ACCESSIONING FILES FROM COMPUTERS

CONTENTS

Although ITS and Institutional Archives encourage staff to save their files on the network, it is still fairly common for staff to save their files on local drives. Consequently there will be occasions where we will need to either assist staff in transferring files from their computer or transfer files from a computer after a staff departure. This document provides guidance on copying files from Windows-based computers with USB ports.

I. BASIC WORKFLOW

Workflow for ADTriage. Use for 1) imaging the computer, 2) copying files that meet search criteria, or 3) bypassing Windows login.

1. Image entire computer (E01 image) and/or create image of select files or folders (AD1 image) using ADTriage.
2. Open image in ADTriage Administrative console to decrypt and save to "[accession #]_original" folder on ira_locked. Change filenames to incorporate accession number.
3. Export files from AD1 images as soon as possible. Only export files from E01 images after files have been appraised and non-archival files have been identified in Forensic Toolkit.
4. Save exported files to "[accession #]_original" folder on ira_locked and bag in place. Validate bag and maintain files in bag.

Workflow for Bagger. Use for transferring known files in known location with Windows login access

1. Transfer files using Bagger. Use unique identifier as bag name.

2. If computer is connected to the network, save files to "[accession #]_original" folder on ira_locked. If not, save to external drive and then transfer files in bag to ira_locked. Validate bag and maintain files in bag.
3. Delete Bagger program and profile files from staff computer if necessary.

II. Unique Identifier

Assign transfers from local drives a unique identifier following the format that applies to your scenario. Use the unique identifier as the name of bags, image files, and folders for exported files.

Note: ADTriage automatically generates filenames for images. The names can only be changed after they have been exported from the Triage device.

Scenario	Unique Identifier
Accession consists entirely of a single transfer from a computer.	[accession #] Example: 2016ia38
Hybrid or digital accession that consists of multiple transfers from a computer.	1) Maintain each transfer separately and distinguish the transfers through names based on topic, transfer date, etc. (You may change bag names after a transfer without affecting Bagger validation checks.) [accession #]_[topic, transfer date, etc.] Example: 2016ia38_PressClippings Note: Make sure you do not duplicate identifiers if accession contains network transfers. *Or* 2) Combine files from multiple transfers into a single folder structure. Move existing Bagger tag files to documentation folder and create a new bag in place. Assign "[accession #]" as the new bag name.
Hybrid or digital accession that consists of a mix of digital storage media.	[accession #]_localdrive Example: 2016ia38_localdrive

III. Virus Scans

Staff computers connected to the Getty network undergo regular virus scans. Unless the computer has not been connected to the network for some time, or some of the files on the computer look suspicious, a virus scan is not necessary.

IV. File Transfer

There are two tools that we use to transfer files from a computer: ADTriage and Bagger.

When to use ADTriage:

1. Imaging an entire hard drive. Imaging a computer hard drive is an option if we want to capture the entire computer environment, which is rare for Institutional Archives. When we image a local drive, it is usually because we do not have time to thoroughly examine the computer to determine what exactly we want to transfer or where those files may be located. In such cases, we will only retain the image until we have had time to examine and extract the necessary files for the archives.

2. Finding files that meet specific search criteria. ADTriage has a file filter that allows you to search for documents matching specific criteria, such as file date/time, file extension, file path, file size, filename, and keywords. This is useful when files are saved in different locations on the computer. ADTriage compiles the files that meet the search criteria and saves them together as an AD1 image. Since AD1 is a proprietary format that is not ideal for long-term preservation, files need to be exported from the image for preservation.

3. Bypassing the Windows login. It is possible to bypass a Windows login by booting the computer from the Triage device. You will not be able to manually examine the computer, but ADTriage can image the hard drive or copy specific files.

When to use Bagger:

Use Bagger when you or staff can log into the computer and you know exactly what you want to grab and where the files are located. You can save the Bagger program files on the staff computer or run Bagger from a flash drive. If running Bagger from a flash drive, the software will automatically save profile files to the Users folder on the local drive. Using Bagger through either method may require installing Java or adjusting the Java settings on the computer if the software does not run properly. Note: It is possible to install and run Java from a flash drive, but this requires further investigation.

ADTriage

See ADTriage_guide.pdf for guidance on using the software.

1. Use existing Triage device with default Institutional Archives profile for simple imaging of a computer. If you would like to set up search criteria, create a new profile and create new Triage device.

2. Connect Triage device to target computer. If logged into computer, run software. If not able to log into computer, access boot menu and configure system to reboot from USB device. ADTriage should run automatically.
3. Once ADTriage has completed capture, remove Triage device and connect to computer on which the device was created. (The default Triage device was created on Lorain's 2nd computer.)
4. Run ADTriage administrative console to decrypt and save files to "[accession #]_original" folder on ira_locked.
5. Export files from AD1 images as soon as possible using FTK Imager. Only export files from E01 image, using Forensic Toolkit, after files have been appraised and non-archival files have been identified. Maintain exported files in bag in "[accession #]_original" folder on ira_locked.

Bagger

See Bagger_User_Guide.pdf for guidance on using the software.

1. Set up Bagger on target computer or run Bagger off of flash drive.
2. Use unique identifier as bag name.
3. If connected to network, save bag on ira_locked under "[accession #]_original" folder. Otherwise, save to external drive and transfer bag later to ira_locked.
4. Validate the bag to verify files were properly transferred.
5. Maintain files on ira_locked in bag.

V. File Export from Image

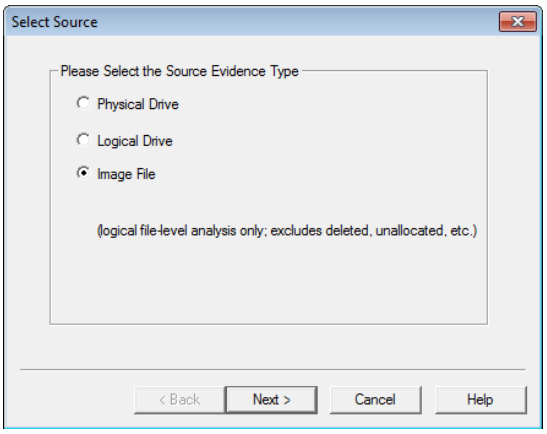
Files should be exported from AD1 images as soon as possible. AD1 is a proprietary format and is not ideal for long term preservation. **Only export files from E01 images after files have been appraised and identified for weeding in Forensic Toolkit.**

A. AD1

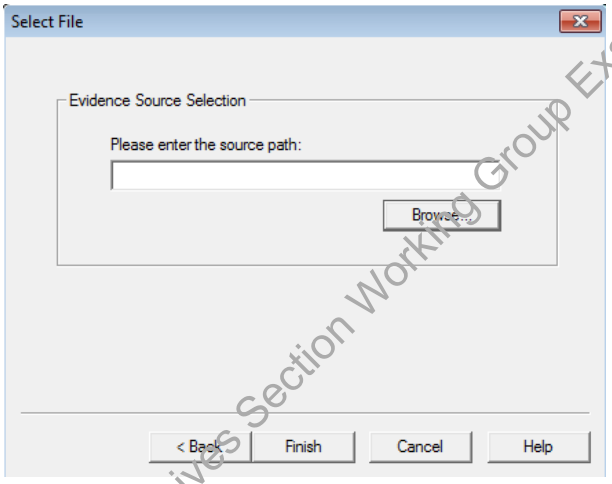
Use FTK Imager to export files from an AD1 image. You may use Forensic Toolkit (see next section) instead if you would like to search for files with sensitive information and weed non-archival files.

1. Click **File→Add Evidence Item** or click  in the toolbar.

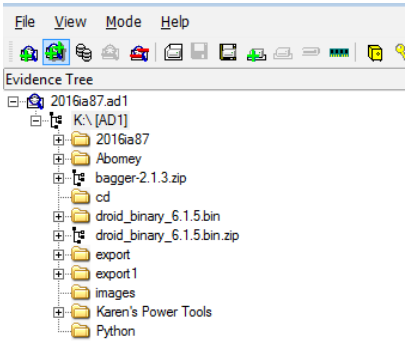
2. Select **Image File** and click **Next.**



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

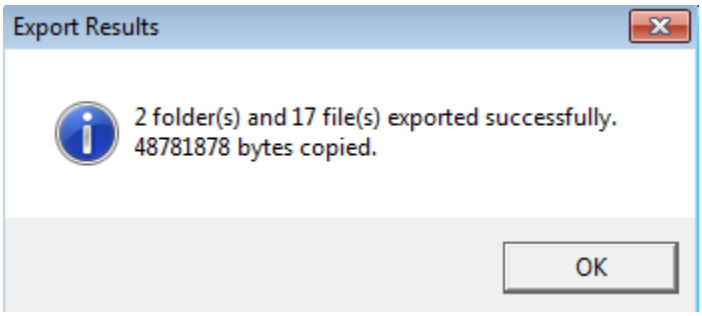


4. The contents of the image file should now appear in the Evidence Tree pane.



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 FRED or Fluffy, save the files on an external hard drive to facilitate file transfer to a networked computer. If working on a networked computer, save the files in "[accession #]_original" folder on ira_locked.

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



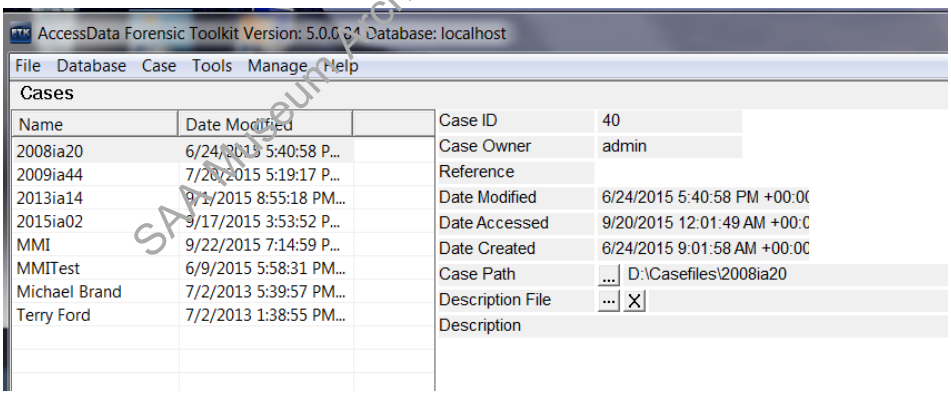
7. Right-click the same folder. This time select **Export File Hash List**. Save the file in the accession's documentation folder on ira_locked. Name the file "[unique identifier]_ftkexport.csv".

8. If exported files are on an external drive, use Bagger to transfer files to ira_locked. Validate bag to confirm files were properly transferred. Maintain files in bag.

B. E01

Use Forensic Toolkit to export files from E01 images. **Do not export files until they have been appraised and non-archival files have been identified.** See section III.B. of IA Electronic record accessioning.pdf for more thorough guidance on using Forensic Toolkit.

1. Go to toolbar and click on **Case**.



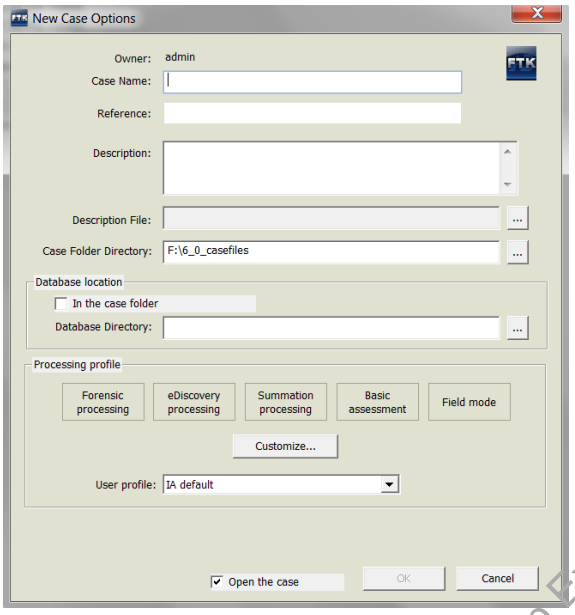
2. Select **New** and the New Case Options window will appear.

   Fill the following fields:

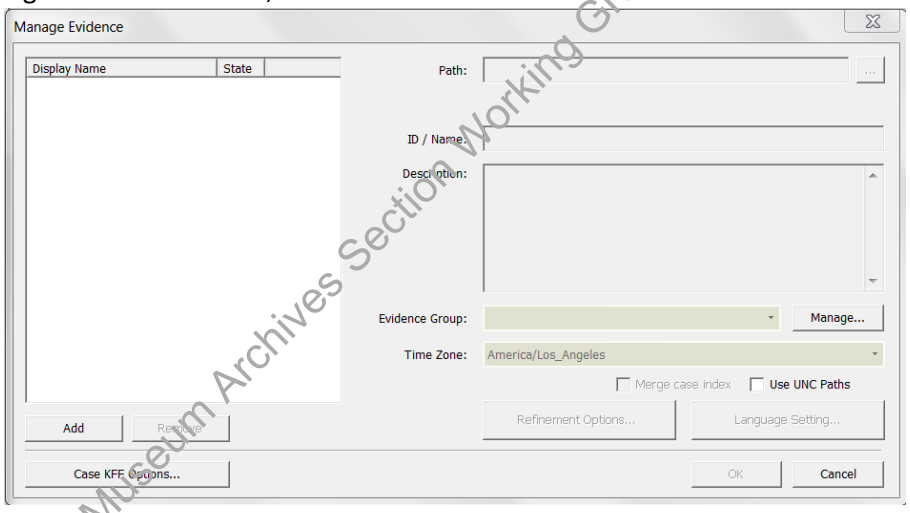
   Case Name: Accession number

   Processing Profile: IA default

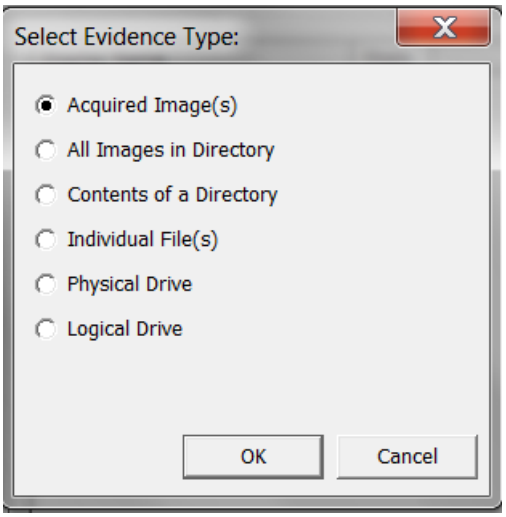
   Click **OK**.



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



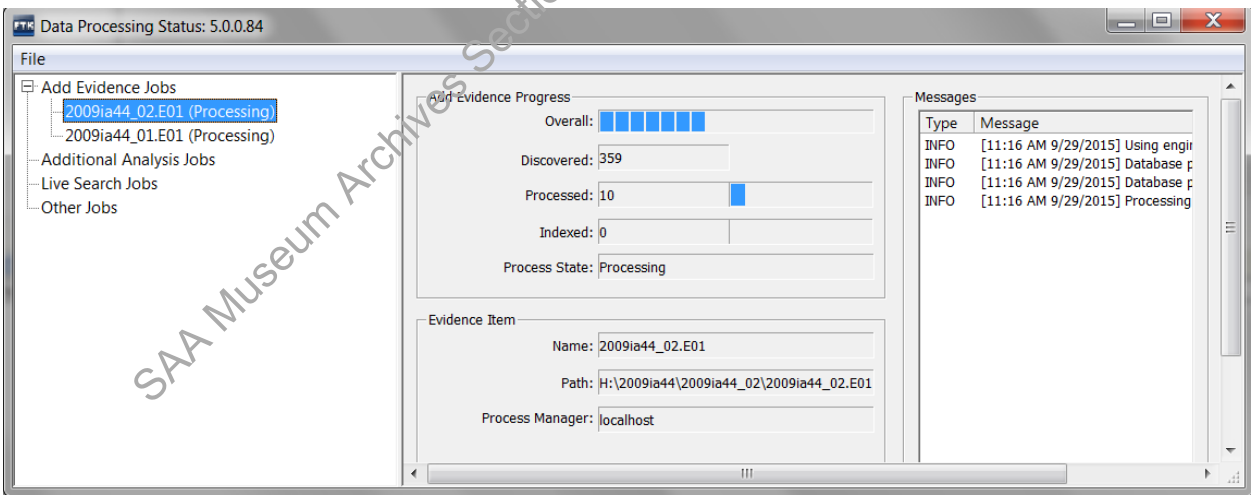
4. Select **Acquired Image** and click **OK**.



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.

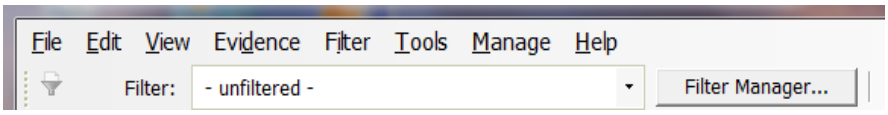


Processing time will vary depending on the size of the image and may possibly take over an hour. It should only take a few minutes at most, however, for files to load in FTK. While you will be able to examine the contents of files before processing is completed, do not conduct index or live searches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

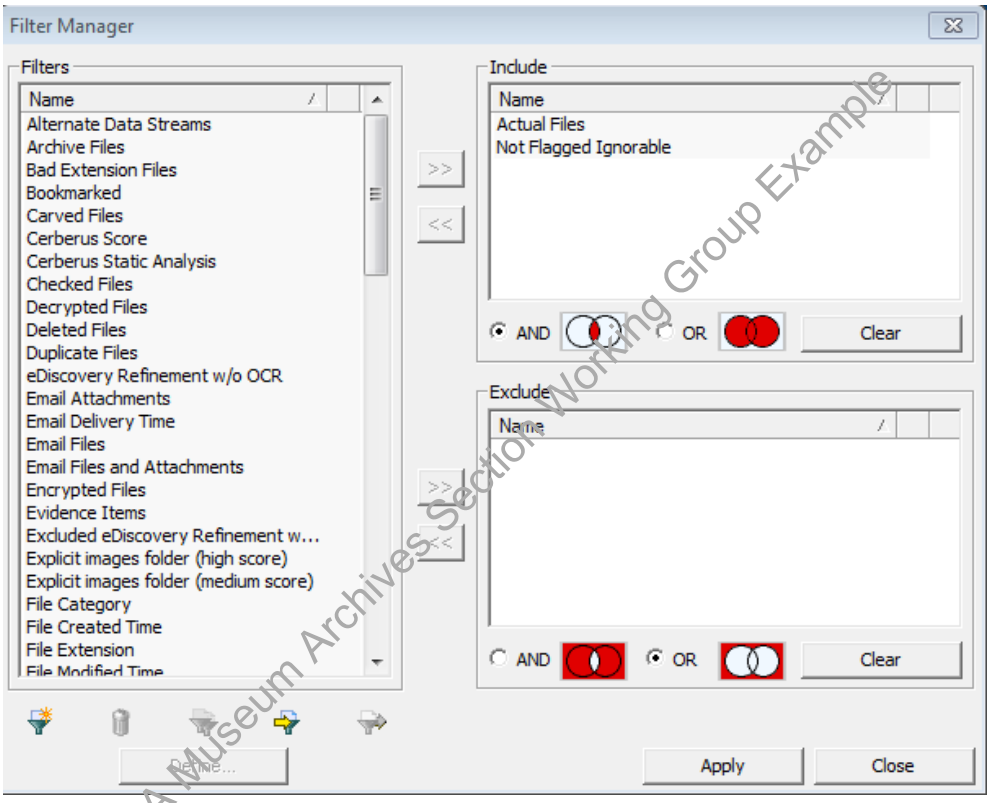
Once the processing job is done, search for and flag documents with sensitive information or non-archival files to weed (exclude from file export).

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.



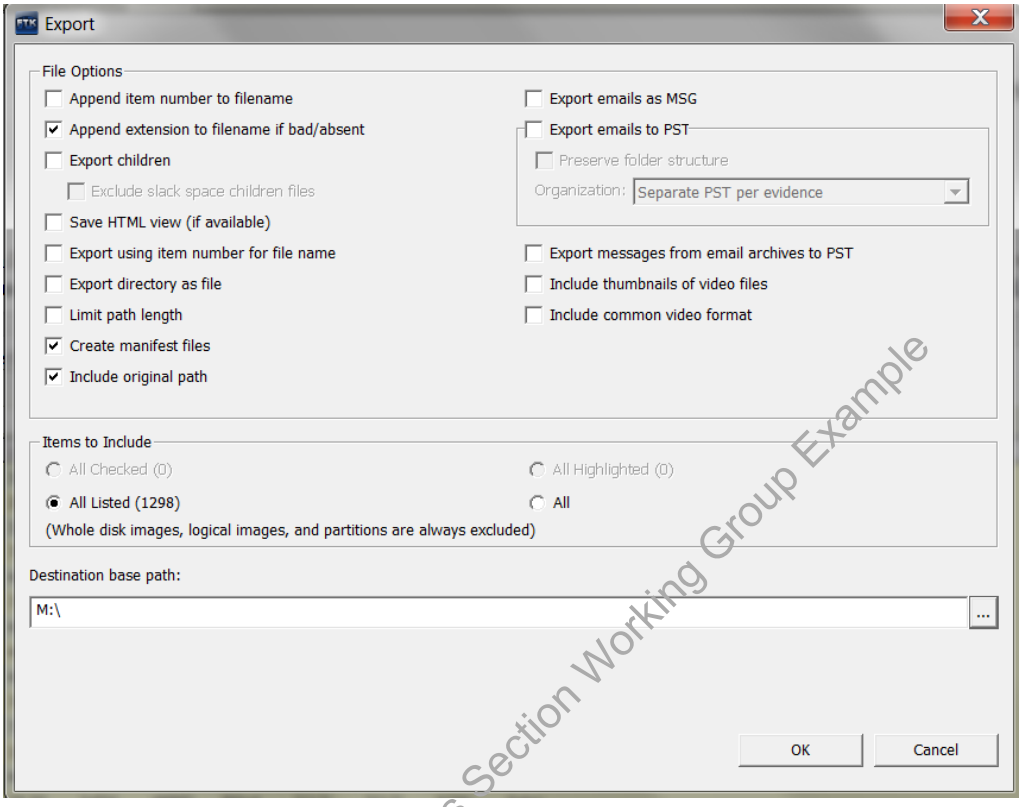
   You can also deselect the icon next to a file or folder to exclude from export.

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 Appendix for an alternate method for identifying problem files.



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

12. Use Bagger to transfer exported files from external drive to "[accession #]_original" folder on ira_locked. Validate bag to confirm files were properly transferred. Maintain files in bag.

VI. DOCUMENTATION

In ASpace 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.

APPENDIX. TROUBLESHOOTING BAGGER

Note: If you are unable to use Bagger, or it is too complicated to use Bagger for your transfer, use ADTriage. You can customize a Triage device to create an AD1 image of files from specific filepaths.

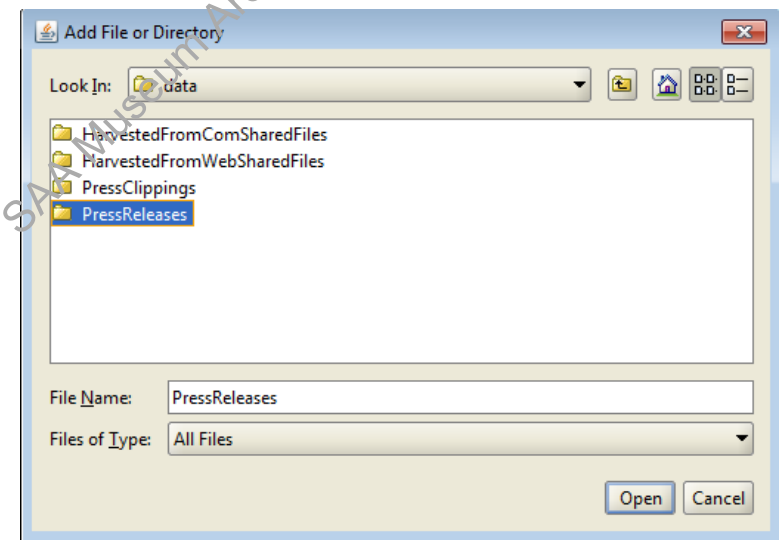
Too large. If you run Bagger first thing in the morning and the progress bar has not appeared by the end of the day, you may want to transfer the files in two or three bags. If transferring files in multiple bags is impractical or may cause confusion, use ADTriage.

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 on ARJ1\\PRD-ARJ\ira_locked\BornDigital. Try to limit the filepath well below 260 to accommodate the destination filepath.

If possible, have the staff member whose files you are trying to transfer edit the filenames. 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.