Research made possible by a grant from the Institute of Museums and Library Services

Removable Media

and the use of Digital Forensics

Miriely Guerrero
Bentley Historical Library
IMLS Digital Preservation Intern
July 2, 2012

Table of Contents

Background

For the last decade, the digital realm has steadily encroached upon archives and libraries, bringing with it collections that lean more toward electronic rather than paper records. These digital files have arrived in a variety of formats, ranging from ancient floppy disks to modern external drives. There is little existent literature that would recommend removal media of any type to be a worthy archival medium. Overwhelmingly, the consensus is for the migration of data off these formats and into archival repositories as obsolesces can occur incredibly fast; less than a decade in some cases. Digital records require periodic file format refreshment or migration into sustainable formats, which cannot be done (or is ill-advised) on records residing in magnetic and optical media.

Consequently, there is a valid need for a thorough understanding of the risks and challenges associated with migrating data off these mediums. A need for guidelines and best practices in order to set a processing precedent for existing and incoming collections. Yet, there is scant literature on how to successfully accomplish this. Sadly, among the literature, one fact holds true across the board. Successful migration diminishes as the age of the medium, or hardware necessary to read it, increases. While most studies focuses on the longevity of the medium, no doubt fueled by manufacturing marketing, the true risk lies in the scarcity of hardware necessary to read these formats. Much can be done in terms of establishing an ideal environment and housing for the media itself, but the corresponding hardware is much harder to preserve, with no "ideal" environment or protocols for its perpetuity. As a result, institutions face the very real danger of losing their electronic collections as the potential for access diminishes.

Archives are therefore turning to digital forensics, a science involving the recovery and analysis of digital information, for assistance. Digital forensics provides tools and methodologies for ensuring authenticity by generating audit trails, write-protection and imaging with hash values.[1] As digital materials continue to arrive with increasing volume, these digital forensic methodologies can assist with the bulk processing of data, allowing archivist to massage clusters of data rather than individual files.

Magnetic Media

The floppy disk is currently the most at risk format due to its scarcity and lack of hardware support in contemporary computers. Floppy disks are composed of a plastic case enclosing a film of polyester or a polyethylene base with magnetic particles glued to it (the binder). Data is

[1] John, "Adapting Existing Technologies for Digitally Archiving Personal Lives: Digital Forensics, Ancestral Computing, and Evolutionary Perspectives and Tools," 3.

read off a spinning plastic platter inside. Both the film and platter are coated with magnetic particles made of ferrous oxide that record and store data.[2]

Conventional floppy disk drives contain three basic components: a spindle clamping mechanism to hold the diskette in place as it spins; one or two magnetic read/write heads mounted on a mechanism that moves the heads across the disk's surface; and a sensor that detects the rotational position of the disk via an index hole or magnetic sensor on the disks. The heads are set to the starting position via a sensor in the drive, though there is no mechanism in place to determine whether the heads are properly positioned. This alignment is of particular importance as a disk saved on a misaligned drive cannot be read by another drive.[3] Drives with error checking do exist but they were more expensive and are therefore not standard equipment on most computers.

Floppy disks were sold in an array of sizes, which referred to both its physical dimensions and data capacity. Unlike today's removable media, where the medium's data capacity has no bearing on the hardware necessary to read it, this is not the case for floppy disks. Drives are specially attuned to their corresponding disks; although in some cases some drives do have backwards compatibility. While floppy disks were sold in such sizes as 8", 2", 2½", 2.8", 3", 3¼", and 4", the most prominently utilized were 3½" and 5¼" floppy disks.

5¼" Floppy Disk

The 5¼" disk's most identifying feature is the large circular hole in the center for the spindle and a small oval aperture in both sides of the plastic, which allows the drive's heads to read and write data. A small notch on the right of the disk identifies that it is writable; if not present the disk is read-only. The first disks were 100 KB in size and eventually were expanded to 1.2 MB.

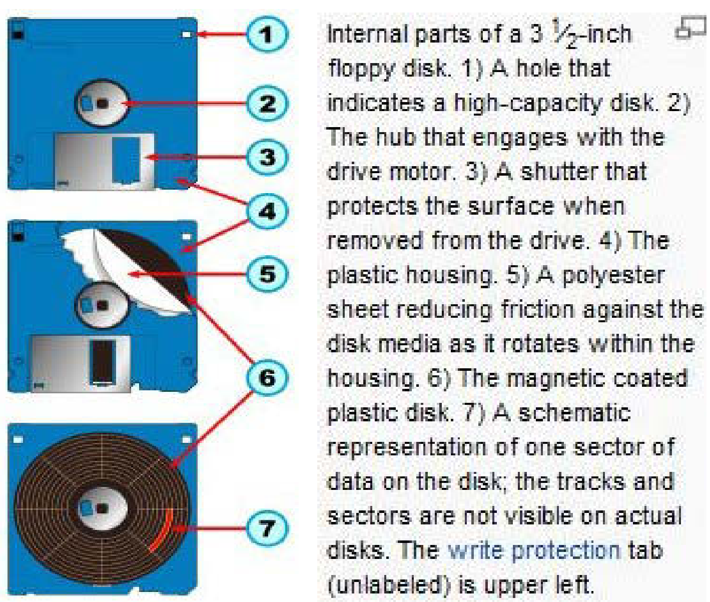
The write protect notch on a 5¼" floppy disk[4]

[2] Florida Department of State Division of Library & Information Services, "Protect your Video and Audio Tapes, and Floppy Disks."
[3] Accurite, "Floppy Disk Drive Primer."
[4] "Digital Archaeology Lab Procedures," 24.

Disks can be either single sided or double sided. While some disks are exclusively marketed as single sided, both sides of the disk are recordable. Despite risk of data loss from friction from the internal magnetic disk rotating in the wrong direction, users developed crude methods for utilizing both sides of a disk by cutting a second write-enabled slot and index hole into the plastic cover. The disk could then be flipped over and reinserted into the drive to expand the capacity, often referred to as flippy disks. This arrangement was the converse of the system used on 8" floppy discs where the notch had to be covered before the disc could be written to. Eventually drives emerged that read a double sided disk without requiring the user to eject and flip the medium. Today flippy disks present a problem in that many drives have difficulty reading the index hole when a disk is inserted upside down because it cannot tell whether the disk is spinning.[5]

3½" Floppy Disk

The 3½" is the most ubiquitous of the floppy disk formats. Most recognizable by its harder plastic shell with spring shutter that covers the magnetic tape, this floppy is an improvement over the 5¼" disk in that it protects the tape from accidental contact or bending. However, due to their hardier appearance, they have traditionally not been treated as delicately as they should have, which increases their likelihood of damage.[6] The write protect mechanism uses a plastic slide, rather than requiring an adhesive label that could fall off inside the drive and cause damage. The data can be protected by moving the slider to uncover the hole.



Cross section of a 3½" floppy disk[7]

[5] Archive Team, "Rescuing Floppy Disks."
[6] Entlich, "One Last Spin: Floppy Disks Head toward Retirement."
[7] *Wikipedia,* "Floppy Disk."

Density

Density refers to how many tracks can be fitted onto a disk and how many bits can be squeezed into those tracks. However, the more data a track has, the greater the likelihood of interference between adjacent tracks. To compensate, higher density disks use weaker write signals, and different magnetic coatings than lower density disks. As a consequence, high density and double density media are not interchangeable and therefore require different drives to be played. While the high density drives are downward compatible with double-density disks, the high-density media itself is not.[8] Disk density can be verified either by the label on the disk or via the properties menu on the computer.

There are five types of available density:

- *Single Density*
- *Double Density:* holds twice as many bits as a single density disk
- *Quad Density:* holds four times as much data as a single density disk
- *High Density:* expands disk capacity allowing a 5¼" disk to store up to 1.2 MB and a 3½" disk to store up to 1.4 MB of data
- *Extended Density:* enlarges disk capacity to 2.8 MB

High density disks have 'HD' displayed on the top right corner and have a hole in the bottom right corner rather than an indent. Taping over or covering up the hole reduces a high density disk to double density. The point of the hole is to help the disk drive determine the density. Extended density disks have a second square hole opposite the high density hole. High density drives can generally read low density disks, but cannot write to low density disks without reformatting or risking the disk's performance in low density drives. High density disks cannot be formatted for use in low density drives.

The most common 3½" disks are the 720 KB double sided, double density disks and the 1.44 MB double sided, high density disks. The 360 KB single sided and the 2.88 MB extra high density type are not very common. Most Macintoshes used either 800 KB double sided, double density or 1.44 MB double sided, high density disks, and the earliest models used 400 KB single sided disks. The 400 KB and 800 KB Macintosh disks used a different encoding scheme that is incompatible with the encoding on PCs. Thus, older Macintosh floppies cannot be read on PC

[8] PC Guide, "Floppy Disk Drives."

drives without special controller hardware. Macintosh floppy drives after 1988 support both types of encoding and can read and write a variety of Mac and PC formats. However, even newer Macintosh disks cannot be read on PCs without special software.[9]

Size	Sides	Densities	Capacity
5¼"	Single	Single	80 KB
	Single	Single	90 KB
	Double	Single	180 KB
	Double	Double	320 KB
	Double	Double	360 KB
	Double	Quad	720 KB
	Double	High	1.2 MB
3½"	Single	Double	360 KB
	Single	High	720 KB
	Double	Double	720 KB
	Double	High	1.4 MB
	Double	Extended	2.8 MB

Variety of formats for the 5¼" and 3½" floppy disks

Formatting

Before a disk can be used, it must be formatted to establish the file system and where the data is to be placed. The formatted capacity is the true maximum capacity of the disk, which is usually about three-quarters of the unformatted capacity.[10] While today's computing options are limited primarily to PC or Mac, the earlier days were host to a diversity of platforms. Among IBM PC and Apple II, were Commodore 64, Atari 810, Kaypro, and many more. Although they all used identical looking 5¼" floppy media, hundreds of incompatible variants existed. Some platforms used single sided media, others double sided. Some used soft sectored disks, while others required hard sectored disks. They also employed several different techniques for encoding the data, organizing file directories, and laying out the invisible tracks and sectors that held that data. For the most part, none of these systems could read each other's data.[11] The plethora of operating systems complicates the preservation of floppy disks as reading the material requires the host operating system it was formatted under. This is further compounded by the fact that unless a disk is labeled, there is no way to identify the operating system, multiplying the host of reasons a disk may not be readable once inserted into the drive.

[9] Entlich, "One Last Spin: Floppy Disks Head toward Retirement."
[10] PC Guide, "Floppy Disk Drives."
[11] Entlich, "One Last Spin: Floppy Disks Head toward Retirement."

There are various possible file formats that are compatible with 5¼" floppy disks, though compatibility also hinges upon the low level format of a disk and the computer drive it is intended for:

- *CP/M:* found on some 5¼" disks intended for use with CP/M operating system. As MS-DOS gained popularity it supplanted CP/M, which then rapidly declined from 1981.

- *File Allocation Table 12 (FAT12):* FAT was, until 2000, the file system of choice for MS-DOS and Microsoft Windows. FAT12, the first FAT version introduced in 1977, was designed specifically for floppy disks and replaced CP/M as the most common file system found on floppy disks.

- *Apple DOS File System:* in 1978 Apple introduced Apple DOS File System, their own system designed for Apple computers and floppy disks and hence only compatible with Apple operating systems.

- *Disc Filing System (DFS):* designed in 1982 by Acorn Computers for their 5¼" floppy disk drives. This uses FM encoding, therefore only produces single density disks. A double density disk can be formatted to use DFS, but this would render it single density.[12]

As floppy disk production developed, so did the range of file systems available. Therefore, there are more possible file systems to be found on 3½" floppy disks:

- *Apple DOS File System:* Apple II's UniDisk 3½" Drive used this file system, but the drive was never very popular and was soon discontinued.

- *Macintosh File System (MFS)***:** created by Apple and introduced along with their Macintosh 128 KB computer in 1984. It can be used with Apple's 400 KB 3½" disks, but cannot support the 800K disks. From the Mac OS 8.1 onwards (1998) Apple computers were no longer able to use MFS.

- *Hierarchical File System (HFS):* developed by Apple in 1985 as a revised version of MFS. An improved version, HFS+ was introduced in 1988. Like MFS, HFS is only compatible with Macintosh operating systems.

- *DFS:* Early Acorn 3½" disks were formatted to use DFS, but this was later replaced with Advanced DFS.

---

[12] PC Guide, "Floppy Disk Drives."

- *Advanced DFS (ADFS):* ADFS, introduced in 1983, uses MFM encoding and so supports Acorn's double density 3½" floppy disks up to 640 KB in size. However, ADFS cannot support high density disks and ADFS formatted drives are not compatible with DFS disks.

- *Extended File System (ext):* ext was created in 1992 specifically for Linux systems and was replaced by ext2 in 1993.

- *FAT12 and FAT16:* FAT12 was the file system of choice for 3½" disks until 1987 when FAT16 was introduced.

- *New Technology File System (NTFS):* in 1993 NTFS was introduced as the standard file system for Windows operating systems, superseding FAT by 2000.[13]

In addition to floppy disks, there are also Zip disks and magnetic optical disks that while not as pervasive, still merit attention.

Zip Disks

While somewhat similar in appearance, the primary difference between a Zip disk and a floppy is the magnetic coating used, as on a Zip disk the coating is of a much higher quality. This means the read/write head on a Zip disk can be significantly smaller than on a floppy disk and squeeze thousands of tracks per inch onto the disk surface. Zip drives also use a variable number of sectors per track to make the best use of disk space. The Jaz cartridge, another type of Zip disk, is somewhat analogous to taking a hard disk and placing it in a case as it is composed of several platters inside, but the read/write heads are located in the drive, rather than the disk. Notably, the Jaz drives do not possess internal cooling mechanisms, exposing the disk and drives to high temperatures.

Much like the floppy disk drive, Zip drives that hold smaller formats will not read larger sized Zip disks, though there is backwards compatibility in that larger drives will read smaller disks (though not write to these disks). The Zip drives comes in several configurations, for both internal and external installation, including SCSI, USB, firewire, parallel port and internal ATAPI. The primary danger associated with Zip disks is the "Click of Death." Resulting from poor manufacturing quality, drives will inexplicably fail, damaging the cartridges used. The failure is generally preceded by a distinguishable clicking sound that indicates the drive is having difficulty reading the data. Once the disk is damaged in a defective drive, it cannot be read in other drives.[14]

[13] Ibid.
[14] *Wikipedia,* "Zip Drive."

Magnetic Optical Disks

On the surface, magnetic optical disks look like floppy disks. However, they are actually written to magnetically (with thermal assist) and read optically. The most common formats are 5¼" and 3½". The Floptical disk, another type of magnetic optical disk, is distinctive in that it has the ability to also read and write 720 KB and 1.44 MB floppy disks. However, there are several drawbacks involved with this format: the need to install a special controller card; drive cannot be attached to a normal SCSI adapter; disks require special BIOS routine in order to be formatted.[15]

Magnetic Media Dangers

Inherit in any media are degradation risk ranging from environmental to hardware. Dust, dirt and fingerprints are particularly dangerous to floppy disks as they can erase or lift information off the media. The more exposed the magnetic tape is, the more danger of data loss. For instance, a 5¼" floppy disk is more likely to be damaged than a 3½" disk due to the exposed magnetic strip. It may take several tries to read a floppy, and transfer of some older formats will be incredibly slow. Due to temperature changes, friction or debris and growths on the tape, magnetic media can fall prey to weak bits, which results in the hardware detectors inability to read the media.[16]

Temperature

The binder is easily damaged by high levels of heat or humidity, becoming soft, sticky or very brittle. Soft or sticky tape can prevent the platter from spinning and reading the information, breaking the hardware. Brittle binder will flake off the tape and lose the information.[17] Changes in temperature can cause condensation to develop and cause the materials to expand or contract, causing the entire unit to warp. This can be somewhat mitigated by allowing the disk to become acclimated before playing (if the environment is different). Mold will start to grow at around 60% relative humidity, and if the humidity fluctuates more than 10% in 24 hours or the temperature is too high, the disk can be subjected to physical stresses that will accelerate the deterioration. Environmental fluctuations can also cause the magnetic and base layers to separate, or cause adjacent layers in a reel of tape to block together. High temperatures may also weaken the magnetic signal, and ultimately completely demagnetize the magnetic layer.

---

[15] Yesterday's Technology, "Floptical Disks."
[16] Cohen, "Recovering Data from Floppy Failing Floppy Disks."
[17] Florida Department of State Division of Library & Information Services, "Protect your Video and Audio Tapes, and Floppy Disks."

Demagnetization

Magnetic fields can be generated by items such as fridge magnets, magnetic screwdrivers and most machines with electric motors. The degree of risk depends on several factors: how close the media is to the source of the field, the strength of the field, and the duration of exposure. The effect of a magnetic field decreases with distance. Single and double density media more susceptible to decay due to lower level magnetic fields used to record the data. The particles which retain the coded information in the magnetic layer can become unstable, leading to a gradual loss of signal quality and eventually to total information loss.

Hardware

Due to their age and lack of contemporary use, floppy disk drives are hard to acquire and improper or unavailable drivers for the appropriate operating systems will render any reading of the media impossible. Installing and booting the necessary hardware and controllers to play different floppy drives is complicated and requires specialized skill. The 5¼" drives present a particular challenge in that generally they cannot be hooked up to modern PCs because the systems lack the proper cabling, controller support, internal drive bay, and/or BIOS support. In addition, hardware for more unusual floppy types, such as hard-sectored disks, is increasingly harder to find and get operational.[18]

Head Misalignment

Over time a floppy disk drive can develop difficulties if the track positioning of the actuator drifts from what is normal, leading to head alignment problems. This reduces the strength of the data signal detected by the head and may also cause unwanted interference between adjacent tracks, or incomplete erasure when data fields are re-recorded while saving. When the heads become misaligned, a disk will work if formatted, written and read in the same drive, but will not work on other drives.[19] This results in disks that while they can be read on the drive where they were saved, are unreadable on other drives that do not possess the exact same misalignment (in other words, it may work just fine for the donor, but not for the archive). In general, a misaligned drive may still read regular disks, but not those of lower quality or in bad shape.

In addition to head misalignment, data errors may also be caused by the heads being rotated slightly on their axis (azimuth), improper head angle, and disk or motor spindle eccentricity.[20] Fortunately, there is significant leeway allotted for in drives, so that a drive would have to be severely out of alignment in order to render it useless. Dust or dirt can damage the hardware

[18] Entlich, "One Last Spin: Floppy Disks Head toward Retirement."
[19] PC Guide, "Floppy Disk Drives."
[20] Accurite, "Floppy Disk Drive Primer."

necessary to read the floppy by scratching the platter and can also affect how the sensors work. Occasionally problems can cause the disk-change sensor or circuitry to malfunction, causing strange problems as a result. This results in the system not recognizing new disks and behaving as if the previous disk is still inside the drive. When a file is accessed on the new disk, the drive will indicate "file not found" because it is consulting its memory of the last disk rather than the one in the drive. If one attempts to write to the new disk, it can potentially scramble its contents, as the controller assumes it is writing to the previous disk.[21]

Copy Protection

Some commercial floppy disks attempted to prevent copying by installing mechanisms to block this action. Some would use the documentation or included items in the package and have the software query the user to verify they paid. Some used hardware dongles (although generally this was high-end software) or copy protection on the disks themselves. For instance, spiral tracking is where a computer will start up off the boot sector of the disk, but then the booted operating system will force the drive head to act counter-intuitive to what any regular floppy would be expected to present. In other words, a standard disk-copy program will duplicate the drive as if it has regular tracks, but will fail on it, resulting in protected software. Consequently, in cases where a drive indicates errors copying a disk, it may not actually be a bad disk, but rather the copy protection.[22]

Recommendations

- Floppy disks should be kept at a temperature of 64°F - 68°F, with relative humidity between 30% - 40% and sudden environmental changes should be avoided. Also avoid leaving disks close to heat sources, such as inside or on PCs. Disks are sensitive to magnetic fields and intense vibrations and should therefore be kept away from magnetic sources like cabinets with magnetic locks or lamps with metal bases.

- As the magnetic tape on a floppy disk is very fragile, and its source of protection (plastic casing on a 5¼" disk or the metal shutter on a 3½"disk) can be easily damaged, avoid writing on floppy disks with pencils or ball point pens, touching the tape, or affixing labels.

- Avoid paper or cardboard based storage slips as they can attract moisture and may raise the RH of the immediate surroundings of the carrier which may increase the rate of chemical decay, as well as generating fibers and dust.[23] Instead store un-crowded disks vertically in Tyvek sleeves.

---

[21] PC Guide, "Floppy Disk Drives."
[22] Archive Team, "Rescuing Floppy Disks."
[23] Finch, *Caring for CDs and DVDs*, 7.

- When reading disks, always ensure the disk is write protected by sliding the write protection tab on the 3½” disk or taping the cut out on a 5¼” disk. Do not say “okay” if prompted to reformat disk. It may take several tries to read a disk and occasionally there are problems with a computer reading the previous disk rather than the current disks (press F5 to refresh when this occurs).

- The use of a test diskette is helpful in determining whether read errors are a result of the disk or hardware. Also recommended is the purchase of drive alignment diskettes to ensure the floppy drive does not become misaligned, as this can occur gradually without warning of impending failure, and the purchase of a drive cleaning kit to prevent gradual residue build up on drive heads, as dirty surface error can lead to copy or read errors.

- The older the format the more in danger it is. Typically the medium outlasts the player as media life is considerably longer than the length of time most users maintain the hardware necessary to play it. Older formats are at higher risk than their younger counterparts (e.g. a 400 KB floppy disk is at higher risk than a 1.44 MB floppy disk).

Optical Media

Recognized as a medium that is read by laser light, optical media is at present the most ubiquitous format due to its continued use – although it is phasing out as a storage medium as flash drives continue to gain traction. The most common formats, CD and DVD, fall under three broad categories: pre-recorded, write-once and rewritable. Pre-recorded and write-once optical media are considered to be more stable than magnetic media. However, studies on disc longevity for the various types of CD and DVD types range from as little as two years to as high as 200 years. It is difficult to ascertain disc longevity at face value, as life span hinges upon several inter-related factors: type, manufacturing quality, disc condition before recording, quality of the disc recording, environmental conditions, handling, and maintenance.[24]

All CDs and DVDs are made of the same basic material, polycarbonate (plastic), which gives the disc sufficient depth to be read by the laser and the strength to lay flat. CDs are comprised of a substrate layer, a reflective layer and a protective lacquer layer. A DVD differs from a CD in that it is composed of two fused pieces of polycarbonate, like two thin CDs glued together.[25] A DVD can also be read and written to on one or both sides, whereas a CD is limited to just one side. Data is recorded in the inner layer of a disc and this is more likely to degrade than the harder outer layers. In addition, brand is no indicator of quality as often discs have been purchased

[24] Byers, *Care and Handling of CDs and DVDs: A Guide for Librarians and Archivists*, 5.
[25] Ibid, 12.

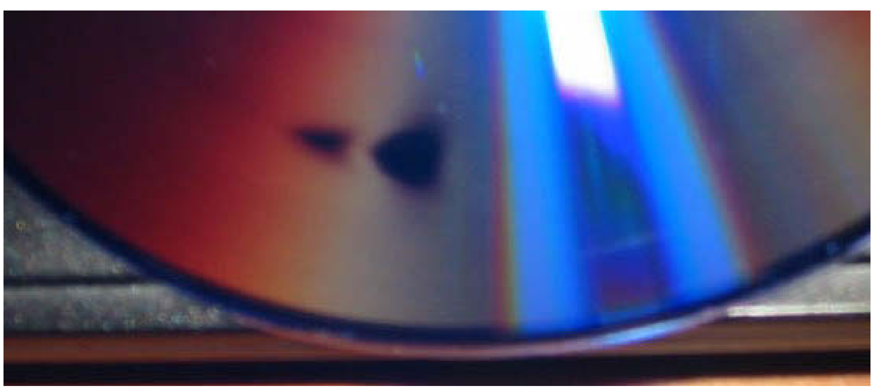
from cheaper manufacturers and rebranded.[26] ISO 9660 is the International Organization for Standardization's file system for CDs that specifies the directory format of the disc and allows read-only interoperability across all computer platforms.[27]

CD-	DVD-	Type	Data Layer	Metal Layer
CD-ROM Audio/Video and PC use	DVD-ROM Video/Audio and PC use	Read only	Molded	Aluminum (also silicon, gold, or silver in double layered DVDs)
CD-R	DVD-R DVD+R	Recordable (Write once only)	Organic dye	Gold, silver, or silver alloy
CD-RW	DVD-RW DVD+RW DVD-RAM	Rewritable (Write, erase, and re-write)	Phase-changing metal alloy film	Aluminum

Optical disc formats[28]

Pre-Recorded Formats

Commercial CDs and DVDs are not written by heat, but by molded data pressed onto a spiral track of pits that hold the information. CD formats written in this manner include Audio-CD, Video-CD, CD-I (Compact Disc Interactive), CD+G (Computer Disc plus Graphic) and DVD-Video and DVD-Audio for DVD. Other formats, such as miniCD and business card CD, are not as common and therefore not discussed in this report. A CD-ROM's or DVD-ROM's propensity to decay is linked to its aluminum layer's exposure to oxygen, since oxygen, via moisture, can travel through the polycarbonate layers. This penetration is augmented by scratches, cracks or delamination on the disc. The end result is oxidation and a decrease in the disc's ability to reflect light, often referred to as disc rot.[29]



Disc rot on an optical disc[30]

[26] Bradley, *Risks Associated with the Use of Recordable CDs and DVDs as Reliable Storage Media in Archival Collections - Strategies and Alternatives*, 9.
[27] JISC Digital Media, "Using Optical Media for Digital Preservation."
[28] Byers, *Care and Handling of CDs and DVDs,* 5.
[29] Byers, *Care and Handling of CDs and DVDs,* 9.
[30] *Wikipedia,* "Disc Rot."

Write-Once Formats

Writable discs, consisting of CD-R, DVD-R, and DVD+R, differ from commercial discs in that they are written on a dye layer between the polycarbonate substrate and the light reflective layer. 3There are three basic dyes that can be identified by color: cyanine (blue), phthalocyanine (clear light green), and azo (deep blue). The ultimate color of the CD depends upon how the dye reacts to the base metal of the reflective layer.

Dye Type		Color appearance (Viewing the laser reading side of the disc)	
	Actual Color	On Gold Metal	On Silver Metal
Phthalocyanine (thalo-sy-a-neen)	clear or very light green	gold or greenish gold	silver
Cyanine (sy-a-neen)	blue	green	blue
Azo (ay-zo)	dark blue or deep blue	dark green	dark blue or deep blue

Writable disc dye color options[31]

The dyes vary in quality and can degrade or become oxidized, leading to a loss of data. Discs optimized for faster recording speeds use less dye and therefore degrade faster. Speed is a more detrimental factor than how densely the data is packed onto the disc, as a low density disc recorded at a high speed will have a higher incidence of error rates. Cyanine is recognized as the least reliable of the dyes with a shorter life span. Azo is commonly used in discs claiming to be archival and tests indicate phthalocyanine has the longest shelf life. It should be noted that for a DVD, disc color is not indicative of the dye used.[32]

Writable CDs that are silver based are at risk of carbon dioxide, which can penetrate the polycarbonate layer via moisture, although it is less likely than with ROM discs. However, these are popular as silver is more reflective and cheaper than gold. In response, many CDs are composed of silver alloys to reduce corrosion. Archival gold CDs are lauded as archival quality as the gold in the discs will not corrode.

While pre-recorded CDs and DVDs are at minimal risk to light sources (e.g., UV, infrared, fluorescent, it would take decades for any damage and would result in potential clouding that may not affect playback), heat from ultraviolet light is incredibly detrimental to writable discs because the polycarbonate substrates react to heat, which leads to warping and causes oxidation of the reflective layers.[33] It can also lead to mold growth. Ultraviolet light accelerates aging by altering the appearance of the recording layers. The different layers will delaminate

[31] Byers, *Care and Handling of CDs and DVDs,* 8.
[32] Bradley, *Risks Associated with the Use of Recordable CDs and DVDs as Reliable Storage Media in Archival Collections - Strategies and Alternatives*, 6.
[33] Byers, *Care and Handling of CDs and DVDs,* 18.

(peel off the CD) or yield to the double bending of light which will result in errors when attempting to read the disk or flat out failure. Error correcting software will correct some of the errors if the delamination is at the outer edge, as data is read from the middle outwards.[34]

Delamination on a CD[35]

Rewritable Formats

Rewritable discs, CD-RW and DVD+/-RW, and DVD-RAM, are the least stable of all the optical mediums as the metal alloy they are composed of is not as stable as the dye present in writable media. It makes the disc sensitive to ultra violet rays and oxidation of the reflective metal layer. Laser heat is used to change the recording area from metallic to crystalline. They can be rewritten 1,000 times, although the frequency in which they are rewritten affects their life expectancy. Consequently, information on a writable disc is deemed more reliable than on a rewritable disc in terms of longevity. DVD-RAM is like a virtual hard disc, formatted for random access, much like a computer hard drive. These can be rewritten 100,000 times.

The primary difference between DVD- and DVD+ is how the laser follows the track while writing data to the disc. This is mainly important when writing data to the disc as some drives can only write to either + or -. However, in regards to reading the media, most drives can read both formats. Consequently, how the disc rotates differs as well as how easily the data is read, particularly on discs with multiple sessions.[36]

---

[34] Finch, *Caring for CDs and DVDs*, 9.
[35] Shahani, "Longevity of CD Media."
[36] Byers, *Care and Handling of CDs and DVDs,* 32.

Optical Media Dangers

Difficult to ascertain at a glance the reliability and quality of a CD as this depends not only on the disc, but also on the hardware used to record and play the disc. For instance, PCs have no problem reading recordable CDs that were left with an open session after burning, but attempting to read such a CD on Mac would require special software. Error correction code is a system of recording redundant data onto disc so that during playback, this redundant information helps to detect and correct errors that may arise.[37] A disc will fail, which may take the form of skipping, data loss, freezing or crashing, once the errors overwhelm the error correction code. While the threat to removable media obsolesces is predominately hardware related, there are still some dangers associated with the medium itself that should be acknowledged.

Labeling and Writing

Labels are frowned upon in general as they pose an additional environmental threat in that they can dry out or absorb moisture and are more sensitive to heat and cold than the disc itself. Inserts and booklets should not be stored with the disc for similar reasons. Poorly made or affixed labels can cause the disc to vibrate in the player, causing read errors or even damaging the drive. Adhesive from earlier labels have been found to react with lacquer surface, potentially leading to delamination. Removing labels off DVDs is not as detrimental as it is with CDs, but it is still ill advised as it can affect the balance of the DVD in the player, making the disc unreadable and eventually wear down the drive itself.[38] DVDs are more susceptible to reading problems from minor imbalances than CDs. Writing on CD/DVDs with solvent based markers or pens can penetrate the hard layer and deform, discolor or corrode the disc, causing permanent reading problems for the laser.

Surface Defects

Since the data is not recorded on the surface of the disc, light scratches do not affect the readability. Error detection and correction coding work toward recovering misread data errors from scratches, so long as they run outward from center of disc. Unfortunately, deep, wide or bunched together scratches do affect the data. Particularly those that run in the direction of the track or the same direction as the laser reads the disc. Very deep scratches cannot be read or repaired. Ironically, scratches or indentations (even from a pen) on the label side of a CD are more detrimental as the data lies closer to that surface and cannot be repaired.[39] As the data in a DVD is recorded in the middle, scratches do not pose such a threat. However, since DVDs

[37] Optical Storage Technology Association, "CD-Recordable Glossary."
[38] Byers, *Care and Handling of CDs and DVDs,* 23.
[39] Finch, *Caring for CDs and DVDs*, 10.

have a much higher data density in that the bits are packaged closer to each other, they are therefore more easily obscured by debris on the disc's surface.

Scratches also open the door for environmental intrusion, allowing moisture and pollutants to more easily penetrate the disc. Fingerprints, smudges, dirt or dust are more disruptive than scratches. Severe instances can cause data to be misread by laser as they cause it to go out of focus and lose intensity. Anything present in or on this surface, such as dust, dirt, fingerprints, smudges, solvents, liquid, or scratches, will cause the disc to misread. Accelerated aging tests indicate discs are susceptible to the development of spots. Either black or white, these markings form either on or within the polycarbonate or reflective surface.[40] Although not very common in later discs, earlier poorly manufactured discs are at risk of developing laser rot, which is the corrosion of the reflective layer that can cause discoloration or pitting.[41]

Surface defects on a disc[42]

Hardware Incompatibilities

Older CD-RW drives lacking appropriate firmware that allows the software to communicate with the hardware in order to handle newer, high speed CD-RW discs (poor forward compatibility), while newer drives can generally record to older CD-RW discs, provided their firmware can set the correct speed, delay and power settings for the task. Standards ensure discs can be written and played on different manufacturers' machines. However, lack of standardization for replay and recording technology exacerbates this problem as the variance in standards can cause irregular incompatibilities between discs and drives, leading to failed discs. Discs that do not play on one machine may still work on another; conversely, discs created on one drive may not play on another. Lack of adherence to standards has resulted in a greater burden on the end user to ensure the disc they have created will endure as there is no reliance

[40] Shahani, "Longevity of CD Media."
[41] Iraci, "The Relative Stabilities of Optical Disc Formats," 134.
[42] Shahani, "Longevity of CD Media."

on technology to ensure optimum disc life as the standards apply only to the medium and not the hardware.[43] For instance, calibration information encoded in the polycarbonate layer may be incorrect or not precisely accurate. Sometimes drives calibrated for dye based discs (writable discs) cannot read rewritable discs.

Recommendations

- Discs should be kept at the ideal temperature of 64° F with relative humidity at 40%. Sudden changes in temperature or humidity can cause optical disks to warp, but they can be flattened out with weights and time. Prolonged exposure to moisture or ultra violet light should also be avoided. Discs should always be stored vertically in their corresponding jewel cases, away from all booklets or paper. They should not be allowed to lean, nor stored too tightly on the shelves.

- Never flex, bend or place pressure on CD, even when removing from jewel case. Do not touch surface or scratch label side of disc. Instead always wear vinyl or nitrite gloves and hold disc by outer edge of center hole.

- Although mild solvents like quick evaporating isopropyl alcohol or methanol is permitted, in general the use of solvents, either for writing or cleaning, should be avoided as they can still affect the label and consequently the disc. For instance, ammonia based cleaners can cloud the disc surface. Use air puffer for the cleaning of media and hardware before attempting to use solvents. Never clean in a circular pattern and scratch filling tools should be used sparingly as they can increase uncorrectable error rates or cause other read errors.

- An error-free disc will open much faster than an error-ridden one. If a particular disc is much slower than other similar discs, consider this a warning and copy it as soon as possible to another disc.

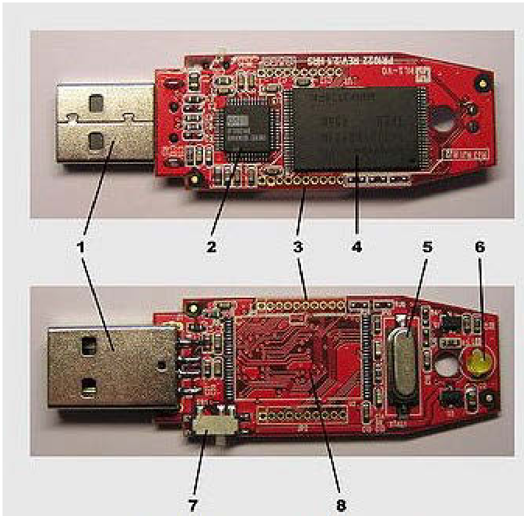
Solid State

Solid state media is so called due to its lack of removable parts. The most common format is the USB flash drive, which is characterized by internal flash memory and an external USB port. Data is written to the medium via an electron gun and high voltage electricity to change the data bits.[44] Most flash drives ship preformatted with the FAT12, FAT16 or FAT32 file systems and can be partitioned just like hard drives. Unlike floppy disks, they do not need to be formatted in order to work in different operating systems as they are part of the mass storage devise class.

---

[43] Bradley, *Risks Associated with the Use of Recordable CDs and DVDs as Reliable Storage Media in Archival Collections - Strategies and Alternatives*, 7.
[44] Tyson, Jeff. "How Removable Storage Works."

This protocol provides an interface to read write data so that a particular file system or drivers are not necessary.



1	USB Standard-A plug
2	USB mass storage controller device
3	Test points
4	Flash memory chip
5	Crystal oscillator
6	LED
7	Write-protect switch (Optional)
8	Space for second flash memory chip

Cross section of a USB flash drive[45]

Although limiting the drive to extremes in temperature and from liquids is a wise practice, a USB drive's longevity is affected more by its use than its storage. An incredibly robust medium impervious to magnetic fields, scratches and dust, it will degrade with repeated use in a manner similar to metal fatigue mode, in that the device fails by refusing to write new data to specific cells.[46] The drives only notable weak spot is the stress point where the metal casing connects to the drive's body.

Solid state media, as well as other formats like external hard drives and computers, can hold massive amounts of data. While a floppy disk at its largest is only 2.88 MB, hard drives can measure up to terabytes in size. As solid state media is not typically utilized as an archival storage format, the primary preservation concern is maintaining the integrity of the information during transfer. Unlike magnetic and optical media, where write protection is easily ensured, solid state media affords no such protection, leaving the data in danger of being accidentally altered during access. Since it is easier to spoof metadata on digital systems, such as author or creation date, it is important to demonstrate not only how the information was acquired but to ensure it was not modified before, during or after transfer. File types like templates, for instance, will update content when opened. The simple act of turning on a computer modifies the environment and can corrupt a file's underlying metadata.

[45] *Wikipedia,* "USB Flash Drive."
[46] Ibid.

Digital Forensics

Digital forensics is a branch of forensic science that focuses on ensuring the authenticity of information as it is transferred from one storage medium to another, generating documentation that can be used to trace an object's chain of custody, determine its integrity, and accurately represent its context within the larger body of materials.[47] The discipline evolved around three basic tenets: acquire the evidence without altering or damaging the original, establish and demonstrate that the examined evidence is the same as that which was originally obtained, and analyze the evidence in an accountable and repeatable fashion.[48] It was originally used as a means for law enforcement, computer security and national defense to discover, authenticate and analyze data in cyber-crimes.[49] It provides a means to verify whether what a system is indicating is in actuality truth and maintains the integrity of the operating environment, thereby allowing archivists to look without touching. Digital forensic output is of particular interest to archivist seeking insight into how a creator worked. The desktop background, font and screen resolution and how a desktop is arranged can be as revealing as the work performed on it.[50]

Institutions	Project	Tools	Website
Kings College London	Forensic Investigation of Digital Objects (FIDO)	Sleuthkit, Autopsy, PTK, Digital Forensic Framework, PyFlag, OSForensic	http://fido.cerch.kcl.ac.uk
Maryland Institute for Technology in the Humanities *University of North Carolina - Chapel Hill*	BitCurator	Guymager, aimage, fiwalk, bulkextractor, sdhash, Nautilus scripts and DFXML tools	http://www.bitcurator.net
University of Virginia *Stanford University* *University of Hull* *Yale University*	An Inter-Institutional Model for Stewardship (AIMS)	FTK3.3, FTK Imager 3.0, Karen's Directory Printer	http://www2.lib.virginia.edu/aims/
Stanford	Sulair's Digital Forensic's Lab	Forensic computer setup	http://lib.stanford.edu/digital-forensics/sulairlab
Maryland Institute for Technology in the Humanities	Mith's Vintage Computers	Forensic computer setup	http://mith.umd.edu/vintage-computers/
University of Texas - Austin	Digital Archaeology Lab	Forensic computer setup	http://www.ischool.utexas.edu/labs/archaeology_lab.php

Institutions currently engaged in digital forensic project work

47 Kirschenbaum, "Digital Forensics and Born-Digital Content in Cultural Heritage Collections," 34.
48 John, "Adapting Existing Technologies for Digitally Archiving Personal Lives: Digital Forensics, Ancestral Computing, and Evolutionary Perspectives and Tools," 2.
49 Kirschenbaum, "Digital Forensics and Born-Digital Content in Cultural Heritage Collections," 1.
50 Ball, "Digital Forensics for Preservation."

Imaging

Imaging is the act of generating a single file containing the complete contents and structure of a data storage medium, such as a floppy disk, a flash drive or a hard drive. A disk image is created by initiating a complete sector-by-sector copy of the source.[51] As digital files are seldom stand-alone objects, but instead connected to their environment, imaging the entire contents of a device ensures all the components necessary to render the file properly are captured. Attempting to transfer individual files from one operating system to another would be very time consuming and potentially generate errors. Imaging, however, involves the bit stream transfer of data without having to worry about incompatibilities between the operating systems, as the image is treated as a single file. However, once individual files are accessed, incompatibility problems do arise.

There are two options, logical or bit-exact (also referred to as a clone), when capturing an image. A logical image copies only the sectors which contain data, ignoring any zero byte sectors and thereby resulting in a smaller file. It can also be directed toward a specific directory, rather than the entire drive. These 'folder contents only' forensic images recreate the device as it would appear in normal use.[52] Bit-exact images contain the entire disk, resulting in a file the same size as the original medium's full capacity.[53] There are three imaging formats:

- *Raw/DD Format:* most basic image file. There is widespread support in range of forensic, virtualization, and other tools. Although it lacks support for embedded metadata and fixity, it does allow for storing metadata as a separate file.[54]

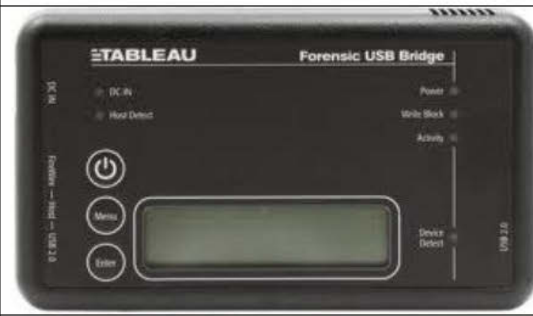
- *Encase Evidence Format:* de-facto standard supported by EnCase and OSS. Supports block-by-block checksums enabling the investigator to determine the sector that has been corrupted.[55]

- *Advanced Forensic Format (AFF):* extensible open format comprised of data storage and disk representation. Has less support than Raw or Encase formats. Enables the storage of metadata that is integrated within the image bitstream and also incorporates the user of digital signatures that facilitate the process of authenticating the hash values themselves.[56] It also stores the imaged disk as a series of pages or segments, allowing the image to be compressed and accessed randomly.[57] Comes with a set of tools including a disk-imaging

[51] *Wikipedia,* "Disk Image."
[52] Herbert, "Forensic Workstation, Pt3."
[53] Kirschenbaum, "Digital Forensics and Cultural Heritage Glossary."
[54] Knight, "Digital Forensics in the Archive: Using Open Source & Free Software to Capture and Curate Archival Digital Records."
[55] Ibid.
[56] John, *Digital Lives: Personal Digital Archives for the 21st Century >> An Initial Synthesis*, 72.
[57] Garfinkel, "AFF: A New File Format for Storing Hard Drive Images," 86.

program (aimage), a program for converting AFF metadata into XML (afxml), and a program for converting raw images to AFF images and back (afconvert).[58]

Before imaging can occur, the source medium must be write protected. With a floppy this involves taping the cut on 5¼" disk or sliding the notch on a 3½" disk (CDs cannot be accidentally written to). Flash drives and hard drives, however, require forensic disk controllers. These devices intercept write commands from the host operating system, preventing them from reaching the drive.[59] Once a write blocker has been attached, the contents can be safely migrated.

Type of Device	Which Write Blocker	
USB devices (external hard drives and pen drives) **Media cards** (use USB card reader)	Use **Write Blocker 1** (T8-R2)	
Hard drives from desktop and laptop computers	Use **Write Blocker 2** (T35es) Use the adapter kit with smaller laptop hard drives	

Sample Write Blockers[60]

Once an image is generated, it must be mounted or a virtual machine set up, in order to access the individual files. Taking an image and mounting it onto a virtual drive essentially fools the computer into thinking there is a new drive. Mounting ensures that the computer recognizes the media's format, and instructs the computer to incorporate the media's file system into the local file system. As mentioned in the magnetic media section, formatting is important as it instructs the computer on where the data begins and ends, where it can be written to, and how to read data that has already been written. If the computer cannot recognize the file format or it is corrupted, it will return errors and will write data incorrectly, possibly rendering unrecoverable all the files stored on the media.[61]

58 Ibid.
59 *Wikipedia,* "Forensic Disk Controller."
60 Hull History Centre, "Idiot's Guide 2 - Tableau Write Blockers."
61 Indiana University Information Technology Services, "What is Meant by Mounting a Drive?"

Processing

The drawback to imaging is it captures files one would not necessarily wish to preserve, such as utility files, proprietary software that is copyright restricted, deleted content and information a donor would not necessarily wish to share, such as medical, financial, and browsing history. To bypass this, hashes can be used to compare against existing libraries to quickly distinguish user created files from information that can be removed or ignored, such as operating system files, third party files, malware, viruses, and Trojan files. Hashes are also used to ensure the copied image is faithful to the original and that the data is not altered in any way. It can also assist with de-duplication, the act of identifying duplicate files for removal.[62]

Digital forensics provides a macro view of the collection and its tools allow for the massaging of data as a whole. Customizable scripts can be devised that manipulate the data, weeding out sensitive information and identifying copyright restrictions. As collections increase in size, this level of automation is beneficial as it reduces the need to engage in item level processing or repetition. Detailed logs of what actions have been performed are also a mainstay of most software and assists in documenting the provenance of a file. Methods and tools of digital forensics can also be applied upon an image to gather a wide range of information.

- Rather than sift through an entire drive, these tools can assist archivist in narrowing in on a topic of interest. Referred to as clustering, this allows for the grouping of similar documents that can assist in narrowing the focus or conducting a directed search.

- Annotation and bookmarking can highlight materials of interest. Visualization and time lining tools can aid in understanding the range of materials in a donation and assist archivists in exploring the history of a record by providing the contextual environment in which the records were created. [63]

- Creation of system-wide metadata of the collection as a whole and a manifest or inventory of the donated files.[64]

- Understanding digital formats offers clues to where to find item-level metadata (e.g., document properties embedded in word processing files, ID3 tags embedded in MP3 audio files, etc.) and suggests migration paths for long-term preservation.[65]

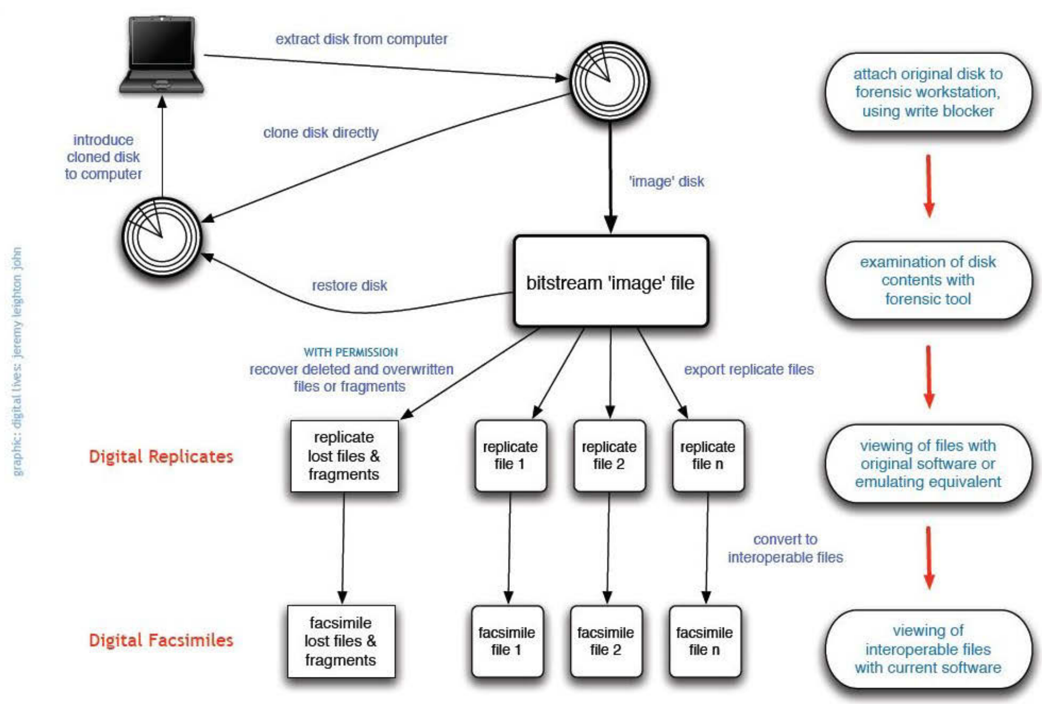
- Software allows for deep indexing (including text within files) and extraction of metadata relating to files including file extensions and types, signature, dates and times,

[62] Ball, "Digital Forensics for Preservation."
[63] Ibid.
[64] Kirschenbaum, "Digital Forensics and Born-Digital Content in Cultural Heritage Collections," 2.
[65] Stollar, "Guarding the Guards: Archiving the Electronic Records of Hypertext Author Michael Joyce."

permissions, hash values, logical size, physical location, and file extents.[66] Such as block device structure and file system, installed operating systems and software components.[67]

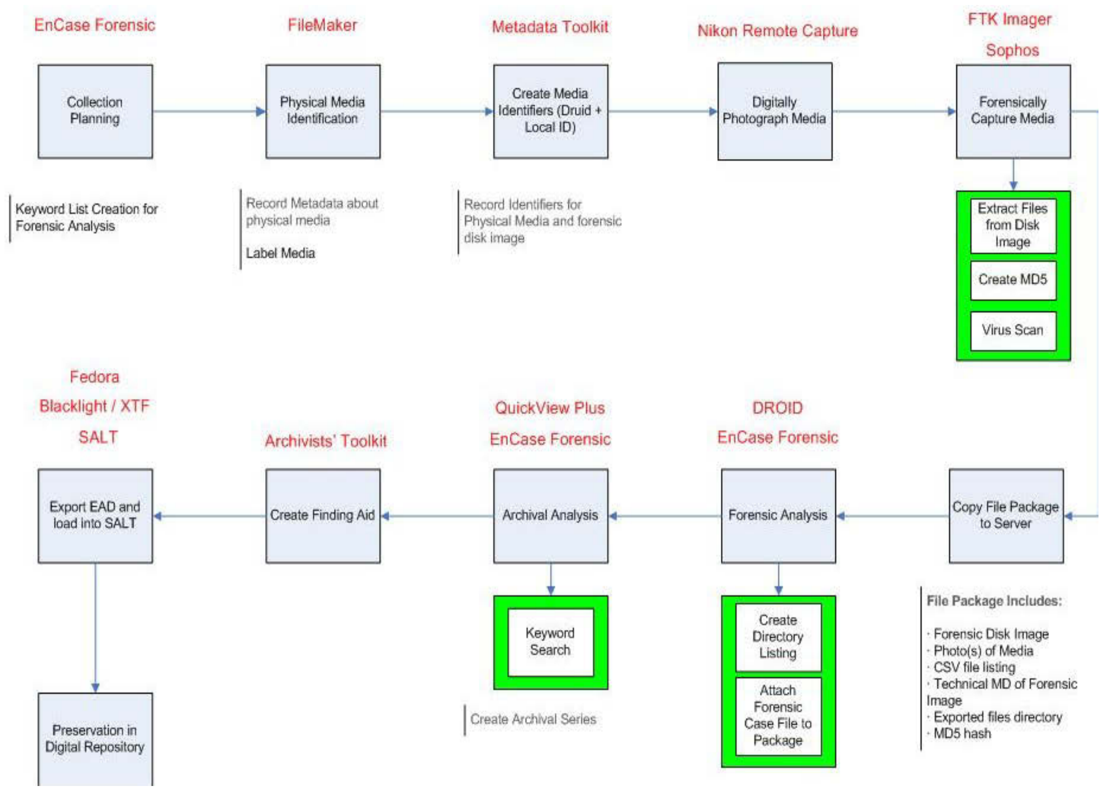
- Encryption software can ensure adequate protection for sensitive materials, and decryption software may aid in accessing the data of donors unable to supply their passwords.[68]

- Generally one is interested in gathering active data. Through carving, however, researchers can also recover inactive data, residual and deleted data or fragmented data in the recesses of the hard disk. Software can aid in the bitstream recovery of data that is not readable, recuperating data from discs that have suffered spillages, scratches and even breakages.[69]



British Library's digital forensics workflow[70]

[66] John, "Adapting Existing Technologies for Digitally Archiving Personal Lives: Digital Forensics, Ancestral Computing, and Evolutionary Perspectives and Tools," 4.
[67] Von Suchodoletz, "Automating Disk Imaging."
[68] Kirschenbaum, "Digital Forensics and Cultural Heritage Glossary."
[69] Finch, Lorraine and John Webster. Caring for CDs and DVDs.
[70] John, *Digital Lives: Personal Digital Archives for the 21st Century >> An Initial Synthesis*, 72.



Stanford University's digital forensics workflow[71]

Digital Forensic Challenges

Digital forensics is by no means an inexpensive venture. The acquisition of the tools, hardware and software necessary to employ its practices can be formidable. Legacy equipment, by nature of its age requires corresponding legacy software. Interfacing with modern operating systems or software is difficult, resulting in considerable time spent in locating pieces, setup and troubleshooting. Purchasing specialized hardware, such as a Forensic Recovery of Evidence Device (FRED), can range upwards of $3,000. As the field is still evolving it requires a commitment to remain abreast of developments in techniques and tools. There is currently no Swiss army tool that can successfully perform a variety of functions, requiring the use of several tools throughout the workflow. Unfortunately, not all tools work well together and not all tools are open source. The variability of media and the hardware and software necessary to access and preserve necessitate archivists possess a strong grasp of the environments in which these files were created. Knowledge of a variety of operating systems, computer registries, servers, and hardware is a must. Imaging requires manually connecting hardware and errors can abound. Since familiar means of handling physical documents are not present with digital documents, knowing how a digital file is created and stored is essential.

[71] Olson, "First Draft of our Forensic Workflow."

Recommendations

- As a partial digital forensic workflow is already in place (photographing the medium, generating log file, checksums, virus check, file normalization and data redaction), the next step would be incorporating the use of imaging. In addition to the metadata currently captured, the following metadata could be captured to assist in recreating the look and feel of an object.

Category	Playback requirement	Details
Operating environment (hardware)	CPU	Conditions such as CPU type and clock speed etc.
	Memory	Minimum memory size and recommended size
	Display	Resolution, number of colors
	CD-ROM drive	Conditions relating to CD read rates etc.
	Audio	Presence or absence, type of sound card
	Other	Hardware requirements other than those listed above
Operating environment (software)	Operating system	Compatible operating systems
	Application	Software necessary for playback
	Other	Software requirements other than those listed above

Sample metadata captured during migration at the National Diet Library[72]

Other metadata considerations include medium manufacturer; medium condition not readily discernible from photograph, such as brittleness or coloring; anything written on object; how the information was written onto the object (such as with pen, adhesive, pencil, etc); corresponding collection or medium's location within collection; age of item; encryption data; software/hardware used to read the medium; how the file behaves or functions.

- As a disk may contain hundreds of files, the use of the donor survey to increase input and/or documentation from donors is necessary to access encrypted files and to facilitate in the identification of disk operating systems and software, establishing preservation hierarchies and identifying which items to process first. Materials should be tested at acquisition to weed out materials that arrive defective (of particular importance for magnetic media).

- A dedicated legacy or Rosetta computer should be set aside for forensic work. Rosetta machines are those that include readers for a variety of media and in addition to USB ports, also have DB-25 parallel ports and RS-232 serial ports. Sample Rosetta machines include those that can read both 5¼" and 3½" floppy disks and Macintosh computers with disk drives that can read both 800 KB and 1.4 MB disks.[73] The use of legacy computers is

[72] *The Long-term Accessibility of Packaged Digital Publications*, 55.
[73] Kirschenbaum, et al., "Digital Forensics and Born-Digital Content in Cultural Heritage Collections," 20.

beneficial in the sense that it may facilitate accessibility by reducing the need for file conversion during appraisal. It is recommended these computers not be connected to the network in order to limit their exposure to threats. As these are delicate machines, care should be taken to inspect both the computer and media before playing as either can cause damage to each other.

- Applications usually only work with a particular version of a particular operating system and applications designed for old operating systems will not necessarily function with the latest operating systems. It is recommended that one not rely solely on just one tool and care should be taken in selecting tools as some can alter the original bitstream. The most popular digital forensic software for archival use are Encase (sold by Guidance Software) and Forensic Tool Kit (sold by AccessData).[74] Also popular are Forensic Toolkit, SleuthKit, Fiwalk, Hypatia, Dc3dd, OSfClone, OSForensics, Digital Forensic Framework, Pyflag, Bulkextractor/afflib, and Gumshoe.

- Since legacy hardware has a tendency of breaking down, establishing a network of contacts from local businesses, university units and even staff for the solicitation of hardware donations will be cost effective. As formats continue to slip into obscurity, collaboration with various institutions in order to pool resources (both intellectual and physical), workflows, and workarounds will also be beneficial.

- Testing in general is crucial as what may not work on one machine may work on another. Consequently, more than one drive would be beneficial for double checking error messages. Creation of an error messages chart would assist in troubleshooting and help identify common problems, like media not opening or file name incompatibility issues between PCs and Macs. The error chart should also identify at which point to give up in the troubleshooting process or when to refer the media to a specialist.

[74] John, *Digital Lives: Personal Digital Archives for the 21st Century >> An Initial Synthesis*, 72.

Result	Probable Format	Action
"Disk not formatted" message AND disc is labelled *Apple* or *Macintosh*	Macintosh	Read in Macintosh drive. (Note: some early 400 K and 800 K disks may not be supported.)
"Disk not formatted" message AND disc is labelled *IBM* or *PC format*	Macintosh (reformatted)	Read in Macintosh drive.
"Disk not formatted" messsage. Label not specific	Unknown (possibly Macintosh)	Try in Macintosh drive. If unsuccessful, use specialised recovery software Disk Recogniser module to try to identify format and/or Read Sector to copy data from unknown format disk.
Directory displays, but includes files such as: *Resource.frk*	PC, but has been used in a Macintosh.	Read in Macintosh drive

Sample error chart[75]

Conclusion

As time progresses, tools, software, documentation and overall demand lessen, thereby increasing the difficulty in accessing specific file formats. The older the medium, the more creativity required in retrieving the data and the diminished likelihood of recuperating the original look and feel of the record.[76] The proportion of cases in which the factor preventing use of the medium increases with the number of years that have elapsed since acquisition. Case studies documenting the migration of removable media are rife with hardware failure, incompatibilities and complications. Despite well-established protocols, procedures or workflows, sometimes there is no rhyme or reason as to why some devices fail. In a CD longevity study conducted by the National Diet Library, in half of the cases the factor preventing the use of digital materials lay in incompatibility between operating systems and applications. In 30% of the cases it was unavailability of applications, incompatibility between applications and plug-ins, and in 10% of cases it was technological obsolescence and deterioration of media.[77]

Next Steps

- In her report "Issues Related to Removable Media in Hybrid Manuscript Collections," Alexis Antracoli raises questions regarding appraisal, processing, and arrangement, which should be addressed before embarking upon a media migration project (Appendix 5).

[75] National Library of Australia, "Recovering and Converting Data from Manuscripts Collection Discs."
[76] Entlich, "Digging Up Bits of the Past: Hands-on With Obsolescence."
[77] *The Long-term Accessibility of Packaged Digital Publications*, 10.

- Decisions should also be made on whether the original storage medium will be kept. While some institutions argue for the retention of storage mediums in case future technology makes them accessible, in all reality any future developments will most likely be in the shape of tools that will allow for the rendering of bitstreams, rather than physical hardware that will facilitate the reading of the actual disk.

- To address legacy items, a removable media inventory should be conducted to identify formats, quantities, surface conditions and pinpoint necessary hardware. Ben Goldman recommends adding up the disk formats and multiplying by their capacity to generate a rough idea of how much content is to be migrated. This will shed light on what hardware is necessary and inform as to whether it is worthwhile or financially feasible to acquire the tools (and skills) necessary to access the data.

- Although still in development, ISO/FDIS 13008 Information and Documentation -- Digital Records Conversion and Migration Process may provide future standards or insight into migration techniques

- While content has not been explicitly addressed in this report, it is recommended that digital video be explored separately as preservation and access concerns vary significantly from those associated from traditional removable media.

Useful Tools

Hardware

- **Catweasel controller**: universal floppy disk controller
  http://www.jschoenfeld.com/products/catweasel_e.htm

- **Digital Intelligence's Image**: source for disk utilities
  http://www.digitalintelligence.com/software/disoftware.php

- **FC5025 5.25**: provides interface for connecting external 5¼" drive to be connected via USB
  http://www.deviceside.com/fc5025.html

- **Gigabyte GA-880GA-UD3H:** motherboard allowing use of Quickview with floppy disks
  http://www.gigabyte.us/products/product-page.aspx?pid=3425#ov

- **Kryoflux** : provides interface for connecting external 5¼" drive to be connected via USB port and creates an image file by reading magnetic signals off the disk and writing to the computer
  http://www.kryoflux.com/

- **Multi-disk drive**: 3½" floppy reader with slots for SD cards and compact flash cards
  http://www.reghardware.com/2008/02/20/maplin_internal_floppy_disk_drive_with_card_reader/

- **Tableau**: sells forensic hardware, such as write blockers and disk controllers
  http://www.tableau.com/

Software

- **ADTPro**: transfers diskettes and disk images for Apple II-era computers
  http://adtpro.sourceforge.net/

- **BadCopy Pro:** recovers corrupted data
  http://www.jufsoft.com/badcopy/

- **Karenware:** file directory printer
  http://www.karenware.com/powertools/ptdirprn.asp

- **Knoppix**: bootable live CD to run Linux on a desktop
  http://www.knopper.net/knoppix/index-en.html

- **CD/DVD Inspector**: Specializes in the analysis of optical discs, which show some profound differences from hard disks in the forensic context. A standard ISO 'image' does not capture all of a CD's potential contents, but CD/DVD Inspector is able to do so.[78]
  http://www.infinadyne.com/cddvd_inspector.html

Useful Resources

- **Legacy applications and formats:**
  http://www.oldapps.com/
  http://alternativeto.net/
  http://mediapedia.nla.gov.au/home.php3
  http://www.vintage-computer.com/

[78] John, "Adapting Existing Technologies for Digitally Archiving Personal Lives: Digital Forensics, Ancestral Computing, and Evolutionary Perspectives and Tools,"2.

http://www.pcguide.com/ref/fdd

- **Digital Forensics:**
  http://www.google.com/cse/home?cx=011905220571137173365:7eskxxzhjj8
  http://www.digitalrecordsforensics.org/index.cfm
  http://www.forensicfocus.com/Forums/
  http://www.forensicswiki.org/wiki/Main_Page
  http://digitalcorpora.org/

- **Case studies and workflows:**
  http://ils.unc.edu/callee/emanuscripts-stewardship/acquisition-tools.html
  https://pacer.ischool.utexas.edu/handle/2081/21808
  BHL Digital Curation Resources / Legacy Digital Content Project in ctools
  http://futurearchives.blogspot.co.uk/
  http://born-digital-archives.blogspot.com/

Appendix 1: Quick Reference Guide for Care and Handling of CDs and DVDs

Quick Reference Guide for Care and Handling

Do:

1. Handle discs by the outer edge or the center hole.
2. Use a non-solvent-based felt-tip permanent marker to mark the label side of the disc.
3. Keep dirt or other foreign matter from the disc.
4. Store discs upright (book style) in plastic cases specified for CDs and DVDs.
5. Return discs to storage cases immediately after use.
6. Leave discs in their packaging (or cases) to minimize the effects of environmental changes.
7. Open a recordable disc package only when you are ready to record data on that disc.
8. Store discs in a cool, dry, dark environment in which the air is clean.
9. Remove dirt, foreign material, fingerprints, smudges, and liquids by wiping with a clean cotton fabric in a straight line from the center of the disc toward the outer edge.
10. Use CD/DVD-cleaning detergent, isopropyl alcohol, or methanol to remove stubborn dirt or material.
11. Check the disc surface before recording.

Do not:

1. Touch the surface of the disc.
2. Bend the disc.
3. Use adhesive labels.
4. Store discs horizontally for a long time (years).
5. Open a recordable optical disc package if you are not ready to record.
6. Expose discs to extreme heat or high humidity.
7. Expose discs to extremely rapid temperature or humidity changes.
8. Expose recordable discs to prolonged sunlight or other sources of ultraviolet light.
9. Write or mark in the data area of the disc (the area the laser "reads").
10. Clean by wiping in a direction going around the disc.

For CDs especially do not:

1. Scratch the label side of the disc.
2. Use a pen, pencil, or fine-tip marker to write on the disc.
3. Write on the disc with markers that contain solvents.
4. Try to peel off or reposition a label.

General recommendations for long-term storage conditions:

For archiving recordable (R) discs, it is recommended to use discs that have a gold metal reflective layer.

Archival Storage Facility—Recommendation for storing CDs and DVDs together

Media	Temperature	Relative Humidity (RH)
CD, DVD	Less than 20°C (68°F) Greater than 4°C (39°F)	20% to 50% RH

A temperature of 18°C and 40% RH would be considered suitable for long-term storage.
A lower temperature and RH is recommended for extended-term storage. [79]

[79] Byers, *Care and Handling of CDs and DVDs* , vi.

Appendix 2: Optical Media Drives

Disc Type	DVD ROM Play only (computer)		DVD-R (General) Records General -R		DVD-R (Authoring) Records Authoring -R		DVD-RW Records -RW, General -R		DVD-RAM Records RAM		DVD+R/+RW Records +R, +RW	
	Read	Write	Read	Write	Read	Write	Read	Write	Read	Write	Read	Write
DVD-ROM	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No
DVD-R (General)	U	No	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes	No
DVD-R (Authoring)	U	No	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	No
DVD-RW	U	No	Yes	No	Yes	No	Yes	Yes	U	No	U	No
DVD-RAM	R	No	No	No	No	No	No	No	Yes	Yes	No	No
DVD+R	U	No	U	No	U	No	U	No	U	No	Yes	Yes
DVD+RW	U	No	U	No	U	No	U	No	U	No	Yes	Yes
CD-ROM	Yes	No	Yes	No	No	No	Yes	No	U	No	Yes	No
CD-R	Yes	No	Yes	Yes	No	No	Yes	Yes	U	No	Yes	Yes
CD-RW	Yes	No	Yes	No	No	No	Yes	Yes	U	No	Yes	Yes
	U = Usually		R = Rarely									
DVD-Video DVD-Audio	All DVD drives should play DVD-Video or DVD-Audio if the computer has DVD-Video or DVD-Audio player software installed. DVD-RAM drives are questionable.											

* Most computer DVD drives are backward compatible to CDs, meaning they can read or read/write CDs.
* Some drives are the combination of more than one drive type, providing compatibility with different DVD and CD disc types.

CD drive types and what they can do with each disc type

Disc Type	CD ROM Play only		CD-RW or CD-R/RW Records -RW, -R		CD-R Records -R	
	Read	Write	Read	Write	Read	Write
CD-ROM	Yes	No	Yes	No	Yes	No
CD-R	Yes	No	Yes	Yes	Yes	Yes
CD-RW	Yes	No	Yes	Yes	No	No
DVD-Video, Audio DVD-ROM DVD-R (General) DVD-R (Authoring) DVD-RW DVD-RAM DVD+R DVD+RW	DVDs do not work in CD drives or CD players.					

Home DVD video player compatibility with each disc type

Disc Type	DVD Video Player	Comment
DVD-Video DVD-Audio	Plays	- DVD-Video and DVD-Audio are a type of DVD-ROM commonly used in home DVD-Video or DVD-Audio players.
DVD-ROM DVD-RAM	N/A	- Use of the term DVD-ROM, typically refers to replicated (commercially available pre-recorded) DVD-ROMs for computer applications.
DVD-R (General)	Depends	If the disc is formatted correctly, it should play in newer home DVD video players.
DVD-R (Authoring)		
DVD-RW, DVD+R, DVD+RW		
CD-ROM (Video-CD)	Depends	If the CD-ROM, CD-R, or CD-RW are formatted as V-CD, (Video-CD), some DVD video players will play them (some DVD players compatible with MPEG 1).
CD-ROM (Audio-CD)	Plays	
CD-R (V-CD or audio formatted)	Usually	
CD-RW (V-CD or audio formatted)		

[80]

[80] Byers, *Care and Handling of CDs and DVDs* , 28.

Appendix 3: Magnetic Media Overview

MAGNETIC MEDIA

Name	8" Floppy Disk
Space Capacity	250 KB SS/SD, 500 KB DB/SD, 1.2 MB DS/DD
Date Span	1971 - 1981
Actual Shelf Life	5 - 30 years
Hardware	Internal 8" floppy disk drive
Platform	CP/M most common, also ODS-1
Environment	Between 64-68°F, relative humidity between 30-40% Keep away from heat, humidity, dirt and dust Prevent sudden changes in temperature and humidity Limit exposure to light (nothing above 75μW/lumen) and ultra-violet light Sensitive to magnetic fields and intense vibrations
Storage	Store vertically inside Tyvek sleeve Keep covered in static-proof-dust-free enclosing (no cardboard/paper) Do not leave on top of heat generating sources, like PC Do not store in cabinet with magnetic lock or catch Keep away from the magnetic ballast and bases in lamps Do not use metal clips, rubber bands or fasteners
Handling	Never directly touch the tape Thin plastic shell bends easily damaging internal disk Do not write on disk with ball point pen or pencil Use felt tip marker to write on labels Do not apply more than one label to disk
Known Issues	Can be double sided Tape can become soft, sticky or brittle Plastic shell reacts to humidity causing internal disk to warp Does not need to be constantly played to be preserved

Name	5¼" Floppy Disk
Space Capacity	80-90 KB SS/SD, 180 KB DS/SD, 320-360 KB DS/DD, 720 KB DS/QD, 1.2 MB DS/HD
Date Span	1972 - 1985, limited use through mid-90s
Actual Shelf Life	5 - 30 years
Hardware	5¼" floppy disk drive for each of the formats
Platform	Apple DOS File System, DFS, CP/M, and FAT
Environment	Between 64-68°F, relative humidity between 30-40% Prevent sudden changes in temperature and humidity Keep away from heat, humidity, dirt and dust Limit exposure to light (nothing above 75µW/lumen) and ultra-violet light Sensitive to magnetic fields and intense vibrations
Storage	Store vertically inside case; do not crowd disc in container Keep covered in static proof, dust free enclosing (no cardboard/paper) Do not leave on top of heat generating sources, like PC Do not store in cabinet with magnetic lock or catch Keep away from the magnetic ballast and bases in lamps Do not use metal clips, rubber bands or fasteners
Handling	Never directly touch the tape Do not write on disk with ball point pen or pencil Use felt tip marker to write on labels Thin plastic shell bends easily damaging internal disk Do not apply more than one label to disk
Known Issues	Can be double sided Open slot lets dirt and dust into casing Compatibility issues with MFM drives and GCR encoded disks and vice versa Spiral tracking, a type of copyright protection that does not allow for disk copying Does not need to be constantly played to be preserved

Name **Space Capacity** **Date Span** **Actual Shelf Life**	3½" Floppy Disk, aka microfloppy 360 KB SS/DD, 720 KB SS/HD, 720 KB DS/DD , 1.4 MB DS/HD, 2.8 MB DS/ED 1982 - late 1990s 5-30 years
Hardware **Platform**	Internal or USB 3½" floppy disk drive for each of the formats FAT, NTFS, DFS, ADFS, Apple DOS File System, MFS, HFS
Environment	Between 64-68°F, relative humidity between 30-40% Prevent sudden changes in temperature and humidity Keep away from heat, humidity, dirt and dust Limit exposure to light (nothing above 75µW/lumen) and ultra-violet light
Storage	Store vertically inside case; do not crowd disc in container Keep covered in static proof, dust free enclosing (no cardboard/paper) Do not leave on top of heat generating sources, like PC Do not store in cabinet with magnetic lock or catch Keep away from the magnetic ballast and bases in lamps Do not use metal clips, rubber bands or fasteners
Handling	Never directly touch the tape
Known Issues	Metal shutters can get bent and damage disk or drive Open hub on back allows dirt and dust inside casing Check for write protection mechanism Does not need to be constantly played to be preserved

Archive Team, "Rescuing Floppy Disks." Last modified January 23, 2012. Accessed June 15, 2012. http://archiveteam.org/index.php?title=Rescuing_Floppy_Disks.

Digital Preservation Management, "Chamber of Horrors: Obsolete and Endangered Media." Accessed June 14, 2012. http://www.dpworkshop.org/dpm-eng/oldmedia/disks.html.

FL Dept of State Divison of Library & Information Services, "Protect your Video and Audio Tapes, and Floppy Disks." Accessed June 15, 2012. http://dlis.dos.state.fl.us/archives/preservation/ma

Appendix 4: Optical Media Overview

OPTICAL MEDIA

Name	Compact Disc [CD-ROM]
Space Capacity	650 MB
Date Span	1984 - Present
Actual Shelf Life	20 - 100 years
Recording Method	Data on molded layer made of aluminum Non-recordable, read only
Hardware	CD-ROM, CD-R, CD-RW, DVD, DVD+/-R, DVD+/-RW drives
Environment	Greater than 39°, but less than 68° F, ideal 64° F Relative humidity should be between 20% and 50%, ideal 40% Avoid prolonged exposure to moisture Avoid sudden changes in temperature and humidity as it can cause warpage
Storage	Store in jewel case or acid-free paper/board housing Limit time spent outside jewel case Do not house next to acidic paper, inks, or adhesives Remove all booklets, notes, paper, and store separately Always store vertically, do not allow to lean Do not store discs too tightly or loosely in shelves Do not tie with rubber bands as they can bend the disc
Handling	Hold disc by outer edge of center hole, not surface of disc Do not touch surface or scratch label side of disc Wear vinyl or nitrite gloves, but not cotton as it is permeable Never flex, bend or place pressure on CD, even when removing from jewel case Do not leave disc in playback equipment Do not write on disc with pen, pencil or fine-tip marker that contains solvents Make all necessary notations on jewel case, not disc Do not clean in a circular pattern

Name	Compact Disc Digital Audio [CD-DA, CD-A]
Space Capacity	650 MB
Date Span	1980 - Present
Actual Shelf Life	20 - 100 years
Recording Method	Data on molded layer made of aluminum Write once, read many times
Hardware	CD-ROM, CD-R, CD-RW drives
Environment	Greater than 39°, but less than 68° F, ideal 64° F Relative humidity should be between 20% and 50%, ideal 40% Avoid prolonged exposure to moisture Avoid sudden changes in temperature and humidity as it can cause warpage
Storage	Store in jewel case or acid-free paper/board housing Limit time spent outside jewel case Do not house next to acidic paper, inks, or adhesives Remove all booklets, notes, paper and store separately Always store vertically, do not allow to lean Do not store discs too tightly or loosely in shelves Do not tie with rubber bands as they can bend the disc
Handling	Hold disc by outer edge of center hole, not surface of disc Do not touch surface or scratch label side of disc Wear vinyl or nitrite gloves, but not cotton as it is permeable Never flex, bend or place pressure on CD, even when removing from jewel case Do not leave disc in playback equipment Do not write on disc with pen, pencil or fine-tip marker that contains solvents Make all necessary notations on jewel case, not disc Do not clean in a circular pattern

Name	Recordable Compact Disc [CD-R]; originally called CD Write Once [CD-WO]
Space Capacity	650 - 870 MB; standard is 700 MB
Date Span	1988 - Present
Actual Shelf Life	20 -100 years
Recording Method	Organic dye-based on either gold, silver, or silver alloy Write once, read many times
Hardware	CD-ROM, CD-R, CD-RW, DVD, DVD+/-R, DVD+/-RW drives High compatibility with many players Drives designed for dye-based discs cannot write to or read rewritable discs
Environment	Greater than 39°, but less than 68° F, ideal 64° F Relative humidity should be between 20% and 50%, ideal 40% Avoid prolonged exposure to moisture Avoid sudden changes in temperature and humidity as it can cause warpage Limit ultraviolet light exposure, extremely photosensitive
Storage	Store in jewel case or acid-free paper/board housing Remove all booklets, notes, paper and store separately Always store vertically, do not allow to lean Limit time spent outside jewel case Do not store discs too tightly or loosely in shelves Do not house next acidic paper, inks, or adhesives Store in the dark Do not tie with rubber bands as they can bend the disc
Handling	Hold disc by outer edge of center hole, not surface of disc Do not touch surface or scratch label side of disc Wear vinyl or nitrite gloves, but not cotton as it is permeable Never flex, bend or place pressure on CD, even when removing from jewel case Do not leave disc in playback equipment Do not write on disc with pen, pencil or fine-tip marker that contains solvents Make all necessary notations on jewel case, not disc Do not attempt to remove labels Do not clean in a circular pattern

Name **Space Capacity** **Date Span** **Actual Shelf Life**	Recordable Compact Disc [CD-RW] 650 - 700 MB 1997 - Present 10 - 50 years
Recording Method	Phase changing aluminum alloy film Can be erased and reused
Hardware	CD-ROM, CD-R, CD-RW, DVD, DVD+/-R, DVD+/-RW Require Special Players, preferably ones certified "MultiRead" Difficult to read on players older than 1997 Older CD-RW drives cannot handle newer CD-RW discs
Environment	Greater than 39°, but less than 68° F, ideal 64° F Relative humidity should be between 20% and 50%, ideal 40% Avoid prolonged exposure to moisture Avoid sudden changes in temperature and humidity as it can cause warpage Limit ultraviolet light exposure, extremely photosensitive
Storage	Store in jewel case or acid-free paper/board housing Limit time spent outside jewel case Store in the dark Remove all booklets, notes, paper and store separately Do not house next to acidic paper, inks, or adhesives Always store vertically, do not allow to lean Do not store discs too tightly or loosely in shelves Do not tie with rubber bands as they can bend the disc
Handling	Hold disc by outer edge of center hole, not surface of disc Do not touch surface or scratch label side of disc Wear vinyl or nitrite gloves, but not cotton as it is permeable Never flex, bend or place pressure on CD, even when removing from jewel case Do not leave disc in playback equipment Do not write on disc with pen, pencil or fine-tip marker that contains solvents Make all necessary notations on jewel case, not disc Do not attempt to remove labels Do not clean in a circular pattern

Name	Digital Video Disc [DVD-ROM]
Space Capacity	4.7 - 17 GB
Date Span	1997 - Present
Actual Shelf Life	20 - 100 years
Recording Method	Data on molded layer made of aluminum, gold, silver, or silicon Non-recordable, read only Can be double sided
Hardware	DVD-ROM, DVD+/-R, DVD+/-RW, DVD-RAM drives Does not play on CD drives or DVD home players
Environment	Greater than 39°, but less than 68° F, ideal 64° F Relative humidity should be between 20% and 50%, ideal 40% Avoid prolonged exposure to moisture Avoid sudden changes in temperature and humidity as it can cause warpage
Storage	Must be stored in DVD jewel cases, as CD cases allow disc to sag at edges Limit time spent outside jewel case Do not store in paper or cardboard sleeves Do not house next to acidic paper, inks, or adhesives Remove all booklets, notes, paper and store separately Always store vertically, do not allow to lean Do not store discs too tightly or loosely in shelves Do not tie with rubber bands as they can bend the disc
Handling	Hold disc by outer edge of center hole, not surface of disc Do not touch surface or scratch label side of disc Wear vinyl or nitrite gloves, but not cotton as it is permeable More sensitive to bending/pressure than CDs Never flex, bend or place pressure on DVD Do not write on disc with pen, pencil or fine-tip marker that contains solvents Make all necessary notations on jewel case, not disc Do not leave disc in playback equipment Do not clean in a circular pattern

Name **Space Capacity** **Date Span** **Actual Shelf Life**	Digital Video Disc Recordable [DVD-R] 3.95 - 4.7 GB 1997 - Present 5 - 10 years before recording
Recording Method **Hardware**	Organic dye-based on either gold, silver, or silver alloy Write once, read many times Can be double sided DVD-ROM(sometimes), DVD+/-R, DVD+/-RW, DVD-RAM drives Drives designed for dye-based discs cannot write to or read rewritable discs Does not play on CD drives
Environment	Greater than 39°, but less than 68° F, ideal 64° F Relative humidity should be between 20% and 50%, ideal 40% Avoid prolonged exposure to moisture Avoid sudden changes in temperature and humidity, as it can cause warpage Limit ultraviolet light exposure, extremely photosensitive
Storage	Must be stored in DVD jewel cases, as CD cases allow disc to sag at edges Limit time spent outside jewel case Do not store in paper or cardboard sleeves Do not house next to acidic paper, inks, or adhesives Remove all booklets, notes, paper and store separately Always store vertically, do not allow to lean Do not store discs too tightly or loosely in shelves Do not tie with rubber bands as they can bend the disc Store in the dark
Handling	Hold disc by outer edge of center hole, not surface of disc Do not touch surface or scratch label side of disc Wear vinyl or nitrite gloves, but not cotton as it is permeable More sensitive to bending/pressure than CDs Never flex, bend or place pressure on DVD Do not attempt to remove or place labels on disc Do not write on disc with pen, pencil or fine-tip marker that contains solvents Make all necessary notations on jewel case, not disc Do not leave disc in playback equipment Do not clean in circular pattern

Name **Space Capacity** **Date Span** **Actual Shelf Life**	Digital Video Disc Recordable [DVD+R] 4.7 GB 2002 - Present 5- 10 years before recording
Recording Method	Organic dye-based on either gold, silver, or silver alloy Write once, read many times Can be double-sided
Hardware	DVD+R, DVD+RW, other drives sporadically Drives designed for dye-based discs cannot write/read rewritable discs Does not play on CD drives
Environment	Greater than 39°, but less than 68° F, ideal 64° F Relative humidity should be between 20% and 50%, ideal 40% Avoid prolonged exposure to moisture Avoid sudden changes in temperature and humidity as it can cause warpage Limit ultraviolet light exposure, extremely photosensitive
Storage	Must be stored in DVD jewel cases, as CD cases allow disc to sag at edges Limit time spent outside jewel case Do not store in paper or cardboard sleeves Do not house next to acidic paper, inks, or adhesives Remove all booklets, notes, paper and store separately Always store vertically, do not allow to lean Do not store discs too tightly or loosely in shelves Do not tie with rubber bands as they can bend the disc Store in the dark
Handling	Hold disc by outer edge of center hole, not surface of disc Do not touch surface or scratch label side of disc Wear vinyl or nitrite gloves, but not cotton as it is permeable More sensitive to bending/pressure than CDs Never flex, bend or place pressure on DVD Do not attempt to remove or place labels on disc Do not write on disc with pen, pencil or fine-tip marker that contains solvents Make all necessary notations on jewel case, not disc Do not leave disc in playback equipment Do not clean in circular pattern

Name **Space Capacity** **Date Span** **Actual Shelf Life**	Digital Video Disc Rewritable [DVD-RW] 4.7 GB 1999 - Present Half of a DVD+/-R
Recording Method	Phase changing aluminum alloy film Can be erased and reused Can be double-sided
Hardware	DVD-R, DVD-RW, other drives sporadically Does not play on CD drives
Environment	Greater than 39°, but less than 68° F, ideal 64° F Relative humidity should be between 20% and 50%, ideal 40% Avoid prolonged exposure to moisture Avoid sudden changes in temperature and humidity as it can cause warpage Limit ultraviolet light exposure, extremely photosensitive
Storage	Must be stored in DVD jewel cases, as CD cases allow disc to sag at edges Limit time spent outside jewel case Do not store in paper or cardboard sleeves Do not house next to acidic paper, inks, or adhesives Remove all booklets, notes, paper and store separately Always store vertically, do not allow to lean Do not store discs too tightly or loosely in shelves Do not tie with rubber bands as they can bend the disc Store in the dark
Handling	Hold disc by outer edge of center hole, not surface of disc Do not touch surface or scratch label side of disc Wear vinyl or nitrite gloves, but not cotton as it is permeable More sensitive to bending/pressure than CDs Never flex, bend or place pressure on DVD Do not attempt to remove or place labels on disc Do not write on disc with pen, pencil or fine-tip marker that contains solvents Make all necessary notations on jewel case, not disc Do not leave disc in playback equipment Do not clean in circular pattern

Name **Space Capacity** **Date Span** **Actual Shelf Life**	Digital Video Disc Rewritable [DVD+RW] 4.7 GB 2002 - Present Half of a DVD+/-R
Recording Method	Phase changing aluminum alloy film Can be erased and reused Can be double-sided
Hardware	DVD+RW, other drives sporadically Does not play on CD drives
Environment	Greater than 39°, but less than 68° F, ideal 64° F Relative humidity should be between 20% and 50%, ideal 40% Avoid prolonged exposure to moisture Avoid sudden changes in temperature and humidity as it can cause warpage Limit ultraviolet light exposure, extremely photosensitive
Storage	Must be stored in DVD jewel cases, as CD cases allow disc to sag at edges Limit time spent outside jewel case Do not store in paper or cardboard sleeves Do not house next to acidic paper, inks, or adhesives Remove all booklets, notes, paper and store separately Always store vertically, do not allow to lean Do not store discs too tightly or loosely in shelves Do not tie with rubber bands as they can bend the disc Store in the dark
Handling	Hold disc by outer edge of center hole, not surface of disc Do not touch surface or scratch label side of disc Wear vinyl or nitrite gloves, but not cotton as it is permeable More sensitive to bending/pressure than CDs Never flex, bend or place pressure on DVD Do not attempt to remove or place labels on disc Do not write on disc with pen, pencil or fine-tip marker that contains solvents Make all necessary notations on jewel case, not disc Do not leave disc in playback equipment Do not clean in circular pattern

Name **Space Capacity** **Date Span** **Actual Shelf Life**	Digital Video Disc Ram [DVD-RAM] 2.6 - 9.4 GB 1996 - Present
Recording Method **Hardware**	Phase changing aluminum alloy film Can be erased and reused Can be double-sided DVD-RAM drive only
Environment	Greater than 39°, but less than 68° F, ideal 64° F Relative humidity should be between 20% and 50%, ideal 40% Avoid prolonged exposure to moisture Avoid sudden changes in temperature and humidity as it can cause warpage Limit ultraviolet light exposure, extremely photosensitive
Storage	Must be stored in DVD jewel cases, as CD cases allow disc to sag at edges Limit time spent outside jewel case Do not store in paper or cardboard sleeves Do not house next to acidic paper, inks, or adhesives Remove all booklets, notes, paper and store separately Always store vertically, do not allow to lean Do not store discs too tightly or loosely in shelves Do not tie with rubber bands as they can bend the disc Store in the dark
Handling	Hold disc by outer edge of center hole, not surface of disc Do not touch surface or scratch label side of disc Wear vinyl or nitrite gloves, but not cotton as it is permeable More sensitive to bending/pressure than CDs Never flex, bend or place pressure on DVD Do not attempt to remove or place labels on disc Do not write on disc with pen, pencil or fine-tip marker that contains solvents Make all necessary notations on jewel case, not disc Do not leave disc in playback equipment Do not clean in circular pattern

Byers, Fred R. *Care and Handling of CDs and DVDs: A Guide for Librarians and Archivists* . Washington, DC: Council on Library and Information Resources, 2003.

Digital Preservation Management, "Chamber of Horrors: Obsolete and Endangered Media." Accessed June 14, 2012. http://www.dpworkshop.org/dpm-eng/oldmedia/disks.html.

Finch, Lorraine and John Webster. *Caring for CDs and DVDs* . National Preservation Office, 2008. www.collectionslink.org.uk (accessed June 14, 2012).

Appendix 5: Report on Issues Related to Removable Media in Hybrid Manuscript Collections by Alexis A. Antracoli

Background

The impetus for this report is the processing of the Jennifer M. Granholm papers by the Michigan Historical Collections Division of the Bentley Historical Library in 2011. After surveying, in detail, over 100 boxes of the collection, not including the Communications records, I have catalogued over 100 CDs and DVDs. Additionally, the Communications Division of the Governor's office includes 8 boxes of scripts, videotapes, and DVDs and one box of miscellaneous CDs and DVDs. While most collections are much smaller in scope than a governor's records, it is increasingly common that collections arrive in Michigan Historical Collections with removable media, including CDs, DVDs, Zip disks, 3.5 inch floppy disks, and 5 ¼ inch floppy disks. Many of these files, and in the case of the Granholm papers, all of the files on removable media can be considered fugitive, meaning that there was no awareness of this material prior to acquisition and it is generally arranged as part of the larger paper component of the collection. Many recent accessions, in addition to the Granholm papers, that include a significant number removable media, both fugitive and non-fugitive are the Boyne USA Resorts records (CDs, DVDs, 3.5 inch floppy disks, and Zip disks), Michael Erlewine collection (CDs, DVDS, and a hard drive), and the Peter Pollack papers (CDs and DVDs). On occasion I have also found 5 ¼ inch floppy disks in a collection. If left on these media issues of hardware, software, and format obsolescence as well as deterioration of physical media will eventually make many or of these files unreadable.[81] Developing a policy for handling this type of media once it arrives at the library will help to insure timely processing of materials and long-term preservation of digital files deemed to be of enduring value. A survey of the literature on electronic personal papers in manuscript collections also highlighted several other areas of consideration such as arrangement and description, processing workflows, and rights management and access that are integral to the acquisition and management of hybrid collections of personal papers in general. These issues are also considered in this report.

Literature Review of Electronic Records in Manuscript Collections

In 2005, Neil Beagrie noted that "in a few more years it will be possible, for example, to envisage individuals being able to store the equivalent of all the texts in the Library of

---

[81] Many of the inherent risks involved in keeping files on various types of optical discs are summarized at the ICPSR Digital Preservation Tutorial http://www.icpsr.umich.edu/dpm/dpm-eng/oldmedia/threats.html. Fred R. Byers provides a more in-depth report on issues surrounding the handling, care, and long-term sustainability of optical discs in *Care and Handling of CDs and DVDs*, Washington, DC: Council on Library and Information Resources, 2003 (http://www.clir.org/pubs/reports/pub121/pub121.pdf).

Congress on their PC."[82] Individuals also have an "increasing consumer digital creativity and an appetite for digital content."[83] Most importantly, however, Beagrie's article brings to our attention the challenges archivists will face in dealing with this material. He emphasized the need for continuous management of digital material for long-term preservation, the necessity of appraisal and selection by repositories, and the potential for emerging services that help individuals archive their own materials. While Beagrie presents no hard and fast rules or sure solutions for dealing with the explosion of digital content in the twenty-first century, his essay highlights the importance of beginning to deal with the challenges of what archivists have termed "personal electronic records," "digital private papers," and "electronic personal records."

The literature on electronic records in manuscript repositories dates to the 1990s. These records are generally referred to in the literature as personal electronic records. The literature, while not extensive, covers a wide variety of topics including acquisition, arrangement, description, preservation, custodial intervention, and the format variety. One of the earliest contributors to the literature on personal electronic records was Adrian Cunningham who recommended that archivists look beyond organizational records, and begin to examine the challenges inherent in the archiving of electronic personal papers. In this essay Cunningham argues several points, the most controversial being his claim that archivists should engage in "pre-custodial intervention" in order to ensure that records are created and managed in ways that maximize an archives' ability to preserve and provide access to them over time.[84] Cunningham's call to examine the role of personal electronic records led to further forays into the topic by archivists concerned with the preservation and accessibility of electronic records created outside of organizational contexts. Cunningham's early assertions about pre-custodial intervention were first challenged by Tom Hyry and Rachel Onuf's argument that pre-custodial intervention would skew the historical record "favoring the work of individuals who gain renown earlier rather than later in life."[85] Instead, Hyry and Onuf suggest a more conservative approach that balances the need to ensure long-term preservation and access with a mission to preserve not only the records themselves, but also to document "how the introduction of information

---

[82] Neil Beagrie, "Plenty of Room at the Bottom? Personal Digital Libraries and Collections," *D-Lib Magazine* 11: No. 6 (June 2005): http://www.dlib.org/dlib/june05/beagrie/06beagrie.html. Accessed May 26, 2011.
[83] Ibid.
[84] See Adrian Cunningham, "The Archival Management of Personal Records in Electronic Form: Some Suggestions," *Archives and Manuscripts* 22 (May 1994): 94-105, Adrian Cunningham, "Waiting for the Ghost Train: Strategies for Managing Electronic Personal Records Before It is Too Late," *Archival Issues* 24 (1999)" 55-64, and Adrian Cunningham, "Digital Curation/Digital Archiving: A View from the National Archives of Australia," 71, No. 2 (2008): 530-543.
[85] Tom Hyry and Rachel Onuf, "The Personality of Electronic Records," *Archival Issues* 22, No. 1 (1997): 37-44.

technologies into both public and private spaces changes the human behavior we strive to document."[86]

While these early archival musings on how to deal with electronic records were mostly theoretical, the last decade has seen the emergence of archival case studies dealing with the practical considerations of managing electronic records in manuscript repositories. Most of this literature has focused on the management of literary manuscripts, although Lucie Pacquet of Library Archives Canada (LAC), provides insight into the management of personal papers of government employees in Canada. Pacquet describes LAC's process for appraising and acquiring electronic records in the field and describes, in-depth, how she manages the process of working with donors of digital materials. Other practical essays include Catherine Peter Stollar's "When Not All Papers are Paper: A Case Study in Digital Archivy," in which she describes the University of Texas Harry Ransom Center's efforts to arrange, describe, and preserve the papers of author Michael Joyce. This project included the use of digital archeology to retrieve files from 5 ¼ inch floppy disks, as well as the arrangement and description of the collection. Stollar, along with Thomas Kiehne and Vivian Spoliansky, have written extensively about their experience with the floppy disks in the Joyce papers, providing reflection on the challenges of archiving electronic personal papers in literary manuscript repositories. Meanwhile, Michael Forstrom demonstrated that DACS can be used to record and make accessible information ensuring the authenticity of electronic personal papers.[87]

Of all these articles, the case of the Michael Joyce papers at the Harry Ransom Center is especially instructive for archivists working with hybrid collections of personal papers that include both paper and digital materials on removable media. While the particular concerns of the Ransom Center and the archivists working with the Joyce papers are not completely applicable to the situation encountered with the Granholm papers or the majority of Michigan Historical Collections acquisitions, the case study presents several important issues that all repositories collecting personal digital materials must now contend with. The main areas of decision making and challenge for acquiring and managing personal electronic records are: 1. arrangement and description, 2. third-party

---

[86] Ibid, p. 43.
[87] Catherine Stollar Peters, "When Not All papers are Paper: A Case Study in Digital Archivy," *Provenance* 24 (2006): 23-35, Catherine Stollar and Thomas Kiehne, "Guarding the Guards: Archiving the Electronic Records of Hypertext Author Michael Joyce," *News Skills for the Digital Era: Proceedings of a Colloquium Sponsored by the National Archives and Records Administration, Society of American Archivist and Arizona State Library, Archives and Public Records* (31 May-2 June 2006), http://www.lib.az.us/diggovt/documents/pdf/4_Stollar_Kiehne.pdf. Accessed May 31, 2011, Thomas Kiehne, Vivian Spoliansky, and Catherine Stollar, "From Floppies to Repository: A Transition of Bits, A Case Study of Preserving the Michael Joyce Digital Papers at the Harry Ransom Center," (May 2005): https://pacer.ischool.utexas.edu/bitstream/2081/941/1/Joyce_project-paper-final-draft.doc. Accessed May 31, 2011, and Michael Forstrom, "Managing Electronic Records in Manuscript Collections: A Case Study from the Beinecke Rare Book and Manuscript Library," *American Archivist* 72 (Fall/Winter 2009): 460-477.

works, 3. practical realities, and 4. the development of policies and procedures. In the case of the Michael Joyce papers the archivists chose to preserve the original order of the physical collection as well as to describe the records in functional series, rather than in series based on format. Digital and paper copies of manuscripts were also preserved in order to document the context in which Joyce composed his works.[88] While the decision to preserve the original physical and intellectual order of the collection in arrangement and description would apply to the Granholm papers, the Ransom Center's focus on the context of authorship proves less useful because the Michigan Historical Collections mission differs from that of a literary manuscript repository such as the Ransom Center. The Ransom Center is concerned with tracking even tiny changes related to the writing and revisions of literary manuscripts leading to their interest in preserving multiple copies in various formats, a focus on the context of creation, and an interest in digital forensics (described more thoroughly in the appendix).

Despite these differences, however, the Joyce case study had significant similarities to issues apparent in the Granholm papers. The Ransom Center's policy on the retention of third-party works, however, is perhaps more instructive. The archivists working on the Joyce papers initially decided to separate these materials because the Center did not hold copyright for them and therefore could not make them accessible in digital form. However, because the Center's policy was to keep third-party works in paper as evidence of context, the archivist also kept the digital third-party works, which were not made immediately accessible to researchers.[89] Other considerations highlighted by the project include practical considerations and the development of policies and procedures. Practical considerations included an assessment of costs, staff time and knowledge, hardware and software tools available and required, and the status of collections. Stollar also emphasizes the importance of developing clear policies and procedures surrounding the long-term preservation of digital records, however, the case study gives no practical examples of what these policies and procedures might be. Neither does Stollar address policies and procedures surrounding acquisition and appraisal, which may also be concerns for collecting repositories.[90] The Granholm papers present an opportunity for Michigan Historical Collections to think through such issues and make decisions about appraisal, arrangement, description, practical considerations, and the development of policies and procedures around hybrid and digital manuscript collections as a guide for future acquisitions.

Other Repositories

[88] Peters, "When Not All Papers Are Paper," p. 28.
[89] Kiehne, Spoliansky, and Stollar, "From Floppies to Repository," p. 15.
[90] Peters, " When Not All Papers Are Paper," pp. 34-35.

During the course of my research I also contacted several other repositories to ascertain their policies on the appraisal, management, and preservation of material that arrives in the archives on removable media. At the University of North Carolina's Carolina Digital Repository (CDR), staff members are implementing a workflow to handle digital materials on removable media from the time of their arrival at the CDR through the processing stage. This will soon include the use of a "jukebox" workstation for processing obsolete media. The workstation will have old drives attached to the machine to handle old media and will be write blocked so that files cannot be altered during processing. Processing is done with the Curator's Workbench, developed in house at the CDR.[91] At Harvard University the staff of the University Archives is currently working with MIT to deal with the issue of removable media. While it has been an ongoing point of discussion, the archives are only now beginning to develop a process for this material. Their plan includes the development of a digital forensics facility to ensure proper transfer of files and provide access to obsolete media.[92] The archivist at Harvard who answered my query is of the opinion that once the files are transferred the removable media can be treated like a box or folder and discarded.

In addition to information culled from practitioners at other repositories, Susan E. Davis's study of electronic records in digital repositories has turned up a lack of policies and procedures at collecting repositories. Instead, repositories are dealing with electronic records in manuscript collections on a case-by-case basis. Davis found that repositories accept digital records at a high rate, but report having policies that deal specifically with the acquisition and management of digital materials at very low rates. Her research indicated that only 24% of the repositories responding to her survey had digital records acquisition policies in place and, of those that did have policies, 57% did not differ from the policies for traditional records. Of repositories having policies for the acquisition of digital records, only 30% have policies for preservation of those records.[93]

Finally, the Bodleian Library's *Paradigm Workbook on Digital Private Papers* provides a comprehensive and practical overview of managing digital and hybrid manuscript collections from initial appraisal and acquisition through long-term preservation. The *Workbook*'s practical tips, examples, and overview of legal, arrangement and description, and preservation concerns makes it the most comprehensive guide to issues related to electronic personal records. It contains best practices for acquiring, appraising, processing, arranging and describing, and preserving digital manuscripts. I

[91] More information on Curator's Workbench can be found at http://www.lib.unc.edu/blogs/cdr/index.php/2010/12/01/announcing-the-curators-workbench/. Also see the appendix for a brief overview of digital forensics possibilities in archival repositories.
[92] A very brief description of the project can be found at http://osc.hul.harvard.edu/liblab/prop1.
[93] Susan E. Davis, "Electronic Records Planning in 'Collecting' Repositories," *American Archivist* 71 (Spring/Summer 2008): 178-180.

refer to the *Workbook* at several points below as a resource to consult in developing policy.[94]

Issues to Consider

Appraisal of Content

The current content on the removable media in the Jennifer Granholm papers includes text, audio, and video files produced by her office, third party materials that were either sent to her staff or collected by them as part of their legal and policy research, and materials produced by the federal government and the government of the State of Michigan for informational, training, and public service purposes. In regard to the paper files, materials are being kept in staff files, however, the digital versions of such material present special challenges that do not exist for the paper materials for reasons of rights and access management noted in the next section.

Current standards for appraisal of electronic records is similar to, but not identical to the appraisal of paper records. In addition to the considerations applied to paper records, the InterPARES 1 (International Research on Permanent Authentic Records in Electronic Systems) recommends that archivists take into account the feasibility of preserving the electronic files long-term, or what the *Paradigm Workbook* refers to as technical appraisal.[95] On the original media, these files present preservation issues because of the uncertainty that those media will remain readable over the long term. However, if the records are removed from the CDs and DVDs, they will likely be able to be preserved long term. The video files, however, are especially vulnerable to loss, as there are no current community standards concerning a preservation format for video.[96] Additional concerns relevant to the digital content are: provision of access and rights management. Unlike paper materials, for which it is easy to limit access and control copying, digital records provide challenges in these areas.

Additional concerns related to the appraisal of not only digital materials, but also hybrid collections is covered by the *Paradigm Workbook*, which covers issues of disposal

---

[94] University of Oxford, University of Manchester, *Paradigm Workbook on Digital Private Papers,* *http://www.paradigm.ac.uk/workbook/index.html*. Accessed May 31, 2011.
[95] InterPARES 1, *Appraisal Task Force Final Report*, http://www.interpares.org/display_file.cfm?doc=ip1_aptf_report.pdf . Accessed May 31, 2011, and http://www.interpares.org/ and *Paradigm Workbook*, http://www.paradigm.ac.uk/workbook/appraisal/appraisal-issues.html. Accessed May 31, 2011.
[96] See the Library of Congress's "Sustainability of Digital Formats: Planning for Library Collections," section on moving images at http://www.digitalpreservation.gov/formats/content/video.shtml. Also see, Howard Besser, "Digital Preservation of Moving Image Material?": *The Moving Image*, Vol. 1, No. 2 (Fall 2001): pp. 39-55.

and issues specific to hybrid collections. *Paradigm* also provides practical solutions, recommended approaches, and tools and resources. They recommend dividing the appraisal of digital and hybrid collections into macro and functional appraisal, bottom-up appraisal, and technical appraisal, while also recommending that archivists consider the content, context, and structure of each collection individually once acquired.[97]

Rights Management, Privacy, Confidentiality and Access

Neal Beagrie's states that "personal collections are often composite drawing material from the individual's private life, work, and education, as well as from external communities and content sources. Ownership and intellectual property rights in such collections are therefore often diverse and complex. These collections are often composed of materials intended solely for private reference and use, and/or materials intended to be shared with others at work or with other communities including family, friends, and interest groups" is especially relevant to the situation presented by the Granholm papers.[98] While analog personal collections also have these characteristics, the ease of copying digital files makes managing their rights more challenging. The materials created by Granholm's office are not necessarily problematic in this area, nor are the government materials, which are, in many cases, already publically accessible. In some cases, there may be privacy and/or confidentiality issues with these materials, such as materials issued only to other government staff for their use on the job. These are, however, a small number of the overall total of digital files on removable media. The third-party materials either sent to or collected by Granholm's staff in the course of their work, however, present a particular problem. While her staff likely used many of these materials, their copyright is held by the producers of the material, which means that copying and use are controlled. While I have not thoroughly checked the copyright status and confidentially/privacy issues for each of the removable media, this material is currently a minority of the content in the collection. Much of the material consists of audio-visual material of the Governor or related to state government activities.

Copyright issues associated with the third-party materials means that provision of access to the material would have to be carefully monitored. Restrictions on access could include restrictions by IP address, e. g. only accessible at the Bentley Historical Library, restrictions by user, e. g. only accessible to authenticated and registered users, the use of terms and conditions statements/access statements, and restrictions by work station, e. g. only available at a non-networked computer in the Bentley reading room. The first three

---

[97] *Paradigm Workbook* http://www.paradigm.ac.uk/workbook/appraisal/appraisal-approaches.html and http://www.paradigm.ac.uk/workbook/appraisal/appraisal-issues.html. Accessed May 31, 2011.
[98] Neil Beagrie, "Plenty of Room at the Bottom? Personal Digital Libraries and Collections," *D-Lib Magazine,* 11, No. 6 (June 2005): http://www.dlib.org/dlib/june05/beagrie/06beagrie.html. Accessed May 26, 2011.

solutions or some combination thereof would not prevent copying, but would insure the ability to track users, however, they could be difficult to implement. The third could potentially restrict access and copying, but could be difficult to implement for reasons of arrangement and description as discussed below. Current technology also includes watermarks and the disabling of copy and save functionalities, however, these are likely not technically feasible at this time.[99] The *Paradigm Workbook* also presents the possibility of risk management or "take down" policies in which material is made accessible after archival review, but removed if objectionable information or copyright infringement is found at a later time.[100]

Processing Workflow

If digital materials are to be moved off of removable material in the Granholm papers and other collections, a workflow for managing this process will be required. This workflow can be based on workflows already established or being established by the University Archives and Records Program (UARP) to deal with digital records of the University of Michigan, however, it will likely have significant differences. Areas of overlap include virus scans, integrity checks (checksums), long-term storage in a dark archive which is not accessible to researchers, and possibly deposit into Deep Blue, the University's institutional repository. Since Michigan Historical Collections is likely to get digital files in multiple formats and on a wide variety of media, hardware and software to read these media and a work station with appropriate drives and software for reading files will be necessary to access files although the Granholm papers seem to contain only CD and DVD media at this time. The acquisition of several "Rosetta computers" or a "jukebox" workstation are potential solutions.[101] Finally, the files will need to be moved from the local computer workstation to server storage, both for long-term storage and preservation and possible ingest into Deep Blue.

In addition to a workflow for processing files that come in on digital media, Michigan Historical Collections may want to develop a field acquisitions survey to assist processors when they encounter a collection with digital media in it. Lucie Pacquet's

---

[99] Several good overviews of issues and systems dealing with access and rights management for digital libraries and archives have been published in *D-Lib Magazine*. Two overviews, one recent, and one from the 1990s provide an overview of some of the technological and policy frameworks that can be used to handle the provision of access to copyrighted content: Kristin R. Eschenfelder and Grace Agnew, "Technologies Employed to Control Access to or Use of Digital Cultural Collections: Controlled Online Collections," *D-Lib Magazine*, vol. 16, No.1/2 (January/February 2010), http://www.dlib.org/dlib/january10/eschefelder/01eschenfelder.html. Accessed May 27, 2011 and William Yeo Arms, "Implementing Policies for Access Management," *D-Lib Magazine*, (February 1998): http://www.dlib.org/dlib/february98/arms/02arms.html. Accessed May 27, 2011.
[100] http://www.paradigm.ac.uk/workbook/legal-issues/impact.html.
[101] Rosetta computers are old computers that have now obsolete hardware on them, making it possible to read files that arrive at the archives on obsolete removable media.

overview of LAC's digital acquisitions survey and transfer process may prove useful in developing a similar tool. The *Paradigm Workbook* also provides significantly helpful information on establishing acquisition and processing workflows for such materials. Especially useful for processing and acquisition are their sample digital records surveys, information on initial assessment and transfer of digital materials, and section on arrangement and cataloging (description).[102]

Arrangement and Description

The arrangement and description of this material could also be challenging. In the case studies of the Michael Joyce papers, noted above in the literature review, the archivists responsible for processing chose to arrange third-party materials separately from the rest of the collection and ingregate other materials with the paper records. The description of their process seemed to indicate that they did not consider the third-party files integral to other parts of the collection. However, in the case of the Granholm papers, and most Michigan Historical Collections collections, the digital files that come on removable media are integrated into paper files. While they could be moved out of the folders in which they came and described separately in order to achieve intellectual control, this would eliminate the contextual basis that gives them value. Doing this for materials that are not third-party materials, but are topically related to paper folders would present the same problem. In the Granholm collection, because files are organized by the staff member who created them removing the files would completely divorce them from the creator of the file. In all likelihood an approach that maintains the content and context of the records will require individually editing the EAD in order to provide links to the digital materials that came in individual folders.

Conclusions

The acquisition and processing of the Jennifer Granholm papers presents an opportunity for the Michigan Historical Collections to begin to develop policies and procedures around the appraisal, arrangement and description, and processing workflow for hybrid and digital manuscript collections. In particular, the concerns outlined above are critical to managing materials that arrive in collections on removable media, which are

---

[102] *Paradigm Workbook*, http://www.paradigm.ac.uk/workbook/appendices/records-survey.html, http://www.paradigm.ac.uk/workbook/record-creators/accessioning.html, http://www.paradigm.ac.uk/workbook/record-creators/common.html, and http://www.paradigm.ac.uk/workbook/cataloguing/index.html. Accessed May 31, 2011. The same approach is advocated by Matthew G. Kirschenbaum, Richard Ovendon, and Gabriela Redwine in *Digital Forensics and Born-Digital Content in Cultural Heritage Collections*, Washington, D. C.: Council on Library and Information Resources, 2010.

not a stable long-term preservation media. The presence of these CDs and DVDs present appraisal concerns about the importance of these files to the larger collection, how they should be described in the finding aid, what rights management and access issues they present, and how they will be processed. The priority concerns for this hybrid collection are: rights management and access to files on removable media, practical processing issues related removing the files from the media, and issues of arrangement and description of these files once they have been removed, processed, and transferred to a preservation repository. Other concerns include policies and procedures for ensuring removable media is discovered at the pre-custodial stage, and perhaps developing general guidelines for donors along the lines of those advocated by the *Paradigm Workbook*.[103]

At this current moment in the processing, I can affirm that most, but not all, of the files currently on CDs and DVDs were produced by the Governor's Office and would likely not present additional rights management or access issues. However, there are removable media in the collection produced by third-parties. One option is to leave these media in the folders as evidence of types of materials the Governor's staff relied on, but not to move them to a preservation repository. Another option would be to transfer them, but to bar access. A third option would be to provide some sort of limited access that limits or prevents copying. This case also presents an opportunity for developing an appraisal policy centered on removable media. What should be kept? What should be destroyed? It also raises the question of whether there should formal acquisition policies and procedures for digital media to highlight such issues before the processing stage and to clarify processing and preservation priorities and capabilities to donors. Finally, if files will be removed from the removable media in this collection it provides an opportunity to not only create a workflow for managing removable media in the Granholm papers, but also to produce a more comprehensive workflow for processing digital media in other collections and to explore the possibility of establishing a write-protected work station for managing the conversion of legacy formats and accessing legacy media.

Appendix

Digital Forensics

According to the Council of Library and Information Resources *Digital Forensics and Born-Digital Content in Cultural Heritage Collections* "digital forensics is an applied field originating in law enforcement, computer security, and national defense. It is concerned with discovering, authenticating, and analyzing data in digital formats to the standard of

[103] *Paradigm Workbook*, http://www.paradigm.ac.uk/workbook/appendices/guidelines.html.

admissibility in a legal setting."[104] The hardware and software capabilities developed to allow professionals in the above settings to engage in digital forensics work also has the potential to assist archivists in the processing, arrangement and description, and preservation of born-digital manuscript collections. Digital forensics software can provide comprehensive manifests of donated electronic files, create disk images to ensure the integrity of the digital content, recover lost or inadvertently deleted files, ensure provenance, and de-duplicate files.

Another advantage of digital forensics is the ability to image entire computer environments. Doing this allows archivists to be able to determine the relationships of the materials contained within these environments, and potentially to document relationship to personal digital devices such as smart phones. One particular advantage of capturing disk images is that it allows a bit-for-bit copy to be created before any of the files are accessed. In this way, the archive can ensure the integrity of all the files and ensure that all of the contents of the original media are captured and preserved, including hidden and deleted files. Digital forensics eases processing by quickly copying the contents of a disk image and allowing archivists to search for and redact personal and private information. This is less time consuming and complex than copying each of the files individually and then processing them in varying ways. Digital forensic techniques also allow archivists to manage disk images with preservation metadata and naming conventions. A technique such as this allows archivists to "simplify the initial stages of capture, preservation metadata, and storage."[105] Once this is done they can save more complex processes for later, more detailed processing. Finally, because digital forensic techniques can uncover changes to files over time, before the current version, they could potentially assist archivists who work with material donated by third parties or family members who are not the creator, to assess whether the files have been tampered with before arriving at the archives or to confirm a chain of custody presented by a donor.

One of the challenges that digital forensics does not solve in the challenge of legacy formats. Even while it has the potential to make processing "more efficient and more secure," it cannot solve the problem of accessing all legacy file formats or removable media types.[106] A digital forensics lab can make it easier read files created on various file systems, but will not always work. Rosetta computers or jukebox workstations, mentioned earlier, are other possible solutions. There is, unfortunately, no one magic bullet for this problem, and, while digital forensics labs could ease this process, it cannot completely solve it.

[104] Matthew G. Kirschenbaum, Richard Ovendon, and Gabriela Redwine, *Digital Forensics and Born-Digital Content in Cultural Heritage Collections*, p. 1.
[105] Ibid, p. 26
[106] Ibid, p. 21.

Digital forensics is a new and evolving field in the cultural heritage community. It has many potential applications, but also raises questions of ethics and level of granularity needed in processing collections. If deleted files can be retrieved, should they? How would this affect donor agreements? On-site assessments? Digital forensics is not a magic bullet. *Digital Forensics and Born-Digital Content in Cultural Heritage Collections* argues that "incorporating forensic methodology and tools into an archival workflow will enable digital archivists and curators to capture more information about the content and makeup of digital objects; help repositories manage the data copies from disks more efficiently and in accordance with established standards; reinforce the importance of documentation to all aspects of the curation cycle; and give archivists, donors, and others the ability to preview the contents of both isolated storage media and complete computing systems to formulate acquisition and preservation strategies."[107] However, the authors of the report also note that "in many cases commercial software and a full forensic workstation may exceed the needs of the repository's collection materials."[108] Additionally, not all repositories will have the financial resources to invest in such technology. However, components of digital forensics methodology to ease process and ensure authenticity can be incorporated in a workflow for digital manuscripts without a full investment in a digital forensics lab. Such solutions will likely be preferable for many small collecting repositories, and those that do not have a mission to comprehensively document the context of creation or minuscule changes in files.

[107] Ibid, p. 60.
[108] Ibid, p. 61.

Appendix 6: Digital Forensic Software Breakdown

Program	Annotation	Automation—Built-in	Automation—Scriptable	Bookmarking	Built-in File Viewers	Command Line	Custom Filtering	Data Carving	Data Visualization	Dead Analysis	Cryptanalysis	Encryption	Export Data/Files	Export Metadata	Identification/Verification	GUI[1]	Hex Editor	Hex Viewer	Imaging/Cloning	Live Analysis	Major OSes/File Systems[2]	RAM Capture	RAM Editing	Registry Analysis	Reporting/Logging	Search	Steganalysis	Timelines	Virtualization	Volume/File Rebuilding	Write-blocking
Autopsy Forensic Browser /Sleuth Kit	Y		Y	P		Y		Y		Y	P		Y	Y	P	Y		Y		Y	P				Y	Y	Y	Y		P	
ByteBack								Y		Y			Y		Y	P	Y		Y		P				Y		P			Y	Y
Coroner's Toolkit[3]						Y		Y		Y	Y		Y		Y				Y	Y	Y						Y			Y	
Encase Forensic	Y	Y	Y	Y	Y		P	P		Y	Y		Y	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y	Y	Y	Y	Y	Y	Y
Forensic Toolkit								Y		Y	Y	Y	Y	Y		Y			Y		Y			Y	Y	Y	Y				Y
Helix 3 Pro					Y					Y	P		Y	Y		Y				Y	Y	Y			Y	Y	Y			Y	Y
iLook	Y		Y		Y		Y	Y	Y	Y	Y		Y			Y		Y	Y		Y			Y	Y	Y		Y			
MacForensicsLab	Y	P		Y	Y		Y	Y		Y				Y		Y		Y	Y	4	Y				Y	Y	Y			Y	P
Macintosh Forensic Suite					P	P		Y		Y						Y										Y	Y				
MacMarshall			Y							Y	Y		Y	Y		Y									Y	Y	Y				Y
NTI Computer Incident Response Suite										Y	P							Y	Y							Y		Y		Y	
Nuix Desktop	Y						Y		Y					Y		Y										Y		P			
Online DFS													Y	Y		Y			Y	Y	Y	Y		Y		Y					
P3 Command Kit	Y			Y	Y	P	Y	Y		Y	Y	Y	Y	Y	Y	Y		Y	Y	5	P	Y		Y	Y	Y	Y			P	Y
ProDiscover Forensics		Y	Y		Y					Y				Y		Y			Y	6	P			Y	Y	Y	Y				Y
Responder Pro			Y						Y	Y						Y				P		Y			Y						
SMART								Y	P	Y			Y	Y	P	Y		Y	Y	P	P			Y	Y	Y					Y
X-Ways Forensics	Y			Y	Y		Y	Y	P	Y	P		Y	Y	Y	Y			Y		P	Y		Y	Y	Y				Y	Y

Program	File Type	Open/ Closed[7]	File-System Support[8]						Compression	Clone	Sparse	HDD	Media
			NTFS	FAT	HFS	EXT	UDF	HPA/ DCO					
Autopsy Forensic Browser /Sleuth Kit[9]	AFF, E01, EWF	Open	Y	Y	HFS+	Y		Y	Y			Y	
ByteBack	Unknown		Y	Y					Y	Y		Y	
Encase Forensic	E01, EWF, Raw	Closed	Y	Y	Y	Y	Y		Y			Y	Y
Forensic Toolkit	EWF, E01, S01, SafeBack, Raw	Closed	Y	Y	Y	Y			Y			Y	Y
Helix 3 Pro[9]	Raw, E01, AFF, ISO	Both	Y	Y	Y	Y		Y	Y	Y		Y	Y
iLook	ASB, IRBF, IEIF, IDIF	Closed	Y	Y	Y	Y		Y	Y	Y		Y	Y
MacForensicsLab	ISO, DMG, Sparseimage, Raw	Both	Y	Y	Y	Y			Y		Y	Y	Y
Macintosh Forensic Suite	DMG, Raw	Closed	Y	Y	Y							Y	
NTI Computer Incident Response Suite	Safeback, dd	Closed	Y	Y		Y					Y	Y	Y
Online DFS[10]	dd	Open								Y		Y	Y
P3 Command Kit[11]	PFR/PFIF, ISO	Closed	Y	Y		Y			Y			Y	Y
ProDiscover Forensics[9]	CMP, EVE, Raw, dd	Open	Y	Y		Y		Y	Y			Y	
Raptor	E01, DMG, Raw	Closed	Y	FAT32	HFS+	EXT3		Y	Y	Y		Y	
SMART	SMART default (.image), SMART Compressed (.S01) E01, EWF, RAW	Closed		Y	Y	Y		Y	Y			Y	Y
X-Ways Forensics	E01, EWF, Raw, WinHex	Closed	Y	Y	Y	Y	Y	Y	Y	Y		Y	

Publisher/Product	Cost	Technical Requirements/Notes
Autopsy Forensic Browser/ Sleuth Kit	Free	UNIX based, but can be accessed through an HTML interface. No information available on system requirements. http://www.sleuthkit.org/contact.php Autopsy provides a front end for Sleuth Kit, which itself is heavily based on the Coroner's Toolkit.
Tools That Work ByteBack	$492.95 Free trial	MS-DOS (includes FreeDOS) Drive + media to create boot disk No information on system requirements available. http://www.toolsthatwork.com/computer-forensic.htm
Guidance Software EnCase Forensic	Standard: $3,600 Government: $2,850	Windows 2000 or newer 3.0 GHz CPU 2 GB RAM 1 USB port http://www.guidancesoftware.com/computer-forensics-digital-investigation-law-enforcement.htm
Access Data Forensic Toolkit (FTK) 2.x	Stand-alone + 1-year subscription $3,835	64-bit edition of Windows Intel i7 2.66 GHz or better CPU 8 GB DDR3 RAM (12 GB recommended) 60 GB 10,000 RPM hard disk (for OS) 20 GB 10,000 RPM hard disk (for Oracle) Supports RAID configurations http://www.accessdata.com/
e-fense Helix3 Pro	$239/year CD only (no support): $150 Free trial available	CD or DVD drive The Forensics Wiki lists some known issues with this software. http://www.e-fense.com/products.php
Perlustro iLook	Free	Windows NT or newer No further information available on system requirements. Free to qualifying institutions with law enforcement missions. Some criminal justice education programs may qualify. http://www.perlustro.com/ustreasury_website/index.html
MacForensicsLab	$1,445 Free trial available	***All versions require a HASP license dongle for license verification (supplied with purchase).*** Mac OS X 10.4 or newer; Windows XP or newer; x86-based Linux distribution with GTK+ 2.0 (or higher), glibc-2.3 (or higher), and CUPS (Common UNIX Printing System) 800 MHZ or faster (2 GHZ or better recommended) CPU 512 MB of RAM (2 GB or more recommended) DVD-ROM drive for Boot CD/DVD and Installation from DVD 1 TB or more hard disk space recommended http://www.macforensicslab.com Extensive documentation available on the Web site
BlackBag Macintosh Forensic Suite	Standard: $799 Government: $699	OS X 10.4 or later 1 GB or more RAM 500 MB available hard disk space http://www.blackbagtech.com/store/software/blackbag_macintosh_forensic_suite.html The Forensic Suite may support more features than listed; little documentation is available.
Architecture Technology Corp. Mac Marshal	$995	Mac OS X 10.4 or 10.5 50 MB available hard disk space http://macmarshal.atc-nycorp.com/
New Technologies, Inc. Computer Incident Response Suite	$1,118	No information available on system requirements. http://www.forensics-intl.com/suite1.html
Nuix Desktop	$7,500–$15,000 per user per year; price dependent on features selected.	Focuses primarily on e-mail. No information available on system requirements. http://www.nuix.com/
Cyber Security Technologies Corporation OnLine Digital Forensic Suite (DFS)	Standard: $9,000 Law Enforcement: $3,000	No information available on system requirements. http://www.onlinedfs.com/products_dfs.asp
Paraben Corp. P3 Command Kit	$3,995 Demo available Prior edition (P2) available for $1,995	Windows 2000 or newer 1.4 GHz or better processor 1 GB RAM 200 MB available hard disk space http://www.paraben-forensics.com/
ProDiscover Forensics	$2,195 Demo available	Windows 2000 or newer 1.2 GHz or higher Pentium-compatible CPU 256 MB RAM (512 MB recommended) 500 MB available hard disk space CD-ROM or DVD-ROM drive VGA or higher-resolution monitor http://www.techpathways.com/prodiscoverdft.htm
HBGary Responder Pro	$9,000 "Field" edition available for $979	Windows 2000 or newer No further information available on system requirements. Primarily used for malware detection and analysis; has many options for visualization. http://www.hbgary.com/
ASR SMART	$2,000	Linux No information available on system requirements. Available as a Live CD http://www.asrdata.com/
X-Ways Forensics	$1,118	Recommended (minimums not listed) Windows 7 64-bit Quadore CPU 4 GB or more RAM Hex viewer/editor and RAM editor available through WinHex, which can be downloaded as an add-on. http://www.x-ways.net/

Title	File Type	OS	NTFS	FAT	HFS	EXT	UDF	HPA/DCO	Compression	Clone	Sparse	HDD	Media	Price	Web Site
AFFlib	AFF, AFM (raw), E0/EWF, splitraw, VMDK	Unix	Y	Y		Y			Y	Y		Y		Free	http://www.afflib.org
Arconis Backup & Recovery (formerly True Image)		Windows/ Linux	Y	Y	N	N	N		Y	Y		Y		$49.99+	http://www.acronis.com
Clonezilla		Unix	Y	Y	Y	Y		?/Y	Y	Y	Y	Y	N	Free	http://www.clonezilla.org/
Daemon Tools Pro	B5T, B6T, BWT, CCD, CDI, CUE, ISO, MDS, NRG, PDI, and ISZ	Windows	N/A	N/A	N/A	N/A	N/A						CD \ DVD	$140	http://www.daemon-tools.cc/
dcfldd	RAW	Unix/Mac	Y	Y	Y	Y	Y	?/Y	N	Y	N	Y	Y	Free	http://dcfldd.sourceforge.net
dd	RAW	Unix/Mac	Y	Y	Y	Y	Y	?/Y	N	Y	N	Y	Y	Free	Built-in command
dd_rescue	RAW	Unix	Y	Y	Y	Y	Y	?/Y	N	Y	N	Y	Y	Free	http://www.gnu.org/software/ ddrescue/ddrescue.htm
Ddrescueddrescue	RAW	Unix	Y	Y	Y	Y	Y	?/Y	N	Y	N	Y	Y	Free	http://www.garloff.de/kurt/ linux/ddrescue
Disk Utility	DMG, CDR	Mac		Y	Y				Y	Y	Y	Y	Y		Included in MacOS
DriveImageXML	Combination of DAT and XML	Windows	Y						Y			Y		Free	http://www.runtime.org/ driveimage-xml.htm
Guymager	Rawraw, EWF, E01, AFF	Unix												Free	http://guymager.sourceforge. net/
Macrium Reflect			Y	Y		Ext2			Y			Y	Y		http://www.macrium.com/
Ntfsclone		Unix	Y							Y	Y	Y		Free	http://linux-ntfs.org/
PartImage		Unix						?/Y					N		

Title	Environment	Specialization	Price	Web Site
BackTrack	Slackware		Free	http://www.remote-exploit.org/backtrack.html
ByteBack DRIS	Freedos	HDD and MBR repair	Free	http://www.toolsthatwork.com/byteback.html
CAINE Live CD	Ubuntu	User-friendly GUI and automated reporting	Free	http://www.caine-live.net/
DEFT Linux	XUbuntu		Free	http://www.deftlinux.net/
Digital Forensics Live CD (DFLCD)			Free	http://www.forensiclivecd.com/ **Note:** No longer actively supported.
FCCU GNU/Linux Forensic Boot CD	Debian		Free	http://www.lnx4n6.be/
Grml	Debian			http://grml.org/
Helix3 and Helix3 Pro	Ubuntu		$0–$239	http://www.e-fense.com/helix/ **Note:** Free version no longer receiving updates.
INSERT Rescue Security Toolkit	Knoppix			http://www.inside-security.de/insert_en.html
MacQuisition		Imaging Mac devices	$400–$599	http://www.blackbagtech.com/
Masterkey	Slackware	Incident response		http://masterkeylinux.com/
Openwall (Owl)	Linux	Password recovery	Free to download, $28.86 to ship.	http://www.openwall.com/john/
Operator	Debian/Knoppix	Network security		http://www.ussysadmin.com/operator/
Professional Hacker's Linux Assault Kit (PHLAK)	Morphix	Network security	Free	http://sourceforge.net/projects/phlakproject/
Raptor	Ubuntu	Acquisition	$49.95	http://www.raptorforensics.com/
SPADA	Knoppix			
System Acquisition Forensic Environment (SAFE) Boot Disk	Windows	Read-only imaging	$399	http://www.forensicsoft.com/catalog/product_info.php?products_id=31http://www.forensicsoft.com/catalog/product_info.php?products_id=31
THE FARMER'S BOOT CD (FBCD)		Preacquisition examination	$225	http://www.forensicbootcd.com/

[109]

[109] Kirschenbaum, "Digital Forensics and Born-Digital Content in Cultural Heritage Collections," 72-77.

Appendix 7: Digital Forensics Glossary

Digital Forensics and Cultural Heritage

Presented by: Matthew Kirschenbaum and Rachel Donahue
University of Maryland

Glossary

The bulk of forensics work done in archives and other cultural heritage institutions uses software to read, rebuild, analyze, and secure data from acquired storage devices and media—-in forensics terms, using software to conduct "dead analysis." These tools may be bundled in a full-blown forensics package or distributed as individual, specialized programs or scripts. They may have graphical user interfaces or may require familiarity with command line interactions. The functions most relevant to archival work are imaging, data recovery, and logging.

Software

Imaging

Imaging is the technique of making a soft copy of an entire storage medium (or partition, in the case of hard drives) rather than copying individual files. The resulting image can be manipulated in the same ways as the original, without the hardware. Images come in two general varieties: sparse and bit-exact (sometimes called a clone). A sparse image copies only the sectors which contain data, ignoring any zero-byte sectors and thereby resulting in a smaller file. Bit-exact images contain the entire disk or partition, resulting in a file the same size as the original medium's full capacity. Disk clones can typically be restored only to a partition of the same size as the original, while sparse images can be restored to any partition large enough to contain the data.

Data Recovery

In addition to imaging, data recovery covers all processes to retrieve damaged, deleted, or otherwise hidden data. The broad categories of data recovery are rebuilding, in which damaged file systems are rebuilt; data carving, which can be used to recover data even in the absence of a healthy file system; and steganalysis, or processes to find and retrieve hidden data.

Logging

As with any preservation activity, processes used to recover data must be recorded. Because forensics software has been designed for legal investigation, many of these programs have robust, automatic logging systems.

Other Uses

Many functions outside these core features may also be valuable to an archivist. Encryption software can ensure adequate protection for sensitive materials, and decryption software may aid in accessing the data of donors unable to supply their passwords. Annotation and bookmarking abilities can aid in highlighting materials of interest or flagging trouble spots. Filtering, search, and (meta)data extraction have their obvious benefits, and it, if the item in question is an entire computer, it is possible that, in the case of a full-workstation donation, RAM and registry analysis could be valuable. Many of the packages also offer a range of visualization and time-lining options that can aid in understanding the range of materials in a donation.

Live Distributions

Live distributions, often referred to as "live CDs" or "live distros," are operating systems designed to run without from external media (CD, DVD, or flash drive)without installation. Working in this way is useful if the target computer is malfunctioning or compromised, or simply lacks the necessary tools.

Hardware

Write-blockers

Floppy disks were once made with a tab that allowed them to be accessed in "write-protect mode." This manual precaution ensured that whatever was done with the data by the computer accessing it, the original disk would not change. Optical media and hard drives offer no such built-in protections, and including a hardware intermediary between the read-device and the computer provides extra assurance that the original data are unchanged.

Prices range from $150–$200 for a simple USB adapter or dock to $1,000–$2,000 for write-blocked data duplication devices.

Cryptography devices

Hardware devices exist for both encryption and decryption. Decryption devices perform brute-force attacks that the user can hook to an encrypted device while using his or her workstation for other tasks. On the encryption side, hardware offers an extra layer of security (or barrier to entry): hardware-encrypted media cannot be decrypted without the physical key.

Because of the extreme processing power required for brute-force attacks, decryption devices cost between $5,000 and $20,000. A USB encryption key may cost as little as $10, while encrypted hard drives run between $500 and $1,000.

Data copiers

Data copiers are equipped with bays for drives or media to be copied from and to. These devices typically take bit-exact images of whatever they are copying, and are often designed with mass-copying in mind.

Adapters

The number of connectors for internal and external devices is astounding: SCSI, IDE, SATA, SAS, ESDI, Firewire, a dozen varieties of USB, and more. Having every type of connection built into a machine is unlikely, especially when dealing with archival (i.e., likely obsolete) materials. In many cases, an adapter is available to convert an acquired drive's interface into one supported by the user's system (e.g. using a SATA-to-USB cable to read a laptop hard drive with a desktop PC).

Adapters may be cables, enclosures, or dongles and range in price from $10–$100.

Website

http://mith.umd.edu/forensics/

Report

Co-authored by Matthew Kirschenbaum, Richard Ovenden of the British Libraries, and Gabriela Redwine of the Harry Ransom Center, with assistance from Rachel Donahue, the full *Digital Forensics and Born-Digital Content in Cultural Heritage Collections* will be available from CLIR in electronic form at the beginning of December, with a print edition to follow soon after. More information can be found at: http://www.clir.org/pubs/pubs.html

[110]

[110] Kirschenbaum, "Digital Forensics and Cultural Heritage Glossary."

References

Accurite. "Floppy Disk Drive Primer." Last modified 2007. http://www.accurite.com/FloppyPrimer.html.

Archive Team. "Rescuing Floppy Disks." Last modified January 23, 2012. http://archiveteam.org/index.php?title=Rescuing_Floppy_Disks.

Ball, Alex. Digital Curation Centre, "Digital Forensics for Preservation." Last modified July 7, 2011. http://www.dcc.ac.uk/news/digital-forensics-preservation.

Bradley, Kevin. *Risks Associated with the Use of Recordable CDs and DVDs as Reliable Storage Media in Archival Collections - Strategies and Alternatives*. Canberra: Unesco, 2006.

Byers, Fred R. *Care and Handling of CDs and DVDs: A Guide for Librarians and Archivists*. Washington, DC: Council on Library and Information Resources, 2003.

Cohen, Frederick, and Preston Charles. *Recovering Data from Floppy Failing Floppy Disks*. *Advances in Digital Forensics IV*. Edited by Ray, Indrajit and Sujeet Shenoi. Springer, 2008.

"Digital Archaeology Lab Procedures." University of Texas - Austin, 2011. https://pacer.ischool.utexas.edu/handle/2081/21808.

Entlich, Richard. "One Last Spin: Floppy Disks Head toward Retirement." *RLG DigiNews*. 8. no. 6 (2004). Accessed June 15, 2012. http://worldcat.org/arcviewer/1/OCC/2007/07/10/0000068923/viewer/file1.html.

Entlich, Richard and Ellie Buckley. "Digging Up Bits of the Past: Hands-on With Obsolescence." *RLG DigiNews*. 10. no. 5 (2006). Accessed June 4, 2012. http://worldcat.org/arcviewer/1/OCC/2007/07/10/0000068996/viewer/file1.html

Finch, Lorraine and John Webster. *Caring for CDs and DVDs*. National Preservation Office, 2008.

Florida Department of State Division of Library & Information Science. "Protect your Video and Audio Tapes, and Floppy Disks." Accessed June 15, 2012. http://dlis.dos.state.fl.us/archives/preservation/magnetic/index.cfm.

Garfinkel, Simson L. "AFF: A New File Format for Storing Hard Drive Images." *Communications of the ACM*. 49. no. 2 (2006): 85-87.

Herbert, Nicola. Born Digital Archives, " Forensic Workstation, Pt3." Last modified August 30, 2011. http://born-digital-archives.blogspot.com/2011/08/forensic-workstation-pt3.html.

Hull History Centre. "Idiot's Guide 2 - Tableau Write Blockers." Last modified September 6, 2011. http://www.hullhistorycentre.org.uk/discover/pdf/Idiot's Guide 2 - Tableau Write Blockers.pdf.

Indiana University Information Technology Services. "What is Meant by Mounting a Drive?" Last modified February 18, 2011. http://kb.iu.edu/data/anqk.html.

Iraci, Joe. "The Relative Stabilities of Optical Disc Formats." *Restaurator*. no. 26 (2005): 134-150.

JISC Digital Media. "Using Optical Media for Digital Preservation." Last modified November 21, 2007. http://www.jiscdigitalmedia.ac.uk/stillimages/advice/using-optical-media-for-digital-preservation/.

John, Jeremy Leighton. “Adapting Existing Technologies for Digitally Archiving Personal Lives: Digital Forensics, Ancestral Computing, and Evolutionary Perspectives and Tools.” Presented at iPRES 2008, London, United Kingdom, September 29-30, 2008.

John, Jeremy Leighton, Ian Rowlands, Peter Williams, and Dean Katrina. *Digital Lives: Personal Digital Archives for the 21st Century >> An Initial Synthesis*. British Library, 2010.

Kirschenbaum, Matthew G., and Rachel Donahue."Digital Forensics and Cultural Heritage Glossary." Washington, DC: Council on Library and Information Resources, 2010.

Kirschenbaum, Matthew G., Richard Ovenden, and Gabriela Redwine. *Digital Forensics and Born-Digital Content in Cultural Heritage Collections.* Washington, DC: Council on Library and Information Resources, 2010.

Knight, Gareth. “Digital Forensics in the Archive: Using Open Source & Free Software to Capture and Curate Archival Digital Records.” Presented at DPC: Digital Forensics for Preservation, The Oxford Centre, Oxford, June 28, 2011.

National Library of Australia. "Recovering and Converting Data from Manuscripts Collection Discs." Accessed June 14, 2012. http://www.nla.gov.au/preserve/digipres/recovering.html.

Olson, Michael. Born Digital Program @ Stanford University, "First Draft of our Forensic Workflow." Last modified February 26, 2010. https://lib.stanford.edu/digital-forensics-stanford-university-libraries/first-draft-our-forensic-workflow

Optical Storage Technology Association. "CD-Recordable Glossary." Accessed June 14, 2012. http://www.osta.org/technology/cdr.htm.

PC Guide. "Floppy Disk Drives." Last modified April 17, 2001. http://www.pcguide.com/ref/fdd/index.htm.

Shahani, Chandru J., Basil Manns, and Michele Youket. Library of Congress, "Longevity of CD Media." Accessed June 14, 2012. www.loc.gov/preservation/resources/rt/studyofCDlongevity.pdf.

Stollar, Catherine and Thomas Kiehne. "Guarding the Guards: Archiving the Electronic Records of Hypertext Author Michael Joyce." Presented at News Skills for the Digital Era: Proceedings of a Colloquium, Washington, DC, May 31-June 2, 2006.

Toyoda, Toru. *NDL Research Report No. 6: The Long-term Accessibility of Packaged Digital Publications*. National Diet Library, 2006.

Tyson, Jeff. How Stuff Works, "How Removable Storage Works." Accessed June 15, 2012. http://computer.howstuffworks.com/removable-storage9.htm.

Von Suchodoletz, Dirk. Open Planets Foundation, "Automating Disk Imaging." Last modified May 4, 2012. http://www.openplanetsfoundation.org/blogs/2012-05-04-automating-disk-imaging.

Wikipedia contributors, "Disc Rot," *Wikipedia, The Free Encyclopedia,* http://en.wikipedia.org/wiki/Disc_rot (accessed June 3, 2012).

Wikipedia contributors, "Disk Image," *Wikipedia, The Free Encyclopedia,* http://en.wikipedia.org/wiki/Disk_image (accessed June 19, 2012).

Wikipedia contributors, "Floppy Disk," *Wikipedia, The Free Encyclopedia,* http://en.wikipedia.org/wiki/Floppy_disk (accessed June 4, 2012).

Wikipedia contributors, "Forensic Disk Controller," *Wikipedia, The Free Encyclopedia,* http://en.wikipedia.org/wiki/Forensic_disk_controller (accessed June 18, 2012).

Wikipedia contributors, "USB Flash Drive," http://en.wikipedia.org/wiki/USB_flash_drive (accessed June 15, 2012).

Wikipedia contributors, "Zip Drive," *Wikipedia, The Free Encyclopedia,* http://en.wikipedia.org/wiki/Zip_Drives (accessed June 15, 2012).

Yesterday's Technology ."Floptical Disks." Accessed June 16, 2012. http://www.yesterdaystechnology.com/html/floptical_disks.html.