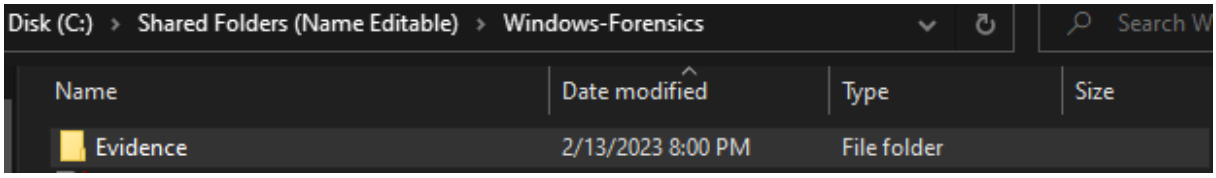
Data Examination Process:

- Monting the disk image.
- Windows files and forensics artifacts.
- Triage data.

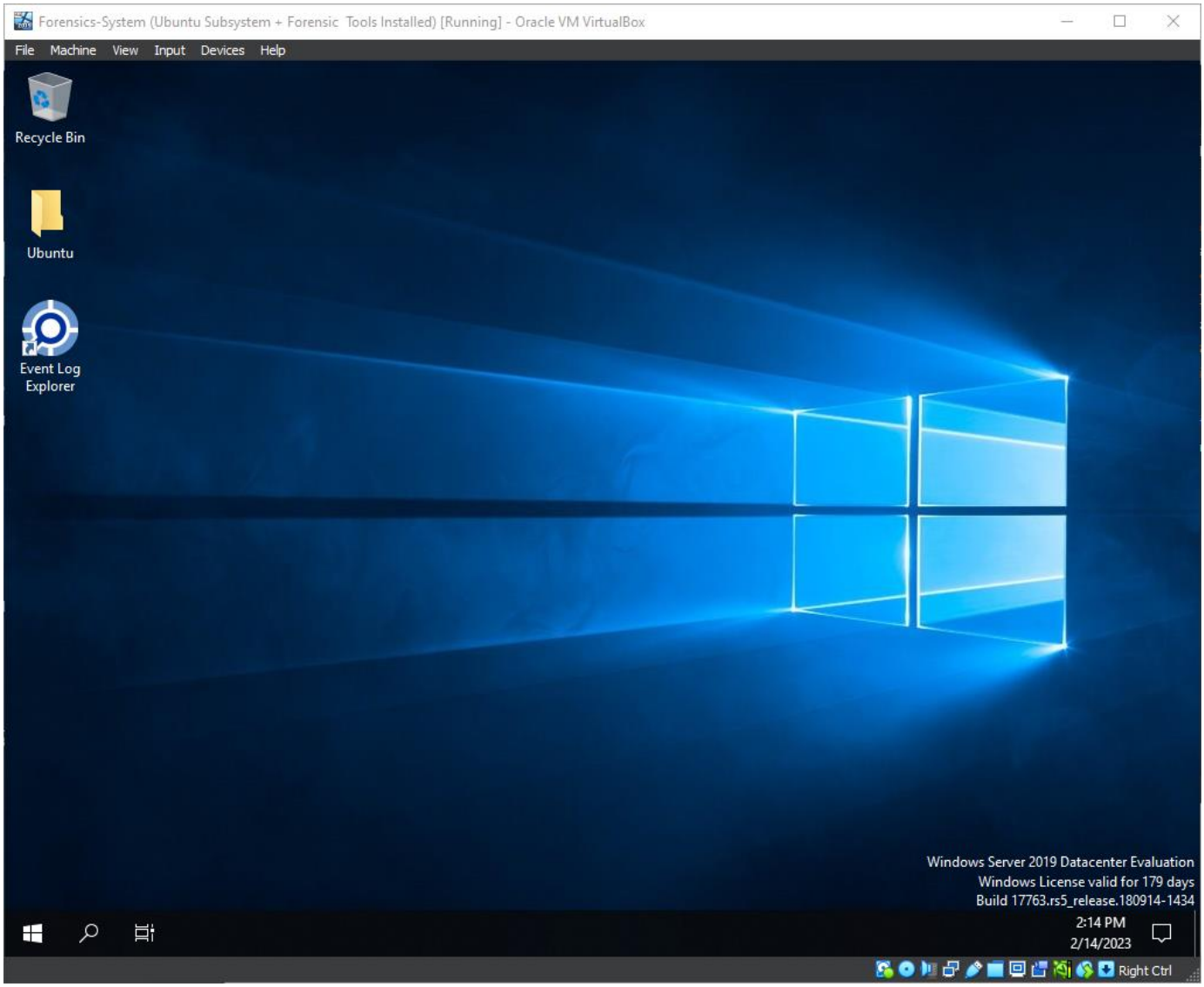
- Examination needs:
    - Data assessment.
    - Data extraction.

Monting the disk image

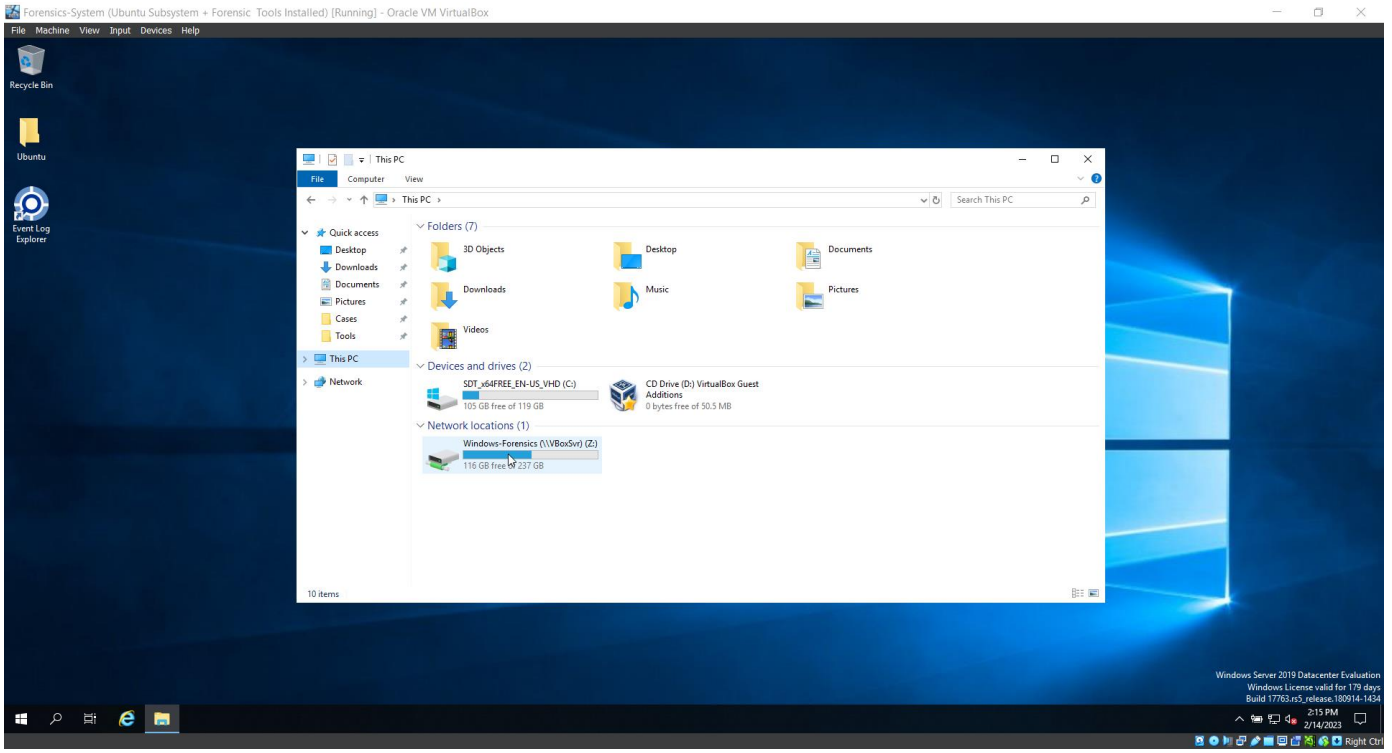
- First, move Evidence folder with the gathered data in the shared folder with the forensics workstation virtual machine:

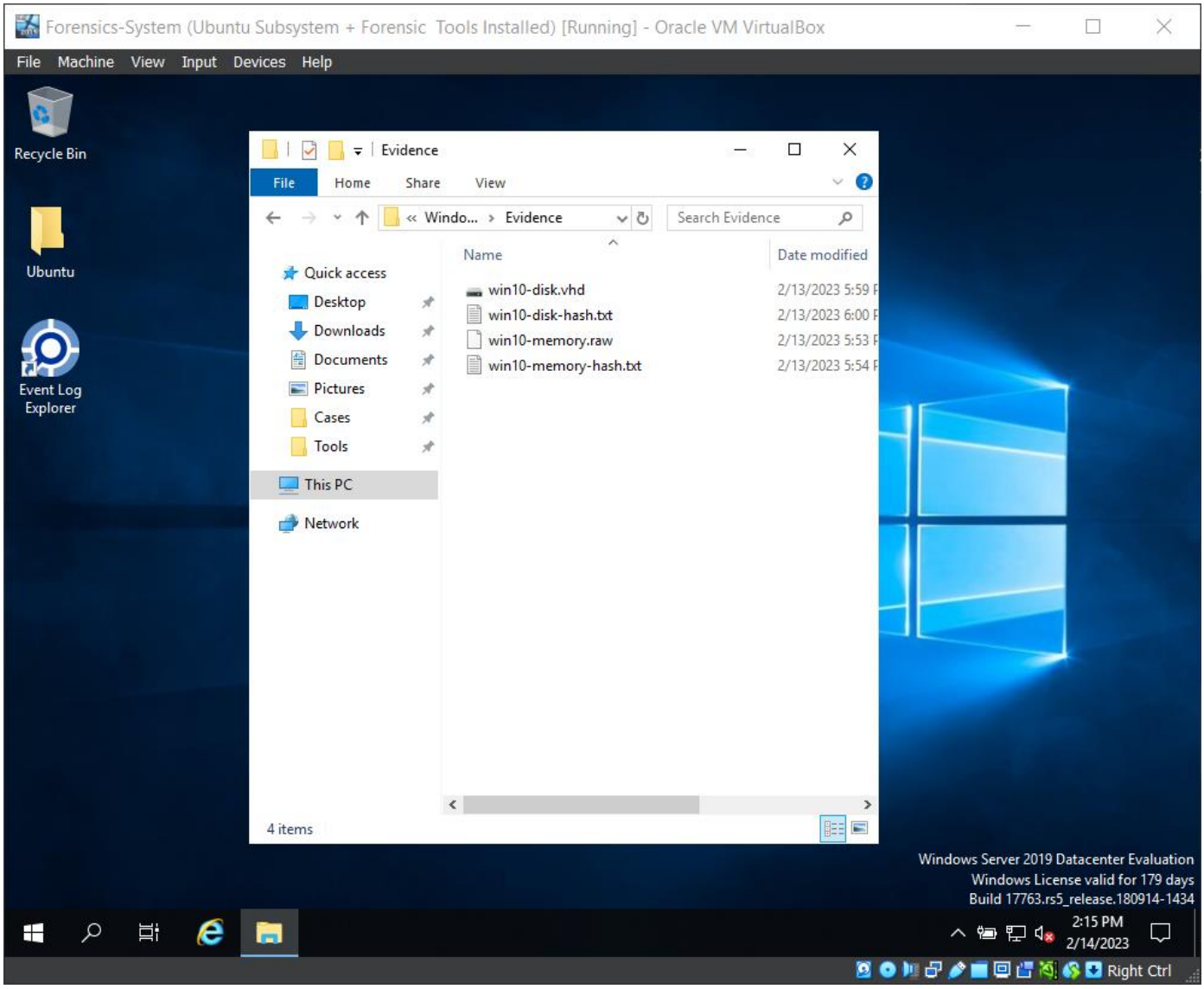


- Start forensic virtual machine:



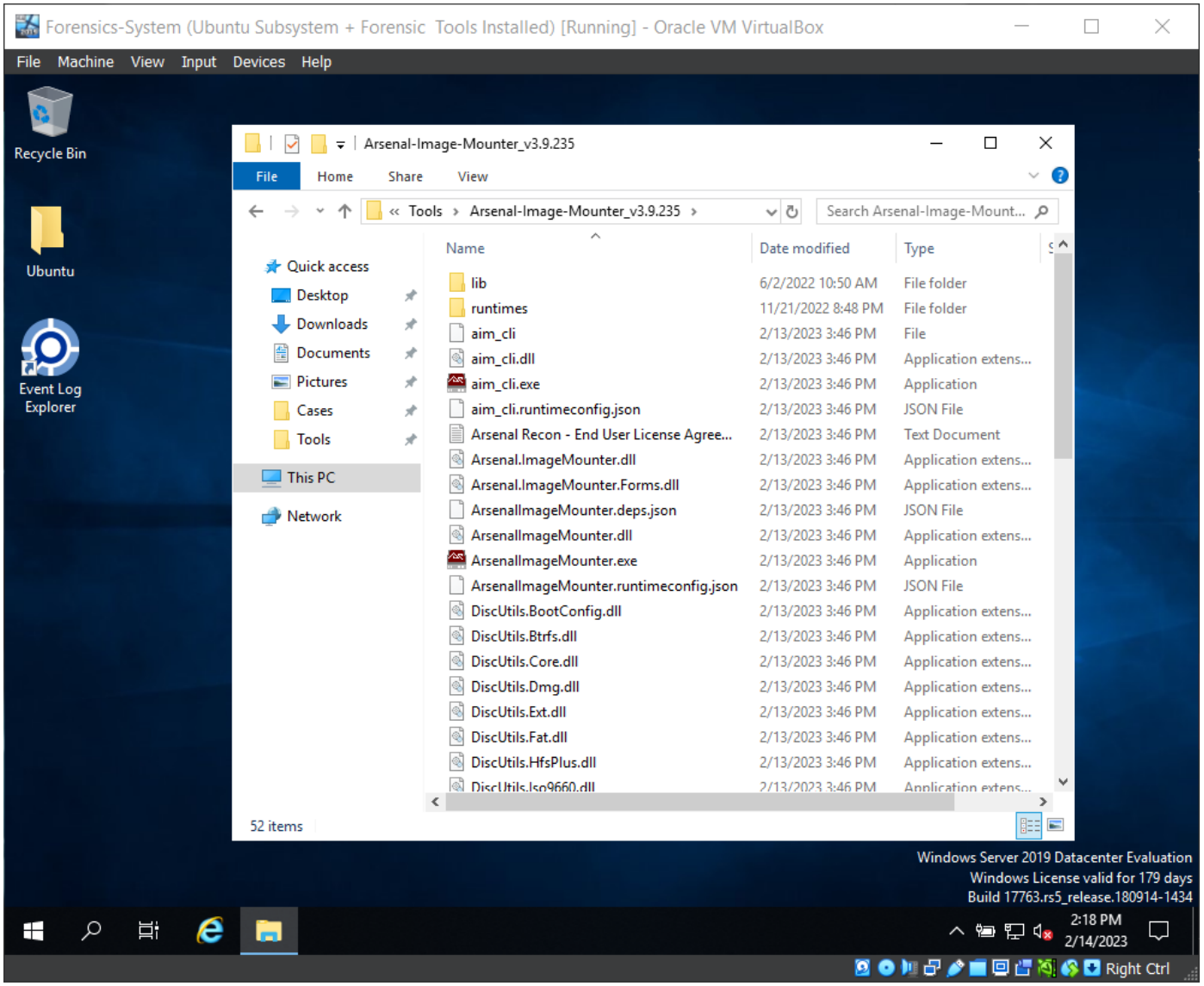
- Go to the virtualbox attached folder:

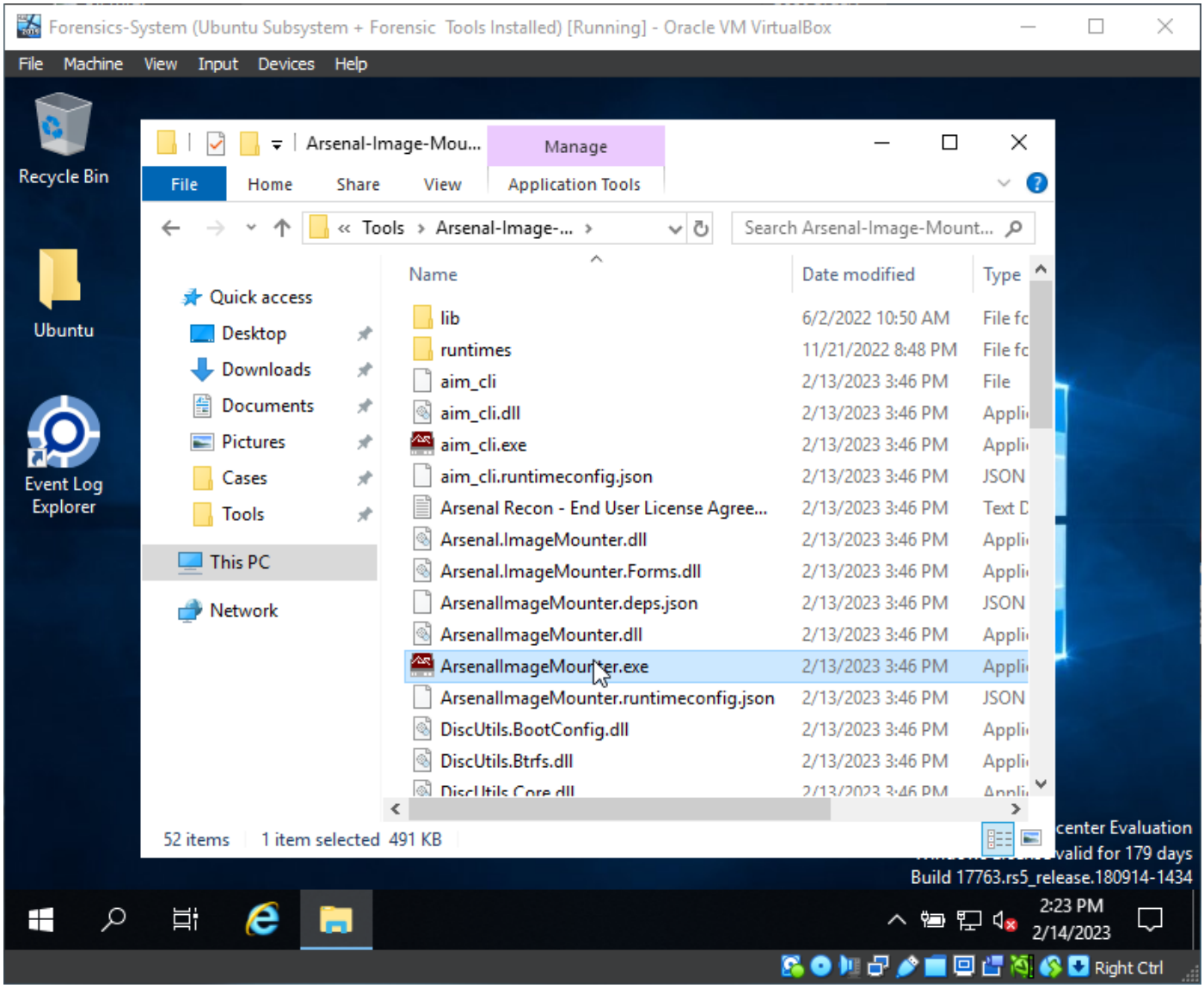

Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Ubuntu
Event Log Explorer
This PC
File Computer View
This PC
Search This PC
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
Folders (7)
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Devices and drives (2)
SDT_x64FREE_EN-US_VHD (C:)
105 GB free of 119 GB
CD Drive (D:) VirtualBox Guest Additions
0 bytes free of 50.5 MB
Network locations (1)
Windows-Forensics (\\VBoxSvr) (Z:)
116 GB free of 237 GB
10 items
Windows Server 2019 Datacenter Evaluation
Windows License valid for 179 days
Build 17763.rs5_release.180914-1434
2:15 PM
2/14/2023
Right Ctrl



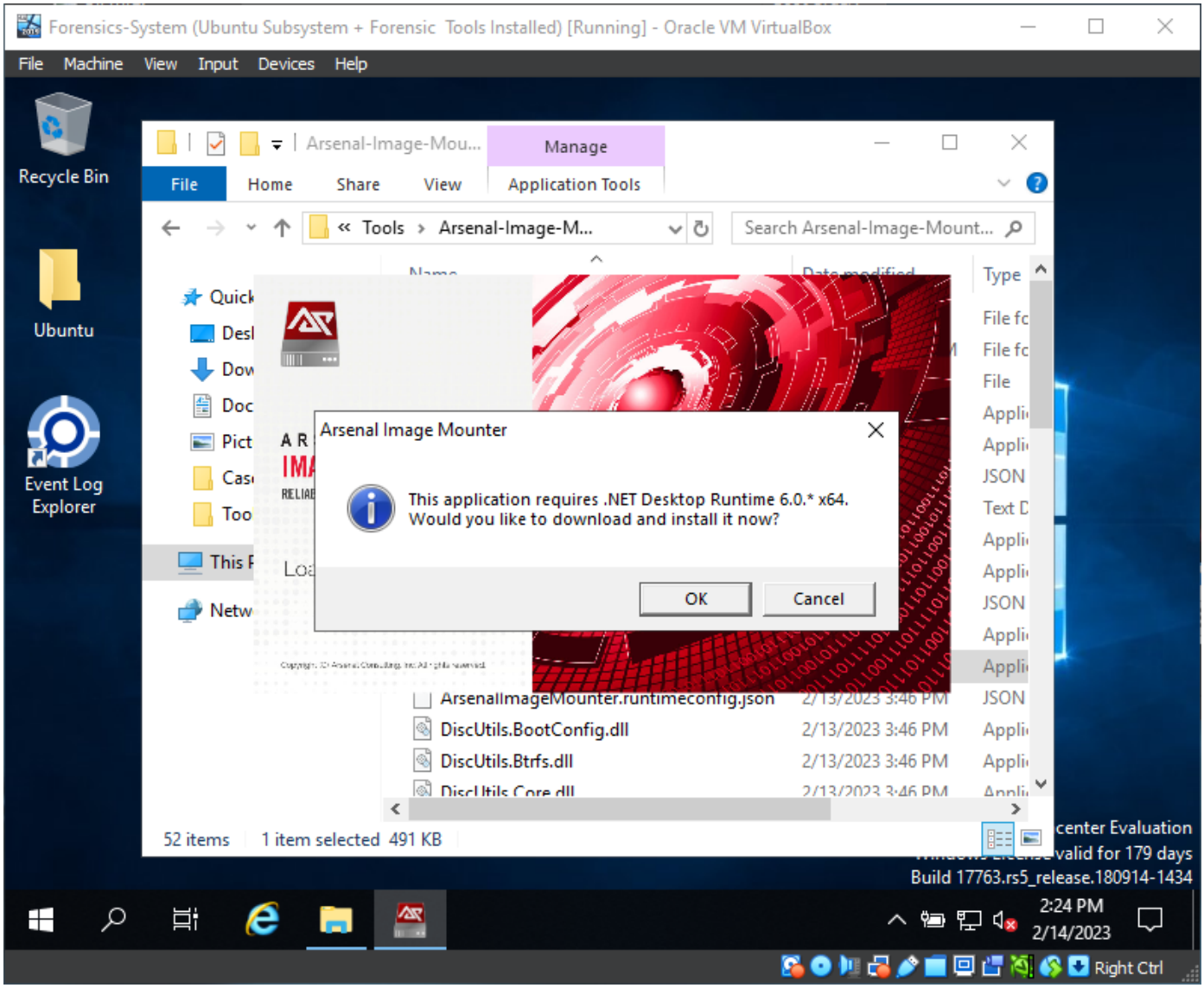
- You would not want to mount the .vhd file in windows directly because then we will have read and write access and it could tamper with the evidence.

- We will use Arsenal Image Mounter that have Raw disk image support, you can read more information about this tool in here: https://arsenalrecon.com/arsenal-image-mounter-aim-walkthrough

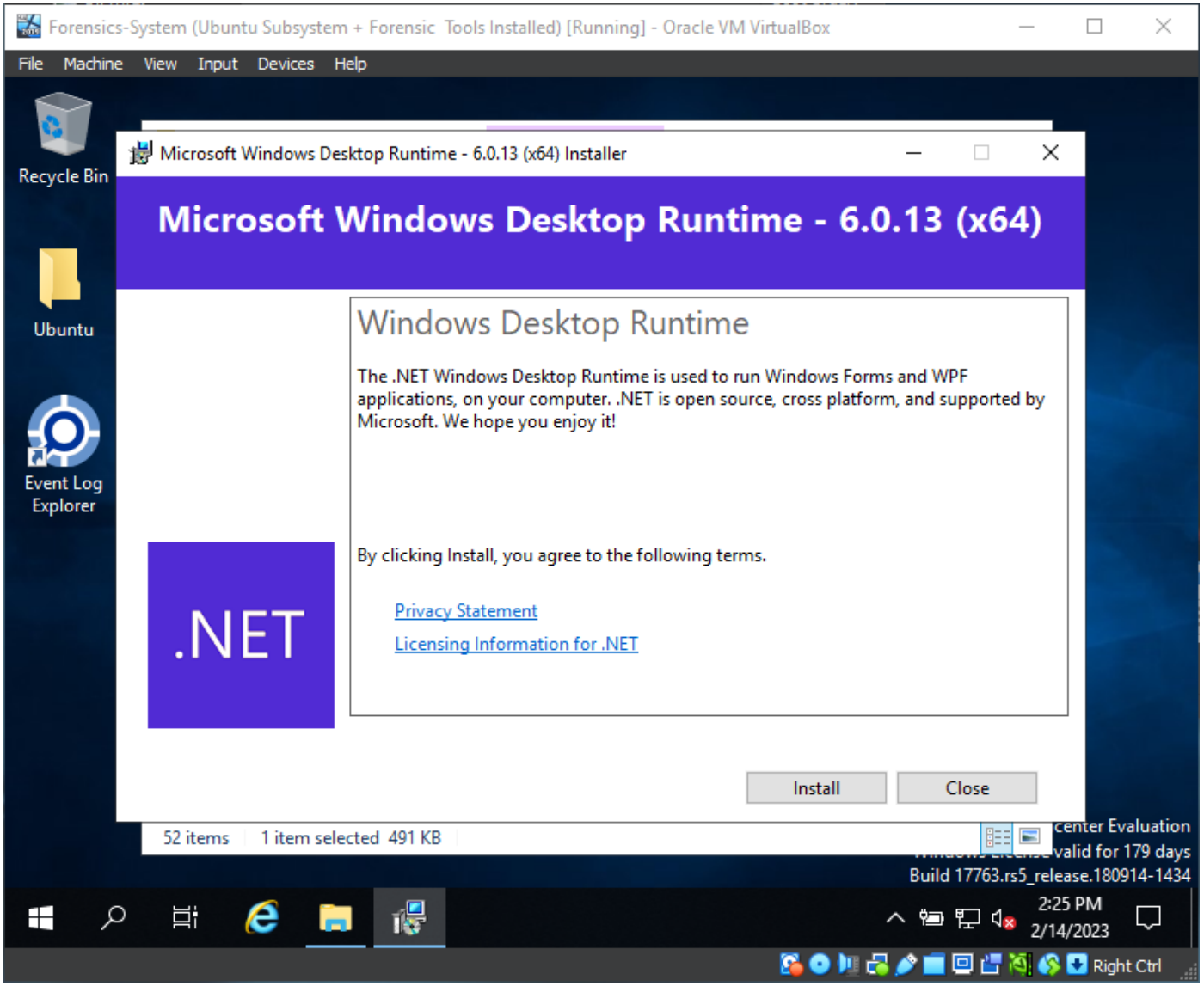

Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Ubuntu
Event Log Explorer
Arsenal-Image-Mounter_v3.9.235
File Home Share View
« Tools › Arsenal-Image-Mounter_v3.9.235 ›
Search Arsenal-Image-Mount...
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
Name
Date modified
Type
lib 6/2/2022 10:50 AM File folder
runtimes 11/21/2022 8:48 PM File folder
aim_cli 2/13/2023 3:46 PM File
aim_cli.dll 2/13/2023 3:46 PM Application extens...
aim_cli.exe 2/13/2023 3:46 PM Application
aim_cli.runtimeconfig.json 2/13/2023 3:46 PM JSON File
Arsenal Recon - End User License Agree... 2/13/2023 3:46 PM Text Document
Arsenal.ImageMounter.dll 2/13/2023 3:46 PM Application extens...
Arsenal.ImageMounter.Forms.dll 2/13/2023 3:46 PM Application extens...
ArsenalImageMounter.deps.json 2/13/2023 3:46 PM JSON File
ArsenalImageMounter.dll 2/13/2023 3:46 PM Application extens...
ArsenalImageMounter.exe 2/13/2023 3:46 PM Application
ArsenalImageMounter.runtimeconfig.json 2/13/2023 3:46 PM JSON File
DiscUtils.BootConfig.dll 2/13/2023 3:46 PM Application extens...
DiscUtils.Btrfs.dll 2/13/2023 3:46 PM Application extens...
DiscUtils.Core.dll 2/13/2023 3:46 PM Application extens...
DiscUtils.Dmg.dll 2/13/2023 3:46 PM Application extens...
DiscUtils.Ext.dll 2/13/2023 3:46 PM Application extens...
DiscUtils.Fat.dll 2/13/2023 3:46 PM Application extens...
DiscUtils.HfsPlus.dll 2/13/2023 3:46 PM Application extens...
52 items
Windows Server 2019 Datacenter Evaluation
Windows License valid for 179 days
Build 17763.rs5_release.180914-1434
2:18 PM
2/14/2023
Right Ctrl


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Ubuntu
Event Log Explorer
Arsenal-Image-Mou...
Manage
File Home Share View Application Tools
Tools › Arsenal-Image-...
Search Arsenal-Image-Mount...
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
Name
Date modified
Type
lib 6/2/2022 10:50 AM File fc
runtimes 11/21/2022 8:48 PM File fc
aim_cli 2/13/2023 3:46 PM File
aim_cli.dll 2/13/2023 3:46 PM Appli
aim_cli.exe 2/13/2023 3:46 PM Appli
aim_cli.runtimeconfig.json 2/13/2023 3:46 PM JSON
Arsenal Recon - End User License Agree... 2/13/2023 3:46 PM Text D
Arsenal.ImageMounter.dll 2/13/2023 3:46 PM Appli
Arsenal.ImageMounter.Forms.dll 2/13/2023 3:46 PM Appli
ArsenalImageMounter.deps.json 2/13/2023 3:46 PM JSON
ArsenalImageMounter.dll 2/13/2023 3:46 PM Appli
ArsenalImageMounter.exe 2/13/2023 3:46 PM Appli
ArsenalImageMounter.runtimeconfig.json 2/13/2023 3:46 PM JSON
DiscUtils.BootConfig.dll 2/13/2023 3:46 PM Appli
DiscUtils.Btrfs.dll 2/13/2023 3:46 PM Appli
52 items 1 item selected 491 KB
center Evaluation
valid for 179 days
Build 17763.rs5_release.180914-1434
2:23 PM
2/14/2023
Right Ctrl

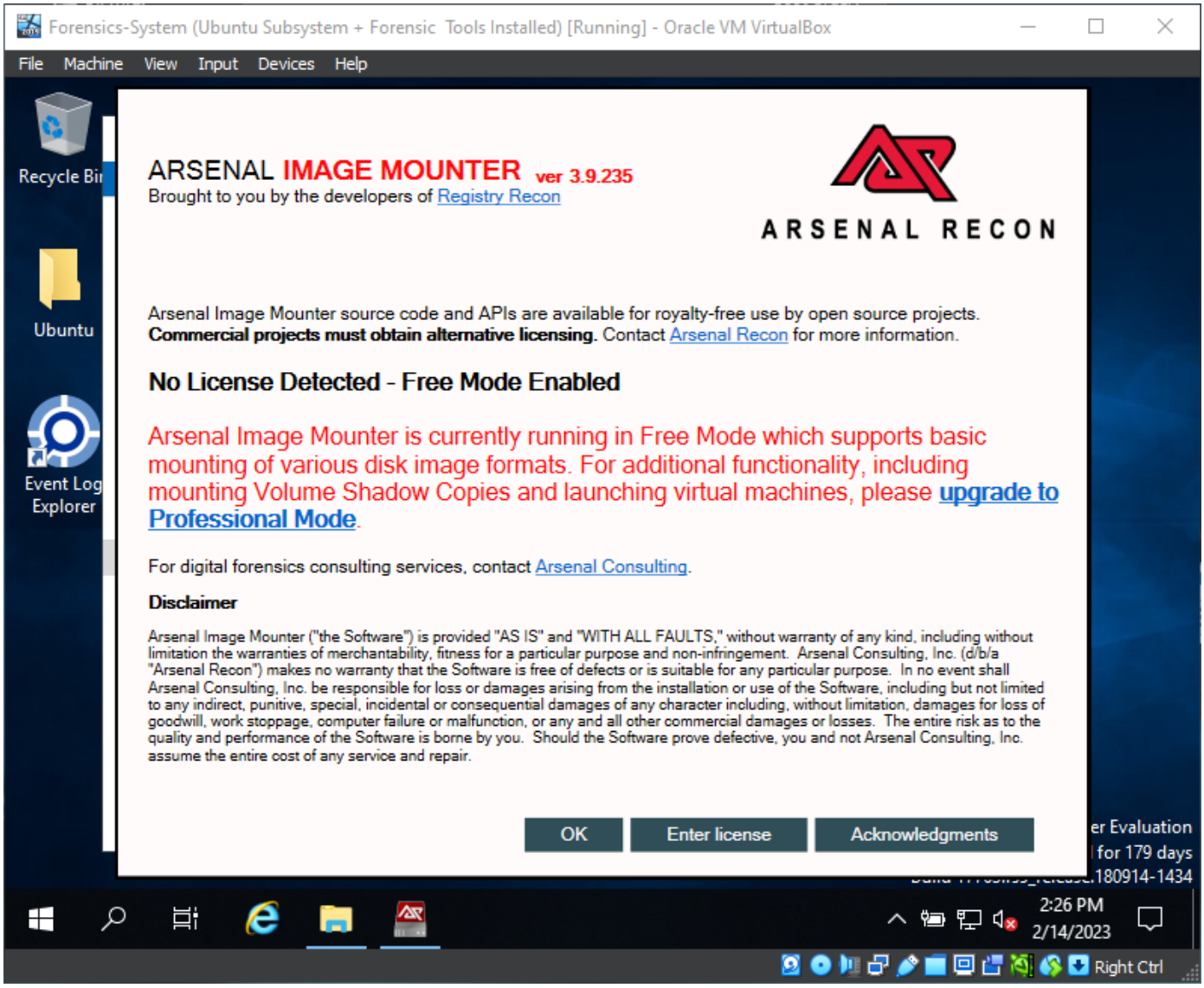
- Press OK:



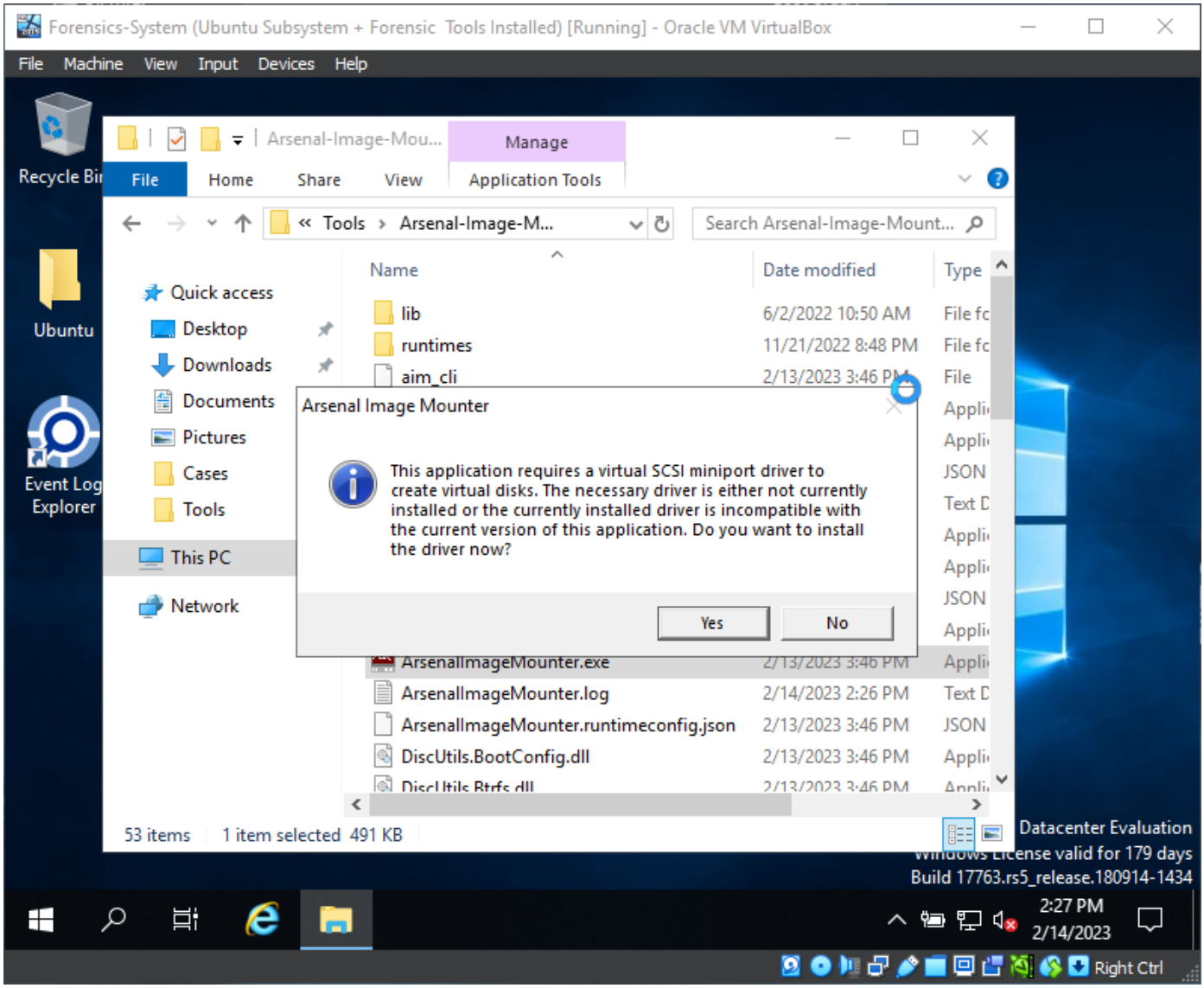
- Install NET6.0:

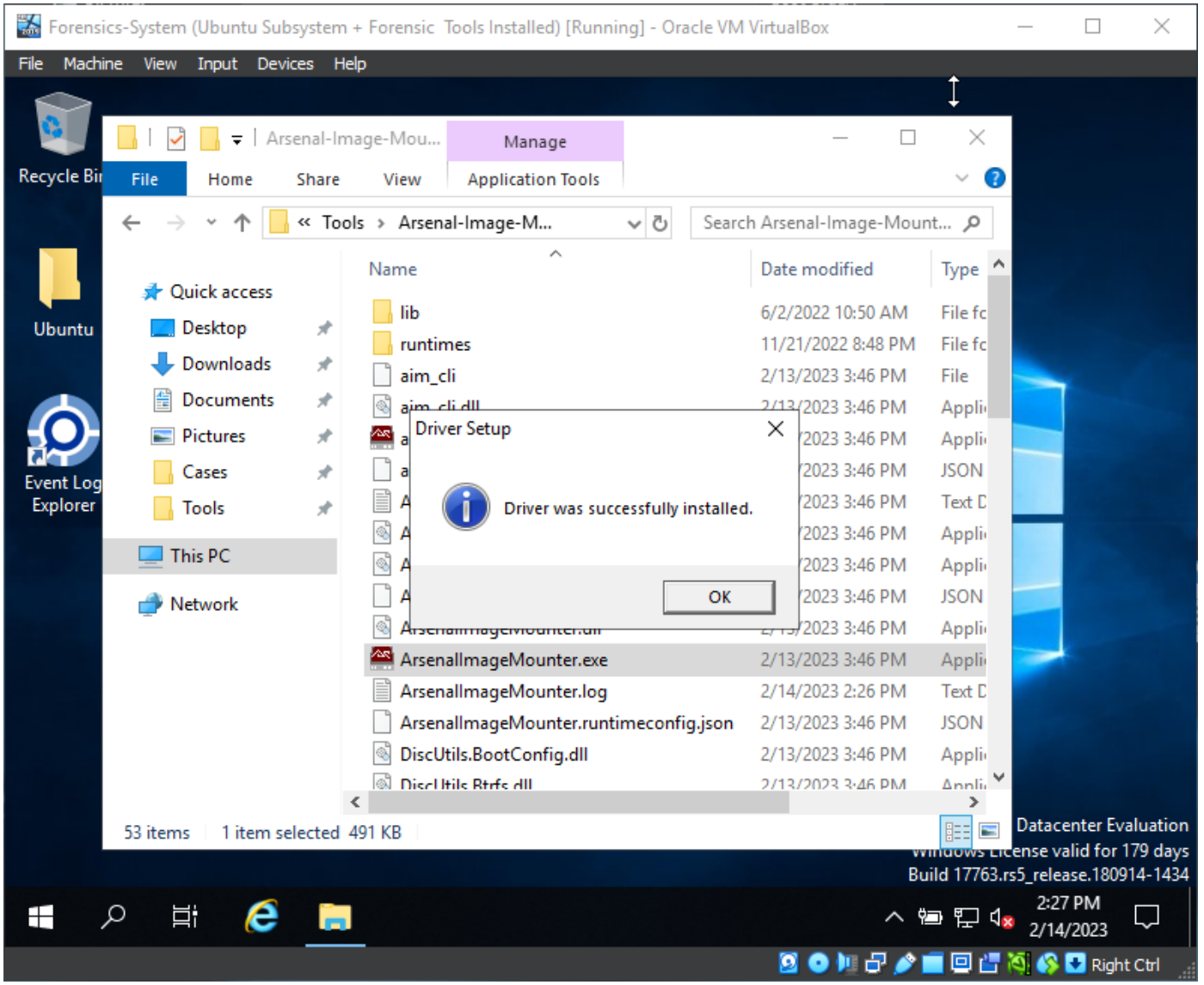


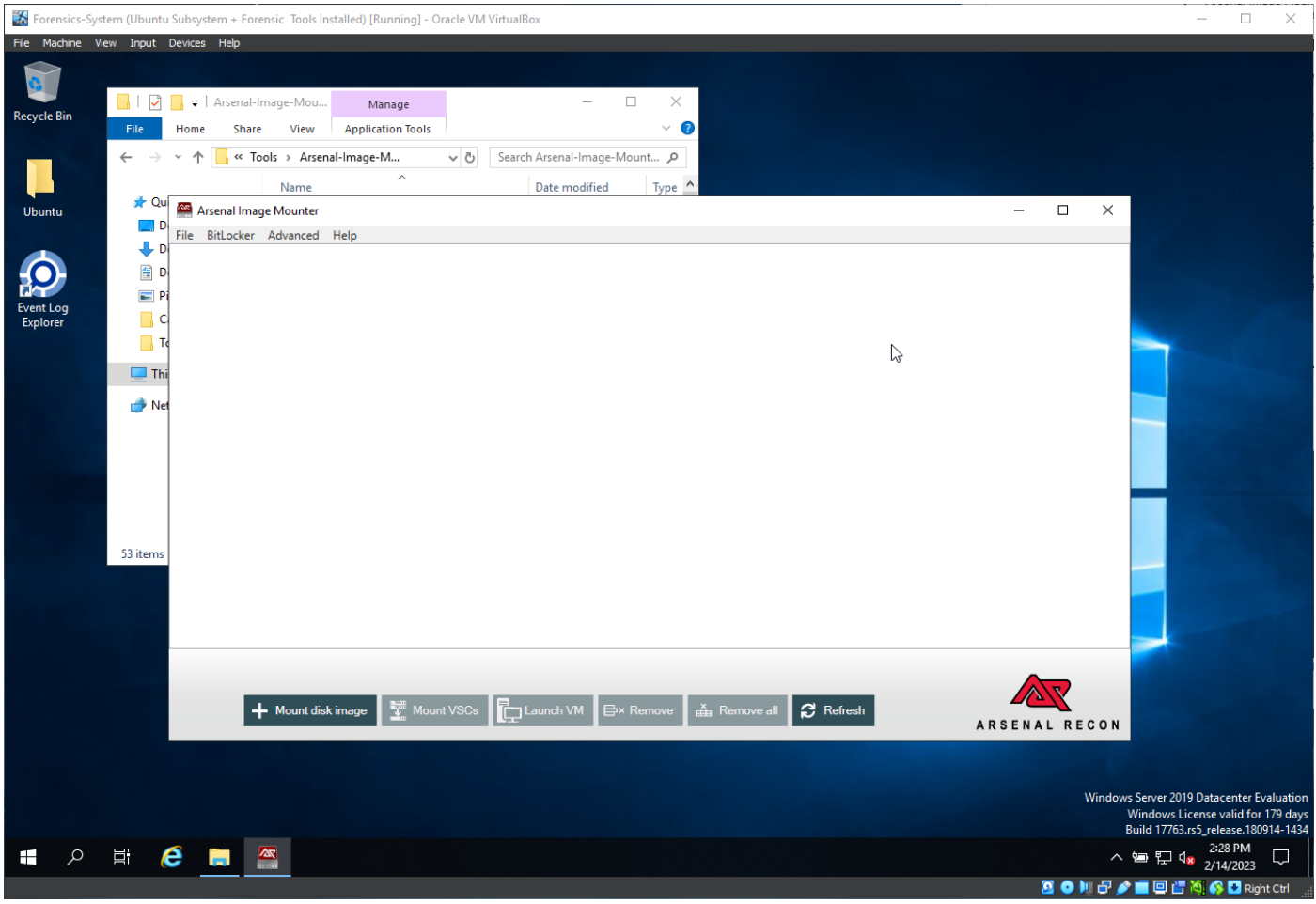
- After that, reenter:



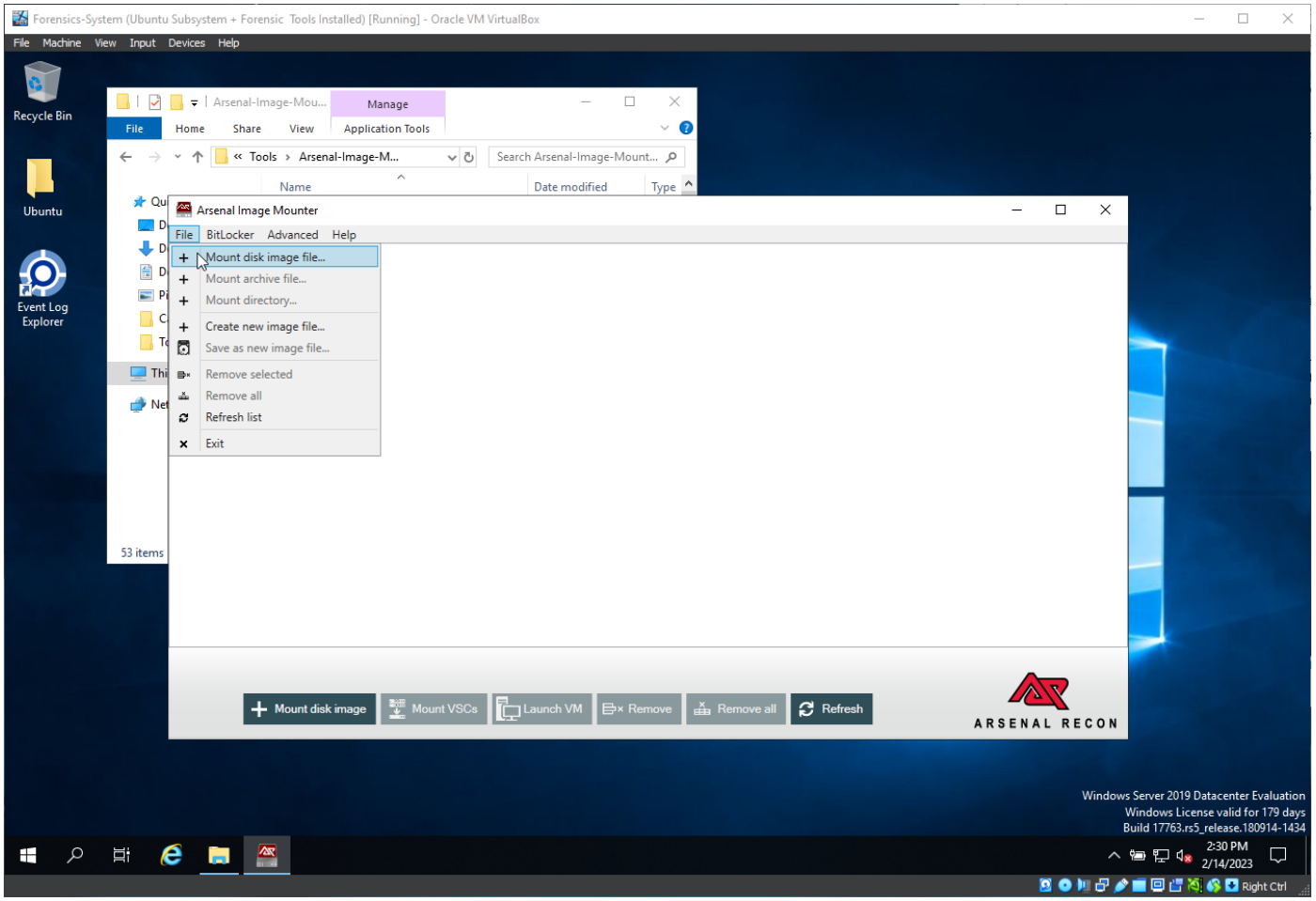
- We are going to use this software in Free Mode. Press OK and Yes, to install a virtual SCSI miniport driver in order to create the virtual disks:

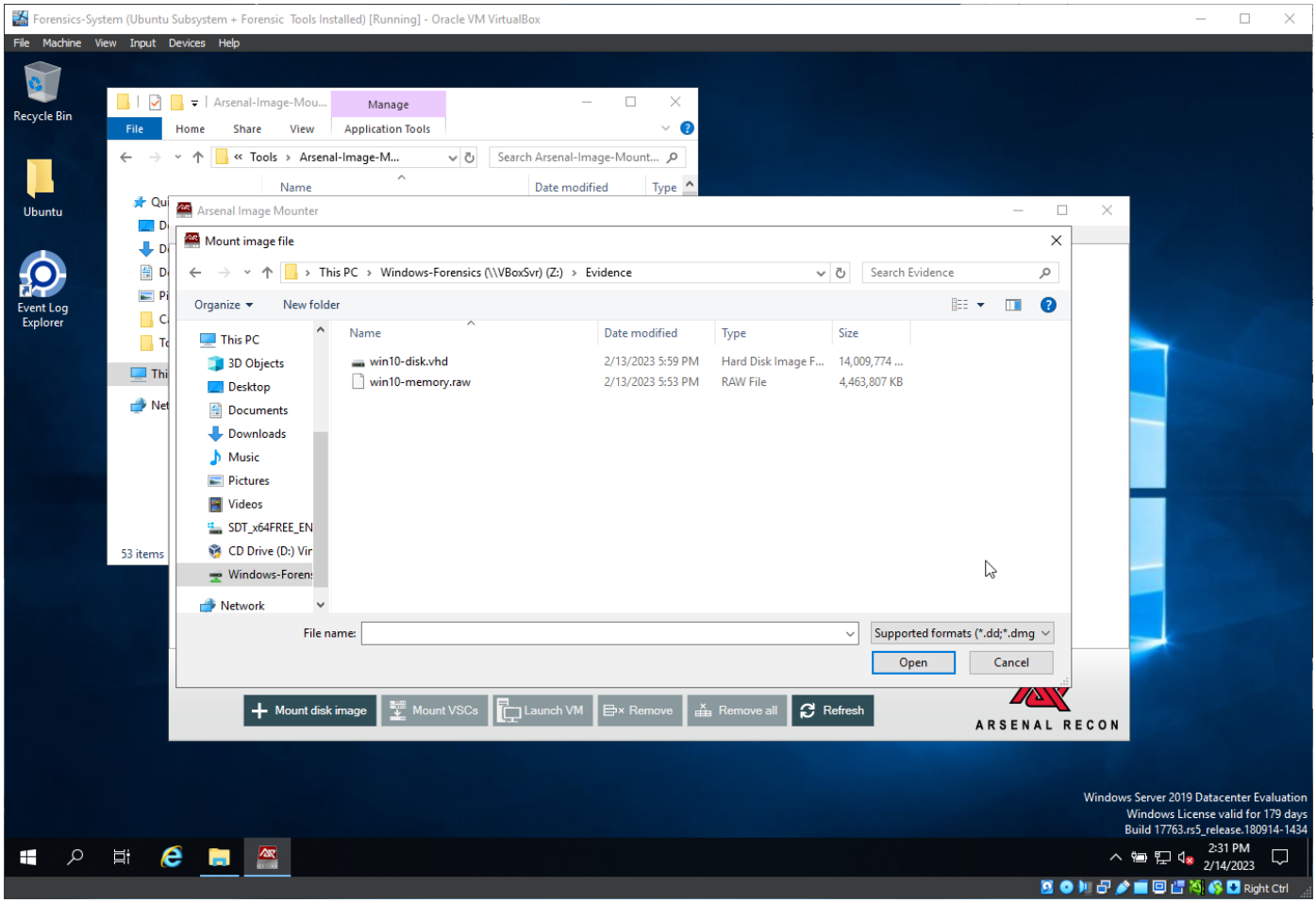

Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bi
Ubuntu
Event Log Explorer
Arsenal-Image-Mou...
Manage
File Home Share View Application Tools
« Tools › Arsenal-Image-M...
Search Arsenal-Image-Mount...
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
Name
Date modified
Type
lib
6/2/2022 10:50 AM
runtimes
11/21/2022 8:48 PM
aim_cli
2/13/2023 3:46 PM
Arsenal Image Mounter
This application requires a virtual SCSI miniport driver to create virtual disks. The necessary driver is either not currently installed or the currently installed driver is incompatible with the current version of this application. Do you want to install the driver now?
Yes
No
ArsenalImageMounter.exe
ArsenalImageMounter.log
2/14/2023 2:26 PM
ArsenalImageMounter.runtimeconfig.json
2/13/2023 3:46 PM
DiscUtils.BootConfig.dll
2/13/2023 3:46 PM
53 items
1 item selected 491 KB
Datacenter Evaluation
Build 17763.rs5_release.180914-1434
2:27 PM
2/14/2023
Right Ctrl


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Ubuntu
Event Log Explorer
Arsenal-Image-Mou...
Manage
File Home Share View Application Tools
« Tools › Arsenal-Image-M...
Search Arsenal-Image-Mount...
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
Name
Date modified
Type
lib 6/2/2022 10:50 AM File fc
runtimes 11/21/2022 8:48 PM File fc
aim_cli 2/13/2023 3:46 PM File
Driver Setup
Driver was successfully installed.
OK
ArsenalImageMounter.exe 2/13/2023 3:46 PM
ArsenalImageMounter.log 2/14/2023 2:26 PM Text D
ArsenalImageMounter.runtimeconfig.json 2/13/2023 3:46 PM JSON
DiscUtils.BootConfig.dll 2/13/2023 3:46 PM
53 items 1 item selected 491 KB
Datacenter Evaluation
Build 17763.rs5_release.180914-1434
2:27 PM
2/14/2023
Right Ctrl

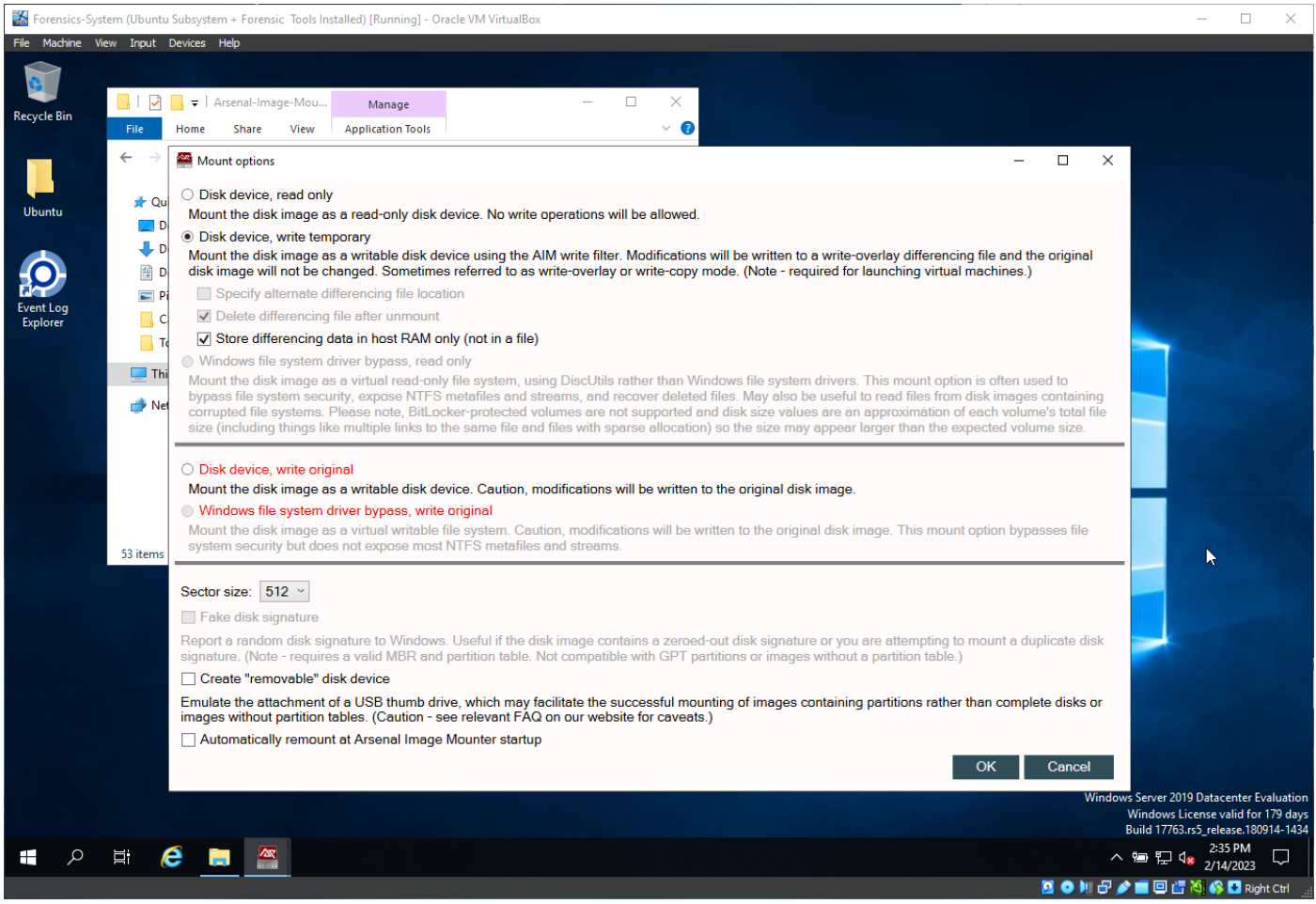


- Mount the .vhd acquired evidence from the attached drive:

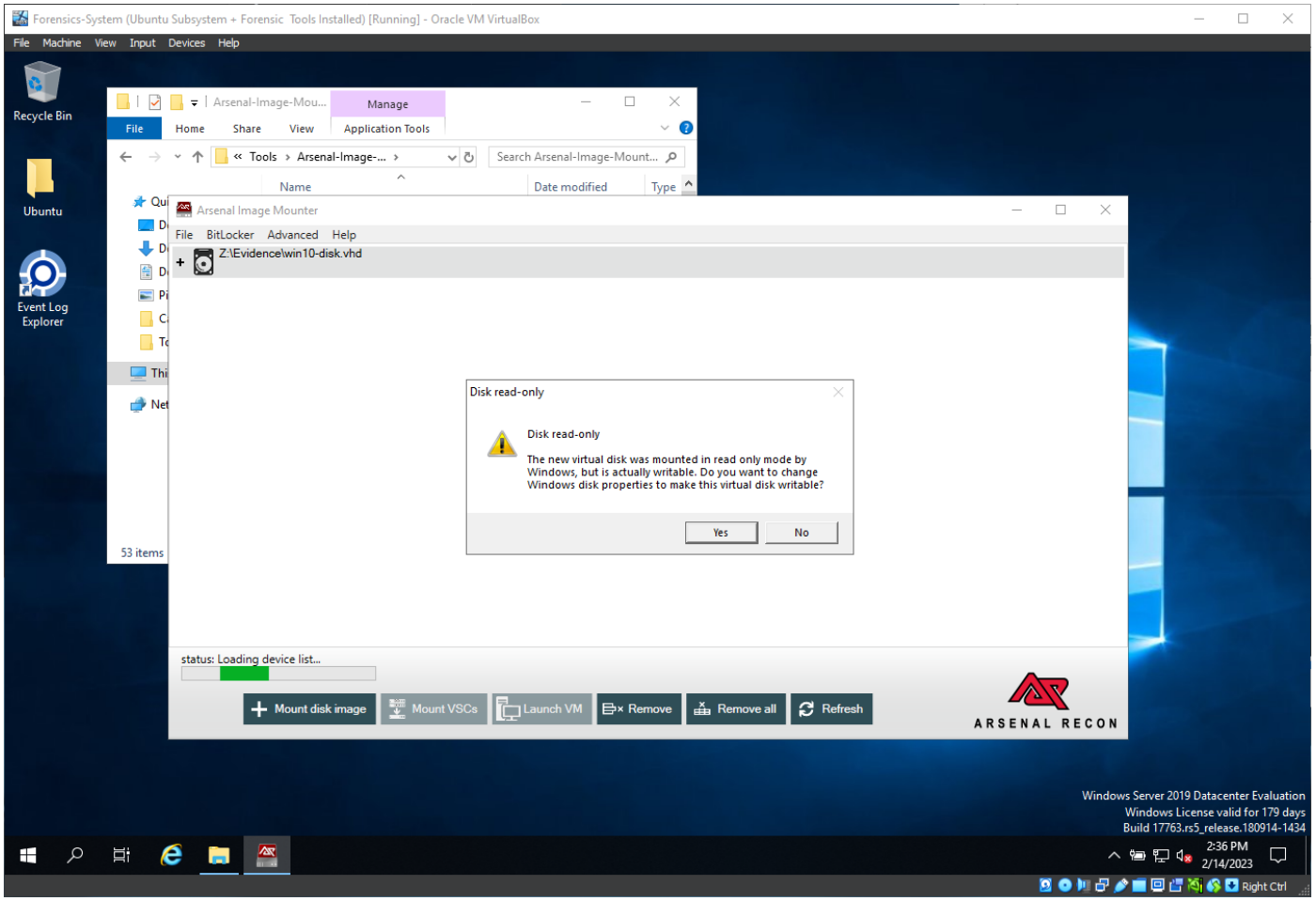

Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Ubuntu
Event Log Explorer
Arsenal-Image-Mou...
Manage
File Home Share View Application Tools
Tools › Arsenal-Image-M...
Search Arsenal-Image-Mount...
Name
Date modified
Type
53 items
Arsenal Image Mounter
File BitLocker Advanced Help
Mount disk image file...
Mount archive file...
Mount directory...
Create new image file...
Save as new image file...
Remove selected
Remove all
Refresh list
Exit
Mount disk image
Mount VSCs
Launch VM
Remove
Remove all
Refresh
ARSENAL RECON
Windows Server 2019 Datacenter Evaluation
Windows License valid for 179 days
Build 17763.rs5_release.180914-1434
2:30 PM
2/14/2023
Right Ctrl



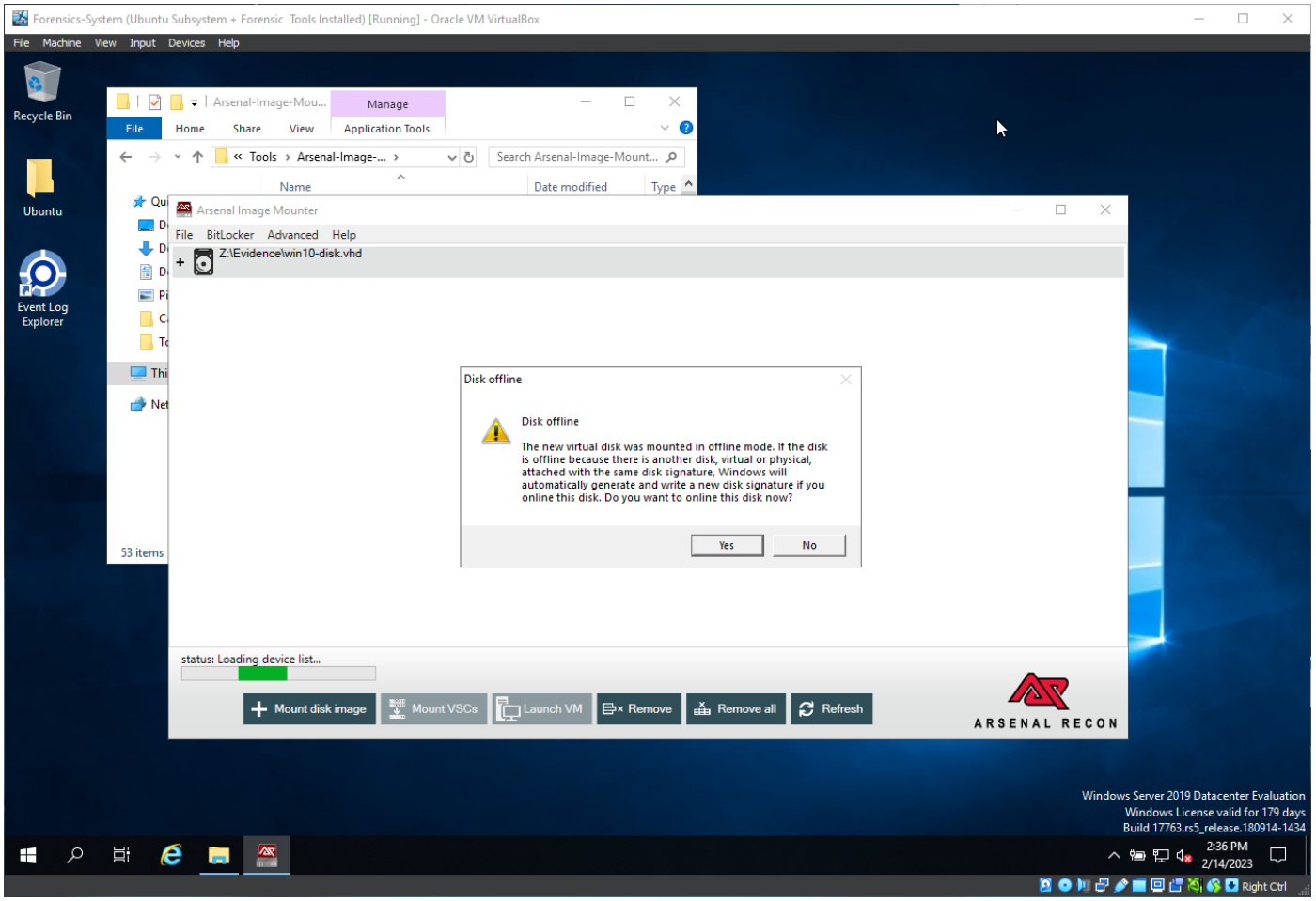
- We will need write action for the forensic analysis, so we will use the second choice that will not tamper with the original disk image, and will let us interact with the disk in other operations, not just reading operation, with storing the differencing data in RAM only, and deleting the differencing data after unmounting the disk image:



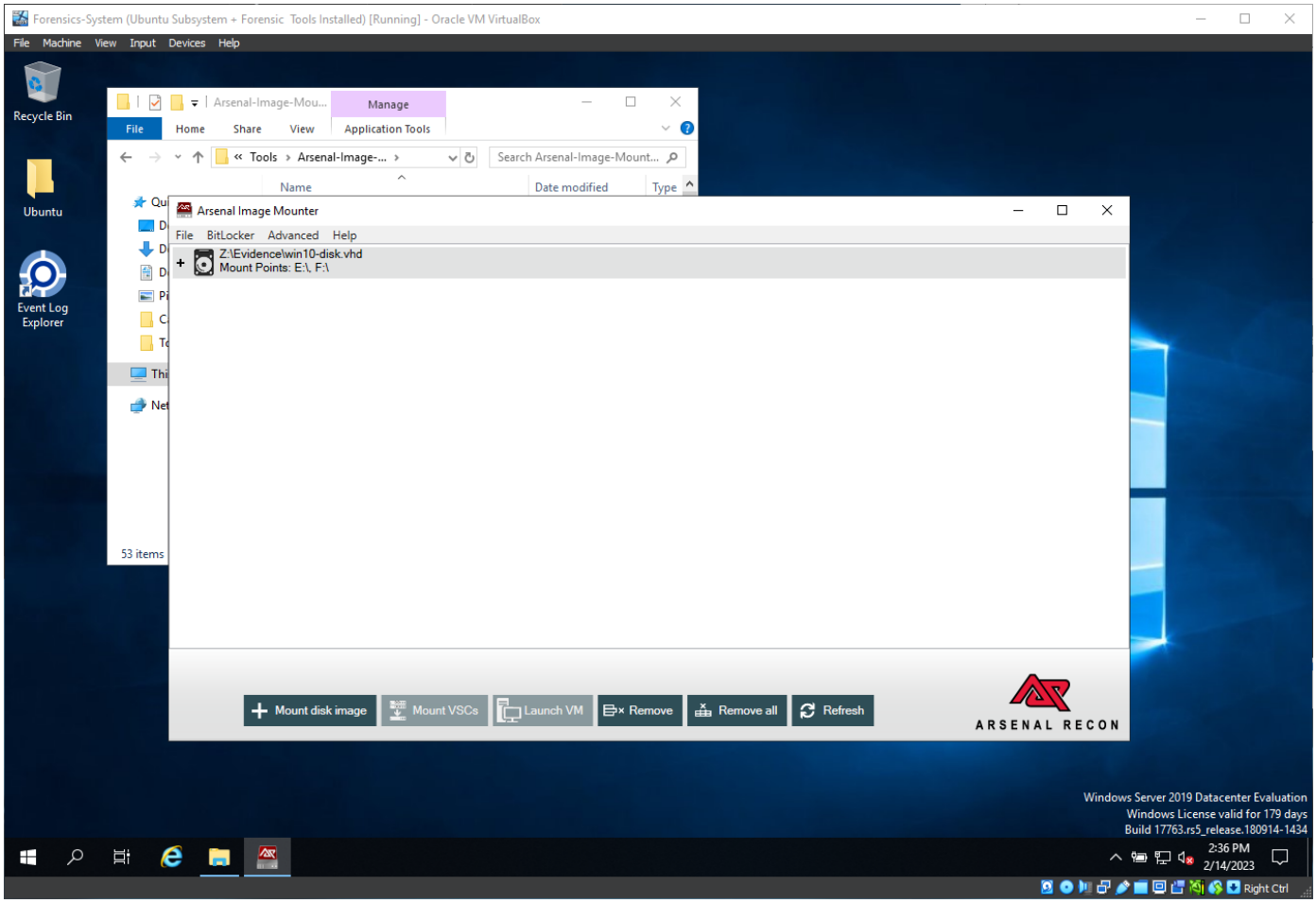
- Press yes, it says that it is actually writable because of the above settings:

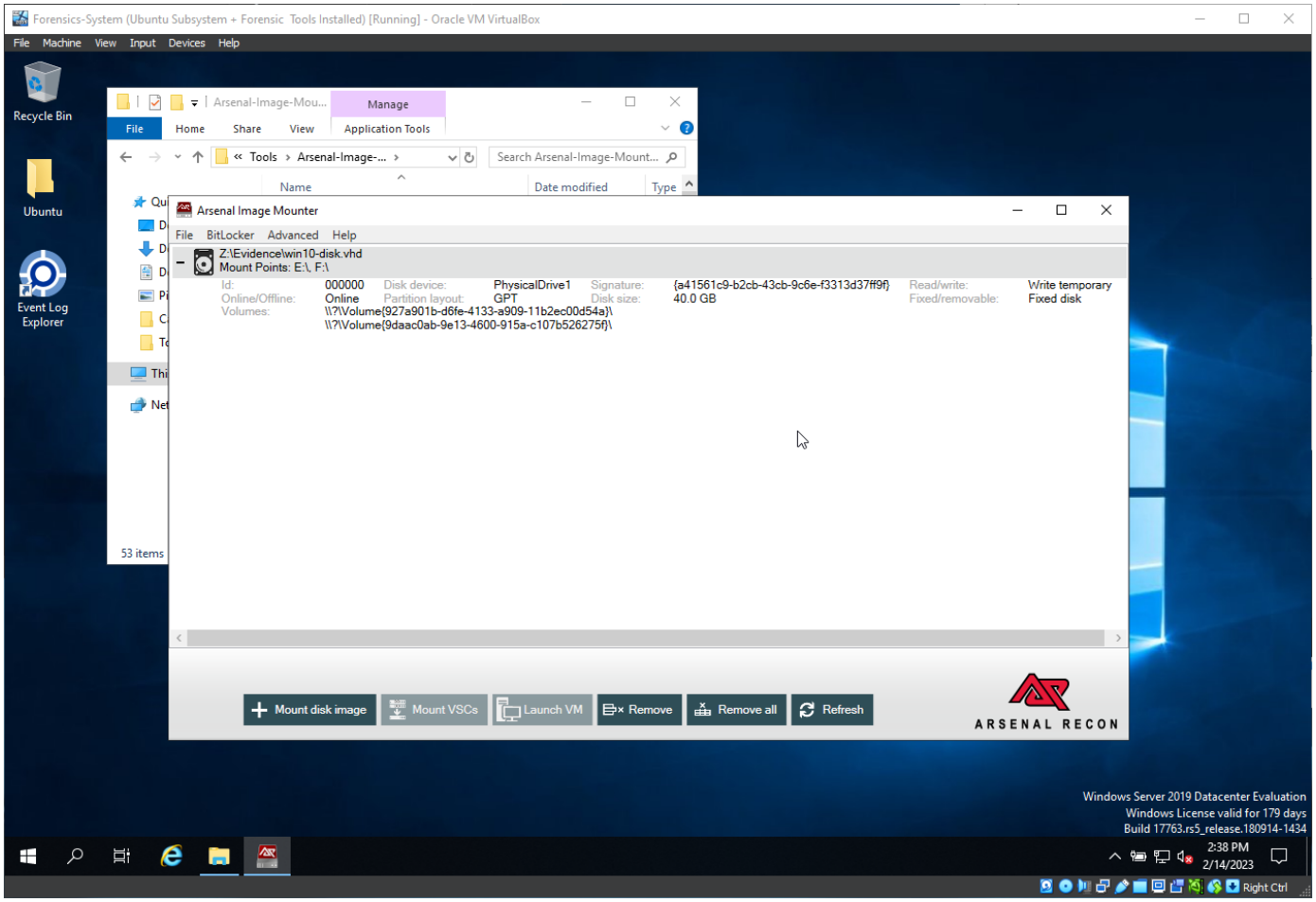


- And put the disk online:

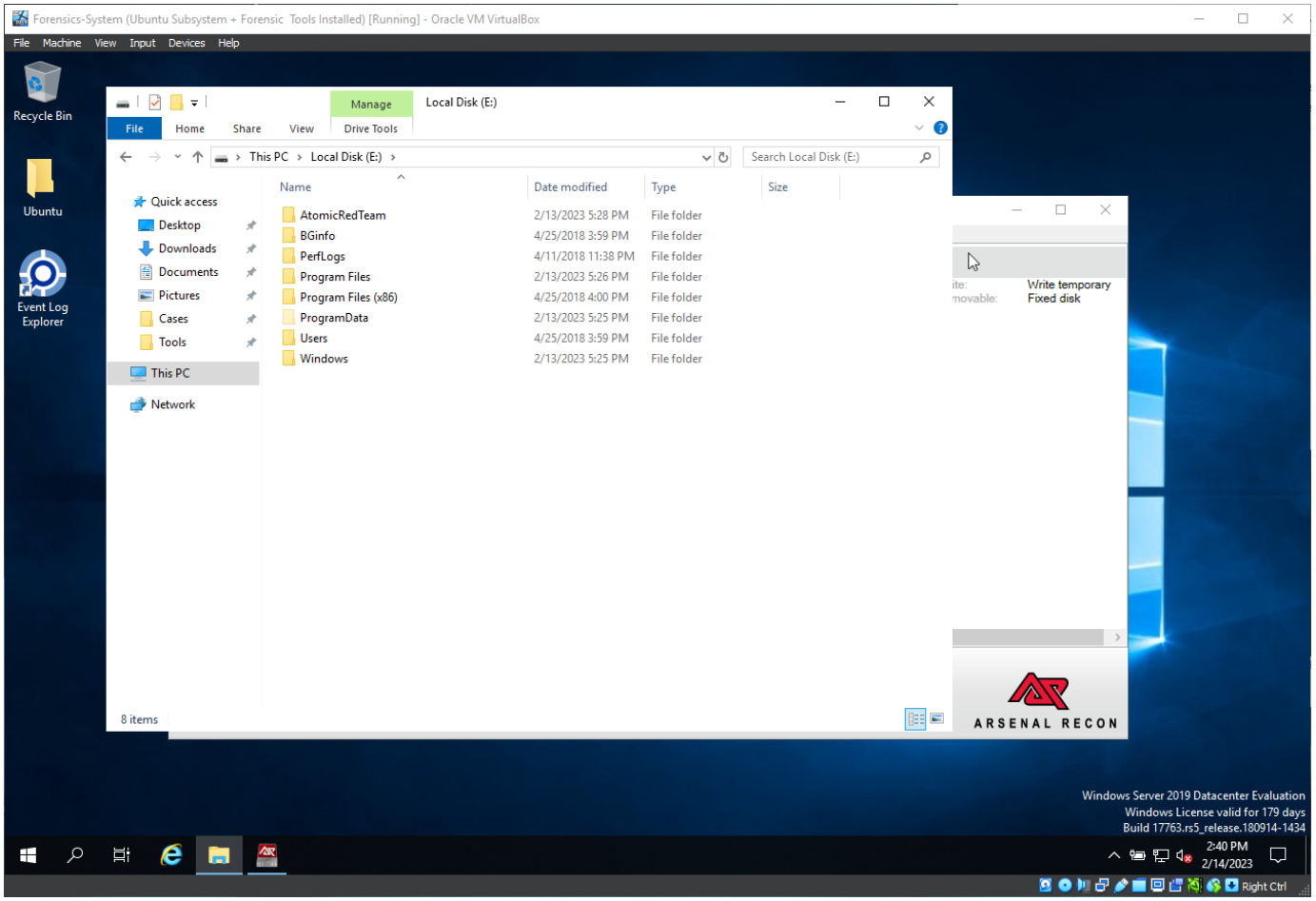


- Mounted disk image:


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Ubuntu
Event Log Explorer
Arsenal-Image-Mou...
Manage
File Home Share View Application Tools
Tools › Arsenal-Image-...
Search Arsenal-Image-Mount...
Name
Date modified
Type
53 items
Arsenal Image Mounter
File BitLocker Advanced Help
Z:\Evidence\win10-disk.vhd
Mount Points: E:\, F:\
Mount disk image
Mount VSCs
Launch VM
Remove
Remove all
Refresh
ARSENAL RECON
Windows Server 2019 Datacenter Evaluation
Windows License valid for 179 days
Build 17763.rs5_release.180914-1434
2:36 PM
2/14/2023
Right Ctrl



- If we go to the Local Disk (E:), we will see the root folder structure from the evidence disk image:



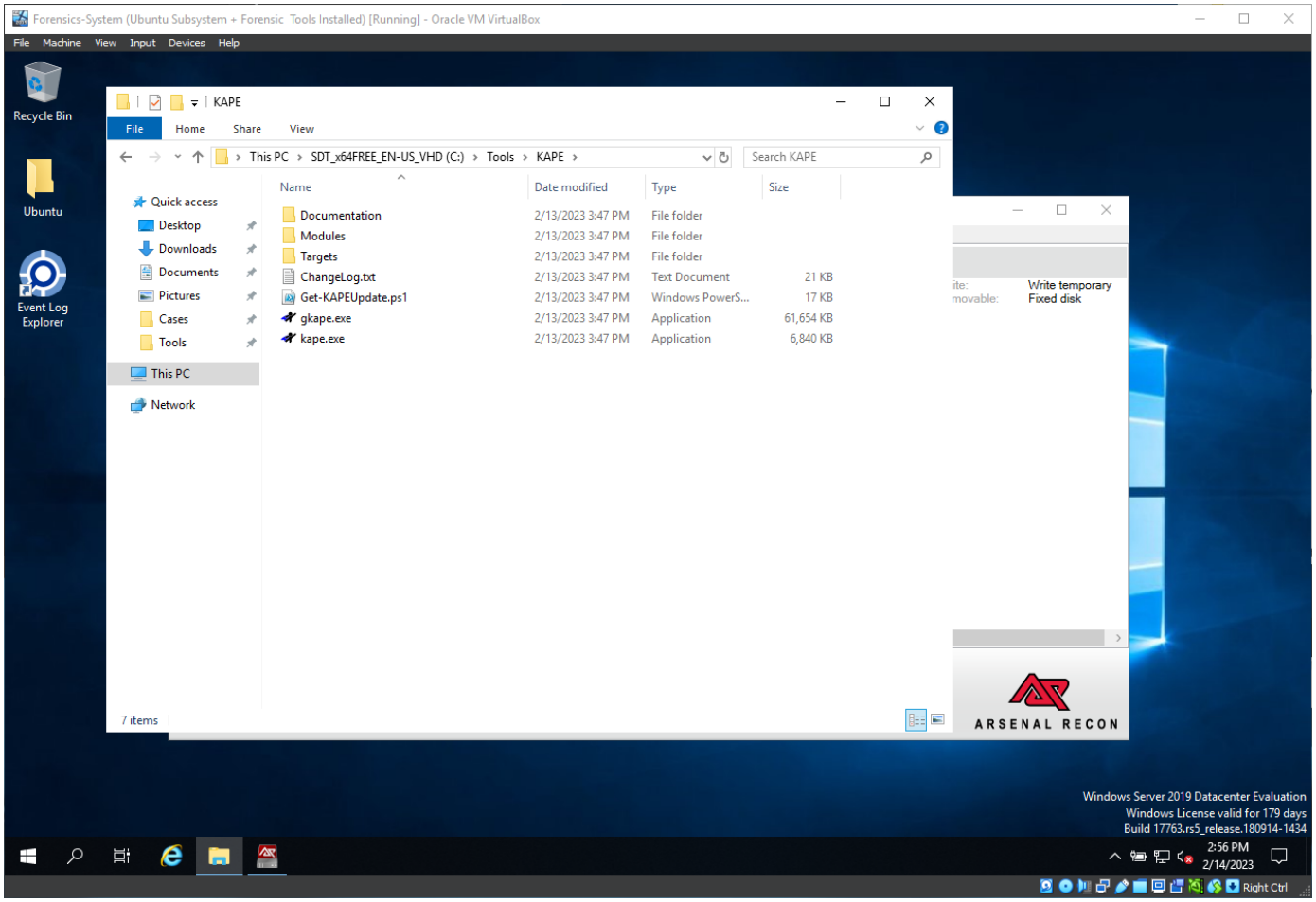
Windows files and forensics important artifacts

- We need to understand the artifacts that are available to us for the analysis purpose, after that we will create a triage of data, which is an export of a subset of the file on the disk image. When we know what to look after, just then we will start to investigate it. We will want to keep forensically relevant files only.

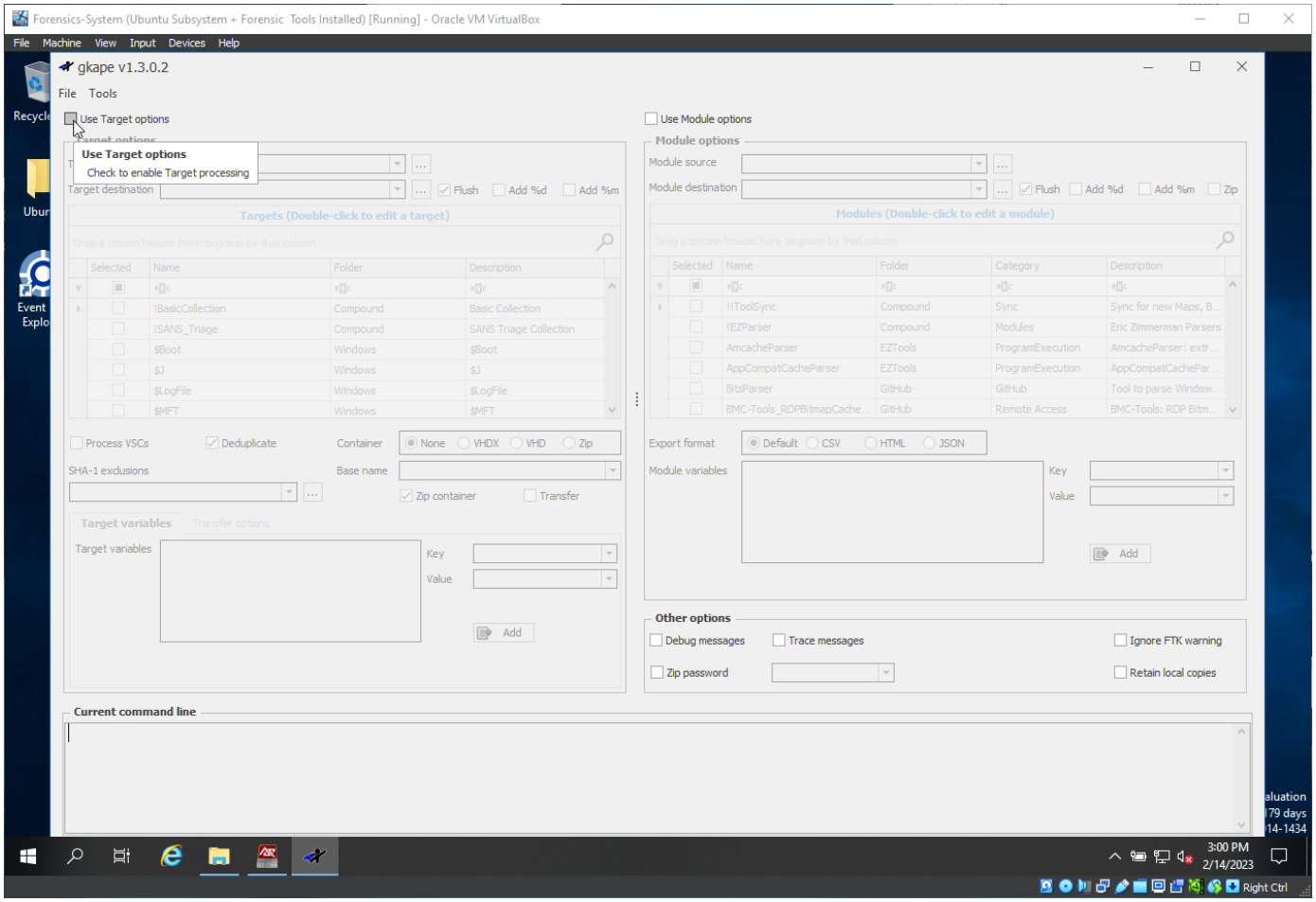
- We need NTFS metafiles for beggining the investigation. We cannot see the $MFT file (Master File Table) with the free edition of Arsenal Image Mounter.

Triage data

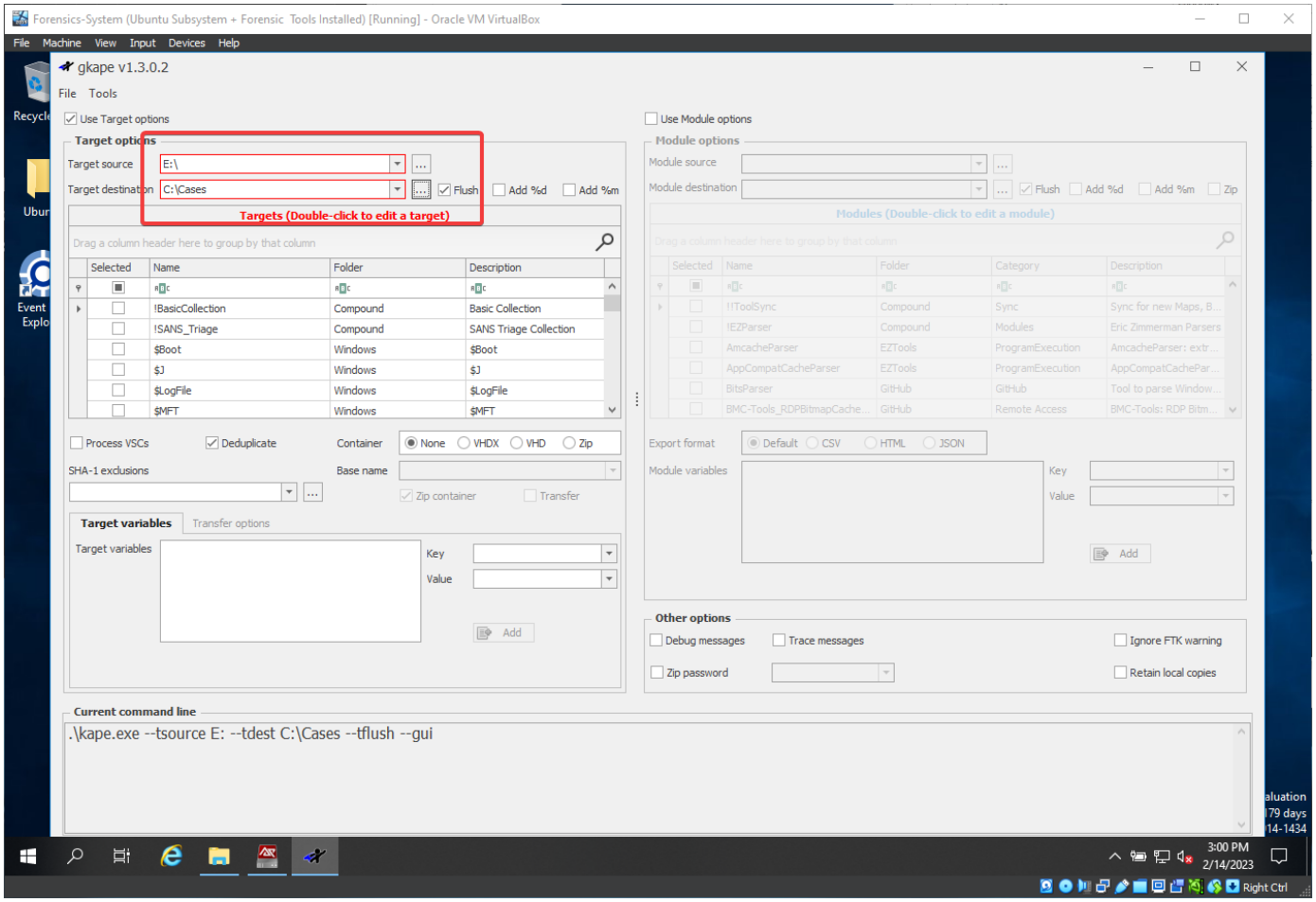
- We will create a triage package of the data using KAPE tool with the GUI of the application:



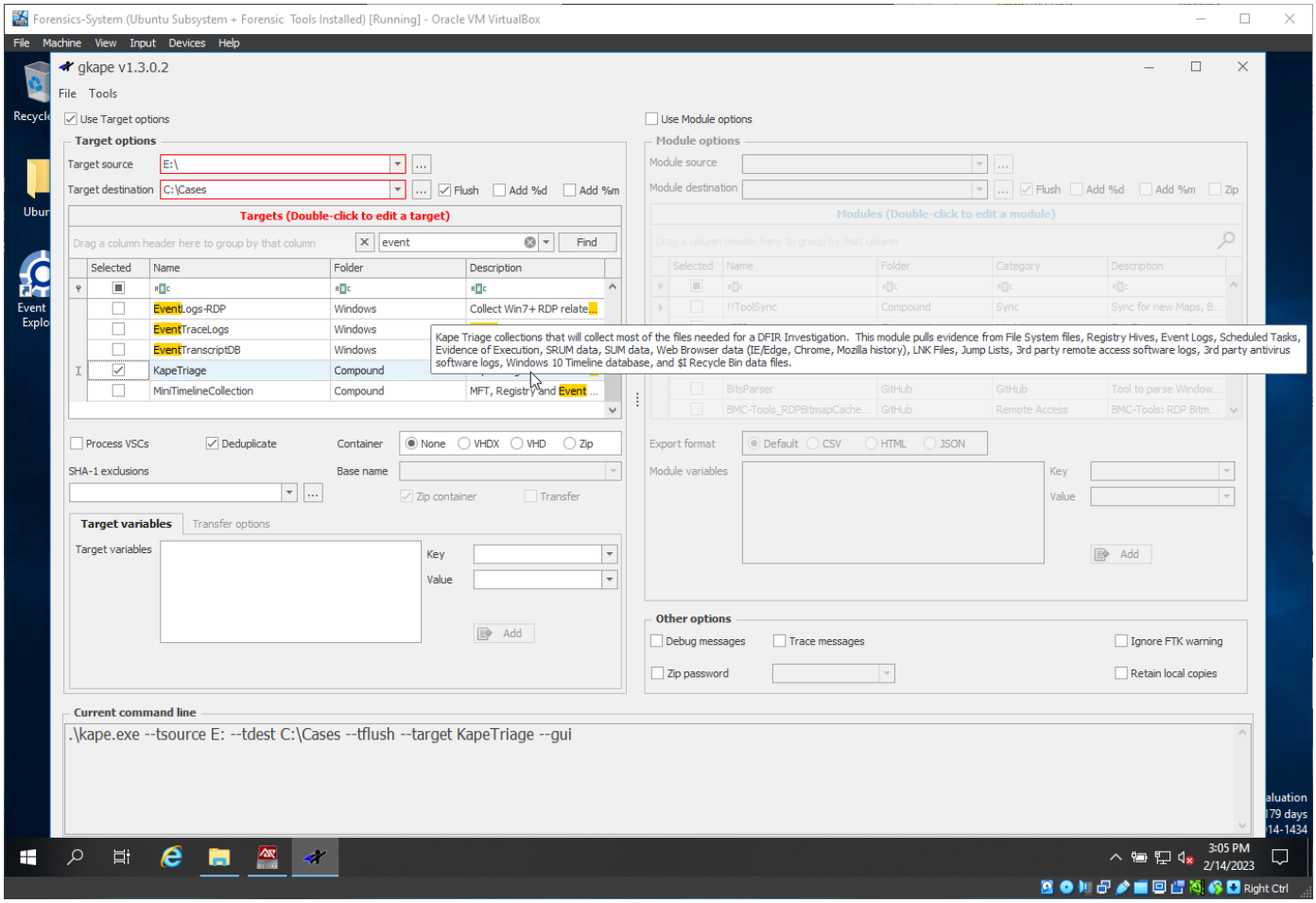
- Enable Target Options:



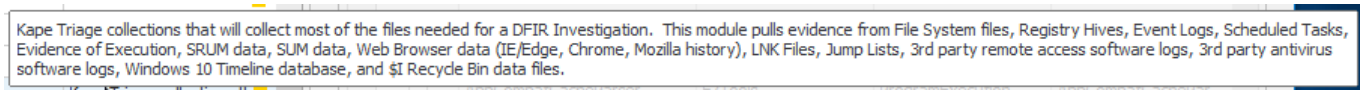
- Choose the drive for the target source, and in my case, i chose the Target destination C:\Cases:



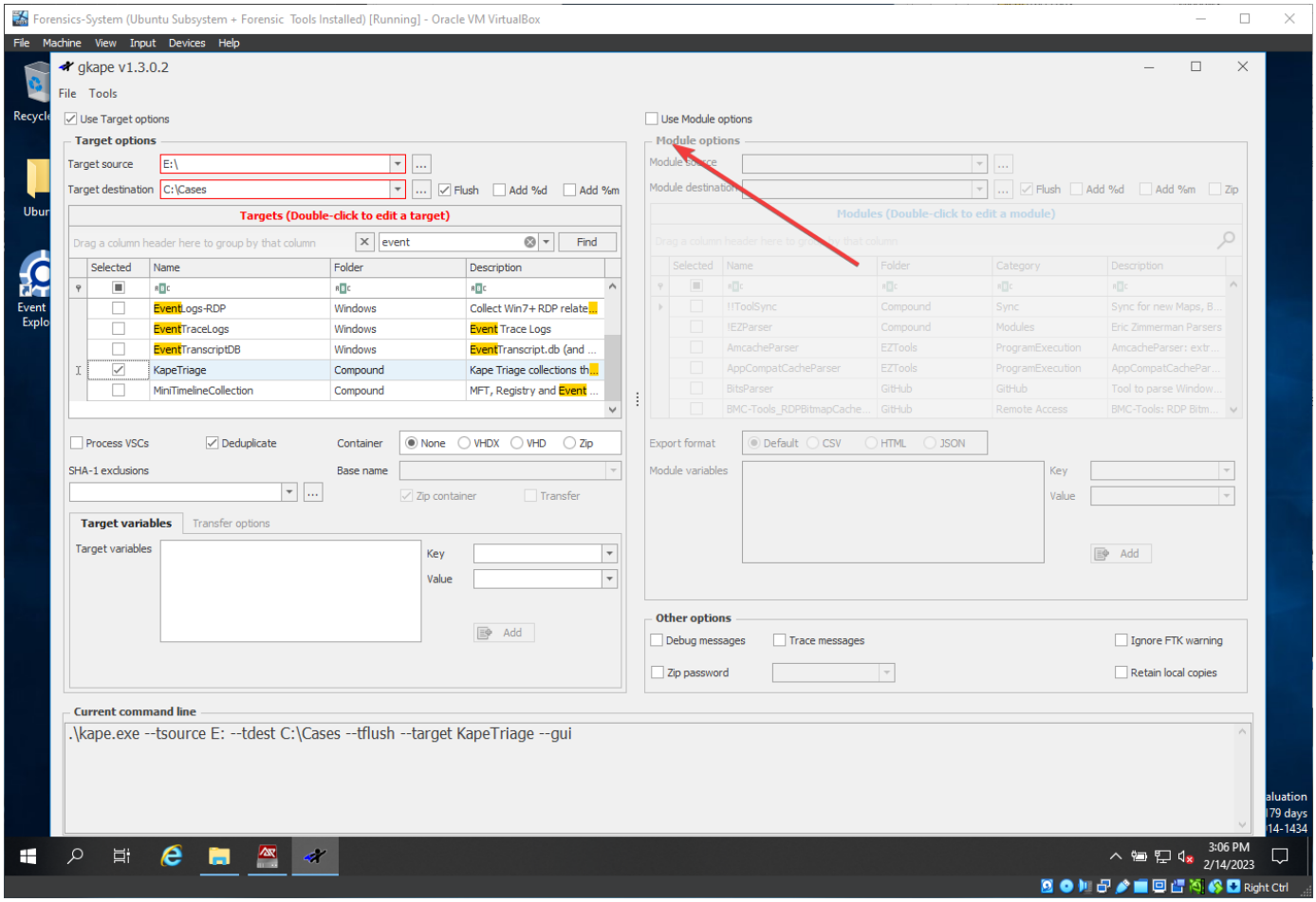
- We will collect files that are common for a windows forensic analysis:

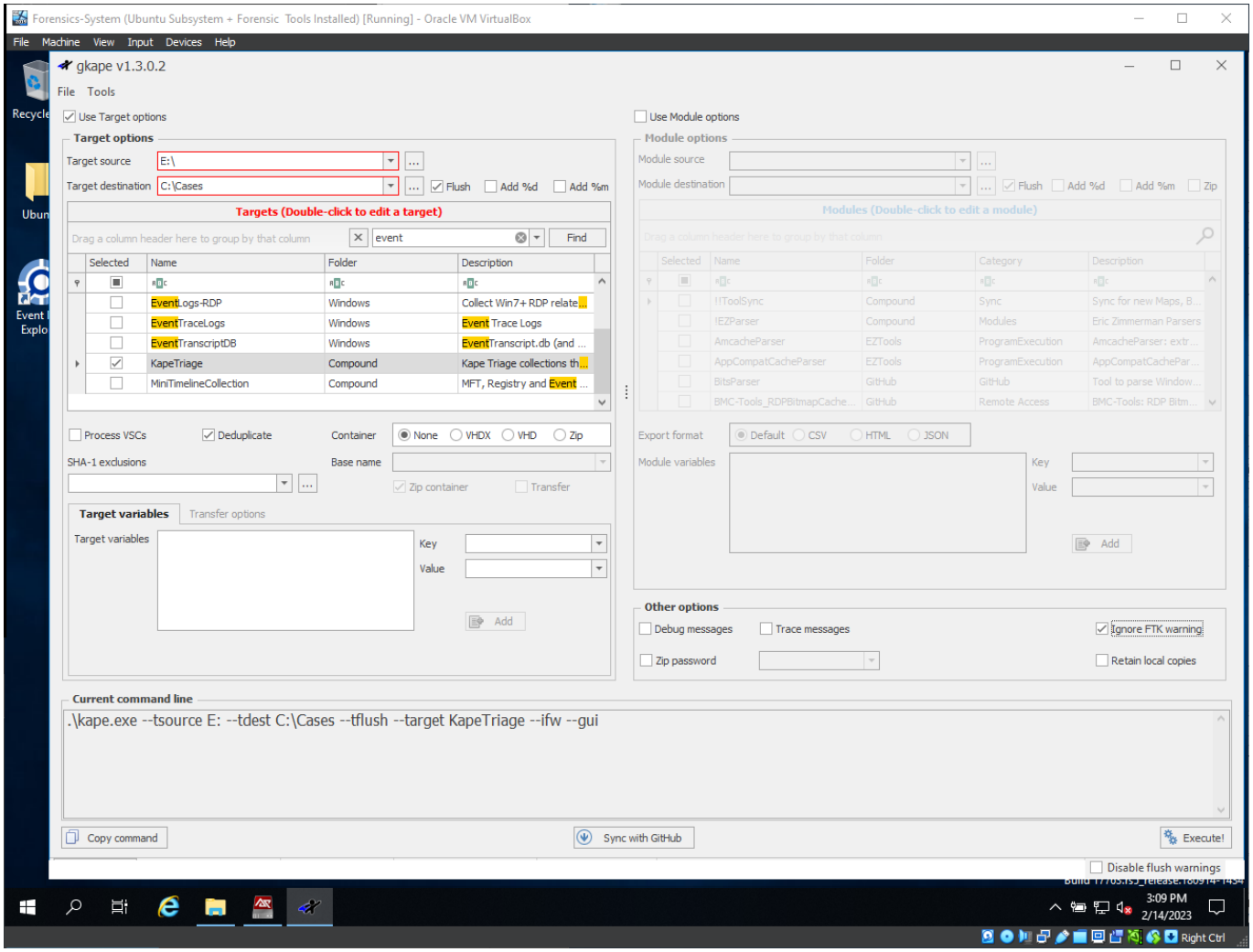


- What it will collect:

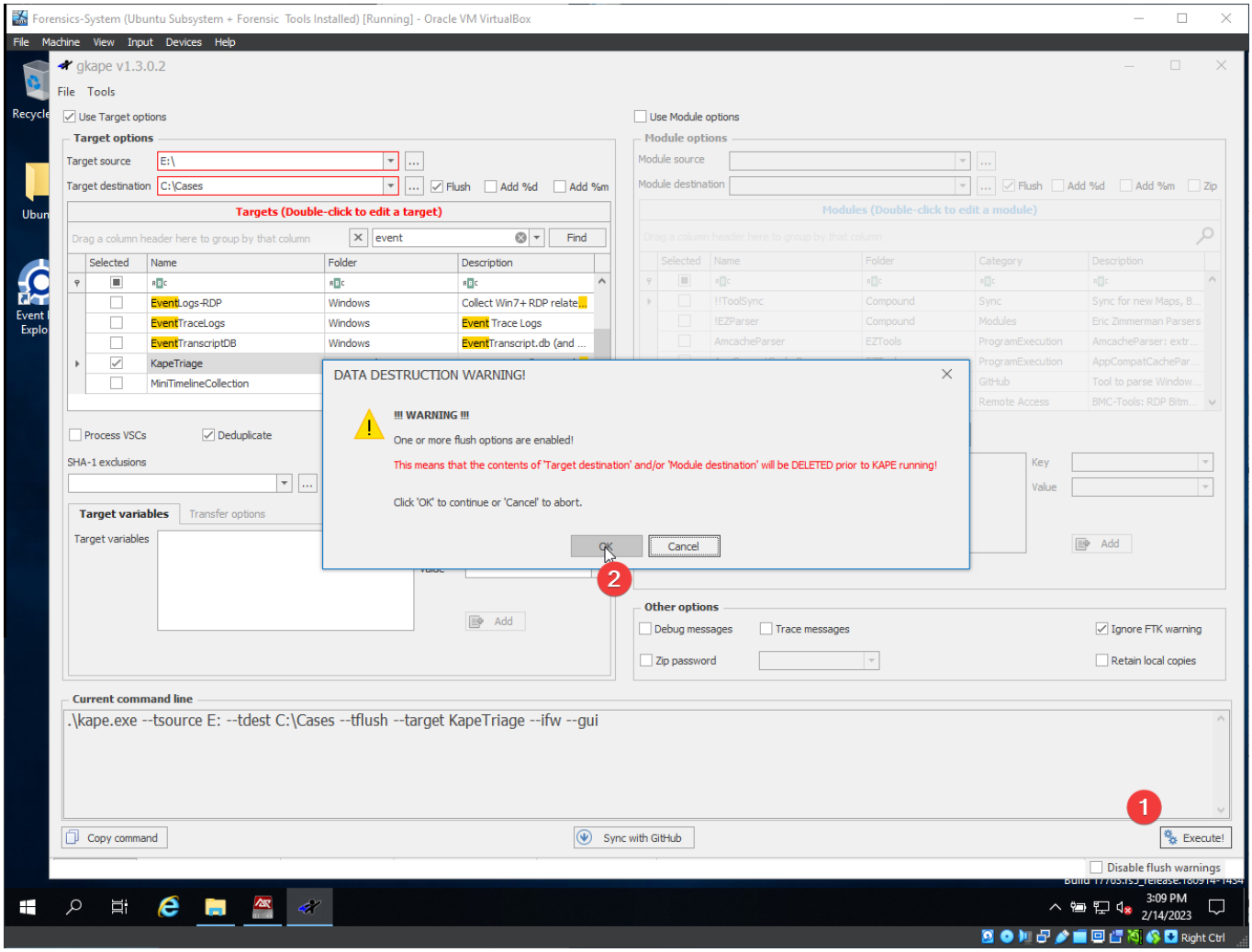


- This program has a feature that applies forensic analysis tools on the data, and exports it, but we will do the analysis manually in this case:

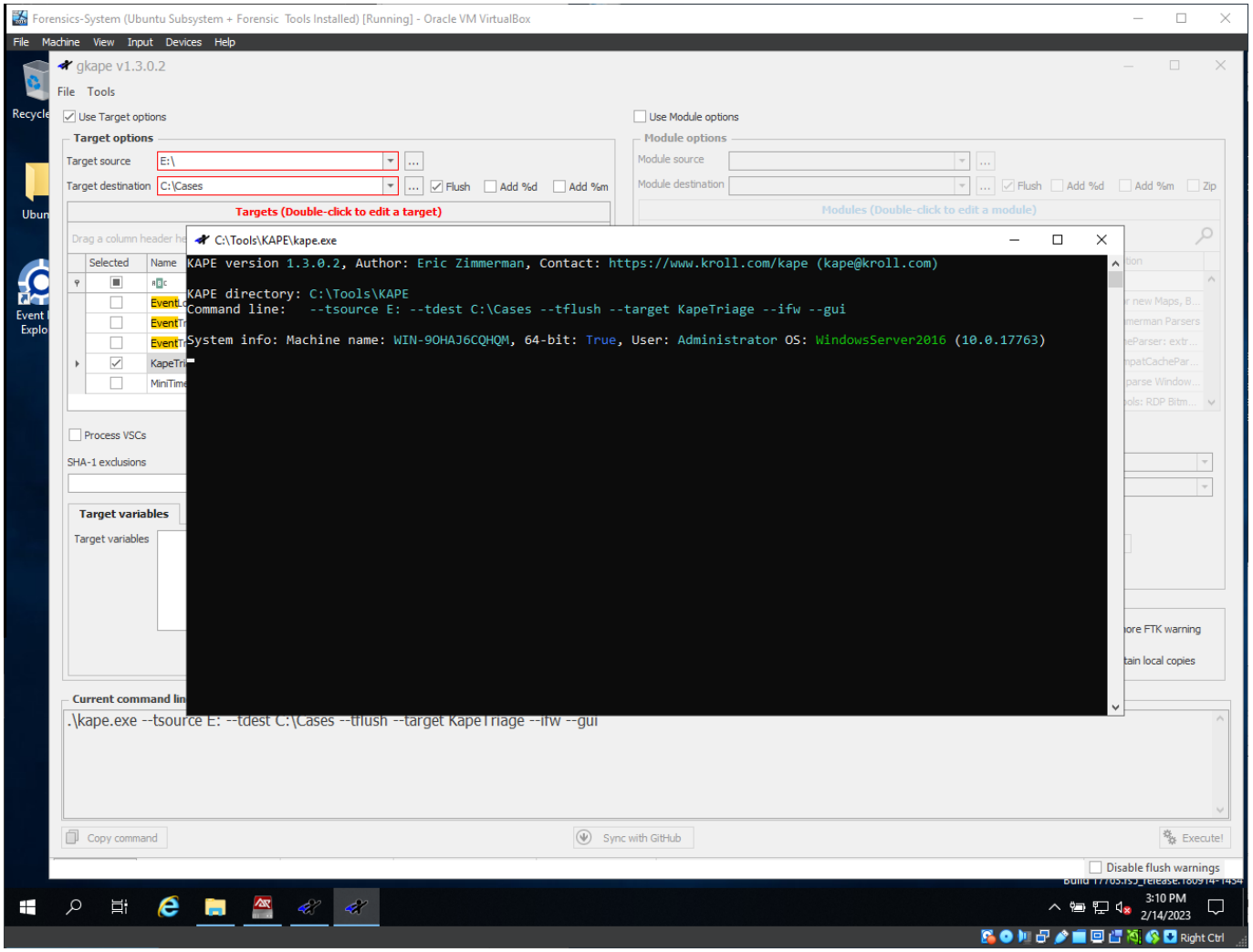

Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
gkape v1.3.0.2
File Tools
Use Target options
Target options
Target source E:\
Target destination C:\Cases
Flush
Add %d
Add %m
Targets (Double-click to edit a target)
Drag a column header here to group by that column
event
Find
Selected
Name
Folder
Description
EventLogs-RDP
Windows
Collect Win7+ RDP relate...
EventTraceLogs
Windows
Event Trace Logs
EventTranscriptDB
Windows
EventTranscript.db (and ...
KapeTriage
Compound
Kape Triage collections th...
MiniTimelineCollection
Compound
MFT, Registry and Event ...
Process VSCs
Deduplicate
Container
None
VHDX
VHD
Zip
SHA-1 exclusions
Base name
Zip container
Transfer
Target variables
Transfer options
Target variables
Key
Value
Add
Use Module options
Module options
Module source
Module destination
Flush
Add %d
Add %m
Zip
Modules (Double-click to edit a module)
Selected
Name
Folder
Category
Description
!!ToolSync
Compound
Sync
Sync for new Maps, B...
!EZParser
Compound
Modules
Eric Zimmerman Parsers
AmcacheParser
EZTools
ProgramExecution
AmcacheParser: extr...
AppCompatCacheParser
EZTools
ProgramExecution
AppCompatCachePar...
BitsParser
GitHub
GitHub
Tool to parse Window...
BMC-Tools_RDPBitmapCache...
GitHub
Remote Access
BMC-Tools: RDP Bitm...
Export format
Default
CSV
HTML
JSON
Module variables
Key
Value
Add
Other options
Debug messages
Trace messages
Ignore FTK warning
Zip password
Retain local copies
Current command line
.\kape.exe --tsource E: --tdest C:\Cases --tflush --target KapeTriage --gui
3:06 PM
2/14/2023
Right Ctrl

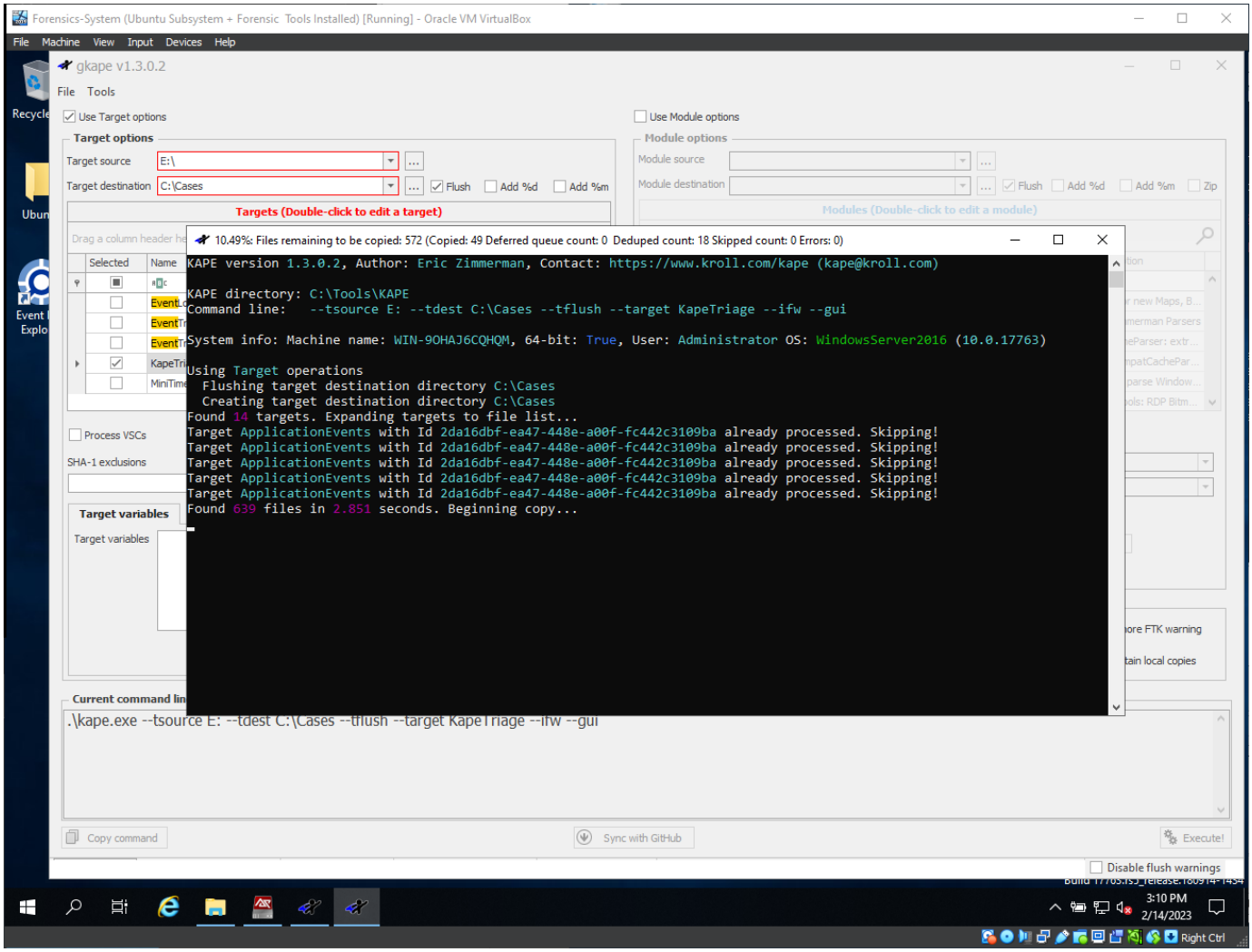

Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
gkape v1.3.0.2
File Tools
Use Target options
Target options
Target source E:\
Target destination C:\Cases
Flush Add %d Add %m
Targets (Double-click to edit a target)
Drag a column header here to group by that column
event
Find
Selected Name Folder Description
EventLogs-RDP Windows Collect Win7+ RDP relate...
EventTraceLogs Windows Event Trace Logs
EventTranscriptDB Windows EventTranscript.db (and ...
KapeTriage Compound Kape Triage collections th...
MiniTimelineCollection Compound MFT, Registry and Event ...
Process VSCs Deduplicate Container None VHDX VHD Zip
SHA-1 exclusions
Base name
Zip container Transfer
Target variables Transfer options
Target variables
Key
Value
Add
Use Module options
Module options
Module source
Module destination
Flush Add %d Add %m Zip
Modules (Double-click to edit a module)
Selected Name Folder Category Description
!!ToolSync Compound Sync Sync for new Maps, B...
!EZParser Compound Modules Eric Zimmerman Parsers
AmcacheParser EZTools ProgramExecution AmcacheParser: extr...
AppCompatCacheParser EZTools ProgramExecution AppCompatCachePar...
BitsParser GitHub GitHub Tool to parse Window...
BMC-Tools_RDPBitmapCache... GitHub Remote Access BMC-Tools: RDP Bitm...
Export format Default CSV HTML JSON
Module variables
Key
Value
Add
Other options
Debug messages Trace messages Ignore FTK warning
Zip password Retain local copies
Current command line
.\kape.exe --tsource E: --tdest C:\Cases --tflush --target KapeTriage --ifw --gui
Copy command
Sync with GitHub
Execute!
Disable flush warnings
3:09 PM
2/14/2023
Right Ctrl

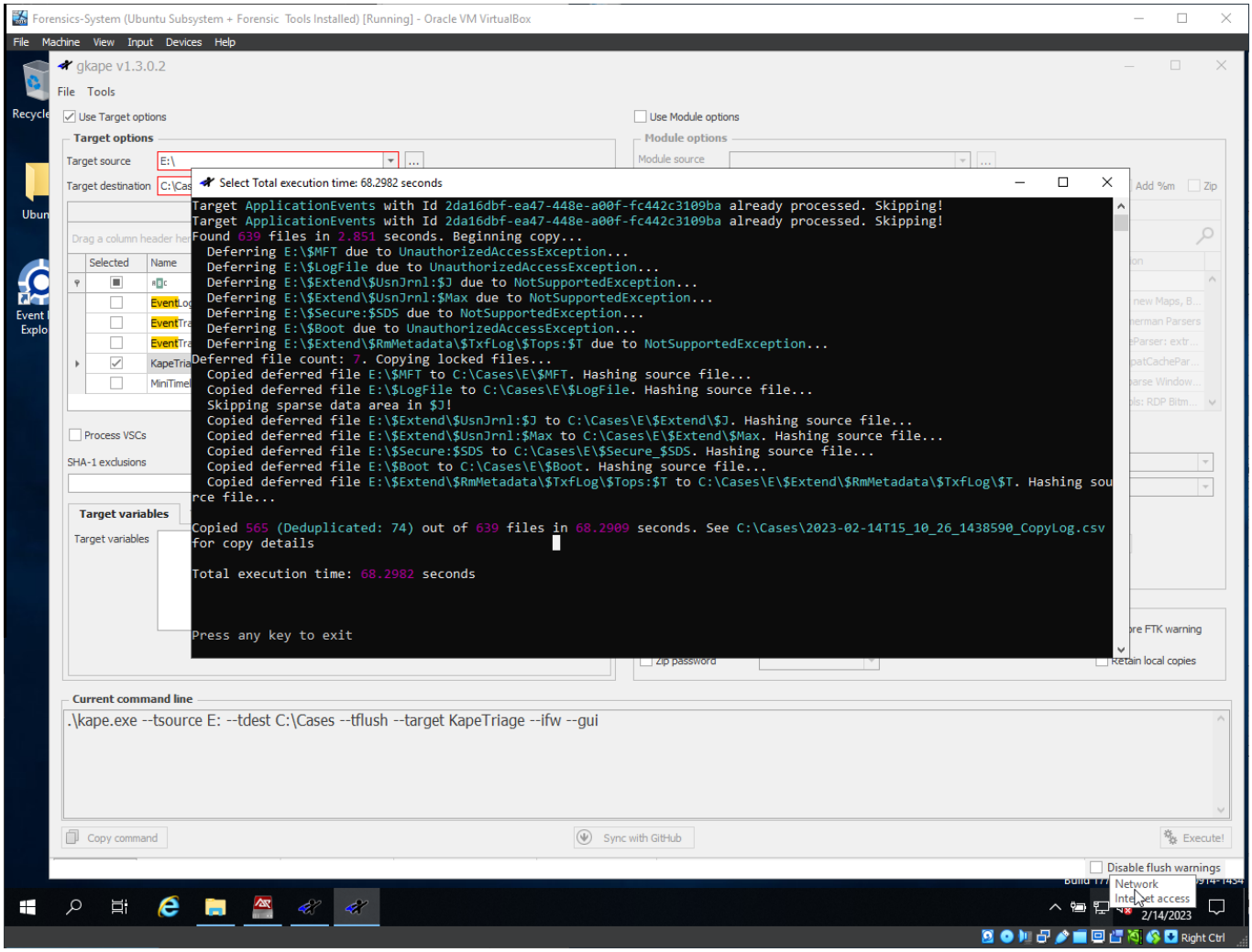
- Execute:

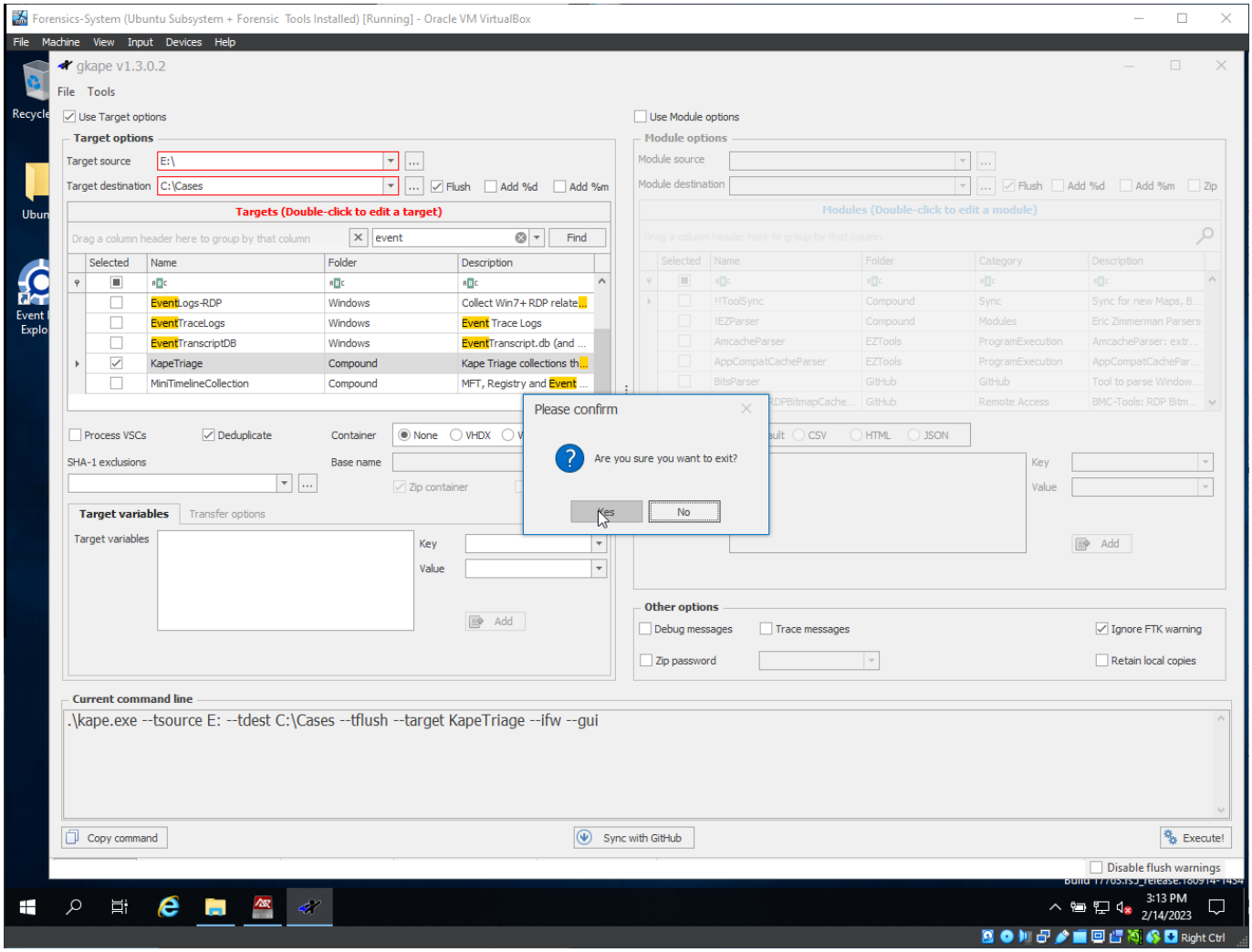


- It will open a terminal and execute the command:

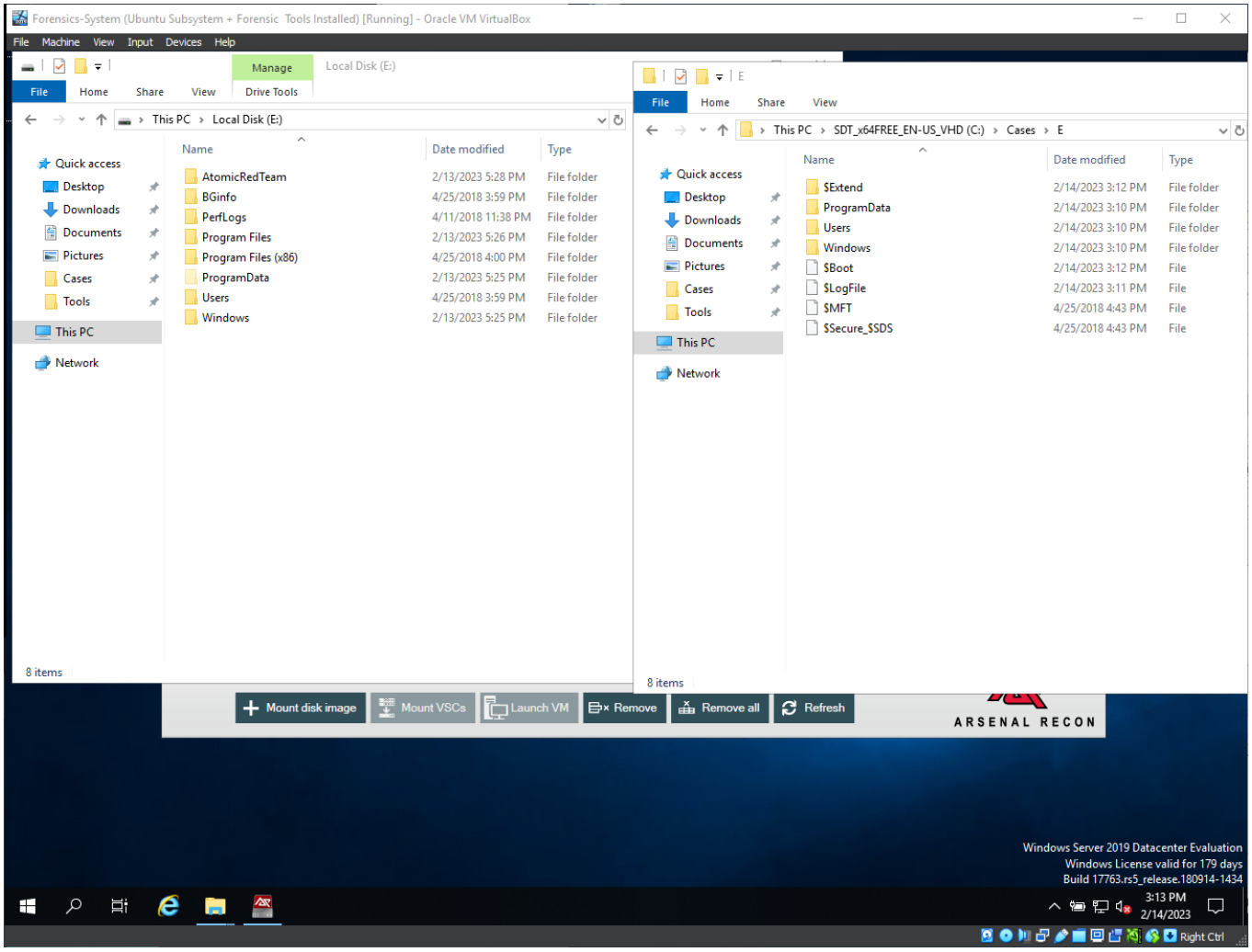

Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
gkape v1.3.0.2
File Tools
Use Target options
Target options
Target source E:\
Target destination C:\Cases
Flush Add %d Add %m
Targets (Double-click to edit a target)
Selected Name
Process VSCs
SHA-1 exclusions
Target variables
Use Module options
Module options
Module source
Module destination
Flush Add %d Add %m Zip
Modules (Double-click to edit a module)
C:\Tools\KAPE\kape.exe
KAPE version 1.3.0.2, Author: Eric Zimmerman, Contact: https://www.kroll.com/kape (kape@kroll.com)
KAPE directory: C:\Tools\KAPE
Command line: --tsource E: --tdest C:\Cases --tflush --target KapeTriage --ifw --gui
System info: Machine name: WIN-9OHAJ6CQHQM, 64-bit: True, User: Administrator OS: WindowsServer2016 (10.0.17763)
Current command line
.\kape.exe --tsource E: --tdest C:\Cases --tflush --target KapeTriage --ifw --gui
Copy command
Sync with GitHub
Execute!
Disable flush warnings
3:10 PM
2/14/2023
Right Ctrl


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
gkape v1.3.0.2
File Tools
Use Target options
Target options
Target source E:\
Target destination C:\Cases
Flush Add %d Add %m
Targets (Double-click to edit a target)
Use Module options
Module options
Module source
Module destination
Flush Add %d Add %m Zip
Modules (Double-click to edit a module)
Process VSCs
SHA-1 exclusions
Target variables
Target variables
Current command line
.\kape.exe --tsource E: --tdest C:\Cases --tflush --target KapeTriage --ifw --gui
Copy command
Sync with GitHub
Execute!
Disable flush warnings
10.49%: Files remaining to be copied: 572 (Copied: 49 Deferred queue count: 0 Deduped count: 18 Skipped count: 0 Errors: 0)
KAPE version 1.3.0.2, Author: Eric Zimmerman, Contact: https://www.kroll.com/kape (kape@kroll.com)
KAPE directory: C:\Tools\KAPE
Command line: --tsource E: --tdest C:\Cases --tflush --target KapeTriage --ifw --gui
System info: Machine name: WIN-9OHAJ6CQHQM, 64-bit: True, User: Administrator OS: WindowsServer2016 (10.0.17763)
Using Target operations
Flushing target destination directory C:\Cases
Creating target destination directory C:\Cases
Found 14 targets. Expanding targets to file list...
Target ApplicationEvents with Id 2da16dbf-ea47-448e-a00f-fc442c3109ba already processed. Skipping!
Target ApplicationEvents with Id 2da16dbf-ea47-448e-a00f-fc442c3109ba already processed. Skipping!
Target ApplicationEvents with Id 2da16dbf-ea47-448e-a00f-fc442c3109ba already processed. Skipping!
Target ApplicationEvents with Id 2da16dbf-ea47-448e-a00f-fc442c3109ba already processed. Skipping!
Target ApplicationEvents with Id 2da16dbf-ea47-448e-a00f-fc442c3109ba already processed. Skipping!
Found 639 files in 2.851 seconds. Beginning copy...
3:10 PM
2/14/2023
Right Ctrl


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
gkape v1.3.0.2
File Tools
Use Target options
Target options
Target source E:\
Target destination C:\Cas
Use Module options
Module options
Module source
Select Total execution time: 68.2982 seconds
Target ApplicationEvents with Id 2da16dbf-ea47-448e-a00f-fc442c3109ba already processed. Skipping!
Target ApplicationEvents with Id 2da16dbf-ea47-448e-a00f-fc442c3109ba already processed. Skipping!
Found 639 files in 2.851 seconds. Beginning copy...
Deferring E:\$MFT due to UnauthorizedAccessException...
Deferring E:\$LogFile due to UnauthorizedAccessException...
Deferring E:\$Extend\$UsnJrnl:$J due to NotSupportedException...
Deferring E:\$Extend\$UsnJrnl:$Max due to NotSupportedException...
Deferring E:\$Secure:$SDS due to NotSupportedException...
Deferring E:\$Boot due to UnauthorizedAccessException...
Deferring E:\$Extend\$RmMetadata\$TxfLog\$Tops:$T due to NotSupportedException...
Deferred file count: 7. Copying locked files...
Copied deferred file E:\$MFT to C:\Cases\E\$MFT. Hashing source file...
Copied deferred file E:\$LogFile to C:\Cases\E\$LogFile. Hashing source file...
Skipping sparse data area in $J!
Copied deferred file E:\$Extend\$UsnJrnl:$J to C:\Cases\E\$Extend\$J. Hashing source file...
Copied deferred file E:\$Extend\$UsnJrnl:$Max to C:\Cases\E\$Extend\$Max. Hashing source file...
Copied deferred file E:\$Secure:$SDS to C:\Cases\E\$Secure_$SDS. Hashing source file...
Copied deferred file E:\$Boot to C:\Cases\E\$Boot. Hashing source file...
Copied deferred file E:\$Extend\$RmMetadata\$TxfLog\$Tops:$T to C:\Cases\E\$Extend\$RmMetadata\$TxfLog\$T. Hashing source file...
Copied 565 (Deduplicated: 74) out of 639 files in 68.2909 seconds. See C:\Cases\2023-02-14T15_10_26_1438590_CopyLog.csv for copy details
Total execution time: 68.2982 seconds
Press any key to exit
Process VSCs
SHA-1 exclusions
Target variables
Target variables
Current command line
.\kape.exe --tsource E: --tdest C:\Cases --tflush --target KapeTriage --ifw --gui
Copy command
Sync with GitHub
Execute!
Disable flush warnings
Network
Internet access
2/14/2023
Right Ctrl



- Comparation of the files structure:


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Manage
Local Disk (E:)
File Home Share View Drive Tools
This PC › Local Disk (E:)
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
This PC
Network
Name
Date modified
Type
AtomicRedTeam 2/13/2023 5:28 PM File folder
BGinfo 4/25/2018 3:59 PM File folder
PerfLogs 4/11/2018 11:38 PM File folder
Program Files 2/13/2023 5:26 PM File folder
Program Files (x86) 4/25/2018 4:00 PM File folder
ProgramData 2/13/2023 5:25 PM File folder
Users 4/25/2018 3:59 PM File folder
Windows 2/13/2023 5:25 PM File folder
8 items
File Home Share View
This PC › SDT_x64FREE_EN-US_VHD (C:) › Cases › E
$Extend 2/14/2023 3:12 PM File folder
ProgramData 2/14/2023 3:10 PM File folder
Users 2/14/2023 3:10 PM File folder
Windows 2/14/2023 3:10 PM File folder
$Boot 2/14/2023 3:12 PM File
$LogFile 2/14/2023 3:11 PM File
$MFT 4/25/2018 4:43 PM File
$Secure_$SDS 4/25/2018 4:43 PM File
8 items
Mount disk image
Mount VSCs
Launch VM
Remove
Remove all
Refresh
ARSENAL RECON
Windows Server 2019 Datacenter Evaluation
Windows License valid for 179 days
Build 17763.rs5_release.180914-1434
3:13 PM
2/14/2023
Right Ctrl