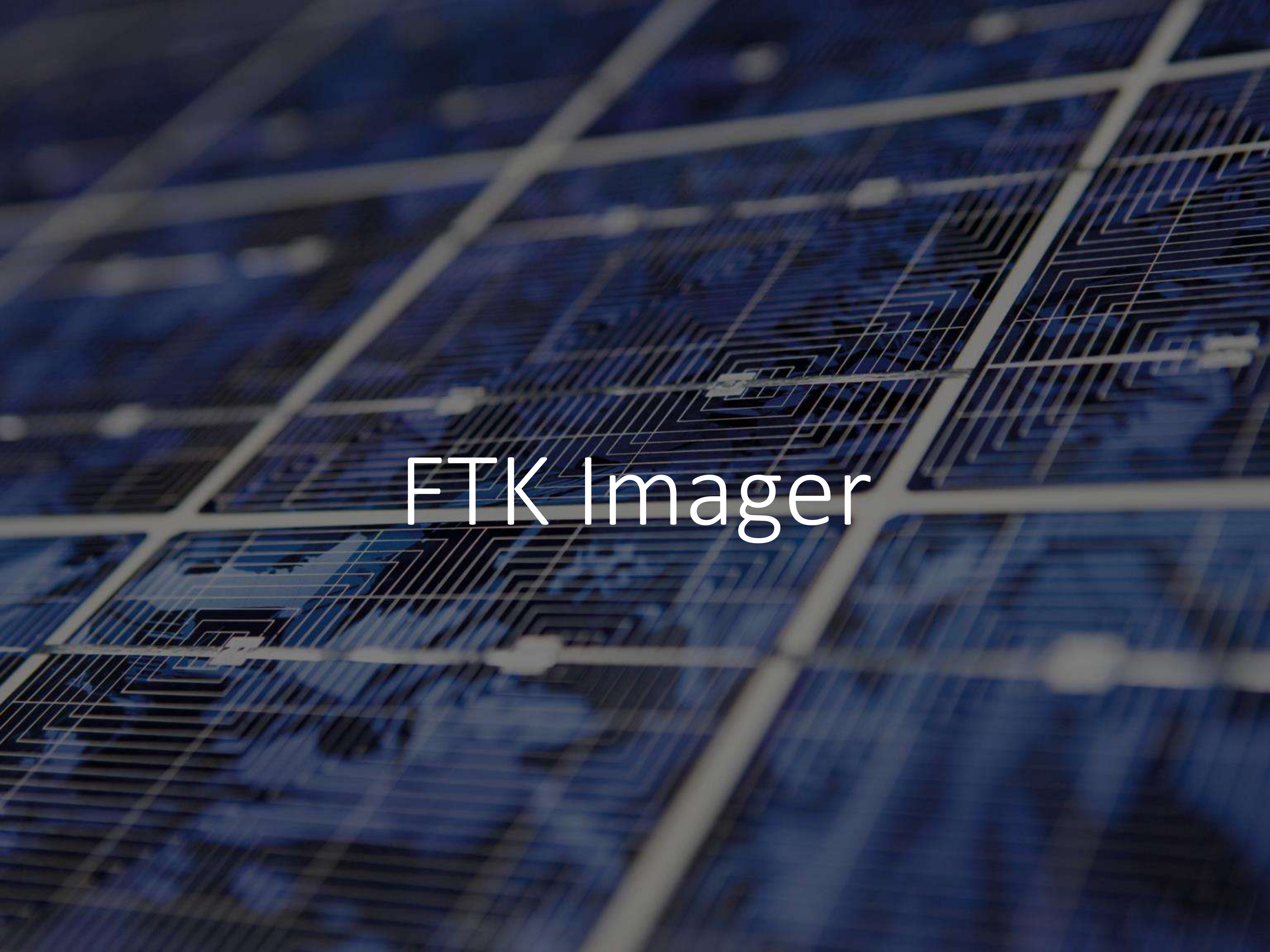
FORGE INSTITUTE

FORGE INSTITUTE

ARKANSAS CYBER STRIKE TEAM TRAINING

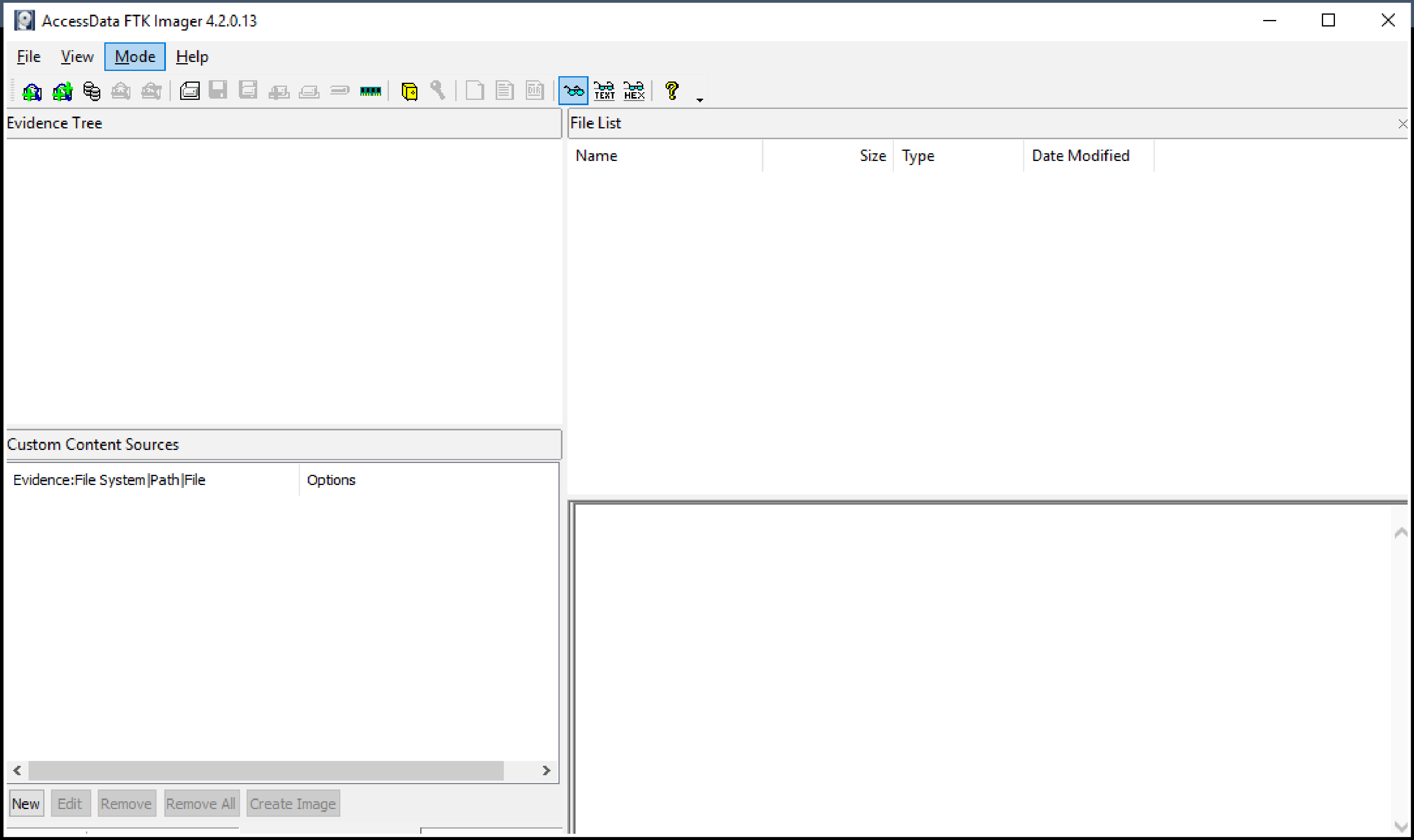
Digital Forensics



FTK Imager

Why use FTK Imager?

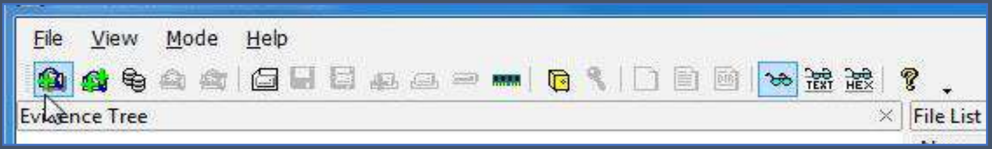
- Free, powerful tool
- Data preview and imaging tool
- Acquire volatile memory
- Preview image created with other tool(s)
- Verification/Forensic Hash
- Mount an image for read-only view
- Export Files and Folders
- Create Custom Content Image (AD1)
- Create Hashes and File List



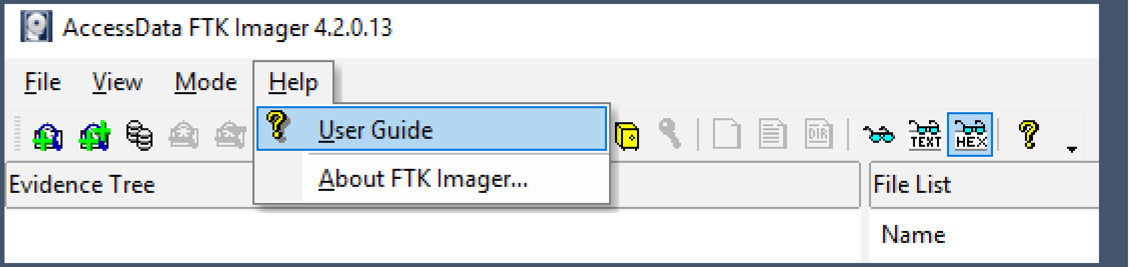
FTK Imager Interface

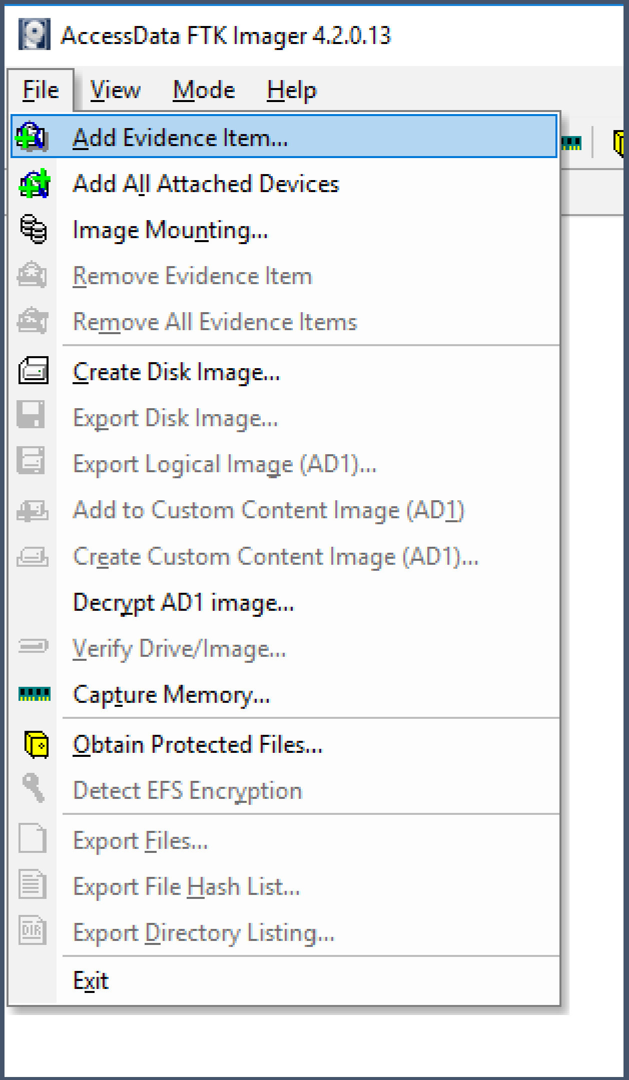
Options in FTK Imager

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



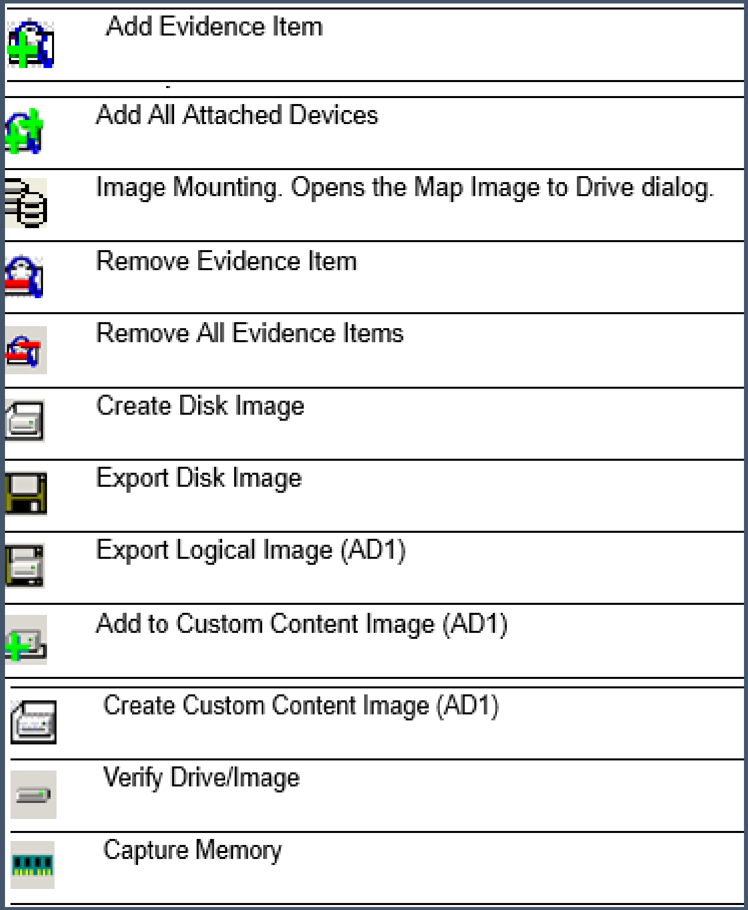
- Access User Guide in Help tab



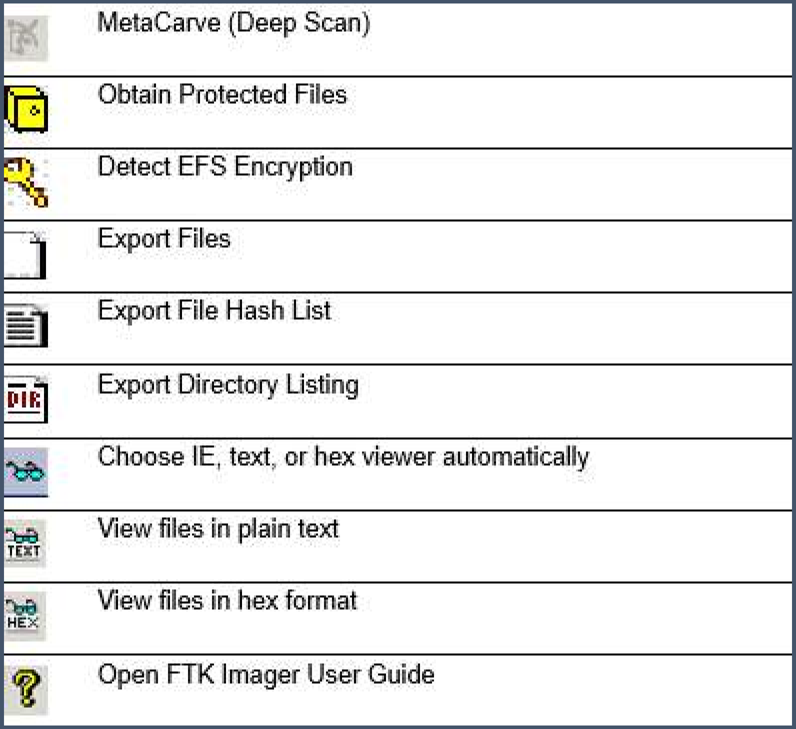


FTK Imager Toolbar

The toolbar contains all the tools, functions, or features, which can be assessed 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



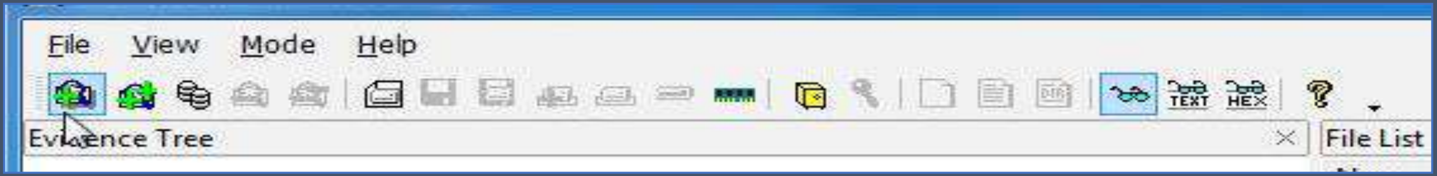
	MetaCarve (Deep Scan)
	Obtain Protected Files
	Detect EFS Encryption
	Export Files
	Export File Hash List
	Export Directory Listing
	Choose IE, text, or hex viewer automatically
	View files in plain text
	View files in hex format
	Open FTK Imager User Guide

Adding Evidence Item

To add an evidence item to the Evidence Tree

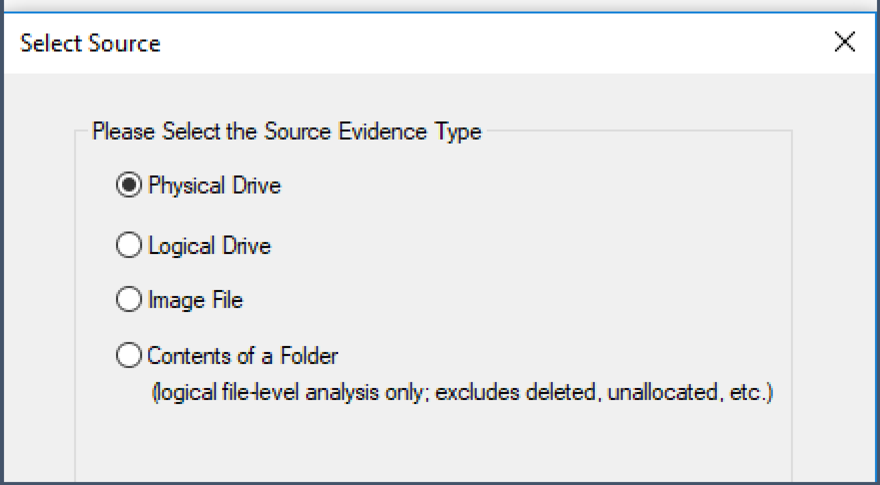
Click File>Add Evidence OR

Click the Add Evidence Item button on the Toolbar.



Select Source Type

- Physical Drive
- Logical Drive
- Image File
- Contents of a Folder



Select Source

Please Select the Source Evidence Type

● Physical Drive

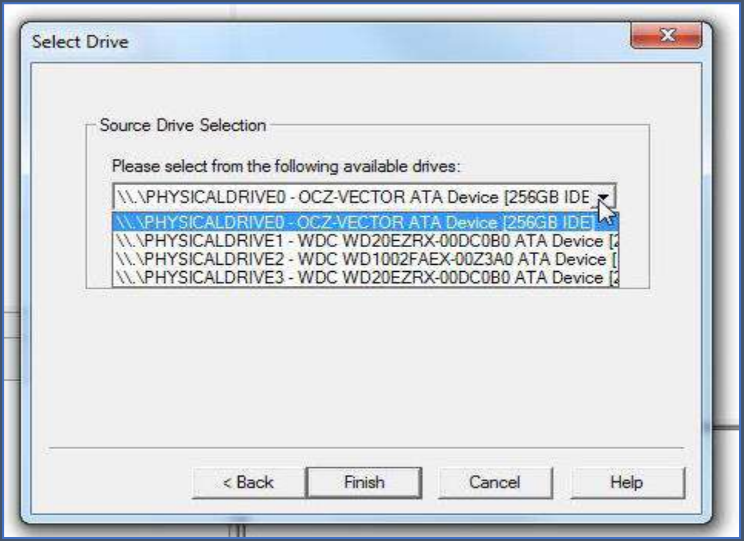
○ Logical Drive

○ Image File

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

Select Source Evidence Type

Physical Drive



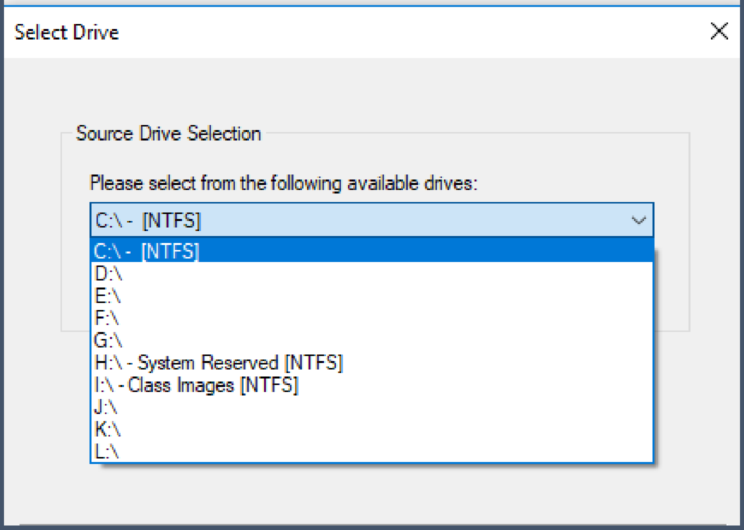
Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE0 - OCZ-VECTOR ATA Device [256GB IDE

\\.\PHYSICALDRIVE0 - OCZ-VECTOR ATA Device [256GB IDE]
\\.\PHYSICALDRIVE1 - WDC WD20EZRX-00DC0B0 ATA Device [2
\\.\PHYSICALDRIVE2 - WDC WD1002FAEX-00Z3A0 ATA Device [
\\.\PHYSICALDRIVE3 - WDC WD20EZRX-00DC0B0 ATA Device [2

Logical Drive



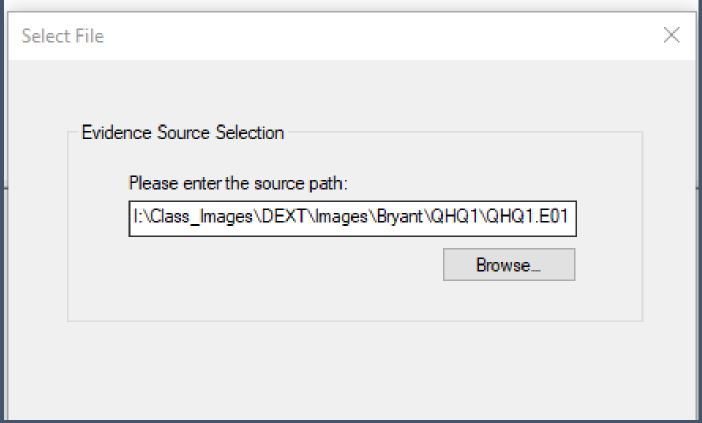
Source Drive Selection

Please select from the following available drives:

C:\ - [NTFS]

C:\ - [NTFS]
D:\
E:\
F:\
G:\
H:\ - System Reserved [NTFS]
I:\ - Class Images [NTFS]
J:\
K:\
L:\

Image File

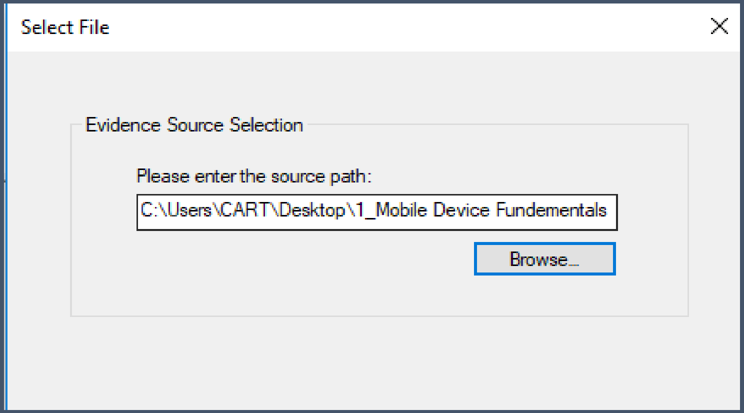


Evidence Source Selection

Please enter the source path:

I:\Class_Images\DEXT\Images\Bryant\QHQ1\QHQ1.E01

Contents of a Folder



Evidence Source Selection

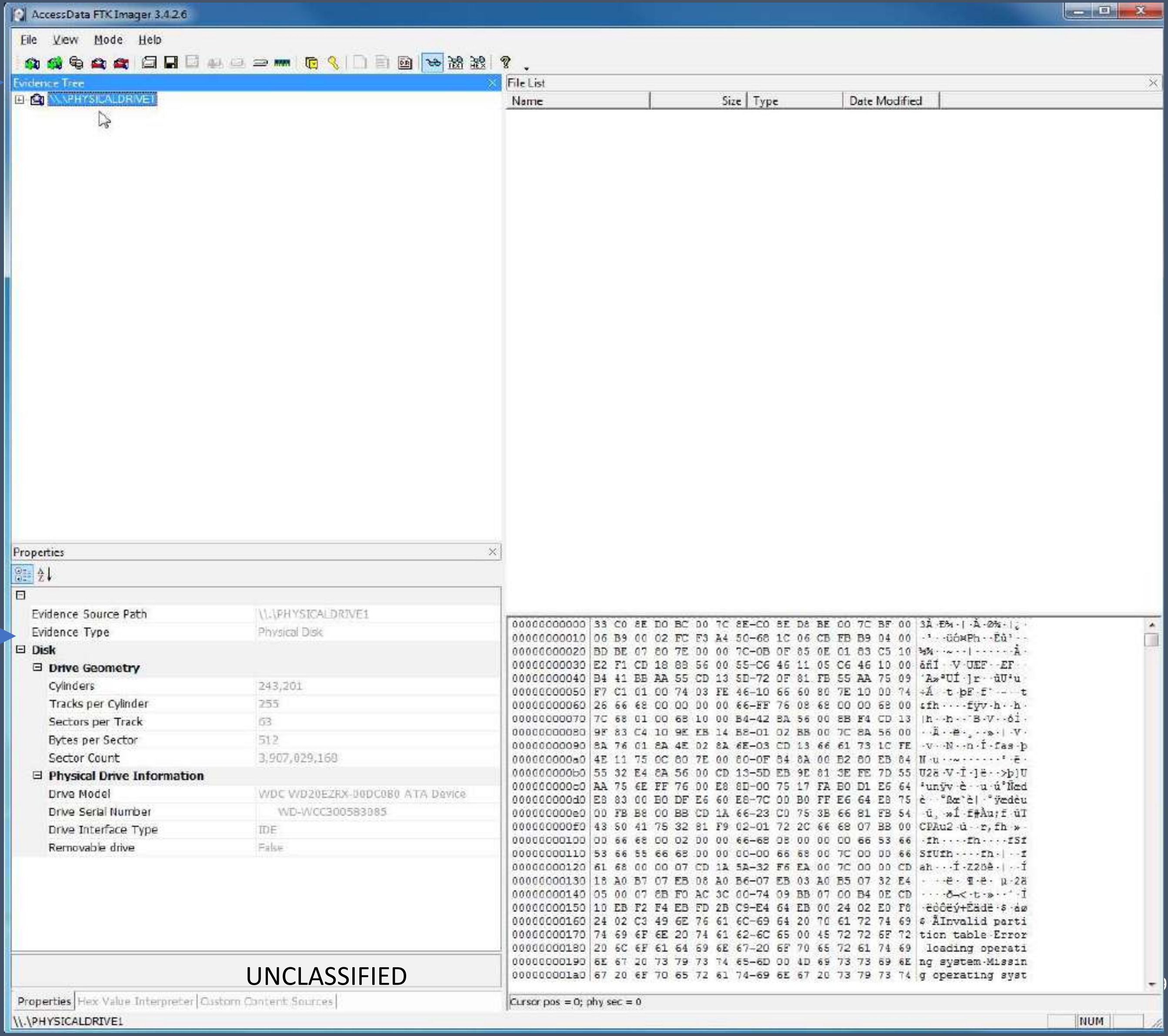
Please enter the source path:

C:\Users\CART\Desktop\1_Mobile Device Fundementals

FTK Imager with Evidence Added

Evidence Item appears in the Evidence Tree.

Properties give important information needed to complete catalog step.



Evidence Source Path	\\.\PHYSICALDRIVE1
Evidence Type	Physical Disk
Disk	
Drive Geometry	
Cylinders	243,201
Tracks per Cylinder	255
Sectors per Track	63
Bytes per Sector	512
Sector Count	3,907,029,168
Physical Drive Information	
Drive Model	WDC WD20EZRX-00DC0B0 ATA Device
Drive Serial Number	WD-WCC300583085
Drive Interface Type	IDE
Removable drive	False

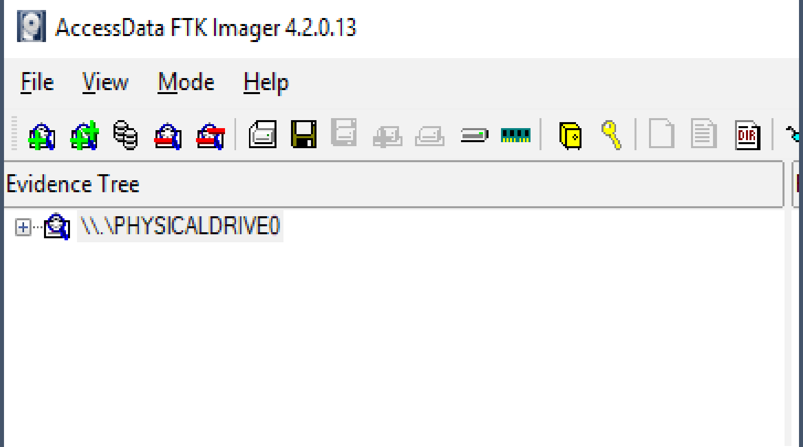
```
0000000000 33 C0 8E D0 BC 00 7C 8E-C0 8E D8 BE 00 7C BF 00 3À·Ð¼·|·À·Ø¾·|¿·
0000000010 06 B9 00 02 FC F3 A4 50-68 1C 06 CB FB B9 04 00 ·¹··üó¤Ph··Ëû¹··
0000000020 BD BE 07 80 7E 00 00 7C-0B 0F 85 0E 01 83 C5 10 ½¾··~··|·······Å·
0000000030 E2 F1 CD 18 88 56 00 55-C6 46 11 05 C6 46 10 00 âñÍ··V·UÆF··ÆF··
0000000040 B4 41 BB AA 55 CD 13 5D-72 0F 81 FB 55 AA 75 09 ´A»ªUÍ·]r··ûUªu·
0000000050 F7 C1 01 00 74 03 FE 46-10 66 60 80 7E 10 00 74 ÷Á··t·þF·f`·~··t
0000000060 26 66 68 00 00 00 00 66-FF 76 08 68 00 00 68 00 &fh····fÿv·h··h·
0000000070 7C 68 01 00 68 10 00 B4-42 8A 56 00 8B F4 CD 13 |h··h··´B·V··ôÍ·
0000000080 9F 83 C4 10 9E EB 14 B8-01 02 BB 00 7C 8A 56 00 ··Ä··ë·¸··»·|·V·
0000000090 8A 76 01 8A 4E 02 8A 6E-03 CD 13 66 61 73 1C FE ·v··N··n·Í·fas·þ
00000000a0 4E 11 75 0C 80 7E 00 80-0F 84 8A 00 B2 80 EB 84 N·u··~········ë·
00000000b0 55 32 E4 8A 56 00 CD 13-5D EB 9E 81 3E FE 7D 55 U2ä·V·Í·]ë··>þ}U
00000000c0 AA 75 6E FF 76 00 E8 8D-00 75 17 FA B0 D1 E6 64 ªunÿv·è··u·ú°Ñæd
00000000d0 E8 83 00 B0 DF E6 60 E8-7C 00 B0 FF E6 64 E8 75 è··°ßæ`è|·°ÿædèu
00000000e0 00 FB B8 00 BB CD 1A 66-23 C0 75 3B 66 81 FB 54 ·û¸·»Í·f#Àu;f·ûT
00000000f0 43 50 41 75 32 81 F9 02-01 72 2C 66 68 07 BB 00 CPAu2·ù··r,fh·»·
0000000100 00 66 68 00 02 00 00 66-68 08 00 00 00 66 53 66 ·fh····fh····fSf
0000000110 53 66 55 66 68 00 00 00-00 66 68 00 7C 00 00 66 SfUfh····fh·|··f
0000000120 61 68 00 00 07 CD 1A 5A-32 F6 EA 00 7C 00 00 CD ah···Í·Z2öê·|··Í
0000000130 18 A0 B7 07 EB 08 A0 B6-07 EB 03 A0 B5 07 32 E4 ··ë··¶·ë··µ·2ä
0000000140 05 00 07 8B F0 AC 3C 00-74 09 BB 07 00 B4 0E CD ····ð¬<·t·»··´·Í
0000000150 10 EB F2 F4 EB FD 2B C9-E4 64 EB 00 24 02 E0 F8 ·ëòôëý+Éädë·$·àø
0000000160 24 02 C3 49 6E 76 61 6C-69 64 20 70 61 72 74 69 $·ÃInvalid parti
0000000170 74 69 6F 6E 20 74 61 62-6C 65 00 45 72 72 6F 72 tion table·Error
0000000180 20 6C 6F 61 64 69 6E 67-20 6F 70 65 72 61 74 69  loading operati
0000000190 6E 67 20 73 79 73 74 65-6D 00 4D 69 73 73 69 6E ng system·Missin
00000001a0 67 20 6F 70 65 72 61 74-69 6E 67 20 73 79 73 74 g operating syst
```

Cursor pos = 0; phy sec = 0

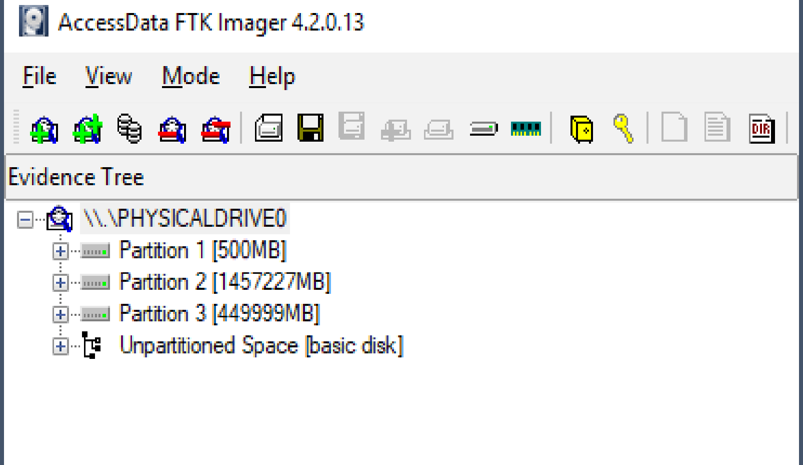
UNCLASSIFIED

Expand the Evidence Item

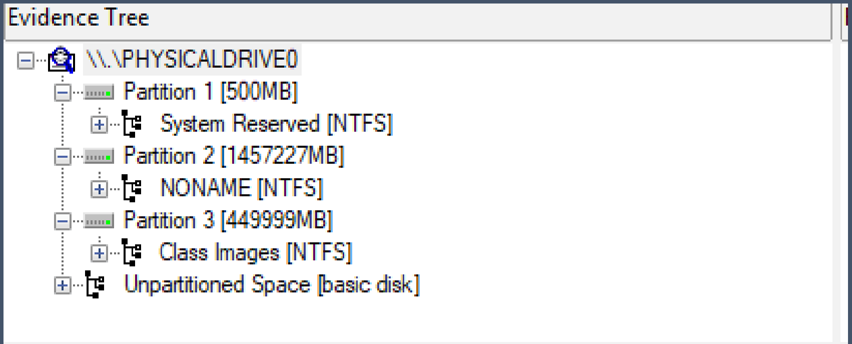
The plus sign "+" indicates the item can be expanded. In this case it unravels the drive "tree" to display catalog of data.



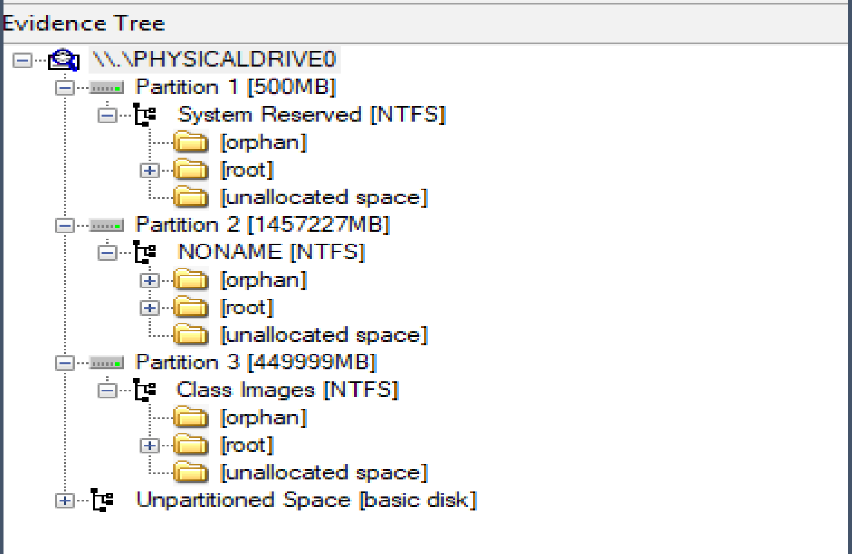
```
⊞ \\.\PHYSICALDRIVE0
```



```
⊟ \\.\PHYSICALDRIVE0
   ⊞ Partition 1 [500MB]
   ⊞ Partition 2 [1457227MB]
   ⊞ Partition 3 [449999MB]
   ⊞ Unpartitioned Space [basic disk]
```



```
⊟ \\.\PHYSICALDRIVE0
   ⊟ Partition 1 [500MB]
      ⊞ System Reserved [NTFS]
   ⊟ Partition 2 [1457227MB]
      ⊞ NONAME [NTFS]
   ⊟ Partition 3 [449999MB]
      ⊞ Class Images [NTFS]
   ⊞ Unpartitioned Space [basic disk]
```



```
⊟ \\.\PHYSICALDRIVE0
   ⊟ Partition 1 [500MB]
      ⊟ System Reserved [NTFS]
           [orphan]
         ⊞ [root]
           [unallocated space]
   ⊟ Partition 2 [1457227MB]
      ⊟ NONAME [NTFS]
         ⊞ [orphan]
         ⊞ [root]
           [unallocated space]
   ⊟ Partition 3 [449999MB]
      ⊟ Class Images [NTFS]
           [orphan]
         ⊞ [root]
           [unallocated space]
   ⊞ Unpartitioned Space [basic disk]
```

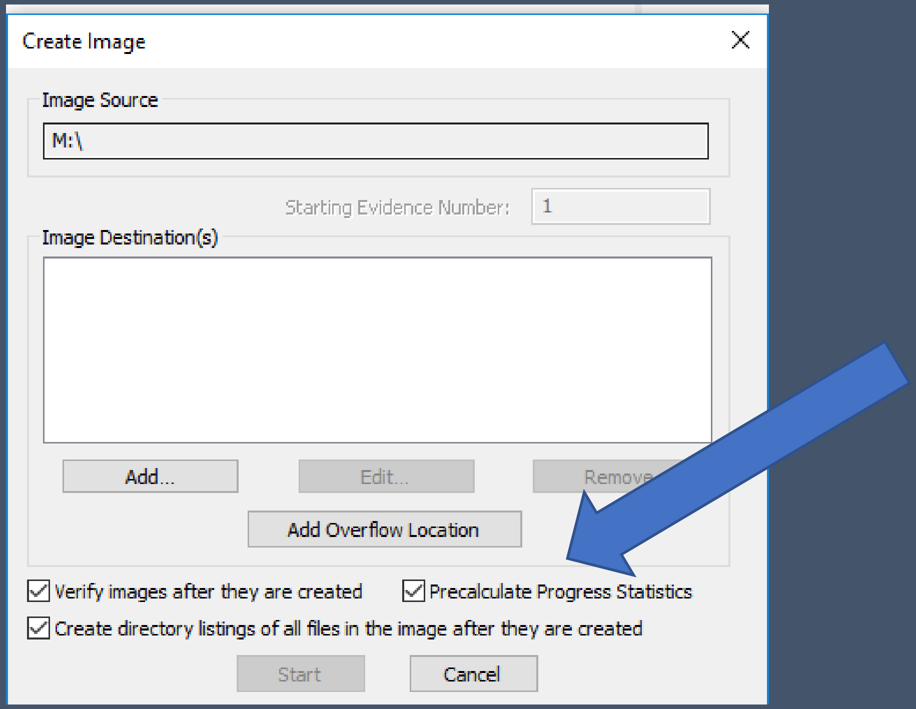
Imaging Evidence item

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



Create Image

Image Source: M:\

Starting Evidence Number: 1

Image Destination(s)

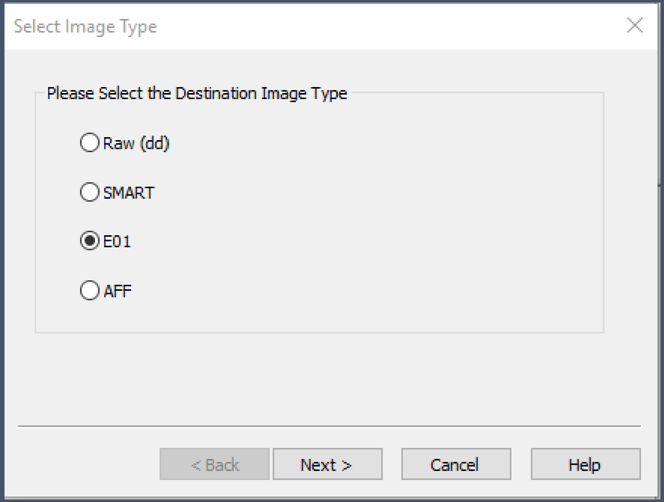
☑ Verify images after they are created ☑ Precalculate Progress Statistics

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

- ❑ 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

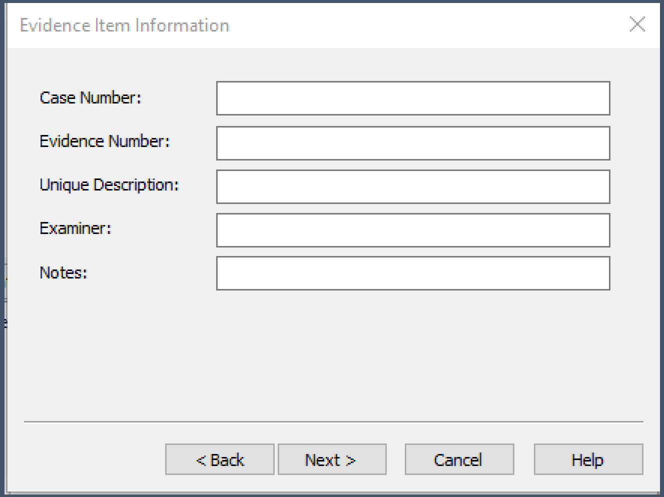
○ AFF

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

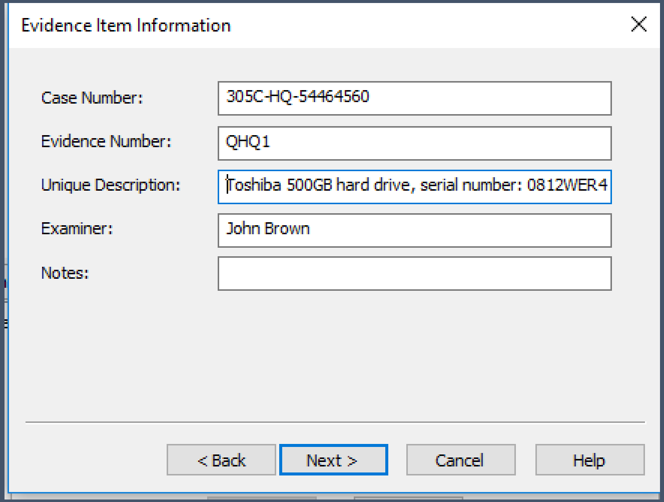
For this class we will focus on E01 only.

*Raw(dd) and E01 most widely supported

Input Evidence Information


Evidence Item Information

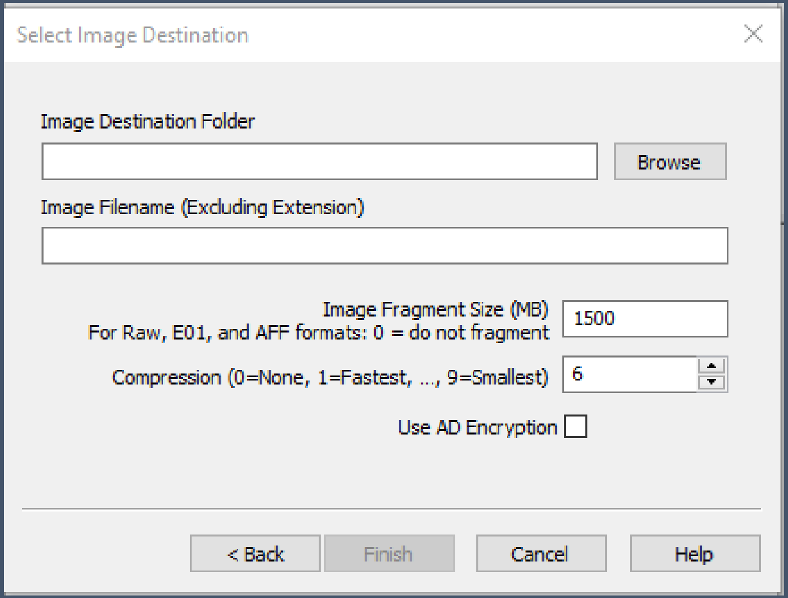
Case Number:	
Evidence Number:	
Unique Description:	
Examiner:	
Notes:	


Evidence Item Information

Case Number:	305C-HQ-54464560
Evidence Number:	QHQ1
Unique Description:	Toshiba 500GB hard drive, serial number: 0812WER4
Examiner:	John Brown
Notes:	

Imaging Evidence Item

Select Image Destination



Select Image Destination

Image Destination Folder

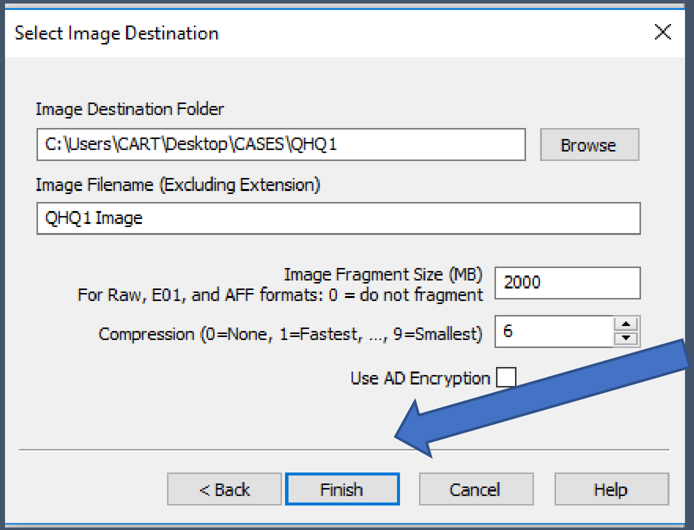
Browse

Image Filename (Excluding Extension)

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

Compression (0=None, 1=Fastest, ..., 9=Smallest) 6

Use AD Encryption □



Select Image Destination

Image Destination Folder
C:\Users\CART\Desktop\CASES\QHQ1

Browse

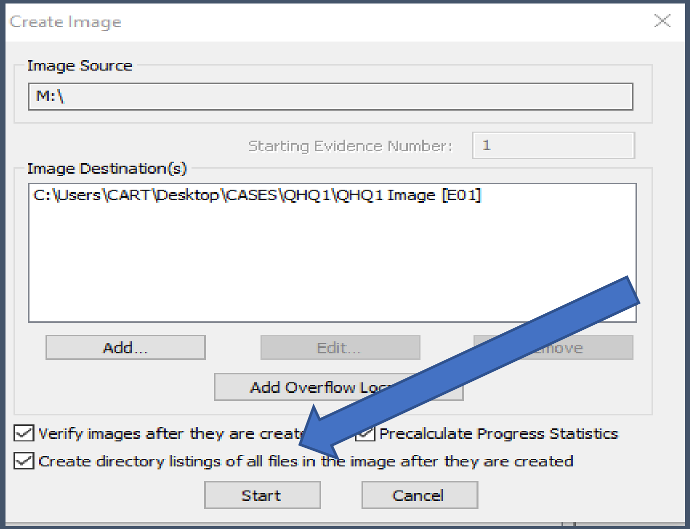
Image Filename (Excluding Extension)
QHQ1 Image

Image Fragment Size (MB) 2000
For Raw, E01, and AFF formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest) 6

Use AD Encryption □

Select Finish



Create Image

Image Source
M:\

Starting Evidence Number: 1

Image Destination(s)
C:\Users\CART\Desktop\CASES\QHQ1\QHQ1 Image [E01]

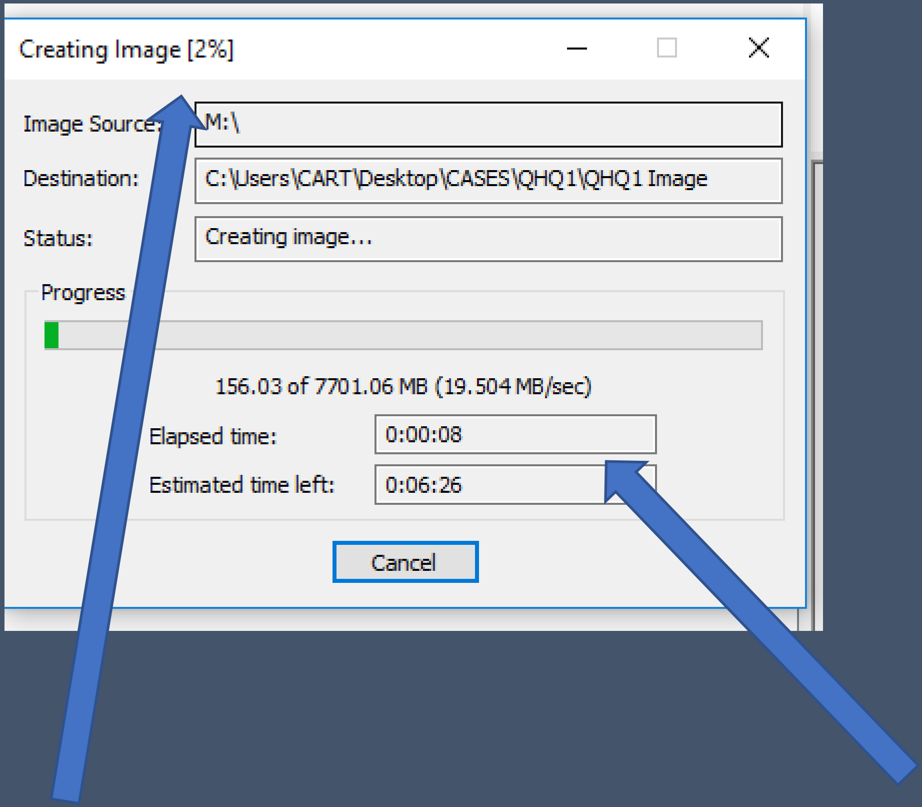
☑ Verify images after they are creat ☑ Precalculate Progress Statistics

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

Select Start

Imaging Evidence Item

Creating Image



Creating Image [2%]

Image Source: M:\

Destination: C:\Users\CART\Desktop\CASES\QHQ1\QHQ1 Image

Status: Creating image...

Progress

156.03 of 7701.06 MB (19.504 MB/sec)

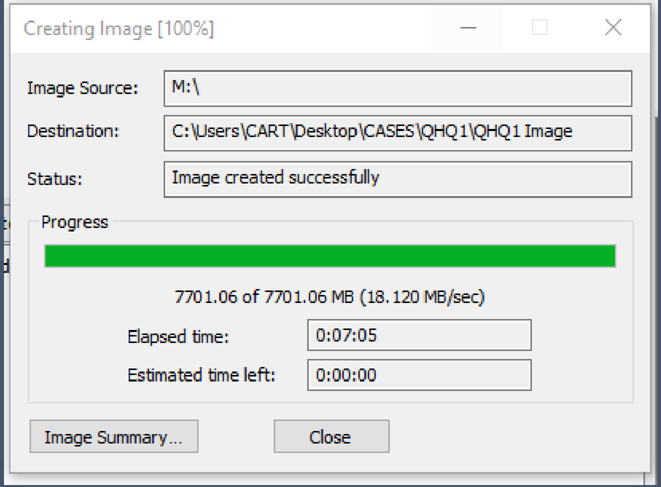
Elapsed time: 0:00:08

Estimated time left: 0:06:26

❑ Pre-calculate Progress Statistics

Imaging Evidence Item

Creating Image (100%)



Creating Image [100%]

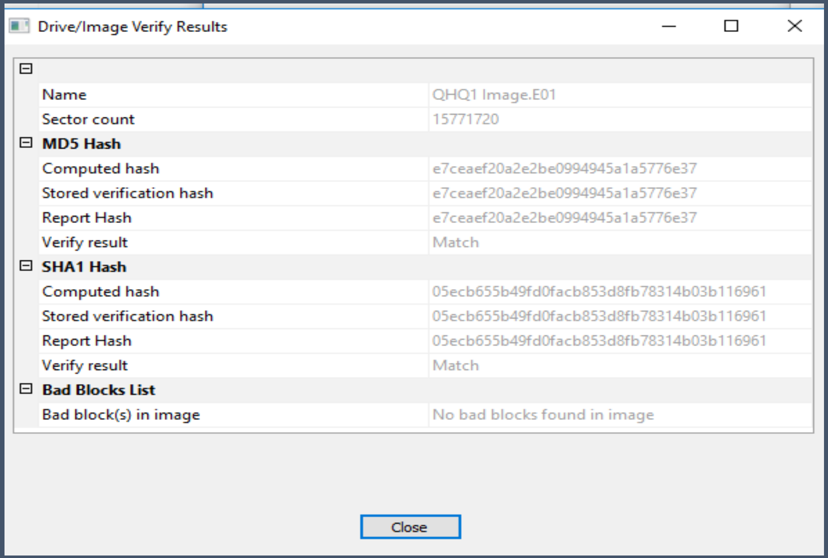
Image Source:	M:\
Destination:	C:\Users\CART\Desktop\CASES\QHQ1\QHQ1 Image
Status:	Image created successfully

Progress

7701.06 of 7701.06 MB (18.120 MB/sec)

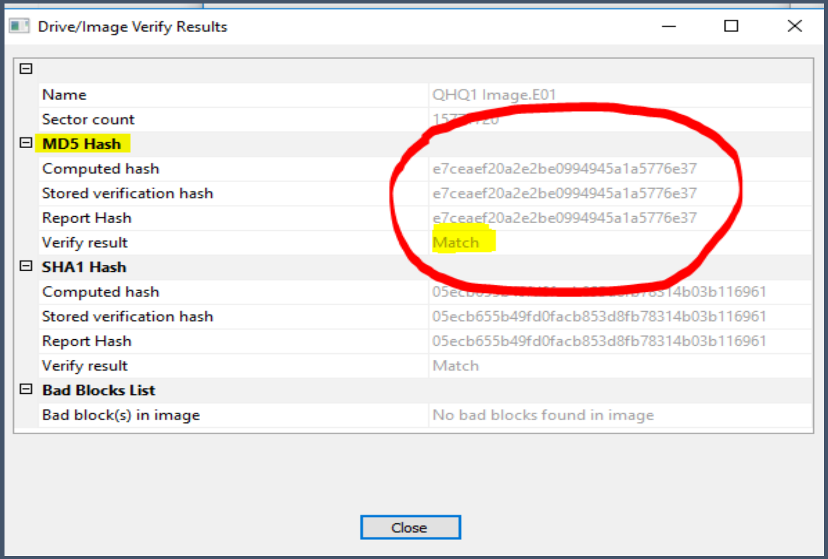
Elapsed time:	0:07:05
Estimated time left:	0:00:00

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



Drive/Image Verify Results

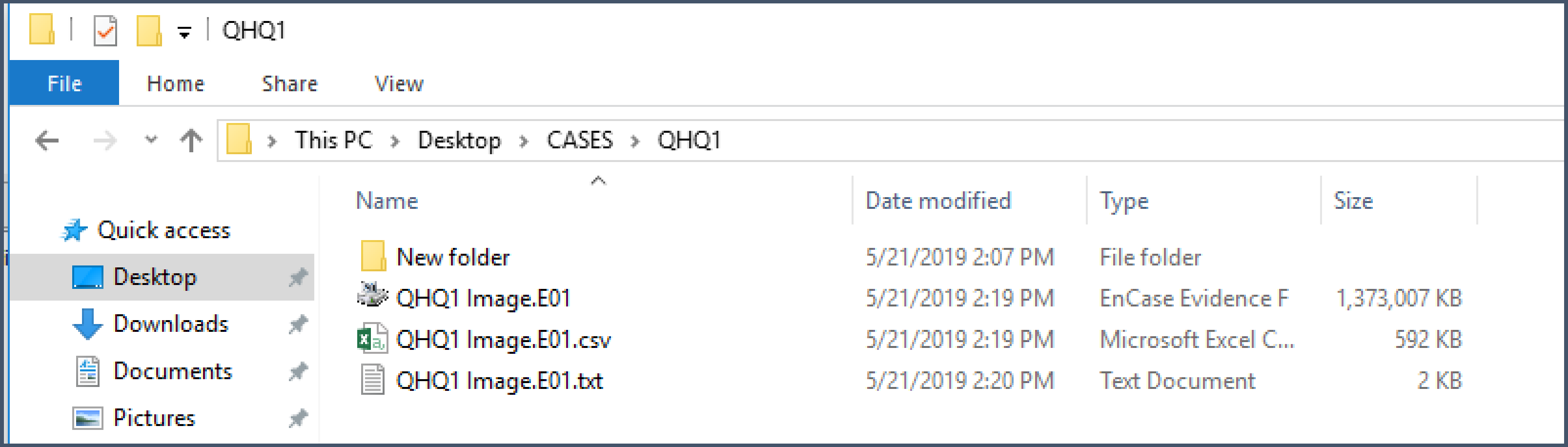
Name	QHQ1 Image.E01
Sector count	15771720
MD5 Hash	
Computed hash	e7ceaef20a2e2be0994945a1a5776e37
Stored verification hash	e7ceaef20a2e2be0994945a1a5776e37
Report Hash	e7ceaef20a2e2be0994945a1a5776e37
Verify result	Match
SHA1 Hash	
Computed hash	05ecb655b49fd0facb853d8fb78314b03b116961
Stored verification hash	05ecb655b49fd0facb853d8fb78314b03b116961
Report Hash	05ecb655b49fd0facb853d8fb78314b03b116961
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image



Drive/Image Verify Results

Name	QHQ1 Image.E01
Sector count	15771720
MD5 Hash	
Computed hash	e7ceaef20a2e2be0994945a1a5776e37
Stored verification hash	e7ceaef20a2e2be0994945a1a5776e37
Report Hash	e7ceaef20a2e2be0994945a1a5776e37
Verify result	Match
SHA1 Hash	
Computed hash	05ecb655b49fd0facb853d8fb78314b03b116961
Stored verification hash	05ecb655b49fd0facb853d8fb78314b03b116961
Report Hash	05ecb655b49fd0facb853d8fb78314b03b116961
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

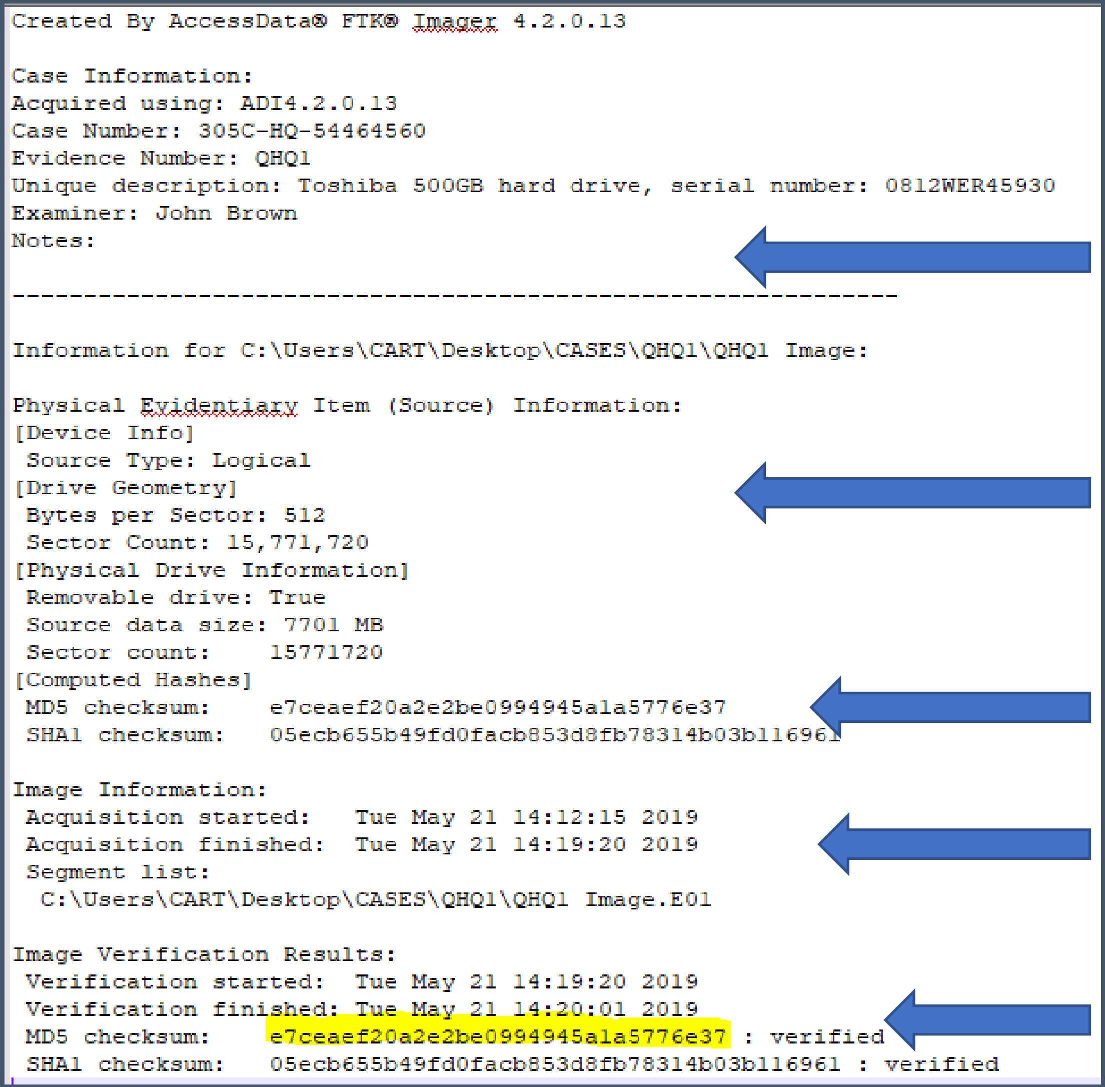
Image Verification Log



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:

--------------------------------------------------------------

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:    e7ceaef20a2e2be0994945a1a5776e37
 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:    e7ceaef20a2e2be0994945a1a5776e37 : verified
 SHA1 checksum:   05ecb655b49fd0facb853d8fb78314b03b116961 : verified
```

Case information entered

Hardware Geometry

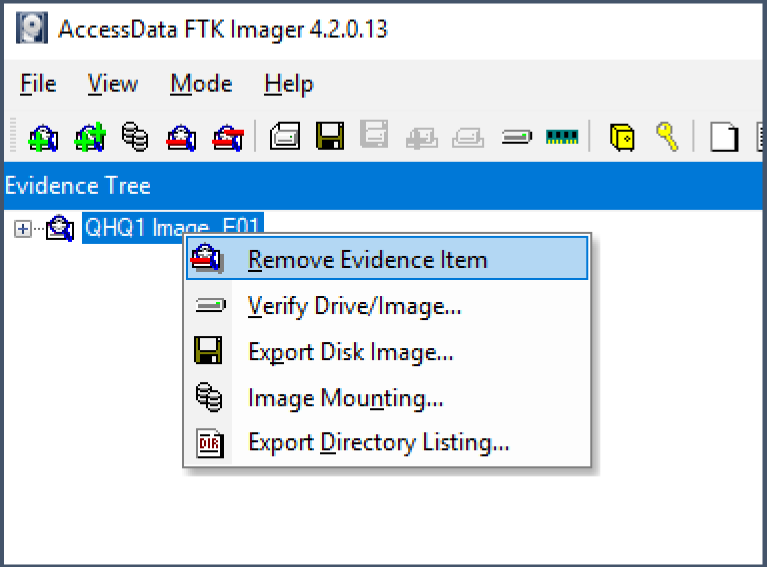
MD5 Checksum (acquisition)

Original acquisition date and time

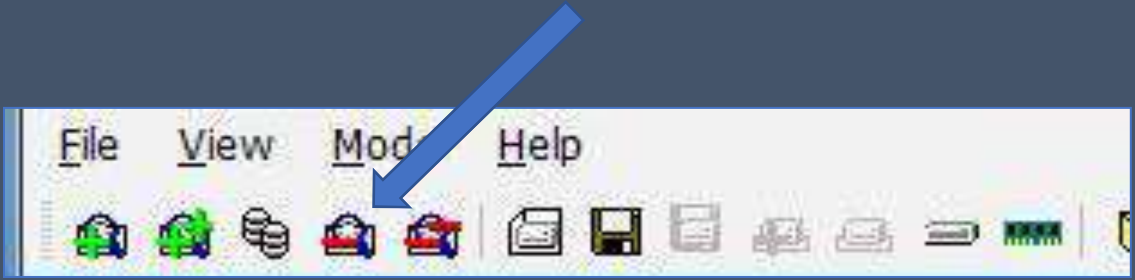
Image Verification Results

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.



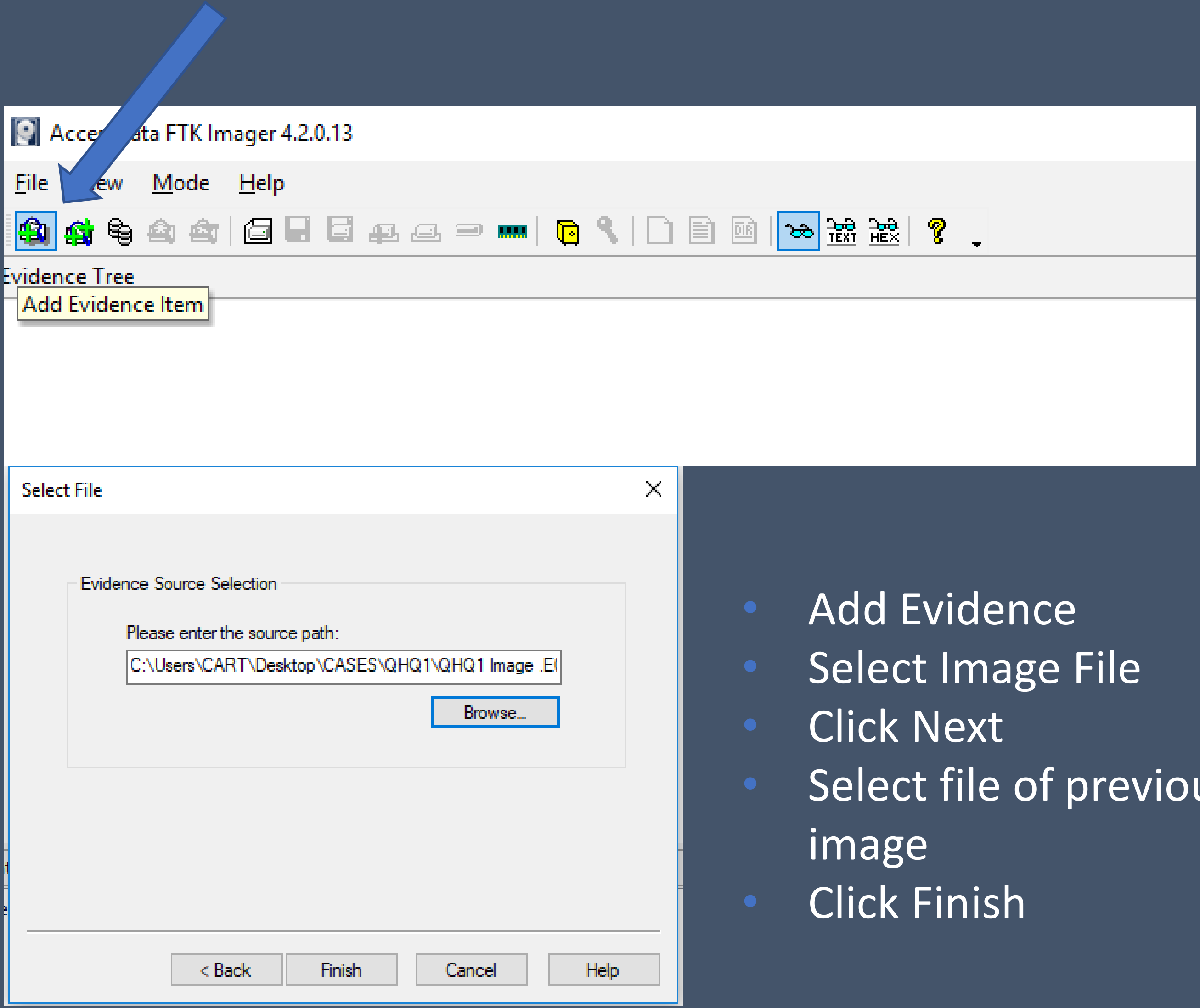
Live Demonstration

Physical Drive – imaged

Contents of a Folder – imaged

Create a AD1 – custom content image

Verify Drive/Image



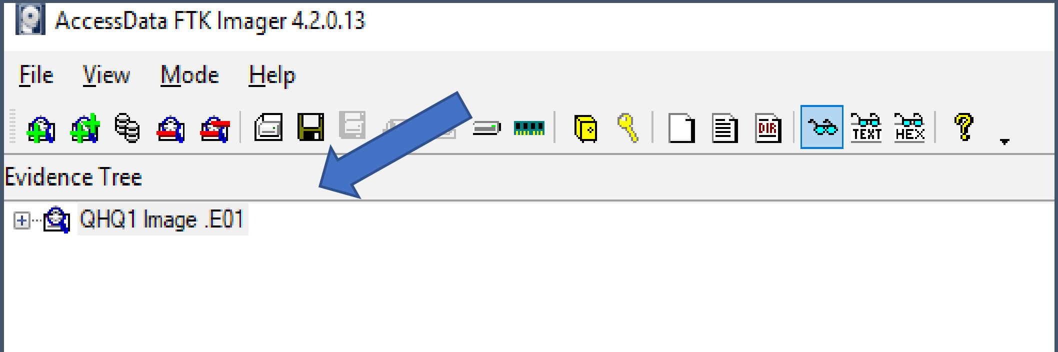
Evidence Source Selection

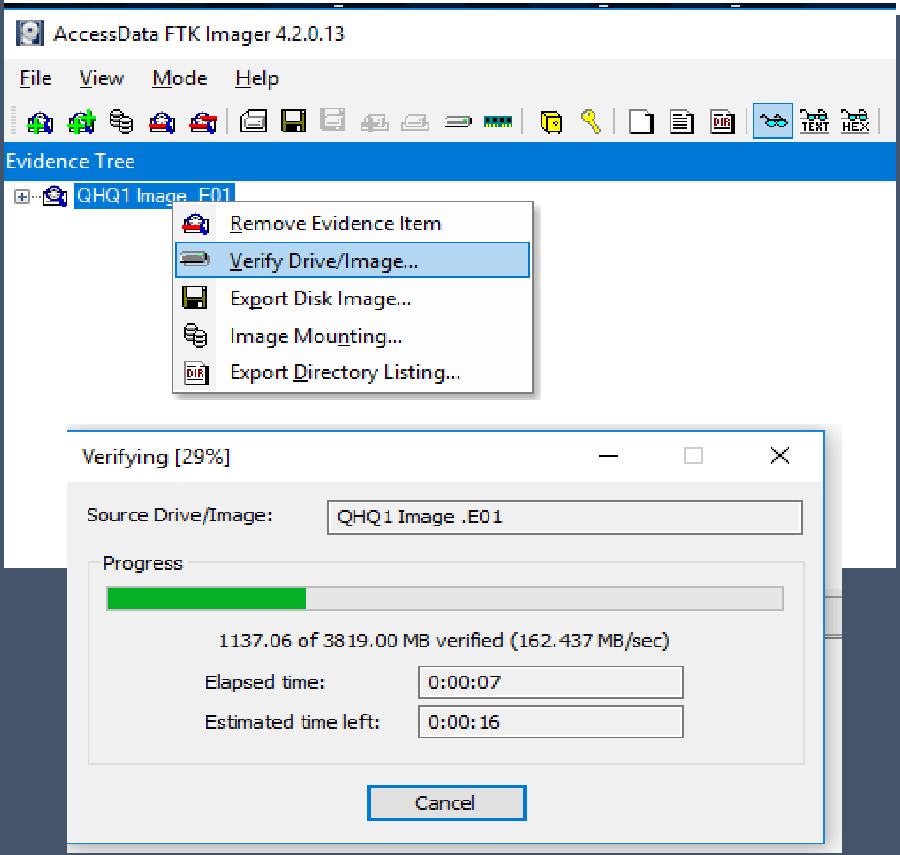
Please enter the source path: C:\Users\CART\Desktop\CASES\QHQ1\QHQ1 Image .E(

- 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





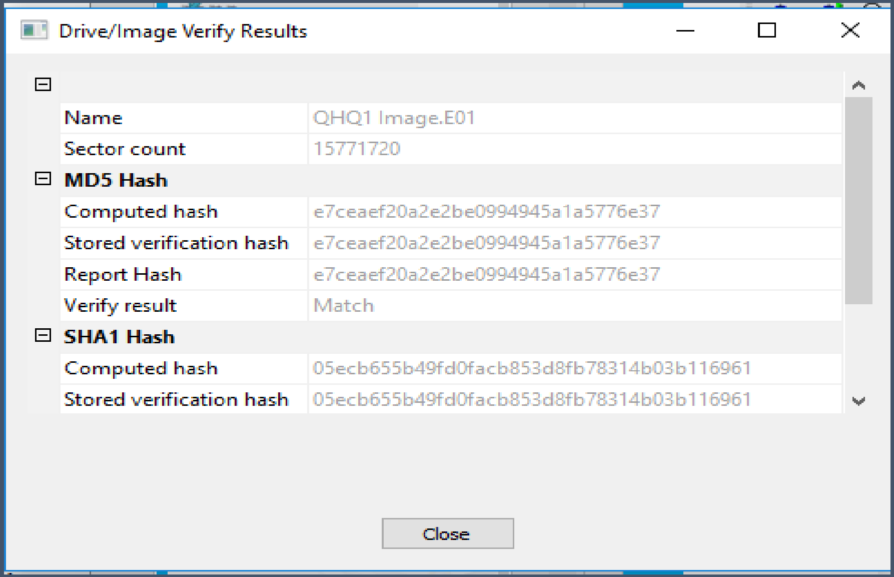
Verifying [29%]

Source Drive/Image: QHQ1 Image .E01

1137.06 of 3819.00 MB verified (162.437 MB/sec)

Elapsed time: 0:00:07

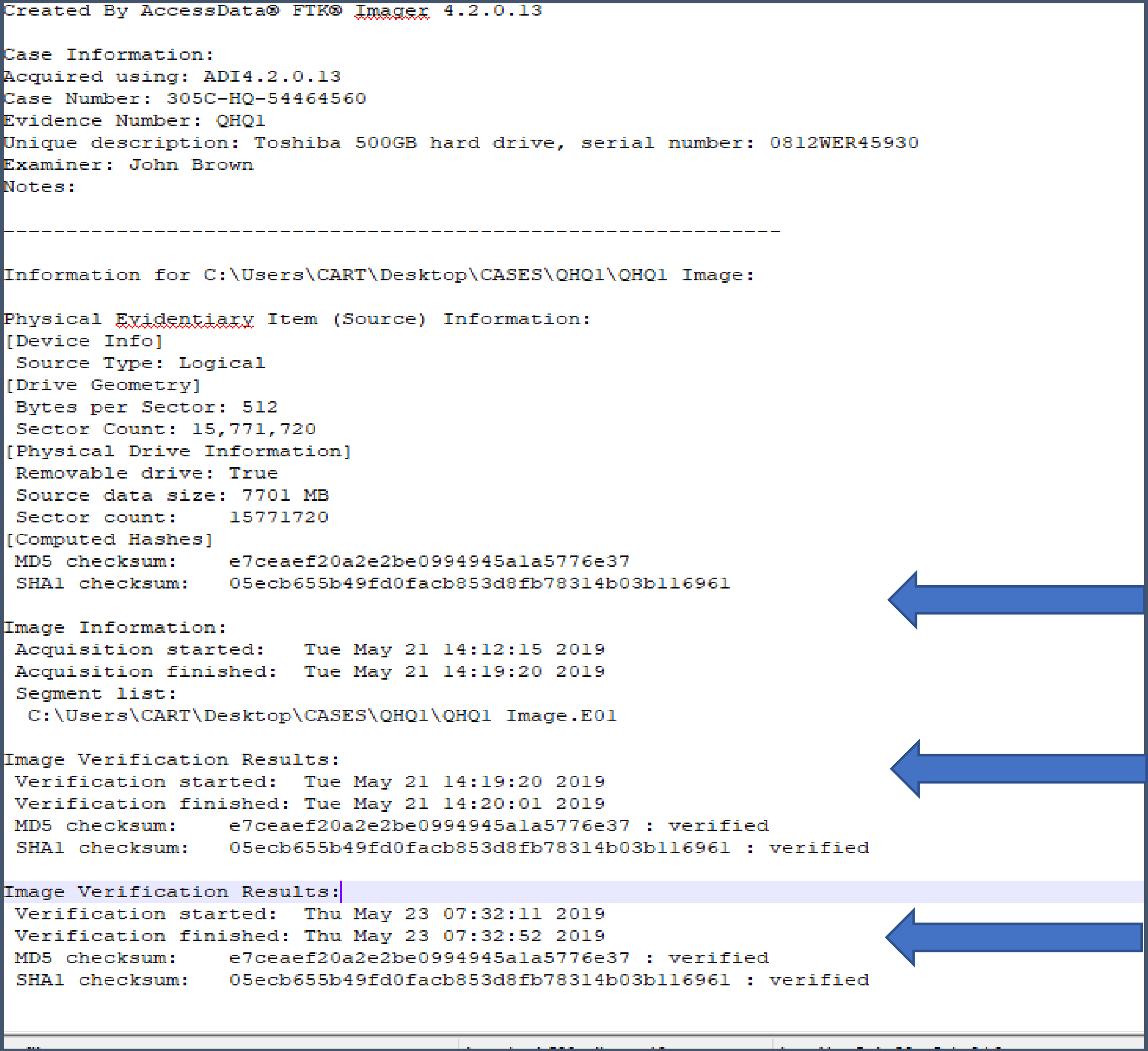
Estimated time left: 0:00:16



Drive/Image Verify Results

Name	QHQ1 Image.E01
Sector count	15771720
MD5 Hash	
Computed hash	e7ceaef20a2e2be0994945a1a5776e37
Stored verification hash	e7ceaef20a2e2be0994945a1a5776e37
Report Hash	e7ceaef20a2e2be0994945a1a5776e37
Verify result	Match
SHA1 Hash	
Computed hash	05ecb655b49fd0facb853d8fb78314b03b116961
Stored verification hash	05ecb655b49fd0facb853d8fb78314b03b116961

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:    e7ceaef20a2e2be0994945a1a5776e37
 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:    e7ceaef20a2e2be0994945a1a5776e37 : 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:    e7ceaef20a2e2be0994945a1a5776e37 : verified
 SHA1 checksum:   05ecb655b49fd0facb853d8fb78314b03b116961 : verified
```

Original Acquisition date and time

Verification Results

Verification Results appended to log file

Live Demonstration

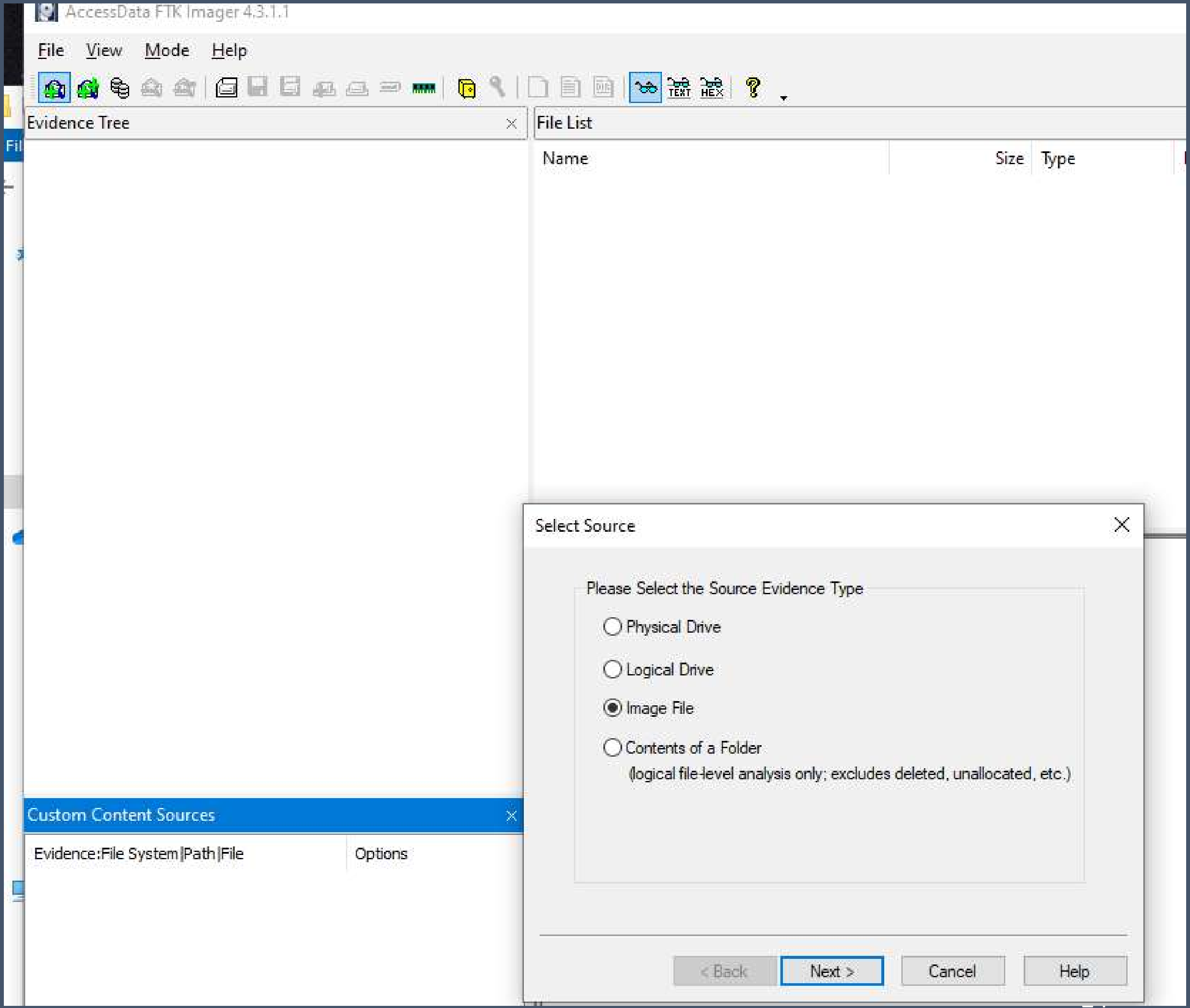
Verify an Image File

Verification Log Append

Export Files in FTK Imager

Add Evidence

Select Image File



Please Select the Source Evidence Type

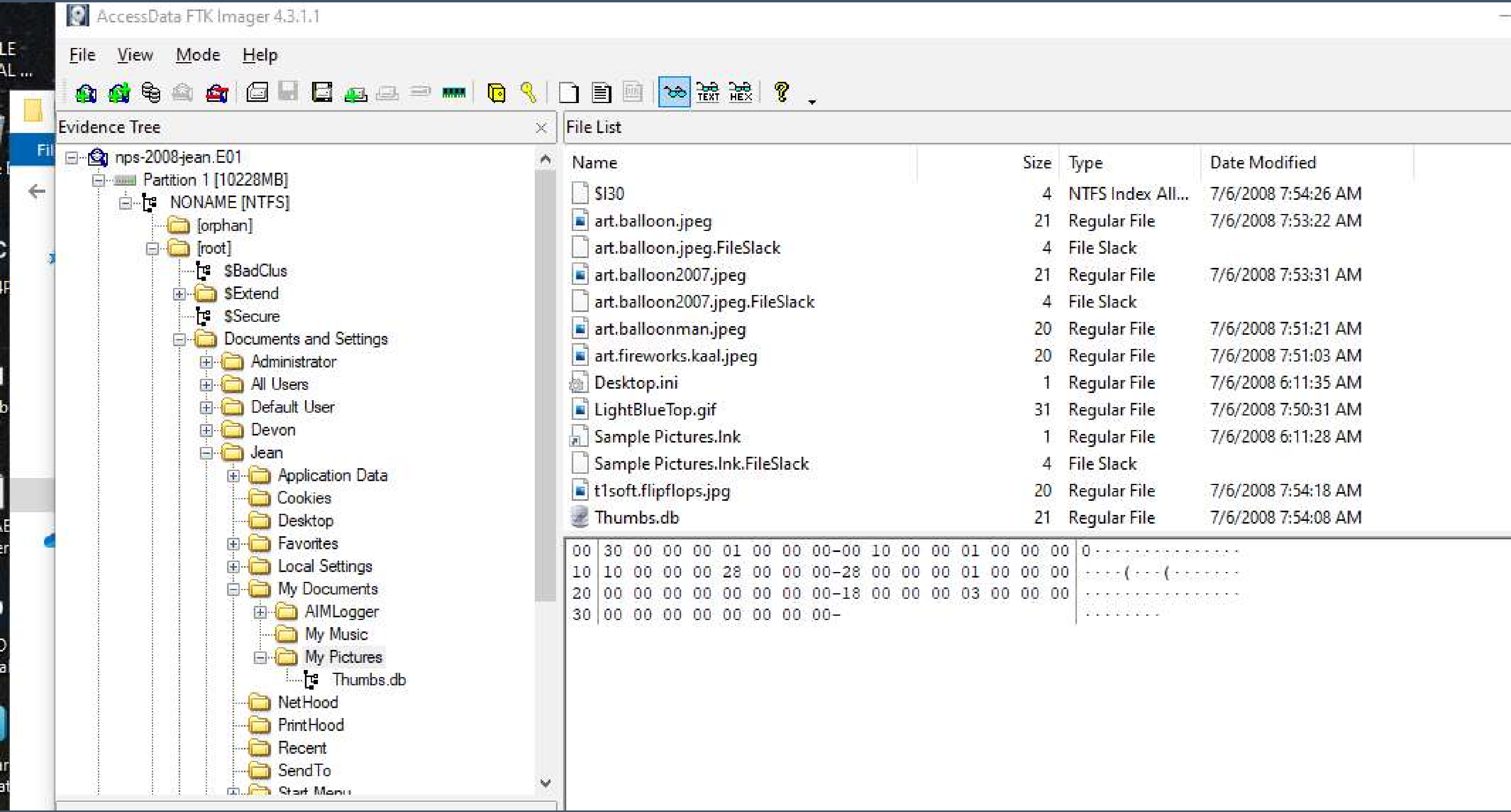
○ Physical Drive

○ Logical Drive

● Image File

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

Export Files in FTK Imager



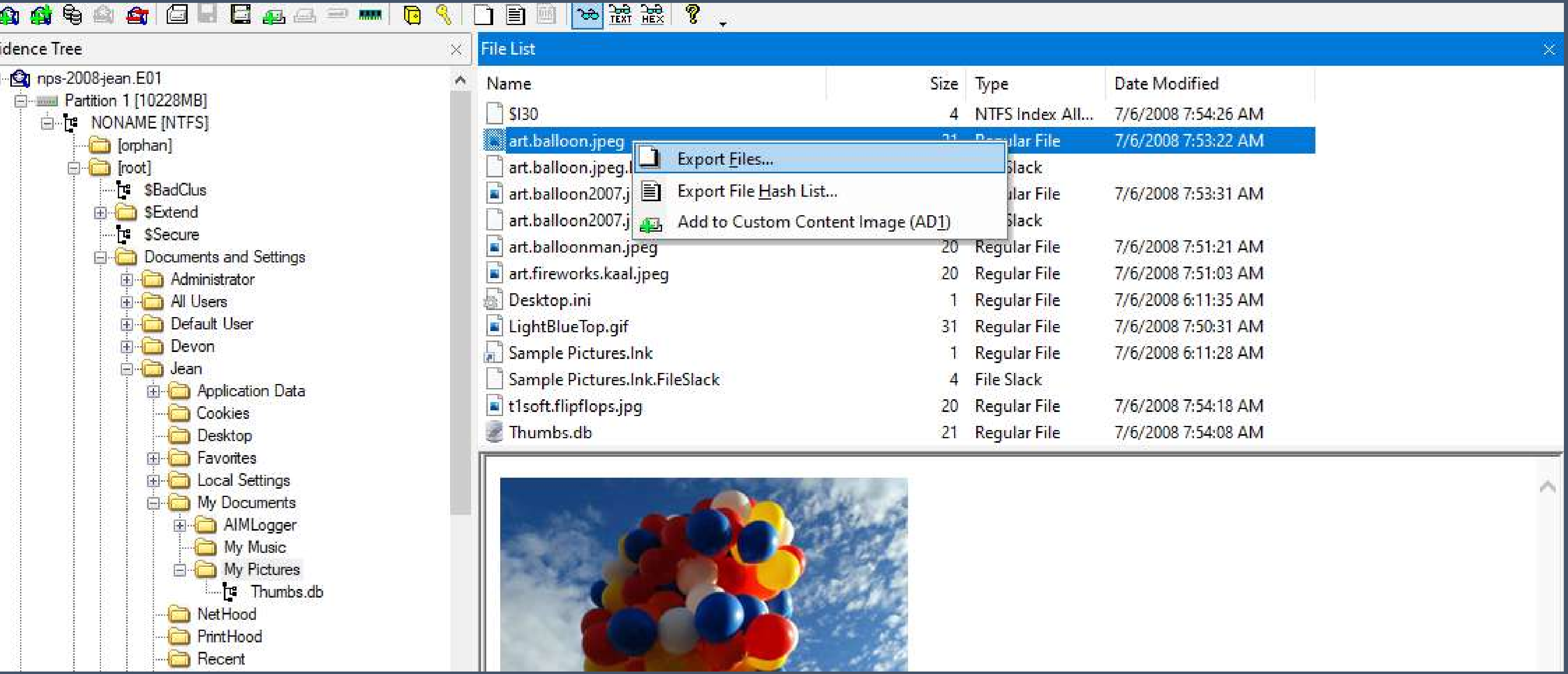
```
nps-2008-jean.E01
  Partition 1 [10228MB]
    NONAME [NTFS]
      [orphan]
      [root]
        $BadClus
        $Extend
        $Secure
        Documents and Settings
          Administrator
          All Users
          Default User
          Devon
          Jean
            Application Data
            Cookies
            Desktop
            Favorites
            Local Settings
            My Documents
              AIMLogger
              My Music
              My Pictures
                Thumbs.db
            NetHood
            PrintHood
            Recent
            SendTo
            Start Menu
```

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.lnk	1	Regular File	7/6/2008 6:11:28 AM
Sample Pictures.lnk.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



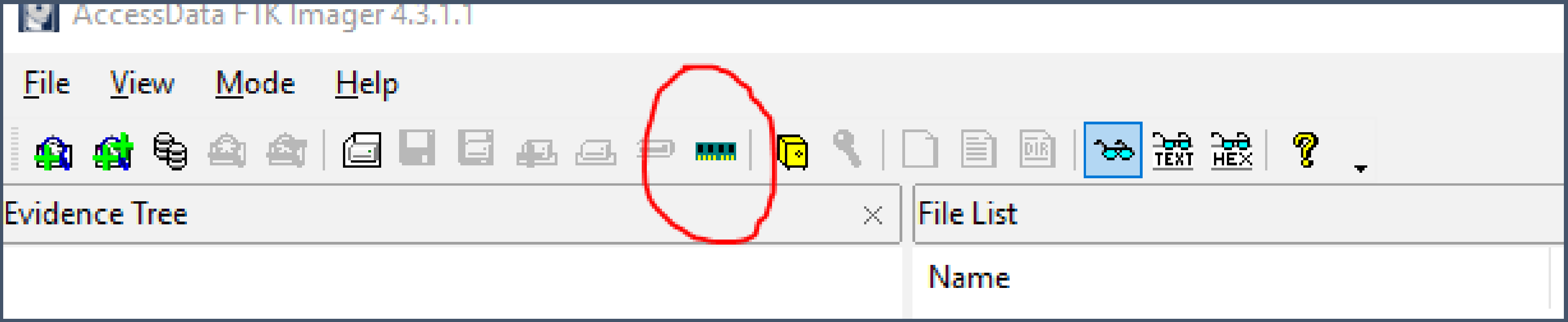
Name	Size	Type	Date Modified
$I30	4	NTFS Index All...	7/6/2008 7:54:26 AM
art.balloon.jpeg	21	Regular File	7/6/2008 7:53:22 AM
art.balloon.jpeg.l		Slack	
art.balloon2007.j		lar File	7/6/2008 7:53:31 AM
art.balloon2007.j		Slack	
art.balloonman.jpeg	20	Regular File	7/6/2008 7:51:21 AM
art.fireworks.kaal.jpeg	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.lnk	1	Regular File	7/6/2008 6:11:28 AM
Sample Pictures.lnk.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

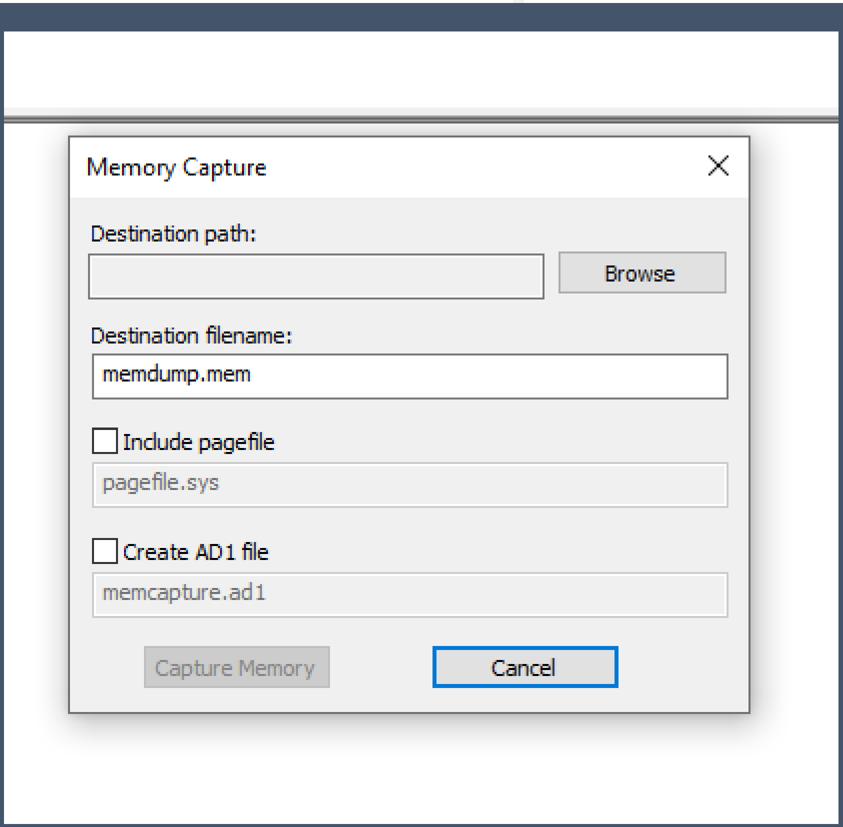
Select file - > Right click
Select destination for exported file

Live Demonstration

Export Files

Create a Memory Capture




Memory Capture

Destination path:

Browse

Destination filename:

memdump.mem

□ Include pagefile

pagefile.sys

□ Create AD1 file

memcapture.ad1

Capture Memory

Cancel

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