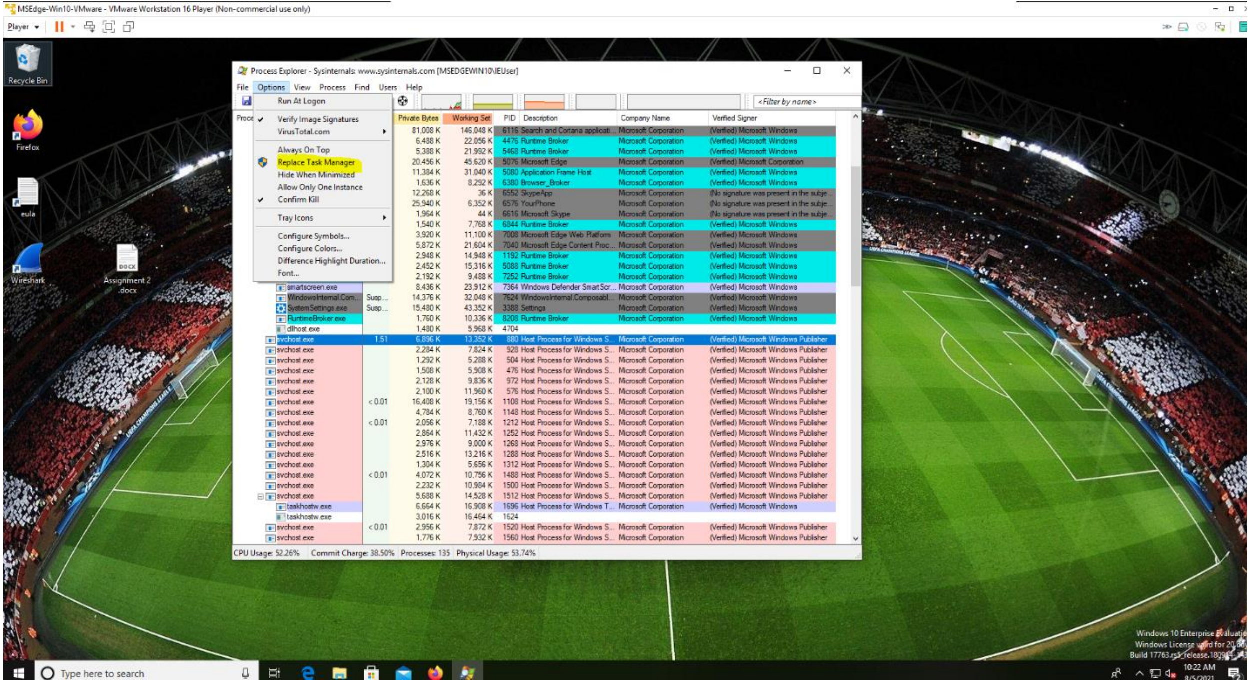
Welcome

These Terms of Service govern your access to and use of www.virustotal.com (our "**Site**") and our products and services (collectively, the "**Service**"), and any information, text, graphics, URLs, files, audio, video, photos or other materials uploaded, downloaded or appearing on the Service ("**Samples**"). Any reference to "you" or "your" means you as a user of the Service, any reference to "we", "us", "our" or "VirusTotal" is to Chronicle Security Ireland Limited ("**CSIL**"), an Irish Limited Company with registered number 507502, the company that owns VirusTotal. Both VirusTotal and CSIL are owned by Chronicle LLC.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer	VirusTotal
Interrupts	2.27	0 K	0 K	n/a	Hardware Interrupts and DPCs			
smss.exe		488 K	900 K	284				
Memory Compression	< 0.01	248 K	62,004 K	1404				
csrss.exe		1,628 K	4,468 K	380				
wininit.exe		1,340 K	5,848 K	484				
services.exe		4,760 K	7,996 K	620				
svchost.exe		920 K	3,592 K	800	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher	
svchost.exe	< 0.01	9,808 K	25,256 K	824	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher	
WmiPrvSE.exe		6,520 K	14,024 K	3448				
SppExtComObj.Exe		1,768 K	7,036 K	4208				
WmiPrvSE.exe		12,872 K	12,644 K	4424				
ShellExperienceHost....		23,232 K	64,352 K	5992	Windows Shell Experience H...	Microsoft Corporation	(Verified) Microsoft Windows	
SearchUI.exe	Susp...	81,032 K	76,564 K	6116	Search and Cortana applicati...	Microsoft Corporation	(Verified) Microsoft Windows	
RuntimeBroker.exe		6,472 K	21,056 K	4476	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	0/73
RuntimeBroker.exe		5,728 K	23,020 K	5468	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	0/73
MicrosoftEdge.exe	< 0.01	29,732 K	81,652 K	5076	Microsoft Edge	Microsoft Corporation	(Verified) Microsoft Corporation	
ApplicationFrameHost...		14,188 K	31,396 K	5080	Application Frame Host	Microsoft Corporation	(Verified) Microsoft Windows	
browser_broker.exe		7,928 K	30,320 K	6380	Browser_Broker	Microsoft Corporation	(Verified) Microsoft Windows	
SkypeApp.exe	Susp...	12,268 K	36 K	6552	SkypeApp	Microsoft Corporation	(No signature was present in the subje...	
YourPhone.exe	Susp...	25,940 K	6,352 K	6576	YourPhone	Microsoft Corporation	(No signature was present in the subje...	
SkypeBackgroundHo...	Susp...	1,964 K	44 K	6616	Microsoft Skype	Microsoft Corporation	(No signature was present in the subje...	
RuntimeBroker.exe		10,536 K	34,944 K	6844	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	0/73
MicrosoftEdgeSH...		4,892 K	16,016 K	7008	Microsoft Edge Web Platform	Microsoft Corporation	(Verified) Microsoft Windows	
MicrosoftEdgeCP.exe		5,904 K	26,276 K	7040	Microsoft Edge Content Proc...	Microsoft Corporation	(Verified) Microsoft Windows	
RuntimeBroker.exe		2,948 K	14,368 K	1192	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	0/73
RuntimeBroker.exe		2,520 K	14,604 K	5088	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	0/73
RuntimeBroker.exe		2,268 K	8,972 K	7252	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	0/73
smartscreen.exe		13,704 K	28,520 K	7364	Windows Defender SmartScr...	Microsoft Corporation	(Verified) Microsoft Windows	
WindowsInternal.Com...	Susp...	14,376 K	32,048 K	7624	WindowsInternal.Composabl...	Microsoft Corporation	(Verified) Microsoft Windows	
SystemSettings.exe	Susp...	15,480 K	43,352 K	3388	Settings	Microsoft Corporation	(Verified) Microsoft Windows	
Microsoft.Photos.exe	Susp...	24,052 K	56,736 K	1228			(No signature was present in the subje...	
TiWorker.exe		19,292 K	25,940 K	8860				
RuntimeBroker.exe		2,924 K	17,340 K	4780	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows	0/73
MicrosoftEdgeCP.exe	< 0.01	57,736 K	112,132 K	5012	Microsoft Edge Content Proc...	Microsoft Corporation	(Verified) Microsoft Windows	
MicrosoftEdgeCP.exe		6,028 K	26,228 K	7752	Microsoft Edge Content Proc...	Microsoft Corporation	(Verified) Microsoft Windows	
MicrosoftEdgeCP.exe		126,044 K	165,536 K	3112	Microsoft Edge Content Proc...	Microsoft Corporation	(Verified) Microsoft Windows	
dllhost.exe		5,672 K	12,300 K	8560	COM Surrogate	Microsoft Corporation	(Verified) Microsoft Windows	
MicrosoftEdgeCP.exe		5,816 K	26,168 K	6408	Microsoft Edge Content Proc...	Microsoft Corporation	(Verified) Microsoft Windows	
svchost.exe		7,200 K	13,460 K	880	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher	
svchost.exe		2,388 K	7,448 K	928	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher	

CPU Usage: 3.03% Commit Charge: 44.86% Processes: 143 Physical Usage: 58.53%

6. You can replace the task manager with process explorer which is nice because process explorer provides so many better features than windows normal task manager. To do this Click Options, and select Replace Task Manager. Next time when you will press Ctrl + shift + esc, process explorer will pop up rather than window's task Manager.

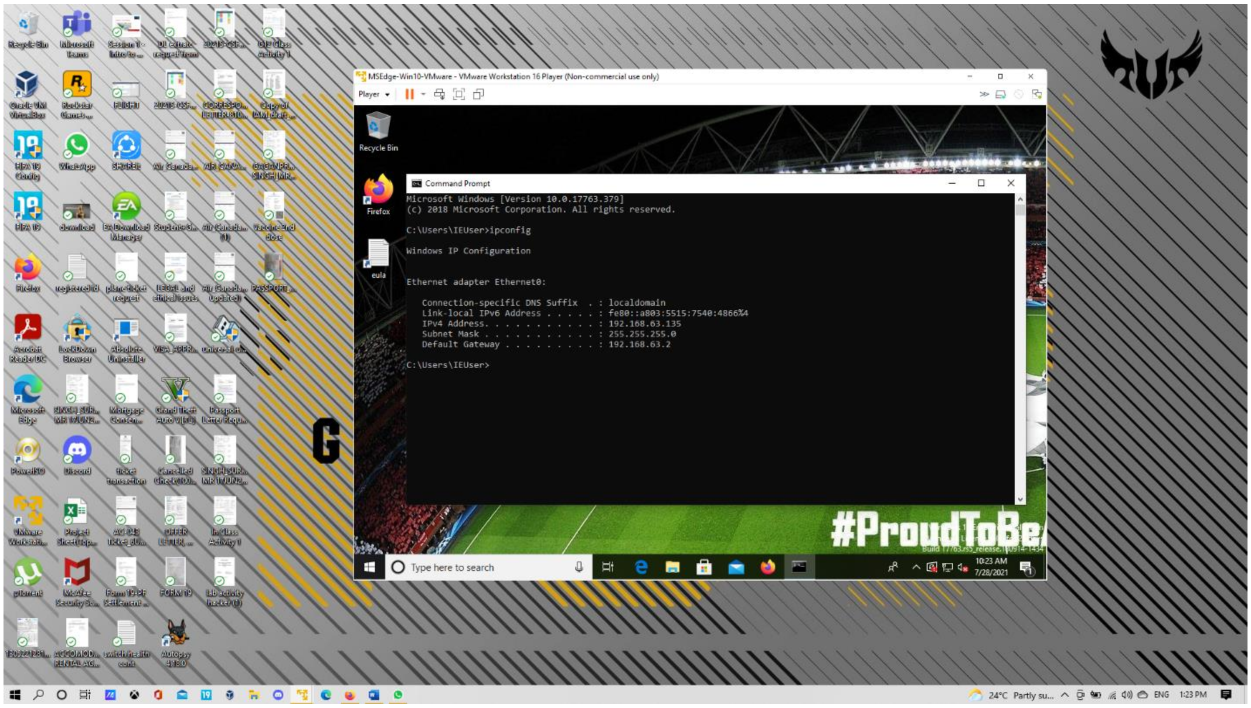

MSEdge-Win10-VMware - VMware Workstation 16 Player (Non-commercial use only)
Player
Recycle Bin
Firefox
eula
Wireshark
Assignment 2 .docx
Process Explorer - Sysinternals: www.sysinternals.com [MSEDGEWIN10\IEUser]
File
Options
View
Process
Find
Users
Help
Run At Logon
✓ Verify Image Signatures
VirusTotal.com
Always On Top
Replace Task Manager
Hide When Minimized
Allow Only One Instance
✓ Confirm Kill
Tray Icons
Configure Symbols...
Configure Colors...
Difference Highlight Duration...
Font...
<Filter by name>
Type here to search
Windows 10 Enterprise Evaluation
Windows License valid for 20 days
Build 17763.rs5_release.180914-1434
10:22 AM

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer
		81,008 K	146,048 K	6116	Search and Cortana applicati...	Microsoft Corporation	(Verified) Microsoft Windows
		6,488 K	22,056 K	4476	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows
		5,388 K	21,992 K	5468	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows
		20,456 K	45,620 K	5076	Microsoft Edge	Microsoft Corporation	(Verified) Microsoft Corporation
		11,384 K	31,040 K	5080	Application Frame Host	Microsoft Corporation	(Verified) Microsoft Windows
		1,636 K	8,292 K	6380	Browser_Broker	Microsoft Corporation	(Verified) Microsoft Windows
		12,268 K	36 K	6552	SkypeApp	Microsoft Corporation	(No signature was present in the subje...
		25,940 K	6,352 K	6576	YourPhone	Microsoft Corporation	(No signature was present in the subje...
		1,964 K	44 K	6616	Microsoft Skype	Microsoft Corporation	(No signature was present in the subje...
		1,540 K	7,768 K	6844	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows
		3,920 K	11,100 K	7008	Microsoft Edge Web Platform	Microsoft Corporation	(Verified) Microsoft Windows
		5,872 K	21,604 K	7040	Microsoft Edge Content Proc...	Microsoft Corporation	(Verified) Microsoft Windows
		2,948 K	14,948 K	1192	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows
		2,452 K	15,316 K	5088	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows
		2,192 K	9,488 K	7252	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows
smartscreen.exe		8,436 K	23,912 K	7364	Windows Defender SmartScr...	Microsoft Corporation	(Verified) Microsoft Windows
WindowsInternal.Com...	Susp...	14,376 K	32,048 K	7624	WindowsInternal.Composabl...	Microsoft Corporation	(Verified) Microsoft Windows
SystemSettings.exe	Susp...	15,480 K	43,352 K	3388	Settings	Microsoft Corporation	(Verified) Microsoft Windows
RuntimeBroker.exe		1,760 K	10,336 K	8208	Runtime Broker	Microsoft Corporation	(Verified) Microsoft Windows
dllhost.exe		1,480 K	5,968 K	4704			
svchost.exe	1.51	6,896 K	13,352 K	880	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher
svchost.exe		2,284 K	7,824 K	928	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher
svchost.exe		1,292 K	5,288 K	504	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher
svchost.exe		1,508 K	5,908 K	476	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher
svchost.exe		2,128 K	9,836 K	972	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher
svchost.exe		2,100 K	11,960 K	576	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher
svchost.exe	< 0.01	16,408 K	19,156 K	1108	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher
svchost.exe		4,784 K	8,760 K	1148	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher
svchost.exe	< 0.01	2,056 K	7,188 K	1212	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher
svchost.exe		2,864 K	11,432 K	1252	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher
svchost.exe		2,976 K	9,000 K	1268	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher
svchost.exe		2,516 K	13,216 K	1288	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher
svchost.exe		1,304 K	5,656 K	1312	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher
svchost.exe	< 0.01	4,072 K	10,756 K	1488	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher
svchost.exe		2,232 K	10,984 K	1500	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher
svchost.exe		5,688 K	14,528 K	1512	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher
taskhostw.exe		6,664 K	16,908 K	1696	Host Process for Windows T...	Microsoft Corporation	(Verified) Microsoft Windows
taskhostw.exe		3,016 K	16,464 K	1624			
svchost.exe	< 0.01	2,956 K	7,872 K	1520	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher
svchost.exe		1,776 K	7,932 K	1560	Host Process for Windows S...	Microsoft Corporation	(Verified) Microsoft Windows Publisher

CPU Usage: 52.26% Commit Charge: 38.50% Processes: 135 Physical Usage: 53.74%

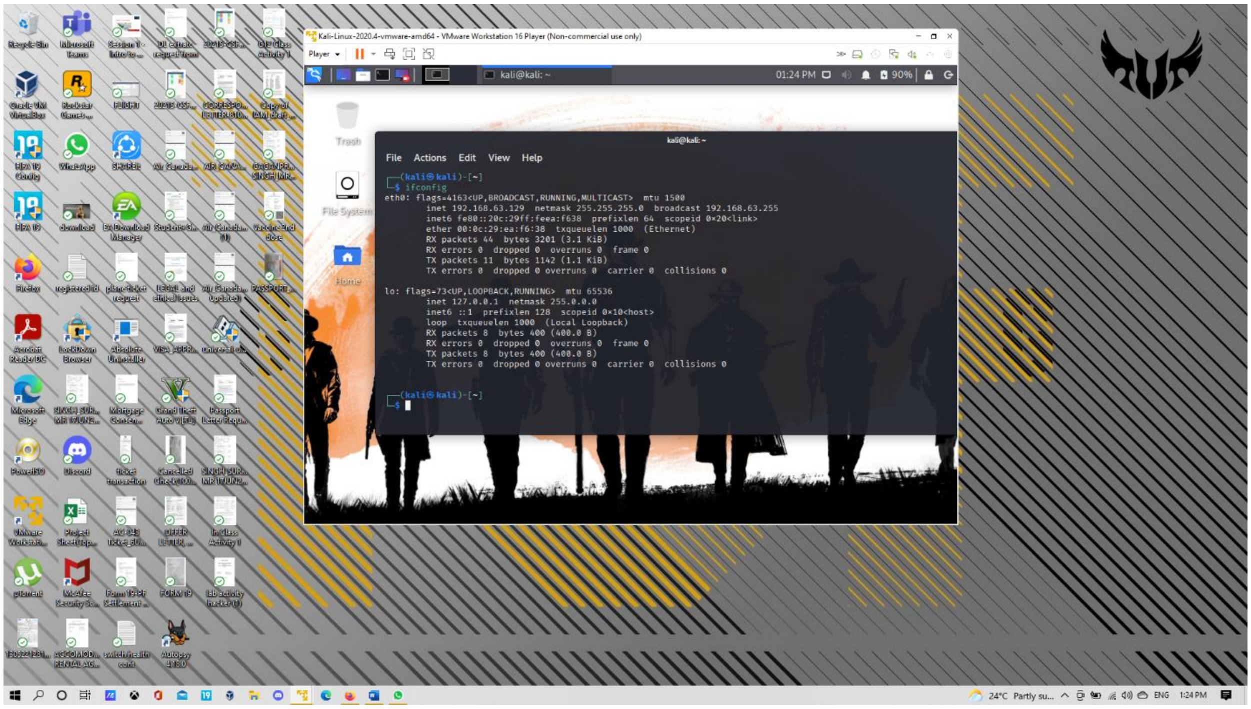
Part 2: Determining the cost of a scan

2.1 The *Windows* VM IP's address


MSEdge-Win10-VMware - VMware Workstation 16 Player (Non-commercial use only)
Command Prompt
#ProudToBe

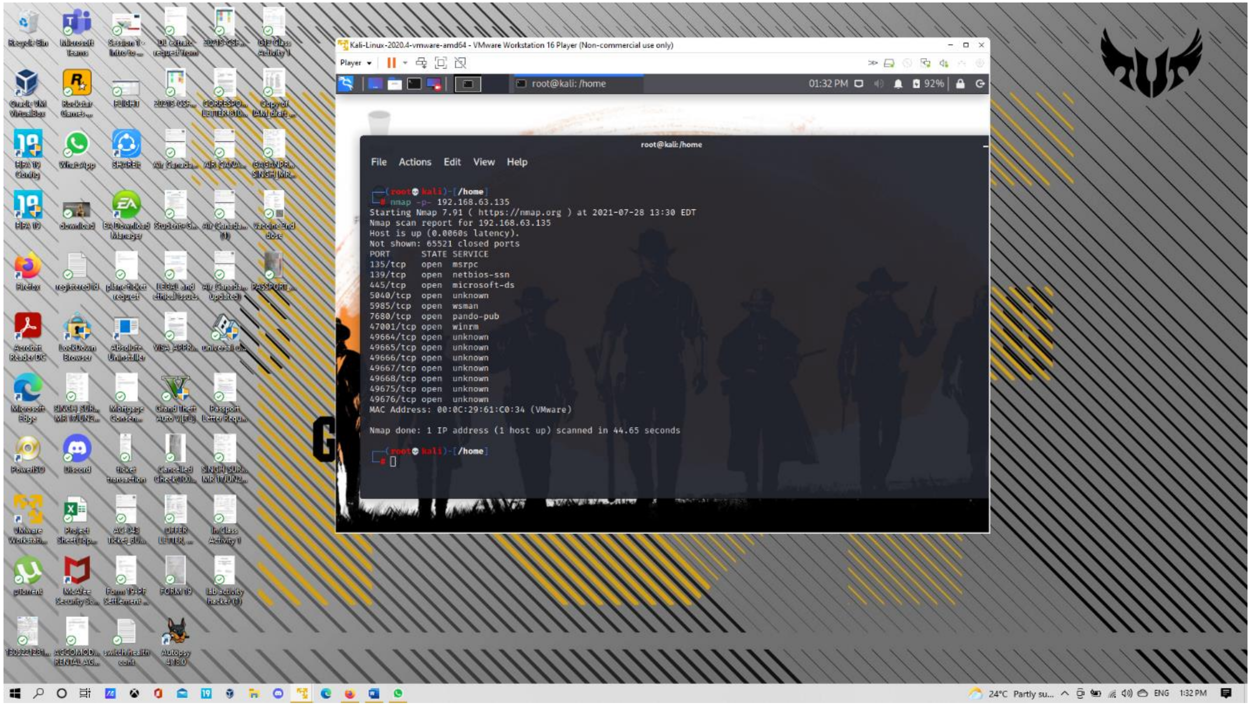
```
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::a803:5515:7540:4866%4
   IPv4 Address. . . . . . . . . . . : 192.168.63.135
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.63.2

C:\Users\IEUser>
```

2.2 The *Kali* VM's IP address


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
kali@kali: ~
01:24 PM
90%
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.63.129  netmask 255.255.255.0  broadcast 192.168.63.255
        inet6 fe80::20c:29ff:feea:f638  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:ea:f6:38  txqueuelen 1000  (Ethernet)
        RX packets 44  bytes 3201 (3.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11  bytes 1142 (1.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ 
```

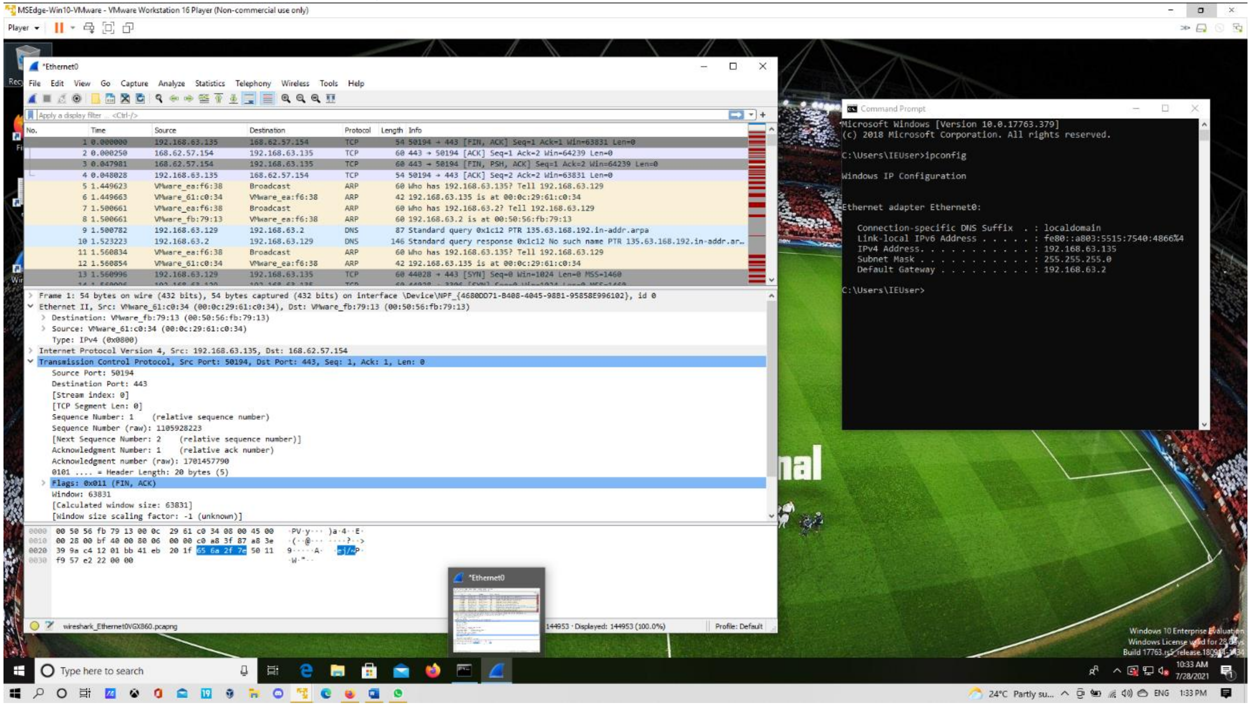
2.3 Kali's desktop with the command-line window visible, with the Nmap command-line and some of Nmap results visible.


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
root@kali: /home
01:32 PM
92%
File Actions Edit View Help

```
┌──(root💀kali)-[/home]
└─# nmap -p- 192.168.63.135
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-28 13:30 EDT
Nmap scan report for 192.168.63.135
Host is up (0.0060s latency).
Not shown: 65521 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5040/tcp  open  unknown
5985/tcp  open  wsman
7680/tcp  open  pando-pub
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49675/tcp open  unknown
49676/tcp open  unknown
MAC Address: 00:0C:29:61:C0:34 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 44.65 seconds

┌──(root💀kali)-[/home]
└─# 
```

2.4 Wireshark open showing the:

2.4.1 Start of the Windows VM scan’s capture.


MSEdge-Win10-VMware - VMware Workstation 16 Player (Non-commercial use only)
Player
*Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Command Prompt
Type here to search
Windows 10 Enterprise Evaluation
10:33 AM
7/28/2021
24°C Partly su...
ENG
1:33 PM

```
No.   Time       Source           Destination      Protocol Length Info
    1 0.000000   192.168.63.135   168.62.57.154    TCP      54 50194 → 443 [FIN, ACK] Seq=1 Ack=1 Win=63831 Len=0
    2 0.000250   168.62.57.154    192.168.63.135   TCP      60 443 → 50194 [ACK] Seq=1 Ack=2 Win=64239 Len=0
    3 0.047981   168.62.57.154    192.168.63.135   TCP      60 443 → 50194 [FIN, PSH, ACK] Seq=1 Ack=2 Win=64239 Len=0
    4 0.048028   192.168.63.135   168.62.57.154    TCP      54 50194 → 443 [ACK] Seq=2 Ack=2 Win=63831 Len=0
    5 1.449623   VMware_ea:f6:38  Broadcast        ARP      60 Who has 192.168.63.135? Tell 192.168.63.129
    6 1.449663   VMware_61:c0:34  VMware_ea:f6:38  ARP      42 192.168.63.135 is at 00:0c:29:61:c0:34
    7 1.500661   VMware_ea:f6:38  Broadcast        ARP      60 Who has 192.168.63.2? Tell 192.168.63.129
    8 1.500661   VMware_fb:79:13  VMware_ea:f6:38  ARP      60 192.168.63.2 is at 00:50:56:fb:79:13
    9 1.500782   192.168.63.129   192.168.63.2     DNS      87 Standard query 0x1c12 PTR 135.63.168.192.in-addr.arpa
   10 1.523223   192.168.63.2     192.168.63.129   DNS     146 Standard query response 0x1c12 No such name PTR 135.63.168.192.in-addr.ar…
   11 1.560834   VMware_ea:f6:38  Broadcast        ARP      60 Who has 192.168.63.135? Tell 192.168.63.129
   12 1.560854   VMware_61:c0:34  VMware_ea:f6:38  ARP      42 192.168.63.135 is at 00:0c:29:61:c0:34
   13 1.560996   192.168.63.129   192.168.63.135   TCP      60 44028 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

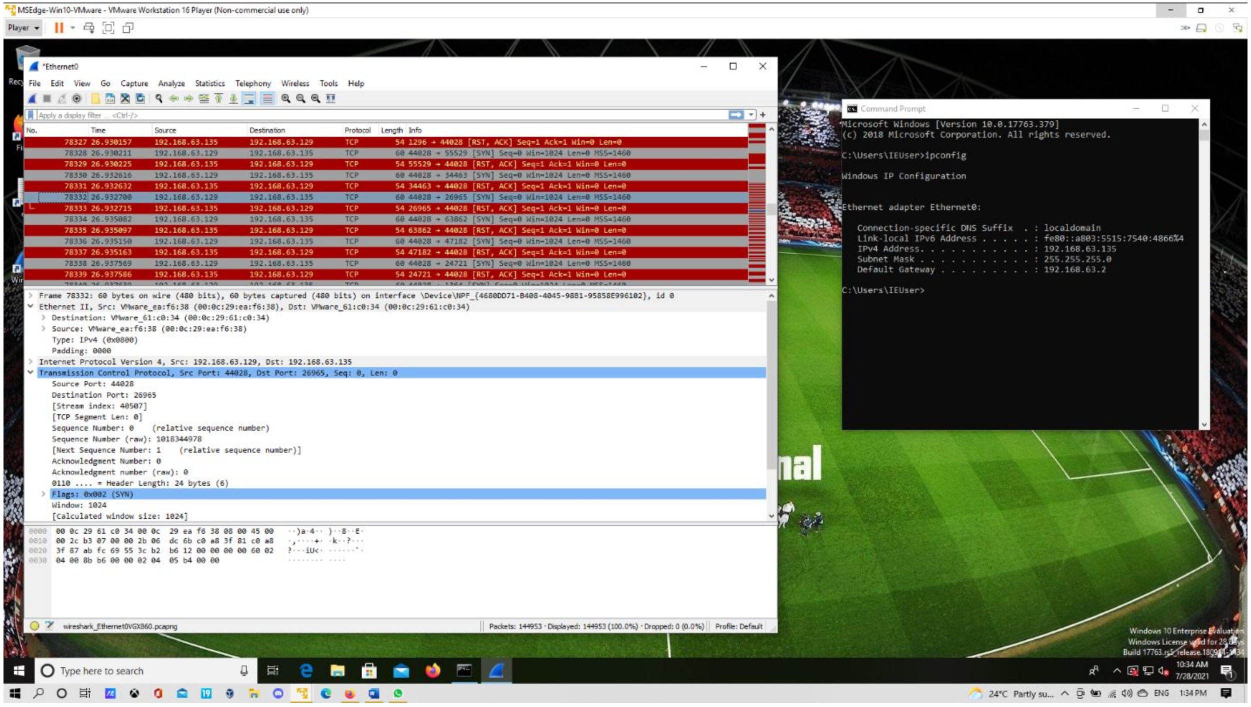
```
> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{4680DD71-B408-4045-9881-95858E996102}, id 0
v Ethernet II, Src: VMware_61:c0:34 (00:0c:29:61:c0:34), Dst: VMware_fb:79:13 (00:50:56:fb:79:13)
  > Destination: VMware_fb:79:13 (00:50:56:fb:79:13)
  > Source: VMware_61:c0:34 (00:0c:29:61:c0:34)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.63.135, Dst: 168.62.57.154
v Transmission Control Protocol, Src Port: 50194, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
    Source Port: 50194
    Destination Port: 443
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1105928223
    [Next Sequence Number: 2    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1701457790
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x011 (FIN, ACK)
    Window: 63831
    [Calculated window size: 63831]
    [Window size scaling factor: -1 (unknown)]
```

```
0000  00 50 56 fb 79 13 00 0c  29 61 c0 34 08 00 45 00   ·PV·y··· )a·4··E·
0010  00 28 00 bf 40 00 80 06  00 00 c0 a8 3f 87 a8 3e   ·(··@··· ····?··>
0020  39 9a c4 12 01 bb 41 eb  20 1f 65 6a 2f 7e 50 11   9·····A·  ·ej/~P·
0030  f9 57 e2 22 00 00                                  ·W·"··
```

```
wireshark_Ethernet0VGX860.pcapng    144953 · Displayed: 144953 (100.0%)    Profile: Default
```

```
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::a803:5515:7540:4866%4
   IPv4 Address. . . . . . . . . . . : 192.168.63.135
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.63.2

C:\Users\IEUser>
```

2.4.2 Mid-section of the Windows VM scan’s capture.


MSEdge-Win10-VMware - VMware Workstation 16 Player (Non-commercial use only)
Player
*Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Command Prompt
Type here to search
Windows 10 Enterprise Evaluation
10:34 AM
7/28/2021
24°C Partly su...
ENG
1:34 PM

```
No.   Time        Source           Destination      Protocol Length Info
78327 26.930157   192.168.63.135   192.168.63.129   TCP      54 1296 → 44028 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
78328 26.930211   192.168.63.129   192.168.63.135   TCP      60 44028 → 55529 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78329 26.930225   192.168.63.135   192.168.63.129   TCP      54 55529 → 44028 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
78330 26.932616   192.168.63.129   192.168.63.135   TCP      60 44028 → 34463 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78331 26.932632   192.168.63.135   192.168.63.129   TCP      54 34463 → 44028 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
78332 26.932700   192.168.63.129   192.168.63.135   TCP      60 44028 → 26965 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78333 26.932715   192.168.63.135   192.168.63.129   TCP      54 26965 → 44028 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
78334 26.935082   192.168.63.129   192.168.63.135   TCP      60 44028 → 63862 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78335 26.935097   192.168.63.135   192.168.63.129   TCP      54 63862 → 44028 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
78336 26.935150   192.168.63.129   192.168.63.135   TCP      60 44028 → 47182 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78337 26.935163   192.168.63.135   192.168.63.129   TCP      54 47182 → 44028 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
78338 26.937569   192.168.63.129   192.168.63.135   TCP      60 44028 → 24721 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
78339 26.937586   192.168.63.135   192.168.63.129   TCP      54 24721 → 44028 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

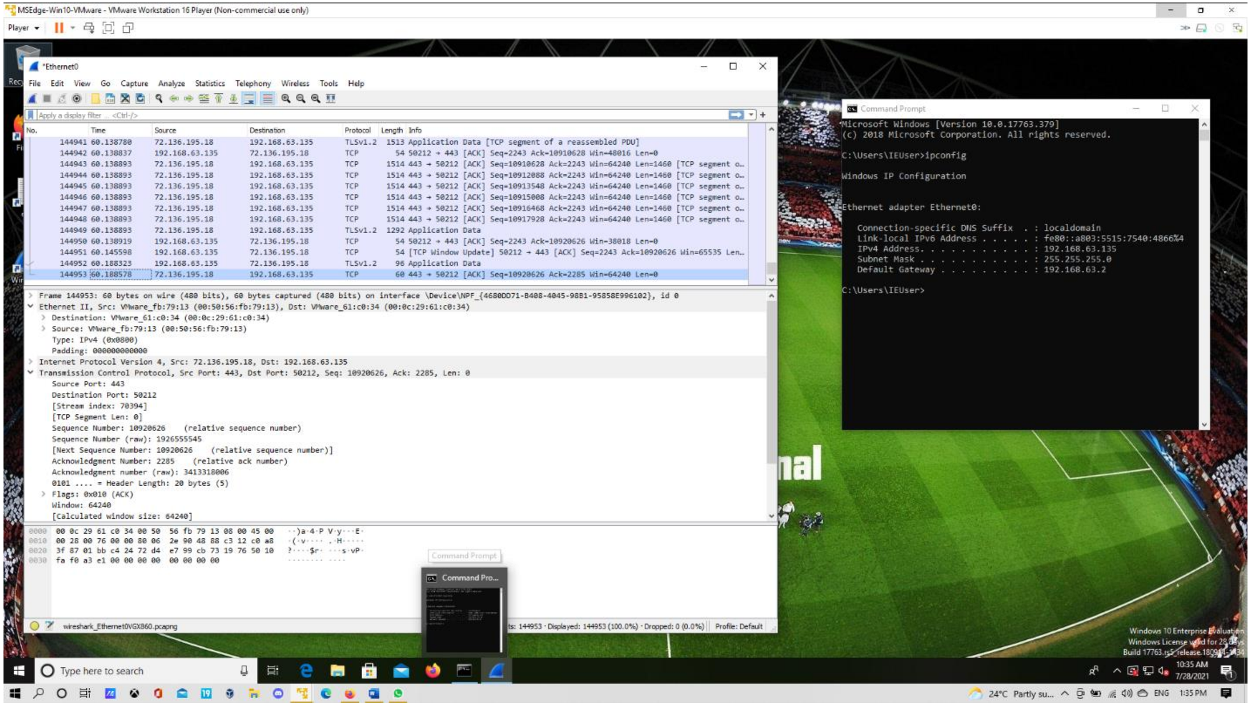
```
> Frame 78332: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{4680DD71-B408-4045-9881-95858E996102}, id 0
v Ethernet II, Src: VMware_ea:f6:38 (00:0c:29:ea:f6:38), Dst: VMware_61:c0:34 (00:0c:29:61:c0:34)
  > Destination: VMware_61:c0:34 (00:0c:29:61:c0:34)
  > Source: VMware_ea:f6:38 (00:0c:29:ea:f6:38)
    Type: IPv4 (0x0800)
    Padding: 0000
> Internet Protocol Version 4, Src: 192.168.63.129, Dst: 192.168.63.135
v Transmission Control Protocol, Src Port: 44028, Dst Port: 26965, Seq: 0, Len: 0
    Source Port: 44028
    Destination Port: 26965
    [Stream index: 40507]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1018344978
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    0110 .... = Header Length: 24 bytes (6)
  > Flags: 0x002 (SYN)
    Window: 1024
    [Calculated window size: 1024]
```

```
0000  00 0c 29 61 c0 34 00 0c  29 ea f6 38 08 00 45 00   ··)a·4·· )··8··E·
0010  00 2c b3 07 00 00 2b 06  dc 6b c0 a8 3f 81 c0 a8   ·,····+· ·k··?···
0020  3f 87 ab fc 69 55 3c b2  b6 12 00 00 00 00 60 02   ?···iU<· ······`·
0030  04 00 8b b6 00 00 02 04  05 b4 00 00               ········ ····
```

```
wireshark_Ethernet0VGX860.pcapng    Packets: 144953 · Displayed: 144953 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

```
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::a803:5515:7540:4866%4
   IPv4 Address. . . . . . . . . . . : 192.168.63.135
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.63.2

C:\Users\IEUser>
```

2.4.3 End of the Windows VM scan's capture.


MSEdge-Win10-VMware - VMware Workstation 16 Player (Non-commercial use only)
Player
*Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Command Prompt
Type here to search

```
No.     Time      Source          Destination     Protocol Length Info
 144941 60.138780 72.136.195.18   192.168.63.135  TLSv1.2  1513 Application Data [TCP segment of a reassembled PDU]
 144942 60.138837 192.168.63.135  72.136.195.18   TCP        54 50212 → 443 [ACK] Seq=2243 Ack=10910628 Win=48016 Len=0
 144943 60.138893 72.136.195.18   192.168.63.135  TCP      1514 443 → 50212 [ACK] Seq=10910628 Ack=2243 Win=64240 Len=1460 [TCP segment o…
 144944 60.138893 72.136.195.18   192.168.63.135  TCP      1514 443 → 50212 [ACK] Seq=10912088 Ack=2243 Win=64240 Len=1460 [TCP segment o…
 144945 60.138893 72.136.195.18   192.168.63.135  TCP      1514 443 → 50212 [ACK] Seq=10913548 Ack=2243 Win=64240 Len=1460 [TCP segment o…
 144946 60.138893 72.136.195.18   192.168.63.135  TCP      1514 443 → 50212 [ACK] Seq=10915008 Ack=2243 Win=64240 Len=1460 [TCP segment o…
 144947 60.138893 72.136.195.18   192.168.63.135  TCP      1514 443 → 50212 [ACK] Seq=10916468 Ack=2243 Win=64240 Len=1460 [TCP segment o…
 144948 60.138893 72.136.195.18   192.168.63.135  TCP      1514 443 → 50212 [ACK] Seq=10917928 Ack=2243 Win=64240 Len=1460 [TCP segment o…
 144949 60.138893 72.136.195.18   192.168.63.135  TLSv1.2  1292 Application Data
 144950 60.138919 192.168.63.135  72.136.195.18   TCP        54 50212 → 443 [ACK] Seq=2243 Ack=10920626 Win=38018 Len=0
 144951 60.145598 192.168.63.135  72.136.195.18   TCP        54 [TCP Window Update] 50212 → 443 [ACK] Seq=2243 Ack=10920626 Win=65535 Len…
 144952 60.188323 192.168.63.135  72.136.195.18   TLSv1.2    96 Application Data
 144953 60.188578 72.136.195.18   192.168.63.135  TCP        60 443 → 50212 [ACK] Seq=10920626 Ack=2285 Win=64240 Len=0
```

```
> Frame 144953: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{4680DD71-B408-4045-98B1-95858E996102}, id 0
v Ethernet II, Src: VMware_fb:79:13 (00:50:56:fb:79:13), Dst: VMware_61:c0:34 (00:0c:29:61:c0:34)
   > Destination: VMware_61:c0:34 (00:0c:29:61:c0:34)
   > Source: VMware_fb:79:13 (00:50:56:fb:79:13)
     Type: IPv4 (0x0800)
     Padding: 000000000000
> Internet Protocol Version 4, Src: 72.136.195.18, Dst: 192.168.63.135
v Transmission Control Protocol, Src Port: 443, Dst Port: 50212, Seq: 10920626, Ack: 2285, Len: 0
     Source Port: 443
     Destination Port: 50212
     [Stream index: 70394]
     [TCP Segment Len: 0]
     Sequence Number: 10920626    (relative sequence number)
     Sequence Number (raw): 1926555545
     [Next Sequence Number: 10920626    (relative sequence number)]
     Acknowledgment Number: 2285    (relative ack number)
     Acknowledgment number (raw): 3413318006
     0101 .... = Header Length: 20 bytes (5)
   > Flags: 0x010 (ACK)
     Window: 64240
     [Calculated window size: 64240]
```

```
0000  00 0c 29 61 c0 34 00 50  56 fb 79 13 08 00 45 00   ··)a·4·P V·y···E·
0010  00 28 00 76 00 00 80 06  2e 90 48 88 c3 12 c0 a8   ·(·v···· .·H·····
0020  3f 87 01 bb c4 24 72 d4  e7 99 cb 73 19 76 50 10   ?····$r· ···s·vP·
0030  fa f0 a3 e1 00 00 00 00  00 00 00 00               ········ ····
```

wireshark_Ethernet0VGX860.pcapng

ts: 144953 · Displayed: 144953 (100.0%) · Dropped: 0 (0.0%) Profile: Default

```
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::a803:5515:7540:4866%4
   IPv4 Address. . . . . . . . . . . : 192.168.63.135
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.63.2

C:\Users\IEUser>
```