ACCESSIONING FILES FROM 3.5” FLOPPY DISKS

CONTENTS

I. BASIC WORKFLOW

1. Assign a unique identifier to disk.
2. Slide tab on disk to open position to write-protect disk before inserting in 3.5” drive on Fluffy.
3. Scan disk for viruses. Record virus scan results and actions as Virus Check event in ASpace.
4. Use Bagger to transfer files from disk to external drive. Validate bag.
5. Transfer files in bag 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. Name bags using the unique identifier.

Scenario	Unique Identifier
Accession consists entirely of a single disk.	[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 storage 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

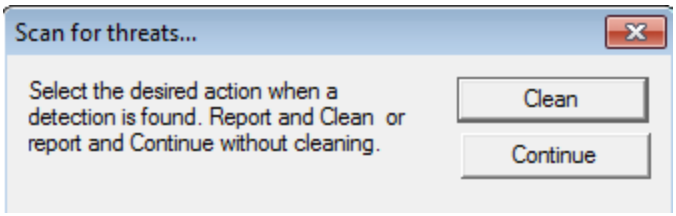
The Tableau USB bridge does not recognize our 3.5 inch floppy drive so we will need to rely on the disk's built-in write-protection. Before inserting a disk in the drive, slide the tab in the corner of the disk to the open position so you can see through the square hole. The disk is now write-protected.

Write-protected floppy

IV. VIRUS SCANS

Run a virus scan on the disk before transferring or examining files. **Do not open any of the files before you have verified that the disk is virus free.**

1. Right-click the floppy drive in file explorer and select Scan for threats.
2. A message box will appear. Select Continue and the virus scan will begin.

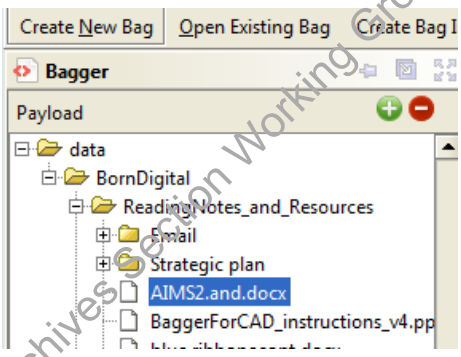


3. If one or more viruses are found, save a log of the infected files in the accession's documentation folder on ira_locked according to the following format: [unique identifier]_viruslog.

   There are four options for dealing with infected files:

   (1) Transfer files with Bagger from disk to an empty external drive and have the antivirus program clean the infected file. Make sure the Ethernet cord is disconnected.

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



   (3) If cleaning an infected file is not an option and it needs to be retained, create an E01 image of the disk using FTK Imager and only access the infected file through Forensic Toolkit.

   (4) Do not accession the disk.

   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 VI.

V. File Transfer

Use Bagger to transfer files from 3.5" floppy disks. See Bagger_User_Guide.pdf for guidance on using the software.

1. Run Bagger to transfer files from the 3.5" floppy disk to an external drive.
2. Use the unique identifier for the bag name.

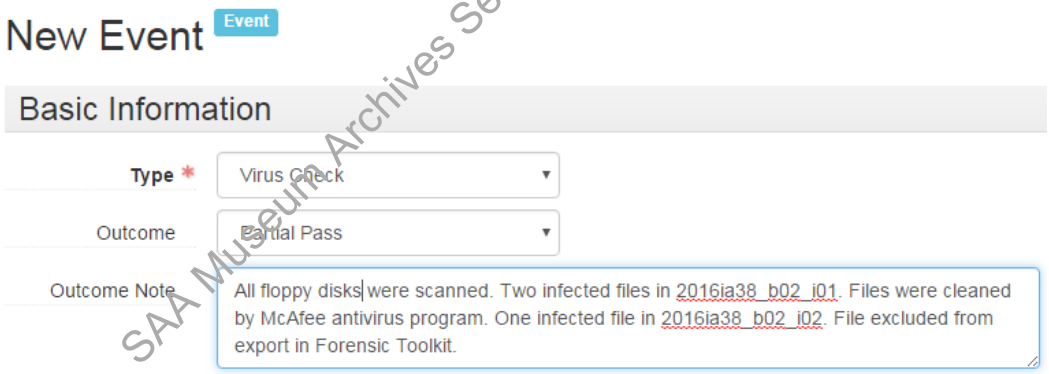
3. Validate the bag to verify files were properly transferred from the disk.
4. Copy the bag from external drive to "[accession #]_original" folder on ira_locked. Validate bag again and maintain files in bag.

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.

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.xls 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 only some of the disks within the accession, specify in the Outcome note so it is clear which disks have been scanned.



VII. 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.