

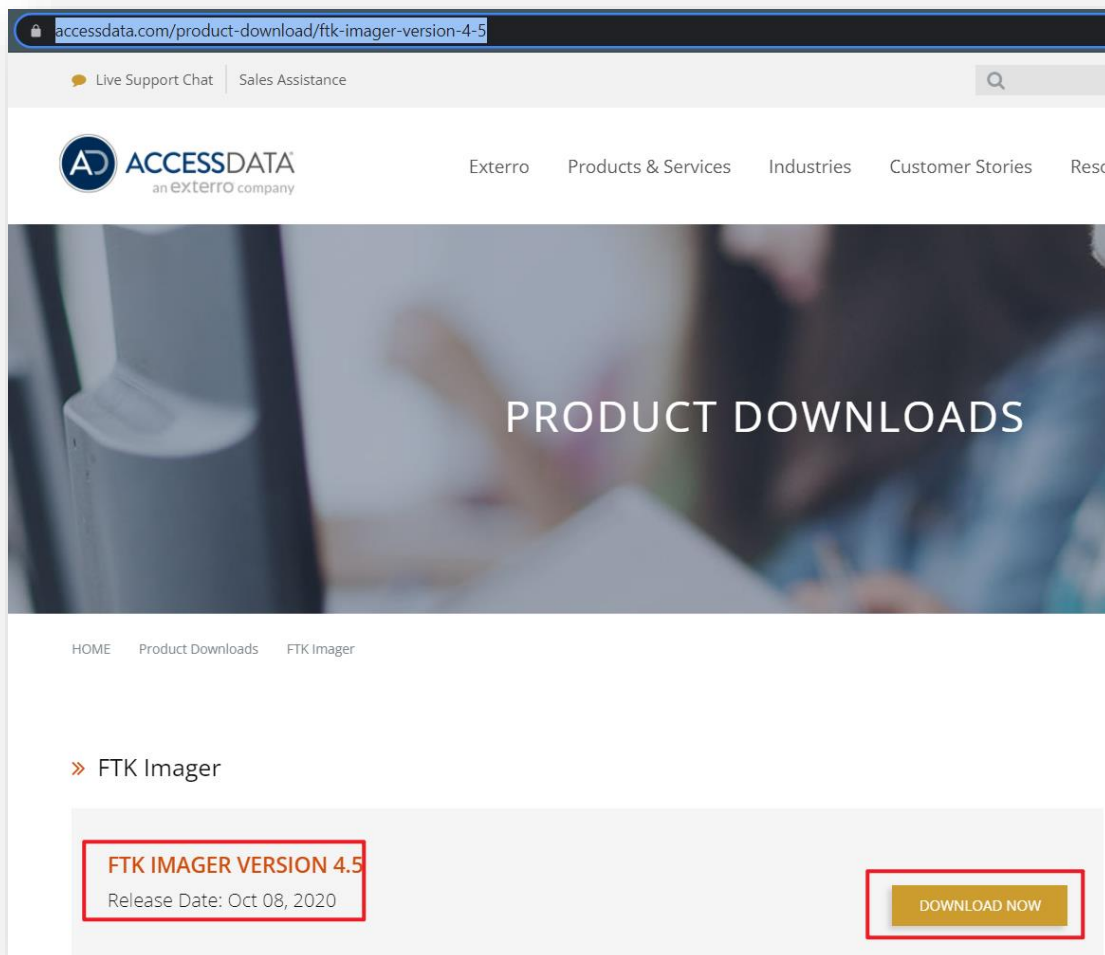
Lab 3: USB_Image_Acquisition

What You Need for this lab

- Install Virtualbox : <https://www.virtualbox.org/wiki/Downloads>
- Install Kali 2021.4. : <https://old.kali.org/kali-images/kali-2021.4/>
 - Notes: Suggest You configure the disk size of Kali VM 80G because the size of each leakage cases image is 30G+
- FTK Imager for windows
<https://accessdata.com/product-download/ftk-imager-version-4-5>
- A flash drive
- The dd utility:
<http://www.chrysocome.net/downloads/dd-0.5.zip>

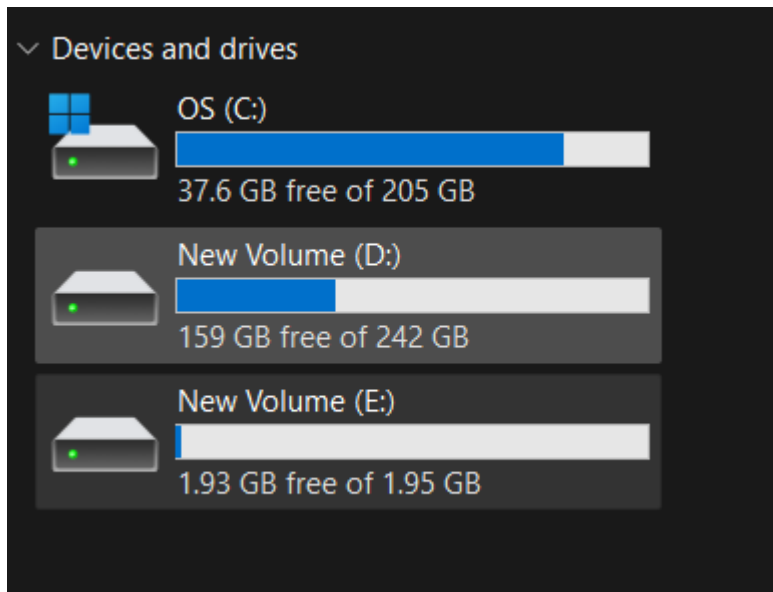
Step 1.

- Download and install FTK



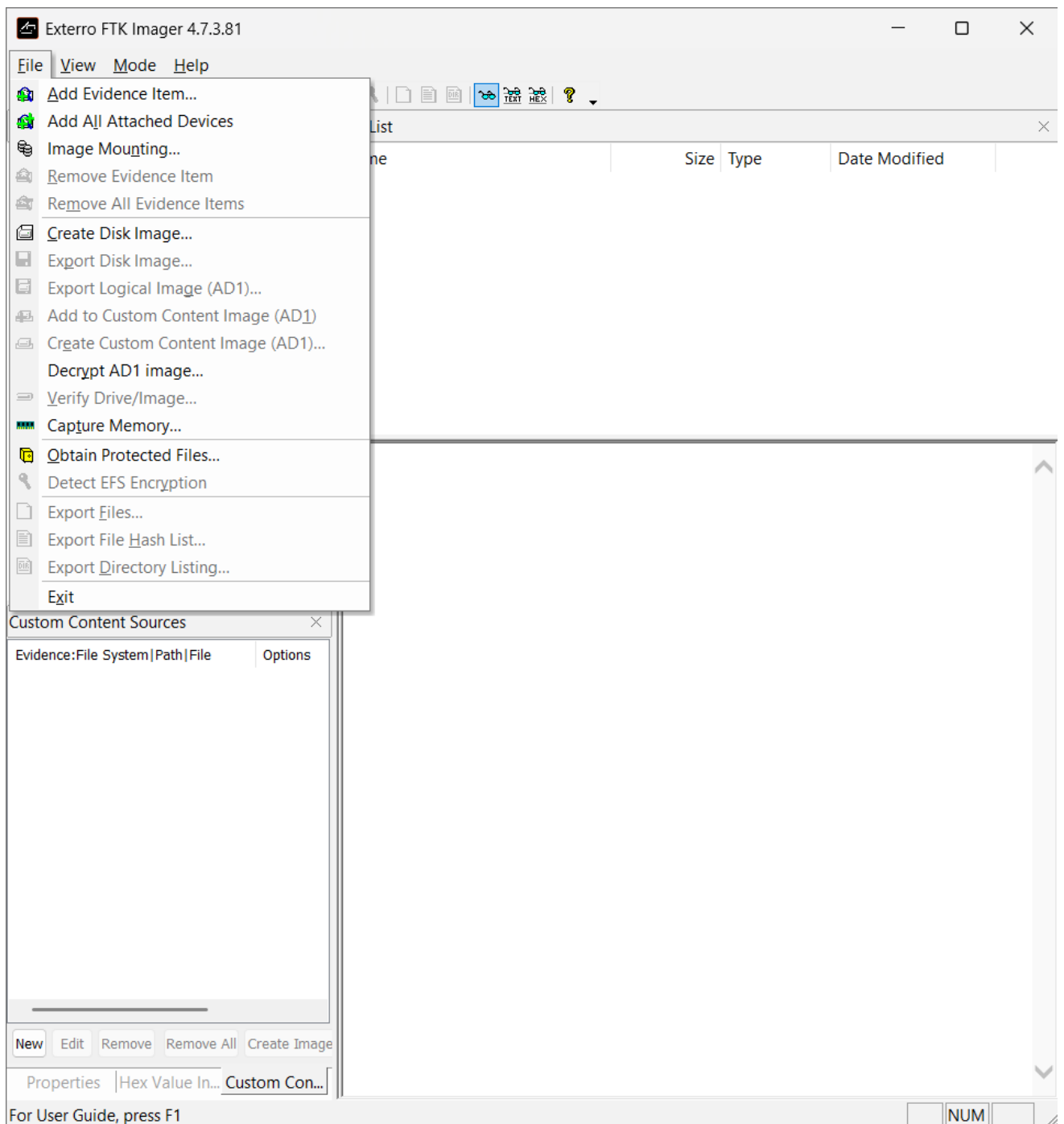
Step 2.

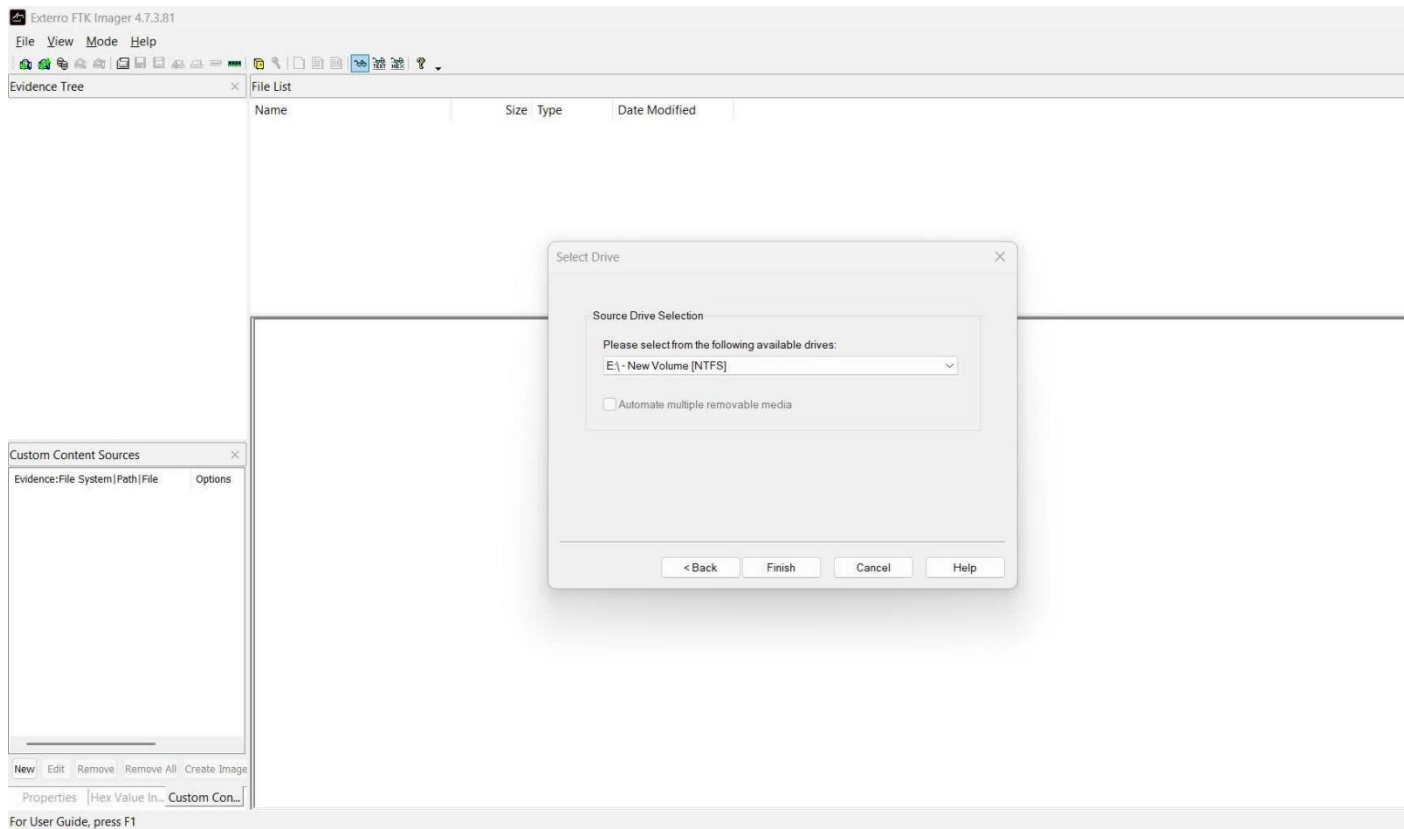
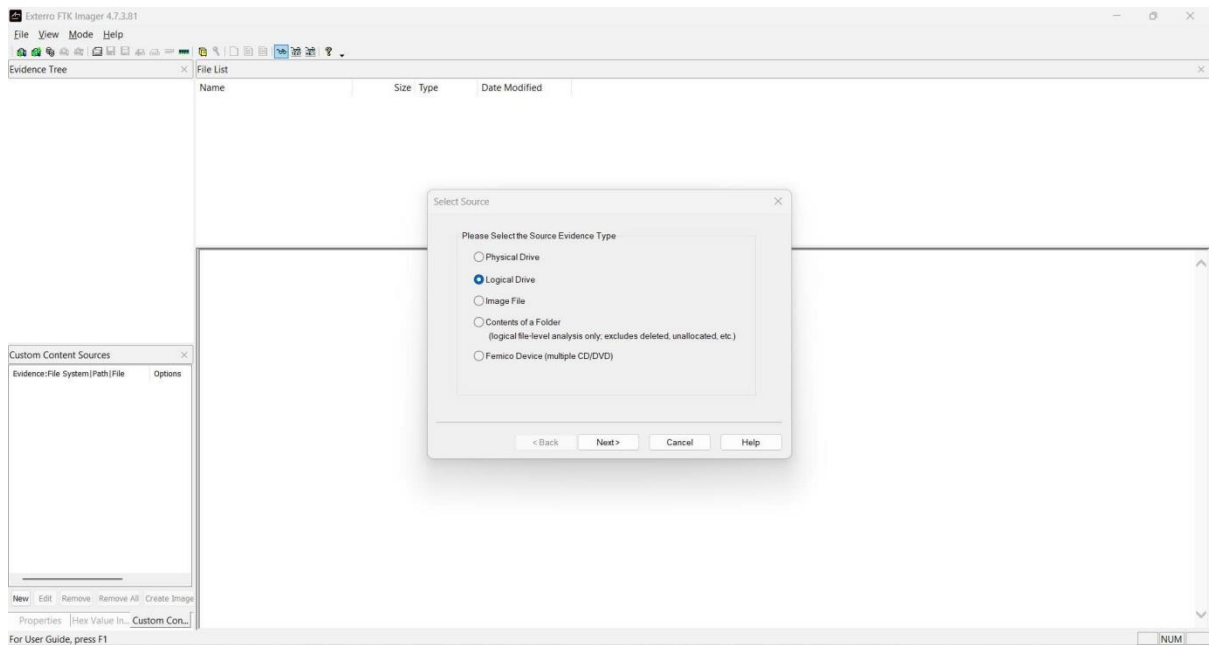
- Plug in a Flash Drive to your computer : you can copy some files to the USB.
- Verify your PC can read the USB drive

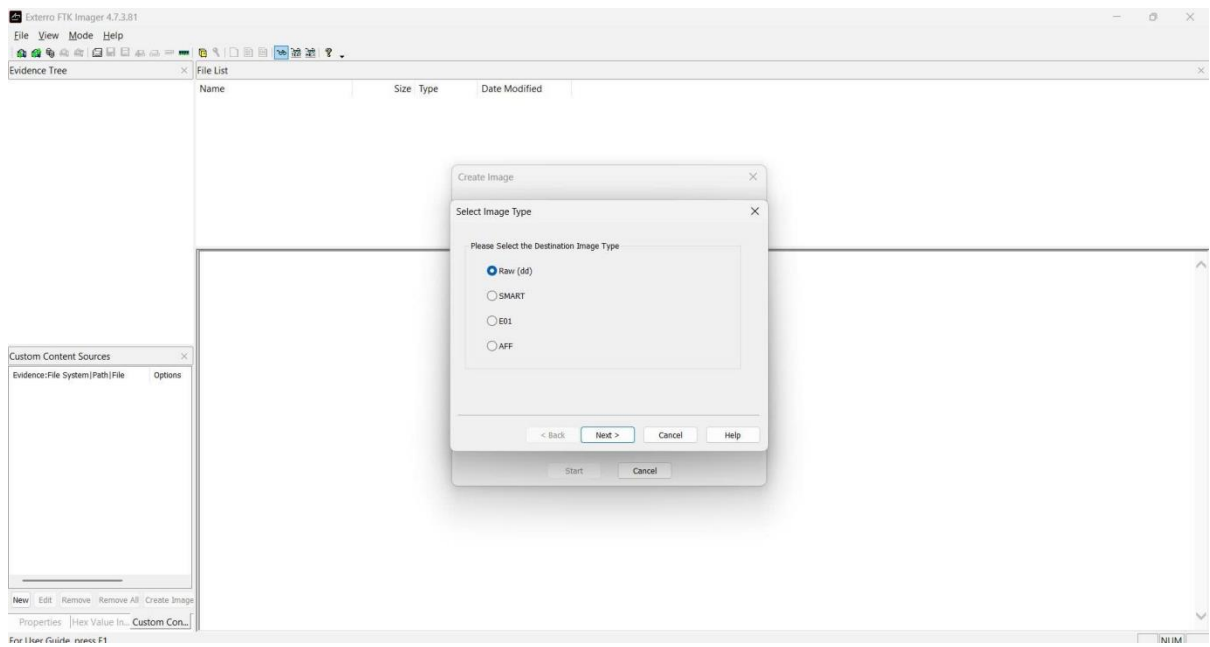
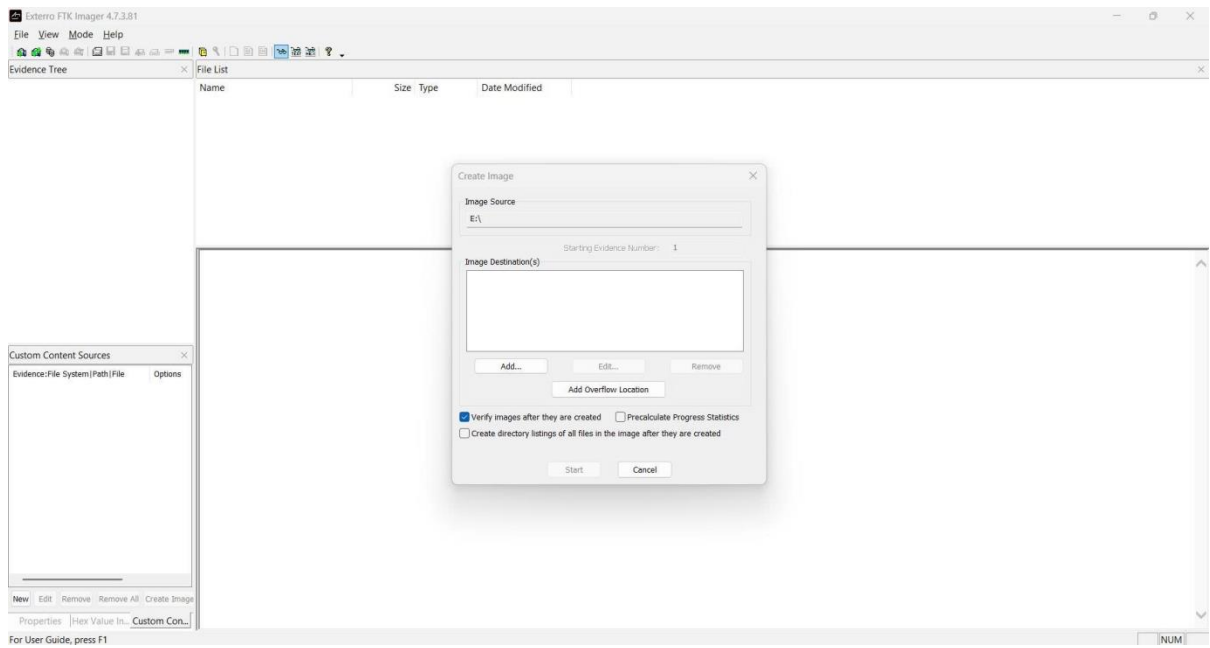


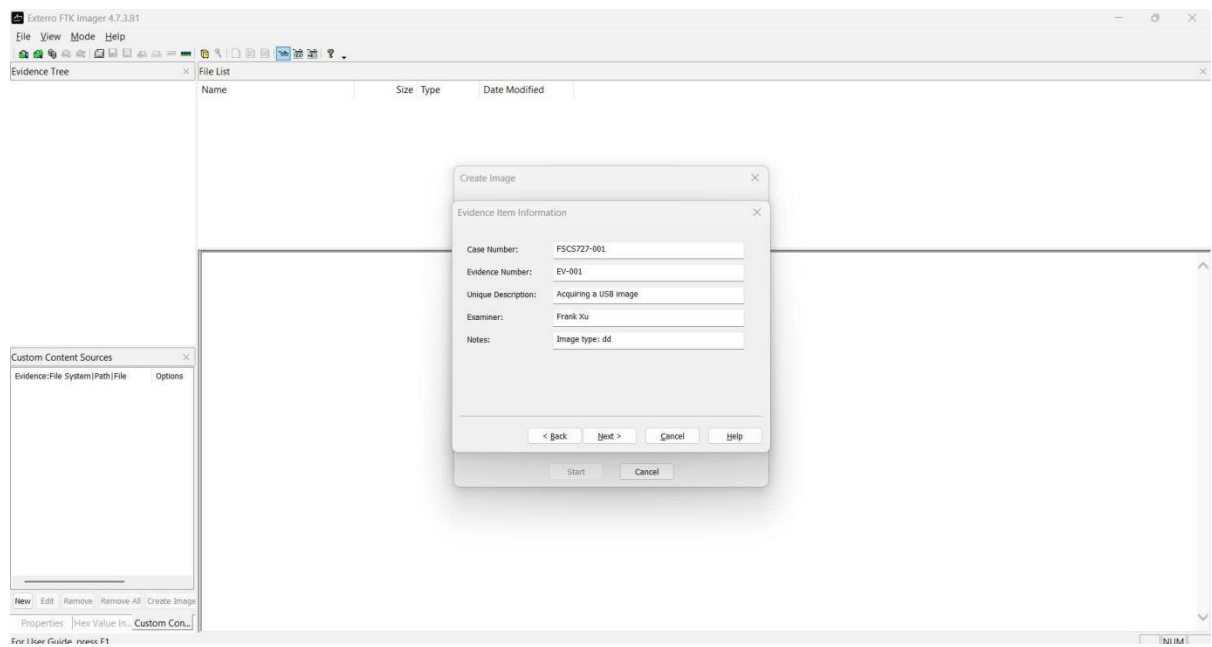
Step 3.

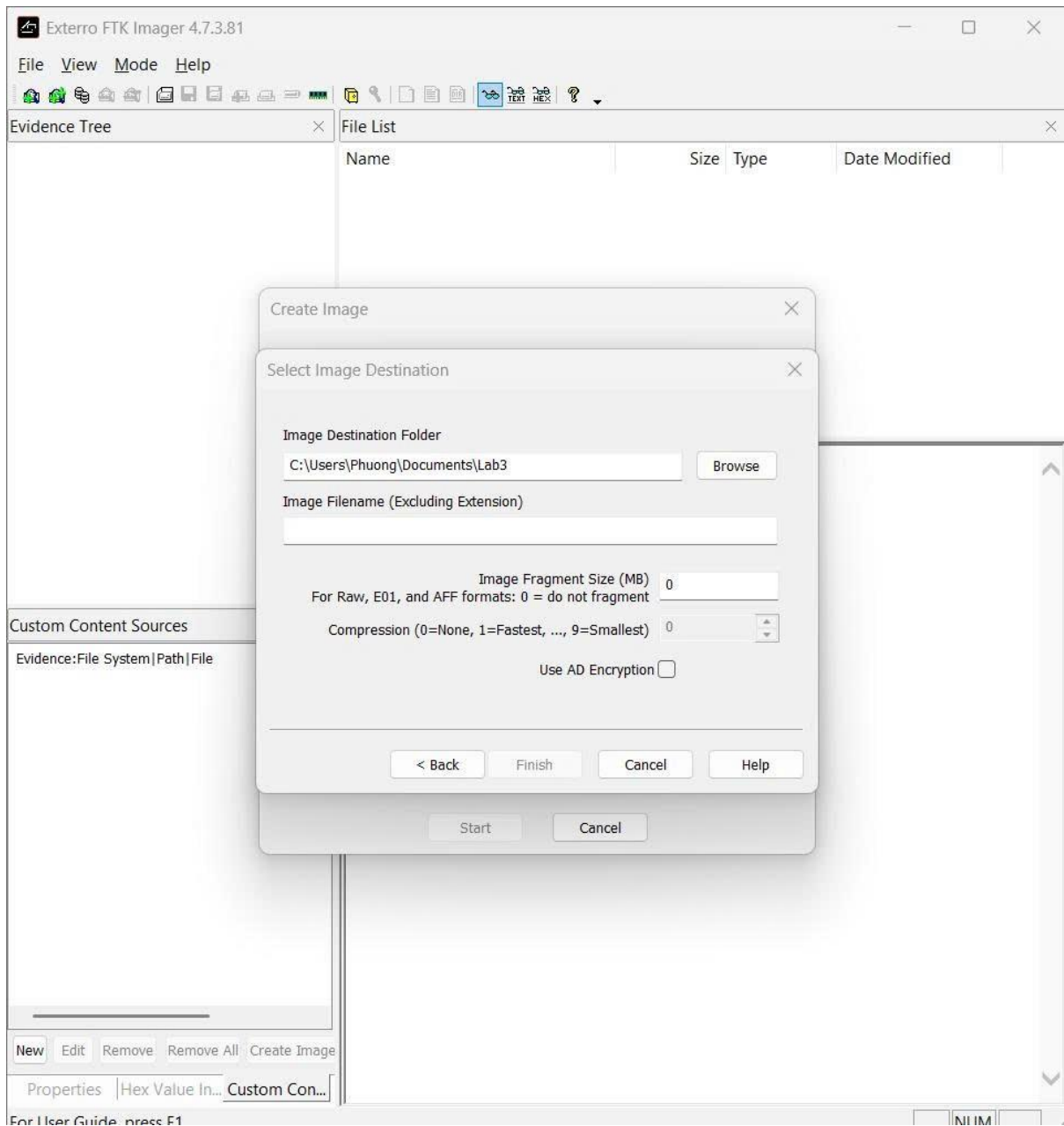
- Acquiring a USB using FTK

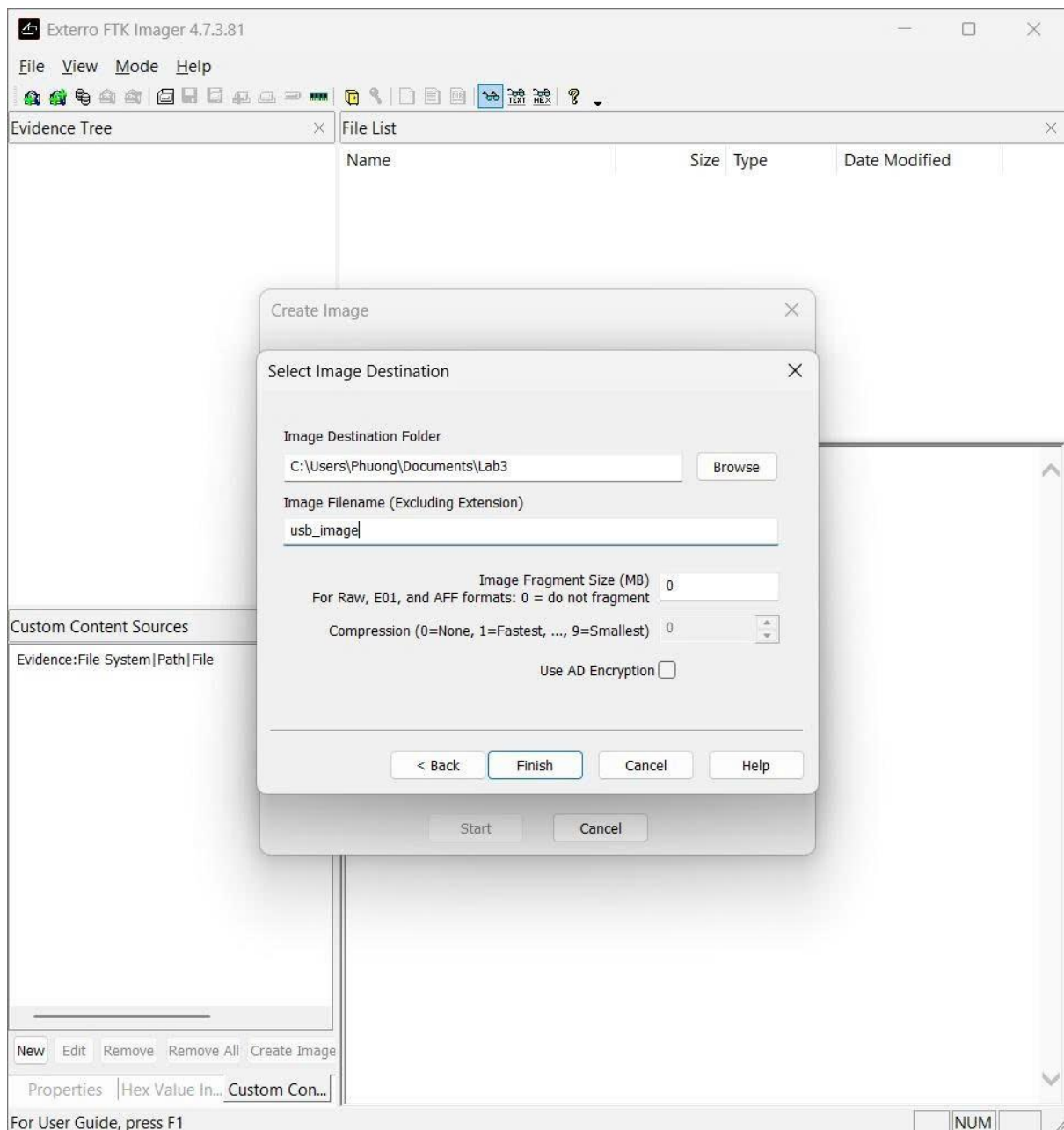


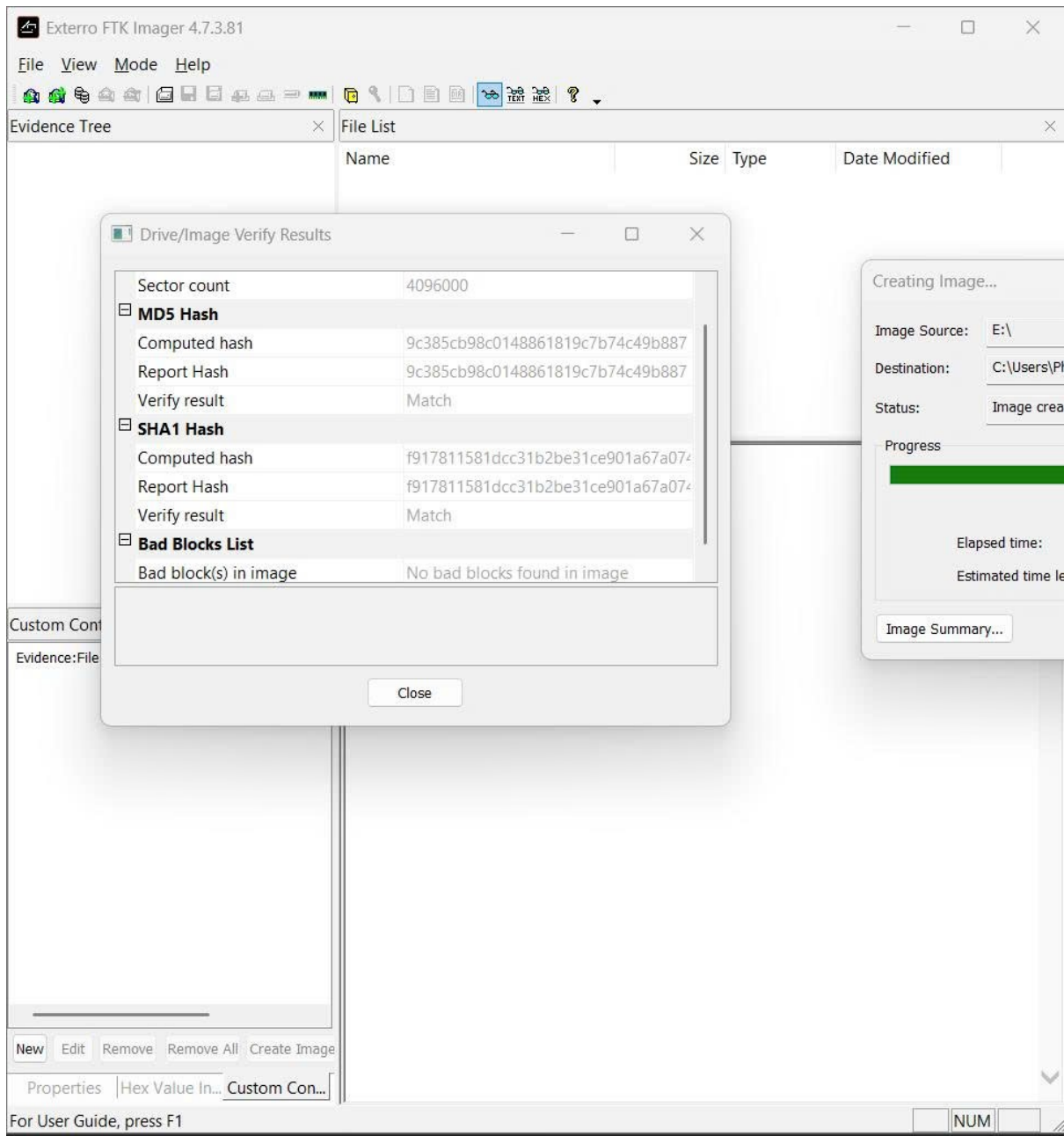








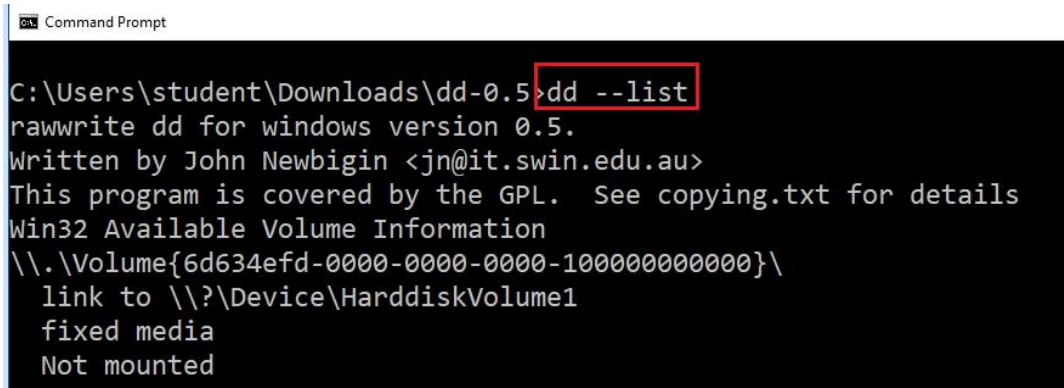




Name	Date modified	Type	Size
usb_image.001	5/27/2025 10:02 AM	WinRAR archive	2,048,000 ...
usb_image.001.txt	5/27/2025 10:02 AM	Text Document	2 KB

-
- 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`



```
Command Prompt
C:\Users\student\Downloads\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{6d634efd-0000-0000-0000-100000000000}\
  link to \\?\Device\HarddiskVolume1
  fixed media
  Not mounted
```

YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT!

Save the document with the filename "**YOUR NAME Lab 3.pdf**", replacing "YOUR NAME" with your real name.

Email the image to the instructor as an attachment to an e-mail message. Send it to: **xxx@fe.edu.vn** with a subject line of "**Lab 3 From YOUR NAME**", replacing "YOUR NAME" with your real name.