USB MEDIA FILE TRANSFER 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 | 26 August 2018

THE WORKFLOW

Part I: Preparation

1. Prepare directory
2. Photograph media
3. Update record in tracking database

Part II: Transfer Files

4. Configure hardware for disk imaging based on media format
5. Transfer files and generate checksums

Part III: Brunnhilde

6. Navigating to the BitCurator Virtual Machine
7. Run Brunnhilde

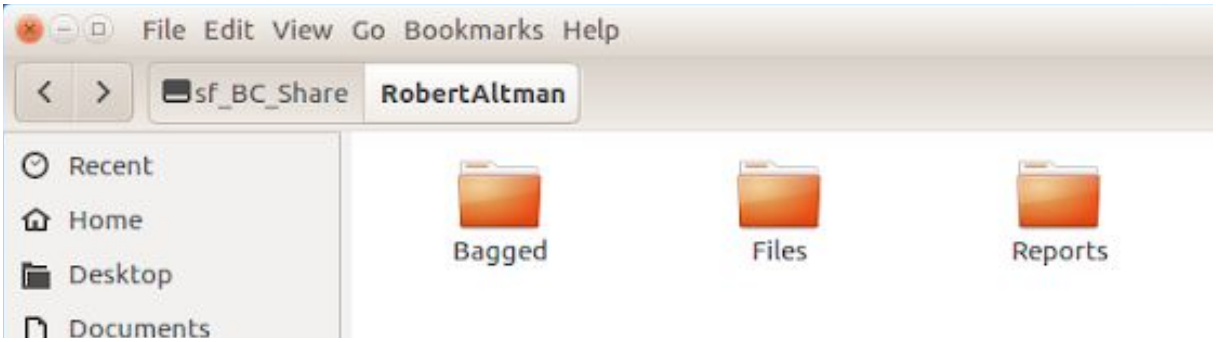
Part IV: Bagging and Transfer to Storage

8. Package SIP using BagIt
9. Validate bag
10. Transfer to the Network Attached Storage (NAS)

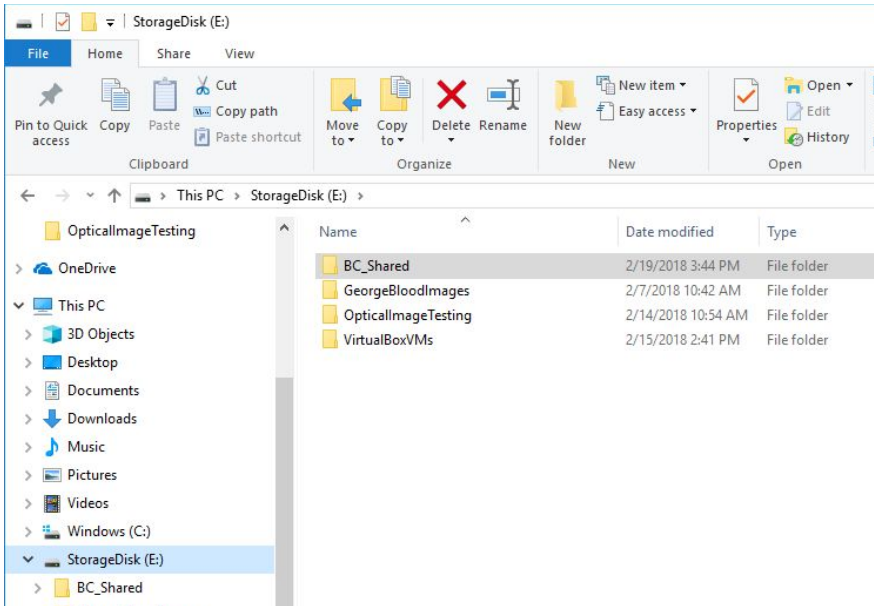
PART I: PREPARATION

[STEP 1] Prepare Directory/Media

- Barcode all media.
  - All media should be barcoded at the beginning, during the inventorying process.
  - If the media has a storage case or container, the media item and the storage case or container should be given the same barcode.
- Prepare the directory for disk images, reports, and bagged folders by creating three folders in the *BC_Shared* folder, which is the folder that is shared by the BitCurator Virtual Machine (BC VM) and the host computer.
  - This is to distinguish between 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.
  - Within the *Files* folder, you will later create a folder with the barcode of the media. You will also need to create a folder for your files called *files* (see last screenshot in [Step 6])

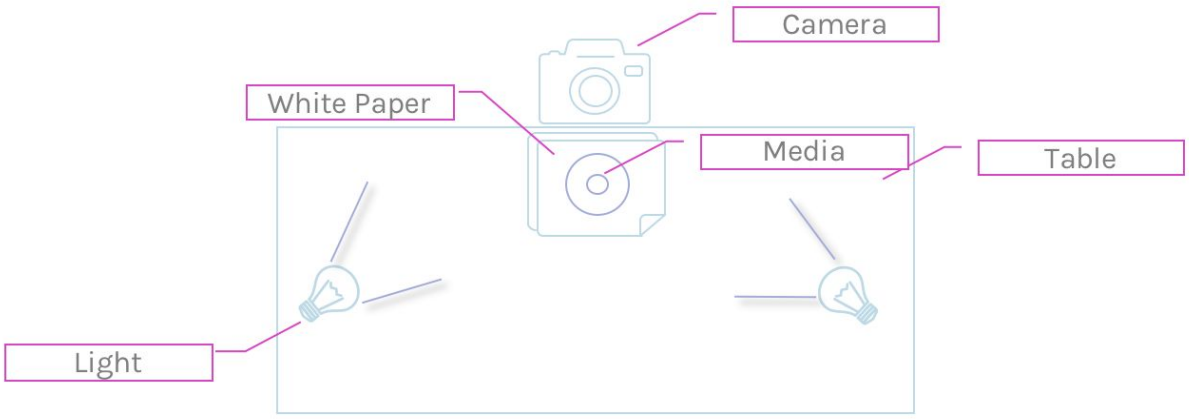


  - The *sf_BC_Shared* folder can be found on the BC desktop or in the StorageDisk (E:) hard disk on the host computer's desktop.



[STEP 2] 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.
- 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 or back.



- 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.
- 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. (However, both the media and its case should have a unique ID handwritten on them).
    - Take 3 sets of photos (resulting in a total of 8 photos per media and case) that are set to different exposures.
        - To set the exposure, turn the camera on.
        - Then, 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.
- Upload images to the computer using the camera cable.
- Select the photos with the most similar lighting of the highest quality. Once the photos have been moved into the *metadata* folder scratchspace, delete all the photos

on the camera before unmounting.
- Rename the photos with the barcode underscore and description of the image.
  - Some descriptions you can use are:
    - MediaFront
    - MediaBack
    - CaseFront
    - CaseBack
    - Notes01
  - An example for an optical disk would “1234567890_MediaFront”
- Save the photographs you have taken of the media in the barcoded folder for the disk image. These will be dragged into the *metadata* folder that Brunnhilde generates.

[STEP 3] Update Record in Tracking Database

Before you begin, create a working database that includes an inventory of all the objects you have in your collection. Most of the time, if the content is coming from Special Collections, there will be some metadata transferred with the content. This information can be incorporated into the working database along with metadata we will create during the imaging process and the media’s transfer to and from Special Collections. An example of this working database is the one for the John Sayles collection.

The following information should be inputted into the working database prior to imaging:
- 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

The following information should be inputted into the working database after/while imaging:
- 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 for whether reports directory for Special Collections 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

PART II: TRANSFER FILES

[STEP 4] Configure Hardware for Disk Imaging

ALL MEDIA

- 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.

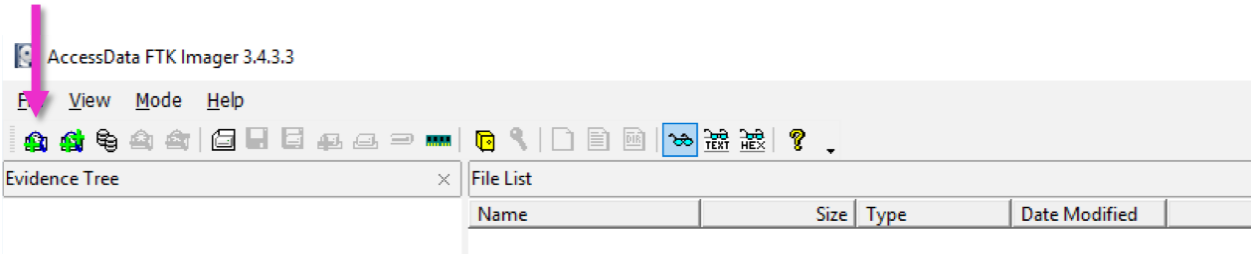
USB DRIVES & HARD DRIVES:

- Connect the external hard drive or USB drive directly to the write-blocker while it is turned off. Follow the instructions in the forensic bridge's QuickStart Guide.
- We have been connecting the forensic bridges to the USB port on the back of the computer because it is faster and more direct connection to the computer.
- Once the drive is connected, turn on the write-blocker.
- The media will be detected by BitCurator.
    - If the device is not detected, turn the write-blocker off again and make sure the connection is secure at both the write-blocker input, as well as, the computer input.
    - The USB drive icon will appear in the navigation bar on the left of the screen once detected.

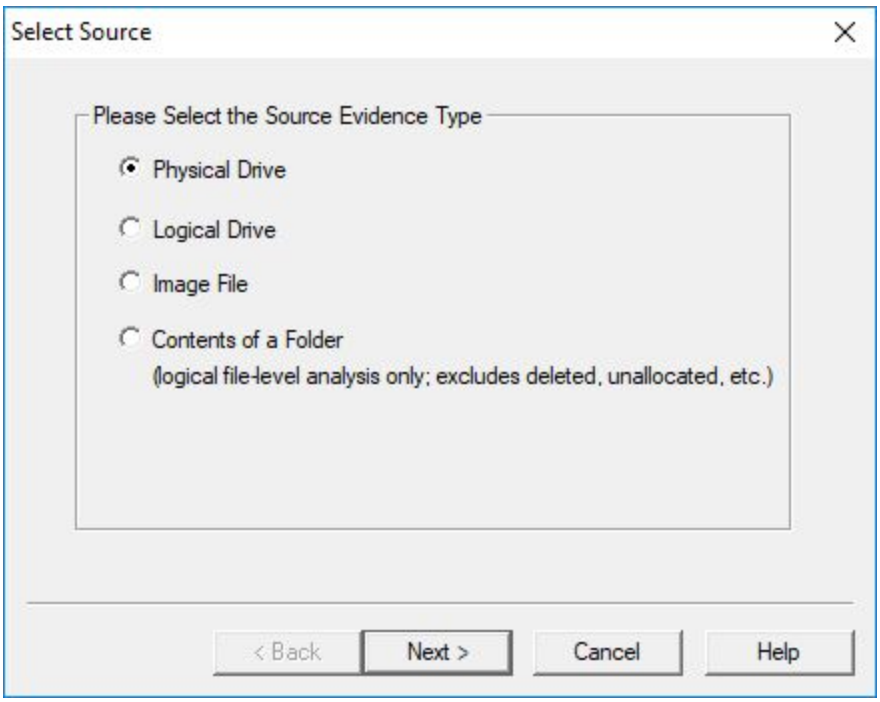
[STEP 5] Transfer Files and Generate Checksums

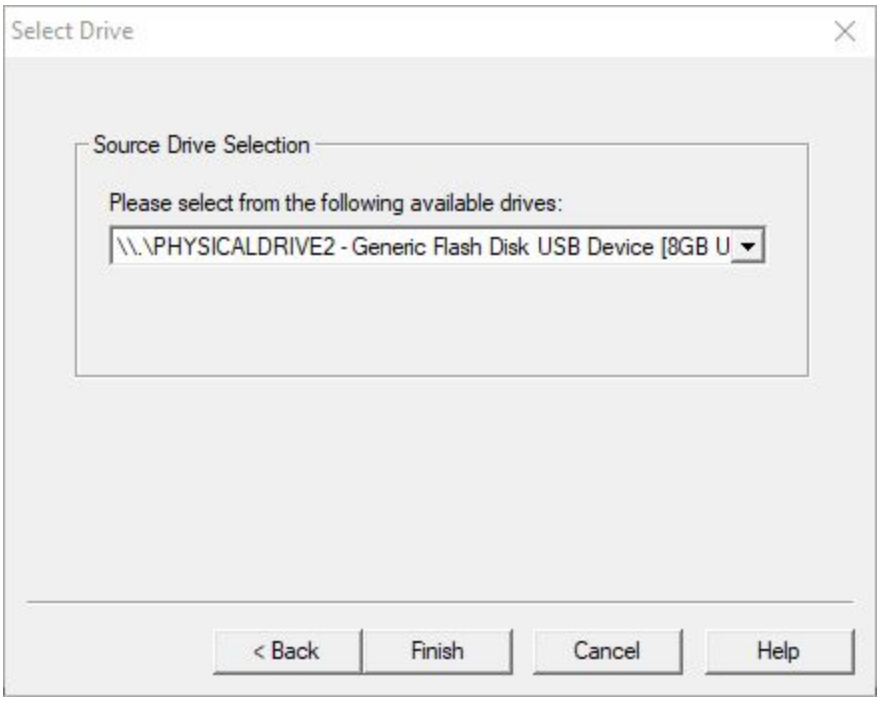
- Open FTK Imager on the host computer desktop.

    - It will prompt you to enter the username and password. Enter the information and the FTK Imager will open.
- Once FTK Imager is open, select “Add Evidence Item”.

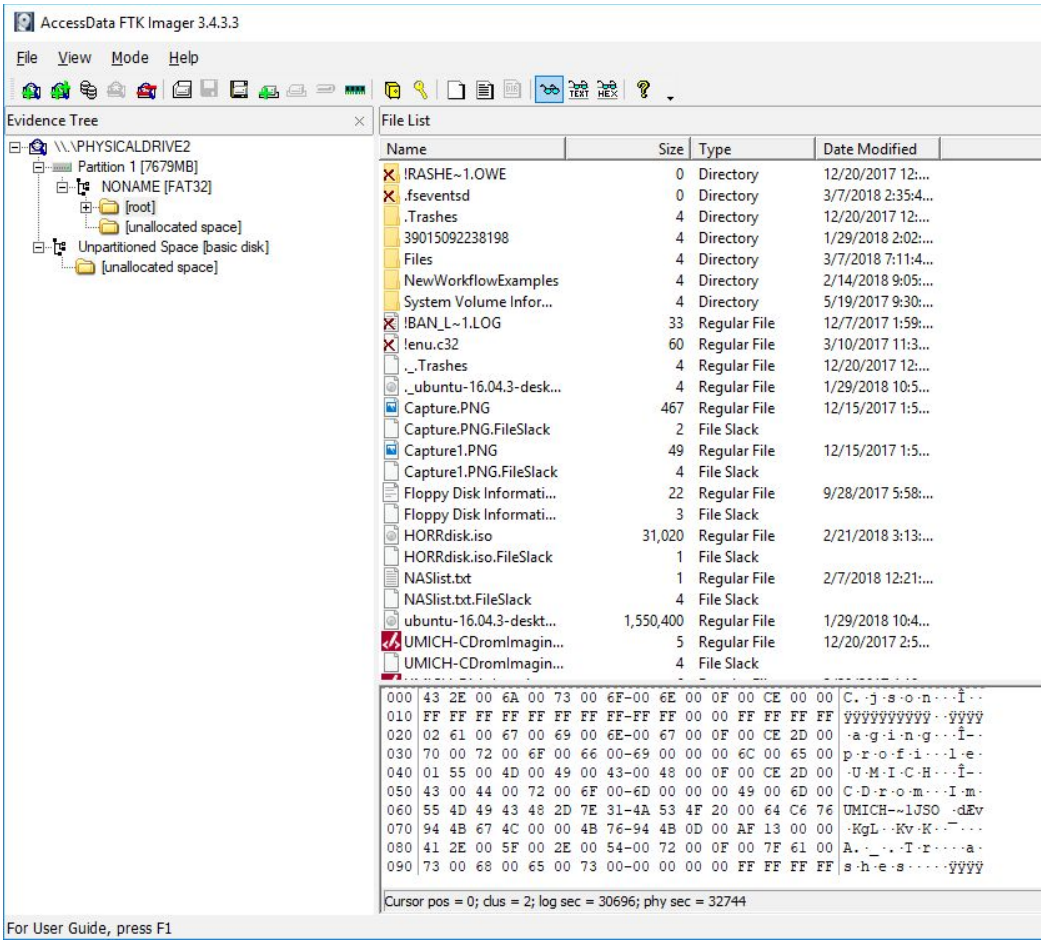


- A window that says “Select Source” will pop open. Click “Physical Drive” and select the *files* folder in your barcoded folder as your “Source Drive Selection”. Then, click “Finish”.

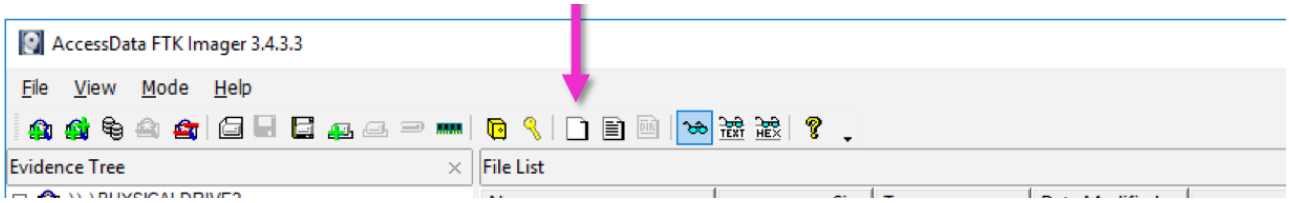




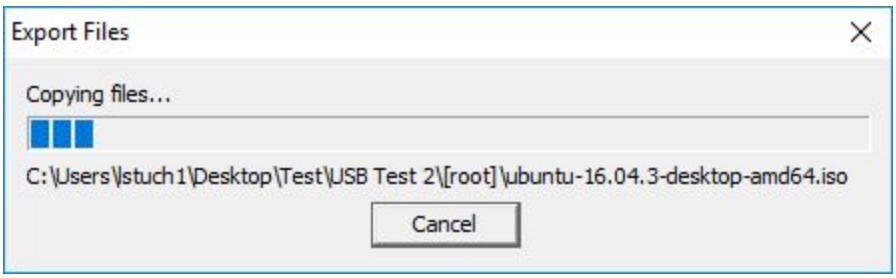
- Once you have chosen the file to add as evidence, you will see it appear under the “Evidence Tree” section.



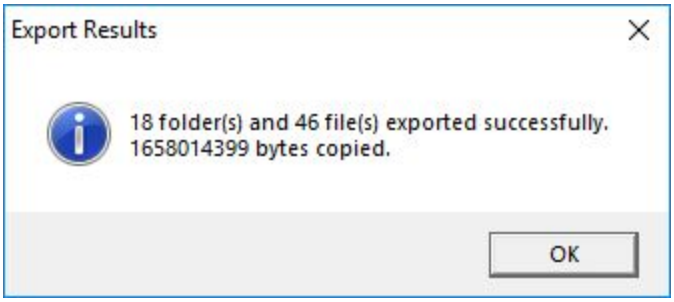
- Once FTK Imager has added the evidence item, the “Export Files” icon will become selectable.



- Once the “Export Files” icon becomes selectable, highlight any and all files that are NOT *[unallocated space]*. Then, click on the “Export Files” icon and it will prompt you to select a destination folder.
- Create a new folder called *files* and store the image in that file.
- Once you select the destination, FTK Imager will begin copying the files and exporting them to your destination folder.



- You will know that the exporting is finished when you see the following pop-up:



- Once you are finished, right click the drive and select “Remove Evidence Item” and close out of FTK Imager.

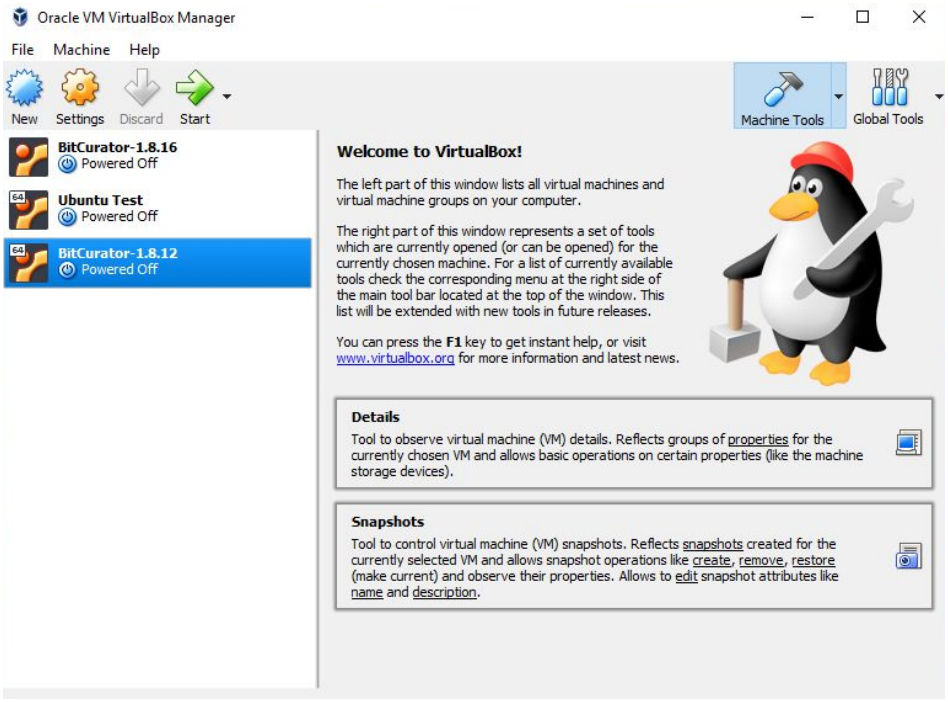
PART III: BRUNNHILDE

[STEP 6] Navigating to the BitCurator Virtual Machine

- In order to run Brunnhilde, 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-1.8.12” VM and click “Start”.

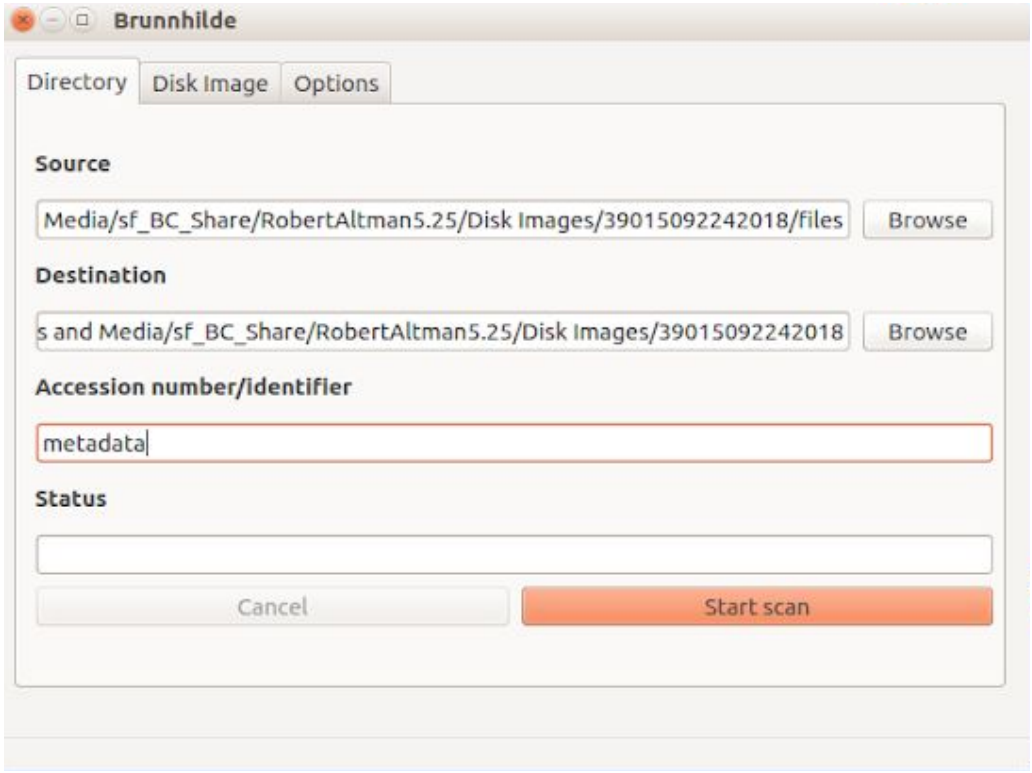
- If you have already used this, it will automatically be highlighted when you launch the VirtualBox and all you will have to do click “Start”.
- It will take a while for the BC VM to warm up. There will be two pop-ups that have to do with your keyboard and mouse. Ignore these or just close out of them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



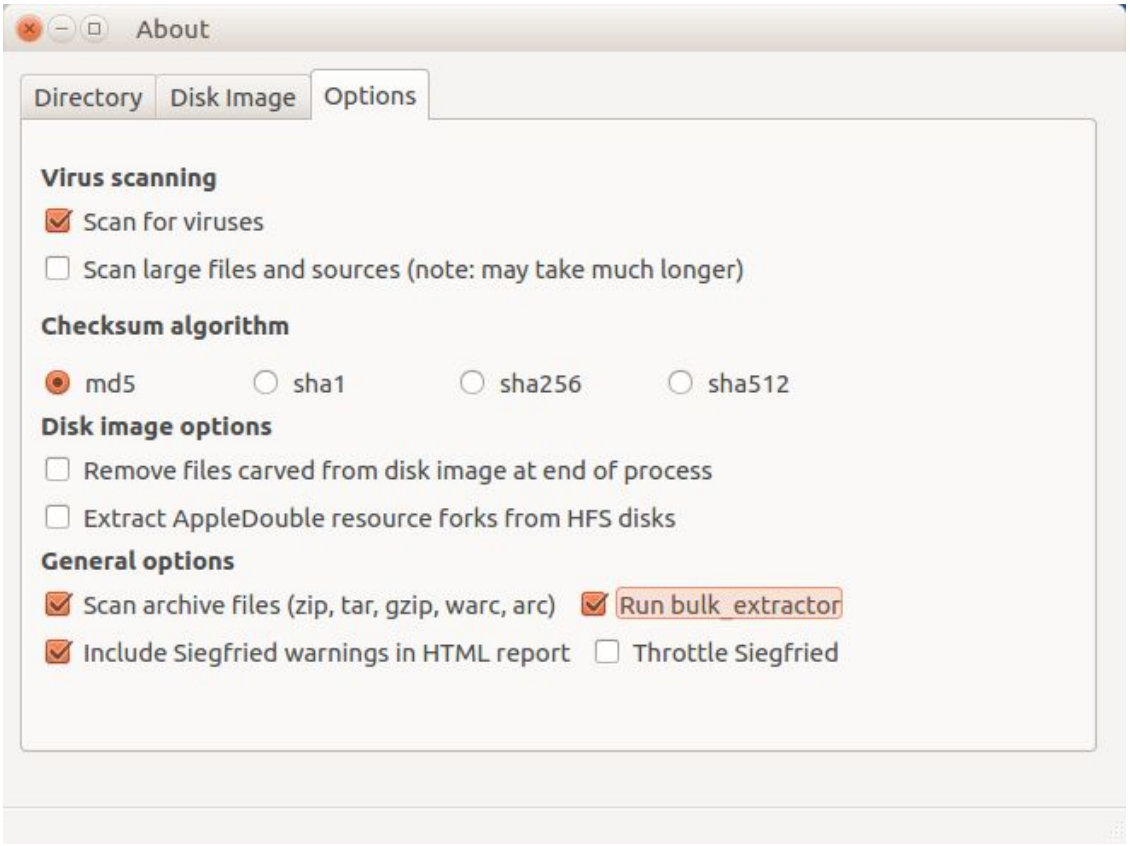
- Once the BC VM loads, you can use all the tools that come in the BC package and access the *BC_Shared* folder, which is located on the BC VM desktop.
- When you are ready to shut everything down, just click on the power button at the top right hand corner of the BC VM screen, scroll all the way down on the dropdown menu, and select “Shut Down…”.

[STEP 7] Run Brunnhilde

- Open the Brunnhilde GUI in the *Forensics and Reporting* folder.
- You can choose to run a directory or a disk image. But for our purposes, choose directory.
- In the “Source” section, select the disk image.
- In the “Destination” section, store the image in the barcoded folder that matches the respective media.
- In the “Accession number/Identifier” section, input the following output file name:
  - “Metadata”



- 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.”
- Navigate to the *bulk_extractor* folder and 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.
- Make a copy of the “tree.txt”, “formats.csv”, and “metadata.html” files into the *Reports* folder with the folder name being the barcode of the media. Follow this path to get to *Reports*.
  - 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.
  - This is the package of reports that will be sent to Special Collections.

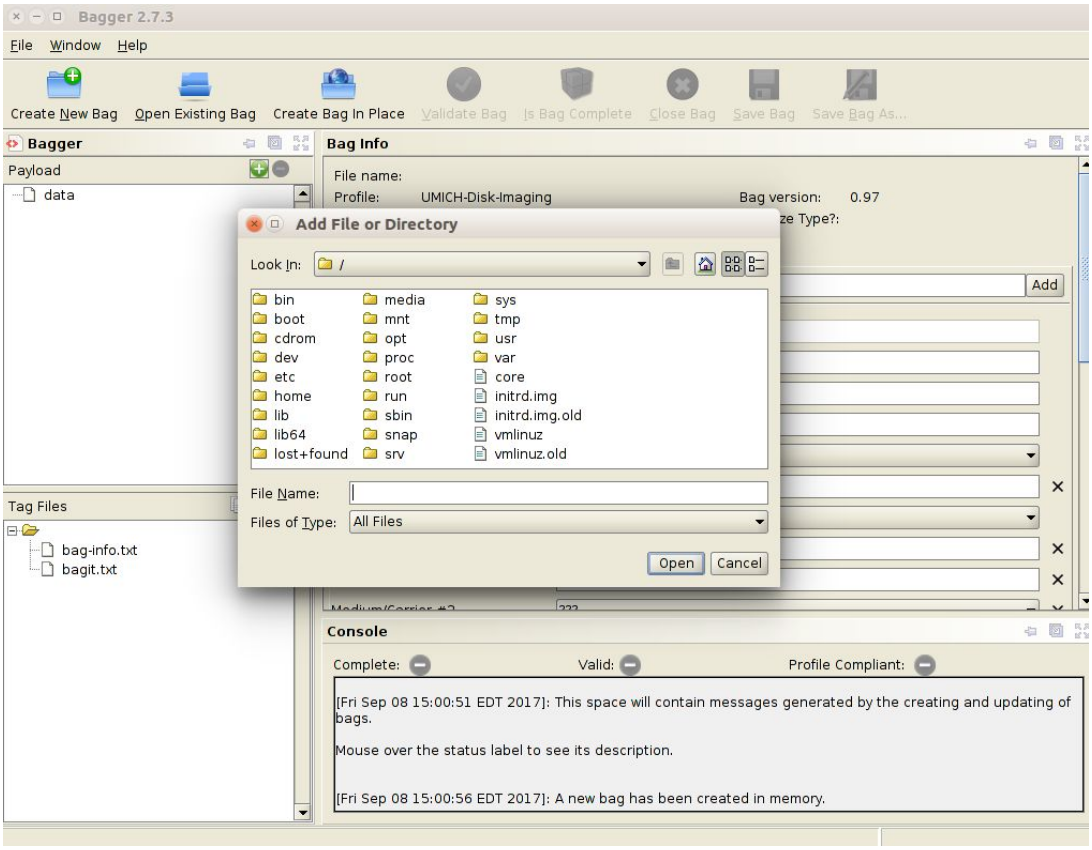
PART IV: BAG AND TRANSFER TO STORAGE

[STEP 8] Package SIP Using BagIt

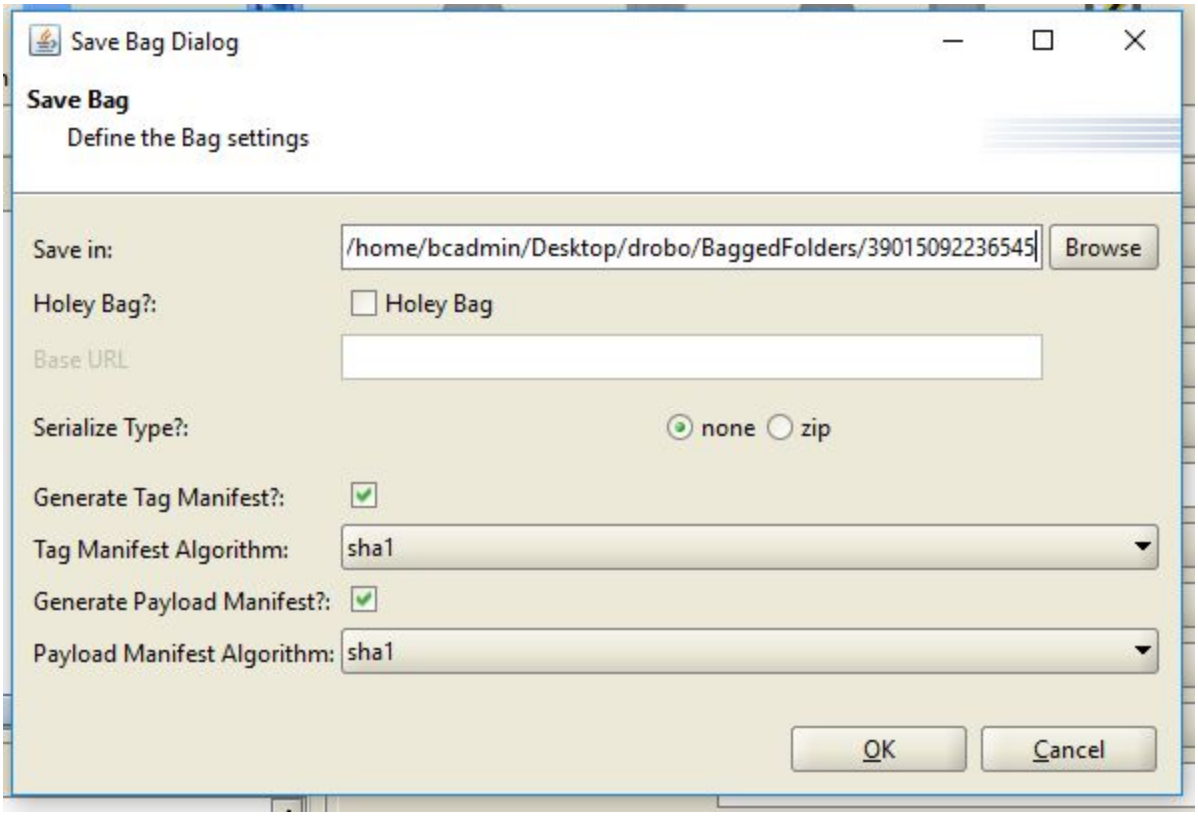
****NOTE: It is important to follow these steps in order to ensure that the metadata saves properly.*

- Now, switch from the BC VM to the host computer's desktop, and open the "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".



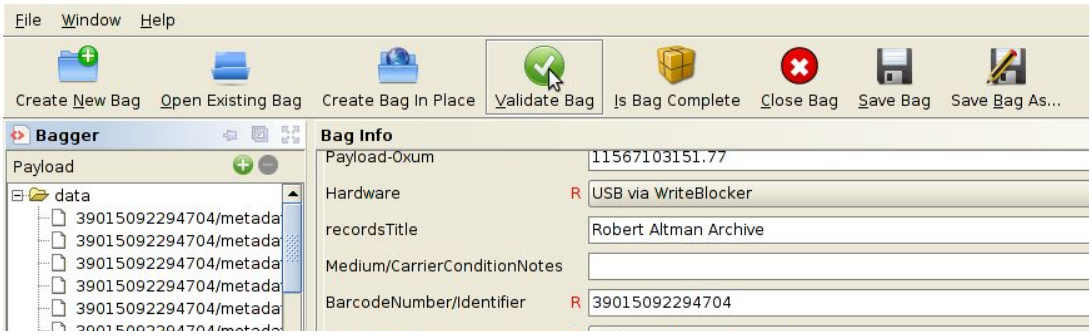
- Under the “Payload” section on the left, the folder you selected will show. Select (only click once) the folder prior to saving your bag.
  - It is recommended that you do this in the beginning in case you forget to do it at the end.
- Fill out the profile with metadata by consulting the Imaging Metadata 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:”)



- 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.

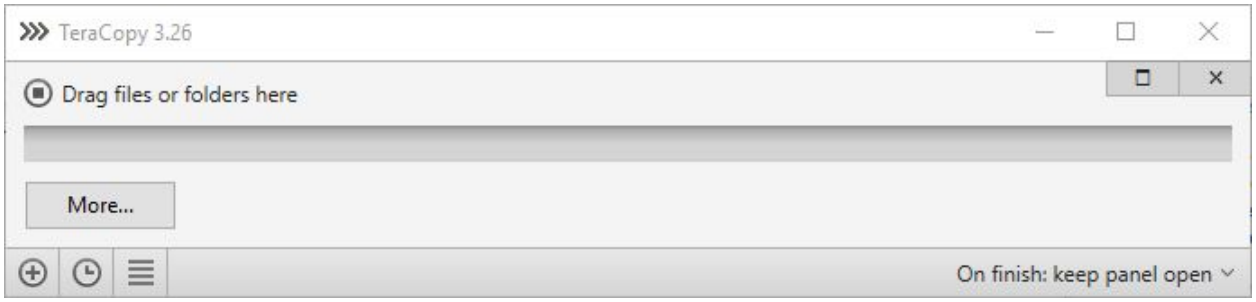
[STEP 9] Validate Bag

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

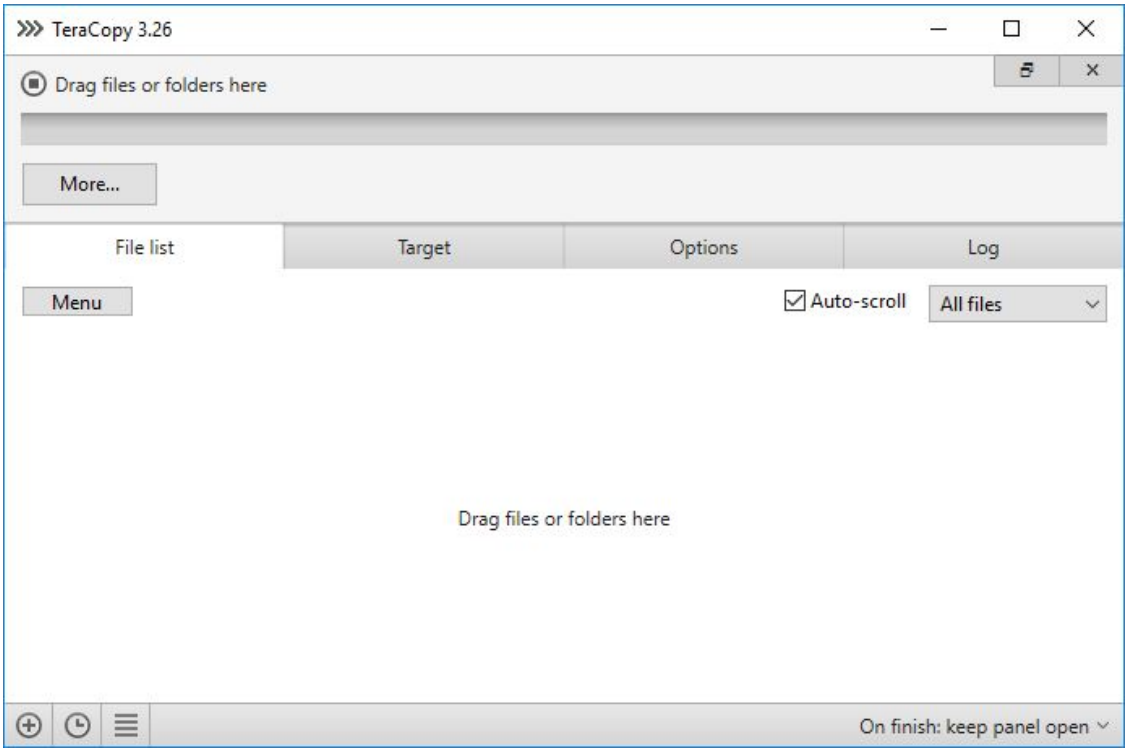


[STEP 10] Transfer to the Network Attached Storage (NAS)

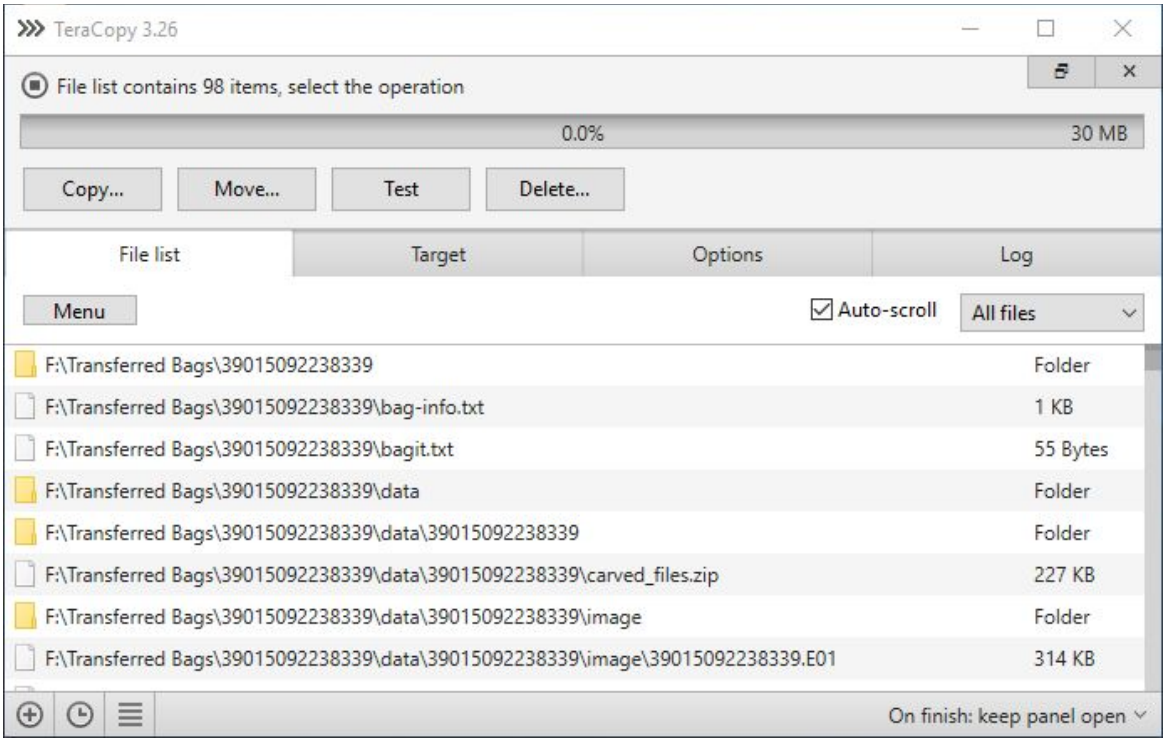
- At then end of the week, connect scratchspace to a computer connected to the NAS.
  - Connect scratchspace to a USB 3 port. The bottom of the port will say “SS” or the port will be the color blue.
  - The scratchspace should automatically appear. Open up the “Bagged Folder” directory.
- Search for “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 files from scratchspace are dragged. The screen should now look like this:



- Select the files from the open “Bagged Folder” window and drag them into TeraCopy. Files will appear like this:



- Under the “Target” tab, select “Browse” → public(//192.158.255.10)(Z:) → “TransferQueue”.
- “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 directories from scratchspace and onto 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.
- Move bags from “Bagged Bags” to “Transferred Bags” on scratchspace.
- Eject scratchspace.