FORGE INSTITUTE

FORGE INSTITUTE ARKANSAS CYBER STRIKE TEAM TRAINING

Digital Forensics

© 2020 Forge Institute | Confidential & Proprietary. Do Not Distribute

FTKImager

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

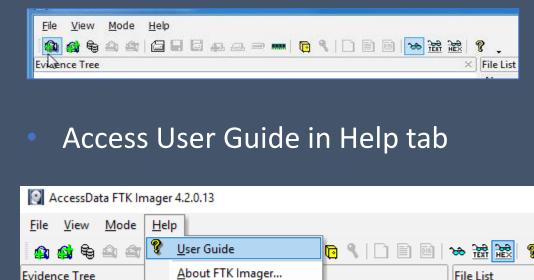


🔯 AccessData FTK Imager 4.2.0.13					-	×
<u>File View Mode</u> <u>H</u> elp						
\$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$	🖻 🐱 👬 📆 🦿 🖕					
Evidence Tree	File List					×
	Name	Size Ty	/pe	Date Modified		
Custom Content Sources						
Evidence:File System Path File Options						
						_
<	>					
New Edit Remove All Create Image						
-						 ~

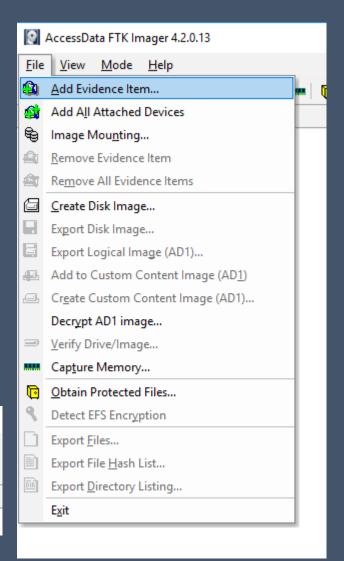
FTK Imager Interface

Options in FTK Imager

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



Name



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
<u>c</u> i	Add All Attached Devices
à	Image Mounting. Opens the Map Image to Drive dialog.
a	Remove Evidence Item
a	Remove All Evidence Items
	Create Disk Image
H	Export Disk Image
	Export Logical Image (AD1)
<u>i</u>	Add to Custom Content Image (AD1)
	Create Custom Content Image (AD1)
-	Verify Drive/Image
	Capture Memory

Ř	MetaCarve (Deep Scan)
	Obtain Protected Files
<mark>9</mark> .	Detect EFS Encryption
Ĩ	Export Files
Ĩ	Export File Hash List
<u>PIR</u>	Export Directory Listing
æ	Choose IE, text, or hex viewer automatically
	View files in plain text
HEX	View files in hex format
Ŷ	Open FTK Imager User Guide

Adding Evidence Item

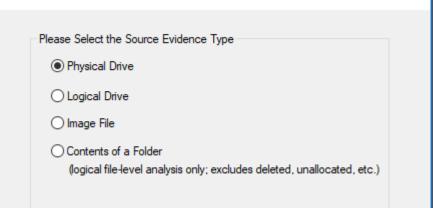
To add an evidence item to the Evidence Tree Click File>Add Evidence OR Click the Add Evidence Item button a on the Toolbar.

Select Source



Select Source Type

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



х

Select Source Evidence Type

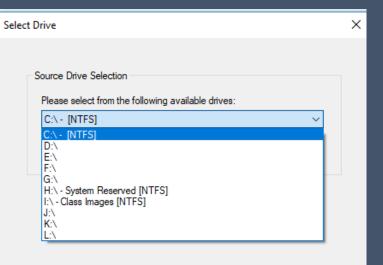
Physical Drive

lease select from the fo	- OCZ-VECTOR ATA Device	1256GB IDE -
\.\PHYSICALDRIVE1	OCZVECTOR ATA Device WDC WD20EZRX-00DC08 WDC WD1002FAEX-00Z3 WDC WD20EZRX-00DC08	BO ATA Device [2 AO ATA Device [

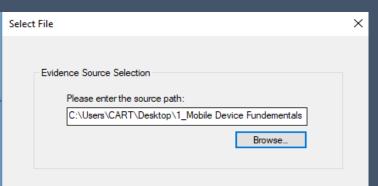
Image File

Select File	\times
Evidence Source Selection Please enter the source path: I:\Class_Images\DEXT\Images\Bryant\QHQ1\QHQ1.E01 Browse_	

Logical Drive



Contents of a Folder



FTK Imager with Evidence Added

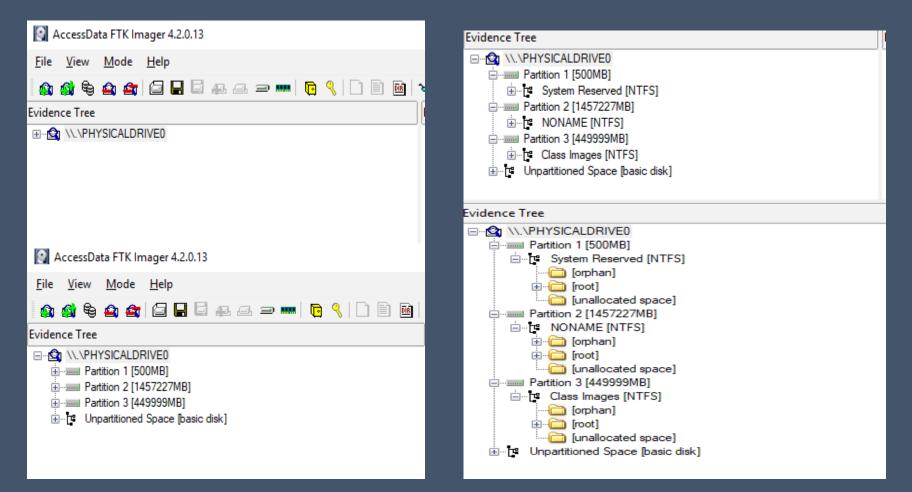
Evidence Item appears in the Evidence Tree.

Properties give important information needed to complete catalog step.

	l 💷 📟 📘 🥄 🗋 🗎 🗃 🐱 😹 😹		
Evidence Tree		File List	
		Name Size Type Date Modified	
Properties 11 2↓		×	
₽ 2↓		×	
2↓ Evidence Source Path	\\-\PHYSICALDRIVE1 Physical Disk	×	1
₽ 2↓	\\.\PHYSICALDRIVE1 Physical Disk	00000000010 06 B9 00 02 FC F3 A4 50-68 1C 06 CB FB B9 04 00	
2 ↓ Evidence Source Path Evidence Type Disk		00000000010 06 B9 00 02 FC F3 A4 50-68 1C 06 CE FB B9 04 00 - → → → → → → → → → → → → → → → → →	
2↓ Evidence Source Path Evidence Type		00000000010 06 B9 00 02 FC F3 A4 50-68 1C 06 CB FB B9 04 00 - ¹ .·ūó×Ph.·Ěů ¹ 00000000020 BD BE 07 80 7E 00 00 7C-0B 0F 85 0E 01 83 CS 10 ₩4 ·····Å. 0000000030 E2 F1 CD 18 88 56 00 55-66 46 11 05 C6 46 10 00 åñī.····UEF.·EF.· 00000000040 B4 41 BB AA 55 CD 13 5D-72 0F 81 FB 55 AA 75 09 ¹ As ⁴ UĨ·Jr.·du ² u.	
2 ↓ Evidence Source Path Evidence Type Disk Disk Drive Geometry	Physical Disk	$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$	
2 ↓ ↓ Evidence Source Path Evidence Type Disk Drive Geometry Cylinders Tracks per Cylinder	Physical Disk 243,201	$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$	
2 2↓ Evidence Source Path Evidence Type Disk Disk Cylinders	Physical Disk 243,201 255	$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$	
	Physical Disk 243,201 255 63	00000000010 06 B9 00 02 FC F3 A4 50-68 1C 06 CF FB B9 04 00 ······àsFh-·Èà······À 00000000020 BD BE 07 80 7E 00 00 7C-0B 0F 85 0E 01 83 C5 10 M4À 00000000030 EZ F1 CD 18 85 56 00 55-C6 46 11 05 C6 46 10 00 ff. ···UEF··EF·· \mathbf{M4A 00000000030 EZ F1 CD 18 85 56 00 55-C6 46 11 05 C6 46 10 00 74 \mathbf{m4A \mathbf{m4A 00000000040 B4 41 BB A4 55 CD 13 5D-72 0F 81 FB 55 AA 75 09 \mathbf{m4A \mathbf{m4A \mathbf{m4A 00000000050 F7 C1 01 00 74 03 FE 46-10 66 60 80 7E 10 00 74 \mathbf{m4A \mathbf{m4	
2 ↓ 2 ↓ Evidence Source Path Evidence Type Disk Disk Cylinders Tracks per Cylinder Sectors per Track Bytes per Sector	Physical Disk 243,201 255 63 512	$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$	
	Physical Disk 243,201 255 63 512	$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$	
	Physical Disk 243,201 255 63 512 3,907,029,168	$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$	
	Physical Disk 243,201 255 63 512 3,907,029,168 WDC WD20EZRX-00DC0B0 ATA Device	$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$	
	Physical Disk 243,201 255 63 512 3,907,029,168 WDC WD20EZRX-00DC080 ATA Device WD-WCC300583085	$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$	
 2↓ Evidence Source Path Evidence Type Disk Drive Geometry Cylinders Tracks per Cylinder Sectors per Track Bytes per Sector Sector Count Physical Drive Information Drive Serial Number Drive Interface Type 	Physical Disk 243,201 255 63 512 3,907,029,168 WDC WD20EZRX-00DC0B0 ATA Device WD-WCC300583085 IDE	$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$	

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.



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)	
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	

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

Select Image Type

Se	lect Image Type	\times
	Please Select the Destination Image Type	
	O Raw (dd)	
	● E01	
	OAFF	
-	< 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 Informat	ion	\times
Case Number: Evidence Number:]
Unique Description:]
Examiner:]
Notes:]
2		
<	Back Next > Cancel Help	
Evidence Item Informat	ion	Х
		×
Evidence Item Informat Case Number:	ion 305C-HQ-54464560	×]
		×]
Case Number:	305C-HQ-54464560]
Case Number: Evidence Number:	305C-HQ-54464560 QHQ1]
Case Number: Evidence Number: Unique Description:	305C-HQ-54464560 QHQ1 (roshiba 500GB hard drive, serial number: 0812WER4]
Case Number: Evidence Number: Unique Description: Examiner:	305C-HQ-54464560 QHQ1 (roshiba 500GB hard drive, serial number: 0812WER4]
Case Number: Evidence Number: Unique Description: Examiner:	305C-HQ-54464560 QHQ1 (roshiba 500GB hard drive, serial number: 0812WER4]
Case Number: Evidence Number: Unique Description: Examiner:	305C-HQ-54464560 QHQ1 (roshiba 500GB hard drive, serial number: 0812WER4]
Case Number: Evidence Number: Unique Description: Examiner:	305C-HQ-54464560 QHQ1 (roshiba 500GB hard drive, serial number: 0812WER4]

Select Image Destination

Select Image Destination	×
Image Destination Folder	
Image Filename (Excluding Extension)	
Image Fragment Size (MB) 1500 For Raw, E01, and AFF formats: 0 = do not fragment 1500 Compression (0=None, 1=Fastest,, 9=Smallest) 6 Use AD Encryption	
< Back Finish Cancel Help	

elect Image Destination	×	
Image Destination Folder		
C:\Users\CART\Desktop\CASES\QHQ1 Browse		
Image Filename (Excluding Extension)		
QHQ1Image		
Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment Compression (0=None, 1=Fastest,, 9=Smallest)		Selec Finisl
USE AD EICH PURCH		
	_	
< Back Finish Cancel Help		
Image Source	×	
M:\		
Starting Evidence Number: 1		
Image Destination(s) C:\Users\CART\Desktop\CASES\QHQ1\QHQ1 Image [E01]		
בי שפר פיטרורי שבפונטא עבורבי על ולד ולג ולד דווספר (רס ד)		Select
		Start
Add Edit		
Add Overflow Loc		
Verify images after they are creat		
✓ Create directory listings of all files in the image after they are created		
Start Cancel		
	_	13

Creating Image

Creating Image	[2%] — 🗆 🗙
Image Source Destination: Status: Progress	M:\ C:\Users\CART\Desktop\CASES\QHQ1\QHQ1 Image Creating image 156.03 of 7701.06 MB (19.504 MB/sec)
	bsed time: 0:00:08 mated time left: 0:06:26
	Cancel

Pre-calculate Progress Statistics

Creating Image (100%)

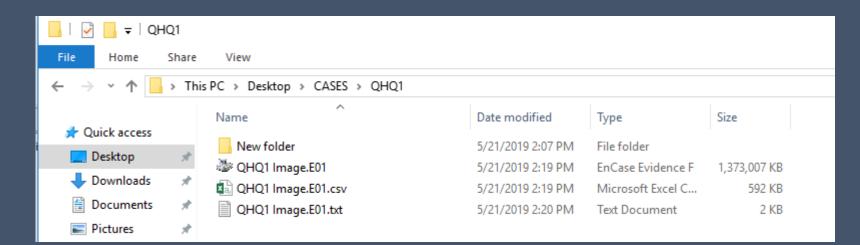
Creating Image	[100%]		_		×
Image Source:	M:\				
Destination:	C:\Users\CART\	Desktop\CASES\Q	HQ1\QHC	(1 Image	
Status:	Image created s	uccessfully			
Progress					
	7701.06 of 770	1.06 MB (18.120 M	B/sec)		
Elap	sed time:	0:07:05			
Estin	nated time left:	0:00:00			
Image Summar	y	Close			

- 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
	Close
Drive/Image Verify Results	
Drive/Image Verify Results	
Name Sector count	
Name Sector count MD5 Hash	QHQ1 Image.E01 1570 Tes
Name Sector count	QHQ1 Image.E01
Name Sector count MD5 Hash Computed hash Stored verification hash	QHQ1 Image.E01 1577.000 e7ceaef20a2e2be0994945a1a5776e37 e7ceaef20a2e2be0994945a1a5776e37
Name Sector count MD5 Hash Computed hash Stored verification hash Report Hash	
	QHQ1 Image.E01 1577.000 e7ceaef20a2e2be0994945a1a5776e37 e7ceaef20a2e2be0994945a1a5776e37
Name Sector count MD5 Hash Computed hash Stored verification hash Report Hash Verify result SHA1 Hash	
Name Sector count MD5 Hash Computed hash Stored verification hash Report Hash Verify result SHA1 Hash Computed hash	
Name Sector count MD5 Hash Computed hash Stored verification hash Verify result SHA1 Hash Computed hash Stored verification hash	- QHQ1 Image.E01 1575.0.65 e7ceaef20a2e2be0994945a1a5776e37 e7ceaef20a2e2be0994945a1a5776e37 e7ceaef20a2e2be0994945a1a5776e37 e7ceaef20a2e2be0994945a1a5776e37 Match 05ccbo555049fd0facb853d8fb78314b03b116961 05ecb655b49fd0facb853d8fb78314b03b116961
Name Sector count MD5 Hash Computed hash Stored verification hash Report Hash Verify result SHA1 Hash Computed hash	
Name Sector count MD5 Hash Computed hash Stored verification hash Verify result SHA1 Hash Computed hash Stored verification hash	- CHQ1 Image.E01 1575.0.65 e7ceaef20a2e2be0994945a1a5776e37 e7ceaef20a2e2be0994945a1a5776e37 e7ceaef20a2e2be0994945a1a5776e37 e7ceaef20a2e2be0994945a1a5776e37 Match 05ccb0555049fd0facb853d8fb78314b03b116961 05ecb655b49fd0facb853d8fb78314b03b116961
Name Sector count MD5 Hash Computed hash Stored verification hash Report Hash Verify result SHA1 Hash Computed hash Stored verification hash Report Hash	- QHQ1 Image.E01 1570.00 e7ceaef20a2e2be0994945a1a5776e37 e7ceaef20a2e2be094945a1a5776e37 e7ceaef20a2e2be094945a1a5776e37 e7ceaef20a2e2be094945a1a5776e37 e7ceaef20a2e2be094945a1a5776e37 e7ceaef20a2e2be094945a1a5776e37 e7ceaef20a2e2be094945a1a5776e37 e7ceaef20a2e2be094945a1a5776e37 e7ceaef20a2e2be094945a1a5776e37 e7ceaef20a2e2be094945a1a5776e37 e7ceaef20a2e2be094945a1a5776e37 e7ceaef20a2e2be094945a1a5776e37 e7ceaef20a2e2be094945a1a5776e37 e7ceaef20a2e2be094945a1a5776e37 e7ceaef20a2e2be094445a1a576e37 e7ceaef20a2e2be094445a1a576e37 e7ceaef20a2e2be094445a1a576e37 e7ceaef20a2e2be094445a1a576e37 e7ceaef20a2e2be09445a1a576e37 e7ceaef20a2e2be094445a1a576e37 e7ceaef20a2e2be094445a1a576e37 e7ceaef20a2e2be094445a1a576e37 e7ceaef20a2e2be094445a1a576e37 e7ceaef20a2e2be094445a1a576e37 e7ceaef20a2e2be094445a1a576e37 e7ceaef20a2e2be094445a1a576e37 e7ceaef20a2e2be094445a1a576647 e7ceaef20a2e2be094445a1a576647 e7ceaef20a2e2be094445a1a57

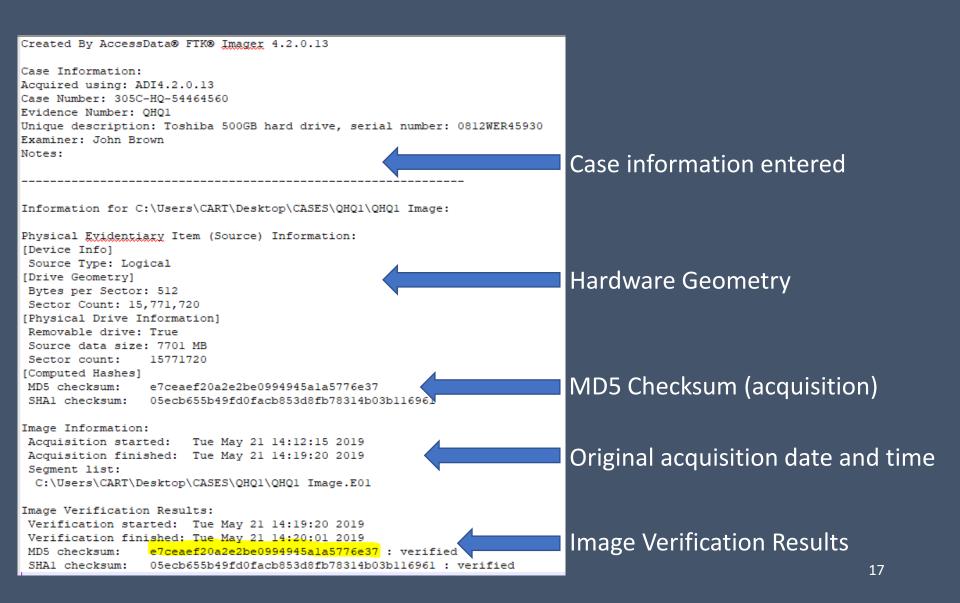
Close

Image Verification Log



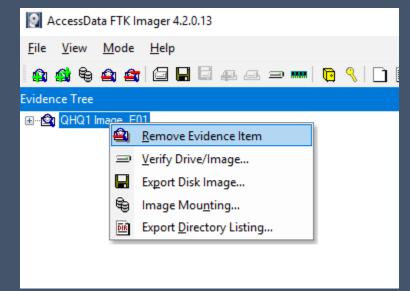
- Locate image file created
- Open Text File (QHQ1 Image.E01.txt)

Image Verification Log

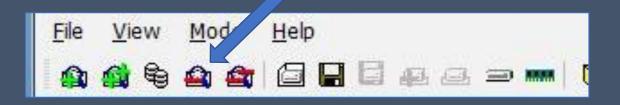


Remove Evidence

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

Accer data FTK Imager 4.2.0.13	
<u>File</u> w <u>M</u> ode <u>H</u> elp	
😫 🏘 🗣 🗠 👉 🖾 🖬 🖬 🖬 🗛 🚙 📟 🖪 🔁 化	
Evidence Tree Add Evidence Item	
Select File X	
Evidence Source Selection Please enter the source path: C:\Users\CART\Desktop\CASES\QHQ1\QHQ1 Image .El Browse	 Add Evidence Select Image File Click Next Select file of previously created image Click Finish
S buok million Canoor Molp	

Verify Drive/Image

AccessData FTK Imager 4.2.0.13	
<u>F</u> ile <u>V</u> iew <u>M</u> ode <u>H</u> elp	
🏩 🏩 😂 😂 🖾 🖬 🖾 🖬 🗁 📨 🖛 📴 🔍 🗋 🗎 🗎	च्छे हेल्हे हेल्हे 😵
Evidence Tree	
⊞ 😭 QHQ1 Image .E01	
AccessData FTK Imager 4.2.0.13	
<u>F</u> ile <u>V</u> iew <u>M</u> ode <u>H</u> elp	
🏩 🔩 😂 🚔 🗁 🖬 🗔 42 a a a an in 🦻 🔍 🗋 🗎 🔤 😒	
Evidence Tree	
B 😰 QHQ1 Image F01 and Remove Evidence Item	
Verify Drive/Image	
Export Disk Image	
B Image Mounting	🔳 Dri
Export Directory Listing	
	N
Verifying [29%] — 🗆 🗙	Se
Source Drive/Image: QHQ1 Image .E01	St
Progress	Re
	- Ve □ SI
1137.06 of 3819.00 MB verified (162.437 MB/sec)	
Elapsed time: 0:00:07	St
Estimated time left: 0:00:16	
Cancel	

Right click image file

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

	and the set				<u> </u>
в	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	05ecb655b49fd0facb853d8fb78314b03	3b11696	1	
	Stored verification hash	05ecb655b49fd0facb853d8fb78314b03	3b11696	1	~

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] e7ceaef20a2e2be0994945a1a5776e37 MD5 checksum: 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: e7ceaef20a2e2be0994945ala5776e37 : verified SHAl 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: e7ceaef20a2e2be0994945ala5776e37 : verified SHAl checksum: 05ecb655b49fd0facb853d8fb783l4b03bl16961 : verified Original Acquisition date and time

Verification Results

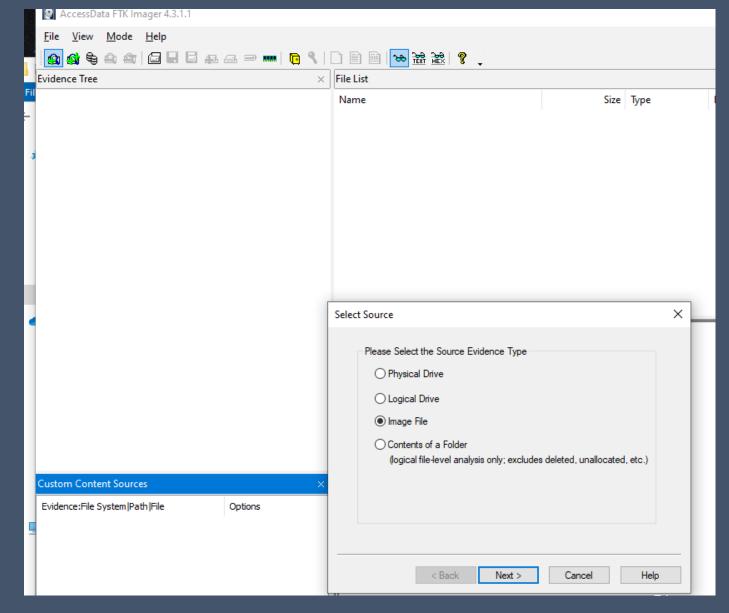
Verification Results appended to log file

Live Demonstration Verify an Image File Verification Log Append

Export Files in FTK Imager

Add Evidence

Select Image File



Export Files in FTK Imager

AccessData FTK Imager 4.3.1.1 <u>File View Mode Help</u> 🏩 🏩 🗣 🚔 🔚 🔚 🔚 🚛 🖅 🧰 🣴 🥄 🗋 🗎 🔤 🐱 😹 🦹 🢡 🖕 Evidence Tree File List Fil Date Modified Name Size Type Partition 1 [10228MB] ← **\$I30** 4 NTFS Index All... 7/6/2008 7:54:26 AM NONAME [NTFS] art.balloon.jpeg 21 Regular File 7/6/2008 7:53:22 AM (orphan) 🗄 🦳 [root] art.balloon.jpeg.FileSlack 4 File Slack \$BadClus art.balloon2007.jpeg 21 Regular File 7/6/2008 7:53:31 AM SExtend art.balloon2007.jpeg.FileSlack 4 File Slack Secure \$ art.balloonman.jpeg 20 Regular File 7/6/2008 7:51:21 AM - Documents and Settings art.fireworks.kaal.jpeg 20 Regular File 7/6/2008 7:51:03 AM Administrator 🔊 Desktop.ini 7/6/2008 6:11:35 AM All Users 1 Regular File 🗄 🦳 Default User LightBlueTop.gif 31 Regular File 7/6/2008 7:50:31 AM 🗄 🦳 Devon Sample Pictures.Ink 1 Regular File 7/6/2008 6:11:28 AM 🚊 🛅 Jean Sample Pictures.Ink.FileSlack 4 File Slack Application Data t1soft.flipflops.jpg 20 Regular File 7/6/2008 7:54:18 AM Cookies Thumbs.db 21 Regular File 7/6/2008 7:54:08 AM Desktop Havorites 00 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00 0 0..... E Local Settings 10 10 00 00 00 28 00 00 00-28 00 00 00 01 00 00 00(..... My Documents 20 00 00 00 00 00 00 00 00-18 00 00 03 00 00 00 AIMLogger 30 00 00 00 00 00 00 00 00-My Music My Pictures Thumbs.db NetHood PrintHood Recent SendTo 🗄 🦳 Start Menu

Traverse through the + symbols down to files to be exported

Export Files in FTK Imager

a 🟟 🗣 🗠 🚘 🖾 🖶 🗳 🚛 🗁 🚥 </u> 🧟 🦿 🌆 🔁 🔛 🚬

idence Tree	× File List					×
⊷ 💁 nps-2008-jean.E01	^ Name		Size	Туре	Date Modified	
⊡	\$130		4	NTFS Index All	7/6/2008 7:54:26 AM	
······································	art.balloon.jpeg		21	Pular File	7/6/2008 7:53:22 AM	
ie [root]	📄 art.balloon.jpeg.l 🖵	Export <u>F</u> iles		Slack		
	ब art.balloon2007.j 🗎	Export File <u>H</u> ash List		ılar File	7/6/2008 7:53:31 AM	
iaicii \$Extend ti≇ \$Secure	📄 art.balloon2007.j 🚌	Add to Custom Content Image	e (AD <u>1</u>)	Slack		
⊡⊡ Documents and Settings	📓 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	
🗄 🖓 🧰 All Users	🔄 Desktop.ini		1	Regular File	7/6/2008 6:11:35 AM	
⊕ 🛅 Default User	🔳 LightBlueTop.gif		31	Regular File	7/6/2008 7:50:31 AM	
🗄 😁 🛅 Devon	📄 Sample Pictures.Ink		1	Regular File	7/6/2008 6:11:28 AM	
iaian Jean iaian Application Data	Sample Pictures.Ink.Fil	eSlack	4	File Slack		
Cookies	🔳 t1soft.flipflops.jpg		20	Regular File	7/6/2008 7:54:18 AM	
🛅 Desktop	🖉 Thumbs.db		21	Regular File	7/6/2008 7:54:08 AM	
Favorites Favorites Local Settings My Documents My Music My Pictures My Pictures	2					^

Select file - > Right click Select destination for exported file

26

Live Demonstration Export Files

Create a Memory Capture

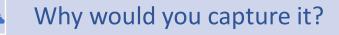
2 /	AccessDa	ita FIK Im	ager 4.3.1	.1					
<u>F</u> ile	<u>V</u> iew	<u>M</u> ode	<u>H</u> elp		\bigcap	1			
	😫 😫	()	a I	886	a 🗇 📖	•)	•		🗋 🖻 🐱 😹 📆 💡 🖕
Evider	nce Tree					J		×	File List
									Name

Memory Capture	×
Destination path:	
	Browse
Destination filename:	
memdump.mem	
Include pagefile	
Include pagefile pagefile.sys	
pagefile.sys	
pagefile.sys	

Create a Memory Capture



What is pagefile.sys?





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

Live Demonstration Memory Capture