

# Lab Assignment



Copyright © 1996–2021 HackerU Ltd.  
All Rights Reserved.

Cybersecurity Professional Program

Digital Forensics &  
Incident Response

## Data Acquisition

**DFIR-04-L2**

**FTK Drive Capture**

## Lab Objective

Become familiar with the **FTK Imager** and **OSFMount** tools used to mount and view drives.

## Lab Mission

Create a disk image with **FTK Imager** and mount it using **OSFMount**.

## Lab Duration

20–30 minutes

## Requirements

- Basic knowledge of the Linux environment
- Knowledge of data acquisition

## Resources

- Environment & Tools
  - VirtualBox
    - Windows 10
- Extra Lab Files
  - ***Window.png***
  - ***osfmount.exe***
  - ***AccessDataFTKImager.exe***



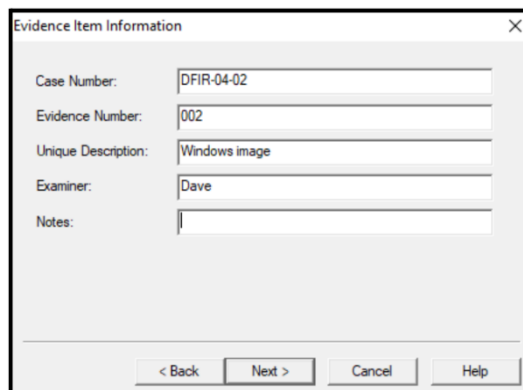
## Textbook References

- Chapter 4: Data Acquisition
  - Section 2: Drive Capture
  - Section 3: Advanced Capture Tools
  - Section 4: Evidence Inspection

## Lab Task: Create & Mount a Disk Image

Create a capture of a drive using **FTK Imager** and mount the image using **OSFMount**.

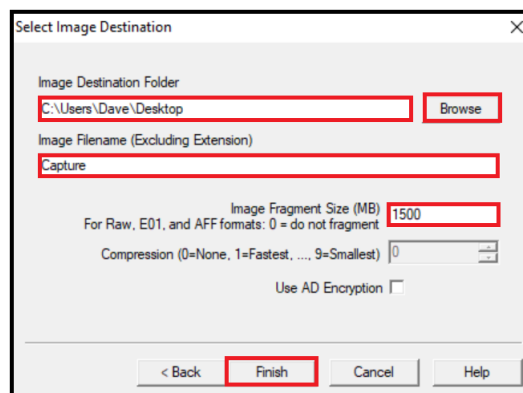
- 1 Copy the provided **Window.png** file to the 10 GB drive in your Windows 10 VM created in DFIR-04-L1.
- 2 Transfer the provided **AccessData FTK Imager.exe** file to the Windows 10 machine's desktop and install it.
- 3 In **FTK Imager**, go to **File**, click **Create Disk Image** to make an image of the **10 GB** drive, and save it to the **C** drive.  
**Note:** Be sure to select the 10 GB drive in the dropdown menu within the **Source Drive Selection** window.
- 4 In **Image Source**, press **Add** and select **E01**. Then, enter the evidence item information. In the **Select Image Destination** window, set the destination folder to the desktop, name the image, and set the fragment size to 1500. Click **Finish** and start the image capture.



The 'Evidence Item Information' dialog box contains the following fields:

Case Number:	DFIR-04-02
Evidence Number:	002
Unique Description:	Windows image
Examiner:	Dave
Notes:	

At the bottom are buttons: < Back, Next >, Cancel, and Help.

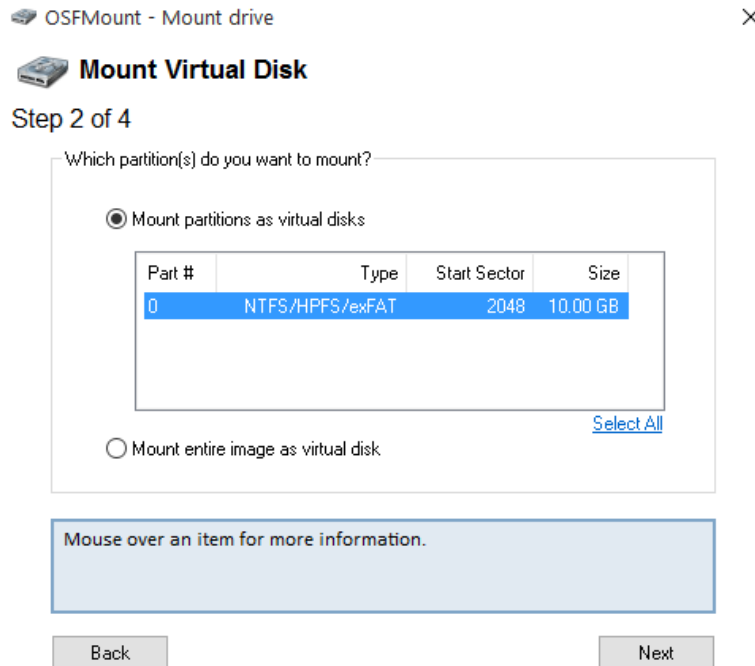


The 'Select Image Destination' dialog box contains the following fields and options:

Image Destination Folder	C:\Users\Dave\Desktop	Browse
Image Filename (Excluding Extension)	Capture	
Image Fragment Size (MB)	1500	
Compression (0=None, 1=Fastest, ..., 9=Smallest)	0	
Use AD Encryption	<input type="checkbox"/>	

At the bottom are buttons: < Back, Finish, Cancel, and Help. The 'Finish' button is highlighted with a red box.

- 5 Transfer the **OSFMount.exe** file to the Windows 10 machine and install it.
- 6 Mount the E01 image in **OSFMount** by clicking **Mount New** and selecting the **Capture.E01** file. Make sure you use partition **0** and continue with the default settings.



- 7 Double-click the mounted device to view the content inside. You should have the same image from the 10 GB drive, which means a successful drive capture.