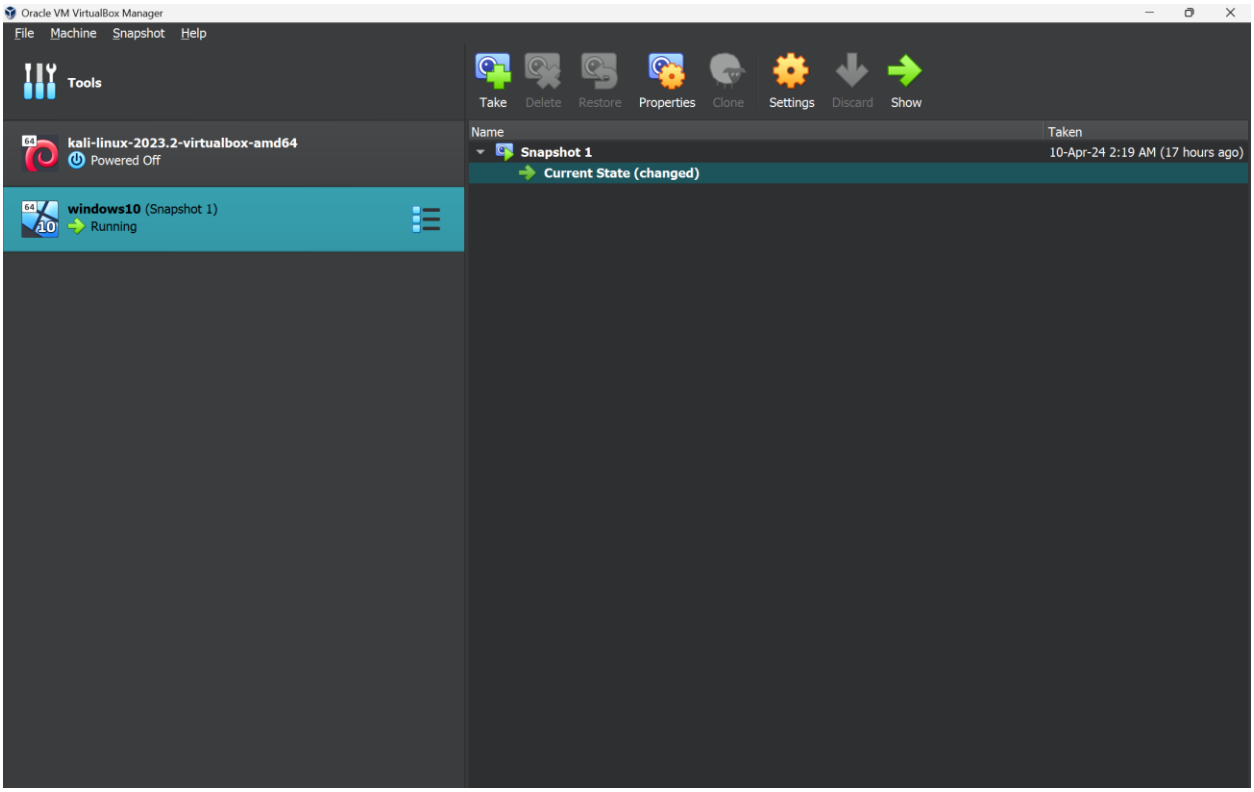
MIDTERM PROJECT

BY:
ABDULLAH(FA22-BCT-004)
SUBMITTED TO:
MUHAMMAD MUSTAFA KHATTAK

APRIL 15, 2024

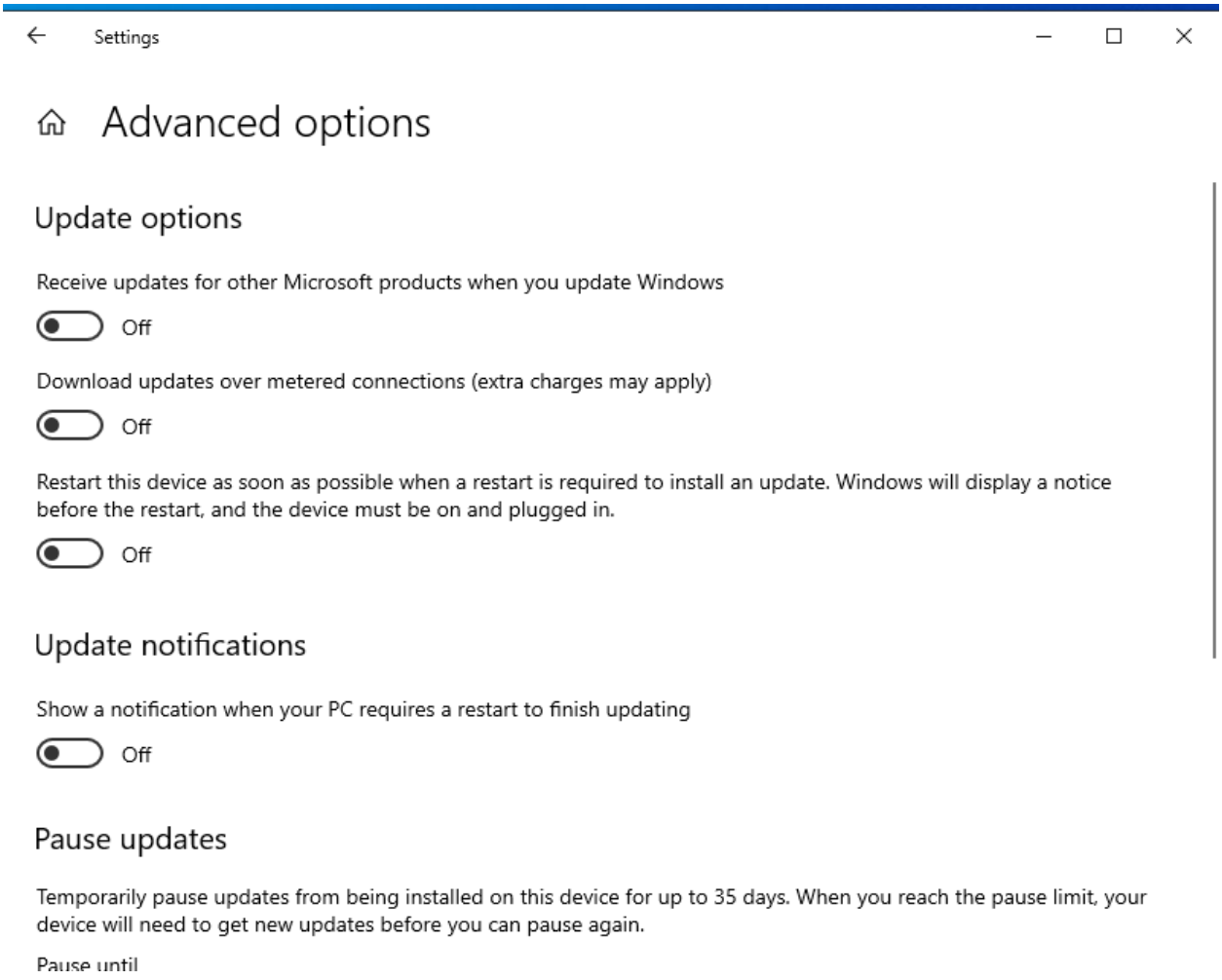
COMSATS UNIVERISTY
ISLAMABAD

CREATED THE SETUP FOR WINDOWS 10 AND TOOK A SNAPSHOT OF INTIAL IMPORT

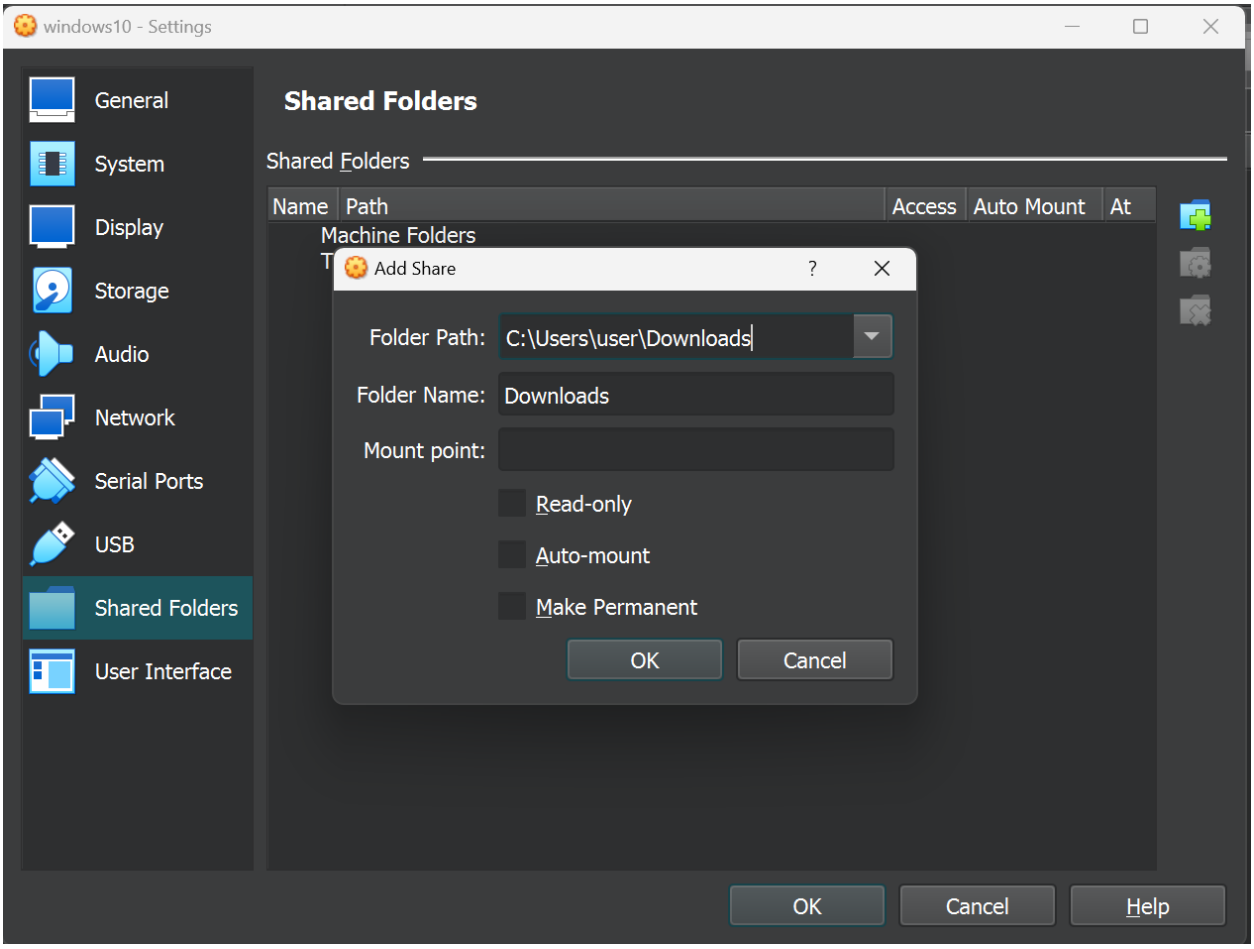


TURNED OFF VIRUS AND THREAT PROTECTION SETTINGS

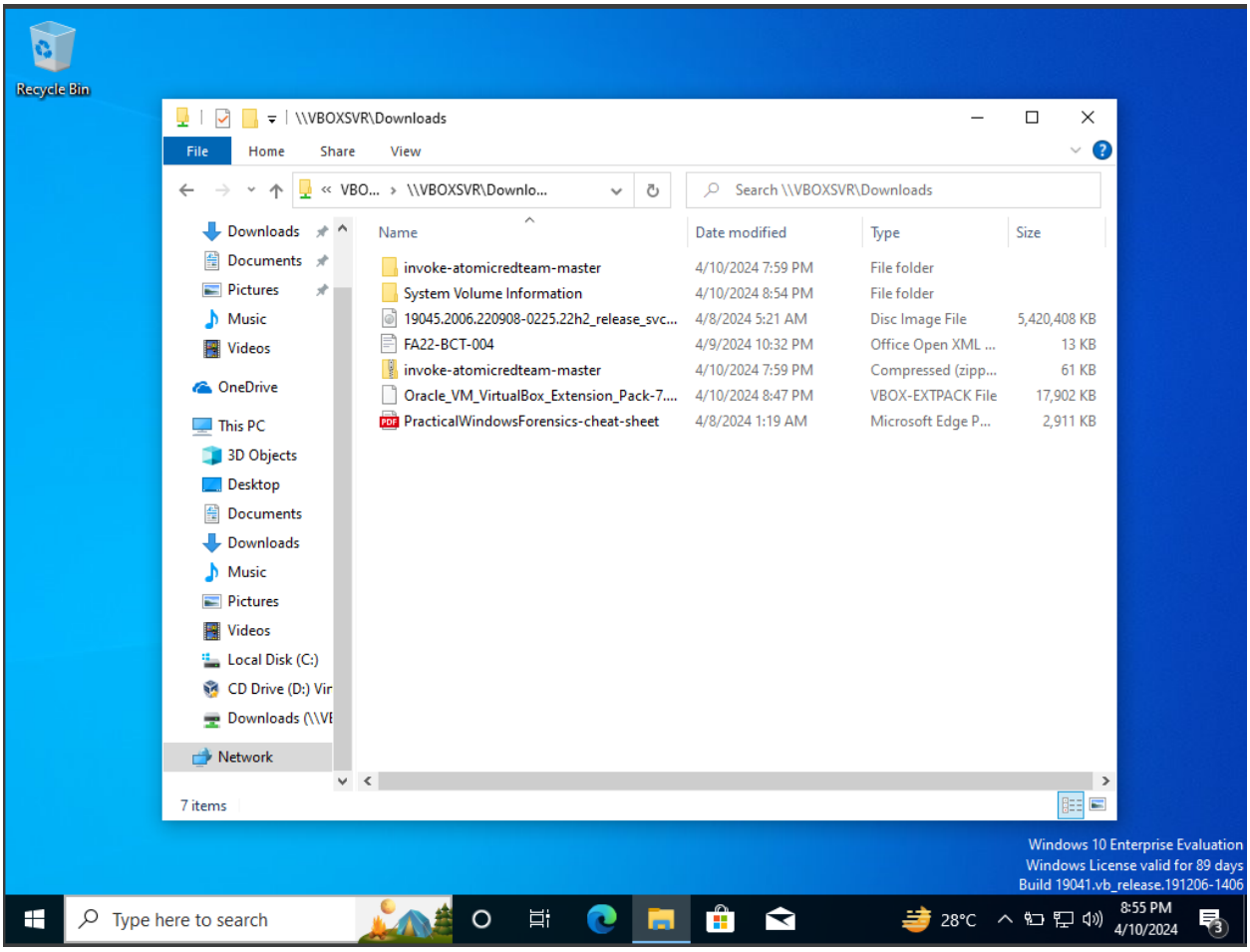
TURNED OFF ALL THE UPDATES



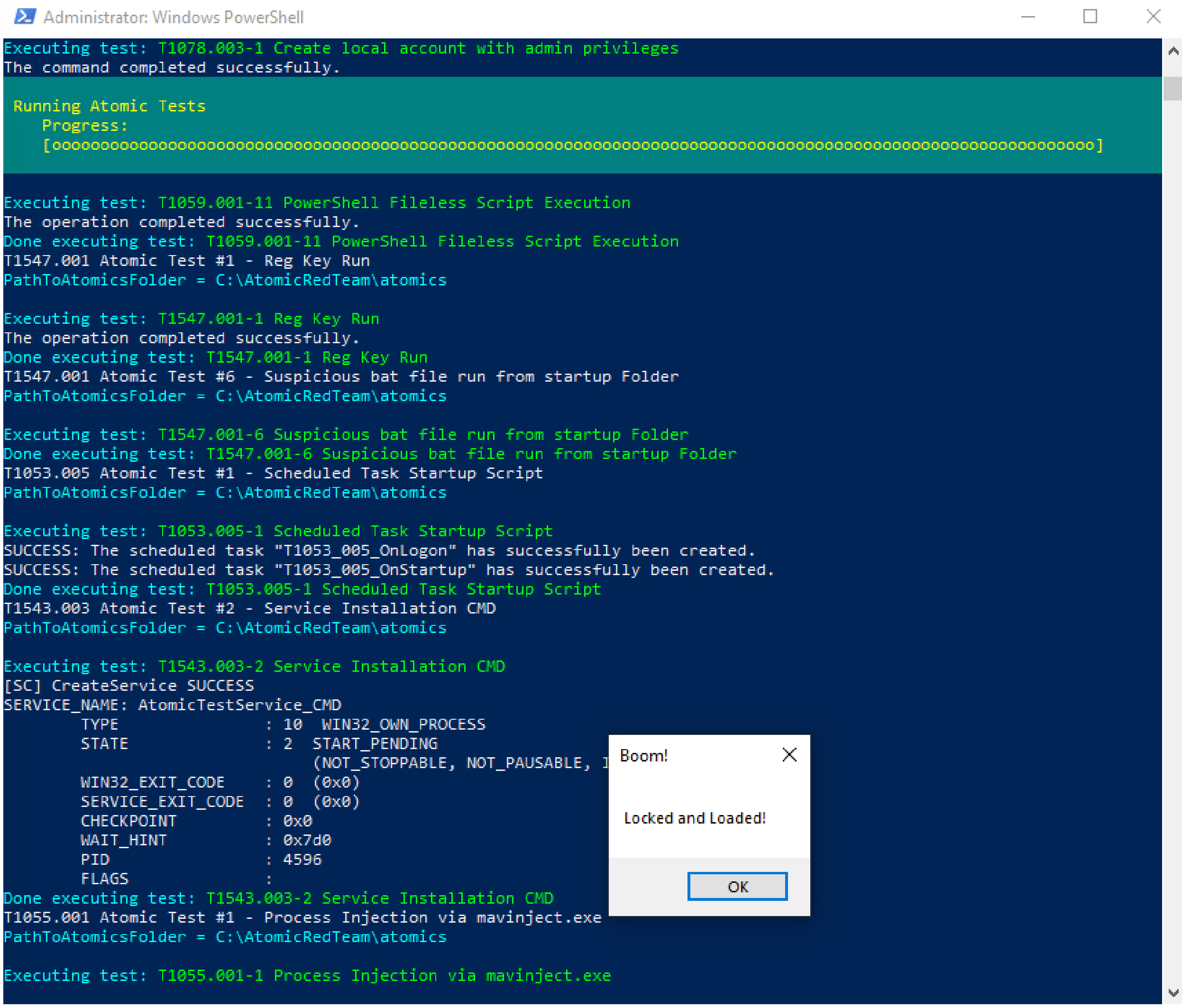
CREATED A SHARED FOLDER



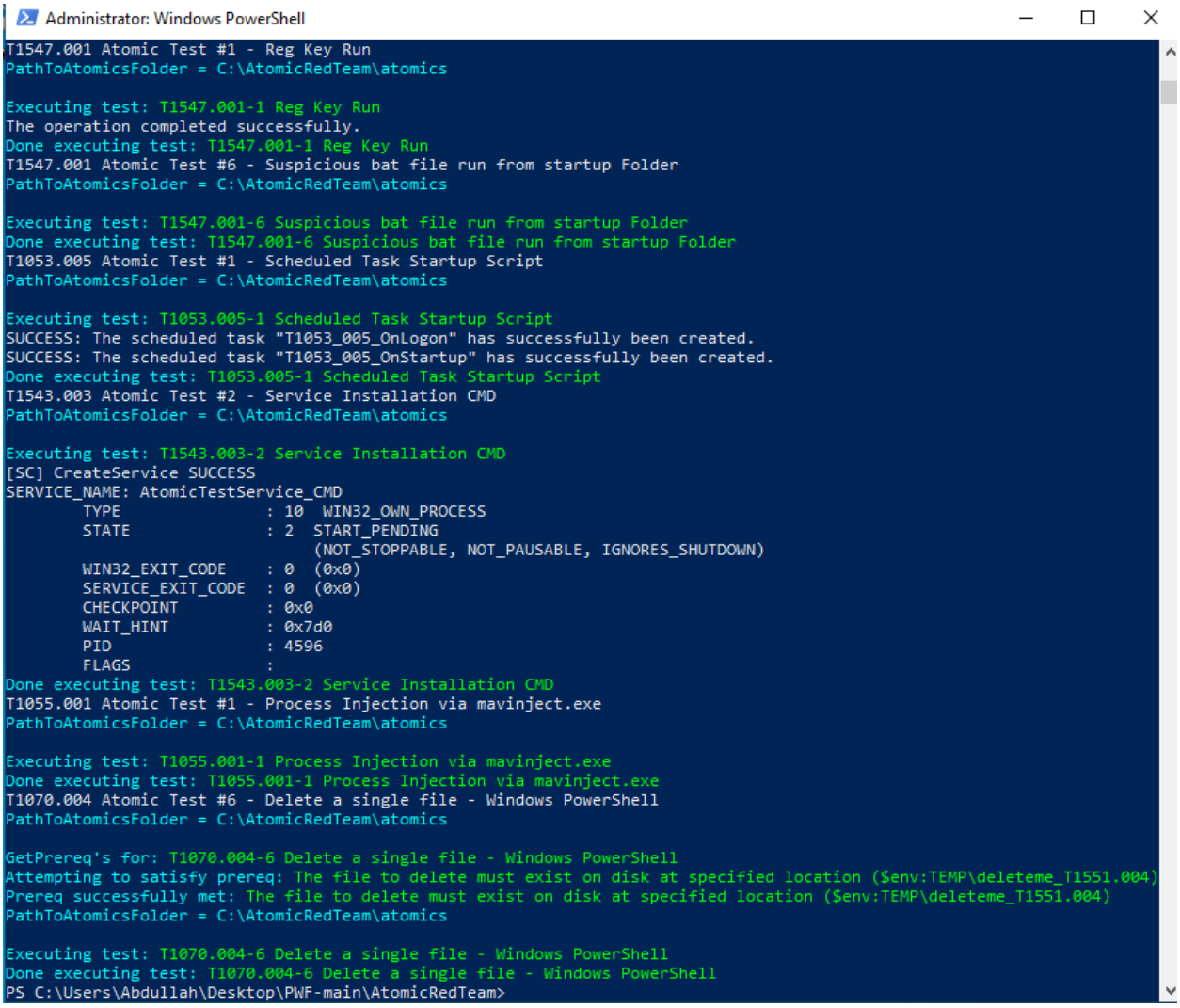
DOWNLOADED THE SCRIPT SETUP



STARTING THE EXECUTION OF ART SCRIPT

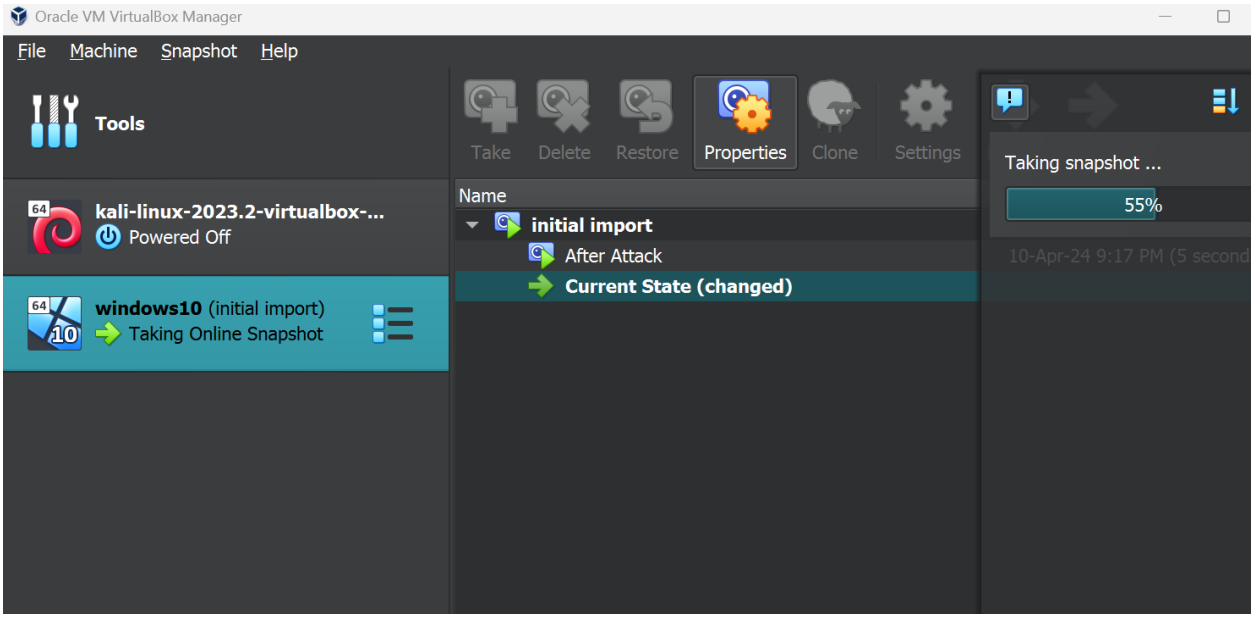


ART SCRIPT EXECUTED:

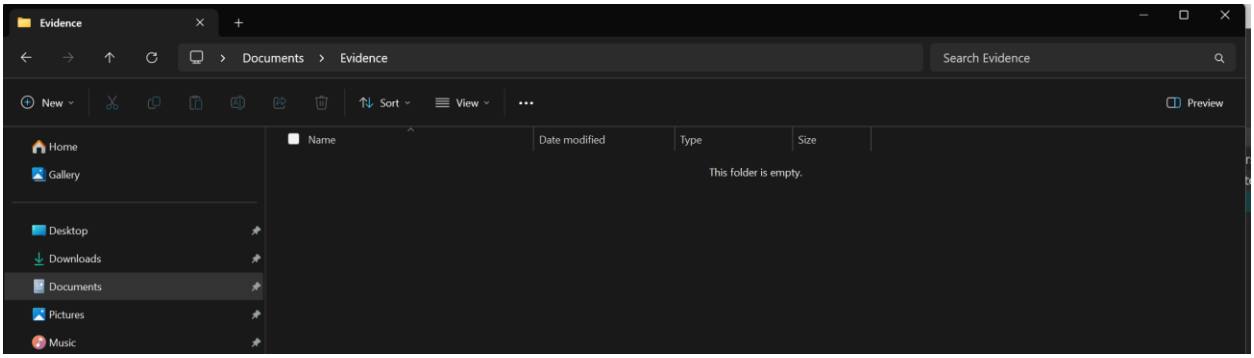


PAUSED THE WINDOW SESSION:

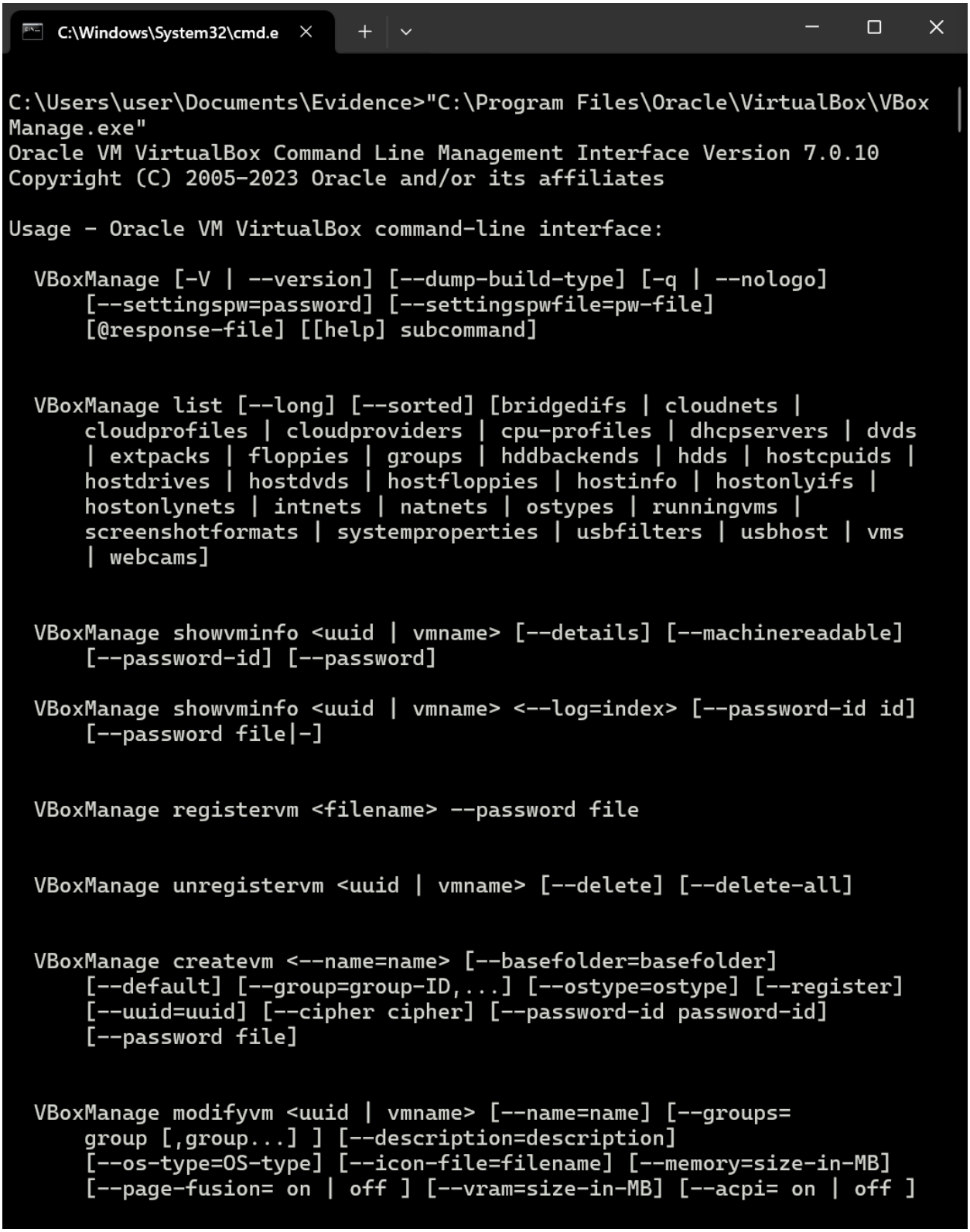
TOOK A SNAPSHOT AFTER THE ATTACK



CREATED AN EVIDENCE FOLDER:



STARTED CMD AND VBOXMANAGE COMMANDS:

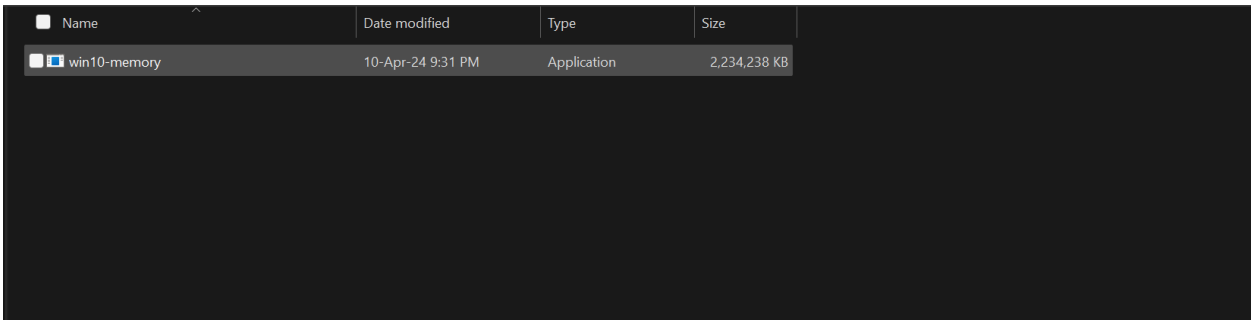


VBOXMANAGE LIST VMS COMMAND TO GET THE VM ID

```
C:\Users\user\Documents\Evidence>vboxmanage list vms
"kali-linux-2023.2-virtualbox-amd64" {f43a94b9-4908-4cf7-bab9-4584b7c5473
c}
"windows10" {9c9b18d4-c97e-452f-aa1c-6f395998e0b9}
```

COMMAND TO GET THE MEMORY DUMP OF DISK

```
C:\Users\user\Documents\Evidence>vboxmanage debugvm 9c9b18d4-c97e-452f-aa
1c-6f395998e0b9 dumpvmcore --filename win10-memory.exe
```

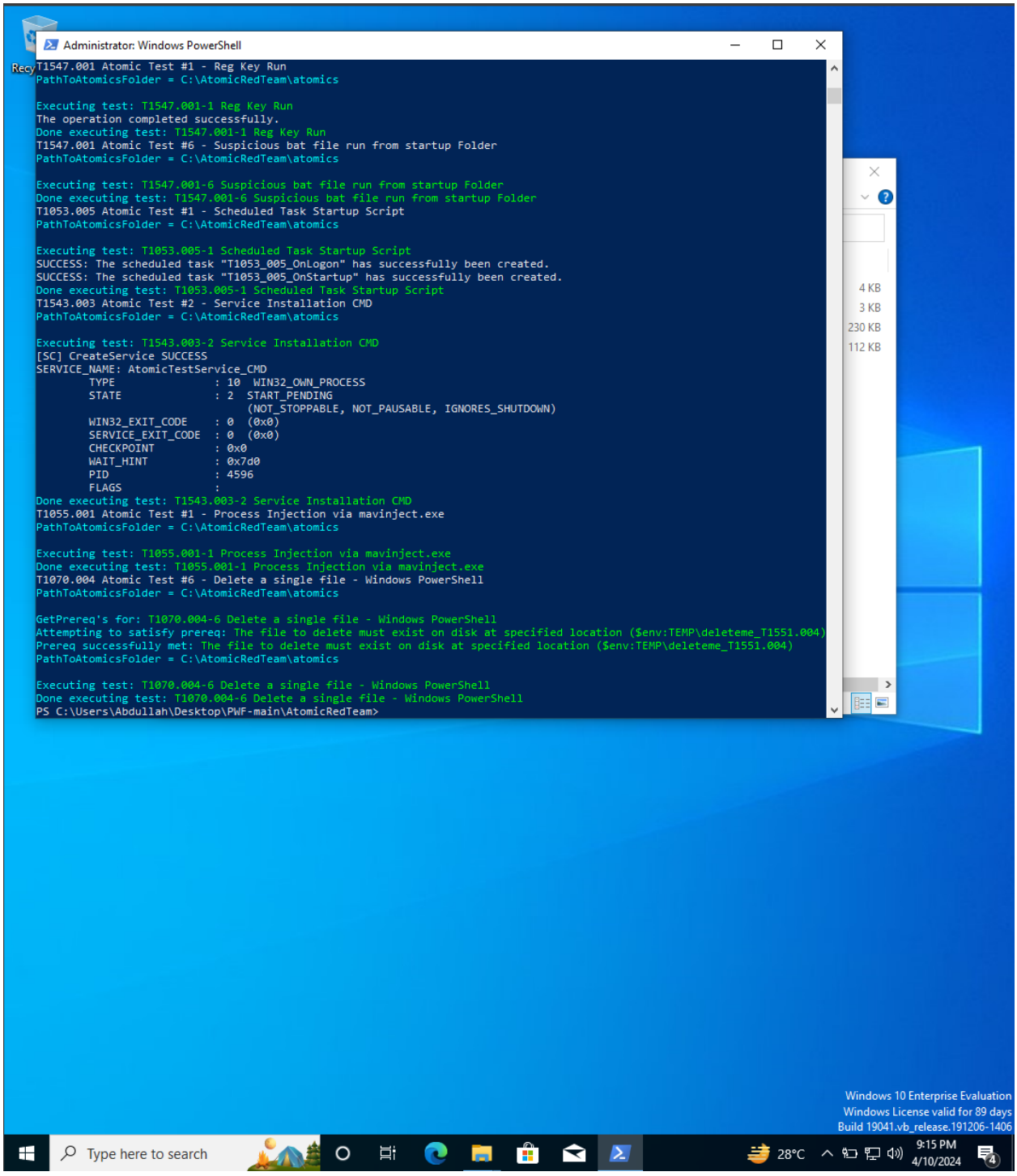


MEMORY DUMP HASH FILE CALCULATION

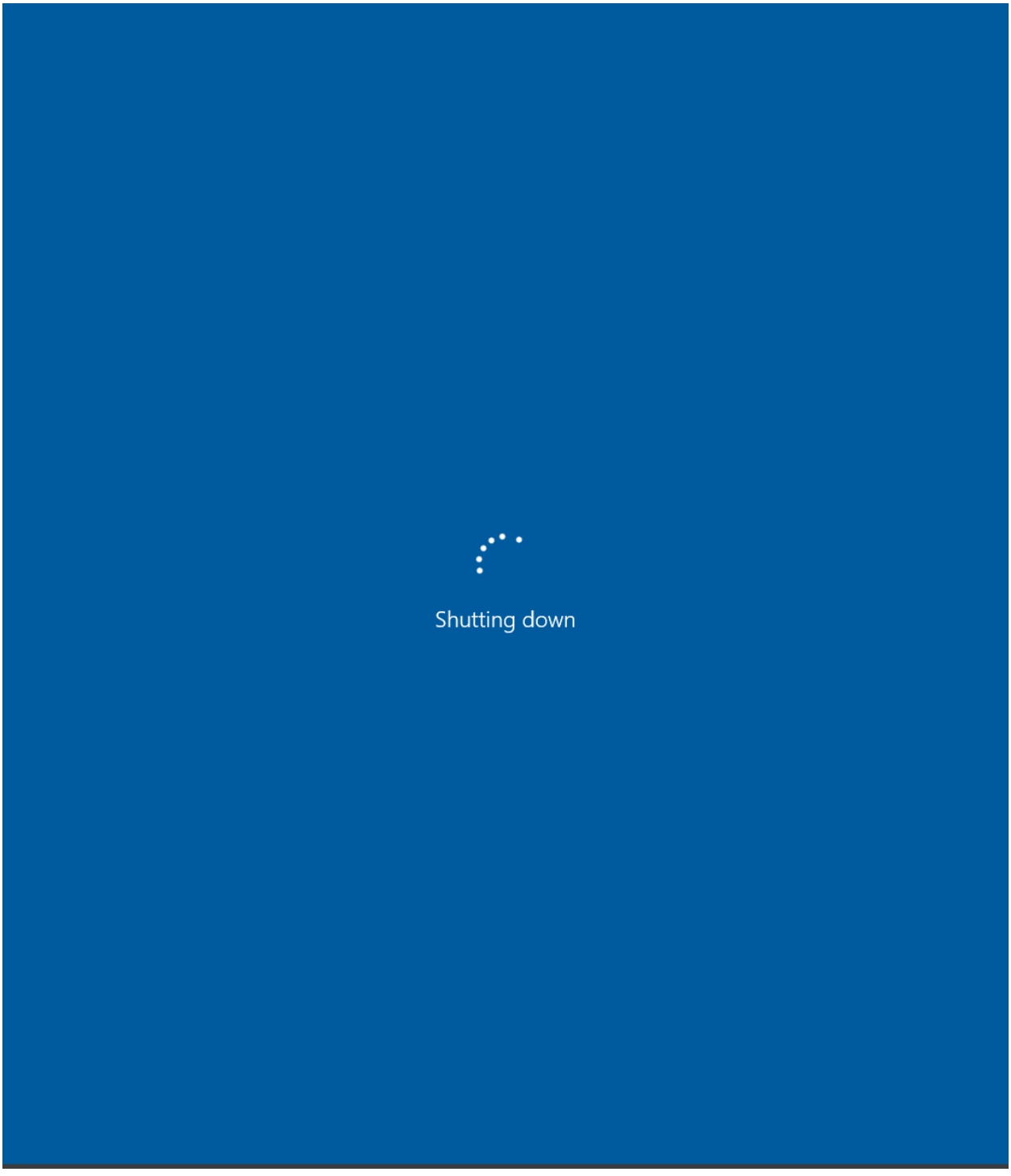
```
C:\Users\user\Documents\Evidence>certUtil -hashfile win10-memory.exe > wi
n10-memory-hash.txt
```

```
SHA1 hash of win10-memory.exe:
11417c1851f125f89b5599b70688e1ab71825d1f
CertUtil: -hashfile command completed successfully.
```

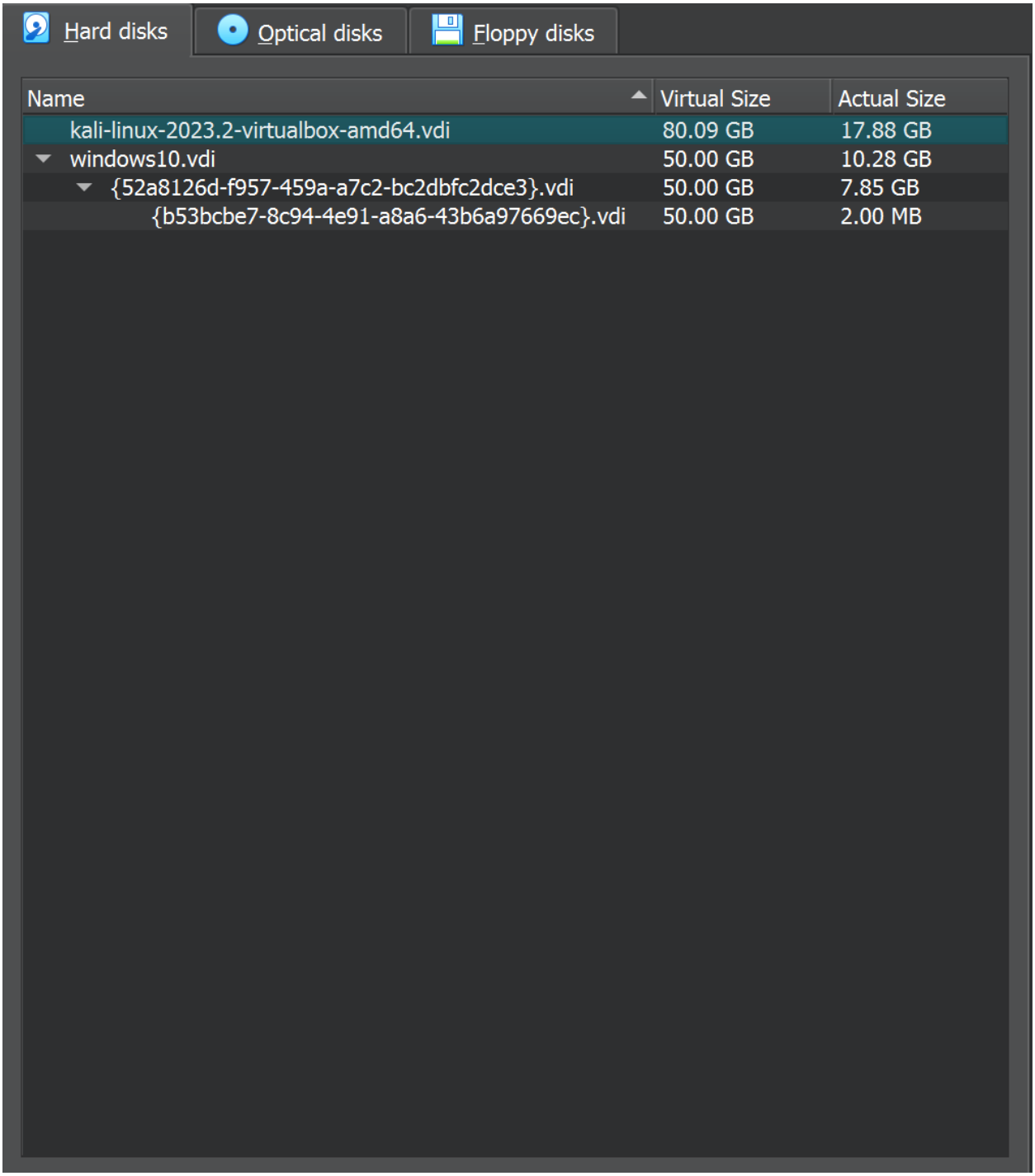
UNPAUSED THE WINDOWS SESSION:



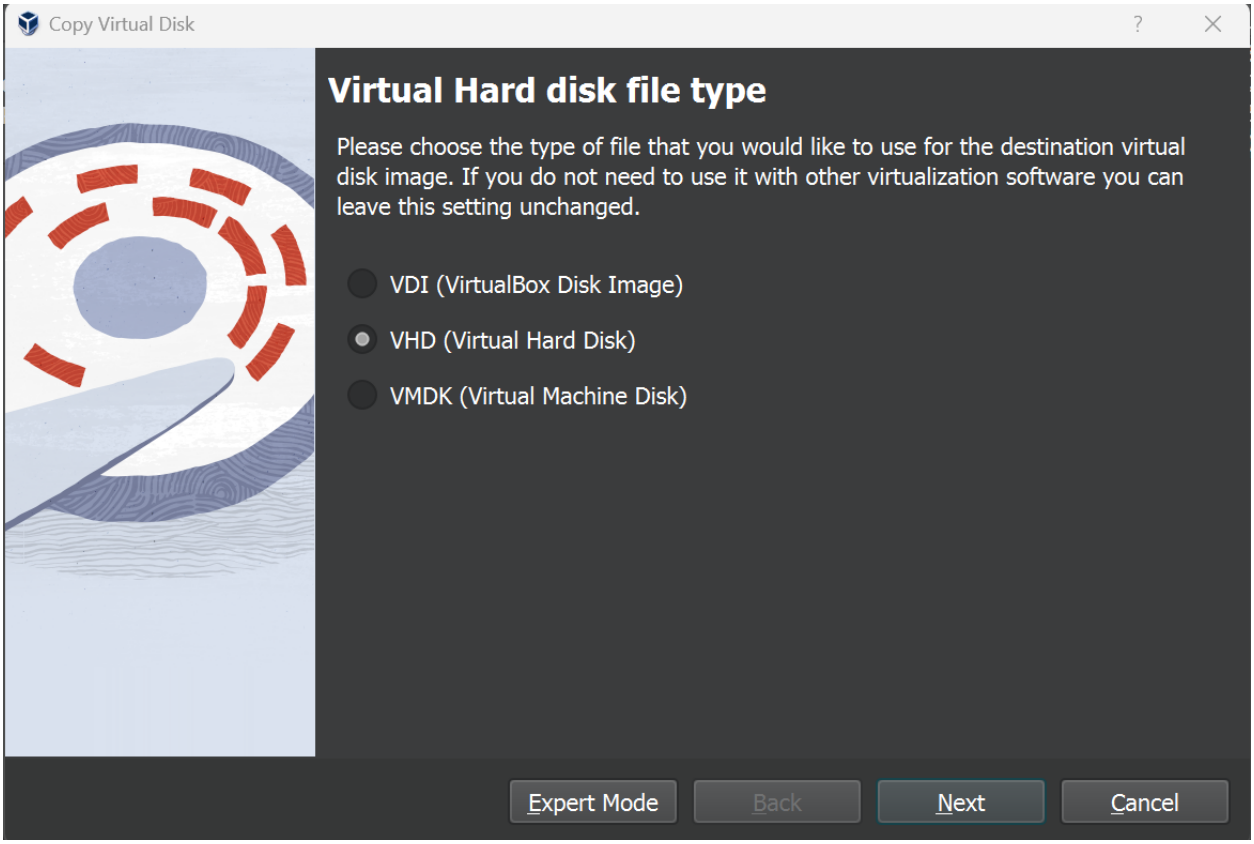
SHUTTING DOWN THE WINDOWS:



GETTING IDS FOR THE SNAPSHOTS



GUI BASED COMMAND EXECUTION:



CLI BASED EXECUTION:

```
C:\Users\user\Documents\Evidence>vboxmanage list hdds
UUID:           4ba8cabb-da30-4f5e-bc64-294628622460
Parent UUID:    base
State:          created
Type:           normal (base)
Location:       C:\Program Files\Oracle\kali-linux-2023.2-virtualbox-amd6
4\kali-linux-2023.2-virtualbox-amd64\kali-linux-2023.2-virtualbox-amd64.v
di
Storage format: vdi
Capacity:       82015 MBytes
Encryption:     disabled

UUID:           0d748506-ca96-4109-9c41-1e7789d3b586
Parent UUID:    base
State:          created
Type:           normal (base)
Location:       C:\Users\user\VirtualBox VMs\windows10\windows10.vdi
Storage format: VDI
Capacity:       51200 MBytes
Encryption:     disabled

UUID:           52a8126d-f957-459a-a7c2-bc2dbfc2dce3
Parent UUID:    0d748506-ca96-4109-9c41-1e7789d3b586
State:          created
Type:           normal (differencing)
Location:       C:\Users\user\VirtualBox VMs\windows10\Snapshots\{52a8126
d-f957-459a-a7c2-bc2dbfc2dce3}.vdi
Storage format: VDI
Capacity:       51200 MBytes
Encryption:     disabled

UUID:           b53bcbe7-8c94-4e91-a8a6-43b6a97669ec
Parent UUID:    52a8126d-f957-459a-a7c2-bc2dbfc2dce3
State:          created
Type:           normal (differencing)
Location:       C:\Users\user\VirtualBox VMs\windows10\Snapshots\{b53bcbe
7-8c94-4e91-a8a6-43b6a97669ec}.vdi
Storage format: VDI
Capacity:       51200 MBytes
Encryption:     disabled
```

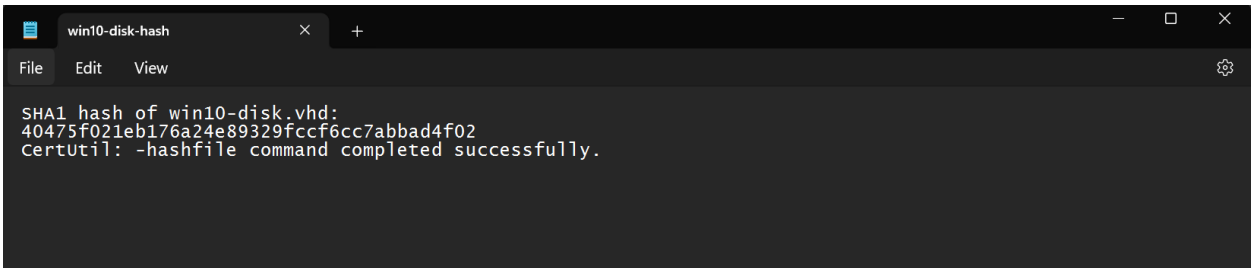
CLONE MEDIUM AFTER ATTACK:

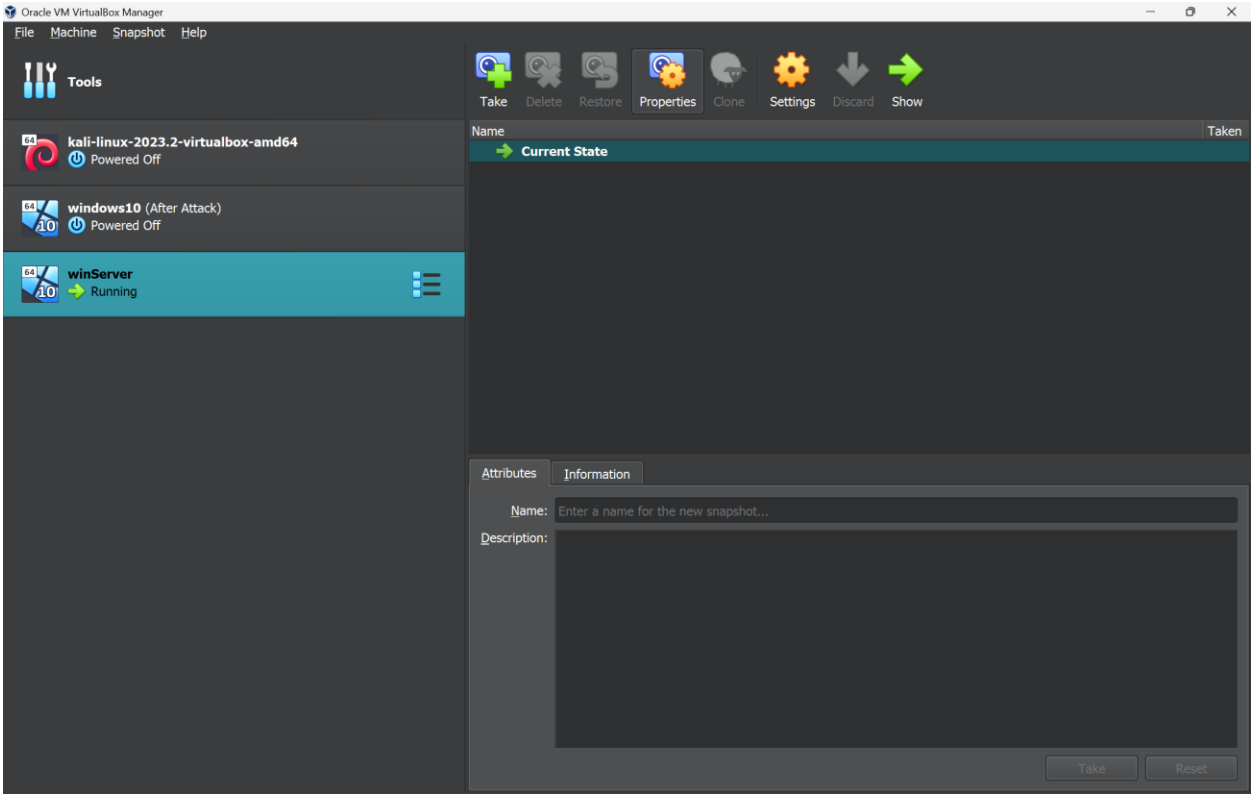
```
C:\Users\user\Documents\Evidence>vboxmanage clonemedium disk b53bcbe7-8c9
4-4e91-a8a6-43b6a97669ec --format VHD win10-disk.vhd
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Clone medium created in format 'VHD'. UUID: 3f863ee8-a7ba-4c54-aca7-fd5a8
8a2d9df
```

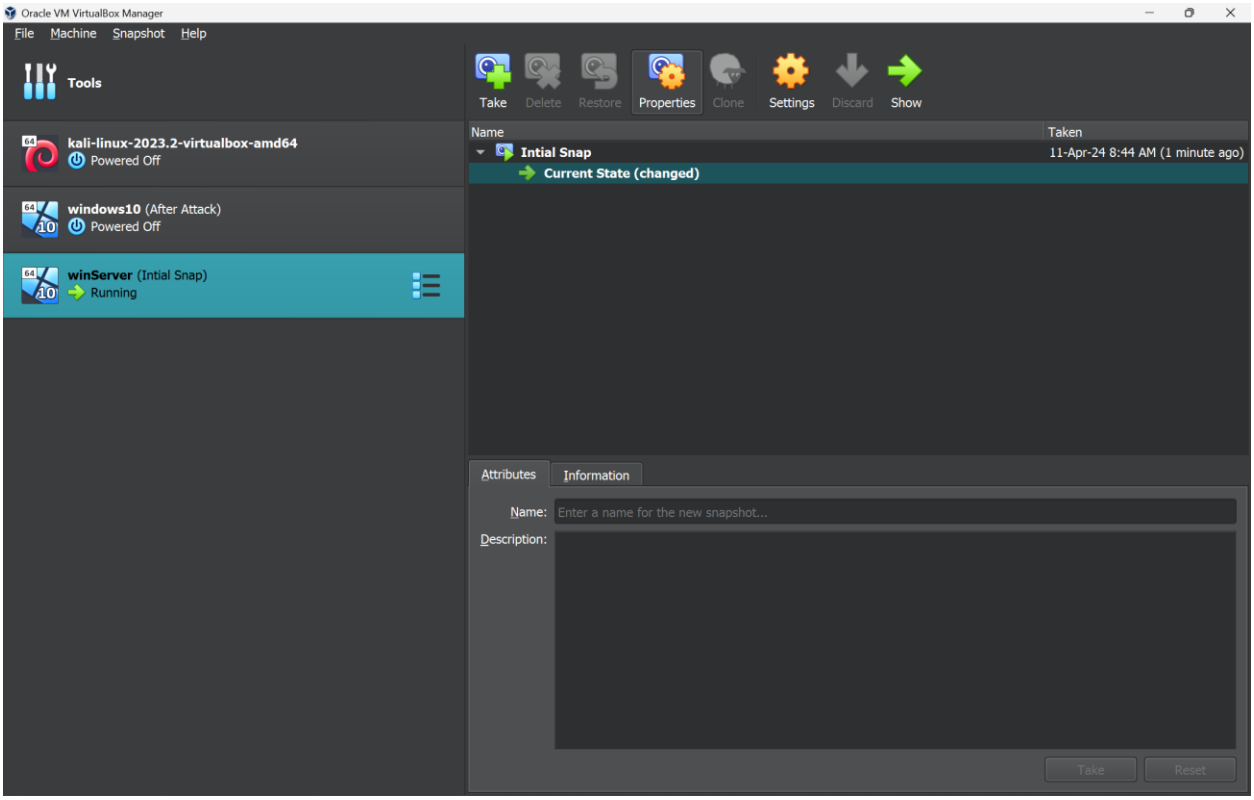
```
C:\Users\user\Documents\Evidence>dir
 Volume in drive C is Windows
 Volume Serial Number is CC1C-F525

 Directory of C:\Users\user\Documents\Evidence

10-Apr-24  09:44 PM    <DIR>          .
10-Apr-24  09:19 PM    <DIR>          ..
10-Apr-24  09:44 PM    14,012,499,968 win10-disk.vhd
10-Apr-24  09:33 PM               127 win10-memory-hash.txt
10-Apr-24  09:31 PM     2,287,859,552 win10-memory.exe
               3 File(s) 16,300,359,647 bytes
               2 Dir(s)  55,249,915,904 bytes free
```

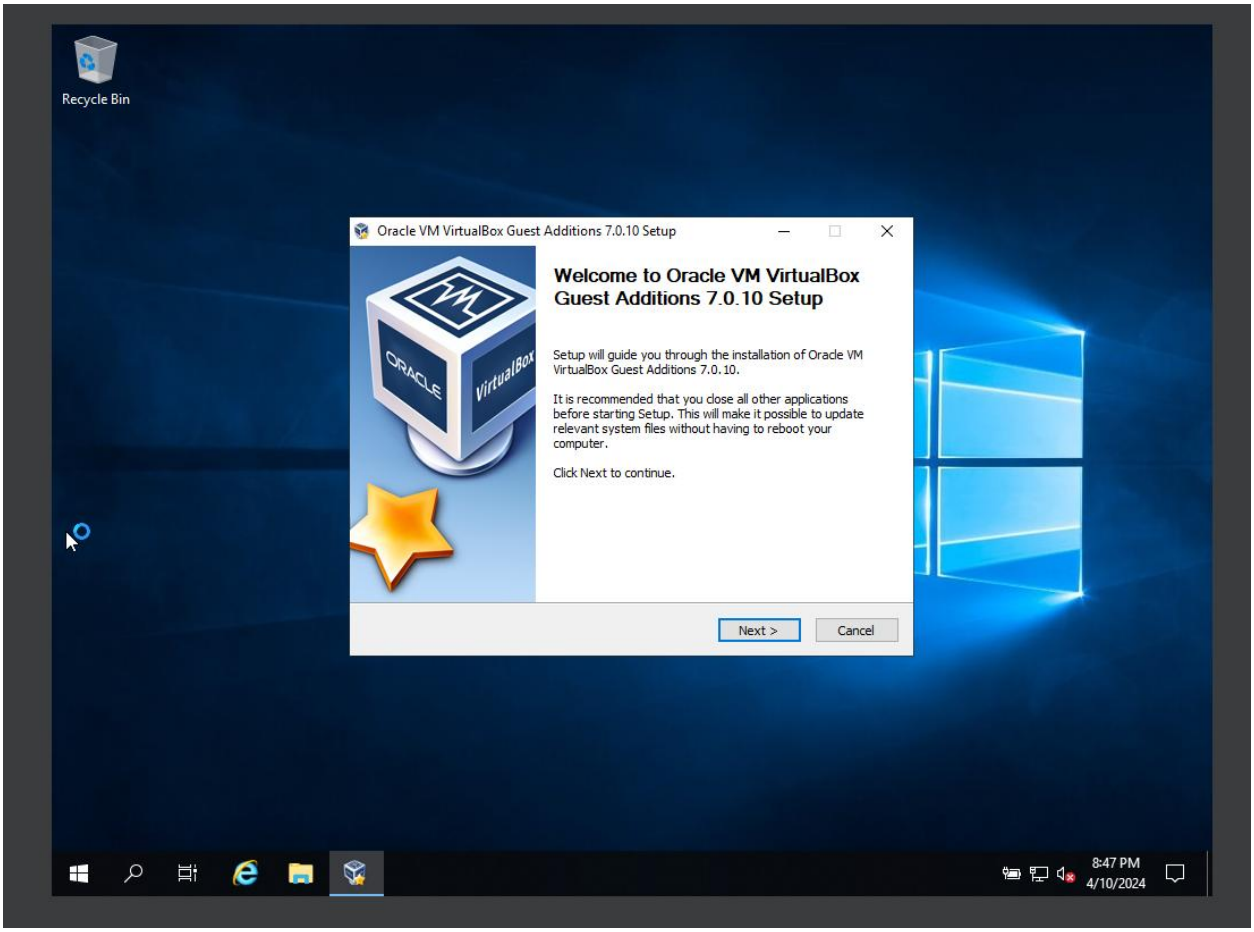
HASH CALCULATIONS OF VHD FILE:

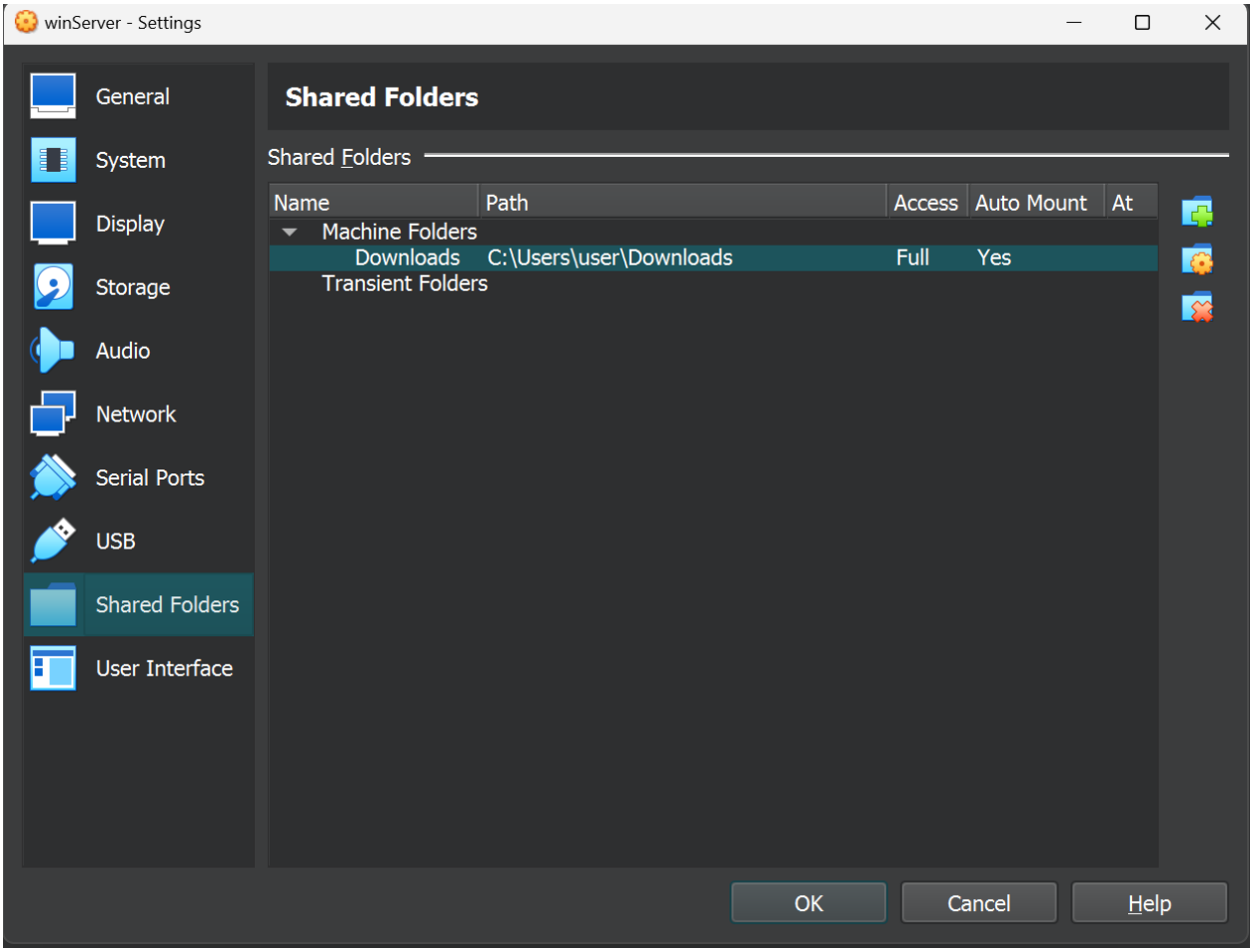
```
C:\Users\user\Documents\Evidence>certUtil -hashfile win10-disk.vhd  > win
10-disk-hash.txt
```

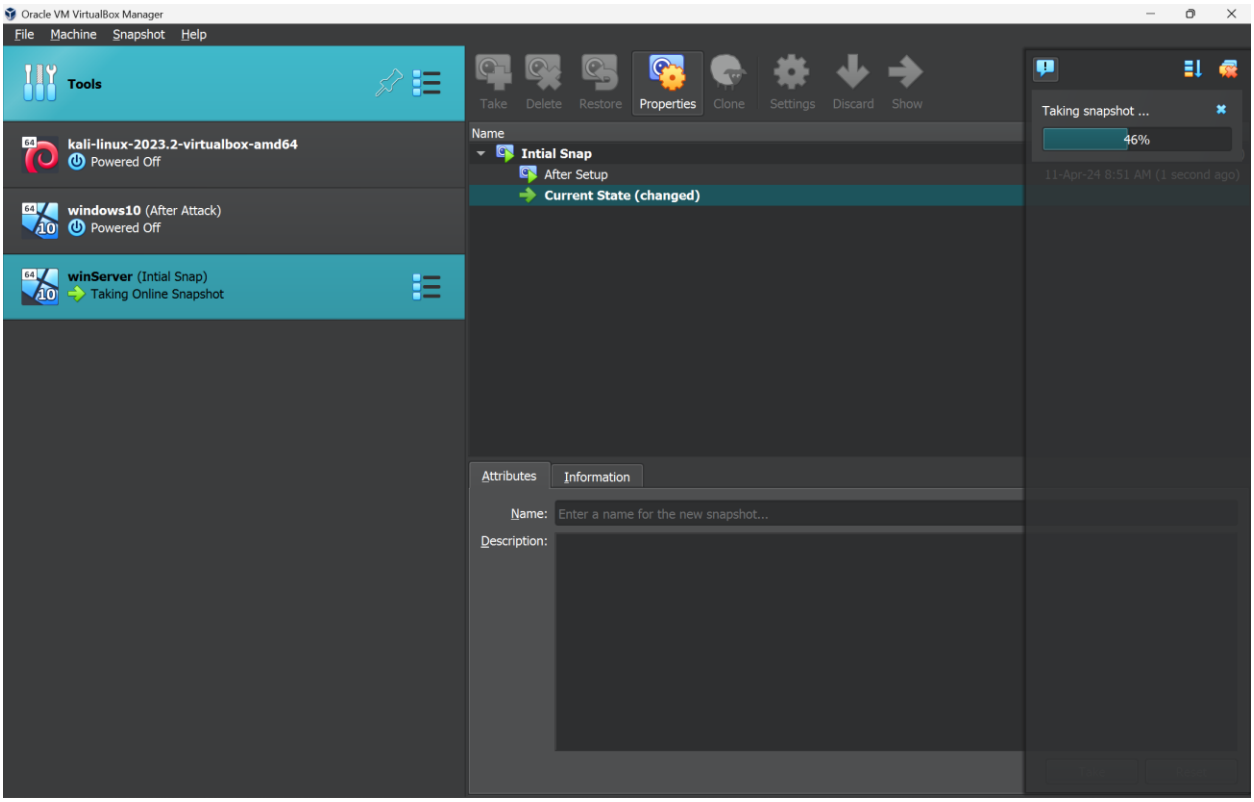


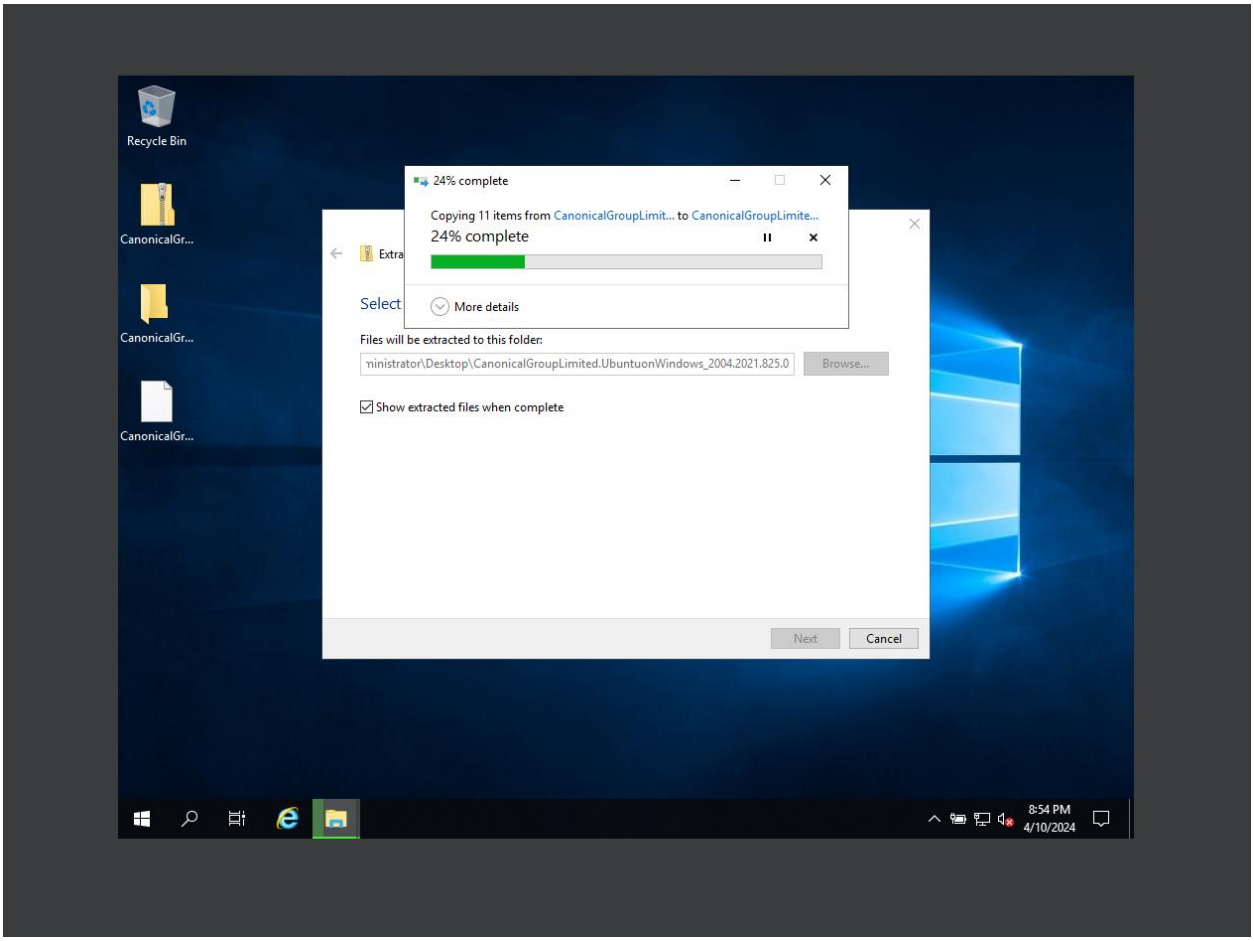

Oracle VM VirtualBox Manager
File Machine Snapshot Help
Tools
Take Delete Restore Properties Clone Settings Discard Show
kali-linux-2023.2-virtualbox-amd64
Powered Off
windows10 (After Attack)
Powered Off
winServer
Running
Name Taken
Current State
Attributes Information
Name: Enter a name for the new snapshot...
Description:
Take Reset

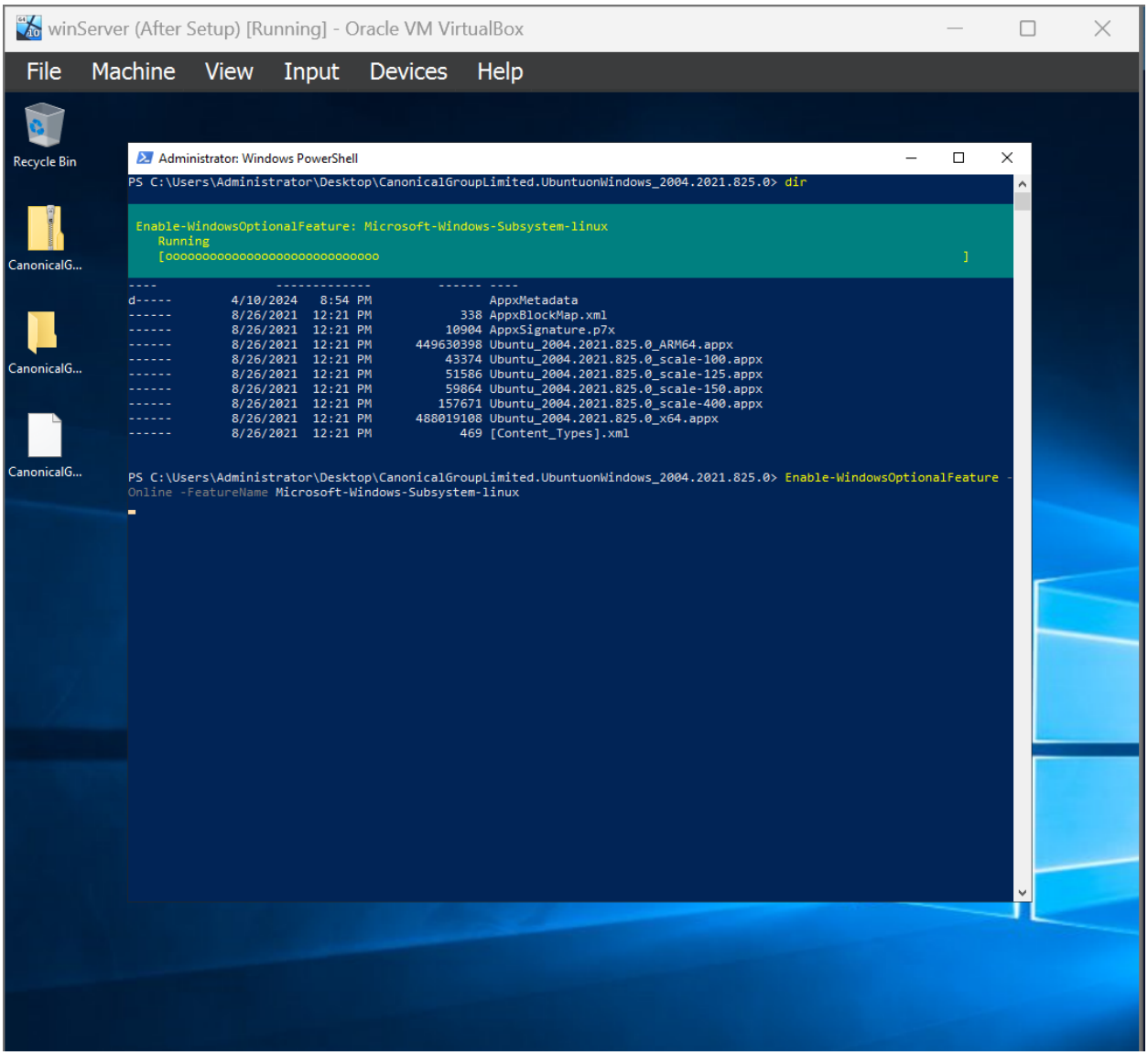

Oracle VM VirtualBox Manager
File Machine Snapshot Help
Tools
Take Delete Restore Properties Clone Settings Discard Show
kali-linux-2023.2-virtualbox-amd64
Powered Off
windows10 (After Attack)
Powered Off
winServer (Intial Snap)
Running
Name Taken
Intial Snap 11-Apr-24 8:44 AM (1 minute ago)
Current State (changed)
Attributes Information
Name: Enter a name for the new snapshot...
Description:
Take Reset

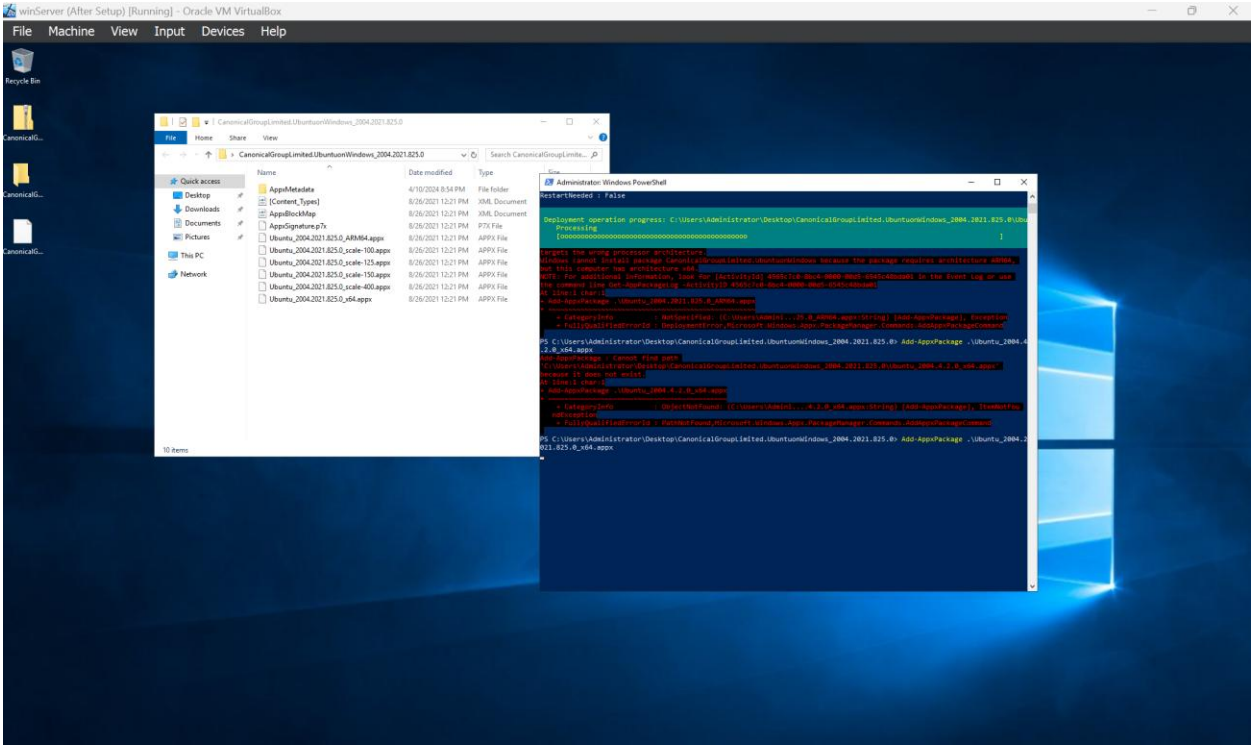

Recycle Bin
Oracle VM VirtualBox Guest Additions 7.0.10 Setup
Welcome to Oracle VM VirtualBox Guest Additions 7.0.10 Setup
Setup will guide you through the installation of Oracle VM VirtualBox Guest Additions 7.0.10.
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.
Click Next to continue.
Next >
Cancel
8:47 PM
4/10/2024

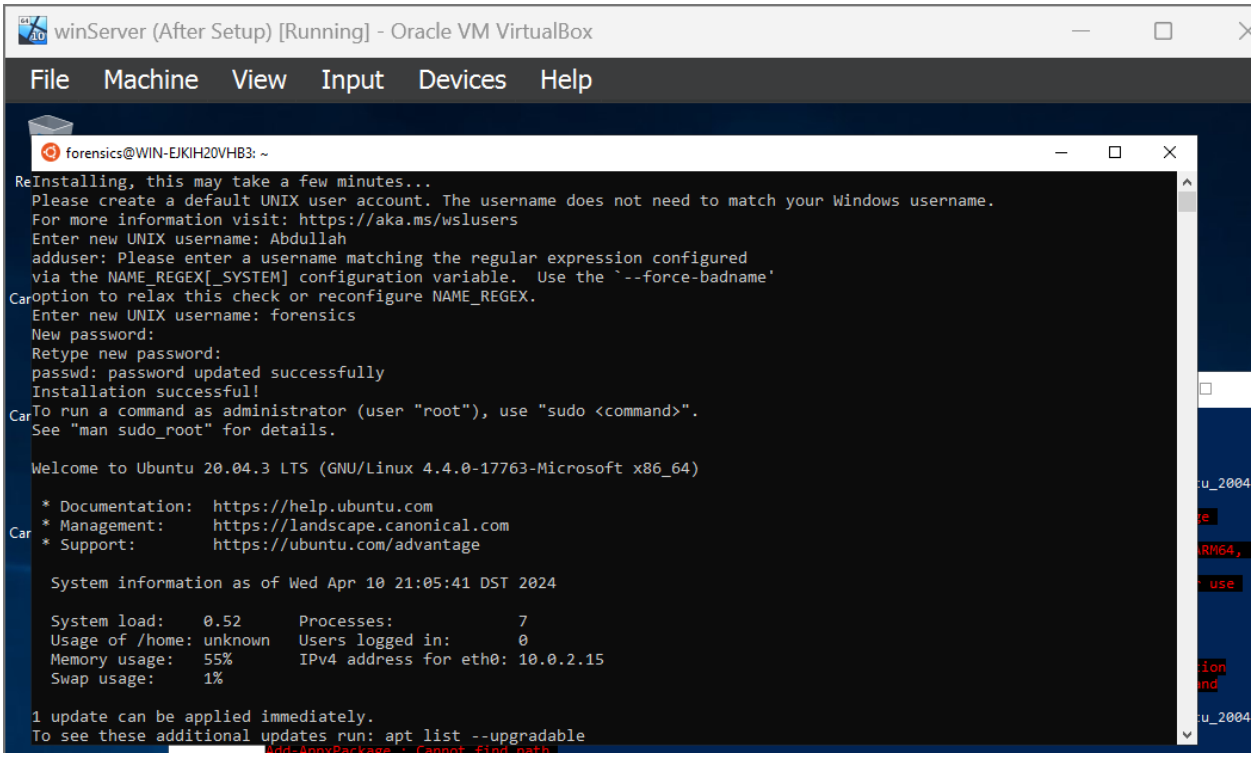

winServer - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Shared Folders
Shared Folders
Name
Path
Access
Auto Mount
At
Machine Folders
Downloads
C:\Users\user\Downloads
Full
Yes
Transient Folders
OK
Cancel
Help

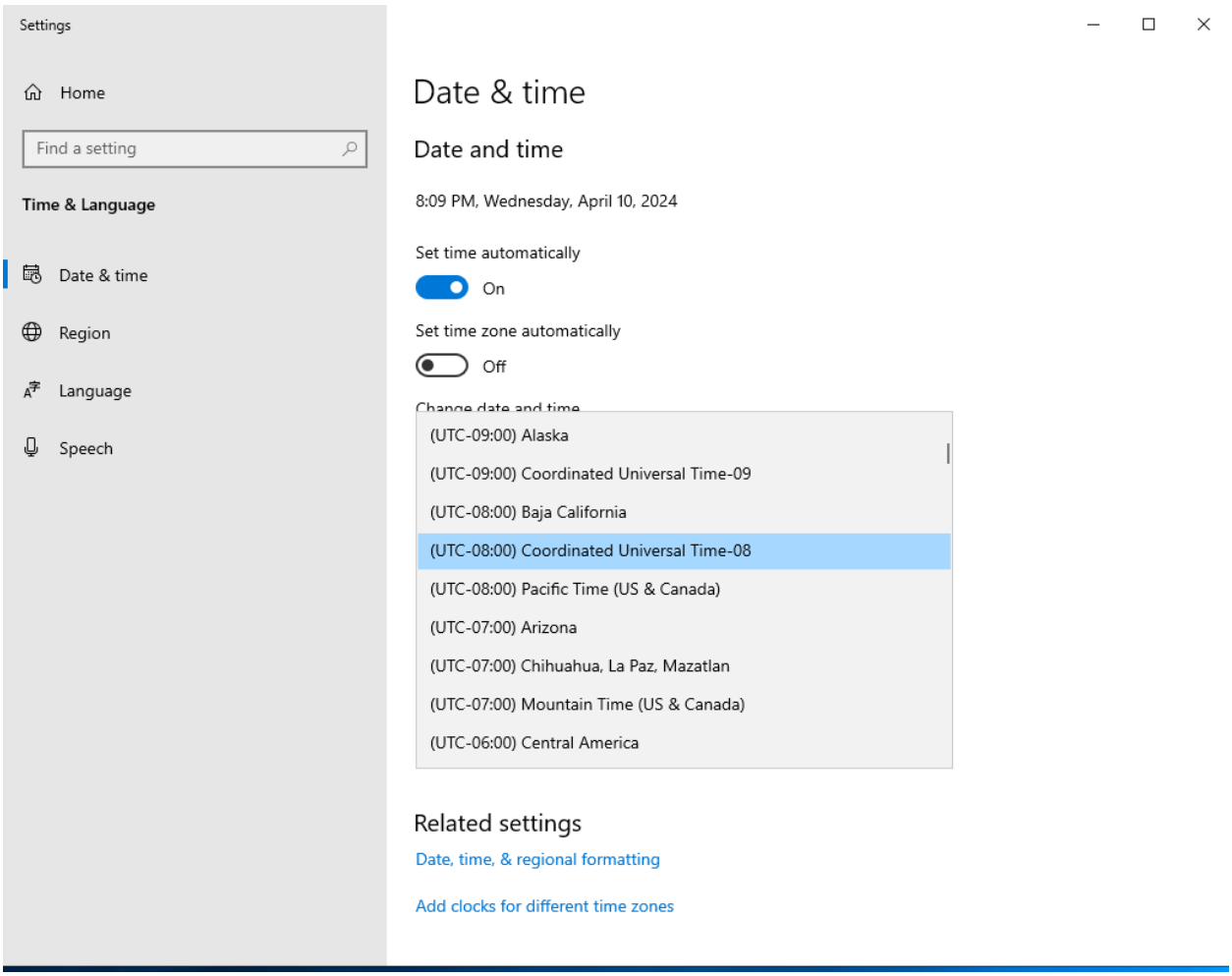

Oracle VM VirtualBox Manager
File Machine Snapshot Help
Tools
kali-linux-2023.2-virtualbox-amd64
Powered Off
windows10 (After Attack)
Powered Off
winServer (Intial Snap)
Taking Online Snapshot
Take Delete Restore Properties Clone Settings Discard Show
Name
Intial Snap
After Setup
Current State (changed)
Taking snapshot ...
46%
11-Apr-24 8:51 AM (1 second ago)
Attributes Information
Name: Enter a name for the new snapshot...
Description:

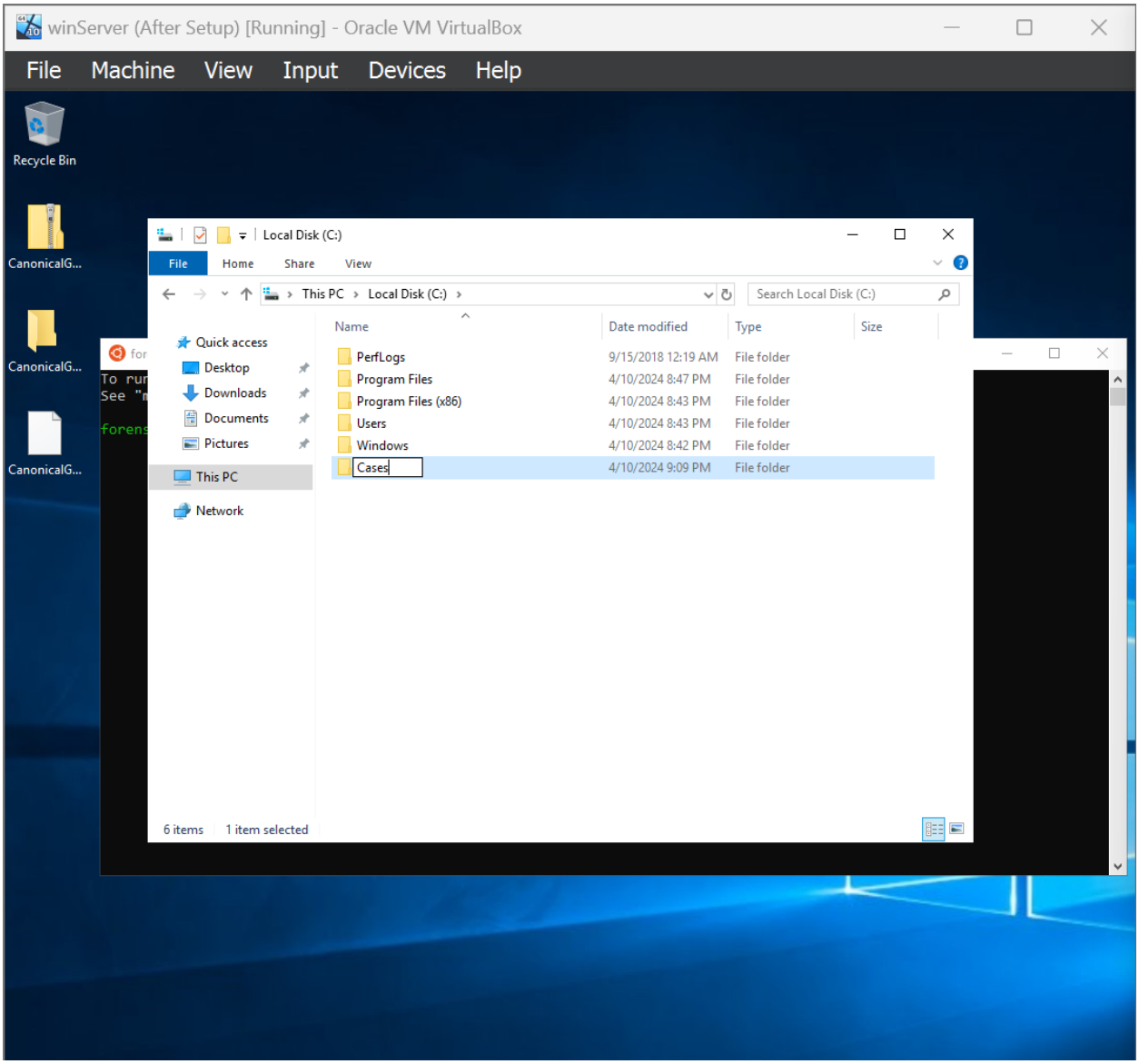

Recycle Bin
CanonicalGr...
CanonicalGr...
CanonicalGr...
24% complete
Copying 11 items from CanonicalGroupLimit... to CanonicalGroupLimite...
24% complete
More details
Select
Files will be extracted to this folder:
ninistrator\Desktop\CanonicalGroupLimited.UbuntuonWindows_2004.2021.825.0
Browse...
Show extracted files when complete
Next
Cancel
8:54 PM
4/10/2024

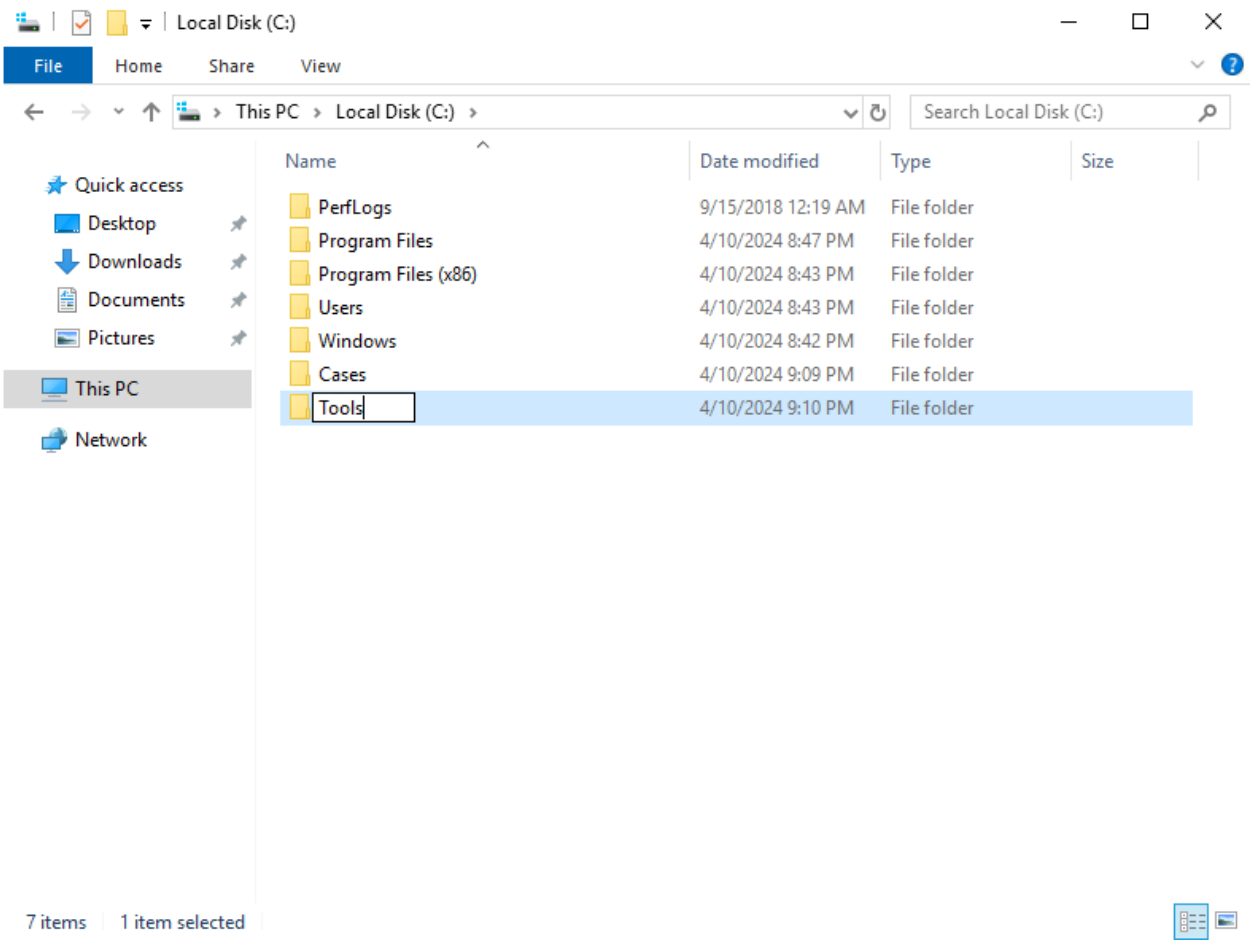

winServer (After Setup) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
CanonicalG...
CanonicalG...
CanonicalG...
Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop\CanonicalGroupLimited.UbuntuonWindows_2004.2021.825.0> dir
Enable-WindowsOptionalFeature: Microsoft-Windows-Subsystem-linux
Running
[oooooooooooooooooooooooooooo]
Mode LastWriteTime Length Name
d----- 4/10/2024 8:54 PM AppxMetadata
------ 8/26/2021 12:21 PM 338 AppxBlockMap.xml
------ 8/26/2021 12:21 PM 10904 AppxSignature.p7x
------ 8/26/2021 12:21 PM 449630398 Ubuntu_2004.2021.825.0_ARM64.appx
------ 8/26/2021 12:21 PM 43374 Ubuntu_2004.2021.825.0_scale-100.appx
------ 8/26/2021 12:21 PM 51586 Ubuntu_2004.2021.825.0_scale-125.appx
------ 8/26/2021 12:21 PM 59864 Ubuntu_2004.2021.825.0_scale-150.appx
------ 8/26/2021 12:21 PM 157671 Ubuntu_2004.2021.825.0_scale-400.appx
------ 8/26/2021 12:21 PM 488019108 Ubuntu_2004.2021.825.0_x64.appx
------ 8/26/2021 12:21 PM 469 [Content_Types].xml
PS C:\Users\Administrator\Desktop\CanonicalGroupLimited.UbuntuonWindows_2004.2021.825.0> Enable-WindowsOptionalFeature -
Online -FeatureName Microsoft-Windows-Subsystem-linux

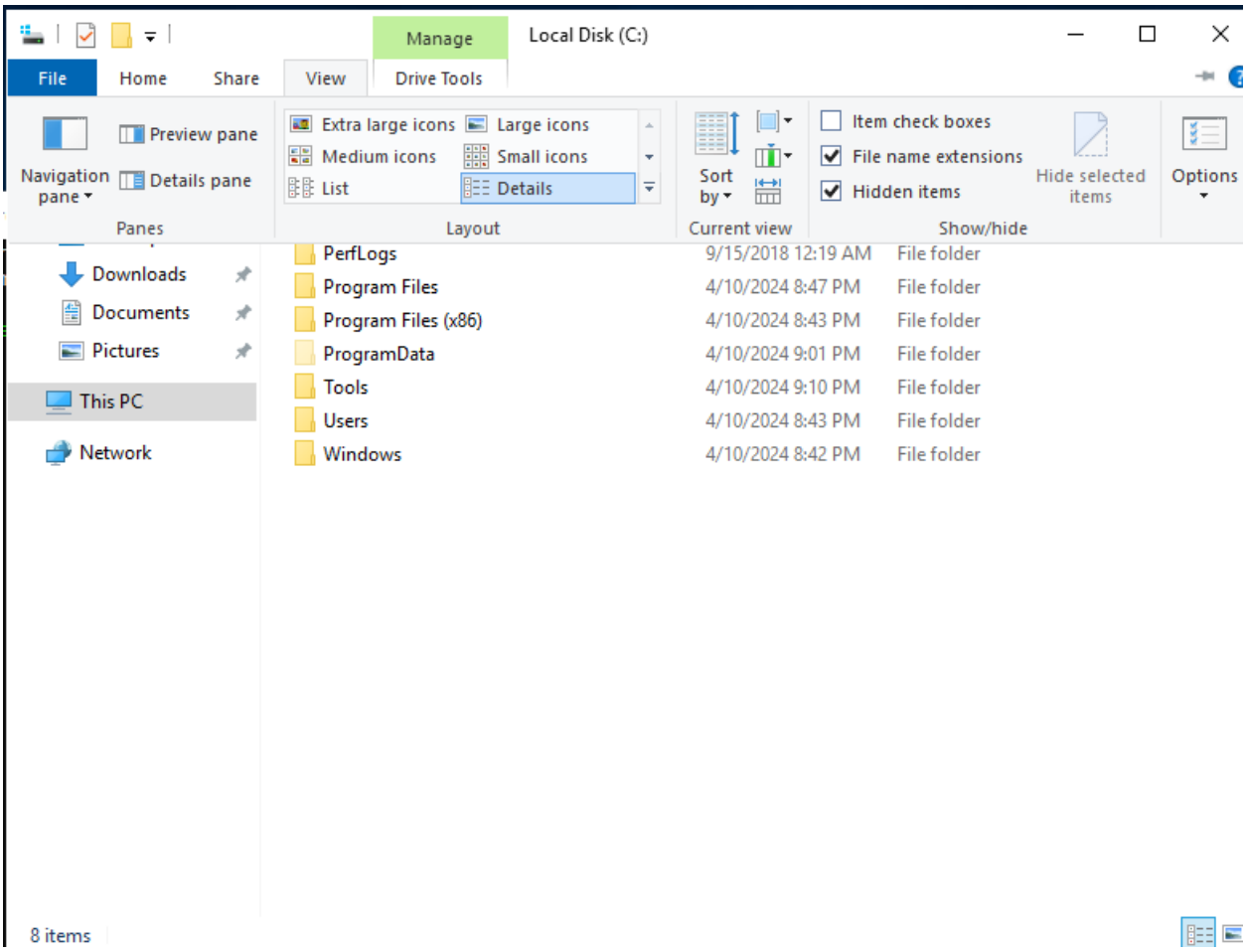

winServer (After Setup) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Administrator: Windows PowerShell

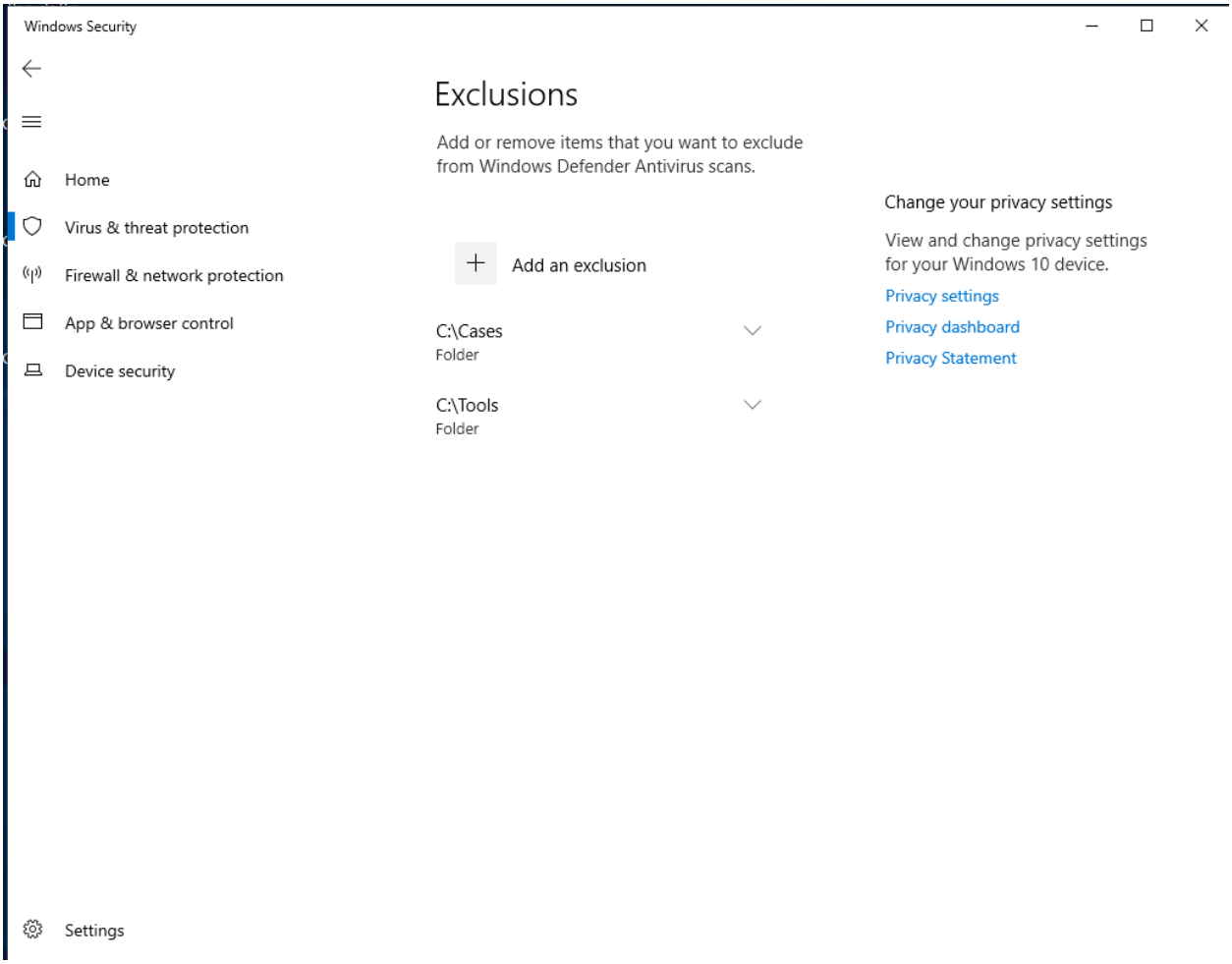

winServer (After Setup) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
forensics@WIN-EJKIH20VHB3: ~
Installing, this may take a few minutes...
Please create a default UNIX user account. The username does not need to match your Windows username.
For more information visit: https://aka.ms/wslusers
Enter new UNIX username: Abdullah
adduser: Please enter a username matching the regular expression configured
via the NAME_REGEX[_SYSTEM] configuration variable. Use the `--force-badname'
option to relax this check or reconfigure NAME_REGEX.
Enter new UNIX username: forensics
New password:
Retype new password:
passwd: password updated successfully
Installation successful!
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 4.4.0-17763-Microsoft x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Wed Apr 10 21:05:41 DST 2024
System load: 0.52 Processes: 7
Usage of /home: unknown Users logged in: 0
Memory usage: 55% IPv4 address for eth0: 10.0.2.15
Swap usage: 1%
1 update can be applied immediately.
To see these additional updates run: apt list --upgradable

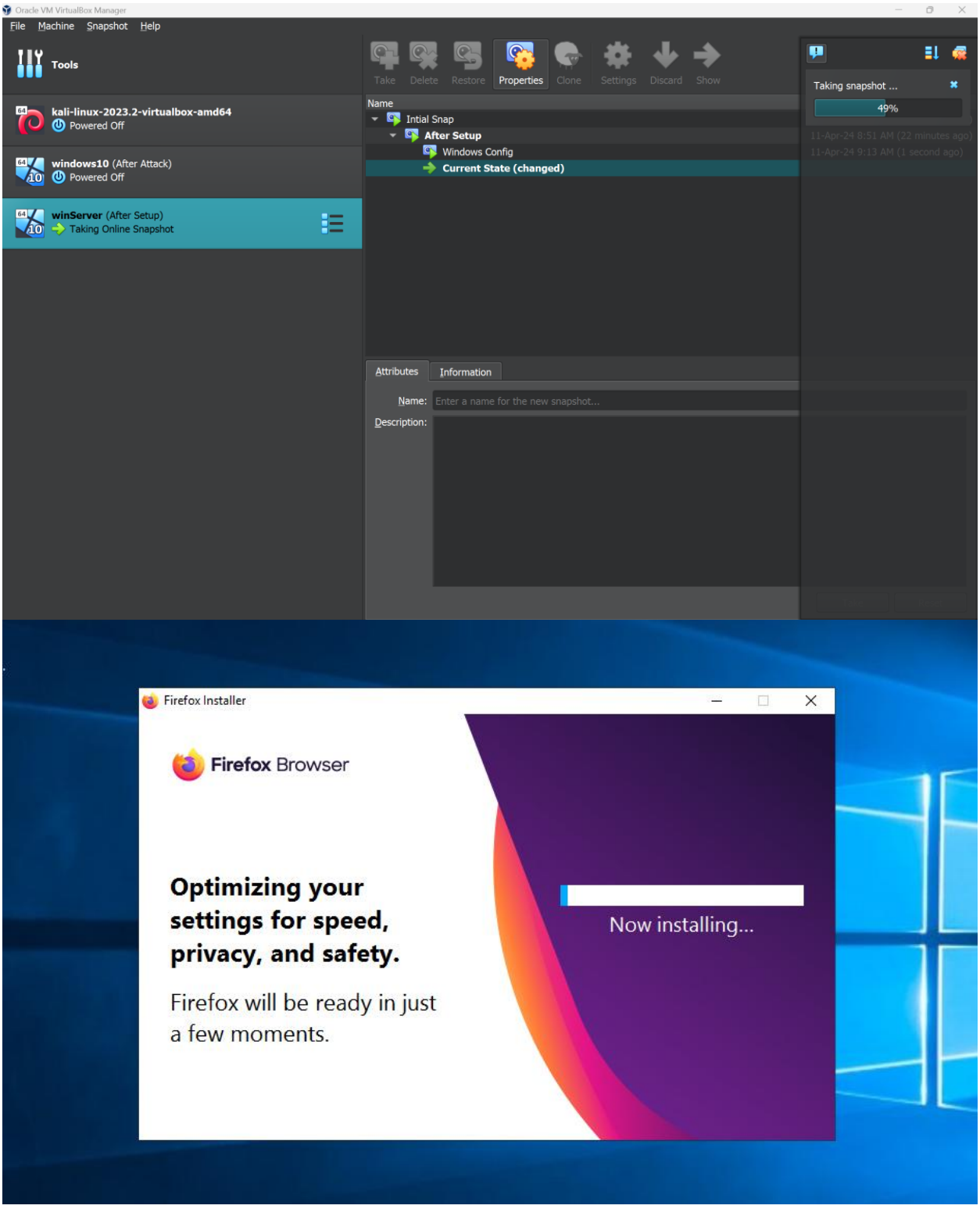

Settings
Home
Find a setting
Time & Language
Date & time
Region
Language
Speech
Date & time
Date and time
8:09 PM, Wednesday, April 10, 2024
Set time automatically
On
Set time zone automatically
Off
Change date and time
(UTC-09:00) Alaska
(UTC-09:00) Coordinated Universal Time-09
(UTC-08:00) Baja California
(UTC-08:00) Coordinated Universal Time-08
(UTC-08:00) Pacific Time (US & Canada)
(UTC-07:00) Arizona
(UTC-07:00) Chihuahua, La Paz, Mazatlan
(UTC-07:00) Mountain Time (US & Canada)
(UTC-06:00) Central America
Related settings
Date, time, & regional formatting
Add clocks for different time zones

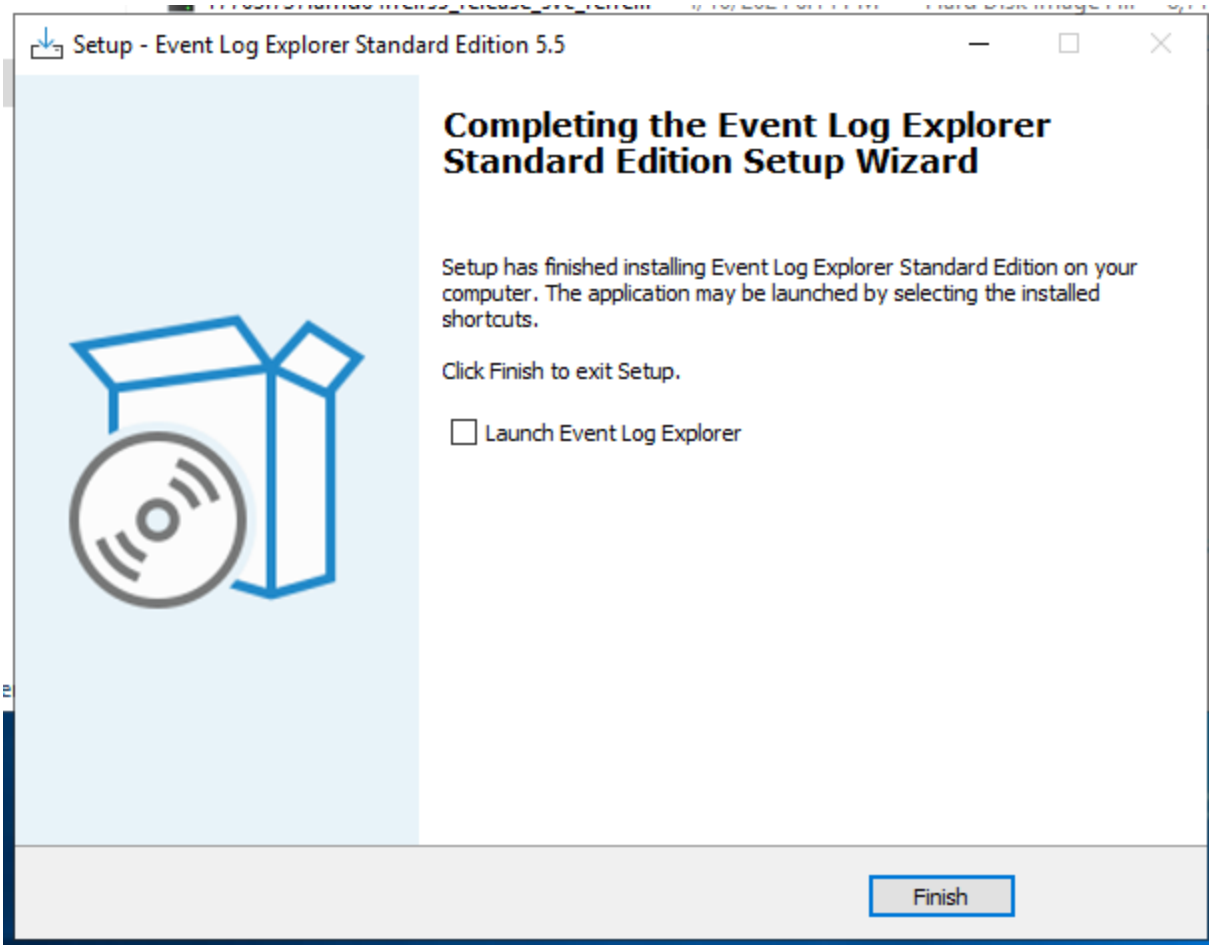

winServer (After Setup) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
CanonicalG...
CanonicalG...
CanonicalG...
Local Disk (C:)
File Home Share View
This PC › Local Disk (C:) ›
Search Local Disk (C:)
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modified
Type
Size
PerfLogs 9/15/2018 12:19 AM File folder
Program Files 4/10/2024 8:47 PM File folder
Program Files (x86) 4/10/2024 8:43 PM File folder
Users 4/10/2024 8:43 PM File folder
Windows 4/10/2024 8:42 PM File folder
Cases 4/10/2024 9:09 PM File folder
6 items 1 item selected

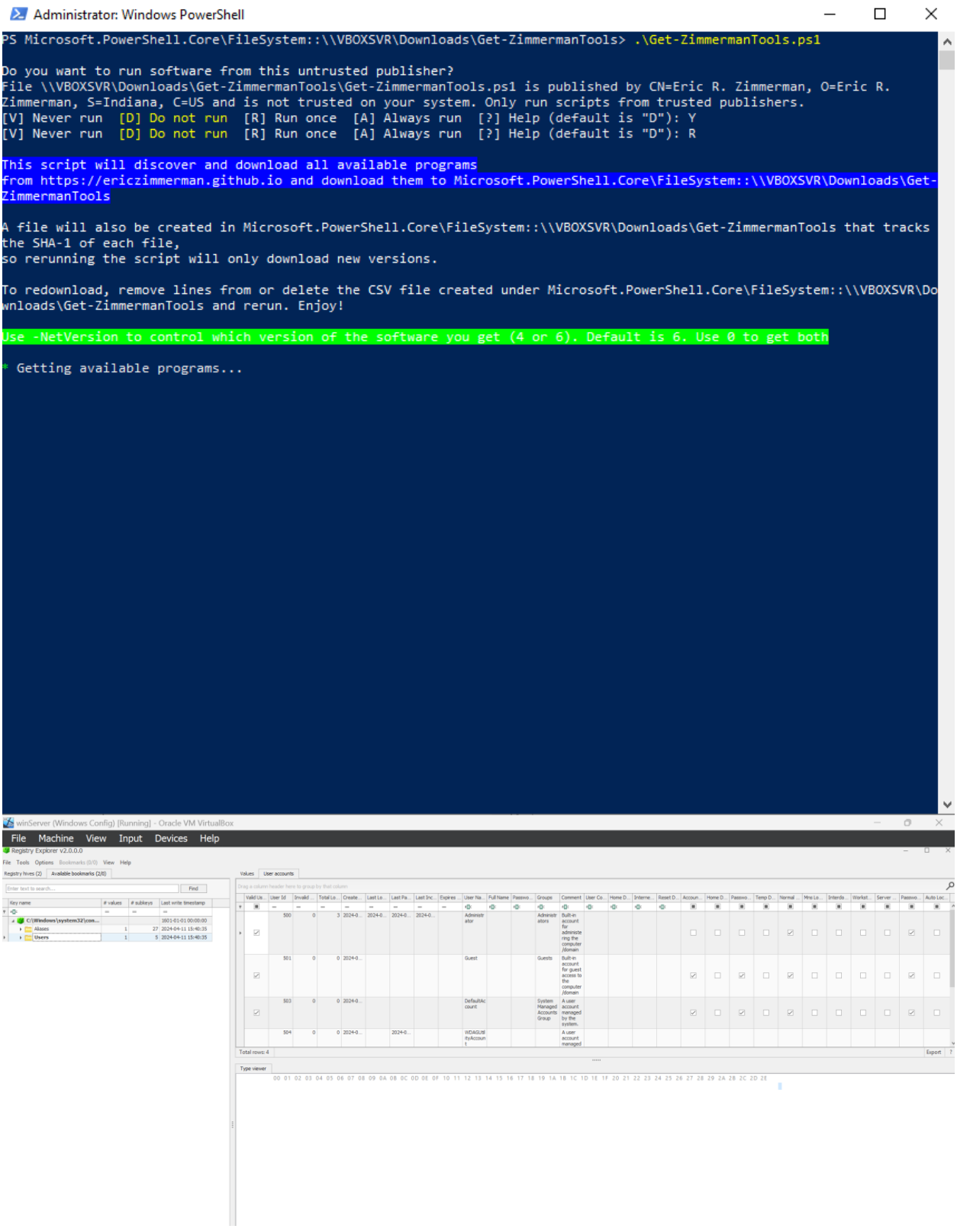

Local Disk (C:)
File
Home
Share
View
This PC
Local Disk (C:)
Search Local Disk (C:)
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modified
Type
Size
PerfLogs 9/15/2018 12:19 AM File folder
Program Files 4/10/2024 8:47 PM File folder
Program Files (x86) 4/10/2024 8:43 PM File folder
Users 4/10/2024 8:43 PM File folder
Windows 4/10/2024 8:42 PM File folder
Cases 4/10/2024 9:09 PM File folder
Tools 4/10/2024 9:10 PM File folder
7 items
1 item selected

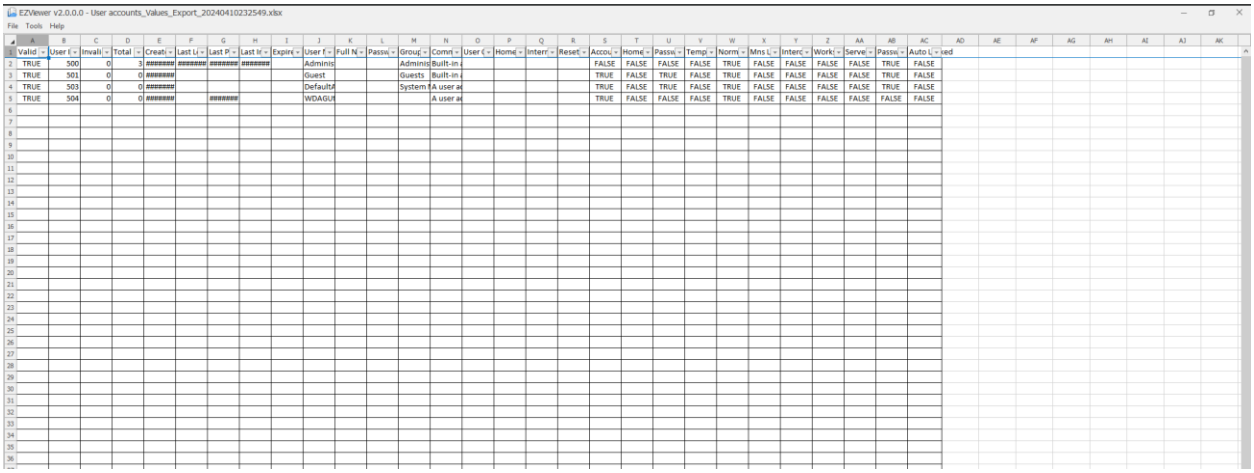

Manage
Local Disk (C:)
File
Home
Share
View
Drive Tools
Preview pane
Navigation pane
Details pane
Panes
Extra large icons
Large icons
Medium icons
Small icons
List
Details
Layout
Sort by
Current view
Item check boxes
File name extensions
Hidden items
Hide selected items
Show/hide
Options
Downloads
Documents
Pictures
This PC
Network
PerfLogs 9/15/2018 12:19 AM File folder
Program Files 4/10/2024 8:47 PM File folder
Program Files (x86) 4/10/2024 8:43 PM File folder
ProgramData 4/10/2024 9:01 PM File folder
Tools 4/10/2024 9:10 PM File folder
Users 4/10/2024 8:43 PM File folder
Windows 4/10/2024 8:42 PM File folder
8 items


Windows Security
Exclusions
Add or remove items that you want to exclude from Windows Defender Antivirus scans.
Add an exclusion
C:\Cases
Folder
C:\Tools
Folder
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement
Home
Virus & threat protection
Firewall & network protection
App & browser control
Device security
Settings


Oracle VM VirtualBox Manager
File Machine Snapshot Help
Tools
kali-linux-2023.2-virtualbox-amd64
Powered Off
windows10 (After Attack)
Powered Off
winServer (After Setup)
Taking Online Snapshot
Take Delete Restore Properties Clone Settings Discard Show
Name
Intial Snap
After Setup
Windows Config
Current State (changed)
Taking snapshot ...
49%
11-Apr-24 8:51 AM (22 minutes ago)
11-Apr-24 9:13 AM (1 second ago)
Attributes Information
Name: Enter a name for the new snapshot...
Description:
Firefox Installer
Firefox Browser
Optimizing your settings for speed, privacy, and safety.
Firefox will be ready in just a few moments.
Now installing...


Setup - Event Log Explorer Standard Edition 5.5
Completing the Event Log Explorer Standard Edition Setup Wizard
Setup has finished installing Event Log Explorer Standard Edition on your computer. The application may be launched by selecting the installed shortcuts.
Click Finish to exit Setup.
Launch Event Log Explorer
Finish


Administrator: Windows PowerShell
PS Microsoft.PowerShell.Core\FileSystem::\\VBOXSVR\Downloads\Get-ZimmermanTools> .\Get-ZimmermanTools.ps1
Do you want to run software from this untrusted publisher?
File \\VBOXSVR\Downloads\Get-ZimmermanTools\Get-ZimmermanTools.ps1 is published by CN=Eric R. Zimmerman, O=Eric R. Zimmerman, S=Indiana, C=US and is not trusted on your system. Only run scripts from trusted publishers.
[V] Never run [D] Do not run [R] Run once [A] Always run [?] Help (default is "D"): Y
[V] Never run [D] Do not run [R] Run once [A] Always run [?] Help (default is "D"): R
This script will discover and download all available programs
from https://ericzimmerman.github.io and download them to Microsoft.PowerShell.Core\FileSystem::\\VBOXSVR\Downloads\Get-ZimmermanTools
A file will also be created in Microsoft.PowerShell.Core\FileSystem::\\VBOXSVR\Downloads\Get-ZimmermanTools that tracks the SHA-1 of each file,
so rerunning the script will only download new versions.
To redownload, remove lines from or delete the CSV file created under Microsoft.PowerShell.Core\FileSystem::\\VBOXSVR\Downloads\Get-ZimmermanTools and rerun. Enjoy!
Use -NetVersion to control which version of the software you get (4 or 6). Default is 6. Use 0 to get both
* Getting available programs...
winServer (Windows Config) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help



EZViewer v2.0.0.0 - User accounts_Values_Export_20240410232549.xlsx

File Tools Help

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK
1	Valid	User I	Invali	Total	Creati	Last Li	Last P	Last In	Expire	User f	Full N	Passw	Group	Comm	User C	Home	Interr	Reset	Accou	Home	Passw	Temp	Norm	Mns L	Interc	Work	Serve	Passw	Auto L	ved								
2	TRUE	500	0	3	########	########	########	########		Adminis			Adminis	Built-in					FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE									
3	TRUE	501	0	0	########					Guest			Guests	Built-in					TRUE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE									
4	TRUE	503	0	0	########					DefaultA			System	A user ac					TRUE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE									
5	TRUE	504	0	0	########		########			WDAGUt				A user ac					TRUE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE									

Investigator's information

Name:

Abdullah

Registration Number:

FA22-BCT-004

System Information

Computer Name:

Name DESKTOP-4N3KRH7 Recent Activity

Program Name Windows 10 Enterprise Evaluation Recent Activity

Processor Architecture AMD64Recent Activity

Temporary Files Directory %SystemRoot%\TEMP Recent Activity

Path C:\Windows Recent Activity

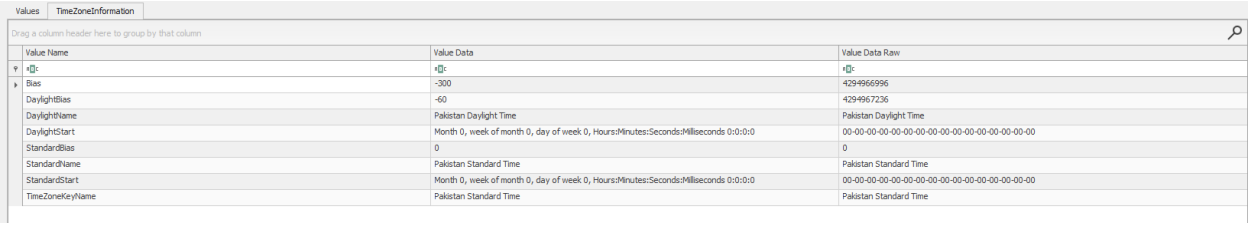
Product ID 00329-20000-00001-AA223 Recent Activity

Owner Abdullah Recent Activity

Source File Path /img_win10-disk.vhd

Artifact ID -9223372036854775711

Time zone:



Values | TimeZoneInformation

Drag a column header here to group by that column

Value Name	Value Data	Value Data Raw
×□×	×□×	×□×
Bias	-300	4294966996
DaylightBias	-60	4294967236
DaylightName	Pakistan Daylight Time	Pakistan Daylight Time
DaylightStart	Month 0, week of month 0, day of week 0, Hours:Minutes:Seconds:Milliseconds 0:0:0:0	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
StandardBias	0	0
StandardName	Pakistan Standard Time	Pakistan Standard Time
StandardStart	Month 0, week of month 0, day of week 0, Hours:Minutes:Seconds:Milliseconds 0:0:0:0	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
TimeZoneKeyName	Pakistan Standard Time	Pakistan Standard Time

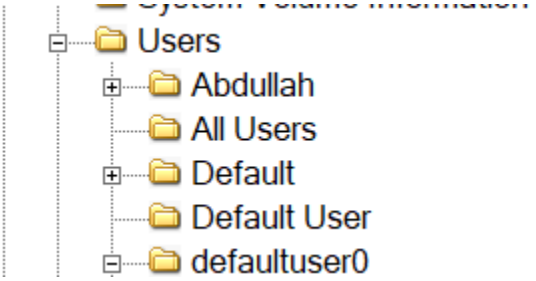
Network Information:

Values | DHCPNetworkHints | NetworkSettings

Drag a column header here to group by that column

IP Address	Subnet Mask	DHCP Subnet Mask	DHCP Server	DHCP Name Server	DHCPIP Address	DHCP Default Gateway	Enabled DHCP
		255.255.255.0	10.0.2.2	192.168.18.1	10.0.2.15	10.0.2.2	☑
							☑
							☐

Users, Groups and User Profiles



Active accounts during the attack timeframe?

Vc	Us	Int	Tc	Cr	La	La	La	Ex	Us	Fu	Pa	Gr	Cc	Us	Hc	Int	Re	Ac	Hc	Pa	Te	Nc	M	Int	W	Se	Pa	Aut	ocked	
####	500	0	0	####					Admi			Admi	Built-					####	####	####	####	####	####	####	####	####	####	FALSE		
####	501	0	0	####					Guest			Guest	Built-					####	####	####	####	####	####	####	####	####	####	FALSE		
####	503	0	0	####					Defau			Syste	A use					####	####	####	####	####	####	####	####	####	####	FALSE		
####	504	0	0	####		####			WDA				A use					####	####	####	####	####	####	####	####	####	####	FALSE		
####	1001	0	4	####	####				Abdu			Admi					{"vers	####	####	####	####	####	####	####	####	####	####	FALSE		
####	1002	0	0	####		####			art-te			Admi						####	####	####	####	####	####	####	####	####	####	FALSE		

Which account(s) were created?

S-1-5-21-239386965-2826860934-2307490478-1(	0	Abdullah	win10-disk.vhd_1 Host	Domain		2024-04-10 02:13:34 PKT	
S-1-5-21-239386965-2826860934-2307490478-1(	0		win10-disk.vhd_1 Host	Domain			
S-1-5-80-2620923248-4247863784-3378508180-2	0		win10-disk.vhd_1 Host	Local	NT SERVICE		
S-1-5-20		NETWORK SERVICE	win10-disk.vhd_1 Host	Local	NT AUTHORITY		
S-1-5-21-3933942852-973373972-2766786355-1(	0		win10-disk.vhd_1 Host	Domain			
S-1-5-21-239386965-2826860934-2307490478-5(	0	Administrator	win10-disk.vhd_1 Host	Domain		2024-04-10 14:12:03 PKT	
S-1-5-21-239386965-2826860934-2307490478-5(	0	Guest	win10-disk.vhd_1 Host	Domain		2024-04-10 14:12:03 PKT	
S-1-5-21-239386965-2826860934-2307490478-5(	0	WDAGUtilityAccount	win10-disk.vhd_1 Host	Domain		2024-04-10 14:12:03 PKT	
S-1-5-21-239386965-2826860934-2307490478-5(	0	DefaultAccount	win10-disk.vhd_1 Host	Domain		2024-04-10 14:12:03 PKT	
S-1-5-21-239386965-2826860934-2307490478-1(	0	art-test	win10-disk.vhd_1 Host	Domain		2024-04-10 21:13:13 PKT	

User Behavior

UserAssist: Applications opened

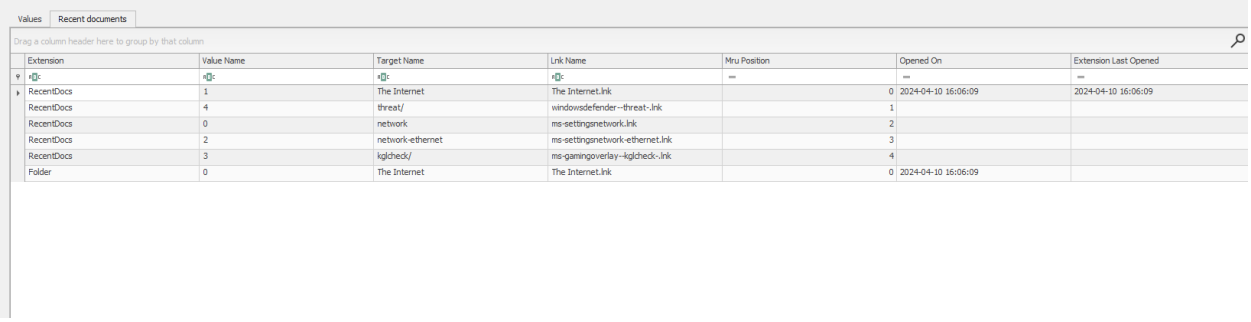
Drag a column header here to group by that column

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
UEME_CTLSESSION	104	195	0d, 1h, 31m, 12s	
Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe!App	13	19	0d, 0h, 06m, 08s	2024-04-09 21:12:19
Microsoft.WindowsMaps_8wekyb3d8bbwe!App	12	17	0d, 0h, 05m, 17s	2024-04-09 21:12:19
Microsoft.People_8wekyb3d8bbwe!x4c7a3b7dy2188y46d4ya362y19ac5a5805e5x	11	15	0d, 0h, 04m, 25s	2024-04-09 21:12:19
Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe!App	10	13	0d, 0h, 03m, 34s	2024-04-09 21:12:19
{System}\SnippingTool.exe	9	11	0d, 0h, 02m, 42s	2024-04-09 21:12:19
Microsoft.WindowsCalculator_8wekyb3d8bbwe!App	8	9	0d, 0h, 01m, 51s	2024-04-09 21:12:19
{System}\mspaint.exe	7	7	0d, 0h, 01m, 00s	2024-04-09 21:12:19
Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy!App	0	10	0d, 0h, 05m, 09s	
Microsoft.Windows.Search_cw5n1h2txyewy!CortanaUI	0	9	0d, 0h, 01m, 24s	
Microsoft.Windows.SecHealthUI_cw5n1h2txyewy!SecHealthUI	4	5	0d, 0h, 04m, 36s	2024-04-10 16:06:06
{System}\WindowsPowerShell\v1.0\powershell.exe	2	14	0d, 0h, 15m, 12s	2024-04-09 22:05:55
windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel	8	15	0d, 0h, 06m, 48s	2024-04-10 16:05:50
{System}\msdt.exe	0	1	0d, 0h, 00m, 06s	

Total rows: 26 Export ?

Type viewer | Slack viewer

RecentDocs: Files and folders opened



Values | Recent documents

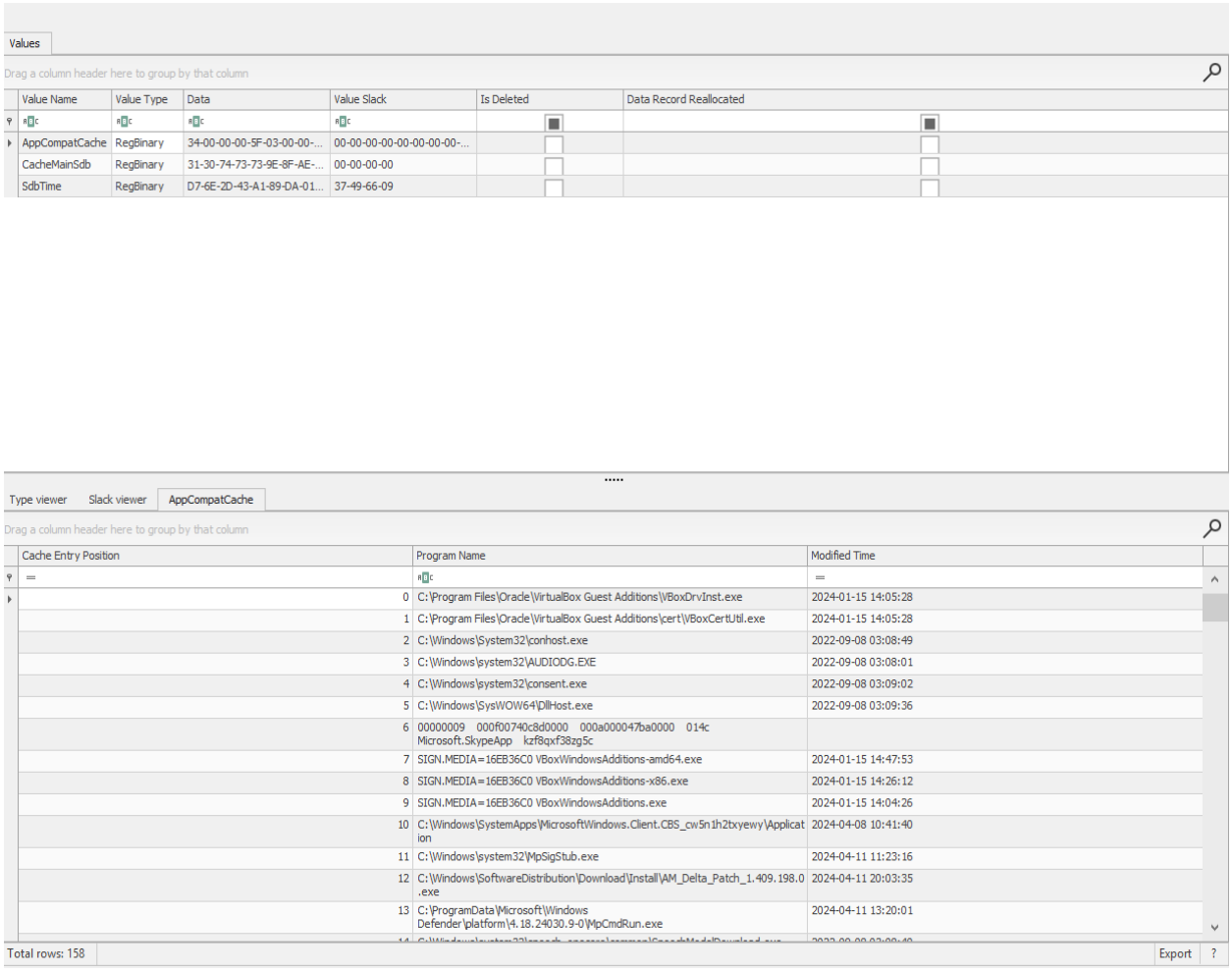
Drag a column header here to group by that column

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Opened
RecentDocs	1	The Internet	The Internet.lnk	0	2024-04-10 16:06:09	2024-04-10 16:06:09
RecentDocs	4	threat/	windowsdefender--threat-.lnk	1		
RecentDocs	0	network	ms-settingsnetwork.lnk	2		
RecentDocs	2	network-ethernet	ms-settingsnetwork-ethernet.lnk	3		
RecentDocs	3	kglcheck/	ms-gamingoverlay--kglcheck-.lnk	4		
Folder	0	The Internet	The Internet.lnk	0	2024-04-10 16:06:09	

Shellbags: Locations browsed by the user

Open / Save MRU: Files that were opened

Last-Visited MRU: Applications used to open files



Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
AppCompatCache	RegBinary	34-00-00-00-5F-03-00-00-...	00-00-00-00-00-00-00-00-...	☐	☐
CacheMainSdb	RegBinary	31-30-74-73-73-9E-8F-AE-...	00-00-00-00	☐	☐
SdbTime	RegBinary	D7-6E-2D-43-A1-89-DA-01...	37-49-66-09	☐	☐

Type viewer | Slack viewer | AppCompatCache

Drag a column header here to group by that column

Cache Entry Position	Program Name	Modified Time
0	C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxDrvInst.exe	2024-01-15 14:05:28
1	C:\Program Files\Oracle\VirtualBox Guest Additions\cert\VBoxCertUtil.exe	2024-01-15 14:05:28
2	C:\Windows\System32\conhost.exe	2022-09-08 03:08:49
3	C:\Windows\system32\AUDIODG.EXE	2022-09-08 03:08:01
4	C:\Windows\system32\consent.exe	2022-09-08 03:09:02
5	C:\Windows\SysWOW64\DllHost.exe	2022-09-08 03:09:36
6	00000009 000f00740c8d0000 000a000047ba0000 014c Microsoft.SkypeApp kzf8qxf38zg5c	
7	SIGN.MEDIA=16EB36C0 VBoxWindowsAdditions-amd64.exe	2024-01-15 14:47:53
8	SIGN.MEDIA=16EB36C0 VBoxWindowsAdditions-x86.exe	2024-01-15 14:26:12
9	SIGN.MEDIA=16EB36C0 VBoxWindowsAdditions.exe	2024-01-15 14:04:26
10	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\Application	2024-04-08 10:41:40
11	C:\Windows\system32\MpSigStub.exe	2024-04-11 11:23:16
12	C:\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.409.198.0.exe	2024-04-11 20:03:35
13	C:\ProgramData\Microsoft\Windows Defender\platform\4.18.24030.9-0\MpCmdRun.exe	2024-04-11 13:20:01

Total rows: 158 | Export | ?

Which accounts are Administrator group members?

Abdullah and art-test

NTFS - File System Analysis

Which files are in My Computer\CLSID_Desktop\PWF-main\PWF-main\AtomicRedTeam?

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
[current folder]				2024-04-10 21:13:06 PKT	2024-04-10 21:13:06 PKT	2024-04-10 21:13:27 PKT	2024-04-10 21:08:47 PKT	56	Allocated	Allocated
[parent folder]				2024-04-10 21:08:47 PKT	2024-04-10 21:08:47 PKT	2024-04-10 21:36:22 PKT	2019-12-07 14:03:44 PKT	56	Allocated	Allocated
atomics				2024-04-10 21:13:06 PKT	2024-04-10 21:13:06 PKT	2024-04-10 21:13:27 PKT	2024-04-10 21:13:03 PKT	56	Allocated	Allocated
invoke-atomicredteam				2024-04-10 21:08:54 PKT	2024-04-10 21:08:54 PKT	2024-04-10 21:14:26 PKT	2024-04-10 21:08:52 PKT	56	Allocated	Allocated

What is the MFT Entry Number for the file "ART-attack.ps1"?

Name	ART-attack.ps1
File Class	Regular File
File Size	3,360
Physical Size	4,096
Start Cluster	561,503
Date Accessed	10-Apr-24 4:08:45 PM
Date Created	10-Apr-24 4:02:33 PM
Date Modified	10-Apr-24 4:02:01 PM
Encrypted	False
Compressed	False
Actual File	True
Start Sector	4,596,472

What are the MACB timestamps for "ART-attack.ps1"?

Date Accessed	10-Apr-24 4:08:45 PM
Date Created	10-Apr-24 4:02:33 PM
Date Modified	10-Apr-24 4:02:01 PM

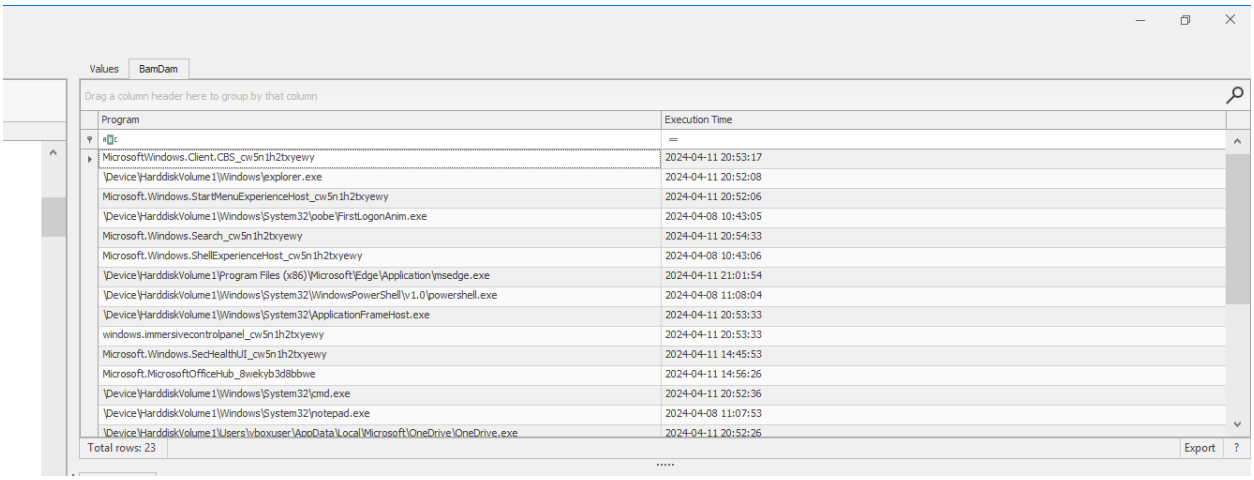
Was "ART-attack.ps1" timestomped?

Yes

NTFS Access Control Entry	
ACE Type	Allow Access
SID	S-1-5-21-239386965-2826860934-2307490478-100
Name	Abdullah
Access Mask	001f01ff
Execute File	True
Read Data	True
Write Data	True
Append Data	True
Delete	True
Read Permissions	True
Change Permissions	True
Take Ownership	True

Execution Artifacts Background Activity Moderator (BAM)

Registry:
HKLM\SYSTEM\CurrentControlSet\Services\bam\UserSettings



Values | BamDam

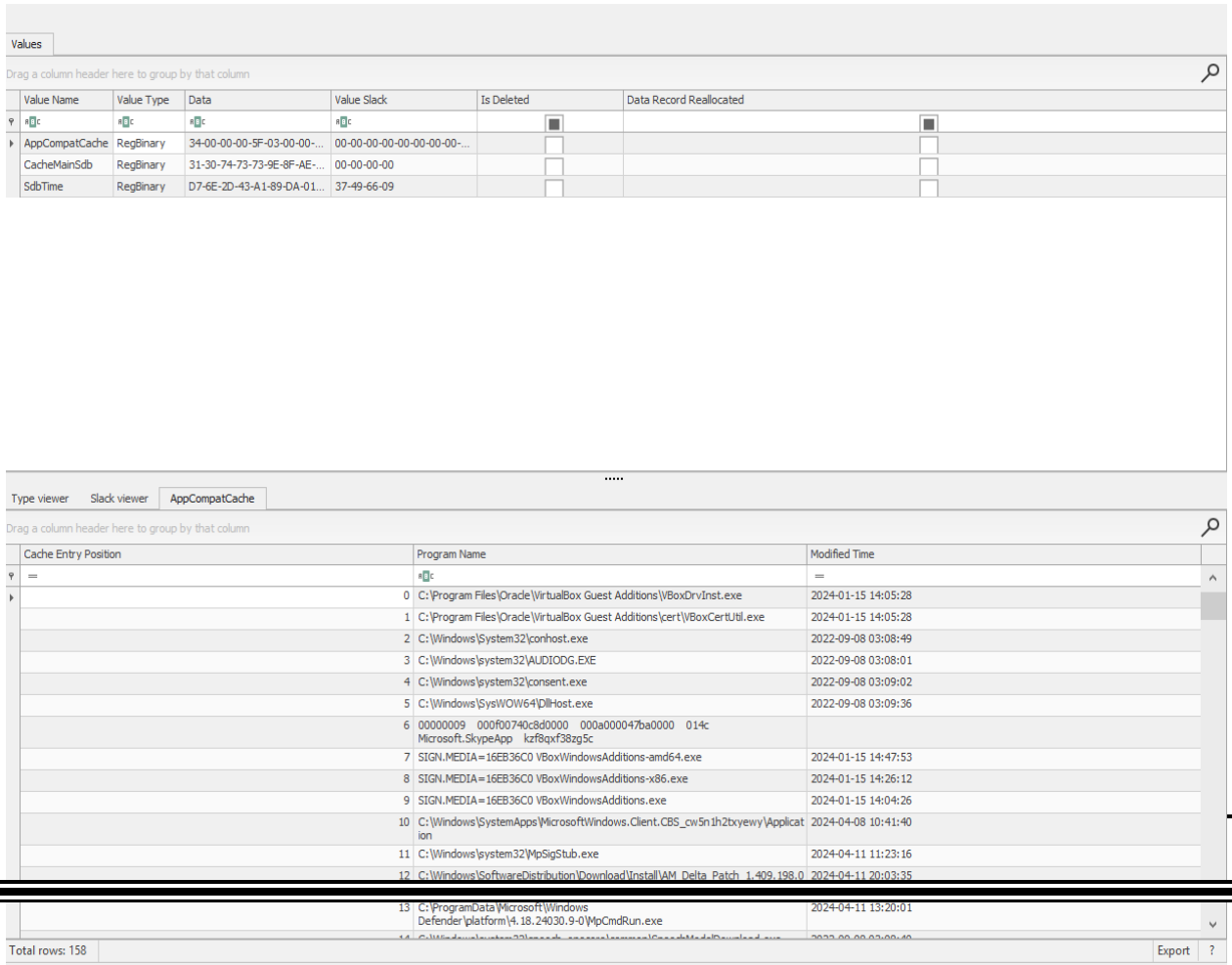
Drag a column header here to group by that column

Program	Execution Time
MicrosoftWindows.Client.CBS_cw5n1h2txyewy	2024-04-11 20:53:17
\Device\HarddiskVolume1\Windows\explorer.exe	2024-04-11 20:52:08
Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy	2024-04-11 20:52:06
\Device\HarddiskVolume1\Windows\System32\oobe\FirstLogonAnim.exe	2024-04-08 10:43:05
Microsoft.Windows.Search_cw5n1h2txyewy	2024-04-11 20:54:33
Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy	2024-04-08 10:43:06
\Device\HarddiskVolume1\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	2024-04-11 21:01:54
\Device\HarddiskVolume1\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	2024-04-08 11:08:04
\Device\HarddiskVolume1\Windows\System32\ApplicationFrameHost.exe	2024-04-11 20:53:33
windows.immersivecontrolpanel_cw5n1h2txyewy	2024-04-11 20:53:33
Microsoft.Windows.SecHealthUI_cw5n1h2txyewy	2024-04-11 14:45:53
Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe	2024-04-11 14:56:26
\Device\HarddiskVolume1\Windows\System32\cmd.exe	2024-04-11 20:52:36
\Device\HarddiskVolume1\Windows\System32\notepad.exe	2024-04-08 11:07:53
\Device\HarddiskVolume1\Users\vboxuser\AppData\Local\Microsoft\OneDrive\OneDrive.exe	2024-04-11 20:52:26

Total rows: 23 | Export | ?

Application Compatibility Cache ("AppCompatCache") / Shimcache

Registry: SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache



Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
AppCompatCache	RegBinary	34-00-00-00-5F-03-00-00-...	00-00-00-00-00-00-00-00-...	☐	☐
CacheMainSdb	RegBinary	31-30-74-73-73-9E-8F-AE-...	00-00-00-00	☐	☐
SdbTime	RegBinary	D7-6E-2D-43-A1-89-DA-01...	37-49-66-09	☐	☐

Type viewer | Slack viewer | AppCompatCache

Drag a column header here to group by that column

Cache Entry Position	Program Name	Modified Time
0	C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxDrvInst.exe	2024-01-15 14:05:28
1	C:\Program Files\Oracle\VirtualBox Guest Additions\cert\VBoxCertUtil.exe	2024-01-15 14:05:28
2	C:\Windows\System32\conhost.exe	2022-09-08 03:08:49
3	C:\Windows\system32\AUDIODG.EXE	2022-09-08 03:08:01
4	C:\Windows\system32\consent.exe	2022-09-08 03:09:02
5	C:\Windows\SysWOW64\DllHost.exe	2022-09-08 03:09:36
6	00000009 000f00740c8d0000 000a000047ba0000 014c Microsoft.SkypeApp kzf8qxf38zg5c	
7	SIGN.MEDIA=16EB36C0 VBoxWindowsAdditions-amd64.exe	2024-01-15 14:47:53
8	SIGN.MEDIA=16EB36C0 VBoxWindowsAdditions-x86.exe	2024-01-15 14:26:12
9	SIGN.MEDIA=16EB36C0 VBoxWindowsAdditions.exe	2024-01-15 14:04:26
10	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\Application	2024-04-08 10:41:40
11	C:\Windows\system32\MpSigStub.exe	2024-04-11 11:23:16
12	C:\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.409.198.0	2024-04-11 20:03:35
13	C:\ProgramData\Microsoft\Windows Defender\platform\4.18.24030.9-0\MpCmdRun.exe	2024-04-11 13:20:01

Total rows: 158 | Export | ?

Startup Folder

Paths: