ACCESSIONING FILES FROM 5.25” FLOPPY DISKS

CONTENTS

I. BASIC WORKFLOW

1. Assign a unique identifier to disk.
2. Use FC5025 software on Fluffy to create disk image or copy files from disk.
3. If time permits, use FTK Imager on Fluffy to export files from disk image.
4. Scan files extracted from image or disk for viruses. Record virus scan results and actions as Virus Check event in ASpace.
5. Use Bagger to transfer files to “[accession #]_original” folder on ira_locked. Validate bag and maintain files in bag.
6. Record actions in Digital File Management Note of accession record in ASpace.
7. Shred disk or retain disk in collection.

II. UNIQUE IDENTIFIER

Assign each disk 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 disk.	File: [accession #] Example: 2016ia38

Disk 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** disks or multiple types of digital media -purely digital accessions with **multiple** disks or multiple types of digital storage media.	[accession #]_i[item number] Example: 2016ia38_i02
Disk is to be retained. *or* Disk 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

The FC5025 controller that we use to connect the 5.25 inch floppy drive to Fluffy (laptop) allows only read-only access. If using a different drive without this protection, cover the square notch in the corner of the disk with a thin piece of electrical tape or a file label.

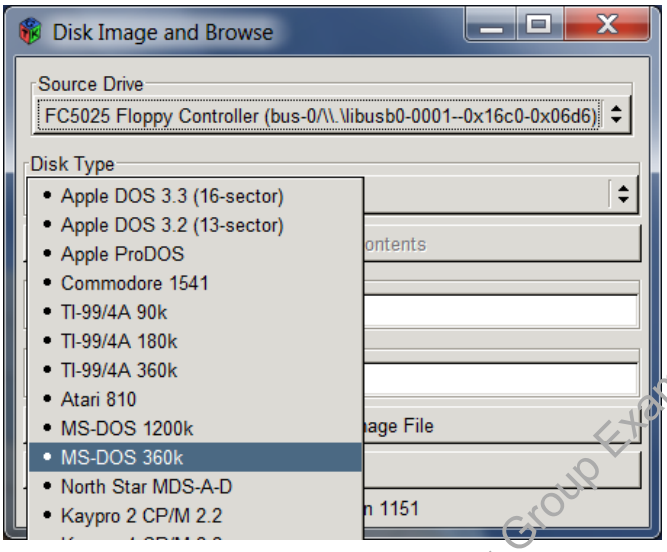
IV. FILE TRANSFER FROM DISKS

Use FC5025 software on Fluffy to image 5.25 inch floppy disks. For certain disk types it is possible to browse file lists and copy individual files. The software comes packaged with the FC5025 controller, which is used to connect the 5.25 inch floppy drive through USB to Fluffy.

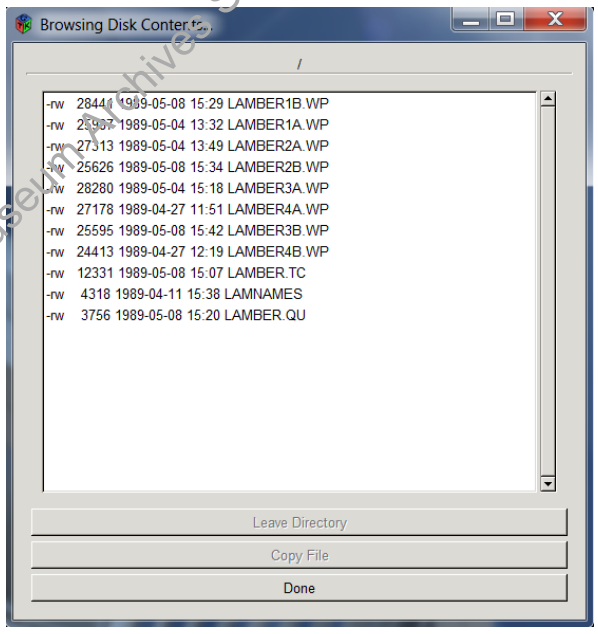
1. Insert floppy disk in 5.25" drive upside down. (The drive itself is upside down due to missing hardware casing.) Once you have inserted the disk, lock the disk in place using the switch on the drive. The mechanisms on the drive should whirl into action. If it does not, make sure the power cable is plugged in and connected to the drive.

2. Double-click the software icon on Fluffy's desktop:

3. On the program screen, click on **Disk Type** and you will see a dropdown menu. If known, select the disk type and continue to step 4. Information you have about the content creator's computer or information written on the disk label may help you determine the disk type.



If no information is available, select **MS-DOS 360k** and then click on **Browse Contents**. If MS-DOS 360k is the correct format type, the program will generate a file listing.



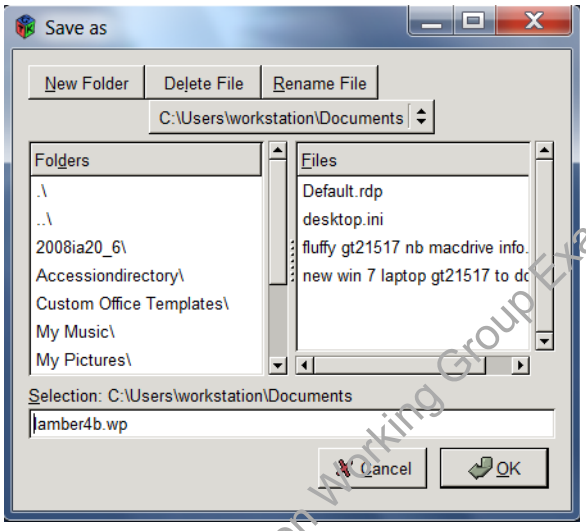
If MS-DOS 360k is not the correct format, you will see "Unable to get file listing!" Select another disk type and try browsing the contents again. Repeat with a different type until a file list is successfully generated. **Note that the browsing feature is only available for ProDOS, MS-DOS, Kaypro, PMC**

MicroMate, Disk BASIC, and VersaDOS disks. To test the other disk types, you will need to proceed to step 4 and try to create an image.

Note regarding Browsing Disk Contents:

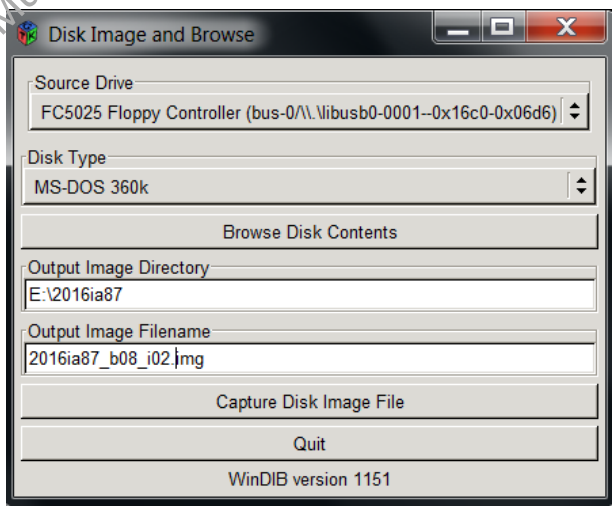
-If you only want to grab certain files, select a file and click **Copy File**.

-This will bring up a window. In the Folders box select the save location (this should be an external drive) and click the **OK** button.

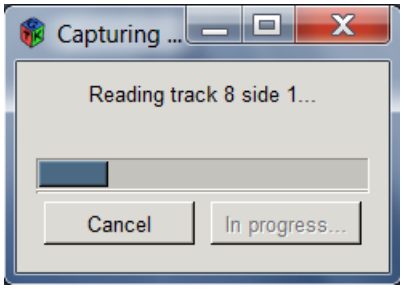


-The file should now be available in the location where you saved it. Click **Done** to exit the Browsing Disk Contents window.

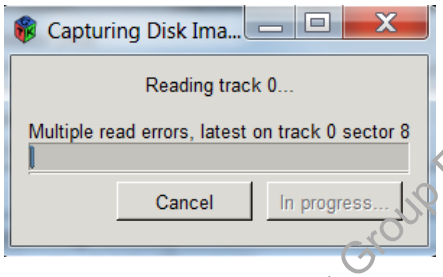
4. To create an image of the disk, indicate the save location (this should be an external drive) under Output Image Directory. Use the disk's unique identifier as the filename under Output Image Filename.



5. Click **Capture Disk Image File** and a window will appear, displaying the capturing progress.

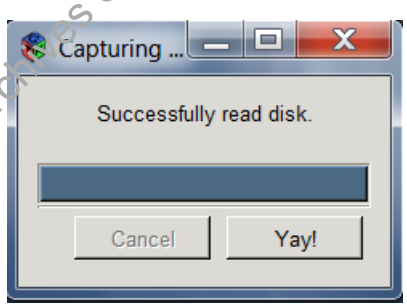


If the disk type is incorrect, the progress screen will display a read error for every single track.

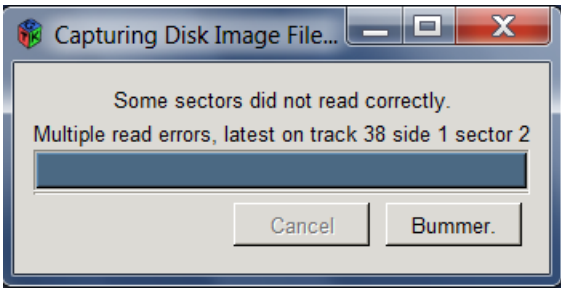


Cancel and select a different disk type until the software is able to successfully read tracks on the disk.

If the disk was successfully imaged, you will see this message:

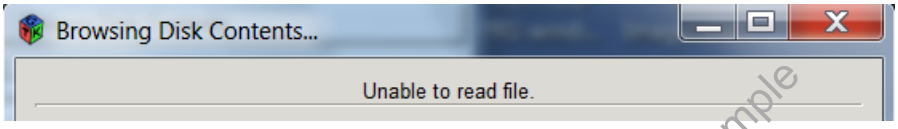


If there are problems imaging a disk, you should see something like this:



The disk image will still save so make sure to delete the file or add "error" to the filename. Try imaging again at another time as you may be able to successfully image the disk on your second, third, or even fourth try.

If you still receive errors after multiple tries, salvage as much of the content as you can by keeping the image. Although some data may be missing, the files can still be read. The problem is that it is not immediately obvious which files are incomplete. To identify the problem files, if the option is available, copy each file through the browse contents window. If the file is corrupt, it will save as an empty file and "Unable to read file" will appear at the top of the Browsing Disk Contents window.



For an extra layer of confirmation, you can also compare the checksums of the files exported from the image with the checksums of the copied files. The checksums of the non-corrupt files should match. If you choose to keep corrupt files, you may also want to examine deleted files on the disk and file slack (see section V.) as they may hold fragments of previous versions or temporary files of the corrupt file.

6. If you have multiple floppies, insert the next disk and repeat from step 2. Pay close attention to the Output Image Filename field. After each attempt to capture an image, whether successful, unsuccessful, or cancelled, if the filename ends with a number, the program will automatically increase the last digit in the filename by one. Make sure the filename is correct before imaging.

7. See section V. for extracting files from the image or use Bagger to transfer image files from the external drive to "[accession #]_original" folder on ira_locked.

Note regarding double-sided disks:

We may not be able to image the second side of double-sided disks (also known as "flippy" disks). While double-sided disks were commercially distributed, users could easily convert a single-sided disk to double-sided by cutting a write unprotect notch on the opposite side of the disk. When flippy disks were first developed, they had to be removed from drives and flipped to read or save to the second side. Drives were later developed to read both sides without ejecting the disk. Most PC-style drives are not able to read the second side of disks, even when the disk is flipped. Although we have not yet encountered flippy disks, chances are that our drive cannot read these disks. You can generally identify flippy disks by looking for a notch on both sides of the disk.

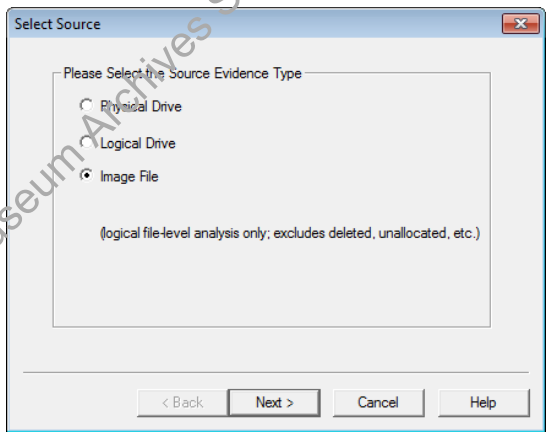
Example of a flippy disk. (Image from http://ascii.textfiles.com/archives/4226)

Document in your notes (see section VII.) if you encounter a flippy disk and confirm that our drive is unable to read the second side.

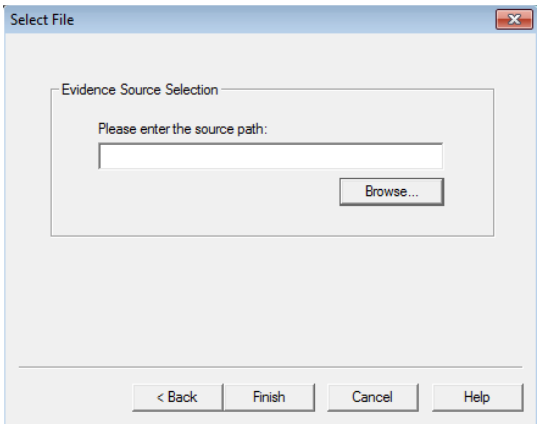
V. File Export from Images

If an *.img file was created from a floppy disk, use FTK Imager on Fluffy to extract files from the image. (You will need to run a virus scan on the exported files before saving them on ira_locked.)

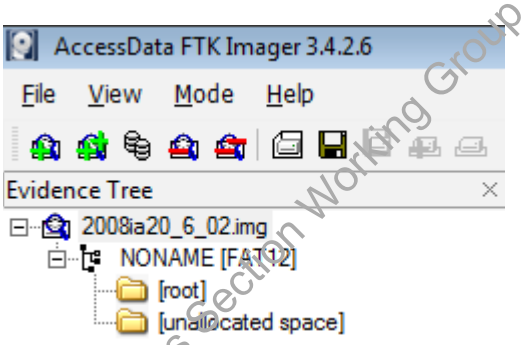
1. Click **File→Add Evidence Item** or click  in the toolbar.
2. Select **Image File** and click **Next.**



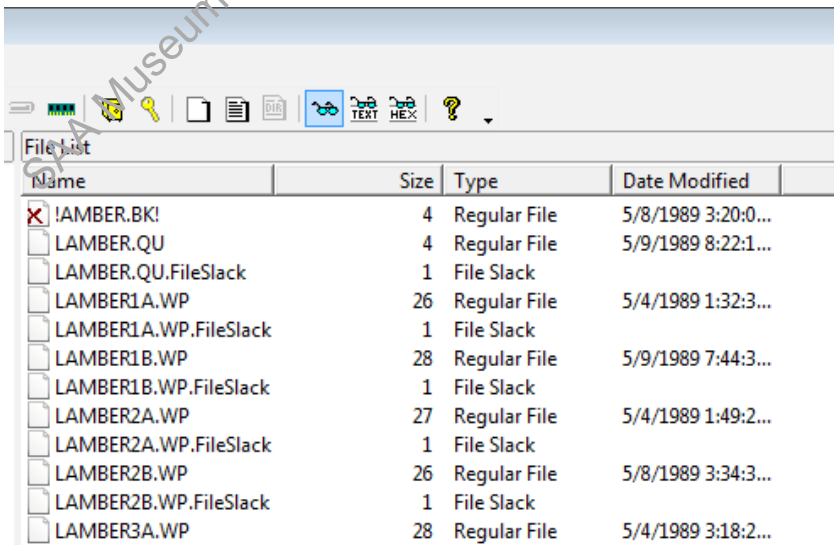
3. In the next window click **Browse** and navigate to the image file and click **Finish**.



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



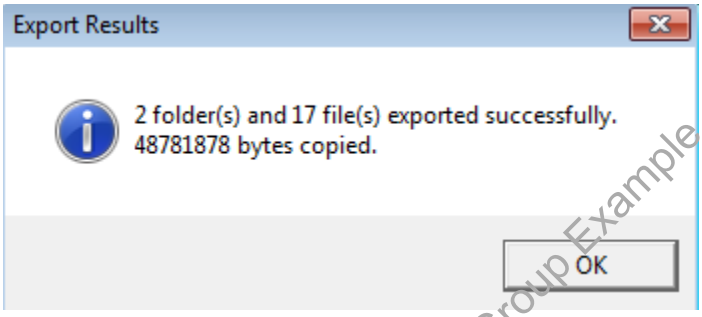
Most PC floppy disks use the FAT12 file system. Click on the root folder to find the files you will want to extract.



The red X next to the first file indicates a deleted file. File Slack refers to “unused” storage space that was allocated to a file. Both file slack and the unallocated space data may contain residual

data of old deleted files. Unless we are trying to reconstruct lost data, we typically do not need to (and would prefer not to) preserve these kind of files.

5. To extract files, you have two options:
   a. Right-click the root folder and select **Export Files**. This will export all "regular files" including deleted files, which you will need to manually delete.
   b. Click on a file in the file list, or use control+click or click and drag to select multiple files, and right-click to select **Export Files.**
6. In the next window, save the files on an empty external drive.
7. Once export is successfully completed, you should see something like this:

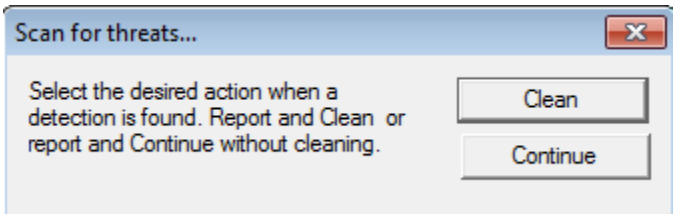


8. Right-click the same folder or files (the files you just exported should still be highlighted) and this time select **Export File Hash List**. Save the file in the accession's documentation folder on ira_locked. Name the file "[unique identifier]_ftkexport.csv".
9. Run a virus scan on the exported files.
10. Use Bagger to transfer exported files to "[accession #]_original" folder on ira_locked. Validate bag and maintain files in bag.

VI. VIRUS SCANS

Run a virus scan on the exported files on Fluffy before examining or transferring to ira_locked. While viruses from the heyday of 5.25" floppy disks are not as harmful as the viruses produced today, it is still a good safety precaution to take. **Do not open any of the files before you have verified that the disk is virus free.**

1. Make sure the Ethernet cord is disconnected.
2. Right-click the folder of extracted files and select Scan for threats.
3. A message box will appear. Select Continue and the virus scan will begin.



4. 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 three options for dealing with infected files:

   (1) Rerun the antivirus program and have it clean the infected file.

   (2) Delete the infected file.

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

   Before proceeding, consult with the Head of Institutional Archives.

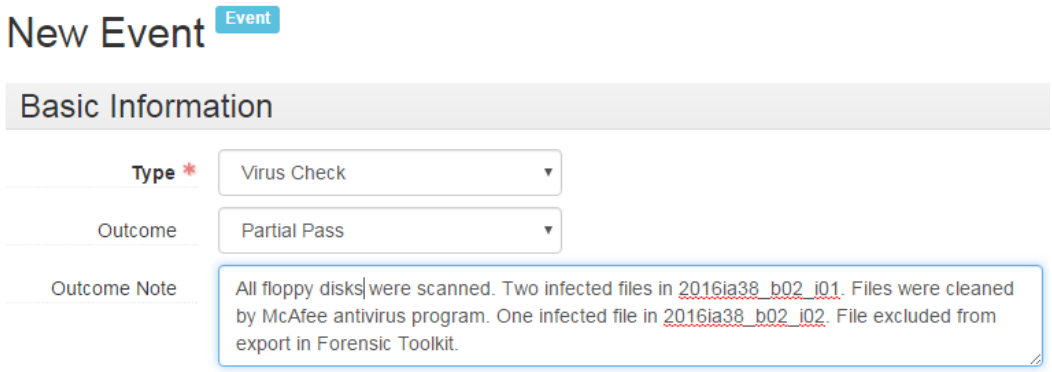
5. Record virus scan results (even if no virus was found) and actions as a Virus Check event in the accessions record of ASpace. See section VII.

VII. 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.

Create a spreadsheet if you need to transcribe labels or document other information about each disk that might be confusing to track in ASpace. You may use Imagingsummary_sample.xsl on ARJ1\\PRD-ARJ\ira_locked\BornDigital as a model. Add or remove columns as necessary. Save the file under the accession's documentation folder and make sure to reference the spreadsheet in the Digital Files Management Notes field.

Record virus scan results (even if no viruses were found) and actions as a Virus Check event in the accessions 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 you run a virus check on select disks (or digital storage media) within the accession, specify in the Outcome note so it is clear which disks have been scanned and which have not.



VIII. Handling of Disk Post-Digital Capture

Institutional Archives views disks as physical carriers that, in most cases, do not hold artefactual value. Once we have captured and preserved the digital content off a disk, the disk can be placed in an Alt Media shred box for destruction. There are, however, certain circumstances in which we may decide to retain a disk. Disks with custom labeling, for example, may warrant retention. Consult the Head of Institutional Archives as necessary.