Disk Image Forensics

Dr. Darryl J D’Souza
Mob No: 9986382162

Basic Terminology

Disk Image

A disk image is a bit-by-bit copy of an entire disk (such as a hard drive, USB, etc.) or partition that preserves the exact content and structure of the original data. It includes not only the files and folders but also the empty space, metadata, and other hidden data that is not normally visible.

Disk Imaging

Disk imaging is the process of creating a forensic copy of a storage device, such as a hard drive or USB drive. It is a crucial step in digital forensics because it ensures that the original data remains intact and unmodified. Cryptographic hashes are used to verify that the copy is exactly the same as the original, ensuring that no modifications have been made to the original data. This approach allows forensic investigators to work with the copy without worrying about accidentally altering the original data.

Basic Terminology

Disk Image Forensics

Disk image forensics is the process of analyzing a disk image to search for evidence of interest. This includes using tools like Autopsy and FTK Imager to uncover useful information and analyze system artifacts like the windows registry, web browsers, LNK Files, event logs, command prompt history, etc.

There are several tools that can be used for disk image forensics, such as Autopsy and FTK Imager. While Autopsy offers more features during analysis, we'll be using FTK Imager for its lightweight nature.

The tool can be downloaded from https://www.exterro.com/ftk-imager.

Steps to Run FTK Imager from a Flash Drive:

1. **Download FTK Imager:**
   - Visit the official website of AccessData (now part of Exterro) or a trusted source to download the FTK Imager executable.
   - Ensure you download the correct version compatible with your system (32-bit or 64-bit).
2. **Prepare the Flash Drive:**
   - Insert your flash drive into a USB port on your computer.
   - Ensure the flash drive has enough free space to store the FTK Imager executable and any associated files.
3. **Copy FTK Imager to the Flash Drive:**
   - Locate the downloaded FTK Imager executable file (usually named something like FTK Imager.exe).
   - Copy the executable file to the root directory or a specific folder on your flash drive.
4. **Run FTK Imager from the Flash Drive:**
   - Safely eject the flash drive from your computer.
   - Insert the flash drive into the USB port of the computer where you want to run FTK Imager.
   - Open the flash drive in File Explorer.
   - Double-click the FTK Imager.exe file to launch the application.
5. **Using FTK Imager:**
   - Once FTK Imager is running, you can use it to create disk images, preview files, and perform other forensic tasks as needed.

Steps to Run FTK Imager from a Flash Drive:

Additional Tips:

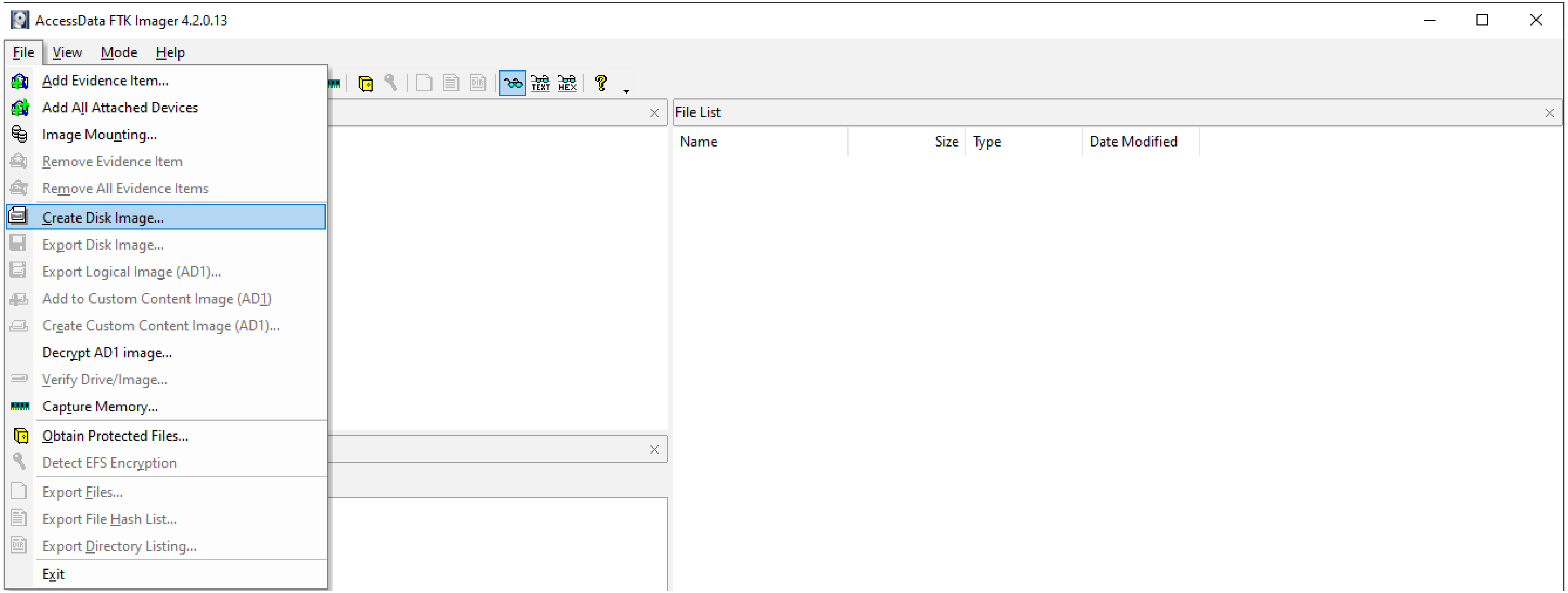
- **Administrator Privileges:** Depending on the tasks you’re performing, you might need to run FTK Imager with administrator privileges. Right-click the FTK Imager.exe file and select **Run as administrator**.
- **Antivirus Software:** Some antivirus programs might flag FTK Imager as a potential threat due to its forensic capabilities. Ensure your antivirus software is configured to allow FTK Imager to run.
- **Portable Mode:** Since FTK Imager is portable, it won’t leave traces on the host system, making it ideal for forensic investigations.

Important Considerations:

- **Legal Compliance:** Ensure you have the proper authorization to use FTK Imager on the system you’re investigating. Unauthorized use of forensic tools can be illegal.
- **Data Integrity:** Be cautious when working with live systems to avoid altering data. FTK Imager is designed to be read-only, but always double-check your actions.

Acquiring a Disk Image

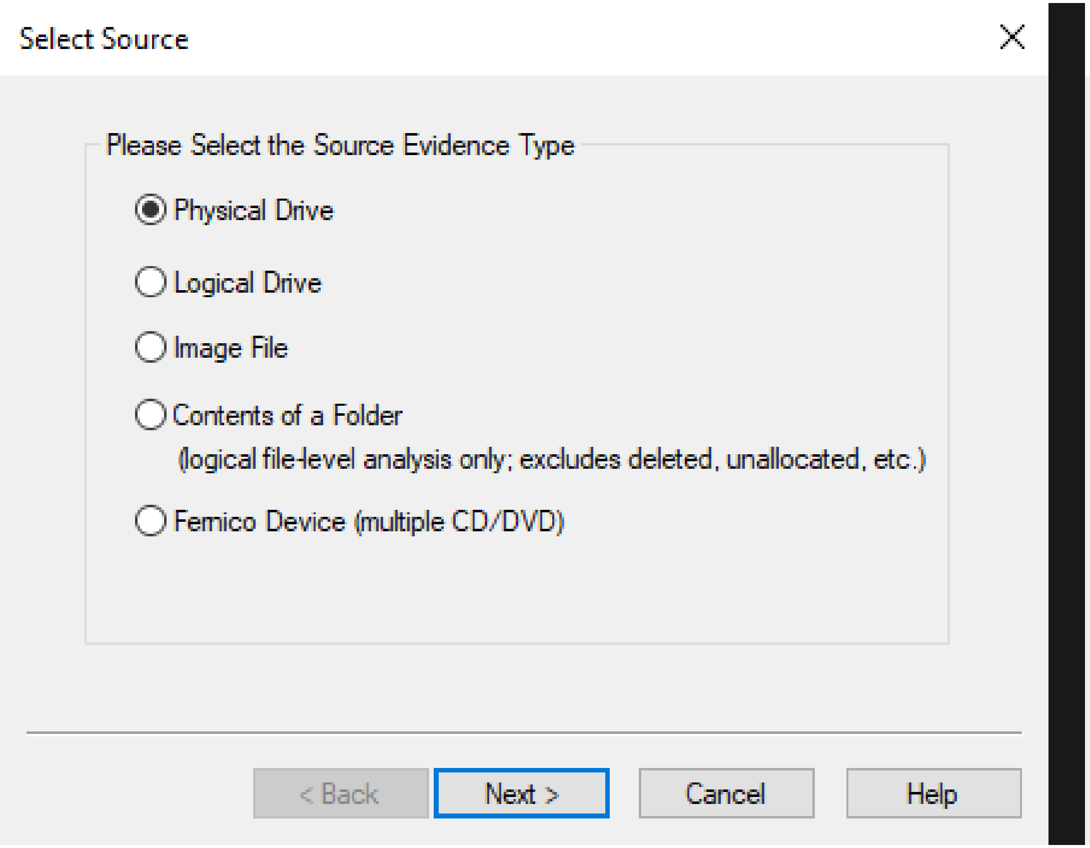
1. Open FTK Imager, go to File → Create Disk Image.



Dr. Darryl J D’Souza

Acquiring a Disk Image

2. Select Physical Drive, then click next and choose the drive you want to create an image of. For this example, I'll pick my USB drive.



Select Source

Please Select the Source Evidence Type

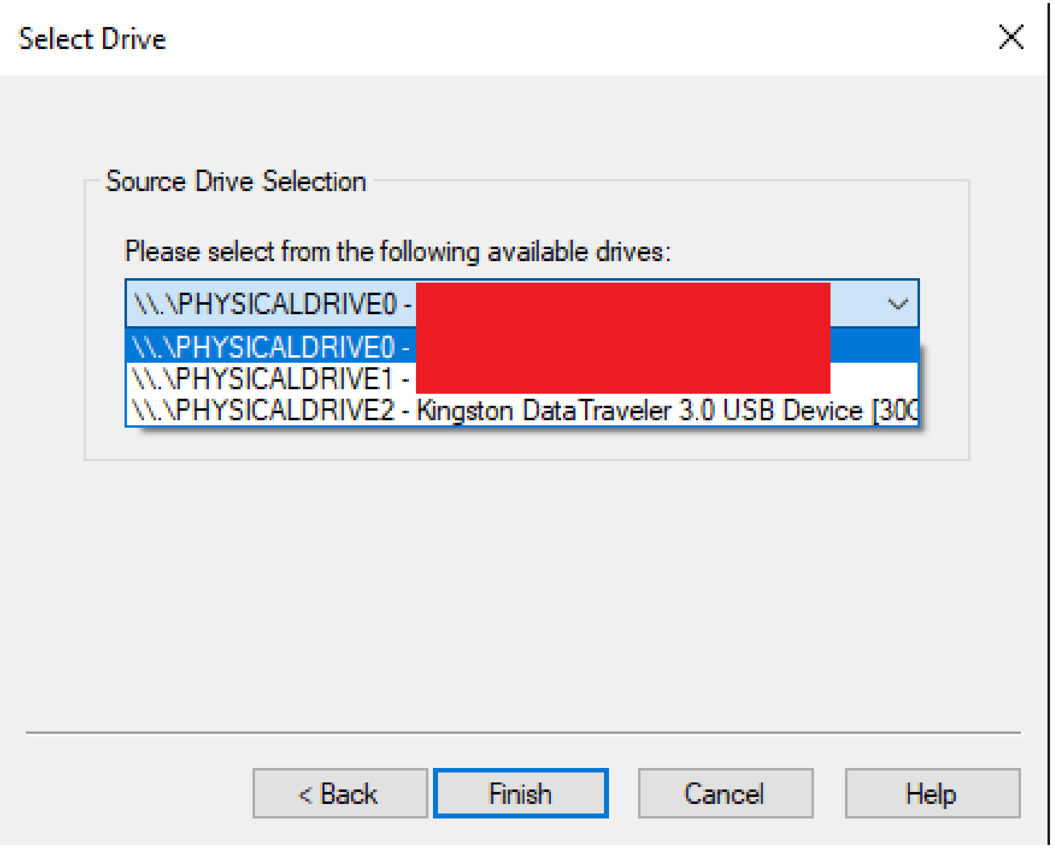
● Physical Drive

○ Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Fernico Device (multiple CD/DVD)



Select Drive

Source Drive Selection

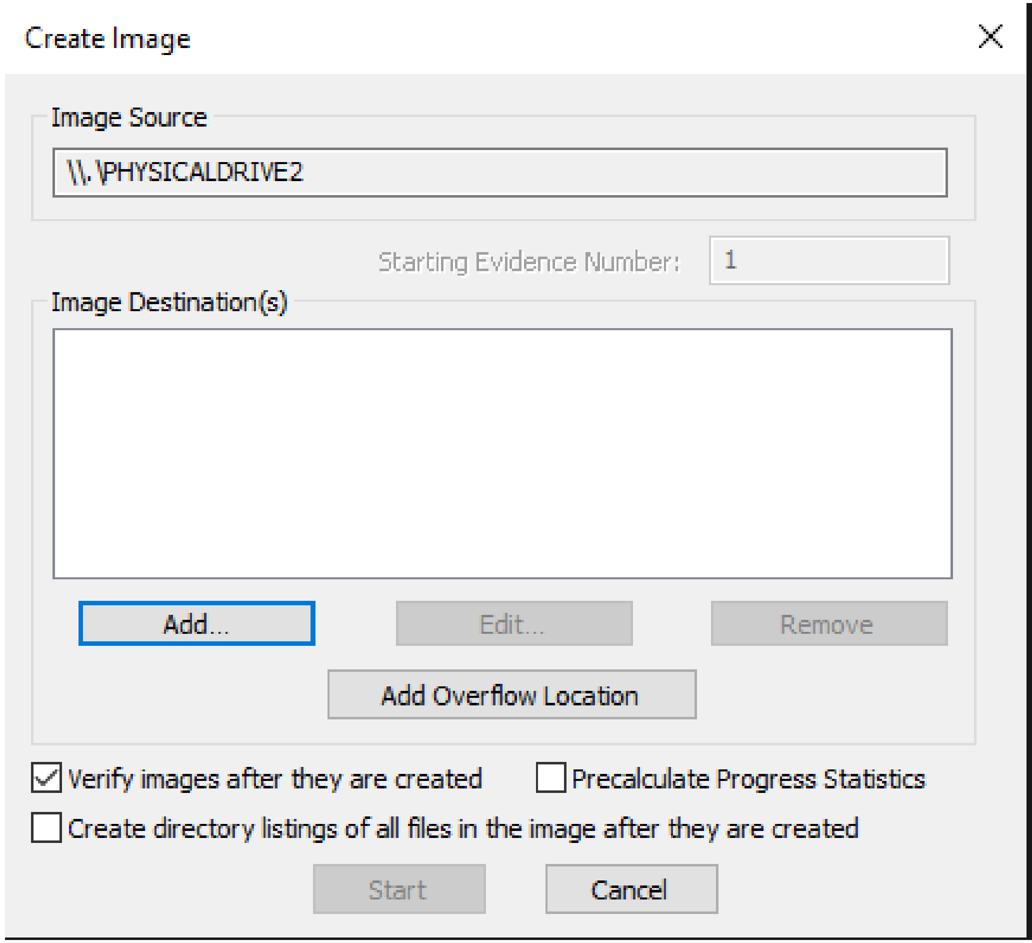
Please select from the following available drives:

\\.\PHYSICALDRIVE0 - [redacted]

\\.\PHYSICALDRIVE0 - [redacted]
\\.\PHYSICALDRIVE1 - [redacted]
\\.\PHYSICALDRIVE2 - Kingston DataTraveler 3.0 USB Device [300

Acquiring a Disk Image

3. Next, click the Add button under Image Destination(s). Then, select the destination image type as Raw (dd).



Create Image

Image Source

\\.\PHYSICALDRIVE2

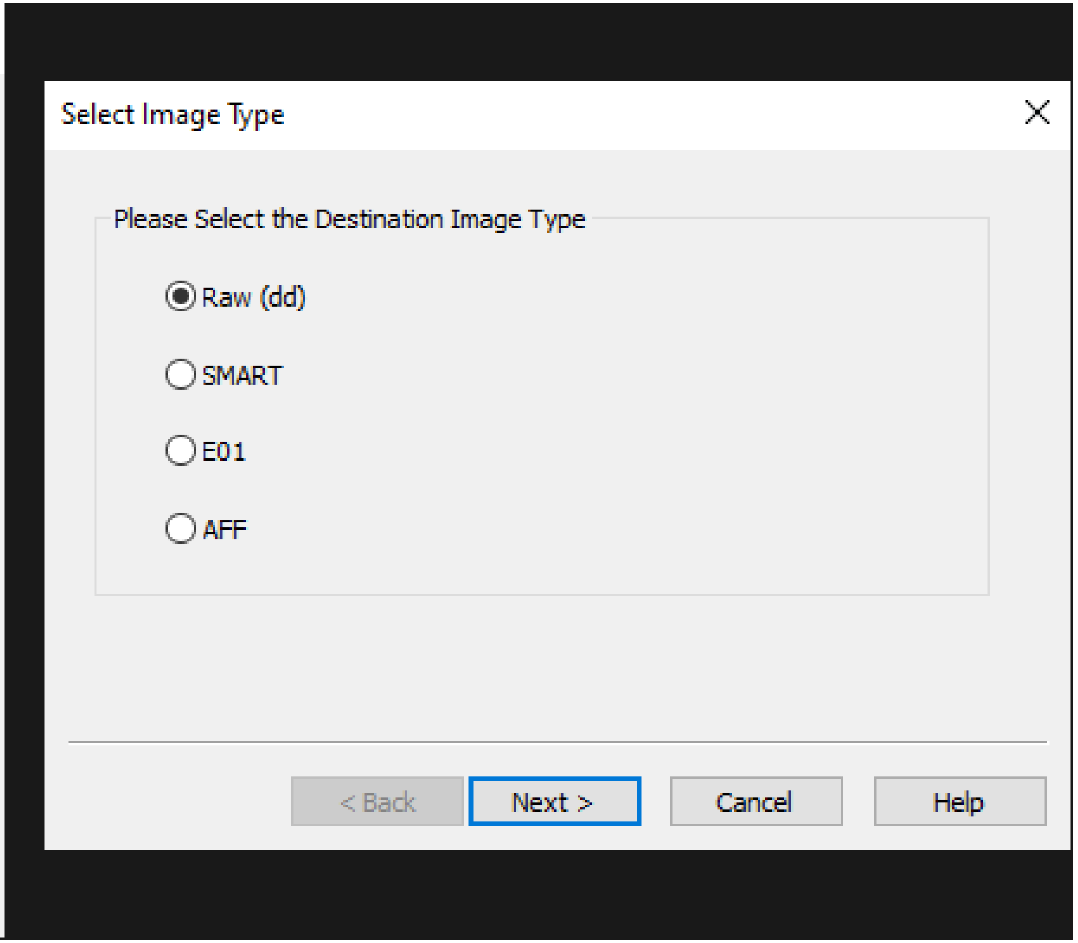
Starting Evidence Number: 1

Image Destination(s)

☑ Verify images after they are created

□ Precalculate Progress Statistics

□ Create directory listings of all files in the image after they are created



Select Image Type

Please Select the Destination Image Type

● Raw (dd)

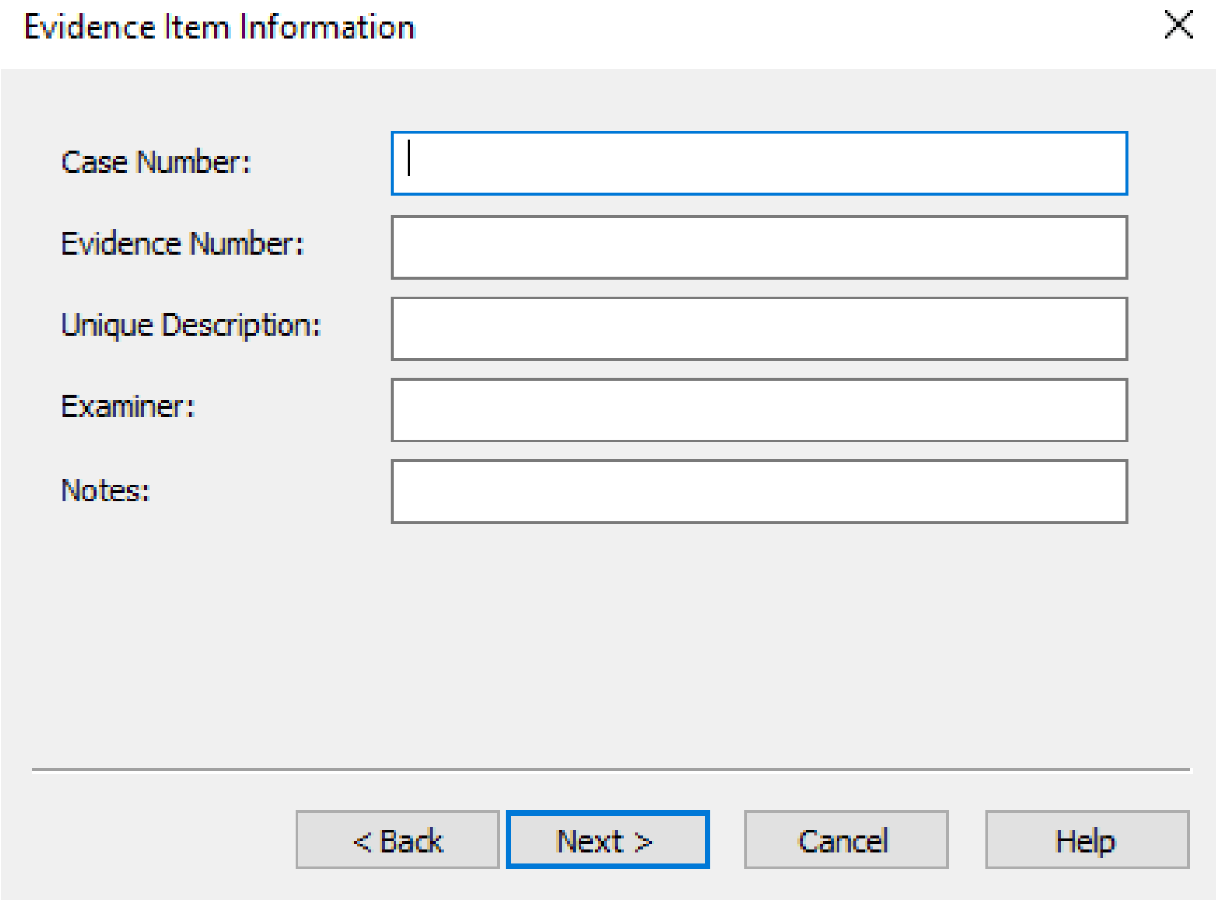
○ SMART

○ E01

○ AFF

Acquiring a Disk Image

4. Enter the relevant details about the evidence, then choose a folder and a name to save the disk image.



Evidence Item Information

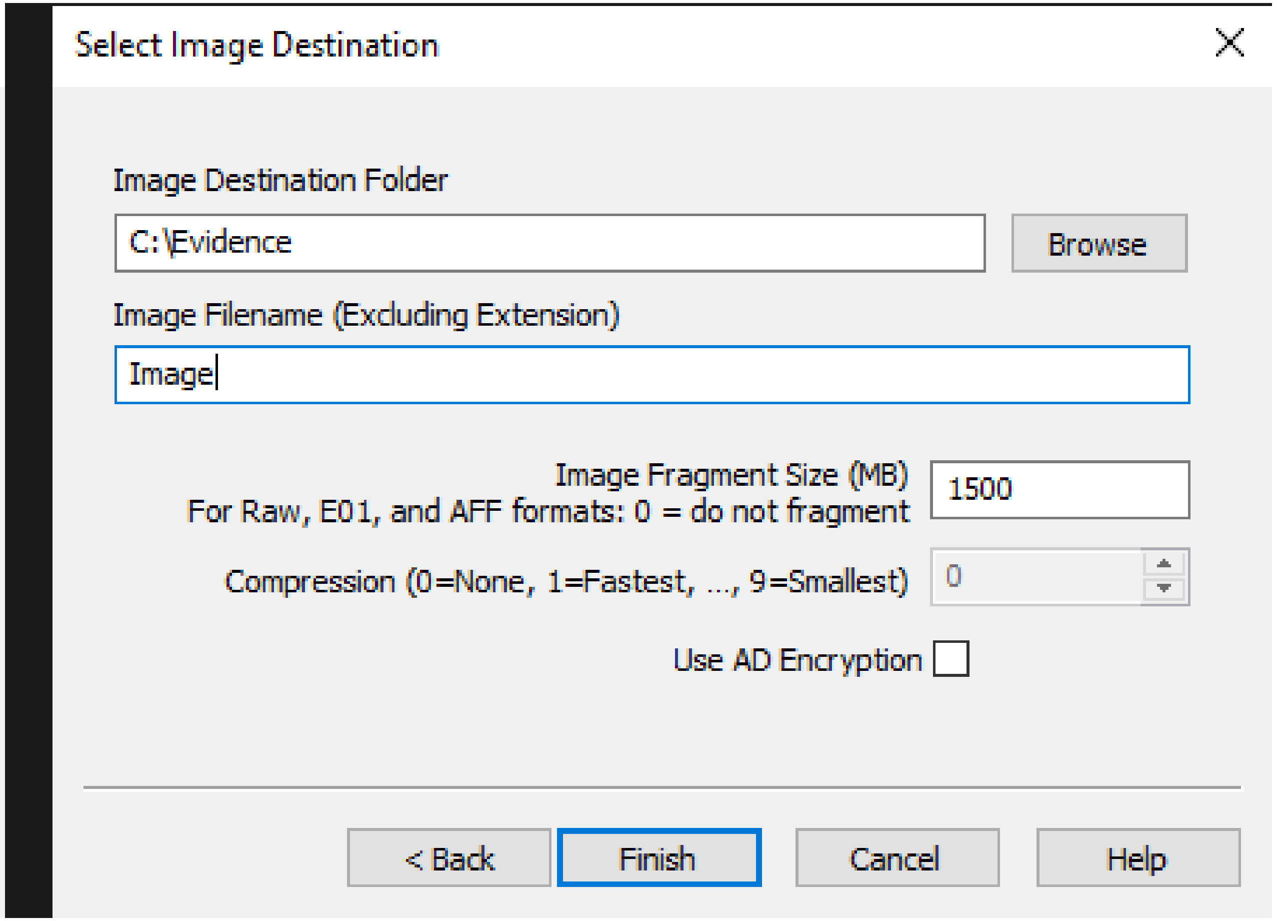
Case Number:

Evidence Number:

Unique Description:

Examiner:

Notes:



Select Image Destination

Image Destination Folder

C:\Evidence

Image Filename (Excluding Extension)

Image

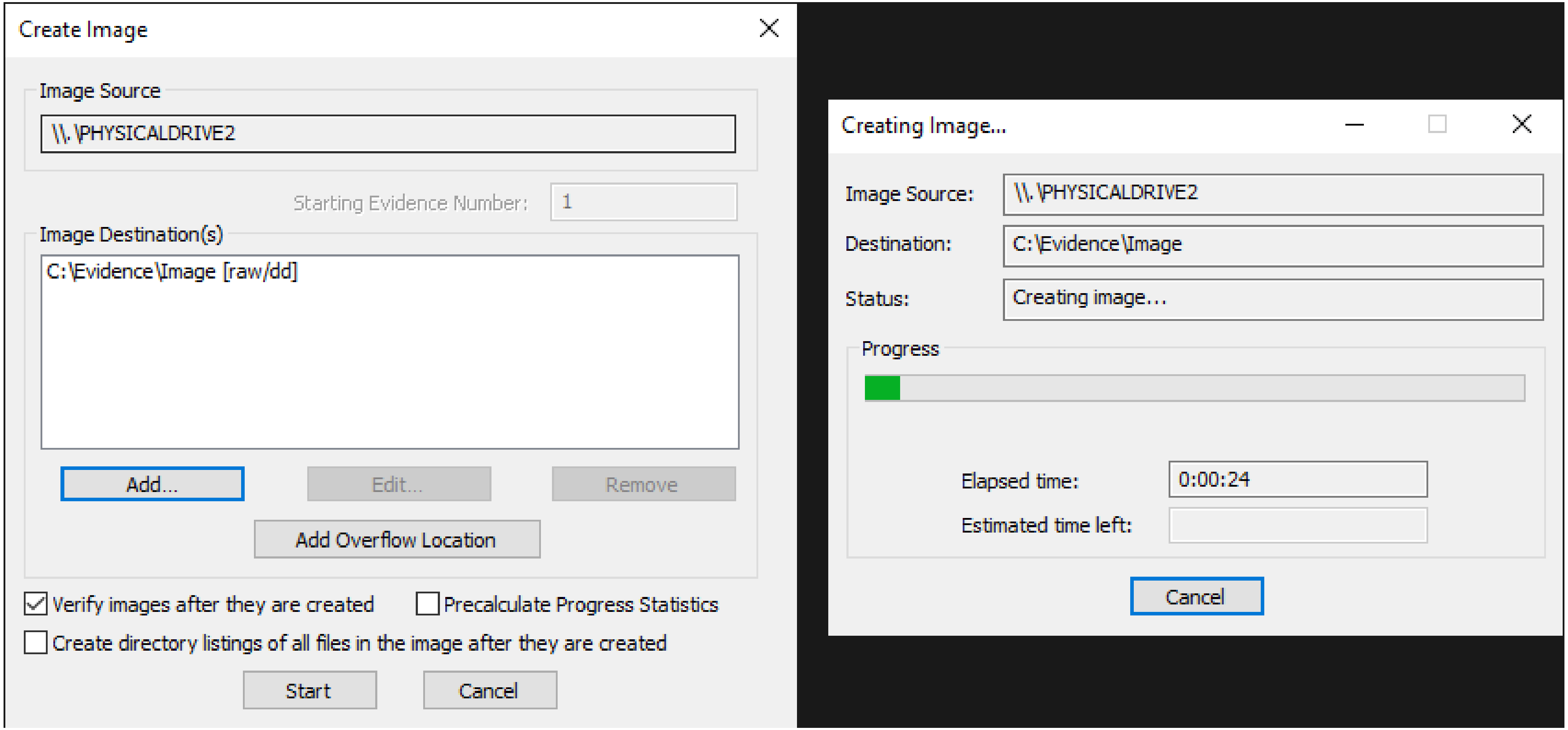
Image Fragment Size (MB) 1500
For Raw, E01, and AFF formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest) 0

Use AD Encryption ☐

Acquiring a Disk Image

5. Finally, click start to begin the creation process. It can take a little while to complete depending on the size of the drive.



Create Image

Image Source

\\.\PHYSICALDRIVE2

Starting Evidence Number: 1

Image Destination(s)

C:\Evidence\Image [raw/dd]

☑ Verify images after they are created □ Precalculate Progress Statistics

□ Create directory listings of all files in the image after they are created

Creating Image...

Image Source: \\.\PHYSICALDRIVE2

Destination: C:\Evidence\Image

Status: Creating image...

Progress

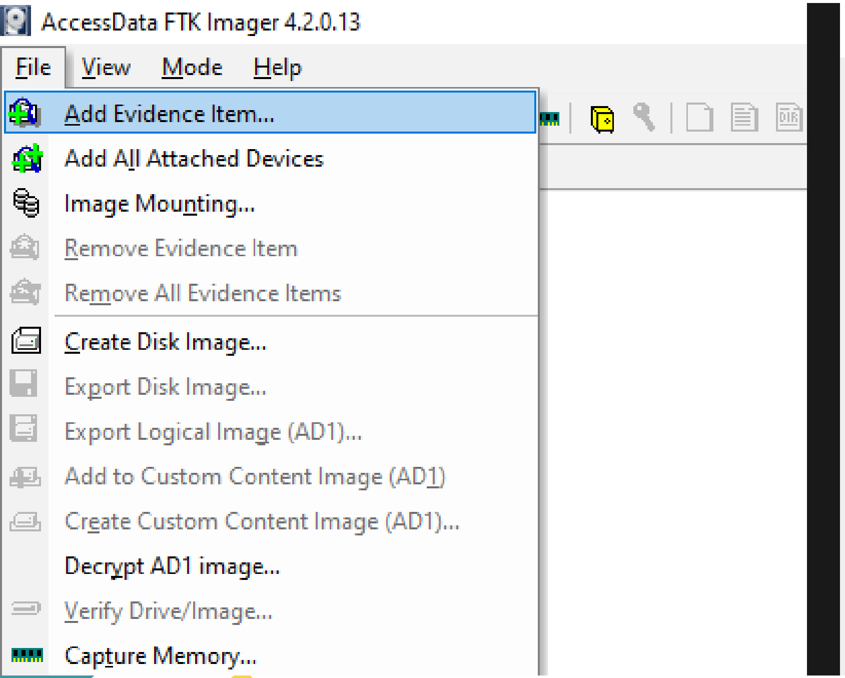
Elapsed time: 0:00:24

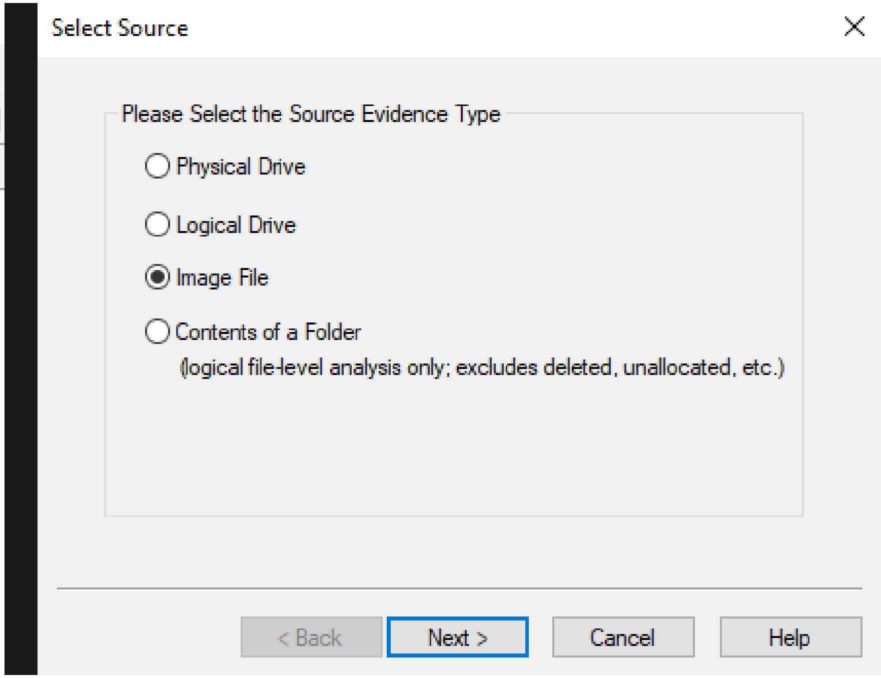
Estimated time left:

Analyzing a Disk Image

Download this disk image from your teams Lab 6 folder - Image.ad1

To open a disk image in FTK Imager, click on "File" and then select "Add Evidence Item". From there, choose "Image File" and select the disk image you want to analyze:





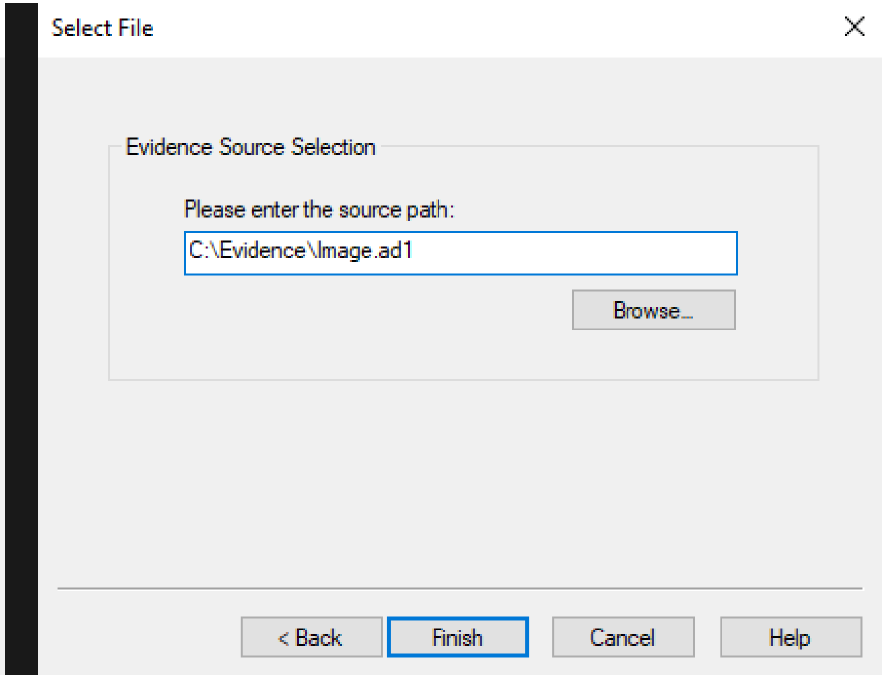
Please Select the Source Evidence Type

○ Physical Drive

○ Logical Drive

● Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)



Please enter the source path: C:\Evidence\Image.ad1

💡 Although FTK Imager is lightweight, it requires us to have prior knowledge about the files that are present inside a disk image and their locations. On the other hand, Autopsy automatically parses useful information such as images, internet history, geolocation, timeline, etc. It can also recover deleted files, search for patterns within the disk image, and generate detailed reports. So I'll suggest you to explore it as well.

Analyzing a Disk Image

Once you have opened the disk image on FTK Imager, you'll be able to see four sections on the window:

- Evidence Tree in the top left area, which displays the hierarchical layout of the disk image.
- Properties on the bottom left, which displays the metadata associated with the selected file, such as its name, last modify and access dates, md5 and sha1 hashes, etc.
- File List in the center towards the top, which displays the list of files and directories within the selected partition or image.
- Preview in the bottom, which displays the preview or hex contents of the selected file.

Analyzing a Disk Image

To be able to explore the file system in the disk image, we need to extend the evidence tree located in the top left area:

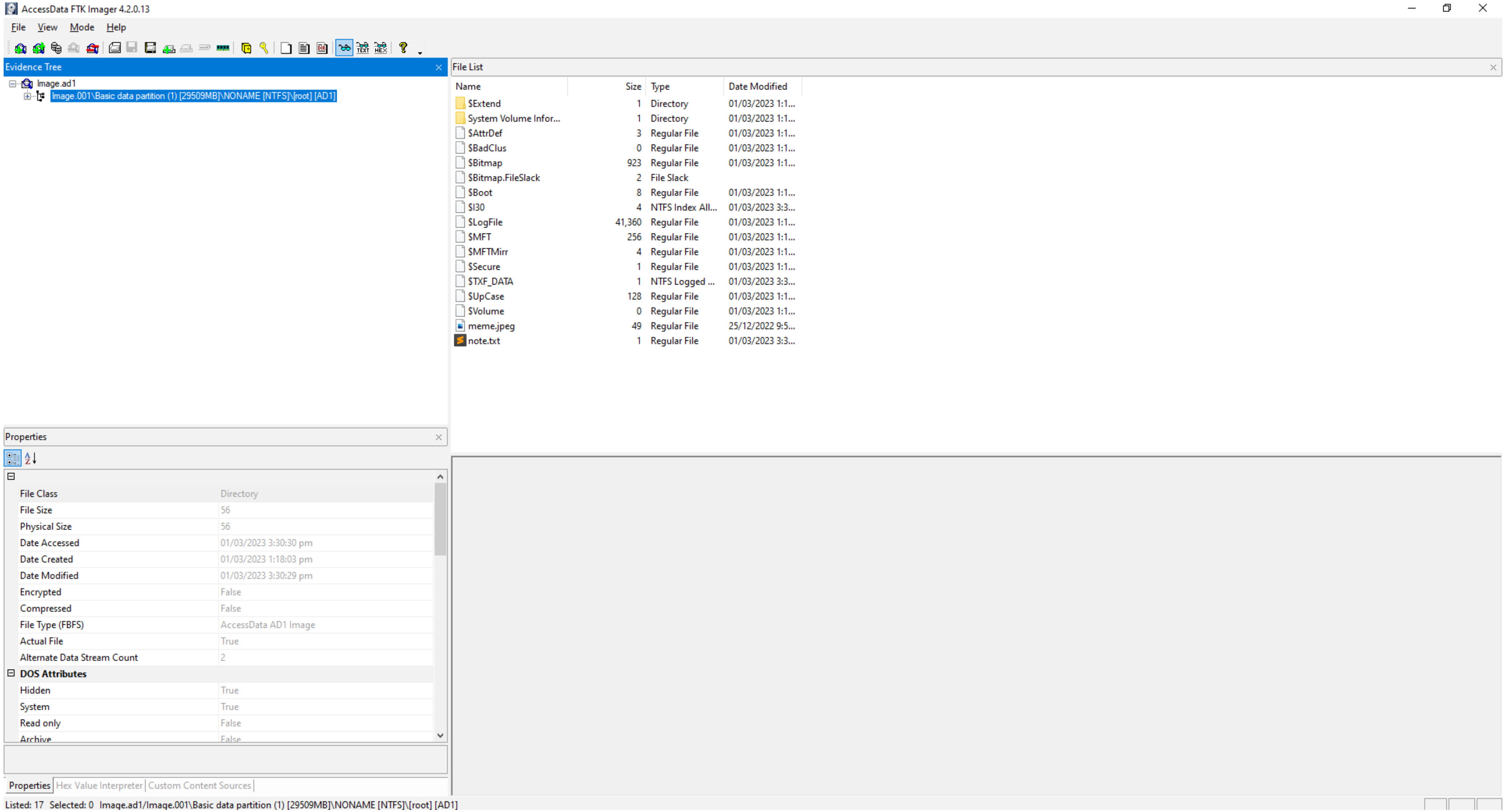


Image.ad1
Image.001\Basic data partition (1) [29509MB]\NONAME [NTFS]\[root] [AD1]

Name	Size	Type	Date Modified
$Extend	1	Directory	01/03/2023 1:1...
System Volume Infor...	1	Directory	01/03/2023 1:1...
$AttrDef	3	Regular File	01/03/2023 1:1...
$BadClus	0	Regular File	01/03/2023 1:1...
$Bitmap	923	Regular File	01/03/2023 1:1...
$Bitmap.FileSlack	2	File Slack	
$Boot	8	Regular File	01/03/2023 1:1...
$I30	4	NTFS Index All...	01/03/2023 3:3...
$LogFile	41,360	Regular File	01/03/2023 1:1...
$MFT	256	Regular File	01/03/2023 1:1...
$MFTMirr	4	Regular File	01/03/2023 1:1...
$Secure	1	Regular File	01/03/2023 1:1...
$TXF_DATA	1	NTFS Logged ...	01/03/2023 3:3...
$UpCase	128	Regular File	01/03/2023 1:1...
$Volume	0	Regular File	01/03/2023 1:1...
meme.jpeg	49	Regular File	25/12/2022 9:5...
note.txt	1	Regular File	01/03/2023 3:3...

File Class	Directory
File Size	56
Physical Size	56
Date Accessed	01/03/2023 3:30:30 pm
Date Created	01/03/2023 1:18:03 pm
Date Modified	01/03/2023 3:30:29 pm
Encrypted	False
Compressed	False
File Type (FBFS)	AccessData AD1 Image
Actual File	True
Alternate Data Stream Count	2
DOS Attributes	
Hidden	True
System	True
Read only	False
Archive	False

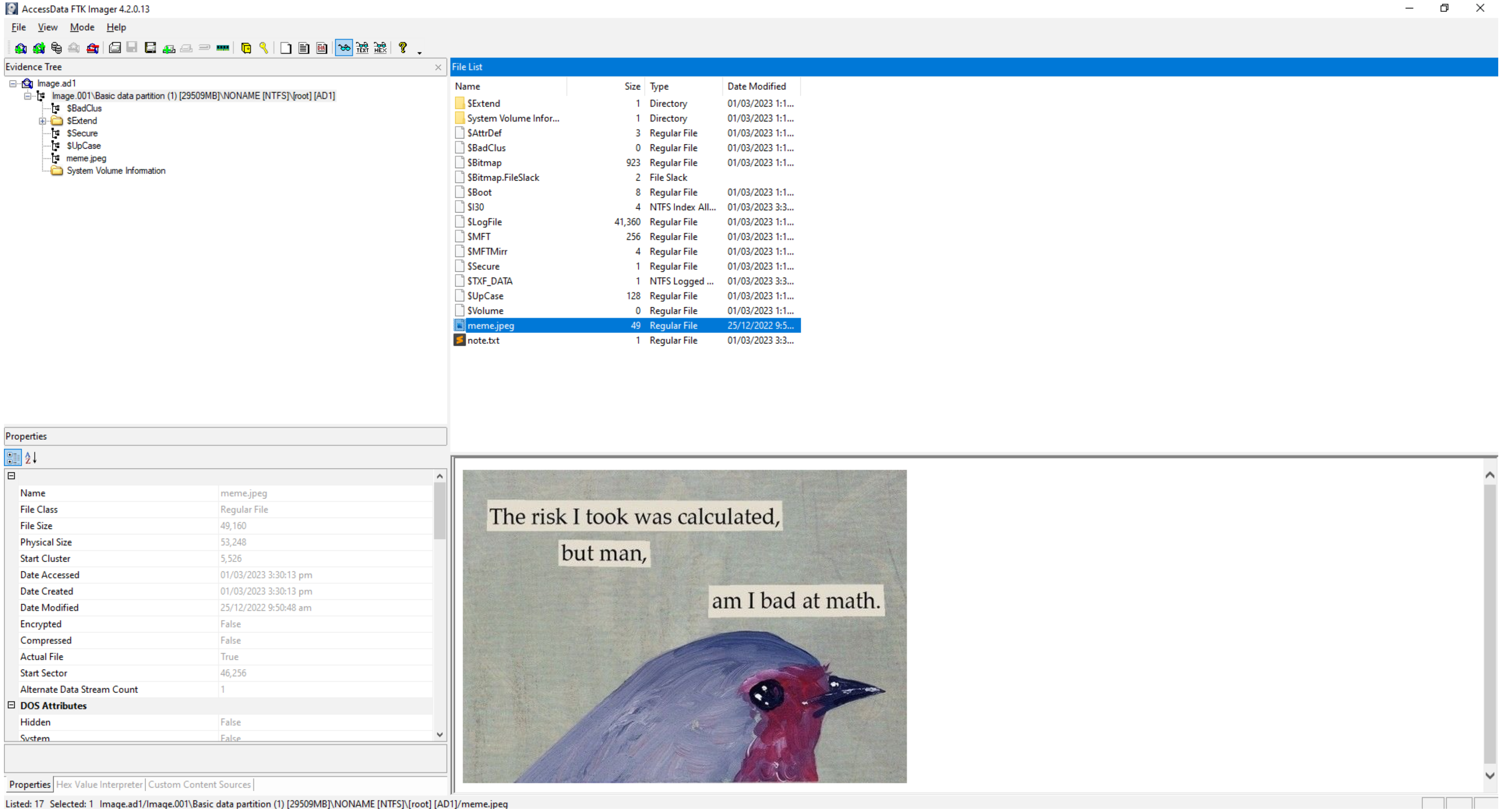
Listed: 17 Selected: 0 Image.ad1/Image.001\Basic data partition (1) [29509MB]\NONAME [NTFS]\[root] [AD1]

Dr. Darryl J D’Souza

Analyzing a Disk Image

The root directory of the imaged USB Drive is displayed, allowing us to select and view the contents of any file. For instance, we can access and view the note.txt and meme.jpeg files that were originally stored on the USB drive.

We can also extract any of the files that may be of interest by simply right-clicking on them and selecting "Export Files".



Evidence Tree:

- Image.ad1
  - Image.001\Basic data partition (1) [29509MB]\NONAME [NTFS]\[root] [AD1]
    - $BadClus
    - $Extend
    - $Secure
    - $UpCase
    - meme.jpeg
    - System Volume Information

File List:

Name	Size	Type	Date Modified
$Extend	1	Directory	01/03/2023 1:1...
System Volume Infor...	1	Directory	01/03/2023 1:1...
$AttrDef	3	Regular File	01/03/2023 1:1...
$BadClus	0	Regular File	01/03/2023 1:1...
$Bitmap	923	Regular File	01/03/2023 1:1...
$Bitmap.FileSlack	2	File Slack	
$Boot	8	Regular File	01/03/2023 1:1...
$I30	4	NTFS Index All...	01/03/2023 3:3...
$LogFile	41,360	Regular File	01/03/2023 1:1...
$MFT	256	Regular File	01/03/2023 1:1...
$MFTMirr	4	Regular File	01/03/2023 1:1...
$Secure	1	Regular File	01/03/2023 1:1...
$TXF_DATA	1	NTFS Logged ...	01/03/2023 3:3...
$UpCase	128	Regular File	01/03/2023 1:1...
$Volume	0	Regular File	01/03/2023 1:1...
meme.jpeg	49	Regular File	25/12/2022 9:5...
note.txt	1	Regular File	01/03/2023 3:3...

Properties:

Name	meme.jpeg
File Class	Regular File
File Size	49,160
Physical Size	53,248
Start Cluster	5,526
Date Accessed	01/03/2023 3:30:13 pm
Date Created	01/03/2023 3:30:13 pm
Date Modified	25/12/2022 9:50:48 am
Encrypted	False
Compressed	False
Actual File	True
Start Sector	46,256
Alternate Data Stream Count	1
DOS Attributes	
Hidden	False
System	False

Listed: 17 Selected: 1 Image.ad1/Image.001\Basic data partition (1) [29509MB]\NONAME [NTFS]\[root] [AD1]/meme.jpeg

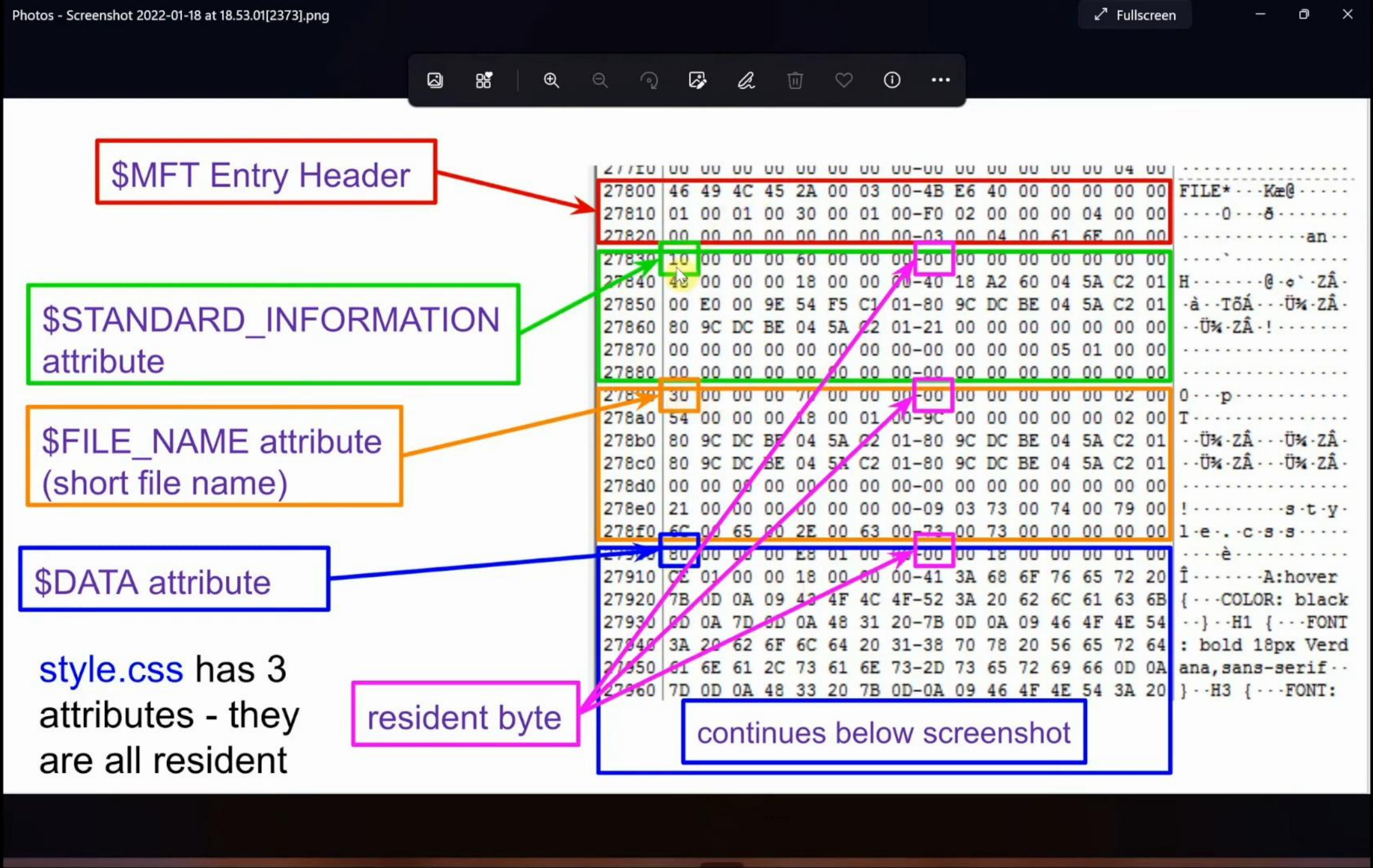
Analyzing a Disk Image

Some essential files in disk images

- **$MFT** — The Master File Table is an important file in NTFS file systems that stores information about all files and directories on a volume, including their names, permissions, and attributes. It also contains information about the location of each file on the disk.
- **$MFTMirr** — This file stands for MFT Mirror and serves as a backup of the $MFT, and is crucial in case the original $MFT becomes corrupted.
- **$LogFile** — This file records transaction journal information of metadata (MFT area), and can be used to recover from system crashes.

For analyzing these files, there are several tools available such as analyzeMFT,
or MFTECmd available for download at https://ericzimmerman.github.io/#!index.md.

💡 There may be a lot more files that may be present in a disk image like $Boot, $Secure, $Volume, etc. However, I encourage you to explore these on your own as part of your learning process.



$MFT Entry Header

$STANDARD_INFORMATION attribute

$FILE_NAME attribute (short file name)

$DATA attribute

style.css has 3 attributes - they are all resident

resident byte

```
277f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 04 00 ················
27800 46 49 4C 45 2A 00 03 00-4B E6 40 00 00 00 00 00 FILE*···Kæ@·····
27810 01 00 01 00 30 00 01 00-F0 02 00 00 00 04 00 00 ····0···ð·······
27820 00 00 00 00 00 00 00 00-03 00 04 00 61 6E 00 00 ············an··
27830 10 00 00 00 60 00 00 00-00 00 00 00 00 00 00 00 ····`···········
27840 48 00 00 00 18 00 00 00-40 18 A2 60 04 5A C2 01 H·······@·¢`·ZÂ·
27850 00 E0 00 9E 54 F5 C1 01-80 9C DC BE 04 5A C2 01 ·à··TõÁ···Ü¾·ZÂ·
27860 80 9C DC BE 04 5A C2 01-21 00 00 00 00 00 00 00 ··Ü¾·ZÂ·!·······
27870 00 00 00 00 00 00 00 00-00 00 00 00 05 01 00 00 ················
27880 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
27890 30 00 00 00 70 00 00 00-00 00 00 00 00 00 02 00 0···p···········
278a0 54 00 00 00 18 00 01 00-9C 00 00 00 00 00 02 00 T···············
278b0 80 9C DC BE 04 5A C2 01-80 9C DC BE 04 5A C2 01 ··Ü¾·ZÂ···Ü¾·ZÂ·
278c0 80 9C DC BE 04 5A C2 01-80 9C DC BE 04 5A C2 01 ··Ü¾·ZÂ···Ü¾·ZÂ·
278d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
278e0 21 00 00 00 00 00 00 00-09 03 73 00 74 00 79 00 !·········s·t·y·
278f0 6C 00 65 00 2E 00 63 00-73 00 73 00 00 00 00 00 l·e·.·c·s·s·····
27900 80 00 00 00 E8 01 00 00-00 00 18 00 00 00 01 00 ····è···········
27910 CE 01 00 00 18 00 00 00-41 3A 68 6F 76 65 72 20 Î·······A:hover 
27920 7B 0D 0A 09 43 4F 4C 4F-52 3A 20 62 6C 61 63 6B {···COLOR: black
27930 0D 0A 7D 0D 0A 48 31 20-7B 0D 0A 09 46 4F 4E 54 ··}··H1 {···FONT
27940 3A 20 62 6F 6C 64 20 31-38 70 78 20 56 65 72 64 : bold 18px Verd
27950 61 6E 61 2C 73 61 6E 73-2D 73 65 72 69 66 0D 0A ana,sans-serif··
27960 7D 0D 0A 48 33 20 7B 0D-0A 09 46 4F 4E 54 3A 20 }··H3 {···FONT: 
```

continues below screenshot

Conclusion

In this lab, we covered some basic terminology, then moved on to learning how to acquire a disk image. After that, we explored some commonly found files in a disk image and even did a basic analysis using FTK Imager. However, it's important to keep in mind that the disk image we analyzed was a small USB drive and there is much more to analyze in a larger hard drive disk image. This may require looking for common artifacts, such as the Windows Registry, Browser History, Event Logs, Console History, and anything which may provide valuable insights for the investigation.

Exercises

Utilize the disk image Image.ad1 from Lab 7 files folder to answer the following questions:

1. What are the MD5 and SHA1 hashes of the note.txt file?
2. What's the MFT record number of the note.txt file? The answer may vary depending on the method used.
3. Can you determine the parent directory of the file named $Txf? You can use either analyzeMFT or MFTECmd to inspect the contents of the $MFT file to answer this question.
4. The meme.jpeg image was originally downloaded from a twitter URL. Can you use MFTECmd to determine the original URL?
5. Can you analyze the $Boot file and determine the volume serial number in raw hexadecimal format?