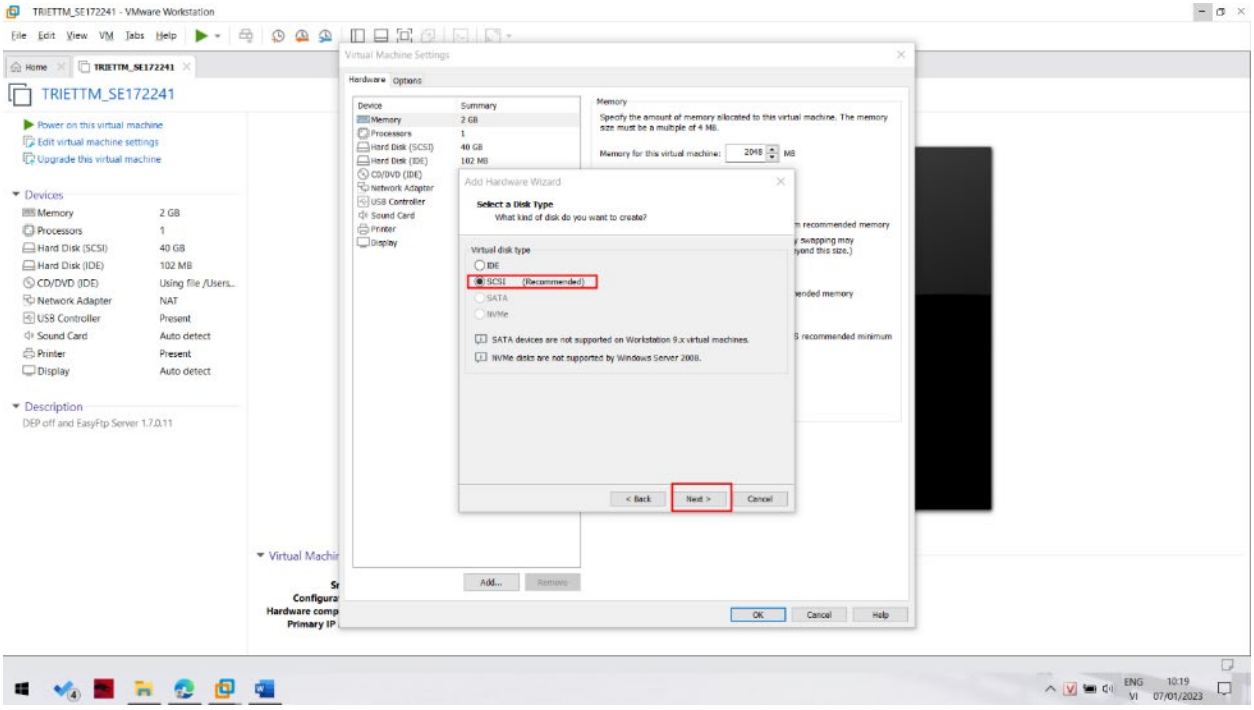
Lab 11: Using FTK

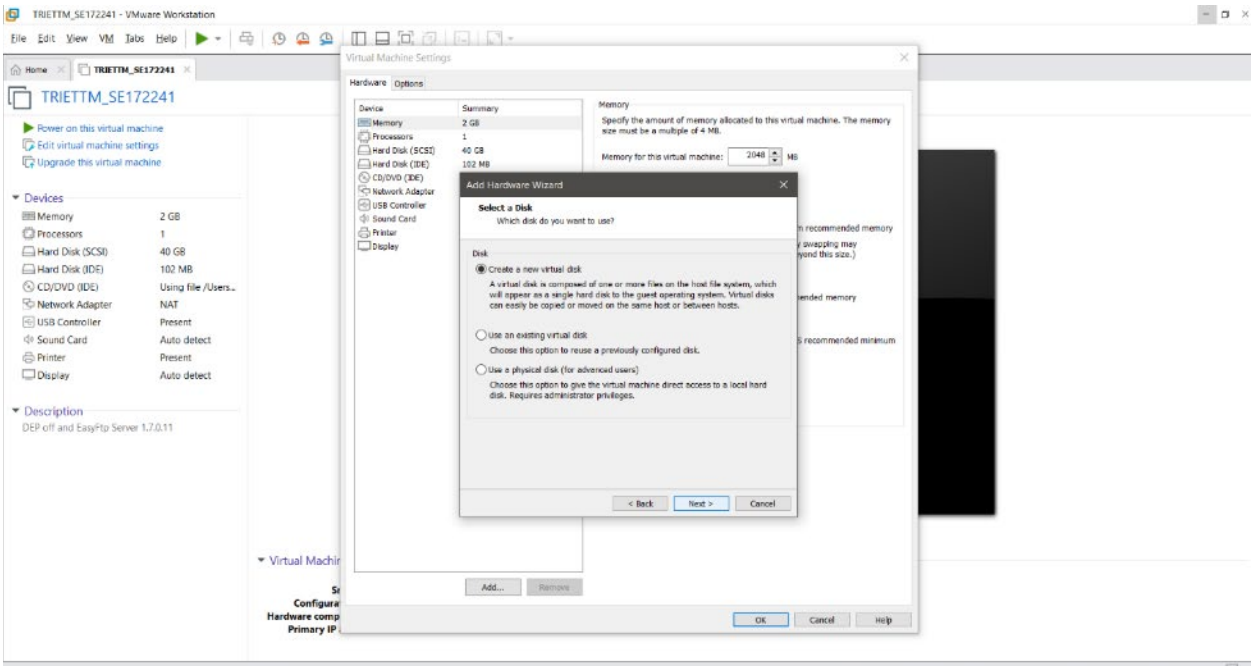
Making a Clean Disk

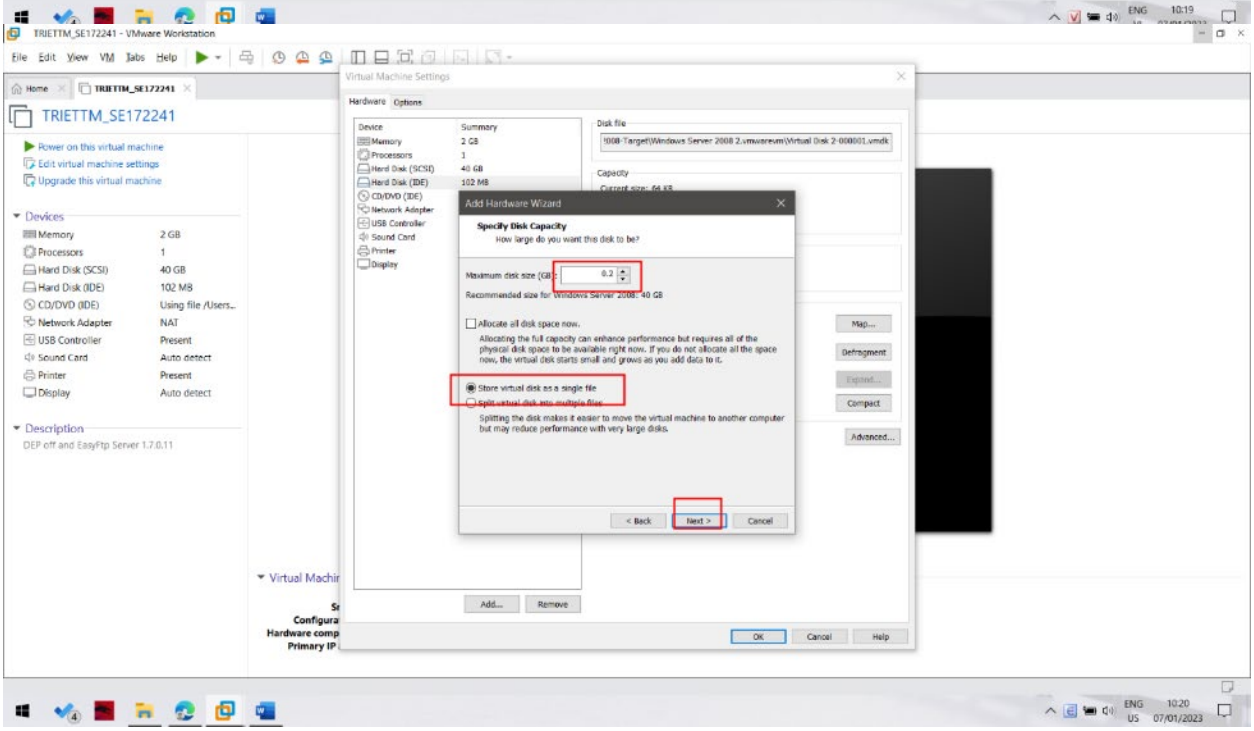
You should have a small virtual hard drive attached to your VM, which you created in a previous project. If you don't have one, create one now, or plug in a USB flash drive. It doesn't matter what data is on it for now

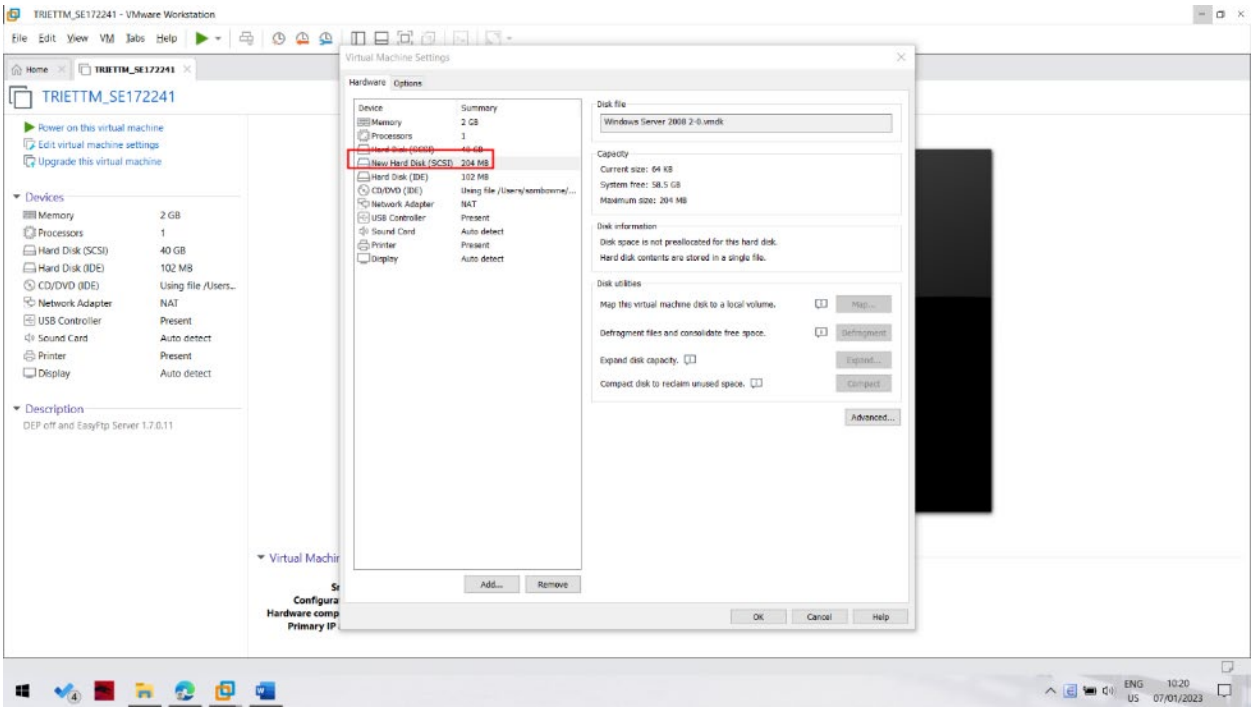
Click Start, right-click "My Computer", and click Manage.

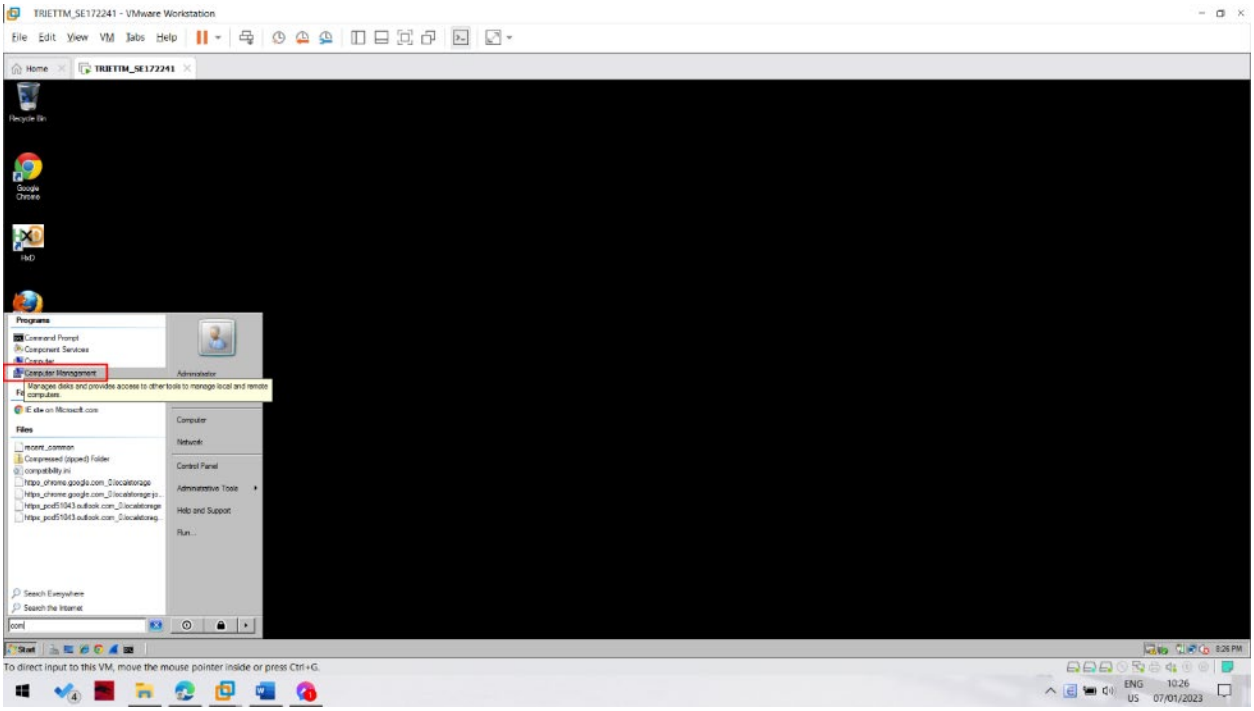
You should see your second small disk labelled "Disk 1", as shown, e.g. below.

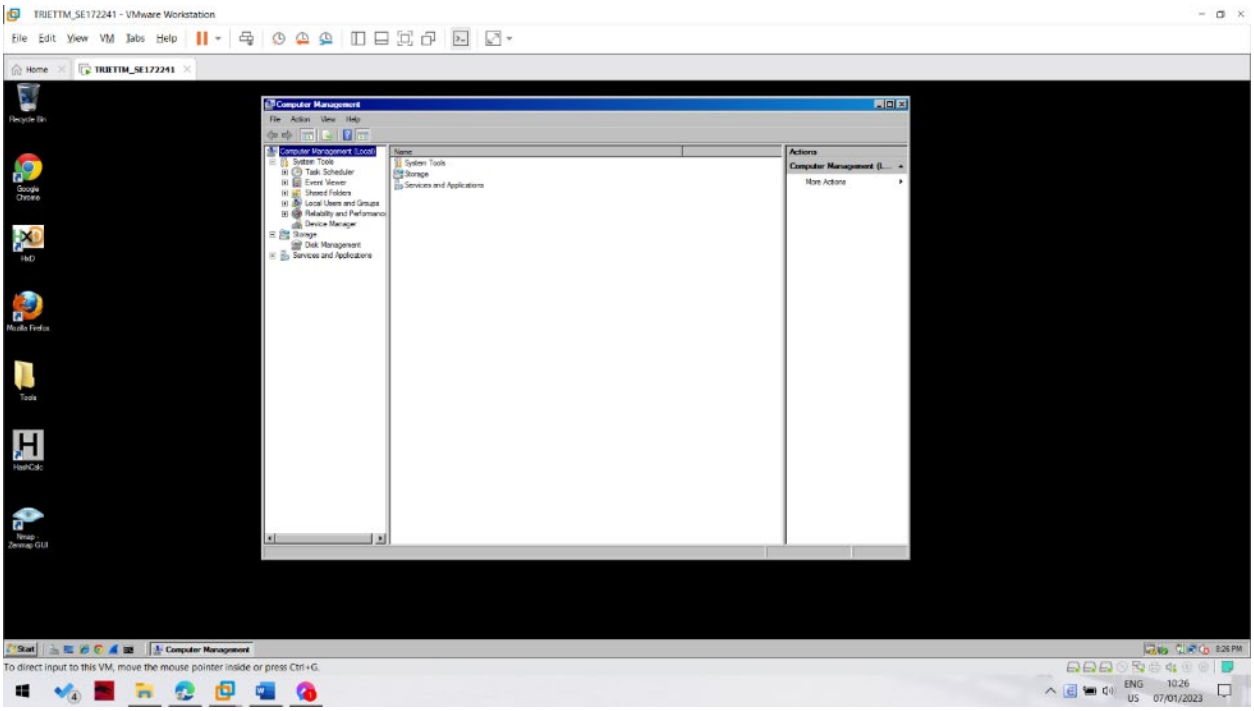


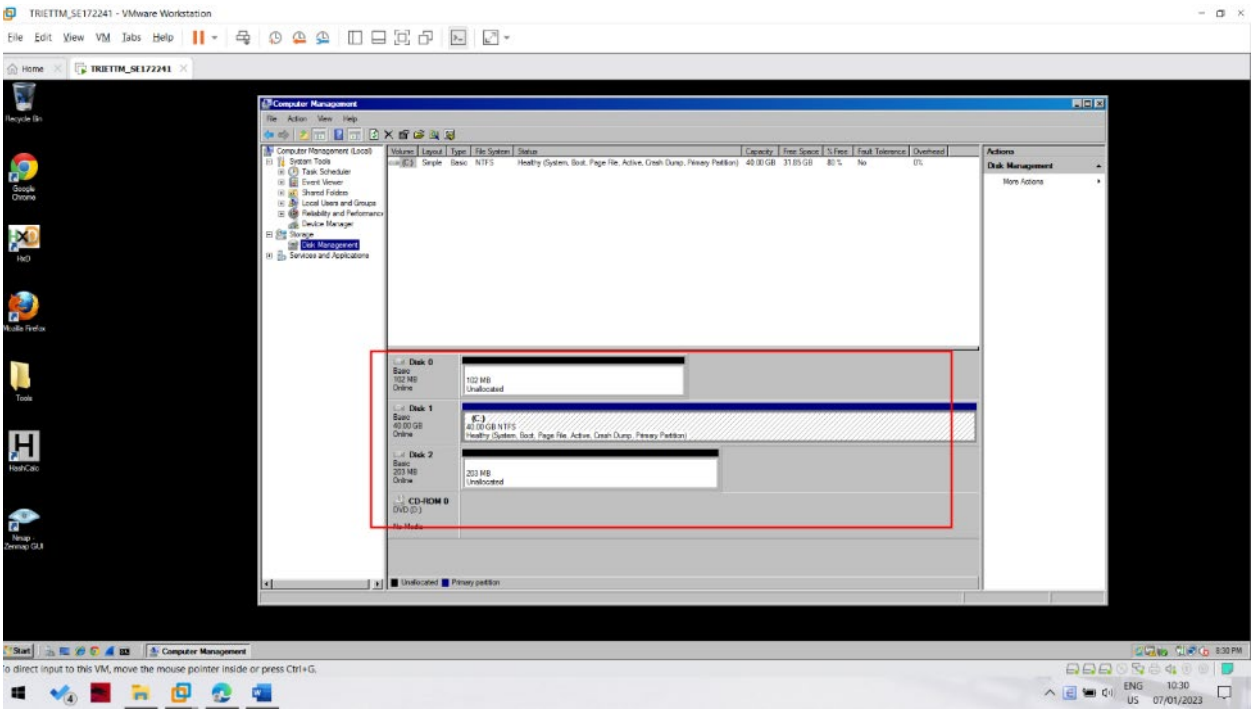

TRIETTM_SE172241 - VMware Workstation
File Edit View VM Tabs Help
TRIETTM_SE172241
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine
Devices
Memory 2 GB
Processors 1
Hard Disk (SCSI) 40 GB
Hard Disk (IDE) 102 MB
CD/DVD (IDE) Using file /Users...
Network Adapter NAT
USB Controller Present
Sound Card Auto detect
Printer Present
Display Auto detect
Description
DEP off and EasyFtp Server 1.7.0.11
Virtual Machine Settings
Hardware Options
Device Summary
Memory 2 GB
Processors 1
Hard Disk (SCSI) 40 GB
Hard Disk (IDE) 102 MB
CD/DVD (IDE)
Network Adapter
USB Controller
Sound Card
Printer
Display
Memory
Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.
Memory for this virtual machine: 2048 MB
Add Hardware Wizard
Select a Disk
Which disk do you want to use?
Disk
Create a new virtual disk
A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts.
Use an existing virtual disk
Choose this option to reuse a previously configured disk.
Use a physical disk (for advanced users)
Choose this option to give the virtual machine direct access to a local hard disk. Requires administrator privileges.
< Back Next > Cancel
Add... Remove
OK Cancel Help
ENG US 10:19 07/01/2023


TRIETTM_SE172241 - VMware Workstation
File Edit View VM Tabs Help
TRIETTM_SE172241
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine
Devices
Memory 2 GB
Processors 1
Hard Disk (SCSI) 40 GB
Hard Disk (IDE) 102 MB
CD/DVD (IDE) Using file /Users...
Network Adapter NAT
USB Controller Present
Sound Card Auto detect
Printer Present
Display Auto detect
Description
DEP off and EasyFtp Server 1.7.0.11
Virtual Machine Settings
Hardware Options
Device Summary
Memory 2 GB
Processors 1
Hard Disk (SCSI) 40 GB
Hard Disk (IDE) 102 MB
CD/DVD (IDE)
Network Adapter
USB Controller
Sound Card
Printer
Display
Disk file
1008-Target\Windows Server 2008 2.vmwarevm\Virtual Disk 2-000001.vmdk
Capacity
Add Hardware Wizard
Specify Disk Capacity
How large do you want this disk to be?
Maximum disk size (GB): 0.2
Recommended size for Windows Server 2008: 40 GB
Allocate all disk space now.
Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.
Store virtual disk as a single file
Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Map...
Defragment
Expand...
Compact
Advanced...
< Back Next > Cancel
Add... Remove
OK Cancel Help
ENG US 10:20 07/01/2023


TRIETTM_SE172241 - VMware Workstation
File Edit View VM Tabs Help
Home
TRIETTM_SE172241
TRIETTM_SE172241
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine
Devices
Memory 2 GB
Processors 1
Hard Disk (SCSI) 40 GB
Hard Disk (IDE) 102 MB
CD/DVD (IDE) Using file /Users...
Network Adapter NAT
USB Controller Present
Sound Card Auto detect
Printer Present
Display Auto detect
Description
DEP off and EasyFtp Server 1.7.0.11
Virtual Machine Settings
Hardware Options
Device Summary
Memory 2 GB
Processors 1
New Hard Disk (SCSI) 204 MB
Hard Disk (IDE) 102 MB
CD/DVD (IDE) Using file /Users/sambowne/...
Network Adapter NAT
USB Controller Present
Sound Card Auto detect
Printer Present
Display Auto detect
Add... Remove
Disk file
Windows Server 2008 2-0.vmdk
Capacity
Current size: 64 KB
System free: 58.5 GB
Maximum size: 204 MB
Disk information
Disk space is not preallocated for this hard disk.
Hard disk contents are stored in a single file.
Disk utilities
Map this virtual machine disk to a local volume. Map...
Defragment files and consolidate free space. Defragment
Expand disk capacity. Expand...
Compact disk to reclaim unused space. Compact
Advanced...
OK Cancel Help
ENG US 10:20 07/01/2023


TRIETTM_SE172241 - VMware Workstation
File Edit View VM Tabs Help
Home
TRIETTM_SE172241
Recycle Bin
Google Chrome
HxD
Programs
Command Prompt
Component Services
Computer
Computer Management
Manages disks and provides access to other tools to manage local and remote computers.
Files
Computer
Network
Control Panel
Administrative Tools
Help and Support
Run...
Search Everywhere
Search the Internet
com
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG US 10:26 07/01/2023





Click Start, Run. Type CMD and press Enter.

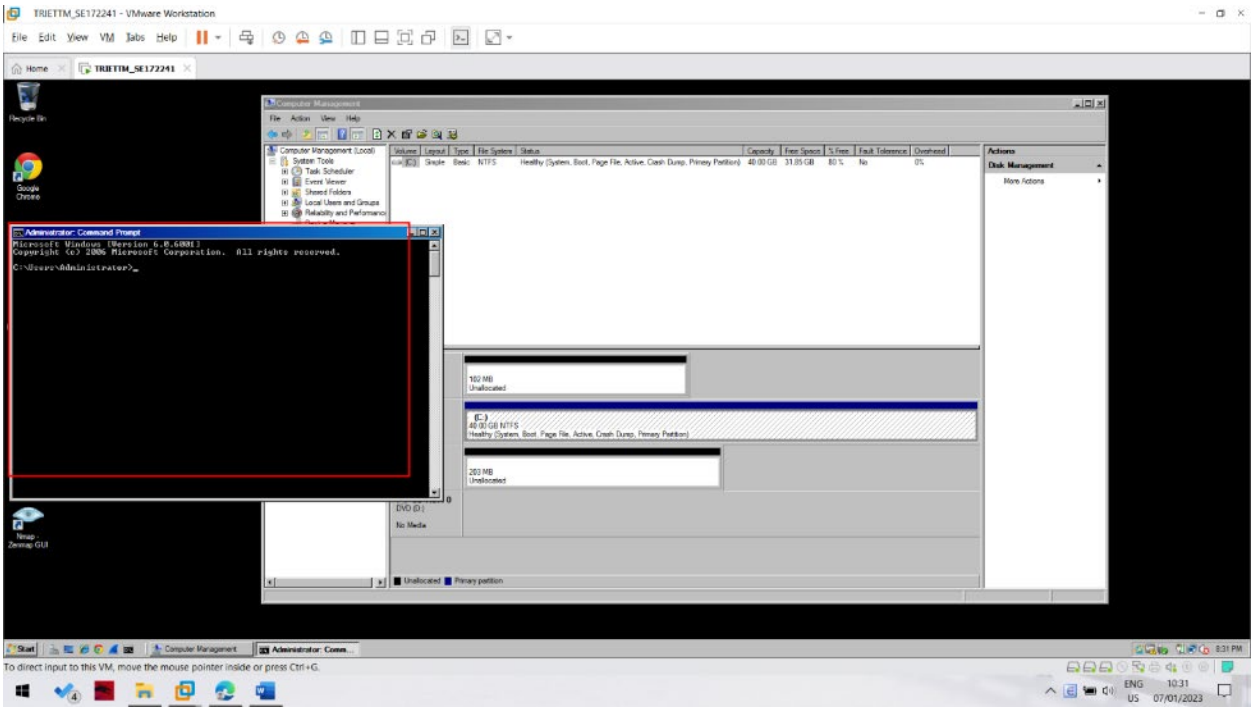
Execute these commands to clean your second disk. Be careful not to erase the wrong disk!

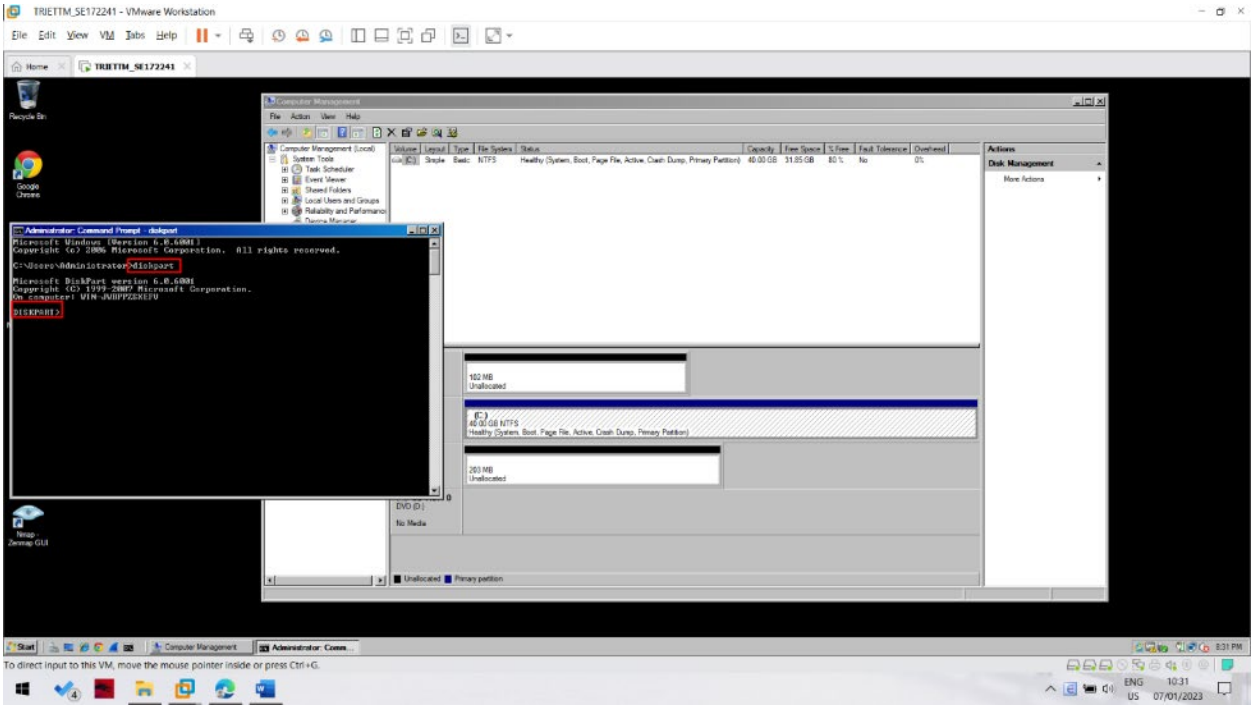
DISKPART

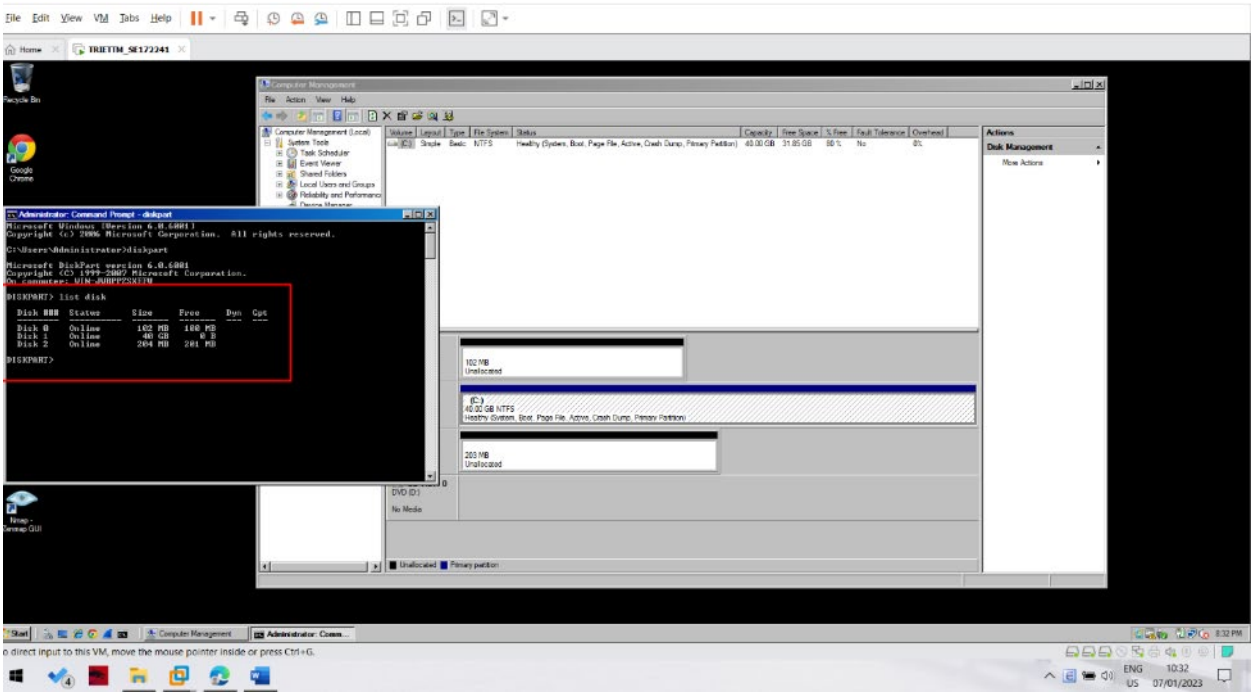
LIST DISK

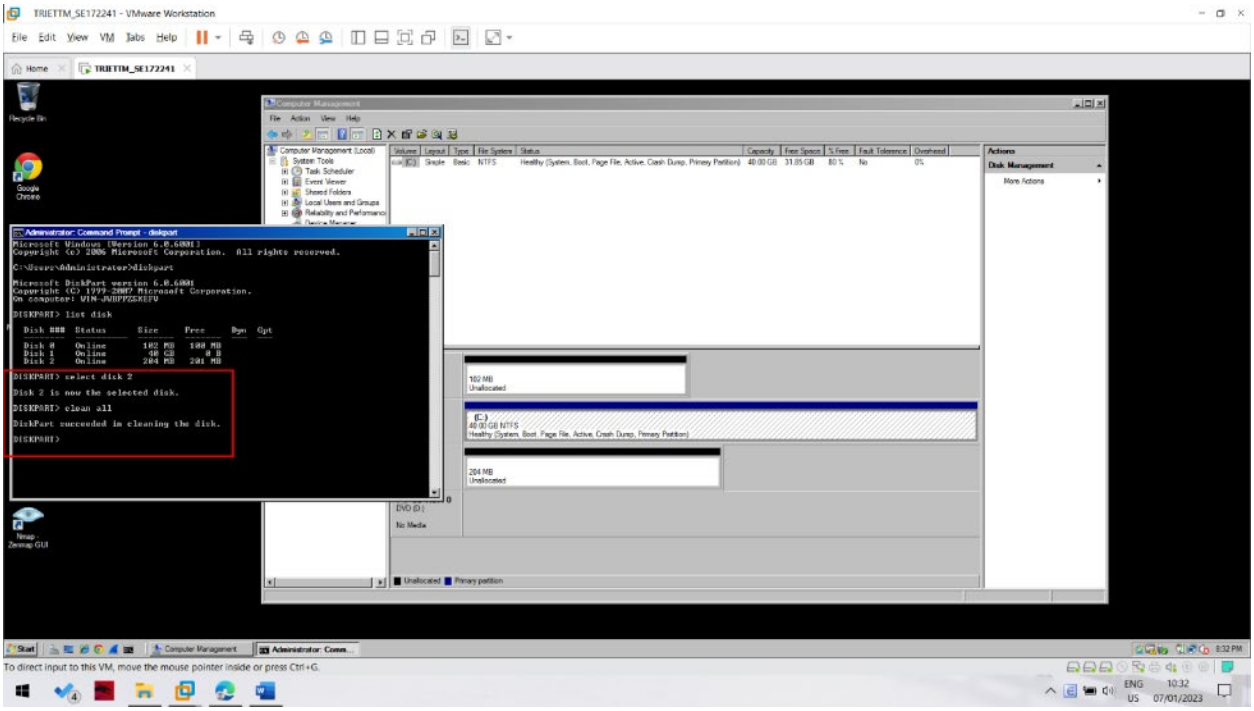
SELECT DISK 1

CLEAN ALL

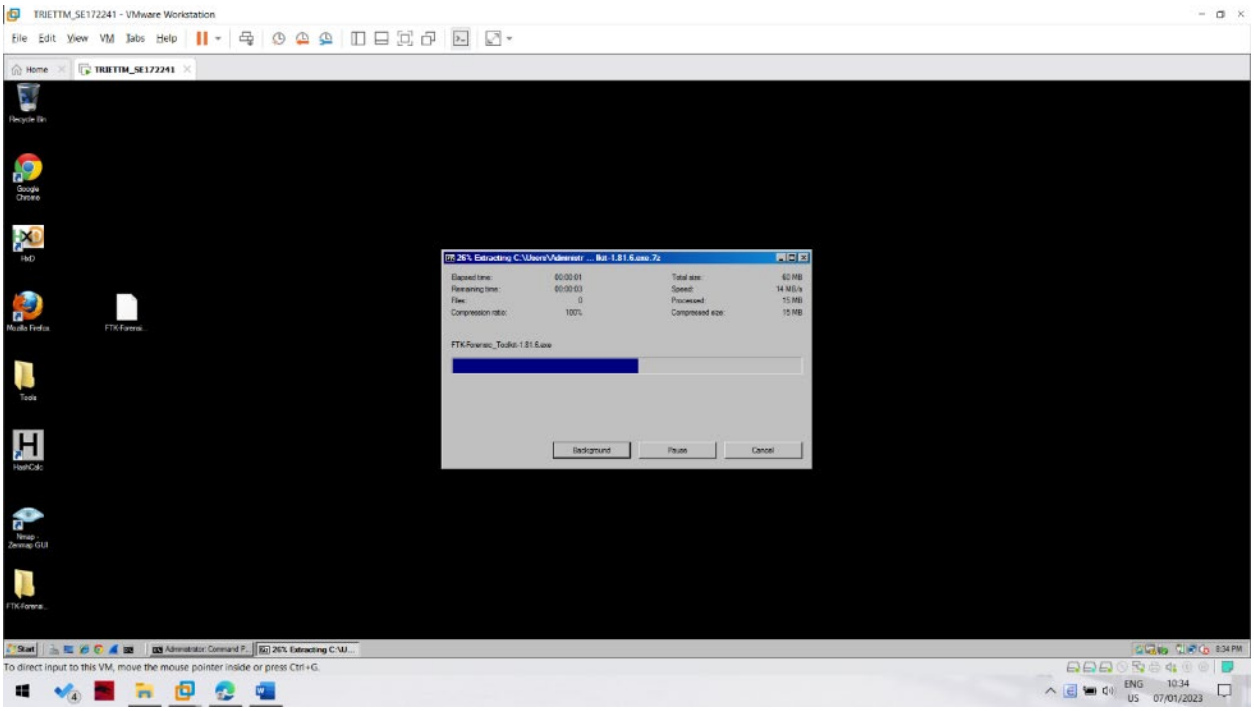


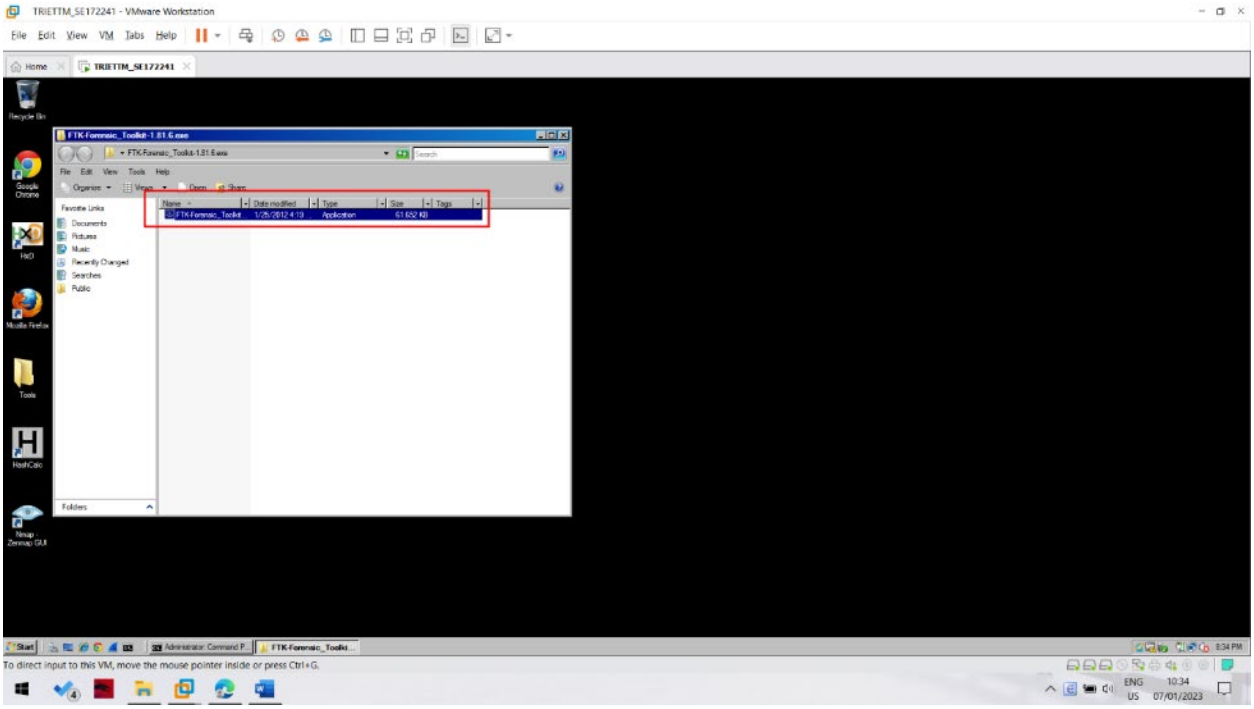


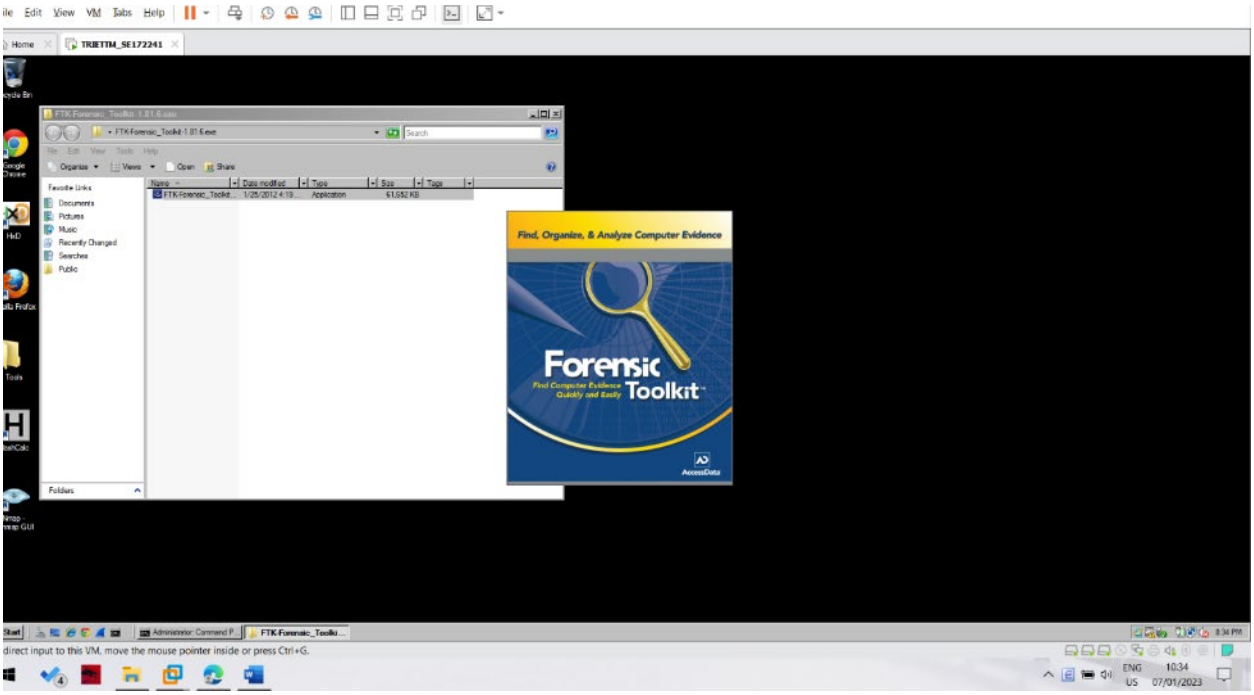


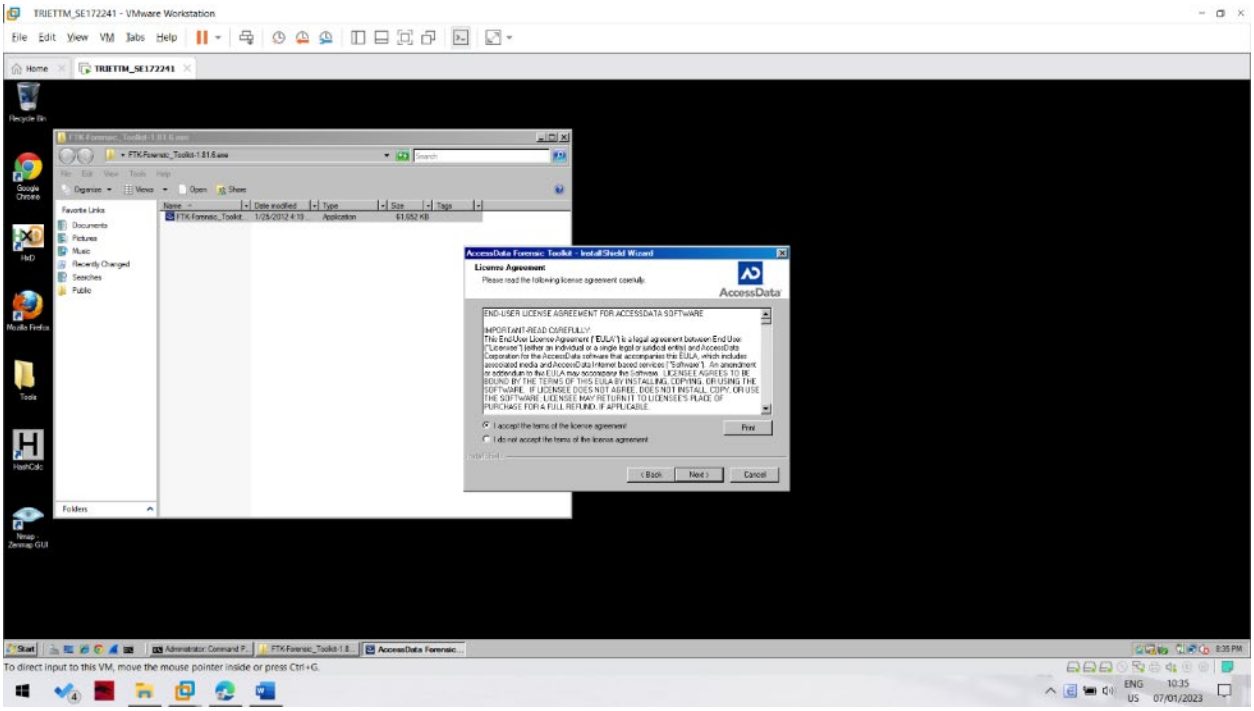


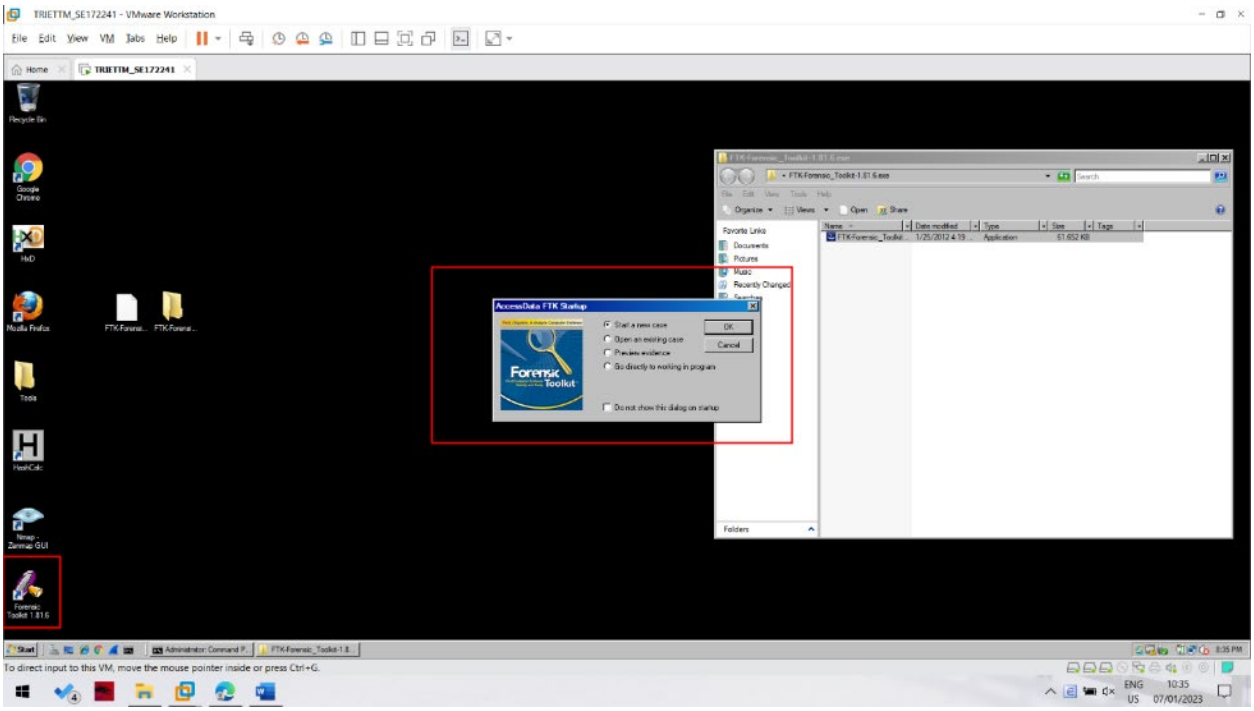
Downloading FTK

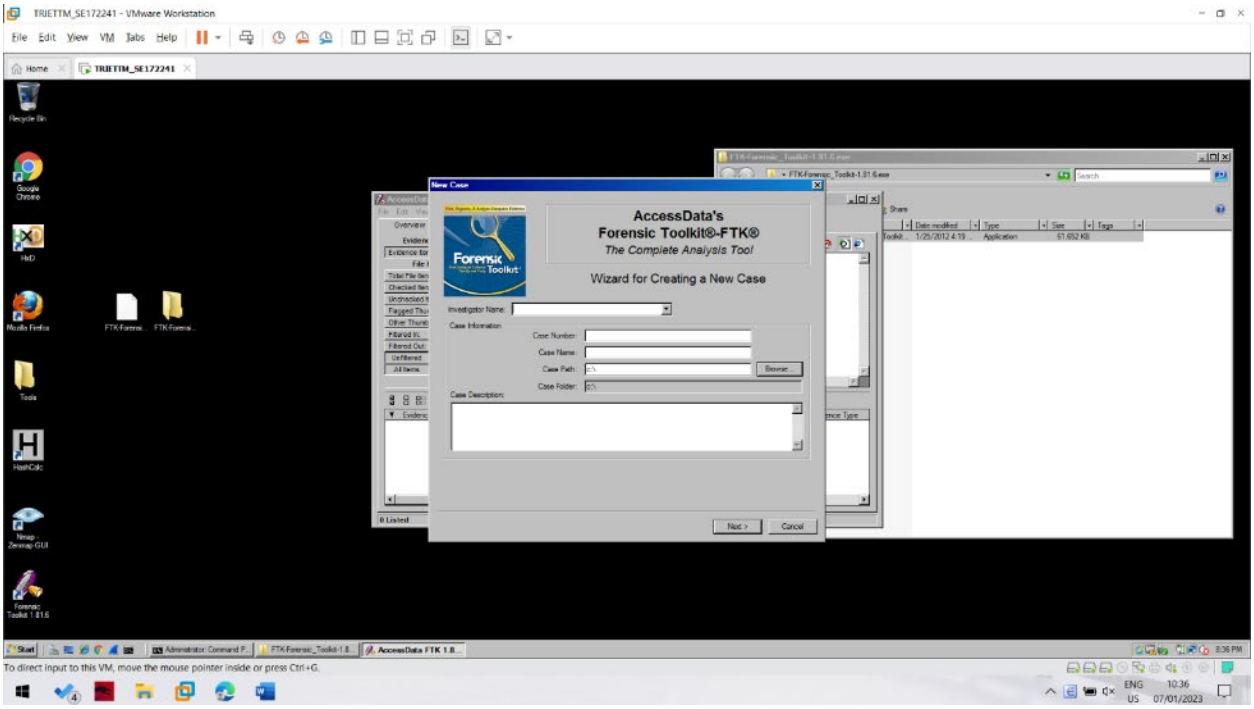

TRIETTM_SE172241 - VMware Workstation
File Edit View VM Tabs Help
Home
TRIETTM_SE172241
Recycle Bin
Google Chrome
HxD
Mozilla Firefox
FTK Forensi...
Tools
HashCalc
Nmap - Zenmap GUI
FTK Forensi...
26% Extracting C:\Users\Administr ... lkit-1.81.6.exe.7z
Elapsed time:
Remaining time:
Files:
Compression ratio:
Total size:
Speed:
Processed:
Compressed size:
FTK-Forensic_Toolkit-1.81.6.exe
Background
Pause
Cancel
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG
US
10:34
07/01/2023

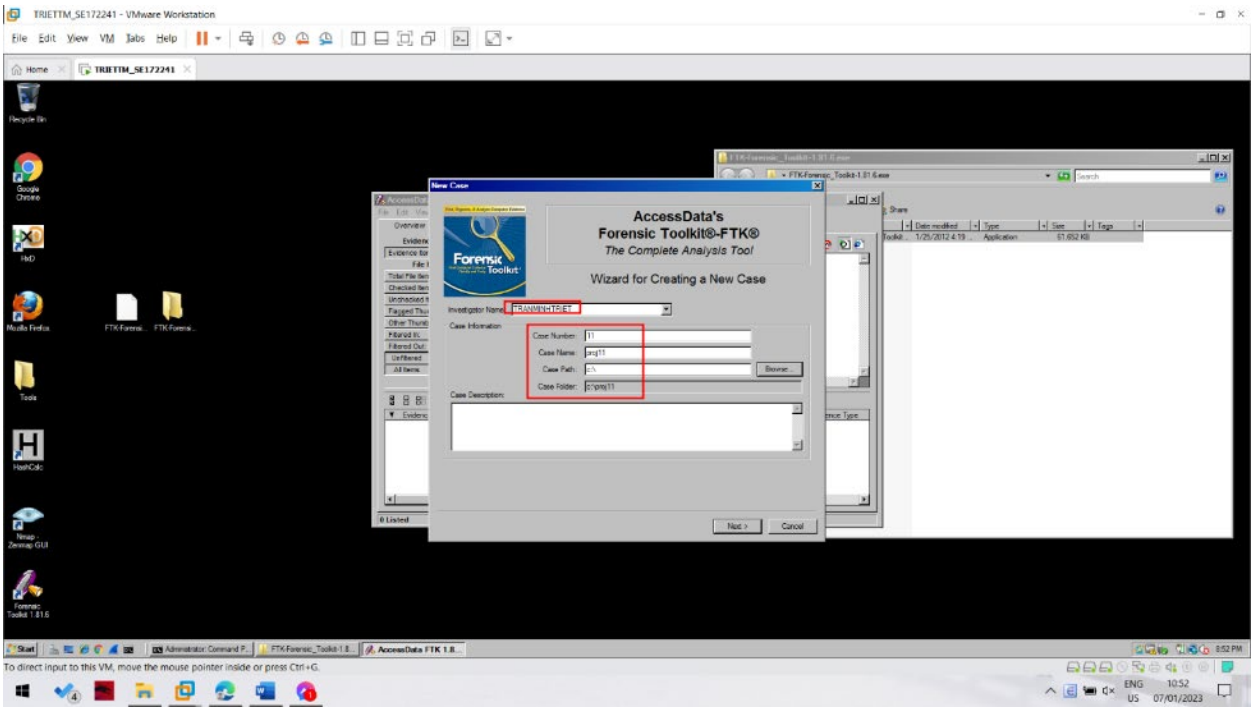

TRIETTM_SE172241 - VMware Workstation
File Edit View VM Tabs Help
Home
TRIETTM_SE172241
Recycle Bin
Google Chrome
HxD
Mozilla Firefox
Tools
HashCalc
Nmap - Zenmap GUI
FTK-Forensic_Toolkit-1.81.6.exe
FTK-Forensic_Toolkit-1.81.6.exe
File Edit View Tools Help
Organize
Open
Share
Favorite Links
Documents
Pictures
Music
Recently Changed
Searches
Public
Name
Date modified
Type
Size
Tags
FTK-Forensic_Toolkit...
1/25/2012 4:19
Application
61,652 KB
Folders
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG
US
10:34
07/01/2023


File Edit View VM Tabs Help
Home
TRIETTM_SE172241
Find, Organize, & Analyze Computer Evidence
Forensic Toolkit
AccessData
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG US
10:34
07/01/2023


TRIETTM_SE172241 - VMware Workstation
File Edit View VM Tabs Help
Home
TRIETTM_SE172241
AccessData Forensic Toolkit - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
AccessData
END-USER LICENSE AGREEMENT FOR ACCESSDATA SOFTWARE
IMPORTANT-READ CAREFULLY:
I accept the terms of the license agreement
I do not accept the terms of the license agreement
Print
< Back
Next >
Cancel
InstallShield
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG US
10:35
07/01/2023


TRIETTM_SE172241 - VMware Workstation
File Edit View VM Tabs Help
Home
TRIETTM_SE172241
AccessData FTK Startup
Start a new case
Open an existing case
Process evidence
Go directly to working in program
Do not show this dialog on startup
OK
Cancel
Forensic Toolkit
Folders
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG
US
10:35
07/01/2023

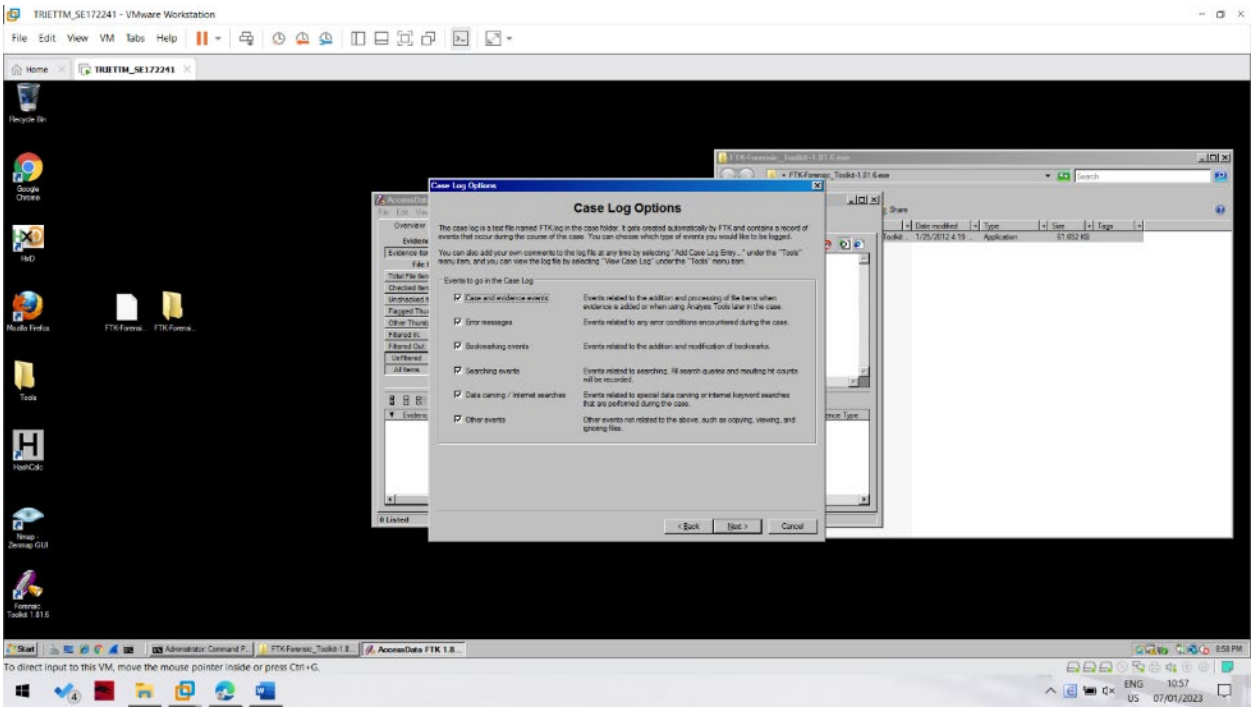

TRIETTM_SE172241 - VMware Workstation
File Edit View VM Tabs Help
Home
TRIETTM_SE172241
New Case
AccessData's
Forensic Toolkit®-FTK®
The Complete Analysis Tool
Wizard for Creating a New Case
Investigator Name:
Case Information
Case Number:
Case Name:
Case Path:
Browse...
Case Folder:
Case Description:
Next >
Cancel
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG
US
10:36
07/01/2023

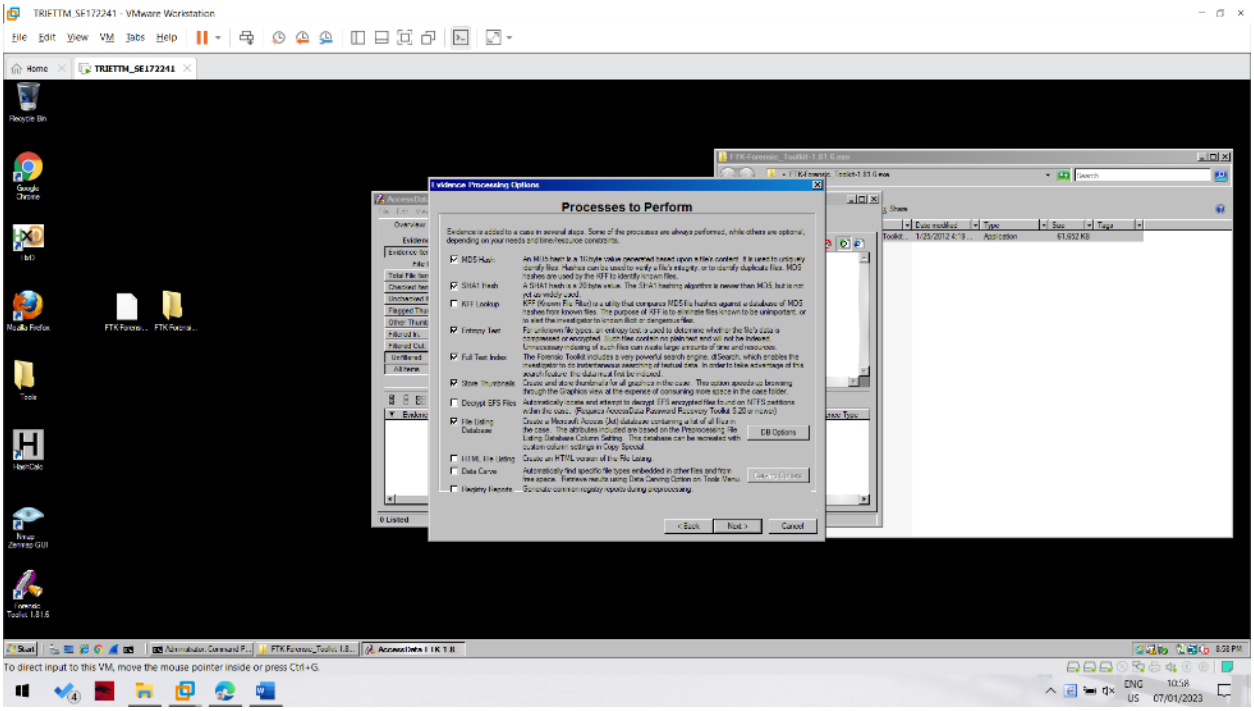


In the screen titled "Forensic Examiner Information", leave the fields blank and click Next.

In the screen titled "Case Log Options", accept the default selections, which will log everything. Click Next.

In the screen titled "Processes to Perform", deselect "KFF Lookup" and "Decrypt EFS Files", because those features won't work in the demo version, as shown below. Click Next.

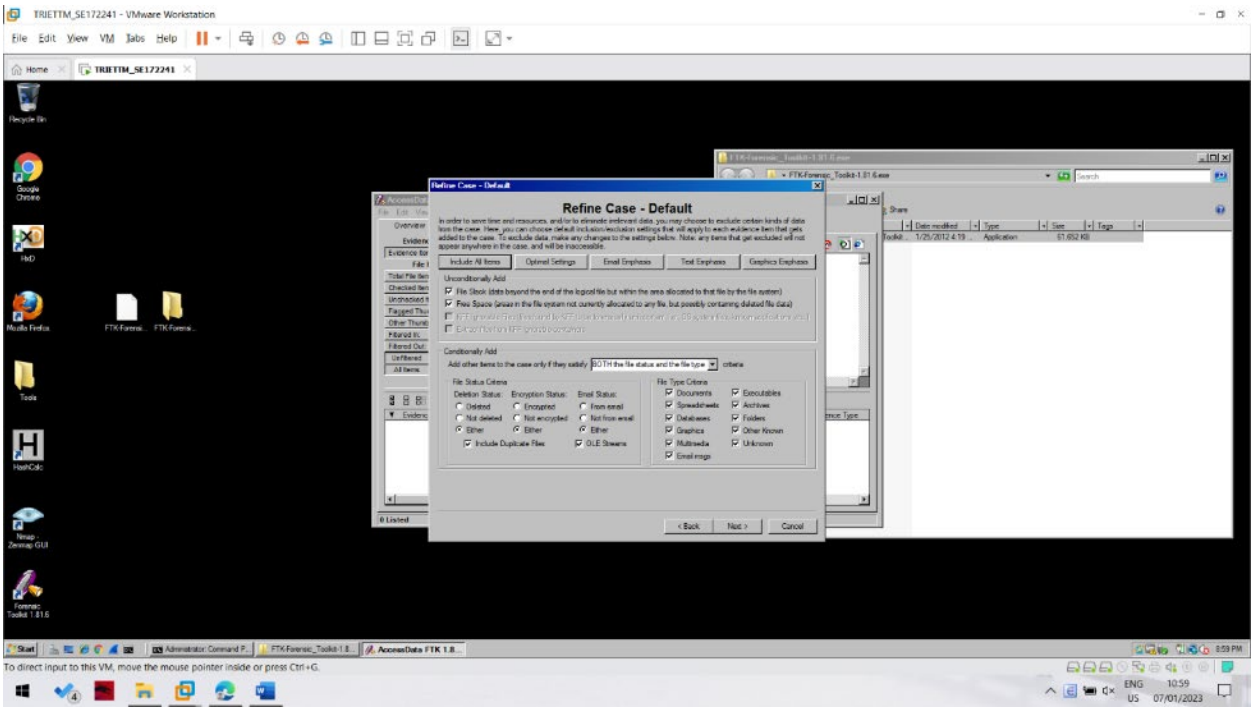


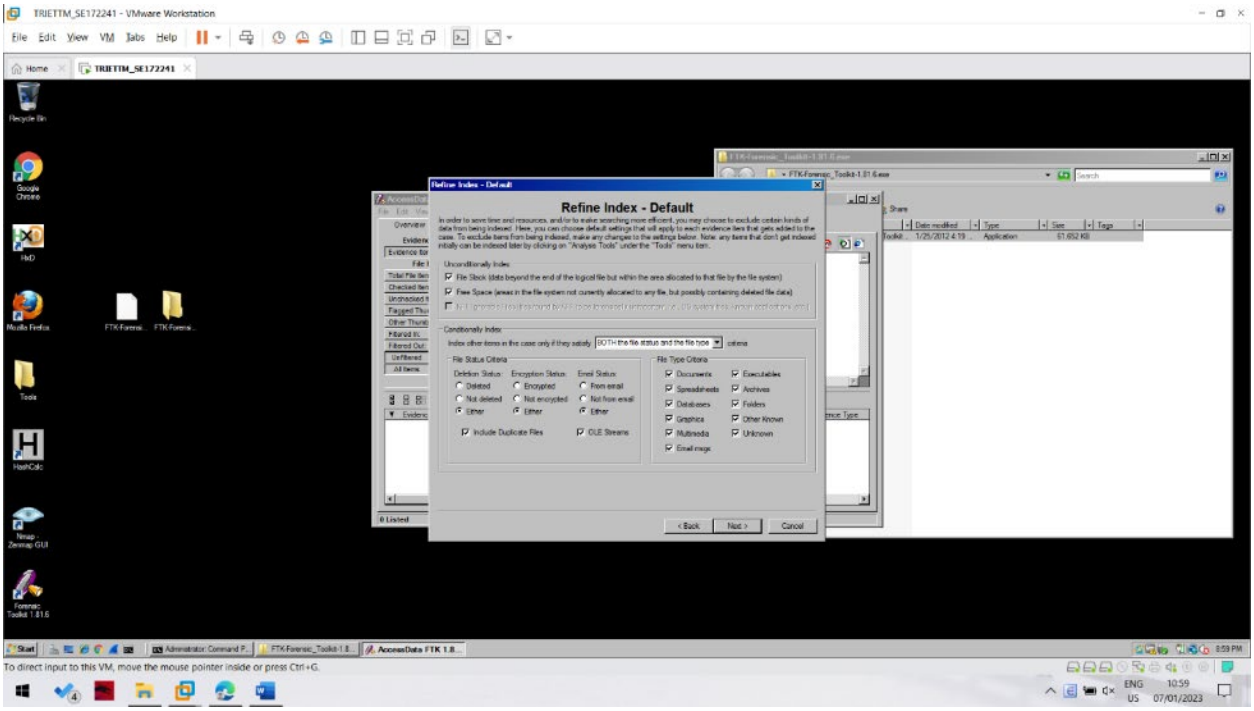


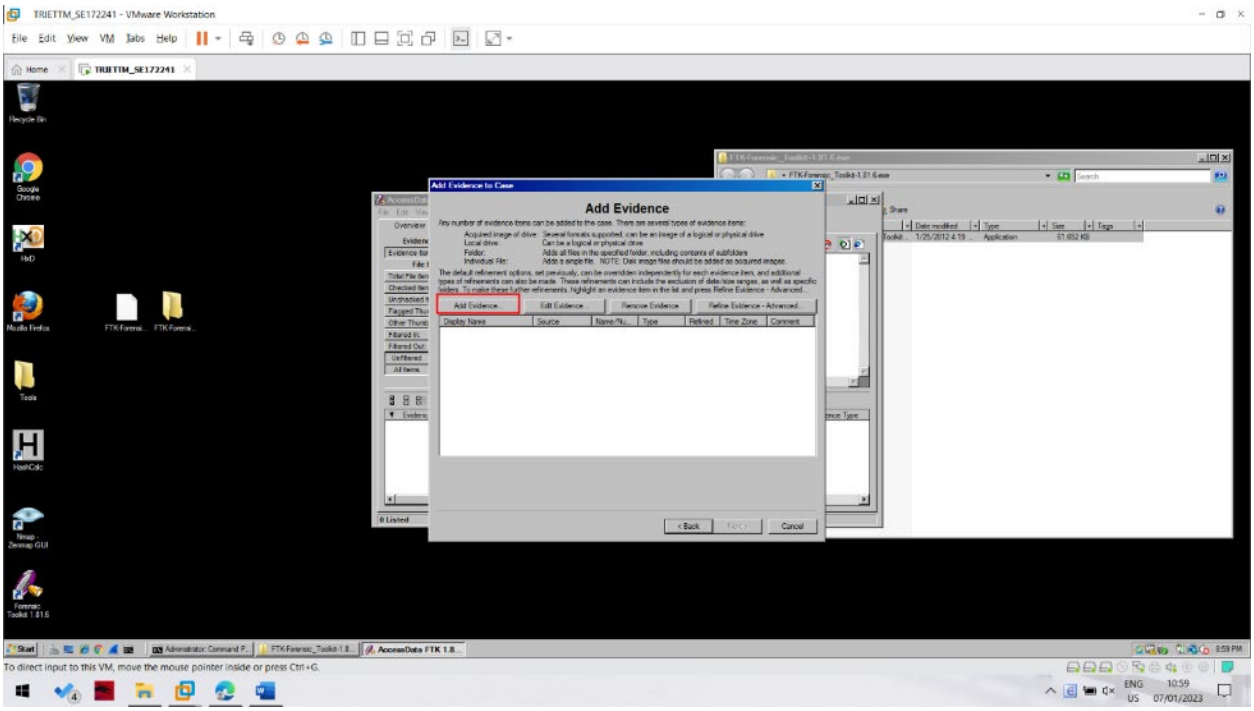
In the screen titled "Refine Case-Default", accept the default of "Include All Items". Click Next.

In the screen titled "Refine Index -Default", accept the default options. Click Next.

Now you see the "Add Evidence" screen, as shown below.


TRIETTM_SE172241 - VMware Workstation
File Edit View VM Tabs Help
Refine Case - Default
Refine Case - Default
Include All Items
Optimal Settings
Email Emphasis
Text Emphasis
Graphics Emphasis
Unconditionally Add
File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
Conditionally Add
Add other items to the case only if they satisfy BOTH the file status and the file type criteria
File Status Criteria
Deletion Status:
Deleted
Not deleted
Either
Encryption Status:
Encrypted
Not encrypted
Either
Email Status:
From email
Not from email
Either
Include Duplicate Files
OLE Streams
File Type Criteria
Documents
Spreadsheets
Databases
Graphics
Multimedia
Email msgs
Executables
Archives
Folders
Other Known
Unknown
< Back
Next >
Cancel
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


TRIETTM_SE172241 - VMware Workstation
File Edit View VM Tabs Help
Refine Index - Default
Refine Index - Default
Unconditionally Index
File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
Conditionally Index
Index other items in the case only if they satisfy BOTH the file status and the file type criteria
File Status Criteria
Deletion Status:
Deleted
Not deleted
Either
Encryption Status:
Encrypted
Not encrypted
Either
Email Status:
From email
Not from email
Either
Include Duplicate Files
OLE Streams
File Type Criteria
Documents
Spreadsheets
Databases
Graphics
Multimedia
Email msgs
Executables
Archives
Folders
Other Known
Unknown
< Back
Next >
Cancel
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

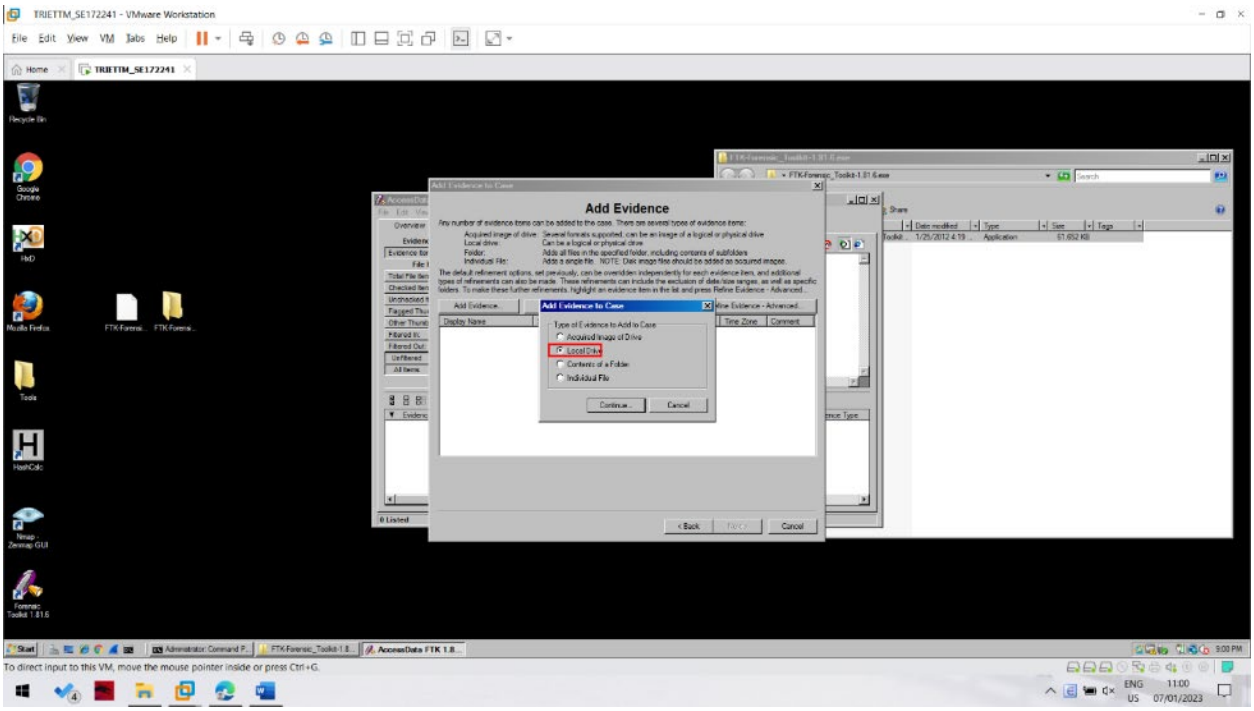


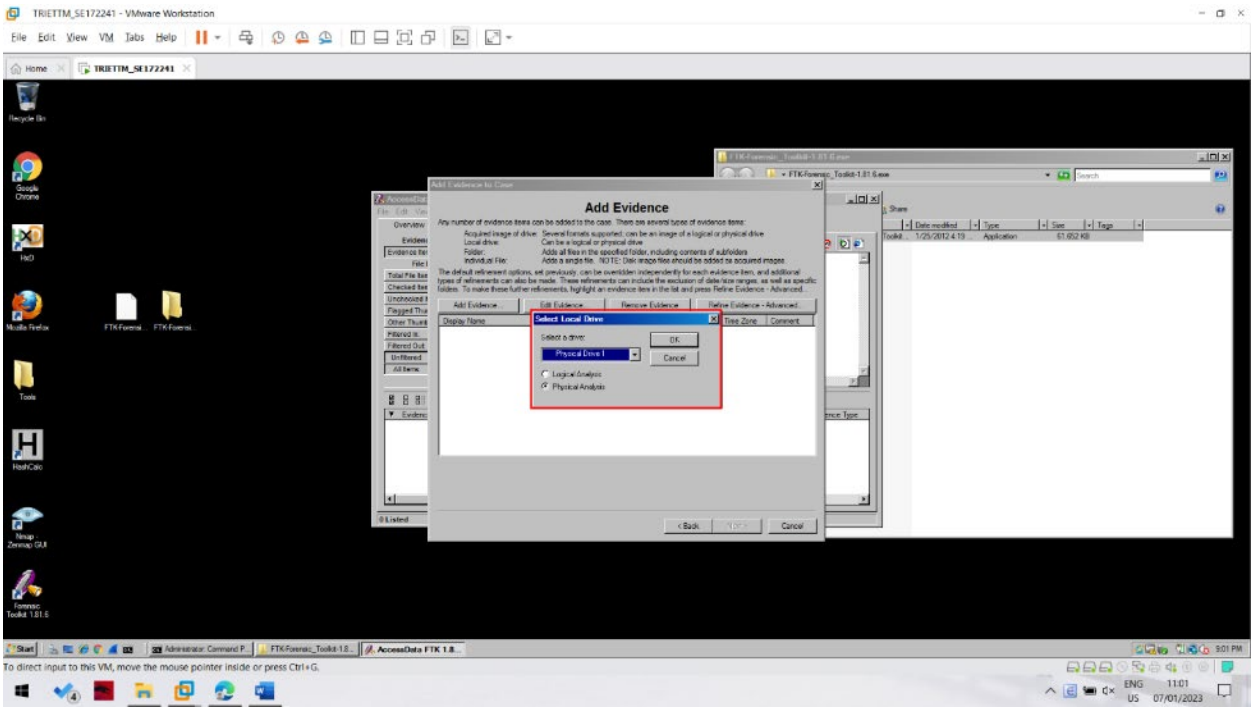
Adding Evidence to the Case

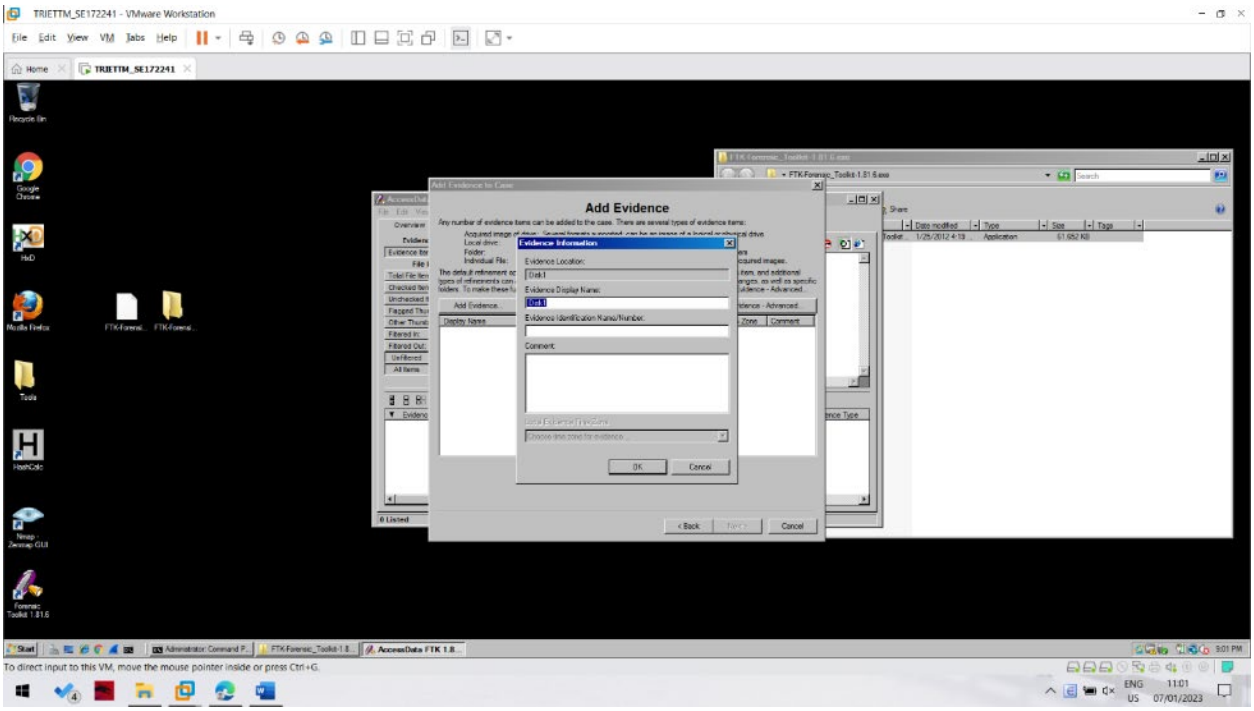
In the "Add Evidence" box, click the "Add Evidence...". button.

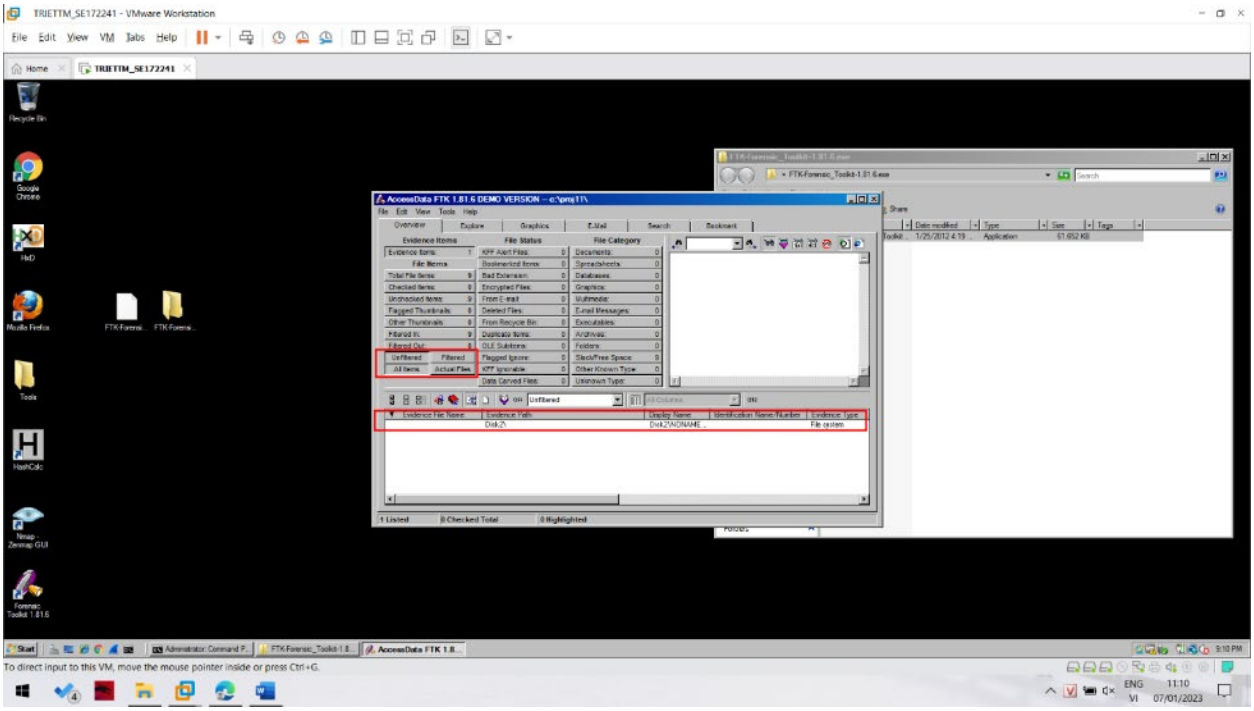
In the "Add Evidence to Case" box, select "Local Drive", and click Continue.

In the "Select Local Drive" box, click "Physical Analysis" and select the drive "Physical Drive 1", as shown below. Click OK.

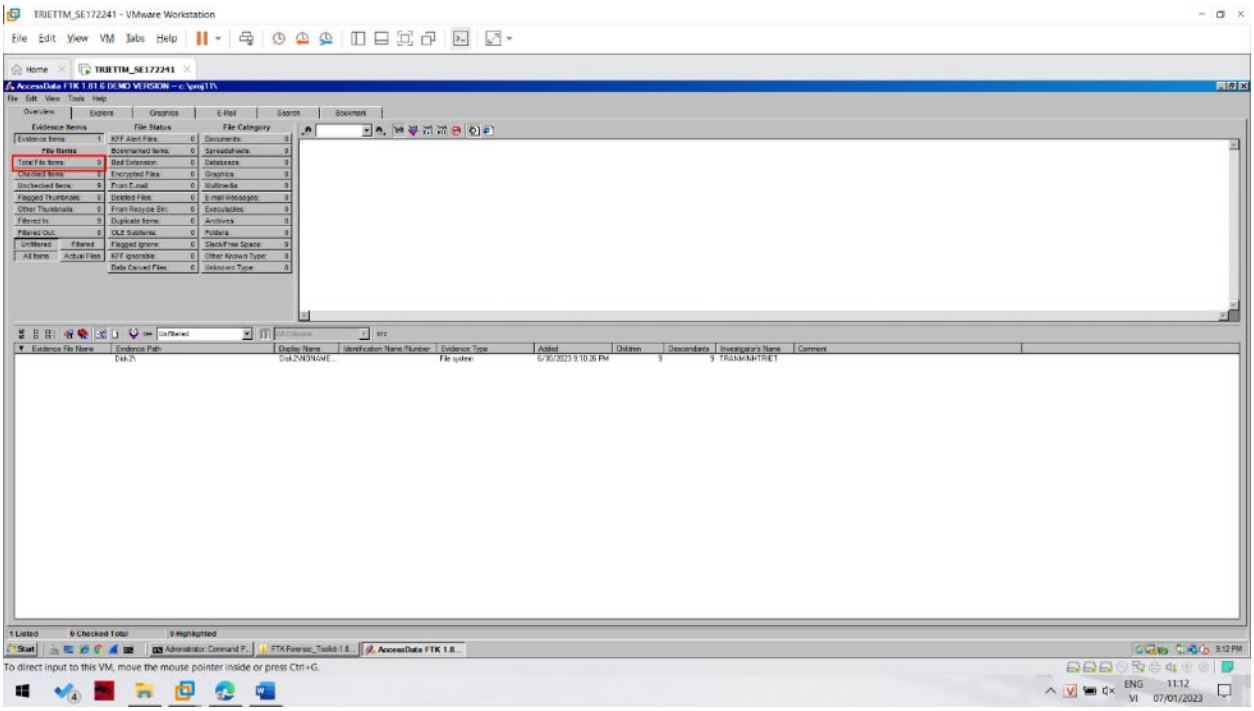

TRIETTM_SE172241 - VMware Workstation
File Edit View VM Tabs Help
Add Evidence
Add Evidence to Case
Type of Evidence to Add to Case
Acquired Image of Drive
Local Drive
Contents of a Folder
Individual File
Continue...
Cancel
< Back
Next >
Cancel
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG US
11:00
07/01/2023


TRIETTM_SE172241 - VMware Workstation
File Edit View VM Tabs Help
Add Evidence
Select Local Drive
Select a drive:
Physical Drive1
OK
Cancel
Logical Analysis
Physical Analysis
< Back
Next >
Cancel
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG US
11:01
07/01/2023



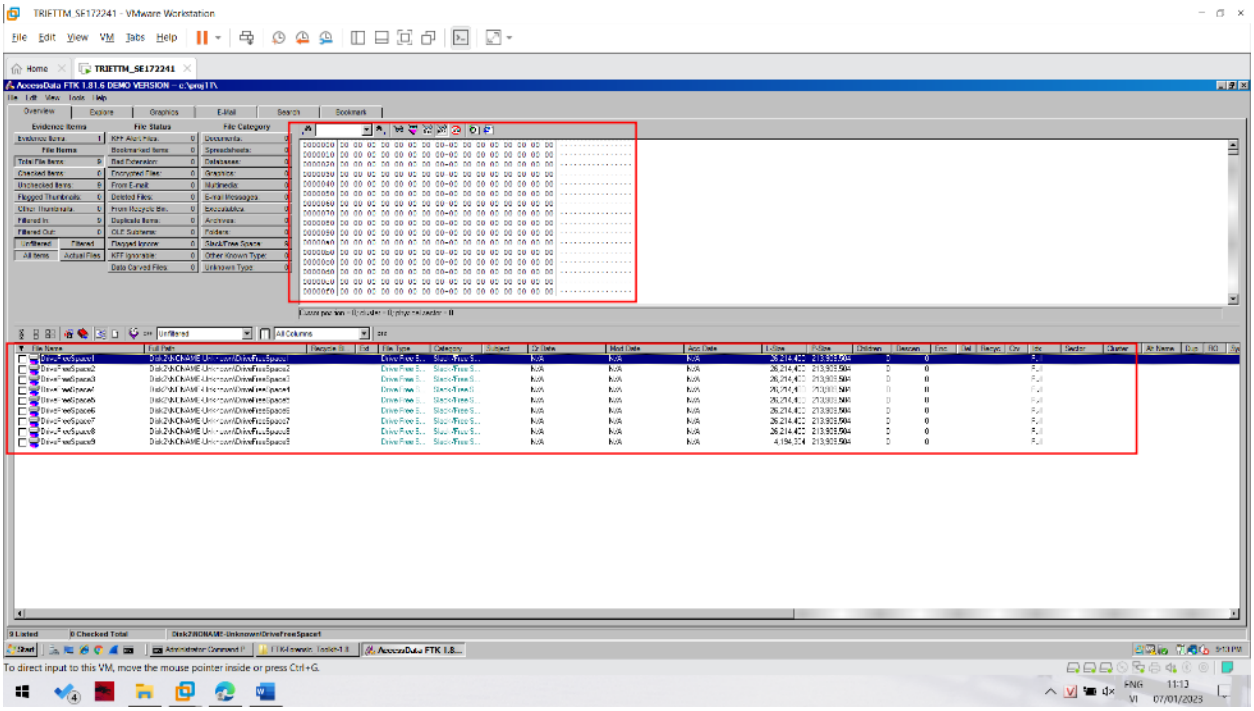


The FTK Window



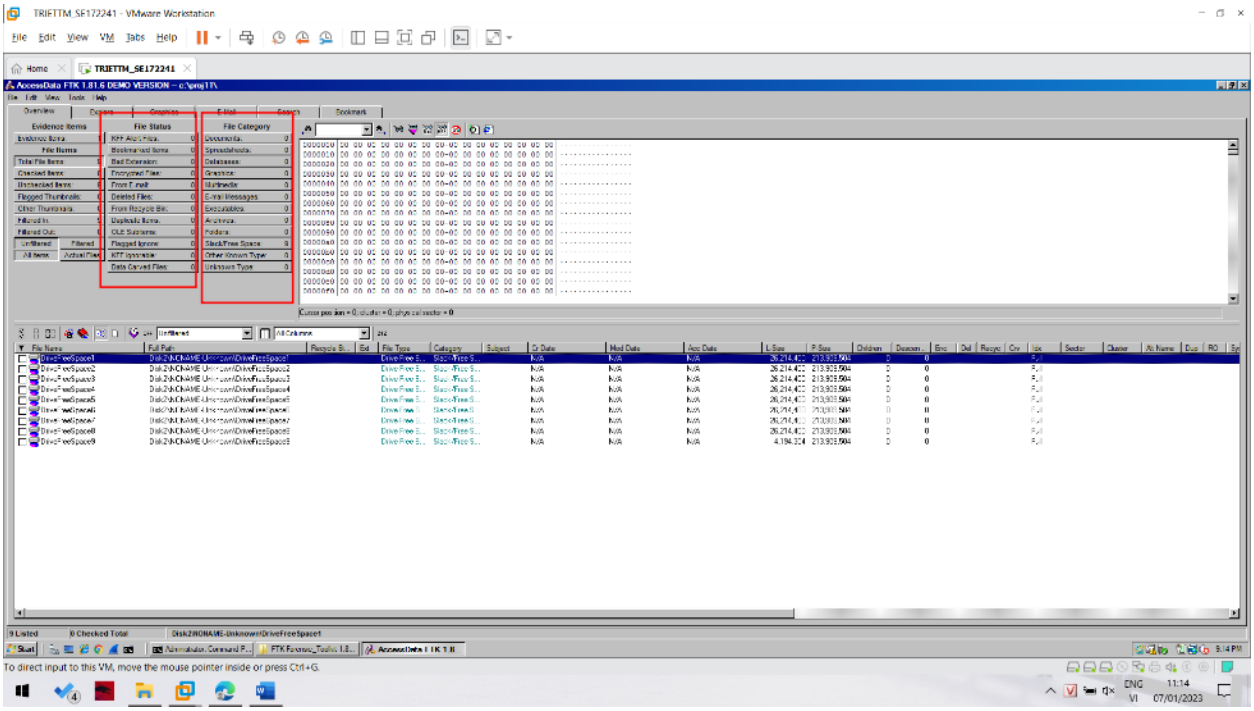
To find out, click the "Total File Items:" button. The lower pane now shows five items, named "DriveFreeSpace1","DriveFreeSpace2","DriveFreeSpace3", etc.

In the bottom pane of the FTK window, click "DriveFreeSpace1". The upper right corner now shows a hexadecimal view of the bytes in that file, as shown below.

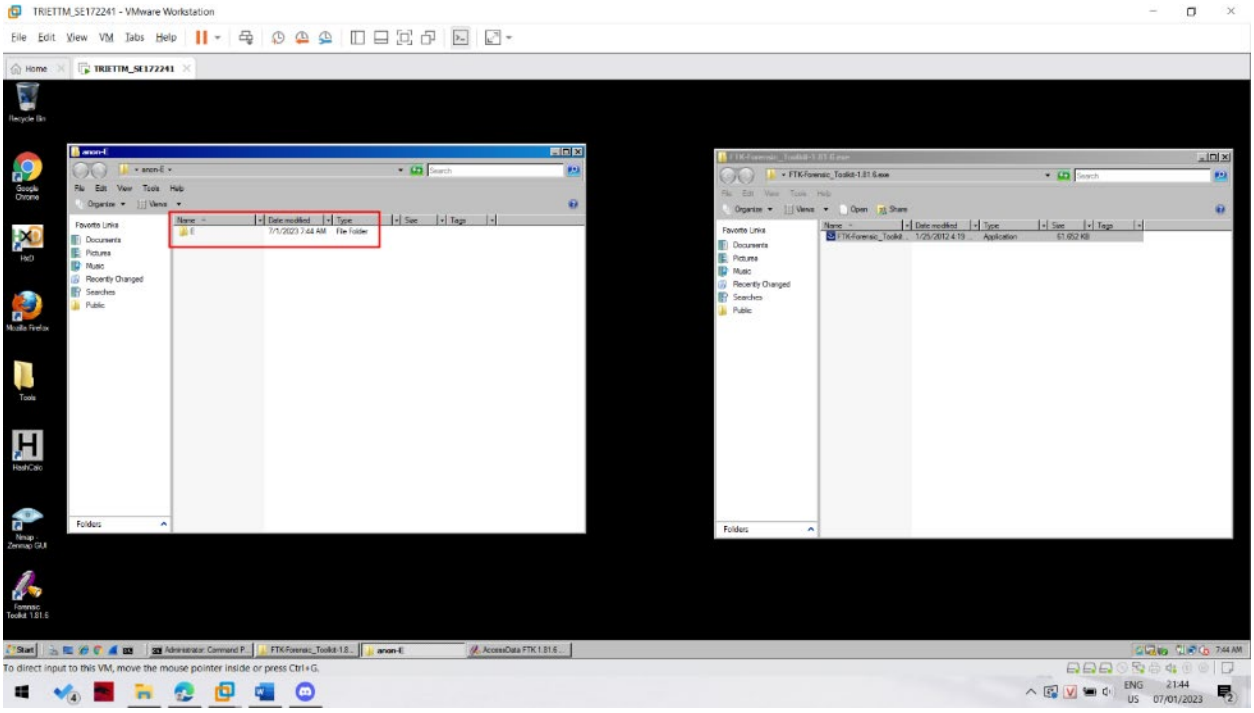


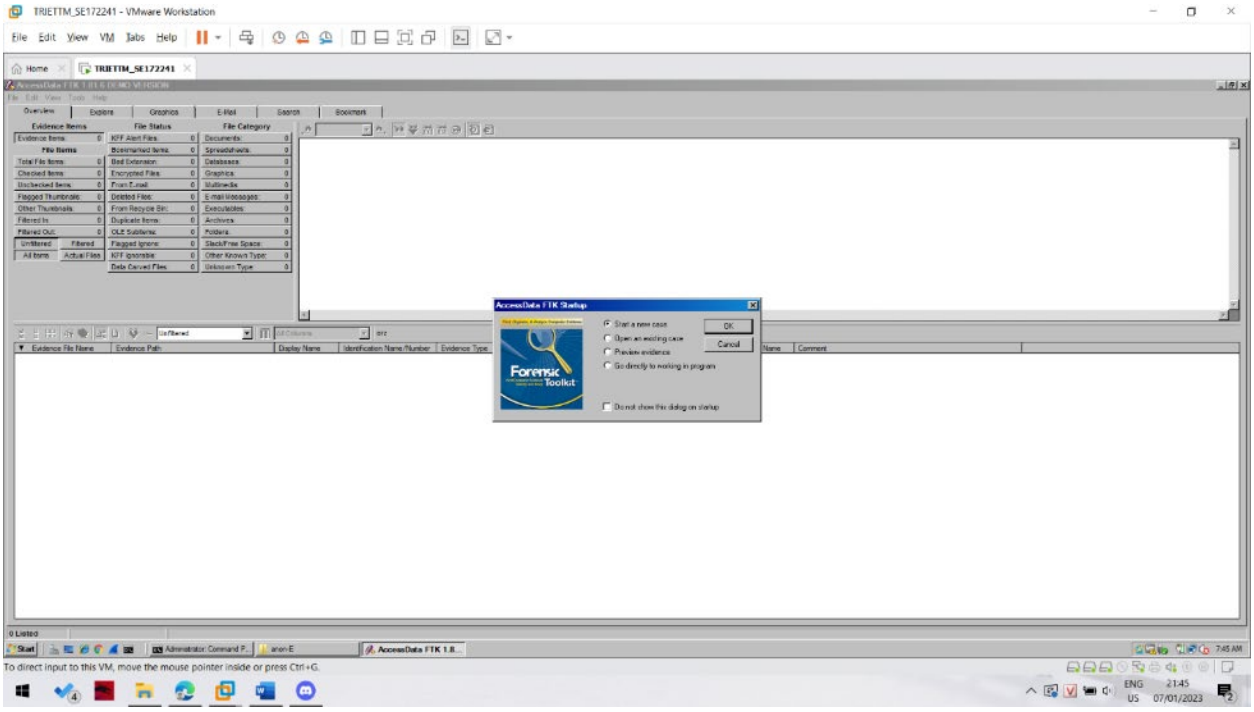
This is just like the HxD utility you used in a previous project. As you can see, the file is empty--it's not really a file at all, because it has no header or footer or file name or any data at all. FTK just breaks empty space up into chunks it calls 'Files" for handling.

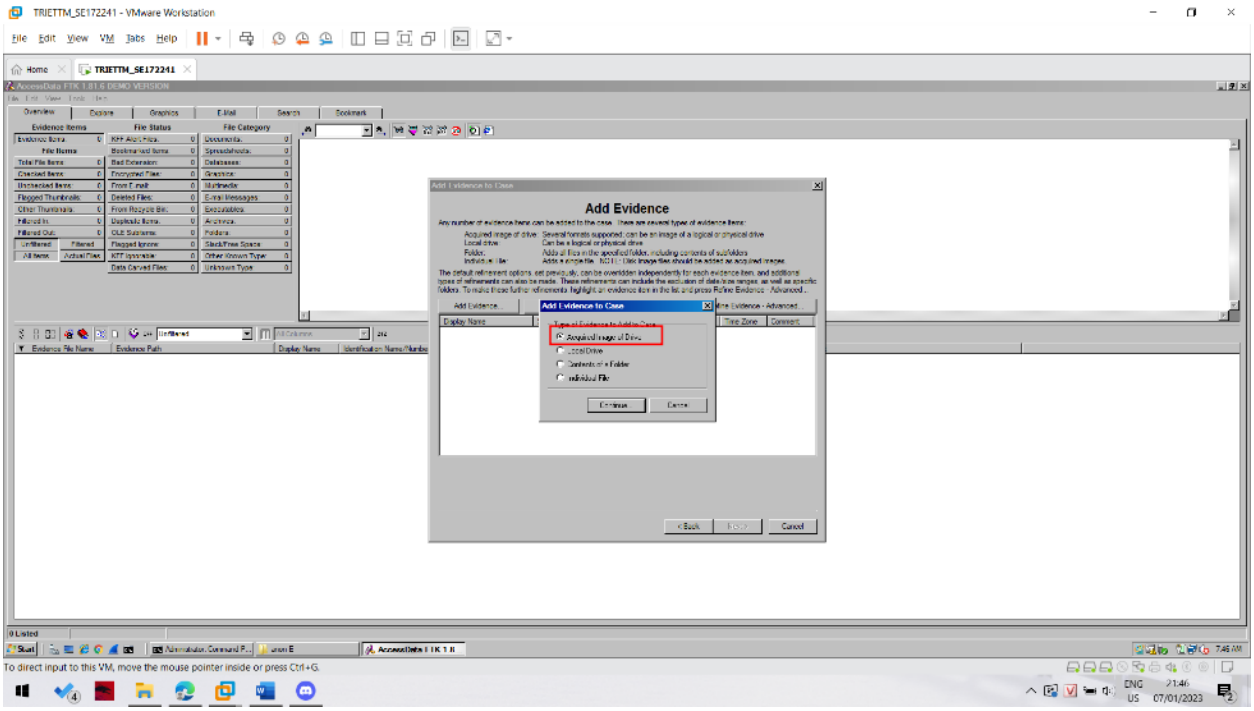
To see that the disk is really empty, look at the "File Status" and "File Category" columns in the upper left portion of the FTK window. You can see that FTK was unable to find any usable data in any known format on this disk--it's clean.

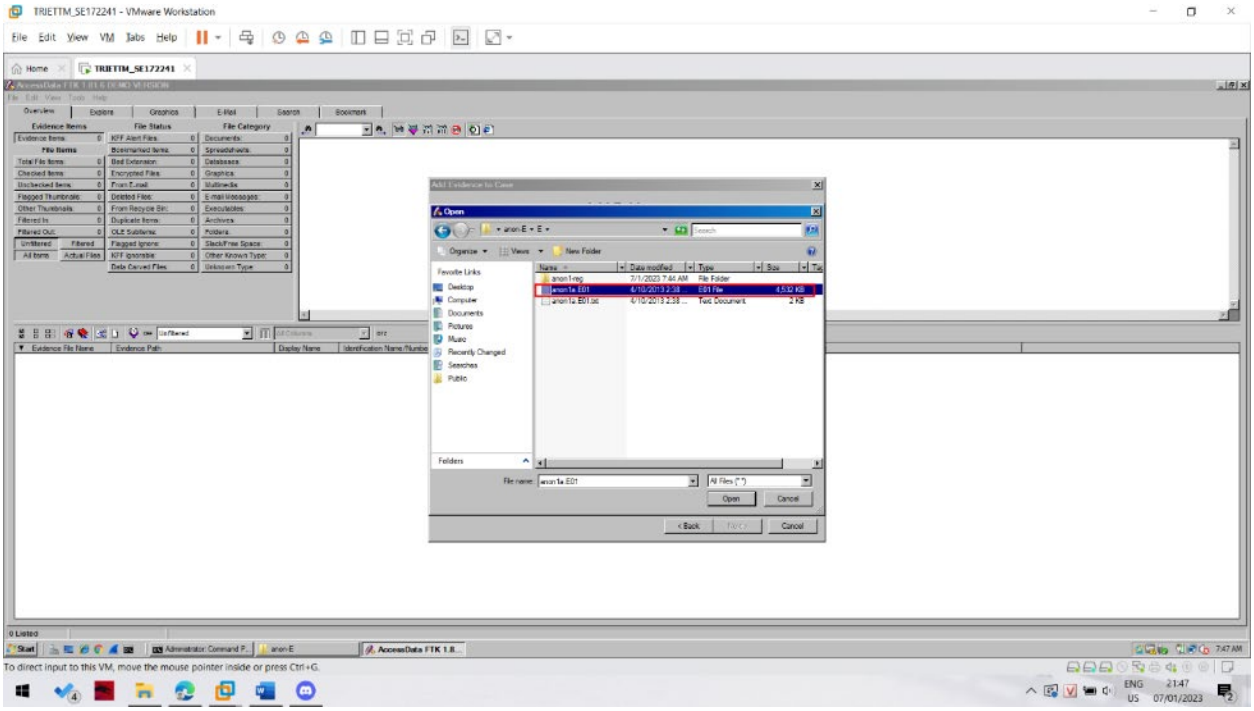


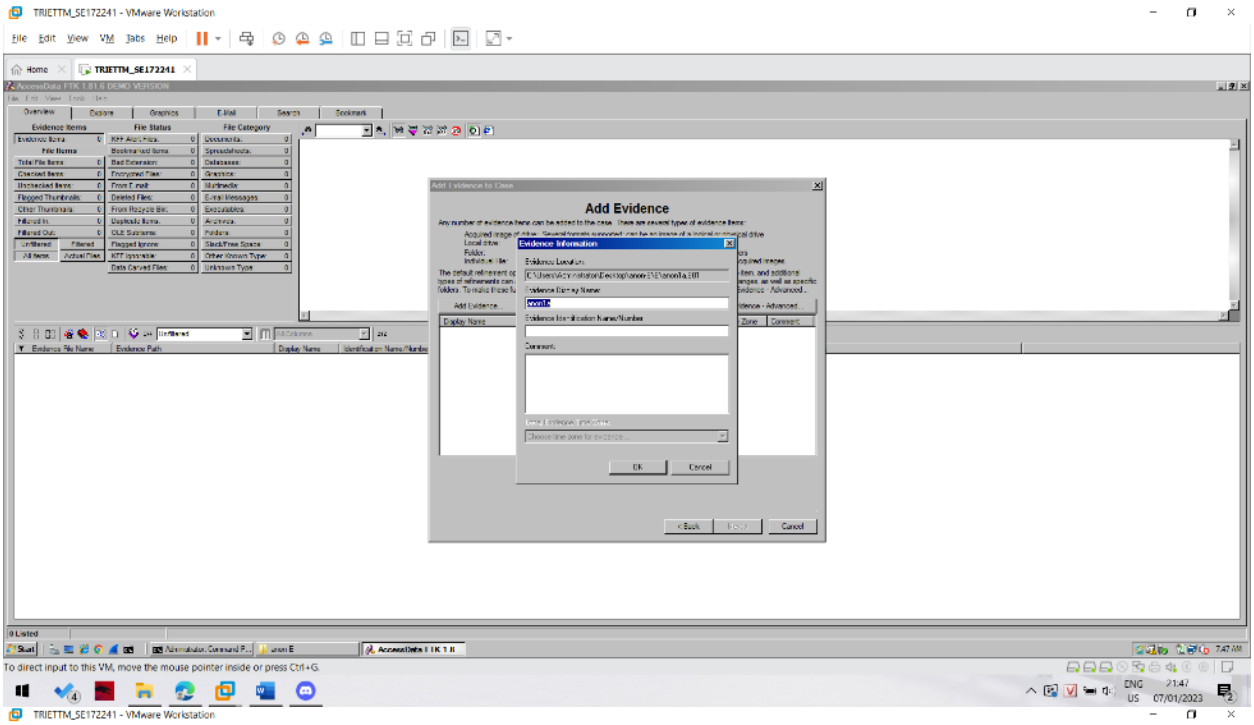
Downloading the Evidence File

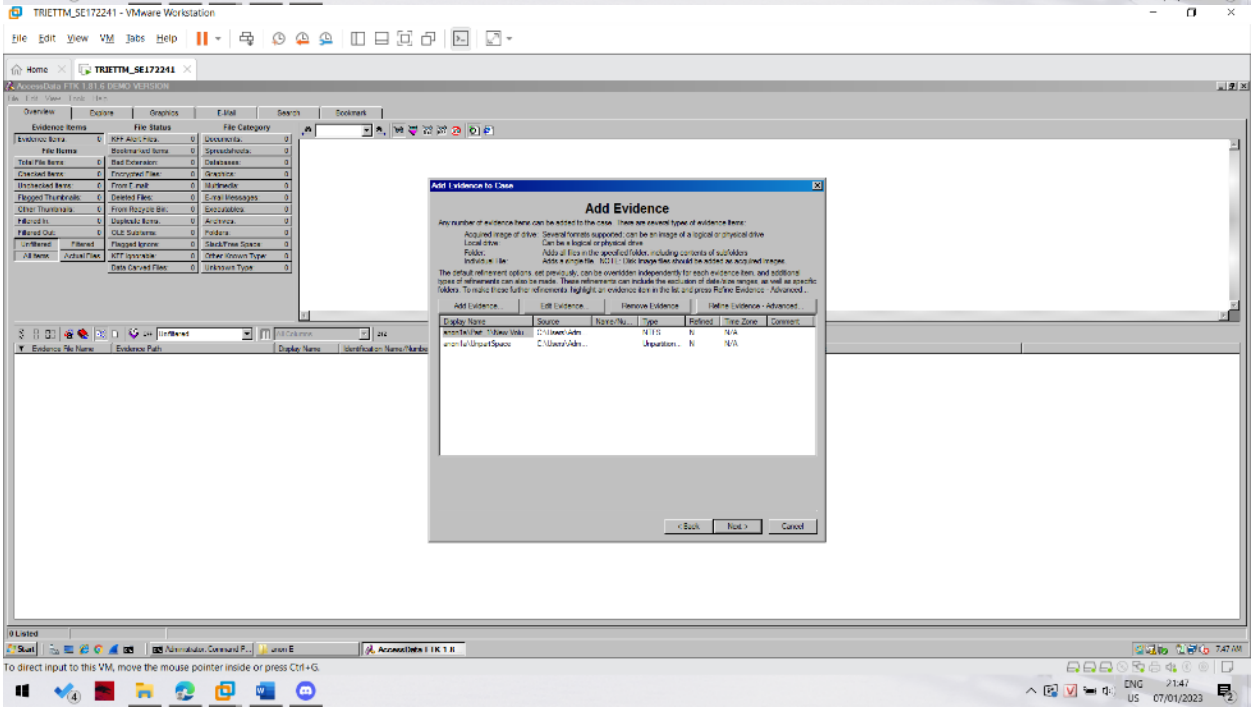

TRIETTM_SE172241 - VMware Workstation
File Edit View VM Tabs Help
Home
TRIETTM_SE172241
anon-E
FTK-Forensic_Toolkit-1.81.6.exe
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

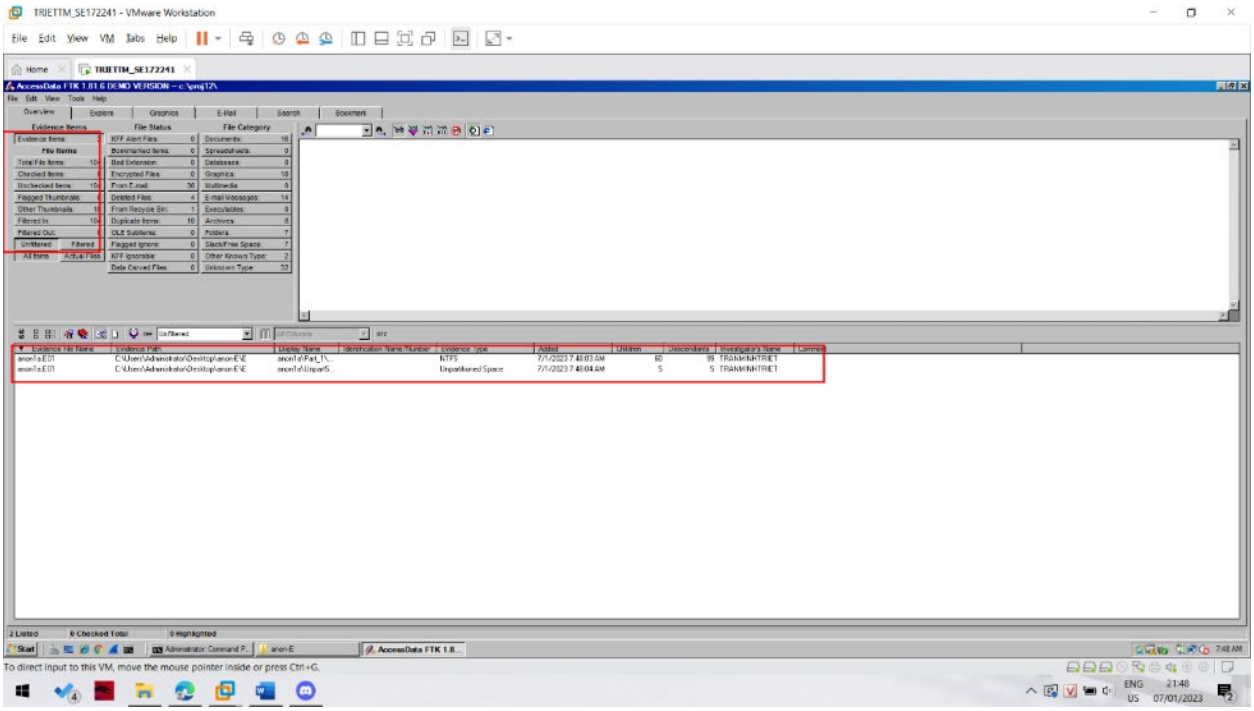

TRIETTM_SE172241 - VMware Workstation
File Edit View VM Tabs Help
Home
TRIETTM_SE172241
AccessData FTK Startup
Forensic Toolkit
OK
Cancel
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


TRIETTM_SE172241 - VMware Workstation
File Edit View VM Tabs Help
Add Evidence
Add Evidence to Case
Acquired image of drive
Local drive
Contents of a Folder
Individual File
Continue
Cancel
< Back
Next >
Cancel
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG US
21:46
07/01/2023


TRIETTM_SE172241 - VMware Workstation
File Edit View VM Tabs Help
Open
Add Evidence to Case
Open
Cancel
< Back
Next >
Cancel
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG US
21:47
07/01/2023


TRIETTM_SE172241 - VMware Workstation
File Edit View VM Tabs Help
Home
TRIETTM_SE172241
Add Evidence
Evidence Information
OK
Cancel
< Back
Next >
Cancel
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


TRIETTM_SE172241 - VMware Workstation
File Edit View VM Tabs Help
Home
TRIETTM_SE172241
Add Evidence
Add Evidence
Edit Evidence
Remove Evidence
Refine Evidence - Advanced...
< Back
Next >
Cancel
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


TRIETTM_SE172241 - VMware Workstation
File Edit View VM Tabs Help
Home
TRIETTM_SE172241
AccessData FTK 1.81 6 DEMO VERSION – c:\prog12\
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
Evidence Items
File Status
File Category
Unfiltered
Filtered
All Items
Actual Files
Evidence File Name
Evidence Path
Display Name
Identification Name/Number
Evidence Type
Added
Children
Descendants
Investigator's Name
Comment
anon1.e.E01
C:\Users\Administrator\Desktop\anon-E\E
anon1.e\Part_1\...
NTFS
7/1/2023 7:48:03 AM
60
99
TRANMINHTRIET
anon1.e\Unpar5...
Unpartitioned Space
7/1/2023 7:48:04 AM
5
5
TRANMINHTRIET
2 Listed
0 Checked Total
0 Highlighted
Start
Administrator: Command P...
anon-E
AccessData FTK 1.8...
7:48 AM
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG
US
21:48
07/01/2023