



## Helpful Links

[FTKImager User Guide](#)

### I. Overview

FTK Imager is a forensic imaging and analysis tool designed to acquire, create forensic images, and perform detailed analysis of various types of digital media

#### Types of disc files it produces

- Raw
- Encase
- Smart
- AFF

### II. Acquiring a disc image

- Step by step setup
- Proper configuration

### III. Use Cases/ Applications and scenarios

- Output generated
- Useful artifacts

### V. Forensic walkthroughs and examples

FTK Imager is a digital forensics software tool developed by AccessData. It is used primarily to acquire and analyze disk images and is highly regarded in the field of computer forensics for its robust imaging capabilities

What is a disc image? A forensic disk image encompasses everything on the drive—not just visible data files but also the file system metadata (like file allocation tables), slack space, and unallocated (or "free") space. This unallocated space can contain deleted files and fragments of data that are not visible to the user but can be crucial in an investigation

Disk image files can come in various formats, each with its own file extension. These formats might vary based on the tools used to create the images and their intended use. Here are some of the common file extensions for disk images, particularly in the context of digital forensics and general IT:

1. **ISO (.iso):** This is a popular format for optical disk images and can also be used for creating images of hard drives. It is commonly used to distribute large software and game installations.
2. **Raw Image (.img or .raw):** This format is a sector-by-sector copy of a disk and does not contain any metadata about the filesystem or the structure of the disk. It's very flexible and widely supported.
3. **Advanced Forensics Format (.aff):** AFF is an open and extensible format that includes not only the disk data but also associated metadata and optional compression. It's specifically designed for use in forensics.
4. **AccessData FTK Imager (.ad1):** This format is used by AccessData's FTK Imager, a popular forensic tool. It supports metadata and is optimized for forensic tasks.
5. **Encase Image File Format (.e01):** This is a proprietary format developed by Guidance Software for its EnCase forensic software. It includes compression and integrity checks and is widely used in professional forensics.
6. **Apple Disk Image (.dmg):** Commonly used on macOS systems, DMG files are used for distributing software and for backups and can be mounted as a drive within the OS.
7. **Virtual Hard Disk (.vhd and .vhdx):** Used by virtualization software like Microsoft's Hyper-V, these formats are used for virtual machine disks but can also be used for imaging real disks.
8. **VMware Virtual Disk (.vmdk):** Commonly used by VMware virtualization software, this format is used for virtual machine disks and can be useful for forensic investigations of virtual environments.

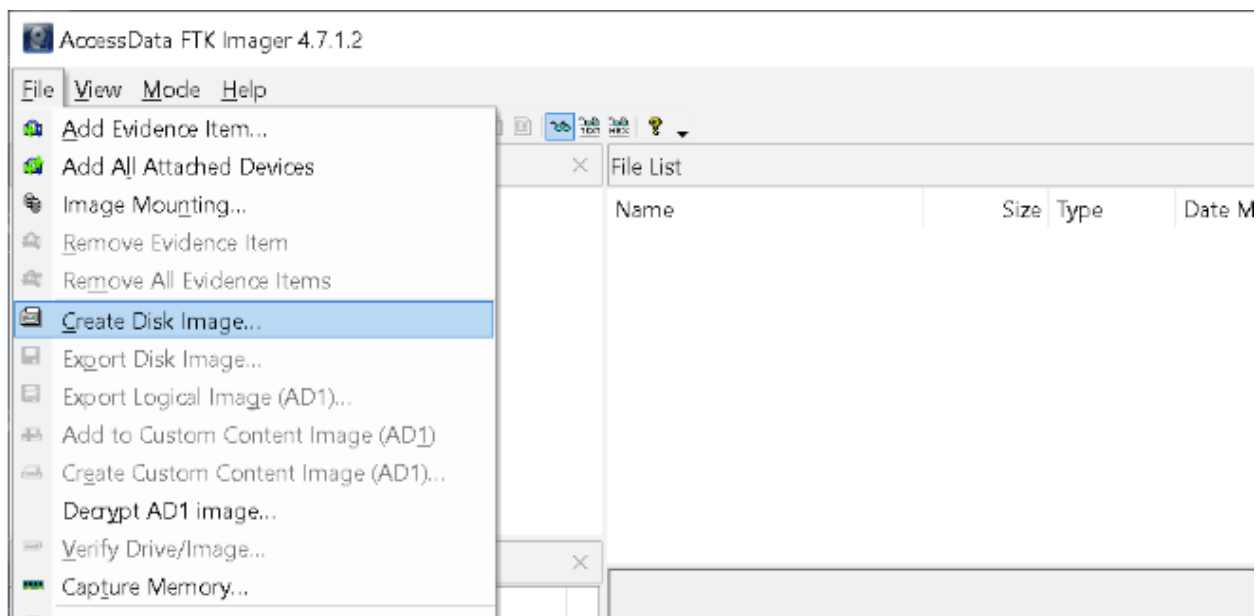
## II. Acquiring disk image

Acquiring Digital Artifacts and Evidence.

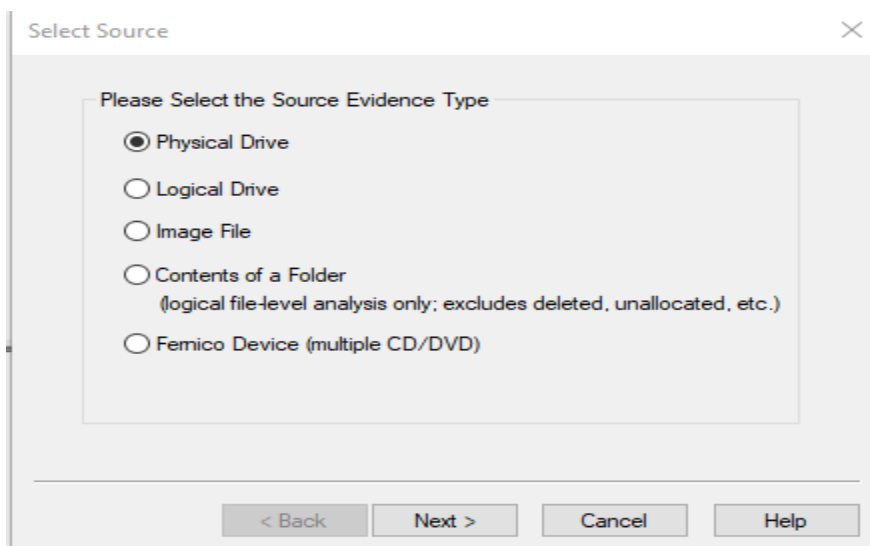
Download: <https://www.exterro.com/ftk-product-downloads/ftk-imager-version-4-7-1>

Lets create a disk image to examine. Note: created disk image should be output on a different drive. Either another hard drive, USB, shared drive, etc. FTK doesn't like when you create the image on the same drive. In this example we're running FTK imager on the drive we want to create a disk image and outputting into the D drive.

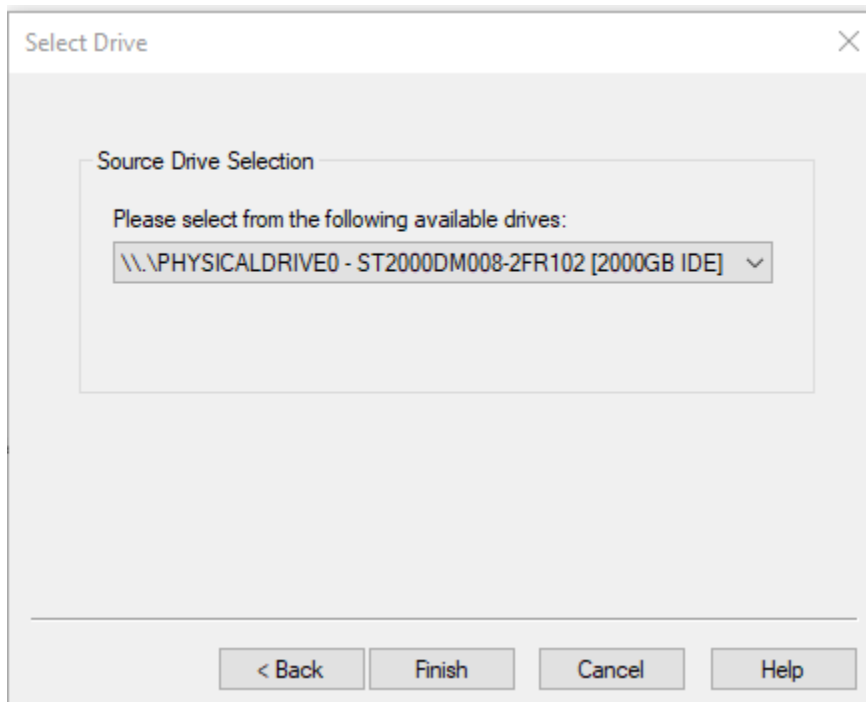
### 1. Open FTK and click "Create Disk Image"



### 2. Select Physical Drive (should work unless the drive is encrypted) and next

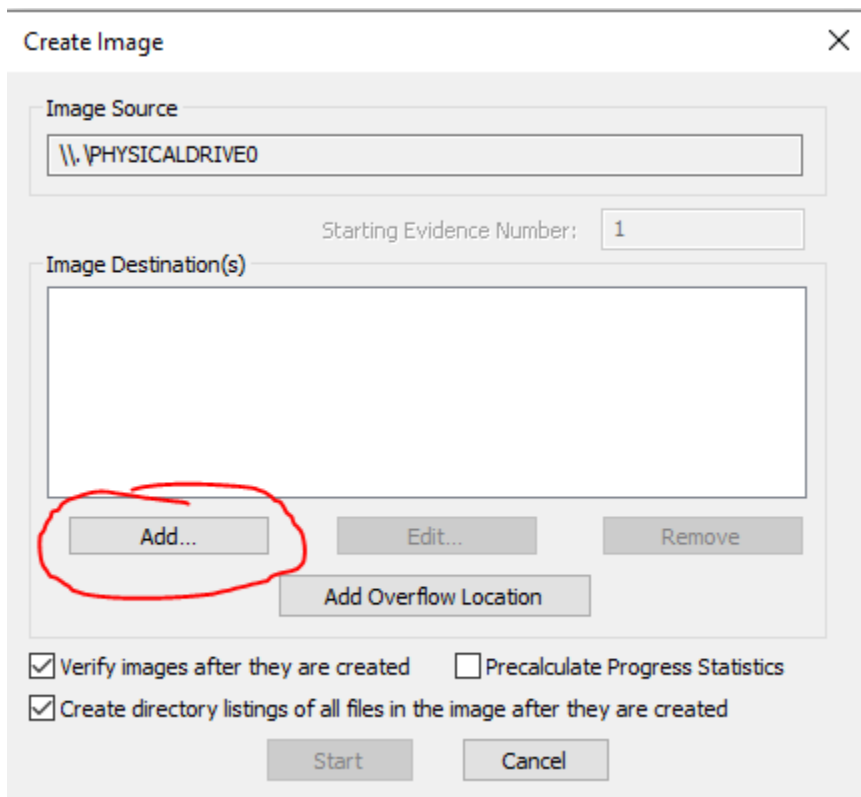


3. Select the Drive to derive the image, then “Finish”

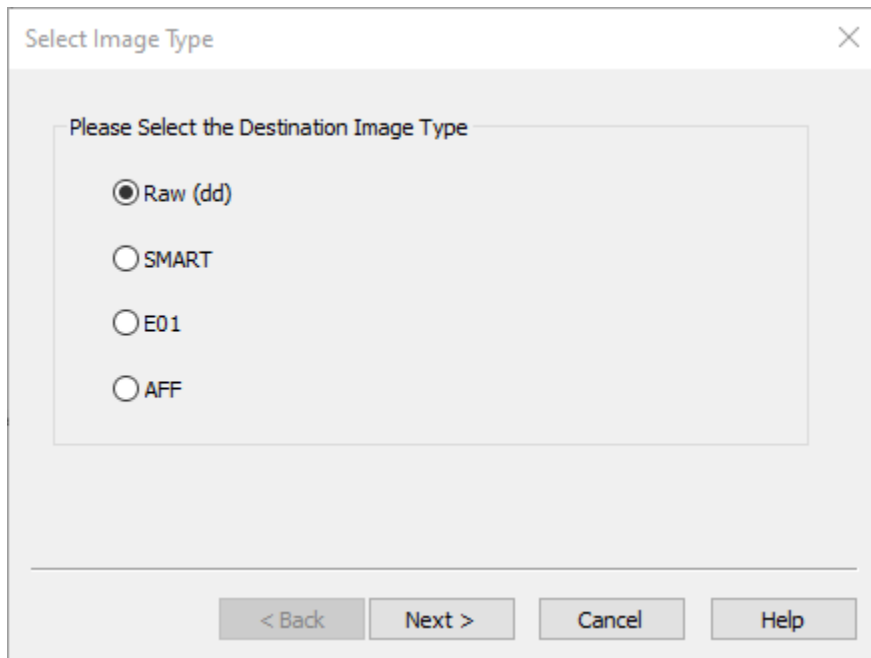


4. Select “add” the image destination (can’t be on the same drive being copied)

Also make sure the applicable boxes are checked (see image below)

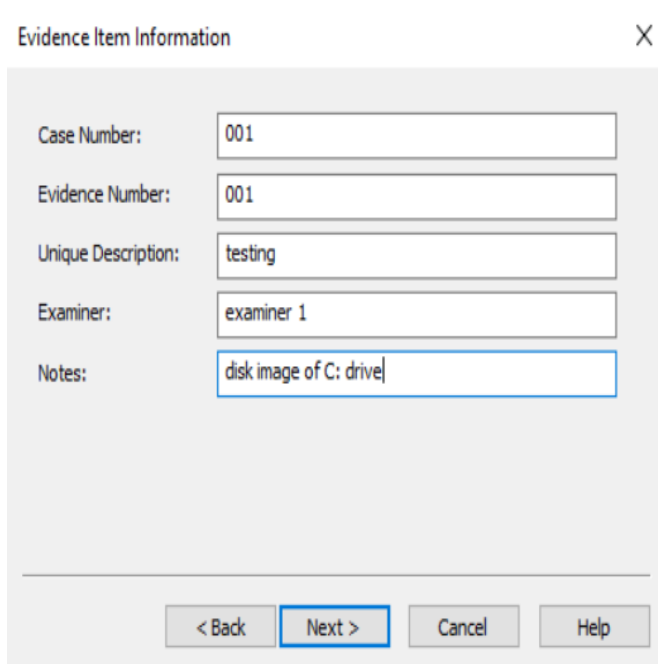


5. Choose the Image type. We'll do Raw (dd)



A dialog box titled "Select Image Type" with a close button (X) in the top right corner. Inside the dialog, there is a section titled "Please Select the Destination Image Type" containing four radio button options: "Raw (dd)" (which is selected), "SMART", "E01", and "AFF". At the bottom of the dialog, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

6. Fill in applicable case information



A dialog box titled "Evidence Item Information" with a close button (X) in the top right corner. It contains five text input fields with the following labels and values: "Case Number:" (001), "Evidence Number:" (001), "Unique Description:" (testing), "Examiner:" (examiner 1), and "Notes:" (disk image of C: drive). At the bottom, there are four buttons: "< Back", "Next >" (which is highlighted with a blue border), "Cancel", and "Help".

7. select image destination folder and file name (remember output to a different drive). Note: The "Image Fragment Size" if you input 0 it will assemble in one file, however this file will equal the size of the physical disk. Segmenting it will create many different files that FTK will know how to reassemble. We will try doing 1500 MB fragments (it was set as default). Click "Finish" after the configurations are set

Select Image Destination

Image Destination Folder  
E:\cases\001\images Browse

Image Filename (Excluding Extension)  
disc\_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 ☐

< Back Finish Cancel Help

8. Click start

Create Image

Image Source  
\\.\PHYSICALDRIVE0

Starting Evidence Number: 1

Image Destination(s)  
E:\cases\001\images\disc\_image [raw/dd]

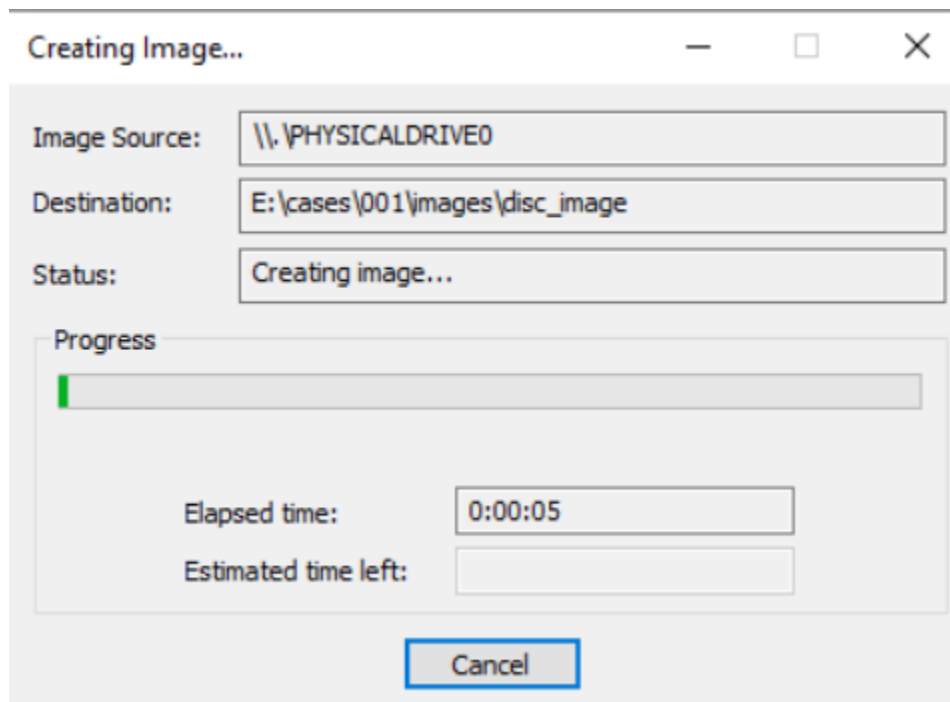
Add... Edit... Remove

Add Overflow Location

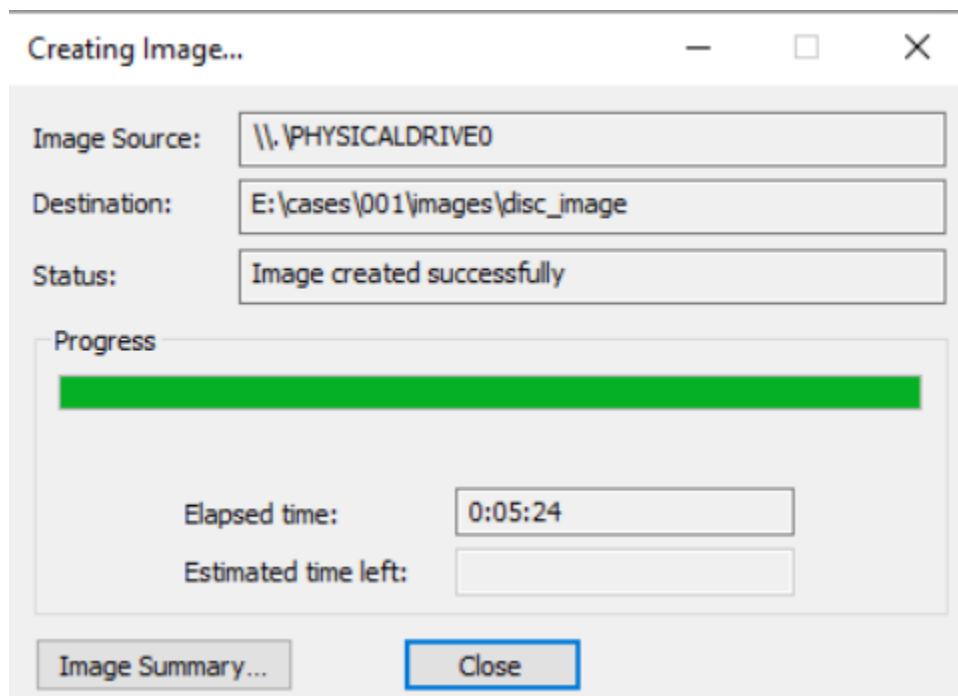
☒ Verify images after they are created ☐ Precalculate Progress Statistics  
☒ Create directory listings of all files in the image after they are created

Start Cancel

9. Wait, while the image is being created (may take some time depending on the size of the drive)



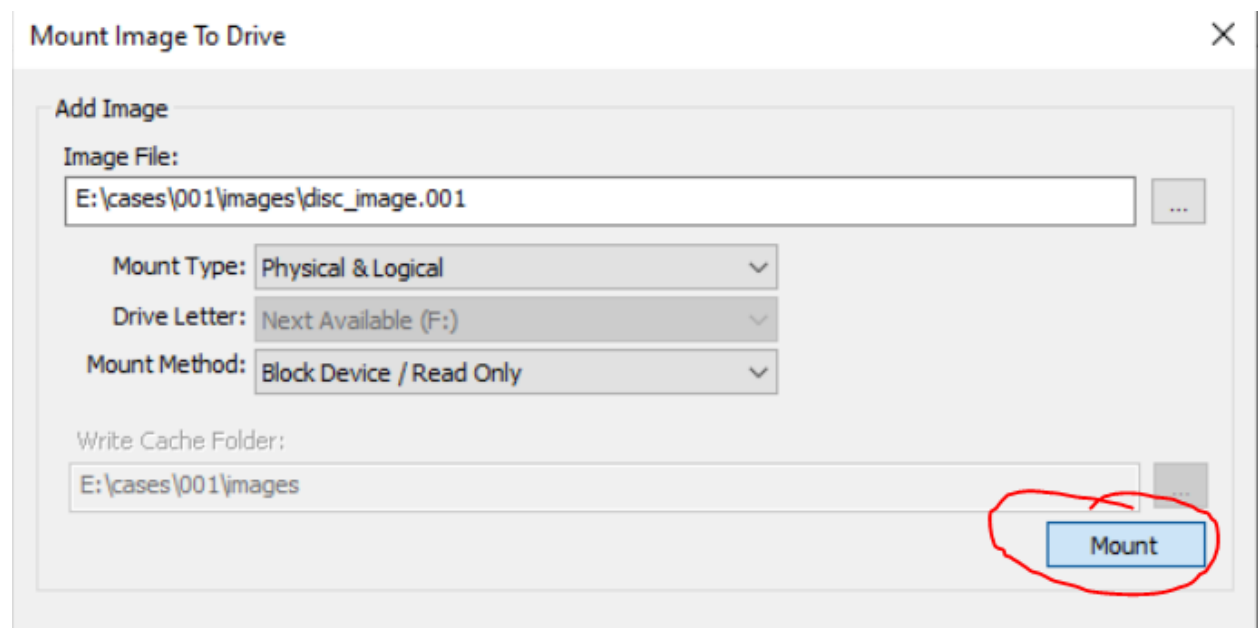
10. When it is complete, select close



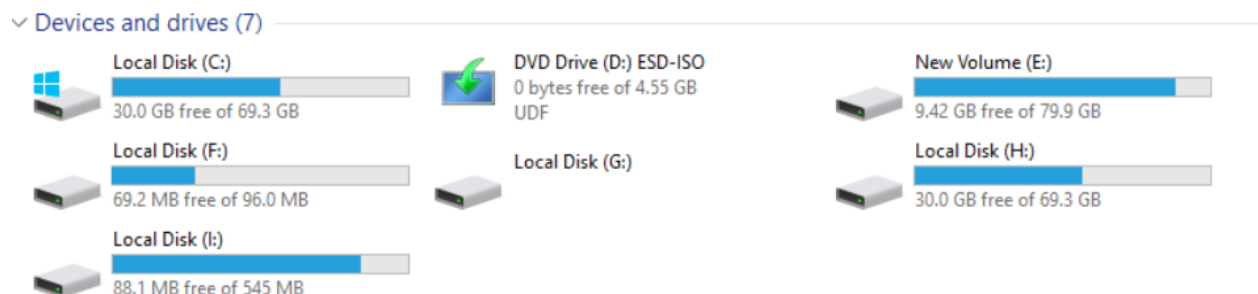
11. Now lets check out the results in the E: drive. Note the segmented drive, split in 1500 MB segments

is PC > New Volume (E:) > cases > 001 > images					Search images
Name	Date modified	Type	Size		
disc_image.001	5/29/2024 9:17 PM	001 File	1,536,000 KB		
disc_image.001.csv	5/29/2024 9:28 PM	Comma Separate...	489,788 KB		
disc_image.001.txt	5/29/2024 9:31 PM	Text Document	4 KB		
disc_image.002	5/29/2024 9:17 PM	002 File	1,536,000 KB		
disc_image.003	5/29/2024 9:17 PM	003 File	1,536,000 KB		
disc_image.004	5/29/2024 9:17 PM	004 File	1,536,000 KB		
disc_image.005	5/29/2024 9:17 PM	005 File	1,536,000 KB		
disc_image.006	5/29/2024 9:17 PM	006 File	1,536,000 KB		

12. Lets reassemble this back in FTK imager. Go back to FTK imager, we need to mount the drive to view it in FTK. Go to File → “Image Mounting”. Choose our “disc\_image.001”, the first file as the image to add. FTK will know to go into this directory and reassemble the disk image. Click “Mount”



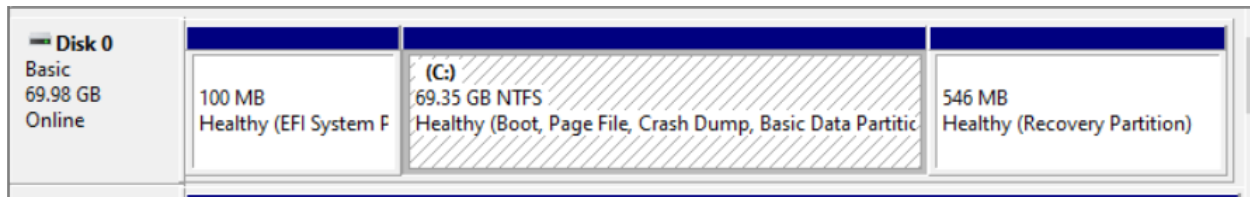
13. Now it gets a little confusing. Go to “This PC” and check out the mounted drives



The H:/ drive is our disc image mounted (It is a copy of the original C:\ drive NTFS)

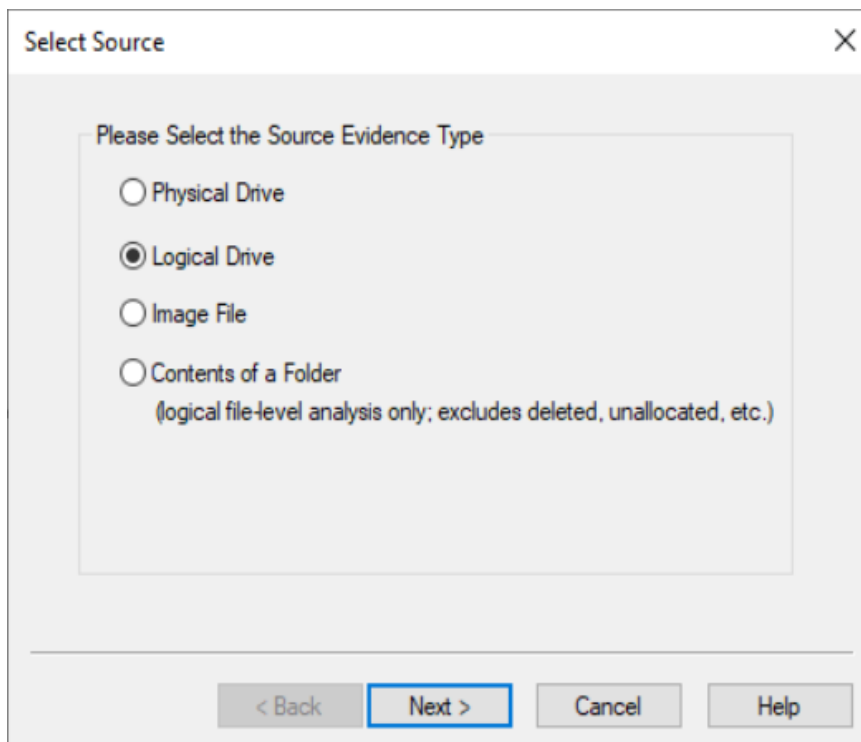


This happens because in the original “physical drive” we imaged, the drive contained 3 “logical” partitions inside it. Hence, all the extra drives that were mounted.

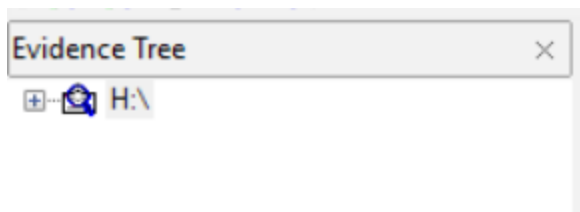
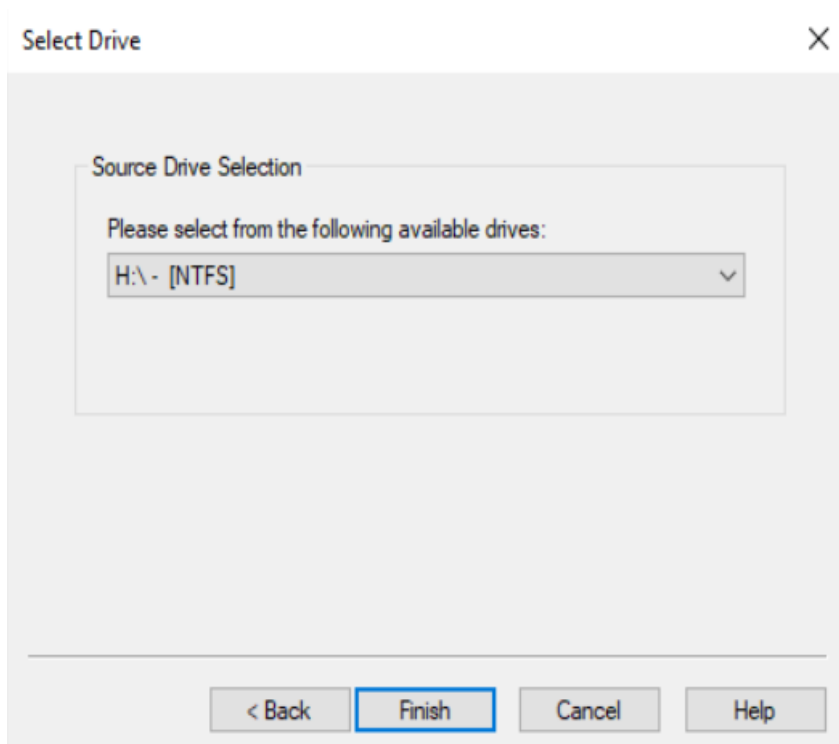


Anyway, the drive we are looking at in this instance is the H: drive, it is the forensic disk image of the C: drive. Notice how they all have the same byte size.

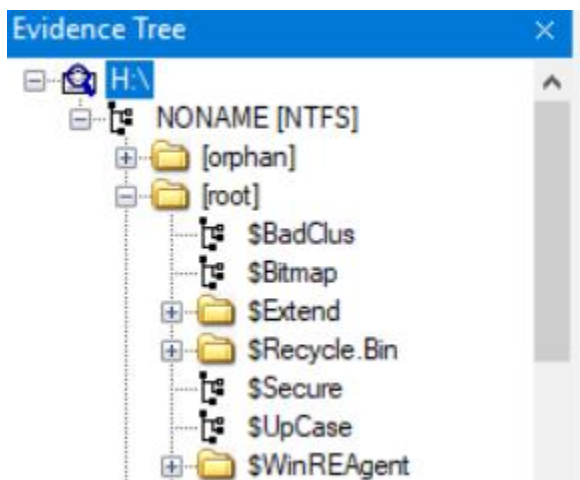
14. Go back to FTK, select File → “Add Evidence Item” then “Logical Drive”



15. Select our H: drive (in this scenario). Notice an H:\ drive appears in our evidence tree

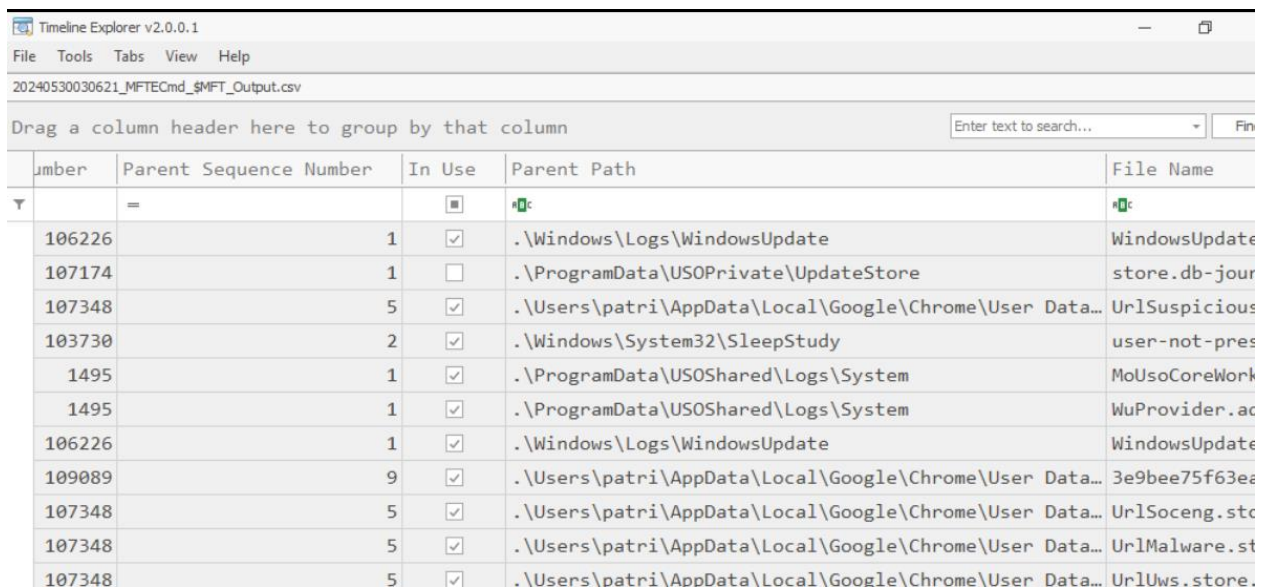


16. Drill down until you get to the root folder



```
C:\Users\patri\OneDrive\Desktop\net6>MFTECmd.exe -f c:\Users\patri\OneDrive\Desktop\MFT --csv C:\Users\patri\OneDrive\Desktop
```

4. We have the parsed csv, lets open it with timeline explorer



Timeline Explorer v2.0.0.1

File Tools Tabs View Help

20240530030621\_MFTECmd\_sMFT\_Output.csv

Drag a column header here to group by that column

Enter text to search... Fin

umber	Parent Sequence Number	In Use	Parent Path	File Name
106226	1	<input checked="" type="checkbox"/>	.\Windows\Logs\WindowsUpdate	WindowsUpdate
107174	1	<input type="checkbox"/>	.\ProgramData\USOPrivate\UpdateStore	store.db-jour
107348	5	<input checked="" type="checkbox"/>	.\Users\patri\AppData\Local\Google\Chrome\User Data...	UrlSuspicious
103730	2	<input checked="" type="checkbox"/>	.\Windows\System32\SleepStudy	user-not-pres
1495	1	<input checked="" type="checkbox"/>	.\ProgramData\USOShared\Logs\System	MoUsoCoreWork
1495	1	<input checked="" type="checkbox"/>	.\ProgramData\USOShared\Logs\System	WuProvider.ac
106226	1	<input checked="" type="checkbox"/>	.\Windows\Logs\WindowsUpdate	WindowsUpdate
109089	9	<input checked="" type="checkbox"/>	.\Users\patri\AppData\Local\Google\Chrome\User Data...	3e9bee75f63e2
107348	5	<input checked="" type="checkbox"/>	.\Users\patri\AppData\Local\Google\Chrome\User Data...	UrlSoceng.stc
107348	5	<input checked="" type="checkbox"/>	.\Users\patri\AppData\Local\Google\Chrome\User Data...	UrlMalware.st
107348	5	<input checked="" type="checkbox"/>	.\Users\patri\AppData\Local\Google\Chrome\User Data...	UrlUws.store.

The parsed MFT is a powerful forensic tool to timeline what happened on a host.

## One More Forensic example

Lets pull the chrome history file

1. Go to the FTK evidence tree and navigate to

C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\History

Grab the History File

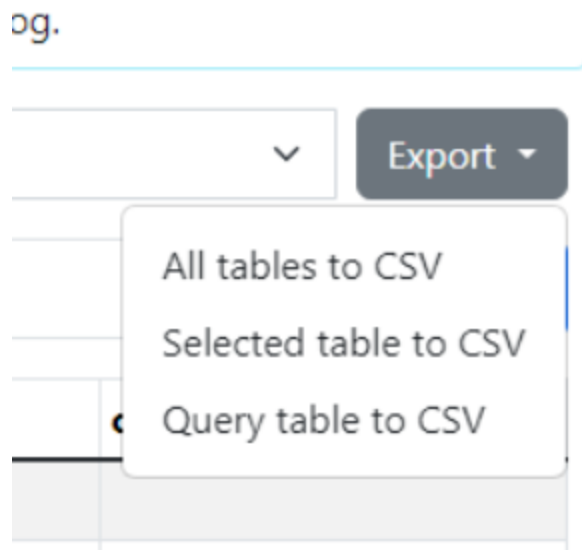
heavy_ad_intervention_opt_out.db-journal	0	Regular File	5/29/2024 8:09:33 PM
History	256	Regular File	5/29/2024 11:13:55 PM
History-journal	9	Regular File	5/29/2024 11:14:47 PM
History-journal.FileSlack	56	File Slack	
History.FileSlack	20	File Slack	

Right click history and export the file. (I'm just sending it to my desktop)

Go to <https://inloop.github.io/sqlite-viewer/>

And drop the history file (it's not an upload)

2. Select Export → all tables to CSV



3. extract the zip and open any of the CSVs (I'll use timeline explorer to do this)

downloads.csv	5/29/2024 10:28 PM	Comma Separat
downloads_slices.csv	5/29/2024 10:28 PM	Comma Separat
downloads_url_chains.csv	5/29/2024 10:28 PM	Comma Separat
history_sync_metadata.csv	5/29/2024 10:28 PM	Comma Separat
keyword_search_terms.csv	5/29/2024 10:28 PM	Comma Separat
meta.csv	5/29/2024 10:28 PM	Comma Separat
segment_usage.csv	5/29/2024 10:28 PM	Comma Separat
segments.csv	5/29/2024 10:28 PM	Comma Separat
sqlite_sequence.csv	5/29/2024 10:28 PM	Comma Separat
urls.csv	5/29/2024 10:28 PM	Comma Separat
visit_source.csv	5/29/2024 10:28 PM	Comma Separat
visited_links.csv	5/29/2024 10:28 PM	Comma Separat
visits.csv	5/29/2024 10:28 PM	Comma Separat

4. The “downloads” and “urls” tables are useful in seeing the browsing history of the user and what they downloaded. I'll open the URL csv.

urls.csv

Drag a column header here to group by that column

Line	Tag	id	url
1	<input type="checkbox"/>	1	http://google.com/
2	<input type="checkbox"/>	2	https://google.com/
3	<input type="checkbox"/>	3	https://www.google.com/
4	<input type="checkbox"/>	4	https://www.google.com/search?q=ftk+imager+download&sca_esv=13134d05f9161faa&source=hp&ei=g4
5	<input type="checkbox"/>	5	https://www.exterro.com/ftk-product-downloads/ftk-imager-version-4-7-1
6	<input type="checkbox"/>	6	http://accessdata.com/support/adownloads
7	<input type="checkbox"/>	7	https://www.exterro.com/
8	<input type="checkbox"/>	8	https://go.exterro.com/l/43312/2023-05-03/fc4b78
9	<input type="checkbox"/>	9	https://www.exterro.com/top-10-most-underrated-ftk-features-2
10	<input type="checkbox"/>	10	https://www.exterro.com/resources/white-papers/top-10-most-underrated-ftk-features
11	<input type="checkbox"/>	11	https://www.google.com/search?q=ftk+imager+download&rlz=1C1GCEA_enUS1112US1112&oq=ft&gs_lcrp
12	<input type="checkbox"/>	12	file:///C:/Tools/CyberChef/CyberChef_v10.18.3.html
13	<input type="checkbox"/>	13	https://www.google.com/search?q=sqlite+viewer&sca_esv=13134d05f9161faa&source=hp&ei=J6RXZs5
14	<input type="checkbox"/>	14	https://inloop.github.io/sqlite-viewer/

You can see a list of urls that have been visited.

Lets open the downloads csv

Drag a column header here to group by that column

	current_path	target
	<input type="checkbox"/>	<input type="checkbox"/>
9d44	C:\Users\patri\Downloads\AccessData_FTK_Imager_4.7.1.exe	C:\U:
900c	C:\Users\patri\Downloads\exported_all_db.zip	C:\U:
6ac7	C:\Users\patri\Downloads\Get-ZimmermanTools.zip	C:\U:
da1b	C:\Users\patri\Downloads\dotnet-sdk-6.0.423-win-x64.exe	C:\U:
5610	C:\Users\patri\Downloads\exported_all_db (1).zip	C:\U:

You can see me download FTK\_Imager\_4.7.1.exe!