Getty Institutional Records and Archives rev. May 2023

Transferring Files from Digital Storage Media

Contents

I. Introduction

Institutional Archives (IA) receives digital materials on various types of storage devices/drives. Due to bit-rot, media failure, and technological obsolescence, data should be transferred off storage media as soon as possible. At the same time, precautions must be taken to maintain the integrity of files and avoid making irreversible changes. The transfer of files may occur during accessioning or during the processing stage.

The types of media addressed in this manual are: 3.5" floppy disks, 5.25" floppy disks, CDs and DVDs, Zip disks, external storage drives (this includes USB flash drives, external hard drives, external solid state drives, and any other storage drives that you can connect by USB or FireWire), internal storage drives (internal hard drives and internal solid state drives), and network drives. In addition to providing guidance on how to transfer files off media, this document covers assigning unique identifiers, running virus scans, documenting actions in ASpace, and handling media post-transfer.

Consult with the head of Institutional Archives and the digital archivist if you find that the procedures described in this manual are impractical for your situation.

Whichever transfer method or tools you choose to use, the following are essential components of the transfer process for digital media in our holdings:

- Avoid modifying files. Use a write-blocker whenever possible.
- Scan files for viruses. (Unnecessary for files on Getty network drives.)
- Transfer accessioned files to "[accession #]_original" on ira_locked. (Does not apply to staff hard drive files.)
- Verify completeness and file integrity of transferred files. Make sure all files have been transferred and that copied files match the original. While we preference the use of checksums, binary comparisons (available in CDCheck and BeyondCompare) are acceptable as long as the software, verification method, and verification results are documented in the accession record in ASpace.
- If possible and practical, maintain transferred files in bag in ira_locked. The purpose of the bag is to make it easier to verify file integrity when moving files from ira_locked to wbench for processing or when files are on ira_locked for an extended period of time.
- Document tools, actions, and results in **Digital File Mgmt Notes** field in the ASpace accession record.
- Maintain list of checksums of transferred files on ira_locked in "[accession #]_documentation" or maintain files in bag in "[accession #]_original." Checksum logs are usually generated as part of the file transfer process, whether through using Bagger, QuickHash, or other transfer tools. If this list is not created as part of your transfer process and you are unable to use Bagger to bag files in place on ira_locked, you will use QuickHash, Karen's Directory, or any other tool that can generate a manifest that contains checksums, file names, and file paths.

Please note that the workflows documented in this manual are under constant revision as we learn of new tools and gain a better understanding of each media.

II. Media

II.A. 3.5” Floppy Disks

Overview

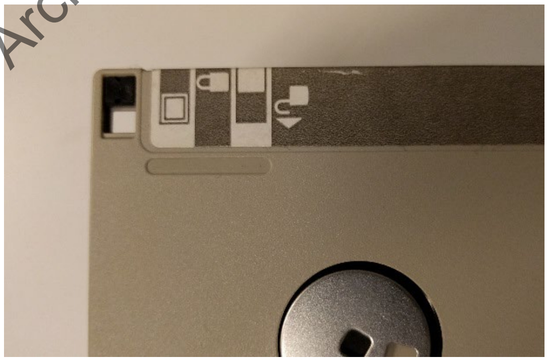
We have two types of drives for reading 3.5” floppy disks. One is a simple USB drive (located in cabinet by Fluffy) that can be used on any computer except FRED. The other is our KryoFlux set-up that is installed on Fluffy.

By default you may use the USB drive to preview and transfer files from 3.5” disks. Use KryoFlux if the disks are Mac-formatted or if you encounter problems reading a disk or transferring files.

Follow the appropriate workflow for the drive you are using to transfer files.

3.5” USB Drive workflow

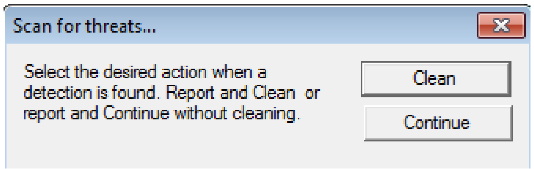
1. Assign and label disk with unique identifier. (See Appendix A. Unique Identifier.) If you are working with multiple disks, it is fine if you need to revise the unique identifier later in the workflow as you determine which to retain or deaccession.
2. Write-protect disk. Since the Tableau USB bridge does not recognize the 3.5” USB drive, we will need to rely on the floppy 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

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

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



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

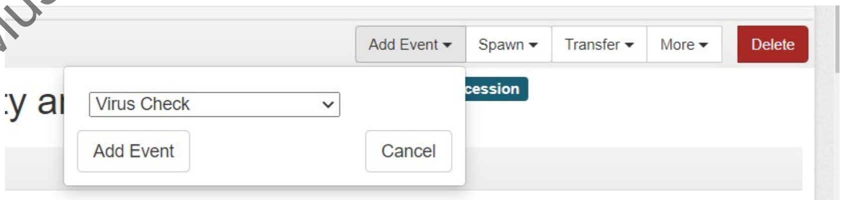
If one or more viruses are found, save a log of the infected files as "[unique identifier]_viruslog" in "[accession #]_documentation" folder on ira_locked.

There are four options for dealing with the infected disk. Discuss with the head of Institutional Archives as needed.

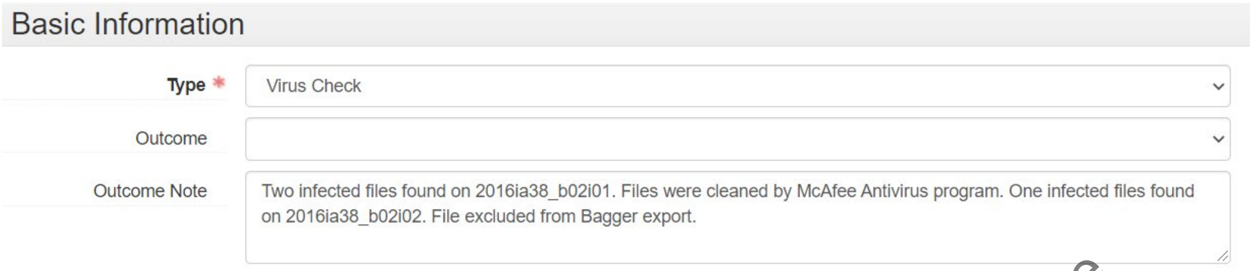
- Keep and clean the infected file(s). Connect floppy drive to Fluffy, if not already, and make sure the Ethernet cord is disconnected. Following step 5, use Bagger to transfer all files from the disk to an empty external drive. Rerun the virus scan on the external drive and have the antivirus program clean the infected file(s). Reformat the drive once files have been transferred to "[accession#]_original folder" on ira_locked.
- Do not transfer infected file(s) from disk. During step 5, exclude the infected file(s) from the Bagger transfer.
- If cleaning an infected file is not an option and it needs to be retained, create an image of the disk using KryoFlux and only view the infected file through the image using FTK Imager (if it's an image or simple text document) or Forensic Toolkit.
- Deaccession the disk.

4. Record virus check activities in the accession record in ASpace. In the **Digital File Mgmt Notes** field, record which disks were scanned, whether or not viruses were found, date of scan, and your initials. The note can be general, such as, "A virus scan was completed on all disks, and no viruses were found. 4/13/2018 LW" or "10 of 30 disks were scanned for viruses. Viruses were found on 2 disks. 4/13/2018 LW."

   If a virus was found, you will also need to add a **Virus Check** event.



Only one **Virus Check** event is needed for an accession. Leave **Outcome** blank and describe all actions taken on infected files.



Basic Information

Type *	Virus Check
Outcome	
Outcome Note	Two infected files found on 2016ia38_b02i01. Files were cleaned by McAfee Antivirus program. One infected files found on 2016ia38_b02i02. File excluded from Bagger export.

Enter date or date range of virus check and add your name under **Agent Links**, with the role as **Implementer**.

5. Use Bagger to transfer files from the disk to "[accession #]_original" folder on ira_locked. Use the unique identifier for the bag name. Validate bag and maintain files in bag. (If needed you can change the bag name later; it will not affect bag validation.)

   If you are working on Fluffy, do not connect the computer to the network. Instead, copy bag to an external drive and then connect drive to a networked computer to transfer to ira_locked.
6. Shred disk or retain disk in collection. IA views disks as physical carriers that, in most cases, do not hold artefactual value. Once we have captured and preserved digital content off a disk, the disk can be placed in an Alt Media shred box for destruction. You may choose to retain the disk, however, if you believe it should be preserved. Disks with custom labeling, for example, may warrant retention. Discuss with the head of Institutional Archives as necessary.
7. Record transfer activities in **Digital File Mgmt Note** of accession record in ASpace and make sure that the box next to "Contains digital content" is checked. Include information such as which floppy drive and software were used, the number of disks worked on, work you've completed, work that needs to be done, any known issues or problems, and whether disks were kept or discarded. Your notes should be clear enough for another archivist to understand what you've done and, if necessary, pick up from where you left off.

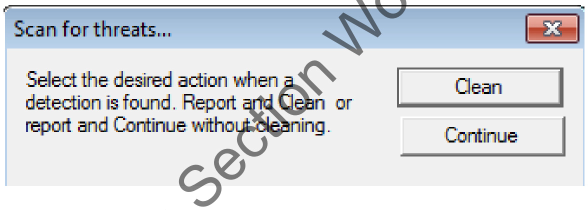
   Create a spreadsheet if you need to transcribe labels or document other information about each disk that might be confusing to track in the ASpace accession record and that you don't want to or you're not ready to add to a resource record. You may use \\prd-arj\arj1\ira_locked\BornDigital\Imagingsummary_sample.xlsx as a model. Add or remove columns as necessary. Save the file in "[accession #]_documentation" folder on ira_locked and make sure to reference the spreadsheet in the **Digital File Mgmt Notes** field.
8. Files are maintained in bags so they can be easily validated to verify that files remain unchanged when they are ready to be processed. If you transferred files from multiple disks and do not plan on processing files immediately, maintain files in a bag at the level that is most practical for validating. Depending on the number of discs, this will vary from maintaining bags at the disc level to a single bag for the entire set of discs. If you decide to create one giant bag for all the discs, you can choose to bag all files within their individual bags or remove files from their bag structure. If removing files from their bag structure, do not delete the bag tags. Move them to the documentation folder, organizing them by unique identifier.

KryoFlux workflow

1. Assign and label disk with a unique identifier. (See Appendix A. Unique Identifier.) If you are working with multiple disks, it is fine if you need to revise the unique identifier later in the workflow as you determine what to retain or deaccession.
2. Use KyroFlux to image disk. Use the unique identifier for the name of the image.
3. Load image in FTK Imager to examine and export files to an empty external drive connected to Fluffy. (The drive can contain exported files from the same accession.) If working on multiple disks, make sure files are organized by unique identifier.

   We will only keep the exported files and not the image file. We will keep the image file, however, if there are problems exporting files.
4. Run virus scan on exported files. Do not open any of the files before you have verified that the files are clean.

   Right-click the folder in file explorer and select **Scan for threats**. 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.

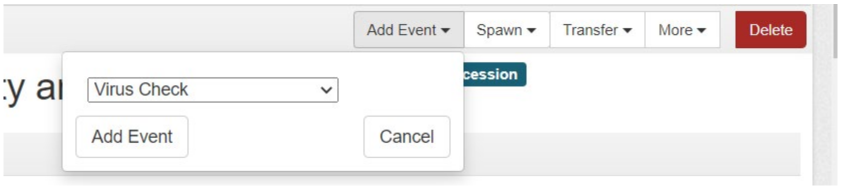
   If one or more viruses are found, save a log of the infected files as "[unique identifier]_viruslog" in "[accession #]_documentation" folder on ira_locked.

   Delete the infected file(s) or rerun the antivirus program and have it clean the infected file(s). If cleaning an infected file is not an option and it needs to be retained, delete the file from the exported set and keep the disk image file. Only access the infected file through the disc image using FTK Imager (if it's an image or simple text document) or Forensic Toolkit.

   Record virus check activities in the accession record in ASpace.

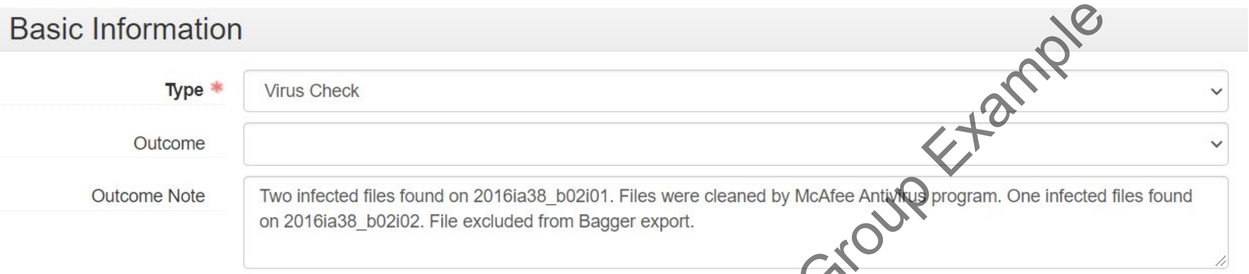
   In the **Digital File Mgmt Notes** field, record which disks were scanned, whether or not viruses were found, date of scan, and your initials. This can be a general note, such as, "A virus scan was completed on all disks, and no viruses were found. 4/13/2018 LW" or "10 of 30 disks were scanned for viruses. Viruses were found on 2 disks. 4/13/2018 LW."

   If a virus was found, you will also need to add a **Virus Check** event.



Virus Check

Only one **Virus Check** event is needed for an accession. Leave **Outcom**e blank and describe all actions taken on infected files.



Basic Information

Type *	Virus Check
Outcome	
Outcome Note	Two infected files found on 2016ia38_b02i01. Files were cleaned by McAfee AntiVirus program. One infected files found on 2016ia38_b02i02. File excluded from Bagger export.

Enter date or date range of virus checks and add your name under **Agent Links**, with the role as **Implementer**.

5. Move KyroFlux image log, FTK Imager exported files list, and, if applicable, the virus log to external drive if not saved there already.
6. If preserving the KryoFlux image, move file to external drive using Bagger. Otherwise, you may delete the image.
7. Connect external drive to networked computer and use Bagger to transfer exported files from external drive to “[accession#_original]” folder on ira_locked. Validate bag and maintain files in bag. If applicable, copy and paste bag with image file to “[accession#_original]” folder and validate bag.
8. Move KyroFlux image log, FTK Imager exported files list, and, if applicable, the virus log to “[accession#]_documentation” folder on ira_locked.
9. Reformat external drive if any of the files had a virus.
10. Shred disk or retain disk in collection. IA views disks as physical carriers that, in most cases, do not hold artefactual value. Once we have captured and preserved digital content off a disk, the disk can be placed in an Alt Media shred box for destruction. You may choose to retain the disk, however, if you believe it should be preserved. Disks with custom labeling, for example, may warrant retention. Discuss with the head of Institutional Archives as necessary.
11. Record transfer activities in **Digital File Mgmt Note** of accession record in ASpace. Include information such as which floppy drive and software were used, the number of disks worked on, work you’ve completed, work that needs to be done, any known issues or problems, and whether disks were kept or discarded. Your notes should be clear enough for another archivist to understand what you’ve done and, if necessary, 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 the ASpace accession record and that you don’t want to or you’re not ready to add to a resource record. You may use Imagingsummary_sample.xsl on \\prd-arj\arj1\ira_locked\BornDigital as a model. Add or remove columns as necessary. Save the file in "[accession #]_documentation" folder on ira_locked and make sure to reference the spreadsheet in the **Digital File Mgmt Notes** field.

12. Maintain files in bag so they can be easily validated to verify that files remain unchanged when they are ready to be processed. If you transferred files from multiple disks and do not plan on processing files immediately, maintain files in a bag at the level that is most practical for validating. Depending on the number of discs, this will vary from maintaining bags at the disc level to a single bag for the entire set of discs. If you decide to create one giant bag for all the discs, you can choose to bag all files within their individual bags or remove files from their bag structure. If removing files from their bag structure, do not delete the bag tags. Move them to the documentation folder, organizing them by unique identifier.

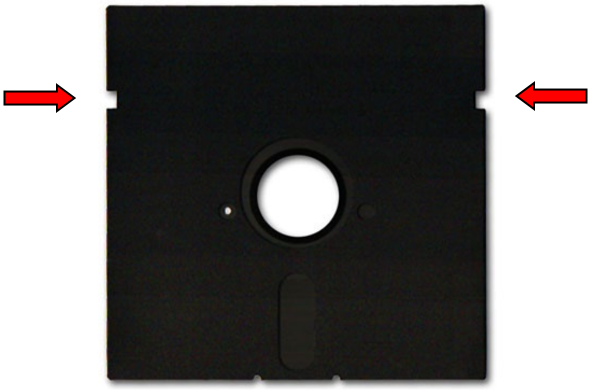
II.B. 5.25" Floppy Disks

Overview

We have two devices for transferring files from 5.25" floppy disks: KyroFlux and FC5025. The 5.25" drive installed in Fluffy uses KryoFlux, while the FC5025 controller card is stored with a second 5.25" drive in a box in the cabinet next to Fluffy. Although setting up the second drive with the FC5025 card is fairly easy, we will use KryoFlux by default as it is ready to use, the software is much more robust (albeit more complicated), and is less damaging to the disk. If you encounter problems, switch to the FC5025 device. (Ask Lorain to help you set it up.) Both devices provide read-only access.

Note regarding double-sided disks:

We may not be able to image the second side of double-sided disks (also known as "flippy" disks). You can generally identify flippy disks by looking for a notch on both sides of the disk. 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.



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

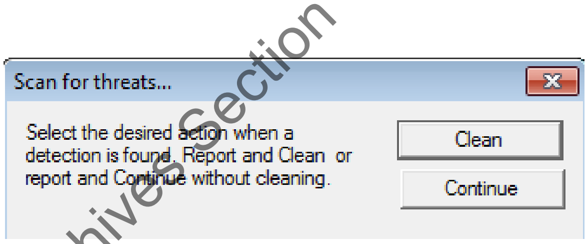
Document in your notes in ASpace if you encounter a flippy disk and confirm that KryoFlux and FC5025 are unable to read the second side.

KryoFlux workflow

1. Assign and label disk with a unique identifier. (See Appendix A. Unique Identifier.) If you are working with multiple disks, it is fine if you need to revise the unique identifier later in the workflow as you determine what to retain or deaccession.
2. Use KyroFlux to image disk. Use the unique identifier for the name of the image.
3. Load image in FTK Imager to examine and export files to an empty external drive connected to Fluffy. (The drive can contain exported files from the same accession.) If working on multiple disks, make sure files are organized by unique identifier.

   We will only keep the exported files and not the image file. We will keep the image file, however, if there are problems exporting files.
4. Run virus scan on exported files. Do not open any of the files before you have verified that the files are clean.

   Right-click the folder in file explorer and select **Scan for threats**. A message box will appear. Select **Continue** and the virus scan will begin.



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

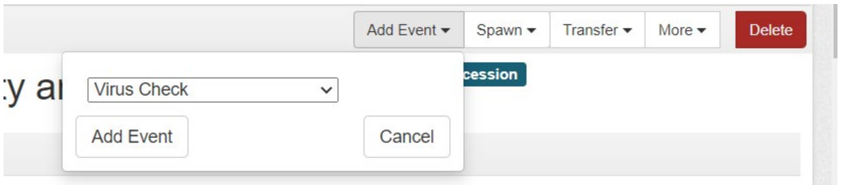
   If one or more viruses are found, save a log of the infected files as "[unique identifier]_viruslog" in "[accession #]_documentation" folder on ira_locked.

   Delete the infected file(s) or rerun the antivirus program and have it clean the infected file(s). If cleaning an infected file is not an option and it needs to be retained, delete the file from the exported set and keep the disk image file. Only access the infected file through the disc image using FTK Imager (if it's an image or simple text document) or Forensic Toolkit.

5. Record virus check activities in the accession record in ASpace.

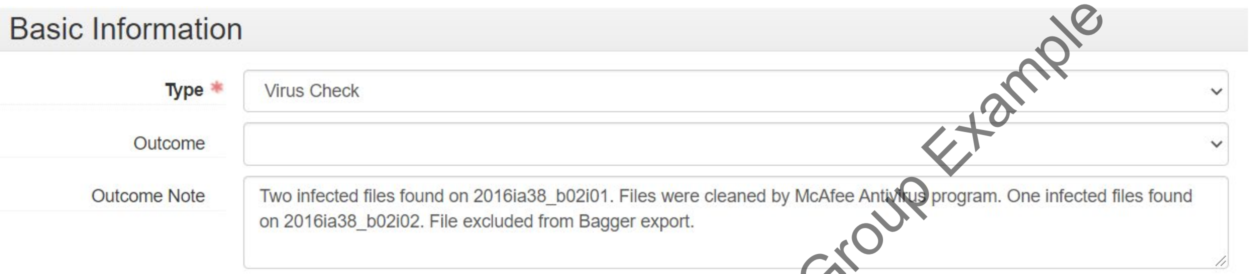
   In the **Digital File Mgmt Notes** field, record which disks were scanned, whether or not viruses were found, date of scan, and your initials. This can be a general note, such as, "A virus scan was completed on all disks, and no viruses were found. 4/13/2018 LW" or "10 of 30 disks were scanned for viruses. Viruses were found on 2 disks. 4/13/2018 LW."

   If a virus was found, you will also need to add a **Virus Check** event.



Virus Check

Only one **Virus Check** event is needed for an accession. Leave **Outcome** blank and describe all actions taken on infected files.



Basic Information

Type *	Virus Check
Outcome	
Outcome Note	Two infected files found on 2016ia38_b02i01. Files were cleaned by McAfee AntiVirus program. One infected files found on 2016ia38_b02i02. File excluded from Bagger export.

Enter date or date range of virus check and add your name under **Agent Links**, with the role as **Implementer**.

6. Move KyroFlux image log, FTK Imager exported files list, and, if applicable, the virus log to external drive if not saved there already.
7. If preserving the KryoFlux image, move to external drive using Bagger. Otherwise, you may delete the image.
8. Connect external drive to networked computer and use Bagger to transfer exported files from external drive to "[accession #_original]" folder on ira_locked. Validate bag and maintain files in bag. If applicable, copy and paste bag with image file to "[accession#_original]" folder and validate bag.
9. Move KyroFlux image log, FTK Imager exported files list, and, if applicable, the virus log to "[accession#]_documentation" folder on ira_locked.
10. Reformat external drive if any of the files on the drive had a virus.
11. Shred disk or retain disk in collection. IA views disks as physical carriers that, in most cases, do not hold artefactual value. Once we have captured and preserved digital content off a disk, the disk can be placed in an Alt Media shred box for destruction. You may choose to retain the disk, however, if you believe it should be preserved. Disks with custom labeling, for example, may warrant retention. Discuss with the head of Institutional Archives as necessary.
12. Record transfer activities in **Digital File Mgmt Notes** of accession record in ASpace and make sure that the box next to "Contains digital content" is checked. Include information such as which floppy drive and software were used, the number of disks worked on, work you've completed, work that needs to be done, any known issues or problems, and whether disks were kept or discarded. Your notes should be clear enough for another archivist to understand what you've done and, if necessary, 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 the ASpace accession record and that you don't want to or you're not ready to add to a resource record. You may use Imagingsummary_sample.xsl on \\prd-arj\arj1\ira_locked\BornDigital as a model. Add or remove columns as necessary. Save the file in "[accession #]_documentation" folder on ira_locked and make sure to reference the spreadsheet in the **Digital File Mgmt Notes** field.

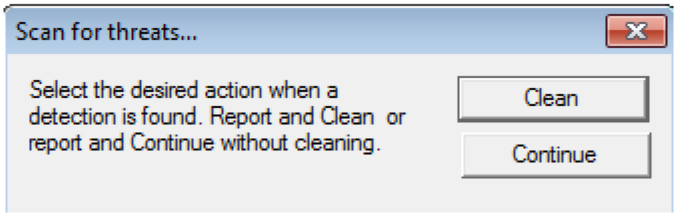
13. Files are maintained in bags so they can be easily validated to verify that files remain unchanged when they are ready to be processed. If you transferred files from multiple disks and do not plan on processing files immediately, maintain files in a bag at the level that is most practical for validating. Depending on the number of discs, this will vary from maintaining bags at the disc level to a single bag for the entire set of discs. If you decide to create one giant bag for all the discs, you can choose to bag all files within their individual bags or remove files from their bag structure. If removing files from their bag structure, do not delete the bag tags. Move them to the documentation folder, organizing them by unique identifier.

FC5025 workflow

1. Assign a unique identifier to disk. (See Appendix A. Unique Identifier.) If you are working with multiple disks, it is fine if you need to revise the unique identifier later in the workflow as you determine what to retain or deaccession.
2. Use FC5025 on Fluffy to image disk or copy files from disk. (See FC5025 for instructions.) You may want to experiment with both methods to determine which you prefer, but if you encounter corrupt files, you may want to copy files *and* create a disk image. Use the unique identifier as the image file name and organize copied files by disk.
3. If you created an image, load image in FTK Imager to examine and export files to empty external drive connected to Fluffy. (The drive can contain files exported from the same accession.) If working on multiple disks, make sure files are organized by unique identifier.

   In general we will only preserve the exported files and not the image file. If there are problems exporting files, however, we will also retain the image file.
4. Run virus scan on exported files. Do not open any of the files before you have verified that the files are clean.

   Right-click the folder in file explorer and select **Scan for threats**. 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.

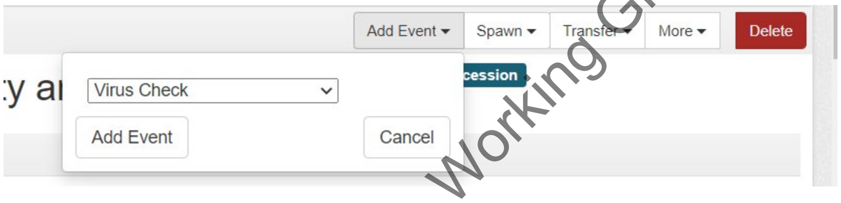
   If one or more viruses are found, save a log of the infected files as "[unique identifier]_viruslog" in "[accession #]_documentation" folder on ira_locked.

Delete the infected file(s) or rerun the antivirus program and have it clean the infected file(s). If cleaning an infected file is not an option and it needs to be retained, delete the file from the exported set and keep the disk image file. Only access the infected file through the disc image using FTK Imager (if it's an image or simple text document) or Forensic Toolkit.

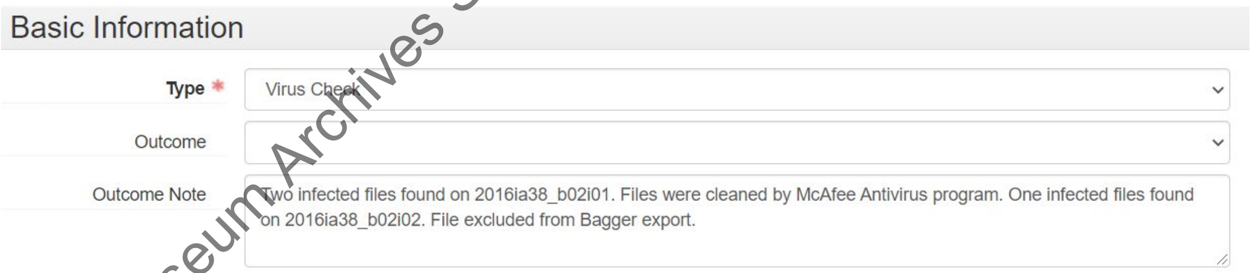
5. Record virus check activities in the accession record in ASpace.

   In the **Digital File Mgmt Notes** field, record which disks were scanned, whether or not viruses were found, date of scan, and your initials. This can be a general note, such as, "A virus scan was completed on all disks, and no viruses were found. 4/13/2018 LW" or "10 of 30 disks were scanned for viruses. Viruses were found on 2 disks. 4/13/2018 LW."

   If a virus was found, you will also need to add a **Virus Check** event.



   Only one **Virus Check** event is needed for an accession. Leave **Outcome** blank and describe all actions taken on infected files.



Basic Information

Type *	Virus Check
Outcome	
Outcome Note	Two infected files found on 2016ia38_b02i01. Files were cleaned by McAfee Antivirus program. One infected files found on 2016ia38_b02i02. File excluded from Bagger export.

   Enter date or date range of virus check and add your name under **Agent Links**, with the role as **Implementer**.

6. Move FTK Imager exported files list and, if applicable, the virus log to external drive if not saved there already.
7. Connect external drive to networked computer and use Bagger to transfer exported files (and image file if preserving) from external drive to "[accession #]_original" folder on ira_locked. Validate bag and maintain files in bag.
8. Move FTK Imager exported files list and virus log to "[accession #]_documentation" folder on ira_locked.
9. Reformat external drive if any of the files had a virus.
10. Shred disk or retain disk in collection. IA views disks as physical carriers that, in most cases, do not hold artefactual value. Once we have captured and preserved digital content off a disk, the disk can be placed in an Alt Media shred box for destruction. You may choose to retain the disk,

however, if you believe it should be preserved. Disks with custom labeling, for example, may warrant retention. Discuss with the head of Institutional Archives as necessary.

11. Record transfer activities in **Digital File Mgmt Notes** of accession record in ASpace and make sure that the box next to “Contains digital content” is checked. Include information such as which floppy drive and software were used, the number of disks worked on, work you’ve completed, work that needs to be done, any known issues or problems, and whether disks were kept or discarded. Your notes should be clear enough for another archivist to understand what you’ve done and, if necessary, 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 \\prd-arj\arj1\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 File Mgmt Notes** field.
12. Files are maintained in bags so they can be easily validated to verify that files remain unchanged when they are ready to be processed. If you transferred files from multiple disks and do not plan on processing files immediately, maintain files in a bag at the level that is most practical for validating. Depending on the number of discs, this will vary from maintaining bags at the disc level to a single bag for the entire set of discs. If you decide to create one giant bag for all the discs, you can choose to bag all files within their individual bags or remove files from their bag structure. If removing files from their bag structure, do not delete the bag tags. Move them to the documentation folder, organizing them by unique identifier.

II.C. CDs and DVDs

Overview

Bagger is the primary tool we use to copy files from CDs and DVDs. Certain discs will require the use of different tools, which are noted below. Only create a disc image if the disc contains software files or interactive features that we want to preserve or if there are problems extracting files.

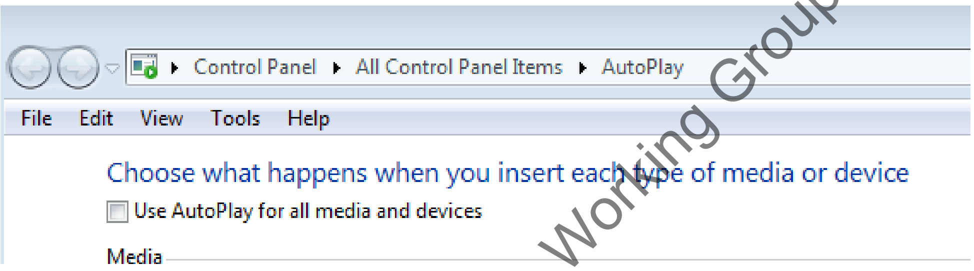
You will likely encounter discs that are unreadable or have bad sectors. The disc might not have been burned properly or is damaged due to improper handling or storage or poor manufacture quality. There are many tools you can use to try to salvage as much data as you can from the disc. These procedures are described below, but you are not required to follow all of them. Recovering files from a bad disc can be time consuming. You are expected to use your best judgement in determining how much time and effort to put in. No matter your decision, you will need to document your decisions and actions in ASpace.

Workflow

Note: If dealing with a Blu-Ray disc (it should be labeled as such), you will need to use FRED or the M-Disc drive connected to Fluffy to read the disc. Lorain also has an M-Disc drive in her office that you can borrow.

Turn off Autoplay

Before you insert a disc, turn off the autoplay function on your computer. A disc with a virus could potentially infect a computer if the disc is programmed to run automatically when inserted into your computer's disc drive. To turn off the autoplay function, navigate to your computer's control panel and search "AutoPlay." In the window that appears, uncheck the box next to "Use AutoPlay for all media and devices." Click **Save** at the bottom of the window.


Control Panel ▸ All Control Panel Items ▸ AutoPlay
File Edit View Tools Help

Choose what happens when you insert each type of media or device

□ Use AutoPlay for all media and devices

Media

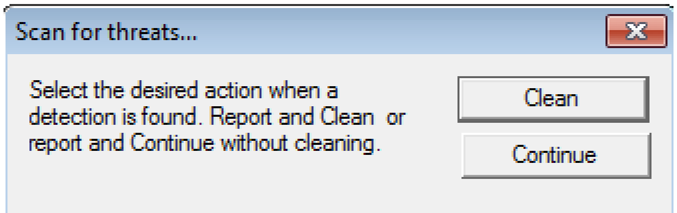
Assign Unique Identifier

Assign a unique identifier to disc. (See Appendix A. Unique Identifier.) If you are working with multiple discs or other types of media, it is fine if you need to revise the unique identifier later in the workflow as you determine what to retain or deaccession.

Run Virus Scan

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

Right-click the optical disc drive in file explorer and select **Scan for threats**. 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.

Notes

- If the only file on the disc in file explorer is a tiny file with a *.cda extension, you are dealing with a CD-DA (Compact Disc Digital Audio) formatted disc. The *.cda file is created by Microsoft Windows as a pointer to the audio track. The files in the audio track can be viewed with CDCheck. Work on Fluffy with the Ethernet cord disconnected and use CDCheck to extract the audio track file(s) (not the *.cda file) to an empty external drive. Run a virus scan on those files. Use CDCheck to compare exported files against the original files.

- If the only files that appear on the disc in file explorer are autorun.inf and udfrinst.exe, you can 1) install a UDF reader from https://www.roxio.com/en/support/software-updates/udf/ and run a virus check on the now visible files or 2) work on Fluffy, which should have the UDF reader already installed.

- If the disc drive is making a lot of noise and the virus scan is taking longer than usual, you may have a bad disc. Eject and reinsert the disc and rerun the virus scan or try using a different optical drive. If the virus scan still does not complete, use an air canister to blow any dust or dirt off the disc. You can also try wiping the disc with a lint-free cloth in a radial (from inner to outer edge) rather than circular direction. If you still experience problems, work on Fluffy (make sure Ethernet cord is disconnected) and follow the instructions in the File transfer section. Export files to an empty external drive and run the virus scan on the exported files before you perform the file verification process. If you are unable to export files, follow Image disc instructions for creating and mounting a disc image. Run a virus scan on the mounted virtual drive.

If one or more viruses are found, save a log of the infected files as "[unique identifier]_viruslog" in "[accession #]_documentation" folder on ira_locked.

There are four options for dealing with the infected disc. Discuss with the head of Institutional Archives as needed.

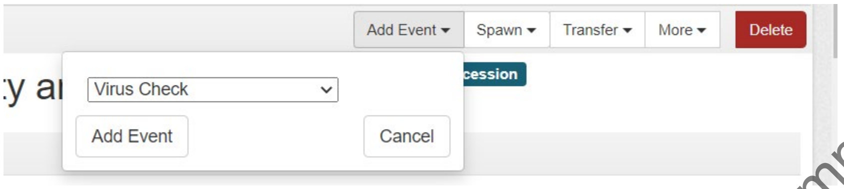
- Keep and clean the infected file(s). Working on Fluffy (make sure Ethernet cord is disconnected), follow instructions in the Transfer files section to transfer all files from the disk to an empty external drive. Before running file verification, rerun the virus scan on the external drive and have the antivirus program clean the infected file(s). After you have transferred files to ira_locked, reformat the external drive.
- Do not transfer infected file(s) from disc. Follow instructions in Transfer files section and transfer all but the infected files.
- If cleaning an infected file is not an option and it needs to be retained, follow instructions in Image disc section to create a disc image and only access the infected file through the image using Forensic Toolkit.
- Deaccession the disk.

Record virus check activities in the accession record in ASpace. In the **Digital File Mgmt Notes** field, record which discs were scanned, whether or not viruses were found, date of scan, and your initials. This step can be done after all discs have been scanned.

Examples:

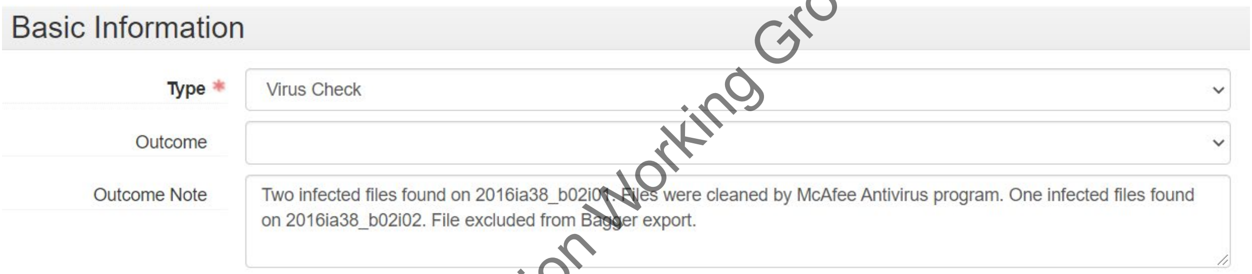
“A virus scan was completed on all discs, and no viruses were found. 4/13/2018 LW”
“10 of 30 discs were scanned for viruses. Viruses were found on 2 disks. 4/13/2018 LW.”

If a virus was found, you will also need to add a **Virus Check** event.



Virus Check

Only one **Virus Check** event is needed for an accession. Leave **Outcome** blank and describe all actions taken on infected files.



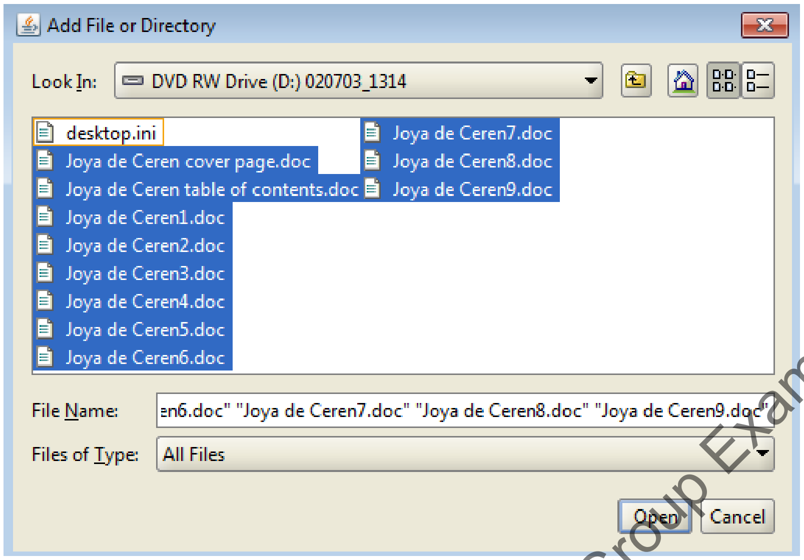
Type *	Virus Check
Outcome	
Outcome Note	Two infected files found on 2016ia38_b02i01. Files were cleaned by McAfee Antivirus program. One infected files found on 2016ia38_b02i02. File excluded from Bagger export.

Enter date or date range of virus check and add your name under **Agent Links**, with the role as **Implementer**.

Transfer files

In most cases you will use Bagger to copy files from disc. For Blu-Ray, use FTK Imager to export files from the disc [need to verify if can use CDCheck or IsoBuster]. See notes in virus scan section if disc contains *.cda or autorun.inf/udfrinst.exe files. You will also create a disc image if the CD or DVD contains software files or interactive features that we want to preserve.

Follow Bagger instructions for creating a bag. Exclude desktop.ini and autorun.inf if present.



Add File or Directory

Look In: DVD RW Drive (D:) 020703_1314

desktop.ini
Joya de Ceren cover page.doc
Joya de Ceren table of contents.doc
Joya de Ceren1.doc
Joya de Ceren2.doc
Joya de Ceren3.doc
Joya de Ceren4.doc
Joya de Ceren5.doc
Joya de Ceren6.doc
Joya de Ceren7.doc
Joya de Ceren8.doc
Joya de Ceren9.doc

File Name: en6.doc" "Joya de Ceren7.doc" "Joya de Ceren8.doc" "Joya de Ceren9.doc"

Files of Type: All Files

Use the unique identifier as the bag name. If you are working on a computer connected to the network, save the bag to the "[accession#]_original" folder on ira_locked. If you are working on Fluffy, save the bag to an external drive. Connect the drive to a networked computer and move the bag to ira_locked. Validate and maintain files in bag.

Troubleshooting transfer problems.

This section provides options for extracting as much data as possible from a corrupt disc. Use your best judgement in determining how much time and effort to put into troubleshooting disc problems. Depending on the research value of the disc contents you may choose to salvage as much data as you can, decide the corrupt files are not worth preserving, or deaccession the disc. Make sure to track all decisions and actions in ASpace.

Optical discs can be finicky, particularly when using Bagger. If the disc drive is making more noise than usual and Bagger's progress bar doesn't appear after 5 minutes, you may need to try the following:

- Eject and reinsert the disc and rerun Bagger.
- Use a different optical drive, including the one on FRED.
- Clean the disc using an air canister or wiping the disc with a lint-free cloth in a radial (from inner to outer edge) direction.

If you are still unable to copy files from a disc with Bagger, use CDCheck, IsoBuster, or FTK Imager (in that order) to extract the files. (If using IsoBuster or FTK Imager, see File systems section to determine which files to export.) To get the most data that you can from the disc, you may need to try all the tools, as well as manually copying files from the disc using the copy and paste function if the disc is particularly problematic. There have been cases where one tool exported more files than another tool, but more files were also corrupt.

Use BeyondCompare (folder compare with binary comparison) to verify the exported files against the files on the disc. (You may also use CDCheck's comparison feature, but BeyondCompare has a better interface.) You may need to re-export a file if there's an error. You can try exporting again with the same or different software. Note that for bad discs, fixity verification can be unreliable as the disc drive may read a file on a corrupt sector differently each time, giving false mismatch errors for exported files. In such cases you may want to use BeyondCompare's file comparison (for text, images, and spreadsheets) to confirm that the content of files match. You may choose to preserve a corrupt file if you are unable to export a pristine version of the original file, but you will need to note this in the **Digital File Mgmt Notes** field in ASpace. File fixity problems and other transfer issues should always be noted in ASpace.

Bag the exported files as instructed above for storage on ira_locked.

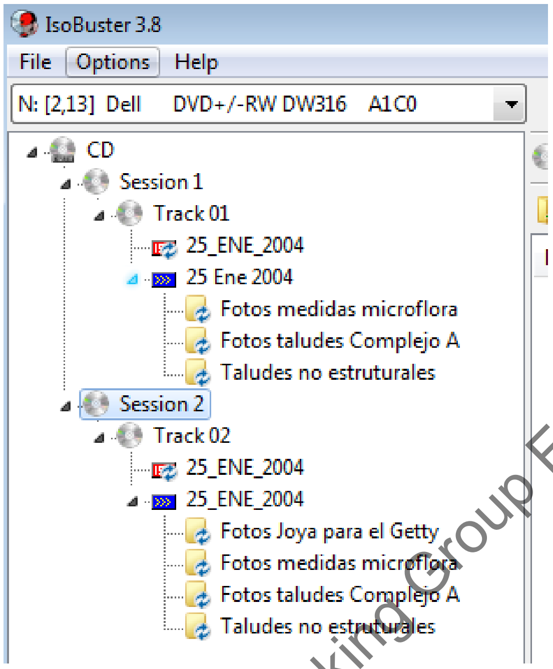
If you are still unable to transfer files, and the files on the disc are readable, you may want to create a disc image.

Image Disc

Only create a disc image if there are problems extracting files from a disc or if the disc contains software files or interactive features that you want to preserve. Use IsoBuster to create a disc image. If IsoBuster does not work, use FTK Imager. Guymager through BitCurator is a third option if you really need to create a disk image and you experience problems with the other two software. (This manual does not cover Guymager but Lorain can assist you with this.)

Before imaging, check if the disc has multiple sessions. The disc creator may have burned files to a disc in one session and added/edited files in a later session. The first session only lists files from the initial burn while the second session will contain files from both the first and second sessions. FTK Imager is only able to image the first session. IsoBuster might be able to image the second session but this needs to be confirmed

To determine if a disc contains multiple sessions, load the disc in IsoBuster or add as an evidence item (select logical drive) in FTK Imager.



After the iso file has been created, mount the image. If on Windows 7, use MagicDisc. If on Windows 10, right-click the iso file and select **Mount**. You should see a new drive appear in file explorer and you will be able to examine the contents of the image as you would with the actual disc.

If you were able to export all the files in the previous section, use BeyondCompare (folder compare with binary comparison enabled) to compare the files on the disc with the files on the mounted image to verify the integrity of the image.

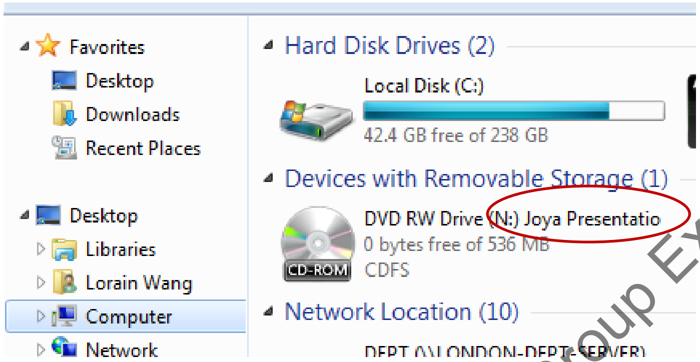
If you were not able to successfully export files from the disc in the previous section, use Bagger to copy the files from the mounted drive. Remember to validate the bag. If you are unable to mount the image, use FTK Imager to export files from the image. Use BeyondCompare (folder compare with binary comparison enabled) to compare exported files with files on the disc. If there are file mismatches, you may need reimage the disc. If you get errors with files exported using FTK Imager, it is possible that the problem is with the export and not the image file. You can verify this by running a comparison on the files on the disc with the files on the mounted image. If the problem is with the export and not the image, you can try exporting the files again with FTK Imager and rerun the comparison.

As noted earlier, file integrity verification can be unreliable for discs with bad sectors. Large amounts of errors may be false mismatches. In such cases you may want to instead use BeyondCompare's file comparison for text, spreadsheets, and images to confirm that the content of files match.

We will preserve the disc image, along the exported files, if the disc contains software files or interactive features that you want to preserve. Depending on research value, we may also want to the preserve the disc image if we are unable to export files that are readable on the disc. Bag the disc image files and exported files as instructed in the Transfer files section for storage on ira_locked.

Transcribe disc labels

Transcribe written information on disc, disc insert, and disc case. You may also want to note the disc's volume label if it provides information about disc contents that cannot be gleaned elsewhere.



If you're not ready to enter this information in a resource record, you can create a spreadsheet to track information for each disc. 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 File Mgmt Notes** field.

Shred or retain disc

Institutional Archives views discs as physical carriers that, in most cases, do not hold artefactual value. Once we have captured and preserved digital content off a disc, the disc can be placed in an Alt Media shred box for destruction. You may choose to retain certain discs if, for example, it has custom labeling and inserts or was created for wide distribution rather than for backup storage. Discuss with the head of Institutional Archives as necessary.

Document transfer activities

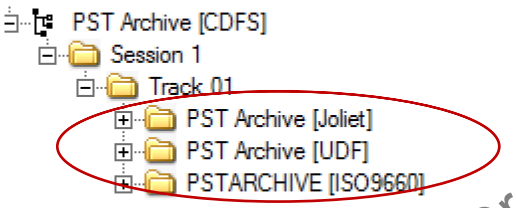
Record transfer activities in the **Digital File Mgmt Notes** field in the accession record in ASpace and make sure that the box next to "Contains digital content" is checked. Include information such as software used, the number of disks worked on, work you've completed, work that needs to be done, any known issues or problems, and whether disks were kept or discarded. Your notes should be clear enough for another archivist to understand what you've done and, if necessary, pick up from where you left off.

Maintain files in bag

Files are maintained in bags so they can be easily validated to verify that files remain unchanged when they are ready to be processed. If you transferred files from multiple discs and do not plan on processing files immediately, maintain files in a bag at the level that is most practical for validating. Depending on the number of discs, this will vary from maintaining bags at the disc level to a single bag for the entire set of discs. If you decide to create one giant bag for all the discs, you can choose to bag all files within their individual bags or remove files from their bag structure. If removing files from their bag structure, do not delete the bag tags. Move them to the documentation folder, organizing them by unique identifier.

File systems

When viewing the contents of a CD or DVD using software such as IsoBuster or FTK Imager, you may see something like this:



```
PST Archive [CDFS]
  Session 1
    Track 01
      PST Archive [Joliet]
      PST Archive [UDF]
      PSTARCHIVE [ISO9660]
```

As you click through each tree, you'll notice that the folder structure and files are the same, although the filenames may look slightly different. While it may appear that there are multiple sets of files on the disc, this is not the case. There is only one set of files but there are multiple file systems used to store information on the disc. The above square brackets indicate the file system names. While certain file systems can be only read by specific operating systems, they are all readable when using IsoBuster, FTK Imager, and Forensic Toolkit. (See end of this section if you would like more information on each of the common file systems used on optical discs.)

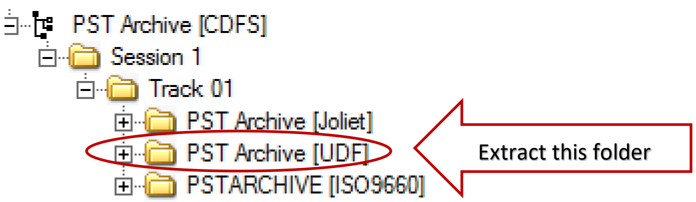
When exporting files, export at the file system level. Do not extract files at the Track 01 level or higher as that will result in multiple sets of the same files. Because filenames may be truncated in the earlier file systems, select the file system that has the least restrictive filenaming rules.

Use the following chart to determine which file system to extract:

Extract	File system
1st choice	UDF
2nd choice	Joliet
3rd choice	ISO 9660
+ when present*	HFS

*Extract HFS when present along with one of the other three file systems if you want to retain compatibility to MacOS.

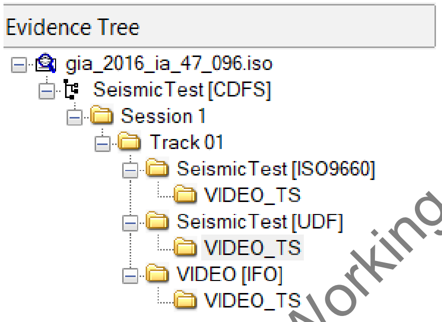
In this example, you would extract folder PST Archive [UDF]:



```
PST Archive [CDFS]
  Session 1
    Track 01
      PST Archive [Joliet]
      PST Archive [UDF]
      PSTARCHIVE [ISO9660]
```

Extract this folder

If you come across IFO as listed below, it can be ignored as it is not a file system but a set used for stand-alone DVD players. This is not to be confused with files with IFO extensions which should be preserved.



```
Evidence Tree
gia_2016_ia_47_096.iso
  SeismicTest [CDFS]
    Session 1
      Track 01
        SeismicTest [ISO9660]
          VIDEO_TS
        SeismicTest [UDF]
          VIDEO_TS
        VIDEO [IFO]
          VIDEO_TS
```

If your disc contains file systems that are not covered in the above chart, examine and compare the file and folder names of each file system folder. Select the file system folder with the most complete names.

Common File Systems on Optical Discs

ISO 9660 is the original file system standard for CD data discs and was first published in 1988. It is sometimes referred to as CDFS (Compact Disc File System), not to be confused with the virtual Linux file system (CDFs). The standard was developed to enable multiple computer operating systems to read files on a disc. Three "levels of interchange" are described in the standard. Level 1 provides compatibility with the largest number of operating systems but is also the most restrictive in terms of file and directory name rules. Directory and filenames are limited to eight characters, with a three-character extension for filenames, which is in accordance with MS-DOS's restrictive file naming rules. Original file and directory names that exceed eight characters will appear abbreviated with a "~". Characters for filenames can also only contain uppercase letters, digits, or an underscore. Levels 2 and 3 have the same limitations of character type for filenames but allow for 30 characters in directory and filenames.

Joliet is an extension to the original ISO 9660 standard and was developed in 1995 by Microsoft for Windows 95 and later Windows operating systems. Joliet supports longer filenames, up to 64 characters, as well as spaces and Unicode characters (this includes diacritics and non-Latin script). Joliet is backwards compatible because filenames are saved in a supplementary volume descriptor that is ignored by ISO 9660. Thus you will see both ISO 9660 and Joliet directory and filenames listed in separate trees on the disc.

UDF (Universal Disk Format) is a file system standard that was introduced in 1995 and has since replaced ISO 9660. It is widely used on DVDs. A major advantage of UDF is that it can be used for packet writing technology – basically files can be created, modified, or deleted on a disc like on your local computer hard drive without burning an entire disc. Files can be dragged and dropped or copy and pasted to the CD using UDF-compatible applications. UDF can also support filenames up to 255 characters. Older optical drives and operating systems are unable to read UDF formatted discs and may display filenames in the Joliet format. Discs with UDF often contain ISO 9660 to allow for backwards compatibility.

HFS (Hierarchical File System) is a Macintosh file system released in 1985. The character limit for filenames is 31. PCs are unable to read HFS formatted discs, although it is possible using Isobuster or FTK Imager. You will sometimes see hybrid discs with both HFS and ISO 9660/Joliet so that the discs are readable on PCs and Macs. HFS should be exported if it is important to maintain compatibility with MacOS.

References

http://www.avpreserve.com/wp-content/uploads/2014/04/OpticalMediaPreservation.pdf

https://books.google.com/books?id=jw7yCQAAQBAJ&printsec=frontcover#v=onepage&q&f=false

II.D. Computer (Internal Hard Drives)

Overview

Getty Digital assists Institutional Archives in harvesting data from the hard drives of departed staff. Currently, data is extracted using CrashPlan, a software that automatically backs up data on the local drive. CrashPlan, which was implemented by Getty Digital in 2016, scans the entire drive and ignores system folders, other folders that were created by Getty Digital [not always the case], and deleted folders. Files are transferred by Getty Digital to \\LONDON-RETAIN-SERVER\retain using Robocopy. (Note that Getty Digital also adds files stored in departed staff's personal network drive, Box account, and Google Drive.)

Prior to CrashPlan, Getty Digital (then known as ITS), would remove drives from computers and periodically send the accumulated drives to IA. We would then create a forensic image of the drives. In 2016, we returned the drives to ITS so that they could copy Groupwise emails for migration to Outlook. The systems administrator also manually searched at the root level and in user folders for data to copy to \\LONDON-RETAIN-SERVER\retain. We are retaining these copies for the archives and deleting the forensic images.

Files are transferred by Lorain from \\LONDON-RETAIN-SERVER\retain to \\prd-arj\wbench1\processing\Staff_harddrives for IA staff to process. Tools used to transfer files include Bagger, QuickHash, and Robocopy. QuickHash or command-line tool CFV were used to generate and verify checksums. Hard drives often take multiple days or weeks (sometimes over a month) to transfer completely and we frequently encounter problems during transfer. Files are not saved to ira_locked because 1) we only want to move the files once, 2) an untouched copy is on the Retain server, and 3) our goal is to ingest them in Rosetta as quickly as possible to reduce our backlog and clear up storage space. Once files are deposited in Rosetta, the hard drives are deleted from wbench1 and the Retain server.

Workflows are listed below in the rare event that we may need to transfer files from the internal hard drive of a computer. For example, preserving a complex database may require that we image the entire computer.

For hard drives removed from a computer, we will connect the drive to FRED and use FTK Imager to create an image. To transfer files from the local drive of a Windows computer, we will primarily use ADTriage and Bagger.

Transfers from a Windows computer

Use ADTriage or Bagger to transfer files from the local drive of a computer. These tools require that the computer have functioning USB ports. If neither ADTriage nor Bagger work, you may use any of the other transfer tools recommended for network and external drive transfers. For nonfunctioning computers, contact Getty Digital for assistance.

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. This is rare for Institutional Archives but it may be an option we need to pursue to preserve complex software or databases. We may also choose to image a local drive 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.

Virus scan

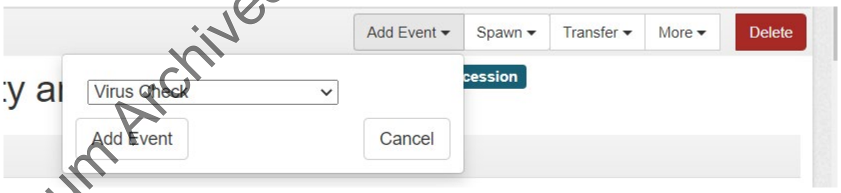
Staff computers connected to the Getty network undergo regular virus scans. Run a virus scan on the computer if it has not been connected to the network for some time or some of the files on the computer look suspicious. Connect the computer to the network and open McAffee. Run updates on the program and then click **Scan System**. Select **Full Scan**. Choose to clean infected files.

If one or more viruses are found among the files that you are grabbing, save a log of the infected files as “[unique identifier]_viruslog” in “[accession #]_documentation” folder on ira_locked.

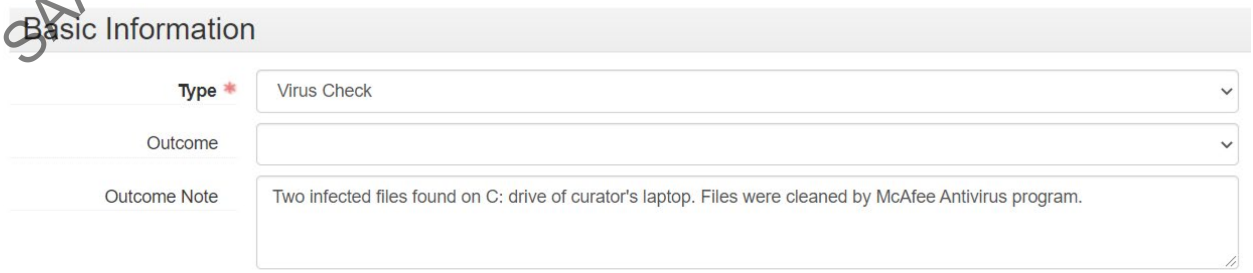
Record virus check activities in the **Digital File Mgmt Notes** field in the accession record in ASpace. Note whether or not any of the files that you are transferring were infected, date of scan, and your initials.

> Example:
> “A virus scan was completed on the C: drive and 1 virus was found. 4/13/2018 LW”

If a virus was found on a file that you are transferring, you will also need to add a **Virus Check** event.



Only one **Virus Check** event is needed for an accession. Leave **Outcome** blank and describe all actions taken on infected files.



Basic Information

Type *	Virus Check
Outcome	
Outcome Note	Two infected files found on C: drive of curator's laptop. Files were cleaned by McAfee Antivirus program.

Enter date or date range of virus check and add your name under **Agent Links**, with the role as **Implementer**.

Workflow for ADTriage

Use for 1) imaging the computer, 2) copying files that meet search criteria, or 3) bypassing Windows login. For instructions, see ADTriage_guide.pdf in \\LONDON-DEPT-SERVER\DEPT\GRI\Institutional Archives\ADMINISTRATION\ADM-135 Policies Procedures Adm\Archives_Policies_procedures_ manuals\Manuals_Current\BornDigital.

1. Use existing Triage device with default Institutional Archives profile for simple imaging of a computer. This will create an E01 image. If you would like to set up search criteria, create a new profile and create a new Triage device. Make sure the capacity of the Triage device is large enough for the file transfer.
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. a. Export files from AD1 images as soon as possible using FTK Imager. AD1 is a proprietary format and is not ideal for long term preservation. You may use Forensic Toolkit instead if you would like to search for files with sensitive information and weed non-archival files.

   b. Export files from E01 images using Forensic Toolkit. Only export files from E01 images after files have been appraised and non-archival files have been identified in Forensic Toolkit. (See section III.B. of IA Electronic record accessioning.pdf (\\LONDON-DEPT-SERVER\DEPT\GRI\Institutional Archives\ADMINISTRATION\ADM-135 Policies Procedures Adm\Archives_Policies_procedures_manuals\Manuals_Current\BornDigital) for more thorough guidance on using Forensic Toolkit for appraisal.)
6. Save exported files to "[accession #]_original" folder on ira_locked and bag in place if possible. Validate bag and maintain files in bag. If files are too large for bagging, use QuickHash, Karen's Directory, or any other tool that can generate a manifest that contains checksums, file names, and file paths. Name the file "[accession #]_manifest" with the appropriate extension and save in "[accession #]_documentation" folder on ira_locked.
7. In ASpace use the **Digital File Mgmt Notes** field under the User Defined section of the accession record to document work you've completed, tools you used, work that still needs to be done, and any known issues or problems. Your notes should be clear enough for another archivist to understand what you've done and, if necessary, pick up from where you left off. Also make sure that the box next to "Contains digital content" is checked

Workflow for Bagger

Use for transferring known files in known location(s) with Windows login access

1. Set up Bagger on target computer or run Bagger off of flash drive. Use unique identifier as bag name.
2. If computer is connected to the network, see if you can log into your network drives and save files to "[accession #]_original" folder on ira_locked. If not, save to external drive and then transfer files in bag to ira_locked.
3. Validate the bag to verify files were properly transferred.
4. Maintain files on ira_locked in bag.
5. Delete Bagger program and profile files from staff computer if necessary.
6. In ASpace use the **Digital File Mgmt Notes** field under the User Defined section of the accession record to document work you've completed, tools you used, work that still needs to be done, and any known issues or problems. Your notes should be clear enough for another archivist to understand what you've done and, if necessary, pick up from where you left off. Also make sure that the box next to "Contains digital content" is checked

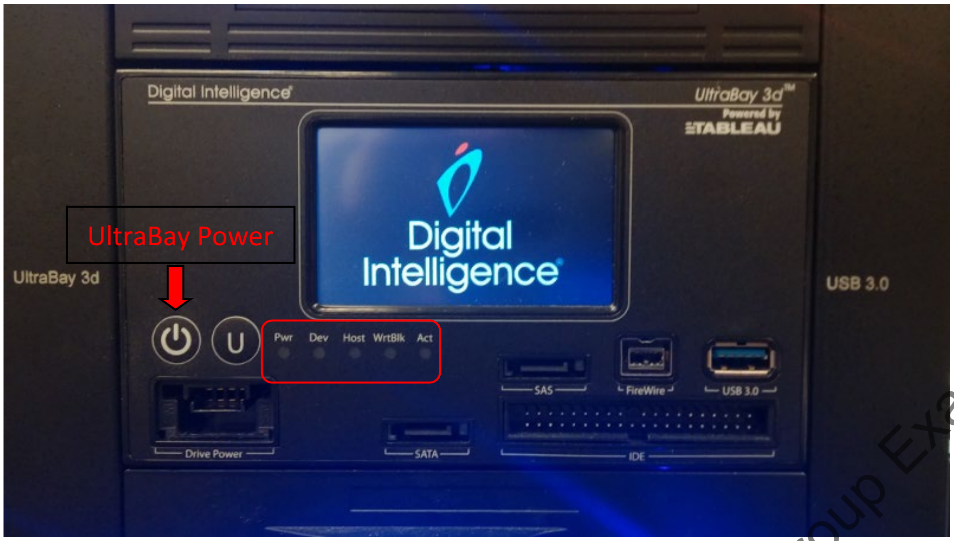
Transfers from internal hard drive

Hard drives removed from computers will be connected to FRED and imaged using FTK Imager. We will create either a forensic or logical image.

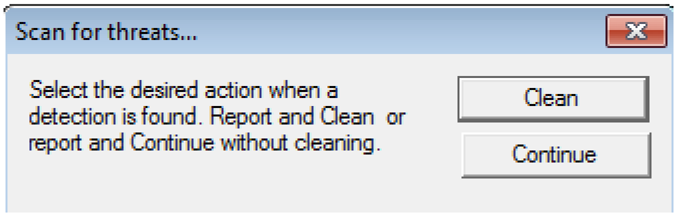
A forensic image is a bit-for-bit copy of the entire drive, which means that it also captures hidden and deleted files and unallocated space. While these are things we typically do not want to keep, creating a forensic image may be necessary for preserving complex databases and software or any other situations in which we are unsure exactly which files we need.

Logical images are essentially copies of visible files and we can specify which files to include in the image. Logical images should be sufficient for most of our needs. The major drawback of logical images is that they are created in AD1 format, which is a proprietary format. Files should be exported from AD1 images as soon as possible.

1. Power on Fred using the rocker switch. Login and password are written on post-it note on pinboard.
2. Confirm that the UltraBay is off (led lights are unlit) and connect the drive to one of the ports in the UltraBay 3D. Ultrabay includes hardware write blocking and ports to allow connections of internal hard drives (IDE, SATA, SAS), USB 3.0/2.0/1.1, and FireWire 400/800. We have various types of connectors stored in a box at the FRED workstation. You will need to closely examine your hard drive to determine which connector to use.



3. Once you have connected the drive, press the power button for the UltraBay. If the hard drive is correctly connected and fully functioning, the 4 left LEDs on the UltraBay will light up green.
4. Use FTK Imager to create either a forensic (select **Physical Drive**) or logical (select **Contents of a Folder**) image. The far-right LED will light up red during imaging. If the red light shuts off during the imaging process, it is an indication of hard drive failure.
5. If imaging fails, try rebooting FRED or reimage on another day. If still unsuccessful after multiple tries, try using Tableau Imager. Click the Tableau Imager icon on the desktop to launch the program. The touch display on FRED should now provide options for selecting a drive to image. You may proceed with imaging using the regular software or through the UltraBay touch display.
6. Once imaging has been completed for the drive, hold down the power button to the UltraBay 3d to turn it off before disconnecting the hard drive.
7. View and export contents of image to an empty external drive using Forensic Toolkit.
8. Connect drive to Fluffy (do not connect through Tableau write-blocker), making sure the ethernet cord is disconnected. Right-click the drive in file explorer and select **Scan for threats**. A message box will appear. Select **Continue** and the virus scan will begin.

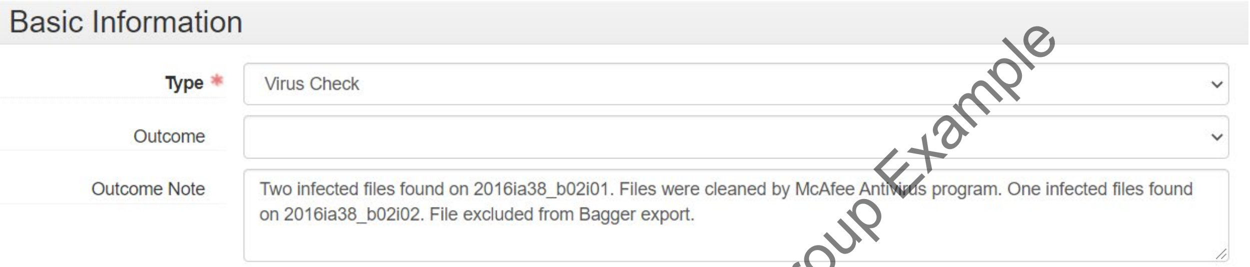


Select the desired action when a detection is found. Report and Clean or report and Continue without cleaning.

If one or more viruses are found, save a log of the infected files as “[unique identifier]_viruslog” in “[accession #]_documentation” folder on ira_locked. You can choose to have the antivirus program clean the infected file or you may choose to delete the file.

In the ASpace accession record, document virus check activities in the **Digital File Mgmt Notes** field, specifying what was scanned, whether or not viruses were found, date of scan, and your initials.

If a virus was found, you will also need to add a Virus Check event. Only one Virus check event is needed for an accession. Leave **Outcome** blank and describe all actions taken on infected files.



Basic Information

Type *	Virus Check
Outcome	
Outcome Note	Two infected files found on 2016ia38_b02i01. Files were cleaned by McAfee Antivirus program. One infected files found on 2016ia38_b02i02. File excluded from Bagger export.

Enter date or date range of virus check and add your name under **Agent Links**, with the role as **Implementer**.

9. Transfer files to "[accession #]_original" folder on ira_locked. See Transfer files section of External Drive for instructions on transferring files from external drive to ira_locked.
10. In ASpace use the **Digital File Mgmt Notes** field under the User Defined section of the accession record to document work you've completed, tools you used, work that still needs to be done, and any known issues or problems. Your notes should be clear enough for another archivist to understand what you've done and, if necessary, pick up from where you left off. Also make sure that the box next to "Contains digital content" is checked

II.E. External Drive

Overview

This section 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.

Whenever possible, connect the drive to a write-blocker. We will primarily use Bagger to transfer files. See troubleshooting section if you have problems accessing files through file explorer.

If dealing with a Mac-formatted drive, see also Transferring Mac files section of II.F. Network Drive.

Workflow

Assign a unique identifier to drive.

Assign a unique identifier if you need to track which files came from which piece of media. (See Appendix A. Unique Identifier.) This is more likely if you have several flash drives as opposed to high capacity external drives used by the department to transfer files to IA. For the latter case, other than an accession number, a unique identifier may not be necessary. You may, however, still want to distinguish a batch of files from other transfers for administrative control on ira_locked by using descriptive folder names (i.e. topic, date, or media). In deciding whether or not to assign a unique identifier, consider how you want to organize and describe files from the hard drive and any other media in the accession in the finding aid. Use your best judgement and discuss with the head of Institutional Archives as needed.

Attach to write-blocker

Connect the external drive to your computer using the Tableau USB bridge for write-blocking protection. The Tableau device is stored in a box in the cabinet next to Fluffy and can be used on any computer.

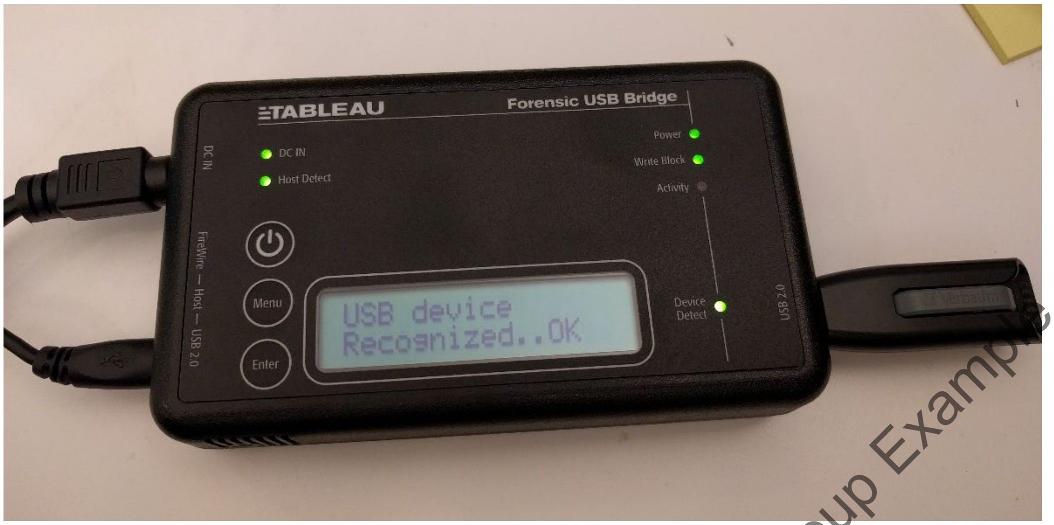
If you have trouble getting Tableau or your computer to recognize the drive, you can try connecting the external drive to FRED through the UltraBay, which has a built-in write blocker. For this method, you will only be able to use FTK Imager and not Bagger to transfer files.

If you are dealing with a Mac-formatted drive, connect the drive to a computer with MacDrive.

See Troubleshooting section if you still encounter problems accessing files on the drive.

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. If the drive does not appear in file explorer, see Troubleshooting section.

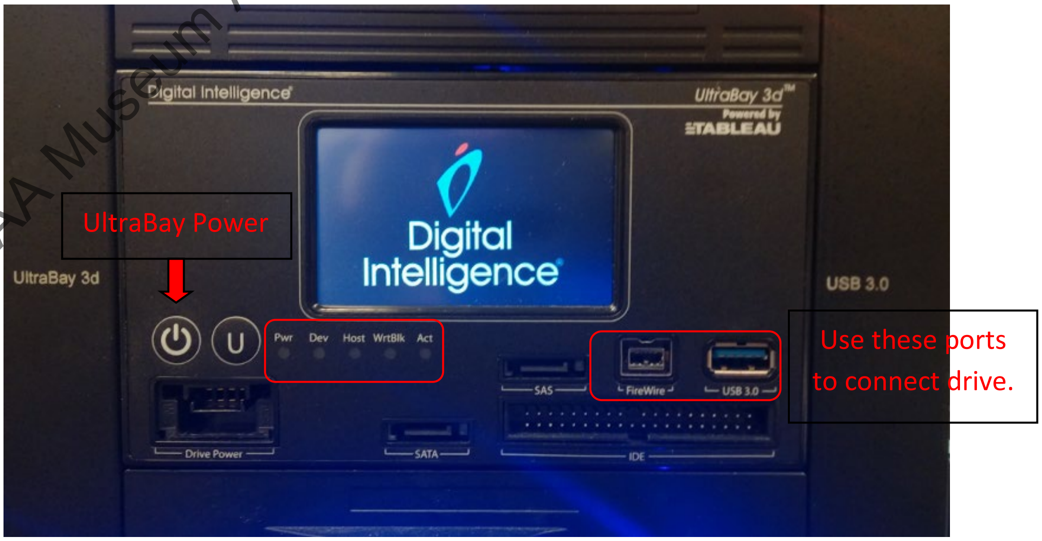


5. To remove the external drive, eject the Tableau device using the **Safe Remove Hardware** utility on your computer. Turn the Tableau device off and remove the external drive.

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. Power on Fred using the rocker switch. Login and password are written on post-it note on pinboard.
2. Confirm that the UltraBay is off (led lights are unlit) and connect the external drive to the USB or FireWire port in the UltraBay.
3. Press the power button on the UltraBay. The Act light should come on if the UltraBay recognizes the drive.



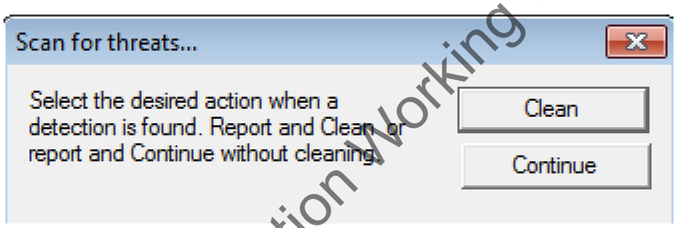
MacDrive

1. Open MacDrive and click on **Settings→Advanced MacDrive Settings**.
2. Click **Yes** in the **User Access Control** window that pops up.
3. In the **MacDrive Options** window under **Advanced**, check the box next to **Prevent changes to all Mac disks (read-only)**. Click **OK**.

Run virus scan

Run a virus scan on the external drive before transferring or examining files. (If drive is connected to FRED through the UltraBay, you will run the virus scan after exporting files from the image to an empty external drive. Use Fluffy to run the virus scan on the exported files.)

Right-click the drive in file explorer and select **Scan for threats**. 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.

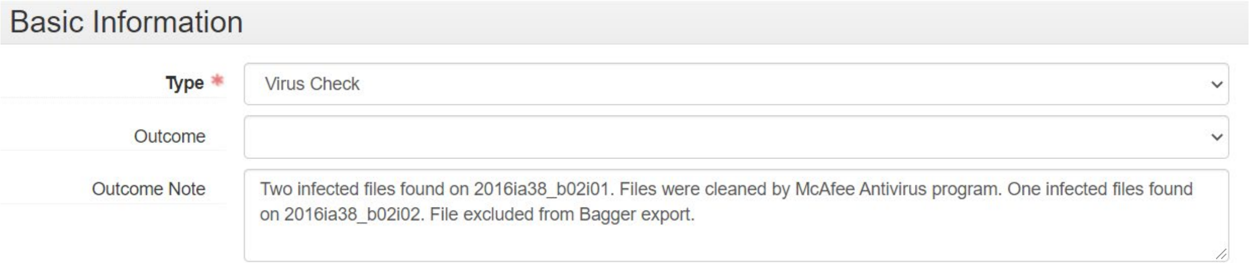
If one or more viruses are found, save a log of the infected files as "[unique identifier]_viruslog" in "[accession #]_documentation" folder on ira_locked.

You can choose to have the antivirus program clean the infected file or exclude it from your transfer. Connect the drive directly to the computer to allow the antivirus program to clean the file.

Record virus check activities in the accession record in ASpace. In the **Digital File Mgmt Notes** field, record which disks were scanned, whether or not viruses were found, date of scan, and your initials. This step can be done after all discs have been scanned.

This can be a general note, such as "A virus scan was completed on all USB drives, and no viruses were found. 4/13/2018 LW" or "External hard drive was scanned for viruses. Viruses were found. 4/13/2018 LW."

If a virus was found, you will also need to add a Virus Check event. Only one Virus check event is needed for an accession. Leave **Outcome** blank and describe all actions taken on infected files.



Basic Information

Type *	Virus Check
Outcome	
Outcome Note	Two infected files found on 2016ia38_b02i01. Files were cleaned by McAfee Antivirus program. One infected files found on 2016ia38_b02i02. File excluded from Bagger export.

Enter date or date range of virus check and add your name under **Agent Links**, with the role as **Implementer**.

Transfer files

Use FTK Imager to image the drive if you are connected to the Ultrabay on FRED. Otherwise, we will primarily use Bagger to transfer files from an external drive to the "[accession#]_original" folder on ira_locked. Use the accession number or unique identifier, if one was assigned, as the bag name or name the bag by topic, date, and/or media to distinguish it from other transfers in the accession.

Under certain circumstance you will want to use a different transfer tool. Check for the following before running Bagger:

1. Examine the file/folder names and folder structure and determine if you need to run the Path Length Checker Tool to verify that file paths do not exceed character limits. (See Appendix B. File Path limits for instructions.) Bagger will stop running if it encounters a file path that is too long.

2. Determine the total size that you are transferring. In file explorer, either right-click the drive or, if you are not transferring everything from the drive, right-click the folder(s). Click **Properties** to locate the size. Bagger does not work well for large transfers. It takes longer than standard transfer processes because it also generates a list of checksums. The size at which Bagger transfers become difficult varies by computer, internet bandwidth, and the external drive. If you run Bagger and the progress bar has not appeared after a few hours, you may want to take a different approach. You can run Bagger overnight but you run the risk of network connections breaking causing the bagging process to fail.

Transferring large volumes

For transferring large volumes, you may want to transfer files in multiple bags or create a holey bag, where the checksums are generated first by Bagger and the files are transferred at a later time. Alternatively, you can use Robocopy, a command-line tool that can resume incomplete transfers. Because of the resume feature, Robocopy is strongly recommended for particularly large transfers.

Transferring files with long file paths

If there are files with character limit issues, do not change folder/file names. Use QuickHash to transfer files. Note that QuickHash is able to transfer files with long file paths depending on the file system of the external drive. If the file system of the external drive prevents this type of transfer, you will need to experiment with mapping virtual drives to specific folders as explained in Appendix B. File path limits. If mapping virtual drives does not work, try the other methods listed in Appendix B.

Transferring large volumes with files that have long file paths

If transferring a large volume of files that also have file path length issues, use Robocopy. Note that as with QuickHash, Robocopy's ability to transfer files with long file paths depends on the file system of the external drive. You may need to experiment with mapping virtual drives to specific folders or follow other methods described in Appendix B. File path limits.

Method of last resort

If you encounter problems in transferring files from the drive using Bagger, QuickHash, and Robocopy, as a last resort you may want to image the entire drive using FTK Imager and export files from the image using FTK Imager. If you would like to examine the files before exporting, use Forensic Toolkit.

Verify transfer

For Bagger transfers, validate and maintain files in the bag.

For non-Bagger transfers, use BeyondCompare's folder comparison to verify that all files have been transferred. Verify file fixity by using QuickHash to compare checksums.

Remove or retain external drive

Once you have captured, verified, and preserved digital content from the media, you may return the external drive to the originating department. If they do not want the drive, we can either keep the drive to reuse (make sure to reformat the drive first) or place it in an External Drive "shred" box. When the box is full, we will contact Shane Greene (ITS), who has a hard drive degausser.

Institutional Archives views external drives as physical carriers that, in most cases, do not hold artefactual value. 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. Discuss with the head of Institutional Archives as necessary.

Document actions in ASpace

In the ASpace accession record use the **Digital File Mgmt Notes** field under the User Defined section of the accession record to document work you've completed, tools used to transfer and verify checksums, work that needs to be done, what was done with the drive after file transfer was completed, and any known issues or problems. Your notes should be clear enough for another archivist to understand what you've done and, if necessary, pick up from where you left off. Make sure that the box next to "Contains digital content" is checked

Troubleshooting drive problems

Connect the drive directly to your computer if Tableau does not recognize the drive. If it does not appear in file explorer, open the Control Panel and click on "View devices and printers" under "Hardware and Sound."

<u>If the drive does not appear in the device list, check for the following hardware/cable/port issues:</u>

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 make sure cables are plugged all the way in.

Malfunctioning or incompatible port. 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. You may need to also plug into different ports or try different computers.

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 Getty Digital.

<u>If the drive appears under the device page but not in file explorer, the problem may be due to software/computer settings issues.</u>

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. Try searching the model number of the external drive online for an updated version of the driver.

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**.

Mac formatted drive. Check if FTK Imager recognizes the drive as a physical drive. Click **File→Add Evidence Item→Physical Drive**. If FTK Imager is able to load the drive, look at the Evidence Tree pane for the file system type. If HFS is listed, you're dealing with a Mac formatted drive. You will need to use MacDrive to access the drive. The software is available on Fluffy. We also may have licenses available to install on your computer. With MacDrive you will be able to transfer files using our standard transfer tools. If for some reason you're not able to use MacDrive, you can use FTK Imager to export the files. If using FTK Imager, make sure to also export the file hash list and use QuickHash to compare checksums of the exported files against the list.

II.F. Network Drive

Overview

Bagger is our preferred tool for transferring files from a network drive. Other software is recommended for dealing with very large transfers and file paths that exceed maximum character limits; these are noted below.

Transferring Mac files

Before you begin transferring files, determine whether you are working with files primarily created on a Mac computer. This is usually indicated by the presence of resource forks or a folder named "__MACOSX". Resource forks are files that begin with a "._" and are accompanied by a second set of files similarly named but without the "._" at the beginning. Sometimes both sets are in the same folder, in parallel subdirectories, or the resource forks are stored separately in a "_MACOSX" folder. The second set of files is important as not all files that begin with a period and underscore are resource forks. (To see resource forks on a PC, your computer settings must be set to view hidden files. Click on **Control Panel → Folder options →View**. Uncheck "Hide protected operating system files." Under **Hidden files and folders** select "Show hidden files, folders, and drives.")

Resource forks typically can be deleted if they are only a few KB in size. For example, it should be safe to delete resource forks for standard documents and image files. (You do not need to delete resource forks until processing and prepping files for deposit in Rosetta.) There are instances, however, where they are necessary for the original file, such as a font file or software, to run properly. The resource forks may also contain information on how files are displayed in a Mac environment if the file creator used color coding and special labels to organize their files. If possible, discuss with the file creator if they used these features and if so, whether this information is important to retain. If they want this information retained, make a note in the **Digital File Mgmt Notes** field that the resource forks should not be deleted. You should also make a note in the **Digital File Mgmt Notes** if that information does not need to be retained, although you may still need to keep certain resource forks for files to run properly.

If there are font files that need to be preserved, in addition to keeping the resource forks, some font files need to be zipped on a Mac computer to transfer properly to a Windows environment. To be safe, it is recommended that all font files be zipped prior to transfer. The issue of font preservation is more of a concern for departments such as Publications or web design teams.

Workflow

Access network location

If you do not have access to the network location, ask the department to contact Getty Digital and request access on your behalf.

Transfer files

Use Bagger to transfer files from the network drive to the "[accession#]_original" folder on ira_locked. Save the bag to "[accession#]_original" folder on ira_locked. Use the accession number or unique identifier, if one was assigned, as the bag name or name the bag by topic, date, and/or media to distinguish it from other transfers in the accession. Validate and maintain files in "[accession#]_original" folder on ira_locked.

Before you run Bagger:

1. Examine the file/folder names and folder structure and determine if you need to run the Path Length Checker Tool to verify that file paths do not exceed character limits. (See Appendix B. File Path limits for instructions.) Bagger will stop running if it encounters a file path that is too long.

2. Determine the total size that you are transferring. In file explorer, right-click the folder and click **Properties** to locate the size. Bagger does not work well for large transfers. It takes longer than standard transfer processes because it also generates a list of checksums. The size at which Bagger transfers become difficult varies by computer and internet bandwidth. If you run Bagger and the progress bar has not appeared after a few hours, you may want to take a different approach. You can run Bagger overnight but you run the risk of network connections breaking causing the bagging process to fail.

Transferring large volumes

For transferring large volumes, you may want to transfer files in multiple bags or create a holey bag, where the checksums are generated first by Bagger and the files are transferred at a later time. Alternatively, you can use Robocopy, a command-line tool that can resume incomplete transfers. Because of the resume feature, Robocopy is strongly recommended for particularly large transfers.

Transferring files with long file paths

If there are files with character limit issues, do not change folder/file names. Use QuickHash to transfer files. QuickHash is able to transfer files with long file paths depending on the file system of the source and destination network drive. NcFsd drives (GRI and individual staff drives) will have problems, but NTFS drives (arj1 and wbench1) will not. You can check the file system by right-clicking the drive in file explorer and clicking **Properties**. If the file system of the external drive prevents these type of transfers, you will need to experiment with mapping virtual drives to specific folders as explained in Appendix B. File Path Limits.

Transferring large volumes with files that have long file paths

If transferring a large volume of files that also have file path length issues, use Robocopy. Note that as with QuickHash, Robocopy's ability to transfer files with long file paths depends on the file system of the external drive. You may need to experiment with mapping virtual drives to specific folders as explained in Appendix B.

Verify transfer

For Bagger transfers, validate and maintain files in the bag.

For non-Bagger transfers, use BeyondCompare's folder comparison to verify that all files have been transferred. Verify file fixity by using QuickHash to compare checksums.

Managing folder on network drive

Once the transfer has completed, check if the department wants to keep the folder on the network drive. If the answer is yes, we need to make sure that 1) they do not edit the contents of the folder and 2) that they do not transfer the same folder to us in the future.

Work with the department to develop a procedure for handling files post-transfer. Possible solutions include renaming folders to indicate that the files have been transferred to IA or moving the folders to a directory on their network drive specifically for transferred files. Whatever they choose to do, you should strongly encourage them to put in a request with Getty Digital to lock the folder to prevent staff from editing files and adding new files to the folder.

Document actions in ASpace

In ASpace use the **Digital File Mgmt Notes** field under the User Defined section of the accession record to document work you've completed, tools you used, work that still needs to be done, and any known issues or problems. Your notes should be clear enough for another archivist to understand what you've done and, if necessary, pick up from where you left off. Also make sure that the box next to "Contains digital content" is checked

Include the original file path of the files you transferred in the accession record's **Content Description** field.

II.G. ZIP Disk

Overview

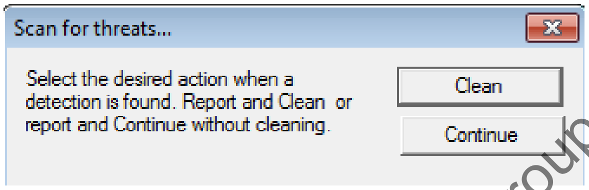
We have one ZIP drive on loan from the Museum. To transfer files from a ZIP disk, connect the ZIP drive to Fluffy or your computer (it does not work on FRED) and use Bagger to transfer files.

Workflow

1. Assign and label ZIP disk with unique identifier.

2. Connect ZIP drive to Fluffy or your computer. (Zip drive does not work with Tableau so we are not able to write-protect the disk.)
3. Run virus scan on disk before transferring or examining files. Do not open any of the files before you have verified that the disk is virus free.

   Right-click the folder in file explorer and select **Scan for threats**. A message box will appear. Select **Continue** and the virus scan will begin.


Scan for threats...

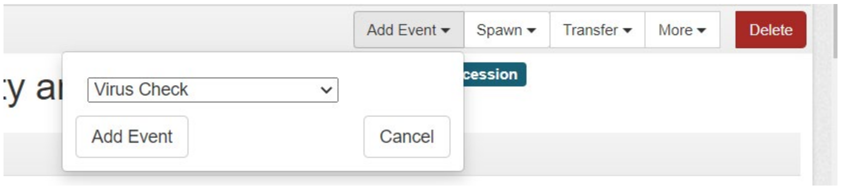
Select the desired action when a detection is found. Report and Clean or report and Continue without cleaning.

4. If one or more viruses are found, save a log of the infected files as "[unique identifier]_viruslog" to "[accession #]_documentation" folder on ira_locked.

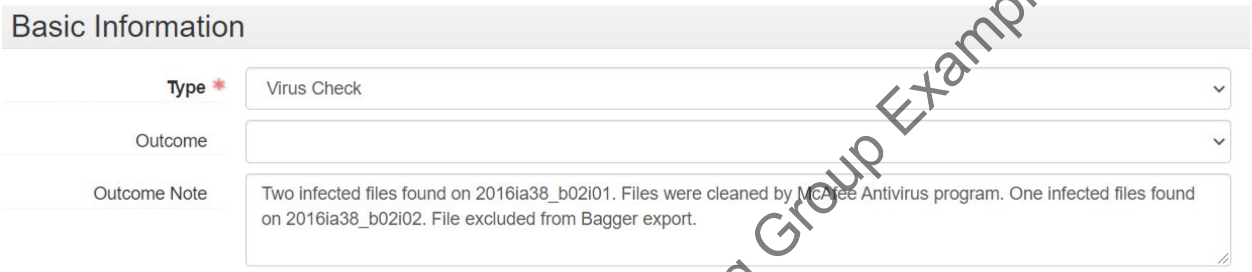
   There are four options for dealing with the infected disk. Discuss with the head of Institutional Archives as needed.
   - Keep and clean the infected file(s). Connect Zip drive to Fluffy, if not already, and make sure the Ethernet cord is disconnected. Following step 5, use Bagger to transfer all files from the disk to an empty external drive. Rerun the virus scan on the external drive and have the antivirus program clean the infected file(s). Reformat the drive once files have been transferred to "[accession#]_original folder" on ira_locked.
   - Do not transfer infected file(s) from disk. During step 5, exclude the infected file(s) from the Bagger transfer.
   - If cleaning an infected file is not an option and it needs to be retained, create an image of the disk using FTK Imager and only view the infected file through the image using FTK Imager (if it's an image or simple text document) or Forensic Toolkit.
   - Deaccession the disk. Record virus check activities in the accession record in ASpace.

In the **Digital File Mgmt Notes** field, record which disks were scanned, whether or not viruses were found, date of scan, and your initials. This can be a general note, such as, "A virus scan was completed on all disks, and no viruses were found. 4/13/2018 LW" or "10 of 30 disks were scanned for viruses. Viruses were found on 2 disks. 4/13/2018 LW."

If a virus was found, you will also need to add a **Virus Check** event.



Only one **Virus Check** event is needed for an accession. Leave **Outcome** blank and describe all actions taken on infected files.



Basic Information

Type *	Virus Check
Outcome	
Outcome Note	Two infected files found on 2016ia38_b02i01. Files were cleaned by McAfee Antivirus program. One infected files found on 2016ia38_b02i02. File excluded from Bagger export.

Enter date or date range of virus check and add your name under **Agent Links**, with the role as **Implementer**.

5. Use Bagger to transfer files. Use the unique identifier as the bag name. If you are working on a computer connected to the network, save the bag to the "[accession#]_original" folder on ira_locked. If you are working on Fluffy, save the bag to an external drive. Connect the drive to a networked computer to move the bag to ira_locked. Validate and maintain files in bag.
6. Shred disk or retain disk in collection. IA views disks as physical carriers that, in most cases, do not hold artefactual value. Once we have captured and preserved digital content off a disk, the disk can be placed in an Alt Media shred box for destruction. You may choose to retain the disk, however, if you believe it should be preserved. Disks with custom labeling, for example, may warrant retention. Discuss with the head of Institutional Archives as necessary.
7. Record transfer activities in **Digital File Mgmt Notes** of accession record in ASpace and make sure that the box next to "Contains digital content" is checked. Include information such as which floppy drive and software were used, the number of disks worked on, work you've completed, work that needs to be done, any known issues or problems, and whether disks were kept or discarded. Your notes should be clear enough for another archivist to understand what you've done and, if necessary, 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 \\prd-arj\arj1\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 File Mgmt Notes** field.
8. Files are maintained in bags so they can be easily validated to verify that files remain unchanged when they are ready to be processed. If you transferred files from multiple disks and do not plan on processing files immediately, maintain files in a bag at the level that is most practical for

validating. Depending on the number of discs, this will vary from maintaining bags at the disc level to a single bag for the entire set of discs. If you decide to create one giant bag for all the discs, you can choose to bag all files within their individual bags or remove files from their bag structure. If removing files from their bag structure, do not delete the bag tags. Move them to the documentation folder, organizing them by unique identifier.

III. SOFTWARE

This part of the manual covers the software referenced in Section II that we use to transfer files, create forensic images, verify fixity, and examine file content. An overview of each tool is provided along with instructions.

To help navigate the large number of tools, the following is a list of recommended tools by function. It is strongly recommended, however, that you still consult Section II for the media you are working with to determine which tools to use.

Transfers

Go-to transfer tool: Bagger

Transfers that won't complete in a day: Robocopy

Transfer files that exceed file path length limits: QuickHash or Robocopy

Transfers that require bypassing Windows login: ADTriage

Extract files from optical disc if Bagger doesn't work: CDCheck

Create image of optical disc: IsoBuster

Create image of internal/external hard drives: FTK Imager

Verifying files (if not using Bagger)

Generate checksum for a single file: QuickHash

Compare checksums of two files: QuickHash

Generate checksums of directory: QuickHash (for comparison and accession documentation) and Karen's Directory (for accession documentation purposes only)

Compare checksums of two directories: QuickHash

Compare folder structure and file names: BeyondCompare

Comparing working folder with original folder: BeyondCompare (with binary comparison turned on)

Compare two documents, spreadsheets, or images based on content: BeyondCompare

Examining files

Examine contents of disk image: FTK Imager (simple image and text files) and Forensic Toolkit (more complex files)

Read Mac-formatted external drives on Windows-based computers: MacDrive

View files without opening: Quick View Plus (not covered in this manual)

A. ADTriage

License is required. We have one license on a dongle. (Product no longer seems to be sold on website.)

Overview

AccessData Triage is a software designed to simplify extraction of data from Windows-based computers with a USB port. Through the AD Triage Administrative Console software, a USB storage device can be configured as a "triage device" to create a bit-level copy (Encase image format) of an entire hard drive or to collect data based on specific criteria, such as file path, file extension, and keywords, when connected to a target computer. It is also able to bypass Windows logins, which is helpful when departments transfer old laptops to us without login information.

For instructions, see ADTriage_guide.pdf in \\LONDON-DEPT-SERVER\DEPT\GRI\Institutional Archives\ADMINISTRATION\ADM-135 Policies Procedures Adm\Archives_Policies_procedures_ manuals\Manuals_Current\BornDigital.

B. Bagger

No license is required.
https://github.com/LibraryOfCongress/bagger/releases/

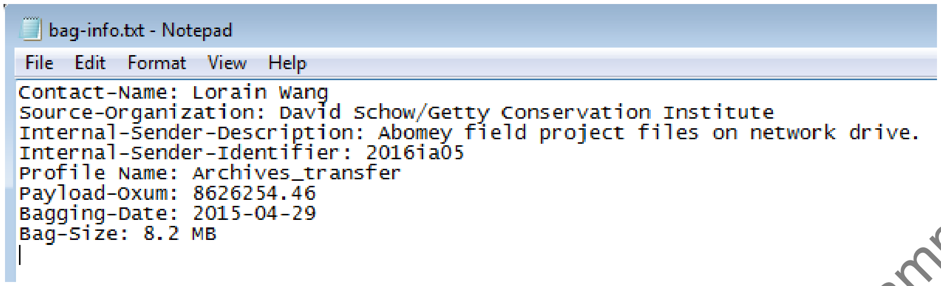
Overview

Bagger is an application based on BagIt, a packaging format developed by Library of Congress for storing and transferring digital files. Bagger includes a validation feature to verify that files were transferred successfully and that no files were lost or corrupted during or since the bagging process. It is the primary transfer tool that we use.

Digital files are packaged into a hierarchical directory structure, called a "bag." A bag consists of the following:

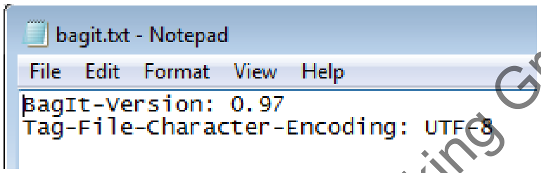
data subdirectory: Contains the transferred files.

bag-info.txt: Provides the number of files in the **data** subdirectory, the size of the bag, the date the bag was created, and any additional metadata fields that may have been assigned by the bag creator.



```
Contact-Name: Lorain Wang
Source-Organization: David Schow/Getty Conservation Institute
Internal-Sender-Description: Abomey field project files on network drive.
Internal-Sender-Identifier: 2016ia05
Profile Name: Archives_transfer
Payload-Oxum: 8626254.46
Bagging-Date: 2015-04-29
Bag-Size: 8.2 MB
```

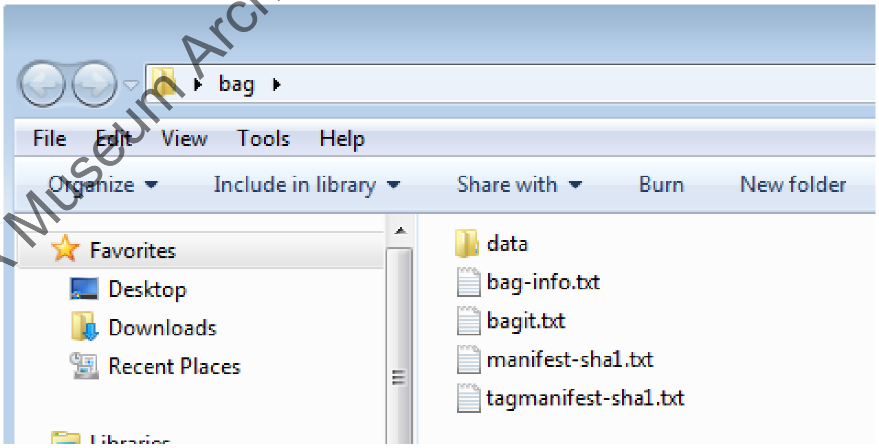
bagit.txt: Provides the version of BagIt used to create the bag.



```
BagIt-Version: 0.97
Tag-File-Character-Encoding: UTF-8
```

manifest-sha1.txt – Provides a list of the files to be transferred and their checksums, generated prior to transfer. (By default we will use sha1 but we can choose to generate checksums using md5, sha256, or sha512.) Bagger compares checksums of the transferred files against this list to determine whether any of the files were corrupted or lost during the transfer.

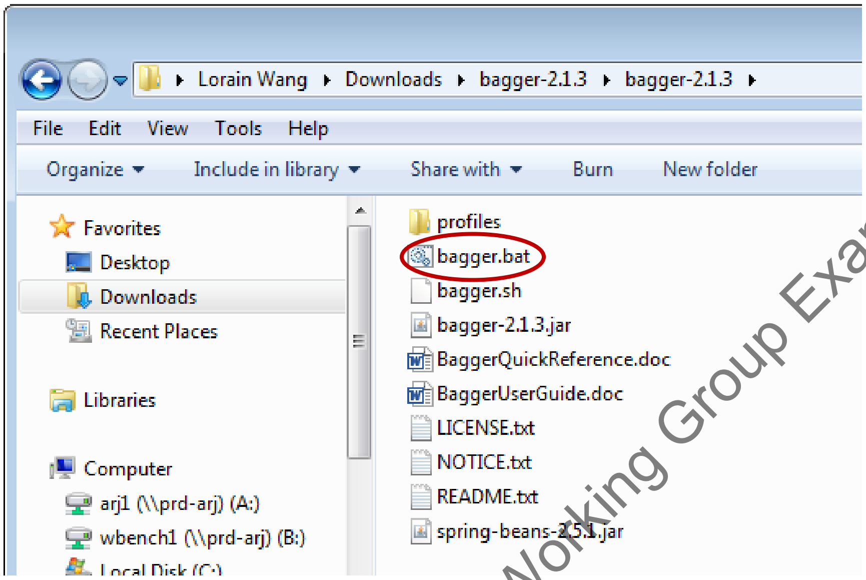
tagmanifest-sha1.txt – Provides checksums for bag-info.txt, bagit.txt, and manifest-sha1.txt.



Getting Started

1. Consult section **Java Runtime Environment configuration** to confirm Java Runtime Environment is properly configured on your computer.

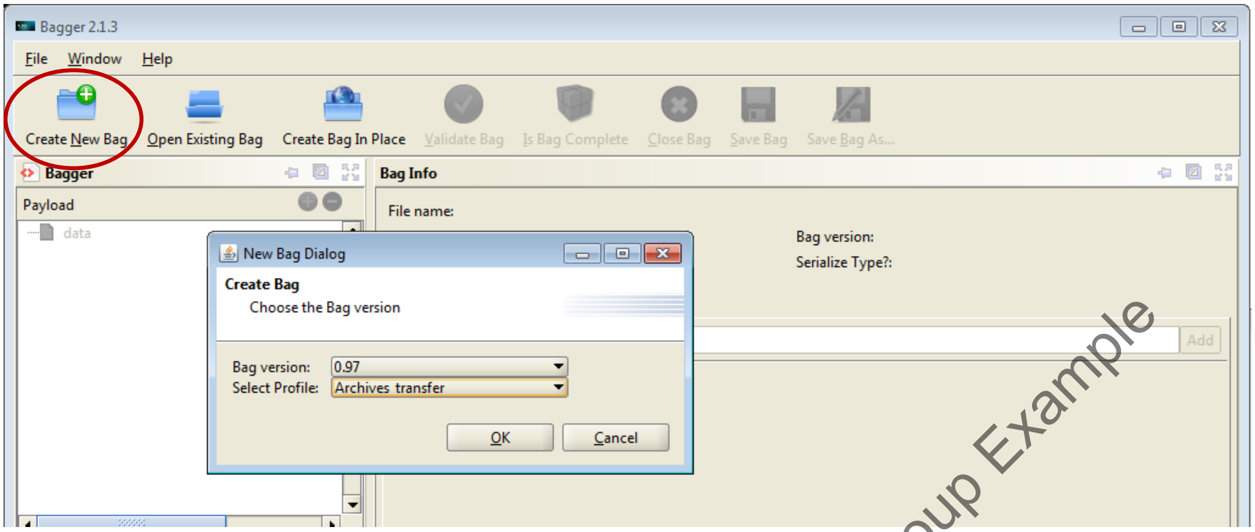
2. To launch Bagger, double-click **bagger.bat**. Depending on your version of bagger, the file may be at the top level or in the “bin” folder. An **Open File – Security Warning** dialog box may pop up. Click **Run.**



3. Bagger allows users to create custom metadata profiles-- specified sets of metadata fields used to describe administrative information about a bag and its contents. We have a custom profile that we use for all our accessioning transfers: **Archives_transfer-profile.json** (G:\Institutional Archives\ENGINEERING\ENG-120 Software_Hardware\BornDigitalToolsInstallation_files\Bagger). The first time you launch Bagger, a folder of profile templates will automatically be created at C:\Users\[your username]\bagger. Save **Archives_transfer-profile.json** in that directory.

Transfer Files (Create new bag)

1. To transfer files click **Create New Bag**.

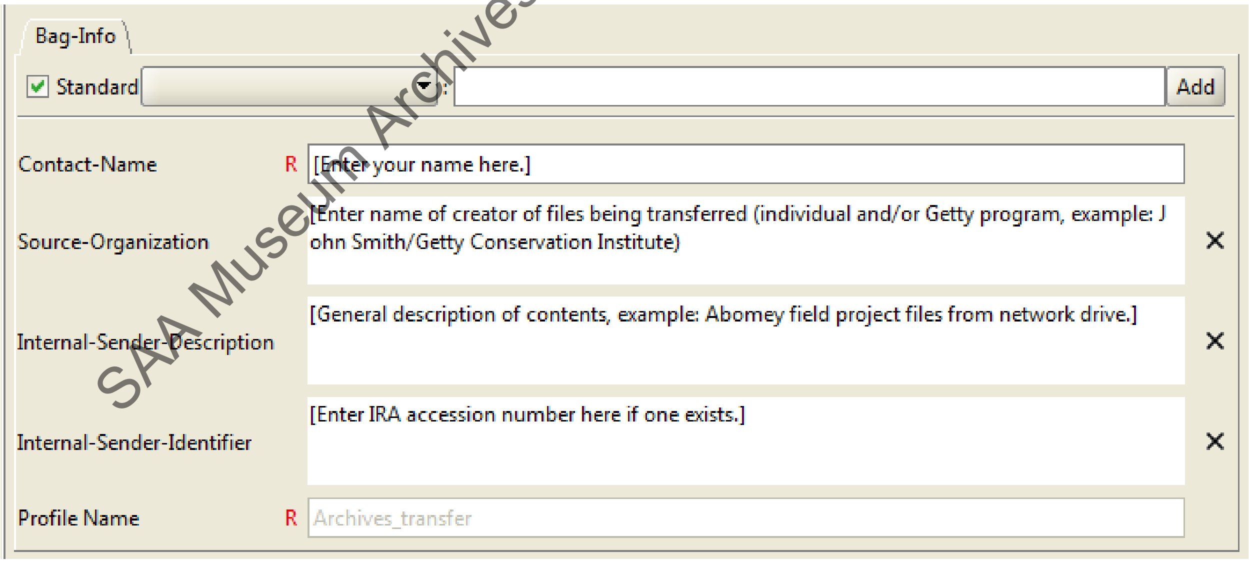


Bag version: 0.97

Select Profile: Archives transfer

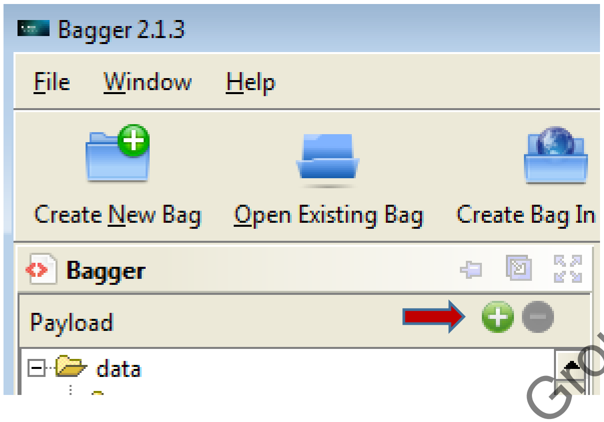
2. In the **New Bag** dialog box, select bag version **0.97** and profile **Archives_transfer** in the drop-down menus. Click **OK**.

3. Fill out the fields as specified. **Profile Name** is prepopulated with the name of the profile and cannot be edited. You may add additional metadata fields by selecting from the drop-down field next to **Standard. Bagging-Date** does not need to be added as it is automatically generated. See Metadata elements section for a complete list and description of available metadata fields.

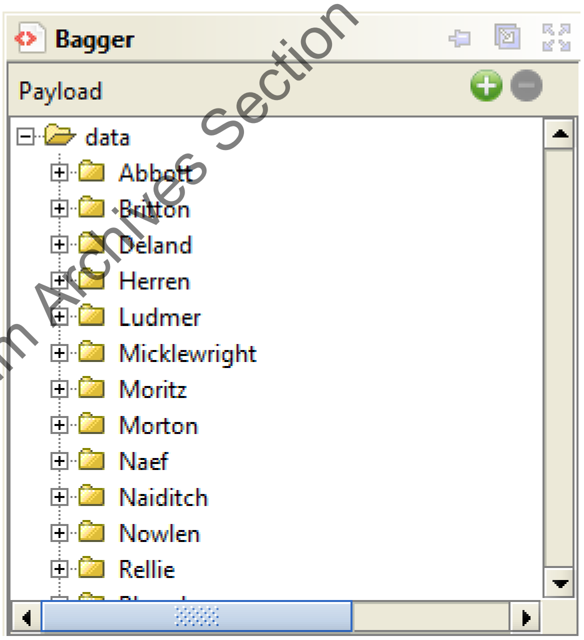


Contact-Name	R	[Enter your name here.]	
Source-Organization		[Enter name of creator of files being transferred (individual and/or Getty program, example: John Smith/Getty Conservation Institute)	×
Internal-Sender-Description		[General description of contents, example: Abomey field project files from network drive.]	×
Internal-Sender-Identifier		[Enter IRA accession number here if one exists.]	×
Profile Name	R	Archives_transfer	

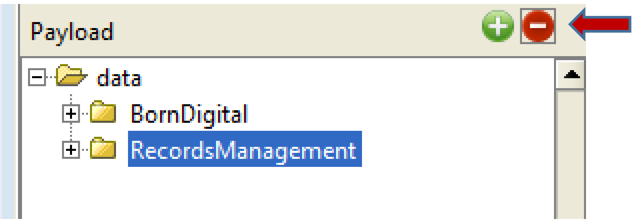
4. The set of files you will be transferring is called the “Payload.” To designate the files to be transferred click the green plus sign to the right of **Payload**. A file browser dialog box should appear.



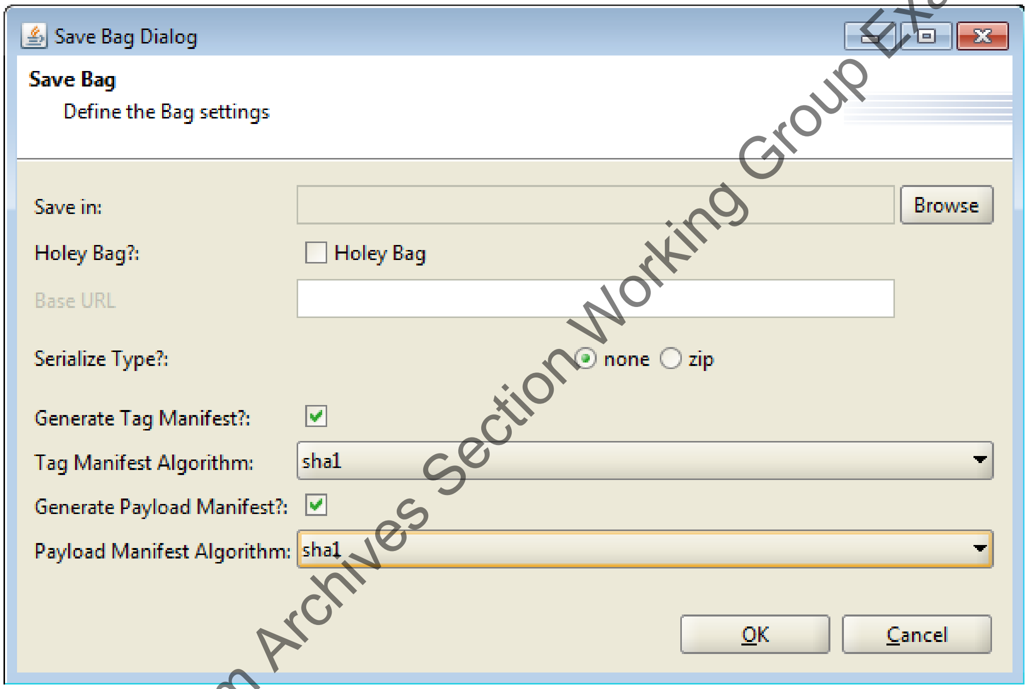
5. In the file browser dialog box navigate to and select the folder or file you wish to transfer and click **Open**. The file or folder should now appear under “data” in the **Payload** pane.



6. You may add additional files or folders by repeating the previous two steps. If you want to exclude a file or folder from your transfer, you can select it and click the red minus button to remove it.



7. After you have added all the files and folders that you will be transferring, click on **Save Bag As**. A dialog window will appear.



Save Bag

Define the Bag settings

Save in: Browse

Holey Bag?: □ Holey Bag

Base URL

Serialize Type?: ● none ○ zip

Generate Tag Manifest?: ☑

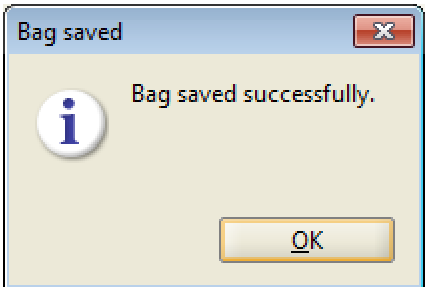
Tag Manifest Algorithm: sha1

Generate Payload Manifest?: ☑

Payload Manifest Algorithm: sha1

8. Click on **Browse** and a file browser dialog box will appear. Navigate to the location you will save the bag. The destination will normally be the "[accession#]_original" folder in a:\ira_locked. Assign a name for the new folder that will be created and click **Save**.
9. Select sha1 in the dropdown menu for both the **Tag** and **Payload Manifest Algorithm**.
10. Leave boxes checked as in the screenshot above.
11. Select **OK.** Depending on the size of the files and network speed, the bagging process can take a few seconds to several hours or even multiple days.

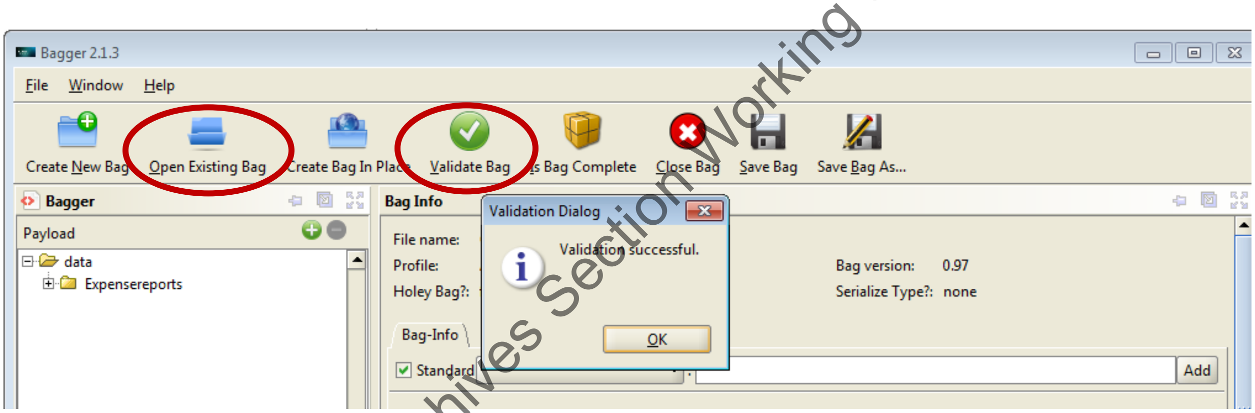
    Bagger may generate an error message if it encounters file/folder names with problematic characters or file paths that exceed character limits. Bagger also does not like certain files, such as **autorun.inf**. You will not always see an error message, but Bagger will stop running.
12. Once the bagging process has been completed, a message should appear confirming that the bag has been created in the new location.



Bag saved successfully.

If Bagger has stopped running and you do not see the above message, this means the Bagger process was interrupted due to a problem file it encountered or network connection issues. You will need to address the problem, delete the incomplete bag, and rerun Bagger.

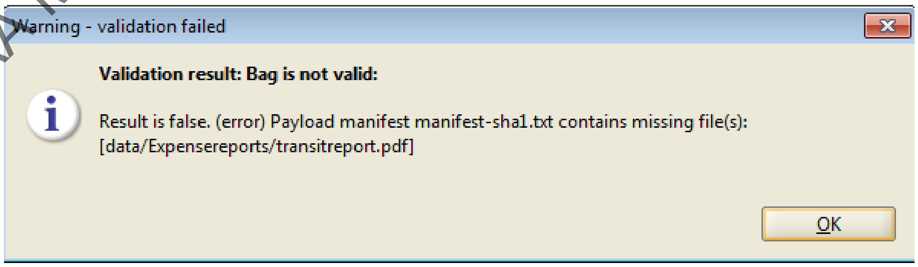
13. Once the bagging process has completed successfuly, verify that files were completely transferred without any corruptions during the transfer process. Click **Validate Bag**. (If the bag is not already loaded in Bagger, click on **Open Existing Bag**.) A message will appear if validation is successful.



Validation successful.

File name:
Profile:
Holey Bag?:
Bag version: 0.97
Serialize Type?: none

If the files were not successfully transferred or were altered after the transfer, a message will appear indicating that validation failed.



Validation result: Bag is not valid:

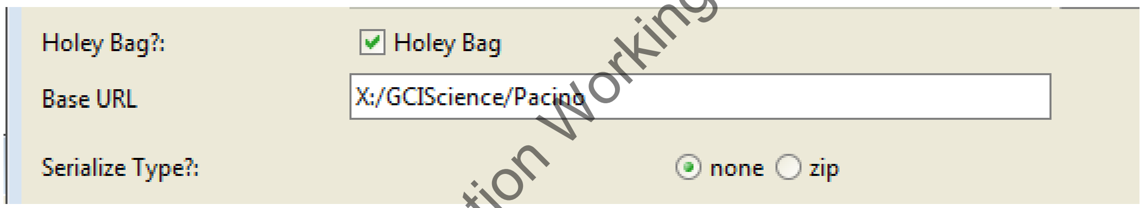
Result is false. (error) Payload manifest manifest-sha1.txt contains missing file(s): [data/Expensereports/transitreport.pdf]

Holey Bag (Create bag w/o files)

You may want to create a holey bag when dealing with large transfers. With a holey bag, Bagger generates the standard bagger tags (i.e. bag-info.txt, bagit.txt, etc.) without copying over the actual files. In this process, an extra file called “fetch.txt” is created and lists the location of the files to be “fetched.” When ready, you can manually copy (or download) the files into the holey bag. If the files are intact and match the checksums in the manifest, the bag will validate as it would with a standard bag.

1. To create a holey bag, follow the steps for creating a regular bag all the way through step 7.
2. In the Save Bag dialog window, check off the “Holey bag” box.
3. In the base url, enter the filepath of the files to be fetched. This information will be used to create fetch.txt. Select “none” for serialize type.

   Note: The information you enter for Base URL is usually not important for us as we do not use a script to automate the transfer of files, and fetch.txt will be deleted once files have been transferred. Bagger will allow you to save a holey bag as long as there is a character in the Base URL field. If you will not be transferring the files for some time, it is a good idea to document the location of the files here for later transfer.

   Holey Bag?: ☑ Holey Bag

   Base URL: X:/GCIScience/Pacino

   Serialize Type?: ● none ○ zip

   Once a holey bag has been created, you may get an error message that the “data” folder could not be created. You can ignore that message.
4. When you are ready to transfer the files, create a folder in the bag named “data.” Move the files into “data” folder.
5. Delete fetch.txt and Validate bag in Bagger.

Metadata elements

The following is a list of possible metadata elements that can be used to describe a bag’s contents or origin. Elements used appear in bag-info.txt.

Contact-Name: Name of individual creating the bag.

Contact-Phone: Not used

Contact-Email: Not used

Source-Organization: Name of creator (individual and/or program) of files to be transferred.

Organization-Address: Not used

Internal-Sender-Description: General description of contents.

Examples:

Abomey field project files stored on network drive.

Disk images of hard drives of former Getty staff.

Internal-Sender-Identifier: Accession number

Profile-Name: Name of metadata profile. This field is automatically prepopulated with the name of the profile selected.

Payload-Oxum: Auomatically generated. A byte count and file count of the files being transferred. The number following the period indicates the number of files being transferred. For example, the payload-oxum 8017330.41 indicates that there are 41 files.

Bagging-Date: Automatically generated. Date that bag was created.

Bag-Size: Automatically generated. Size of bag.

External-Identifier: A sender-supplied identifier for the bag. This field can be used if the files being transferred were assigned a unique identifier by the creator or the originating Trust program.

External-Description: An explanation of the contents of the bag. This will generally not be used.

Bag-Group-Identifier: Unique name assigned to a group of bags being transferred. This field may be used if a set of files was broken up into multiple bags to facilitate transfer.

Bag-Count: Bag's sequence in a group of associated bags. Example: 1 of 2

Java Runtime Environment configuration[1]

Before using Bagger you will need to confirm Java Runtime Environment (JRE) is installed and correctly configured on your computer.

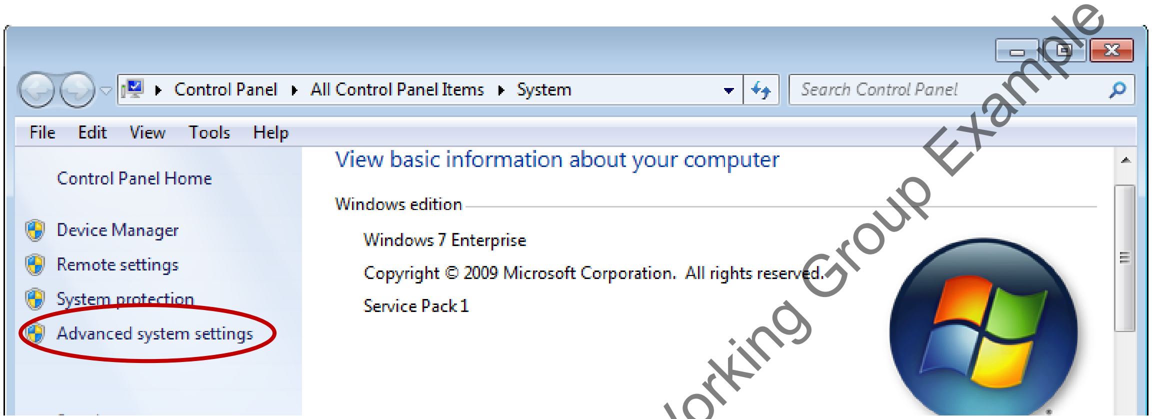
1. To determine if Java is installed on your computer, look for a "Java" folder in C:\Program Files or C:\Program Files (x86). If Java is not installed on your computer, you can download and install Java yourself or contact Getty Digital for assistance.

[1] This section is based on North Carolina Department of Cultural Resources's BagIt User Guide (ver 2.2) <http://www.ncdcr.gov/Portals/26/PDF/guidelines/Using_BagIt.pdf>.

2. Next you will need to configure the JRE environment variable.

   a. Right-click the My Computer icon on your desktop and select the **Properties** option.

   b. Select **Advanced System Settings** on the left-hand panel. Select yes in the dialog box that pops up.



View basic information about your computer

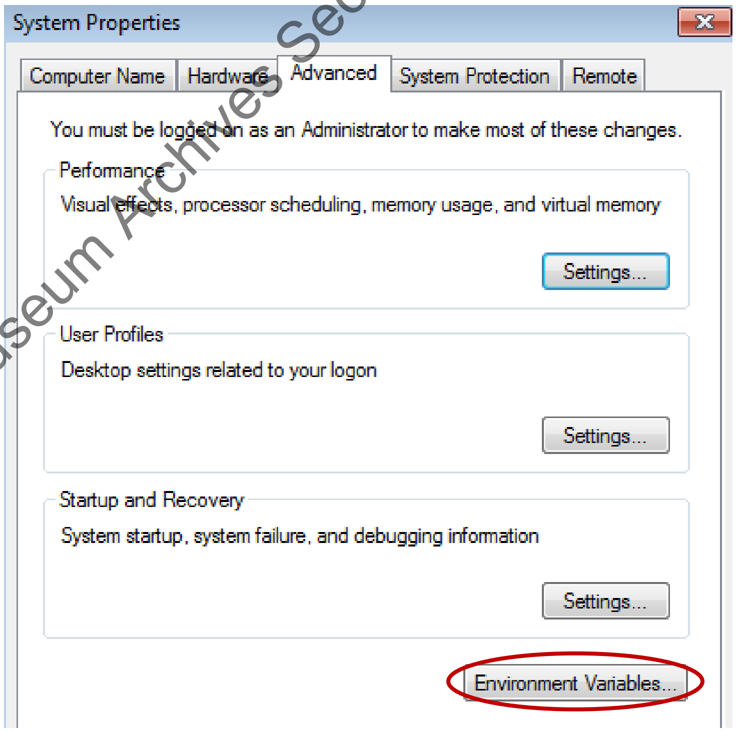
Windows edition

Windows 7 Enterprise

Copyright © 2009 Microsoft Corporation. All rights reserved.

Service Pack 1

   c. Select the **Environment Variables** button near the bottom of the dialog box.



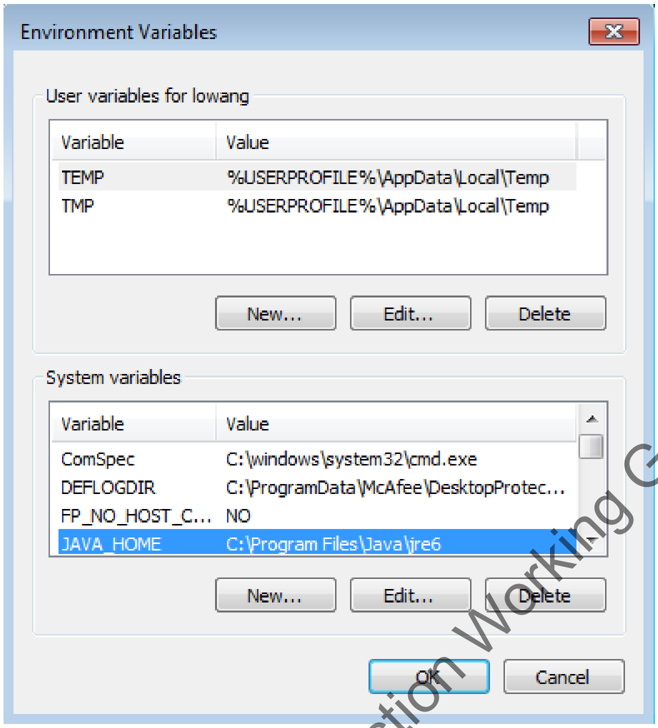
You must be logged on as an Administrator to make most of these changes.

Visual effects, processor scheduling, memory usage, and virtual memory

Desktop settings related to your logon

System startup, system failure, and debugging information

d. In the **Environment Variables** window that appears, verify whether or not the JAVA_HOME environment variable is defined.



User variables for lowang

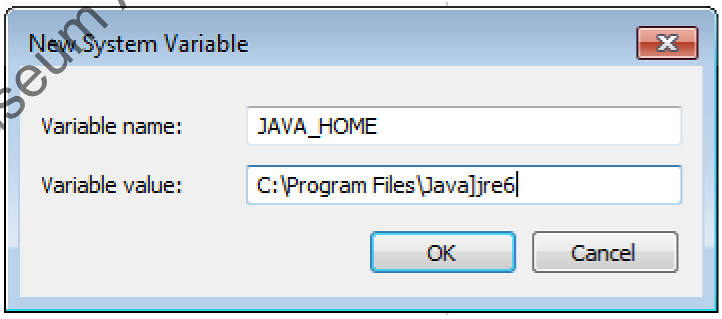
Variable	Value
TEMP	%USERPROFILE%\AppData\Local\Temp
TMP	%USERPROFILE%\AppData\Local\Temp

System variables

Variable	Value
ComSpec	C:\windows\system32\cmd.exe
DEFLOGDIR	C:\ProgramData\McAfee\DesktopProtec…
FP_NO_HOST_C…	NO
JAVA_HOME	C:\Program Files\Java\jre6

If JAVA_HOME is not listed, you will need to create a new Environmental variable by selecting the **New** button in the lower half of the window.

e. A **New System Variable** window will appear.

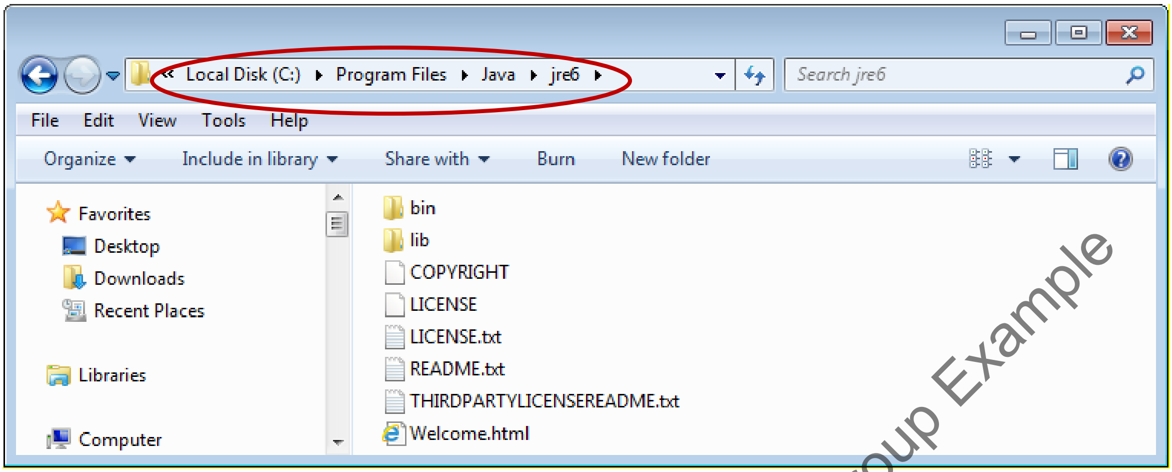


Variable name: JAVA_HOME

Variable value: C:\Program Files\Java]jre6

In the ***Variable name*** field, type JAVA_HOME

In the ***Variable value*** field, type the complete path to the folder that contains the "bin" folder.


« Local Disk (C:) ▸ Program Files ▸ Java ▸ jre6 ▸
Search jre6
File Edit View Tools Help
Organize ▾ Include in library ▾ Share with ▾ Burn New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Computer

bin
lib
COPYRIGHT
LICENSE
LICENSE.txt
README.txt
THIRDPARTYLICENSEREADME.txt
Welcome.html

Click OK to close the **New System Variable** window.

f. Review the list of system variables to confirm JAVA_HOME was added and properly assigned.

C. BeyondCompare

License is required.
https://www.scootersoftware.com/

Overview

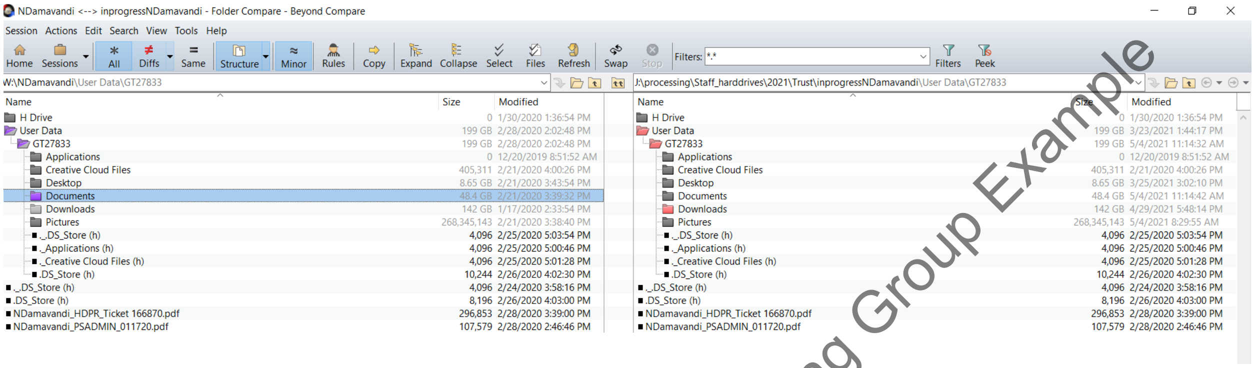
BeyondCompare is a file and folder comparison tool. It can be used to compare folder structures, images, and the content of text documents and spreadsheets. There are other features of the software, such as merge and folder sync, but they will not be covered in this guide. A license is required.

Folder Compare

Select the two folders that you want to compare in the left and right-hand panes. Larger folders will take longer to load as BeyondCompare calculates file and folder sizes. By default comparisons are based on folder/file names, file size, and modified dates, but binary comparisons can be enabled (covered at the end of this section).

Navigate to **Session** in the menu bar (above the **Home** button) and click on **Session Settings.** Under the **Specs** tab, check off **Disable editing** for both folders and click **OK.**

Folders/files are color coded to indicated matches and mismatches. Black indicates that files match, purple indicates that a file is present that is not present in the other folder, red indicates a file is newer or different, and light gray indicates a file is older or unknown. Color coding of folders reflect the contents of the folders and is similar to that of files except that dark gray, and not black, indicates that folder contents match. A folder may also display more than one color if it contains more than one type of mismatch.



NDamavandi <--> inprogressNDamavandi - Folder Compare - Beyond Compare

Filters: *.*

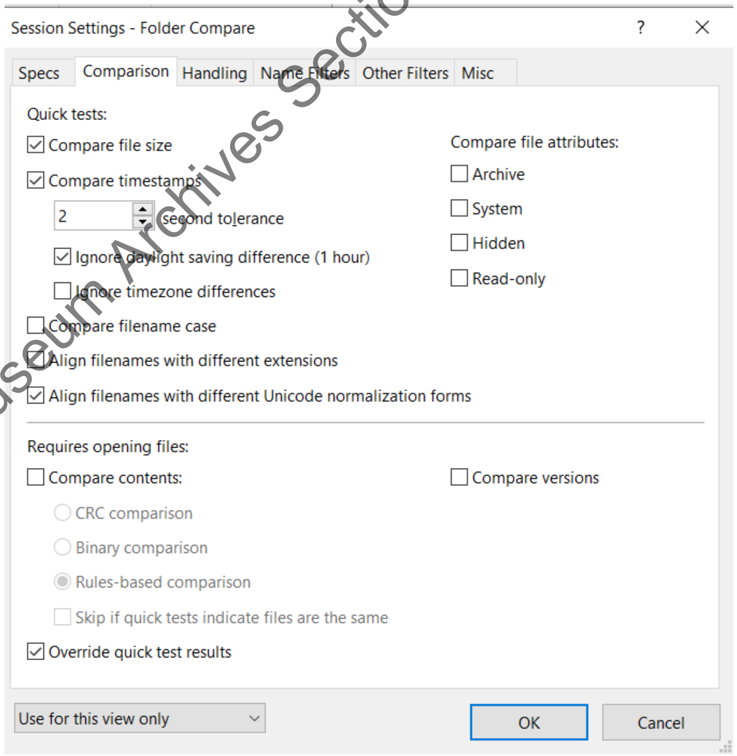
W:\NDamavandi\User Data\GT27833

Name	Size	Modified
H Drive	0	1/30/2020 1:36:54 PM
User Data	199 GB	2/28/2020 2:02:48 PM
GT27833	199 GB	2/28/2020 2:02:48 PM
Applications	0	12/20/2019 8:51:52 AM
Creative Cloud Files	405,311	2/21/2020 4:00:26 PM
Desktop	8.65 GB	2/21/2020 3:43:54 PM
Documents	48.4 GB	2/21/2020 3:39:32 PM
Downloads	142 GB	1/17/2020 2:33:54 PM
Pictures	268,345,143	2/21/2020 3:38:40 PM
._.DS_Store (h)	4,096	2/25/2020 5:03:54 PM
._Applications (h)	4,096	2/25/2020 5:00:46 PM
._Creative Cloud Files (h)	4,096	2/25/2020 5:01:28 PM
.DS_Store (h)	10,244	2/26/2020 4:02:30 PM
._.DS_Store (h)	4,096	2/24/2020 3:58:16 PM
.DS_Store (h)	8,196	2/26/2020 4:03:00 PM
NDamavandi_HDPR_Ticket 166870.pdf	296,853	2/28/2020 3:39:00 PM
NDamavandi_PSADMIN_011720.pdf	107,579	2/28/2020 2:46:46 PM

J:\processing\Staff_harddrives\2021\Trust\inprogressNDamavandi\User Data\GT27833

Name	Size	Modified
H Drive	0	1/30/2020 1:36:54 PM
User Data	199 GB	3/23/2021 1:44:17 PM
GT27833	199 GB	5/4/2021 11:14:32 AM
Applications	0	12/20/2019 8:51:52 AM
Creative Cloud Files	405,311	2/21/2020 4:00:26 PM
Desktop	8.65 GB	3/25/2021 3:02:10 PM
Documents	48.4 GB	5/4/2021 11:14:42 AM
Downloads	142 GB	4/29/2021 5:48:14 PM
Pictures	268,345,143	5/4/2021 8:29:55 AM
._.DS_Store (h)	4,096	2/25/2020 5:03:54 PM
._Applications (h)	4,096	2/25/2020 5:00:46 PM
._Creative Cloud Files (h)	4,096	2/25/2020 5:01:28 PM
.DS_Store (h)	10,244	2/26/2020 4:02:30 PM
._.DS_Store (h)	4,096	2/24/2020 3:58:16 PM
.DS_Store (h)	8,196	2/26/2020 4:03:00 PM
NDamavandi_HDPR_Ticket 166870.pdf	296,853	2/28/2020 3:39:00 PM
NDamavandi_PSADMIN_011720.pdf	107,579	2/28/2020 2:46:46 PM

If all files do not match due to timestamps of files differing by exactly an hour, navigate to **Session** in the menu bar (above the **Home** button) and click on **Session Settings**. Click on the **Comparison** tab and check off the box next to **Ignore Daylight Saving difference** and click **OK**.



Session Settings - Folder Compare

Quick tests:

☑ Compare file size

☑ Compare timestamps

2 second tolerance

☑ Ignore daylight saving difference (1 hour)

☐ Ignore timezone differences

☐ Compare filename case

☐ Align filenames with different extensions

☑ Align filenames with different Unicode normalization forms

Compare file attributes:

☐ Archive

☐ System

☐ Hidden

☐ Read-only

Requires opening files:

☐ Compare contents:

○ CRC comparison

○ Binary comparison

● Rules-based comparison

☐ Skip if quick tests indicate files are the same

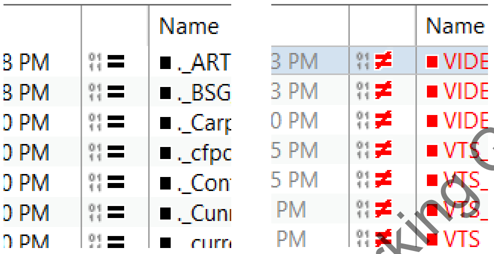
☑ Override quick test results

☐ Compare versions

Use for this view only

Note that comparisons based on file names, size, and date will not always catch corrupt files. While BeyondCompare doesn't offer checksum comparisons, it does do CRC and binary comparisons. For verifying acquisition transfers, we preference using checksum comparisons. If, for some reason, checksum comparisons are not possible, you may use BeyondCompare's binary comparison, which is faster than the CRC comparison, as long as you document the verification method and results in the **Digital File Mgmt Notes** field in ASpace.

To enable the binary comparison, in the **Comparison** tab under **Session Settings**, check off **Compare contents** and check **Binary comparison** and click **OK**. BeyondCompare should automatically begin the binary comparison for each file. An hour glass indicates that the binary comparison is in process. You should see an equal sign in the center column if files match. Mismatches are indicated by a red slashed equal sign.



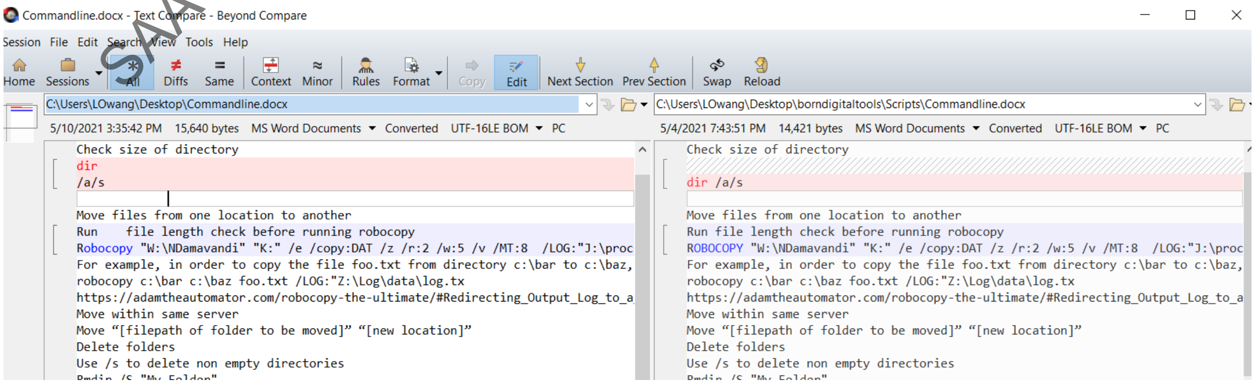
Text Compare

Use Text Compare to compare the contents of two text documents. This includes *doc, *.docx, *.pdf, and *.txt files. Note that BeyondCompare does not recognize review comments in PDF and Word documents.

Select the two files that you want to compare in the left and right-hand panes. BeyondCompare will automatically run a binary comparison on the two files and will indicate at the bottom of the window if the binary is the same.

To prevent accidental edits, navigate to **Session** in the menu bar (above the **Home** button) and click on **Session Settings**. Under the **Specs** tab, check off **Disable editing** for both folders and click **OK.**

Red highlights indicate important differences. Blue indicates minor differences, such as an extra space or differences in capitalization of a word.



C:\Users\LOwang\Desktop\Commandline.docx

5/10/2021 3:35:42 PM 15,640 bytes MS Word Documents Converted UTF-16LE BOM PC

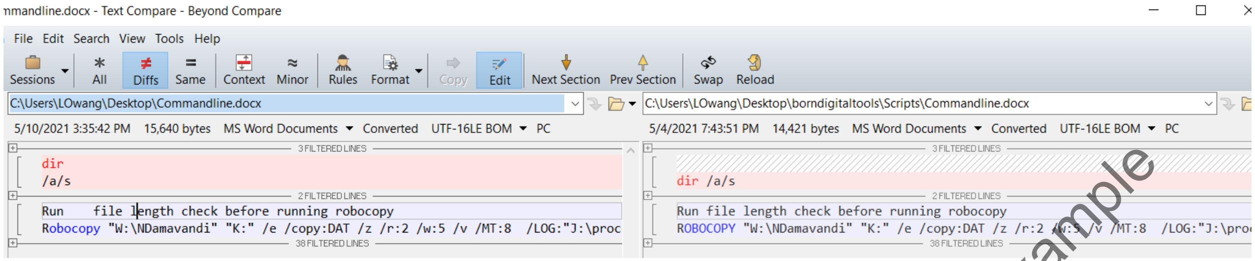
```
Check size of directory
dir
/a/s

Move files from one location to another
Run    file length check before running robocopy
Robocopy "W:\NDamavandi" "K:" /e /copy:DAT /z /r:2 /w:5 /v /MT:8  /LOG:"J:\proc
For example, in order to copy the file foo.txt from directory c:\bar to c:\baz,
robocopy c:\bar c:\baz foo.txt /LOG:"Z:\Log\data\log.tx
https://adamtheautomator.com/robocopy-the-ultimate/#Redirecting_Output_Log_to_a
Move within same server
Move "[filepath of folder to be moved]" "[new location]"
Delete folders
Use /s to delete non empty directories
Rmdir /S "My Folder"
```

C:\Users\LOwang\Desktop\borndigitaltools\Scripts\Commandline.docx

5/4/2021 7:43:51 PM 14,421 bytes MS Word Documents Converted UTF-16LE BOM PC

```
Check size of directory

dir /a/s

Move files from one location to another
Run file length check before running robocopy
ROBOCOPY "W:\NDamavandi" "K:" /e /copy:DAT /z /r:2 /w:5 /v /MT:8  /LOG:"J:\proc
For example, in order to copy the file foo.txt from directory c:\bar to c:\baz,
robocopy c:\bar c:\baz foo.txt /LOG:"Z:\Log\data\log.tx
https://adamtheautomator.com/robocopy-the-ultimate/#Redirecting_Output_Log_to_a
Move within same server
Move "[filepath of folder to be moved]" "[new location]"
Delete folders
Use /s to delete non empty directories
Rmdir /S "My Folder"
```

At the top you can choose to display only the differences by clicking the **Diffs** button or display only matching lines by clicking **Same**. Click or unclick **Minor** if you do or do not want minor differences to be displayed with differences or matching rows. Clicking **All** will display the entire document.



C:\Users\LOwang\Desktop\Commandline.docx

5/10/2021 3:35:42 PM 15,640 bytes MS Word Documents Converted UTF-16LE BOM PC

```
dir
/a/s
Run     file length check before running robocopy
Robocopy "W:\NDamavandi" "K:" /e /copy:DAT /z /r:2 /w:5 /v /MT:8  /LOG:"J:\proc
```

C:\Users\LOwang\Desktop\borndigitaltools\Scripts\Commandline.docx

5/4/2021 7:43:51 PM 14,421 bytes MS Word Documents Converted UTF-16LE BOM PC

```
dir /a/s
Run file length check before running robocopy
ROBOCOPY "W:\NDamavandi" "K:" /e /copy:DAT /z /r:2 /w:5 /v /MT:8  /LOG:"J:\proc
```

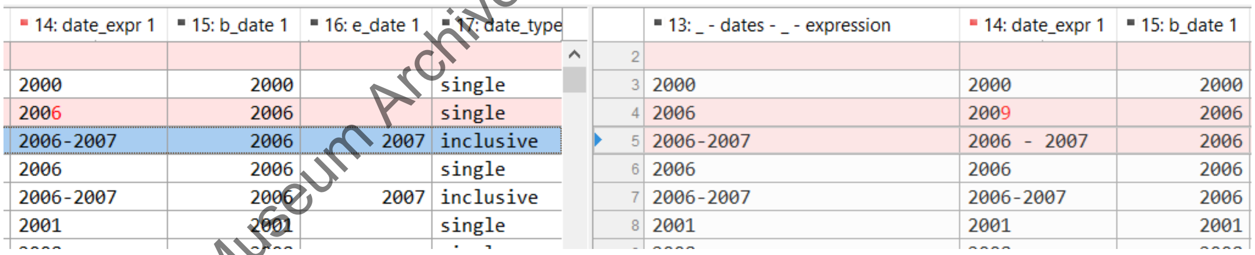
Table Compare

Use Table Compare to compare spreadsheets.

Select the two files that you want to compare in the left and right-hand panes. BeyondCompare will automatically run a binary comparison on the two files and will indicate at the bottom of the window if the binary is the same.

To prevent accidental edits, navigate to **Session** in the menu bar (above the **Home** button) and click on **Session Settings**. Under the **Specs** tab, check off **Disable editing** for both folders and click **OK.**

A red background indicates a major difference in the row, while blue indicates a minor difference. To find the cell(s) that contains the difference, look for the red dot in the column header. The different text is in red while there is no color coding for space differences.



■ 14: date_expr 1	■ 15: b_date 1	■ 16: e_date 1	■ 17: date_type
2000	2000		single
2006	2006		single
2006-2007	2006	2007	inclusive
2006	2006		single
2006-2007	2006	2007	inclusive
2001	2001		single

	■ 13: _ - dates - _ - expression	■ 14: date_expr 1	■ 15: b_date 1
2			
3	2000	2000	2000
4	2006	2009	2006
5	2006-2007	2006 - 2007	2006
6	2006	2006	2006
7	2006-2007	2006-2007	2006
8	2001	2001	2001

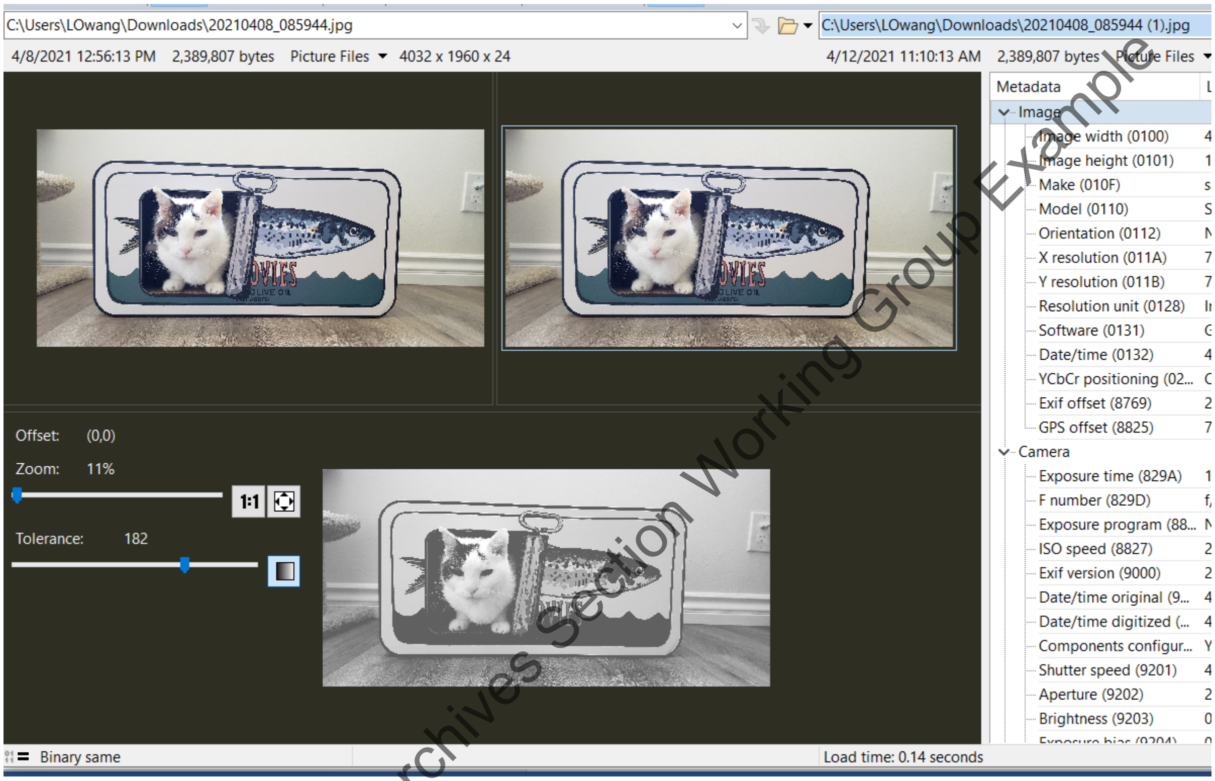
You can customize which columns are compared by clicking the **Columns** tab in **Session Settings**. Click the cell for the left or right file and click the up and down arrow to move it next to the column that you want it to be compared to. Clicking a cell in the first column and clicking the up and down arrow will rearrange the display order of the column, while clicking the minus button will remove the column for comparison. These customizations will not edit the actual spreadsheets.

At the top you can choose to display only the differences by clicking the **Diffs** button or display only matching lines by clicking **Same**. Click or unclick **Minor** if you do or do not want minor differences to be displayed with differences or matching rows. Clicking **All** will display the entire document.

Picture Compare

Use Picture Compare to compare two images and their metadata.

Select the two images that you want to compare in the left and right-hand panes. BeyondCompare will automatically run a binary comparison on the two pictures and will indicate at the bottom of the window if the binary is the same.



C:\Users\LOwang\Downloads\20210408_085944.jpg

C:\Users\LOwang\Downloads\20210408_085944 (1).jpg

4/8/2021 12:56:13 PM 2,389,807 bytes Picture Files 4032 x 1960 x 24

4/12/2021 11:10:13 AM 2,389,807 bytes Picture Files

Metadata	L
Image	
Image width (0100)	4
Image height (0101)	1
Make (010F)	s
Model (0110)	S
Orientation (0112)	N
X resolution (011A)	7
Y resolution (011B)	7
Resolution unit (0128)	I
Software (0131)	G
Date/time (0132)	4
YCbCr positioning (02...	C
Exif offset (8769)	2
GPS offset (8825)	7
Camera	
Exposure time (829A)	1
F number (829D)	f,
Exposure program (88...	N
ISO speed (8827)	2
Exif version (9000)	2
Date/time original (9...	4
Date/time digitized (...	4
Components configur...	Y
Shutter speed (9201)	4
Aperture (9202)	2
Brightness (9203)	0
Exposure bias (9204)	0

Offset: (0,0)

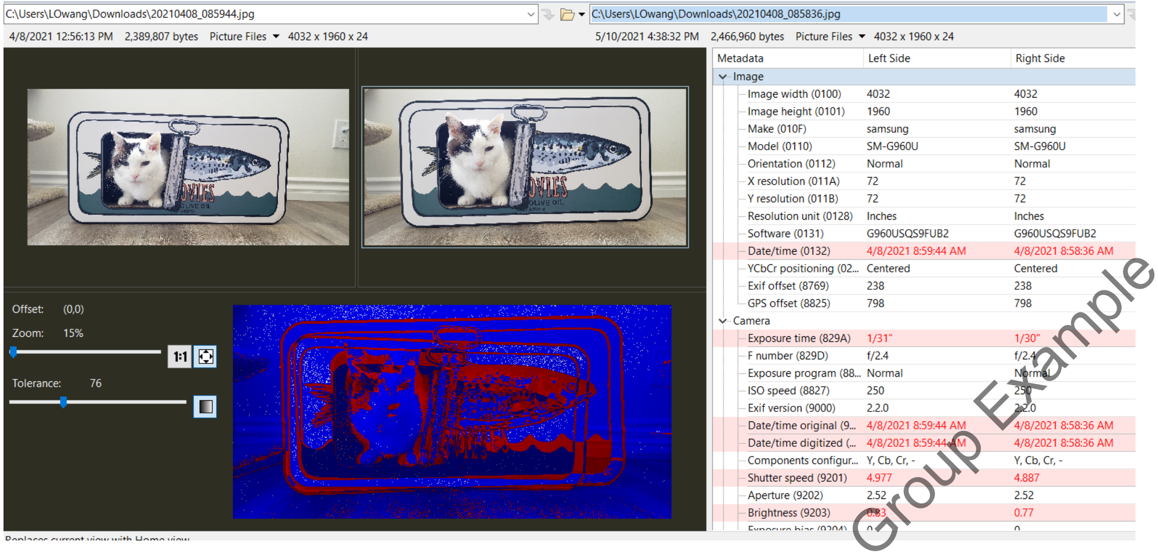
Zoom: 11%

Tolerance: 182

Binary same

Load time: 0.14 seconds

If the binary is not the same, click on the **Tol** button at the top of the window. The image on the bottom is a comparison of the two pictures. Shades of gray represent matches, shades of blue represent unimportant differences, and shades of red represent important differences. Differences in metadata are highlighted in red. Adjusting the degree of tolerance will turn unimportant differences into



C:\Users\LOwang\Downloads\20210408_085944.jpg

4/8/2021 12:56:13 PM 2,389,807 bytes Picture Files ▾ 4032 x 1960 x 24

C:\Users\LOwang\Downloads\20210408_085836.jpg

5/10/2021 4:38:32 PM 2,466,960 bytes Picture Files ▾ 4032 x 1960 x 24

Offset: (0,0)

Zoom: 15%

Tolerance: 76

Metadata	Left Side	Right Side
Image		
Image width (0100)	4032	4032
Image height (0101)	1960	1960
Make (010F)	samsung	samsung
Model (0110)	SM-G960U	SM-G960U
Orientation (0112)	Normal	Normal
X resolution (011A)	72	72
Y resolution (011B)	72	72
Resolution unit (0128)	Inches	Inches
Software (0131)	G960USQS9FUB2	G960USQS9FUB2
Date/time (0132)	4/8/2021 8:59:44 AM	4/8/2021 8:58:36 AM
YCbCr positioning (02...	Centered	Centered
Exif offset (8769)	238	238
GPS offset (8825)	798	798
Camera		
Exposure time (829A)	1/31"	1/30"
F number (829D)	f/2.4	f/2.4
Exposure program (88...	Normal	Normal
ISO speed (8827)	250	250
Exif version (9000)	2.2.0	2.2.0
Date/time original (9...	4/8/2021 8:59:44 AM	4/8/2021 8:58:36 AM
Date/time digitized (...	4/8/2021 8:59:44 AM	4/8/2021 8:58:36 AM
Components configur...	Y, Cb, Cr, -	Y, Cb, Cr, -
Shutter speed (9201)	4.977	4.887
Aperture (9202)	2.52	2.52
Brightness (9203)	0.83	0.77
Exposure bias (9204)	0	0

Replaces current view with Home view

If you have two similar images that are cropped differently, you can adjust the image overlay by clicking on the **Range** button and clicking and dragging the bottom image.

D. CDCheck

Install file: G:\Institutional Archives\ENGINEERING\ENG-120 Software_Hardware\ BornDigitalToolsInstallation_files

License: G:\Institutional Archives\ENGINEERING\ENG-120 Software_Hardware\software_licenses

Note that you will need to copy the file to your local computer to install.

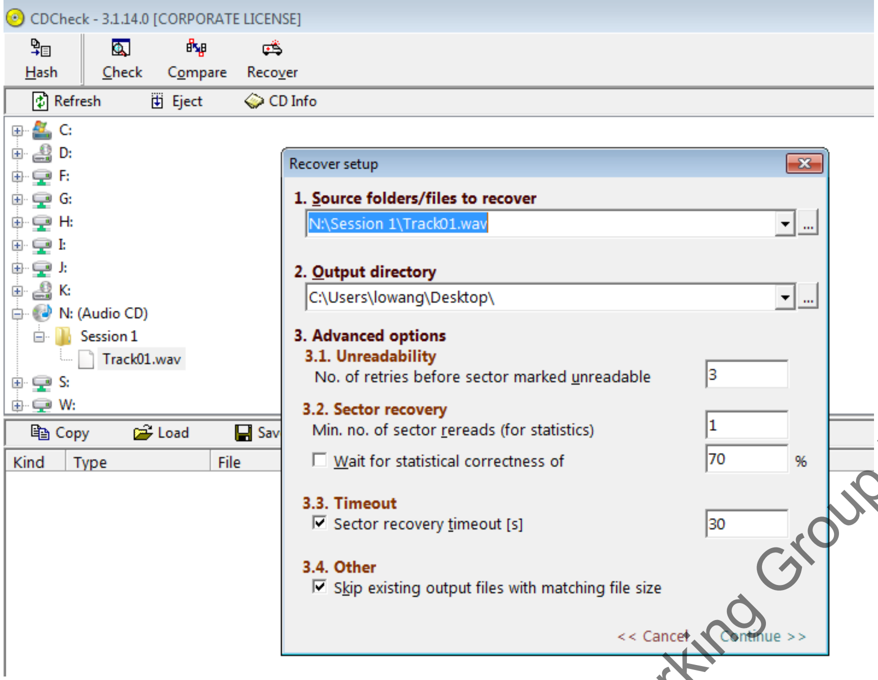
Overview

CDCheck is a tool that we primarily use to extract damaged files from optical discs. It also does binary comparisons and generates checksums, but you may want to use BeyondCompare and QuickHash instead for larger and more complex folders. While the tool was designed specifically for CDs, it can also be used with any folders visible in file explorer.

Extracting files

1. In the directory tree pane select the folder or files to extract.

2. Click Recover. In the Recover Setup window select the file or folder to export and select the save location in the Output directory field. Click Continue.
   Note: You can only recover an entire folder or a single file.



1. Source folders/files to recover: N:\Session 1\Track01.wav

2. Output directory: C:\Users\lowang\Desktop\

3. Advanced options

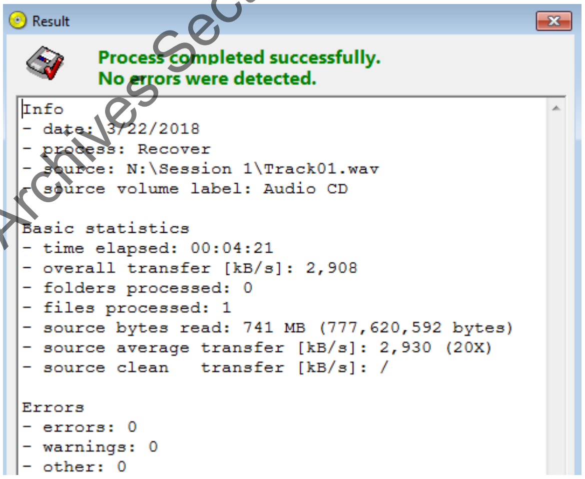
3.1. Unreadability
No. of retries before sector marked unreadable: 3

3.2. Sector recovery
Min. no. of sector rereads (for statistics): 1
☐ Wait for statistical correctness of: 70 %

3.3. Timeout
☑ Sector recovery timeout [s]: 30

3.4. Other
☑ Skip existing output files with matching file size

3. Once the transfer process has completed, a box will appear indicating whether or not there were errors. If there are errors, you may want to try recovering the files again with CDCheck, use a different software, or image the disc.



Process completed successfully.
No errors were detected.

```
Info
- date: 3/22/2018
- process: Recover
- source: N:\Session 1\Track01.wav
- source volume label: Audio CD

Basic statistics
- time elapsed: 00:04:21
- overall transfer [kB/s]: 2,908
- folders processed: 0
- files processed: 1
- source bytes read: 741 MB (777,620,592 bytes)
- source average transfer [kB/s]: 2,930 (20X)
- source clean   transfer [kB/s]: /

Errors
- errors: 0
- warnings: 0
- other: 0
```

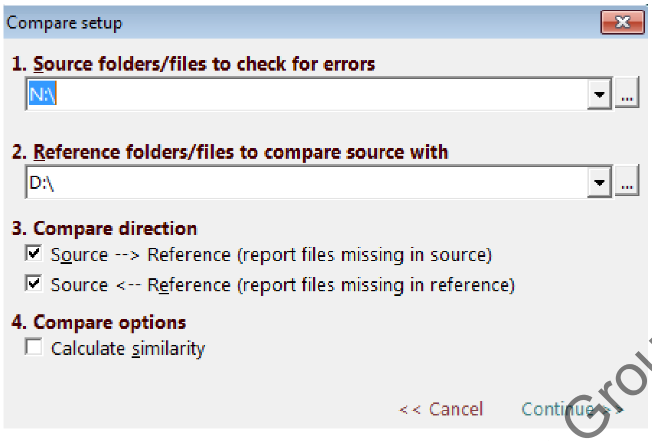
4. Run a comparison to verify files were properly transferred.

Verifying files

CDCheck compares files by doing binary (bit by bit) comparisons.

1. Click Compare.

2. Select the disc drive/folder to compare. The source is the original set while reference is the copied set. Check the box for "report files missing in reference." If it is appropriate for your needs you can also check the box for "report files missing in source." Click Continue.



Compare setup

1. Source folders/files to check for errors

N:\

2. Reference folders/files to compare source with

D:\

3. Compare direction

☑ Source --> Reference (report files missing in source)

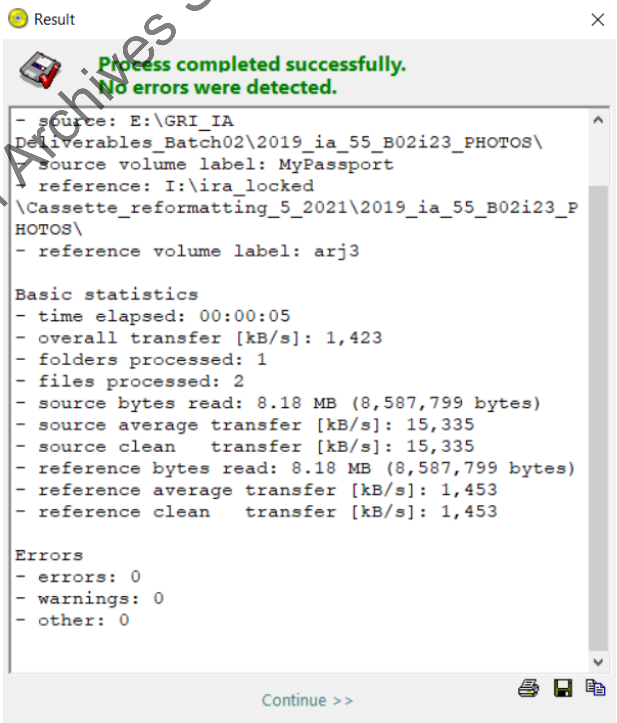
☑ Source <-- Reference (report files missing in reference)

4. Compare options

□ Calculate similarity

3. Once the comparison has completed, you will see a message that errors were or were not detected.

If you are verifying files as part of your accessioning process and no errors were detected, click on the save button at the bottom of the window and save the file in "accession #]_documentation" folder on ira_locked. Name the file "[accession #]_binarycomparison.txt"

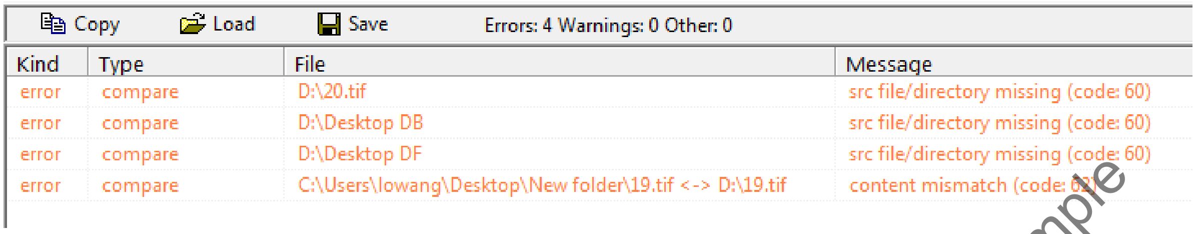


Result

Process completed successfully.
No errors were detected.

```
- source: E:\GRI_IA
Deliverables_Batch02\2019_ia_55_B02i23_PHOTOS\
- source volume label: MyPassport
- reference: I:\ira_locked
\Cassette_reformatting_5_2021\2019_ia_55_B02i23_P
HOTOS\
- reference volume label: arj3

Basic statistics
- time elapsed: 00:00:05
- overall transfer [kB/s]: 1,423
- folders processed: 1
- files processed: 2
- source bytes read: 8.18 MB (8,587,799 bytes)
- source average transfer [kB/s]: 15,335
- source clean   transfer [kB/s]: 15,335
- reference bytes read: 8.18 MB (8,587,799 bytes)
- reference average transfer [kB/s]: 1,453
- reference clean   transfer [kB/s]: 1,453

Errors
- errors: 0
- warnings: 0
- other: 0
```

If errors were detected, the list of errors will appear on the bottom panel of the main window. If you are working with an optical disc, note that there may be false errors due to problems with the disc.



Errors: 4 Warnings: 0 Other: 0

Kind	Type	File	Message
error	compare	D:\20.tif	src file/directory missing (code: 60)
error	compare	D:\Desktop DB	src file/directory missing (code: 60)
error	compare	D:\Desktop DF	src file/directory missing (code: 60)
error	compare	C:\Users\lowang\Desktop\New folder\19.tif <-> D:\19.tif	content mismatch (code: 62)

E. Forensic Toolkit

License is required. We have two licenses (on dongles).

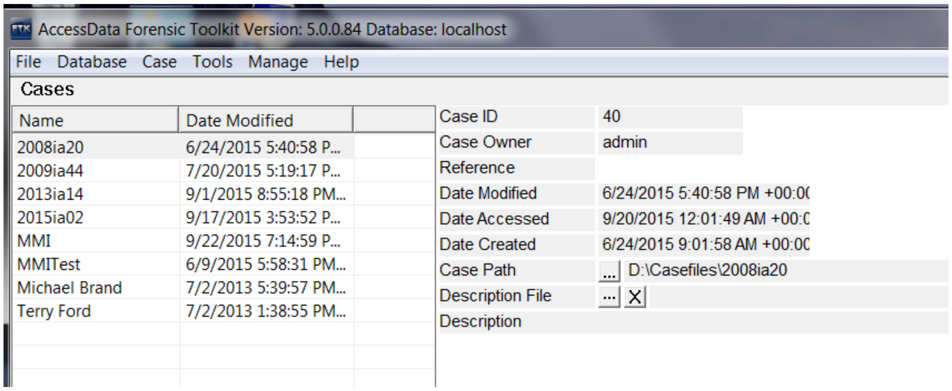
Overview

Forensic Toolkit is installed on Fluffy and FRED. To use Forensic Toolkit, make sure the USB dongle with the Forensic Toolkit license is connected to your computer.

Use Forensic Toolkit to examine the content of disk images and to export files from disk images. While you can also use FTK Imager to export files from images, it is much more limited in terms of being able to preview the content of files. Forensic Toolkit is thus recommended when more thorough appraisal work is required. Since E01 images of hard drives contains files that we do not need to preserve (for example, system files and deleted files), do not export files from these images until they have been appraised and non-archival files have been identified in Forensic Toolkit. (See “IA Electronic record accessioning.pdf” at G:\Institutional Archives\ADMINISTRATION\ADM-135 Policies Procedures Adm\Archives_Policies_procedures_manuals\Manuals_Current\BornDigital for more thorough guidance on using Forensic Toolkit’s appraisal features.)

Loading and viewing image

1. Connect USB dongle with the Forensic Toolkit license to your computer and open program.
2. Go to toolbar and click on Case.



AccessData Forensic Toolkit Version: 5.0.0.84 Database: localhost
File Database Case Tools Manage Help
Cases

Name	Date Modified
2008ia20	6/24/2015 5:40:58 P...
2009ia44	7/20/2015 5:19:17 P...
2013ia14	9/1/2015 8:55:18 PM...
2015ia02	9/17/2015 3:53:52 P...
MMI	9/22/2015 7:14:59 P...
MMITest	6/9/2015 5:58:31 PM...
Michael Brand	7/2/2013 5:39:57 PM...
Terry Ford	7/2/2013 1:38:55 PM...

Case ID	40
Case Owner	admin
Reference	
Date Modified	6/24/2015 5:40:58 PM +00:0(
Date Accessed	9/20/2015 12:01:49 AM +00:(
Date Created	6/24/2015 9:01:58 AM +00:0(
Case Path	... D:\Casefiles\2008ia20
Description File	... X
Description	

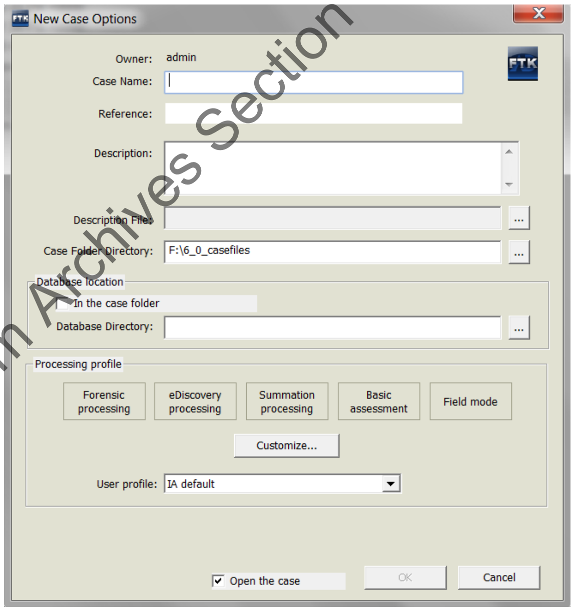
3. Select **New** and the New Case Options window will appear.

   Fill the following fields:

   Case Name: Accession number

   Processing Profile: IA default

   Click **OK**.



Owner: admin

Case Name:

Reference:

Description:

Description File:

Case Folder Directory: F:\6_0_casefiles

Database location

□ In the case folder

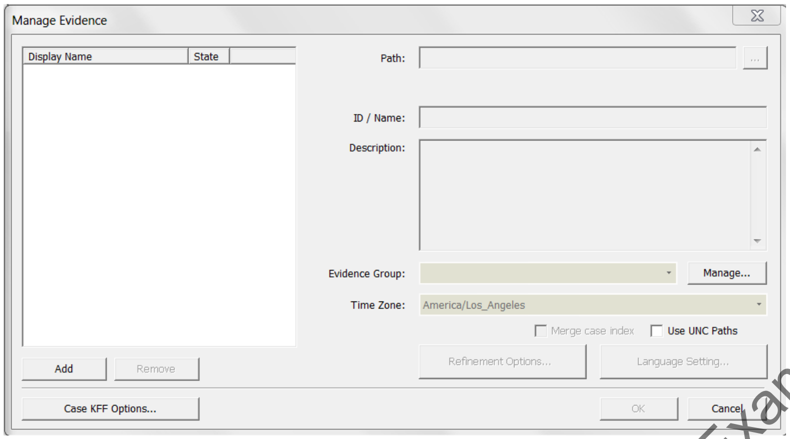
Database Directory:

Processing profile

User profile: IA default

☑ Open the case

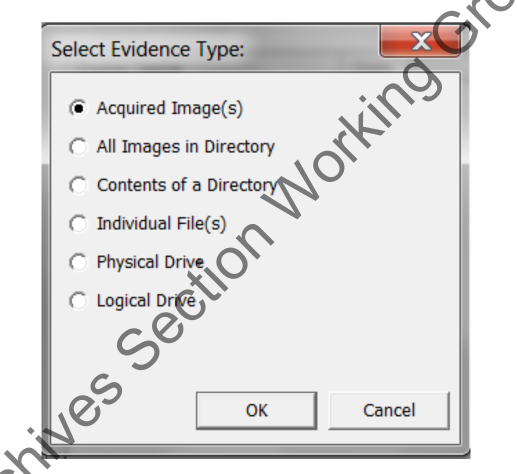
4. In the Manage Evidence window, click **Add**.



Time Zone: America/Los_Angeles

□ Merge case index □ Use UNC Paths

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



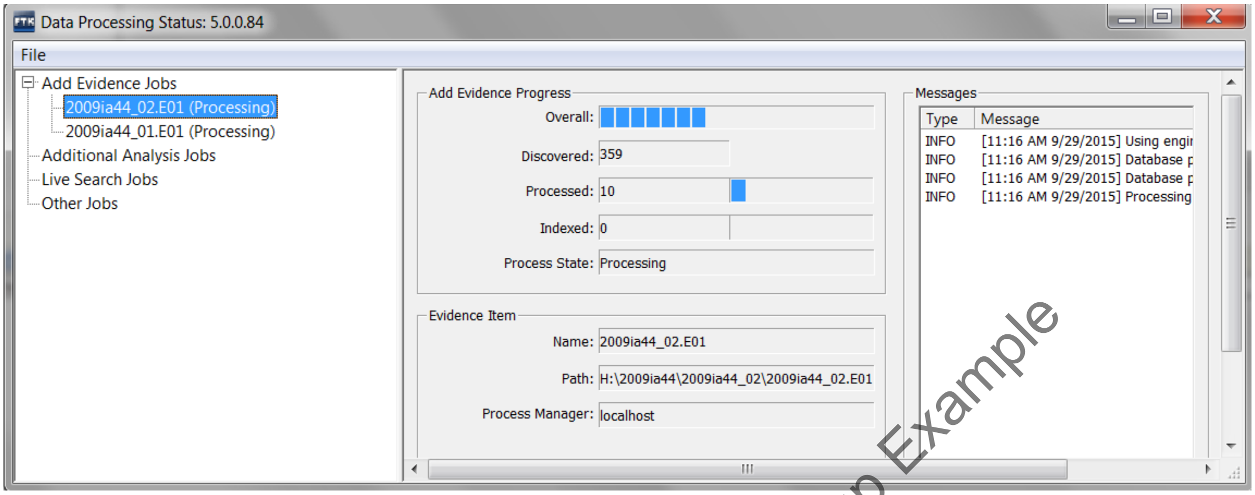
Select Evidence Type:

● Acquired Image(s)
○ All Images in Directory
○ Contents of a Directory
○ Individual File(s)
○ Physical Drive
○ Logical Drive

6. In the next window navigate to the image of the external drive and click **OK**.

7. The file(s)/folder that you selected should now appear in the Manage Evidence window. You may add other images now if needed (for example, if you have multiple images from the same accession), but you also have the option of adding additional evidence at a later time. Click **OK**.

8. A Data Processing Status window will appear.



- Add Evidence Jobs
  - 2009ia44_02.E01 (Processing)
  - 2009ia44_01.E01 (Processing)
- Additional Analysis Jobs
- Live Search Jobs
- Other Jobs

Add Evidence Progress

Overall:

Discovered: 359

Processed: 10

Indexed: 0

Process State: Processing

Evidence Item

Name: 2009ia44_02.E01

Path: H:\2009ia44\2009ia44_02\2009ia44_02.E01

Process Manager: localhost

Messages

```
Type   Message
INFO   [11:16 AM 9/29/2015] Using engi
INFO   [11:16 AM 9/29/2015] Database p
INFO   [11:16 AM 9/29/2015] Database p
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.

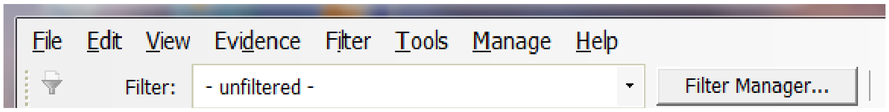
Once the processing job is done, you may want to search for documents with sensitive information or non-archival files to weed (exclude from file export). (See “IA Electronic record accessioning.pdf” at G:\Institutional Archives\ADMINISTRATION\ADM-135 Policies Procedures Adm\Archives_Policies_procedures_manuals\Manuals_Current\BornDigital for instructions.) Otherwise, continue to the next step to export files.

Exporting files

1. Connect USB dongle with the Forensic Toolkit license to your computer and open program and the case you’re working on.

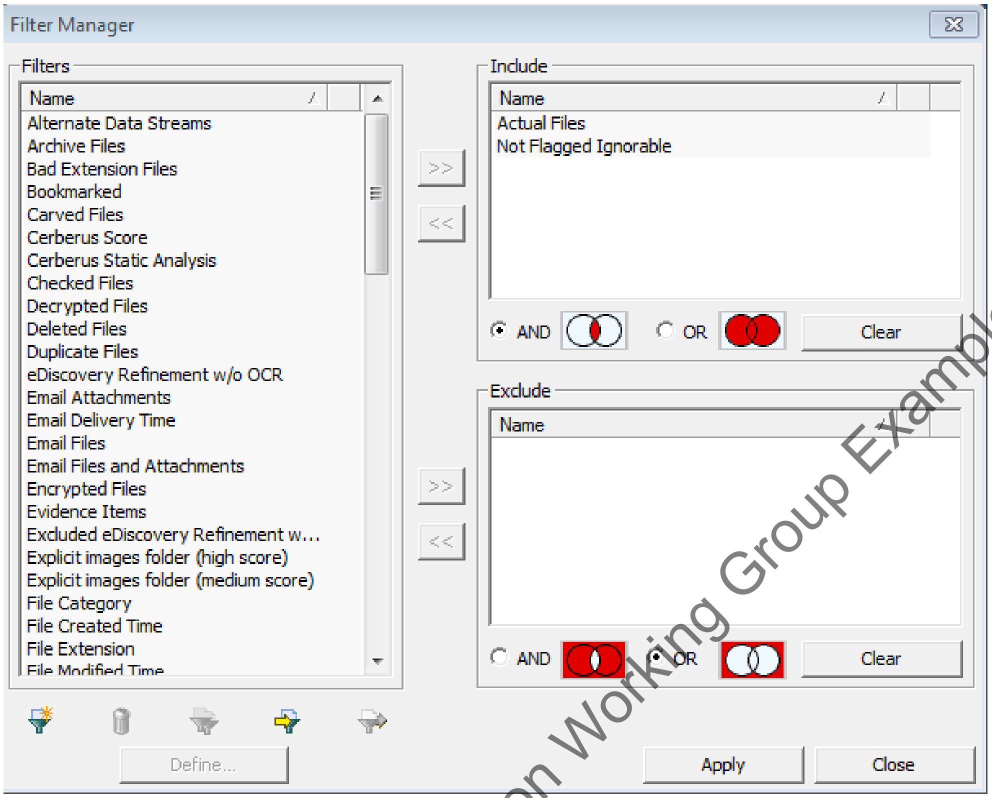
2. To export files, navigate to the Explorer tab. Make sure that all files that you want to export are currently displayed in the File List pane.

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



Filter: - unfiltered -

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



Filter Manager

Filters

Name

Alternate Data Streams
Archive Files
Bad Extension Files
Bookmarked
Carved Files
Cerberus Score
Cerberus Static Analysis
Checked Files
Decrypted Files
Deleted Files
Duplicate Files
eDiscovery Refinement w/o OCR
Email Attachments
Email Delivery Time
Email Files
Email Files and Attachments
Encrypted Files
Evidence Items
Excluded eDiscovery Refinement w...
Explicit images folder (high score)
Explicit images folder (medium score)
File Category
File Created Time
File Extension
File Modified Time

Include

Name

Actual Files
Not Flagged Ignorable

● AND ○ OR Clear

Exclude

Name

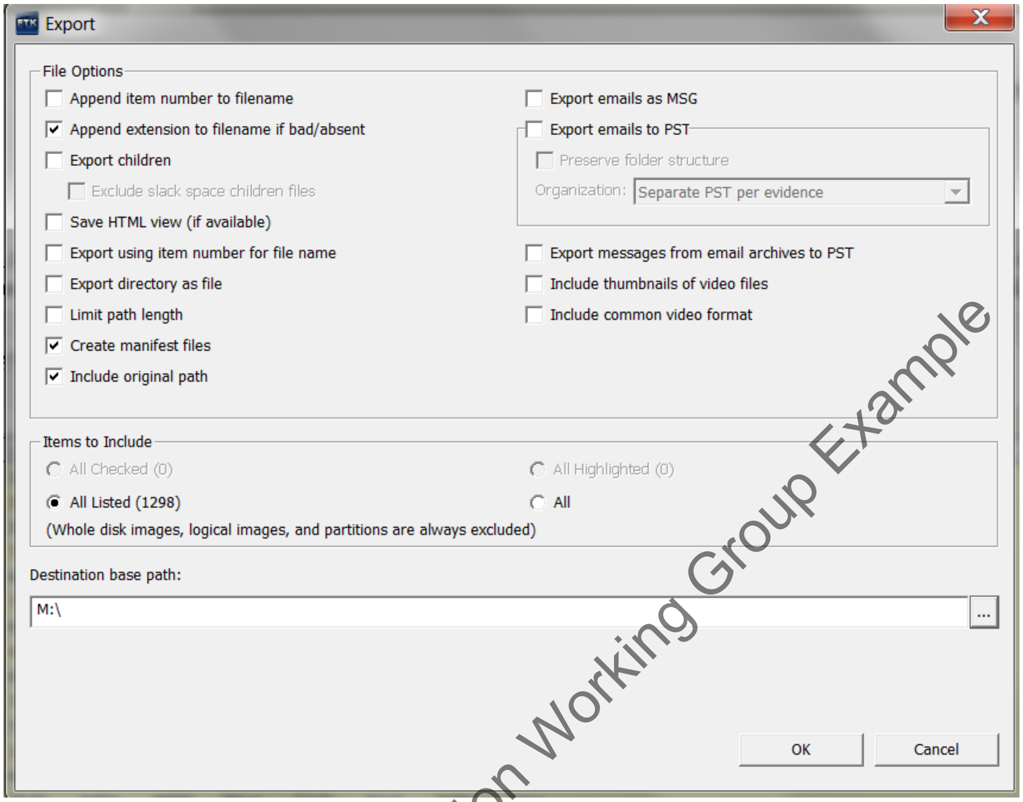
○ AND ● OR Clear

Define... Apply Close

3. 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**.

4. 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.



Export

File Options

☐ Append item number to filename
☑ Append extension to filename if bad/absent
☐ Export children
☐ Exclude slack space children files
☐ Save HTML view (if available)
☐ Export using item number for file name
☐ Export directory as file
☐ Limit path length
☑ Create manifest files
☑ Include original path
☐ Export emails as MSG
☐ Export emails to PST
☐ Preserve folder structure
Organization: Separate PST per evidence
☐ Export messages from email archives to PST
☐ Include thumbnails of video files
☐ Include common video format

Items to Include

○ All Checked (0)
○ All Highlighted (0)
● All Listed (1298)
○ All
(Whole disk images, logical images, and partitions are always excluded)

Destination base path:

M:\

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

6. 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.

F. FC5025

Software installed on Fluffy

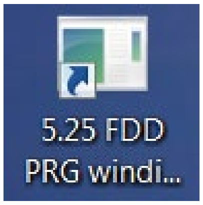
Overview

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.

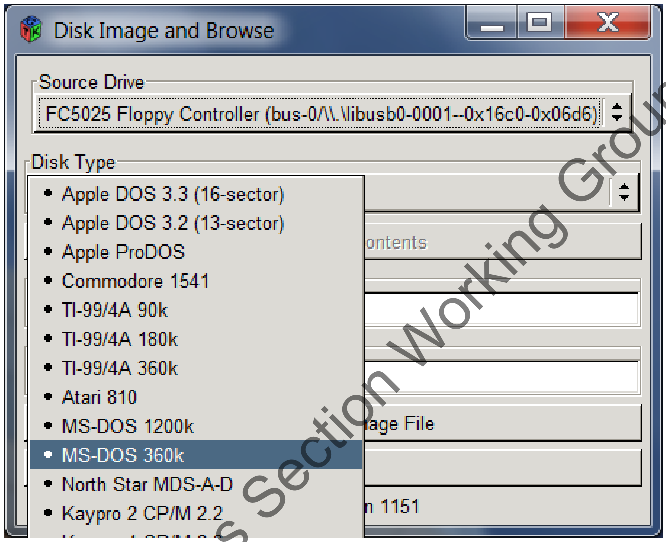
Create image or export files

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.

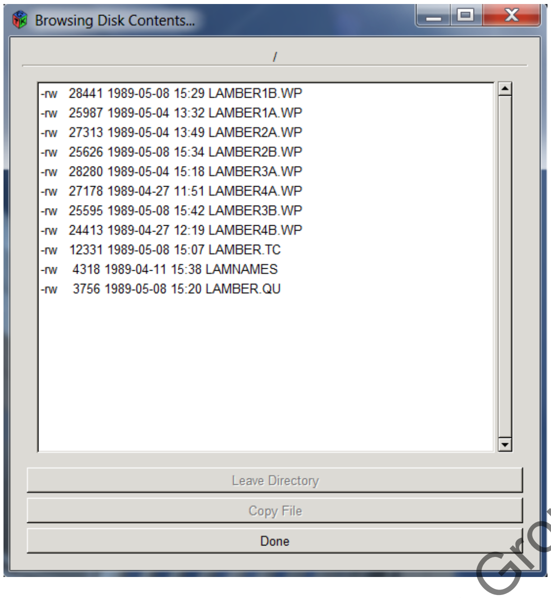
2. Double-click the software icon on Fluffy's desktop:



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.

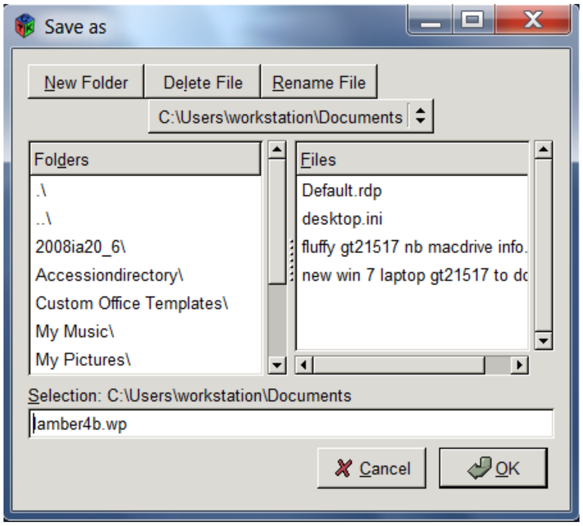


```
-rw   28441 1989-05-08 15:29 LAMBER1B.WP
-rw   25987 1989-05-04 13:32 LAMBER1A.WP
-rw   27313 1989-05-04 13:49 LAMBER2A.WP
-rw   25626 1989-05-08 15:34 LAMBER2B.WP
-rw   28280 1989-05-04 15:18 LAMBER3A.WP
-rw   27178 1989-04-27 11:51 LAMBER4A.WP
-rw   25595 1989-05-08 15:42 LAMBER3B.WP
-rw   24413 1989-04-27 12:19 LAMBER4B.WP
-rw   12331 1989-05-08 15:07 LAMBER.TC
-rw    4318 1989-04-11 15:38 LAMNAMES
-rw    3756 1989-05-08 15:20 LAMBER.QU
```

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 5 and try to create an image.**

When you get a file listing, if you can either 1) continue on to step 4 to transfer files from the disk in the Browsing Disk Contents window, file by file or 2) continue on to step 5 to image the disk and use FTK Imager to export files from the image.

4. To transfer a file from the disk, select a file and click **Copy File**. This will bring up a window to select the save location. Save to an empty external drive. (It's fine if the drive contains files from the same accession.)



Folders: .\ ; ..\ ; 2008ia20_6\ ; Accessiondirectory\ ; Custom Office Templates\ ; My Music\ ; My Pictures\

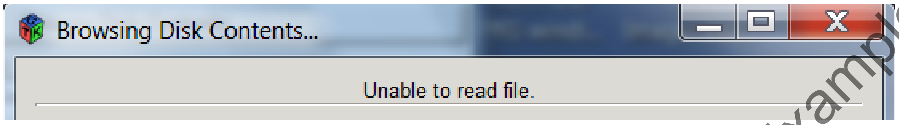
Files: Default.rdp ; desktop.ini ; fluffy gt21517 nb macdrive info. ; new win 7 laptop gt21517 to dc

Selection: C:\Users\workstation\Documents

lamber4b.wp

The file should now be available in the location where you saved it.

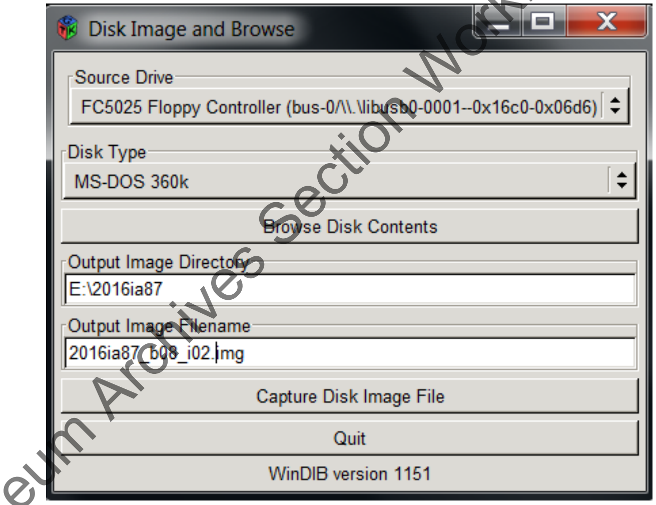
If the file is corrupt, it will save as an empty file and “Unable to read file” will appear at the top of the Browsing Disk Contents window. You can try imaging the disk to see if you can salvage any information in the file.



Unable to read file.

Organize exported files by the disk’s unique identifier. When you have finished copying all the files, click **Done** to exit the Browsing Disk Contents window.

5. To create an image of the disk, indicate under Output Image Directory the save location on Fluffy. Use the disk’s unique identifier as the filename under Output Image Filename.



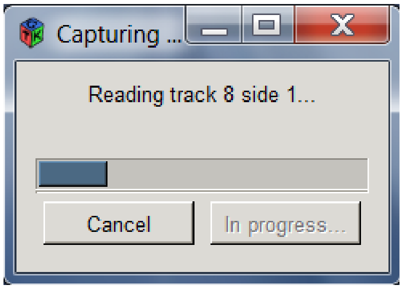
Source Drive: FC5025 Floppy Controller (bus-0/\\.\libusb0-0001--0x16c0-0x06d6)

Disk Type: MS-DOS 360k

Output Image Directory: E:\2016ia87

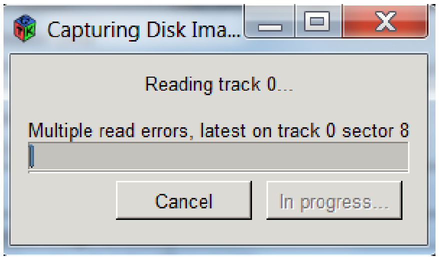
Output Image Filename: 2016ia87_b08_i02.img

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



Reading track 8 side 1...

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

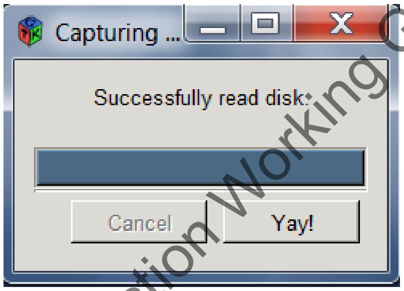


Reading track 0...

Multiple read errors, latest on track 0 sector 8

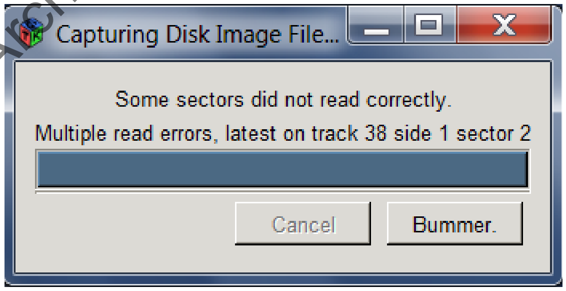
Cancel and select a different disk type until the software is able to successfully read tracks on the disk.

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



Successfully read disk.

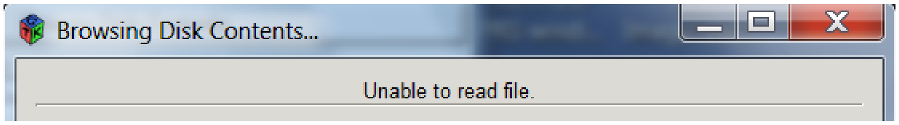
If there are problems imaging a disk, you should see something like this:



Some sectors did not read correctly.

Multiple read errors, latest on track 38 side 1 sector 2

If the software was able to read some or most of the disk, try imaging again under the same disk type. Do not delete the corrupt image just yet as you may be able to salvage data from it if necessary. If imaging fails again and the option is available, try copying files one by one in the Browsing Disk Contents window. You'll be able to identify the problem files if a files saves as an empty file and "Unable to read file" appears at the top of the Browsing Disk Contents window.



Unable to read file.

You can see if you can export the problem files from the corrupt image using FTK Imager. 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 use FTK Imager to examine deleted files on the disk and file slack as they may hold fragments of previous versions or temporary files of the corrupt file.

Troubleshooting corrupt files can be time consuming. Use your best judgement in determining the amount of effort you want to put into salvaging files.

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 FTK Imager for instructions on exporting files from the image. Use Bagger to transfer files to "[accession #]_original" folder on ira_locked.

G. FTK Imager

No license is required.
https://www.exterro.com/ftk-imager

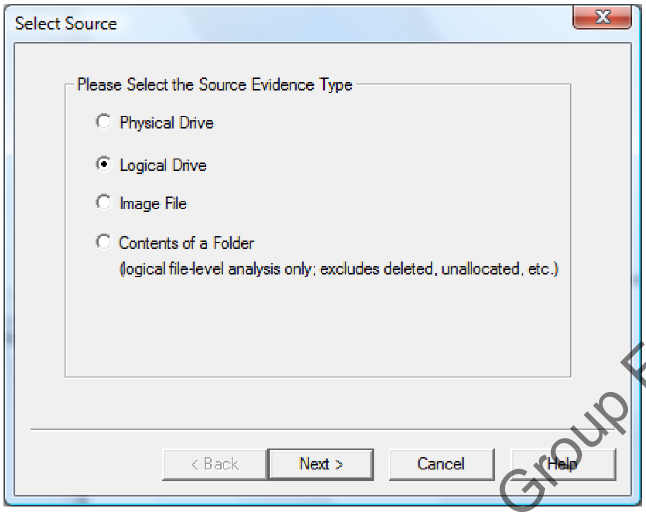
Overview

While we generally preference transferring individual files over capturing the entire environment, there may be instances where we need to create an image due to complex software or databases or problematic files. FTK Imager is our primary tool for imaging internal/external hard drives and one of our options for imaging optical discs. We also use FTK Imager to examine the contents of a disc image (only supports images and simple text documents), and to export files from images and corrupt optical discs. It can also be used to export files from other types of media when our standard transfer tools do not work.

For more thorough examination of images and exporting files from E01 files, use Forensic Toolkit.

Create image

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



Select Source

Please Select the Source Evidence Type

○ Physical Drive

● Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

Internal drive: To image the entire drive, select **Physical Drive**. If you want to only image certain folders, select **Contents of a Folder**. Click **Next**.

External drive: If you are imaging the drive because file path lengths exceed the maximum character limit (see Appendix B. File Path Limits), select **Logical Drive** (if you do not see the drive listed, select **Physical Drive**) and click **Next**. Otherwise, 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**.

Optical discs: Select **Logical Drive** and click **Next**. Note that if the disc contains multiple sessions, FTK Imager is only able to capture the first session.

3. Select a drive or folder to image.

   If imaging multiple optical discs in a single accession that have unique identifiers that are consecutively numbered, you may check the box next to **Automate Multiple Removable Media**. FTK Imager will automatically increment the evidence number with each image by adding "-000[#]" to the end of the filename. Note that while you cannot alter the number of leading zeros, you can adjust the starting evidence number. This is helpful if you are unable to complete imaging of all the discs in one sitting.

   Click **Finish**.

4. The **Create Image** screen will appear. Check off **Verify images after they are created** and **Create directory listings**. (Note that image verication will not work for optical discs.) Check off

Precalculate Progress Statistics if you would like an estimate of how long it will take to create an image.

If **Automate Multiple Removable Media** was selected in the previous window, change the starting evidence number if necessary.

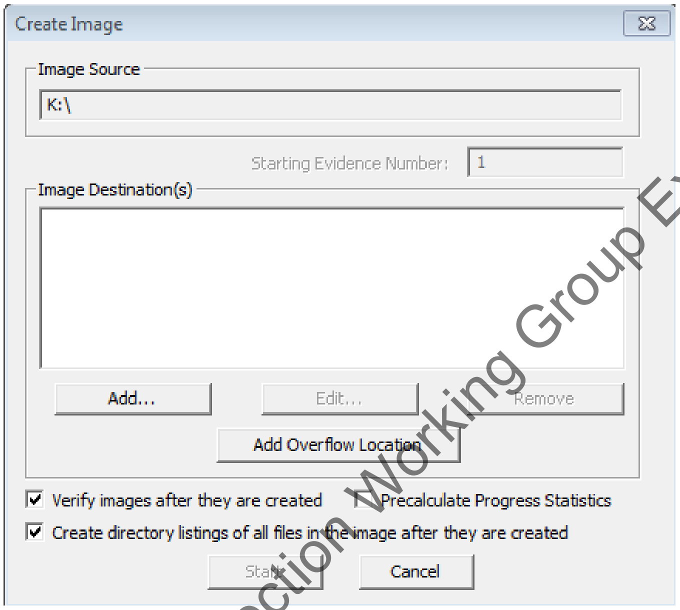


Image Source: K:\

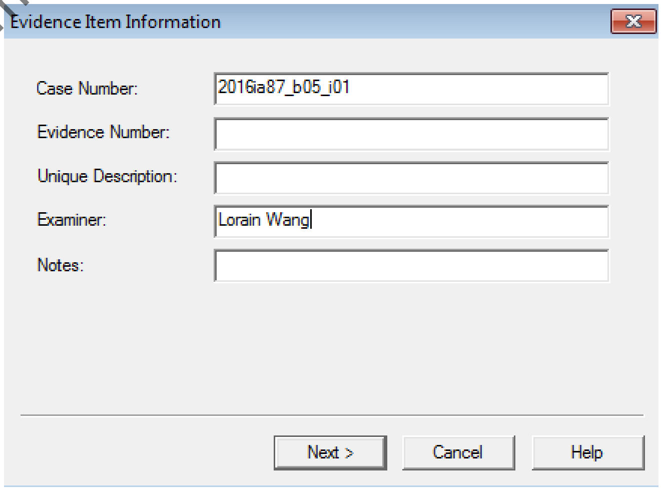
Starting Evidence Number: 1

Image Destination(s):

☑ Verify images after they are created ☐ Precalculate Progress Statistics

☑ Create directory listings of all files in the image after they are created

5. Click **Add**. If you are imaging an internal/external drive and selected **Logical Drive** or **Physical Drive**, select **E01** for image destination type. 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



Case Number: 2016ia87_b05_i01

Evidence Number:

Unique Description:

Examiner: Lorain Wang

Notes:

Click **Next**.

7. The **Select Image Destination** screen will appear.

   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 transfer later to a networked computer. Make sure there is sufficient room on the external hard drive for the image. If imaging a drive or disc 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 (does not apply to optical discs):
   AD1 (Contents of Folder): 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 (Logical/Physical Drive for internal/external drives): 0

   Compression: 5

   Click **Finish**.

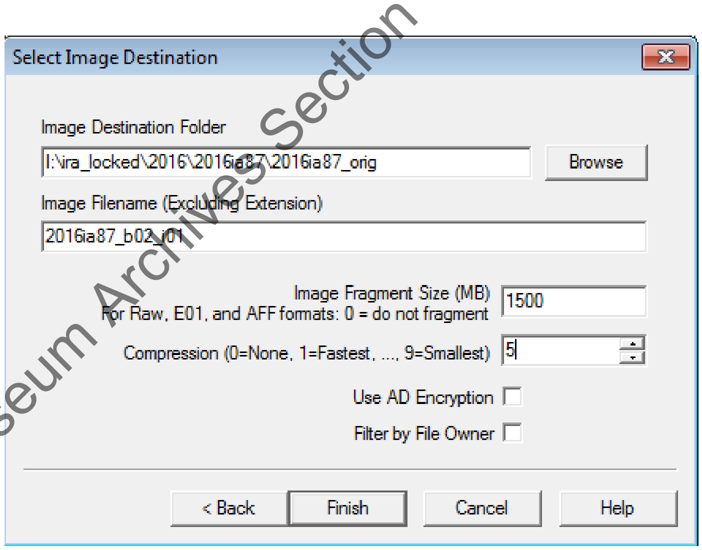

Select Image Destination

Image Destination Folder: I:\ira_locked\2016\2016ia87\2016ia87_orig

Image Filename (Excluding Extension): 2016ia87_b02_i01

Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment: 1500

Compression (0=None, 1=Fastest, ..., 9=Smallest): 5

Use AD Encryption □

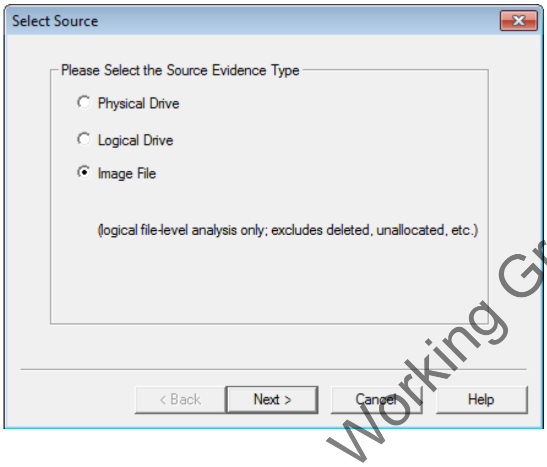
Filter by File Owner □

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.**

Examine and export files from images

Use FTK Imager to extract files from AD1 (contents of folder), IMG (floppy disk), and ISO (optical disc) image files. You may also use to this software to examine the contents of images and simple text files without accidentally editing the files. If you would like to search for files with sensitive information and weed non-archival files, use [Forensic Toolkit]() instead to extract files. Also use Forensic Toolkit for E01 files.

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



Select Source

Please Select the Source Evidence Type

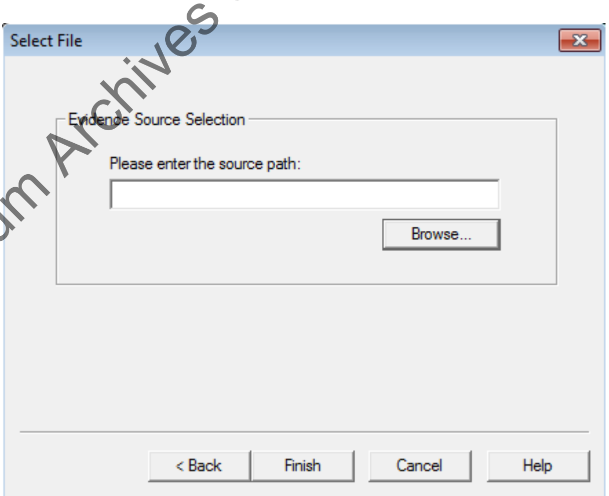
○ Physical Drive

○ Logical Drive

● Image File

(logical file-level analysis only; excludes deleted, unallocated, etc.)

3. In the next window click **Browse** and navigate to the image file. For image files on network drives, you will need to type the entire server path as not all network drives may appear in the directory. For example, for a file on wbench1, you would type: \\prd-arj\arj1\wbench1\processing\2016ia47\gia_2016_ia_47_004.iso.

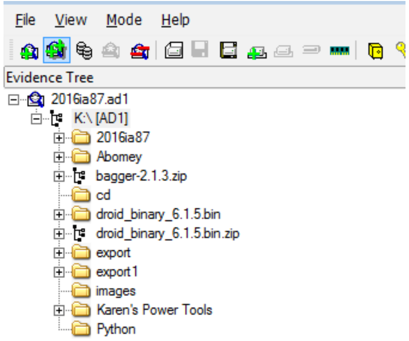


Select File

Evidence Source Selection

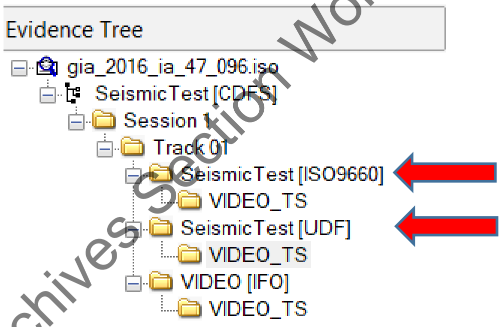
Please enter the source path:

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

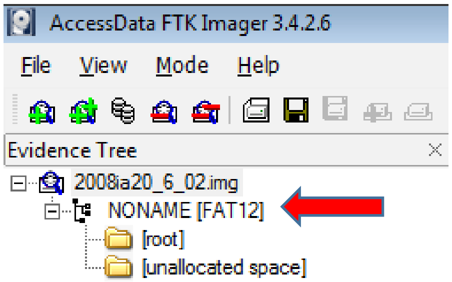


For IMG and ISO files, you will see file systems listed (see red arrows).

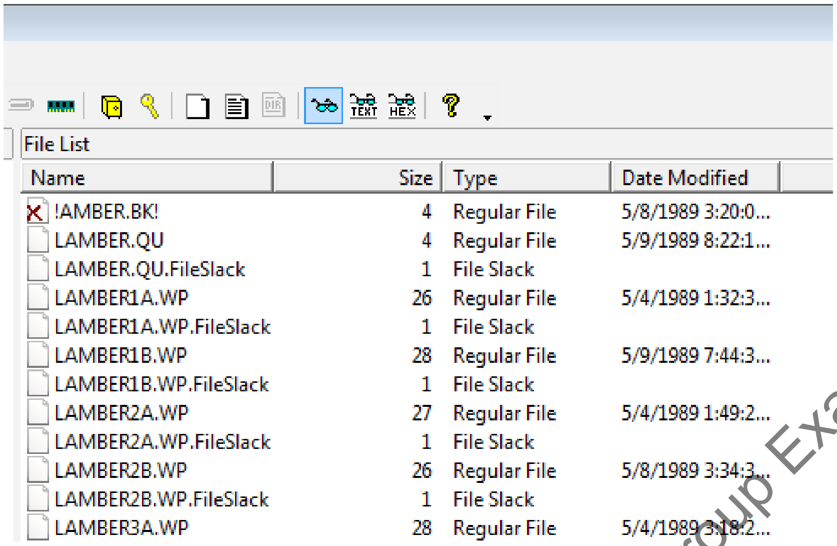
Note that optical discs will have more than one file system.



Most PC floppy disks use the FAT12 file system. Files are located under the "root" folder.



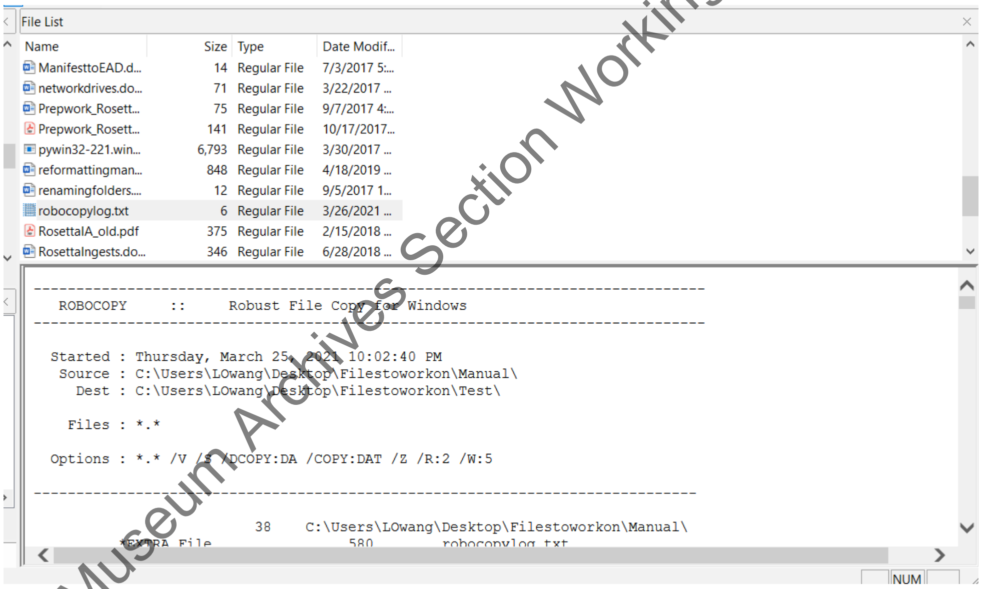
In the file list pane, a red X indicates a deleted file. File Slack refers to "unused" storage space that was allocated to a file. Both file slack and the unallocated space data may contain residual data of old deleted files. Unless we are trying to reconstruct lost data, we typically do not need to (and would prefer not to) preserve these kind of files.



File List

Name	Size	Type	Date Modified
!AMBER.BK!	4	Regular File	5/8/1989 3:20:0...
LAMBER.QU	4	Regular File	5/9/1989 8:22:1...
LAMBER.QU.FileSlack	1	File Slack	
LAMBER1A.WP	26	Regular File	5/4/1989 1:32:3...
LAMBER1A.WP.FileSlack	1	File Slack	
LAMBER1B.WP	28	Regular File	5/9/1989 7:44:3...
LAMBER1B.WP.FileSlack	1	File Slack	
LAMBER2A.WP	27	Regular File	5/4/1989 1:49:2...
LAMBER2A.WP.FileSlack	1	File Slack	
LAMBER2B.WP	26	Regular File	5/8/1989 3:34:3...
LAMBER2B.WP.FileSlack	1	File Slack	
LAMBER3A.WP	28	Regular File	5/4/1989 3:18:2...

For certain file formats (such as PDF, TXT, and JPG) the contents of the file will display.



File List

Name	Size	Type	Date Modif...
ManifesttoEAD.d...	14	Regular File	7/3/2017 5:...
networkdrives.do...	71	Regular File	3/22/2017 ...
Prepwork_Rosett...	75	Regular File	9/7/2017 4:...
Prepwork_Rosett...	141	Regular File	10/17/2017...
pywin32-221.win...	6,793	Regular File	3/30/2017 ...
reformattingman...	848	Regular File	4/18/2019 ...
renamingfolders....	12	Regular File	9/5/2017 1...
robocopylog.txt	6	Regular File	3/26/2021 ...
RosettaIA_old.pdf	375	Regular File	2/15/2018 ...
RosettaIngests.do...	346	Regular File	6/28/2018 ...

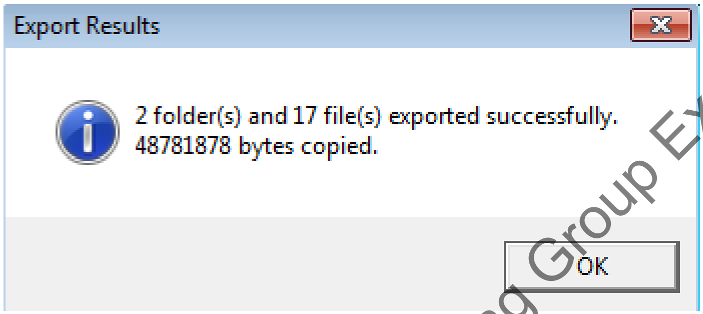
```
-------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows
-------------------------------------------------------------------------------

  Started : Thursday, March 25, 2021 10:02:40 PM
   Source : C:\Users\LOwang\Desktop\Filestoworkon\Manual\
     Dest : C:\Users\LOwang\Desktop\Filestoworkon\Test\

    Files : *.*

  Options : *.* /V /S /DCOPY:DA /COPY:DAT /Z /R:2 /W:5

------------------------------------------------------------------------------

                          38    C:\Users\LOwang\Desktop\Filestoworkon\Manual\
        *EXTRA File                580         robocopylog.txt
```

5. To export files you can right-click a folder in the **Evidence Tree** or **File List** panes to export all the files within a folder or right-click an individual file in the **File List** pane. Right-click the folder right below the top folder to export the entire contents of an image. Note that exporting all the files within a folder will include any file slack and deleted files that are present. To exclude those or other files you can click Ctrl+A and use Ctrl+click to deselect the files that you do not want to export. (If working with a large and complex set of files, it may be easier to use Forensic Toolkit to select the specific files to export.) When you are ready, right-click and select **Export Files**.

For optical discs, you will export files from one file system. See the section on CD and DVD file systems for guidance on which file system to choose.

6. 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.

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

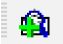


2 folder(s) and 17 file(s) exported successfully.
48781878 bytes copied.

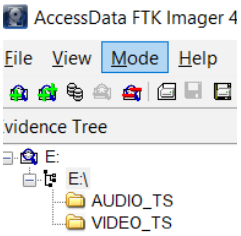
8. Right-click the same folder or files in the **Evidence Tree/File List** panes that you selected earlier. This time select **Export File Hash List**. Save the file in the accession's documentation folder on ira_locked. Name the file "[unique identifier]_ftkexport.csv".

9. Maintain exported files on ira_locked in bag.

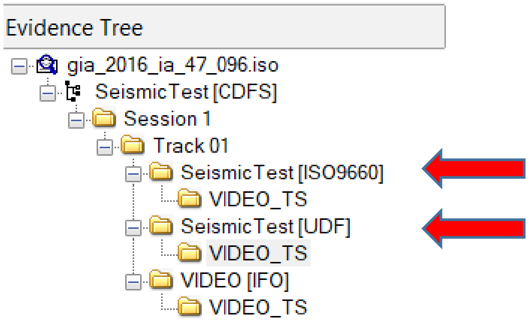
Export files from optical disc



2. Select **Logical Drive** and click **Next.** Select the drive from the drop-down menu and click **Finish**. If you get a "Failed to get drive info" message, select **Contents of a Folder** instead. Browse to the location of the folder/drive and click **Finish**.
3. The contents of the optical disc should appear in the evidence tree pane.



If you selected **Logical Drive**, you will see multiple file systems listed. You will export files from one file system.

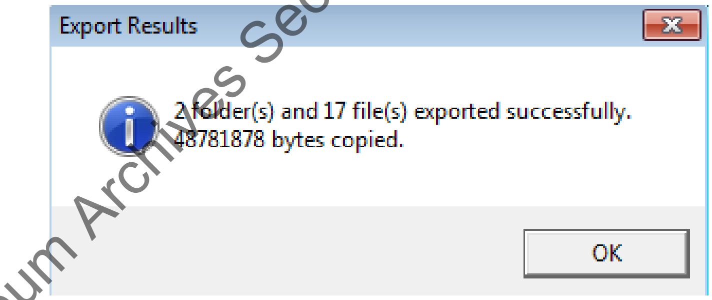


4. In the **Evidence Tree** pane, right-click the folder that you want to export.

   If you selected **Logical Drive** earlier, you will export files from only one file system. See the section on CD and DVD file systems for guidance on which file system to choose.

   If you selected **Contents of a folder,** select 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.
5. Once export is successfully completed, you should see something like this:

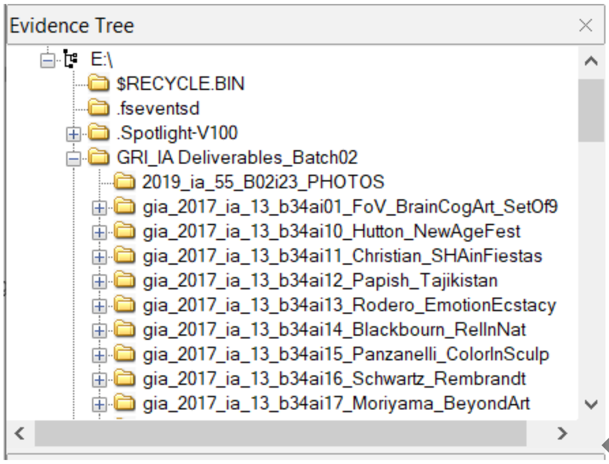


2 folder(s) and 17 file(s) exported successfully.
48781878 bytes copied.

6. Right-click the same folder in the **Evidence Tree** pane that you selected earlier. 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".

Export files from non-optical disc media

2. Select **Contents of a Folder** and click **Next**. Browse to the location of the folder and click **Finish**.
3. The contents should appear in the evidence tree pane.



Evidence Tree

```
E:\
  $RECYCLE.BIN
  .fseventsd
  .Spotlight-V100
  GRI_IA Deliverables_Batch02
    2019_ia_55_B02i23_PHOTOS
    gia_2017_ia_13_b34ai01_FoV_BrainCogArt_SetOf9
    gia_2017_ia_13_b34ai10_Hutton_NewAgeFest
    gia_2017_ia_13_b34ai11_Christian_SHAinFiestas
    gia_2017_ia_13_b34ai12_Papish_Tajikistan
    gia_2017_ia_13_b34ai13_Rodero_EmotionEcstacy
    gia_2017_ia_13_b34ai14_Blackbourn_RelInNat
    gia_2017_ia_13_b34ai15_Panzanelli_ColorInSculp
    gia_2017_ia_13_b34ai16_Schwartz_Rembrandt
    gia_2017_ia_13_b34ai17_Moriyama_BeyondArt
```

4. Right-click the folder that you want to export and click **Export Files**. Select your save location. If working on Fluffy or FRED, save files to an external drive. If working on a networked computer, save files to "[accession #]_original" folder on ira_locked.
5. Right-click the same folder in the **Evidence Tree** pane that you selected earlier. 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".

H. Isobuster

https://www.isobuster.com/download.php (Licensed version offers more features for exporting files. We plan on purchasing at least one license in the near future.)

Extract files [under construction]

Create a disc image of CDs/DVDs.

1. Load your source disc into your drive and startup IsoBuster. It should read the contents of the disc (the entire content, not just the files) and display a tree view on the left pane. In case you do not get any such display, make sure that you have selected the right optical drive in the drop-down box below the menu.
2. Now go to the menu – Options > Image Files. Under "Select when a cuesheet file will be created", make sure that either "Always after a CD or DVD image is created" or "Prompt after a CD or DVD image is created" is selected. It is better to select "Always".
3. Optionally, you may also select "Always" or "Prompt" under "Select when an MD5 checksum file will be created".
4. Click OK to exit dialog.
5. On the left-hand pane of the main window, you will see a tree structure. At the top (-left) of this tree, you will see a small disc icon and CD or DVD-R or something similar based on what kind of medium you have inserted into the drive. Right-click on this.
6. You will see a menu popup. If the disc is a CD, select Extract CD (Image) > RAW (*.bin, *.iso). If it is a DVD, select Extract DVD (Image) > User Data (*.tao, *.iso).
7. Now enter a filename [accessionnumber_[boxnumber]_item# with the extension .iso and press Save.

8. IsoBuster should (successfully) extract your disc data and write it to the image file on your hard disk.

I. Karen's Directory

No license is required.
G:\Institutional Archives\ENGINEERING\ENG-120 Software_Hardware\BornDigitalToolsInstallation_files\Karens_directory

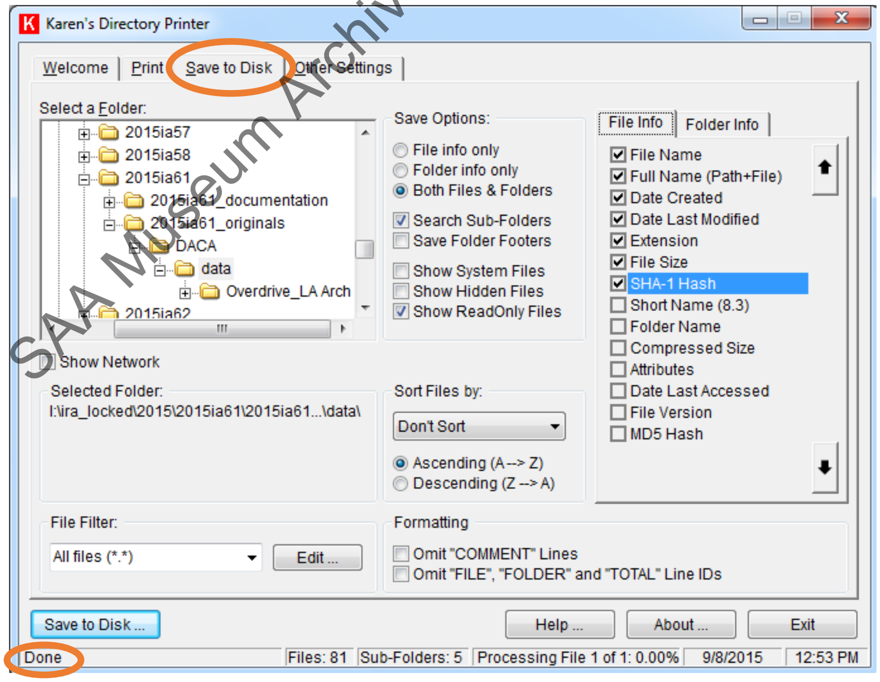
Note that you will need to copy the file to your local computer to install.

Overview

Karen's Directory is one of the tools that we can use to generate a list of checksums of accessioned digital files. In addition to checksums, the manifest we create using Karen's Directory includes a list of file and folder names, file paths, file size, creation date, and date last modified. Note that Karen's Directory will not generate checksums for files with file path lengths that exceed character limits. Add a note in the accession record in the **Digital File Mgmt Notes** field if checksums are missing for certain files.

Generate checksums

1. Open Karen's Directory Printer and click on the **Save to Disk** tab at the top.
2. In the file tree window, select the folder containing the digital files.
3. Select the following options and file/folder information:



☐ Show Network

Selected Folder:
I:\ira_locked\2015\2015ia61\2015ia61...\data\

File Filter: All files (*.*)

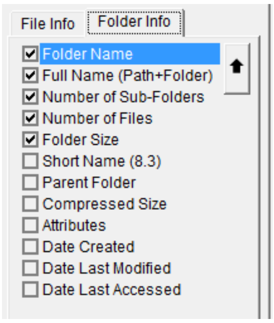
Save Options:
○ File info only
○ Folder info only
● Both Files & Folders
☑ Search Sub-Folders
☐ Save Folder Footers
☐ Show System Files
☐ Show Hidden Files
☑ Show ReadOnly Files

Sort Files by: Don't Sort
● Ascending (A --> Z)
○ Descending (Z --> A)

Formatting
☐ Omit "COMMENT" Lines
☐ Omit "FILE", "FOLDER" and "TOTAL" Line IDs

File Info
☑ File Name
☑ Full Name (Path+File)
☑ Date Created
☑ Date Last Modified
☑ Extension
☑ File Size
☑ SHA-1 Hash
☐ Short Name (8.3)
☐ Folder Name
☐ Compressed Size
☐ Attributes
☐ Date Last Accessed
☐ File Version
☐ MD5 Hash

Done | Files: 81 | Sub-Folders: 5 | Processing File 1 of 1: 0.00% | 9/8/2015 | 12:53 PM



☑ Folder Name
☑ Full Name (Path+Folder)
☑ Number of Sub-Folders
☑ Number of Files
☑ Folder Size
☐ Short Name (8.3)
☐ Parent Folder
☐ Compressed Size
☐ Attributes
☐ Date Created
☐ Date Last Modified
☐ Date Last Accessed

Make sure that the selected file/folder information is in the same order as above. You can change the order using the up and down arrows on the right. Under the **Other Settings** tab, verify that the **Remember my settings** box is checked so that you do not need to repeat this step each time you use Karen's Directory Printer.

4. Click the **Save to Disk** button at the bottom of the screen and select the save location for the manifest in the window that appears. The save location should be the "[accession #]_documentation" folder on ira_locked. Name the file "[accession#]_manifest.txt."
5. When you click the **Save** button, Karen's Directory Printer will begin generating the manifest. Since this includes calculating the checksum for each file, this process may take several hours to complete if there are large video or image files. Upon completion, "Done" will appear at the bottom of the screen.
6. If needed, the generated text document can be transformed into an EAD xml for import into ASpace. (Ask Lorain for assistance with this.)

J. KryoFlux

Software is installed on Fluffy.

Overview

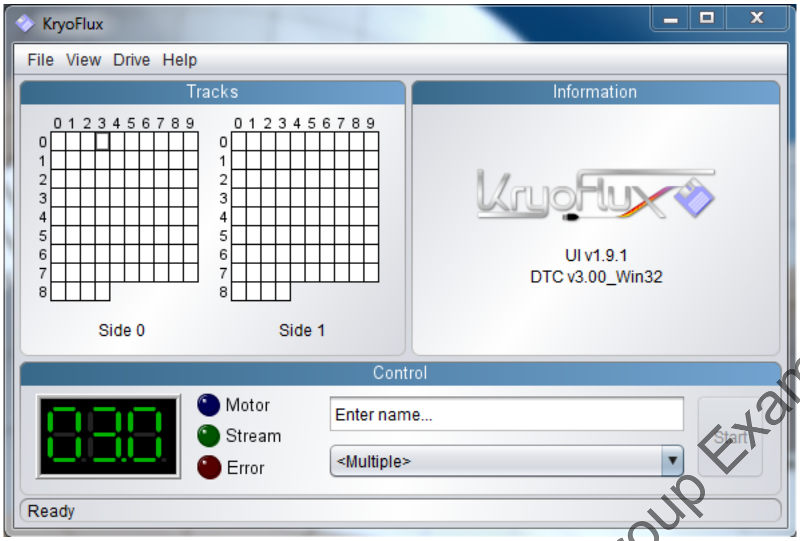
KryoFlux is installed on Fluffy and can be used to image 3.5" and 5.25" floppy disks. KryoFlux has built-in write-blocking so you don't need to write-protect the disk.

For more detailed instructions see The Archivist's Guide to KryoFlux. (Copy is also available in KryoFlux Manuals folder on Fluffy's desktop.)

Create disk image

Important: Remember to unplug the KryoFlux power cable when done imaging.

1. Plug-in KryoFlux power cable.
2. Connect KryoFlux USB.
3. Click on KryoFlux-UI shortcut on desktop.



Enter name...

<Multiple>

Ready

4. Before you start imaging, you will need to calibrate the drive you will be using. Click Drive and select the appropriate drive number.

   Drive 0 – 3.5" floppy drive

   Drive 1 – 5.25" floppy drive

   Next, click Drive→Calibrate. A disk does not need to be in the drive when you calibrate. There should be a message at the bottom of the window that calibration was successful.

   ****You will need to calibrate each time you switch between the two drives during a session. ****

5. By default images will save in the KryoFlux folder on the D: drive. If you would like to change the save location, click File→Settings→Output.

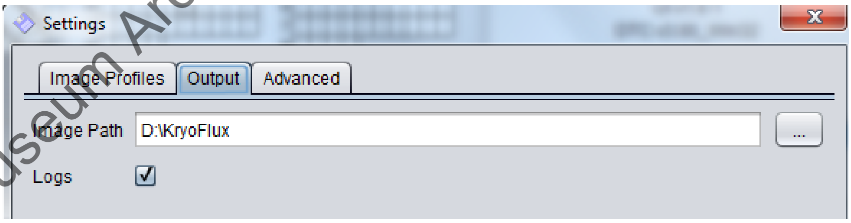


Image Path D:\KryoFlux

Logs ☑

6. Back on the main KryoFlux screen, enter the filename for the image that you want to create. Do not include the extension.
7. If you know what type of floppy format you are dealing with, select the appropriate image format in the drop-down menu and click Start. Continue on to step 10.
8. If you don't know the format (which is usually the case) the safest thing to do is to select "KryoFlux stream files, preservation." Click Start and the cells in the Tracks pane will begin to turn grey as KryoFlux images each sector of the disk.

   The stream format is a proprietary format that is not readable but can be used to create formatted images ("deviceless mode"). This is a useful feature when the user is not able to *identify the file format. Rather than repeatedly imaging the physical disk, which will cause degradation, a user can safely create multiple formats by imaging the stream.*

Once the stream has been created, create formatted images from the stream files by clicking Drive→Stream Files. Enter a filename (use the unique identifier) for the image you want to create and select an image format in the drop-down menu.

If it is a PC formatted disk, it is usually either "MFM (40 Track) sector image" or "MFM (80 Track) sector image." For 3.5" Mac disks, it is usually "Apple DOS 400/800K sector image."

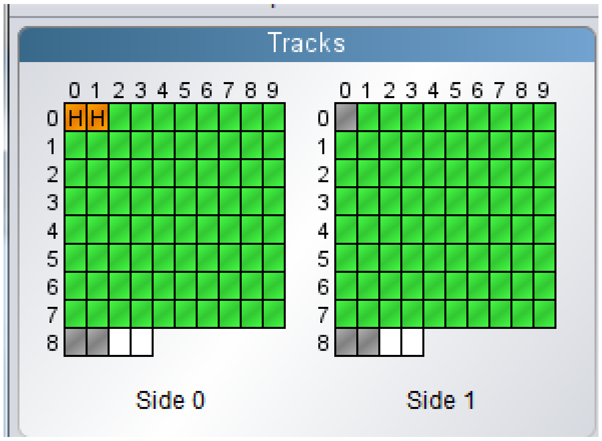
Selecting <Multiple>, which allows you to select multiple formats, is not recommended as it does not clearly indicate which of the resulting files is the best image. In addition, if you select multiple formats with the same extension, files will be overwritten by the last format created (and not necessarily by the best one.)

When you have made your selection, click Start and navigate to the location of the stream files.

9. Once imaging begins, the cells in the Tracks pane will fill with different colors. The colors will help you determine if you've selected the correct image format.

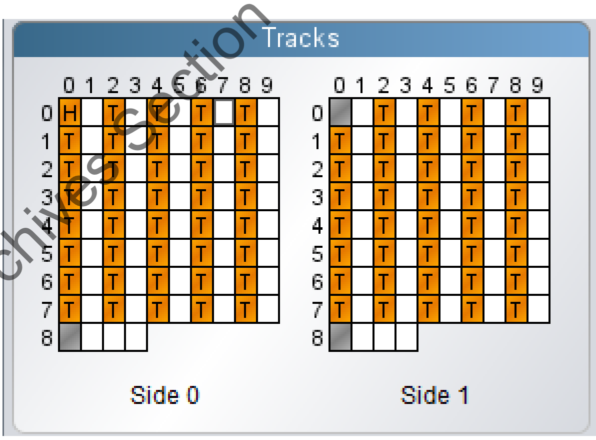
Green (Good)	Imaged successfully.
Orange (Good and modified)	Imaged successfully and sector was modified. This could mean that a file was deleted, edited, or added to the disk.
Grey (Unknown)	KryoFlux could not determine status of the track.
Red (Bad)	Unsuccessful read.
Yellow	[Not sure what this means.]

If at least 90% of the boxes are green or a mix of green and orange you have selected the correct format.



Some things to keep in mind:

- If you selected MFM (40 Tracks) and the cells alternate between white and orange/green, it is often an indication that the correct format is MFM (80 Tracks). If MFM (80 Tracks) does not produce an output that is >90% green/orange, then MFM (40 Tracks) is probably the best format.



- If none of the formats are producing >90% green/orange output, examine and compare (using FTK Imager) the content on the images that have any orange or green tracks. You may still be able to salvage some or all of the content.
- CBM GCR may produce an output with a good amount of green cells. Unfortunately FTK Imager does not recognize these outputs as valid images. I have been unable to determine if this is just an FTK Imager issue.

10. Export files from KryoFlux using FTK Imager.
11. Unplug the KryoFlux cable when done imaging.

K. MacDrive

A license is required. (Check with Teresa Soleau if she has any spare licenses before ordering.)
https://www.macdrive.com/

MacDrive is a software we use to read Mac-formatted external drives on Windows-based computers. When the software is installed and you connect a Mac-formatted drive, MacDrive will automatically detect the drive and you will be able to read the contents of the drive in file explorer.

L. MagicDisc

License is not required. Does not work on Windows 10 machines.
G:\Institutional Archives\ENGINEERING\ENG-120 Software_Hardware\BornDigitalToolsInstallation_files

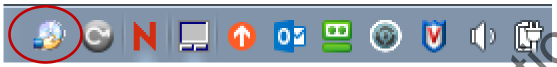
Note that you will need to copy the file to your local computer to install.

Overview

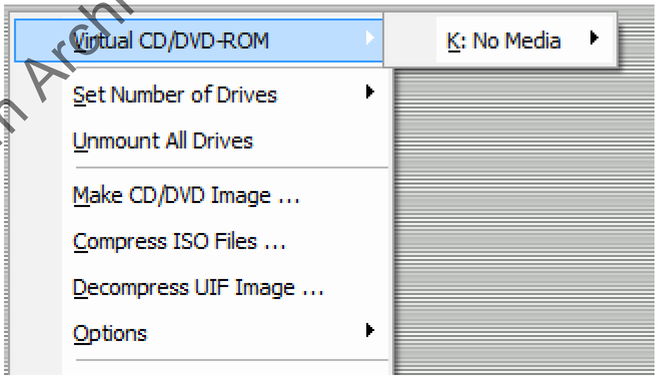
MagicDisc is a tool for examining the contents of iso disc images through file explorer rather than through the interface of special software such as FTK Imager (has a mount image feature but is unable to mount iso files) or Forensic Toolkit. MagicDisc works by allowing a user to "mount" an iso file. A virtual drive is created, allowing you to interact with the iso file like an actual disc in an optical drive. Note that MagicDisc will not work for iso files that are broken into multiple parts.

Mounting disc image

1. If MagicDisc is installed on your computer, you should see a small icon for the software on your taskbar.



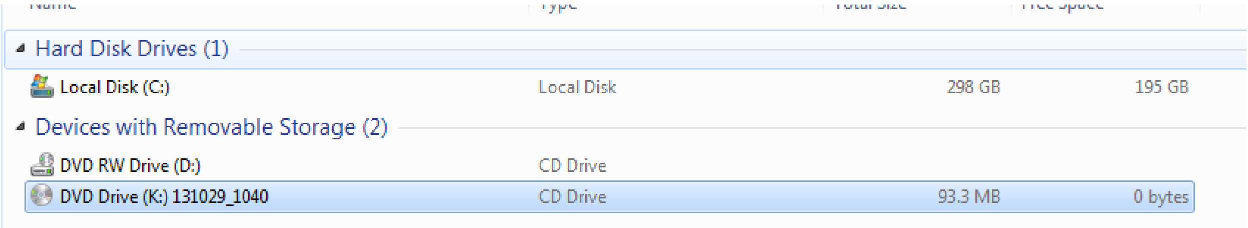
Right-click the icon and click on Virtual CD/DVD-ROM.



Select the available drive. The drive letter will vary from computer to computer. Click Mount in the next menu

2. Browse and select the iso file you want to mount and click OK.

3. Navigate to file explorer.



Hard Disk Drives (1)			
Local Disk (C:)	Local Disk	298 GB	195 GB
Devices with Removable Storage (2)			
DVD RW Drive (D:)	CD Drive		
DVD Drive (K:) 131029_1040	CD Drive	93.3 MB	0 bytes

The image file should now appear mounted on the virtual drive. Double-click the drive and you should be able to see and open files within the disc image. You can also use QuickView Plus on the virtual drive.

M. Robocopy

No installation required if using Windows machine.

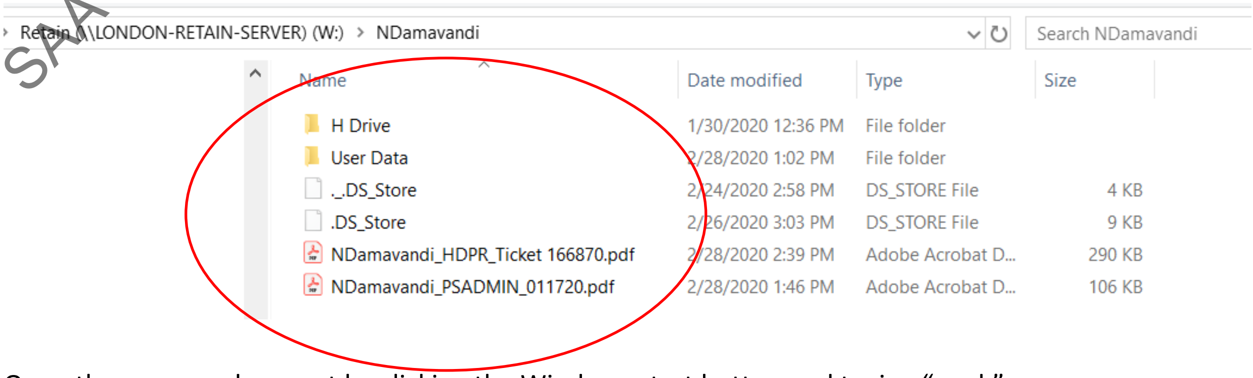
Overview

Robocopy is a command-line tool that copies files and folders from one location to another. It is a standard feature of Windows so no installation is needed. It does not have a GUI (Graphical User Interface) so it is not as user friendly as other file transfer software in our toolkit.

Robocopy is best used for large transfers due to its ability to resume incomplete transfers. It is also able to transfer files with file paths that exceed character limits, but it depends on the file system of the source and destination drive (for example, supported by NTFS but not NcFsd). Unfortunately, it is not good at identifying transfer errors and does not have a built-in verification system. Consequently, we will always need to run other tools to verify every Robocopy transfer.

Transfer files

1. Create a destination folder for the copied files if needed. Robocopy will not copy the folder that you specify for duplication, only the folders and files within that folder. For example, if we run Robocopy to copy the "NDamavandi" folder, only the subfolders will copy over, not the "NDamavandi" folder.



Retain (\\LONDON-RETAIN-SERVER) (W:) > NDamavandi

Name	Date modified	Type	Size
H Drive	1/30/2020 12:36 PM	File folder	
User Data	2/28/2020 1:02 PM	File folder	
._.DS_Store	2/24/2020 2:58 PM	DS_STORE File	4 KB
.DS_Store	2/26/2020 3:03 PM	DS_STORE File	9 KB
NDamavandi_HDPR_Ticket 166870.pdf	2/28/2020 2:39 PM	Adobe Acrobat D...	290 KB
NDamavandi_PSADMIN_011720.pdf	2/28/2020 1:46 PM	Adobe Acrobat D...	106 KB

2. Open the command prompt by clicking the Windows start button and typing "cmd."

3. Check whether the file paths of any of the files to be copied exceed character the character limit. (See Appendix A. File Path limits.) Run Path Length Checker to check file path lengths. If you know or are unsure whether the source or destination file system is unable to handle transfers of long file paths, map drive letter to the source/destination folder as needed to shorten file paths.
4. In the command prompt, type the following command to transfer an entire folder (for transferring specific files or excluding a specific folder see Robocopy parameters section): robocopy "[file path of files to be transferred]" "[destination file path]" /copy:DAT /z /r:2 /w:5 /v /e

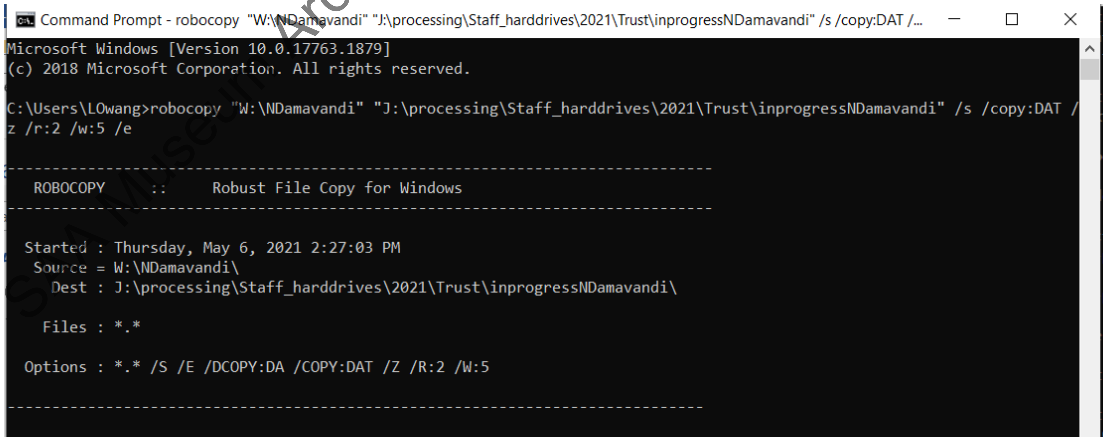
   Example:
   robocopy "W:\NDamavandi" "J:\processing\Staff_harddrives\2021\Trust\inprogress NDamavandi" /s /copy:DAT /z /r:2 /w:5 /v /e

   If you assigned a drive letter to a folder in step 3, use the new drive letter in the command.

   Example:
   If drive K: was mapped to J:\processing\Staff_harddrives\2021\Trust\inprogressNDamavandi

   Type the following in command-line:
   robocopy "W:\NDamavandi" "K:" /s /copy:DAT /z /r:2 /w:5 /v /e

   Robocopy will begin the copy process.


Command Prompt - robocopy "W:\NDamavandi" "J:\processing\Staff_harddrives\2021\Trust\inprogressNDamavandi" /s /copy:DAT /...

```
Microsoft Windows [Version 10.0.17763.1879]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\LOwang>robocopy "W:\NDamavandi" "J:\processing\Staff_harddrives\2021\Trust\inprogressNDamavandi" /s /copy:DAT /
z /r:2 /w:5 /e

-------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows
-------------------------------------------------------------------------------

  Started : Thursday, May 6, 2021 2:27:03 PM
   Source = W:\NDamavandi\
     Dest : J:\processing\Staff_harddrives\2021\Trust\inprogressNDamavandi\

    Files : *.*

  Options : *.* /S /E /DCOPY:DA /COPY:DAT /Z /R:2 /W:5

------------------------------------------------------------------------------
```

5. If you need to stop the transfer, you can press Ctrl+C or close the command prompt window. To resume the transfer, type the exact same command in step 4. If you mapped a drive letter in step 3 and have since restarted the computer or removed the mapping, you will need to remap

the folder. When you re-execute the command, Robocopy will run through all the files and identify and skip the files that have already been copied.

To save time, you can edit the Robocopy command to focus on a specific folder, making sure that the same folder exists in the copied set of files.

For example, working with the same example used in step 4, if you know that Robocopy has transferred all the files except for the ones in the “Documents” folder, using the below command, Robocopy will identify and skip the files that have already been copied in the “Documents” folder and copy over the remaining “Documents” files rather than running through the entire set of files in the “NDamavandi” folder.

```
robocopy "W:\NDamavandi\User Data\GT27833\Documents" "J:\processing\Staff_harddrives\2021\Trust\inprogressNDamavandi\User Data\GT27833\Documents" /s /copy:DAT /z /r:2 /w:5 /v /e
```

6. Once the transfer has completed, you will see a transfer summary indicating the number of files transferred and the number of errors. Whether or not there were any errors, you will need to continue on to the file verification process as the error summary is not always correct and the missing files are not easy to identify.
7. Use BeyondCompare’s Folder Compare function to compare the original and copied folders. This tool will identify which files are missing and which do not match in size. If only a few files are missing or do not match, you may want to simply copy and paste the files. If entire folders are missing, try rerunning Robocopy. The most common reason for failed transfers is due to file paths exceeding character limits, but network connection issues can also interrupt the transfer process. When BeyondCompare shows the original and copied set of files are an exact match, move on to the next step for checksum verification.
8. Use QuickHash to generate and compare checksums of the original and copied folders. Save the first CSV file as “[accession#/unique id]_originalchecksums.csv.” It does not matter what you name the hash file as you can delete it once you have finished comparing files. Name the second CSV file “[accession#/unique id]_checksumcomparison.csv.” Save both CSV files in the “[accession#]_documentation” folder.

   If there are any checksum mismatches, try to retransfer all the files in the **No** list. You can use the QuickHash **File** tab to generate checksums for individual files to verify that files match. Once you have fixed all the problem files, go back to step c and rerun the checksum and regenerate the spreadsheet or you can edit the existing spreadsheet, making sure to revise the checksum and **KnownHashFlag** column.

Robocopy parameters

The following is an explanation of the Robocopy parameters we use for transferring files. The order does not matter.

/copy:DAT - Specifies file properties to be copied. D=Data, A=Attributes, T=Timestamp. (The full version is DATSOU but I couldn't get it to transfer with SOU. S=Security=NTFS ACLs, O=Owner info, U=aUditing info)

/z - Enables partial file transfers to resume. May want to exclude to speed up transfers, but recommended for large a/v and image transfers that won't complete in a single transfer session.

/r:[#] - Number of attempts to copy a file.

/w:[#] - Wait time between tries in seconds.

/e - Copies all subfolders, including empty folders. (Copying empty folders makes comparisons easier when verifying transfers. If you do not want to copy empty folders, substitute "/e" with "/s.")

/v – Displays log in command prompt. May want to turn off to speed up process but highly recommend using to catch mistakes in syntax and any other errors. If this is turned off, make sure to use "/log".

/log – Prints log to file. Info is not very helpful, particularly when transferring over multiple sessions. If you choose to generate a log you do not need to save it in the documentation folder.

/MT:[#] – Enables multi-threading downloads (downloading parts of multiple files at the same time). Do not use this when you are actively using the computer, but you might be able to get away with using "2" for light computer tasks (i.e. Word and emails).

/XD [filepath of folder to exclude] – Excludes specified folder from transfer.

/XF [filepath of file to exclude] – Excludes specified file from transfer.

[File name] – You can include the file name in the Robocopy syntax if you would like to transfer a specific file. Use wildcards (*) to transfer based on keywords or extensions. You can add as many file names as needed.

[keyword] - transfer all files with file names that contain your keyword

[keyword]* - transfer all files with file names that begin with your keyword

*.[extension] – transfer all files with file names containing the specified extension.

Example for transferring files with names containing "memo" and ".doc" or ".docx" as the extension.

```
robocopy "W:\NDamavandi" "J:\processing\Staff_harddrives\2021\Trust\inprogress
NDamavandi" *memo*.doc *memo*.docx /s /copy:DAT /z /r:2 /w:5 /v /e
```

There are many other options to further customize a Robocopy command. For more information see https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/robocopy or https://adamtheautomator.com/robocopy-the-ultimate/.

N. QuickHash

No license is required.
https://www.quickhash-gui.org/downloads/

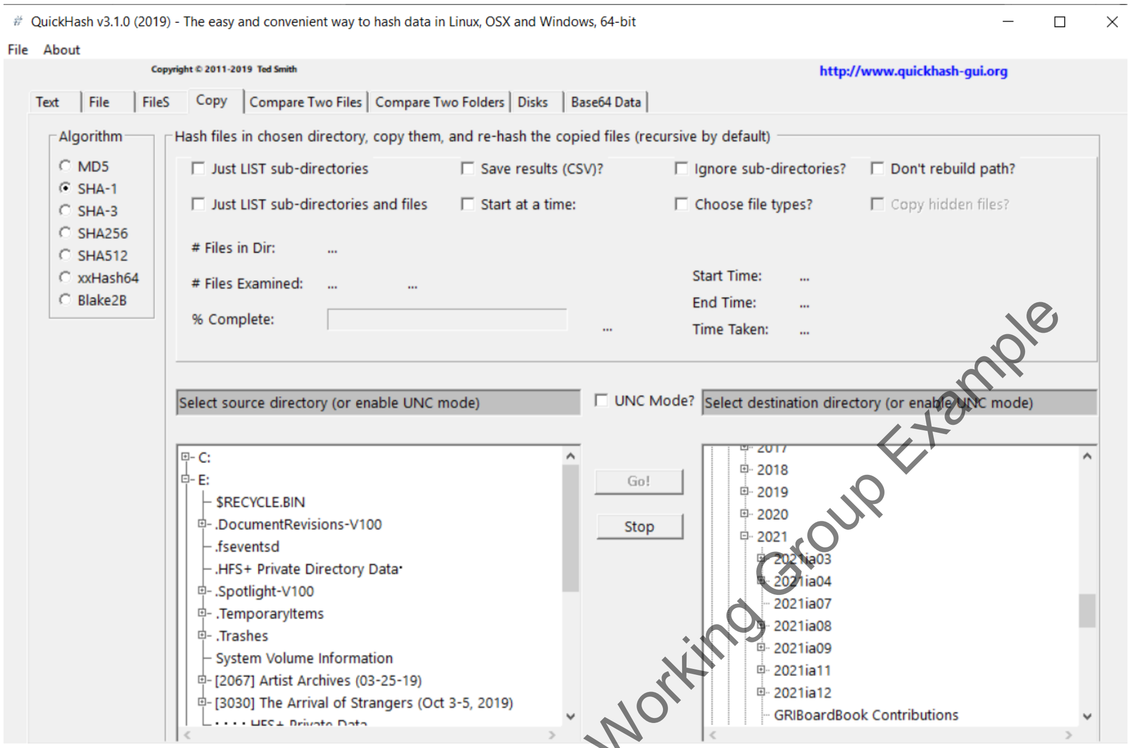
Overview

QuickHash is an open-source software that we use to transfer files and to generate and verify checksums. It is able to transfer files with file paths that exceed character limits, although this does depend on the filesystem of the source and destination drive.

Transfer files

Use the **Copy** function to copy files from one location to another. As part of the transfer process, QuickHash will generate and compare checksums for the original and new files. It will also generate an error log if there are any transfer problems.

1. Click on the **Copy** tab.
2. On the left-hand side, select the folder to be transferred. On the right, select the save location. Check off **Save results (CSV)** and select **SHA-**1. Do not check off **Don’t rebuild path** as files will save without any folder structure. Click **GO** when you’re ready to transfer.



QuickHash v3.1.0 (2019) - The easy and convenient way to hash data in Linux, OSX and Windows, 64-bit

File About

Copyright © 2011-2019 Ted Smith http://www.quickhash-gui.org

Text | File | FileS | Copy | Compare Two Files | Compare Two Folders | Disks | Base64 Data

Algorithm
○ MD5
● SHA-1
○ SHA-3
○ SHA256
○ SHA512
○ xxHash64
○ Blake2B

Hash files in chosen directory, copy them, and re-hash the copied files (recursive by default)

□ Just LIST sub-directories □ Save results (CSV)? □ Ignore sub-directories? □ Don't rebuild path?

□ Just LIST sub-directories and files □ Start at a time: □ Choose file types? □ Copy hidden files?

Files in Dir: ...

Files Examined: ... ...

% Complete: ...

Start Time: ...

End Time: ...

Time Taken: ...

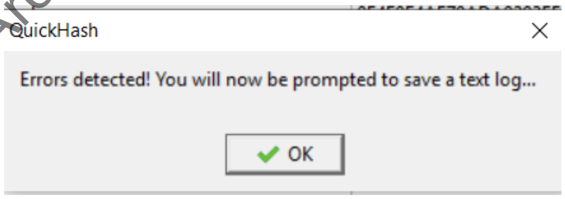
Select source directory (or enable UNC mode) □ UNC Mode? Select destination directory (or enable UNC mode)

```
C:
E:
  $RECYCLE.BIN
  .DocumentRevisions-V100
  .fseventsd
  .HFS+ Private Directory Data
  .Spotlight-V100
  .TemporaryItems
  .Trashes
  System Volume Information
  [2067] Artist Archives (03-25-19)
  [3030] The Arrival of Strangers (Oct 3-5, 2019)
  HFS+ Private Data
```

```
2017
2018
2019
2020
2021
  2021ia03
  2021ia04
  2021ia07
  2021ia08
  2021ia09
  2021ia11
  2021ia12
  GRIBoardBook Contributions
```

3. Once the transfer has completed it will ask you to select a location and file name for the transfer results. Save the transfer log to [accession#_documentation] folder on ira_locked and name the file "[accession#/unique identifier]_QHtransferresults.csv".

   If there were any errors, you will see an error message and you will be prompted to save the error log. Save error log to [accession#_documentation] folder on ira_locked and name the file "[accession#/unique identifier]_QHerrorlog.csv".



QuickHash

Errors detected! You will now be prompted to save a text log...

   If there are only a few errors, you can try to manually copy over the missing/corrupt files and use the Compare Two Files function to verify the checksums. Make sure to document this work in ASpace.

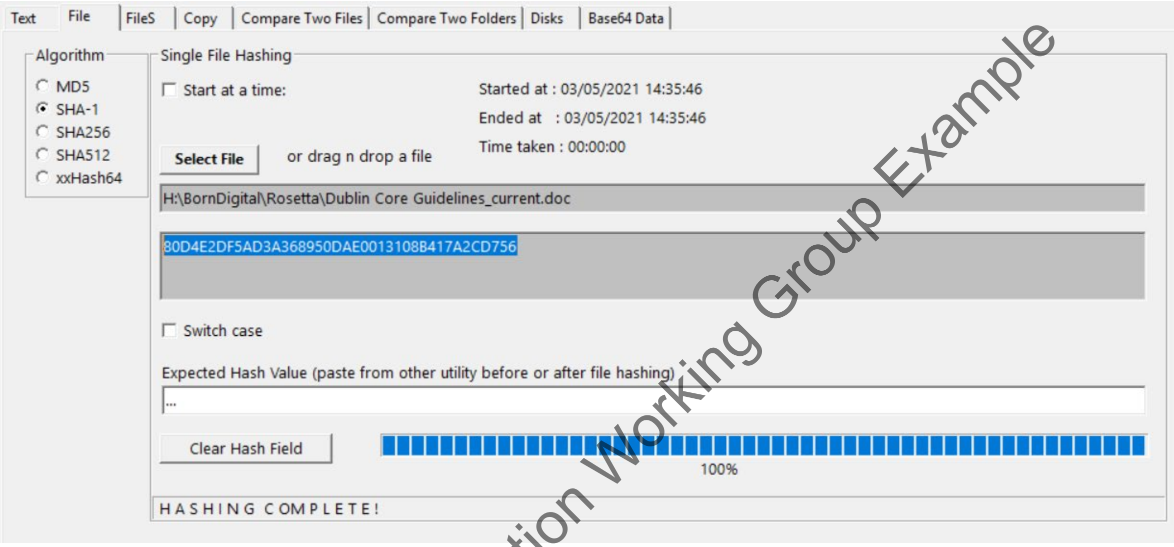
   If a lot of files are missing or are corrupt, depending on the cause of these issues and whether they can be addressed, you may want to rerun QuickHash or use another tool.

Generate checksums

You can use QuickHash to generate a checksum for a single file, all the files within a folder and its subfolders, or only certain file formats. QuickHash also offers the option to compare files against existing checksums. See **Compare checksums** section for guidance on that feature.

Generate checksum for a file

1. Click the **File** tab.
2. Select checksum algorithm. We usually use SHA-1 or MD5.
3. Drag and drop file to be hashed or click **Select File** and navigate to file**.** QuickHash will automatically analyze the file.



Algorithm
○ MD5
● SHA-1
○ SHA256
○ SHA512
○ xxHash64

Single File Hashing

□ Start at a time:

Started at : 03/05/2021 14:35:46
Ended at : 03/05/2021 14:35:46
Time taken : 00:00:00

H:\BornDigital\Rosetta\Dublin Core Guidelines_current.doc

80D4E2DF5AD3A368950DAE0013108B417A2CD756

□ Switch case

Expected Hash Value (paste from other utility before or after file hashing)

...

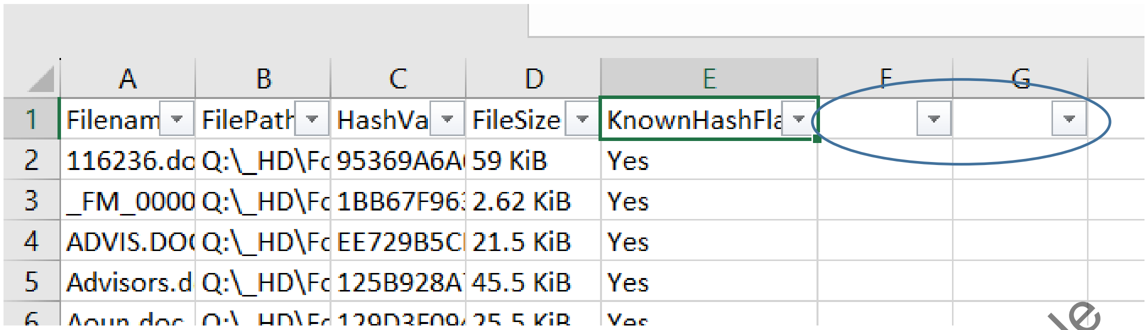
100%

HASHING COMPLETE!

Generate checksum for folder

1. Click the **FileS** tab.
2. Select SHA-1 for the checksum algorithm. If comparing against an existing list of checksums, select the same algorithm used to create that list.
3. Click on **Select Folder** and navigate to location of folder to be hashed.
4. Once QuickHash has finished generating the list of checksums, make sure the percentage complete is 100% and the number of files analyzed matches the number of files in the folder. Sometimes QuickHash may end unexpectedly due to network connection issues and will display a "Done" message when it is not. You will need to rerun the process. (If you decide to export the incomplete list of checksums, please note that the last generated checksum in the list will be inaccurate.)
5. If QuickHash did indeed finish generating checksums, save the results by right-clicking and selecting **Save to CSV file**. If you are dealing with hundreds of thousands of files or more, it may take a while for QuickHash to generate the CSV.

   If any of the folder or file names contain commas, data will not display in the correct columns in the CSV file. A quick way to determine if this is a problem is by using the filter function. If a drop-down menu appears for columns that should be empty, export the results as an html.



	A	B	C	D	E	F	G
1	Filenam	FilePath	HashVa	FileSize	KnownHashFla		
2	116236.do	Q:_HD\Fc	95369A6A	59 KiB	Yes		
3	_FM_0000	Q:_HD\Fc	1BB67F96	2.62 KiB	Yes		
4	ADVIS.DO(	Q:_HD\Fc	EE729B5C	21.5 KiB	Yes		
5	Advisors.d	Q:_HD\Fc	125B928A	45.5 KiB	Yes		
6	Aoun.doc	Q:_HD\Fc	129D3F09	25.5 KiB	Yes		

Copy and paste the data in the html into a new CSV file. The data should now be distributed in the correct columns.
If you are generating a manifest for an accession, name the file "[accession #]_manifest.csv" and save in "[accession #]_documentation" folder on ira_locked.

If you want to compare a second directory against this directory, right-click and select **Copy all hash values**. Paste into a new Excel workbook and save as a csv.

Note that QuickHash is unable to generate checksums for files with file path lengths that exceed the character limits. (See Appendix B. File Path Limits for more information.) If this applies to the files you are working with and you are generating a manifest for accessioning purposes, you will need to make a note of missing checksums in the accession record in the **Digital File Mgmt Notes** field

Compare checksums

You can use QuickHash to compare the checksums of two files or folders. File name differences are ignored.

Compare two files

1. Click on **Compare Two Files** tab.
2. Either paste the file paths for the two files in the fields or navigate to their locations.
3. Select the checksum algorithm by which to compare. It does not matter which you choose since we are simply trying to verify whether or not files match and are not logging the checksum results.

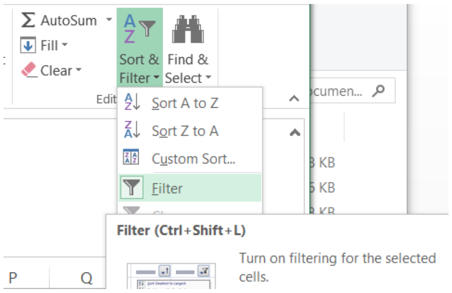
Compare two folders

To compare the checksums of two folders, use the **FileS** tab. You will generate checksums on the first folder and create a log which will be used for comparison when generating the checksums on the second folder. Do not use the **Compare Two Folders** tab as that method does not specify problematic files when there are mismatches.

Note that QuickHash comparisons are based on file count and checksums. Since it does not look at file names or folder structure, it is recommended that you first run a folder comparison check in BeyondCompare to determine if there are missing files.

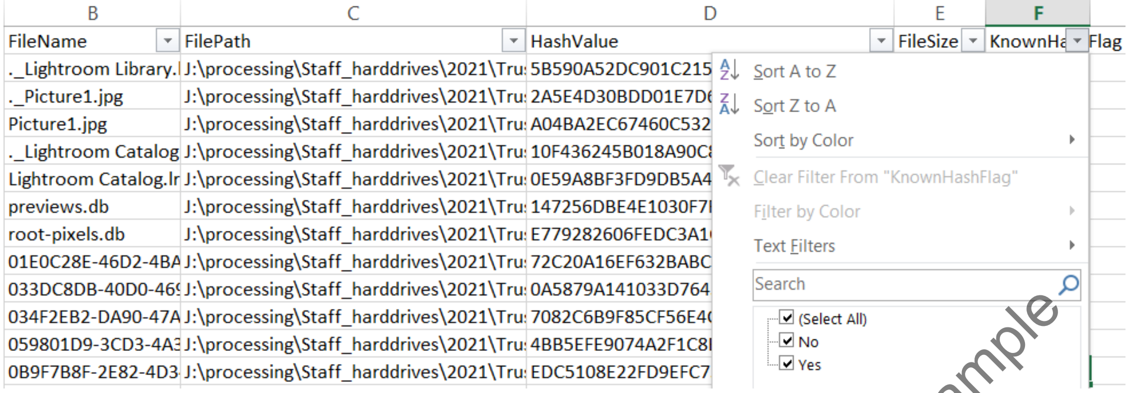
1. Click on the **FileS** tab.
2. Generate a list of checksums for the first folder if you do not already have a checksum log. See Generate checksums section for instructions. Right-click and select **Copy all hash values**. Paste into a new Excel workbook and save as a CSV. (Although the Quickhash instructions specify not to include a row header, a header is needed as the program will not recognize the checksum for the first cell.) The file name and save location does not matter.
3. Generate a list of checksums for the second folder.
    a. Under the **FileS** tab, click **Load HashList** and select the hash list that you just created.
    b. Select the same algorithm that you used to create the hash list.
    c. Click **Select Folder** and select the second folder for comparison. QuickHash should automatically begin calculating checksums and comparing them against the hash list.
4. When the process has finished, you should see a column on the far right indicating whether or not the checksum for a file matched a checksum in the hash list. Right-click the results pane and select **Filter out Hash list – No**. This will display only the files that were not properly transferred.

   To save the results, follow instructions in step 5 of Generate checksums section. (Make sure to check if there are commas in any of the folder or file names.) If you are generating a manifest for the documentation folder, name the file "[accession #]_manifest.csv" and save in "[accession #]_documentation" folder on ira_locked. You can use filter the results in the KnownHashFlag column in Excel if you would like to review the mismatches.



Filter (Ctrl+Shift+L)

Turn on filtering for the selected cells.



FileName	FilePath	HashValue	FileSize	KnownHa Flag
._Lightroom Library.l	J:\processing\Staff_harddrives\2021\Tru:	5B590A52DC901C215		
._Picture1.jpg	J:\processing\Staff_harddrives\2021\Tru:	2A5E4D30BDD01E7D6		
Picture1.jpg	J:\processing\Staff_harddrives\2021\Tru:	A04BA2EC67460C532		
._Lightroom Catalog	J:\processing\Staff_harddrives\2021\Tru:	10F436245B018A90C8		
Lightroom Catalog.lr	J:\processing\Staff_harddrives\2021\Tru:	0E59A8BF3FD9DB5A4		
previews.db	J:\processing\Staff_harddrives\2021\Tru:	147256DBE4E1030F7I		
root-pixels.db	J:\processing\Staff_harddrives\2021\Tru:	E779282606FEDC3A1		
01E0C28E-46D2-4BA	J:\processing\Staff_harddrives\2021\Tru:	72C20A16EF632BABC		
033DC8DB-40D0-469	J:\processing\Staff_harddrives\2021\Tru:	0A5879A141033D764		
034F2EB2-DA90-47A	J:\processing\Staff_harddrives\2021\Tru:	7082C6B9F85CF56E4		
059801D9-3CD3-4A3	J:\processing\Staff_harddrives\2021\Tru:	4BB5EFE9074A2F1C8I		
0B9F7B8F-2E82-4D3	J:\processing\Staff_harddrives\2021\Tru:	EDC5108E22FD9EFC7		

If there are any checksum mismatches, try to retransfer all the files in the **No** list. You can use the QuickHash **File** tab to generate checksums for individual files to verify that they match the checksums in the original CSV file. Once you have fixed all the problem files, go back to step c and rerun the checksum and regenerate the spreadsheet, or you can edit the existing comparison spreadsheet, making sure to revise the checksum and **KnownHashFlag** column.

APPENDIX A. UNIQUE IDENTIFIER

Assign a unique identifier if you need to track which files came from which piece of media. This is usually the case for floppy disks and optical discs. Discuss with head of Institutional Archives as unique identifiers may not always be necessary. Consider how you want to organize and describe files in the finding aid. If you need to distinguish transfers for administrative control within an accession but not within a finding aid, using descriptive folder names (i.e. topic, date, media, etc.) may be sufficient.

When assigning a unique identifier, follow the format that applies to your scenario. You may need to use a mix of identifier formats within a single accession. Make sure you do not duplicate identifiers used for other digital storage media or that have been assigned to analog materials for digitization. Name bags using the unique identifier. If retaining the media in the collection, label the item with the unique identifier or make a note on the folder if the folder only contains one piece of media.

Scenario	Unique Identifier
Accession consists entirely of a single disk, drive, or network drive transfer.	[accession #] Example: 2016ia38
Hybrid or digital accession that consists of multiple transfers from a network drive or computer.	1) Maintain each transfer separately and distinguish the transfers through bag names based on topic, transfer date, etc. (You may change bag

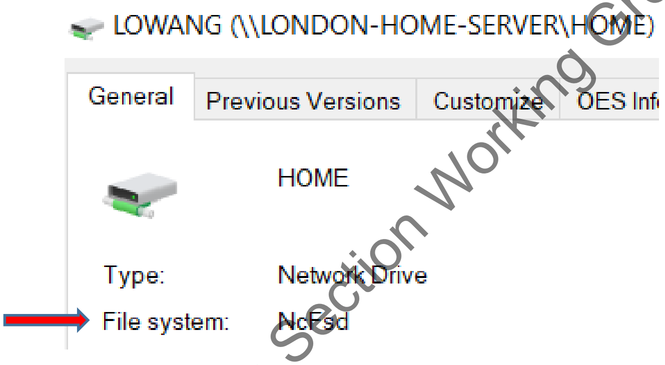
	names after a transfer without affecting Bagger validation checks.) [accession #]_[topic, transfer date, etc.] Example: 2016ia38_PressClippings Note: Make sure you do not duplicate identifiers if accession contains transfers from a local drive. *Or* 2) Combine files from multiple transfers into a single 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 #]_networkdrive [accession]_usbdrive Example: 2016ia38_networkdrive
Disk or 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** disks or drives 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 or drive is to be retained. *or* Disk or drive is not to be retained but the original physical context needs to be recorded.	[accession #]_b[box #]i[item #] Example: 2016ia38_b02i01 Note: Item numbering should restart from 01 with each box. Label the item with the unique identifier

	or make a note on the folder if the folder only contains one piece of media
Event recordings Note: This format follows the one used by GRI. Since this type of unique identifier is also assigned to analog materials that have been digitized make sure you do not duplicate identifiers.	gia_[accession # with underscores]_[item number] Example: gia_2016_ia_48_01 Note: Include box number if appropriate. Also indicate if a recording is on more than one tape or disc. Example: gia_2018_ia_32_b03i04 gia_2018_ia_32_b03i05_1of2 gia_2018_ia_32_b03i05_2of2

Appendix B. File Path Limits

Overview

When a file has a file path that exceeds the maximum character limit, you cannot edit, copy, or move the file. Most software will also have trouble recognizing the file. For example, Karen's Directory and QuickHash will not be able to generate checksums for such files. The character limit depends on the file system of the network drive. For ira_locked and wbench1, which are on the same server, the file system is NTFS and the limit is 259. For the GRI shared drive and the individual network drive the file system is NcFSD and the limit is 232. Note that these numbers may vary depending on your computer settings and version of Microsoft Windows. To determine the file system of a drive, right-click the drive letter in file explorer and click **Properties**.



LOWANG (\\LONDON-HOME-SERVER\HOME)

HOME

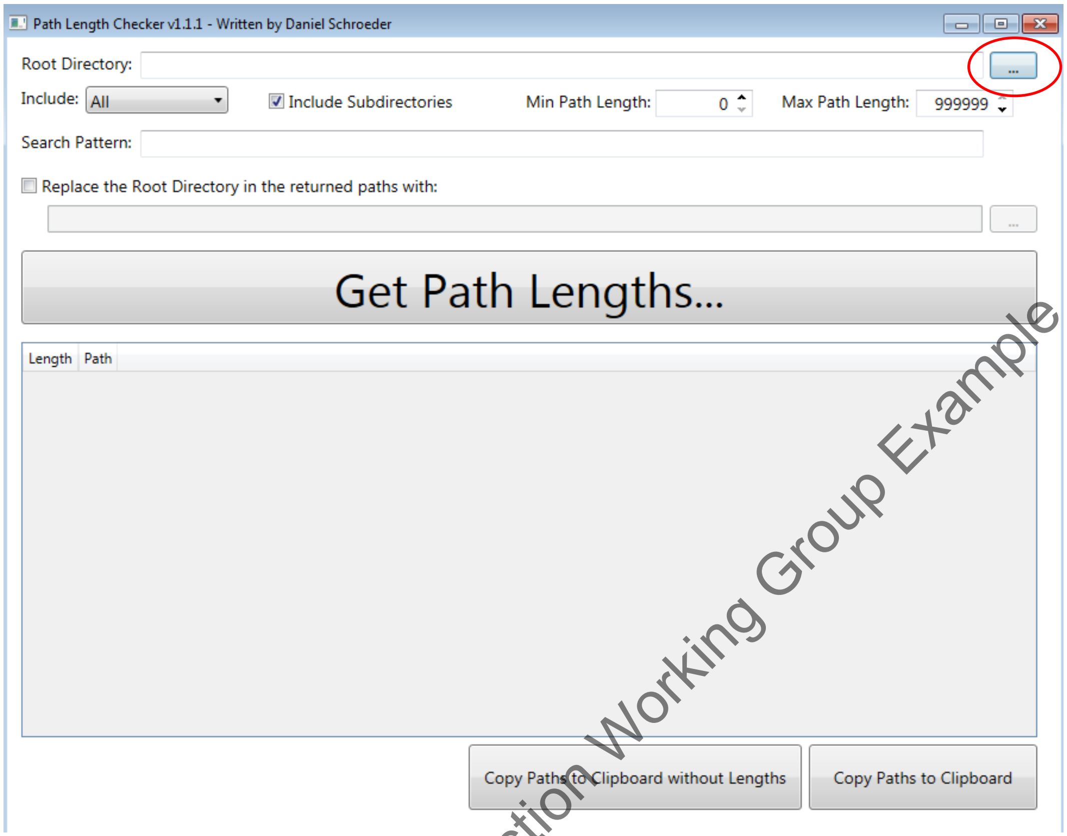
Type: Network Drive

File system: NcFsd

Check file path lengths

Use the Path Length Checker tool to obtain the character count of a file's name and file path and to identify all files that exceed the character limit.
G:\Institutional Archives\ENGINEERING\ENG-120 Software_Hardware\BornDigitalToolsInstallation_files

1. Double-click PathLengthCheckerGUI.exe to open.
2. Click the gray box at the top far right to select your directory. Depending on your location, enter 259 or 232 in Min Path Length. Leave Max Path Length as is. Check off **Replace the Root Directory** if you want to determine how the character counts will change if you move files to a new location.



Path Length Checker v1.1.1 - Written by Daniel Schroeder

Root Directory:

Include: All

☑ Include Subdirectories

Min Path Length: 0

Max Path Length: 999999

Search Pattern:

☐ Replace the Root Directory in the returned paths with:

3. Click **Get Path Lengths**, and file paths that fall between the minimum and maximum path lengths will be listed along with their character count. You can click on the column labels to sort the results.

Working with long file path lengths

There are four options for dealing with files that have file paths that exceed character limits. The method you choose depends on whether you are at the acquisition or processing stage. During acquisition, if possible, avoid permanently editing file and folder names and folder structures. During the processing stage, file paths must fall under 262 characters for deposit in Rosetta, which will necessitate making permanent folder/file name changes.

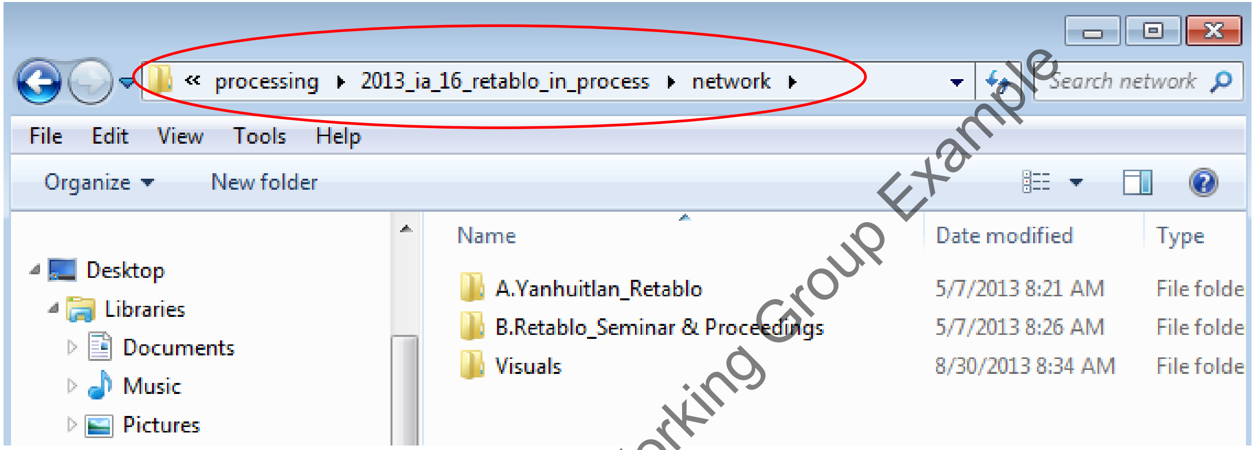
1. Map drive letter to folder
2. Move folder
3. Change folder/file names
4. Create a forensic image

Map drive letter to folder

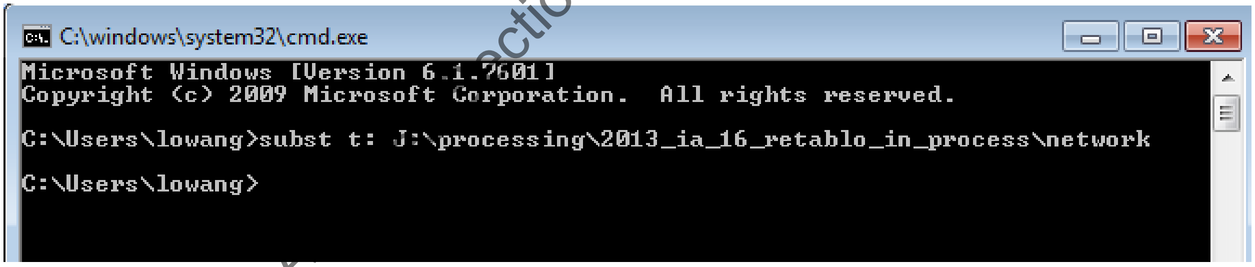
You can try to circumvent character limits by associating a drive letter with part of the file path, thereby shortening the file path. Unfortunately, this does not bypass character limits on NcFsd file systems. *Before proceeding, use Path Length Checker to verify that this method will solve your file path length issue. Check off **Replace the root directory** box and leave field blank.*

1. Type “cmd “in the Windows search box. Command Prompt will open.
2. Type: “subst [unused drive letter]: [file path of folder that you want to map to]”.
   Note: Depending on your version of Windows you can either use right-click in file explorer to copy address as text and paste the file path in Command Prompt or use Ctrl+C to copy and Ctrl+V to paste.

   Example:

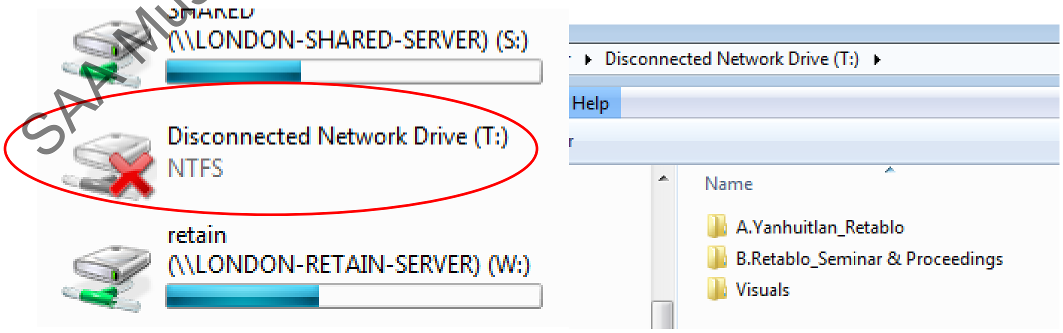

« processing ▸ 2013_ia_16_retablo_in_process ▸ network ▸
Search network
File Edit View Tools Help
Organize ▾ New folder
Desktop
Libraries
Documents
Music
Pictures

Name	Date modified	Type
A.Yanhuitlan_Retablo	5/7/2013 8:21 AM	File folde
B.Retablo_Seminar & Proceedings	5/7/2013 8:26 AM	File folde
Visuals	8/30/2013 8:34 AM	File folde

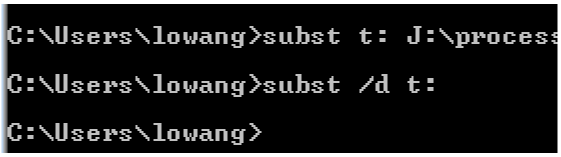


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\lowang>subst t: J:\processing\2013_ia_16_retablo_in_process\network

C:\Users\lowang>
```

3. The new network drive will appear in file explorer containing your files. You should now be able to move, rename, or delete files.


SHARED
(\\LONDON-SHARED-SERVER) (S:)
Disconnected Network Drive (T:)
NTFS
retain
(\\LONDON-RETAIN-SERVER) (W:)
▸ Disconnected Network Drive (T:) ▸
Help
Name
A.Yanhuitlan_Retablo
B.Retablo_Seminar & Proceedings
Visuals

4. When done, type “subst /d [drive letter to be removed]” to remove the drive.



```
C:\Users\lowang>subst t: J:\process
C:\Users\lowang>subst /d t:
C:\Users\lowang>
```

Move folder

Temporarily move the folder with the problem file(s) up in the file path so the character count falls within the character limit. It's important that you note the original location so you can move the folder back when you're done. (If you feel the folder is nested unnecessarily within other folders, you may choose to move the folder permanently and delete the unnecessary folders. Use your best judgement.)

Determine which folder to move. Look at your Path Length Checker results and answer the following questions: By how many characters does the longest file path exceed the limit? Where are the problem files located? You want to try to move as few folders as possible.

When the problem files are spread out in multiple folders, if possible, move a broader folder that contains all of those folders. Try to move as few folders as possible. If problem files are located in a single folder, you can move that folder or any of the parent folders. Whichever folder you choose to move, remember the original location. Choose the strategy that is easiest for you to keep track of which folder you've moved and its original location.

If the move has resolved the file path length issue, you should be able to move, delete, or edit the problem file as needed or generate checksums. When you are done, move the folder back to its original location.

Change folder or file name

Shorten folder names so file paths fall within the character limit. Record original names so you can change them back after you're done working with the problem files. During the initial transfer (accessioning stage), ideally any name changes should be a temporary measure. When processing files for Rosetta, folder/file names may need to be permanent as file paths must be under 262 characters for the deposit.

Determine which folder or folders to rename. Look at your Path Length Checker results and answer the following questions: By how many characters does the longest file path exceed the limit? Where are the problem files located?

Try to change folder names from top to down the hierarchy. When the problem files are spread out in multiple folders, it may be easiest to shorten the topmost folder.

If name changes are permanent, make sure to log folder and file name changes. See RosettaIngestPrep.pdf (G:\Institutional Archives\ADMINISTRATION\ADM-135 Policies Procedures Adm\Archives_Policies_procedures_manuals\Manuals_Current\BornDigital) for how to log file name changes so they can be integrated within the METS file when deposited in Rosetta. While we cannot integrate folder name changes into the METS file, we will keep a record of changes in the "[accession #]_documentation" folder. Track folder name changes in a separate spreadsheet. Enter the original full path with the original folder name in the first column and enter the full path with the changed folder name in the second column. Name the spreadsheet "[accession #]_renamedfolders.csv. You may use Renamer to change file or folder names or do so manually. (See RosettaIngestPrep.pdf for instructions on using Renamer.)

Create a forensic image

Create an E01 image using FTK Imager to bypass file path limits. This is the last resort option when trying to accession files from internal and external hard drives. Use this option when you are short on time and do not have time to experiment with the other methods.

Once you have created an image of the drive, use Forensic Toolkit to export files from the image. You will have the option of checking off **Limit path length**, which 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 folders or problem files and move the files back to their original location.