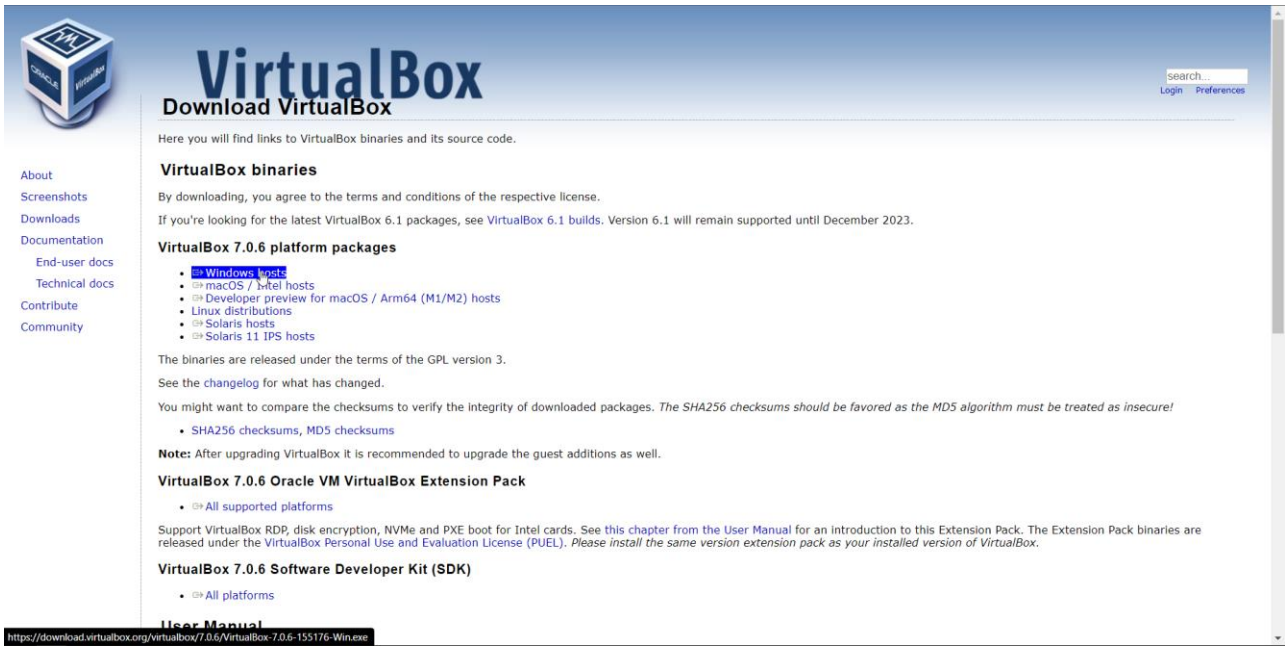
Setup Instructions:

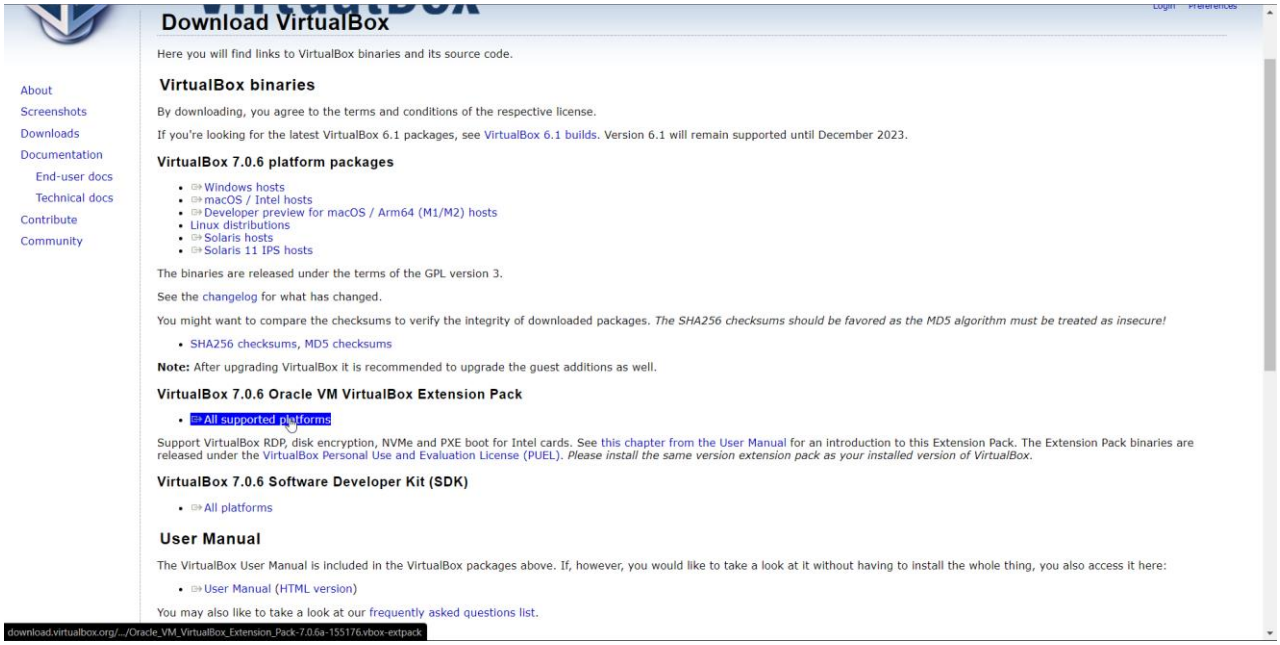
- Installing VirtualBox.
- Installing Windows Server 2019.
- Adding WSL feature for Windows and installing Ubuntu subsystem.
- Configuration for Forensics virtual machine.
- Installing Forensic Tools.

Installing VirtualBox

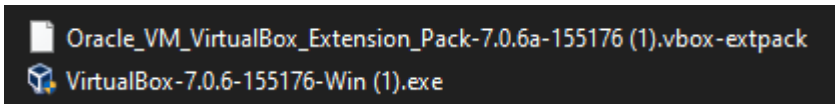
- Link: https://www.virtualbox.org/wiki/Downloads
- Downloading VirtualBox 7.0.6:



- Downloading VirtualBox 7.0.6 Extension Pack:



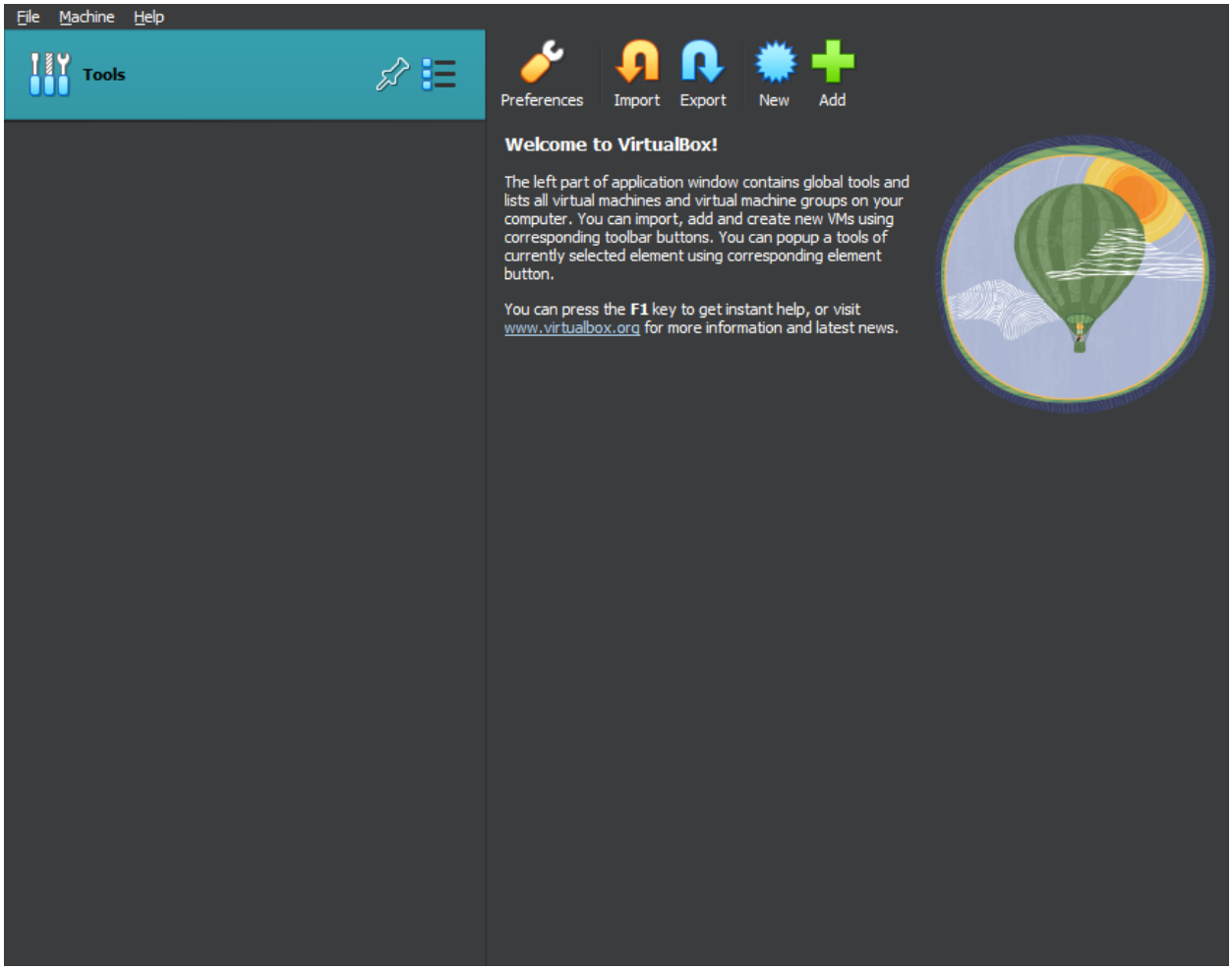
- You will have two files:



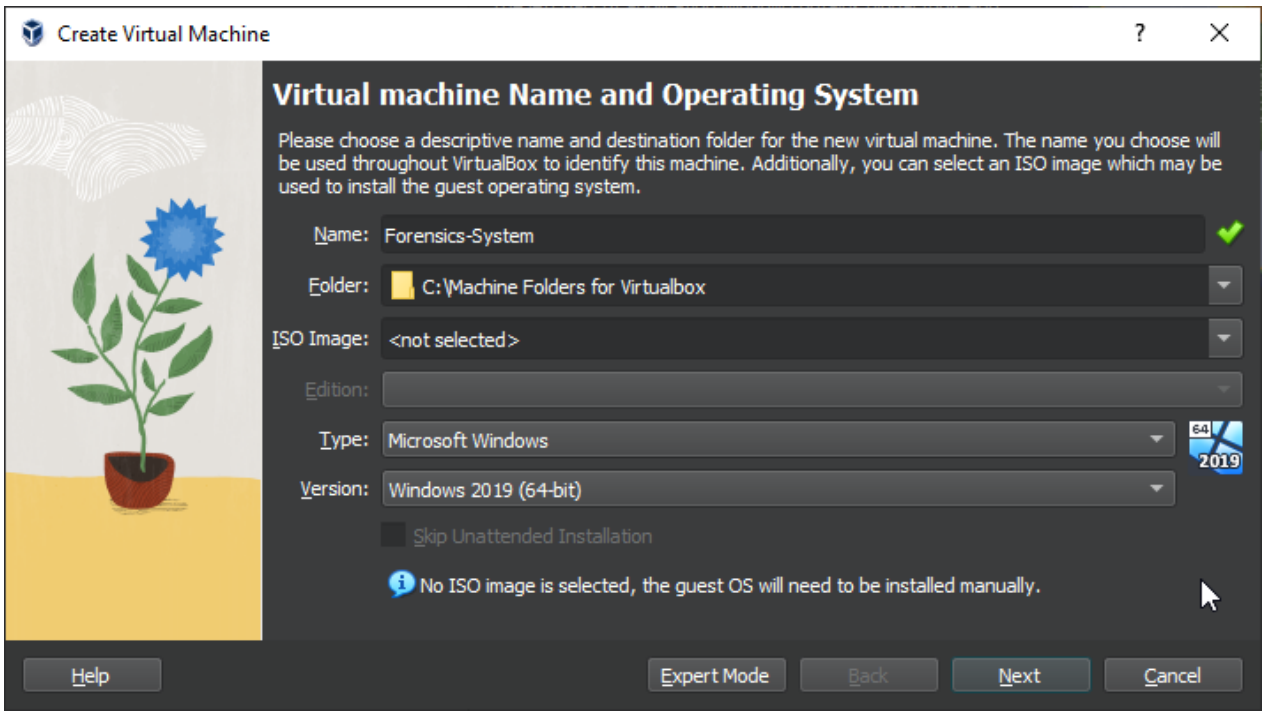
- First install VirtualBox, then import the extension pack for it. There is no need for advanced configuration at installation, just hit next until finish. Now, the system will recognize the extension pack, install it.
- When the extension pack is finished installing, I have used the following folder structure:
    - C:\
        - Machine Folders for VirtualBox.
        - Shared Folders (with the Virtual Machines).
        - VMs (Files for Virtual Machines: .vhd, .ova).

Installing Windows Server 2019

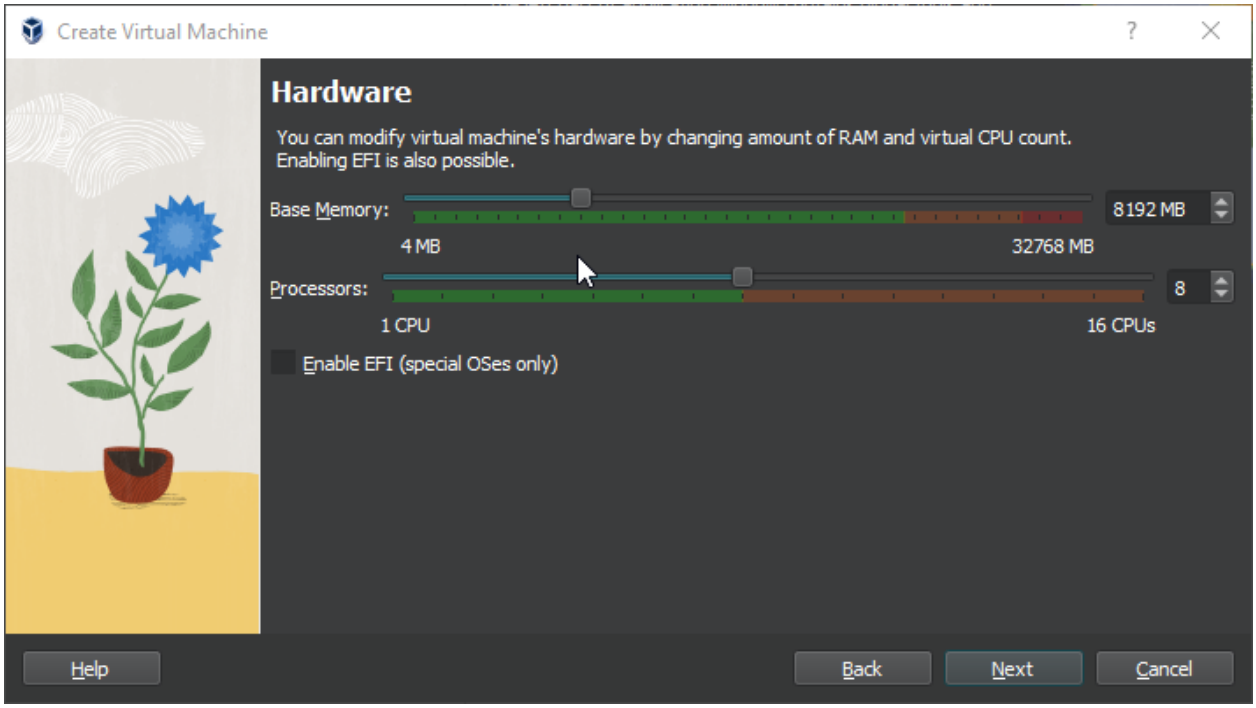
- Link: https://go.microsoft.com/fwlink/p/?linkid=2195334



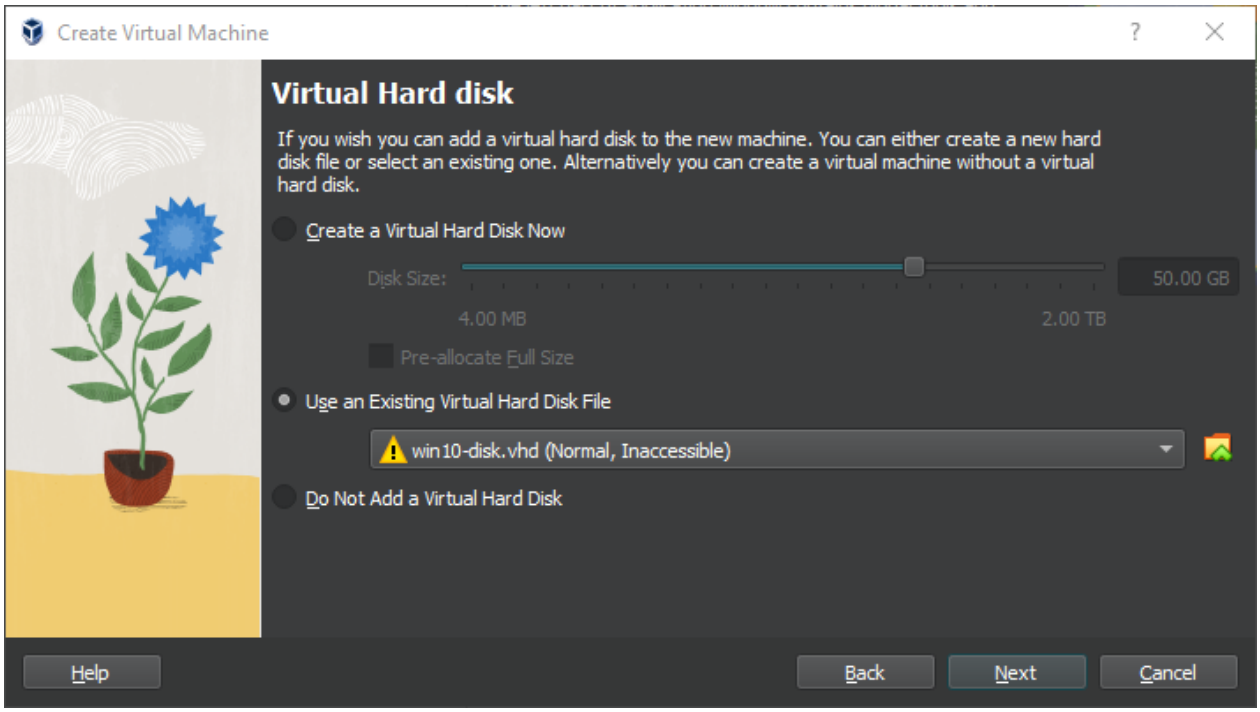
- Press New.

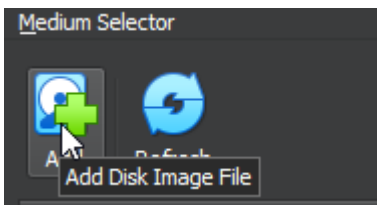


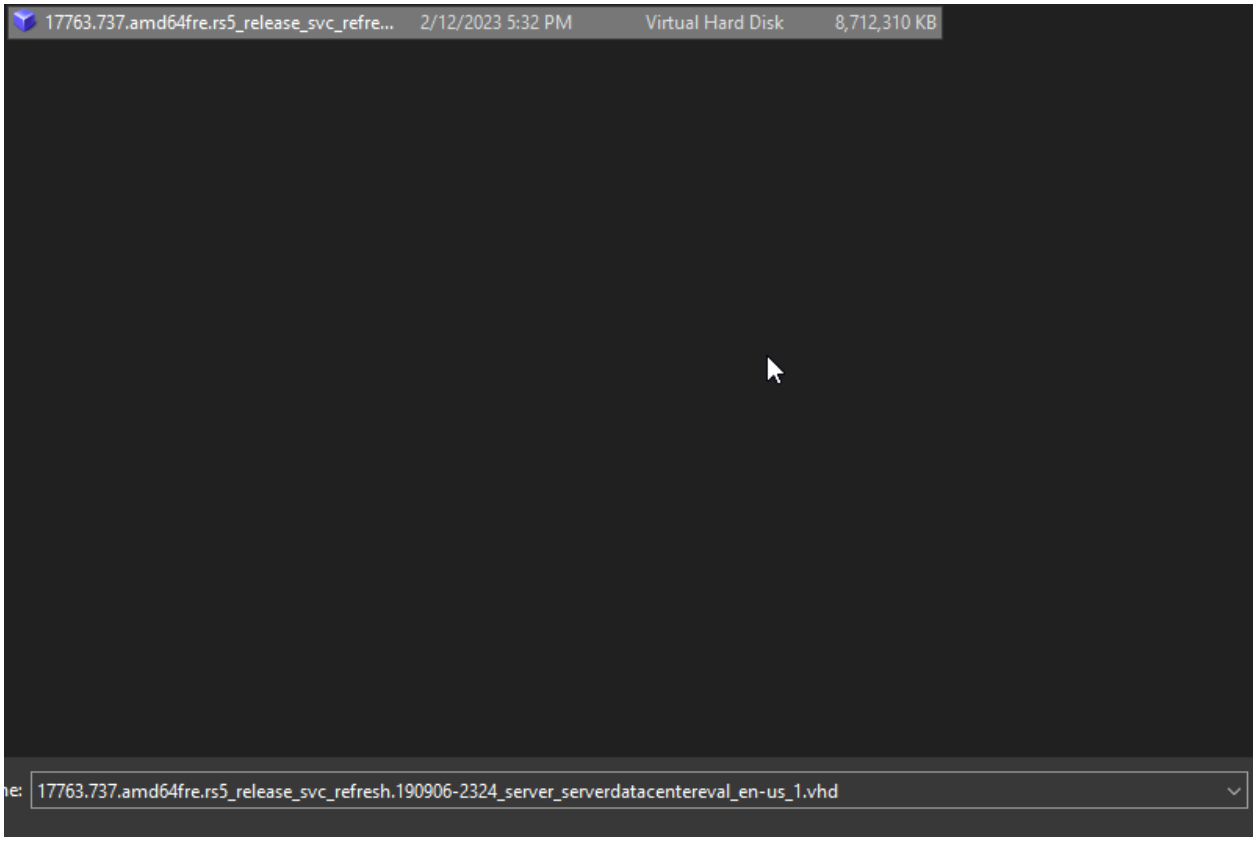
- You can allocate how much resources you want.

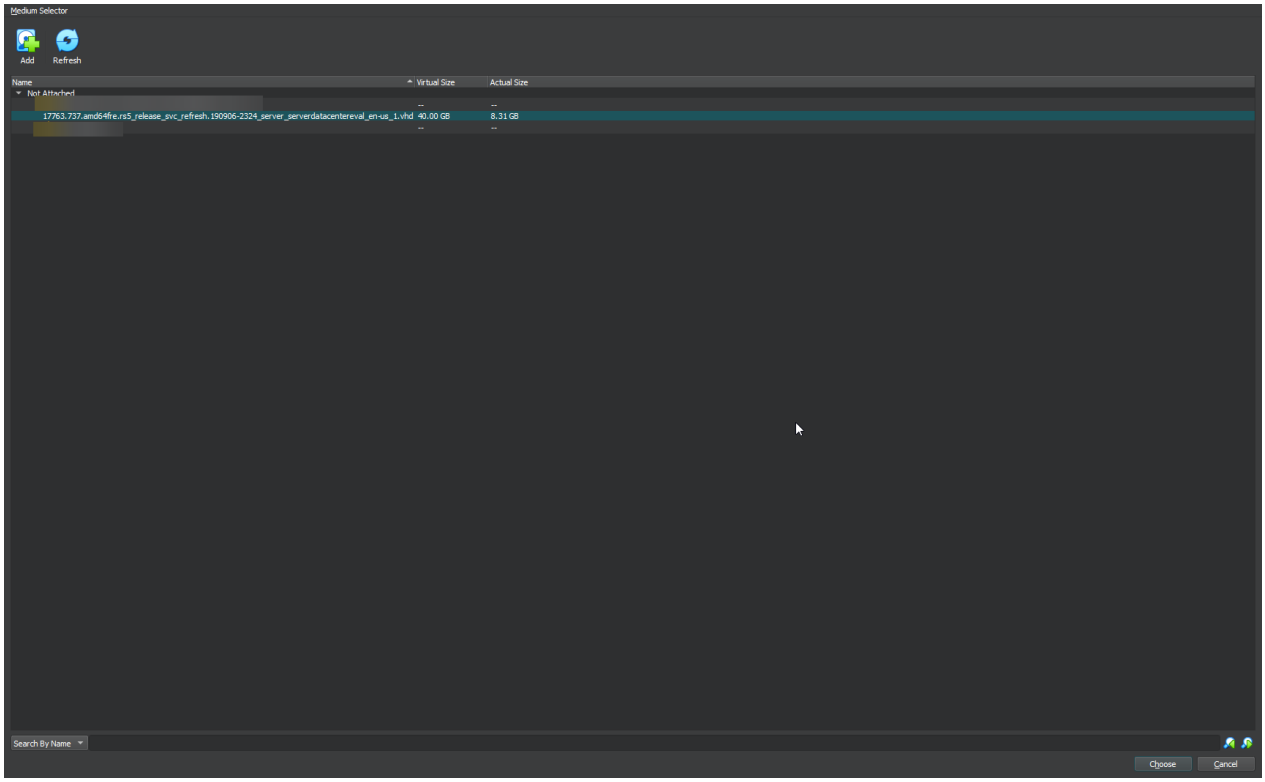


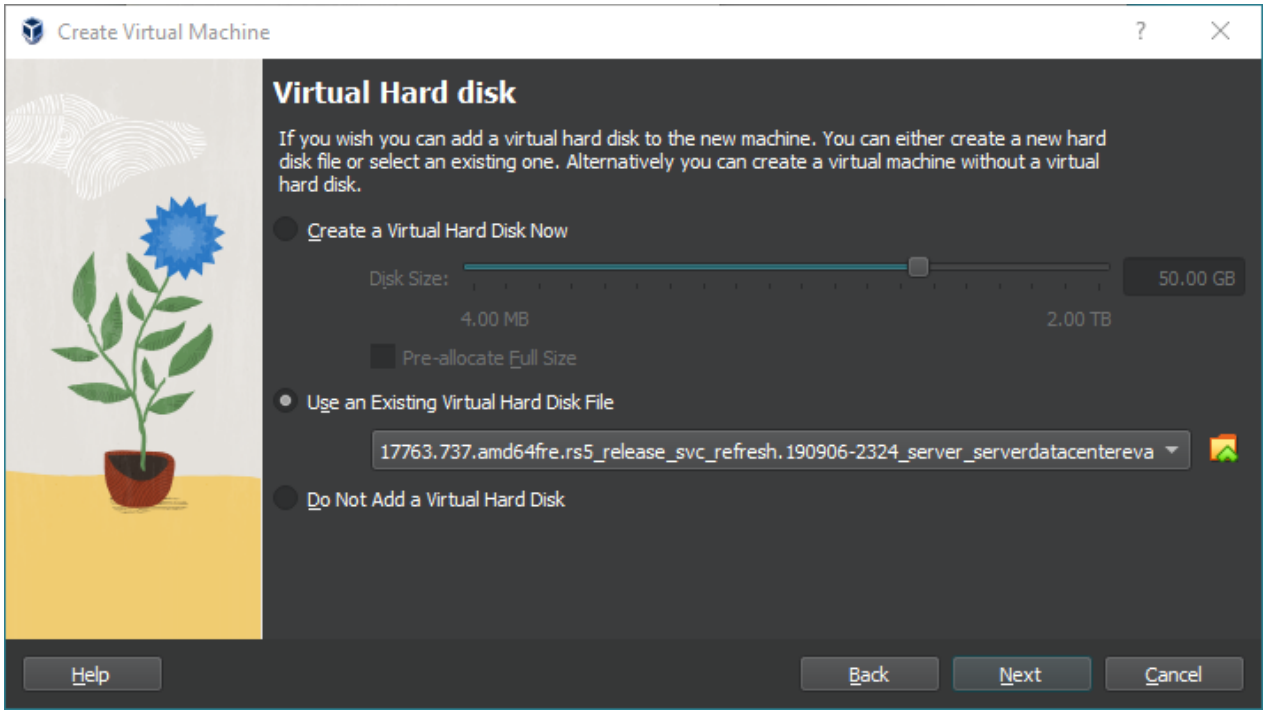
- In this case, we will choose an existing virtual hard disk file (.vhd) we downloaded earlier.

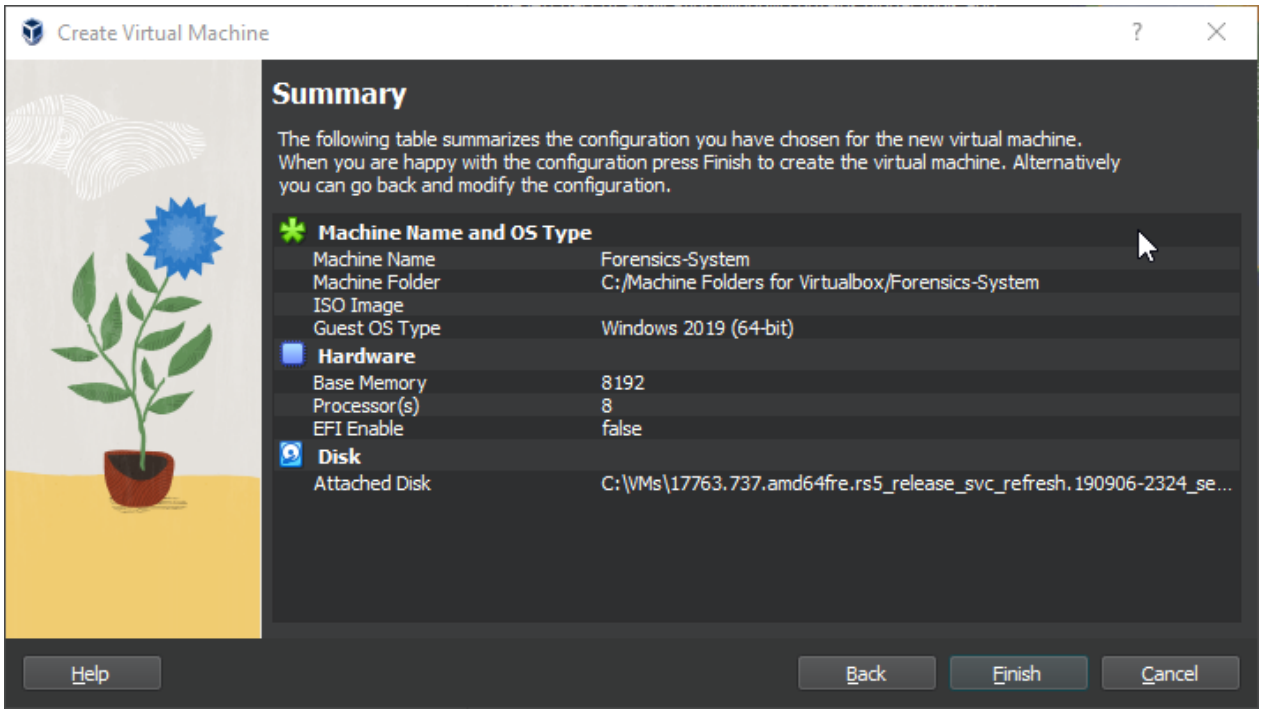


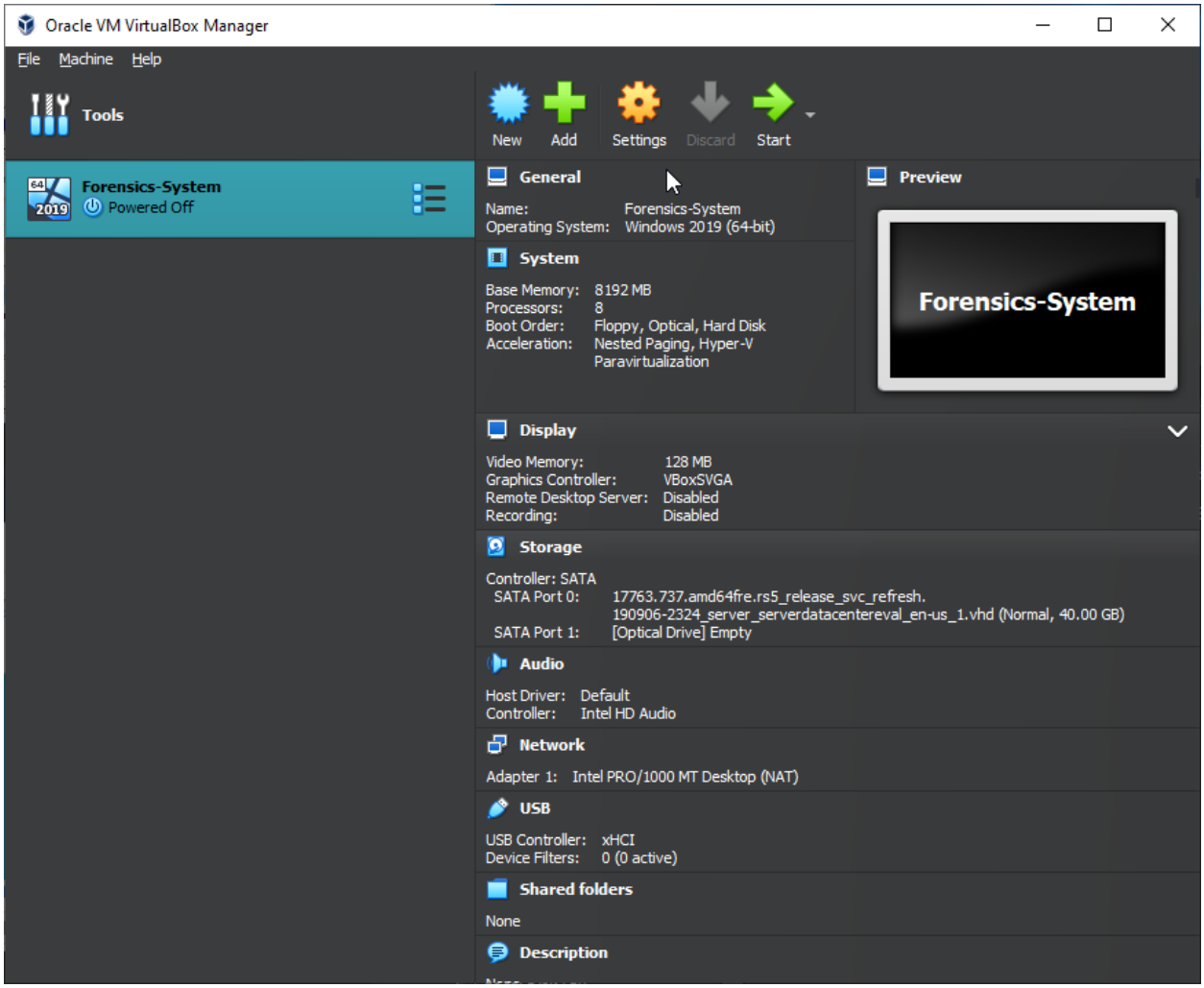



17763.737.amd64fre.rs5_release_svc_refre... 2/12/2023 5:32 PM Virtual Hard Disk 8,712,310 KB
17763.737.amd64fre.rs5_release_svc_refresh.190906-2324_server_serverdatacentereval_en-us_1.vhd

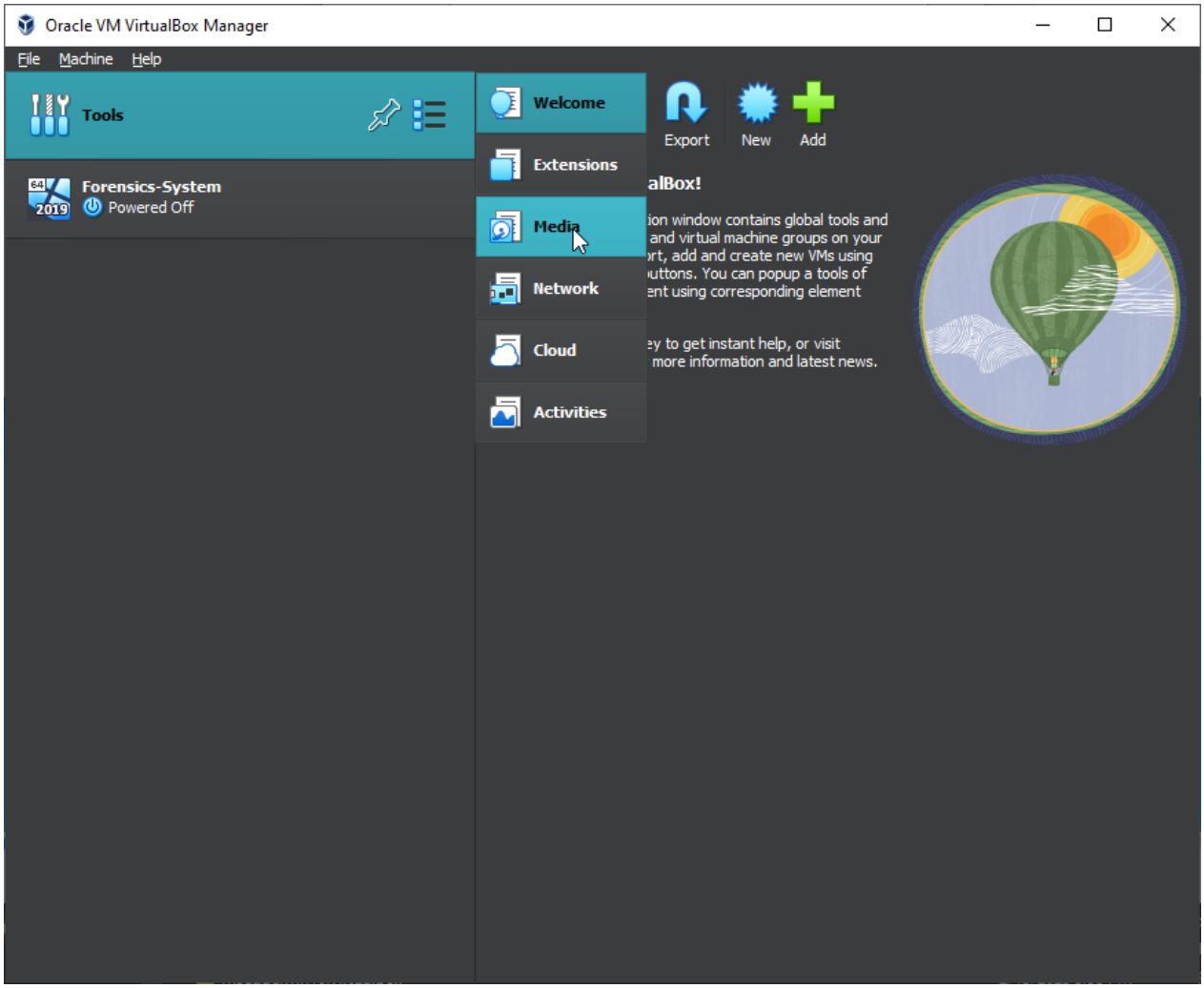

Medium Selector
Add
Refresh
Name
Virtual Size
Actual Size
Not Attached
17763.737.amd64fre.rs5_release_svc_refresh.190906-2324_server_serverdatacentereval_en-us_1.vhd
40.00 GB
8.31 GB
Search By Name
Choose
Cancel

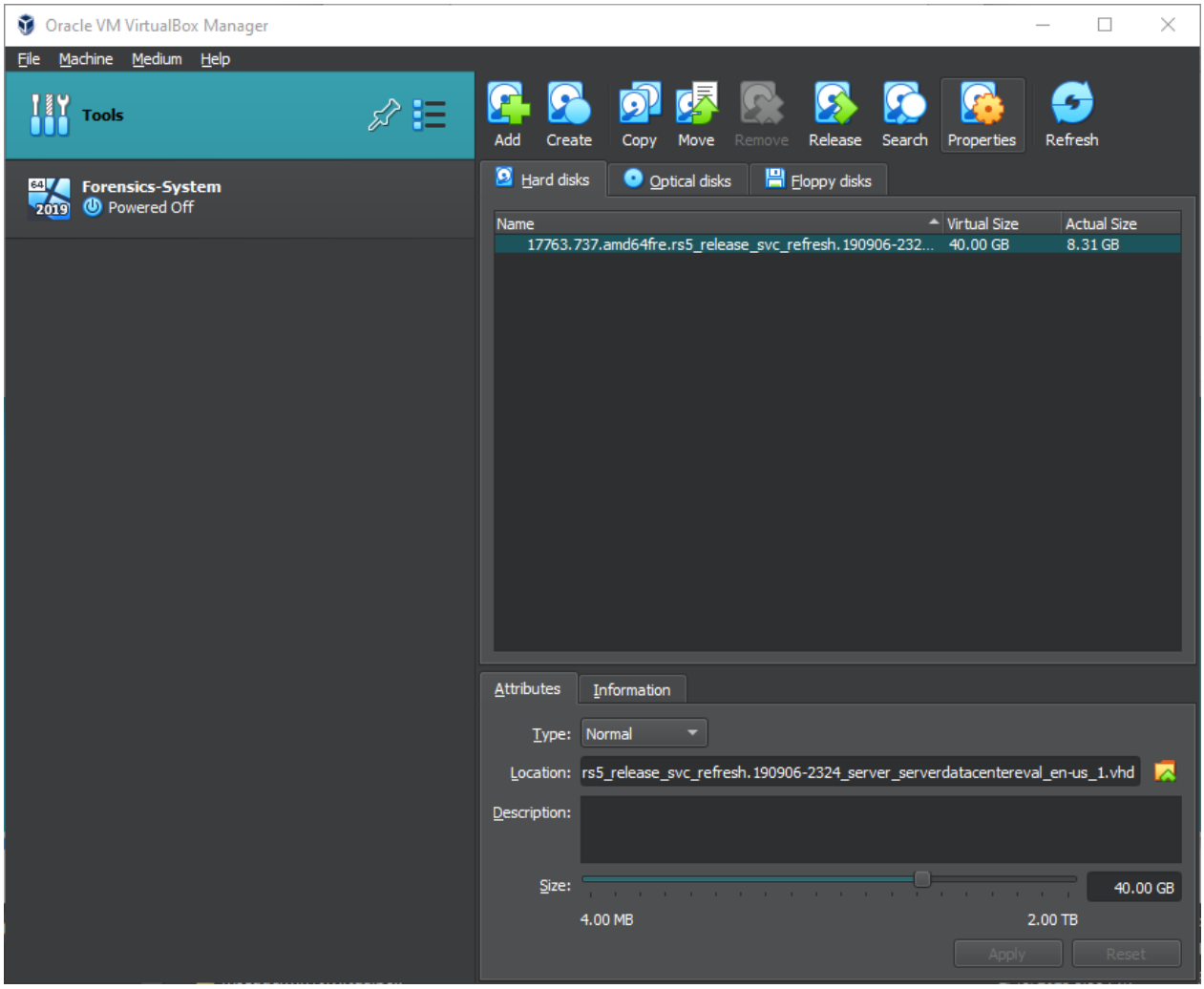

Create Virtual Machine
Virtual Hard disk
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.
Create a Virtual Hard Disk Now
Disk Size:
50.00 GB
4.00 MB
2.00 TB
Pre-allocate Full Size
Use an Existing Virtual Hard Disk File
17763.737.amd64fre.rs5_release_svc_refresh.190906-2324_server_serverdatacentereva
Do Not Add a Virtual Hard Disk
Help
Back
Next
Cancel


Create Virtual Machine
Summary
The following table summarizes the configuration you have chosen for the new virtual machine. When you are happy with the configuration press Finish to create the virtual machine. Alternatively you can go back and modify the configuration.
Machine Name and OS Type
Machine Name Forensics-System
Machine Folder C:/Machine Folders for Virtualbox/Forensics-System
ISO Image
Guest OS Type Windows 2019 (64-bit)
Hardware
Base Memory 8192
Processor(s) 8
EFI Enable false
Disk
Attached Disk C:\VMs\17763.737.amd64fre.rs5_release_svc_refresh.190906-2324_se...
Help
Back
Finish
Cancel

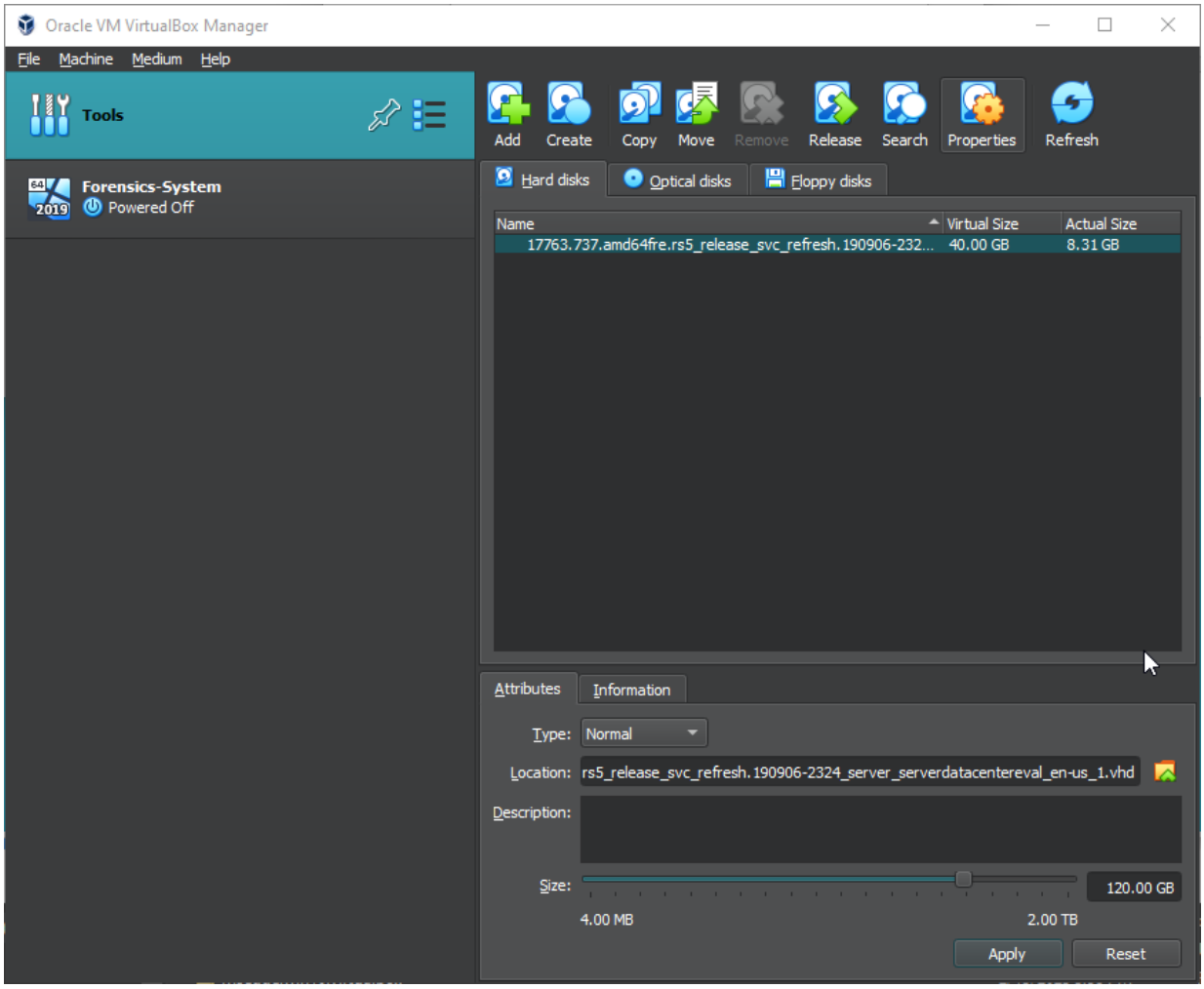


- Now, very important task. Go to Media:

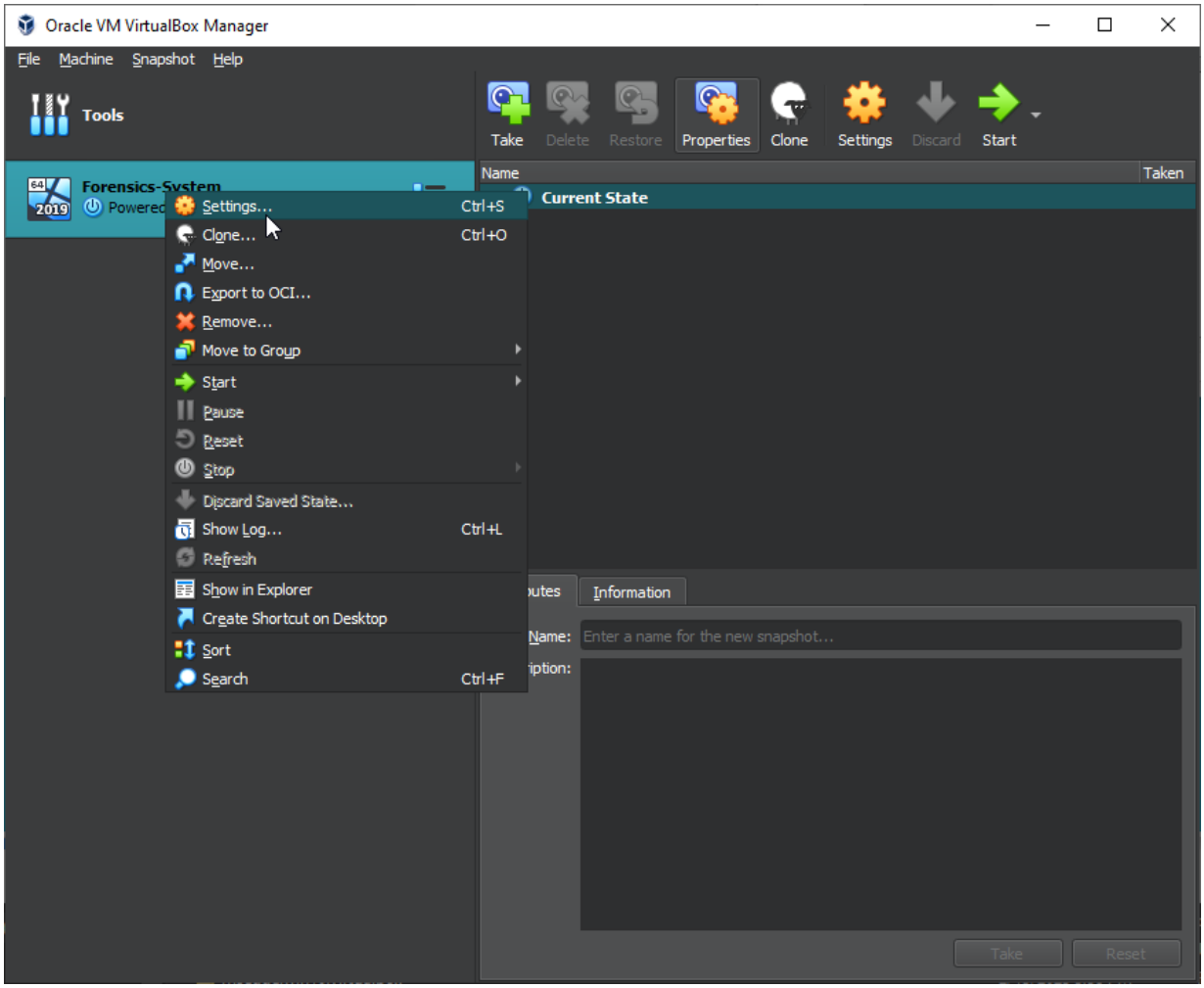

Oracle VM VirtualBox Manager
File
Machine
Help
Tools
Forensics-System
Powered Off
Welcome
Extensions
Media
Network
Cloud
Activities
Export
New
Add
alBox!
ion window contains global tools and
and virtual machine groups on your
rt, add and create new VMs using
uttons. You can popup a tools of
ent using corresponding element
ey to get instant help, or visit
more information and latest news.



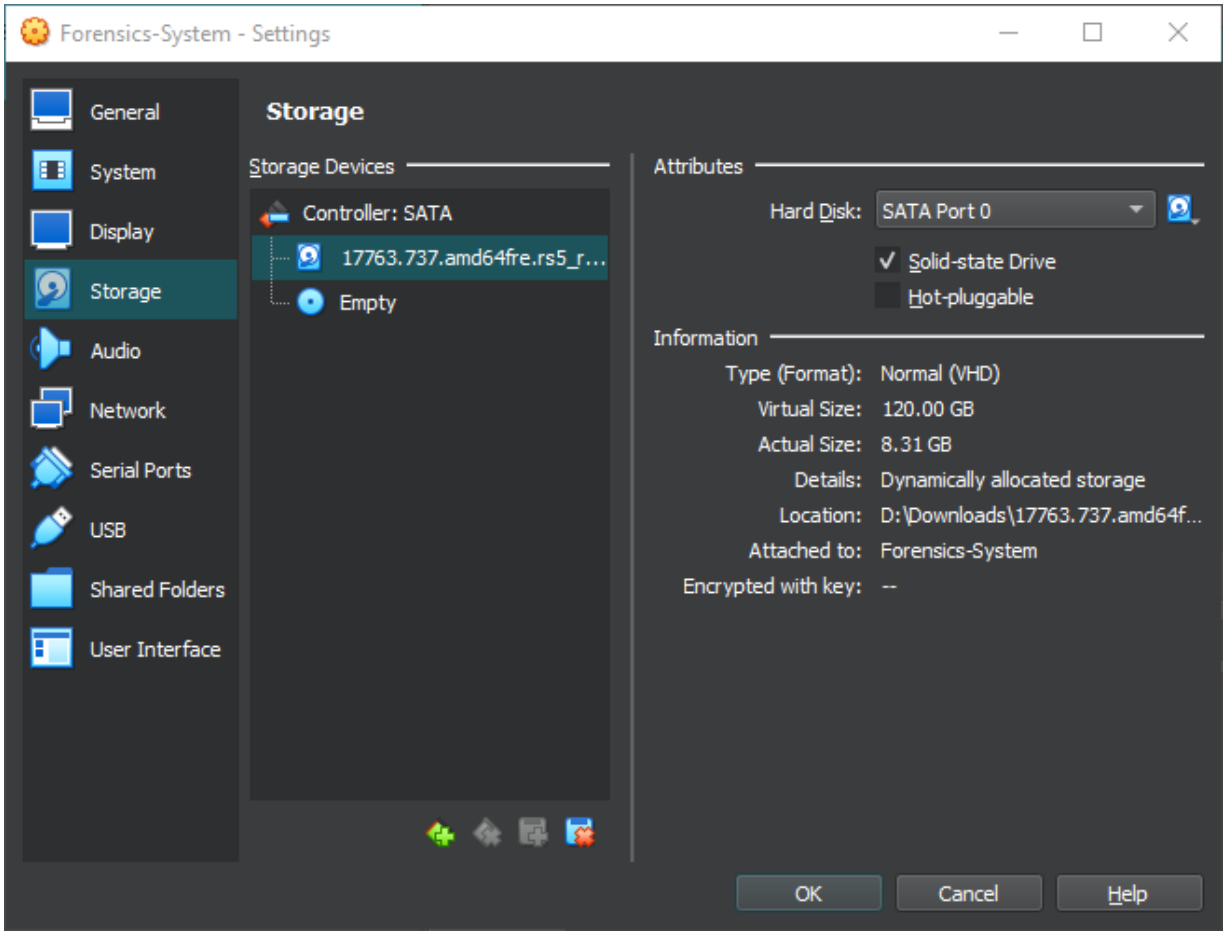
- Change the size of the disk: (Caution!!!: You cannot shrink the virtual disk, make sure you increase the size with what resources you have | You cannot increase the size of a virtual disk for a virtual machine that you have snapshots of).



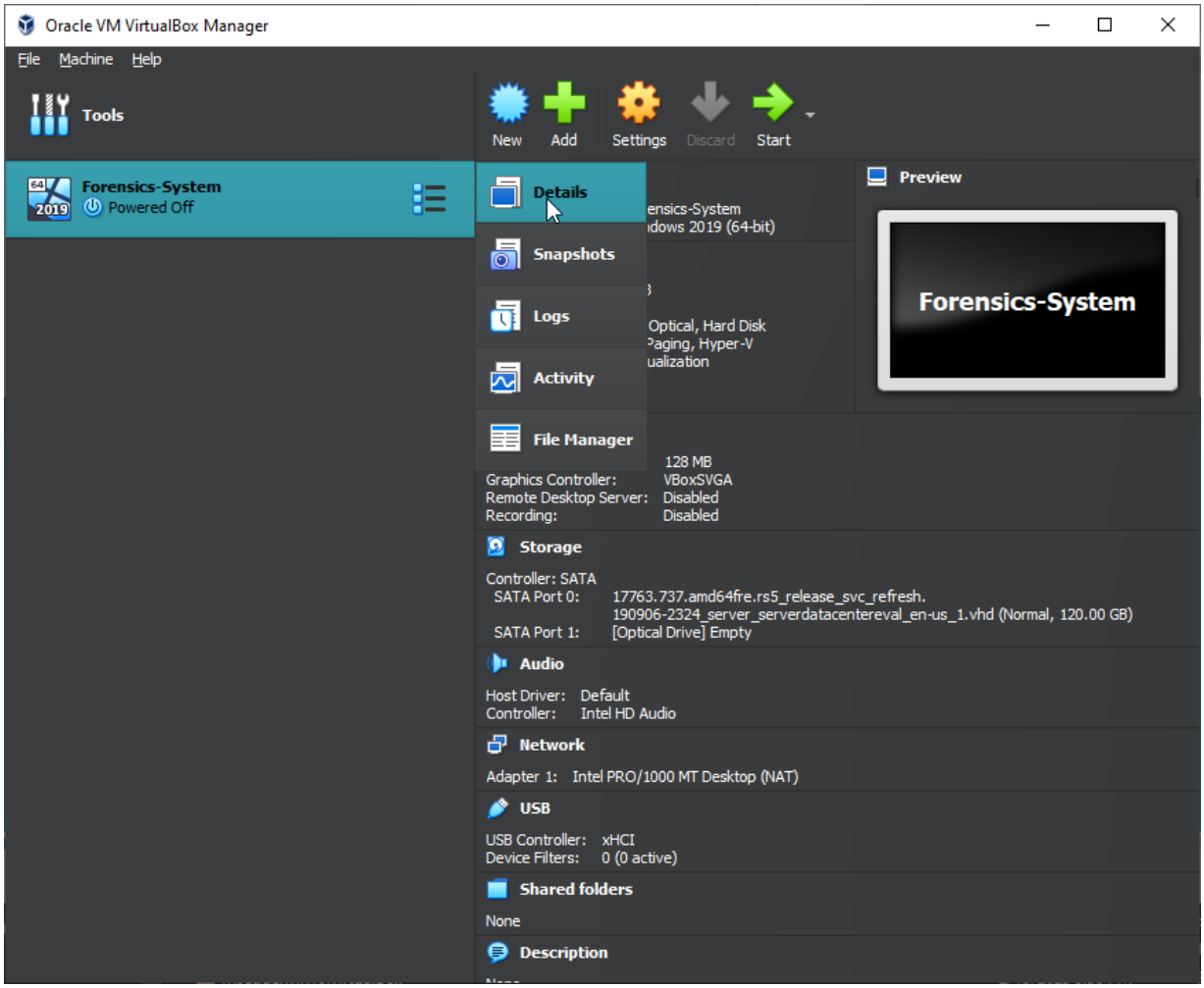
- Press Apply.
- Some performance tweaks:

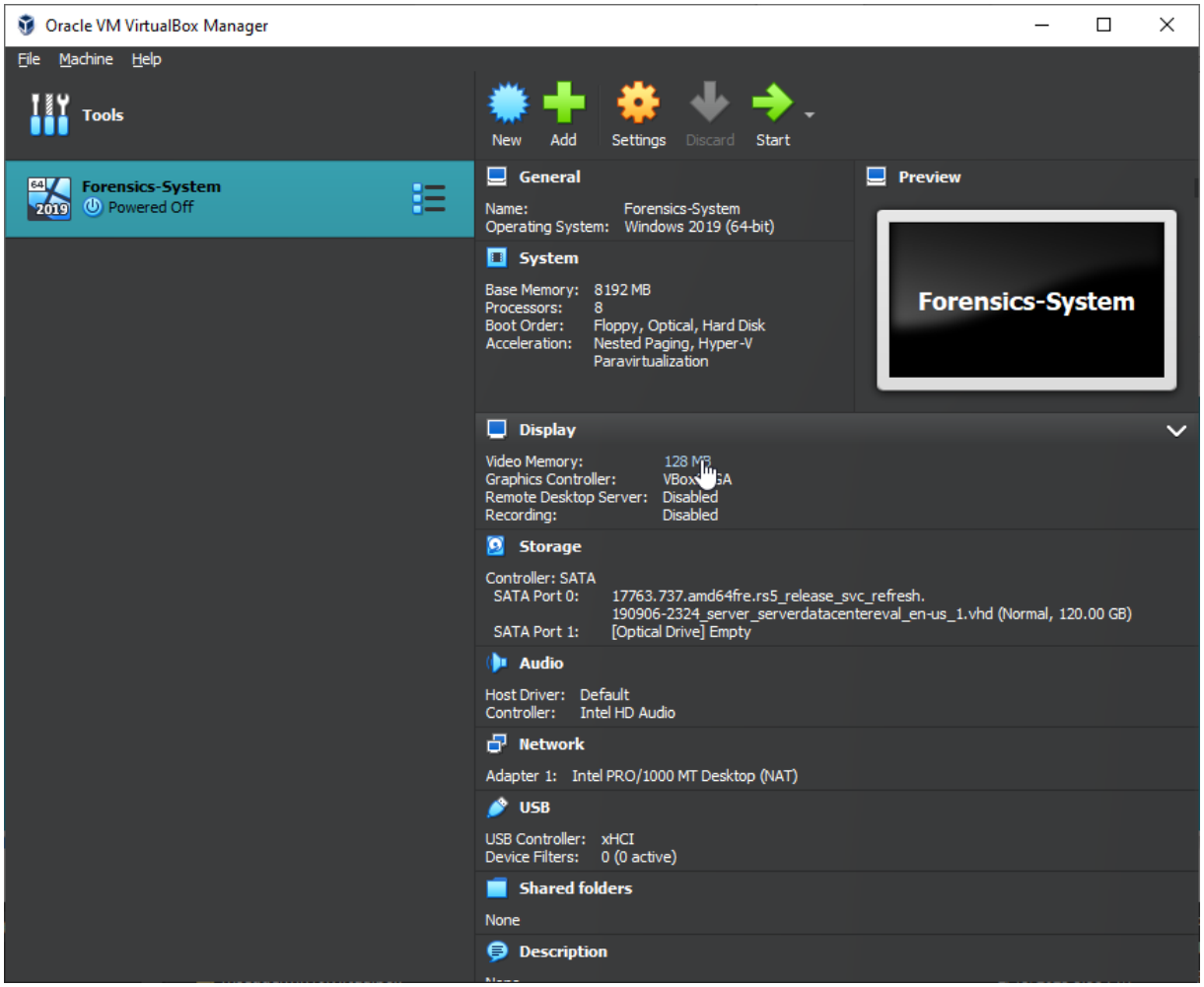


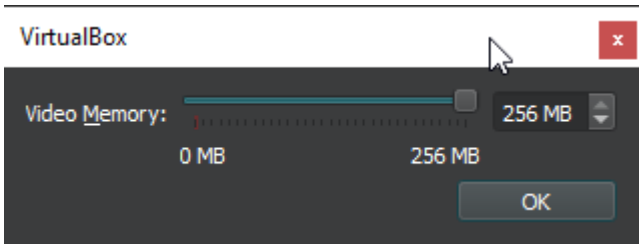
- I have the virtual machines disks on SSD, you can check the Solid-state Drive box for improving performance of the virtual machine.



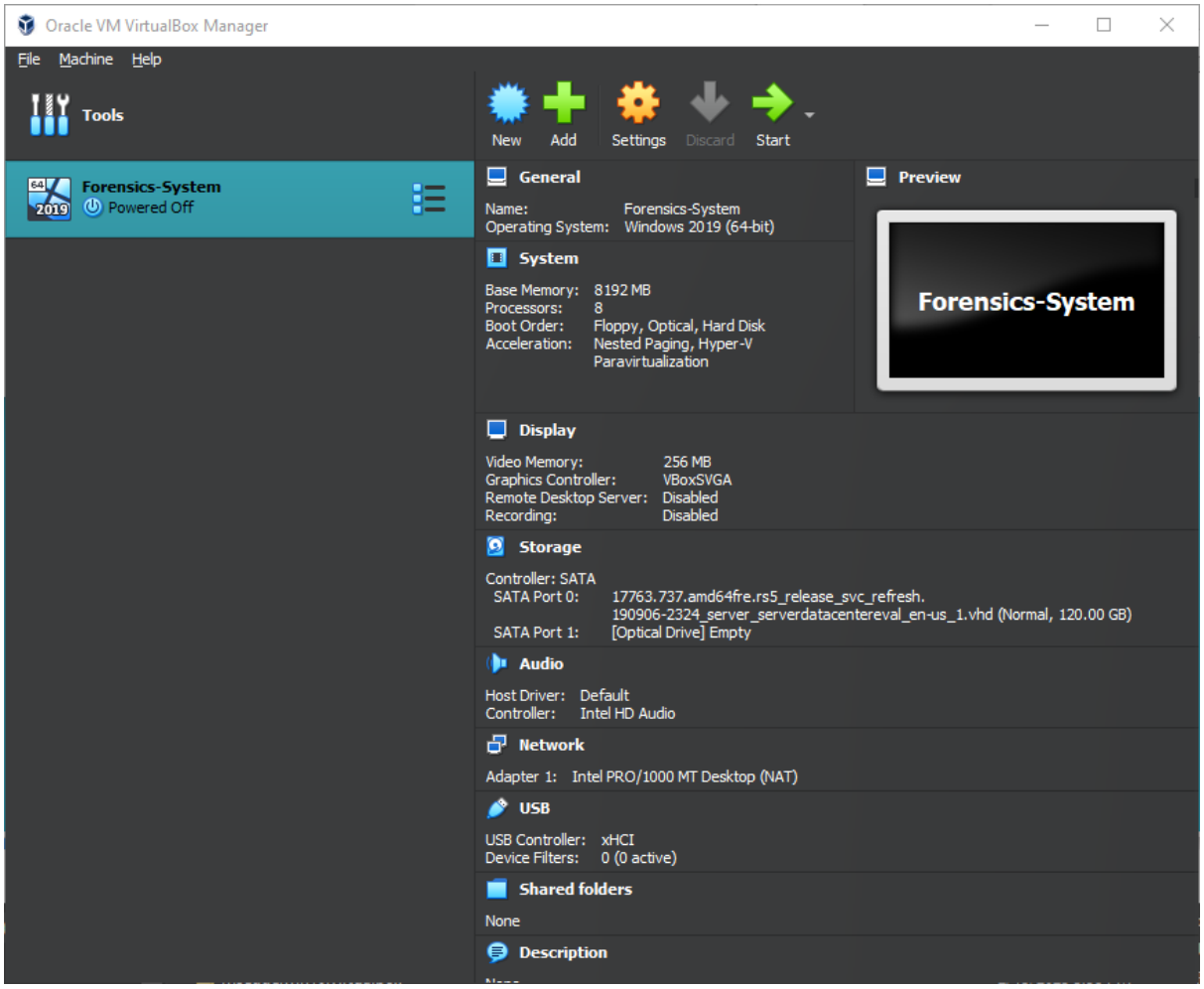
- Go to Details and increase video memory:


Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Add
Settings
Discard
Start
Forensics-System
Powered Off
Details
Snapshots
Logs
Activity
File Manager
Preview
Forensics-System
Optical, Hard Disk
Paging, Hyper-V
ualization
128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: SATA
SATA Port 0: 17763.737.amd64fre.rs5_release_svc_refresh.
190906-2324_server_serverdatacentereval_en-us_1.vhd (Normal, 120.00 GB)
SATA Port 1: [Optical Drive] Empty
Audio
Host Driver: Default
Controller: Intel HD Audio
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)
USB
USB Controller: xHCI
Device Filters: 0 (0 active)
Shared folders
None
Description

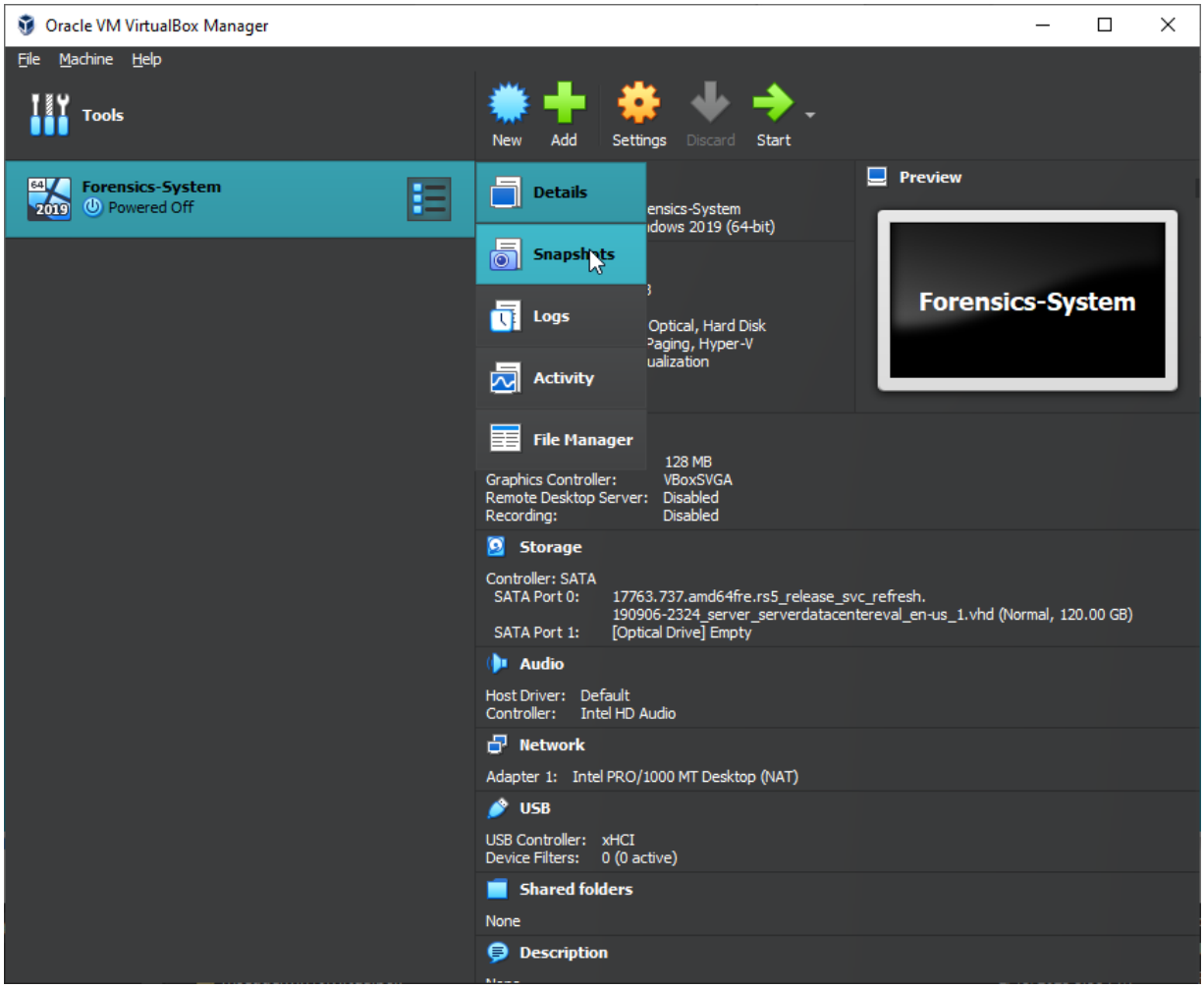


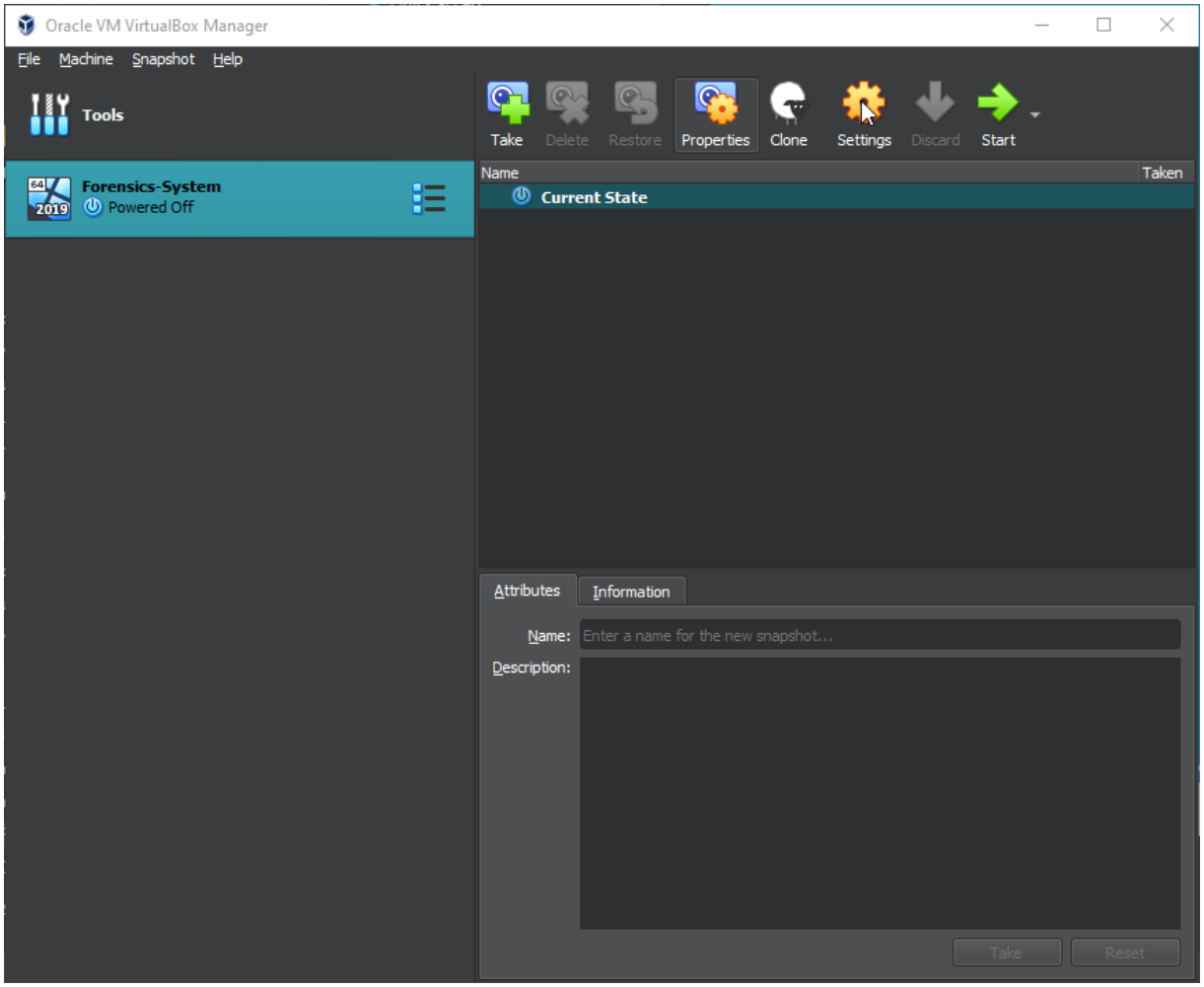


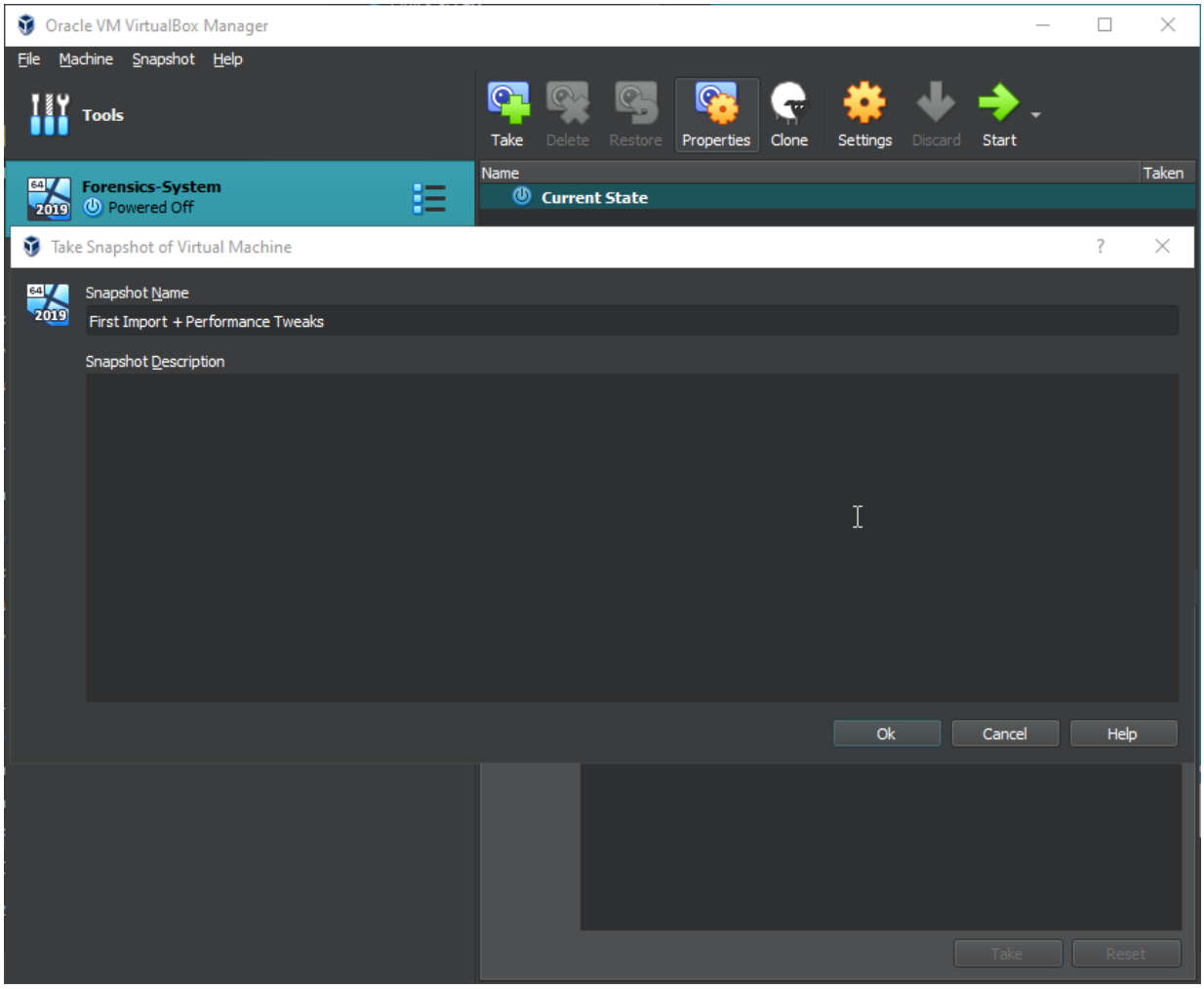
- This is the final form of the virtual machine, ready to take a snapshot.



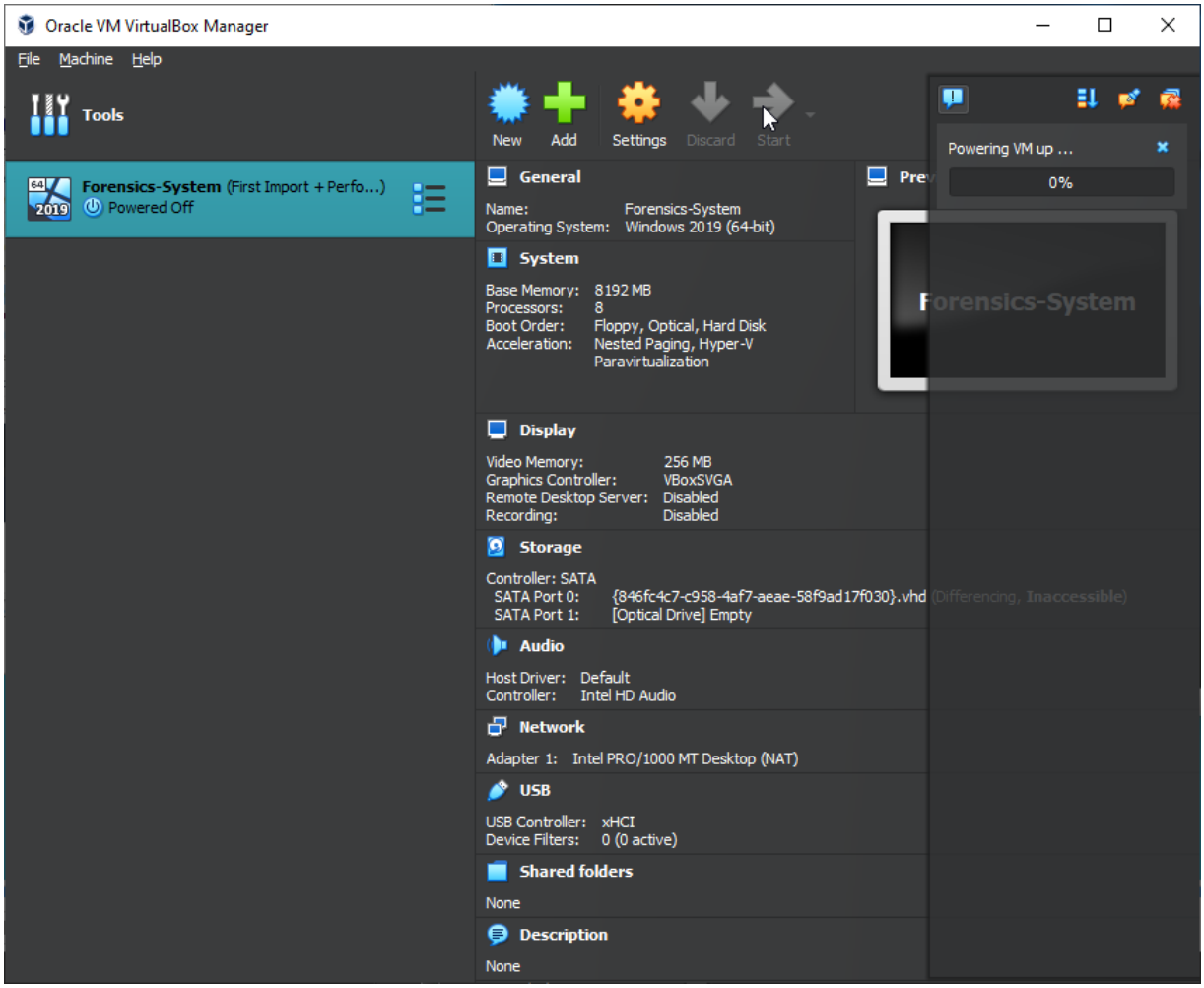
- Now go back and go to Snapshots and take a snapshot.

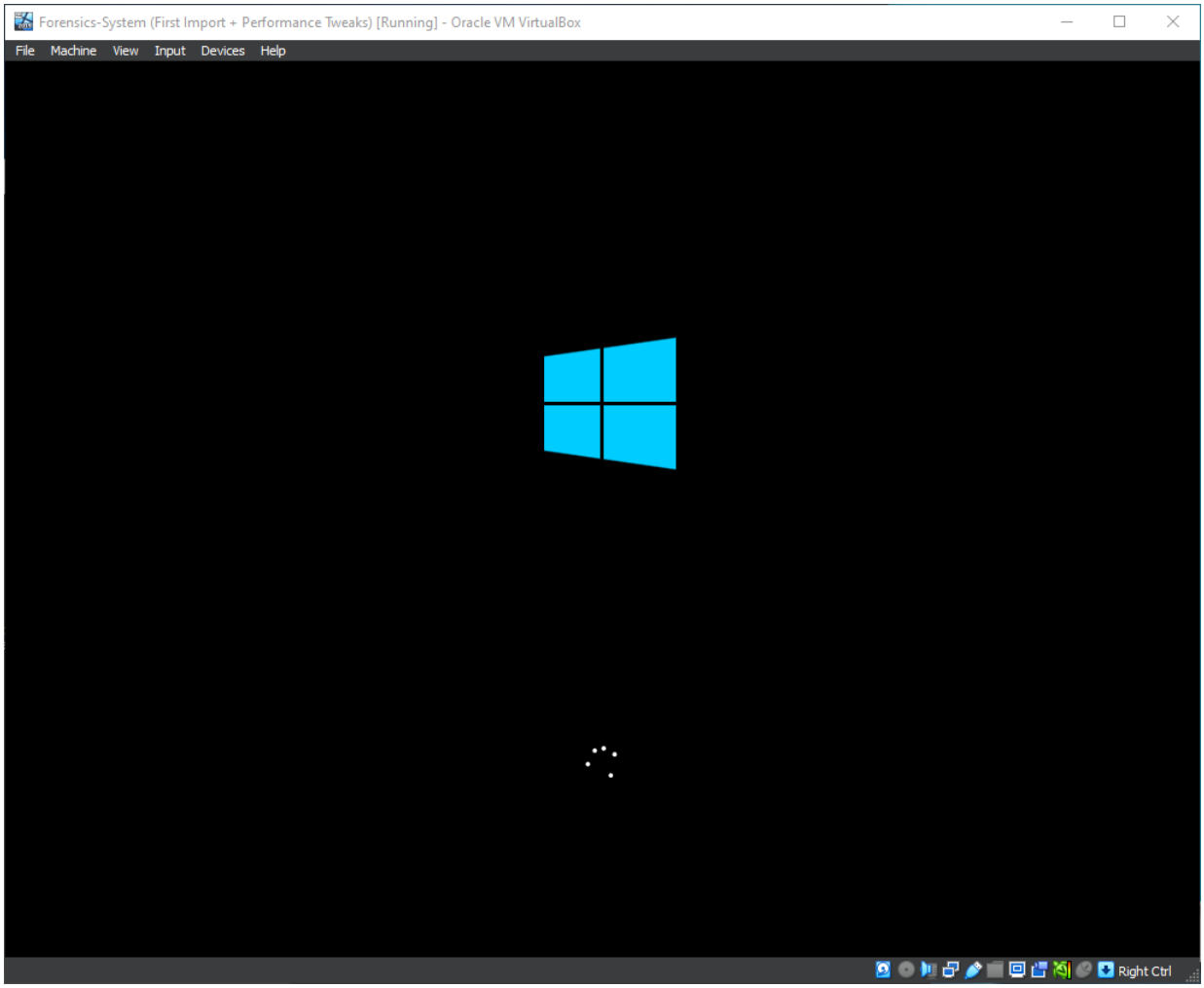

Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Add
Settings
Discard
Start
Forensics-System
Powered Off
Details
Snapshots
Logs
Activity
File Manager
Preview
Forensics-System
Optical, Hard Disk
Paging, Hyper-V
ualization
128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: SATA
SATA Port 0: 17763.737.amd64fre.rs5_release_svc_refresh.
190906-2324_server_serverdatacentereval_en-us_1.vhd (Normal, 120.00 GB)
SATA Port 1: [Optical Drive] Empty
Audio
Host Driver: Default
Controller: Intel HD Audio
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)
USB
USB Controller: xHCI
Device Filters: 0 (0 active)
Shared folders
None
Description


Oracle VM VirtualBox Manager
File
Machine
Snapshot
Help
Tools
Forensics-System
Powered Off
Take
Delete
Restore
Properties
Clone
Settings
Discard
Start
Name
Taken
Current State
Attributes
Information
Name:
Enter a name for the new snapshot...
Description:
Take
Reset

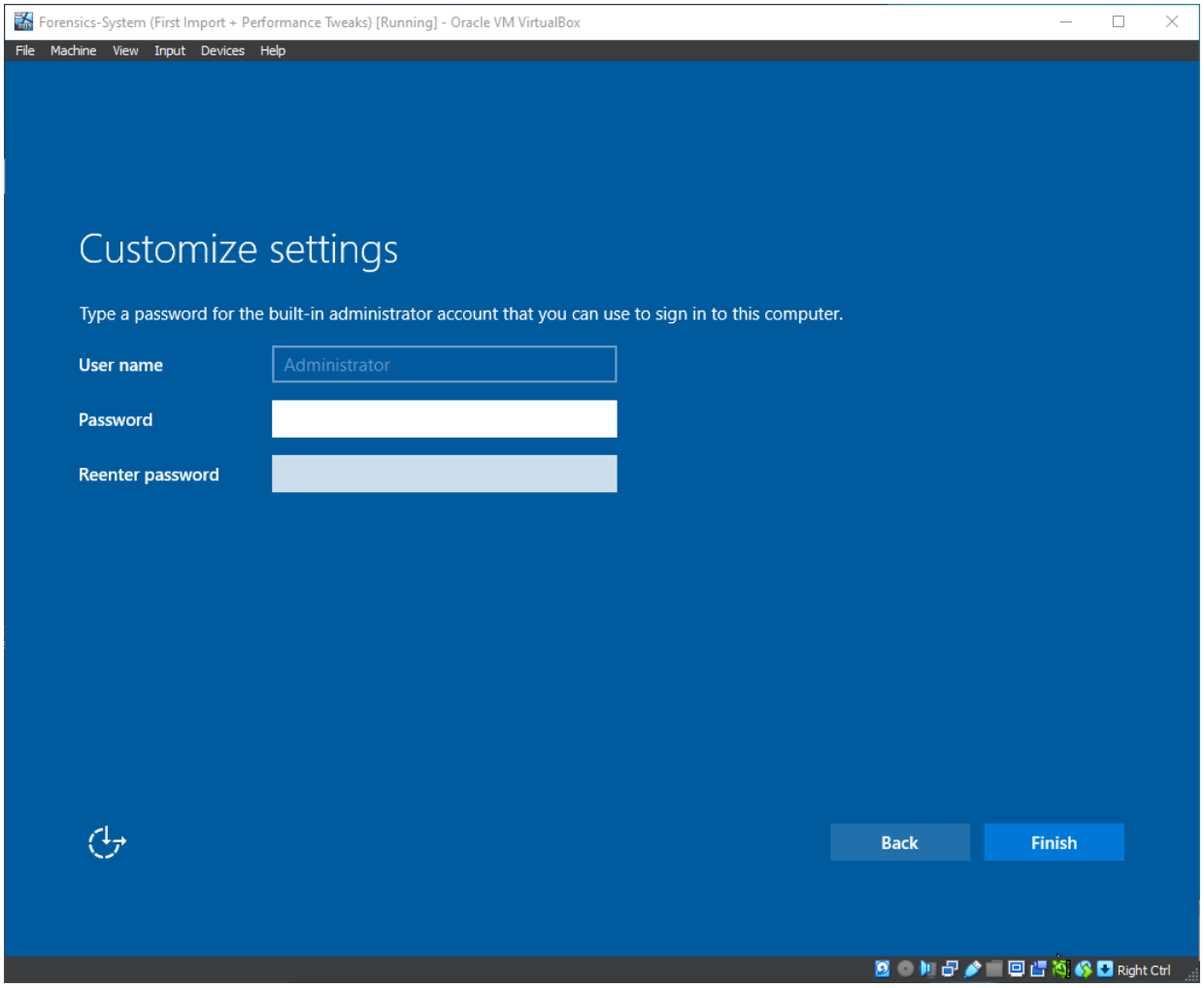

Oracle VM VirtualBox Manager
File Machine Snapshot Help
Tools
Take Delete Restore Properties Clone Settings Discard Start
Forensics-System
Powered Off
Name
Taken
Current State
Take Snapshot of Virtual Machine
Snapshot Name
First Import + Performance Tweaks
Snapshot Description
Ok Cancel Help
Take Reset

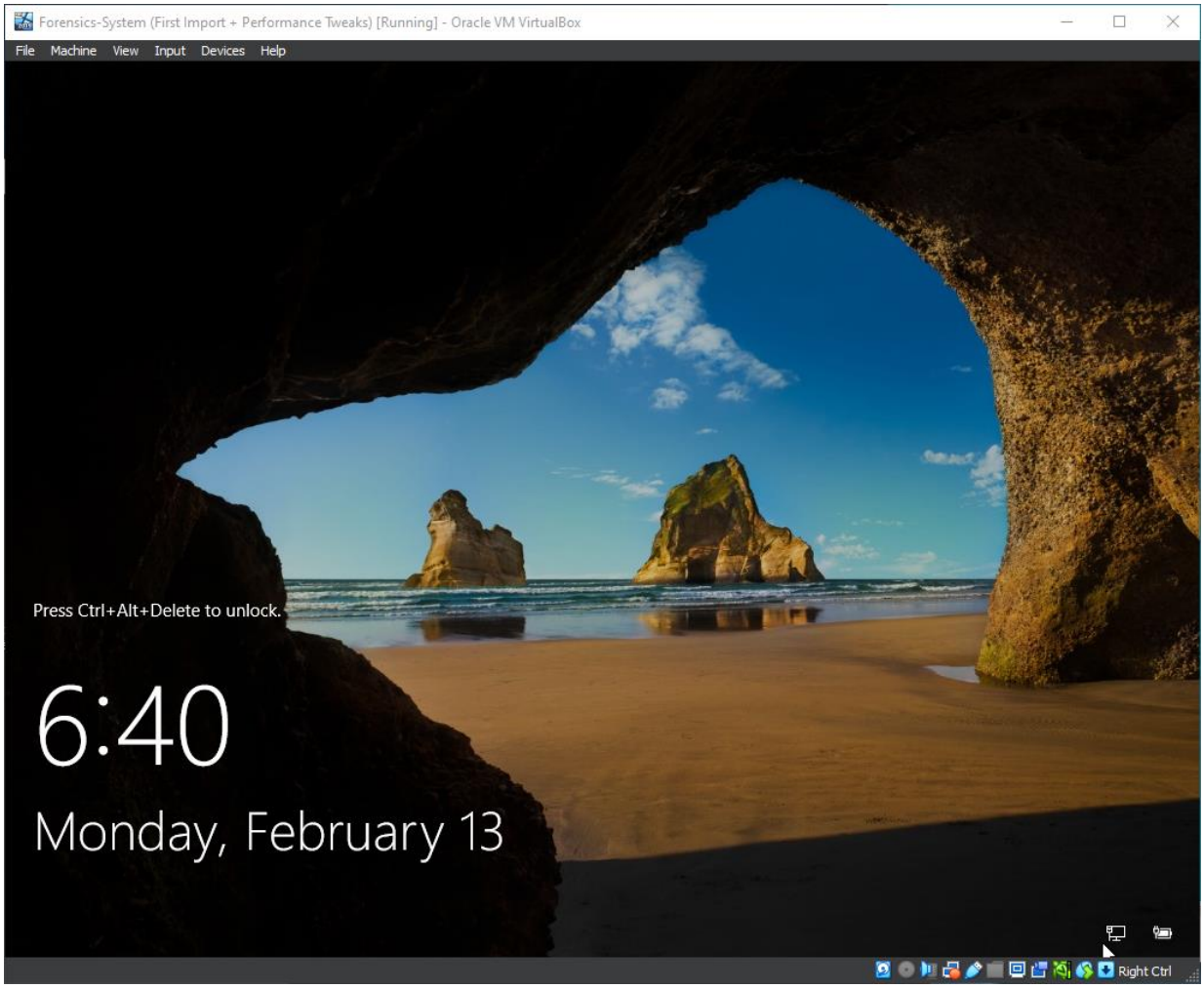
- Start the vm.

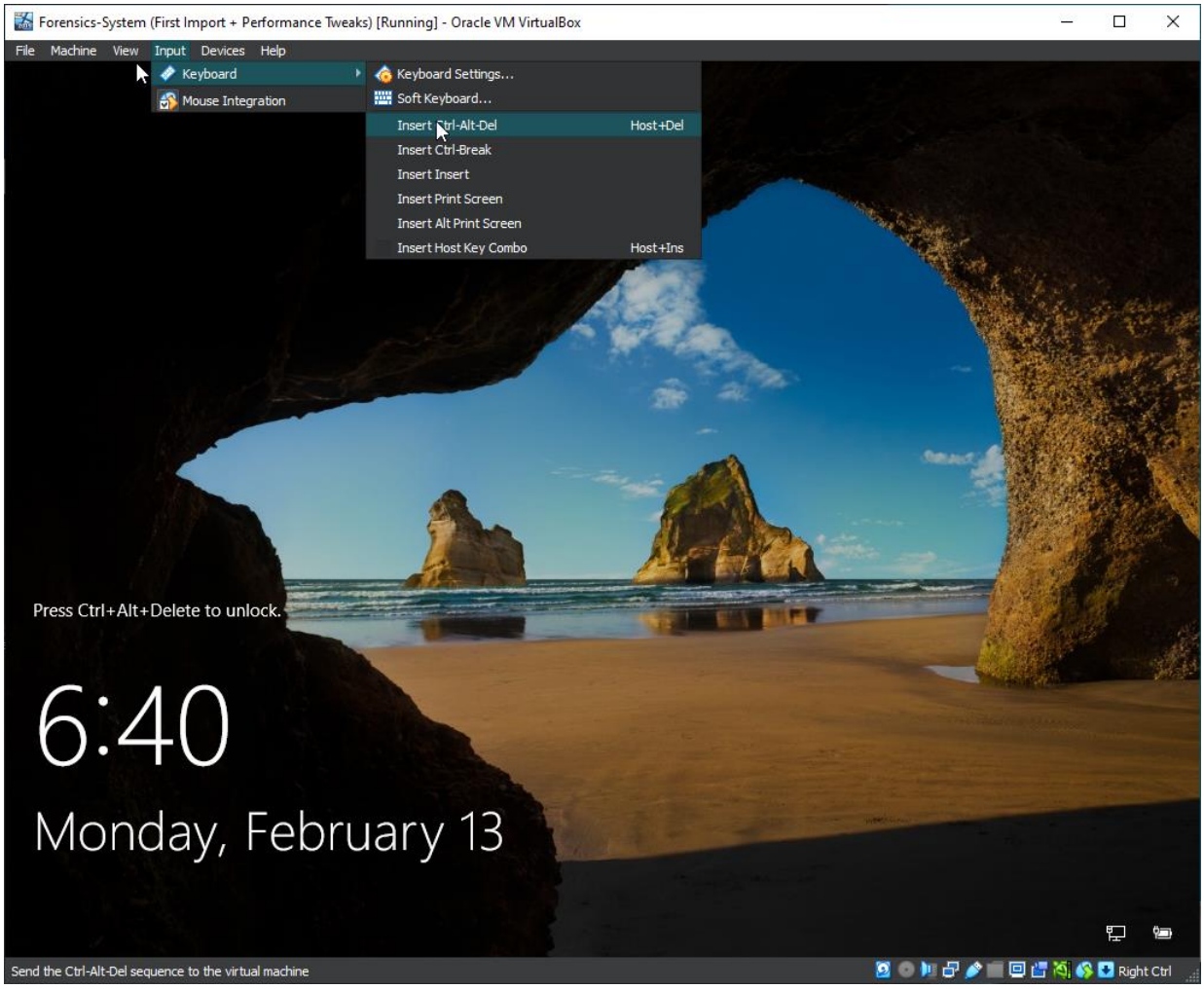

Oracle VM VirtualBox Manager
File Machine Help
Tools
Forensics-System (First Import + Perfo...)
Powered Off
New Add Settings Discard Start
General
Name: Forensics-System
Operating System: Windows 2019 (64-bit)
System
Base Memory: 8192 MB
Processors: 8
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, Hyper-V
Paravirtualization
Display
Video Memory: 256 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: SATA
SATA Port 0: {846fc4c7-c958-4af7-aeae-58f9ad17f030}.vhd (Differencing, Inaccessible)
SATA Port 1: [Optical Drive] Empty
Audio
Host Driver: Default
Controller: Intel HD Audio
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)
USB
USB Controller: xHCI
Device Filters: 0 (0 active)
Shared folders
None
Description
None
Powering VM up ...
0%
Forensics-System



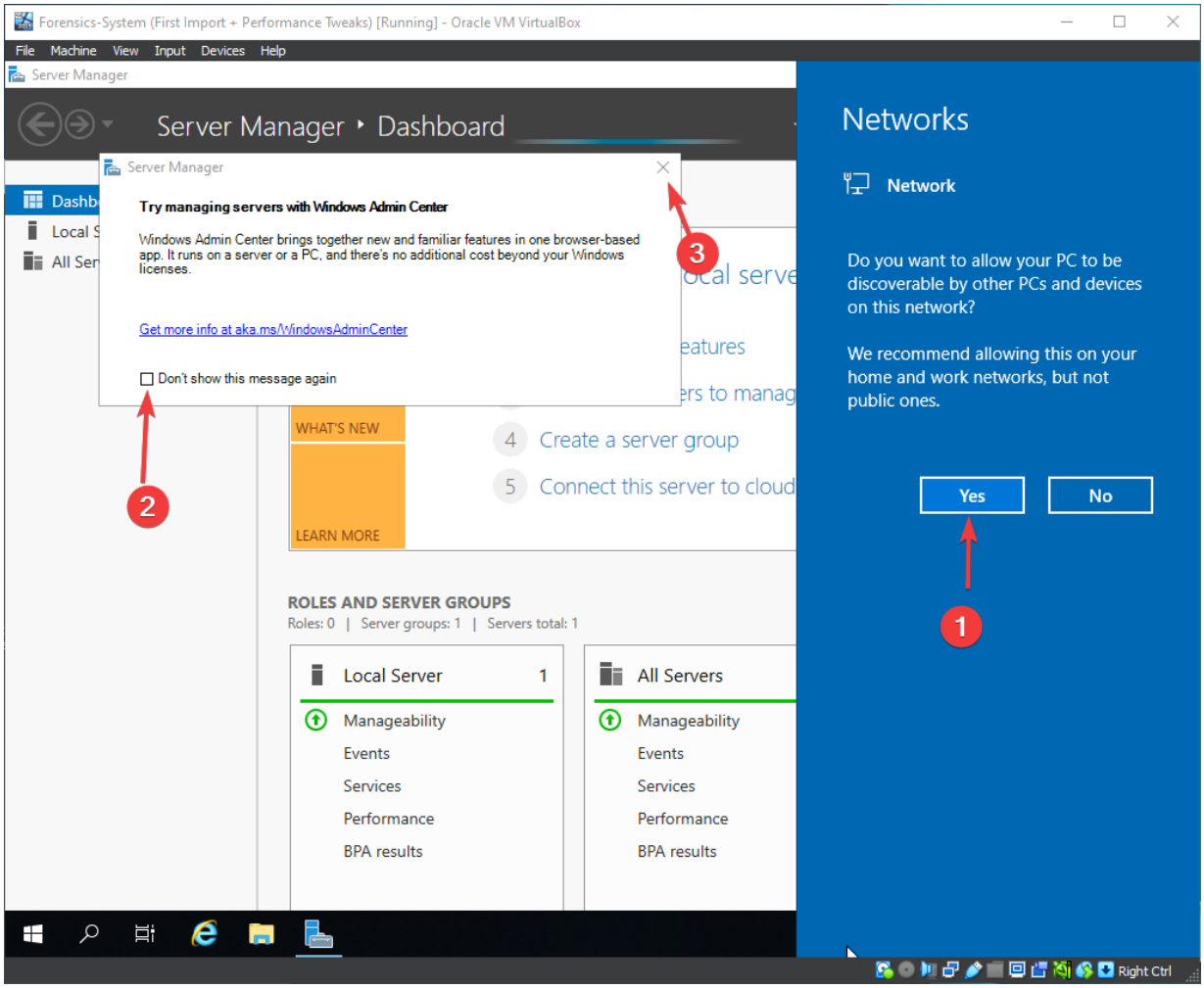
- You need to put an Administrator account password.

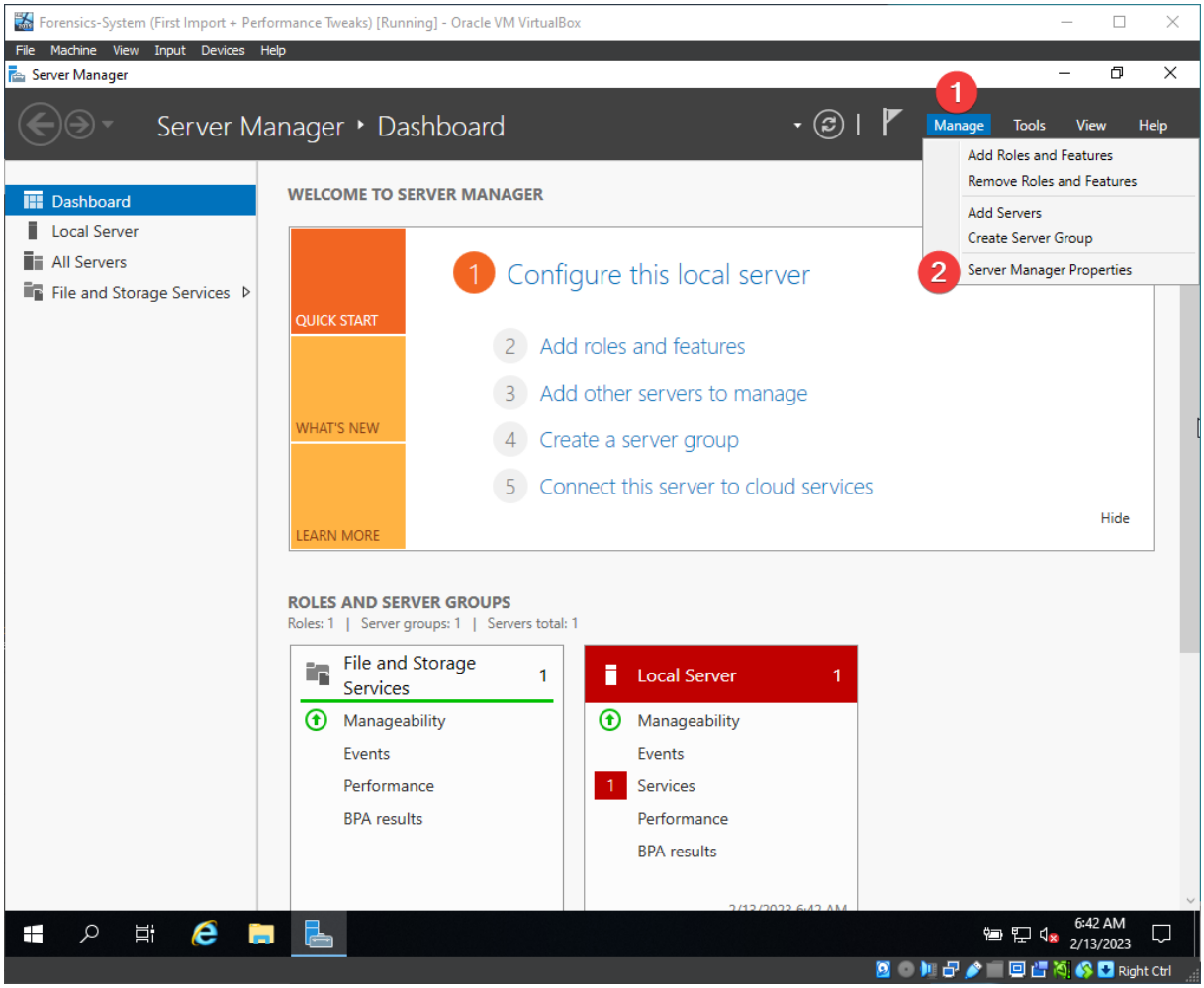

Forensics-System (First Import + Performance Tweaks) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Customize settings
Type a password for the built-in administrator account that you can use to sign in to this computer.
User name
Administrator
Password
Reenter password
Back
Finish
Right Ctrl

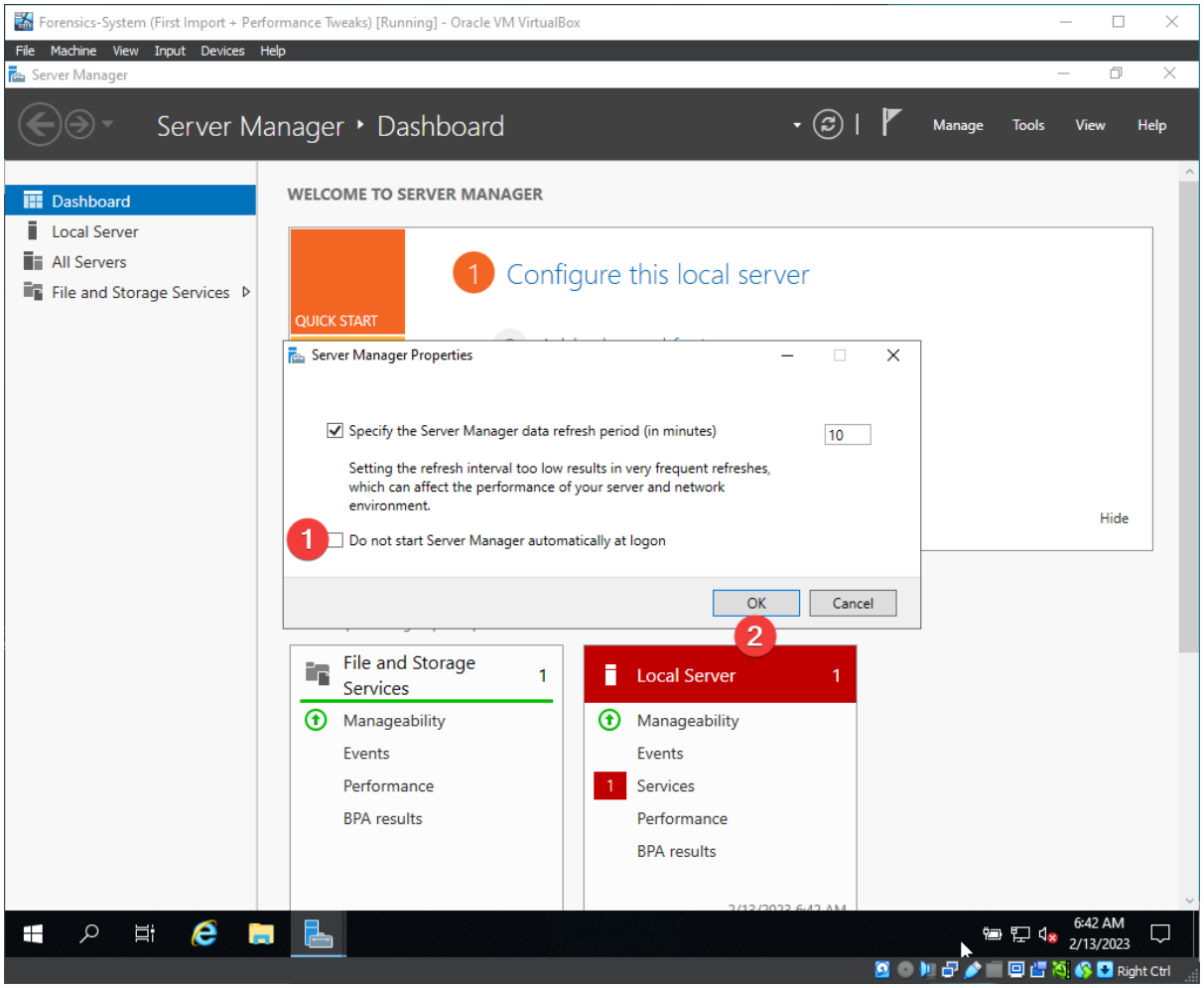

Forensics-System (First Import + Performance Tweaks) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Press Ctrl+Alt+Delete to unlock.
6:40
Monday, February 13
Right Ctrl

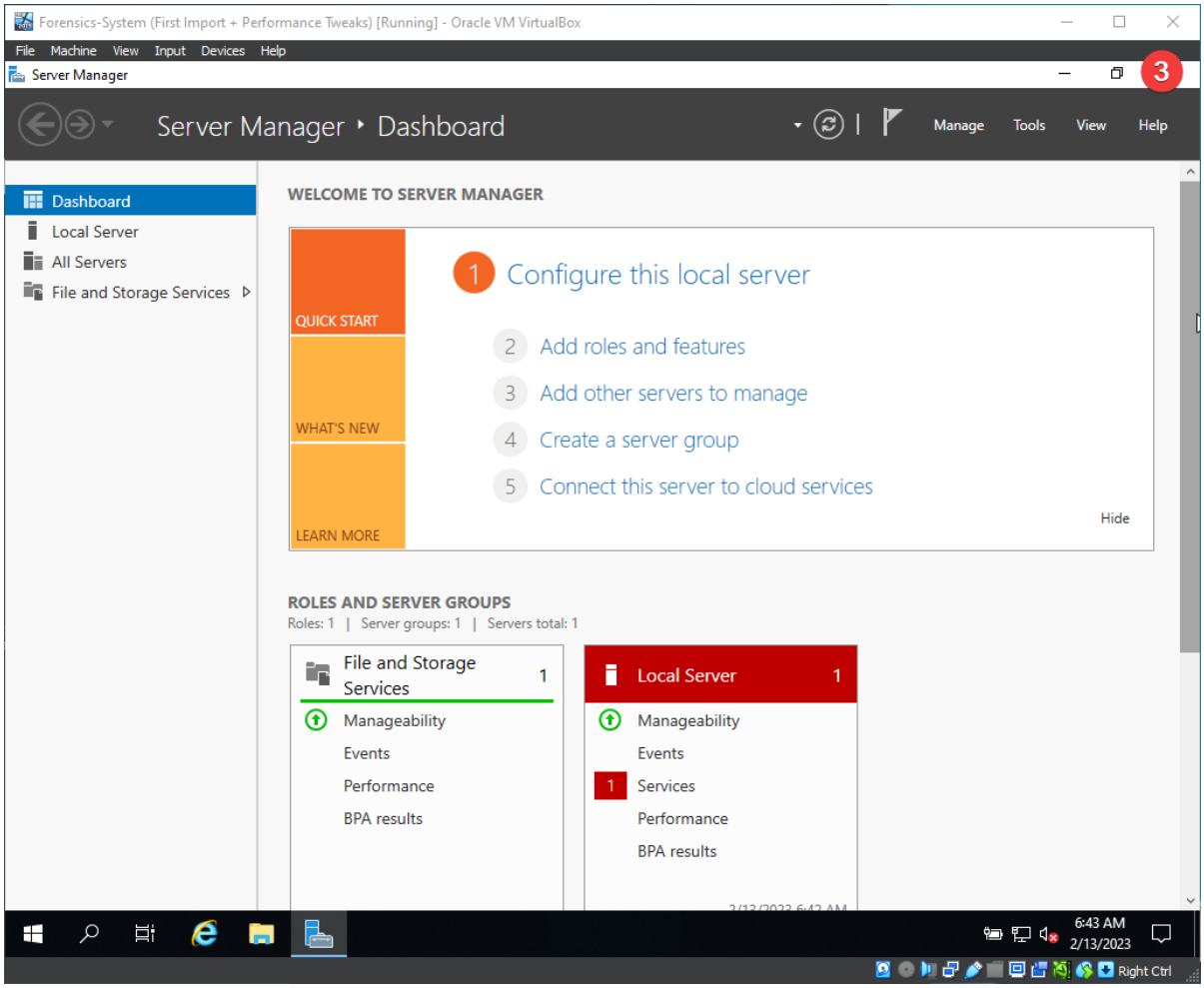


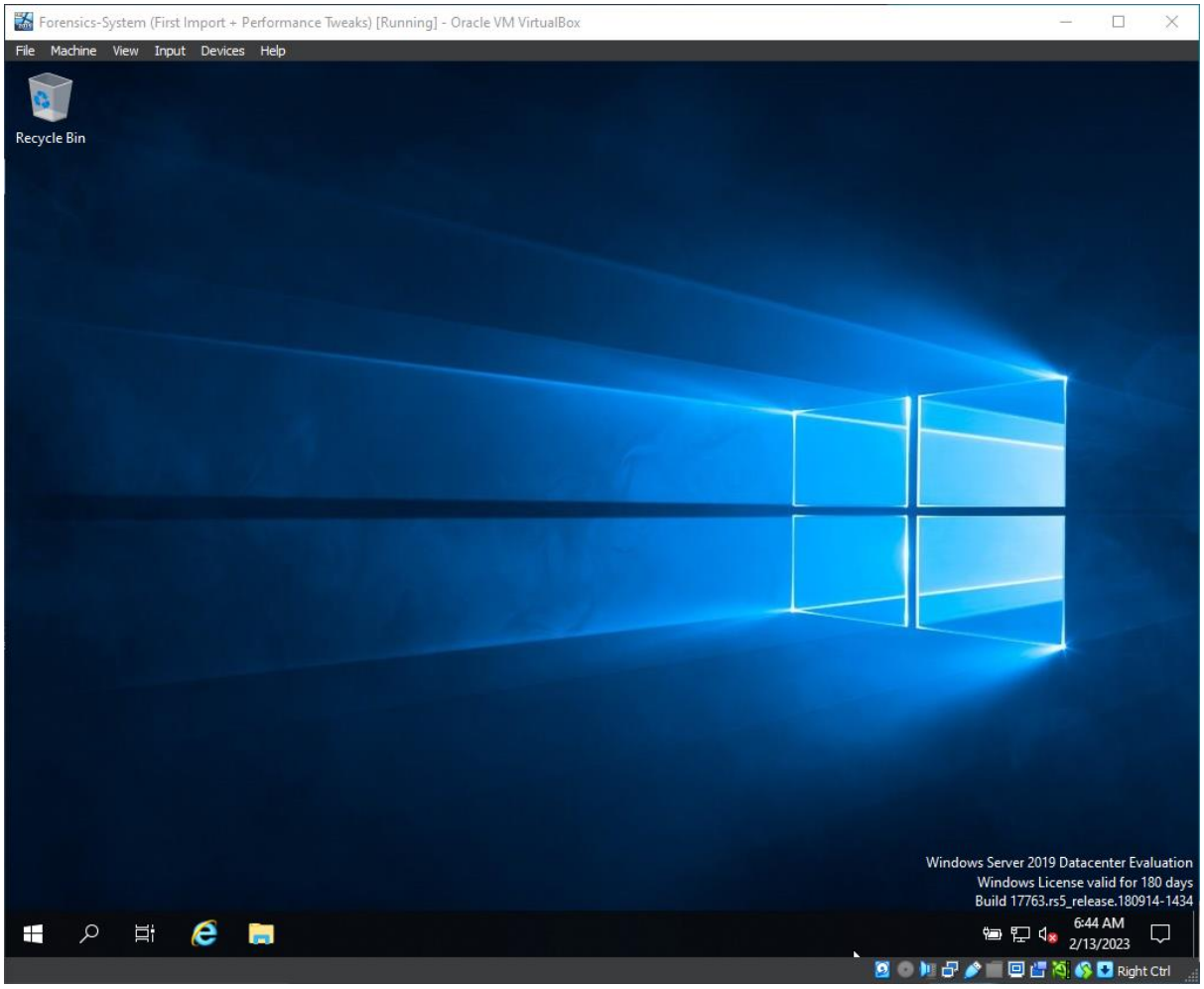
- Input the password, and login.


Forensics-System (First Import + Performance Tweaks) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager • Dashboard
Server Manager
Try managing servers with Windows Admin Center
Windows Admin Center brings together new and familiar features in one browser-based app. It runs on a server or a PC, and there's no additional cost beyond your Windows licenses.
Get more info at aka.ms/WindowsAdminCenter
Don't show this message again
2
3
WHAT'S NEW
LEARN MORE
4 Create a server group
5 Connect this server to cloud
ROLES AND SERVER GROUPS
Roles: 0 | Server groups: 1 | Servers total: 1
Local Server 1
Manageability
Events
Services
Performance
BPA results
All Servers
Manageability
Events
Services
Performance
BPA results
Networks
Network
Do you want to allow your PC to be discoverable by other PCs and devices on this network?
We recommend allowing this on your home and work networks, but not public ones.
Yes
No
1
Right Ctrl

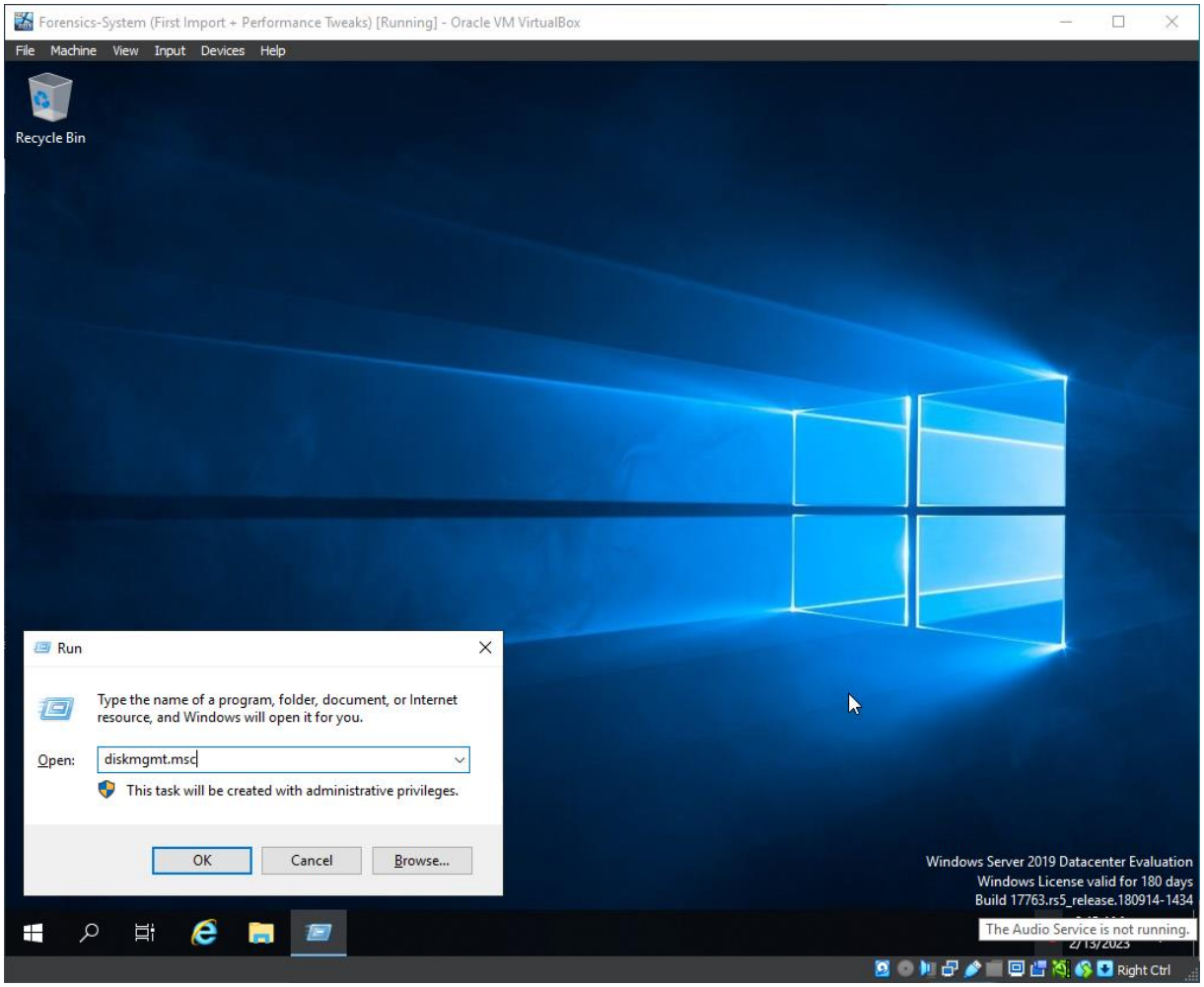

Forensics-System (First Import + Performance Tweaks) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager • Dashboard
1
Manage
Tools
View
Help
Add Roles and Features
Remove Roles and Features
Add Servers
Create Server Group
2
Server Manager Properties
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Events
Performance
BPA results
Local Server 1
Manageability
Events
1 Services
Performance
BPA results
6:42 AM
2/13/2023
Right Ctrl

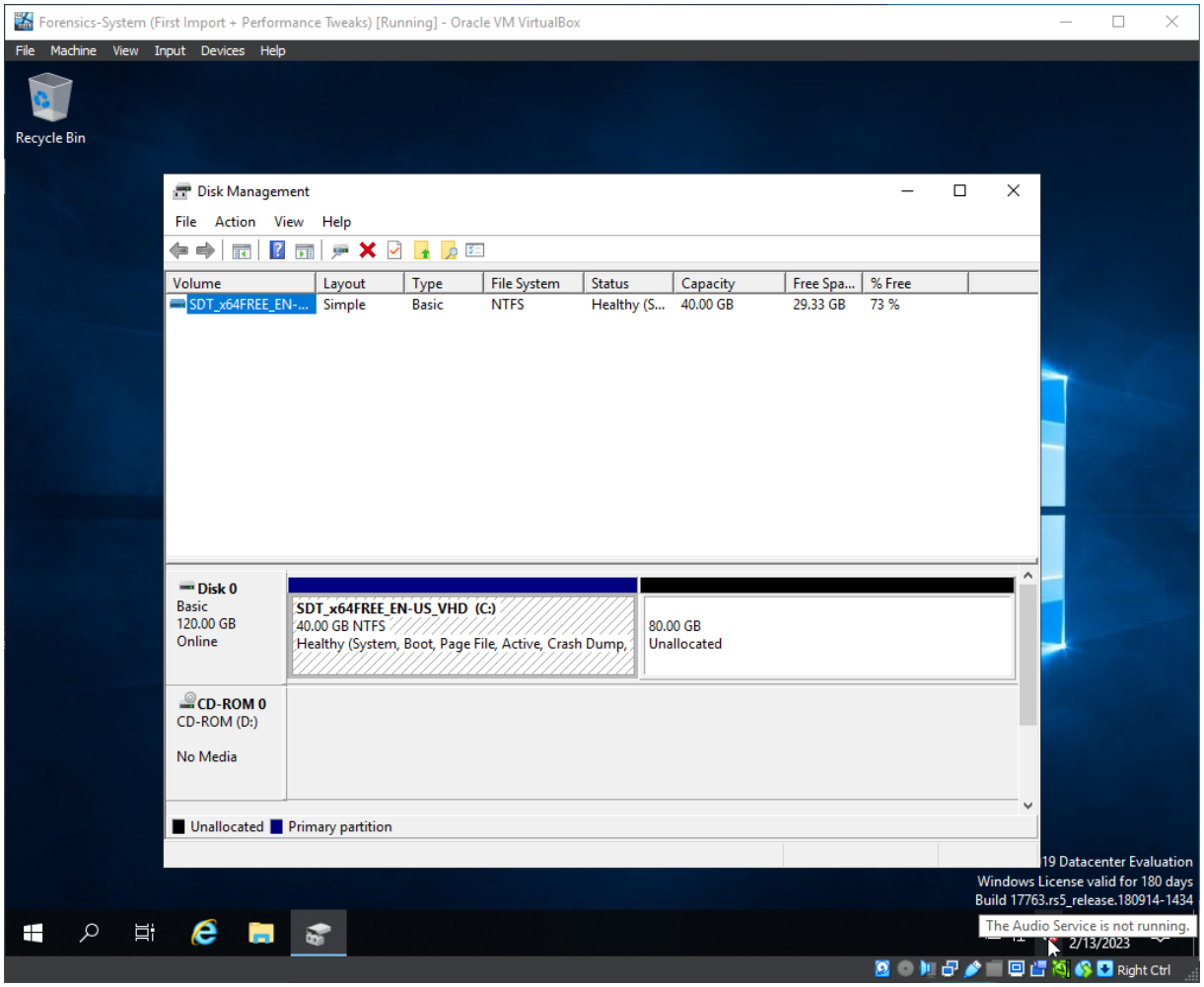

Forensics-System (First Import + Performance Tweaks) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
1 Configure this local server
Server Manager Properties
Specify the Server Manager data refresh period (in minutes)
10
Setting the refresh interval too low results in very frequent refreshes, which can affect the performance of your server and network environment.
1
Do not start Server Manager automatically at logon
OK
Cancel
2
Hide
File and Storage Services 1
Manageability
Events
Performance
BPA results
Local Server 1
Manageability
Events
1 Services
Performance
BPA results
6:42 AM
2/13/2023
Right Ctrl

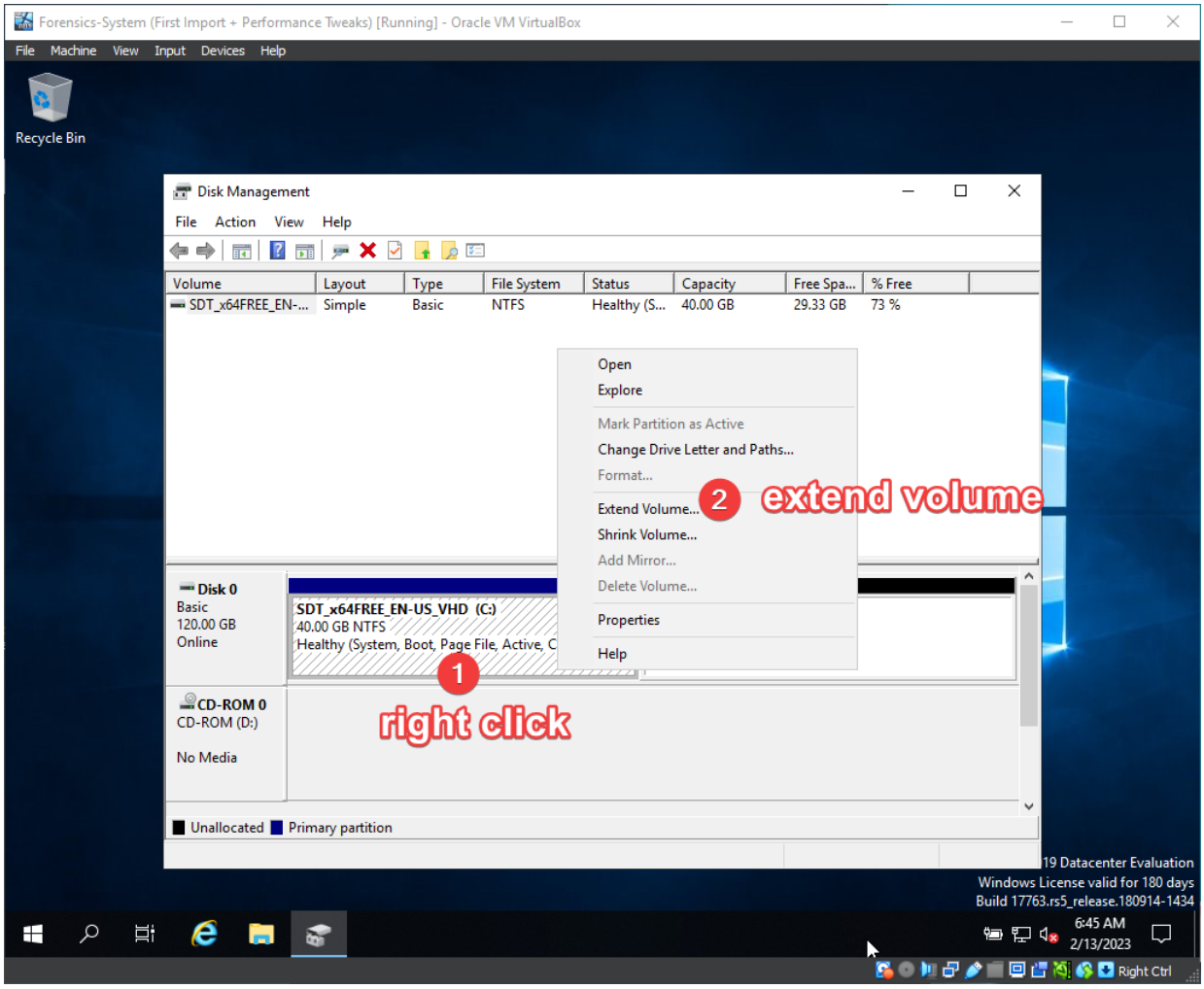

Forensics-System (First Import + Performance Tweaks) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Server Manager
3
Server Manager ‣ Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Events
Performance
BPA results
Local Server 1
Manageability
Events
1 Services
Performance
BPA results
6:43 AM
2/13/2023
Right Ctrl



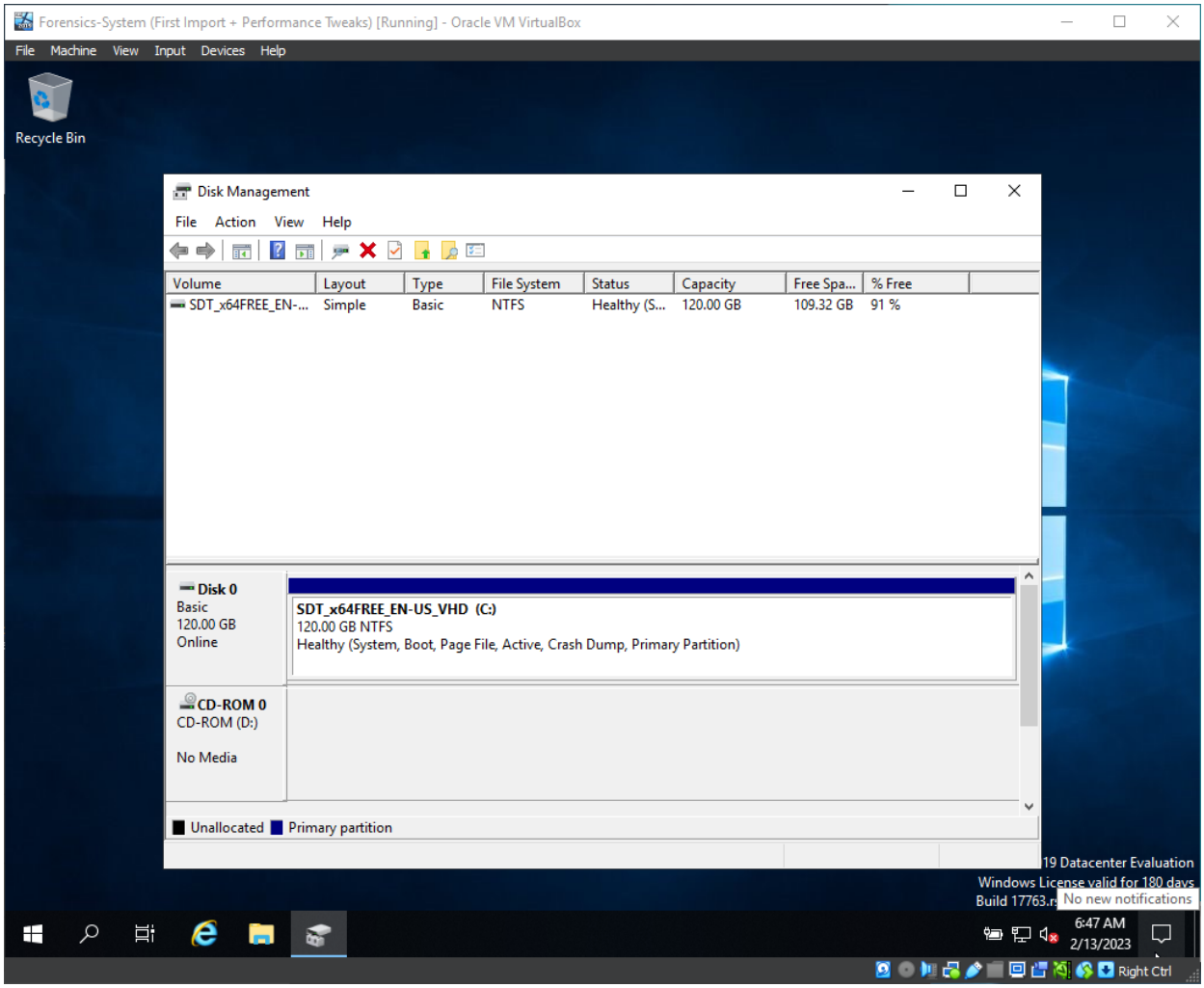
- Go to Disk Management (Win key + R : diskmgmt.msc).


Forensics-System (First Import + Performance Tweaks) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
diskmgmt.msc
This task will be created with administrative privileges.
OK
Cancel
Browse...
Windows Server 2019 Datacenter Evaluation
Windows License valid for 180 days
Build 17763.rs5_release.180914-1434
The Audio Service is not running.
Right Ctrl

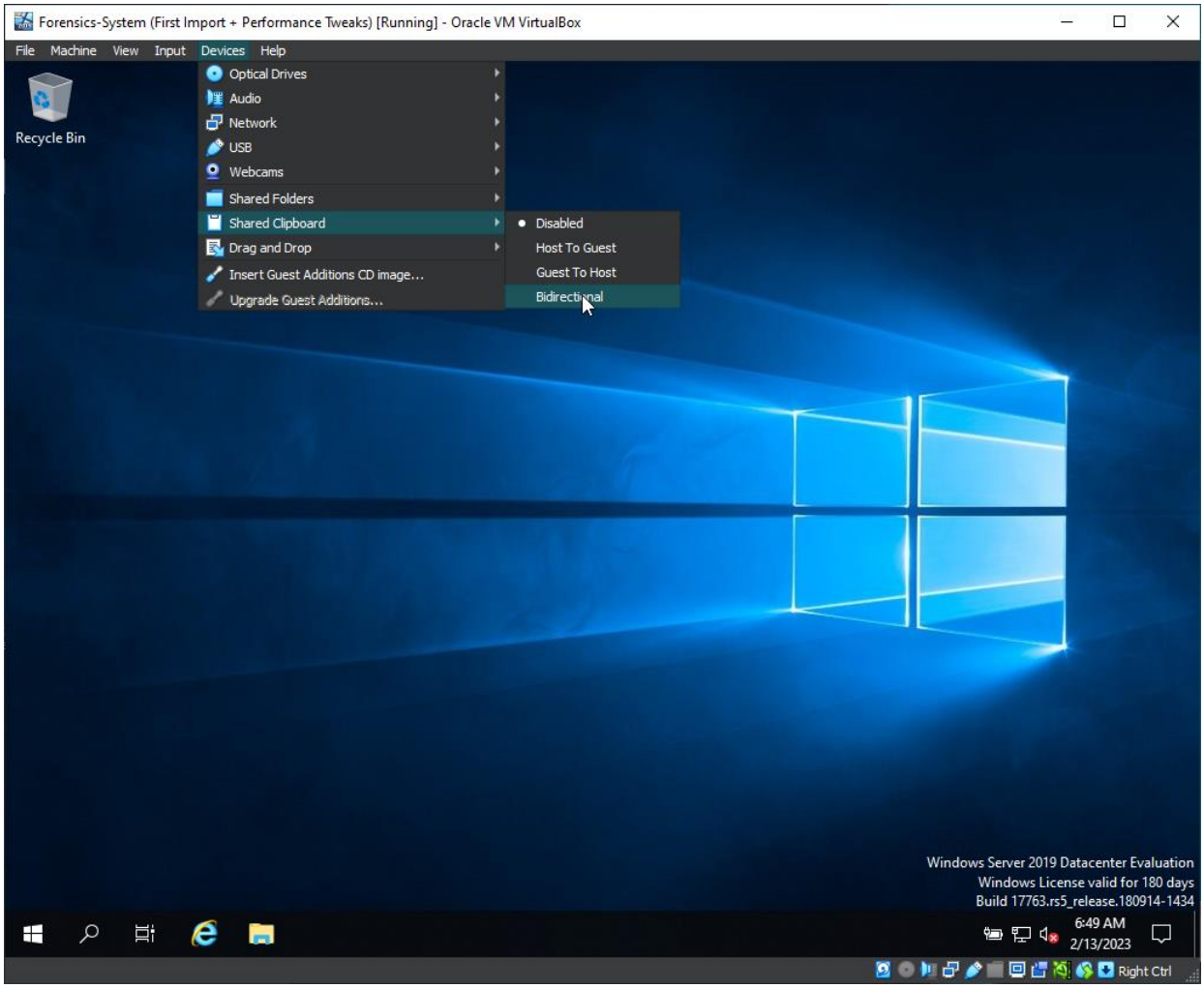

Forensics-System (First Import + Performance Tweaks) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Disk Management
File Action View Help
Volume Layout Type File System Status Capacity Free Spa... % Free
SDT_x64FREE_EN-... Simple Basic NTFS Healthy (S... 40.00 GB 29.33 GB 73 %
Disk 0
Basic
120.00 GB
Online
SDT_x64FREE_EN-US_VHD (C:)
40.00 GB NTFS
Healthy (System, Boot, Page File, Active, Crash Dump,
80.00 GB
Unallocated
CD-ROM 0
CD-ROM (D:)
No Media
Unallocated Primary partition
19 Datacenter Evaluation
Windows License valid for 180 days
Build 17763.rs5_release.180914-1434
The Audio Service is not running.
2/13/2023
Right Ctrl

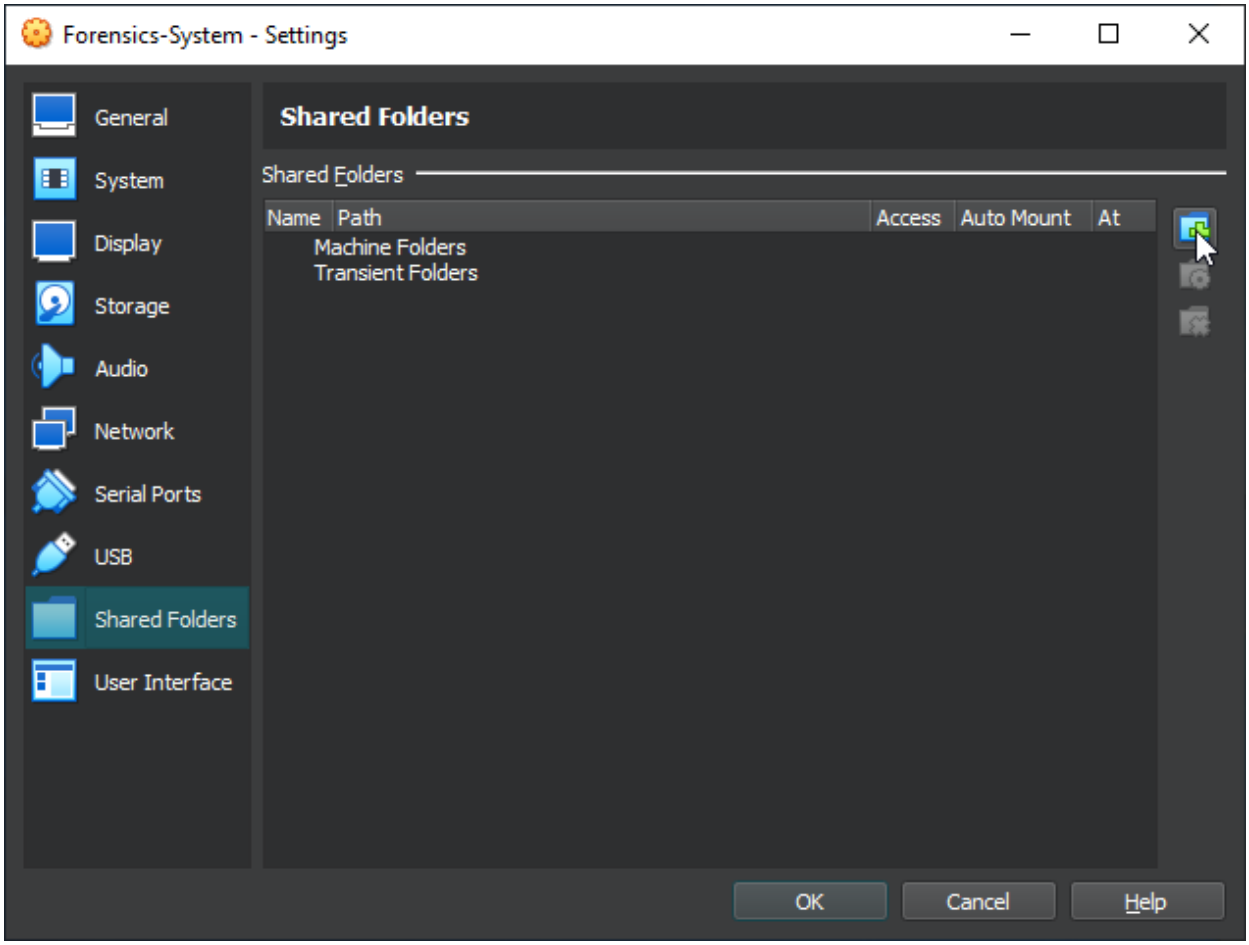


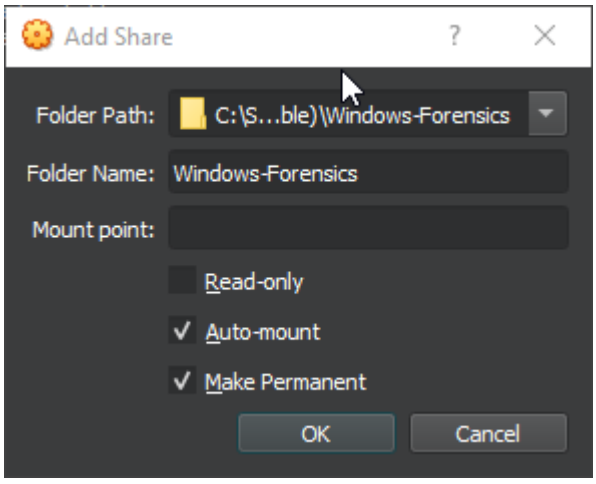
- Next untill finish.



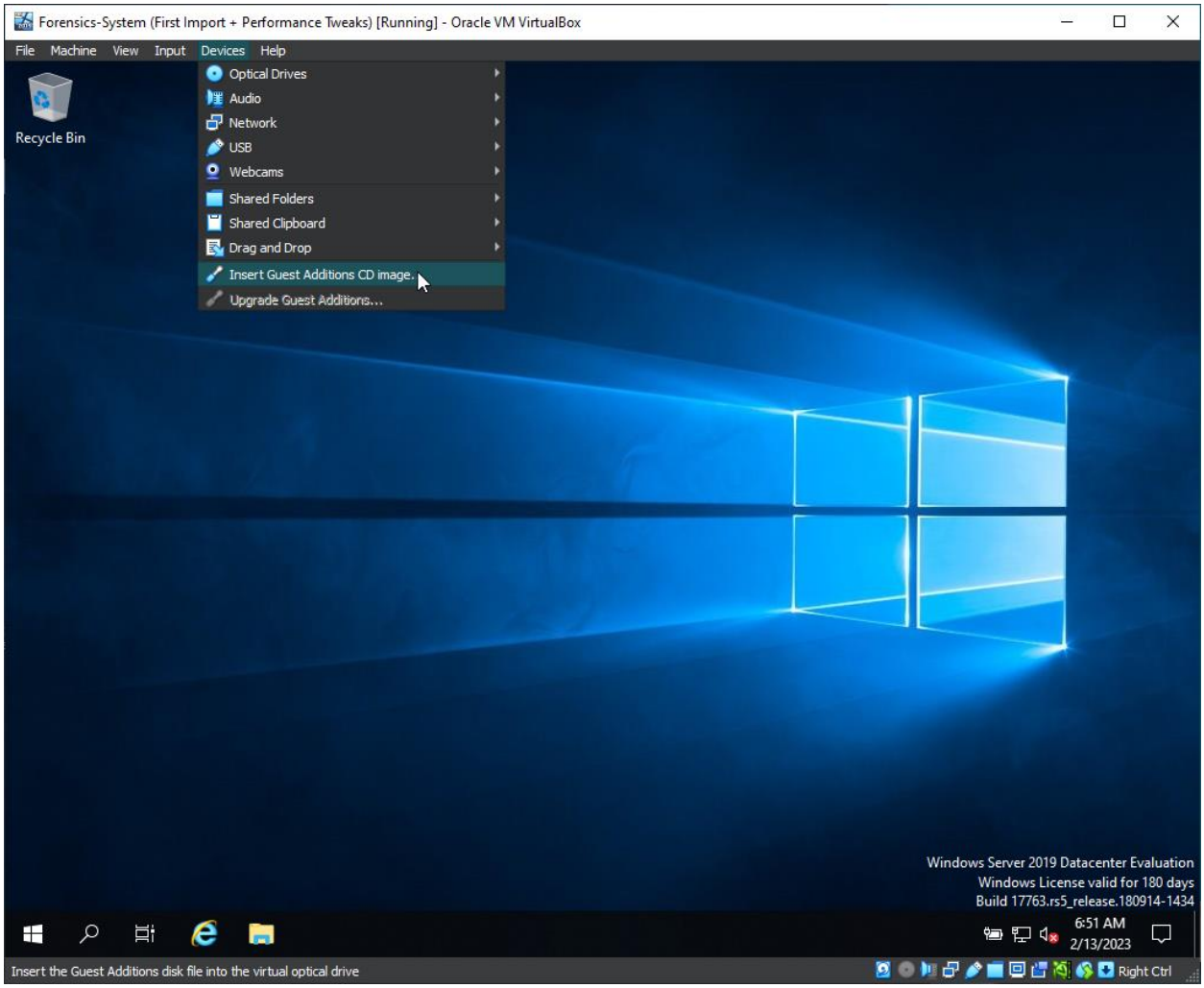
- Adding bidirectional clipboard, file drag and drop, and shared folder. Input what path of the folder do you want to share with the virtual machine.

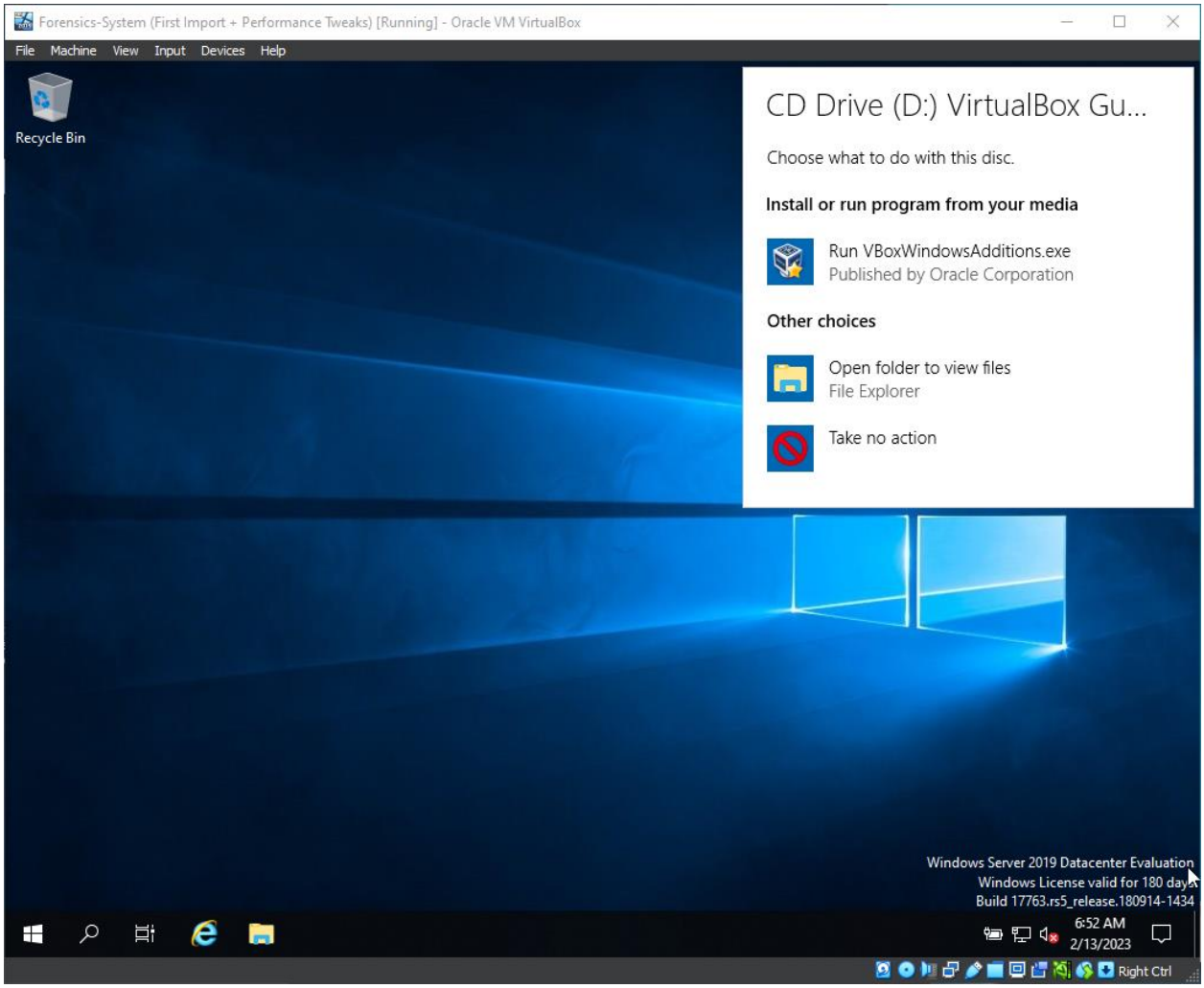

Forensics-System (First Import + Performance Tweaks) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Optical Drives
Audio
Network
USB
Webcams
Shared Folders
Shared Clipboard
Drag and Drop
Insert Guest Additions CD image...
Upgrade Guest Additions...
Disabled
Host To Guest
Guest To Host
Bidirectional
Windows Server 2019 Datacenter Evaluation
Windows License valid for 180 days
Build 17763.rs5_release.180914-1434
6:49 AM
2/13/2023
Right Ctrl

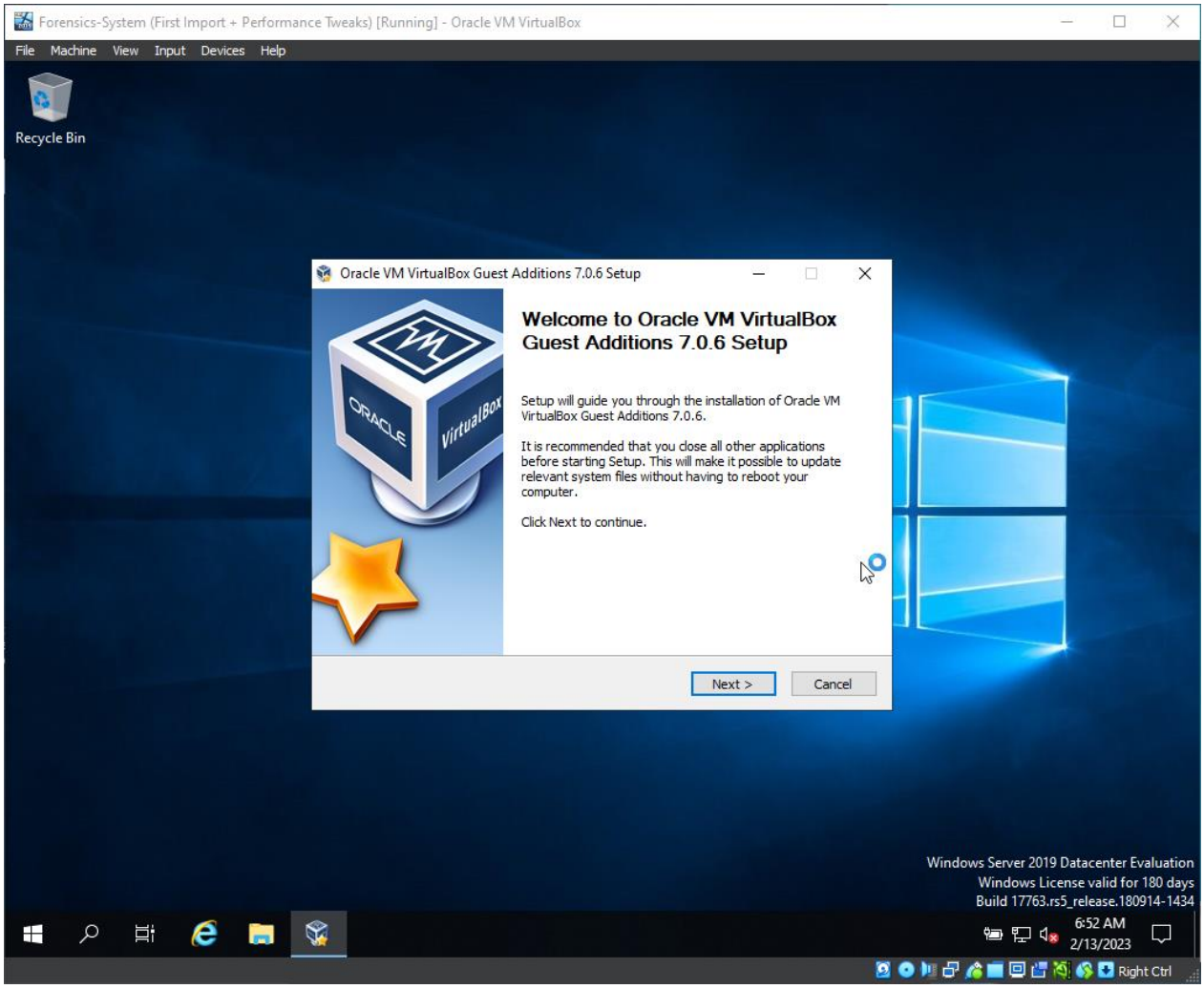




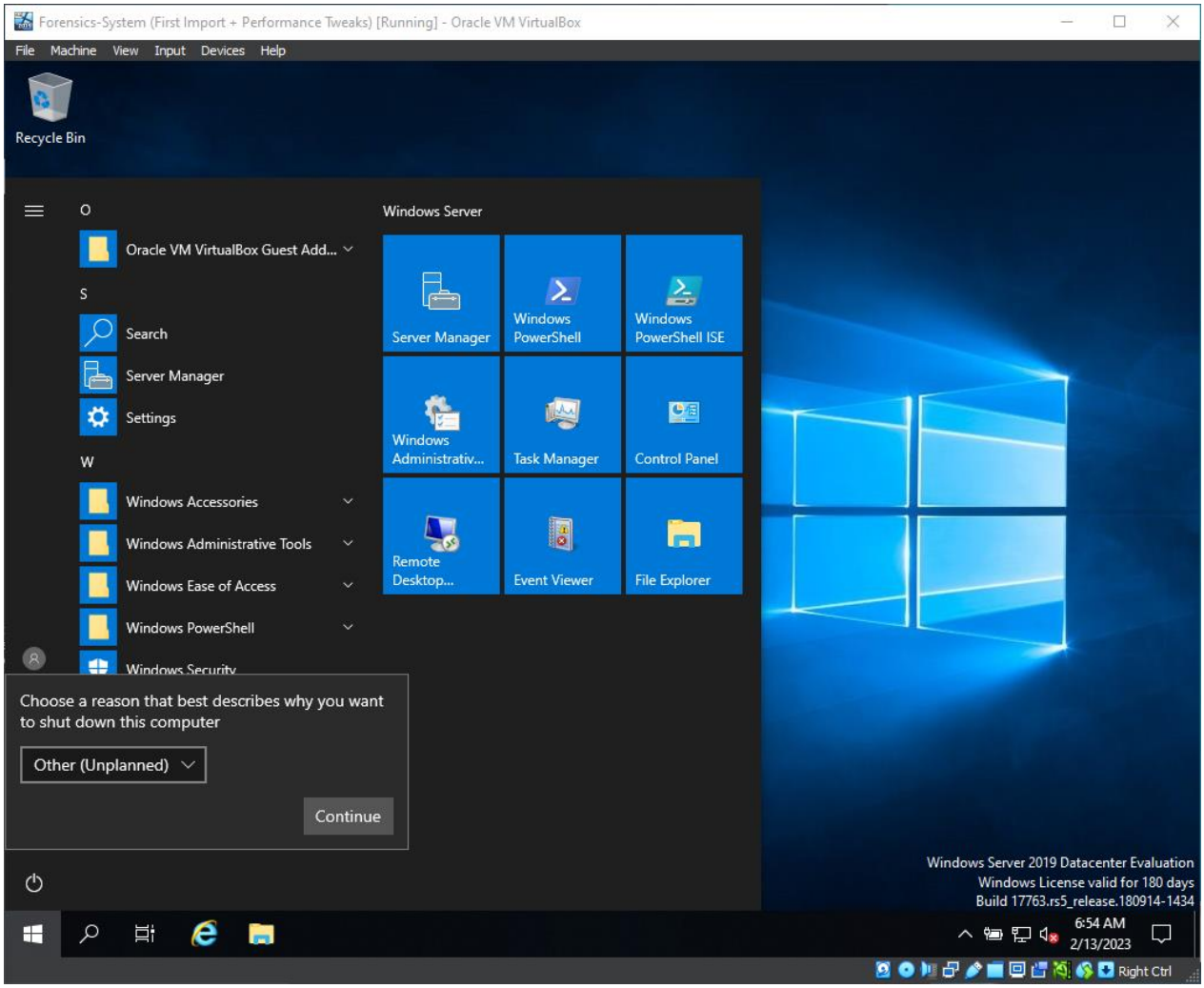
- Insert Guest Additions and install it.

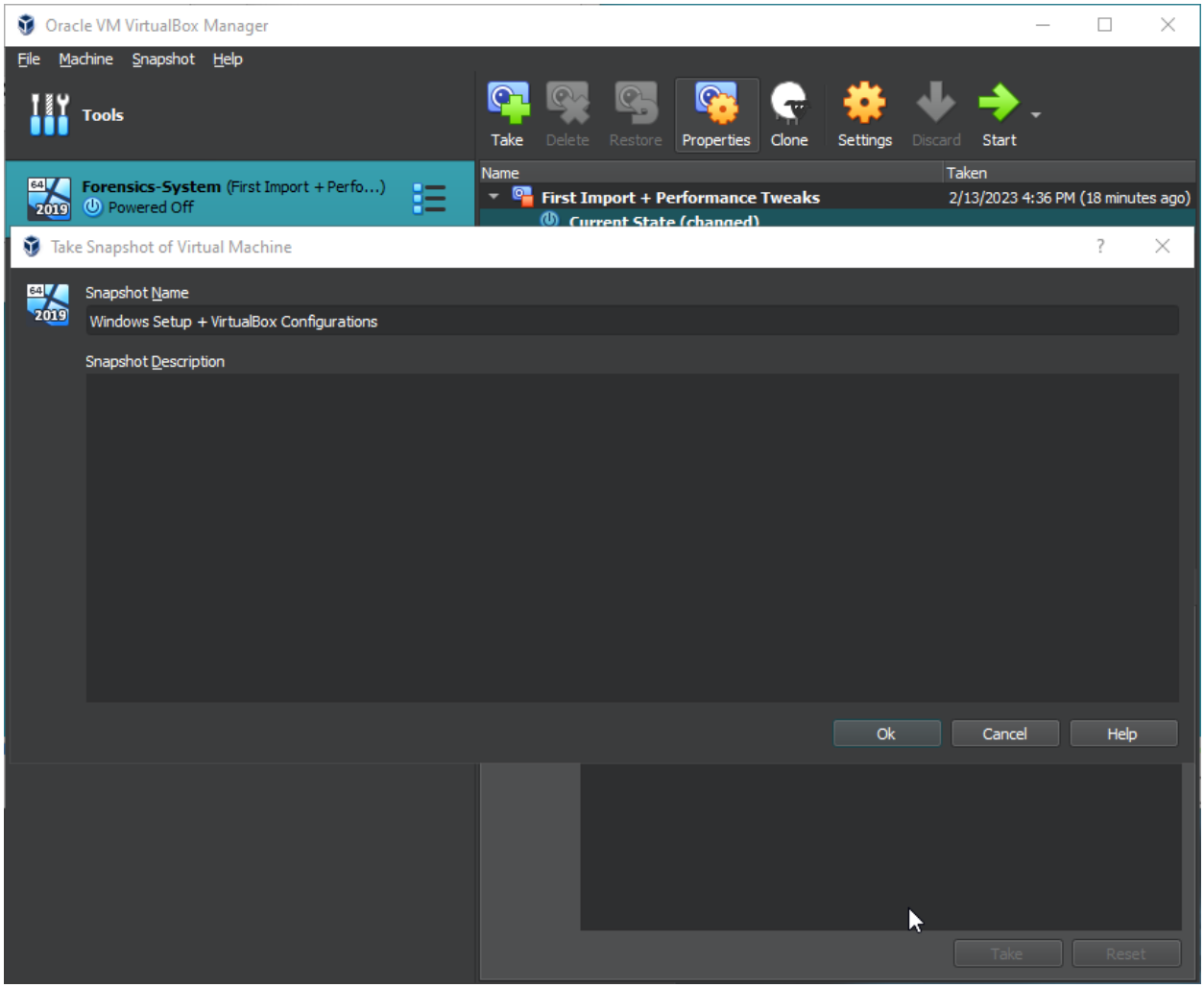

Forensics-System (First Import + Performance Tweaks) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Optical Drives
Audio
Network
USB
Webcams
Shared Folders
Shared Clipboard
Drag and Drop
Insert Guest Additions CD image...
Upgrade Guest Additions...
Windows Server 2019 Datacenter Evaluation
Windows License valid for 180 days
Build 17763.rs5_release.180914-1434
6:51 AM
2/13/2023
Insert the Guest Additions disk file into the virtual optical drive
Right Ctrl


Forensics-System (First Import + Performance Tweaks) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
CD Drive (D:) VirtualBox Gu...
Choose what to do with this disc.
Install or run program from your media
Run VBoxWindowsAdditions.exe
Published by Oracle Corporation
Other choices
Open folder to view files
File Explorer
Take no action
Windows Server 2019 Datacenter Evaluation
Windows License valid for 180 days
Build 17763.rs5_release.180914-1434
6:52 AM
2/13/2023
Right Ctrl



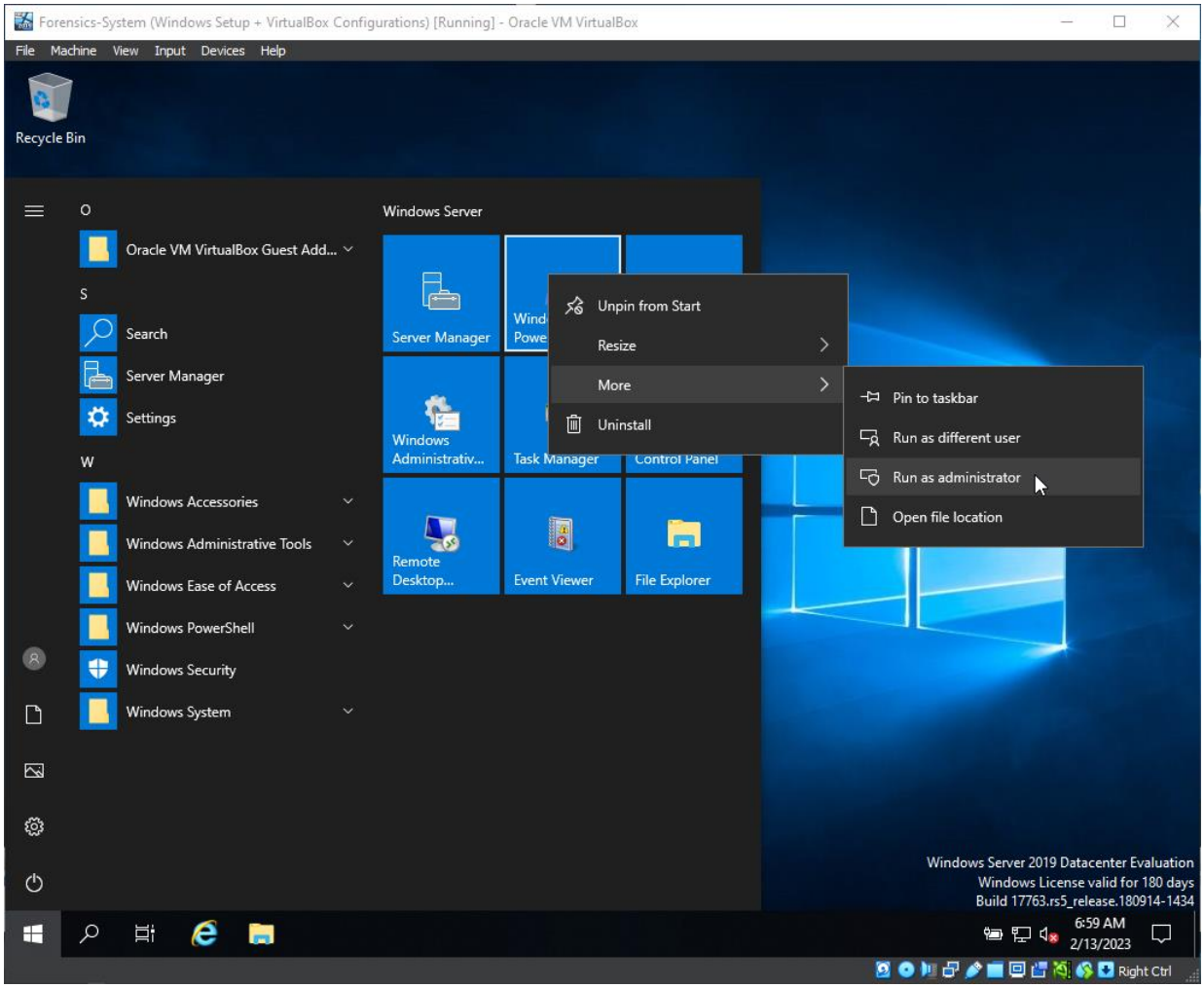
- Reboot the machine. Wait for it to boot, login, then shut it down.


Forensics-System (First Import + Performance Tweaks) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
O
Oracle VM VirtualBox Guest Add...
S
Search
Server Manager
Settings
W
Windows Accessories
Windows Administrative Tools
Windows Ease of Access
Windows PowerShell
Windows Security
Windows Server
Server Manager
Windows PowerShell
Windows PowerShell ISE
Windows Administrativ...
Task Manager
Control Panel
Remote Desktop...
Event Viewer
File Explorer
Choose a reason that best describes why you want to shut down this computer
Other (Unplanned)
Continue
Windows Server 2019 Datacenter Evaluation
Windows License valid for 180 days
Build 17763.rs5_release.180914-1434
6:54 AM
2/13/2023
Right Ctrl



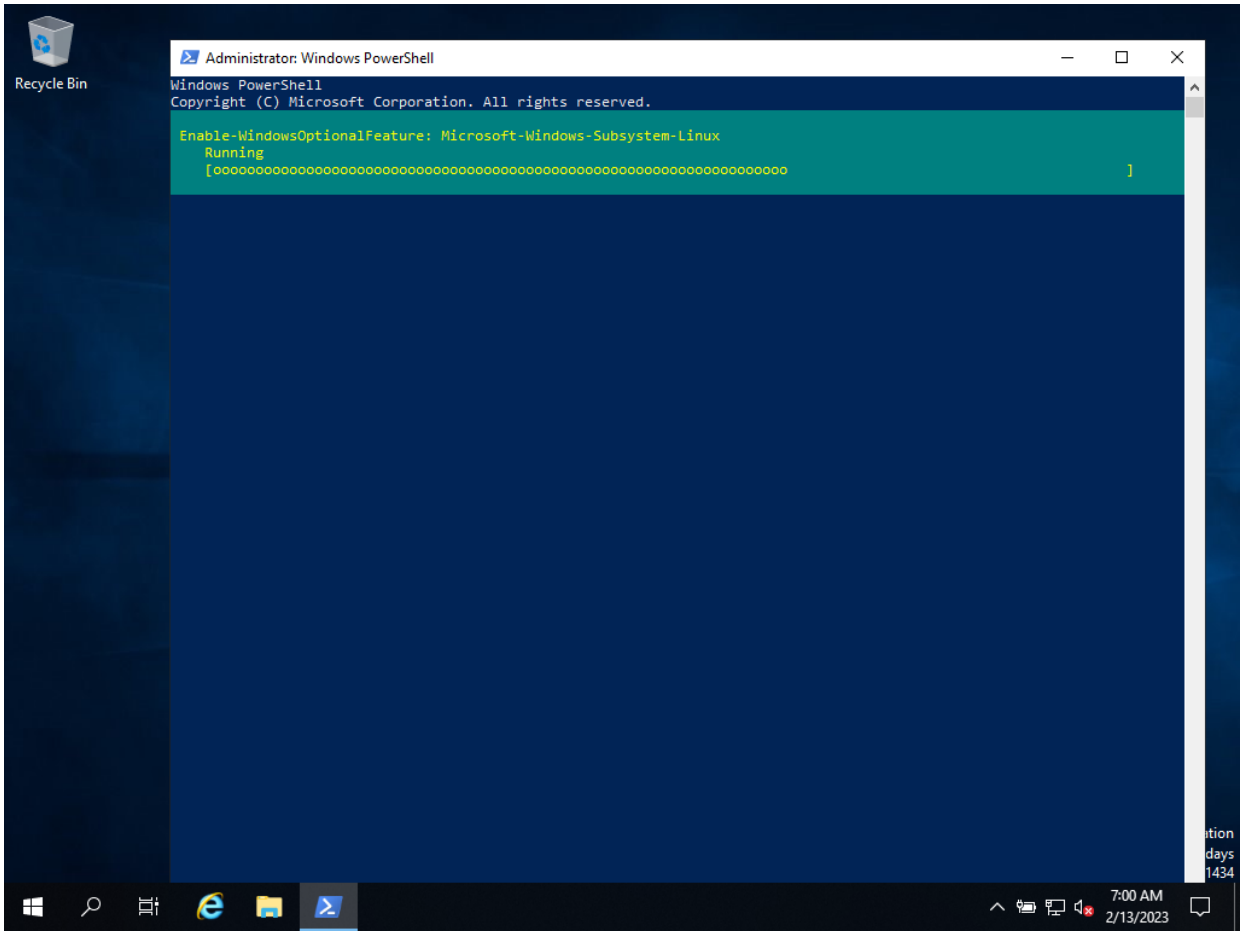
Adding WSL feature for Windows and installing Ubuntu subsystem

- Open up the Forensic virtual machine and enable wsl feature.

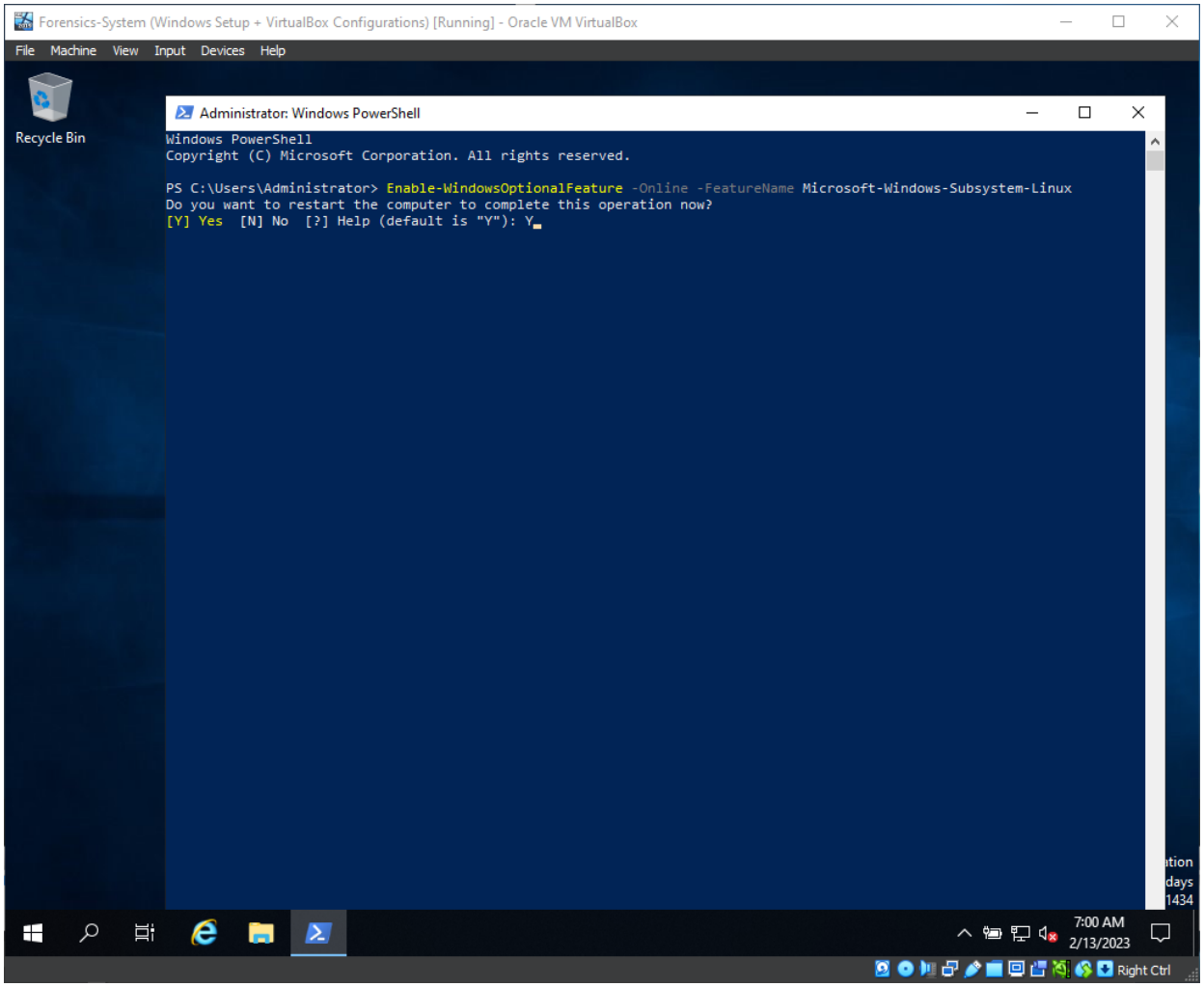


- Input:

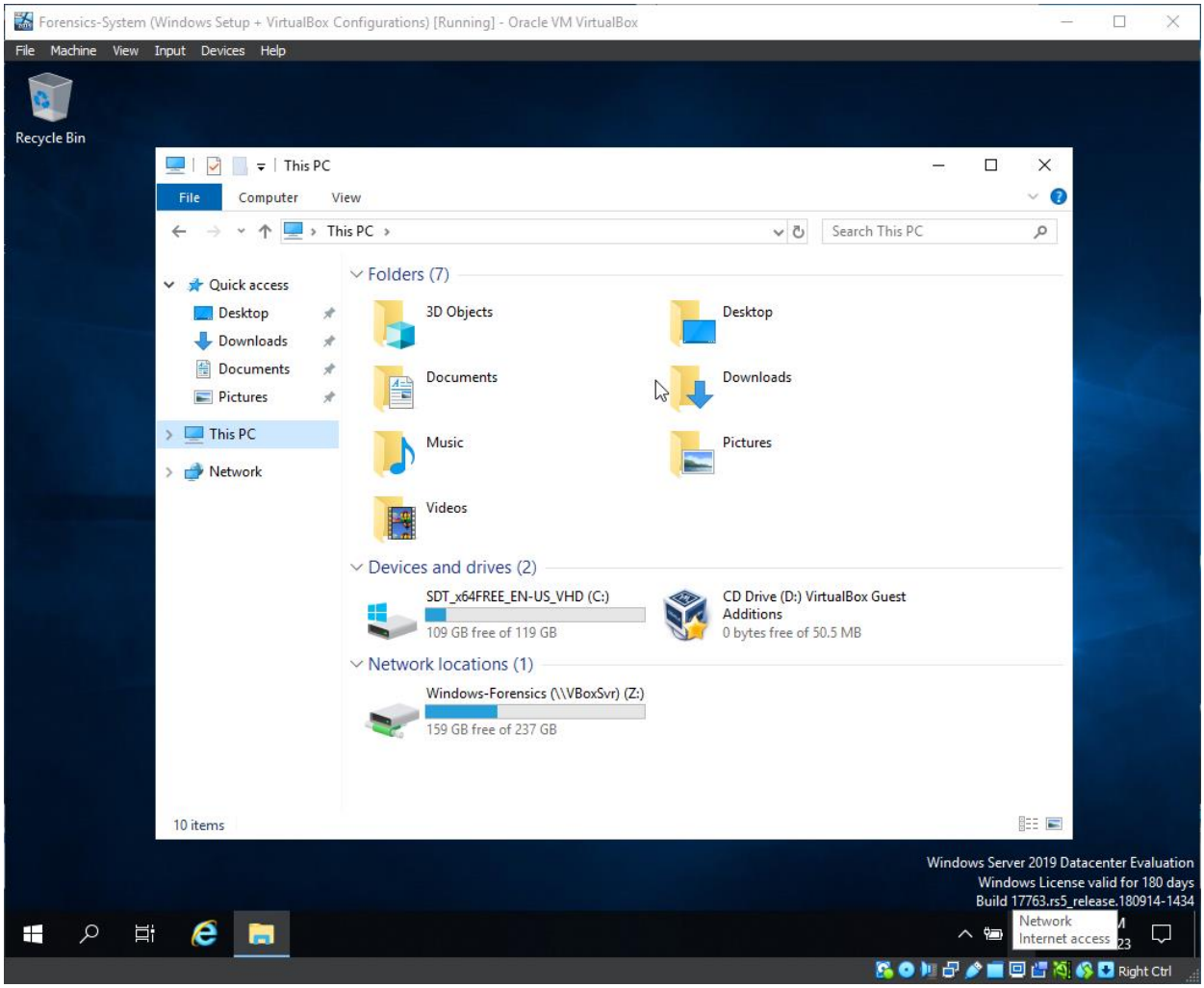
```
Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Windows-Subsystem-Linux
```



- Reboot the system to finish adding the feature.



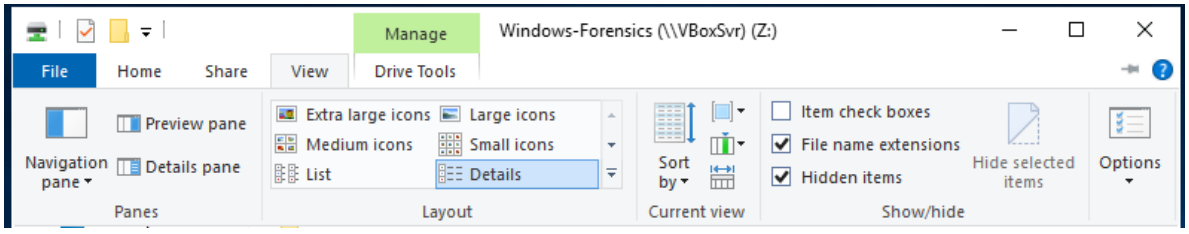
- Download the ubuntu 20.04 distribution: https://aka.ms/wslubuntu2004



- You will download a file with .AppxBundle extension.

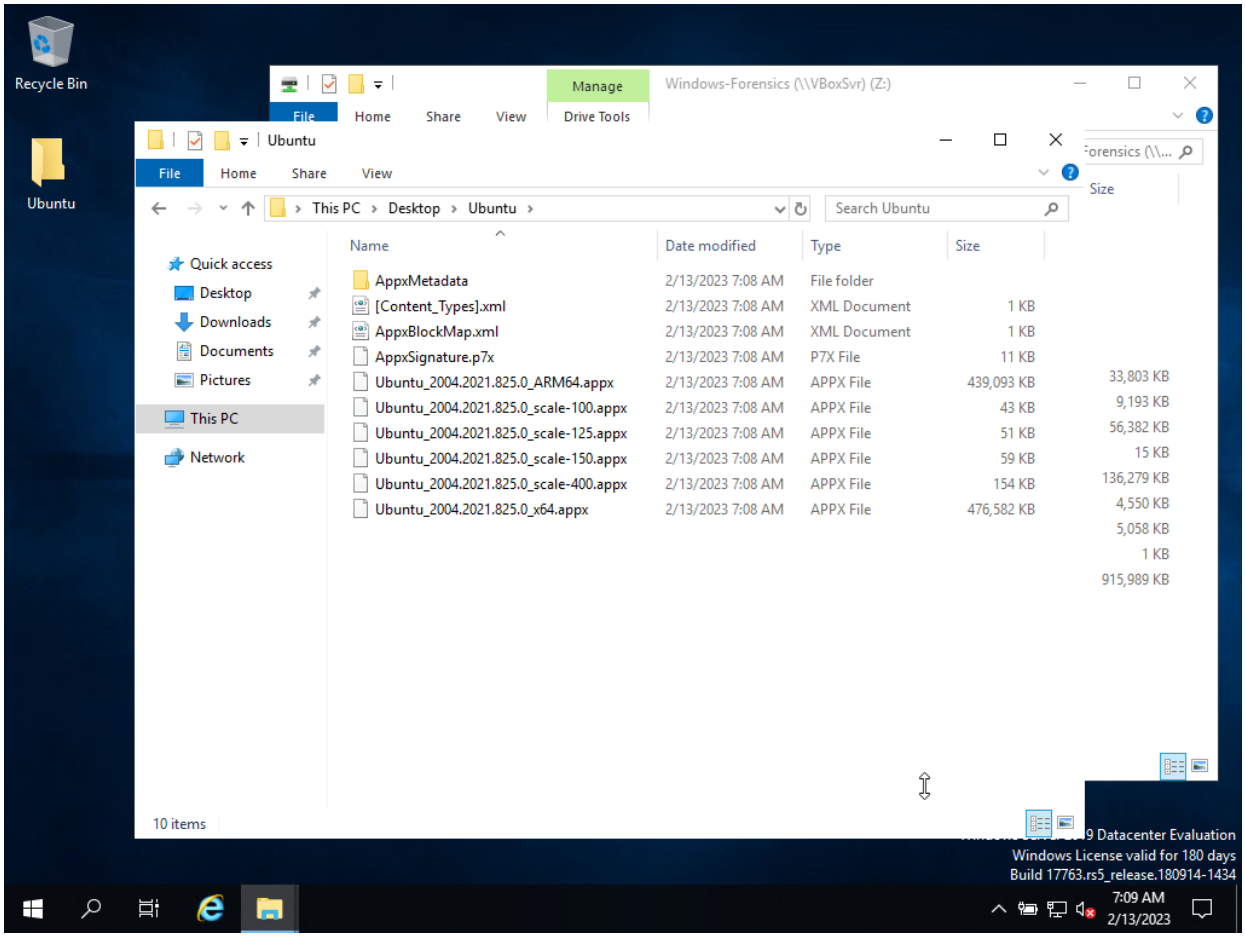
CanonicalGroupLimited.UbuntuonWindows_2004.2021.825.0.AppxBundle

- Change it to .zip (Just by renaming the file in file explorer).
- Make sure to have File name extensions and Hidden items checked in File explorer>View.

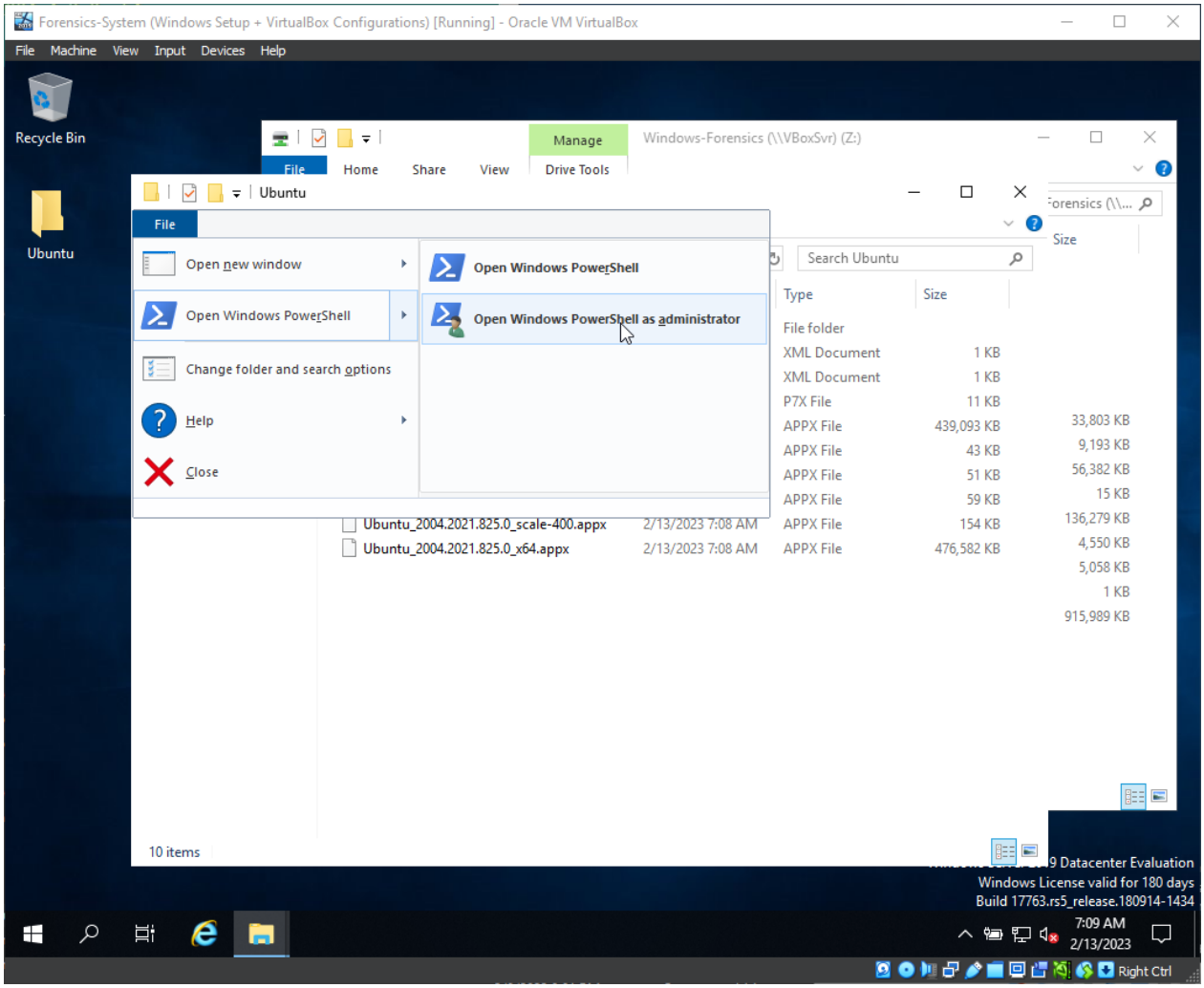


- I renamed the file for more easy management.

- Extract all the files, in my case I extracted all on Desktop:

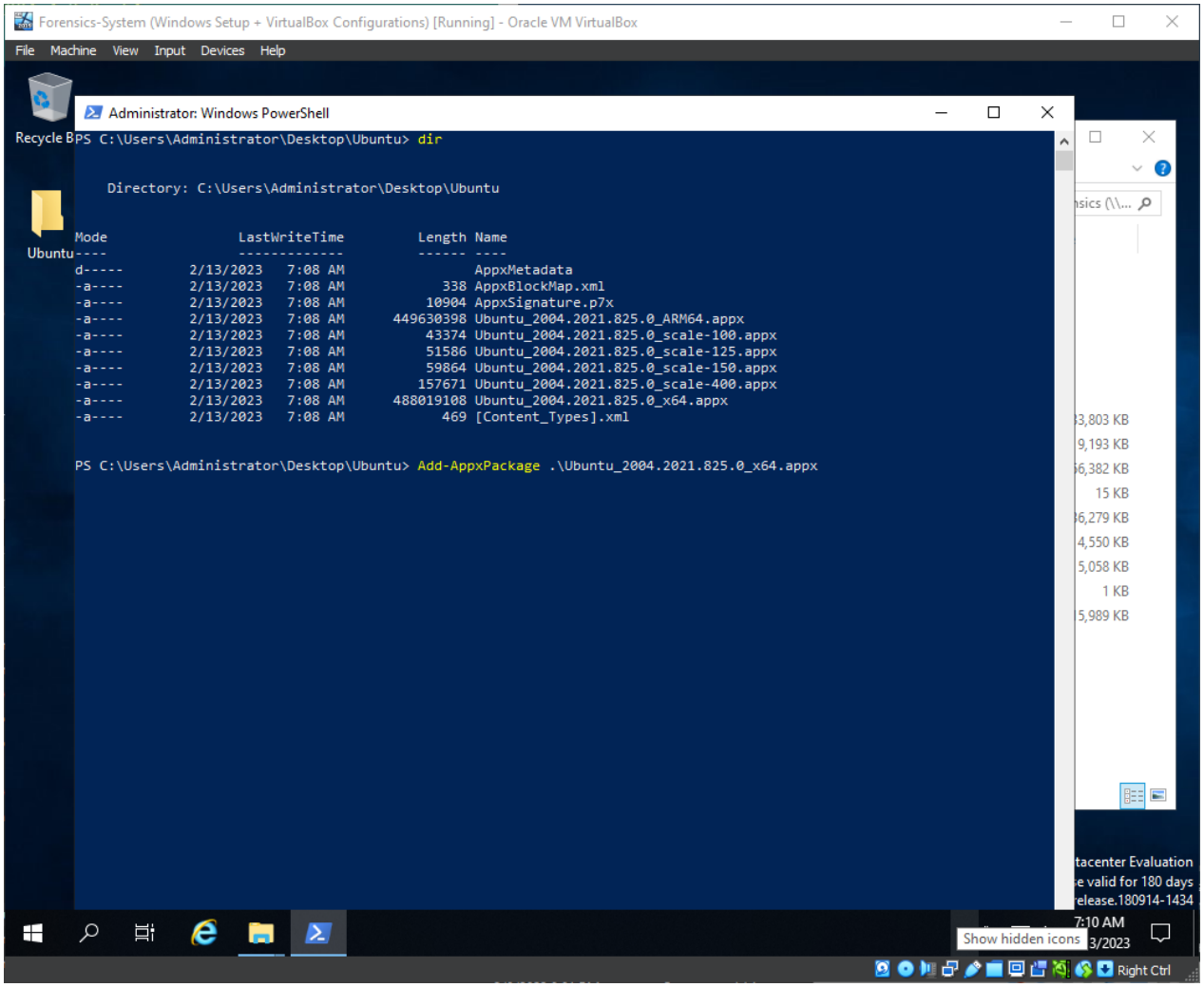


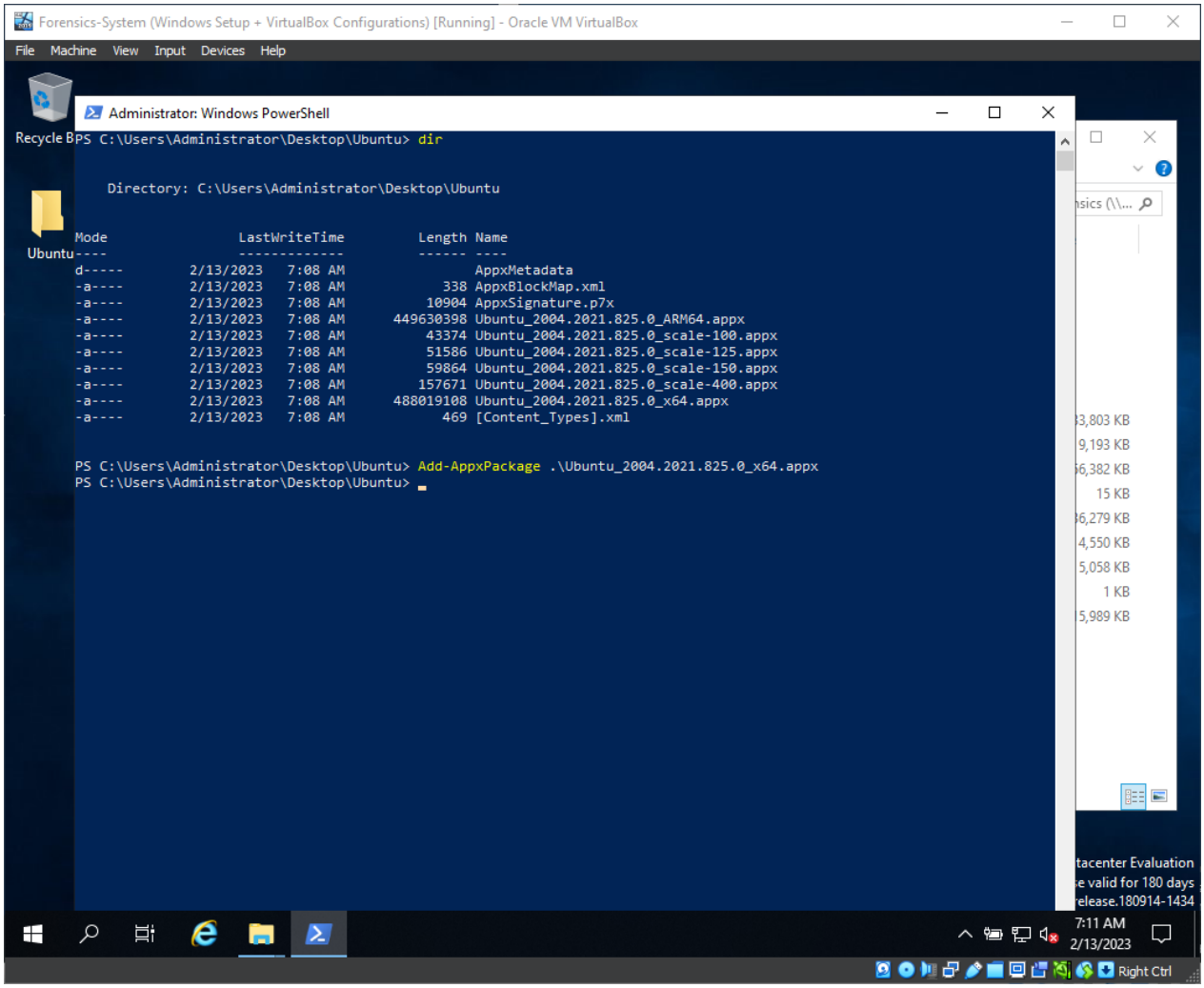
- Open a Powershell command line as administrator.



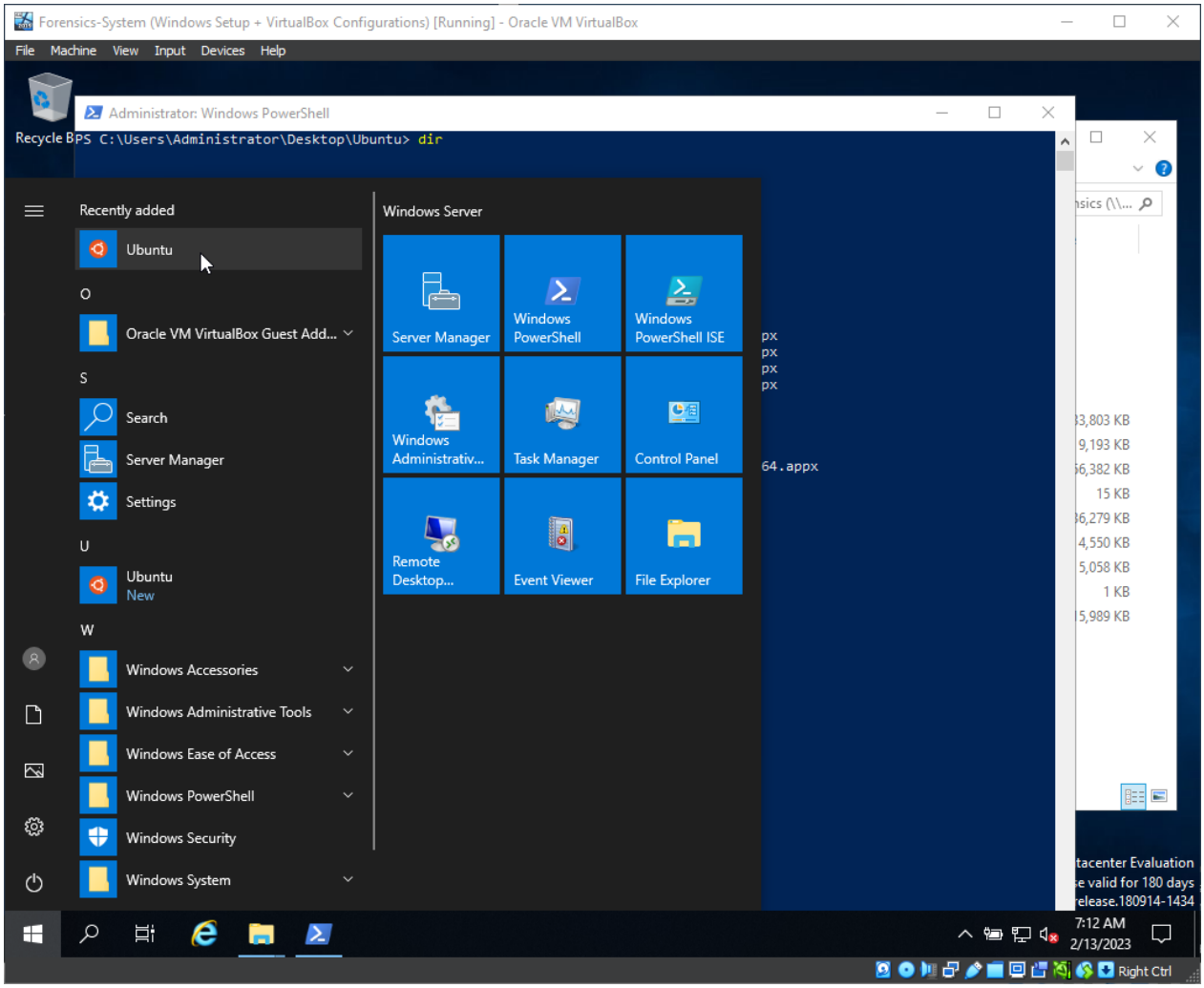
- Input the following command to add ubuntu subsystem:

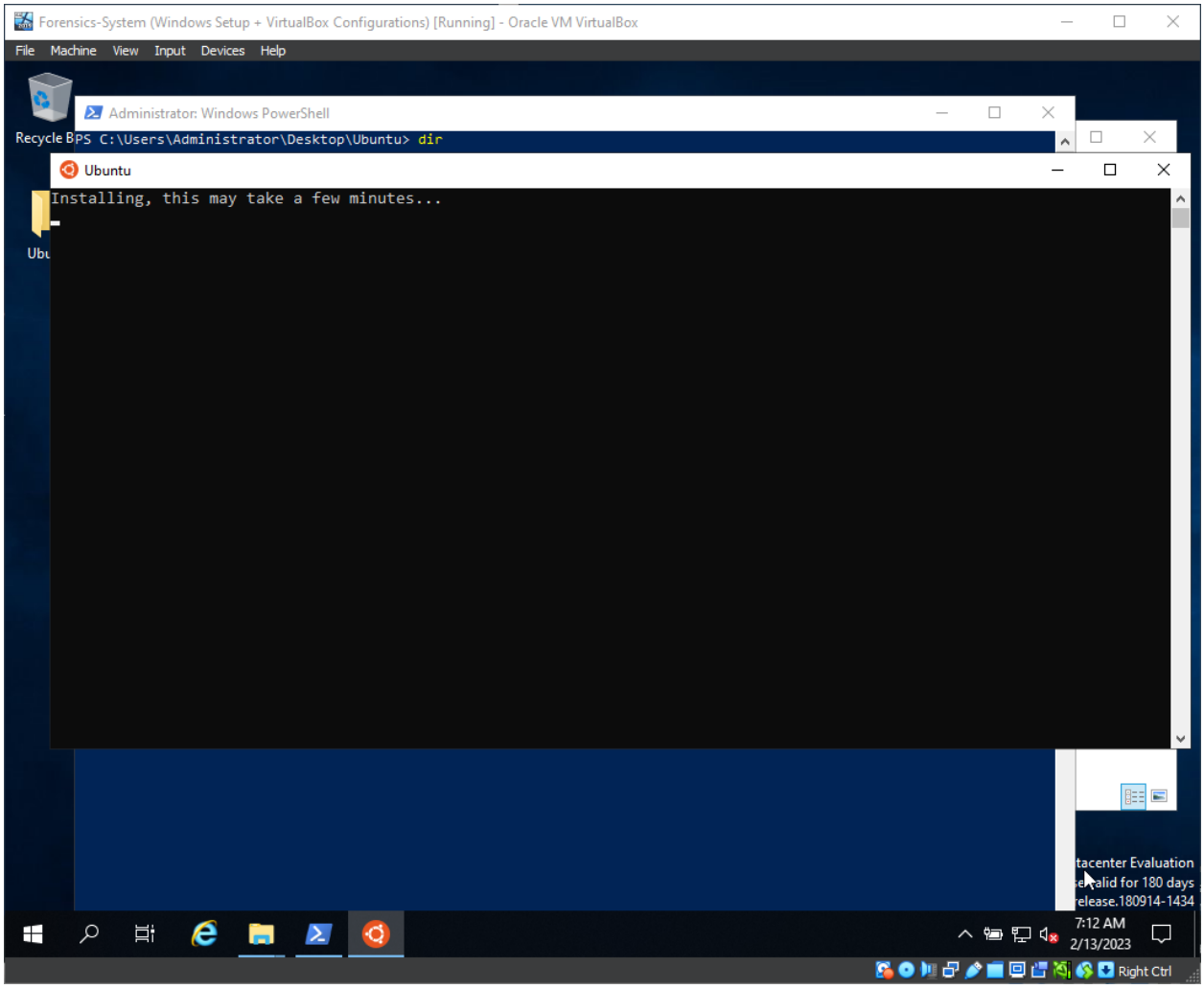
```
Add-AppxPackage .\Ubuntu_2004.2021.825.0_x64.appx
```


Forensics-System (Windows Setup + VirtualBox Configurations) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Ubuntu
Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop\Ubuntu> dir
Directory: C:\Users\Administrator\Desktop\Ubuntu
Mode LastWriteTime Length Name
d----- 2/13/2023 7:08 AM AppxMetadata
-a---- 2/13/2023 7:08 AM 338 AppxBlockMap.xml
-a---- 2/13/2023 7:08 AM 10904 AppxSignature.p7x
-a---- 2/13/2023 7:08 AM 449630398 Ubuntu_2004.2021.825.0_ARM64.appx
-a---- 2/13/2023 7:08 AM 43374 Ubuntu_2004.2021.825.0_scale-100.appx
-a---- 2/13/2023 7:08 AM 51586 Ubuntu_2004.2021.825.0_scale-125.appx
-a---- 2/13/2023 7:08 AM 59864 Ubuntu_2004.2021.825.0_scale-150.appx
-a---- 2/13/2023 7:08 AM 157671 Ubuntu_2004.2021.825.0_scale-400.appx
-a---- 2/13/2023 7:08 AM 488019108 Ubuntu_2004.2021.825.0_x64.appx
-a---- 2/13/2023 7:08 AM 469 [Content_Types].xml
PS C:\Users\Administrator\Desktop\Ubuntu> Add-AppxPackage .\Ubuntu_2004.2021.825.0_x64.appx
Show hidden icons
Right Ctrl

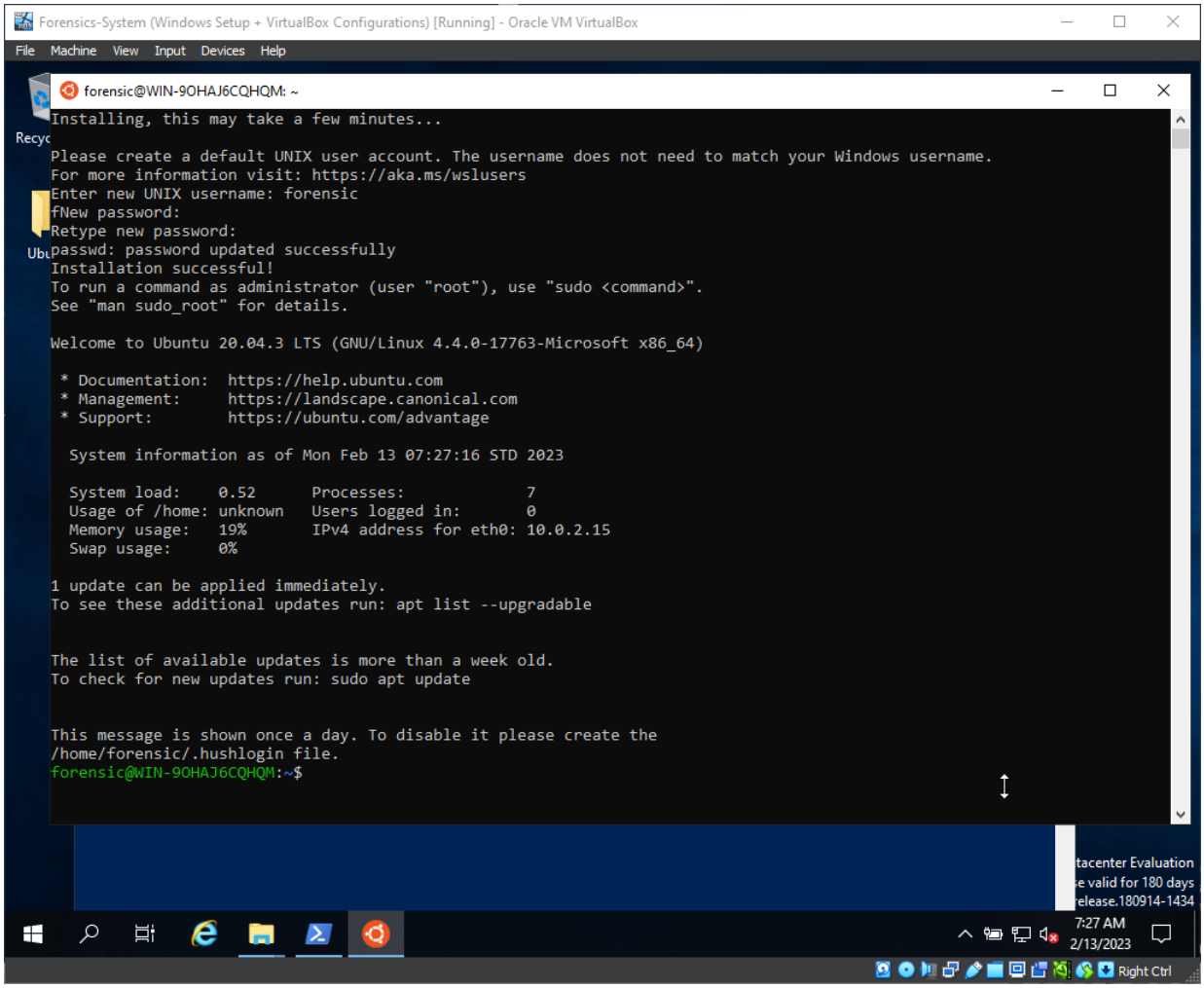


- For finishing installation you need to open the application:


Forensics-System (Windows Setup + VirtualBox Configurations) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Administrator: Windows PowerShell
PS C:\Users\Administrator\Desktop\Ubuntu> dir
Recently added
Ubuntu
O
Oracle VM VirtualBox Guest Add...
S
Search
Server Manager
Settings
U
Ubuntu
New
W
Windows Accessories
Windows Administrative Tools
Windows Ease of Access
Windows PowerShell
Windows Security
Windows System
Windows Server
Server Manager
Windows PowerShell
Windows PowerShell ISE
Windows Administrativ...
Task Manager
Control Panel
Remote Desktop...
Event Viewer
File Explorer
7:12 AM
2/13/2023
Right Ctrl

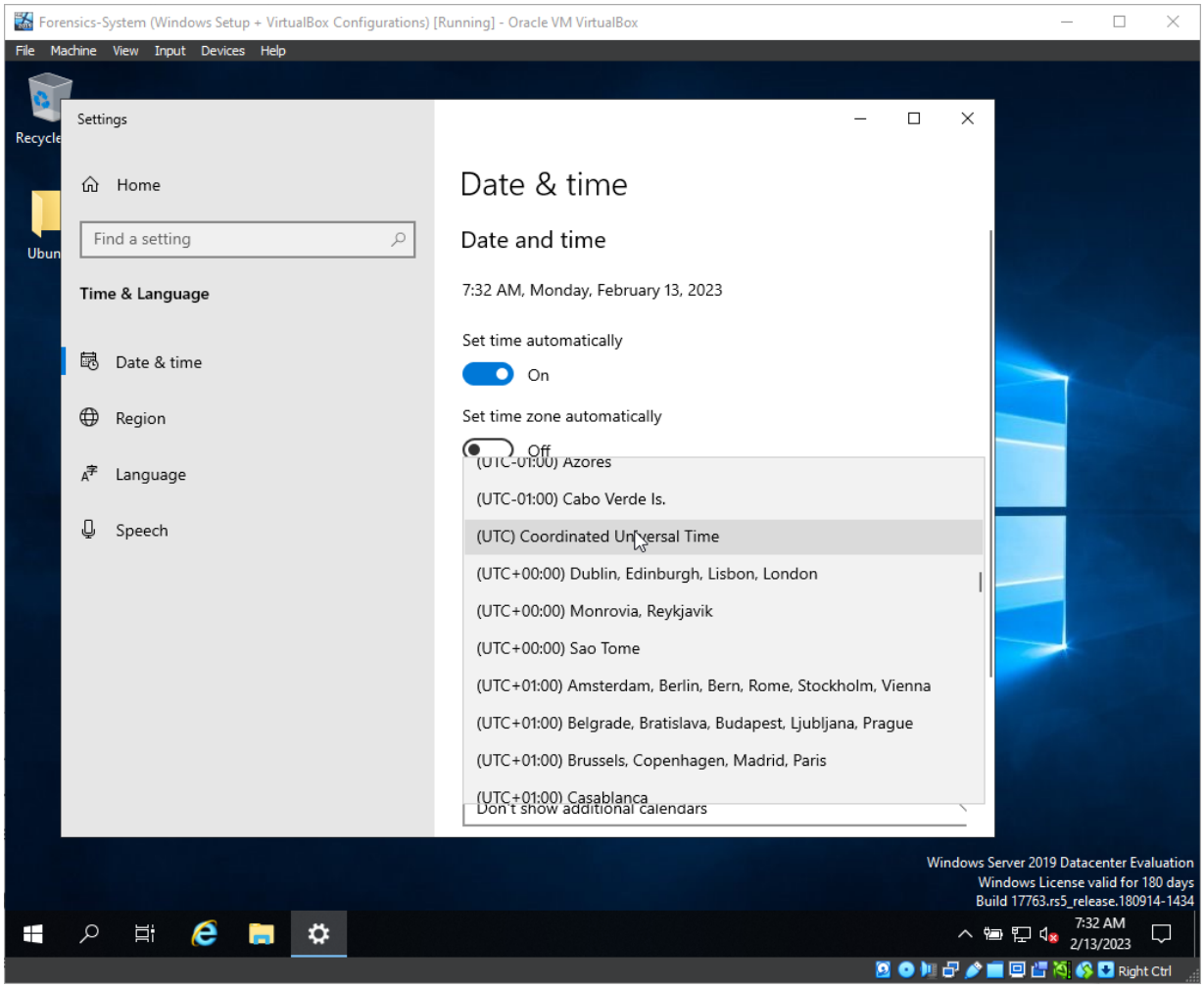


- It will take 5 to 10-15 minutes, depending to the resources of the virtual machine. To finish the installation, you need to enter an username and password, in my case I used forensic/forensic.

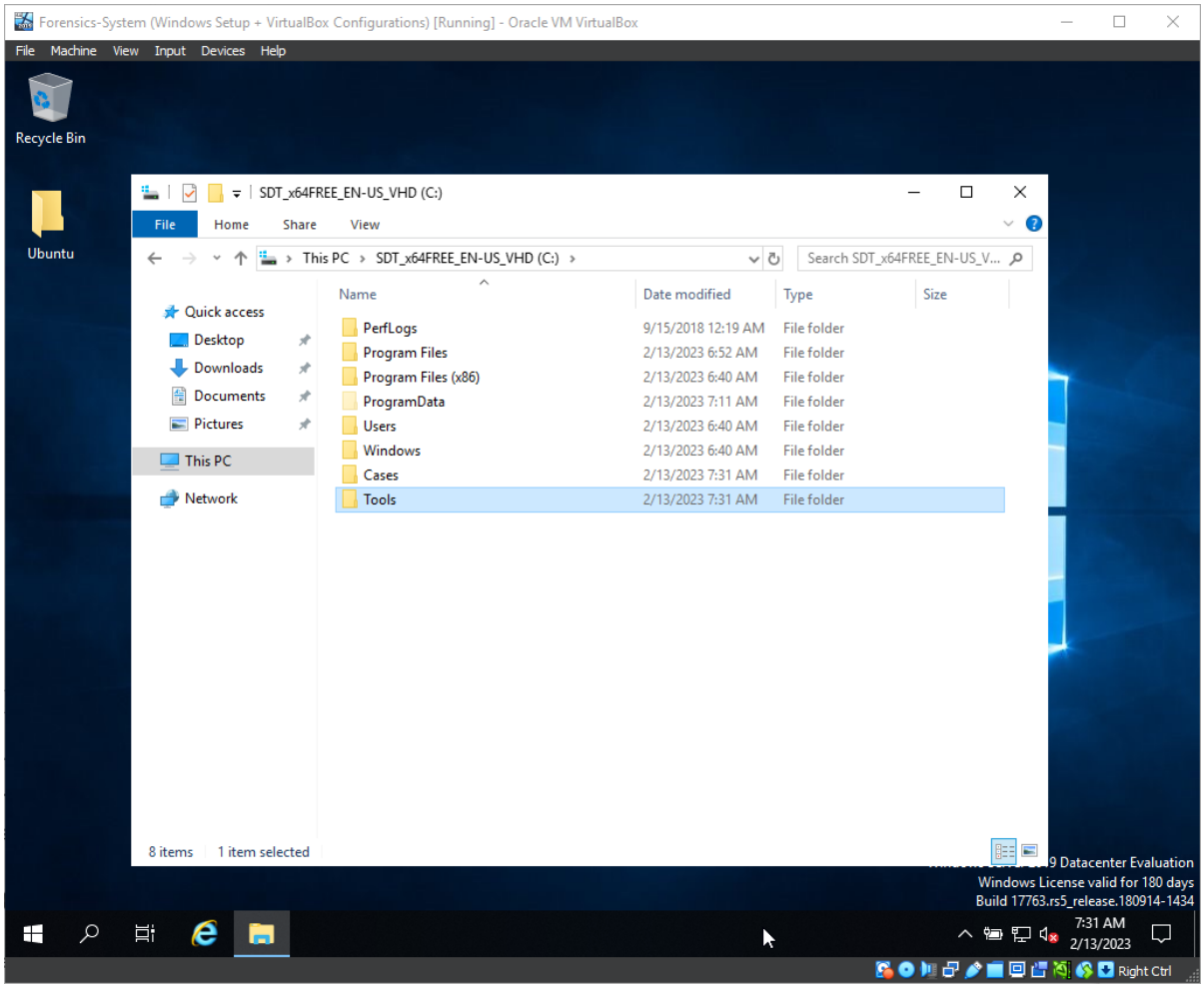


Configuration for Forensics virtual machine

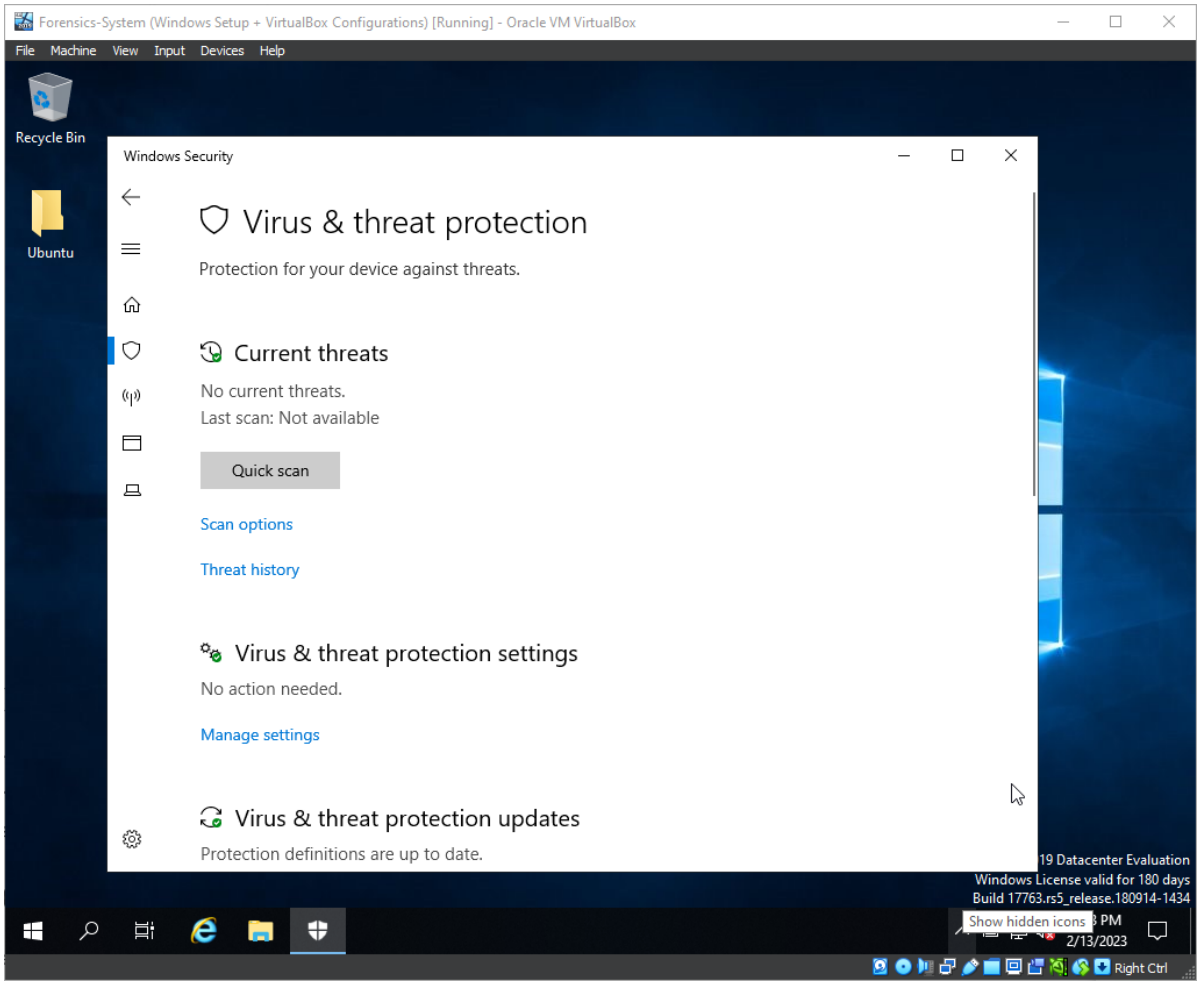
- Change time to UTC, this is a general best practice for working with forensic analysis.

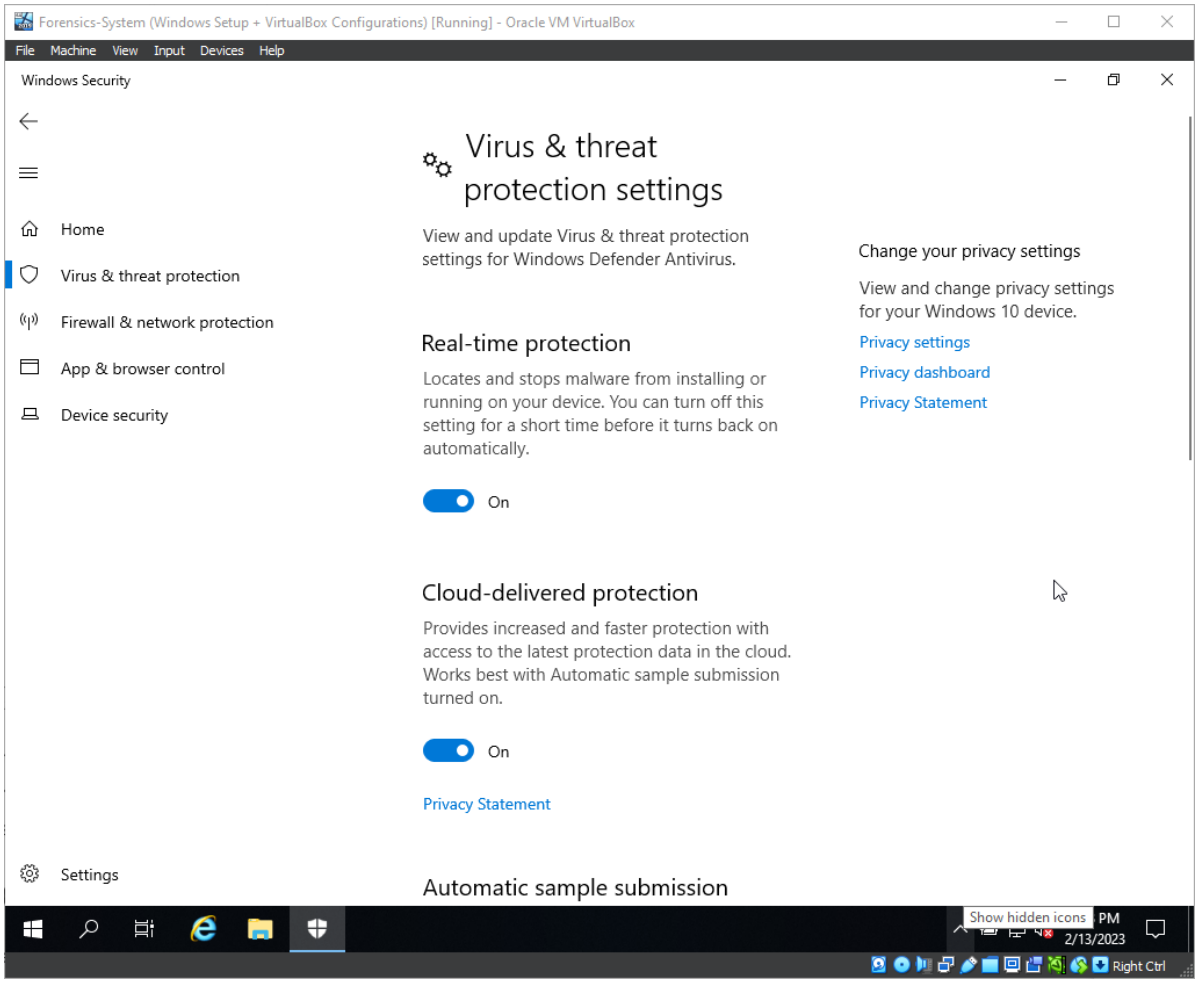


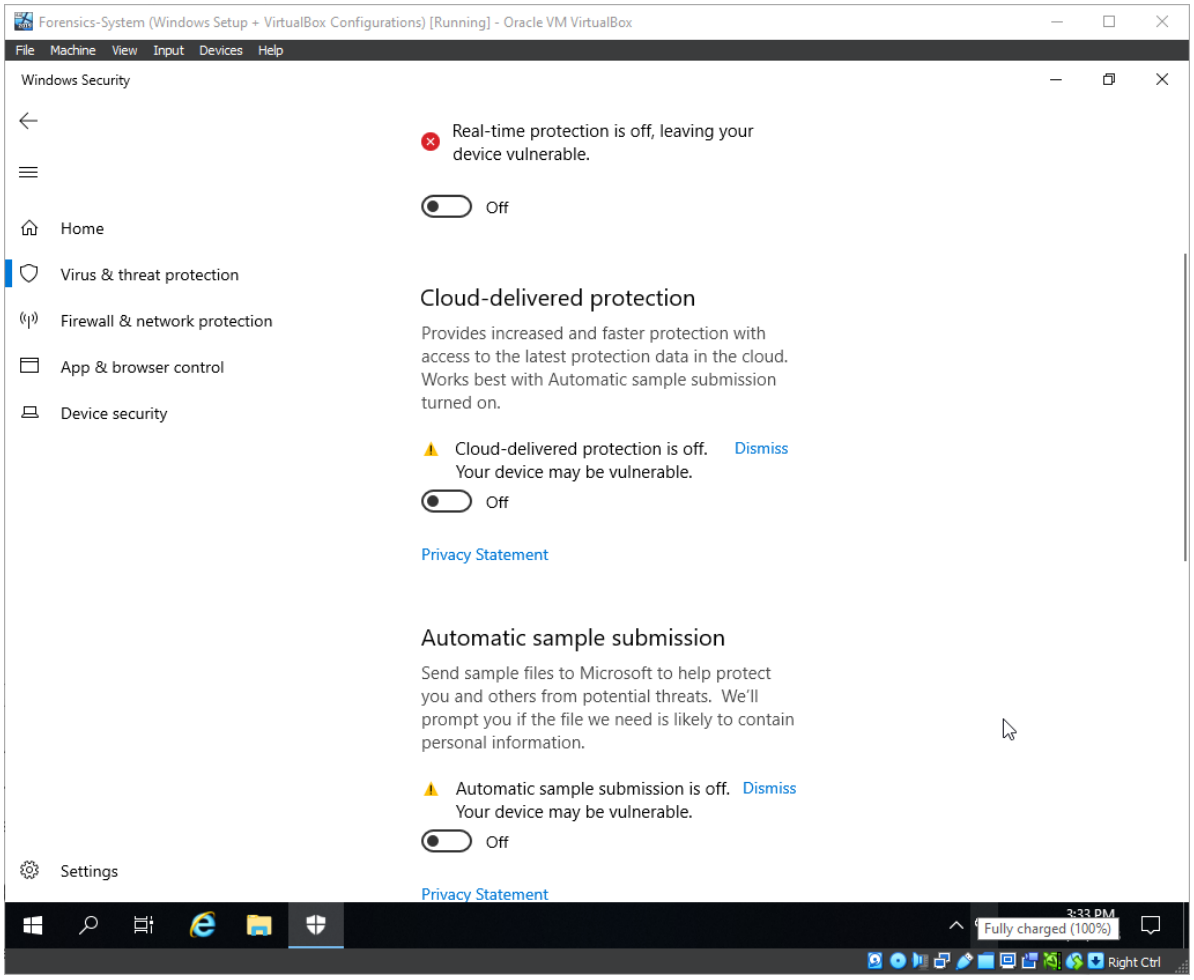
- Create two folders for Cases and Tools.



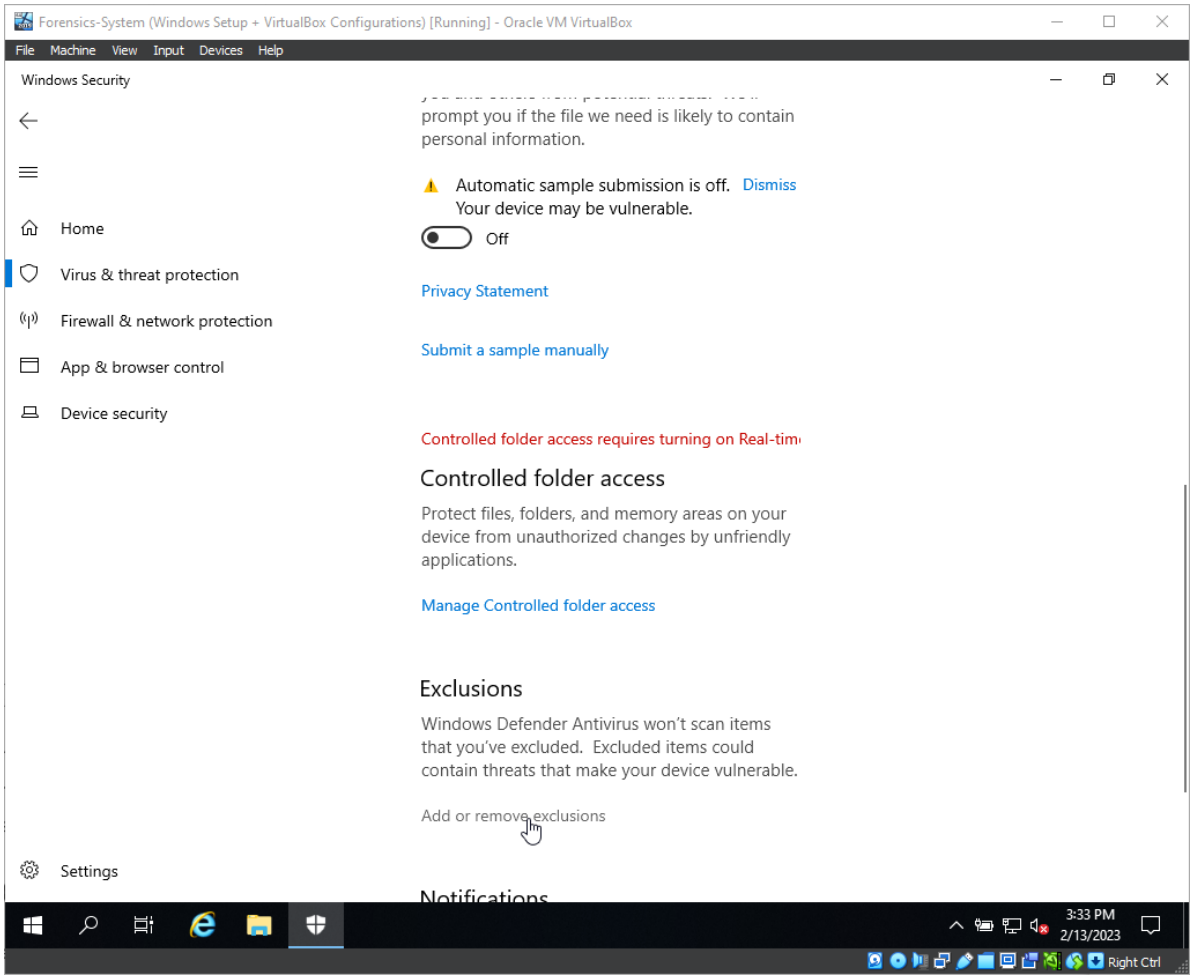
- Disable all protection in Windows Security>Virus & threat protection.

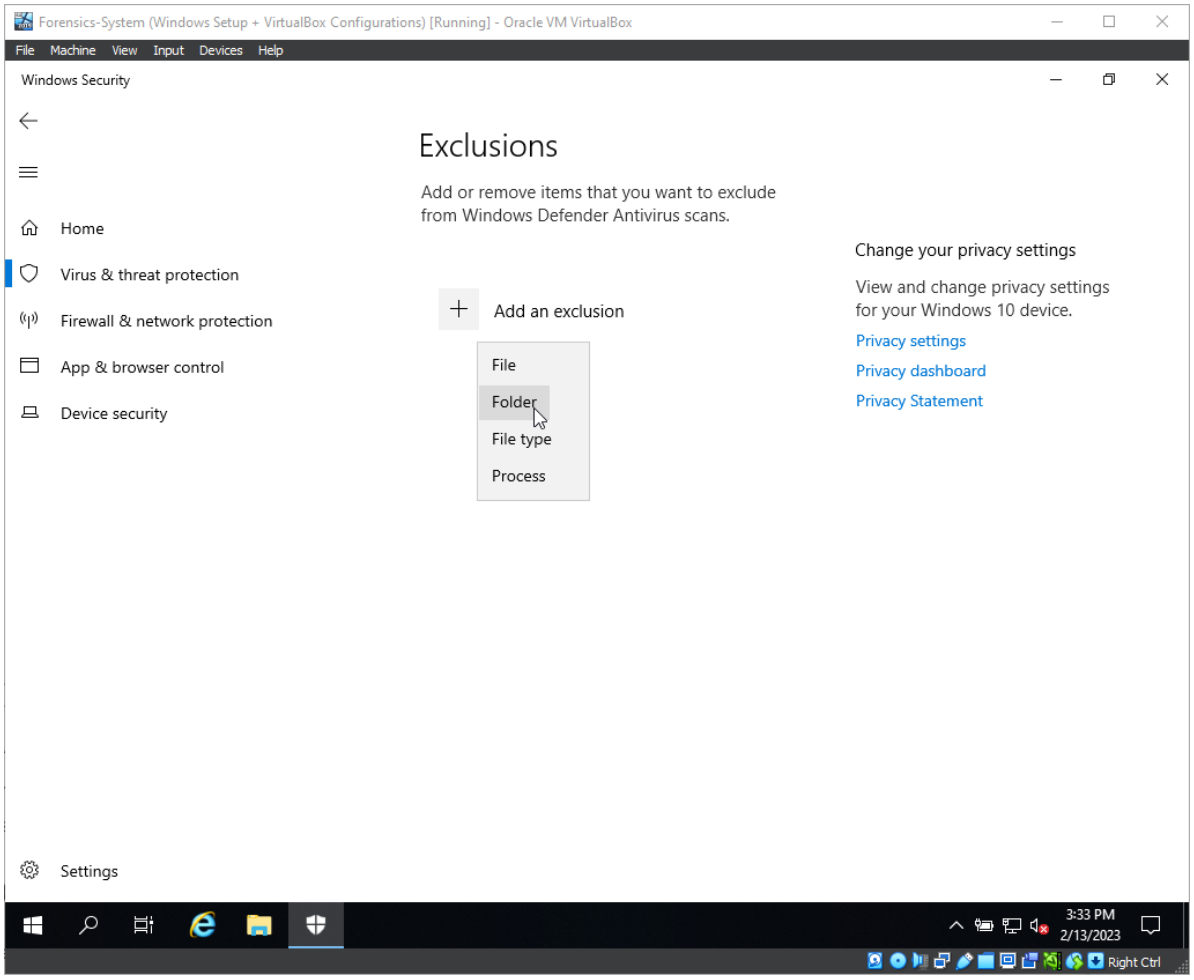

Forensics-System (Windows Setup + VirtualBox Configurations) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Ubuntu
Windows Security
Virus & threat protection
Protection for your device against threats.
Current threats
No current threats.
Last scan: Not available
Quick scan
Scan options
Threat history
Virus & threat protection settings
No action needed.
Manage settings
Virus & threat protection updates
Protection definitions are up to date.
19 Datacenter Evaluation
Windows License valid for 180 days
Build 17763.rs5_release.180914-1434
Show hidden icons
2/13/2023
Right Ctrl

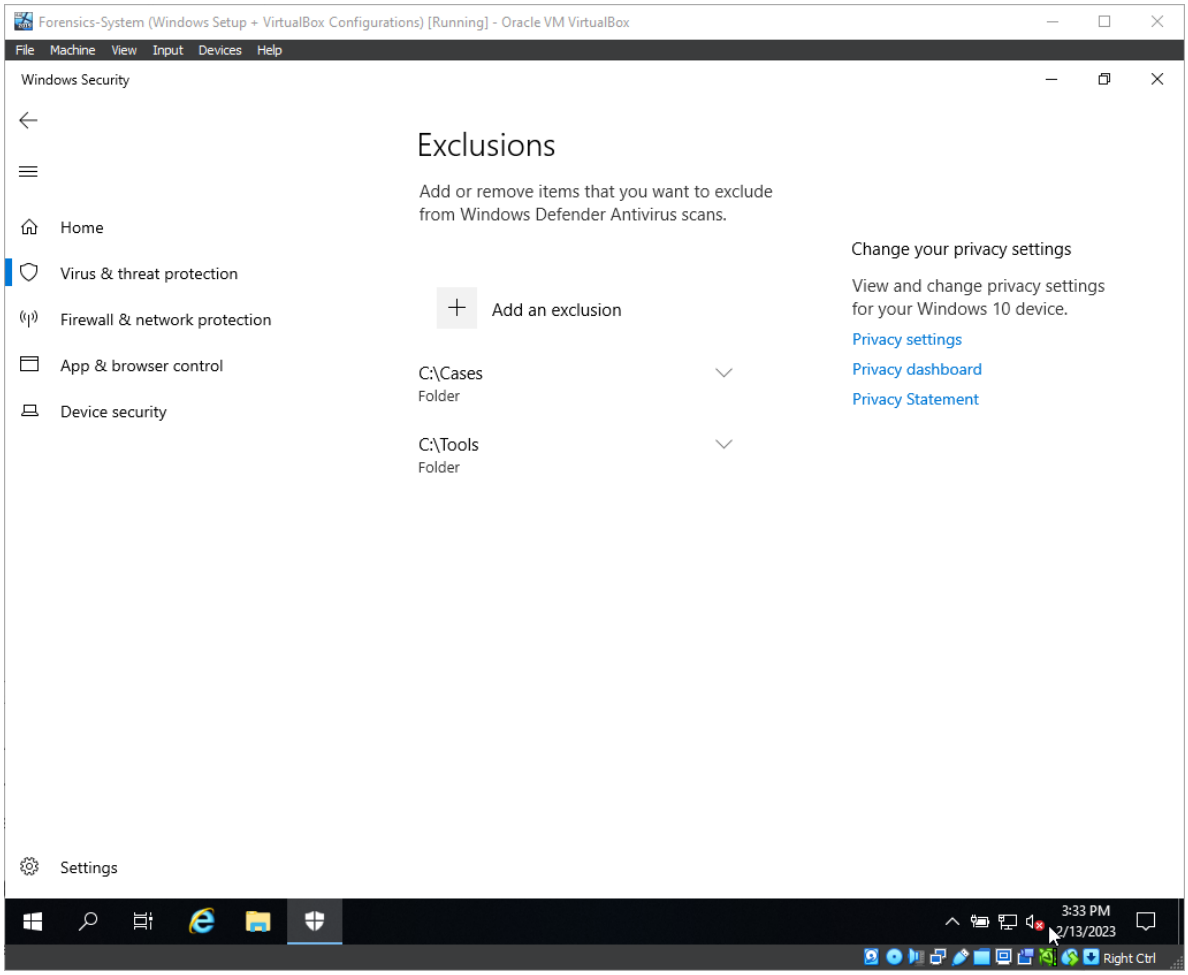

Forensics-System (Windows Setup + VirtualBox Configurations) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows Security
Home
Virus & threat protection
Firewall & network protection
App & browser control
Device security
Settings
Virus & threat protection settings
View and update Virus & threat protection settings for Windows Defender Antivirus.
Real-time protection
Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.
On
Cloud-delivered protection
Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.
On
Privacy Statement
Automatic sample submission
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement
Show hidden icons
PM
2/13/2023
Right Ctrl



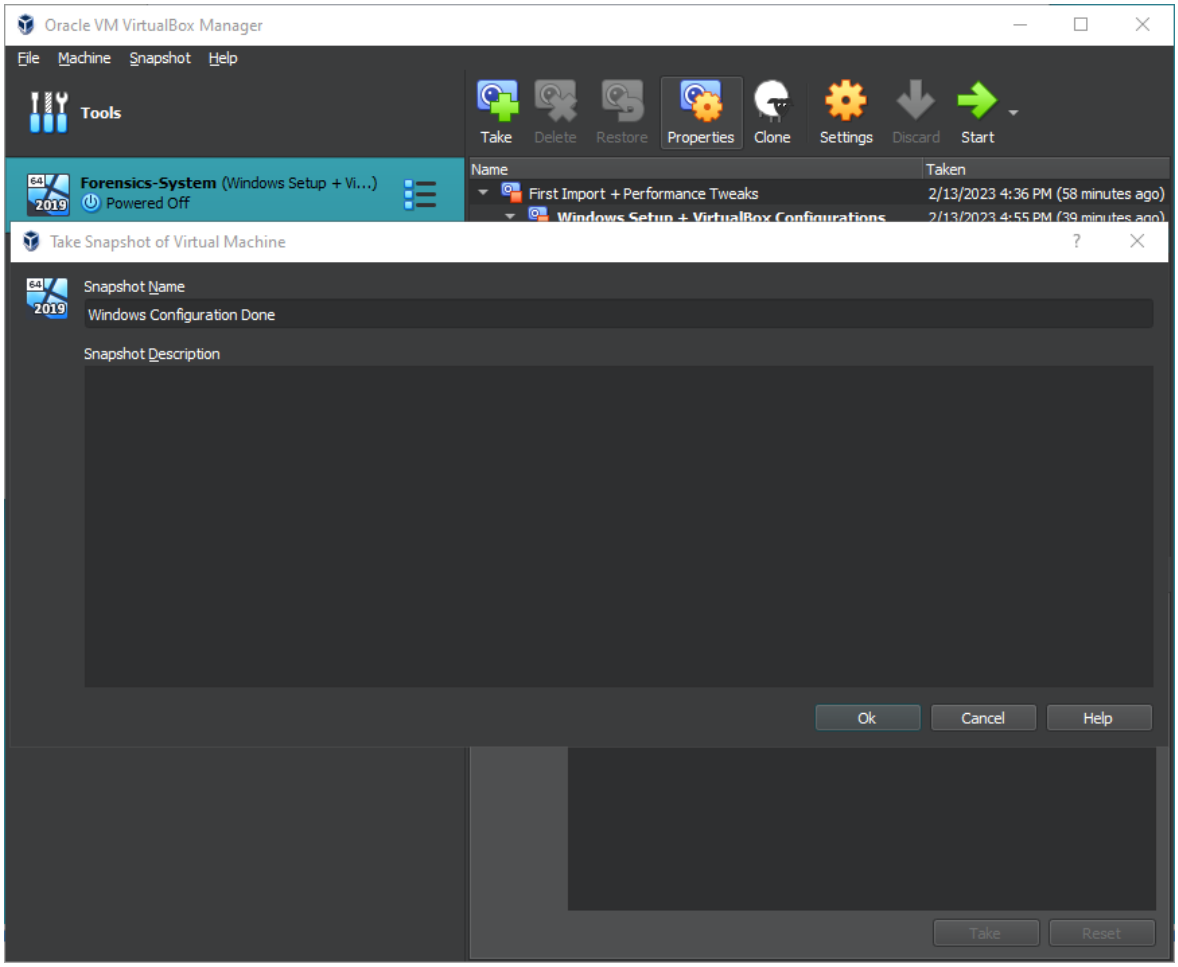
- Exclude the two folders from above from protection scanning, because Windows Security will delete right away all types of files that could be compromisable.


Forensics-System (Windows Setup + VirtualBox Configurations) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows Security
prompt you if the file we need is likely to contain personal information.
Automatic sample submission is off. Dismiss
Your device may be vulnerable.
Off
Privacy Statement
Submit a sample manually
Controlled folder access requires turning on Real-tim
Controlled folder access
Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.
Manage Controlled folder access
Exclusions
Windows Defender Antivirus won't scan items that you've excluded. Excluded items could contain threats that make your device vulnerable.
Add or remove exclusions
Notifications
Home
Virus & threat protection
Firewall & network protection
App & browser control
Device security
Settings
3:33 PM
2/13/2023
Right Ctrl


Forensics-System (Windows Setup + VirtualBox Configurations) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows Security
Exclusions
Add or remove items that you want to exclude from Windows Defender Antivirus scans.
Home
Virus & threat protection
Firewall & network protection
App & browser control
Device security
Settings
Add an exclusion
File
Folder
File type
Process
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement
3:33 PM
2/13/2023
Right Ctrl



- Shut down the virtual machine and take a snapshot.



Installing Forensic Tools.

- We will need the following tools (Make sure you use a browser without adblocking feature, that will interfere with the downloading of some of the tools enumerated below):
    - Arsenal Image Mounter:

https://arsenalrecon.com/downloads

    - Eric Zimmerman Tools:

https://ericzimmerman.github.io/#!index.md

    - Event Log Explorer:

https://eventlogxp.com/

    - KAPE:

https://www.kroll.com/en/insights/publications/cyber/kroll-artifact-parser-extractor-kape

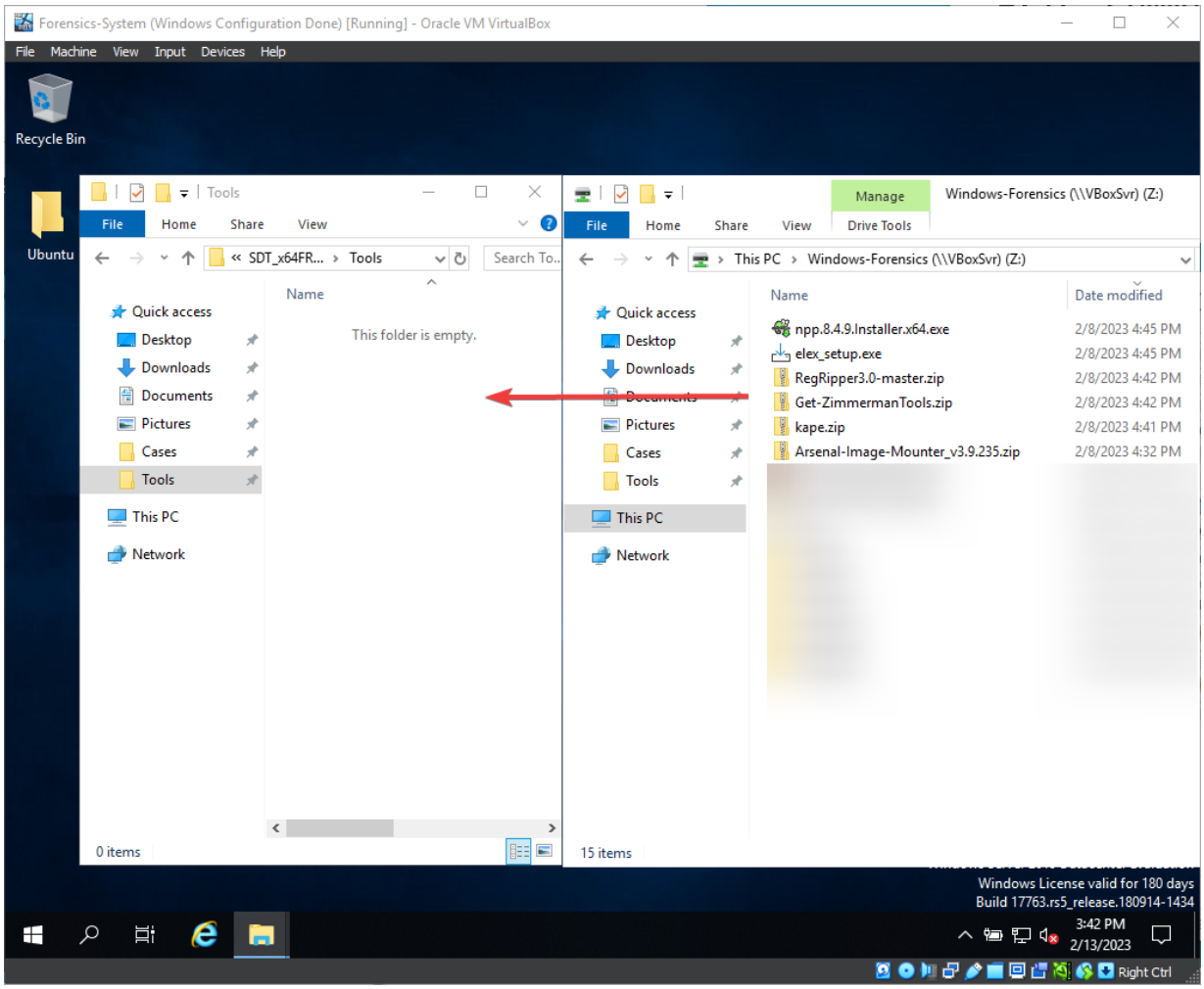
- Notepad++:

https://notepad-plus-plus.org/downloads/

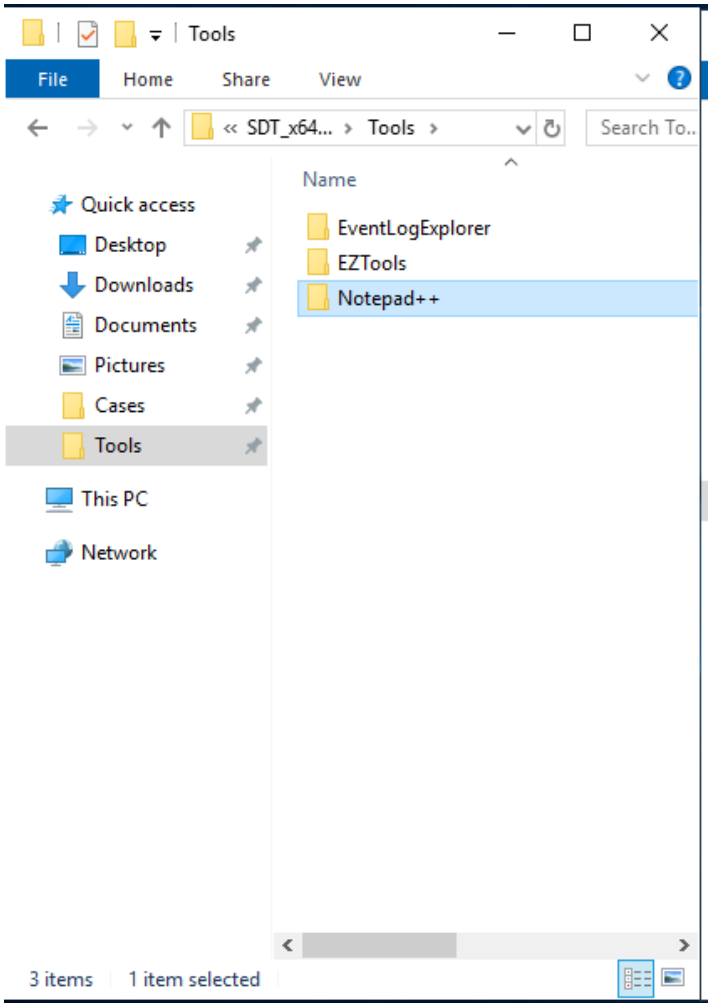
- RegRipper 3.0:

https://github.com/keydet89/RegRipper3.0

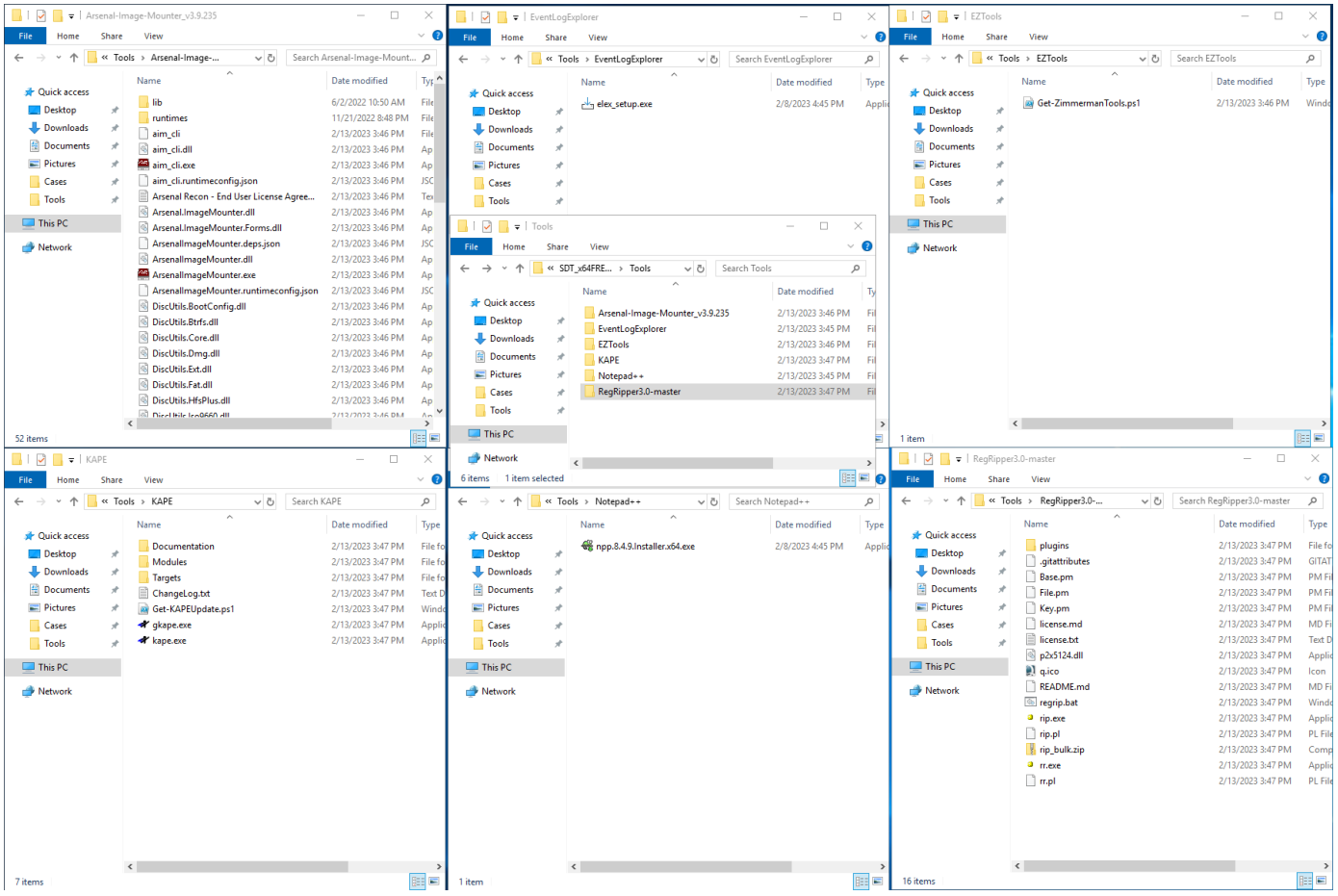
- Extract to C:\Tools.



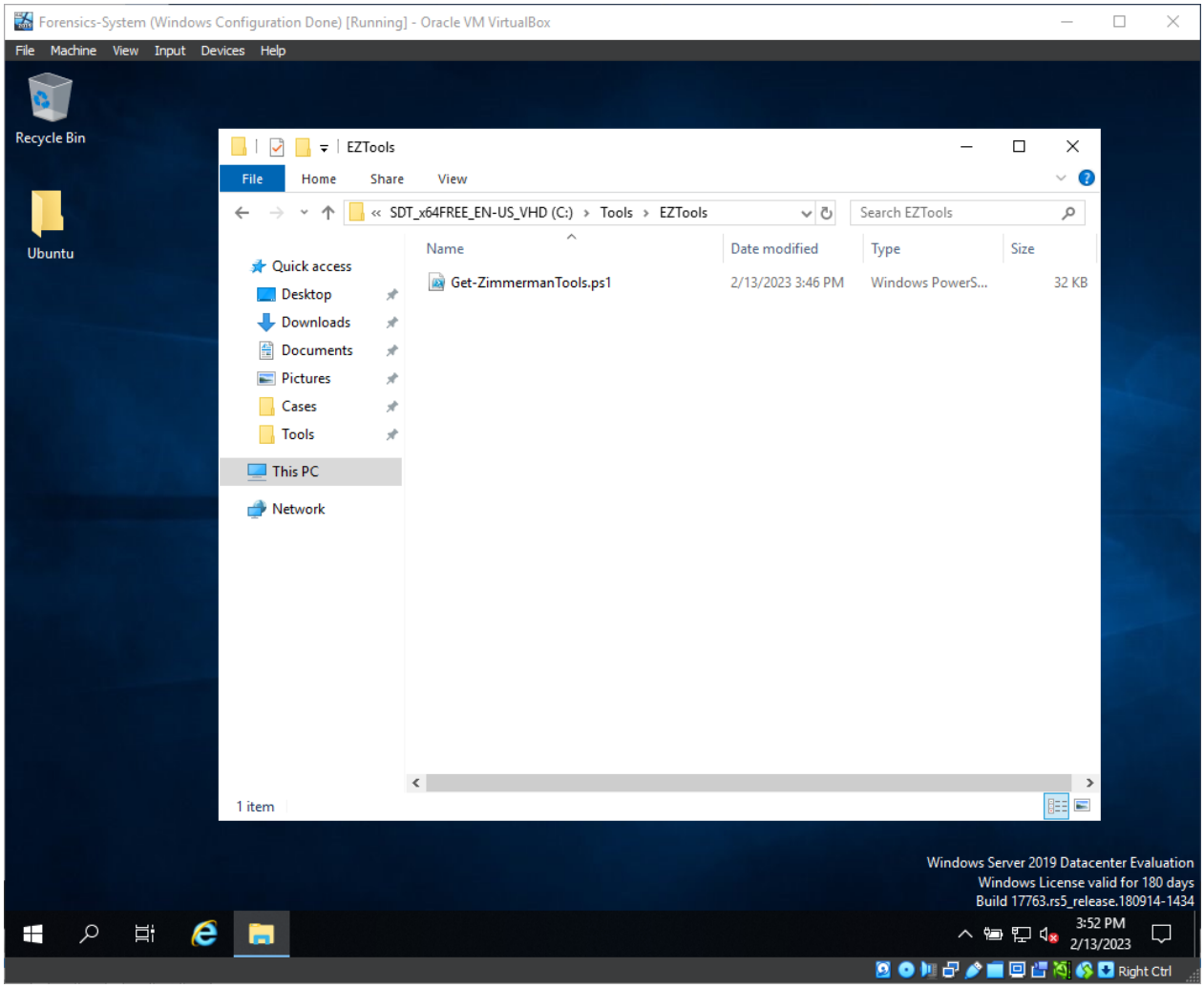
- Create Folders under C:\Tools (for structure purposes):
  - EventLogExplorer.
  - EZTools.
  - Notepad++.

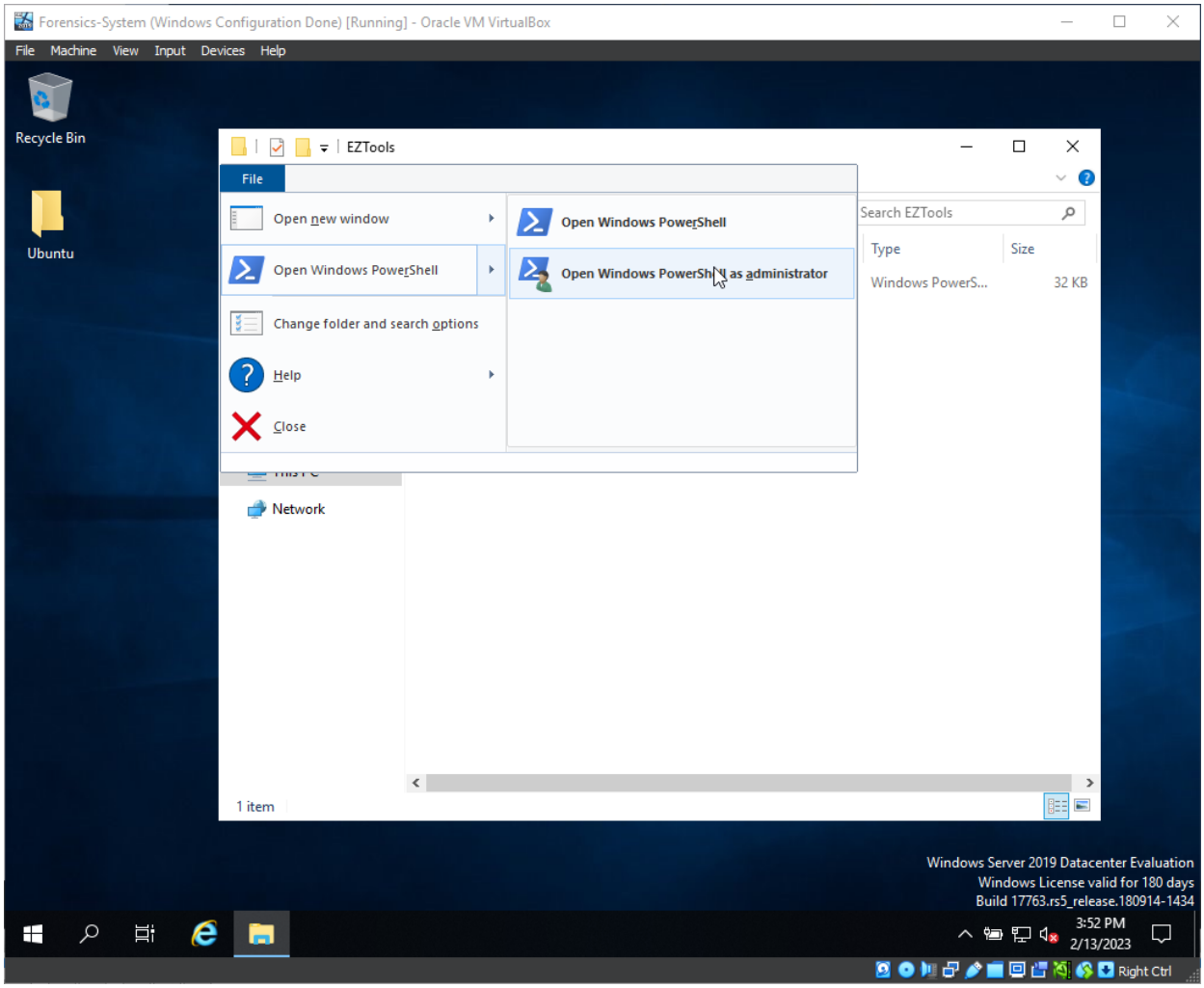


- Copy and paste/Extract installation executables and scripts in above folders.
- Extract to C:\Tools , the remaining ones.
- Folder structure you should have.

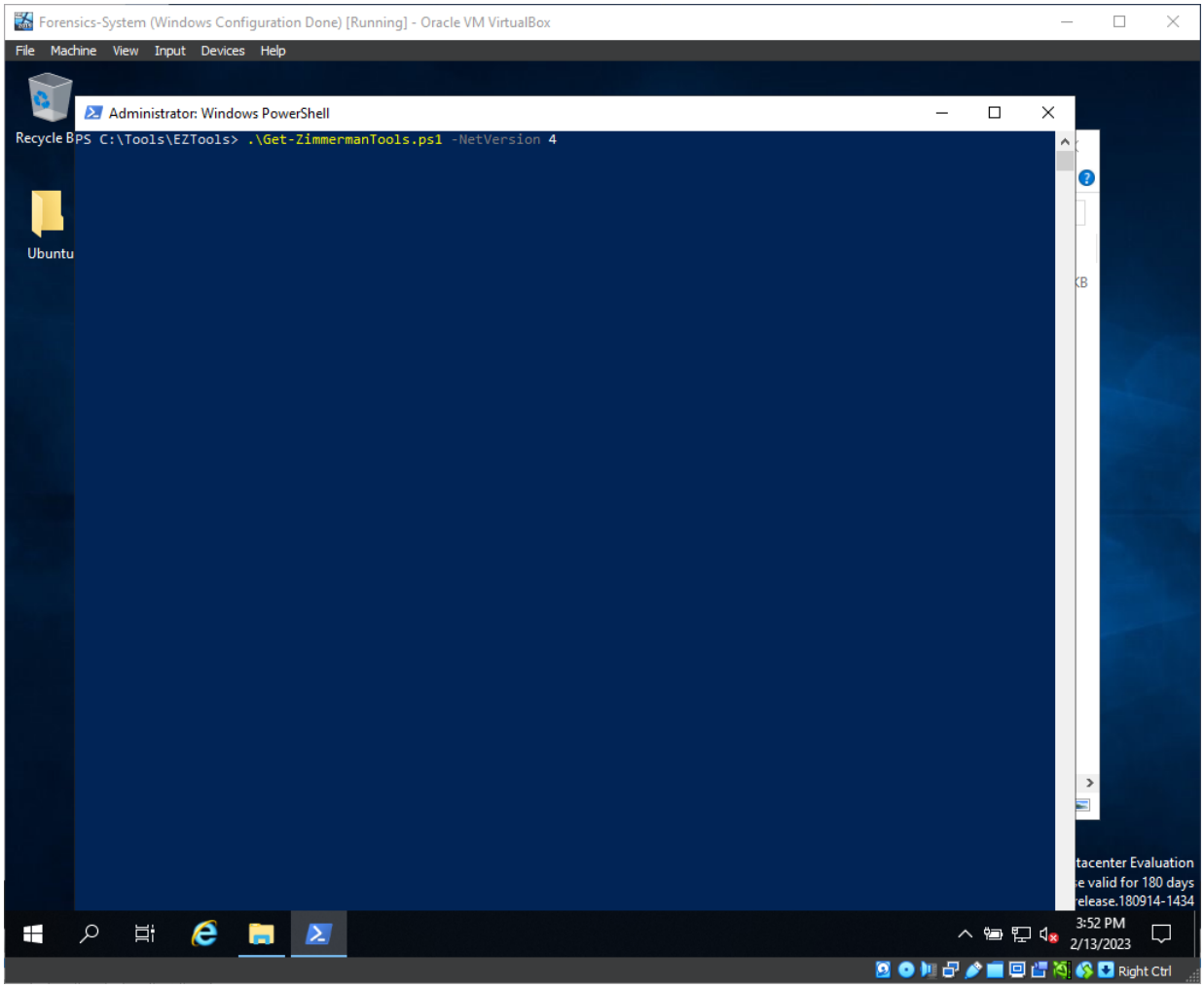


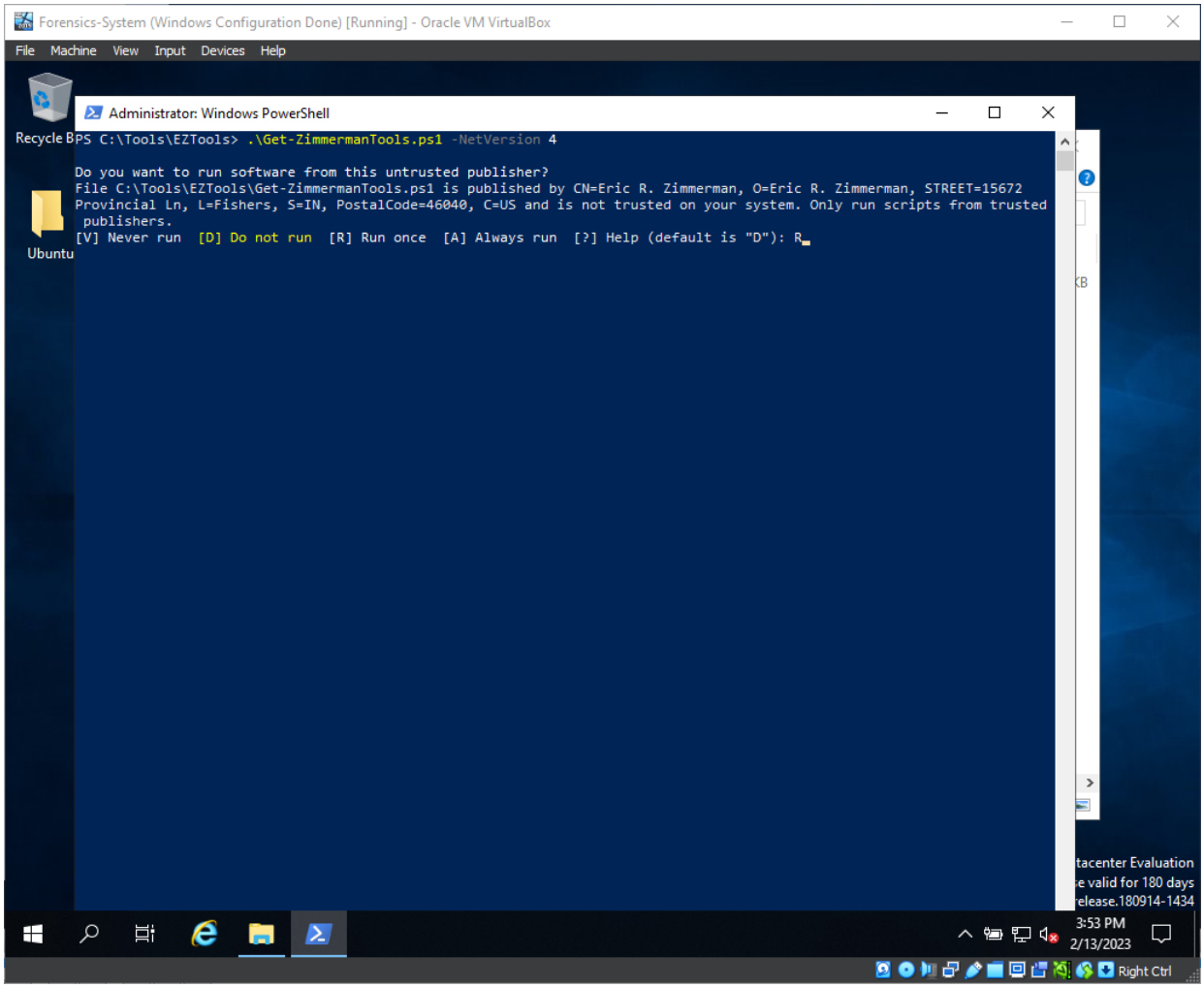
- Installation for EZTools:

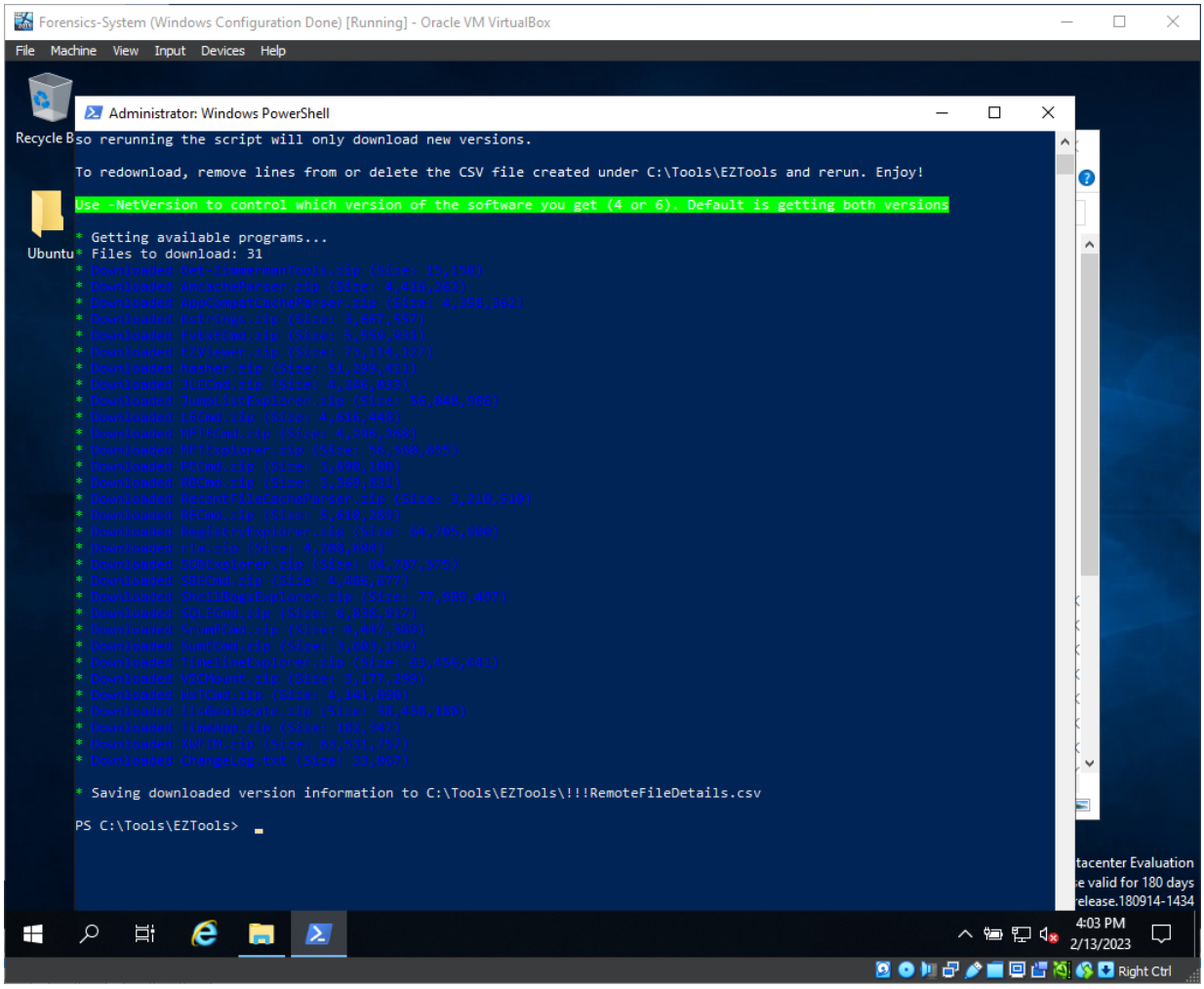

Forensics-System (Windows Configuration Done) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Ubuntu
EZTools
File Home Share View
SDT_x64FREE_EN-US_VHD (C:) › Tools › EZTools
Search EZTools
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
Name
Date modified
Type
Size
Get-ZimmermanTools.ps1
2/13/2023 3:46 PM
Windows PowerS...
32 KB
1 item
Windows Server 2019 Datacenter Evaluation
Windows License valid for 180 days
Build 17763.rs5_release.180914-1434
3:52 PM
2/13/2023
Right Ctrl



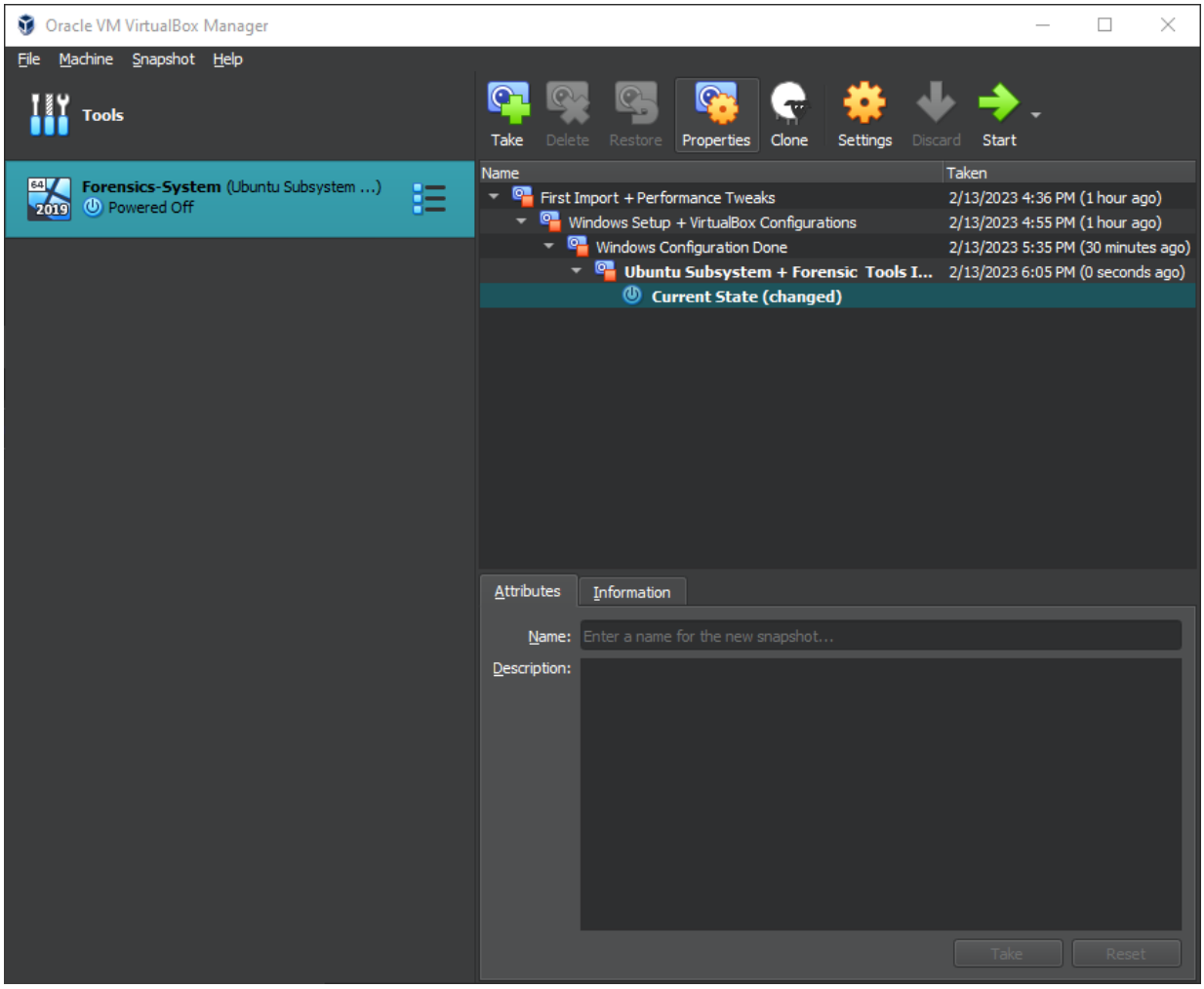
.\Get-ZimmermanTools.ps1 -NetVersion 4


Forensics-System (Windows Configuration Done) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Ubuntu
Administrator: Windows PowerShell
PS C:\Tools\EZTools> .\Get-ZimmermanTools.ps1 -NetVersion 4
tacenter Evaluation
e valid for 180 days
release.180914-1434
3:52 PM
2/13/2023
Right Ctrl


Forensics-System (Windows Configuration Done) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Ubuntu
Administrator: Windows PowerShell
PS C:\Tools\EZTools> .\Get-ZimmermanTools.ps1 -NetVersion 4
Do you want to run software from this untrusted publisher?
File C:\Tools\EZTools\Get-ZimmermanTools.ps1 is published by CN=Eric R. Zimmerman, O=Eric R. Zimmerman, STREET=15672 Provincial Ln, L=Fishers, S=IN, PostalCode=46040, 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"): R
tacenter Evaluation
e valid for 180 days
release.180914-1434
3:53 PM
2/13/2023
Right Ctrl



- For EventLogExplorer and Notepad++, there is no advanced installation, just next untill finish.
- Make a snapshot.


Oracle VM VirtualBox Manager
File Machine Snapshot Help
Tools
Forensics-System (Ubuntu Subsystem ...)
Powered Off
Take Delete Restore Properties Clone Settings Discard Start
Name Taken
First Import + Performance Tweaks 2/13/2023 4:36 PM (1 hour ago)
Windows Setup + VirtualBox Configurations 2/13/2023 4:55 PM (1 hour ago)
Windows Configuration Done 2/13/2023 5:35 PM (30 minutes ago)
Ubuntu Subsystem + Forensic Tools I... 2/13/2023 6:05 PM (0 seconds ago)
Current State (changed)
Attributes Information
Name: Enter a name for the new snapshot...
Description:
Take Reset