

1.44MB 3.5" FLOPPY DISK IMAGING MANUAL

Digital Preservation Unit

Department of Preservation and Conservation | University of Michigan Library

Updated by: Andrea Kang • Christina Min

Authors: Kayla Carucci • Leigh Gialanella • Alexa Hagen • Noa Kasman

Andrea Kang • Christina Min

Public Version 2.0

Last Revised | 23 August 2018

THE WORKFLOW

Part I: Preparation

1. Create Tracking Database
2. Prepare Main Directories
3. Prepare Media Directory
4. Photograph Media

Part II: Disk Imaging

5. Configure Hardware for Disk Imaging
6. Create Disk Image and Generate Checksums

Part III: Brunnhilde

7. Oracle VM Virtualbox
8. Run Brunnhilde
9. Reports

Part IV: Bagging and Transfer to Storage

10. Package SIP using BagIt
11. Validate bag
12. Transfer to Network Attached Storage (NAS)

PART I: PREPARATION

[STEP 1] Create Tracking Database

Create a working database on Google Sheets. This sheet will help keep track of the floppy disks that have been imaged and their results.

If the content is coming from Special Collections Research Center (SCRC), add another sheet to the Preservation Imaging and Logical Transfer Inventory found [here](#). Content from SCRC should come with a finding aid. Incorporate any information you find necessary from the finding aid into the working database.

Input the following information into the working database:

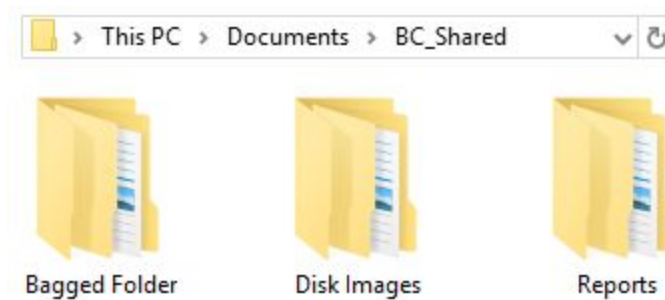
- ▶ Last handled: date the media/media image was last handled
- ▶ Collection: John Sayles
- ▶ Unique ID: copy from the inventory spreadsheet
- ▶ Barcode: barcode of media
- ▶ Label: label on the media
- ▶ Type: type of media
- ▶ Imaging Results: drop down
- ▶ Bad Sectors: note any bad sectors from the imaging results
- ▶ Mount Results: drop down (based on Brunnhilde results)
- ▶ Virus Check Results: drop down (based on Brunnhilde results)
- ▶ Bag Check: write “Y” or “N” for whether package was bagged or not
- ▶ Reports Created: “Y” or “N” for whether reports directory for SCRC and the Digital Preservation Librarian have been copied from the *metadata* folder
- ▶ Transfer Check: write “Y” or “N” for whether bag was transferred or not to DeepBlue
- ▶ Notes: any information regarding the disk (e.g. bent slider) or tools (e.g. Brunnhilde froze)

Reconcile the finding aid with items sent to Buhr and notify the Digital Preservation Librarian of any discrepancies. Barcode and physically inspect all media, examining disks for mold and/or physical damage.

- ▶ Mold on disks looks like spilled milk and smells of mildew. This will be difficult to tell on 3.5” since it is inside a thick plastic jacket with a metal slider. If you suspect mold is present, isolate those disks and notify the Digital Preservation Librarian.
- ▶ Record any damages (e.g. bent plastic jacket) of the media on the working database
- ▶ If the media has a storage case or container, the media item and storage case or container should be given the same barcode and added to the working database.

[STEP 2] Prepare Main Directories

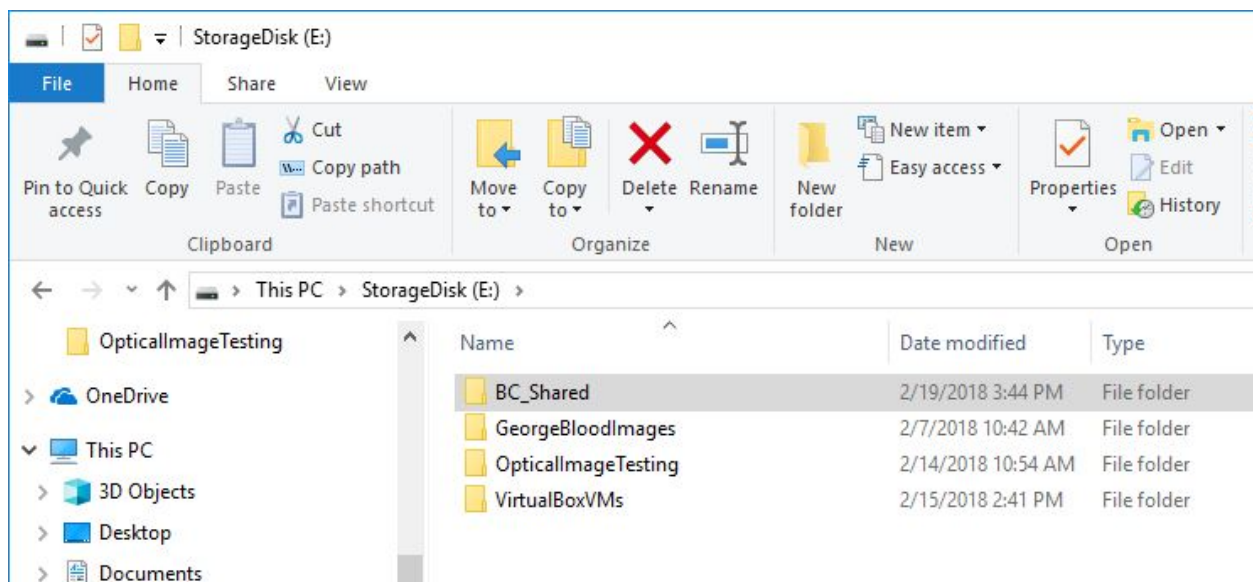
- ▶ Prepare three directories named *Disk Images*, *Reports*, and *Bagged* in the *BC_Shared* folder, which is the folder shared by the BitCurator Virtual Machine (BC VM) and the host computer. It is *BC_Shared* on the host computer and *sf_BC_Shared* on the BC VM.



- These directories distinguish the folder you generate when you create a disk image, the final bagged folder created through Bagger, and the reports that will be sent off to Special Collections and the Digital Preservation Librarian.



- The *sf_BC_Shared* folder can be found on Darth's StorageDisk (E:) or Ms. Pacman's Document folder on the host computer (image below). It is on the BC desktop on the VM (image above).



[STEP 3] Prepare Media Directory

- Create a new folder inside the *Disk Images* folder for each physical disk. Use the barcode scanner to scan the barcode number on the media as the file name.



39015058747869

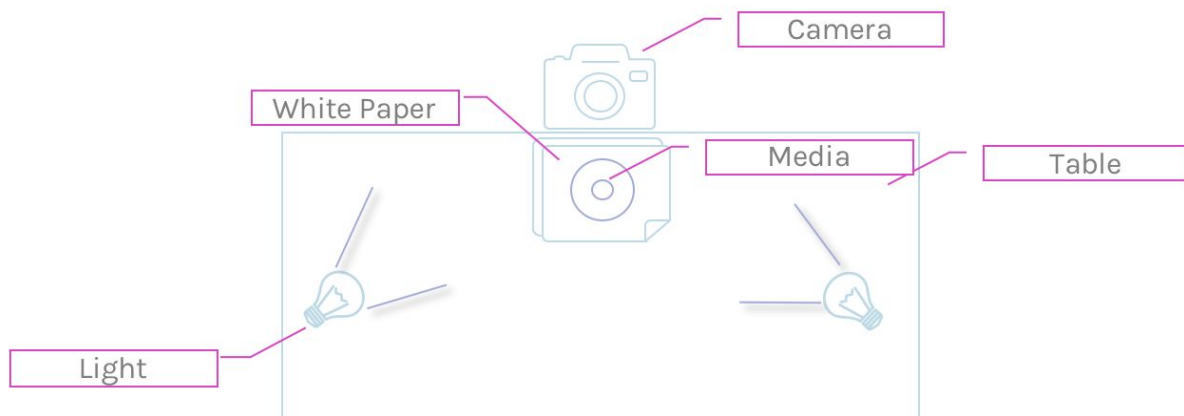
- ▶ Within that new folder, create a new folder called *image*. Other folders will be generated using tools on the BC VM.



image

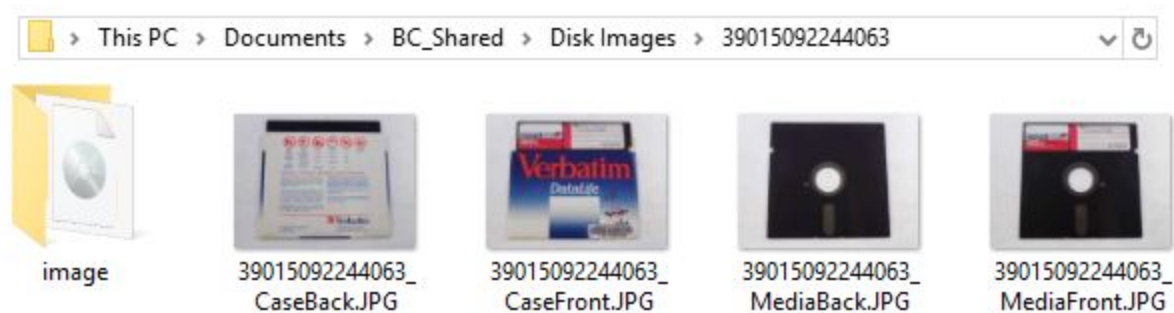
[STEP 4] Photograph Media

- ▶ Next, set up your photographing station by placing a white piece of paper under the cloth to make the backdrop as white as possible.
 - ▷ Make sure to put the paper as close to edge of the table as possible.
 - ▷ If there is lint or other debris on the white backdrop, use tape to make it as clean as possible.
 - ▷ An iron is available for removing wrinkles. Keep it on the synthetic setting and use towels to protect the material from full heat.
- ▶ Place the media you are photographing about an inch or two away from the edge of the table.
- ▶ Point the lights at a 45 degree angle towards the media, but not so directly that the reflection of the light is too strong.
 - ▷ You can also adjust the strength of the lights by pulling them closer to or further away from the source.
 - ▷ The dimmer switch in the room can also be used for lighting purposes.



- ▶ Attach the camera to the tripod and angle the camera lens so that it can capture a flat image of the media.
 - ▷ You may not be able to get it completely flat without photographing outside of the white backdrop. Get it as flat as possible.
- ▶ Zoom into the media to ensure that there is only the white backdrop in the background.
- ▶ Photograph the front and back sides of the media.
 - ▷ If applicable, photograph the front and back sides of the storage case for the media. This is especially important if the case contains relevant writing or a barcode. You do not need to take a photo of the case if you gave it a new storage case during inventory.
 - ▷ Take 3 sets of photos (resulting in a total of 6 photos per media, not including the media case) that are set to different exposures.
 - Turn the camera on.
 - Click the button with the +/- signs that is situated on the right hand side of the camera.
 - Take photos of the front and back of the media at exposures 0.0, +0.3, and +0.7.
- ▶ When finished, connect the camera to the computer using the USB cable.
- ▶ Select the photos with the most similar lighting of the highest quality and move them to the appropriate barcode folder. Once the photos have been moved, delete all the photos on the camera and unmount.

- ▶ Rename the photos with the barcode, underscore, and description of the image.
 - ▷ Some descriptions you can use are:
 - MediaFront
 - MediaBack
 - CaseFront
 - CaseBack
 - Notes01
 - ▷ It is helpful to type the description in first and then scan the barcode in at the beginning of the text.



- ▶ Photos will be dragged into the metadata folder that Brunnhilde generates in [\[Step 8\]](#).

PART II: Disk Imaging

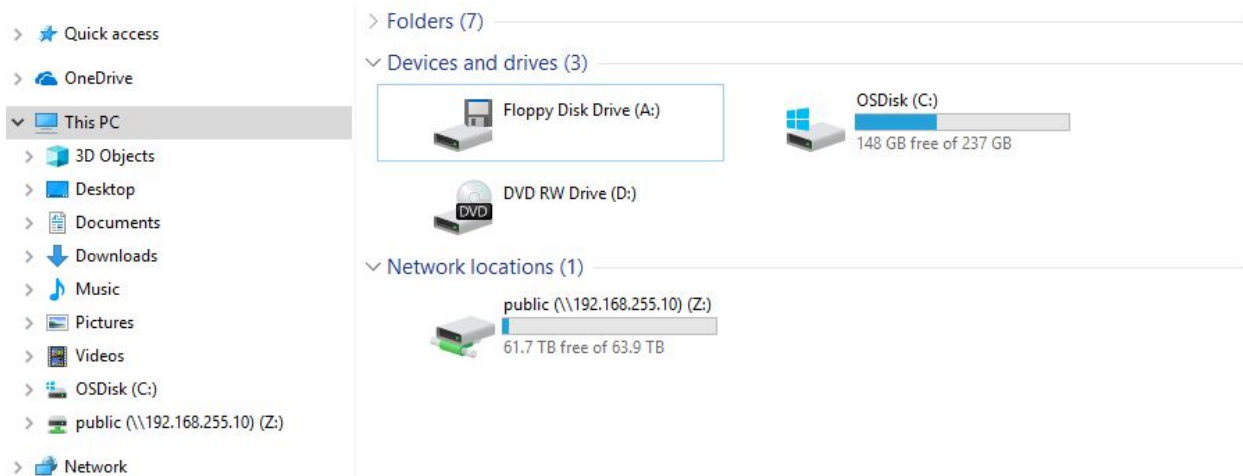
[STEP 5] Configure Hardware for Disk Imaging

FLOPPY DISKS

- ▶ Select the appropriate external floppy drive for the media you wish to image.
- ▶ Connect directly to the computer USB input
- ▶ Switch the floppy disk write-block tab to the correct position.
 - ▷ It may be helpful to do this step before photographing the media.



- ▶ Insert media into the external disk drive.
 - ▷ If the disk does not appear in the left navigation bar, click on “This PC” in File explorer and look for “Devices and Drives” at the top left of the screen. Click your device.



- ▷ If none of these work, eject the floppy disk from the external disk drive.
- ▶ Floppy disks can be difficult to read by new external floppy drives and it may take multiple attempts at inserting and ejecting the disk for the drive to read it.
- ▶ If after multiple attempts, the disk is not detected, you can try a different external drive if available, otherwise the disk may be unreadable.
 - ▷ Set unreadable disks aside for examination by the Digital Preservation Librarian.
 - ▷ Record this in the spreadsheet.

[STEP 6] Create Disk Image and Generate Checksums

STARTING FTK IMAGER

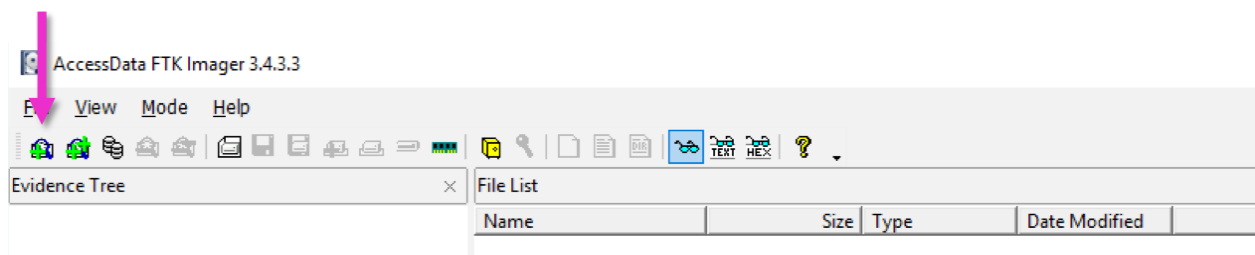
- ▶ Open FTK Imager on the host computer desktop.



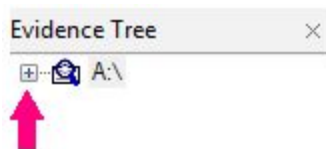
- ▶ It may prompt you to enter the username and password or ask permission to start the program. Enter in the information and FTK Imager will open.

GETTING THE EVIDENCE NUMBER

- ▶ Once FTK Imager is open, click on the “Add Evidence Item” icon below.



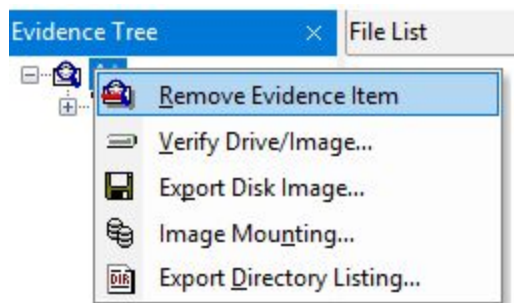
- ▶ In the “Select Source” dialogue box, select “Logical Drive” and click “Next”.
- ▶ In the next “Select Drive” dialogue box, select “A:\” and click “Finish” at the bottom.
- ▶ The dialogue box should have closed out and added the drive underneath the “Evidence Tree”. Expand the tree using the + sign to the left of the ISO file until you get to the file level.



- ▶ Write down the name that appears without “[HFS]”. This will later be entered into the “Evidence Number” field during imaging.

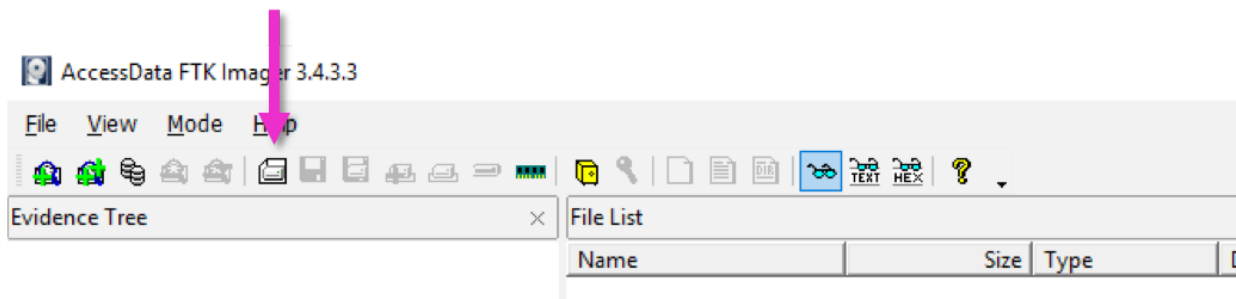


- ▶ Right click the “A:\” drive and click “Remove Evidence Item”.

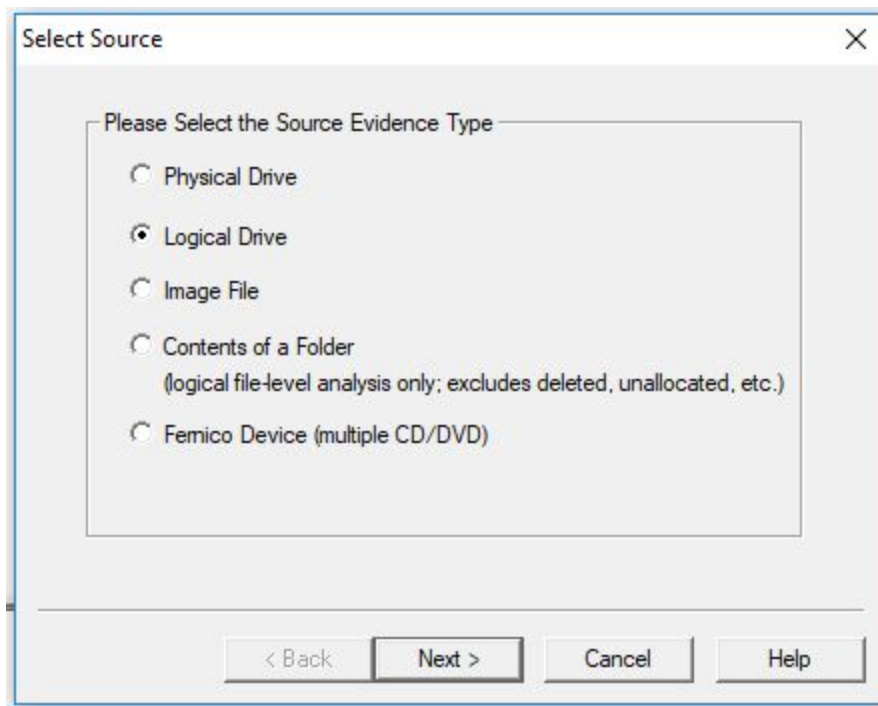


CREATE DISK IMAGE

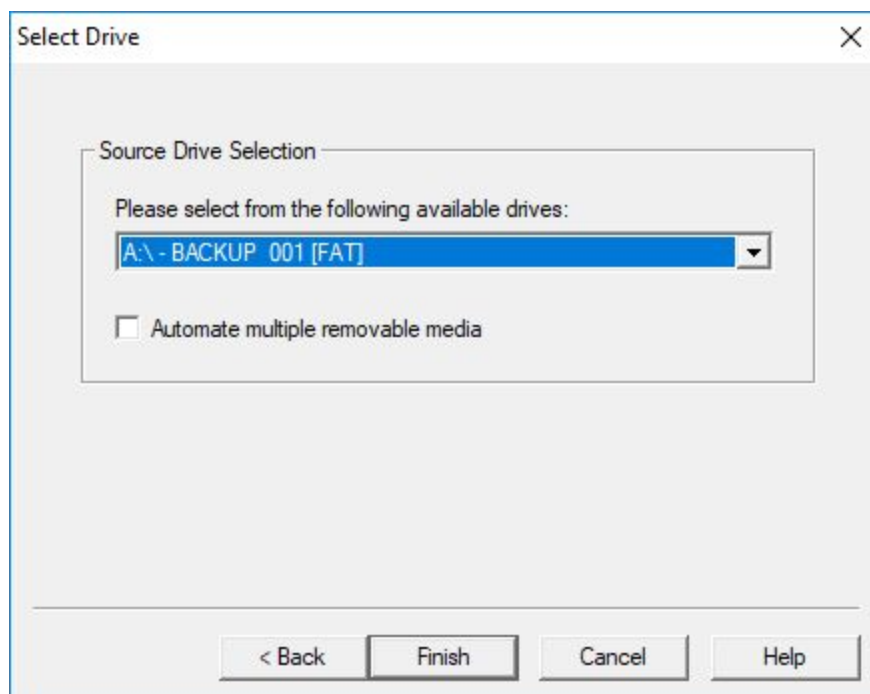
- ▶ To start imaging, click the “Create Disk Image” icon (see picture below).



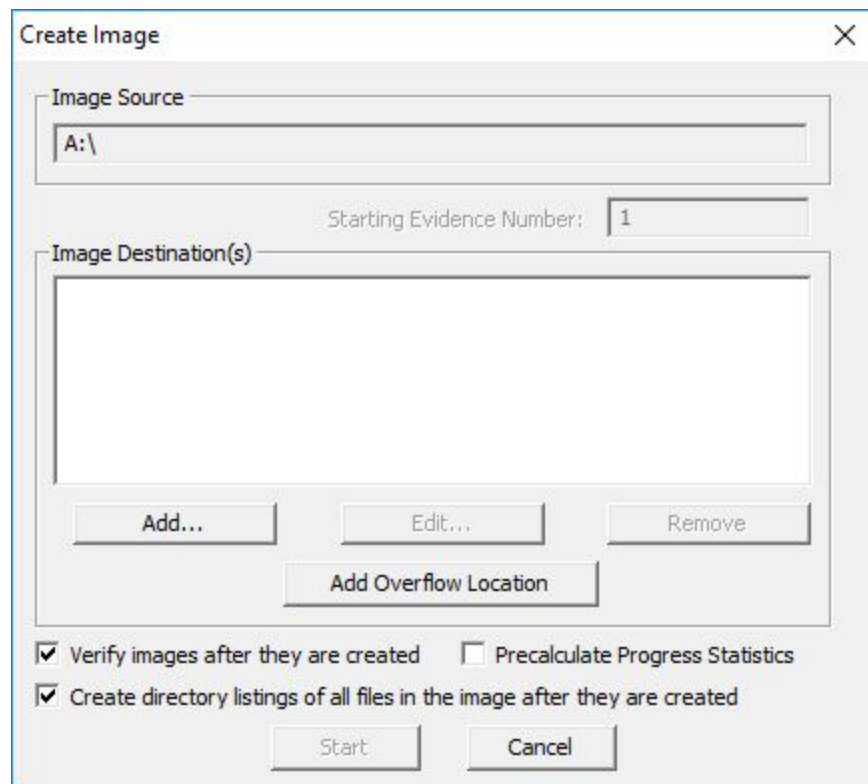
- ▶ A dialogue box will prompt you to select a source. Select “Logical Drive” and click “Next”.

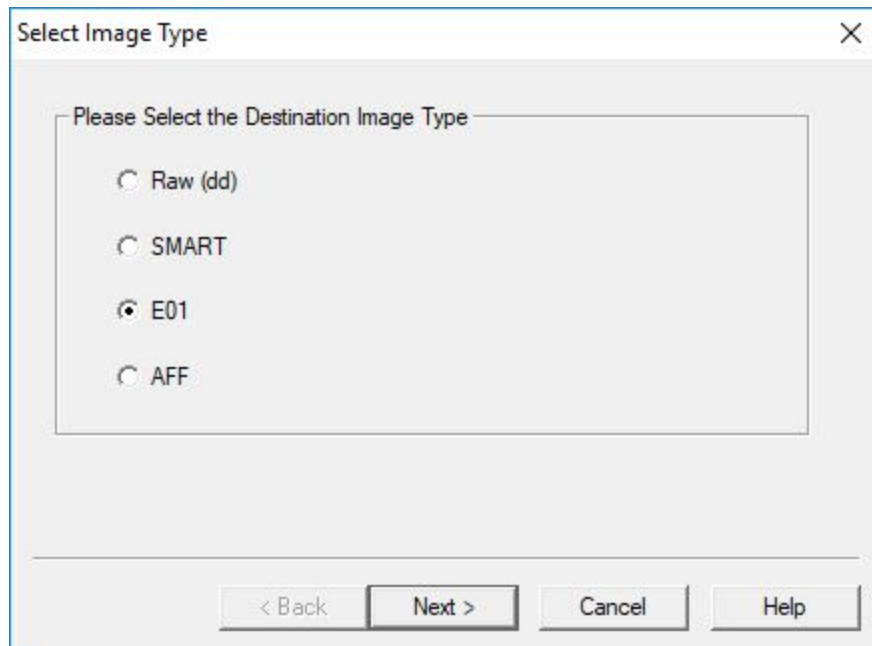


- ▶ You will then be prompted to select the source drive. The drive you want to select is "A:\ - BACKUP 001 [FAT]".



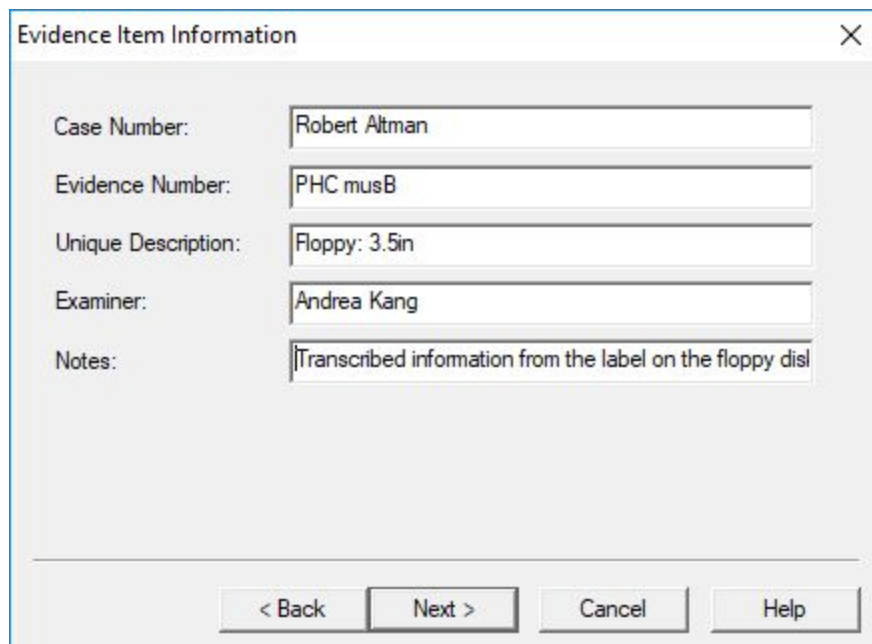
- ▶ Another dialogue box will pop up that says “Create Image”. The “Image Source” should automatically be set to the A:\ drive.
- ▶ Click “Add” under the “Image Destination(s)” and this will allow you to select the type of image you want.
 - ▷ For 3.5” floppy disks, you will always want an E01 image file.





A dialog box titled "Select Image Type" with a close button (X) in the top right corner. Inside the dialog, there is a section titled "Please Select the Destination Image Type" containing four radio button options: "Raw (dd)", "SMART", "E01" (which is selected), and "AFF". At the bottom of the dialog, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

- ▶ When you click "Next", the "Evidence Item Information" dialogue box will appear.



A dialog box titled "Evidence Item Information" with a close button (X) in the top right corner. It contains five text input fields with labels to their left: "Case Number:" (containing "Robert Altman"), "Evidence Number:" (containing "PHC musB"), "Unique Description:" (containing "Floppy: 3.5in"), "Examiner:" (containing "Andrea Kang"), and "Notes:" (containing "Transcribed information from the label on the floppy disl"). At the bottom of the dialog, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

- ▶ The Evidence Item Information is as follows:
 - ▷ Case Number: collection the item is from (i.e. Robert Altman, John Sayles, etc.)
 - ▷ Evidence Number: name from [“Getting the Evidence Number”](#)
 - ▷ Unique Description: Floppy: 3.5in
 - ▷ Examiner: your name
 - ▷ Notes: Transcribed information from the label on the floppy disk: “[insert floppy disk label text here]”.
 - Note any changes you have made to the label at the end of the transcription. For example: “Note: The semicolons were added by the examiner for clarity.”
- ▶ After clicking “Next”, select the image destination. Select the *image* folder you created earlier in [\[STEP 3\]](#).
- ▶ Scan in the barcode in the “Image Filename (Excluding Extension)” field.

Select Image Destination

Image Destination Folder
E:\BC_Shared\Disk Images\39015092239758\image Browse

Image Filename (Excluding Extension)
39015092239758

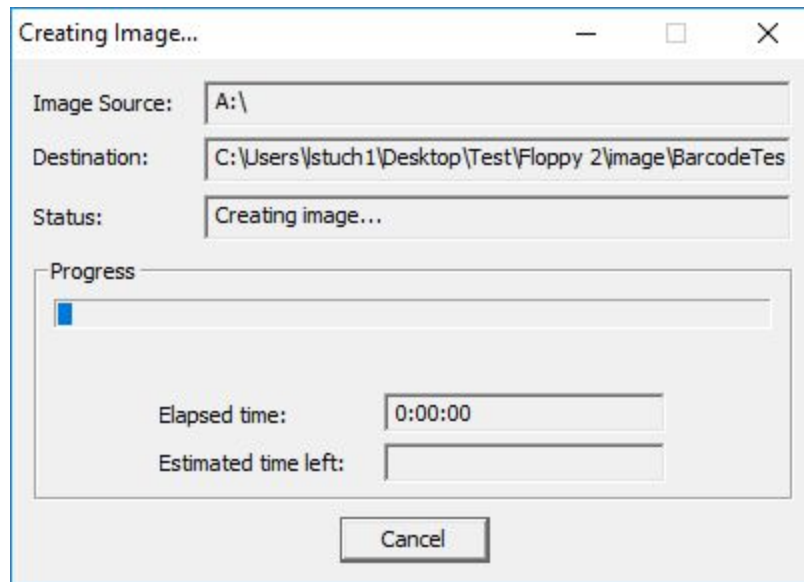
Image Fragment Size (MB) 1500
For Raw, E01, and AFF formats: 0 = do not fragment

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

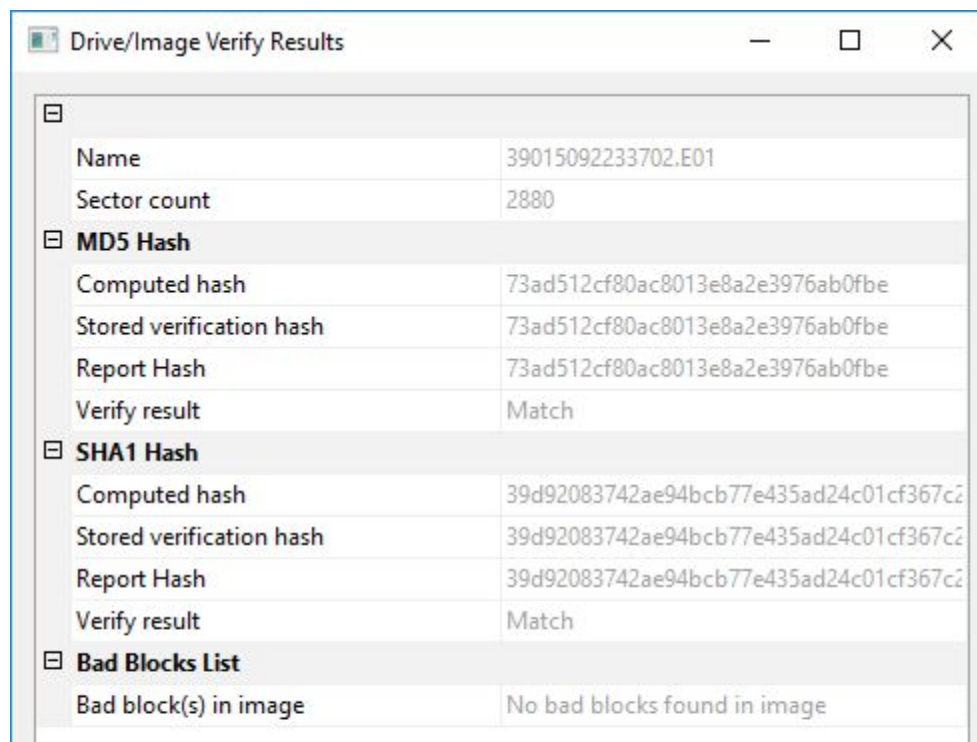
Use AD Encryption ☐

< Back Finish Cancel Help

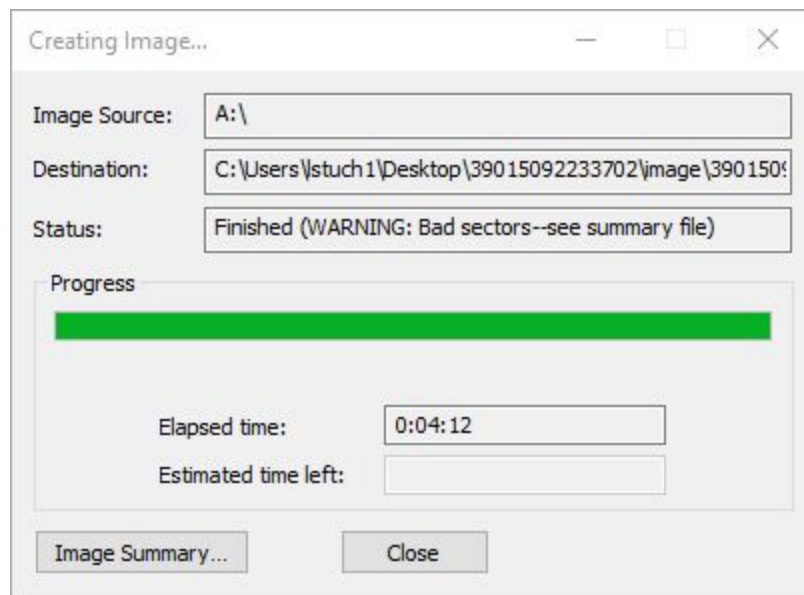
- ▶ Clicking “Finish” will begin the imaging process.



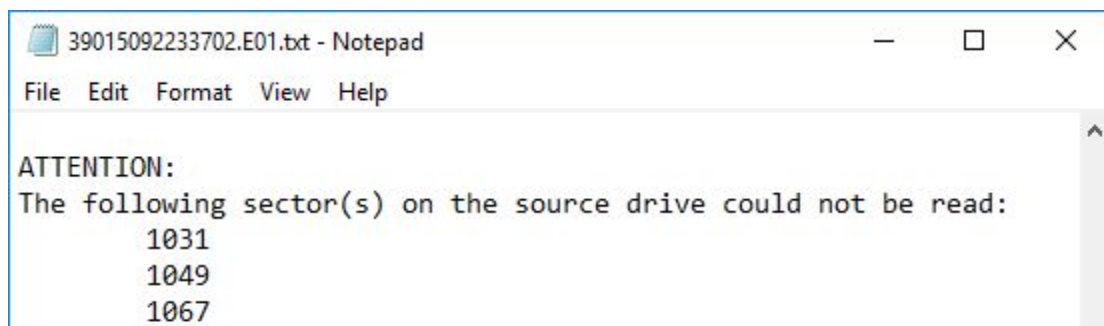
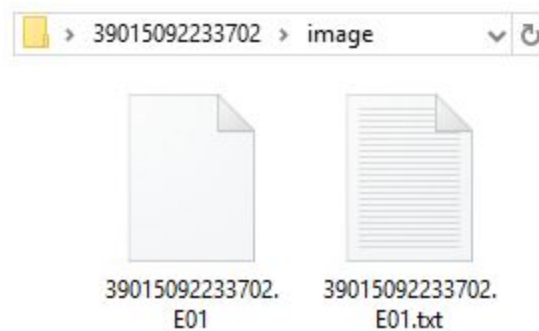
- ▶ Once you are finished, a window that contains verification results will appear. Close out of this window.



- ▶ Refer back to the “Creating Image...” window and read the “Status:” field for any warnings.



- ▶ If it says “Finished”, leave the “bad sectors” column in the working database blank.
- ▶ If there is a warning, open the text file that was created in the *image* file with the E01 file. Scroll down to where it says “ATTENTION: The following sector(s) on the source drive could not be read:”. Count the sector(s) below and note it in the “bad sectors” column in the working database.

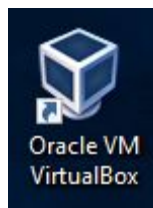


- ▶ Close out of the window, eject disk and minimize FTK Imager.

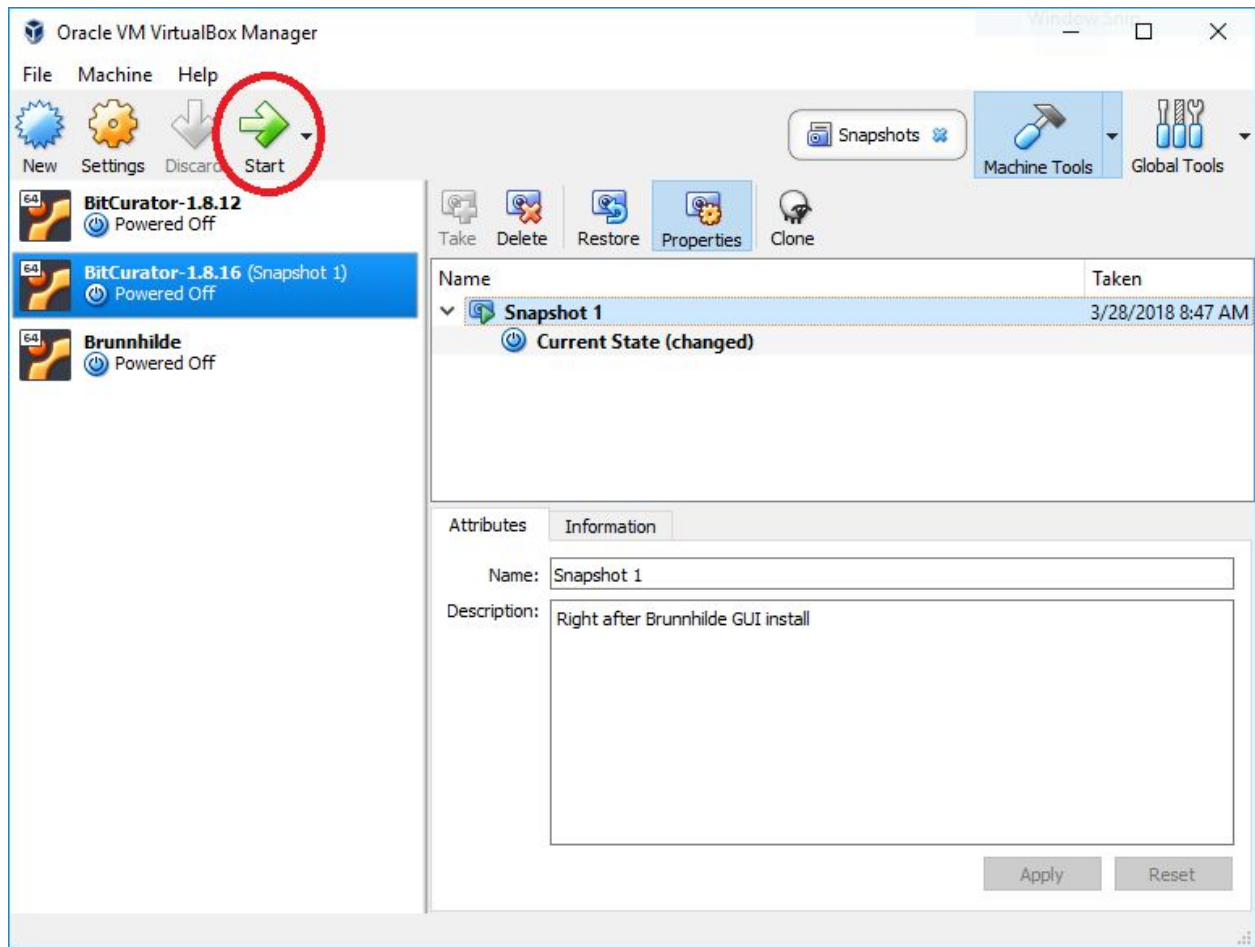
PART III: BRUNNHILDE

[STEP 7] Oracle VM VirtualBox

- ▶ In order to image floppy disks and generate reports, you must access the BitCurator (BC) environment using a virtual machine (VM). The BC VM has already been set up by the Digital Preservation Librarian.
- ▶ Double click the “Oracle VM VirtualBox” on the host computer’s desktop.



- ▶ Then, select the “BitCurator-1.8.16 (Snapshot 1)” VM and click “Start”.
 - ▷ If you have already used this, it will automatically be highlighted when you launch VirtualBox and all you will have to do is click “Start”.
 - ▷ It will take a while for the BC VM to warm up. There may be two pop-ups that have to do with your keyboard and mouse. Ignore these or just close out of them by clicking the “x”.



- Once the BC VM loads, you can use all the tools that come in the BC package and access the `sf_BC_Shared` folder located on the BC VM desktop.



- When you are ready to shut everything down, just click on the power button at the top right hand corner of the BC VM screen, scroll all the way down on the dropdown menu, and select "Shut Down...".

BEFORE YOU START

- ▶ Confirm that BitCurator is in WRITABLE mode.
- ▶ The drive icon at the top right hand corner of the screen will be red if writable mode is activated.
- ▶ We are setting BitCurator to writable due to a mounting related quirk that the read-only mode creates.



[STEP 8] Run Brunnhilde

Brunnhilde is the program used to run reports from the image. It is available in two forms as a Graphical User Interface (GUI) and command line. Instructions for the GUI is below. Command line instructions comes after.

BRUNNHILDE GUI (only available on DARTH)

- ▶ Open the Brunnhilde GUI in the *Forensics and Reporting* folder on the BC VM Desktop.



- ▶ You can choose to run a directory or a disk image. For our purposes, choose disk image.
 - ▷ In the “Source” section, browse for the E01 image file and select it.
 - ▷ In the “Destination” section, select the barcoded folder of the media.
 - ▷ In the “Accession number/Identifier” section, input the following output file name: “metadata”

About

Directory Disk Image Options

Source

d Media/sf_BC_Shared/Disk Images/01234567890123/01234567890123.iso Browse

☐ Hierarchical File System (HFS)-formatted disk

Destination

top/Shared Folders and Media/sf_BC_Shared/Disk Images/01234567890123 Browse

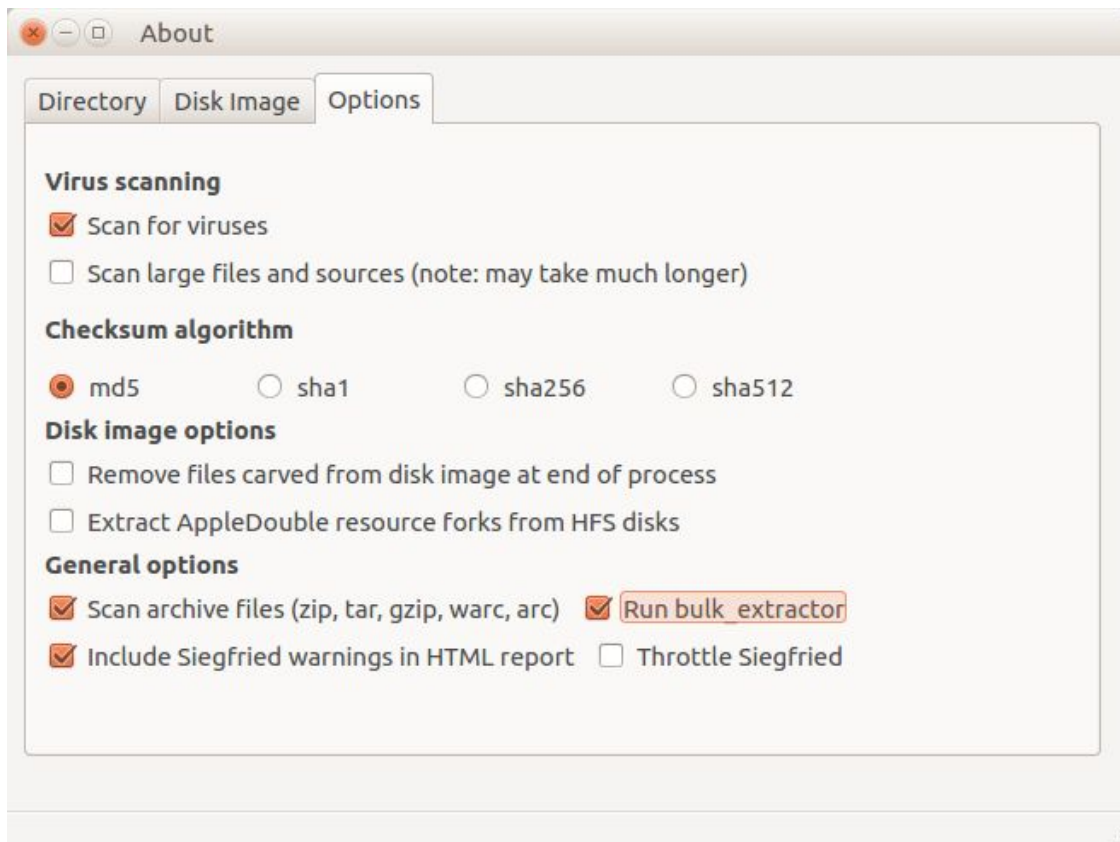
Accession number/identifier

metadata

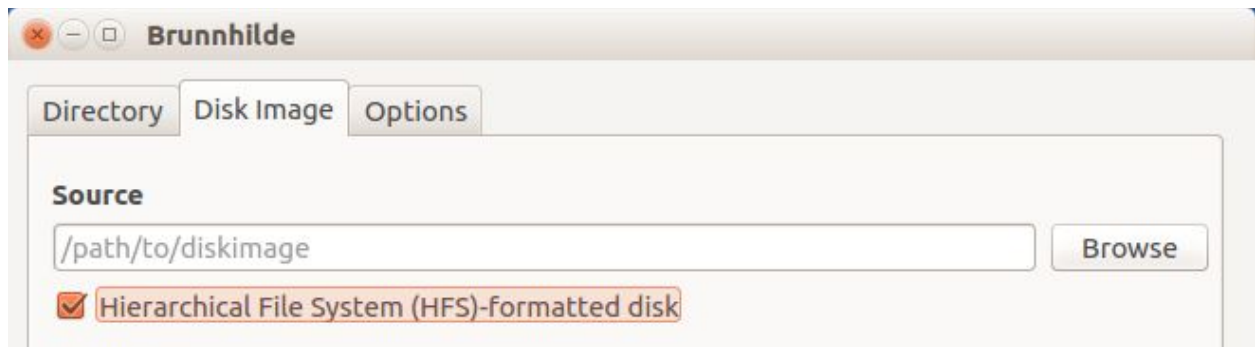
Status

Cancel Start scan

- ▶ In the options tab, make sure the following boxes are checked/selected:
 - ▷ Scan for viruses
 - ▷ md5
 - ▷ Scan archives files (zip, tar, gzip, warc, arc)
 - ▷ Include Siegfried warnings in HTML report
 - ▷ Run bulk-extractor



- ▶ Go back to the disk image tab and click "Start scan".
 - ▷ It will typically take less than a second for Brunnhilde to run on the floppy disk image because of its small size. However, for larger files, it will take longer.
- ▶ Once the scan is completed, click "OK" to close the box that appears saying "Finished Brunnhilde scan complete."
 - ▷ Sometimes, the scan will not work even though it creates the *metadata* folder you wanted it to create. If this happens, delete the newly created *metadata* folder and click the box that says "Hierarchical File System (HFS)-formatted disk". Start the scan again. Note it in the Transfer Inventory spreadsheet.



BRUNNHILDE COMMAND LINE

- ▶ Open Brunnhilde in the *Forensics and Reporting* folder. The icon looks like this:



- ▶ Information on command line options are listed on Brunnhilde's Github [page](#) under "Usage" and on the "DPL Software Information" page in the shared *Digital Preservation Lab Documentation* Folder on Google Drive.
- ▶ Typical command line for an image file is:
 - ▷ `brunnhilde.py -b -d --hash MD5 -z [image file file path] [barcode directory file path] metadata`
- ▶ Drag the image file or directory into the command line interface for file paths. Do not type it out.

```

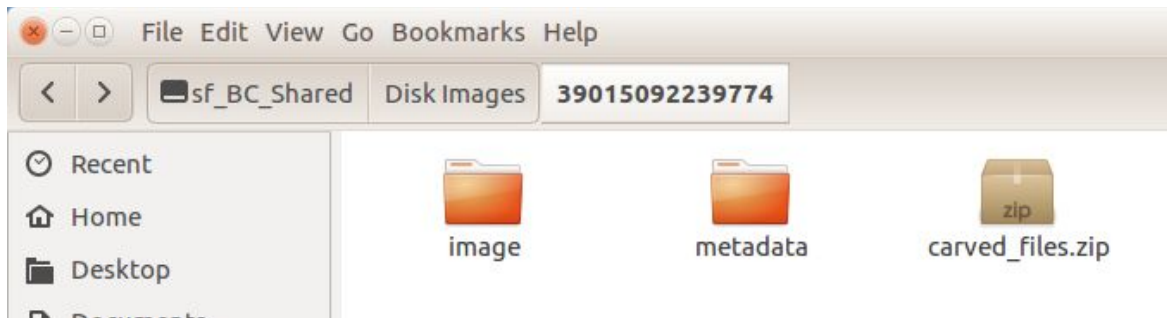
bcadmin@ubuntu:~$ cd ~/
bcadmin@ubuntu:~$ brunnhilde.py
usage: brunnhilde.py [-h] [-a] [-b] [--ssn_mode SSN MODE] [-d] [--hfs]
                    [--resforks] [--tsk_imgtype TSK_IMGTYPE]
                    [--tsk_fstype TSK_FSTYPE]
                    [--tsk_sector offset TSK_SECTOR_OFFSET] [--hash HASH]
                    [-l] [-n] [-r] [-t] [-V] [-w] [-z]
                    source destination basename
brunnhilde.py: error: the following arguments are required: source, destination,
basename
bcadmin@ubuntu:~$ brunnhilde.py -b -d --hash MD5 -z '/media/sf BC_Shared/Disk Images/ReadyForBagging/39015092242513/image/39015092242513.img' 

```

- ▶ Hit “enter” on the keyboard. Any errors and reports (virus scan) will be shown on the command line. Minimize Brunnhilde.

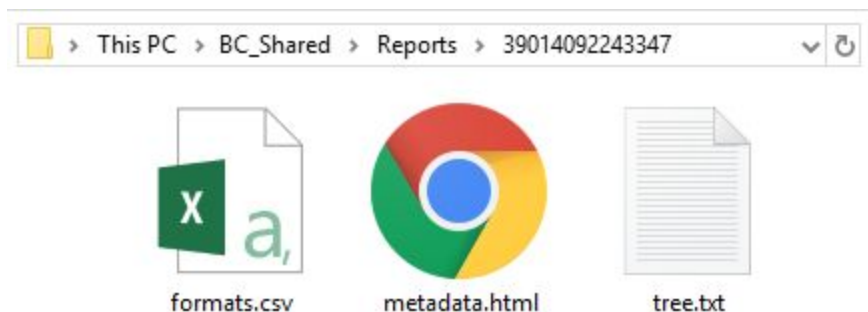
DIRECTORY CLEAN-UP

- ▶ Open File Explorer, navigate to the barcode folder and then the *bulk_extractor* folder. Click on the “view items as a list” icon in the upper righthand corner to change the display of the files. Filter by “size” and delete all files measuring 0 bytes.
 - ▷ These clutter up the *bulk_extractor* folder and do not provide us with any useful information about the disk image.
- ▶ Drag the photos taken earlier that are in the barcoded file into the newly created *metadata* folder.
- ▶ In the *metadata* folder, drag the *carved_files* directory into the same level as *metadata* and *image*.
- ▶ Right-click on *carved_files* and select “Compress...”. In the new window, keep the filename as *carved_files* and select “.zip” as the extension. Hit “Create” and delete the unzipped *carved_files* directory.



[STEP 9] Reports

- ▶ Go to the Reports folder created earlier and create a new directory with the barcode as the filename. Make a copy of the “tree.txt”, “formats.csv”, and “metadata.html” from the metadata folder.
 - ▷ The “tree.txt” and “metadata.html” files will be in the metadata folder while the “formats.csv” file will be in the csv_reports folder in the metadata folder.
 - ▷ This is the package of reports that will be sent to Special Collections.



PART IV: BAG AND TRANSFER TO STORAGE

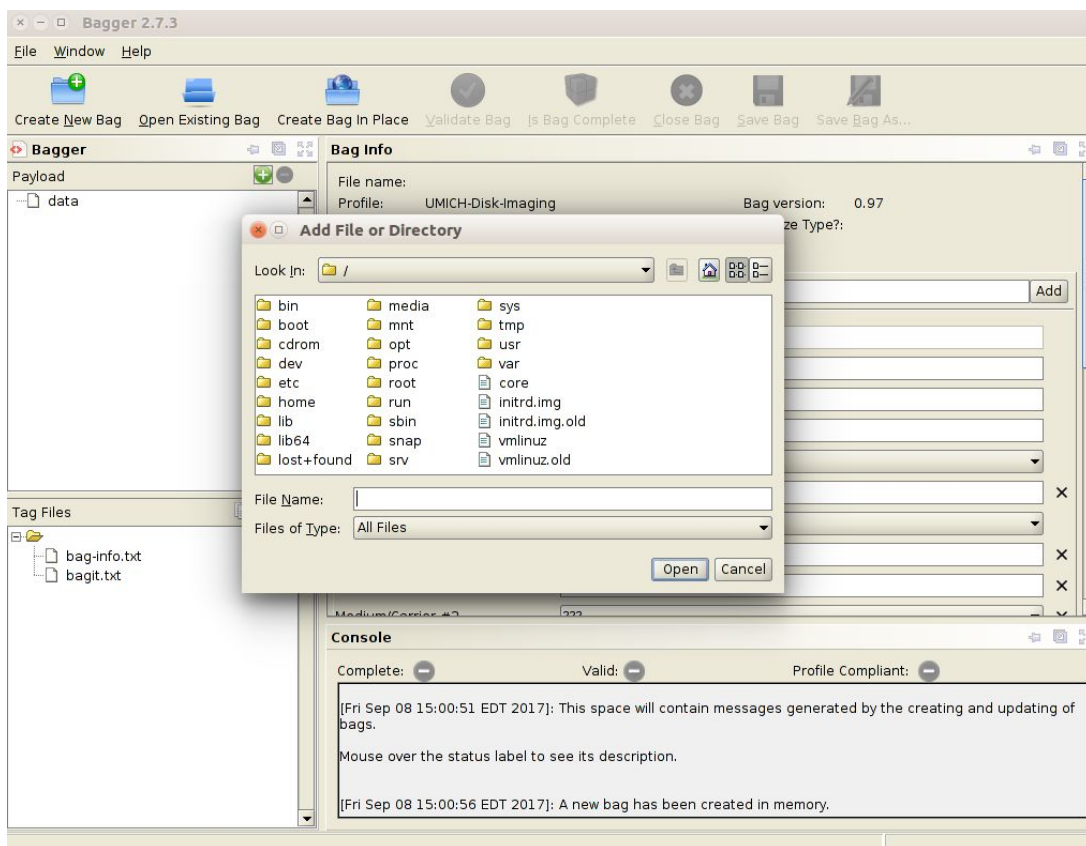
[STEP 10] Package SIP Using BagIt

***NOTE: It is important to follow these steps in order to ensure that the metadata saves properly.

- ▶ Switch from the BC VM to the host computer’s desktop and open “bagger.bat-Shortcut”.



- ▶ On the upper lefthand corner, click “Create New Bag”.
- ▶ Select the “UMICH-DISK-Imaging Profile”.
- ▶ Click on the small green plus sign.
 - ▷ You will be prompted to “Add File or Directory”.
 - ▷ Select the parent folder containing the disk image and metadata (do not double click).
 - ▷ Click “Open”.



- ▶ Under the “Payload” section on the left, the folder you selected will show. Highlight the barcode by selecting (only click once) the folder prior to saving your bag. It is recommended that you do this in the beginning in case you forget to do it at the end.
- ▶ Fill out the profile with metadata by consulting the Imaging Metadata Report.
- ▶ Once you are finished selecting the parent folder and filling out the metadata, click “Save Bag As...”

- ▶ In the “Save Bag Dialog”:
 - ▶ Navigate to the designated directory and create a file with the barcode as the title inside the parent folder.
 - ▶ Make sure to leave “Holey Bag” unchecked.
 - ▶ Select the following:
 - None
 - Generate Tag Manifest?:
 - Generate Payload Manifest?:
 - SHA-1 (for “Tag Manifest Algorithm:” and “Payload Manifest Algorithm:”)

Save Bag Dialog

Save Bag
Define the Bag settings

Save in:

Holey Bag?: ☐ Holley Bag

Base URL

Serialize Type?: ☒ none ☐ zip

Generate Tag Manifest?: ☒

Tag Manifest Algorithm:

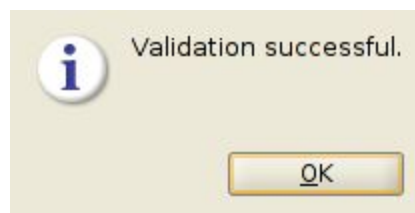
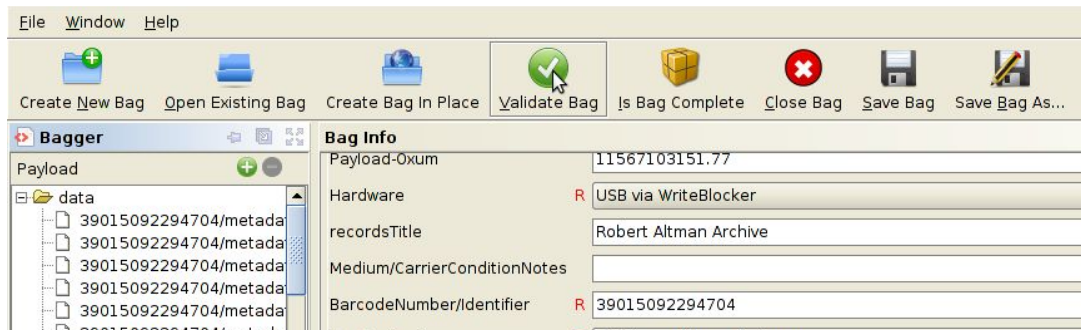
Generate Payload Manifest?: ☒

Payload Manifest Algorithm:

- ▶ Once all of the above are selected, click “OK”
- ▶ The Bag Info will then be generated. The results will appear in Bagger and the Bag will be created in the specified directory.

[STEP 11] Validate Bag


- ▶ After the bag is generated, click “Validate Bag” to validate the zipped bag you just created.




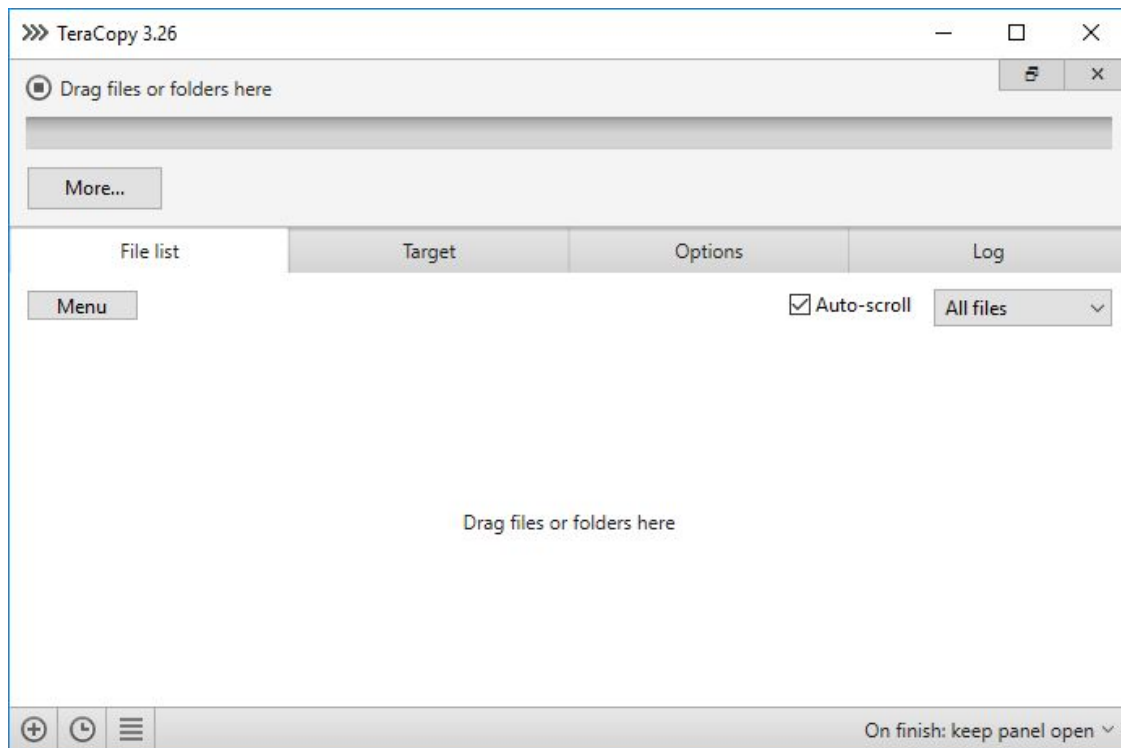
[STEP 12] Transfer to the Network Attached Storage (NAS)

- ▶ At the end of the week, copy all files into public (\\192.168.255.10) (Z:) drive. This is the step prior to moving bags into Deep Blue.
- ▶ Search for “Tera” in Windows menu bar and select “Teracopy”. A window like this will appear:

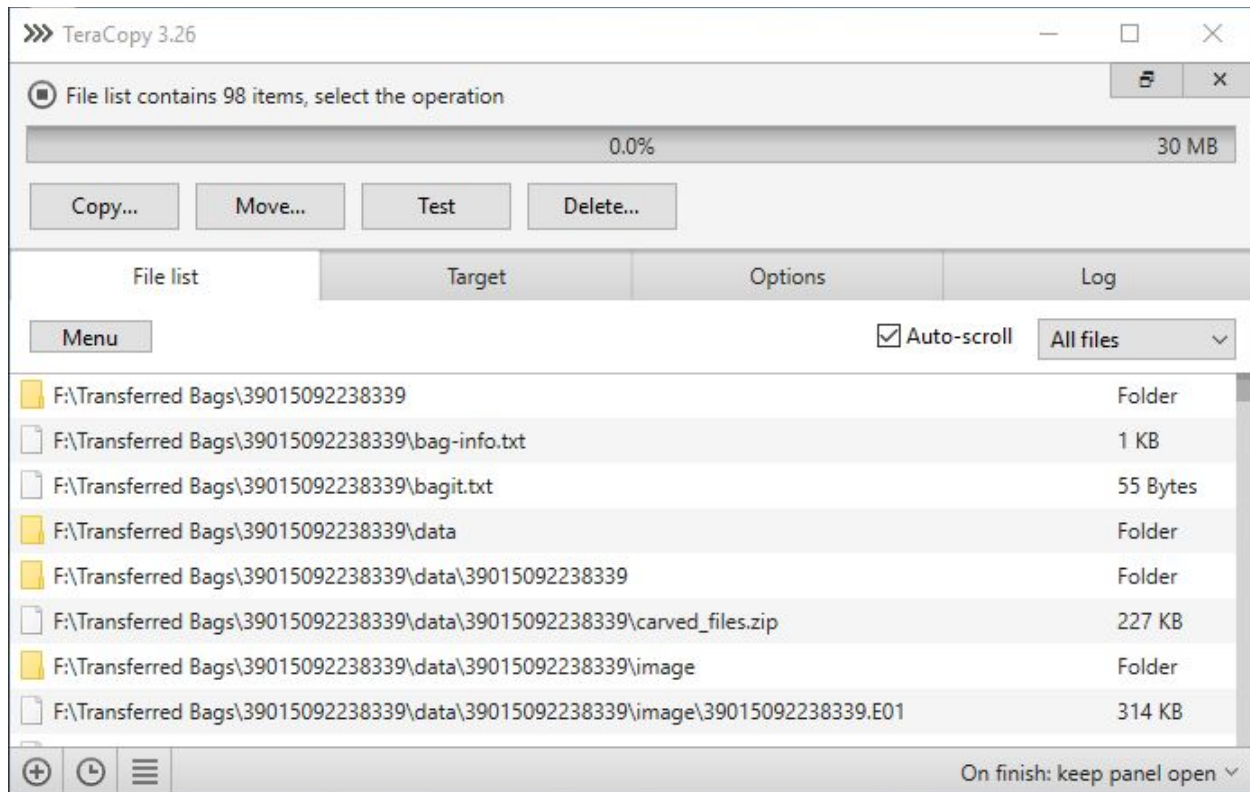


- ▶ Information from the previous transfer may load. If it does, click the  on the bottom left corner for a fresh window and the little “x” on the top right to exit out of the old window.

- ▶ Press the little window button  on the top right to extend the window. The new area is where bags from the *Bagged Folder* are dragged. The screen should now look like this:



- ▶ Select files from *Bagged Folder* that are ready to be transferred. Drag them into TeraCopy. Files will appear like this:



- ▶ Under the “Target” tab, select “Browse” → public(//192.158.255.10)(Z:) → “TransferQueue”.
- ▶ The “Options” tab should stay the same with “Prompt on filename collision” and “MD5” as default.
- ▶ Press “Copy...” near the top of the screen. Selecting “Move...” will remove bags from *Bagged Folder* and into NAS.
- ▶ The “Log” tab reflects directories that have successfully/failed copying.
- ▶ When TeraCopy is finished, check the “TransferQueue” directory to see if files have been copied.
- ▶ Create a new Directory in *Bagged* named *UploadedtoDarkBlue* if it has not been created already. Move the bags you transferred using Teracopy into this new directory so you don’t copy it twice to the NAS.