Lab 3: USB_Image_Acquisition

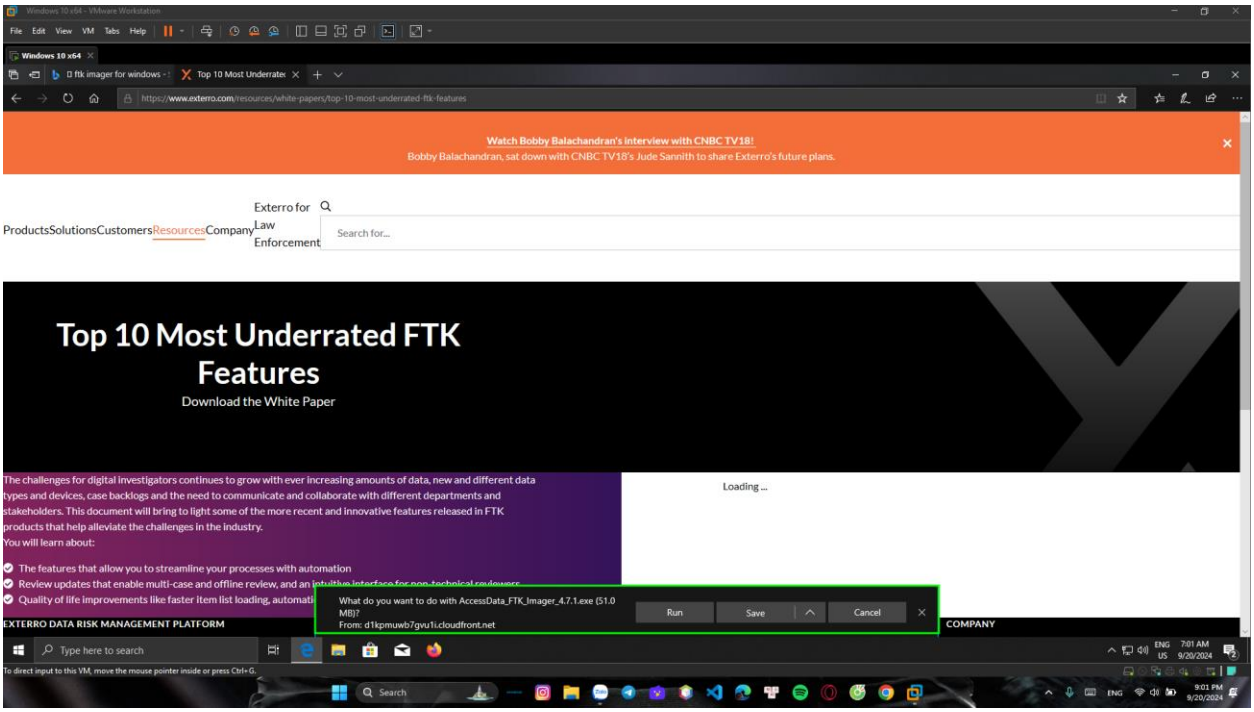
Group: CyberSec_N00b

Member:

- *Huỳnh Ngọc Quang (SE181838)*
- *Hồ Tài Liên Vy Kha (SE181818)*
- *Hoàng Kim Long (DE180860)*
- *Phạm Thành Long (SE181692)*
- *Nguyễn Lê Hoàng Thông (SE182533)*

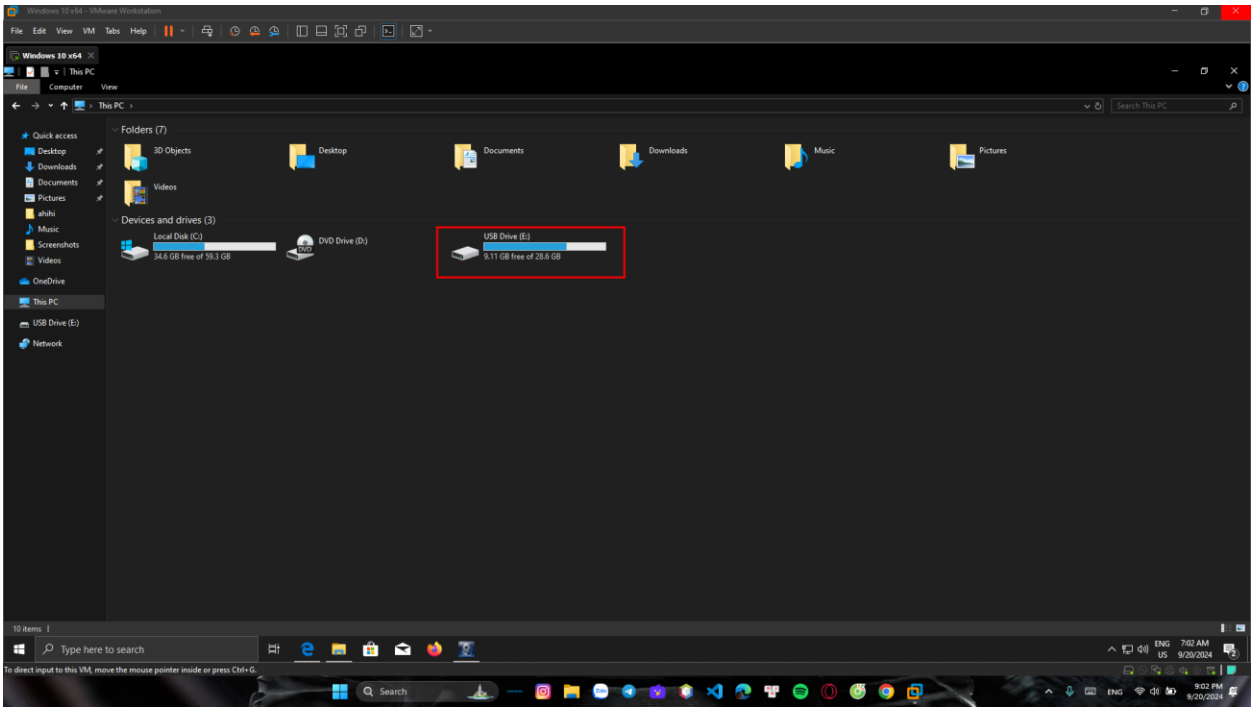
Step 1.

- Download and install FTK



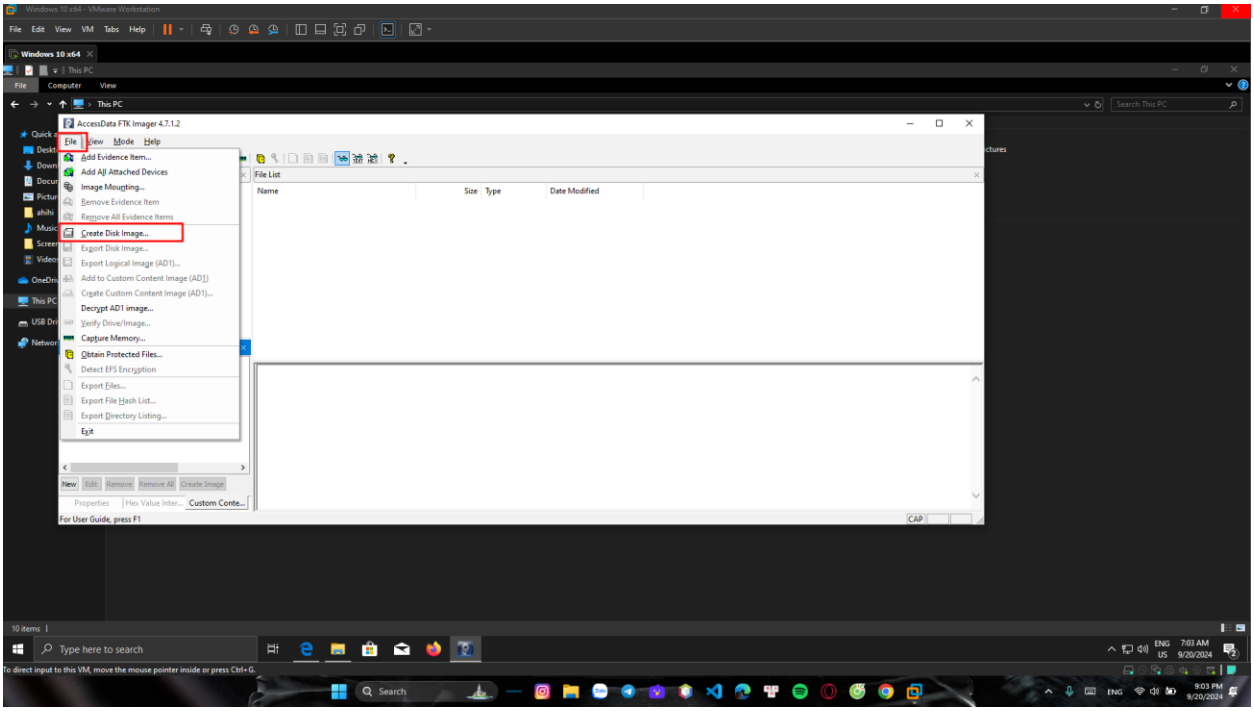
Step 2.

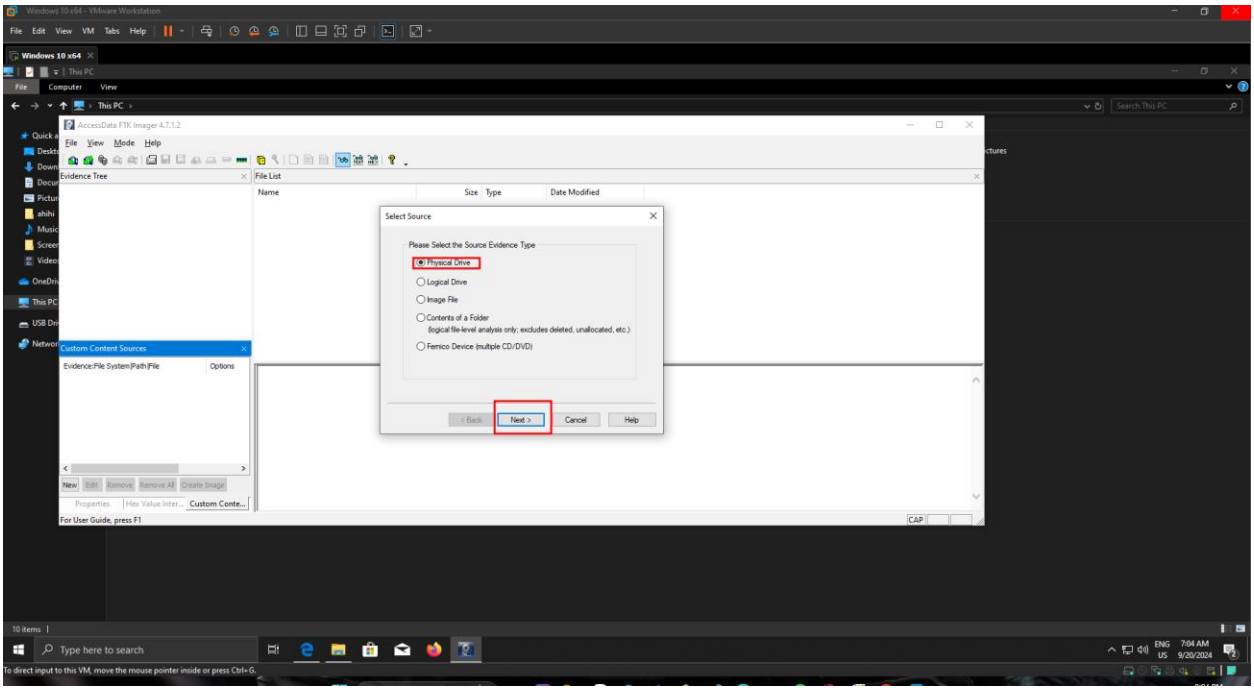
- Plug in a Flash Drive to your computer : you can copy come files to the USB.
- Verify your PC can read the USB drive

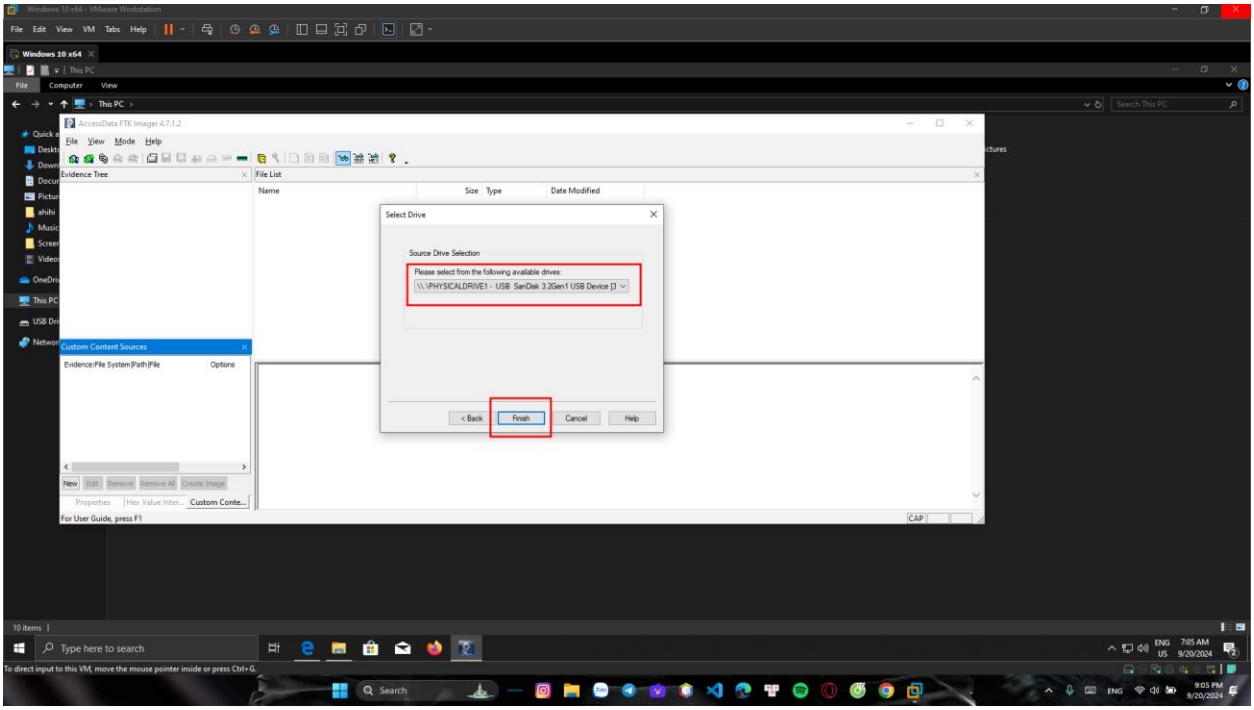


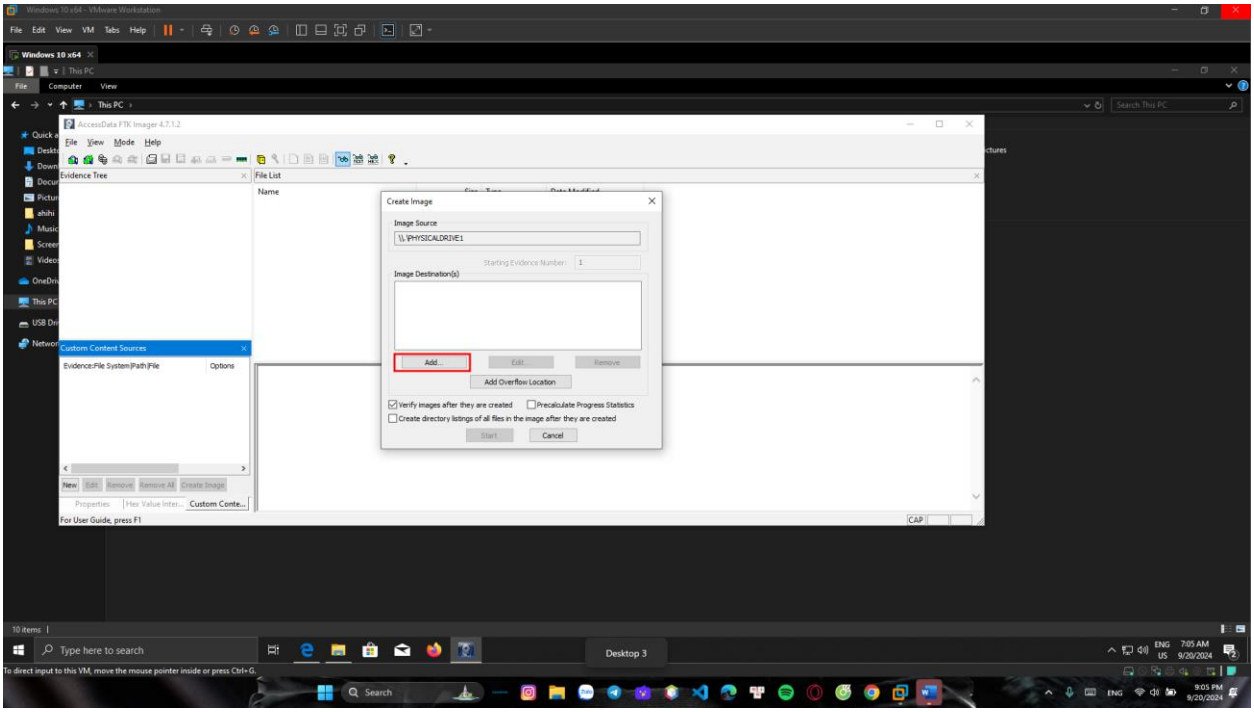
Step 3.

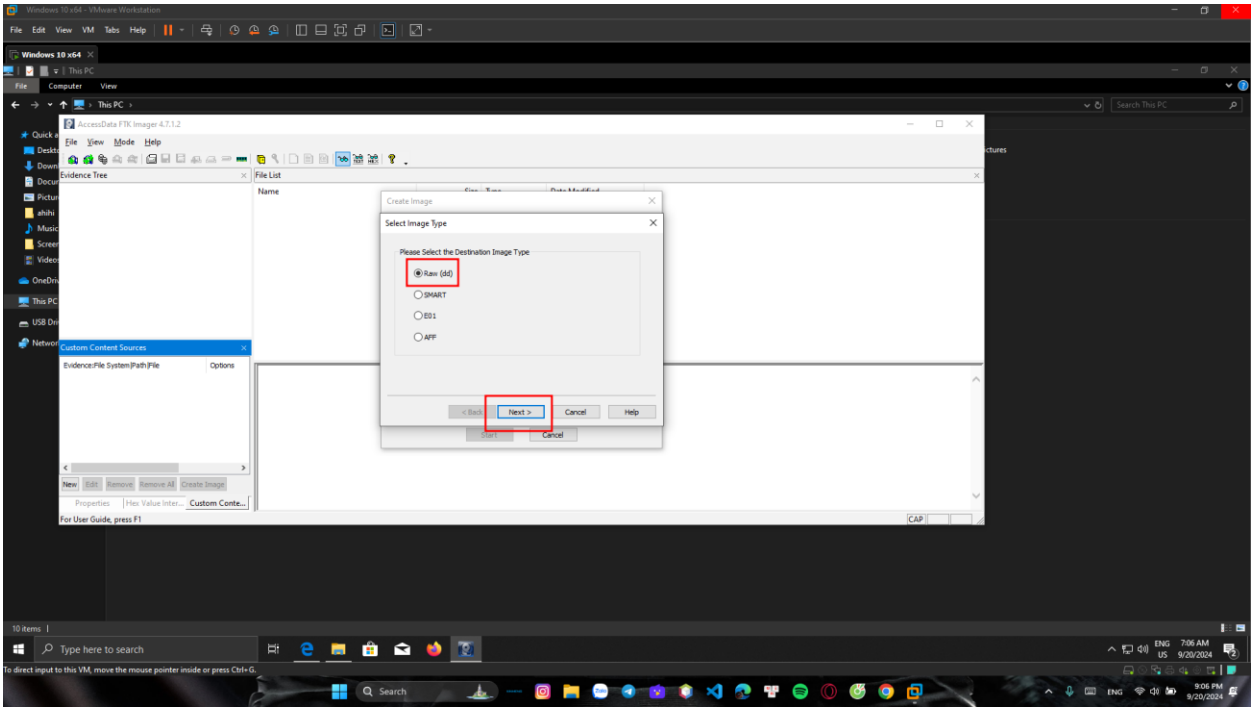
– Acquiring a USB using FTK

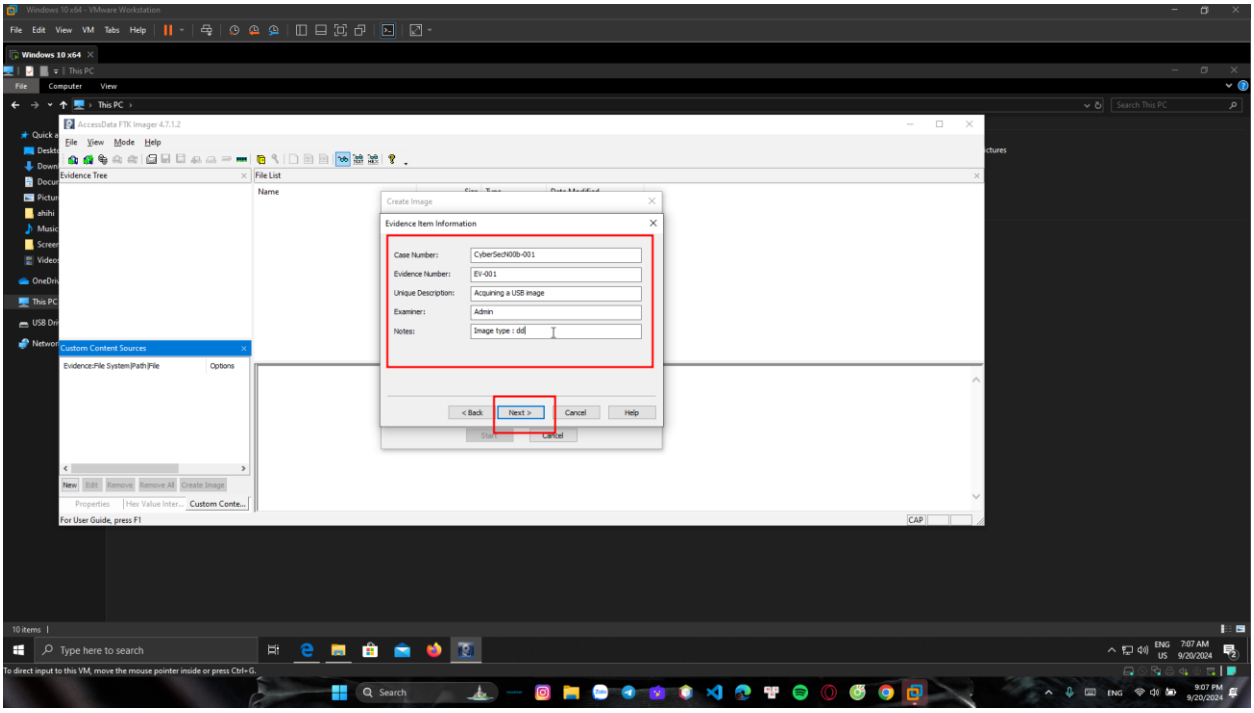


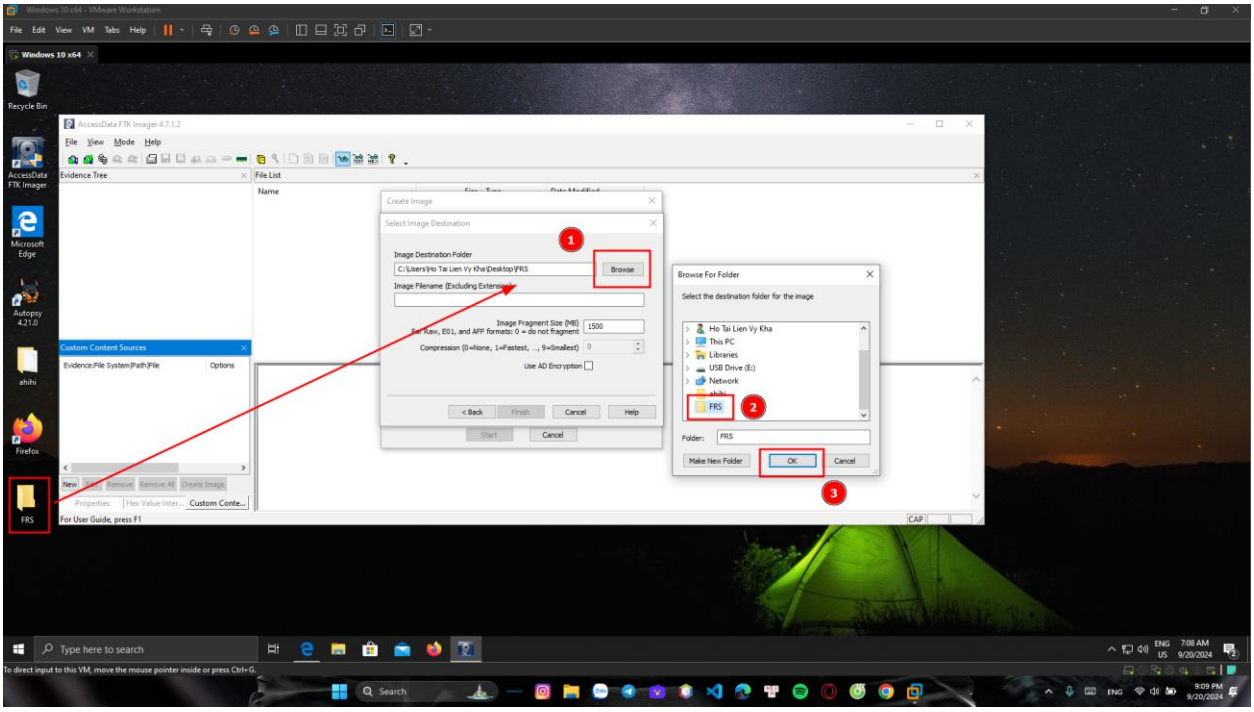

Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
Femico Device (multiple CD/DVD)
< Back
Next >
Cancel
Help

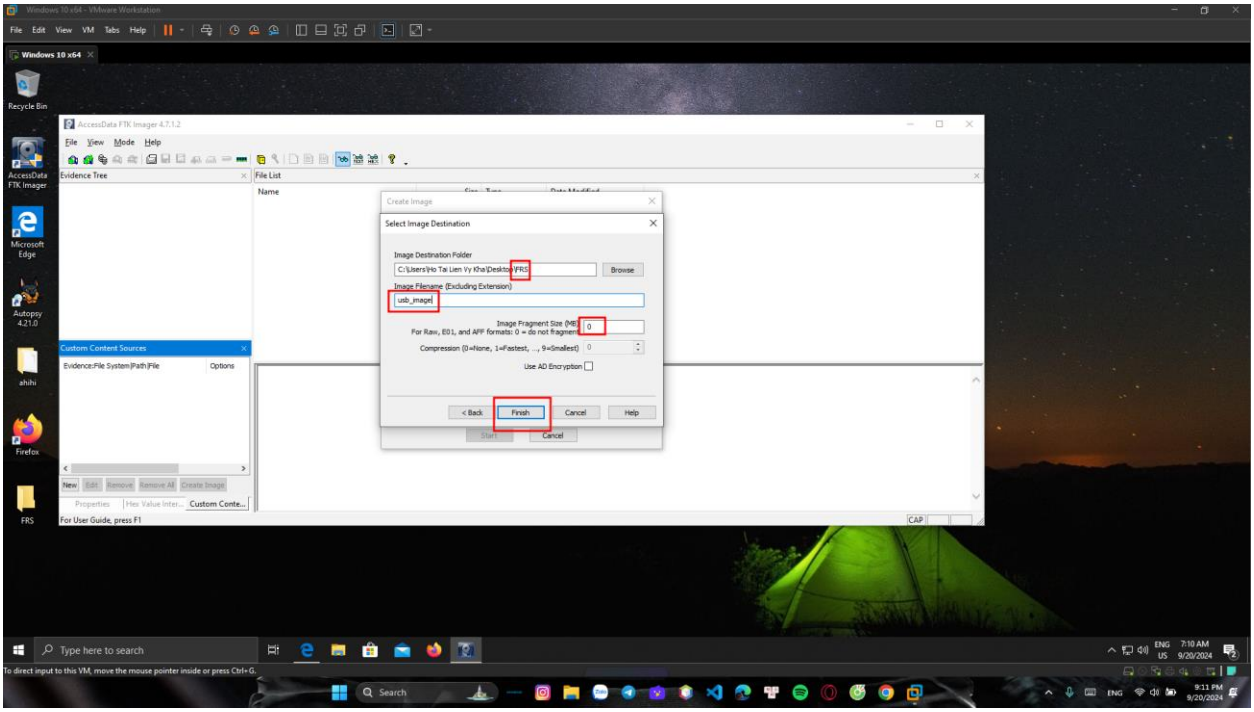

Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE1 - USB SanDisk 3.2Gen1 USB Device
< Back
Finish
Cancel
Help

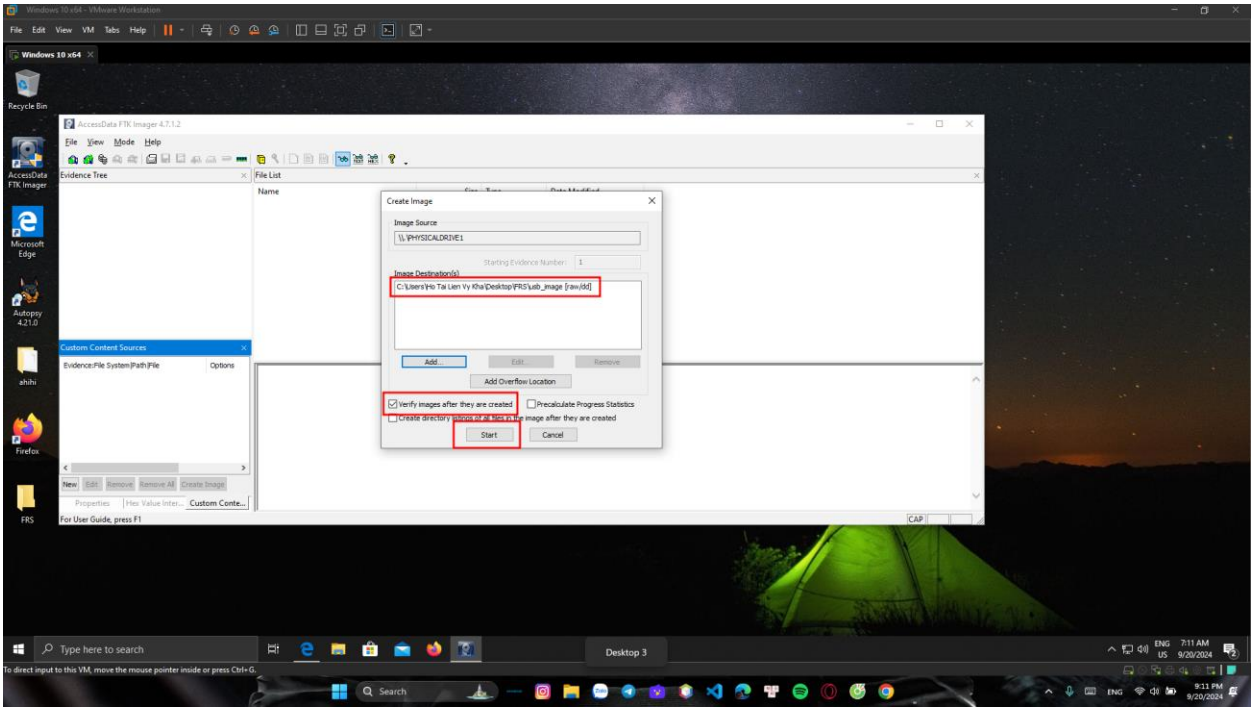

Create Image
Image Source
\\.\PHYSICALDRIVE1
Image Destination(s)
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel
Desktop 3

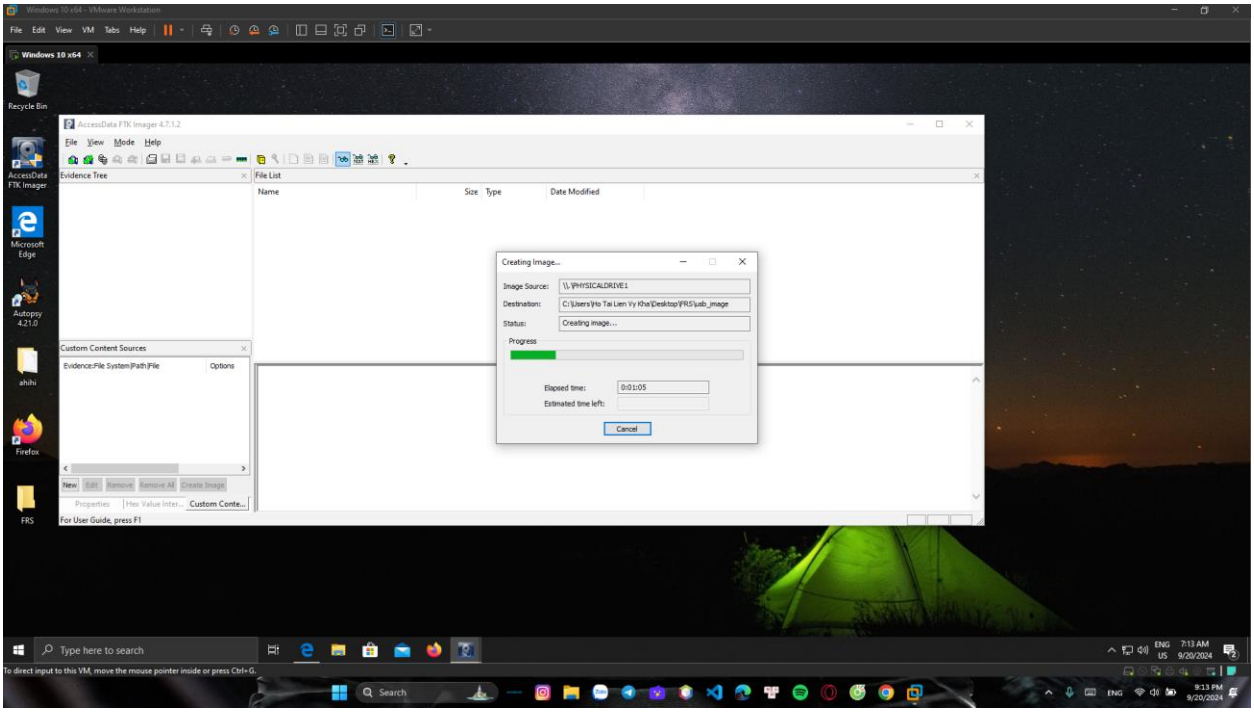

Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Back
Next >
Cancel
Help

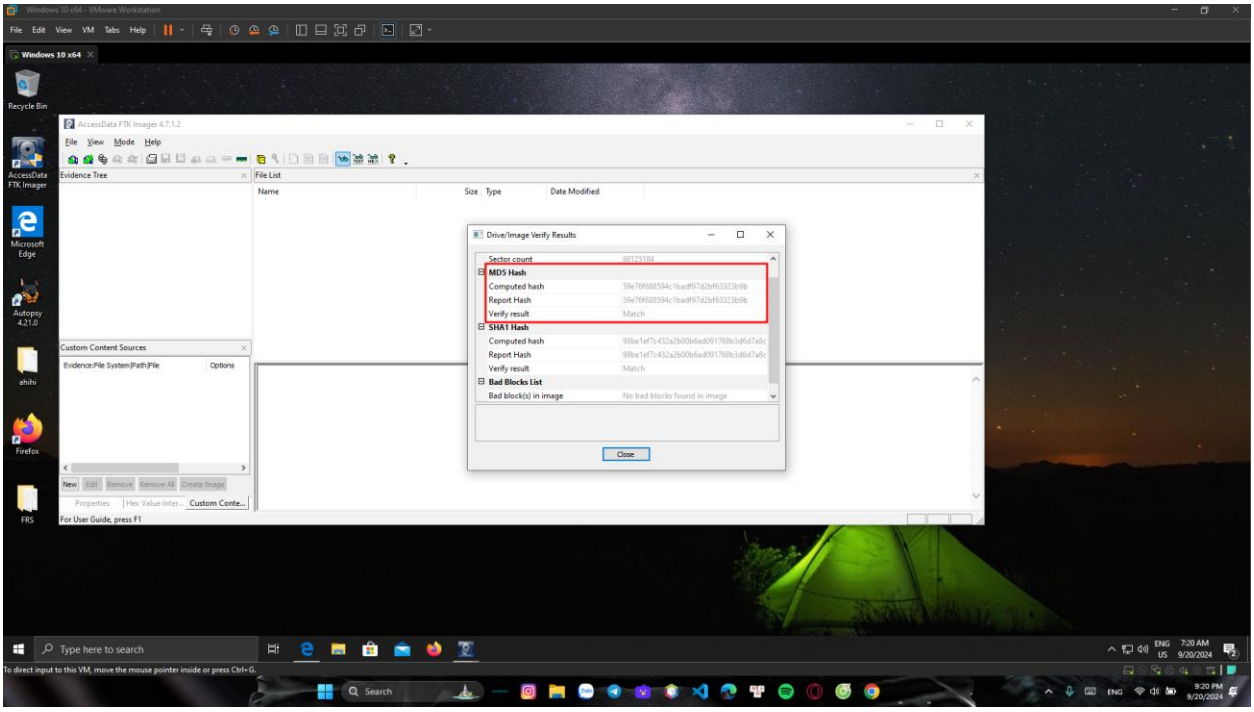

Windows 10 x64 - VMware Workstation
AccessData FTK Imager 4.7.1.2
Create Image
Evidence Item Information
Case Number:
CyberSec400b-001
Evidence Number:
EV-001
Unique Description:
Acquiring a USB image
Examiner:
Admin
Notes:
Image type : dd
< Back
Next >
Cancel
Help
Custom Content Sources
Evidence:File System|Path|File
Options
Type here to search


Windows 10 x64 - VMware Workstation
Recycle Bin
AccessData FTK Imager
Microsoft Edge
Autopsy 4.21.0
ahihi
Firefox
FRS
AccessData FTK Imager 4.7.1.2
Create Image
Select Image Destination
Image Destination Folder
C:\Users\Ho Tai Lien Vy Kha\Desktop\FRS
Browse
Image Filename (Excluding Extension)
Image Fragment Size (MB)
1500
Compression (0=None, 1=Fastest, ..., 9=Smallest)
Use AD Encryption
< Back
Finish
Cancel
Help
Start
Cancel
Browse For Folder
Select the destination folder for the image
Ho Tai Lien Vy Kha
This PC
Libraries
USB Drive (E:)
Network
FRS
Folder:
FRS
Make New Folder
OK
Cancel
1
2
3
Custom Content Sources
Evidence:File System|Path|File
Options
Type here to search


Windows 10 x64
AccessData FTK Imager 4.7.1.2
Create Image
Select Image Destination
Image Destination Folder
C:\Users\Ho Tai Lien Vy Kha\Desktop\FRS
Browse
Image Filename (Excluding Extension)
usb_image
Image Fragment Size (MB)
0
Compression (0=None, 1=Fastest, ..., 9=Smallest)
Use AD Encryption
< Back
Finish
Cancel
Help
Start
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
For User Guide, press F1
Type here to search
Search

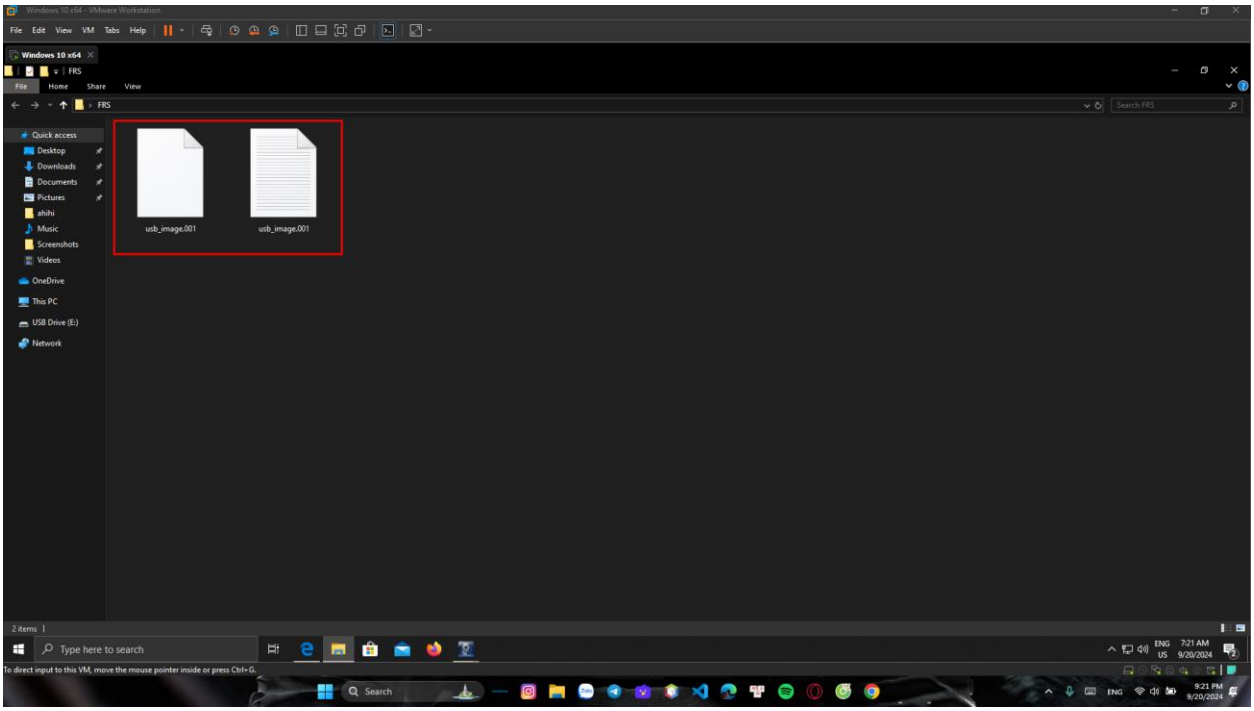

Windows 10 x64
AccessData FTK Imager 4.7.1.2
Create Image
Image Source
\\.\PHYSICALDRIVE1
Starting Evidence Number:
1
Image Destination(s)
C:\Users\Ho Tai Lien Vy Kha\Desktop\FRS\usb_image [raw/dd]
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of files in the image after they are created
Start
Cancel
Custom Content Sources
Evidence:File System|Path|File
Options
For User Guide, press F1
Type here to search
Search
Desktop 3

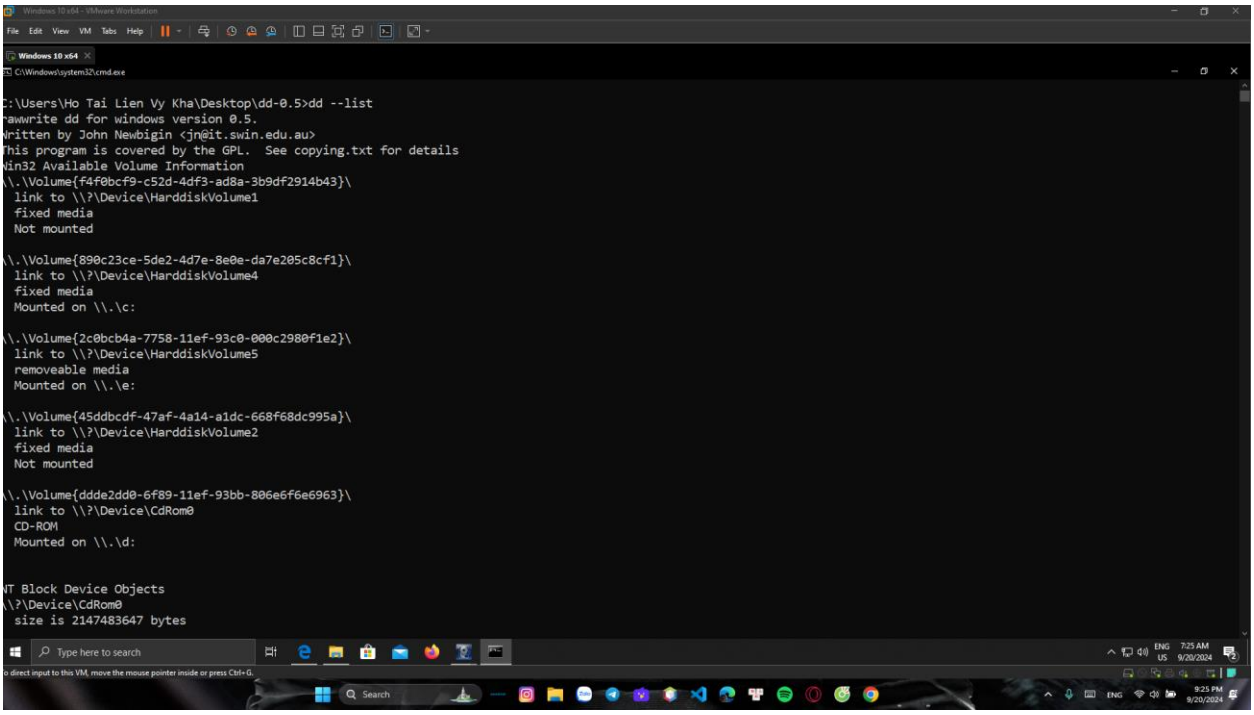


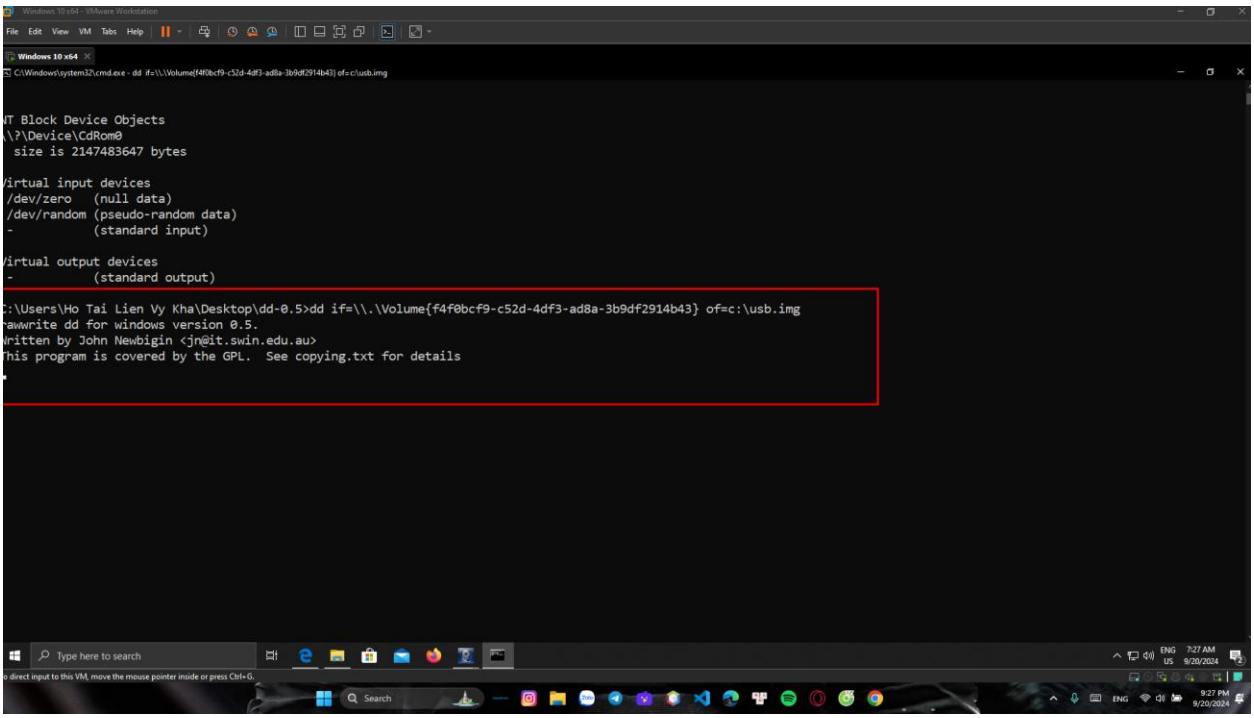


- Unzip dd utility and make a copy on your Desktop
- Check disks
    - *dd --list*
- Acquire the disk image

- *dd if=\\.\Volume{6d634efd-0000-0000-0000-501f00000000} of=c:\usb.img*




C:\Windows\system32\cmd.exe
C:\Users\Ho Tai Lien Vy Kha\Desktop\dd-0.5>dd --list
Rawwrite dd for windows version 0.5.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by the GPL. See copying.txt for details
Win32 Available Volume Information
\\.\Volume{f4f0bcf9-c52d-4df3-ad8a-3b9df2914b43}\
link to \\?\Device\HarddiskVolume1
fixed media
Not mounted
\\.\Volume{890c23ce-5de2-4d7e-8e0e-da7e205c8cf1}\
link to \\?\Device\HarddiskVolume4
fixed media
Mounted on \\.\c:
\\.\Volume{2c0bcb4a-7758-11ef-93c0-000c2980f1e2}\
link to \\?\Device\HarddiskVolume5
removeable media
Mounted on \\.\e:
\\.\Volume{45ddbcdf-47af-4a14-a1dc-668f68dc995a}\
link to \\?\Device\HarddiskVolume2
fixed media
Not mounted
\\.\Volume{ddde2dd0-6f89-11ef-93bb-806e6f6e6963}\
link to \\?\Device\CdRom0
CD-ROM
Mounted on \\.\d:
NT Block Device Objects
\\?\Device\CdRom0
size is 2147483647 bytes
Type here to search
Search


C:\Windows\system32\cmd.exe - dd if=\\.\Volume{f4f0bcf9-c52d-4df3-ad8a-3b9df2914b43} of=c:\usb.img
NT Block Device Objects
\\?\Device\CdRom0
size is 2147483647 bytes
Virtual input devices
/dev/zero (null data)
/dev/random (pseudo-random data)
- (standard input)
Virtual output devices
- (standard output)
C:\Users\Ho Tai Lien Vy Kha\Desktop\dd-0.5>dd if=\\.\Volume{f4f0bcf9-c52d-4df3-ad8a-3b9df2914b43} of=c:\usb.img
Rawwrite dd for windows version 0.5.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by the GPL. See copying.txt for details
Type here to search
Search