

**FORGE
INSTITUTE**

FORGE INSTITUTE
ARKANSAS CYBER STRIKE TEAM TRAINING

Digital Forensics

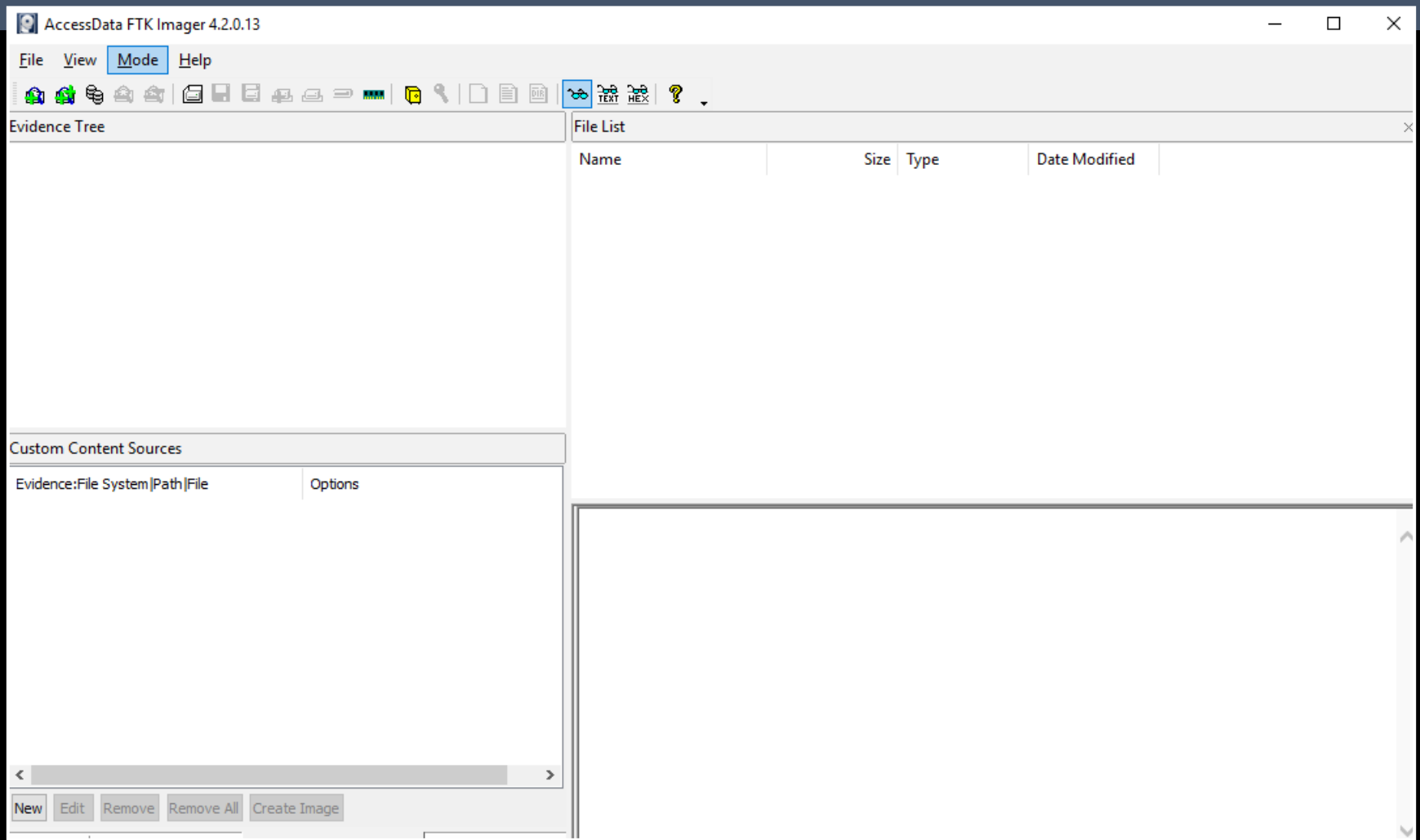


FTK Imager

Why use FTK Imager?

- Free, powerful tool
- Data preview and imaging tool
- Acquire volatile memory
- Preview image created with other tool(s)
- Verification/Forensic Hash
- Mount an image for read-only view
- Export Files and Folders
- Create Custom Content Image (AD1)
- Create Hashes and File List





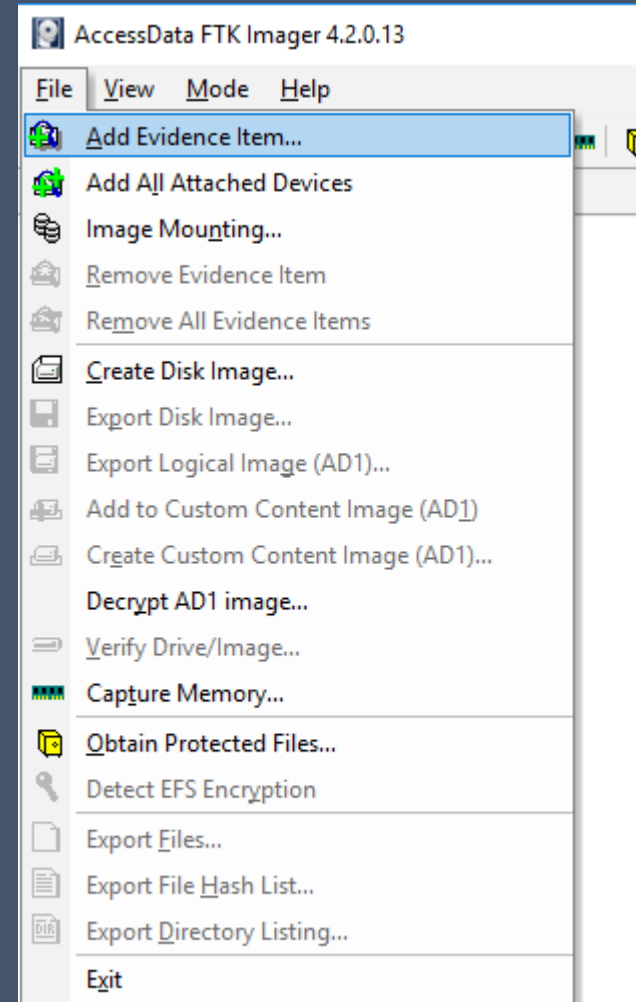
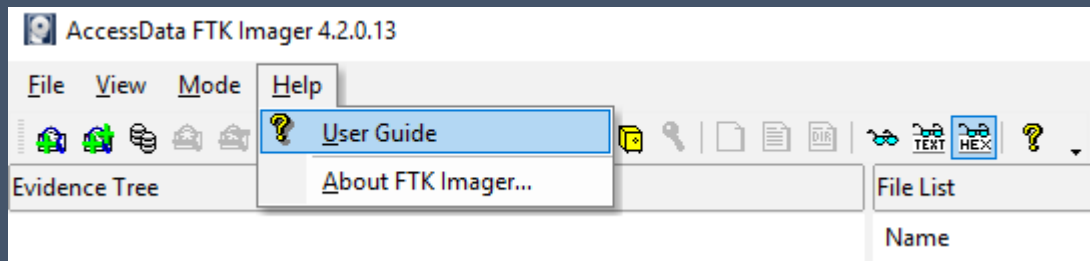
FTK Imager Interface

Options in FTK Imager

- Access options using either the File Menu or the Task Bar. Identify the icons match in both locations.

























- Access User Guide in Help tab



FTK Imager Toolbar

The toolbar contains all the tools, functions, or features, which can be accessed from the File Menu. The table below provides basic information for each feature.

	Add Evidence Item
	Add All Attached Devices
	Image Mounting. Opens the Map Image to Drive dialog.
	Remove Evidence Item
	Remove All Evidence Items
	Create Disk Image
	Export Disk Image
	Export Logical Image (AD1)
	Add to Custom Content Image (AD1)
	Create Custom Content Image (AD1)
	Verify Drive/Image
	Capture Memory

	MetaCarve (Deep Scan)
	Obtain Protected Files
	Detect EFS Encryption
	Export Files
	Export File Hash List
	Export Directory Listing
	Choose IE, text, or hex viewer automatically
	View files in plain text
	View files in hex format
	Open FTK Imager User Guide

Adding Evidence Item

To add an evidence item to the Evidence Tree

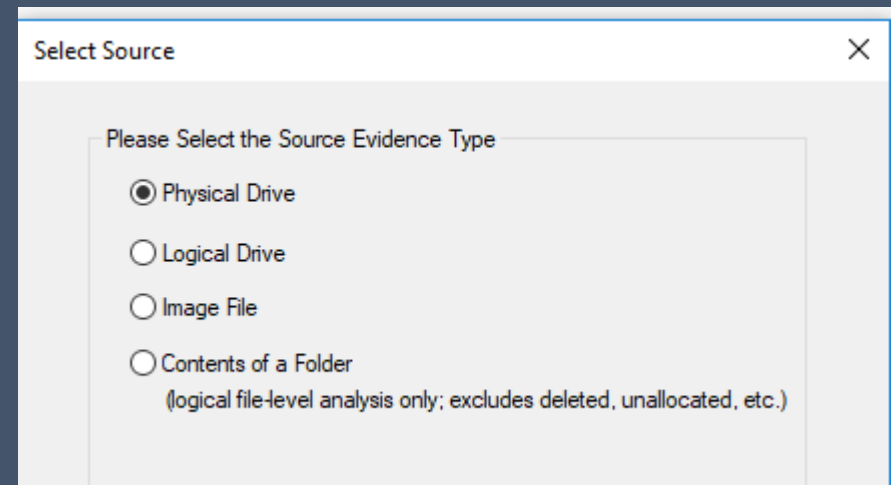
Click File>Add Evidence OR

Click the Add Evidence Item button  on the Toolbar.



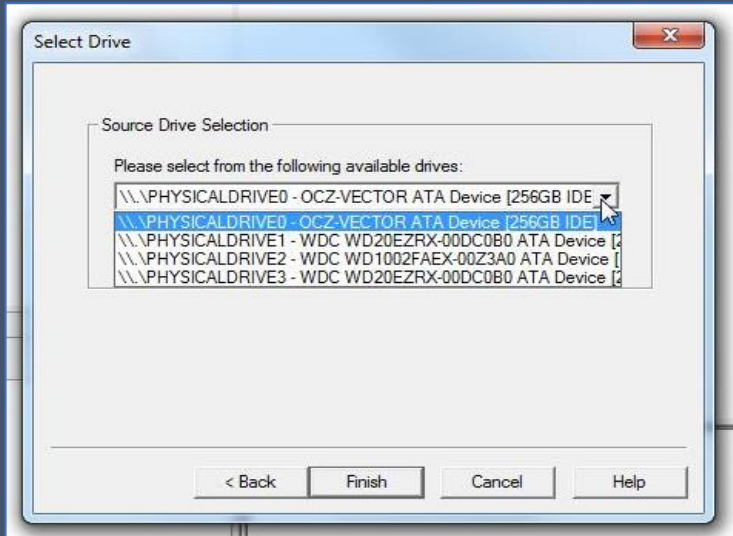
Select Source Type

- Physical Drive
- Logical Drive
- Image File
- Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)



Select Source Evidence Type

Physical Drive



Logical Drive

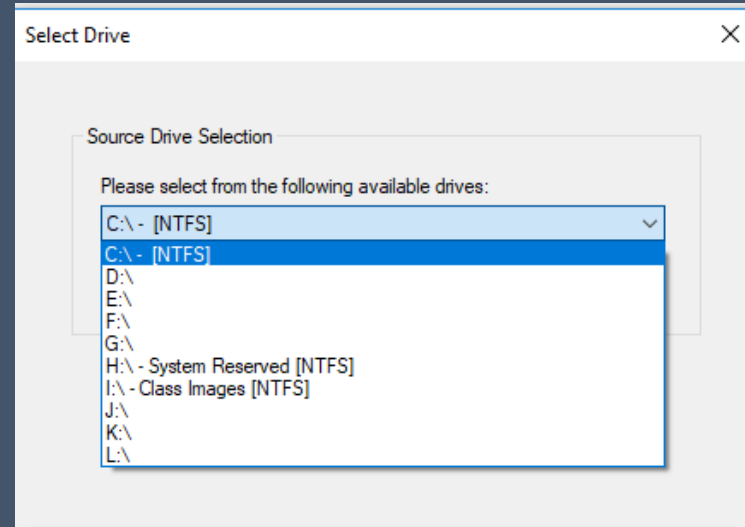
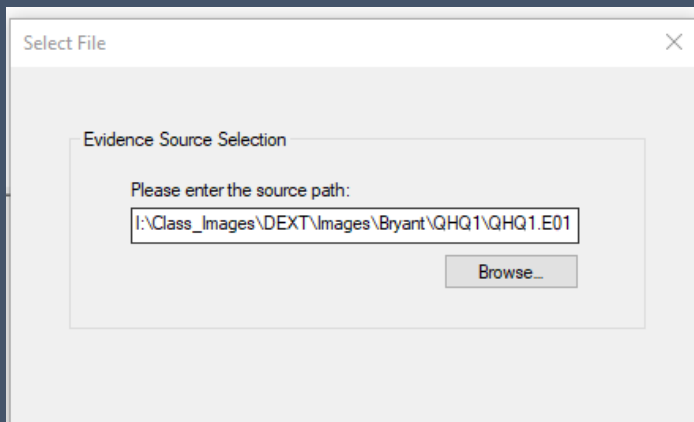
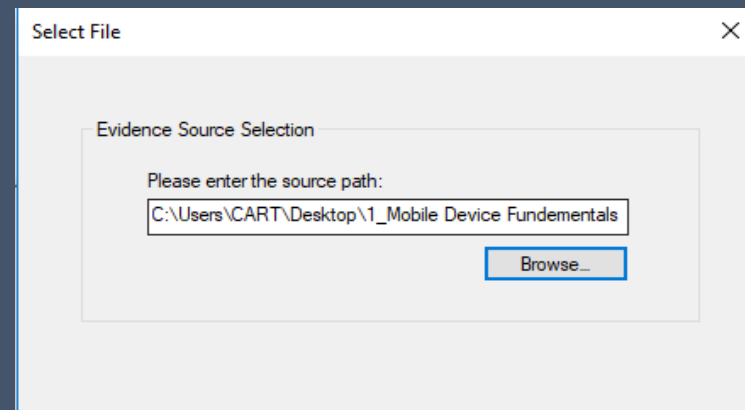


Image File

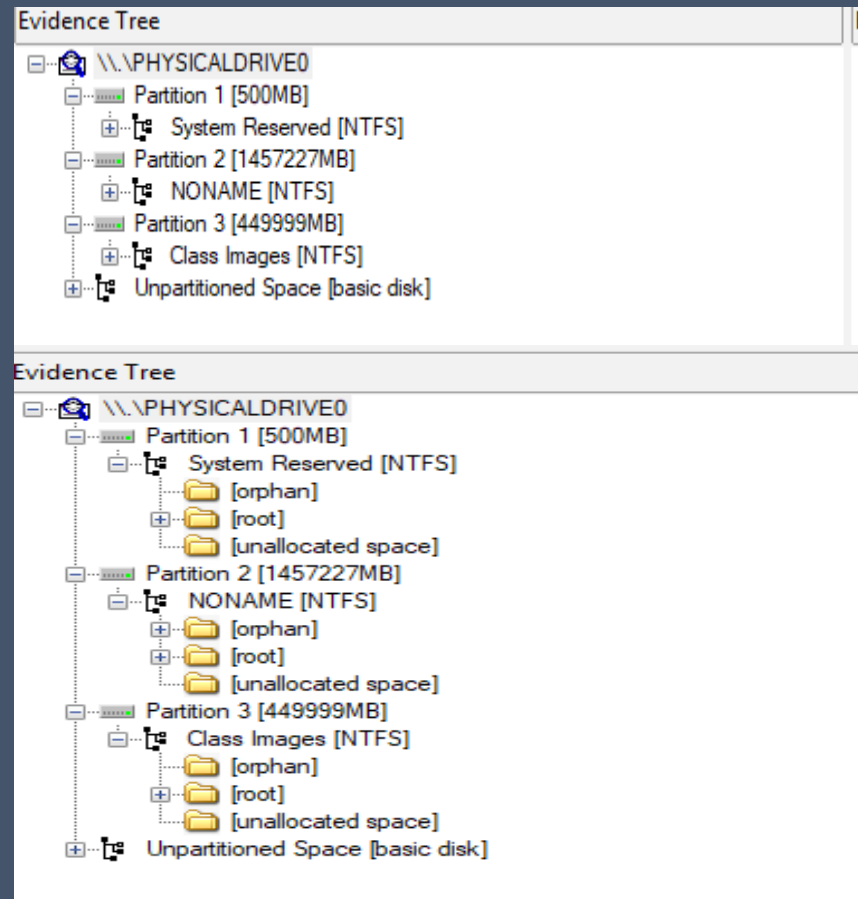
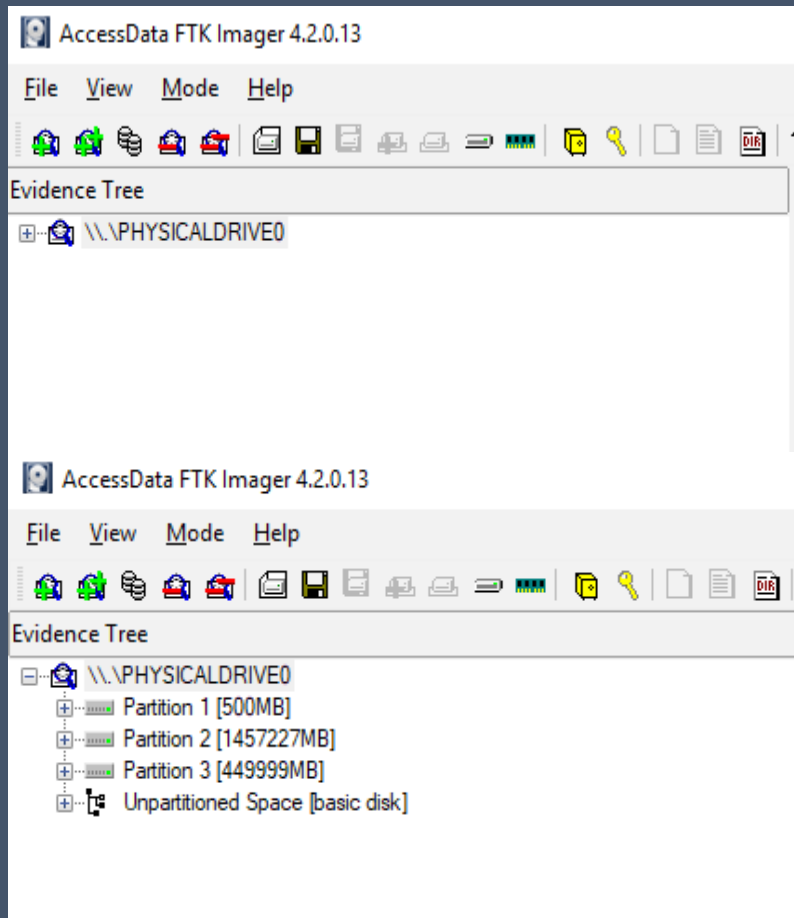


Contents of a Folder



Expand the Evidence Item

The plus sign “+” indicates the item can be expanded. In this case it unravels the drive “tree” to display catalog of data.



Imaging Evidence item

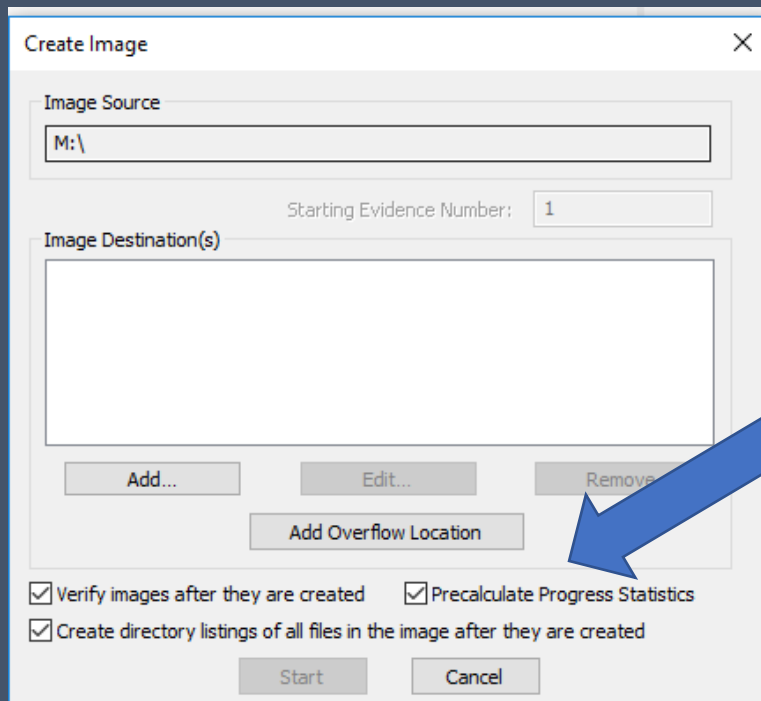
Connect evidence with WriteBlocker

Click File>Create Disk Image OR

Click the Add Evidence Item button  on the Toolbar

Select Evidence Type >choose evidence item

Select Finish



- Verify images after they are created
- Pre-calculate Progress Statistics
- Create Directory listings of all files in the image after they are created

Imaging Evidence Item

Select Image Type

Select Image Type

Please Select the Destination Image Type

Raw (dd)

SMART

E01

AFF

< Back Next > Cancel Help

Most images are created using E01 image type, however there are other options in FTK Imager.

For this class we will focus on E01 only.

*Raw(dd) and E01 most widely supported

Input Evidence Information

Evidence Item Information

Case Number:

Evidence Number:

Unique Description:

Examiner:

Notes:

< Back Next > Cancel Help

Evidence Item Information

Case Number:

Evidence Number:

Unique Description:

Examiner:

Notes:

< Back Next > Cancel Help

Imaging Evidence Item

Select Image Destination

Select Image Destination

Image Destination Folder

Image Filename (Excluding Extension)

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

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

Use AD Encryption

< Back Finish Cancel Help

Select Image Destination

Image Destination Folder

Image Filename (Excluding Extension)

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

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

Use AD Encryption

< Back Finish Cancel Help

Select
Finish

Create Image

Image Source

Starting Evidence Number:

Image Destination(s)

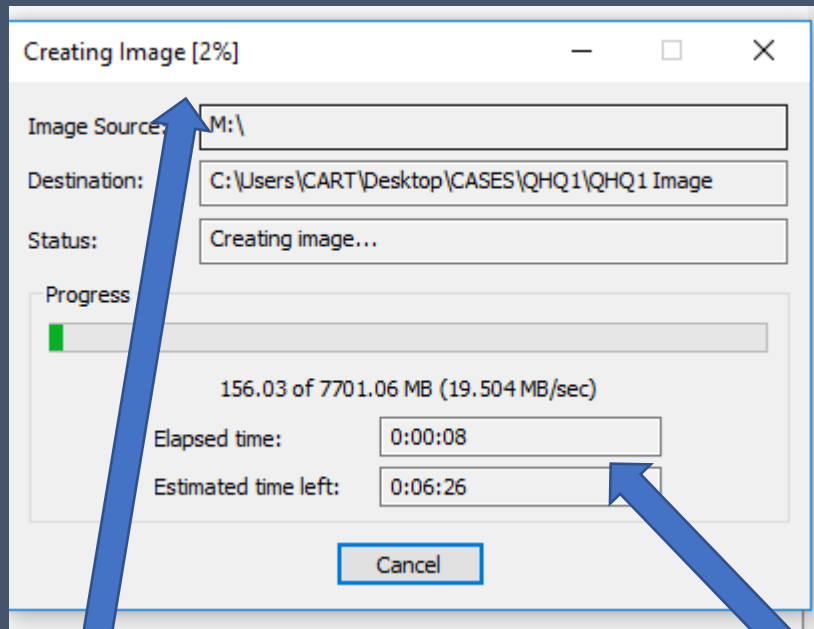
Verify images after they are created Precalculate Progress Statistics
Create directory listings of all files in the image after they are created

Start Cancel

Select
Start

Imaging Evidence Item

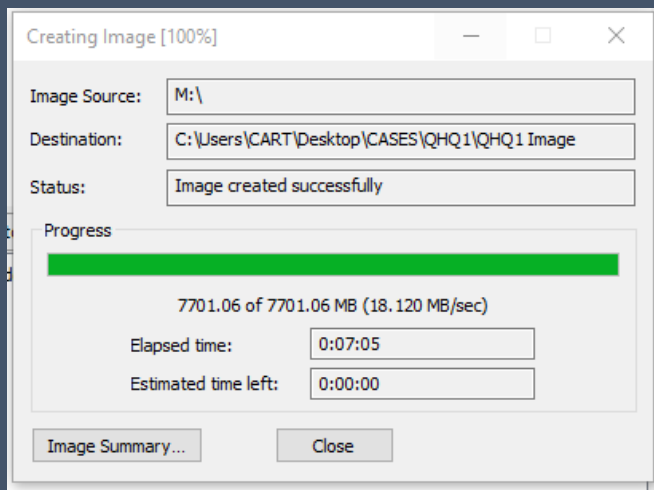
Creating Image



Pre-calculate Progress Statistics

Imaging Evidence Item

Creating Image (100%)



- Image Complete
- Drive/Image Verification Results
- Hash Match

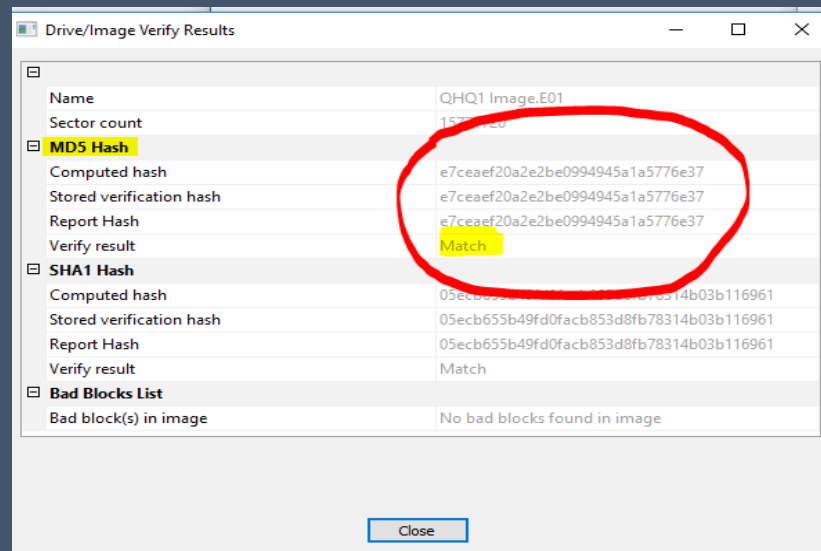
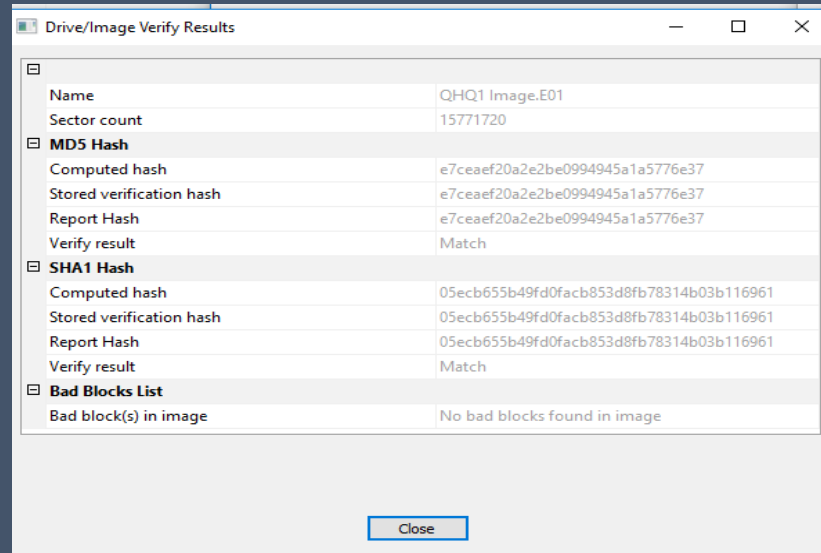
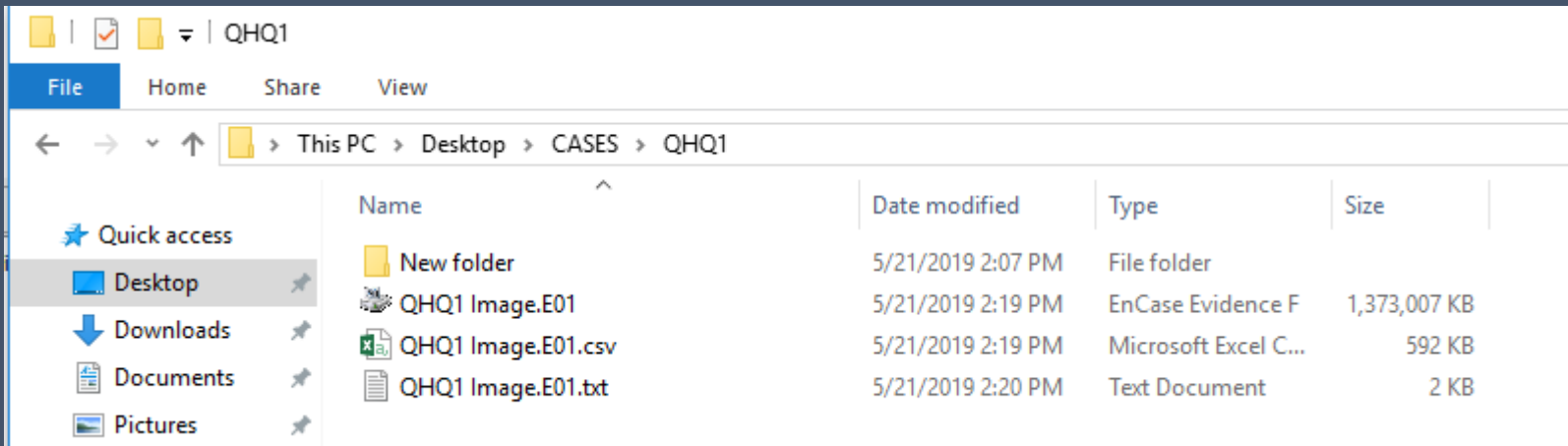


Image Verification Log



The screenshot shows a Windows File Explorer window titled 'QHQ1'. The address bar indicates the path: 'This PC > Desktop > CASES > QHQ1'. The left sidebar shows 'Quick access' with 'Desktop' selected. The main pane displays a list of files and folders with columns for Name, Date modified, Type, and Size.

Name	Date modified	Type	Size
New folder	5/21/2019 2:07 PM	File folder	
QHQ1 Image.E01	5/21/2019 2:19 PM	EnCase Evidence F	1,373,007 KB
QHQ1 Image.E01.csv	5/21/2019 2:19 PM	Microsoft Excel C...	592 KB
QHQ1 Image.E01.txt	5/21/2019 2:20 PM	Text Document	2 KB

- Locate image file created
- Open Text File (QHQ1 Image.E01.txt)

Image Verification Log

Created By AccessData® FTK® ~~Imager~~ 4.2.0.13

Case Information:

Acquired using: ADI4.2.0.13
Case Number: 305C-HQ-54464560
Evidence Number: QHQ1
Unique description: Toshiba 500GB hard drive, serial number: 0812WER45930
Examiner: John Brown
Notes:



Case information entered

Information for C:\Users\CART\Desktop\CASES\QHQ1\QHQ1 Image:

Physical Evidentiary Item (Source) Information:

[Device Info]
Source Type: Logical
[Drive Geometry]
Bytes per Sector: 512
Sector Count: 15,771,720
[Physical Drive Information]
Removable drive: True
Source data size: 7701 MB
Sector count: 15771720
[Computed Hashes]
MD5 checksum: e7ceaef20a2e2be0994945ala5776e37
SHA1 checksum: 05ecb655b49fd0facb853d8fb78314b03b116961



Hardware Geometry

Image Information:

Acquisition started: Tue May 21 14:12:15 2019
Acquisition finished: Tue May 21 14:19:20 2019
Segment list:
C:\Users\CART\Desktop\CASES\QHQ1\QHQ1 Image.E01



Original acquisition date and time

Image Verification Results:

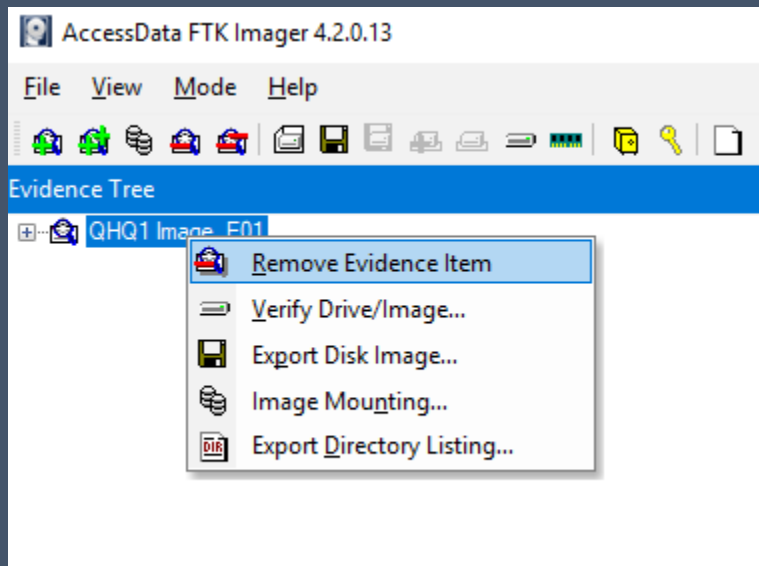
Verification started: Tue May 21 14:19:20 2019
Verification finished: Tue May 21 14:20:01 2019
MD5 checksum: e7ceaef20a2e2be0994945ala5776e37 : verified
SHA1 checksum: 05ecb655b49fd0facb853d8fb78314b03b116961 : verified



Image Verification Results

Remove Evidence

When work is completed, remove the evidence image from FTK Imager.



Right click the evidence item, or highlight the button on the Task Bar.



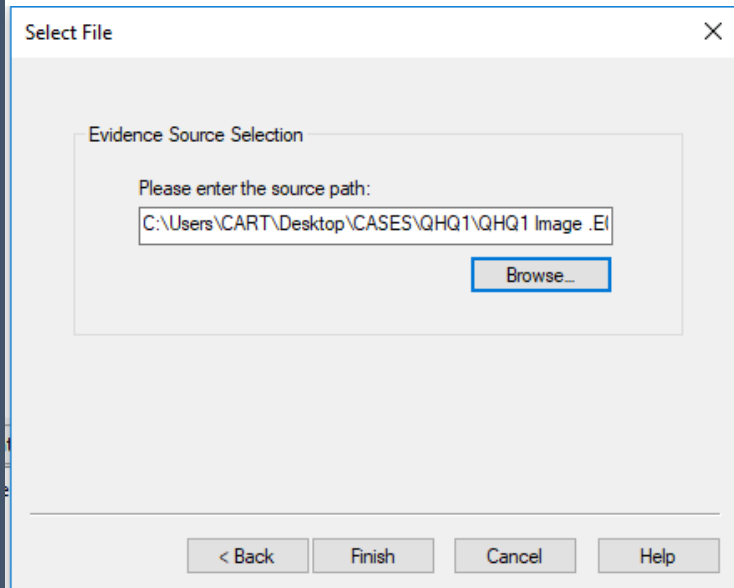
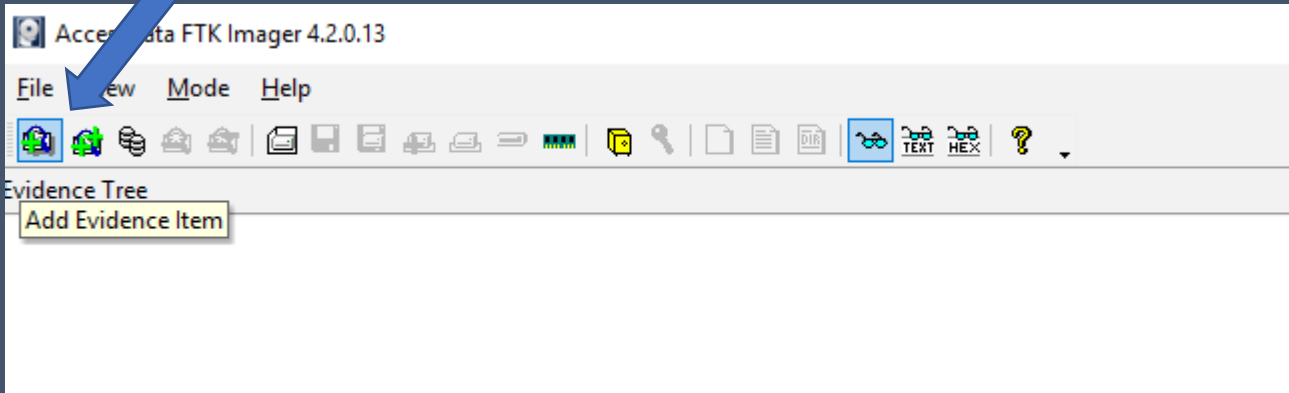
Live Demonstration

Physical Drive – imaged

Contents of a Folder – imaged

Create a AD1 – custom content image

Verify Drive/Image



- Add Evidence
- Select Image File
- Click Next
- Select file of previously created image
- Click Finish

Verify Drive/Image

- Right click image file
- Select Verify Drive/Image
- Select file of previously created image
- Click Finish
- Dialogue box displays Forensic Hash

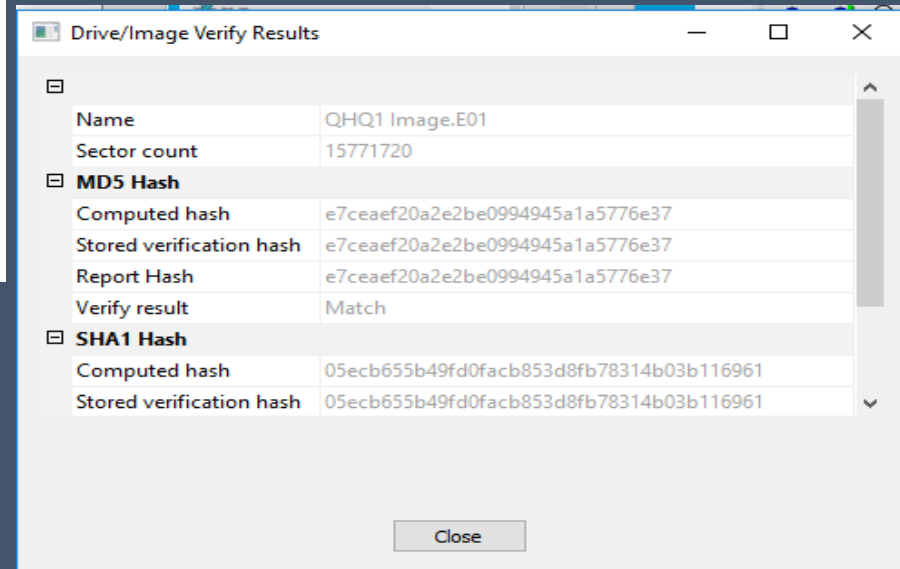
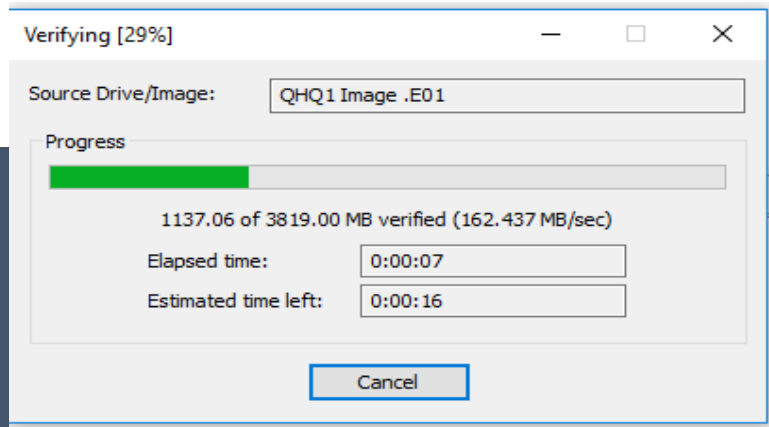
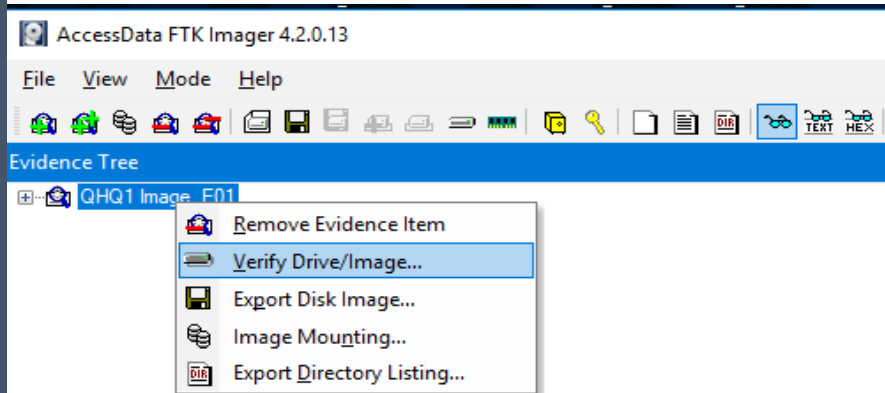
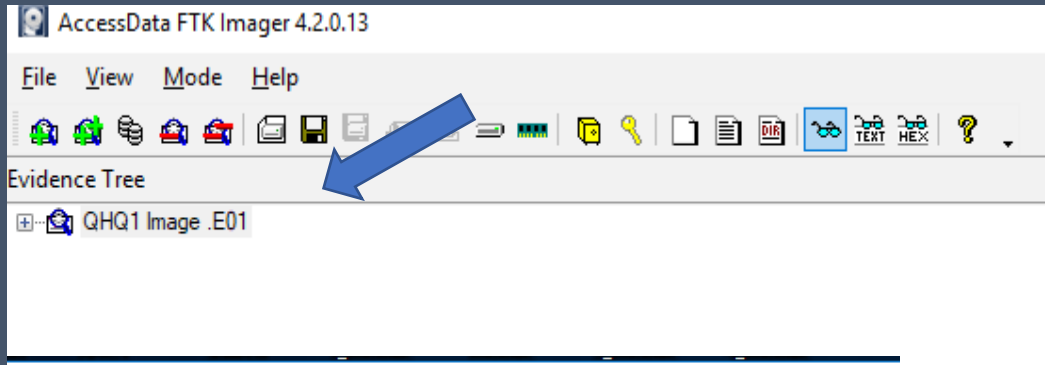


Image Verification Log

```
Created By AccessData® FTK® Imager 4.2.0.13

Case Information:
Acquired using: ADI4.2.0.13
Case Number: 305C-HQ-54464560
Evidence Number: QHQ1
Unique description: Toshiba 500GB hard drive, serial number: 0812WER45930
Examiner: John Brown
Notes:

-----

Information for C:\Users\CART\Desktop\CASES\QHQ1\QHQ1 Image:

Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Logical
[Drive Geometry]
Bytes per Sector: 512
Sector Count: 15,771,720
[Physical Drive Information]
Removable drive: True
Source data size: 7701 MB
Sector count: 15771720
[Computed Hashes]
MD5 checksum: e7ceaeef20a2e2be0994945ala5776e37
SHA1 checksum: 05ecb655b49fd0facb853d8fb78314b03b116961

Image Information:
Acquisition started: Tue May 21 14:12:15 2019
Acquisition finished: Tue May 21 14:19:20 2019
Segment list:
C:\Users\CART\Desktop\CASES\QHQ1\QHQ1 Image.E01

Image Verification Results:
Verification started: Tue May 21 14:19:20 2019
Verification finished: Tue May 21 14:20:01 2019
MD5 checksum: e7ceaeef20a2e2be0994945ala5776e37 : verified
SHA1 checksum: 05ecb655b49fd0facb853d8fb78314b03b116961 : verified

Image Verification Results:
Verification started: Thu May 23 07:32:11 2019
Verification finished: Thu May 23 07:32:52 2019
MD5 checksum: e7ceaeef20a2e2be0994945ala5776e37 : verified
SHA1 checksum: 05ecb655b49fd0facb853d8fb78314b03b116961 : verified
```

Original Acquisition
date and time

Verification Results

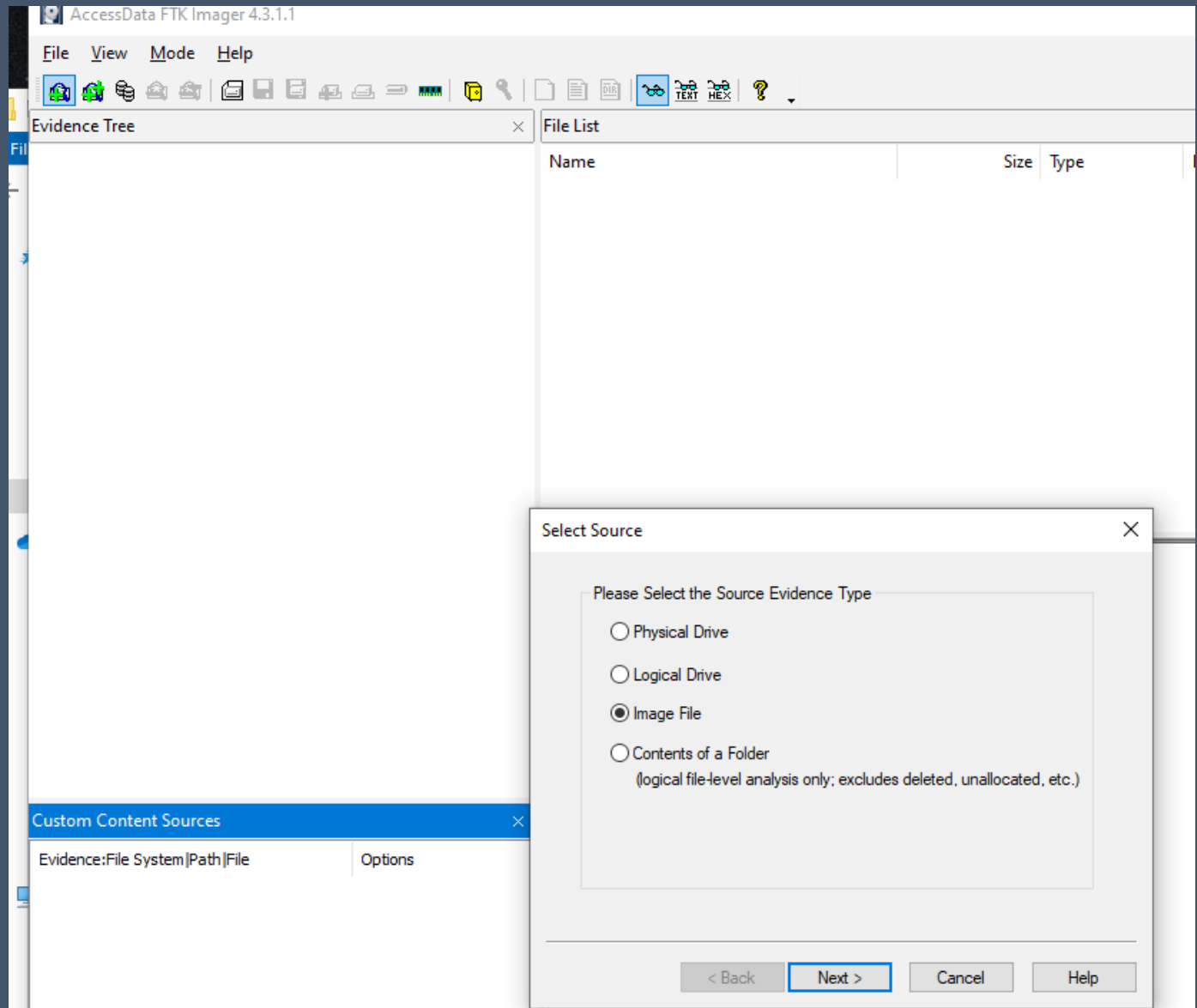
Verification Results
appended to log file

Live Demonstration
Verify an Image File
Verification Log Append

Export Files in FTK Imager

Add Evidence

Select Image File



Export Files in FTK Imager

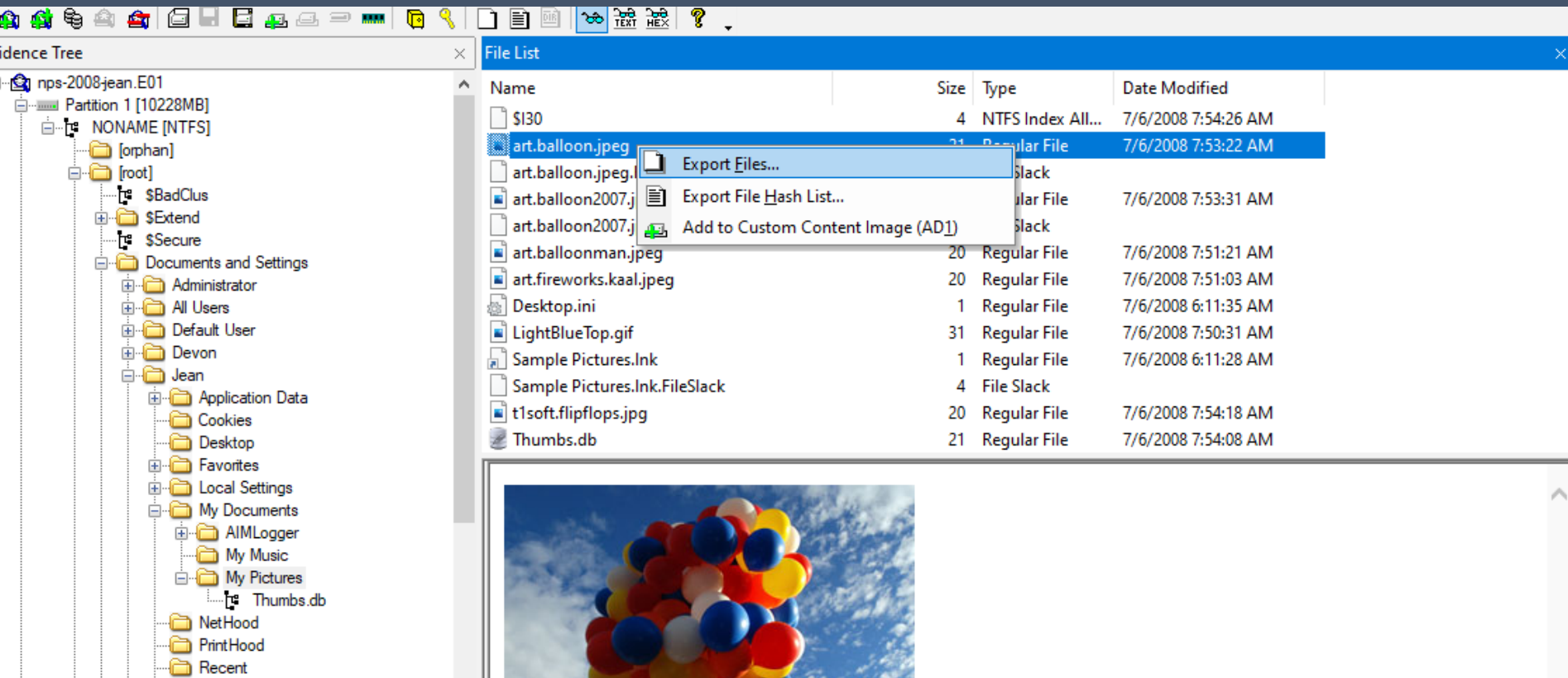
The screenshot displays the AccessData FTK Imager 4.3.1.1 interface. The 'Evidence Tree' on the left shows a file system structure for 'nps-2008:jean.E01'. The 'File List' on the right shows a table of files with columns for Name, Size, Type, and Date Modified. Below the file list is a hex dump of the selected file.

Name	Size	Type	Date Modified
\$I30	4	NTFS Index All...	7/6/2008 7:54:26 AM
art.balloon.jpeg	21	Regular File	7/6/2008 7:53:22 AM
art.balloon.jpeg.FileSlack	4	File Slack	
art.balloon2007.jpeg	21	Regular File	7/6/2008 7:53:31 AM
art.balloon2007.jpeg.FileSlack	4	File Slack	
art.balloonman.jpeg	20	Regular File	7/6/2008 7:51:21 AM
art.fireworks.kaal.jpeg	20	Regular File	7/6/2008 7:51:03 AM
Desktop.ini	1	Regular File	7/6/2008 6:11:35 AM
LightBlueTop.gif	31	Regular File	7/6/2008 7:50:31 AM
Sample Pictures.Ink	1	Regular File	7/6/2008 6:11:28 AM
Sample Pictures.Ink.FileSlack	4	File Slack	
t1soft.flipflops.jpg	20	Regular File	7/6/2008 7:54:18 AM
Thumbs.db	21	Regular File	7/6/2008 7:54:08 AM

```
00 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00 0
10 10 00 00 00 28 00 00 00-28 00 00 00 01 00 00 00
20 00 00 00 00 00 00 00 00-18 00 00 00 03 00 00 00
30 00 00 00 00 00 00 00 00-
```

Traverse through the + symbols down to files to be exported

Export Files in FTK Imager

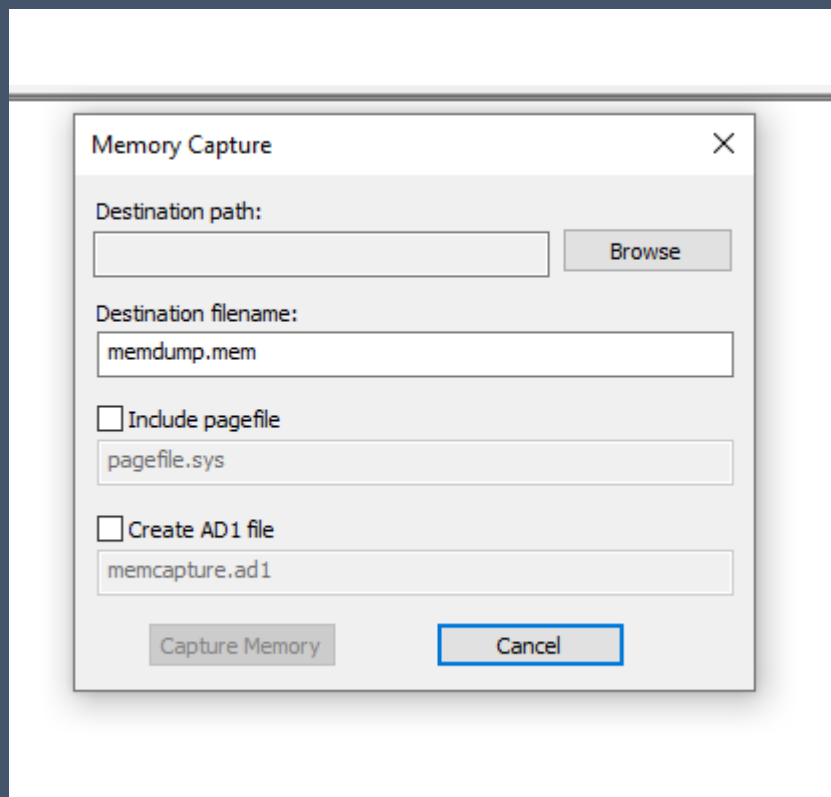
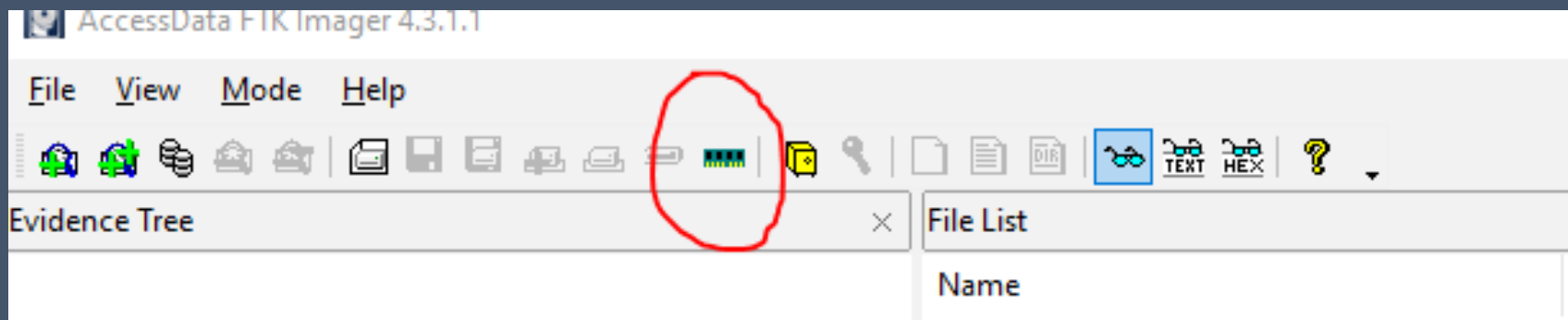


Select file -> Right click
Select destination for exported file

Live Demonstration

Export Files

Create a Memory Capture



Create a Memory Capture



What is pagefile.sys?



Why would you capture it?



What's the benefits of creating a AD1 image from a Memory Capture?

Live Demonstration Memory Capture