This document is not an original work but adds additional resources to information given in:

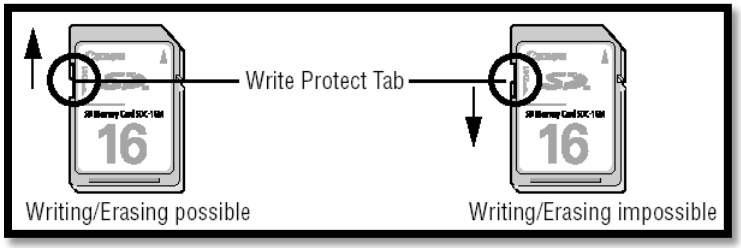
Erway, Ricky. 2012. You've Got to Walk Before You Can Run: First Steps for Managing BornDigital Content Received on Physical Media. Dublin, Ohio: OCLC Research. http://www.oclc.org/research/publications/library/2012/2012-06.pdf.

Erway's article includes a "Technical Steps for Readable Media" and those steps are included here in *italics*. This document includes some additional resources for some of the steps that may trip people up while they are trying to shift from walking to running.

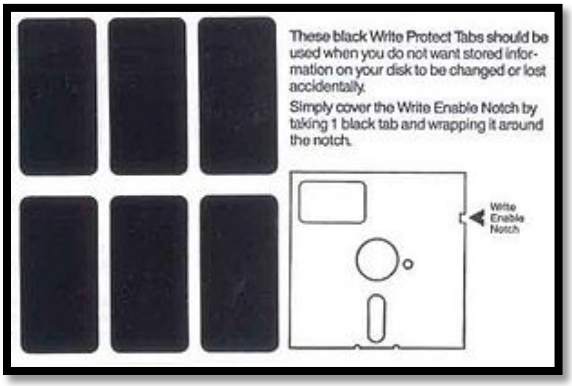
1. Use a "clean" computer (a dedicated computer that is regularly scanned with up-to-date antivirus software and that is not used for online activities that may introduce viruses or used for other work that might be affected by viruses introduced when accessing media).

2. Use a write blocker on the clean computer and set any write-protect tabs on the media to prevent changes to the content.

- Depending on your physical media this is going to be different.
- Many devices such as floppy disks, VHS tapes, cassette tapes, and small memory cards (such as those used in digital cameras) have a switch on them, or an area that can be covered with a sticker to enable write protection.



(Memory disc image: http://www.canon-europe.com/Support/Consumer_Products/products/cameras/Digital_Compact/Powershot_S_series/PowerShot_S20.aspx?faqtcmuri=tcm:13-521580&page=1&type=faq)



(Floppy image: http://wpcontent.answcdn.com/wikipedia/commons/thumb/9/9b/Floppy_tabs_3x2.jpg/300px-Floppy_tabs_3x2.jpg)

- Devices such as external hard drives and USB drives can be protected by getting a physical Write Blocker which some forensic companies have, or enabling a Write Block on the computer (How-to: http://www.techbuzz.in/enable-device-media-write-protection-usb-flash-drives-vista-xp.php). This technique may also protect CDs and DVDs.

3. Insert disk in the appropriate drive (or other medium in appropriate reader or attach other storage device to appropriate port). Do not attempt to open any files.

4. Create a directory on the clean machine for the current project, with a subdirectory for the data files.

- Instructions for creating a new folder in PCs: http://www.computerhope.com/issues/ch000742.htm

5. Copy data from physical media to the subdirectory. Consider copying the data as a disk image, which is a single file that contains an exact, sector-by-sector bitstream copy of the disk's content and ensures that various forms of essential metadata and technical dependencies will be retained. Alternatively, directly copy directories and files from the original medium to the subdirectory, but note that various forms of associated data and metadata may not be transferred. Moving the data directly from the original medium into a zip-compressed archive can help to preserve some file system metadata (e.g., timestamps, directory structures, and file permissions).

- Creating a disk image: http://www.makeuseof.com/tag/create-disk-images-mount-virtual-drive-windows/
- Creating a disk image on Macs: http://www.ehow.com/how_2093946_create-disk-image-mac-osx.html
- Creating a zip file (Both Mac and PC): http://geekbeat.tv/how-to-create-zip-files/

6. Generate a copy of the disk directory information (file names, sizes, extensions, and dates). Store a digital copy in the project directory and print out a copy to keep with the collection.

- How to generate a copy of the disk directory information without downloading software: http://www.theeldergeek.com/file_list_generator.htm
- A similar strategy (again no downloaded software necessary): http://www.forwestmedia.com/resources/how-to-guides/text-file-of-a-directory/

7. Generate and record a checksum (a unique value based on the contents of a file) on the disk image. Alternatively, if you copied the files instead of copying a disk image, generate and record a checksum on each file in the subdirectory.

- A discussion on checksum software: http://www.dpconline.org/advice/faqs/589-faq-simple-checksum-software (Includes links to many free checksum creation and checking programs)

8. Create a readme file containing pertinent information from the above steps, indicating the related analog materials and documenting each step taken. Store the file in the project directory and store a printout of the readme file with the physical collection materials.

- If you are unfamiliar with README files they are basically an instructional/information text file that come with a group of documents: http://en.wikipedia.org/wiki/README (More info)
- To create a README file you can open any text editing program and type the necessary information and then save it as README.txt or something similar to the correct directory location.

9. Copy the project directory to trustworthy archival storage where it will receive regular back up, with a copy stored in another location.

- What is trustworthy archival storage? ...Good question, that doesn't necessarily have an answer yet.
- But…Here is a document that gives criteria and checklist for a trusted repository: http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf

10. Return the original physical media to storage. (This is optional, but it provides one more possibility for back up if something goes wrong. If you choose not to retain the media, discard them responsibly.)

11. Create or update an associated finding aid, collection level record, or accession record with information about the steps that were taken and the location of the files.

These resources were located by: Sarah Fraser