GUGGENHEIM
Conservation Department

Workflow for Disk Imaging

Last updated: 7/25/2019

TAKE PHOTOS OF THE HOST COMPUTER AND THE REMOVABLE MEDIA OR HARD DRIVE

1. Take photographic images of all items below that apply (it is possible to cover more than one item in a single photo):
    - Artist-provided computer, unopened
    - Hard drive and how it is installed in the computer
    - Labels, model numbers, and serial numbers of the computer
    - All input/output ports on the computer
    - Any artist signatures, inscriptions, or edition numbers on any item
    - Custom designs and modifications of computer cases or components
    - Cable connections between hard drive and motherboard/logic board
    - The top, bottom, and relevant sides of the physical media to be disk imaged (hard drive, CD, or floppy disk). Images of a hard drive should include a detail of the drive interface (all ports or pin connections on the back of the drive).

If possible, include an AIC PhD Target with the component number of the computer in the photos. If there are multiple hard drives within the same computer, they will receive the same component number, but they should be labelled “X of X” in the AIC PhD Target used in the photos

2. Photos should be saved in the Object File for the artwork.

DOCUMENT THE ENVIRONMENT OF THE HOST COMPUTER

If an image is being acquired of an optical disc, a floppy disk, or an external hard drive where an entire computer is not involved, this section can be skipped.

1. Gather information about the computer, ideally by using the computer being imaged to generate a report about its configuration. If possible, this procedure should be done while the artwork is still installed—the computer will be able to more accurately report on any devices or peripherals that were attached during exhibition, for example, audio devices, computer monitors, keyboards, mice, and printers. In addition, any logs and other installed files will be as accurate to the specifications for the exhibition as possible. This procedure may not be possible or desirable on historic computers, so the hardware information may need to be obtained through other means.

CAUTION: The procedures described below can potentially create new files on a host computer. Alternatively, photos of the screen can be taken with a camera. It may also be possible to use an external hard drive or flash drive and copy the files directly there instead of on the computer's hard drive. If photos are taken, then transfer these photos to the same location detailed below for the System Information files.

To create System Information files on computers running Apple's macOS (also known as OS X):

a. Start up the computer normally.
b. Click on the Apple Logo in the top left corner of the screen and select "About this Mac".
c. A new window will appear with information about the computer. Click on the "System Report" button. This will start up the System Information program.
d. With the System Information program open, go to the "File" menu and select "Save". Choose to name the file "[Component_number]_system_report" and select where to save the file. The program will create an .spx file
e. If applicable, transfer the file off of the original computer and delete all created files on the original computer.
f. Transfer the files to the Conservation Media drive.

On computers running Microsoft Windows XP through Windows 10:

a. Click the "Start" button and select "Run". In the Command Prompt window that appears, run the command "msinfo32".
b. A new window should appear with configuration information. Within the new window, choose "File > Save". Name the file "[Component number]_system_report" and select where to save it.
c. Transfer the files with system information to the Conservation Media drive. The files should be placed in the following directory: [Accession number]_Artist_Title/File Transfer and Metadata/[Component number] _DISK_IMAGE_METADATA.
d. If applicable, delete the files off of the original computer.

On computers running GNU/Linux:
Note: The procedures below have only been tested on Ubuntu v16. These procedures may not apply to all GNU/Linux distributions.

a. Open a new Terminal window
b. Hardinfo can be used to create the most comprehensive text-based or HTML reports of system information. To run Hardinfo type:
```
$ hardinfo
```
c. A new window should appear with a graphical user interface. Click the "Generate Report" button. Click "Select All" to choose all of the reporting tools. Click "Generate" to generate the report.

d. Choose to save the report on the Desktop or an external drive and name it [Component number]_hardinfo_report. Choose to save the file as HTML.

   Note: Hardinfo may not be installed on the computer. If it is not installed, you must determine if it is acceptable to install additional software on the computer. To install Hardinfo on Ubuntu run the following command:

   ```
   $ sudo apt-get install hardinfo
   ```

The following steps below do not require the installation of new software on a Linux machine.

e. Run the following command to get information about the hardware and print it to a text file on the computer's desktop or external drive (where the $ represents the command prompt):

   ```
   $ sudo lshw > [Destination directory]/[component_number]_system_report.txt
   ```
f. Transfer the files to the Conservation Media drive.

ACQUIRE A DISK IMAGE OF A HARD DRIVE

1. Determine the drive interface of the computer. If it has an obscure or proprietary connection type (many Solid-State Drives on Apple products) it may be necessary to leave the drive inside the computer and acquire an image of it using Target Disk Mode (see Appendix I below). Otherwise, remove the hard drive from the original computer.

2. Check to ensure that the disk imaging computer has enough space to hold the disk image that will be created.

3. Use the template Disk Imaging Report for Hard Drives and start recording information about the drive, including the model, serial number, listed capacity, and connection type.

4. If there are multiple hard drives within the same computer, each drive will have its own imaging report. Be sure to include information about the number of the drive "X of X" in the disk imaging report.

5. Position the hard drive next to the write-blocker so there is at least some slack in the cables and the drive will not move. Place the drive so that it is completely level, immobile, and reasonably protected from sudden physical shocks or movements.

6. Connect the hard drive to the appropriate write-blocker and turn on the write blocker.

7. Open the imaging program (typically FTK Imager or Guymager) and add or select the drive to be imaged.

8. Examine the number of drive partitions and their names. Record this information in the Disk Imaging Report. If not using FTK Imager, use the command “disktype” to create a record of the partitions. Use the following example command (this will also output the results into a text file:
   $ disktype [path to device, for example /dev/sr0] > [Destination path]/[Component number of physical media]_disktype.txt

9. In the imaging program, choose to acquire the image in the E01 format.

10. Fill out the metadata fields as follows in the imaging program:

    - **Case Number** — Use the component number assigned to the disk image itself (For example, 99.4088.2).
    - **Evidence Number** — Enter the text "Disk image taken from", then type the component number assigned to the computer or physical media that is the source of the disk image. (for example, 99.4088.1). If the computer or drive will not become a component, use a brief description of the source computer, for example "SRGM device #101070".
    - Unique Description — Fill in this field using the following format: [Artist], [Title of Artwork]
    - Examiner — Fill in the name of the person creating the disk image.
    - Notes — Start this field with the text "Inscriptions:" and after the colon, record any inscriptions that are deemed important on the drive or computer. This would typically include the drive's serial number, or any text that the artist or SRGM staff wrote on the computer or the drive that might identify it. If there are no inscriptions worth noting, type "Inscriptions: None." After listing the inscriptions type a comma. Now include any information about the version or iteration of the artwork that the computer is running, for example "2016 version" or "2017 SRGM iteration". If there are multiple hard drives within the same computer, the number of the drive should be recorded as “X of X”. The examiner should also include information about where the drive is plugged into the computer or where it sits in a cable run in relation to other the drives.

11. Select the following path on the imaging computer to save the image: Disk Imaging /[Accession number]_Artist_Artwork

12. The filename of the image should be formatted as follows: [Component number]_Artist_ArtworkTitle_SRGM_DiskImage_YearofImaging". The imaging program should automatically add the appropriate file extension when it creates the image.

13. Choose to verify the image after creation. If using Guymager, choose to re-read the source media after imaging.

14. If the program has a fragmentation option, do not use it. In FTK Imager type 0 for no fragmentation. The goal is to produce a single file for the entire disk image.

15. Wait while the image is being acquired. If possible, do not run any other programs on the imaging computer or move or copy any files. Do not move the hard drive, the computer, or any of the cables while the image is being acquired.

16. Ensure that the image has been verified by the imaging program. If the image was not verified, the drive may need to be imaged again. Note that the first attempt at verification failed in the disk imaging report.

17. Check to the info reports that the imaging program generates to see if any bad sectors were detected. Bad sectors could indicate an immanently failing or damaged drive.

18. Fill out Section 1 of the Disk Imaging Report. The report should be named: [Component number]_Disk_Image_Report.txt.

19. Proceed to the QC section below.

ACQUIRE A DISK IMAGE OF A FLOPPY DISK

(Adapted from "Solomon R. Guggenheim Foundation Electronic Records Start-Up Project: Processing Obsolete or Removable Media" by Anthony Cocciolo)

1. Collect information about the floppy disk. Record this information in the first section of the Floppy Disk Imaging Report.

2. Enable write protection on the disk:

   For 3.5 inch floppy disks, enable the write protection tab by sliding the plastic tab. When viewing the disk from the front (label side), you should be able to see through the tiny window on the right side of the disk.

   For 5.25 inch floppy disks, make sure the notch on the top-right part of the disk is not blocked. Remove any tape or other object that is blocking this notch to engage write protection.

3. Connect a floppy disk drive to the imaging station and insert the disk. Since write protection has been enabled on the disk, a write blocker is not necessary.

4. Start up the imaging program and choose to create an image in the E01 format.

5. Fill out the metadata fields as follows in the imaging program:

   - **Case Number** – Use the component number assigned to the disk image itself (For example, 99.4088.2).
   - **Evidence Number** – Type "Disk image taken from" then type the component number assigned to the computer or physical media that is the source of the disk

image. (for example, 99.4088.1). If the computer or drive will not become a component, use a brief description of the source computer, for example "SRGM device #101070".

- Unique Description – Fill in this field using the following format: [Artist], [Title of Artwork]
- Examiner – Fill in the name of the person creating the disk image.
- Notes – Start this field with the text "Inscriptions:" and after the colon, record any inscriptions that are deemed important on the drive or computer. This would typically include the computer or drive's serial numbers, or any text that the artist or SRGM staff wrote on the computer that might identify it. If there are no inscriptions worth noting, type "Inscriptions: None.". After inscriptions include any description of the role and status of the computer, include any information about the version or iteration of the artwork that the computer is running, for example "2016 version" or "2017 SRGM iteration".

6. Tell the program to write the image to the following path on the imaging computer: Disk Imaging Acquisition/[Accesion number]_Artist_Artwork

7. The filename of the image should be "[Component number]_Artist_ArtworkTitle_SRGM_DiskImage_YearofImaging". The imaging program should automatically add the appropriate file extension when it creates the image. If applicable, make the info filename the same as the filename of the image.

8. Choose to verify the image after creation. If using Guymager, choose to re-read the source media after imaging.

9. If the program has a fragmentation option, chose no fragmentation. In FTK Imager type 0 for no fragmentation. The goal is to produce one file for the entire disk image.

10. Wait while the image is being acquired. If possible, do not run any other programs on the imaging computer or move or copy any files. Do not move the drive, the computer, or any of the cables while the imaging is being acquired.

11. Ensure that the image has been verified by the imaging program.

12. Complete Section 1 of the Floppy Disk Imaging Report. Be sure to include specific information about the how the image was acquired.

13. Proceed to the QC section below.

ACQUIRE A DISK IMAGE OF AN OPTICAL DISC

(Adapted from Eddy Colloton's "Optical Imaging Workflow" for the Denver Art Museum)

1. Collect information about the disc including disc type (CD-R, DVD-R, CD, DVD-R-DL) and serial number. Record this information in Section 1 of the Optical Disk Imaging Report.

2. Determine the number of sessions on the disk. To do this, run:
   ```
   $ cdrdao disk-info --device [path to disc such as /dev/sr0]
   ```

3. Record the number of sessions. Most discs will return 1 session. If the disc only has a single session, go to step 4. If the command returns multiple sessions, consult the separate (experimental) workflow for imaging multi-session discs.

4. Based on research in the Guggenheim Media Lab, the preferred imaging program for optical media is currently GNU ddrescue. Ddrescue is preferred as it offers more detailed error messages and re-reading of bad sectors. Guymager should not be used as the program's recovery routine in the case of bad sectors is hard on optical drives.

5. Use disktype to determine the bytes per sector to input into ddrescue. Use the following example command (this will also output the results into a text file:
   ```
   $ disktype [path to device, for example /dev/sr0] > [Destination path]/[Component number of physical media]_disktype.txt
   ```

6. Transfer the resulting text file to the ″File Transfer and Metadata″ folder of the Conservation Media drive for the artwork.

7. To acquire an image with ddrescue use the following example command:
   ```
   $ ddrescue -b [bytes per sector, usually 2048 for CD-ROM] -r4 -v [path to the newly created image file, for example /dev/sr0 mydisk.iso] [path to write log file, for example mydisk.log]
   ```

   The filename of the image should follow this format: [Accession number]_Artist_TitleOfWork_SRGM_DiskImage_YearofImaging.iso″.

8. If there continue to be errors, try ddrescue again with different options to attempt to recover more data from bad sectors:
   ```
   $ ddrescue -d -b 2048 -r1 -v /dev/sr0 mydisk.iso mydisk.log
   ```

9. If you are still encountering errors, try another optical disc drive.

10. After disk image is created, create an error correction file with DVDisaster. This .ecc file should be named "[Component number of disk image]_error_correction" and saved in the same folder as the image.

11. Use the "Verify" button on DVDisaster to test the original image and the error correction file.

12. Assuming both files pass verification, keep the error correction file with the disk image at all times.

13. Fill out Section 1 of the Disk Imaging Report. The Disk Imaging Report should be named: [component number]_Disk_Image_Report.txt.

14. Attempt to verify the checksums of the disk image and the original disc. Run the two commands below in succession:

    ```
    $ md5sum [path to disk image file] > [Destination folder]/[Filename of disc image].iso.md5
    $ md5sum [path to physical media, such as /dev/sr0] > [Destination folder]/[Component number of disk image]_verification.md5
    ```

15. The commands should have created two text files, one with the MD5 checksum of the disk image and one for the checksum of the original media. Compare the two checksums to see if they match.

16. If the checksums match, the disk image can be considered verified. If the checksums do not match, run the md5 command again for the source media and see if the same checksum is produced.

    NOTE: Because of error correction inherent in optical media and differences in how different drives read the media, it may not be possible to verify optical discs via checksums. However, this fact should be noted in the disk imaging report.

PEFORM QUALITY CONTROL (QC) INSPECTION OF THE DISK IMAGE

1. Create a duplicate copy of the disk image in the staging area to perform testing. DO NOT TEST THE ORIGINAL DISK IMAGE.

2. Verify that the duplicate copy is exactly the same as the original image with MD5 checksums or the “diff” command.

3. For items that are not optical discs, ensure that the disk image has been verified successfully. If the image was not created in Guymager, run the following commands to verify the integrity of the image against the original source media:

    ```
    $ md5sum mydiskimage.E01
    $ md5sum [device ID of original media such as /dev/sr0]
    ```

If the md5 checksums created from these commands match, the disk has been verified. Record this information in the disk imaging report.

4. Fill out Section 2 of the Disk Imaging Report and go through the tests described (Exploring the disk image, exporting files from the image, and running the image in an emulator or virtual machine). Some legacy filesystems (such as HFS) will give strange results if the image is

explored within FTK Imager.

5. Disk images of optical discs and floppy discs should be tested to mount properly on at least two computers with different operating systems. Optical discs only need to go through an emulation/virtualization/playback test if they run as executable software (like a Windows install disc), contain a software environment, or autoplay media (like a DVD).

6. If there are any errors in QC, the original media may need to be imaged again and the checksums compared. The command ddrescue may also need to be used to recover data from the drive or disk.

7. Capture any settings that were not collected before (additional metadata about hardware, software licenses, etc. that are needed to run the disk image in a virtual machine or emulator). Add this information to the disk imaging report.

CONDUCT FILE ANALYSIS OF THE DISK IMAGE

1. Run Fiwalk on disk images to generate a Digital Forensics XML (DFXML) file. This can be done within Bitcurator's Disk Image Analysis tool or by running the following command on a computer with SleuthKit/Fiwalk installed
   ```
   $ fiwalk -f -X [path to put DFXML file, for example ~/Desktop/2002.17.5_fiwalk.xml] [path to disk image]
   ```
   Note: Fiwalk cannot read HFS (legacy Macintosh) formatted disks, so this step can be skipped for those disks or drives.

2. Place the DFXML file generated in the Conservation Media drive.

BAG THE IMAGE AND VERIFY THE BAG

1. Use the following command to create a bag for the image on the SRGM Conservation Media drive:
   ```
   $ bagit create [path to destination] [path to source] --verbose
   ```

2. Verify the bag with the following command:
   ```
   $ bagit verifyvalid [path to bag] --verbose
   ```

3. Place any FTK reports, DFXML, or other metadata in the Conservation Media drive.

4. Save the terminal output of the bagging procedure and place in "File Transfer and Metadata" folder of the Conservation Media drive.

5. After bagging and verification have been completed successfully, the files can be deleted from the staging area.

CREATE A RAW IMAGE

1. A raw image is often necessary for the final stage of QC (running the disk image in an emulator or virtual machine). Either FTK Imager or the command "ewfexport" can be used to create a raw image.

2. Start a new disk imaging report. Fields can be copied from the report for the E01. Note in the report that the raw image was exported from the E01.

3. Create a raw image in FTK Imager: Open the program and choose to "Add Evidence Item". Select the "Image File" radio button. Select the path to the E01 disk image file. The disk image should now show up in the "Evidence Tree".

   a. Right-click on the disk image in the Evidence Tree.

   b. Select "export disk image". A new window will appear with options for the image. Click the "add" button. Select "raw". Follow the steps for adding metadata and naming the file as outlined in the sections above. Do not use encryption or fragmentation of the file.

   c. When the raw image is created it should be re-named with the file extension .dd. The extension .raw is not used because it could be confused with a Camera RAW image file.

4. Create a raw image with "ewfexport": Open a terminal window and run the following command:
   ```
   $ ewfexport [path to disk image file]
   ```
   The program will provide a number of interactive prompts. In general, the defaults can be accepted.

5. When the raw image is created it should be re-named with the file extension .dd.

6. Finish filling out the disk imaging report. Assuming the raw image has been verified against the E01, QC is not necessary since the E01 image already went through QC.

7. Place any reports from imaging programs, disk imaging reports, or other metadata on the Conservation Media drive.

8. Bag and verify the raw image on the Conservation Media drive as described in the section above.

9. After bagging and verification of the raw image have been completed successfully, the files can be deleted from the staging area.

APPENDIX I: FORENSIC IMAGING IN TARGET DISK MODE FOR APPLE COMPUTERS

Adapted from "Forensically Sound Mac Acquisition in Target Mode" by Paul Henry (https://digital-forensics.sans.org/blog/2011/02/02/forensically-sound-mac-acquisition-target-mode)

1. Connect a keyboard and monitor to the computer that needs to be imaged (the "target computer"). If the computer is a laptop with integrated keyboard and screen, this step is not necessary.

2. Check to see if there is a firmware password on the target computer. Boot up the computer and hold down the "option" key. If there is a firmware password, the screen will show a lock, otherwise it will display the Start Up Manager with a picture of a hard drive.

3. You may be able to disable the firmware password by shutting down the computer and starting it up again while simultaneously holding down the "command" "option" "P" and "R" keys. If this is unsuccessful it may also be possible to reset the PMU or SMC.

   More information about resetting the PMU can be found here: https://support.apple.com/en-us/HT1431. To reset the SMC for laptops power off the computer. Then hold "Shift" "Control" and "Option" keys on the left side of the keyboard and press the power button at the same time. Hold the keys and the power button for 10 seconds. Release all keys. Press the power button to power on the Mac. For more information, see the following Apple Support article: https://support.apple.com/en-us/HT201295. Note that resting the PMU will reset the date and time on the computer.

4. If there is no firmware password, shut down the target computer.

5. Wait at least 20 seconds and power on the target computer again while holding down the T key on the target computer's keyboard.

6. If the computer successfully starts up in target mode you should see a Firewire or Thunderbolt icon on the screen.

7. Power on the imaging station, turn on the write blocker and connect the target computer to the write-blocker via a Firewire connection. If the target computer only uses Thunderbolt, a Thunderbolt to Firewire adapter will need to be used.

8. Start the disk imaging program of choice. The hard drive of the target computer should now be visible on the imaging station as a mounted device. Go through the standard steps for

imaging a hard drive outlined above.

9. When the image has been acquired, unmount the target computer's hard drive from the imaging computer and shut down the target computer by holding down the power button.