ACCESSIONING FILES FROM EXTERNAL DRIVE

CONTENTS

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.
2. 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 E01 image. Export files from AD1 images as soon as possible using FTK Imager. Only export files from E01 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 #] Example: 2016ia38
External drive does not need to be retained and it is not necessary to record its original physical context. 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.	[accession #]_i[item number] Example: 2016ia38_i02
External drive is to be retained. *or* External drive is not to be retained but the original physical context needs to be recorded.	[accession #]_b[box #]_i[item #] Example: 2016ia38_b02_i01 Note: Item numbering should restart from 01 with each box.

III. Write-Blocking

Whenever possible, connect the external drive to your computer using the Tableau USB bridge for write-blocking 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

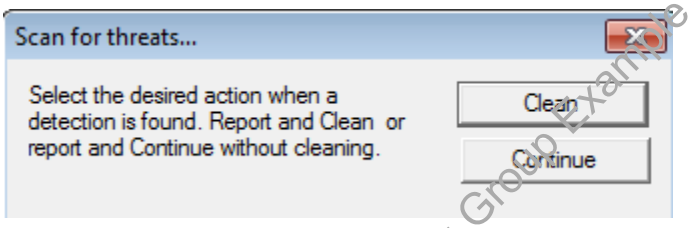
Note: By connecting through the UltraBay, the external drive will not appear in file explorer. You will only be able to copy content from the drive by using FTK Imager to create an image.

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.

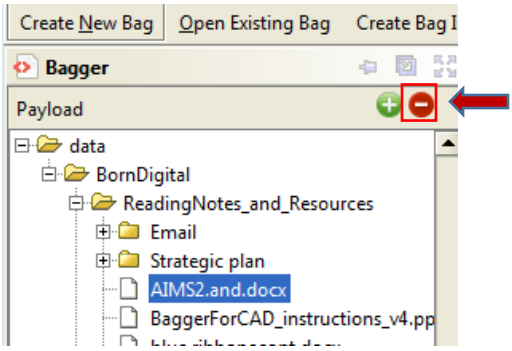


3. If one or more viruses are found, save a log of the infected files in the accession's documentation folder on ira_locked according to the following format: [unique identifier]_viruslog.

   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.



   (3) If cleaning the infected file is not an option and it needs to be retained, create an E01 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 section VII.

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

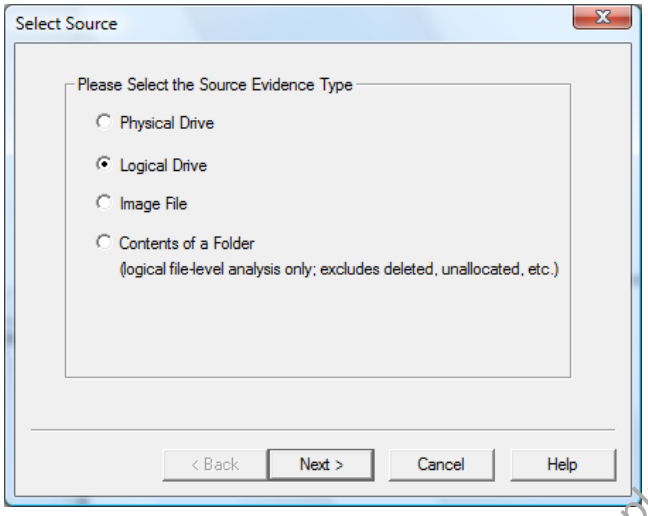
See Bagger_User_Guide.pdf for guidance on using the software.

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 Image** in the file drop-down menu.
2. You will be presented with the following source options:



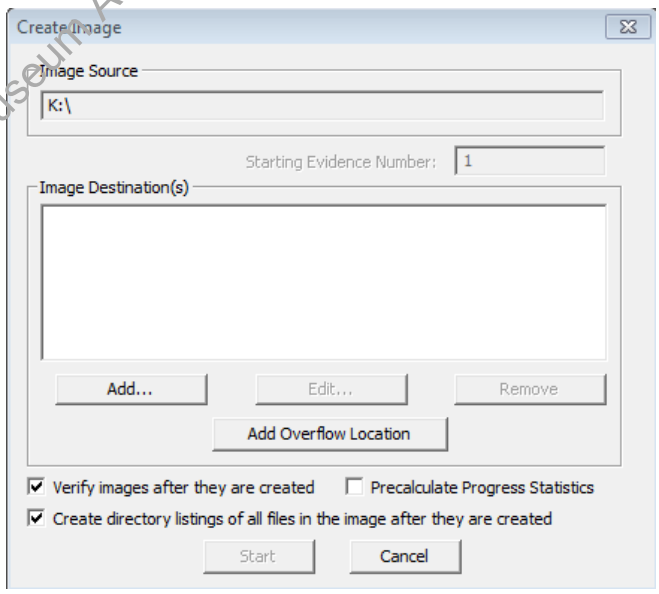
If creating AD1: Select **Contents of a Folder**. You may see a message asking you to confirm if you want to create a logical image (not to be confused with logical drive). Click **Yes**.

If creating E01: Select **Logical Drive.**

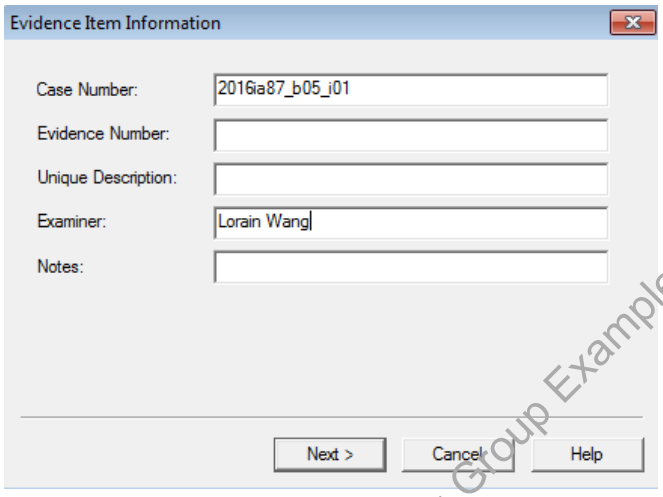
Click **Next.**

3. Select a drive to image and click **Finish**.

4. The Create Image screen will appear. Check 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.



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



7. Click **Next** and the Select Image Destination screen will 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).

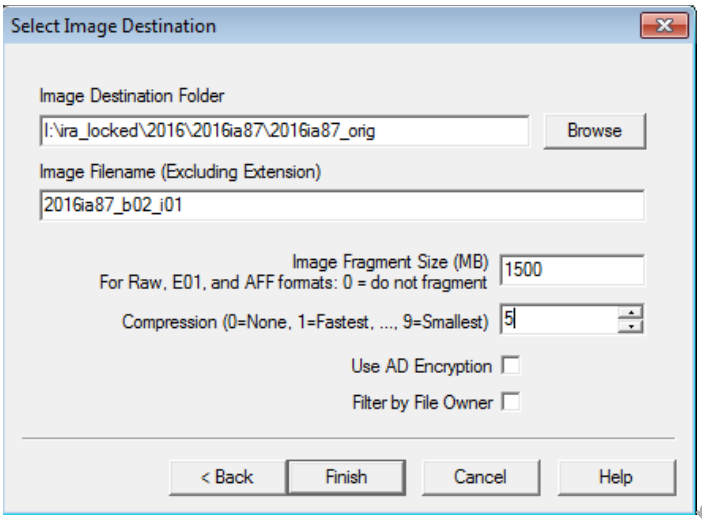
   Image fragment size:

   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.

   E01: 0

   Compression: 5

   Click **Finish**.



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 imaging has completed. You may click **Close.**

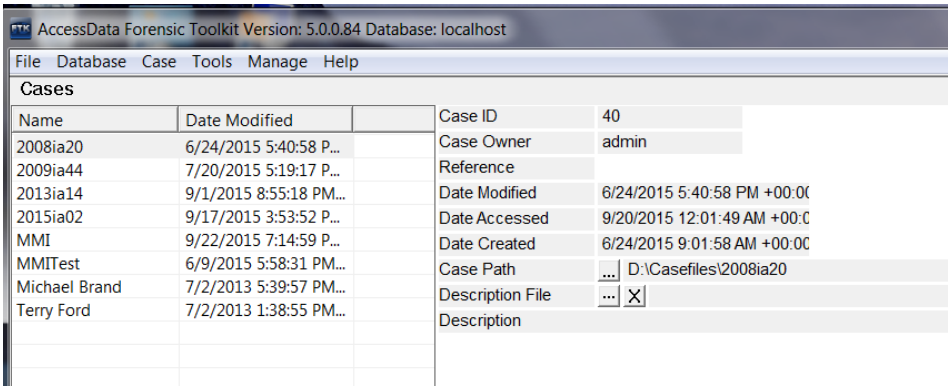
VI. File Export from Image

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 ira_locked. 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.



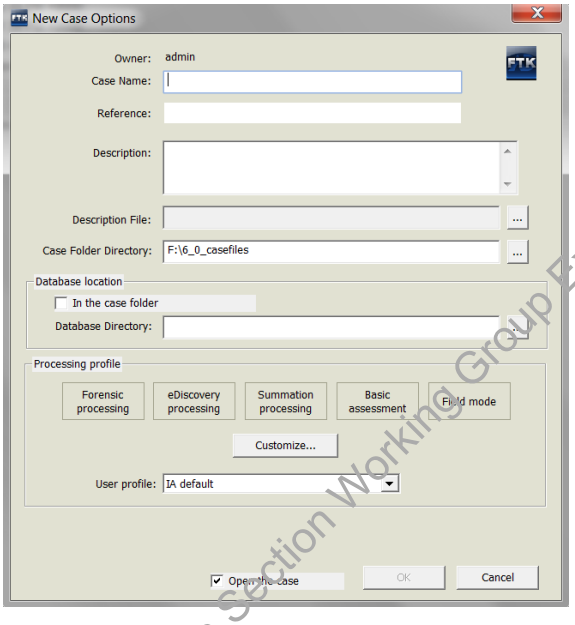
2. Select **New** and the New Case Options window will appear.

   Fill the following fields:

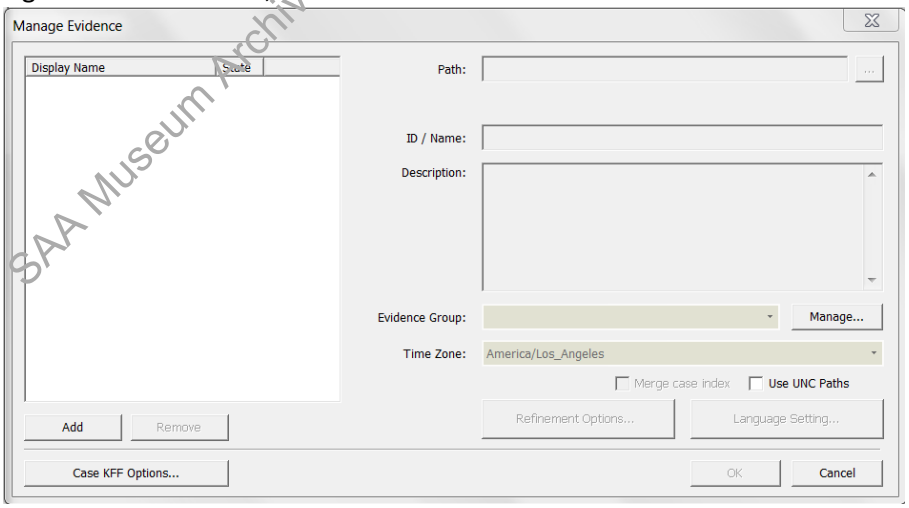
   Case Name: Accession number

   Processing Profile: IA default

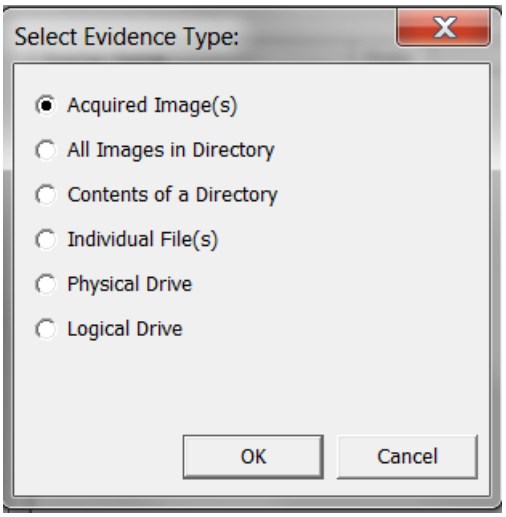
   Click **OK**.



3. In the Manage Evidence window, click **Add**.



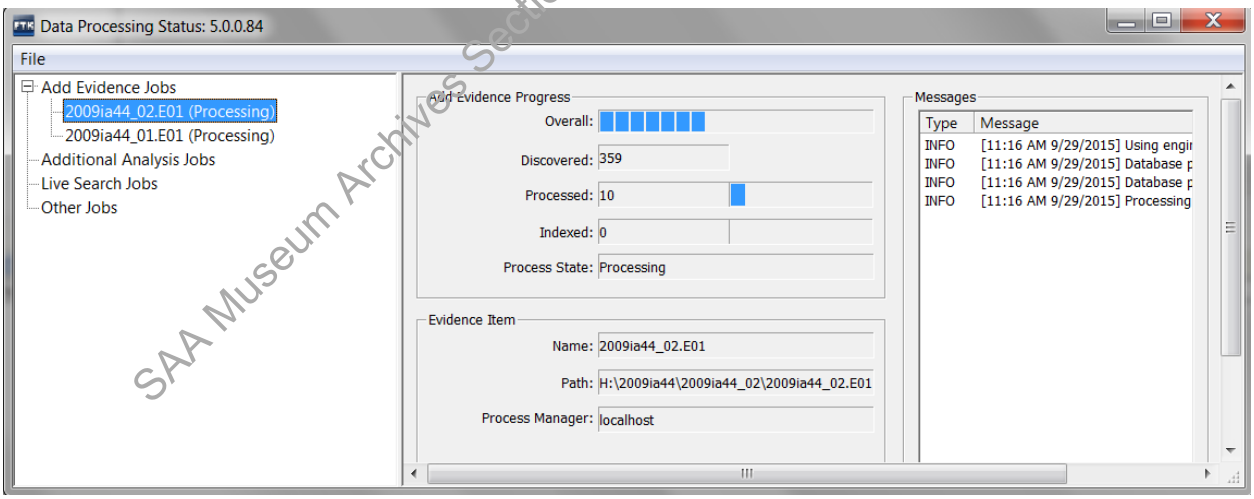
4. Select **Acquired Image** and click **OK**.



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**.

7. A Data Processing Status window will appear.

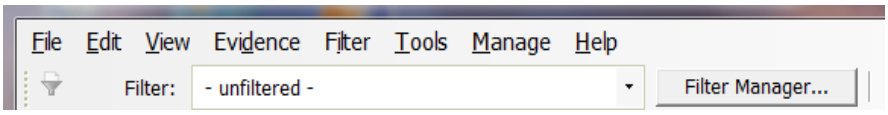


Processing time will vary depending on the size of the image and may possibly take over an hour. It should only take a few minutes at most, however, for files to load in FTK. While you will be able to examine the contents of files before processing is completed, do not conduct index or live searches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

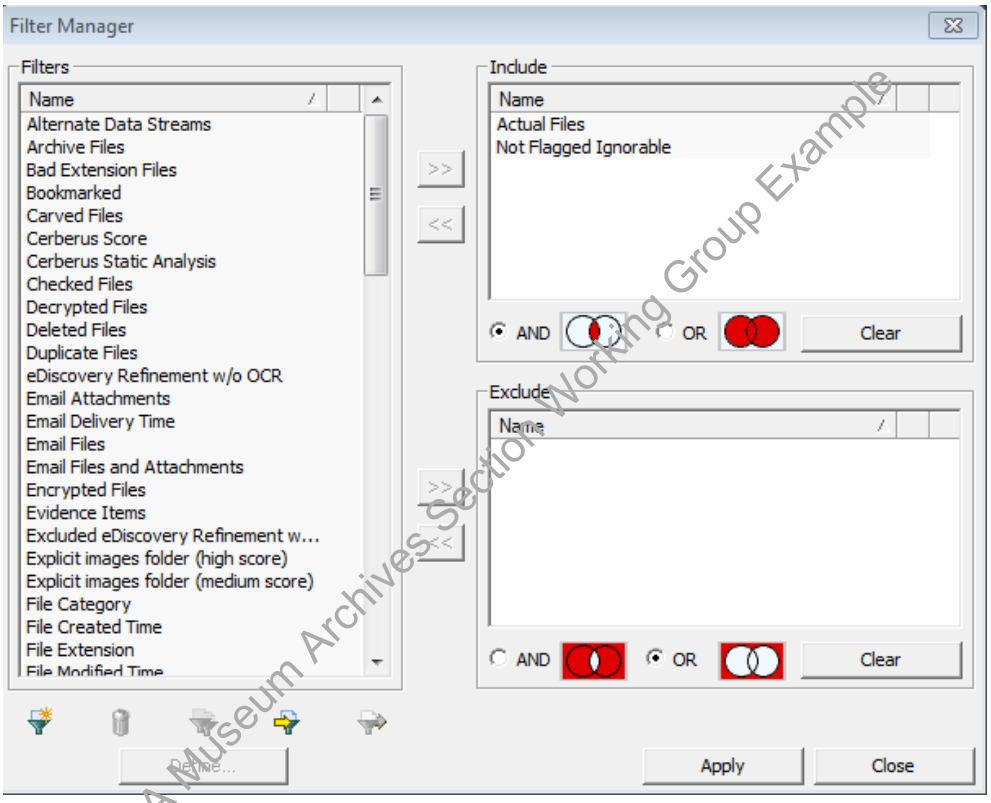
Once the processing job is done, you may want to search for documents with sensitive information or non-archival files to weed (exclude from file export). Otherwise, continue to the next step to export files.

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.



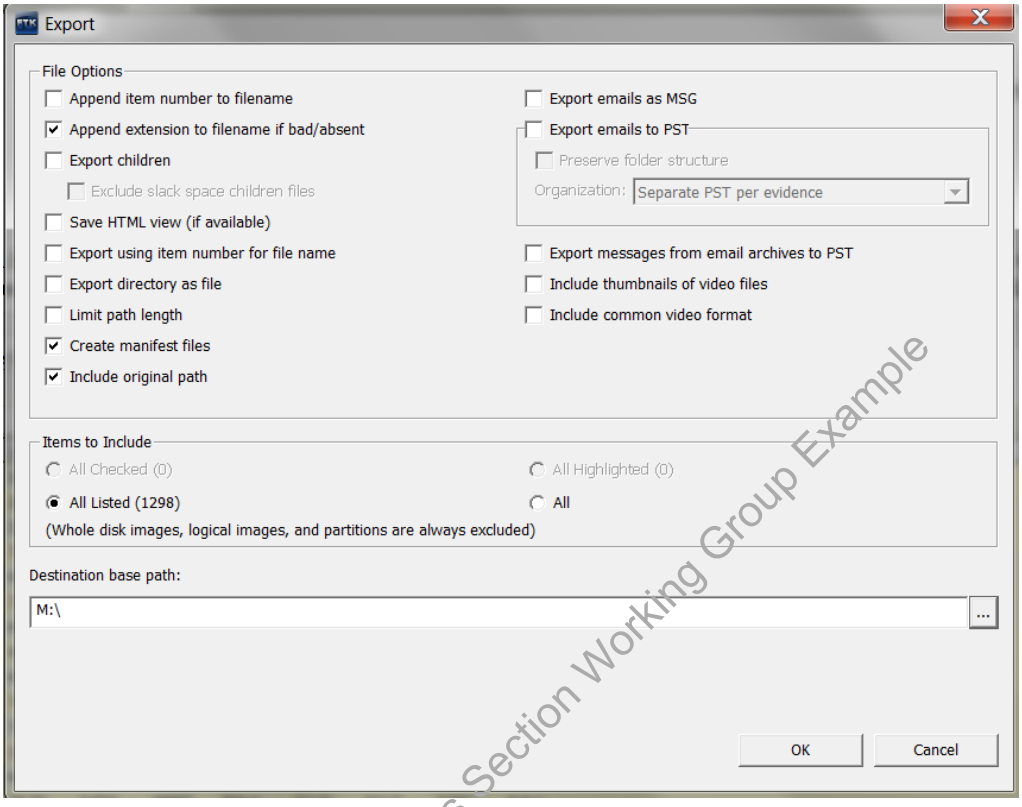
   You can also deselect the icon next to a file or folder to exclude from export.

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 Bagger issues section for an alternate method for identifying problem files.



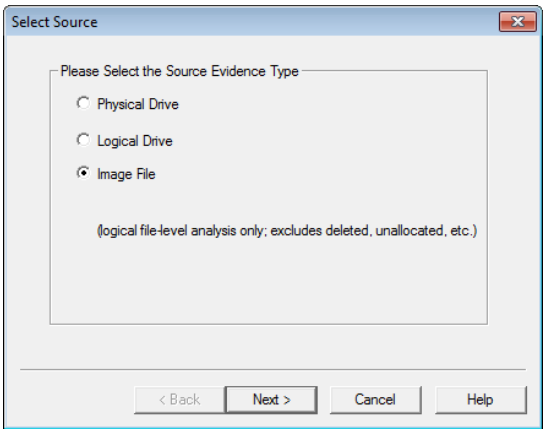
11. Under Destination base path select an external drive to save the exported files.

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.

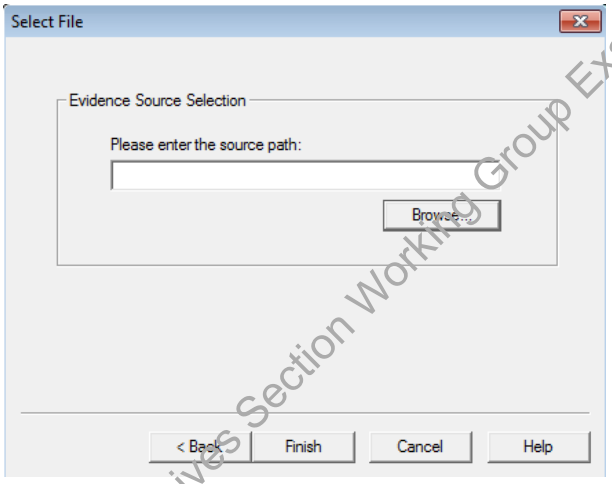
B. AD1

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

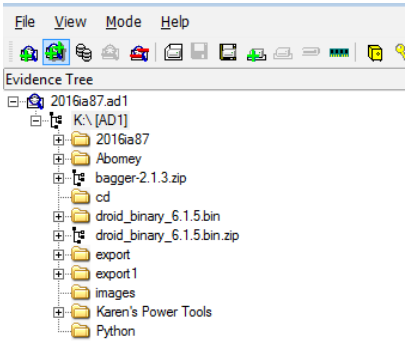
1. Click **File→Add Evidence Item** or click  in the toolbar.
2. Select **Image File** and click **Next.**



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

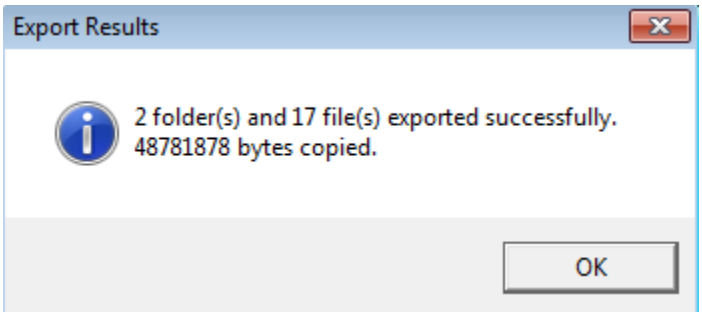


4. The contents of the image file should now appear in the Evidence Tree pane.



5. 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]_ftkexport.csv".

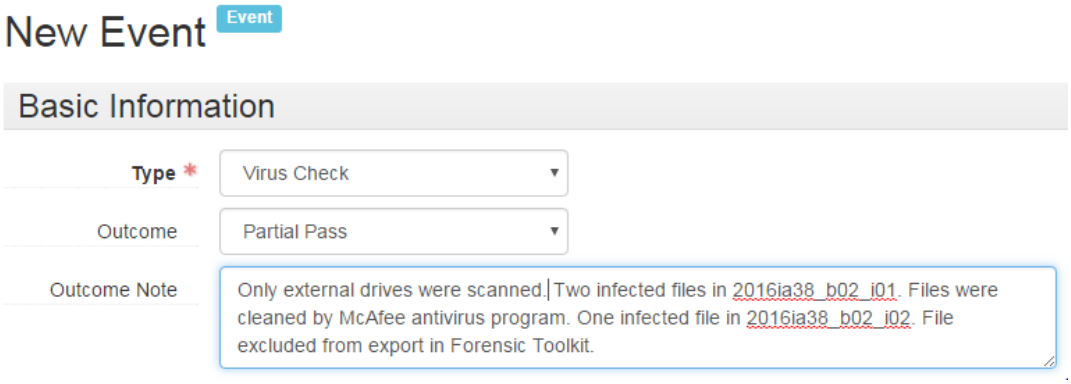
8. If an image was created due to filenames that are too long, now is the time to fix them. See the Bagger issues section for guidance on identifying problem files.

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 link 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.



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 we decide to retain an external drive. Flash drives with custom labeling, for example, may warrant retention. Consult the Head of Institutional Archives as necessary.

Appendix. Troubleshooting

A. Bagger issues

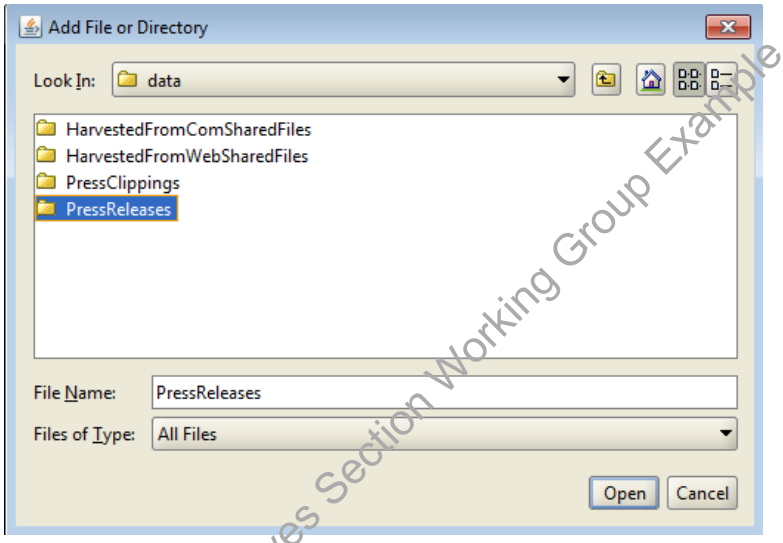
Too large. If the set of files you're trying to transfer is extremely large (e.g. over 500 GB), you may want to use FTK Imager. A good rule of thumb is if you run Bagger first thing in the morning and the progress bar has not appeared by the end of the day, switch over to FTK Imager and create an E01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

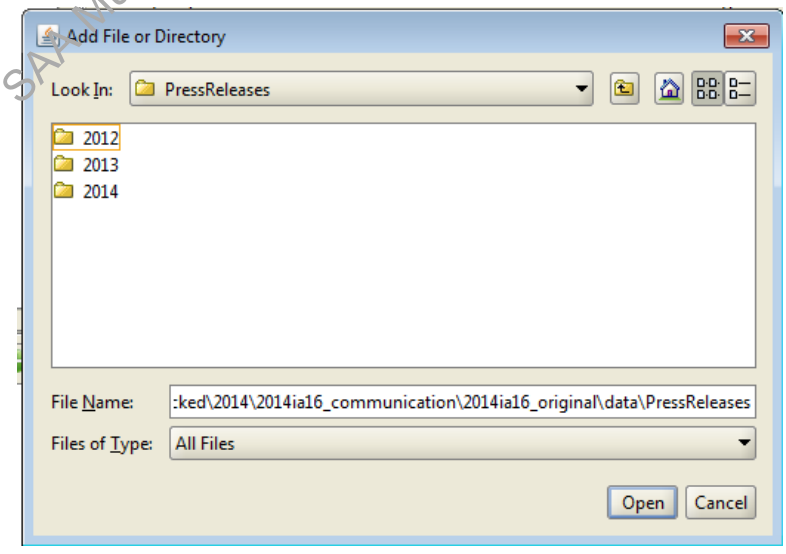
If possible, ask the staff member who maintained the files on the external drive to shorten the names. If that is not possible, or changing the filenames will be complicated, use FTK Imager to create an image. We will still need to shorten the names once we export the files from the image, but we will 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 . . .



try double-clicking so that you are within 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 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 → Computer Management. If the external drive 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 drive online for an 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.