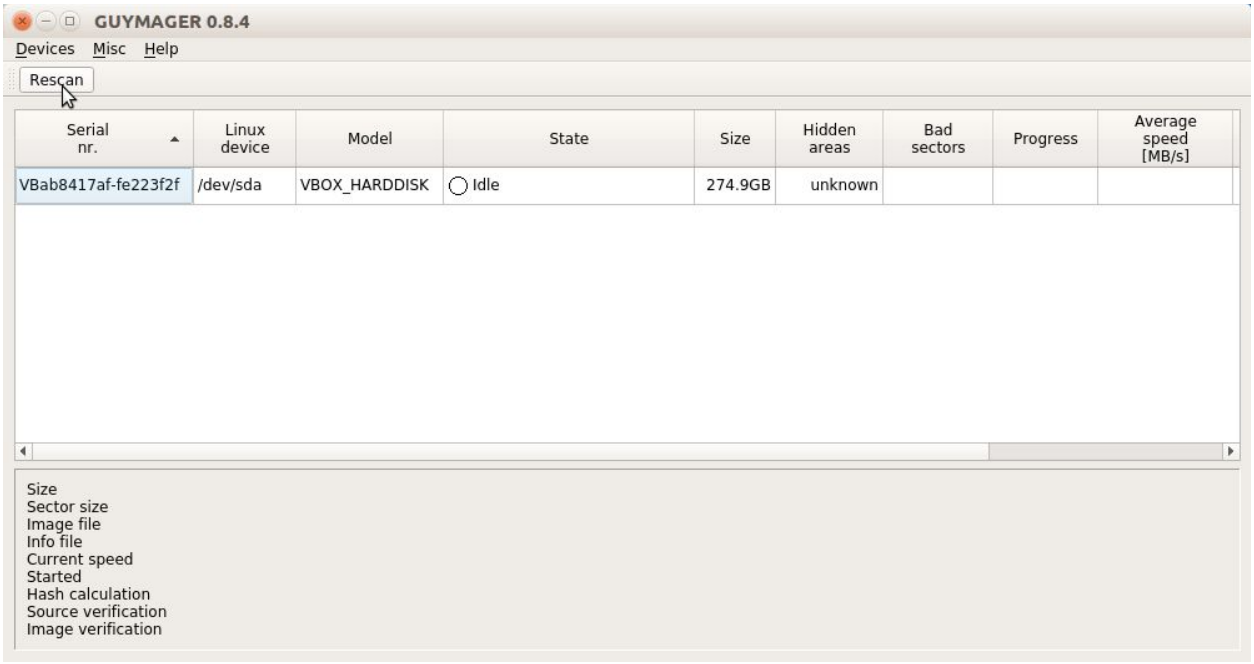
Optical Disks

Dependencies: BitCurator (installed on the MediaLab computer as Virtual Machine, accessible via Virtualbox), Guymager, Dvdisaster, disktype, isolyzer)

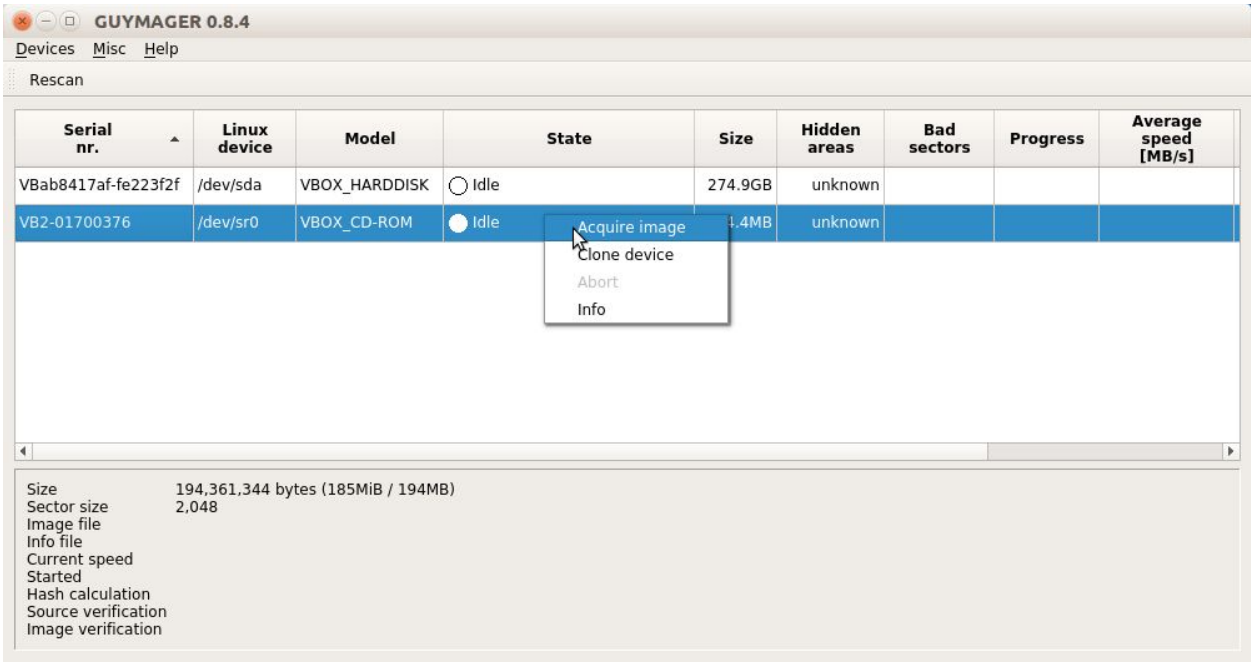
I. Image the disk using Guymager

A. Open the Guymager GUI from the “Imaging Tools” directory on the Desktop

B. The optical disc should appear in the list of devices, with the “Linux Device” listed as “dev/sr0” and the “Model” of “VBOX_CD-ROM” - if this does appear click the “Rescan” button in the top left corner

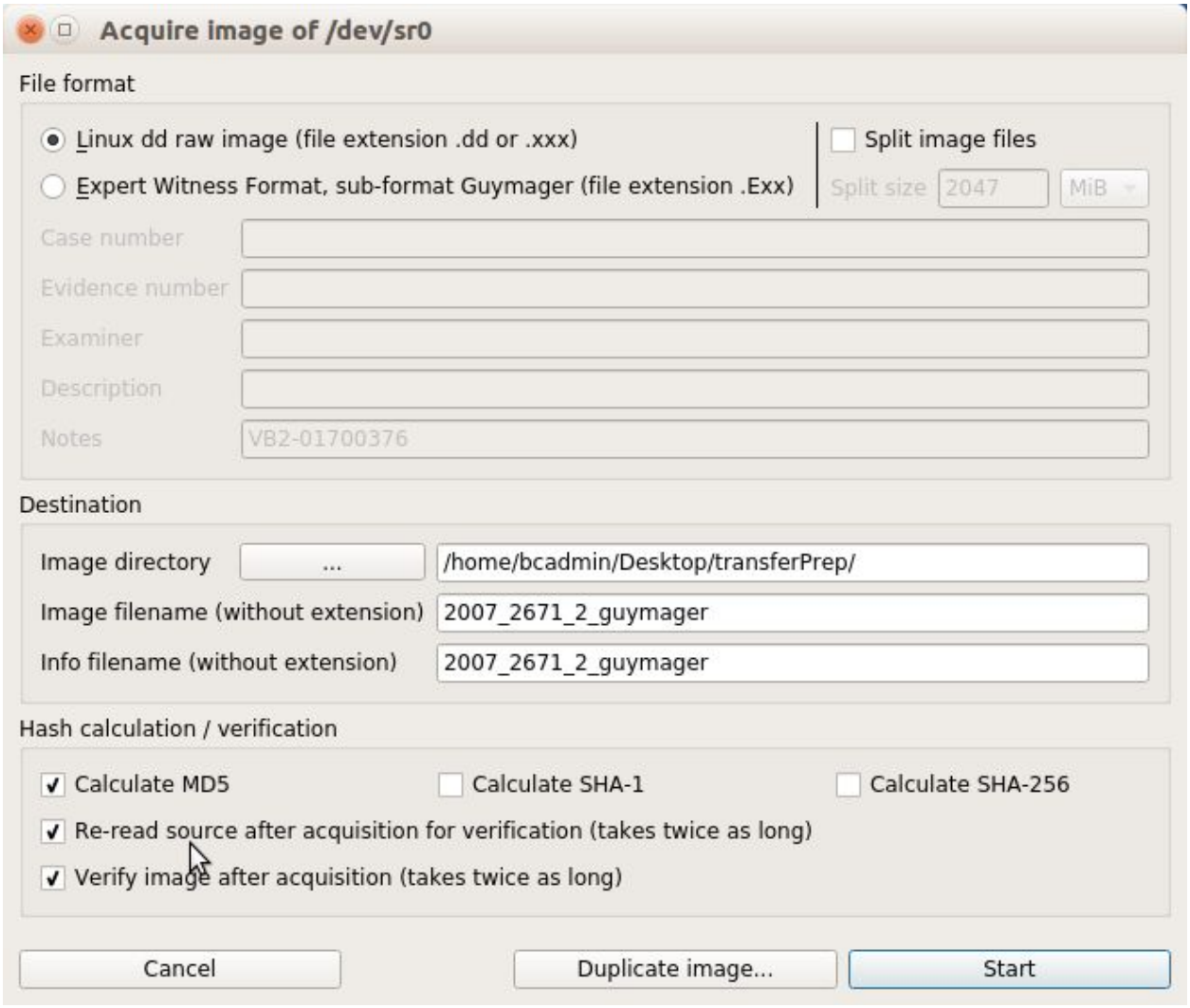


C. Right click on the optical disc and select “Acquire image,” a pop-up window will open



D. In the pop-up window, choose the “Linux dd raw image” option from the top left, and be sure to deselect the “Split image files” checkbox. Stage the disk image in the “transferPrep” directory on the Desktop by choosing the folder in the “Image Directory” field in the “Destination” section of the pop-up. Name the image using the Argus catalog number, replacing periods with underscores, and adding the suffix “_guymager.” This suffix is important as it indicates the source of both the disk image and the “.info” file the Guymager application creates. Finally, select the “Re-read source after

acquisition for verification" checkbox beginning the disk imaging process by pressing "Start"



E. Take note if bad sectors were reported during the imaging process, bad sectors will change the workflow

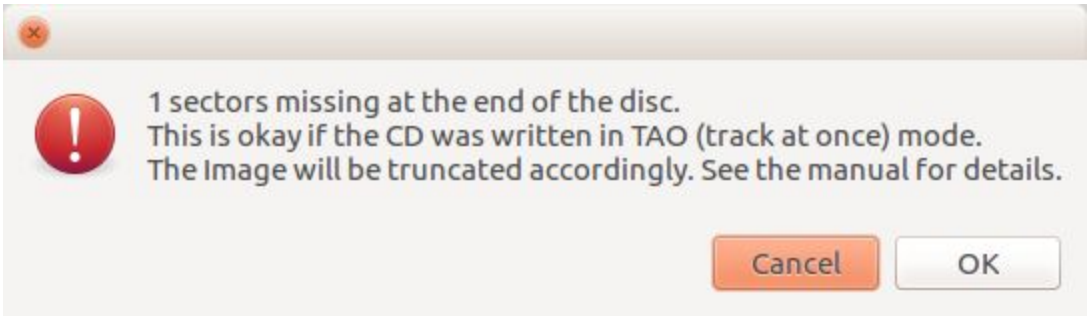
II. Create an Error Correction file using Dvdisaster
(Dvdisaster creates "Error Correction Files" using Reed-Solomon error correction code, the application is currently set to use RS03. Some forms of optical media will have RS error correction code already, and the application is designed to scan for and record this code if present. Currently the interoperability of these files is unknown, but they can be used to supplement a damaged disc or disk image using dvdisaster.)

A. Open the Dvdisaster GUI located in the Downloads directory

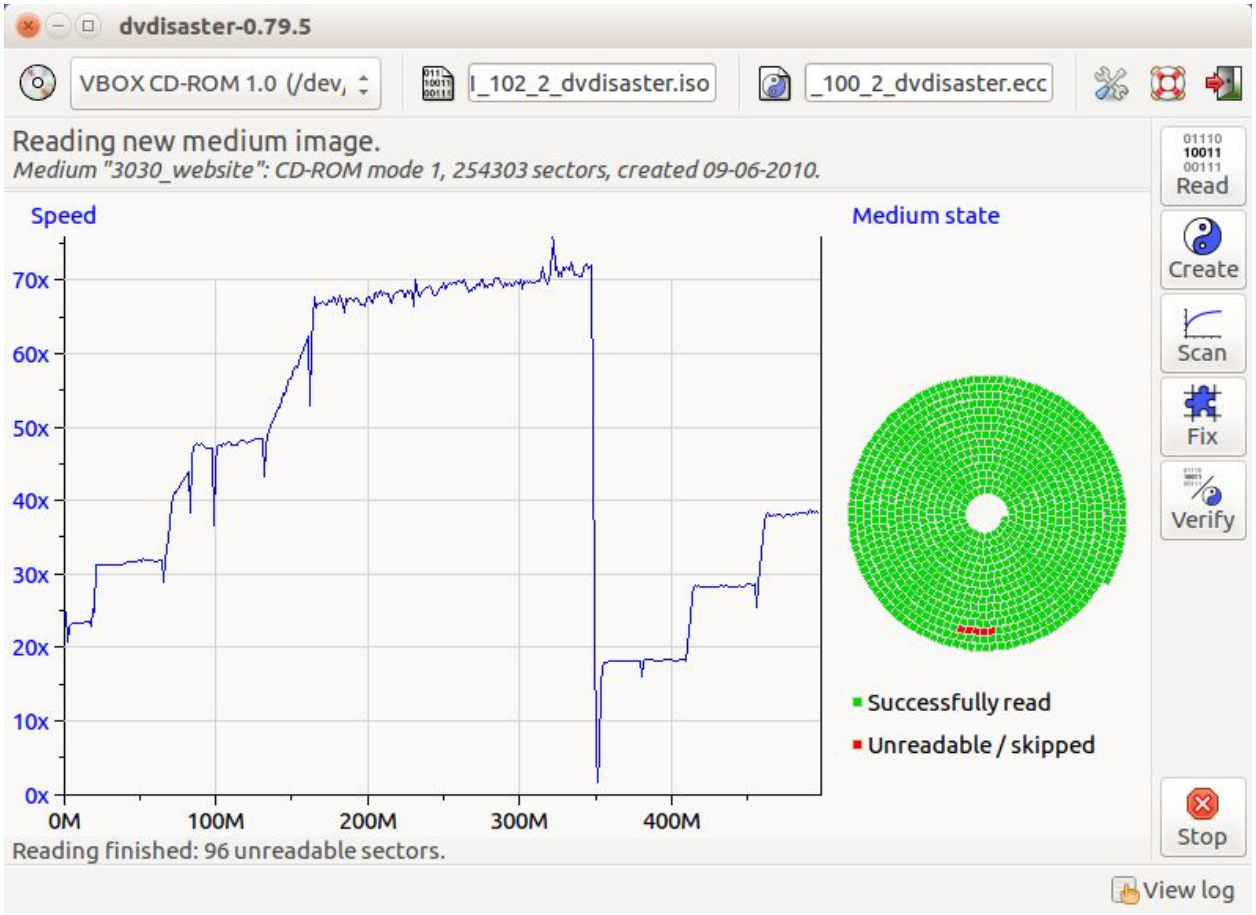
B. If bad sectors were encountered in Step I:

1. If only 1 bad sector was encountered, it was likely the last sector on the disc. Use the "Scan" option in Dvdisaster (located on the right side) to confirm that the bad sector is at the end. You will

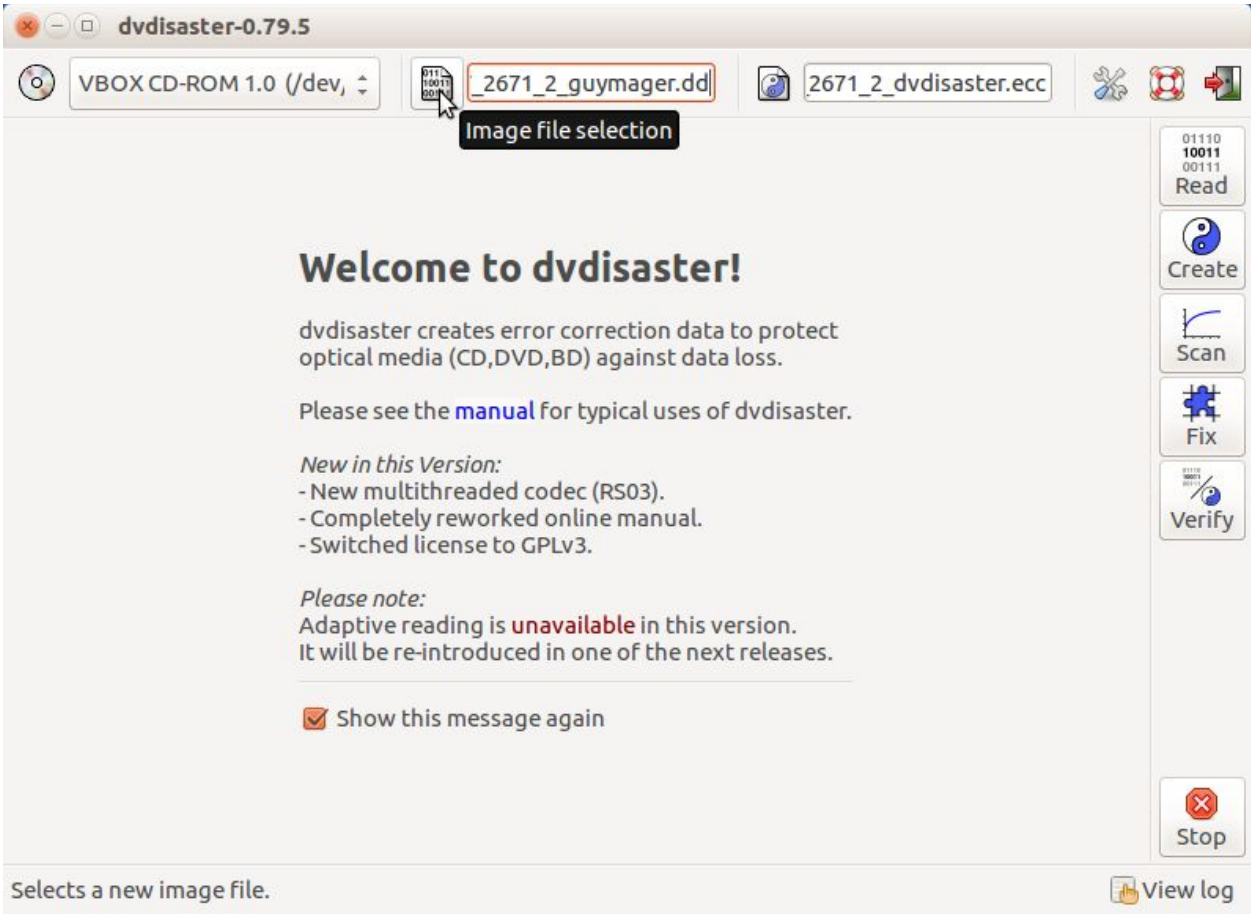
receive an error message that looks like this:



2. If more than one bad sector was encountered, create a new disk image using the “Read” option on the top right of the Dvdisaster window
   a) Monitor the imaging process and take note of bad sectors encountered. Information on assessing the drive speed is available in the Dvdisaster manual: http://dvdisaster.org/en/misc.html#manual



C. Click the “Image File Selection” icon and select the disk image created in Guymager:



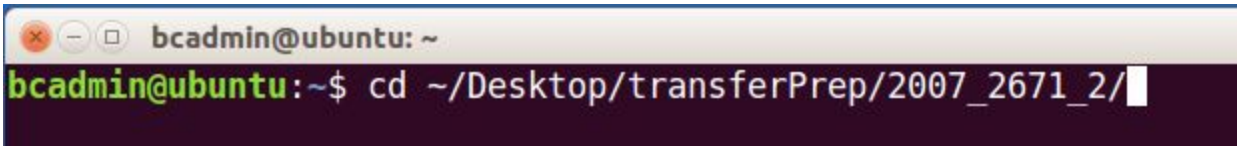
D. Fill in the “Error Correction File Selection” field with the same name as the disk image filename, replacing the “_guymager.dd” suffix with “_dvdisaster.ecc”

E. Click the “Create” option on the right side of the Dvdisaster window

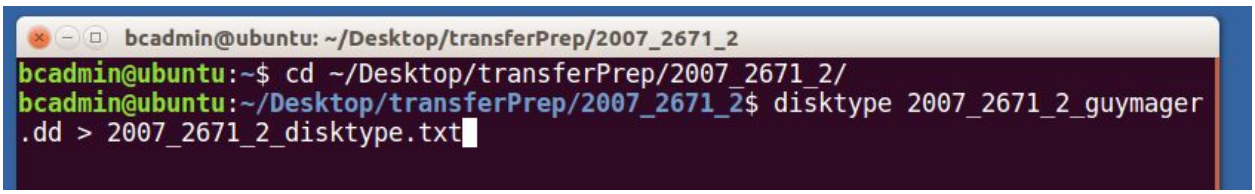
III. Collect metadata on the disk image using disktype

(The disktype application can be used to determine the amount of data in a disk image, the number of partitions in an image, the file systems of the partitions, the sectors those partitions occupy, as well as any embedded metadata.)

A. Navigate to the directory with the disk image in it using the “cd” or “change directory” command



B. Then type the “disktype” command followed by the disk image filename, and print “>” the results to a text file:

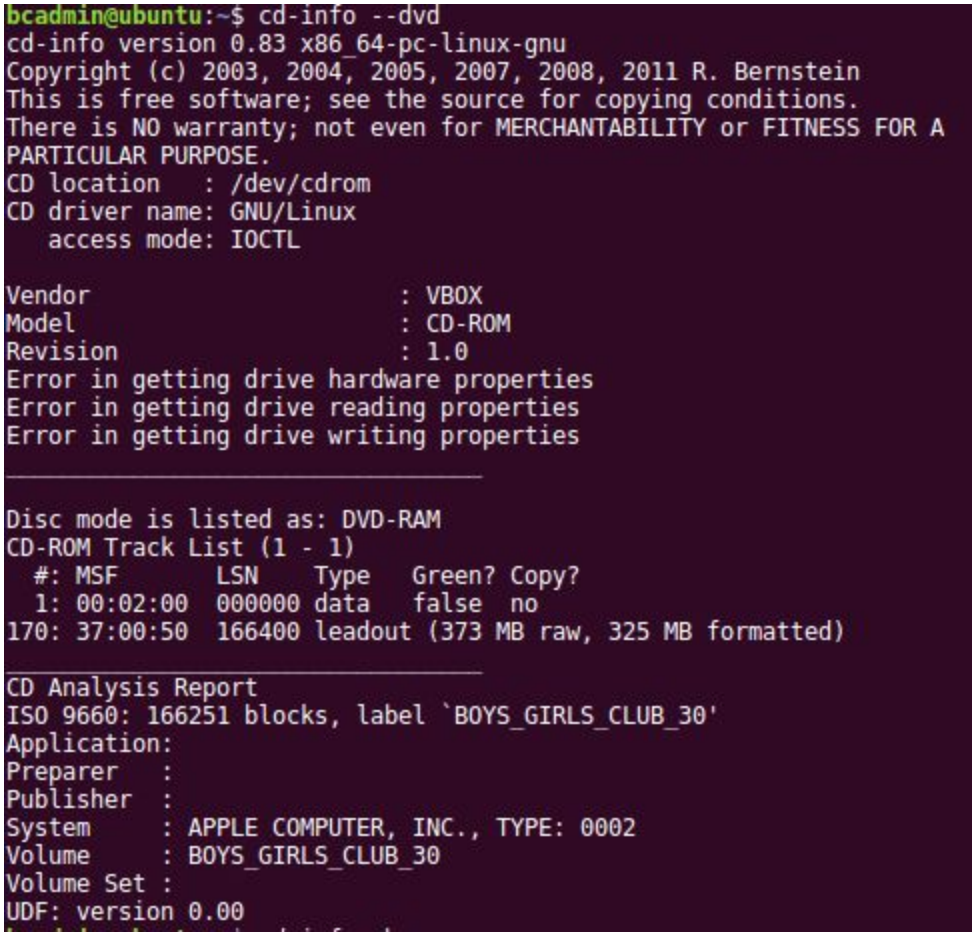


Use tab completion to avoid typos! Type the first few characters of the filename you are searching for, and press “tab” and the command line will attempt to complete the filename. This technique can be used for directories as well.

C. Other optical disc metadata applications:

1. Find path to disc drive:
   `mount|grep ^'/dev'`
2. Cdrdao command
   a) Must be run on an unmounted volume:
      `Sudo umount /dev/sr0`
   b) This command should give you the number of sessions:
      `cdrdao disk-info --device /dev/sr0`
   c) But often returns this text with the metadata (does not give this message when no volume is mounted):
      “That data below may not reflect the real status of the inserted medium if a simulation run was performed before. Reload the medium in this case.”
   d) Multi-session/CD-Extra discs not currently showing up in BitCurator, and mounting as 2 volumes on Mac OS so not really using this tool right now
3. cd-info command
   a) From the libcdio library
      `cd-info --dvd`
      Or
      `cd-info --iso9660`

b) Example Output:



4. Isolyzer
   a) Locate the image's Primary Volume Descriptor (PVD). From the PVD, read the Volume Space Size (number of sectors/blocks) and Logical Block Size (number of bytes for each block) fields. Calculate the expected file size as (Volume Space Size x Logical Block Size). If the image contains an Apple Partition Map, read the Block Size and Block Count fields from the 'zero block'. Calculate the expected file size as (Block Size x Block Count). If the image contains an Apple Master Directory Block, read its Block Size and Block Count fields. Calculate the expected file size as (Block Size x Block Count). Calculate the final expected file size as the largest value out of any of the above 3 values. Compare this against the actual size of the image files. (from Detecting Broken ISO Images by John Van Der Knijff)
   b) Look for <sizeAsExpected> XML field and <smallerThanExpected> XML field. If <smallerThanExpected> is "True" image may be damaged
   c) See scripts related to batch running isolyzer
      (1) Run isolyzer on all disk images with ".dd" extension:

```
for f in $(find /home/bcadmin/Desktop/transferPrep/in_AIPstore/ -name '*.dd'); do
isolyzer $f > /home/bcadmin/Desktop/test_xml_output/"$(basename $f .dd).xml"; done
```

(2) Create manifest of all disk images that are “smaller than expected” based on calculation using Primary Volume Descriptor (PVD) field:
for f in $(find /home/bcadmin/Desktop/test_xml_output/ -name '*.xml'); do grep -i smallerThanExpected $f > /home/bcadmin/Desktop/test_xml_output/smallerthan/"$(basename $f .xml).txt"; done

D. Resources on optical disc:

1. Preserving optical media from the command line, by JOHAN VAN DER KNIJFF, NOVEMBER 13, 2015: http://blog.kbresearch.nl/2015/11/13/preserving-optical-media-from-the-command-line/
2. Digital Asset Technical Specifications, NYPL, Oct 2016: https://github.com/nypl/ami-specifications
3. Preserving Write-Once DVDs, Morgan Morel, April 2014: http://www.digitizationguidelines.gov/audio-visual/documents/Preserve_DVDs_BloodReport_20140901.pdf?loclr=blogsig
4. Detecting Broken ISO images, Johan Van Der Knijff, January 2017: http://openpreservation.org/blog/2017/01/13/detecting-broken-iso-images-introducing-isolyzer/
5. Isolyzer github: https://github.com/KBNLresearch/isolyzer
6. Audio CDs behave differently than other optical media, more info here: To Image or Copy -The Compact Disc Digital Audio Dilemma, Alice Prael, December 20, 2016

For Kryoflux in BitCurator

Connecting the kryoflux

1. attach kryoflux board USB to computer
2. Attach power to floppy disk drive
3. Using the command line, navigate to the “dtc” folder within the kroflux directory: cd ~/Downloads/kryoflux_2.6_linux/dtc
4. run the command: sudo ./dtc -c2
5. This should configure the drive and, after the drive spins around for a bit, should return the statement: CM: maxtrack=83
6. Open the GUI from the command line by typing the following command: sudo java -jar '/home/bcadmin/Downloads/kryoflux_2.6_linux/dtc/kryoflux-ui.jar'
7. or, if you are still in the “dtc” folder” simply type: sudo java -jar kryoflux-ui.jar
8. Notes: you MUST use “sudo” when calling the java application, or the GUI will not be able to communicate with the kryoflux.
9. You must keep the command line terminal window open when using the kryoflux GUI.

Notes:

Format Assessment- Disk Image Formats, Harvard/AVPreserve, 2015:
https://wiki.harvard.edu/confluence/display/digitalpreservation/Disk+Image+Formats

For Computer HDDs

1. Evaluate the machine, determine if powering on the computer is safe
    a. The museum does not have a formal policy on this procedure. For the IMLS e-media project, the age of the computer was the primary determining factor. New machines were powered on before imaging, and older machines were not turned on until after the hard drive had been imaged.
    b. Testing the machined before imaging allows the conservator to be sure that their intervention did not create any issues that the machine is exhibiting.
2. If the machine is powered on before imaging, test the computer's functionality, and export information on the machine's hardware.
    a. For a Mac running OS X, this can be done easily by exporting a report from the "System Profiler." More information on System Profiler: https://support.apple.com/en-us/ht203001
    b. Change the System Profiler report file extension to XML to open with any text editor
3. Remove hard disk drive
    a. Search the internet for tutorial videos for the particular model of machine you will be working with. There are often videos or images that show the layout of the machine, and identify the hdd for you, so you will know how to easily open the computer and find the part you are looking for.
    b. Removing a hard drive should not be done while the computer is on. In fact, many tutorials suggest unplugging the machine, and holding down the power button for 10-15 seconds to ensure now charge is left in the machine.
        i. However, several tutorials suggest not unplugging the machine until after you have grounded yourself to the machine's chassis: https://blog.macsales.com/2225-discharging-static-electricity-for-safe-computer-upgrading
    c. Ground yourself by touching an unpainted metal object, and then put on the anti-static wrist strap
    d. Open the computer, and connect the anti-static wrist strap to the metal chassis of the computer. Other conservators and technicians have recommended connecting the strap to a different unpainted metal object.
    e. Remove the hard drive, handling the drive by its sides. Be careful not to touch the circuit boards.
    f. Connect the drive to the enclosure, and then power the enclosure on.
4. Connect the enclosure to the read/write blocker, and then to the computer.
    a. I have been powering on the enclosure, and then powering on the read/write blocker, and then connecting them to each other, and finally the computer, with

the hopes of avoiding power surges when the devices are turned on. This may be more cautious than necessary.

5. Open terminal, and run diskutil list to identify the location of the drive.
    a. The output of diskutil list will look like this:

```
media-lab:Volumes mediamigration$ diskutil list
/dev/disk0 (internal, physical):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      GUID_partition_scheme                        *1.0 TB     disk0
   1:                        EFI EFI                     209.7 MB   disk0s1
   2:                  Apple_HFS Untitled                999.9 GB   disk0s2
/dev/disk1 (external, physical):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      GUID_partition_scheme                        *9.0 TB     disk1
   1:                        EFI EFI                     209.7 MB   disk1s1
   2:                  Apple_HFS Collections Storage     9.0 TB     disk1s2
/dev/disk3 (disk image):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      GUID_partition_scheme                        +60.0 GB    disk3
   1:                        EFI EFI                     209.7 MB   disk3s1
   2:                  Apple_HFS Macintosh HD            59.7 GB    disk3s2
```

6. Disk Image Naming convention
    a. Review the Argus records for the work. Disk images created for computers during the IMLS e-media project were named after their source computer (and not after the computer's disk image record). The reasoning for this was to decrease the length of the file name and hopefully prevent confusion when retrieving disk images. Include the suffix of the application that created the disk image in the file name. This will provided added provenance information, and help with identifying the "info" file that many disk imaging applications automatically create.
7. Fun FTKimager on the desired disk
    a. FTKimager is a command line application downloaded from the internet and currently stored on the Desktop. The command can be run by dragging the file from the desktop into the Terminal window. You will need to use the "sudo" prefix to be able to run this command on an external volume, and provide your username's password.
    b. Use the --e01 flag to create an EWF disk image.
    c. Use the --compress 5 flag to run "level 5" compression (based on recommendation from colleague).
    d. The final command will look like this (where, "/dev/disk2" is the volume you are imaging, and "/Volumes/Collections\ Storage/RAID_shared_w_VM/2010_398_4_ftkimager" is the name and destination of the disk image):

        sudo /Users/mediamigration/Desktop/ftkimager /dev/disk2 /Volumes/Collections\

Storage/RAID_shared_w_VM/2010_398_4_ftkimager --e01 --compress 5

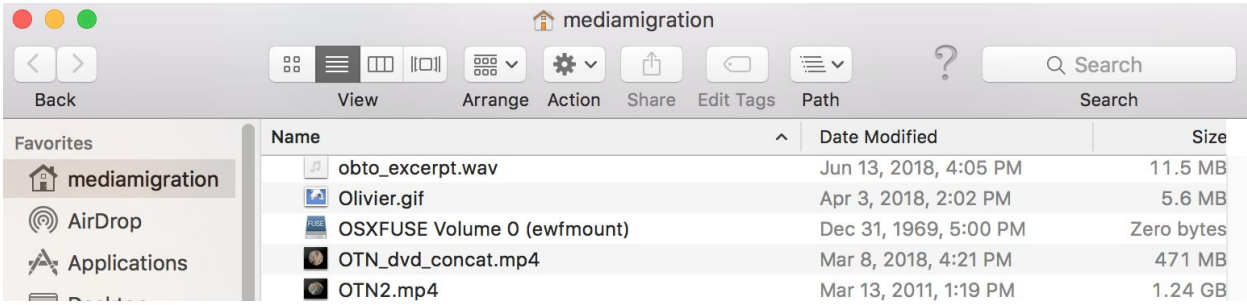
8. Time permitting, verify the disk image by creating an md5 checksum on the original volume. If the volume was mounted as /dev/disk2, then the command to create an md5 checksum of that volume through the macOS terminal application would be:

   Md5 /dev/disk2

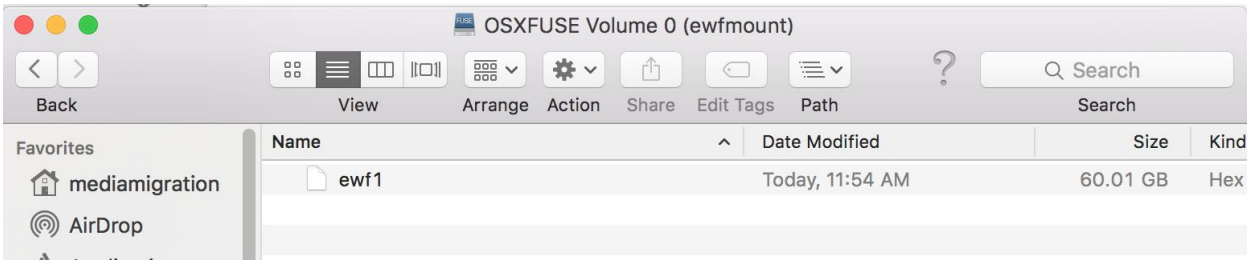
   a. Compare the result of the command above with the checksum listed in the info file created by FTKimager, it should be a text file with the same file name as the disk image.
9. Assuming the checksums match, eject the hard drive, disconnect both the read/write blocker from the computer and each other, then power down both devices.
10. Mount the EWF disk image by running the ewfmount command.
    a. Navigate to the “mediamigration” directory (at the top of the directory structure), by running “cd ~/.” Unless you have navigated elsewhere, you are likely already in that directory. You can verify your location by running “pwd” for “print working directory.”
    b. Once in “mediamigration” run the ewfmount command

       Ewfmount -X allow_other [disk image] mnt00/

    c. You need the “-X allow_other” to give you permissions to mount the image, open the mount point, and eject the image.
11. Navigate to the fuse mount point
    a. Fuse is an application that ewfmount uses to create mount points. More information here: https://github.com/libyal/libewf/wiki/Mounting
    b. The fuse mount point will have taken the place of the “mnt00” directory in the mediamigration directory, and will now be listed as “OSXFUSE Volume 0”. It will now look like this:



c. Double click the OSXFUSE Volume 0 directory like you would any other, and you will see a disk image with the “ewf1.”



d. Unfortunately, because the macOS does not recognize the ewf1 file as a disk image without the “.iso” extension, and because you cannot change the filename of the disk image due to it’s permissions, you must copy the raw disk out from the mount point to mount the disk image. Simply copying and pasting the image does not work well, and has resulted in the file being hidden from finder in the past.

12. Copy the raw disk image using rsync
    a. You can copy the disk image from the mount point to another location using rsync. Rsync is a command line application built into Linux and macOS.
    b. The syntax for rsync is very straightforward. Simply open terminal and type the command, “rsync,” the file you want to copy and the copy’s destination. For this example the command should be :

       rsync /Users/mediamigration/mnt00/ewf1 /Volumes/Collections\
       Storage/arch01/transfer_staging/

    c. You’ll know the rsync command is complete when terminal has returned a new line, i.e. “media-lab:~ mediamigration$” with a blinking cursor.
13. Change the name of the disk image to something more descriptive, with an .iso extension.
    a. Ewf1 -> 2011_297_1.iso
14. You should now be able to mount the disk image.
15. Unmount the EWF image by running the following command:

    Sudo umount mnt00/

16. Before submitting to archviematica, run “disktype” (see previous sections) and “mmls” (like disktype, but slightly different information) on the renamed .iso disk image.

For Macs

1. After following steps 1 and 2 of the previous section “For Computer HDDs”, boot up the computer while holding down the “T” key on the keyboard.
    a. After the computer boots up and chimes, you should see a firewire symbol on the screen.

2. Connect the Firewire cable to the Tableau Firewire forensic bridge, and then connect the USB output from the bridge to the imaging computer.
    a. Running firewire out from the forensic bridge has caused the Mac Pro to freeze, more research needed.
3. The Forensic Bridge may ask you to select a LUN. This is a "Logical Unit Number." I have found that selecting the first option leads to an "unrecognizable device," and nothing connected to the Mac Pro, so I have selected the 2nd option, which has captured both the Mac hard drive partition and the EFI firmware partition.
4. Resume procedure from step 5 of previous section, "For Computer HDDs."
5. For more on using Target Disk Mode for creating Forensic Disk Images see: Forensic Acquisition of Mac Computers by Kevin J. Ripa
   http://www.computerpi.com/forensic-acquisition-of-mac-computers/