**Imaging and Born Digital Content Acquisition Procedures**

**Table of Contents**

[Format Workflows 2](#_Toc786866668)

[Digital Transfer 2](#_Toc1846973856)

[Donor Guidance 2](#_Toc40899171)

[Ideal Workflow 2](#_Toc1423307456)

[Exactly 2](#_Toc1958177135)

[Acceptable Workflow 2](#_Toc1631047422)

[Windows Users 2](#_Toc1389238808)

[Apple Users 3](#_Toc163220838)

[Procedures Upon Arrival to WVRHC 3](#_Toc738712916)

[CDs and DVDs 4](#_Toc218524530)

[CD-DA 4](#_Toc1099418053)

[All Other CD and DVD Formats 5](#_Toc832333756)

[3.5 inch floppy disks 7](#_Toc1622609811)

[Thumb drives, internal hard drives, external hard drives, and memory cards 9](#_Toc645472466)

[Thumb drives and external hard drives 10](#_Toc1628994564)

[Internal hard drives 11](#_Toc1631716786)

[Memory cards 13](#_Toc1596883907)

[Hardware Workflows 14](#_Toc1301149050)

[Tableau Forensic Bridge 15](#_Toc615267299)

[Software Workflows 15](#_Toc1550214374)

[FTK Imager 15](#_Toc168979249)

[Imaging an Item 15](#_Toc1446691615)

[Viewing a Disk Image or Media Item 17](#_Toc1170485076)

[Extracting Content from a Disk Image or Media Item 18](#_Toc564512156)

[IsoBuster 18](#_Toc98864769)

[Identifying the Format of a Disc 18](#_Toc2112750587)

[Imaging an Item 18](#_Toc649021187)

[Viewing a Disk Image or Media Item 19](#_Toc1947435209)

[Troubleshooting Potential Errors 19](#_Toc139268712)

[HFS Explorer 21](#_Toc1752991511)

[Exact Audio Copy 21](#_Toc1417674466)

[Extracting Content 22](#_Toc49886557)

[TeraCopy 24](#_Toc479433839)

[Command Line Tools 26](#_Toc979386461)

[Tree 26](#_Toc15286329)

[Brunnhilde 26](#_Toc248492909)

[Exactly 27](#_Toc967949704)

# **Format Workflows**

All workflows in this document assume a collection or accession has been formally received by the West Virginia & Regional History Center and is accompanied by a Deed of Gift or Loan. Ideally, all materials will have an accession number and, if applicable, an A&M number. If an item or set of items does not have an accession number, talk to the Accessioning Archivist.

The DVD, CD, IsoBuster, and FTK Imager workflows are greatly informed by Annie Schweikert’s [work on optical media at NYU](https://archive.nyu.edu/handle/2451/43877).

## **Digital Transfer**

Sometimes donors have a limited quantity of content and would like to transfer their materials exclusively digitally rather than via a hard drive or other physical media. Depending on the quantity, this transfer may be via email or a file share such as Box, OneDrive, or Google Drive.

The following workflows outlines two transfer methods: Ideal and Acceptable.

* The Ideal method is best for donors with technical expertise or content that is highly valuable and needs to retain as much built-in metadata as possible.
* The Acceptable method is best for donors with limited technical expertise or content that only needs to maintain most metadata.

### **Donor Guidance**

#### **Ideal Workflow**

##### **Exactly**

*Work in progress*

This section outlines an ideal workflow for donors with moderate technical expertise who are donating highly valuable content.

|  |  |
| --- | --- |
| **Software** | Exactly |
| **Hardware** | None |

<https://www.weareavp.com/wp-content/uploads/2022/04/Exactly_UserGuide_0.1.6.pdf>

#### **Acceptable Workflow**

This workflow requires minimal technical expertise and maintains most metadata. The instructions below can be forwarded directly to donors.

##### **Windows Users**

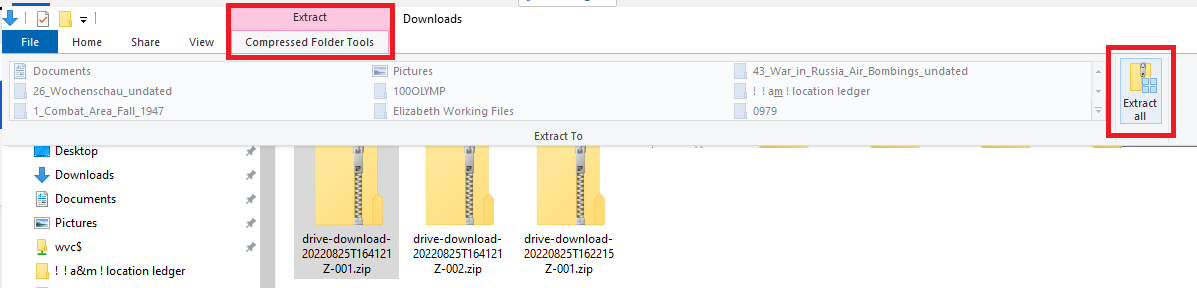
1. Locate the file or folder that you want to zip.
2. Right-click the file or folder, click “Send to” in the menu that pops up, and then select “Compressed (zipped) folder.”
3. Name the compressed folder something that is descriptive of the content—such as including your name and the date of the transfer.
4. If the compressed item is small enough to email, attach it and email it to the archivist you’ve been working with. If it is too large, upload it to the link provided to you by the archivist and let the archivist know you’ve uploaded it.
   1. Note: the Archivist receiving the materials must create a folder in OneDrive that has edit permissions for non-WVU users. The URL for this folder should then be sent to the donor.

##### **Apple Users**

1. Locate the file or folder that you want to zip.
2. Control-click it or tap it using two fingers, then choose Compress from the shortcut menu.
3. If you compress a single item, the compressed file has the name of the original item with the .zip extension. If you compress multiple items at once, the compressed file is called Archive.zip. Rename the compressed folder something that is descriptive of the content—such as including your name and the date of the transfer.
4. If the compressed item is small enough to email, attach it and email it to the archivist you’ve been working with. If it is too large, upload it to the link provided to you by the archivist and let the archivist know you’ve uploaded it.
   1. Note: the Archivist receiving the materials must create a folder in OneDrive that has edit permissions for non-WVU users. The URL for this folder should then be sent to the donor.

### **Procedures Upon Arrival to WVRHC**

1. Once the content has been deposited to a shared space or sent via email, add information about the transfer to the digital media inventory for the collection or accession, found in the Administration folder for the collection or accession. If there is no folder for the collection or accession, consult the [Born-Digital Materials Accessioning procedures](https://westvirginiauniversity.sharepoint.com/:w:/s/DigitalArchivesWork/ETljOmkUl2VGoHNqB1Ot9GgBhdrrmogHlk6Tzr8b5FhzwA?e=Q5BMeF) to create a folder.
2. Create two folders on the desktop using the media item’s identifier identified in the digital media inventory: identifier\_content and identifier\_metadata. The word “identifier” should be the identifier for the item, not the word identifier. Example: 2828\_disc\_1\_content
3. Download the .zip file to your desktop.
4. Unzip the file by selecting the .zip file, clicking the **Extract/Compressed Folder Tools** (boxed in red on the left)option on the toolbar at the top and then selecting **Extract All**. Extract the content to the identifier\_content folder on the desktop.



1. Run the following command on the command line, being sure that the input directory is the identifier\_content folder and the output directory is the identifier\_metadata folder.
   1. brunnhilde.py -b -z --ssn\_mode=2 [input directory, or content folder for item] [output directory, or File Metadata folder for item]
   2. Example: brunnhilde.py -b -z --ssn\_mode=2 C:\Working Files\2828\_disc\_1\_content C:\Working Files\2828\_disc\_1\_metadata
   3. **Note:** if an item is flagged as a virus by ClamAV (visible on the command line output), contact the Digital Archivist with the identifier for the item and immediately delete all content on the desktop and empty the Recycling Bin. Update the PREMIS spreadsheet in the Administrative folder within the folder for the collection or accession to include the event of Quarantine (if necessary) for the item. Do not continue to any additional steps.
2. Move the identifier\_content folder to the Content folder for the collection or accession and the identifier\_metadata folder to the Metadata folder within the Administration folder within the accession or collection folder using the [TeraCopy instructions](#_TeraCopy). Remove \_content and \_metadata from the folder names.
3. Update the PREMIS spreadsheet in the Administrative folder within the folder for the collection or accession to include the events for Brunnhilde report, Replication, and/or Quarantine (if necessary) for the item.

## **CDs and DVDs**

The method of extracting content from CDs and DVDs varies depending on the format and method of saving data on the disc. For instance, CD-DA, or compact disk digital audio, has a higher error rate and therefore requires specialized software for transferring files. A disk image will copy with a higher rate of error due to the format. Optical media may require multiple attempts to accurately acquire content, possibly using multiple drives to access content.

To determine what type of CD or DVD you have to select from the CD-DA or All Other CD and DVD Formats workflows, follow the [Identifying the Format of a Disc](#_Identifying_the_Format) instructions. Then, follow the instructions in the applicable section.

If content acquisition for an item is unsuccessful or duplicate media items within a single collection are present, forward the identifiers for these materials to the Digital Archivist.

### **CD-DA**

|  |  |
| --- | --- |
| **Software** | Exact Audio Copy, Teracopy, Brunnhilde |
| **Hardware** | External CD/DVD drive |

1. Insert the disc into the external USB CD/DVD drive.
2. Create two folders on the desktop using the media item’s identifier identified in the digital media inventory: identifier\_content and identifier\_metadata. The word “identifier” should be the identifier for the item, not the word identifier. Example: 2828\_disc\_1\_content
3. Follow the [Exact Audio Copy](#_Exact_Audio_Copy) instructions.
4. Once all content has been transferred to the identifier\_content and identifier\_metadata folders, run the following command on the command line, being sure that the input directory is the identifier\_content folder and the output directory is the identifier\_metadata folder.
   * brunnhilde.py -b -z --ssn\_mode=2 [input directory, or content folder for item] [output directory, or File Metadata folder for item]
   * Example: brunnhilde.py -b -z --ssn\_mode=2 C:\Working Files\2828\_disc\_1\_content C:\Working Files\2828\_disc\_1\_metadata
   * **Note:** if an item is flagged as a virus by ClamAV (visible on the command line output), contact the Digital Archivist with the identifier for the item and immediately delete all content on the desktop and empty the Recycling Bin. Update the PREMIS spreadsheet in the Administrative folder within the folder for the collection or accession to include the event of Quarantine (if necessary) for the item. Do not continue to any additional steps.
5. Move the identifier\_content folder to the Content folder for the collection or accession and the identifier\_metadata folder to the Metadata folder within the Administration folder within the accession or collection folder using the [TeraCopy instructions](#_TeraCopy). Remove \_content and \_metadata from the folder names.
6. Update the PREMIS spreadsheet in the Administrative folder within the folder for the collection or accession to include the events for Brunnhilde report, Replication, and/or Quarantine (if necessary) for the item.

### **All Other CD and DVD Formats**

|  |  |
| --- | --- |
| **Software** | Teracopy, optionally FTK Imager, Brunnhilde, IsoBuster |
| **Hardware** | External CD/DVD drive |

1. Insert the disc into the external USB CD/DVD drive.
2. Create two folders on the desktop using the media item’s identifier identified in the digital media inventory: identifier\_content and identifier\_metadata. The word “identifier” should be the identifier for the item, not the word identifier. Example: 2828\_disc\_1\_content
3. Next, examine the contents of the disc without opening any files. To access the content of the disc via Windows Explorer, go to **File Explorer**->**This PC**->**Devices and Drives** and select the relevant drive by right clicking on the device or drive and selecting **Open in New Window**. Examine the disc in IsoBuster by following [Viewing a Disk Image or Media Item in IsoBuster](#_Viewing_a_Disc) instructions.
4. If the disc:
   1. Has multiple sessions (visible in IsoBuster)
   2. Has Mac file systems such as Hierarchical File System Plus (HFS+), Hierarchical File System (HFS), or Macintosh File System (MFS)

Use the [FTK Imager instructions to image the disc](#_Imaging_an_Item). For items formatted with multiple drives, be sure to capture each sub-drive with the FTK Imager instructions to image the item.

If the disc:

* 1. Is a DVD video disc (which consists of a folder titled VIDEO\_TS as the primary/only content)

Use the [Isobuster Imaging an Item](#_Imaging_an_Item_1) instructions.

Otherwise, if the content is identical in all file systems in Windows Explorer vs. IsoBuster, follow the [Teracopy](#_TeraCopy) instructions to copy all items from the disc to the identifier\_content folder on the desktop. If the content does not match, follow the [FTK Imager instructions for content extraction](#_Extracting_Content_from) to accomplish the same task.

1. Once all content is in the identifier\_content folder, run the following command on the command line, being sure that the input directory is the identifier\_content folder and the output directory is the identifier\_metadata folder.
   1. brunnhilde.py -b -z --ssn\_mode=2 [input directory] [output directory]
   2. Example: brunnhilde.py -b -z --ssn\_mode=2 C:\Working Files\2828\_disc\_1\_content C:\Working Files\2828\_disc\_1\_metadata
   3. **Note:** if an item is flagged as a virus by ClamAV (visible on the command line output), contact the Digital Archivist with the identifier for the item and immediately delete all content on the desktop and empty the Recycling Bin. Update the PREMIS spreadsheet in the Administrative folder within the folder for the collection or accession to include the event of Quarantine (if necessary) for the item. Do not continue to any additional steps.
2. Move the identifier\_content folder to the Content folder for the collection or accession and the identifier\_metadata folder to the Metadata folder within the Administration folder within the accession or collection folder using the [TeraCopy instructions](#_TeraCopy). Remove \_content and \_metadata from the folder names.
3. Update the PREMIS spreadsheet in the Administrative folder within the folder for the collection or accession to include the events for Brunnhilde report, Imaging (if necessary), Replication (if necessary), and/or Quarantine (if necessary) for the item.

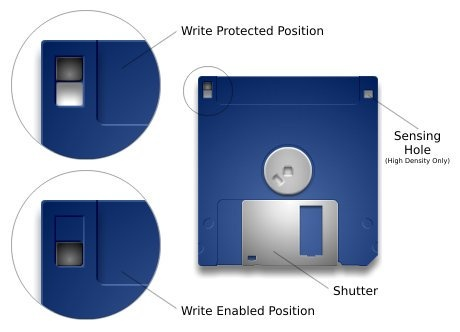
## **3.5 inch floppy disks**

Floppy disks are a notoriously temperamental format. Exploration of other hardware and software for imaging floppy disks, such as those used by KryoFlux or usage of a contemporary 3.5 inch floppy drive, may be explored in the future to improve content capture results. This workflow is meant to serve as an initial “first pass” for floppy disks in WVRHC collections.

If content acquisition for an item is unsuccessful or duplicate media items within a single collection are present, forward the identifiers for these materials to the Digital Archivist.

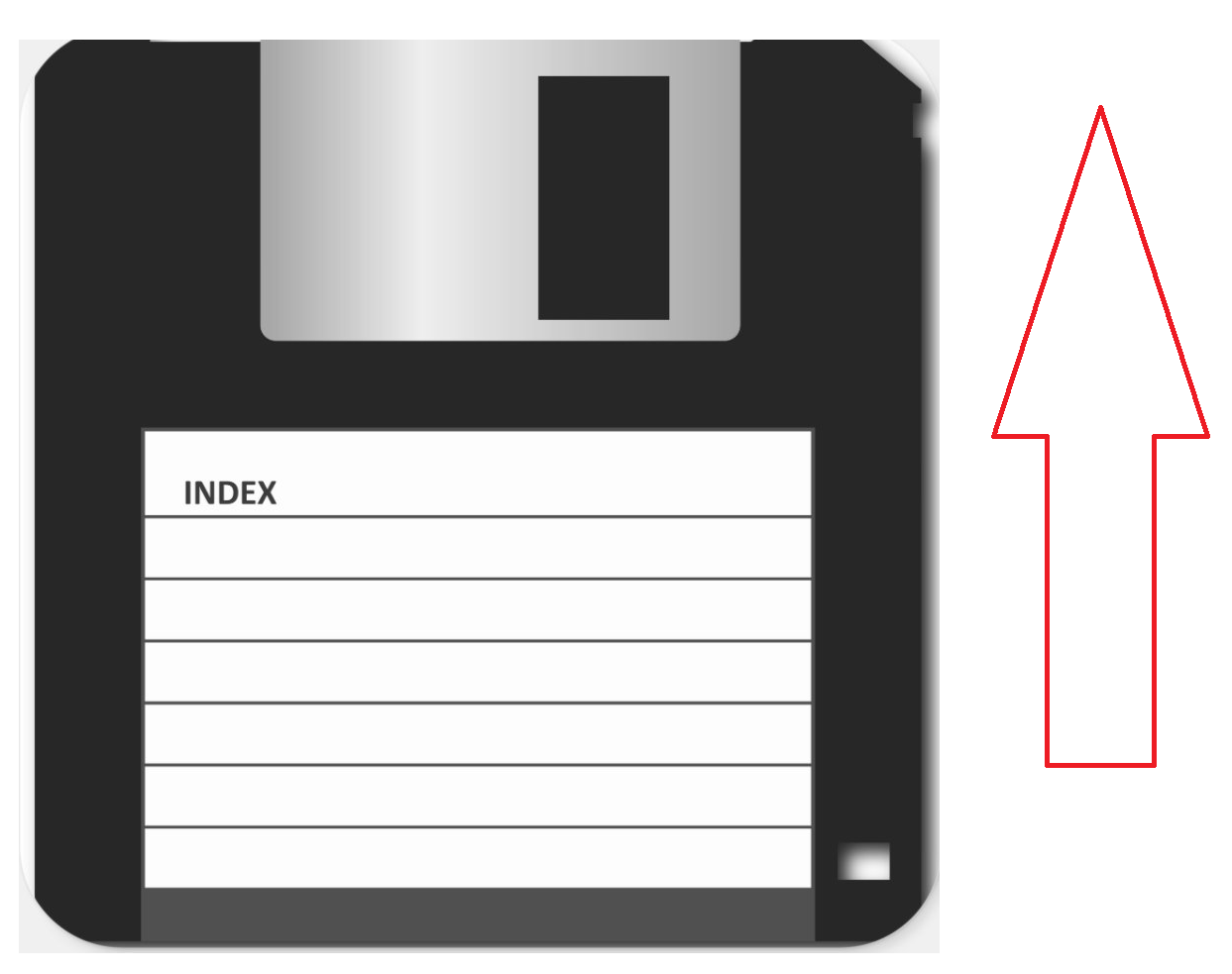
|  |  |
| --- | --- |
| **Software** | FTK Imager, IsoBuster, Brunnhilde, TeraCopy |
| **Hardware** | USB Floppy disk drive |

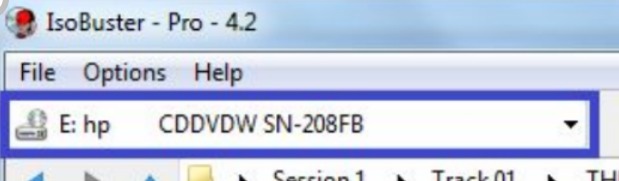
1. Write protect the floppy disk by sliding the tab to uncover the hole on the corner of the floppy disk opposite the shutter. An example of the write protected position can be seen in the top left zoomed in image below.

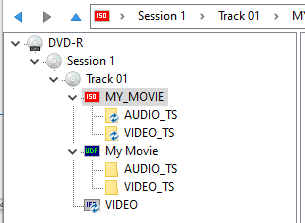


*Image from* [*3.5” Floppy Disks*](https://uisapp2.iu.edu/confluence-prd/pages/viewpage.action?pageId=623051010)

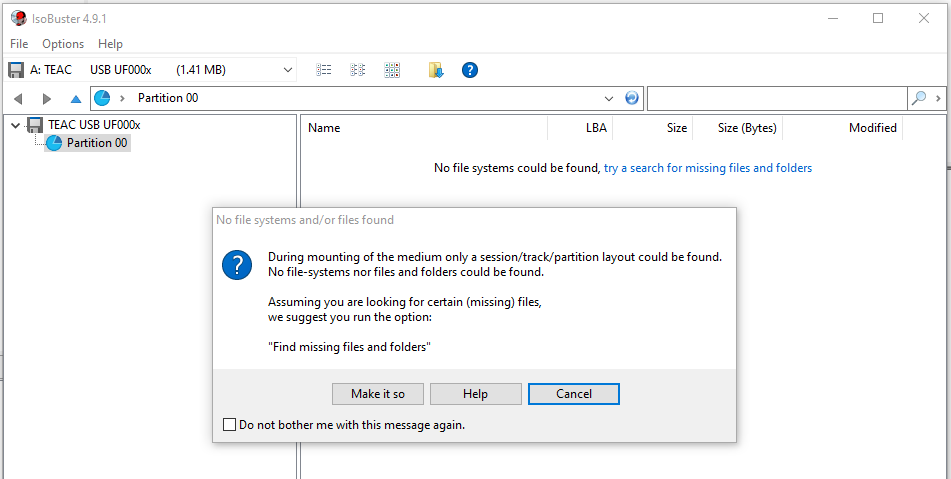
1. Plug in the USB floppy disk drive. Insert the floppy disk into the drive with the label side up and metal bracket first, as seen in the following image.



1. Create two folders on the desktop using the media item’s identifier identified in the digital media inventory: identifier\_content and identifier\_metadata. The word “identifier” should be the identifier for the item, not the word identifier. Example: 2828\_disc\_1\_content
2. Open IsoBuster. Use the dropdown in the upper left corner (shown boxed in blue below) to select the correct drive. For floppy disks this is usually the A: drive.
   1. 
3. Once the A: or other relevant drive is selected, IsoBuster will begin to read the item. If you see a list of files and/or file systems appear on the left pane (example below of a DVD), follow [FTK Imager instructions](#_FTK_Imager) to image the disk and skip to the “If content was retrievable” section after step 6.



1. If you see the below popup instead, skip to the “If content was unretrievable” section after this step.



If content was retrievable:

1. Once all content is in the identifier\_content folder, run the following command on the command line, being sure that the input directory is the identifier\_content folder and the output directory is the identifier\_metadata folder.
   1. brunnhilde.py -b -z --ssn\_mode=2 [input directory] [output directory]
   2. Example: brunnhilde.py -b -z --ssn\_mode=2 C:\Working Files\2828\_disc\_1\_content C:\Working Files\2828\_disc\_1\_metadata
   3. **Note:** if an item is flagged as a virus by ClamAV (visible on the command line output), contact the Digital Archivist with the identifier for the item and immediately delete all content on the desktop and empty the Recycling Bin. Update the PREMIS spreadsheet in the Administrative folder within the folder for the collection or accession to include the event of Quarantine (if necessary) for the item. Do not continue to any additional steps.
2. Move the identifier\_content folder to the Content folder for the collection or accession and the identifier\_metadata folder to the Metadata folder within the Administration folder within the accession or collection folder using the [TeraCopy instructions](#_TeraCopy). Remove \_content and \_metadata from the folder names.
3. Update the PREMIS spreadsheet in the Administrative folder within the folder for the collection or accession to include the events for Brunnhilde report, Imaging, and/or Quarantine (if necessary) for the item.

If content was unretrievable:

If content acquisition for an item is unsuccessful, record a failure for the Imaging event in the PREMIS spreadsheet.

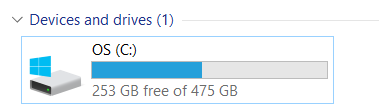
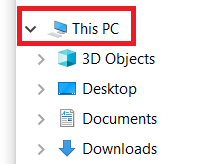
## **Thumb drives, internal hard drives, external hard drives, and memory cards**

Though each of the physical formats described here use the same software for content acquisition, the hardware needed to access that content differs significantly.

If content acquisition for an item is unsuccessful or duplicate media items within a single collection are present, forward the identifiers for these materials to the Digital Archivist.

**Note:** Some thumb and hard drives may be too large to simply save to the desktop as in other procedures. In that case, contact the Digital Archivist and they will arrange an external hard drive for use in accessioning and processing.

* To determine the size of the item’s drive and the computer:
  + Follow the [Tableau instructions](#_Tableau_Forensic_Bridge) to plug in the drive for the item.
  + Go to File Explorer -> This PC -> Devices and Drives



* + Compare the drive space of your computer to the external drive. Your computer will usually be the C: or H: drive. The external drive will usually be labelled with a brand name that is identifiable. In the above example 253GB is available on the computer.
  + If your computer has less space than the external drive, contact the Digital Archivist and move on to the next item.

### **Thumb drives and external hard drives**

|  |  |
| --- | --- |
| **Software** | FTK Imager, TeraCopy, IsoBuster |
| **Hardware** | Tableau Forensic USB 3.0 Bridge |

1. Follow the [Tableau instructions](bookmark://_Tableau_Forensic_Bridge) to plug in the drive for the item.
2. Check that there is sufficient space to process the content using the instructions in the beginning of the [Thumb drives, internal hard drives, external hard drives, and memory cards](#_Thumb_drives,_internal) section.
3. Create two folders on the desktop using the media item’s identifier identified in the digital media inventory: identifier\_content and identifier\_metadata. The word “identifier” should be the identifier for the item, not the word identifier. Example: 2828\_disc\_1\_content
4. Next, examine the contents of the item without opening any files. To access the content of the item via Windows Explorer, go to **File Explorer**->**This PC**->**Devices and Drives** and select the relevant drive by right clicking on the device or drive and selecting **Open in New Window**. Examine the item in IsoBuster by following [Viewing a Disk Image or Media Item in IsoBuster](#_Viewing_a_Disc) instructions.
5. If the disc:
   1. Has multiple sessions (visible in IsoBuster)
   2. Is a DVD video disc (which consists of a folder titled VIDEO\_TS as the primary/only content)
   3. Has Mac file systems such as Hierarchical File System Plus (HFS+), Hierarchical File System (HFS), or Macintosh File System (MFS)
   4. Is formatted as multiple drives that show separately on IsoBuster

Use the [FTK Imager instructions to image the disc](#_Imaging_an_Item). For items formatted with multiple drives, be sure to capture each sub-drive with the FTK Imager instructions to image the item.

Otherwise, if the content is identical in all file systems in Windows Explorer vs. IsoBuster, follow the [Teracopy](#_TeraCopy) instructions to copy all items from the disc to the identifier\_content folder on the desktop. If the content does not match, follow the [FTK Imager instructions for content extraction](#_Extracting_Content_from) to accomplish the same task.

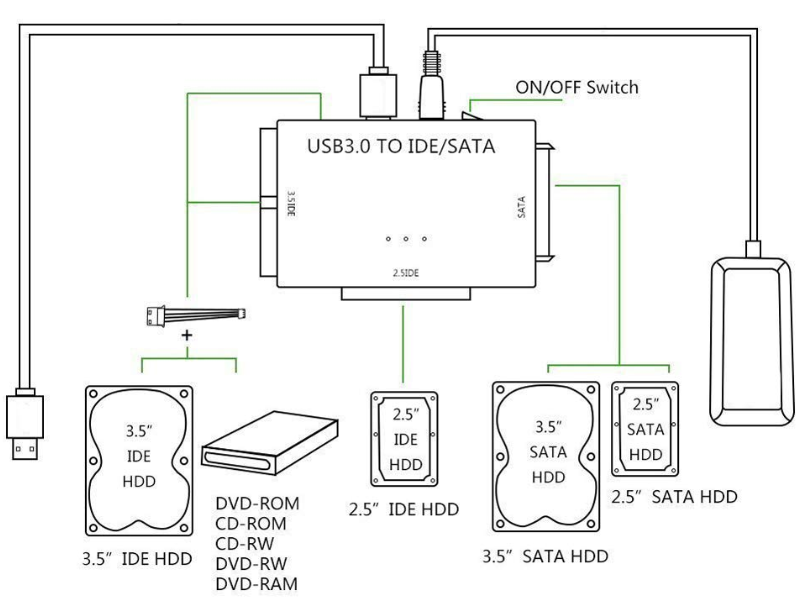
1. Once all content is in the identifier\_content folder, run the following command on the command line, being sure that the input directory is the identifier\_content folder and the output directory is the identifier\_metadata folder.
   1. brunnhilde.py -b -z --ssn\_mode=2 [input directory] [output directory]
   2. Example: brunnhilde.py -b -z --ssn\_mode=2 C:\Working Files\2828\_disc\_1\_content C:\Working Files\2828\_disc\_1\_metadata
   3. **Note:** if an item is flagged as a virus by ClamAV (visible on the command line output), contact the Digital Archivist with the identifier for the item and immediately delete all content on the desktop and empty the Recycling Bin. Update the PREMIS spreadsheet in the Administrative folder within the folder for the collection or accession to include the event of Quarantine (if necessary) for the item. Do not continue to any additional steps.
2. Move the identifier\_content folder to the Content folder for the collection or accession and the identifier\_metadata folder to the Metadata folder within the Administration folder within the accession or collection folder using the [TeraCopy instructions](#_TeraCopy). Remove \_content and \_metadata from the folder names.
3. Update the PREMIS spreadsheet in the Administrative folder within the folder for the collection or accession to include the events for Brunnhilde report, Imaging (if necessary), Replication (if necessary), and/or Quarantine (if necessary) for the item.

### **Internal hard drives**

Currently, SATA (2.5 and 3.5 inch) and IDE (2.5 and 3.5 inch) connections are supported for internal hard drives.

|  |  |
| --- | --- |
| **Software** | FTK Imager, TeraCopy, IsoBuster |
| **Hardware** | Tableau Forensic USB 3.0 Bridge, SATA and IDE adapter |

1. Follow the [Tableau instructions](bookmark://_Tableau_Forensic_Bridge) to plug in the drive for the item.
2. Check that there is sufficient space to process the content using the instructions in the beginning of the [Thumb drives, internal hard drives, external hard drives, and memory cards](#_Thumb_drives,_internal) section.
3. Connect the hard drive to the computer as follows: the below configuration shows how to use the adapter kit to connect the hard drive to the adapter. The setup below will then be connected to the Tableau Forensic USB 3.0 Bridge. Use the [Tableau Forensic USB 3.0 Bridge instructions](#_Tableau_Forensic_Bridge) to correctly connect the hard drive adapter to the Tableau and the computer.



*Illustration taken from documentation for the adapter demonstrating the connection*

*configurations for IDE and SATA drives.*

1. Create two folders on the desktop using the media item’s identifier identified in the digital media inventory: identifier\_content and identifier\_metadata. The word “identifier” should be the identifier for the item, not the word identifier. Example: 2828\_disc\_1\_content
2. Use the [FTK Imager instructions to image the drive](#_Imaging_an_Item).
   1. **Note:** Some items, particularly hard drives, may be formatted as multiple drives that show separately. For these items, be sure to capture each sub-drive with[FTK Imager instructions to image the drive](#_Imaging_an_Item).
3. Once all content is in the identifier\_content folder, run the following command on the command line, being sure that the input directory is the identifier\_content folder and the output directory is the identifier\_metadata folder.
   1. brunnhilde.py -b -z --ssn\_mode=2 [input directory] [output directory]
   2. Example: brunnhilde.py -b -z --ssn\_mode=2 C:\Working Files\2828\_disc\_1\_content C:\Working Files\2828\_disc\_1\_metadata
   3. **Note:** if an item is flagged as a virus by ClamAV (visible on the command line output), contact the Digital Archivist with the identifier for the item and immediately delete all content on the desktop and empty the Recycling Bin. Update the PREMIS spreadsheet in the Administrative folder within the folder for the collection or accession to include the event of Quarantine (if necessary) for the item. Do not continue to any additional steps.
4. Move the identifier\_content folder to the Content folder for the collection or accession and the identifier\_metadata folder to the Metadata folder within the Administration folder within the accession or collection folder using the [TeraCopy instructions](#_TeraCopy). Remove \_content and \_metadata from the folder names.
5. Update the PREMIS spreadsheet in the Administrative folder within the folder for the collection or accession to include the events for Brunnhilde report, Imaging (if necessary), Replication (if necessary), and/or Quarantine (if necessary) for the item.

### **Memory cards**

There are many types of memory cards and each requires a different type of card reader. At the WVRHC we have two card readers that support multiple types of memory cards.

If content acquisition for an item is unsuccessful or duplicate media items within a single collection are present, forward the identifiers for these materials to the Digital Archivist.

|  |  |
| --- | --- |
| **Software** | FTK Imager, TeraCopy, IsoBuster |
| **Hardware** | Tableau Forensic USB 3.0 Bridge, all-in-one memory card readers |

1. Follow the [Tableau instructions](bookmark://_Tableau_Forensic_Bridge) to plug in the drive for the item.
2. Check that there is sufficient space to process the content using the instructions in the beginning of the [Thumb drives, internal hard drives, external hard drives, and memory cards](#_Thumb_drives,_internal) section.
3. Create two folders on the desktop using the media item’s identifier identified in the digital media inventory: identifier\_content and identifier\_metadata. The word “identifier” should be the identifier for the item, not the word identifier. Example: 2828\_disc\_1\_content
4. Next, examine the contents of the item without opening any files. To access the content of the item via Windows Explorer, go to **File Explorer**->**This PC**->**Devices and Drives** and select the relevant drive by right clicking on the device or drive and selecting **Open in New Window**. Examine the item in IsoBuster by following [Viewing a Disk Image or Media Item in IsoBuster](#_Viewing_a_Disc) instructions.
5. If the disc:
   1. Has multiple sessions (visible in IsoBuster)
   2. Is a DVD video disc (which consists of a folder titled VIDEO\_TS as the primary/only content)
   3. Has Mac file systems such as Hierarchical File System Plus (HFS+), Hierarchical File System (HFS), or Macintosh File System (MFS)
   4. Is formatted as multiple drives that show separately on IsoBuster

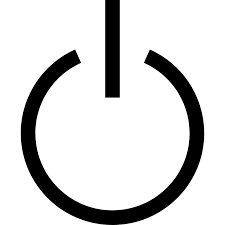
Use the [FTK Imager instructions to image the disc](#_Imaging_an_Item). For items formatted with multiple drives, be sure to capture each sub-drive with the FTK Imager instructions to image the item.

Otherwise, if the content is identical in all file systems in Windows Explorer vs. IsoBuster, follow the [Teracopy](#_TeraCopy) instructions to copy all items from the disc to the identifier\_content folder on the desktop. If the content does not match, follow the [FTK Imager instructions for content extraction](#_Extracting_Content_from) to accomplish the same task.

1. Once all content is in the identifier\_content folder, run the following command on the command line, being sure that the input directory is the identifier\_content folder and the output directory is the identifier\_metadata folder.
   1. brunnhilde.py -b -z --ssn\_mode=2 [input directory] [output directory]
   2. Example: brunnhilde.py -b -z --ssn\_mode=2 C:\Working Files\2828\_disc\_1\_content C:\Working Files\2828\_disc\_1\_metadata
   3. **Note:** if an item is flagged as a virus by ClamAV (visible on the command line output), contact the Digital Archivist with the identifier for the item and immediately delete all content on the desktop and empty the Recycling Bin. Update the PREMIS spreadsheet in the Administrative folder within the folder for the collection or accession to include the event of Quarantine (if necessary) for the item. Do not continue to any additional steps.
2. Move the identifier\_content folder to the Content folder for the collection or accession and the identifier\_metadata folder to the Metadata folder within the Administration folder within the accession or collection folder using the [TeraCopy instructions](#_TeraCopy). Remove \_content and \_metadata from the folder names.
3. Update the PREMIS spreadsheet in the Administrative folder within the folder for the collection or accession to include the events for Brunnhilde report, Imaging (if necessary), Replication (if necessary), and/or Quarantine (if necessary) for the item.

# **Hardware Workflows**

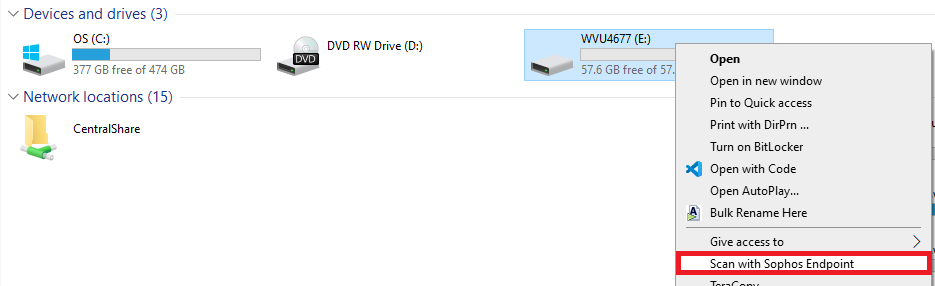
## **Tableau Forensic Bridge**

1. With the Tableau Forensic Bridge turned off, plug in the external device or adapter for the external device you wish to write protect into the USB port.
2. Connect the Tableau to the workstation with the blue USB 3.0 cable.
3. Connect the two black power cables together and then attach the power cable to the Tableau and then plug the cable into an outlet.
4. Power on the Tableau using the power button, which features the following symbol.
   1. 
5. The lights on the right side of the forensic bridge will indicate the power, connection to the device and workstation, and indicate that write-blocking is activated.
6. The external device will appear in Windows File Manager.
7. When data on the device is read, the 'Activity' light will glow red.

# **Software Workflows**

## **FTK Imager**

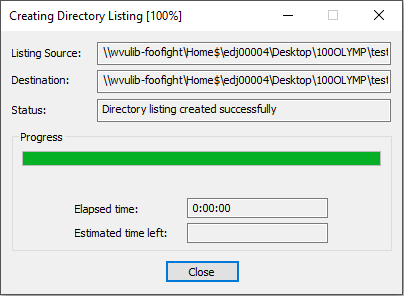
### **Imaging an Item**

1. Conduct a virus scan on the item. To do this via Windows Explorer, go to **File Explorer**->**This PC**->**Devices and Drives**, right click on the drive, and select **Scan with Sophos Endpoint.** You should receive a notification that no viruses were found—if so, continue. If there were viruses found, note the name(s) and the item identifier and return the item to the Digital Archivist. 
2. Open FTK Imager. The FTK Imager icon is located on the desktop and named AccessData FTK Imager.
3. Click **File** then select **Create Disk Image..** from the dropdown.
4. Select the **Source Evidence Type**. For typical purposes, select **Logical Drive.**

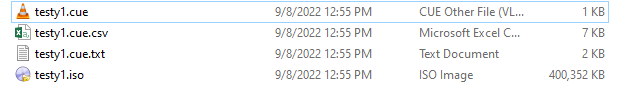
Note: The choice of source evidence type depends on context of acquisition, including whether environment and file structure matter.

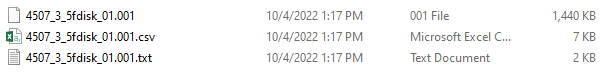
|  |  |
| --- | --- |
| Source Evidence Type | Reasoning |
| Physical Drive | Captures every sector of the physical media including hidden and deleted files. Requires the most imaging time and storage space |
| Logical Drive | Acquires image of a single logical volume (e.g. C:\). Does not capture hidden and deleted files. This is the only available option for optical media. |
| Contents of a Folder | Acquires a logical image of a specific folder’s contents |

1. Select the **Source Drive** from the dropdown menu. The actual text will vary based on the item being imaged. For instance, a thumb drive may appear as: \\.\PHYSICALDRIVE1 - MUSHKIN MKNUFDVS64GB USB Device, indicating that the item is a 64GB USB drive, or a floppy disk might simply appear as A:\ Click **Finish.**
2. In the **Image Destination(s)** window, click **Add...** Select **Raw (dd)** as the **Destination Image Type.** Click **Next.**
3. In the **Evidence Item Information** window, populate the fields as follows:
   1. Case Number – accession or archives and manuscript number
   2. Evidence Number – identifier for the item
   3. Unique Description – If desired, enter a brief description of the media and/or its annotations (e.g., '3.5" floppy disk labelled "FOA Photos 2002"')
   4. Examiner – name of person creating the image
   5. Notes – leave blank
4. FTK Imager will now ask you for information about where to save the resulting disk image and metadata files. Enter the following and then select **Finish**:
   1. Image destination folder: Select the identifier\_content folder on the desktop.
   2. Image filename: Enter the item's identifier.
5. Double-check to make sure that the Image Destination and settings appear correct. Click **Start** to begin the disk imaging process.
   1. These options will be checked by default when acquiring a logical image. You don’t need to change anything:
      1. Verify images after they are created
      2. Precalculate Progress Statistics
      3. Create directory listings of all files in the image after they are created
6. A dialogue box with progress bar and elapsed time will pop up and remain up once the image is successfully created (see pop up below) or the imager fails. **If the imager fails or seems to get hung up on a large number of bad sectors (aka the image progress bar fails to continue):** Document the failure in the PREMIS Spreadsheet for the collection that the Imaging event failed for FTK Imager. Forward the identifier to the Digital Archivist with information about the failure.



1. Close the remaining windows and go to the identifier\_content folder on the desktop where you saved the items. You will see three or four files depending on the input format:

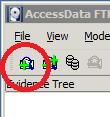




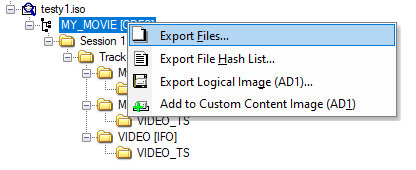
* 1. .iso or .001 - the disk image file for the item. This is a disk image for a disc rather than a hard drive, so it appears as an .iso. Other items may appear as .001
  2. .cue.csv - list of files present in the disk image.
  3. .cue.txt - text file representing the structure of the disk
  4. .cue - used only for CD or DVD items, additional information about the structure of the compact disc

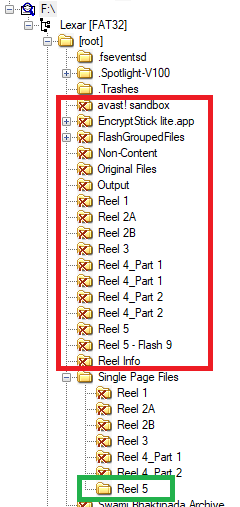
1. Move the files ending in .cue, .cue.csv, and .cue.txt to the identifier\_metadata folder on the desktop.

### **Viewing a Disk Image or Media Item**

1. Click **File**, then **Add Evidence Item**. Or click on the “Add Evidence Item” icon
2. From the dialogue box that appears, select one of the sequences below.
   1. Physical Drive – View the entire drive, which can include multiple logical drives. This is only really necessary to verify internal and external hard drives do not have multiple logical drives that should be imaged or examined separately.
   2. Logical Drive – For most media and for all optical media choose Logical Drive.
   3. Image File – To view a disk image.
   4. Contents of a Folder – Self explanatory.
3. Follow the prompts for the relevant selection. This may include selecting the physical or logical drive you’d like to view or selecting the disk image file.
4. In the upper left Evidence Tree pane you can explore the file system(s) of the mounted evidence item by clicking on plus symbols to expand folders.
5. Clicking on a folder will display its contents in the File List pane (top right) and Hex Viewer pane (bottom right).
6. Clicking on a file in the File List pane (top right) will display its text contents in the Hex Viewer pane (bottom right).

**Extracting Content from a Disk Image or Media Item**

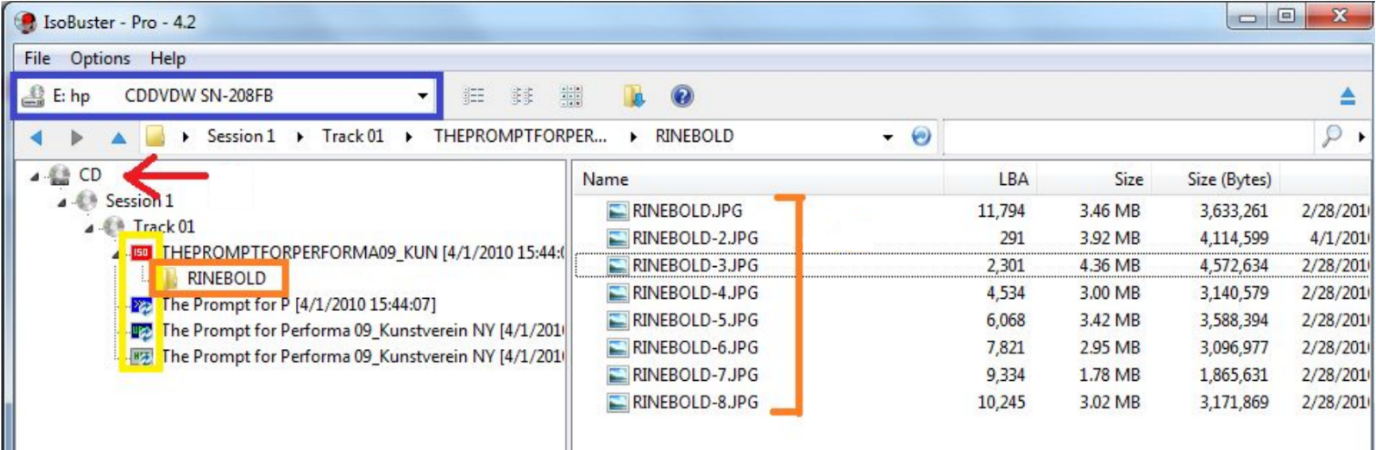
1. To extract content from a disk image, first follow the directions to [View a Disk Image or Media Item.](#_Viewing_a_Disk)
2. For disk image files, navigate to the top level folder or file you would like to extract. This might be the [root] folder. Right click on the folder or file and select **Export Files...** Optionally, you can extract a directory listing with checksums for each file using **Export File Hash List...**
   1. 
3. For logical drives, navigate to the top level folder or file you would like to extract. Right click on the folder or file and select **Export Files...** Export files to the identifier\_content folder. NOTE: Be sure to ignore any system folders (like .fseventsd or .Trashes) and any folders with a red x over them (seen boxed in red below). These folders contain deleted materials and should not be removed from the original media unless explicit donor permission to recover media has been granted. Only grab folders that are simply a folder icon with content that does not have a red x (seen boxed in green below). If there is a significant amount of deleted content that makes it hard to navigate, consider making a logical disk image and then extracting content from the image file.



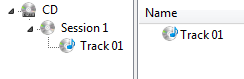
## **IsoBuster**

### **Identifying the Format of a Disc**

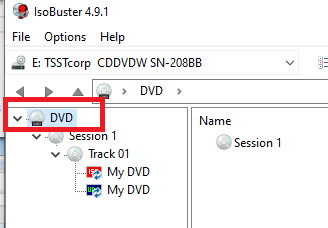
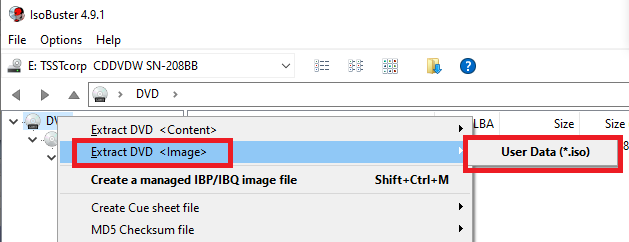
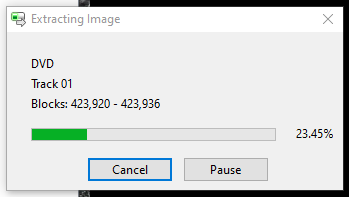
1. Insert the disk into the CD/DVD drive and open IsoBuster.
2. In the drop-down menu on top (outlined by the blue box in the image below, image from Annie Schweikert), select the disc drive you are using. This is D: if you are using an internal disc drive but will vary if using an external disc drive. Once the disc drive is selected, the disc’s directory structure will appear in the left-hand menu.
   1. The red arrow indicates the type of disc. You can navigate through the disc structure by clicking on the directories in the left menu. The contents of the active directory (the one you most recently clicked on, marked in orange on the right) will appear on the right. In the below view, the directory “RINEBOLD” (in orange box on left) is active, and the right side displays the contents of that directory. The yellow box contains the file systems present on the disc.



1. If the type of disc indicates CD or CD-DA, only contains audio files (see example audio icon next to “Track 01” below), only contains one session (see example below) and contains no filesystems, follow the [instructions for CD-DA](#_CD-DA). Otherwise, follow the instructions for [All Other CD and DVD Formats.](#_All_Other_CD)

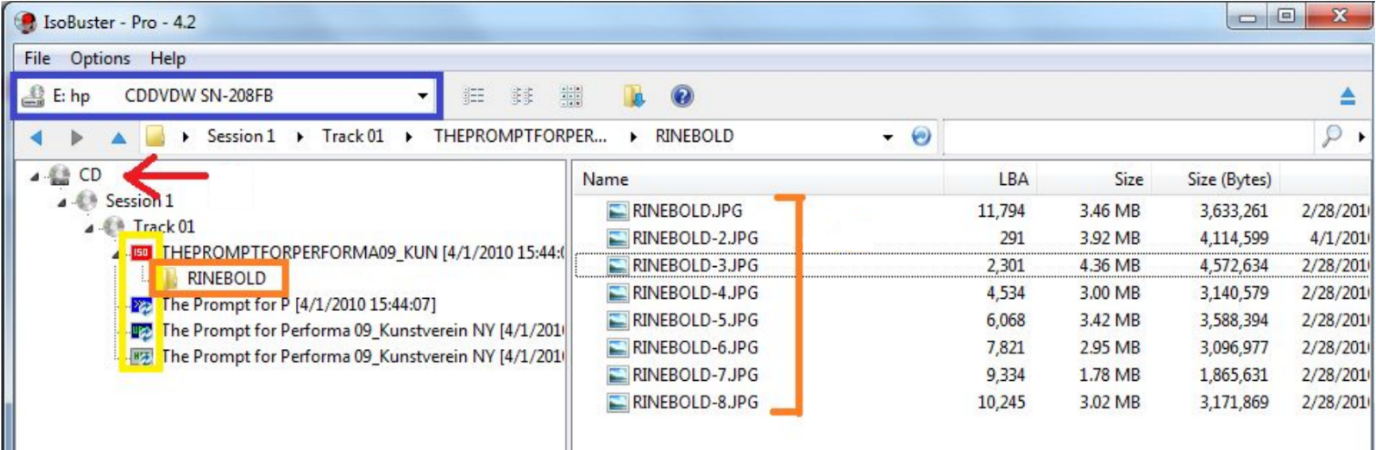


### **Imaging an Item**

1. Open IsoBuster. Click on the top level **DVD** directory (boxed in red below) and make sure it is highlighted in blue. Be sure you select the **DVD** directory—selecting a session or track will only image those portions of the DVD.
   1. 
2. Right click on the **DVD** directory. Select **Extract DVD <Image>** and click **User Data (\*.iso)** (both boxed in red below).
   1. 
3. In the **Save** dialog box that pops up, direct the file to save to the identifier\_content folder on your desktop. The following popup will appear and show your progress:
   1. 
4. Move the .cue and .md5 files in the identifier\_content folder to the identifier\_metadata folder on the desktop.

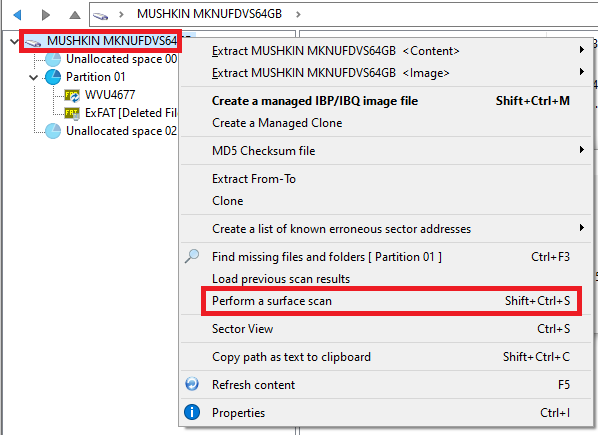
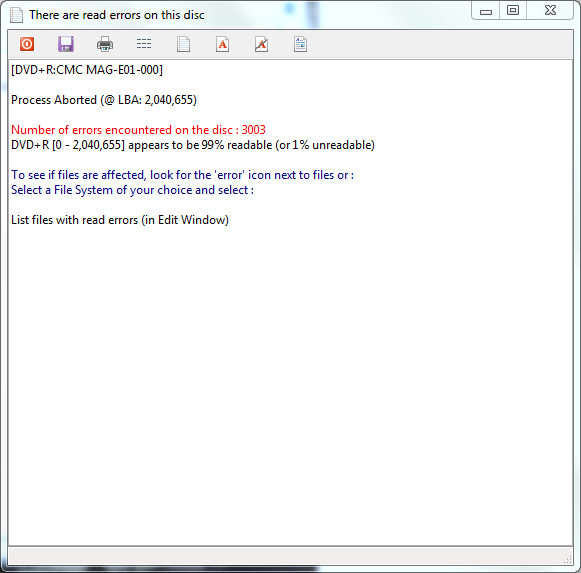
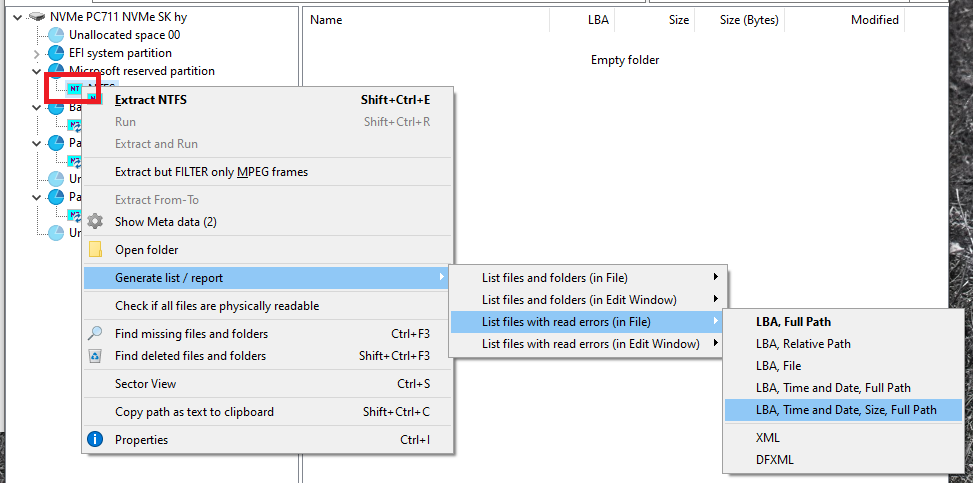
### **Viewing a Disk Image or Media Item**

1. Open IsoBuster. If you are viewing a media item, continue to step two. If you are viewing a disk image, click **File** -> **Open Image File** and select your image file.
2. If viewing an item directly, in the drop-down menu on top (outlined by the blue box in the image below), select the drive you are using. Once the disc drive is selected, the disc’s directory structure will appear in the left-hand menu.
   1. The red arrow indicates the type of item. You can navigate through the disc structure by clicking on the directories in the left menu. The contents of the active directory (the one you most recently clicked on, marked in orange on the right) will appear on the right. In the below view, the directory “RINEBOLD” (in orange box on left) is active, and the right side displays the contents of that directory. The yellow box contains the file systems present on the disc.



**Troubleshooting Potential Errors**

Troubleshooting steps for reading an item might include:

1. Conducting a surface scan by right clicking on the media item in IsoBuster and selecting **Perform a surface scan** (see below).
   1. 
2. After the scan is done, IsoBuster gives you more information on the state of your item. If everything’s good, the message “No physical errors encountered. Your -item\_type- is still in good shape.” will show up. Otherwise, IsoBuster generates a report showing you the readability of the disk (in percentage). Use the floppy disk icon to save the report to the identifier\_metadata folder.
   1. 
3. You can launch a more detailed report by right-clicking on the File System Icon (boxed in red) **-> Generate list/report -> List files with read errors (in File) -> LBA, Time and Date, Size, Full Path.** Save the report in the identifier\_metdata folder for the item.
4. Depending on the results from the two previous analysis, you can either proceed to the extraction of the disk image or identify that the item cannot be disk imaged in the PREMIS spreadsheet. Save the errors logs to the identifier\_metadata folder on the desktop and be sure to save the logs to the Metdata folder for the collection in a folder named with the item’s identifier.

## **HFS Explorer**

http://www.catacombae.org/hfsexplorer/

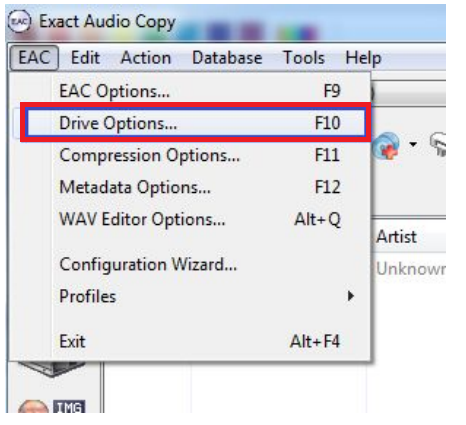
For mac stuff

To explore in the future when mac file systems are encountered

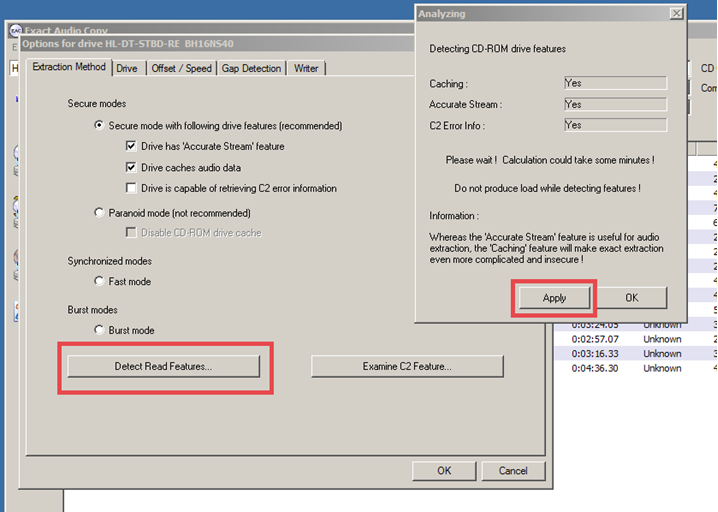
## **Exact Audio Copy**

### **Extracting Content**

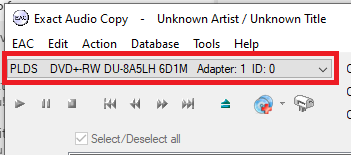
1. Open Exact Audio Copy.
2. Confirm **Secure Mode** by selecting **EAC** and then **Drive Options** from the dropdown. Secure mode must be confirmed at the beginning of each imaging session but does not need to be confirmed between discs.



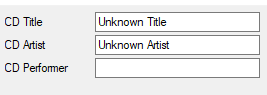
1. A warning may appear notifying you that secure mode options depend on your CD-ROM drive. Select **OK** and proceed.
2. Select **Detect Read Features…** A window will appear and detect CD-ROM drive features. Once the analysis is complete select **Apply** at the bottom of the window (see screenshot below). Select **OK** if necessary.



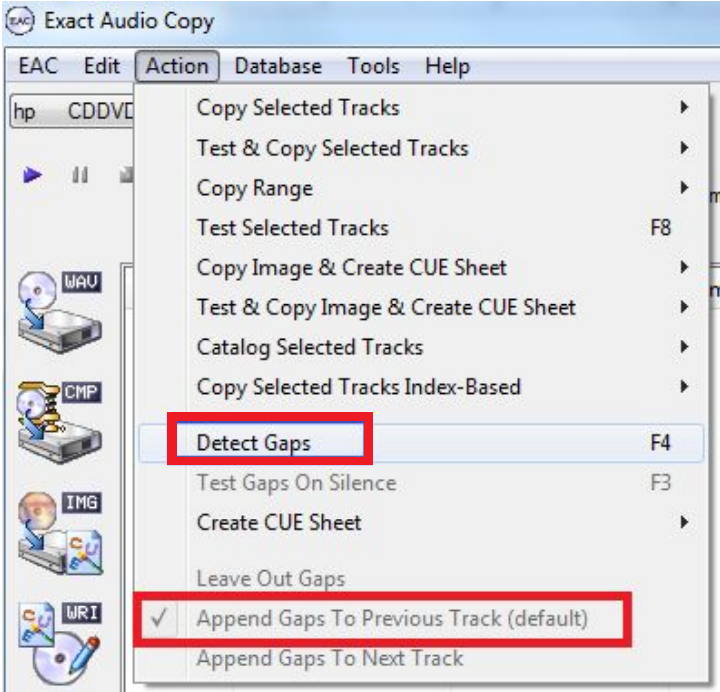
1. In the drop-down menu at the top of the program (outlined in red below), select the drive you are using. This is usually D: but can be another drive if you are using an external disc drive.



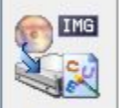
1. Fill in **CD Title** (seen below) with the item’s identifier. Delete the content from **CD Artist.**



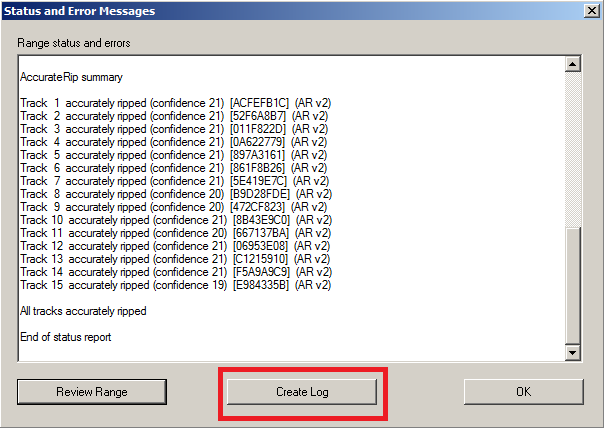
1. Click on the **Action** menu and select **Detect Gaps**. Once detected, Exact Audio Copy should preserve these gaps; make sure “Append gaps to previous track” is checked to enable this (in red). The gaps may represent important timing information in art performances.



1. On the left side menu, select the **Copy Image and Cue Sheet** icon (seen below) and navigate to the identifier\_content folder for storing content.



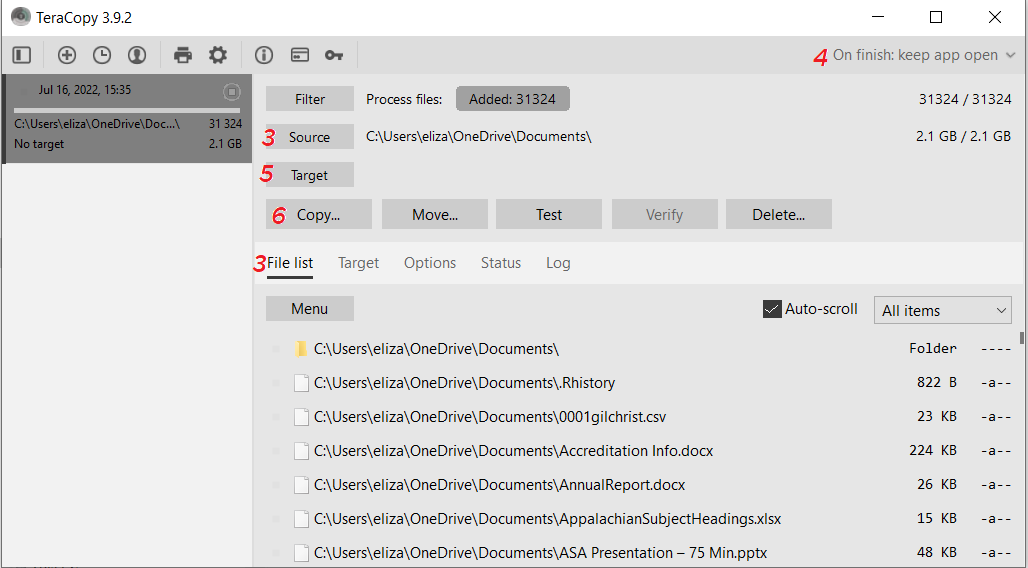
1. Once copying is complete, select **OK.**
2. A dialog box will appear with **Status and Error Messages**. Select **Create Log** at the bottom. Save the log file with item’s identifier in the identifier\_metadata folder for the item.



## **TeraCopy**

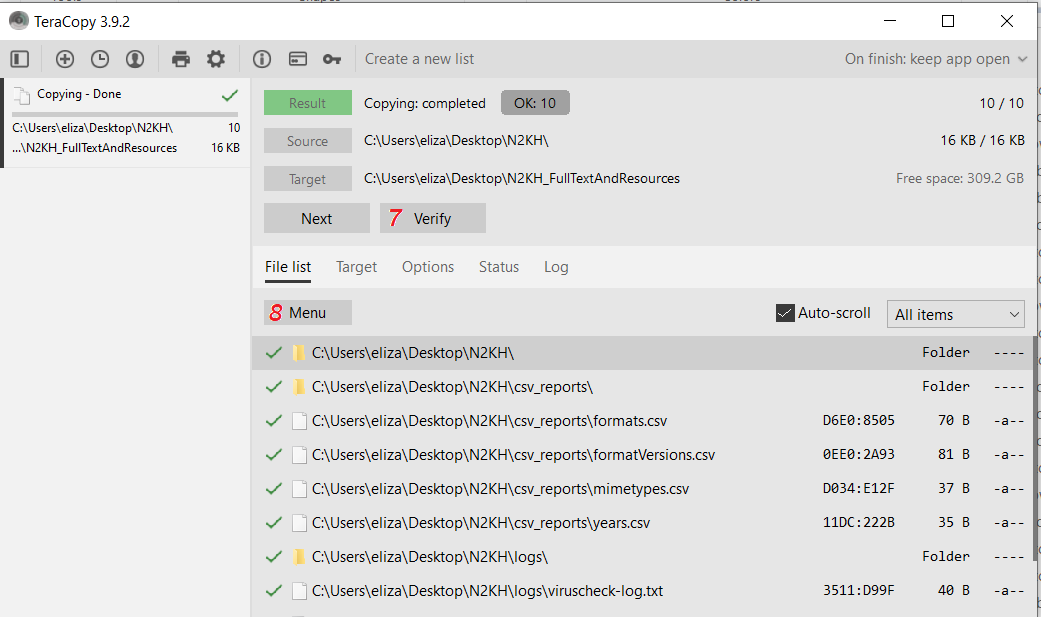
*These instructions are applicable to TeraCopy 3.9.2.*

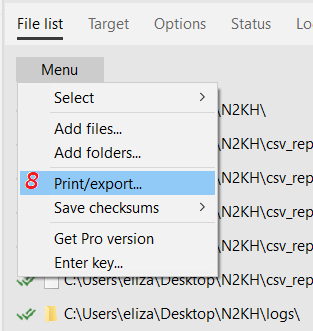
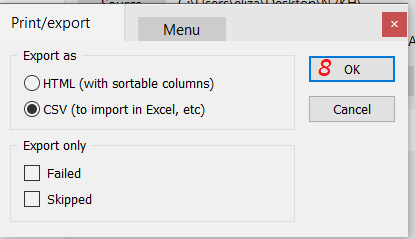
1. Select and right click on the folder(s) or individual files ready for transfer.
2. Select “Teracopy…” and the Teracopy window should automatically open.
   1. If it does not automatically open, search for Teracopy from the start menu and open app. When you open Teracopy your files should be loaded and ready for transfer.
3. Confirm that all selected files and folders you want to move are listed in the File List tab. The directory you plan to move is listed as the “Source.”
4. Check that the dropdown in the upper right corner is set to “On finish: keep app open”.
5. Click the “Target” button. Select the location where you would like to move the files to—this is usually the folder for the media item within the content folder of the folder for the collection on the Z: drive.
6. Click “Copy”.



*The graphic above is a screenshot of TeraCopy. Each number in red corresponds to the steps outlined above and represents a button/area to check or click for steps 3-6. For instance, a red 3 means that the area should be checked in step 3.*

1. Click the “Verify” button to verify the copying process was completed accurately. Click on the Log tab to double check that no errors occurred.
2. After transfer and verification is complete return to the File List tab and click on “Menu” and “Print/export…” and export a CSV file. The CSV File will be in the User/Documents/Teracopy/Reports folder with the file name as the date and time of transfer. Change the CSV file name to A&MNumber\_YYYY-MM-DD\_Log.csv and move the CSV to the logs folder within the administration folder of the folder for the collection on the Z: drive.



*Steps 7 and 8 are marked above in red.*

## **Command Line Tools**

### **Tree**

tree /a [input directory] > [output.txt or output.csv file]. An optional flag of /f may be used after /a (be sure to include a space between) to list all files if desired.

### **Brunnhilde**

brunnhilde.py -b -z --ssn\_mode=2 [input directory, or content folder for collection] [output directory, or File Metadata folder for collection]

Create file manifest by opening the command prompt and run:

Sf -csv [path to media] > [path to Metadata folder]\[CUID].csv

## **Exactly**

<https://www.weareavp.com/wp-content/uploads/2018/06/Exactly-User-Guide_v.0.1.5.pdf>

<https://archives.ncdcr.gov/government/digital-records/north-carolina-digital-repository/bagger-gui-user-guide>