

ACCESSIONING FILES FROM EXTERNAL DRIVE

CONTENTS

Ι.	Basic Workflow	1
II.	Unique Identifier	. 2
III.	Write-Blocking	2
IV.	Virus Scans	. 4
V.	File Transfer	. 5
A.	Bagger	5
В.	FTK Imager	5
VI.	File Export from Image	8
A.	E01	8
В.	AD1	12
VII.	Documentation	14
VIII.	Handling of Drive Post-Digital Capture	15
Арре	endix. Troubleshooting	15
A.	Bagger issues	15
В.	Computer doesn't recognize drive	17

This document provides guidance on accessioning external drives. This encompasses USB flash drives (also known as thumb drives and jump drives) and external hard drives that connect to a computer by a USB or FireWire cable.

- I. BASIC WORKFLOW
- 1. Assign a unique identifier to the drive.
- Plug drive into Tableau write-blocker on your computer or on Fluffy. Note: You may plug drive into UltraBay of FRED but you will be limited to creating an image of files on the drive.
- 3. Scan the drive for viruses. Record virus scan results and actions as Virus Check event in ASpace.
- 4. Transfer files from drive using Bagger and save in "[accession #]_original" folder on ira_locked. Validate bag and maintain files in bag.

Note: If Bagger does not work or it is impractical to use Bagger, use FTK Imager to create an AD1 or EO1 image. Export files from AD1 images as soon as possible using FTK Imager. Only export files from EO1 images after files have been appraised and non-archival files have been identified in Forensic Toolkit.



- If on networked computer save exported files directly in "[accession #]_original" folder on ira_locked and bag files in place using Bagger. Validate bag and maintain files in bag.
- If working on Fred or Fluffy, save exported files on external drive and use Bagger to transfer files to "[accession #]_original" folder on ira_locked. Validate bag and maintain files in bag.
- 5. Record actions in Digital File Management Note of accession record in ASpace.
- 6. Place drive in an external drive "shred" box or retain in collection.
- II. UNIQUE IDENTIFIER

Assign each disc a unique identifier following the format that applies to your scenario. You may need to use a mix of formats within a single accession. Make sure you do not duplicate identifiers used for other digital storage media in the accession. Use the unique identifier as the filename for disk images and folder name for exported files.

Scenario	Unique Identifier
Accession consists entirely of a single external drive.	[accession #]
	22
- A	Example: 2016ia38
External drive does not need to be retained and it is not	[accession #]_i[item number]
necessary to record its original physical context.	
City City City City City City City City	Example: 2016ia38_i02
This applies to:	
-hybrid collections with one or multiple drives or multiple	
types of digital storage media	
-purely digital accessions with multiple drives or multiple	
types of digital storage media.	
External drive is to be retained.	[accession #]_b[box #]_i[item #]
or R	Example: 2016ia38_b02_i01
Sr	
External drive is not to be retained but the original physical	Note: Item numbering should
context needs to be recorded.	restart from 01 with each box.

III. WRITE-BLOCKING

Whenever possible, connect the external drive to your computer using the Tableau USB bridge for writeblocking protection. The Tableau device is stored in a box next to Fluffy and can be used on any computer. You may also connect the external drive to FRED through the UltraBay, which has a built-in write blocker, but you will only be able to use FTK Imager and not Bagger to transfer files.

Tableau USB Bridge.



- 1. Connect Tableau device to power source.
- 2. Connect external drive to Tableau device. Only connect one drive at a time.
- 3. Connect Tableau device to computer.
- 4. Power on Tableau device. "USB device recognized" should flash by on the screen and the write block light should be green. The external drive should appear in file explorer.



5. To remove the external drive, eject the Tableau device using the Safe Remove Hardware utility on your computer. Turn the Tableau device off and remove the external drive.

FRED UltraBay

Note: By connecting through the UltraBay, the external drive will not appear in file explorer. You will only be able to copy content from the drive by using FTK Imager to create an image.

- 1. Confirm that the UltraBay is off (led lights are off) and connect the external drive.
- 2. Power on the UltraBay, the Act light should come on if the UltraBay recognizes the drive.



IV. VIRUS SCANS

Run a virus scan on the external drive before transferring or examining files. For certain drives, virus scans may not be necessary if we know the drive was created on virus-free computers. Keep in mind that although Getty computers are regularly scanned for viruses, we cannot always assume that drives transferred to us by staff were created on Getty computers. In addition, we have come across malware on staff computers that were not recognized by the antivirus program.

- 1. Right-click the external drive in file explorer and select Scan for threats. Do not open any of the files before you have verified that the drive is virus free.
- 2. A message box will appear. Select **Continue** and the virus scan will begin.

Scan for threats	
Select the desired action when a detection is found. Report and Clean or report and Continue without cleaning.	Clean Continue
	0

 If one or more viruses are found, save a log of the infected files in the accession's documentation folder on ira_locked according to the following format: [unique identifier]_viruslog.

There are four options for dealing with infected files:

(1) Working on Fluffy, transfer files with Bagger to an empty external drive. Run a virus scan on the bag and have the antivirus program "clean" the infected file. Make sure the antivirus software is up-to-date and that the Ethernet cord is disconnected before connecting the external drive through the Tableau device.

(2) Exclude infected files from Bagger transfer. To do this simply click on the file in the payload and click • to remove from the list.

Create <u>N</u> ew Bag	Open Existing Bag	Create Bag
📀 Bagger		- 0 :
Payload		0
🖃 🗁 data		-
🗄 🗁 BornDig	ital	
🖨 🗁 Read	ingNotes_and_Resou	rces
🕀 🖾 Ei	mail	
🕀 🗀 St	trategic plan	
🗅 🗚	IMS2.and.docx	
🗋 B	aggerForCAD_instruc	tions_v4.pp
l in d	المرجان فيرجع والمراب المراب	

(3) If cleaning the infected file is not an option and it needs to be retained, create an EO1 image of the drive and only access the infected file through Forensic Toolkit.

(4) Do not accession the drive.

Before proceeding, consult with the Head of Institutional Archives.

4. Record virus scan results (even if no virus was found) and actions as a Virus Check event in the accessions record of ASpace. See <u>section VII</u>.

V. FILE TRANSFER

There are two methods for copying content off external hard drives.

- 1. Transfer files using Bagger.
- 2. Create image using FTK Imager.

As a general rule, use Bagger to transfer files off external drives. If you encounter problems using Bagger that cannot be resolved after consulting the Troubleshooting section, use FTK Imager to create an image.

A. BAGGER

See <u>Bagger_User_Guide.pdf</u> for guidance on using the software.

- 1. Run Bagger to transfer files from external drive to "[accession #]_original" folder on ira_locked.
- 2. Use unique identifier for the bag name.
- 3. Validate the bag to verify files were properly transferred. Maintain files in bag.
- B. FTK IMAGER

Use FTK Imager if you are unable to transfer files using Bagger or it is impractical. Create an **E01** image if the files are too large to transfer with Bagger or you do not plan to immediately export files from an image. Only create an **AD1** image if you plan to export files from the image immediately.

- 1. Click on **Create mage** in the file drop-down menu.
- 2. You will be presented with the following source options:



Select S	jource
Г	Please Select the Source Evidence Type
	C Physical Drive
	Cogical Drive
	C Image File
	C Contents of a Folder (logical file-level analysis only; excludes deleted, unallocated, etc.)
	< Back Next > Cancel Help

If creating AD1: Select **Contents of a Folder**. You may see a message sking you to confirm if you Lal Q Cro Kr want to create a logical image (not to be confused with logical diffe). Click Yes.

If creating E01: Select Logical Drive.

Click Next.

- **3.** Select a drive to image and click **Finish**.
- 4. The Create Image screen will appear. Coeck off Verify images after they are created and Create directory listings. Check off Precalculate Progress Statistics if you would like an estimate of how long it will take to image the drive.

	Createdmage	8
	Ofmage Source	_
	Γκ:\	-
A	Starting Evidence Number: 1	
SY	Image Destination(s)	- 1
		-
	Add Edit Remove	
	Add Overflow Location	
	✓ Verify images after they are created	
	$\overline{ec{v}}$ Create directory listings of all files in the image after they are created	
	Start Cancel	





- Click Add. If you selected Logical Drive, you will select E01 for image destination type and click Next.
- In the evidence item information window, enter the following: Case Number: Unique identifier for external drive Examiner: Name of archivist performing imaging

Evidence Item Informat	ion 🗾
Case Number: Evidence Number: Unique Description: Examiner:	2016ia87_b05_j01
Notes:	
	and the second se
	4 tal
	Next > Cancel O Help
	On:

7. Click **Next** and the Select Image Destination screen with come up.

Image Destination Folder: Select the save location for the image file. If working on FRED or Fluffy, save the files on an external hard drive to facilitate file transfer to a networked computer. Make sure there is sufficient room on the external hard drive for the image. If imaging the drive on a networked computer, save the files in "[accession #]_original" folder on ira_locked.

Image Filename: Enter the unique identifier as the filename (excluding the extension).

Image fragment size:

AD1: Enter 4095 for the maximum fragment size, 3.99GB. If creating an image for a set of files larger than 3.99GB, the image will be broken into multiple AD files.



Compression: 5

Click Finish.



Select Image Destination
Image Destination Folder I:\ira_locked\2016\2016ia87\2016ia87_orig Browse
Image Filename (Excluding Extension)
2016ia87_b02_i01
Image Fragment Size (MB) [1500 For Raw, E01, and AFF formats: 0 = do not fragment
Compression (0=None, 1=Fastest,, 9=Smallest) 5
Use AD Encryption
Filter by File Owner
< Back Finish Cancel Help

- 8. You will return to the Create Image screen. There should now be a location listed under Image Destination(s). Click Start to begin imaging and a window with a progress bar will appear. The status message will change to "Image created successfully" once maging has completed. You may click Close. , Norking
- VI. FILE EXPORT FROM IMAGE

A. E01

Use Forensic Toolkit to export files from E01 images. Note: If an E01 image was created due to size issues, do not export the files until they have been appraised and non-archival files have been identified in Forensic Toolkit.

See section III.B. of IA Electronic record accessioning.pdf for more thorough guidance on using Forensic Toolkit. You can use Forensic Toolkit on either Fluffy or FRED, but this will ultimately require using Bagger for transferring files to palocked. If there were problems using Bagger before that cannot be easily resolved, you may need to use Forensic Toolkit on a networked computer to export files directly to ira locked.

1. Go to toolbar and click on Case.

AccessData For	AccessData Forensic Toolkit Version: 5.0.0.84 Database: localhost			
File Database Case Tools Manage Help				
Cases				
Name	Date Modified	Case ID	40	
2008ia20	6/24/2015 5:40:58 P	Case Owner	admin	
2009ia44	7/20/2015 5:19:17 P	Reference		
2013ia14	9/1/2015 8:55:18 PM	Date Modified	6/24/2015 5:40:58 PM +0	0:00
2015ia02	9/17/2015 3:53:52 P	Date Accessed	9/20/2015 12:01:49 AM +	00:C
MMI	9/22/2015 7:14:59 P	Date Created	6/24/2015 9:01:58 AM +0	D:0C
MMITest	6/9/2015 5:58:31 PM	Case Path	D:\Casefiles\2008ia20)
Michael Brand	7/2/2013 5:39:57 PM	Description File	X	
Terry Ford	7/2/2013 1:38:55 PM	Description		





2. Select New and the New Case Options window will appear.

Fill the following fields:

Case Name: Accession number

Processing Profile: IA default

Click OK.

www Case Options		
Owner:	admin FTK	
Case Name:		
Reference:		
Description:		
Description File:		and,
Case Folder Directory:	F:\6_0_casefiles	10.
Database location		
In the case folder	0.	
Database Directory:		
Processing profile	6	
Forensic processing	eDiscovery Summation Basic Field mode	
	Customize	
User profile:	IA default	
	ction	
	V Open the case	

3. In the Manage Evidence window, click Add.

Manage Evidence			X
Display Name State	Path:		
LSEUM!	ID / Name:		
SPANN	Description:		~ ~
	Evidence Group:		 Manage
	Time Zone:	America/Los_Angeles	٣
		🗖 Merge ca	ase index 🔲 Use UNC Paths
Add Remove		Refinement Options	Language Setting
Case KFF Options			OK Cancel

4. Select Acquired Image and click OK.



Select Evidence Type:	X
Acquired Image(s)	
O All Images in Directory	
Contents of a Directory	
Individual File(s)	
O Physical Drive	
C Logical Drive	
ОК	Cancel

- 5. In the next window navigate to the image of the external drive and click **OK**.
- 6. The file(s)/folder that you selected should now appear in the Manage Evidence window. You may add other images now if needed, but you also have the option of adding additional

	evidence at a later time. Click OK	MAIN 9	
7.	A Data Processing Status window	will appear.	
	Data Processing Status: 5.0.0.84		
	 Add Evidence Jobs <u>2009ia44_02.E01 (Processing)</u> 2009ia44_01.E01 (Processing) Additional Analysis Jobs Live Search Jobs Other Jobs 	Videvidence Progress Overall: Discovered: 359 Processed: Indexed: 0 Process State: Processing	Messages Type Message INFO [11:16 AM 9/29/2015] Using engir INFO [11:16 AM 9/29/2015] Database r INFO [11:16 AM 9/29/2015] Database r INFO [11:16 AM 9/29/2015] Processing
		•	

Processing time will vary depending on the size of the image and may possibly take over an hour. It should only take a few minutes at most, however, for files to load in FTK. While you will be able to examine the contents of files before processing is completed, do not conduct index or live searches or export files until then.

Once the processing job is done, you may want to search for documents with sensitive information or non-archival files to weed (exclude from file export). Otherwise, continue to the next step to export files.

8. To export files, navigate to the Explorer tab. Make sure that all files that you want to export are currently displayed in the File List pane.

If you did not mark any files to ignore, select Actual Files in the filter drop-down menu.



If you did mark files to ignore, use the filter manager to include **Not Flagged Ignorable**, **Actual Files**, and any other filters.

Filter Manager	8
Filters	Include
Name 🛆 🔺	Name
Alternate Data Streams	Actual Files
Archive Files	Not Flagged Ignorable
Bad Extension Files >>	Lit
Bookmarked E	
Carved Files	Q
Cerberus Score	
Cerberus Static Analysis	
Checked Files	
Decrypted Files	
Deleted Files	🖲 AND 🕻 🌒 🕅 🖉 OR 📢 👘 Clear
Duplicate Files	
eDiscovery Refinement w/o OCR	Fund and O
Email Attachments	EXClude
Email Delivery Time	Name
Email Files	
Email Files and Attachments	
Encrypted Files	M I I
Evidence Items	
Excluded eDiscovery Refinement w	
Explicit images folder (high score)	
Explicit images folder (medium score)	
File Category	
File Created Time	
File Extension	CAND () OR () Clear
🕈 👔 🗮 C 🗣 🔿	
Celhae	Apply Close

You can als meselect the 🛸 icon next to a file or folder to exclude from export.

- 9. Once you have finished adjusting the filters so that only the files to be exported are displayed in the File List pane of the Explore view, go to **File** in the menu bar and click **Export**.
- 10. In the Export Window, check off boxes as in image below.

Note: If an image was created due to filenames that are too long, you have the option of checking off **Limit path length**. This will move problem files out of their original hierarchy into a new "[overflow]" folder at the top level. Forensic Toolkit will also generate an overflow log with the original and new path names. Since we ideally want to keep files in their original structure, we will need to shorten the names of problem files and move them back to their original



locations. Consult the Head of Institutional Archives before checking off **Limit path length**. See the <u>Bagger issues</u> section for an alternate method for identifying problem files.

🚥 Export				
File Options				
Append item number to filename	Export emails as MSG			
Append extension to filename if bad/absent	Export emails to PST			
Export children	Preserve folder structure			
Exclude slack space children files	Organization: Separate PST per evidence			
Save HTML view (if available)				
Export using item number for file name	Export messages from email archives to PST			
Export directory as file	Include thumbnails of video files			
Limit path length	Include common video format			
Create manifest files	0			
✓ Include original path	ampi			
_ Items to Include	47			
C All Checked (0)	C All Highlighted (0)			
All Listed (1298) C All				
(Whole disk images, logical images, and partitions are always e	excluded)			
Destination base path:				
M:\				
No				
OK Cancel				
6	2			

- 11. Under Destination base path select an external drive to save the exported files.
- 12. Once you have exported the files, use Bagger to transfer the files from the external drive to "[accession #]_original folder on ira_locked. Validate to confirm files were properly transferred and maintain files in bag.



Use FTK Imager to extract files from an AD1 image. You may use Forensic Toolkit (see <u>above</u>) instead if you would like to search for files with sensitive information and weed non-archival files.

- 1. Click **File** \rightarrow **Add Evidence Item** or click in the toolbar.
- 2. Select Image File and click Next.



Select Source	×
Please Select the Source Evidence Type Physical Drive Logical Drive (o logical Drive (ogical file-level analysis only; excludes deleted, unallocated, etc.)	×.

3. In the next window click Browse and navigate to the AD1 file and click Finish,

Select File
C. C.
Evidence Source Selection
Please enter the source path:
Biowa
- The
ction .
Cancel Help
Chi
P

4. The contents of the image file should now appear in the Evidence Tree pane.



Right-click the folder below the top level. Select Export Files and in the next window select the location to save the files. If working on a networked computer, save the files in "[accession #]_original" folder on ira_locked. If working on FRED or Fluffy, save the files on an external hard drive and then transfer to ira_locked using Bagger.



6. Once export is successfully completed, you should see something like this:



- 7. Right-click the same folder. This time select Export File Hash List. Save the file in the accession's documentation folder on ira_locked. Name the file "[unique identifier]_ftke@port.csv".
- 8. If an image was created due to filenames that are too long, now is the time to fix them. See the -s. orking Group Bagger issues section for guidance on identifying problem files.
- 9. Maintain exported files on ira_locked in bag.
- VII. DOCUMENTATION

In the ASpace accession record use the Digital Files Management Notes field under the User Defined section of the accession record to document the work you've completed, work that needs to be done, and any known issues or problems. Your notes should be clear enough for someone to be able to pick up from where you left off.

Work relating to virus scans should be documented as a Virus Check event. Record virus scan results (even if no viruses were found) and actions as a Virus Check event in the accession record of ASpace. Select the appropriate outcome in the drop-down menu and fill out the Outcome Note if any viruses were found. Include a his in the External Documents section to the infected files logs in the "[accession #]_documentation" folder on ira_locked. If there are multiple drives or other types of media in the accession and only some have been scanned, make sure it is clear in the Outcome note exactly which ones have been scanned.

New Event Event Basic Information Type * Virus Check Ŧ Partial Pass . Outcome Outcome Note Only external drives were scanned. Two infected files in 2016ia38 b02 i01. Files were cleaned by McAfee antivirus program. One infected file in 2016ia38 b02 i02. File excluded from export in Forensic Toolkit.

VIII. HANDLING OF DRIVE POST-DIGITAL CAPTURE

Institutional Archives views external drives as physical carriers that, in most cases, do not hold artefactual value. Once we have captured and preserved the digital content off a drive, the drive can be placed in an External Drive "shred" box. When the box is full, we will contact Shane Greene (ITS), who has a hard drive degausser.

While rare, there may be certain circumstances in which wedecide to retain an external drive. Flash In Archives Section drives with custom labeling, for example, may warrant retention. Consult the Head of Institutional Archives as necessary.

APPENDIX. TROUBLESHOOTING

A. BAGGER ISSUES

Too large. If the set of files you're trying to transfer is extremely large (e.g. over 500 GB), you may want to use FTK Imager. A good rule of thumb is if you run Bagger first thing in the morning and the progress bar has not appeared by the end of the day, switch over to FTK Imager and create an EO1 image. (We will maintain files in the E01 image until they are ready to be appraised in Forensic Toolkit.)

Filepaths too long. Bagger only identifies the first problem file it encounters. To identify all files that exceed the filepath limit, generate a listing of the file paths using Karen's Directory, saving as a tsv. Open the tsv in Excel and in the spreadsheet add a column with the formula "=len([cell# of file path name])". This will produce the number of characters of the file paths, by which you can then filter and sort. Alternatively, you can copy file path information from the Karen's Directory manifest and paste in character count.xsl. Try to limit the filepath well below 260 to accommodate the destination filepath.

If possible, ask the staff member who maintained the files on the external drive to shorten the names. If that is not possible, or changing the filenames will be complicated, use FTK Imager to create an image. We will still need to shorten the names once we export the files from the image, but we will at least be able to reexport the files in case accidents occur during the renaming process.



Can't read Shell folder. You may see this error when trying to add a folder to the payload.



In such circumstances, instead of single-clicking the folder and clicking open as in this example . . .

🕌 Add File or [Directory					
Look <u>I</u> n: 🗀	data 🔹 🛍 🔛 🔤					
🗀 Harvested	FromComSharedFiles					
🗀 Harvested	HarvestedFromWebSharedFiles					
PressClipp	PressClippings					
🗀 PressRelea	PressReleases					
	1 Alexandree					
File <u>N</u> ame:	PressReleases					
Files of <u>T</u> ype:	All Files					
	Open Cancel					

try double-clicking so that you are withig the folder and then click Open.





If that still doesn't work, use FTK Imager.

B. COMPUTER DOESN'T RECOGNIZE DRIVE

The drive does not appear in file explorer and may or may not appear under Devices and Printers.

External drive not powering on. Check if the drive's activity light is lit. If dealing with an older mechanical hard drive (as opposed to SSD-based drives), listen for a whirling sound. If there is no light or sound, check the power switch (if one is present) and cable connections.

Malfunctioning or incompatible port. If Tableau does not recognize the external drive, try plugging the drive directly into different ports on your computer. If that doesn't work, try plugging it into different Exami ports on different computers.

Bad cable. Switch out the USB or FireWire cable. Repeat step 1.

External drive appears under an existing letter or was not assigned a letter. Open Control Panel → Administrative Tools \rightarrow Computer Management. If the external dri(a) is listed, you may need to assign the drive a drive letter or change the drive letter. Right click the drive and click Change Drive Letter and Paths.

Bad driver. You may need to install or reinstall the driver for the external drive. External drives usually come with the driver and install automatically when connected. If there is a problem with the driver, try searching the model number of the external driver on updated version of the driver.

Problem with internal connectors. The drive may need to be removed from its casing and placed in a new casing. This requires the assistance of Alan Berta.

SAA MUSEUM Arr