Analysis of a Photocopier Hard Drive for Forensically Relevant Artifacts

Trevor M. Bobka, B.S., Marshall University Science Forensic Science Center,

1401 Forensic Science Dr. Huntington, WV 25701

Agency Supervisor - Ian Levstein, M.S., Marshall University Forensic Science Center,

1401 Forensic Science Dr., Huntington, WV 25701

Technical Assistant - Nevin Westurn, Superior Office Service Inc.,

108 Eighth Avenue West, Huntington, WV 25701

MU Topic Advisor - Terry Fenger, Ph.D., Marshall University Forensic Science Center,

1401 Forensic Science Dr., Huntington, WV 25701

Abstract:

In the world of digital forensics, many people fail to recognize photocopiers, or multifunction peripherals (MFPs), as having any probative value. These machines actually contain a hard drive to aid in processing or sorting multitasking functions. Thus, the hard drive acts as a storage media and saves the documents sent to it for the various jobs the machine performs. These machines are heavily used in many organizations (businesses, government, universities, etc.), and the devices can potentially be a gold mine if the data falls into the wrong hands. Contrary to popular belief, the hard drives are fairly easy to obtain if the photocopier breaks or gets replaced by a newer model. This is due in part to some offices simply tossing out the old copiers and paying no attention to the hard drive left in the machine; thus, making the hard drive available to anyone who wants to take the time to remove it.

As technology becomes more pervasive in everyday tasks, the threat against it or misuse it increases. The same goes for photocopiers. Organizations are creating more security measures to help prevent the leak of data from used machines. These security measures include putting a firmware ATA password on the hard drive so the contents cannot be viewed unless the password is removed, and having the options to encrypt copier jobs or to automatically delete the job metadata after the job is finished. These steps are needed and help to prevent data leakage on the physical and cyber level.

This project involved removing the hard drive from a Canon® imageRUNNER ADVANCE 4035 photocopier during the four stages of its life cycle and analyzing the content. The four stages consist of: a brand new hard drive, applying the operating system (OS), generating data, and wiping or initializing the machine. The hard drives were cloned twice using a Disk Jockey Pro Forensic Edition to have, both, an actual copy and a working copy to follow

normal evidence handling protocols. The results showed that data generated on the machines was able to be recovered using forensic software programs such as FTK® 5.6.0 and Autopsy® 4.0.0. The files that were obtained corresponded to: time stamps for the various jobs performed, phone numbers for faxes, Email addresses, and other log files. In one case, an exact document matching the original was found as a PDF file. After initializing the photocopier, the data was overwritten by the machine and only the working OS remained. No other pertinent files were recovered from the data.

Introduction:

When it comes to digital forensics, some of the common things that come to mind are computers, cell phones, camcorders, and hard drives. However, the term digital forensics encompasses anything that is able to store digital media. Thus, gaming systems, home appliances, routers, and multi-function peripherals (MFPs) are considered in the discussion of the digital field. An MFP is a device that can perform several functions, such as printing, scanning, copying, and faxing, that would normally require separate devices.[3] Because MFPs can do so many functions in one device, the machine needs a hard drive (HD) to make sense of all the data that is generated while multi-tasking.[8] Like other devices with hard drives, it can contain valuable information about a company or a particular person. According to Marcella, approximately 125,000 to 250,000 pages of text can reside on the hard drive of a photocopier in a corporate setting.[4]

As technology becomes a more dependent part of society, most people would not throw out a hard drive without deleting the content or at least encrypting it. However, most people fail to realize that photocopiers are capable of storing information, and deleting the data may not be enough to ensure it is gone. For example, when a file is deleted from a computer, the hard drive

simply removes the address or pointer to that file; the file still resides on the hard drive until it is overwritten.[7]

This similar thinking can be applied to the organization level, as well, where some files are considered proprietary. When an organization no longer uses an old MFP, the company simply sends them elsewhere to be resold. The resale could move the photocopier across the nation or across the world![1,2] According to an investigation produced by CBS, an old warehouse in New Jersey contained 6,000 used photocopiers waiting to be sold.[2] During the investigation, John Juntunen, the owner of the company, Digital Copier Security, bought four used machines for roughly $300 apiece. After the photocopiers were plugged in, he found that one machine was from an insurance company in New York, one was from a construction company in New York, and two machines were from the Buffalo Police Department, Sex Crimes Unit and Narcotics Unit, respectively.[2] Juntunen was able to recover documents pertaining to individual health records, pay stubs with social security numbers, $40,000 in copied checks, domestic violence complaints, wanted sex offenders lists, and materials from drug raids. The worst part was that Juntunen was able to remove the hard drives and download the files in a day's work.[2]

The CBS investigation wasn't the only time photocopiers were detailed. In 2014, John McCash, a forensic examiner, tried his hand at recovering information from the devices. His results were published as a blog on the SANS website.[5] He had extracted the hard drive from a Canon® ImageRUNNER ADVANCE C5240 photocopier. However, McCash hit a wall on his first attempt because the hard drive contained an ATA firmware password. To overcome the firmware password, McCash sent the drive to a data recovery firm where they had access to a password removal tool. After getting the password removed from the hard drive, McCash was able to recover a number of JPG and PDF files from unallocated space on one partition.[5] The

files appeared to be from various scan jobs that had occurred on the copier. He was also able to obtain log files that contained information on what jobs were performed, the time stamp for those jobs, and information on where the job was going such as a phone number or email address.[5]

Other studies that concerned recovering information from photocopiers included experiments from Lee and Rackley.[3,6] Lee was able to recover files from the secure print function using EnCase® 6.15.0, a forensic software program from Guidance Software. The file was said to have the file code, "H2P00002;" however, the exact machine that the code referred to was not mentioned.[3] From a photocopier hard drive, Rackley was able to recover Email addresses belonging to people in a U.S. Government office. The Emails were then traced back to the individuals to obtain some public information, such as office position, salary, and office address.[6]

Photocopiers are different from regular printers in that they contain a hard drive, but how is the printing system different? Generally, a copier will have two main circuits for handling data storage. For example, the copy/print/scan data will have a different circuit bored than the fax interface.[4] This allows the photocopier to multi-task to make it useful in corporate settings. According to Marcella,[4] photocopiers have the circuit board isolation as illustrated below.

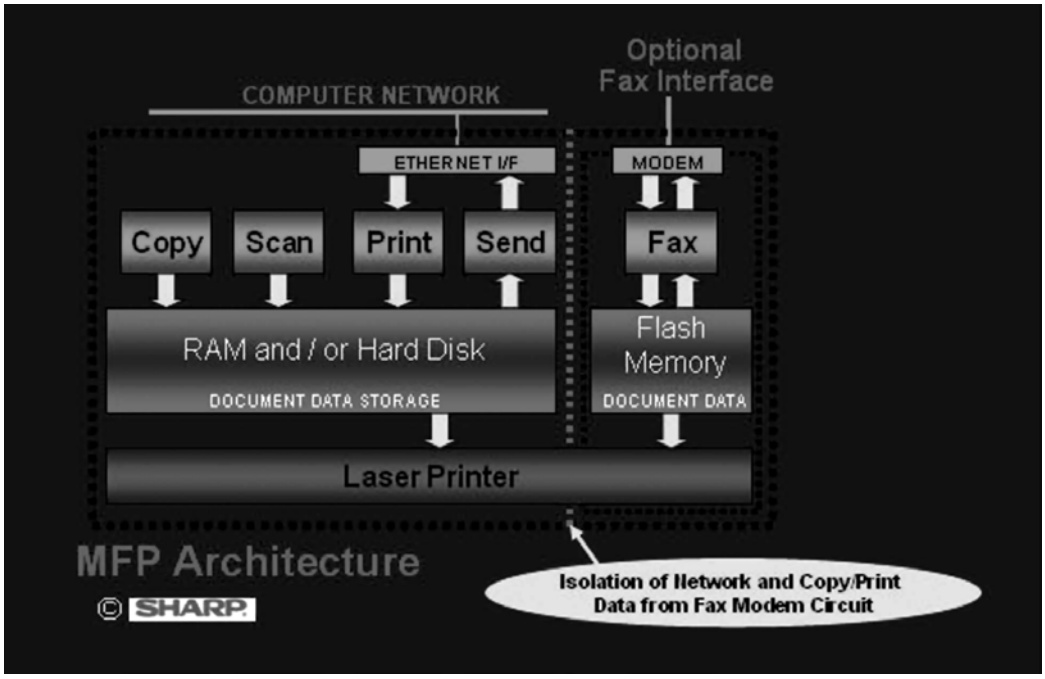

Figure 1: Division of the circuit board in a Sharp MFP.[4]

Therefore, some information is present on the hard drive, in RAM, or some other form of flash memory. For instance, some copiers could have a buffer system that simply overwrites data each time a file is copied;[1,6] thus, making it impossible to recover. The file types that are generally of interest are JPGs, PDFs, Plain Text Files, PCL files, and Postscript files.[3,4,5,6]

With the threat of gaining access to pertinent information, manufacturing companies are taking action to make clients feel secure. For instance, most manufactures are implementing encryption routines on their hard drives. Thus, even when the hard drive is removed there is a firmware password on the disk to prevent access.[1,5] This password is not fully secure because there are software programs that can bypass the feature such as Atola Insight®.[5] Another security measure includes the photocopier having an option to overwrite the data immediately after the job completes.[1] This feature might cost extra for a company, but it is worth it depending on the information an organization is putting through the machine. A third option is that some resale

companies partner with smaller organizations and will initialize or fully delete the data on the hard drive before it is placed into another machine for resale.[1]

Hypothesis:

Based on previous studies, it is hypothesized that forensic data can be obtained from the hard drives in photocopiers. The goals of the experiment are to determine if a photocopier hard drive contains any relevant forensic data during the stages of its life cycle, and to determine how accurate the wiping process is before the machines are resold. The purpose of the research is to make organizations aware that their valuable data can exist on the MFP's hard drive, and that it must be securely deleted prior to removal of the machine.

Materials and Methods:

Materials:

- MHDD™ with Fast Disk Eraser v4.4
- Western Digital® Data LifeGuard™ Diagnostics
- Canon® imageRUNNER ADVANCE 4035 photocopier
- Toshiba 160 GB hard drive (SATA)
- USB flash drive with photocopier OS install
- 8 Seagate 500 GB hard drives (IDE)
- Disk Jockey Pro Forensics Edition
- Dell Optiplex 960 desktop computer
- StarTech.com USB/SATA/IDE adapter
- FTK® 5.6.0 (Forensic ToolKit)®
- Access Data FTK Imager® 3.4.0.1
- Autopsy® 4.0.0

Scope:

The photocopier hard drive was forensically imaged during four stages: empty or zeros on the drive, after adding the OS, after generating data, and after initializing or deleting the generated data. Two forensic images were created during each stage. The first image served as the actual copy of the photocopier hard drive, and the second as the working copy. This was done to ensure the project followed the guidelines set forth via the common protocols of digital forensics. The goal was to observe whether or not any relevant forensic data could be pulled from the hard drives through the various stages. The data of interest consisted of image files such as JPEGs and PNGs, and Adobe® PDF documents.

Obtaining the Zero Hard Drive:

The copier resale company associated with this project didn't readily have a brand new photocopier hard drive available. Therefore, in order to illustrate a completely new drive, the hard drive needed to be wiped. Wiping, or writing zeros to the 160 GB Toshiba hard drive, was done via the Fast Disk Eraser v4.4 software that was a part of the MHDD™ project shown in Figure 2. The process involved writing zeros to each sector of the hard drive and took 45 minutes to complete.

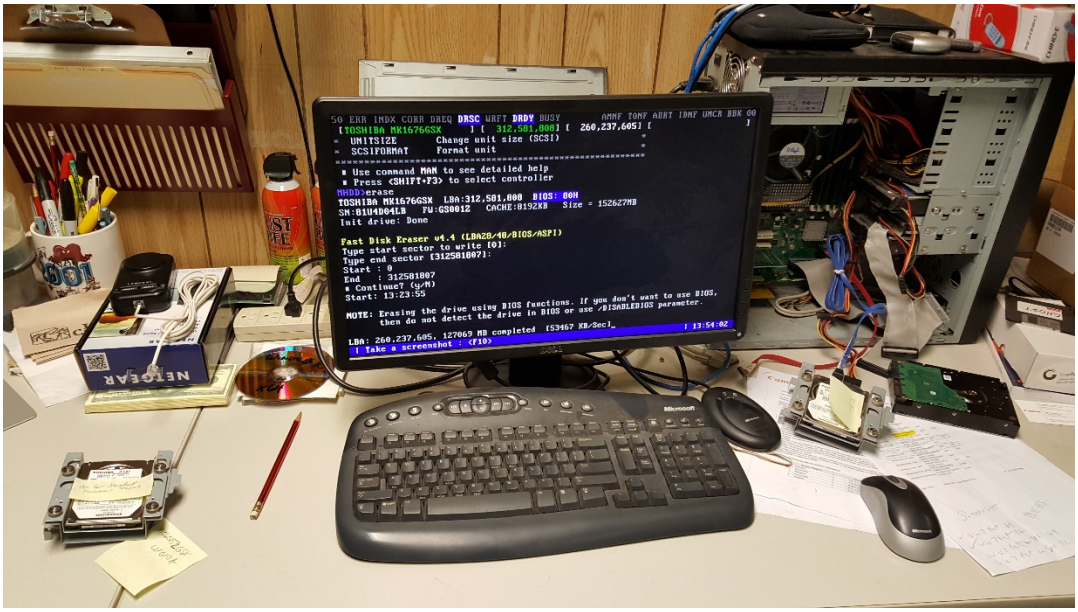

Figure 2: Still of Fast Disk Eraser v4.4.

The Disk Jockey Pro was used to obtain a forensic image or clone of the wiped hard drive. The device allowed the transition of data between a SATA (Serial ATA) connected drive and an IDE connected drive while employing a write-blocker. A write-blocker prevents any information from being written to the digital media; thus, aiding in the integrity of the evidence. To produce the clone, the photocopier hard drive was connected to the source input on the Disk Jockey Pro using SATA cables. It was important to connect the original media to the source input because it was write-blocked. The destination hard drive was connected to the destination output, right side, using IDE cables, as shown in Figure 3. It took 22 minutes to copy the information bit by bit to the destination drive. Once the first clone was made, a second clone was produced to act as the working copy.

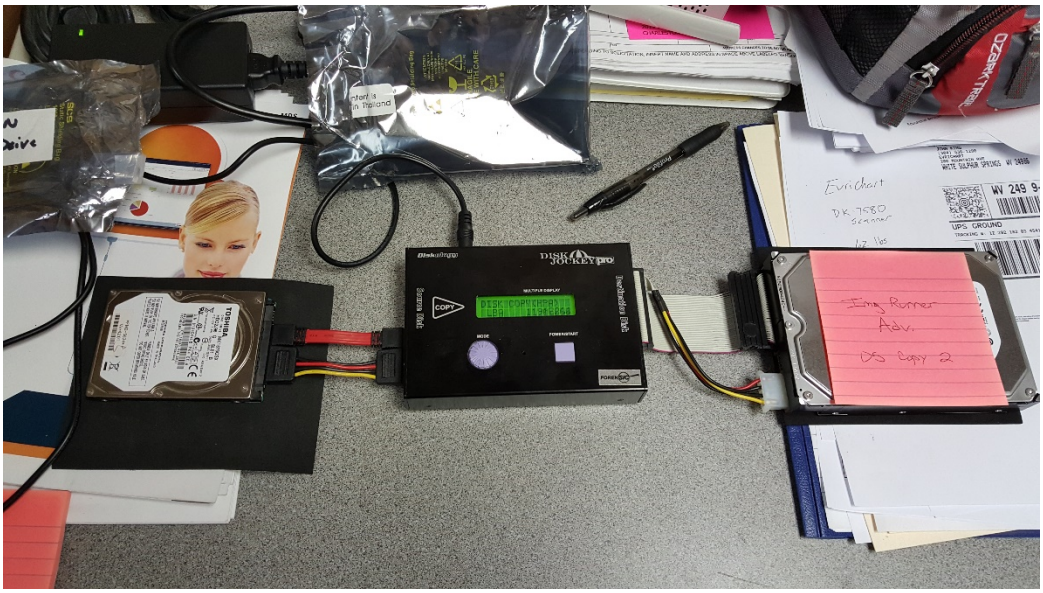

Figure 3: Disk Jockey Pro set up for copying hard drives. Data is transferred left to right.

Applying the OS on the Photocopier:

The OS was downloaded to a USB flash drive from the Canon® website, and the flash drive was inserted into the photocopier. (see Figure 4) The machine was powered on, and the 2 and 8 buttons were held down simultaneously to allow the photocopier to boot into the machine's download-shell. In the shell, a white display box appeared and informed the user that the machine was updating software, as seen in Figure 5.

Figure 4: Inserted USB flash drive with the loaded OS.

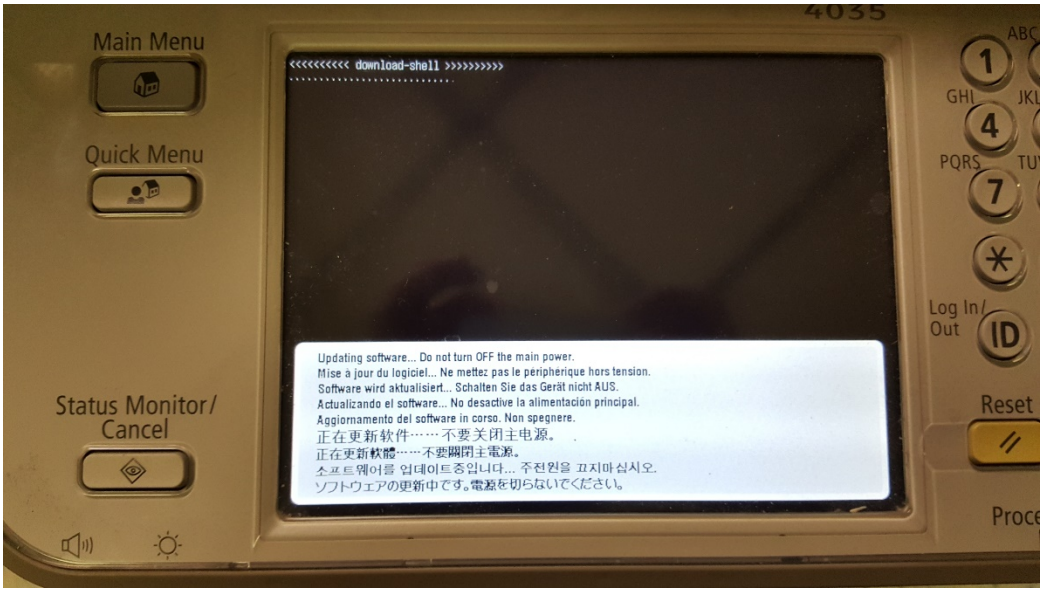

Figure 5: Image of the download-shell during the OS installation.

The screen then displayed the status of the various checks and upgrades that were being performed during this process. The process took 10 minutes to complete. After the OS was installed, the hard drive was removed from the copier, and two forensic clones were made using the same set up shown in Figure 3. Images of the completion process and the resulting opening screen are illustrated in Figures 6 and 7, respectively.

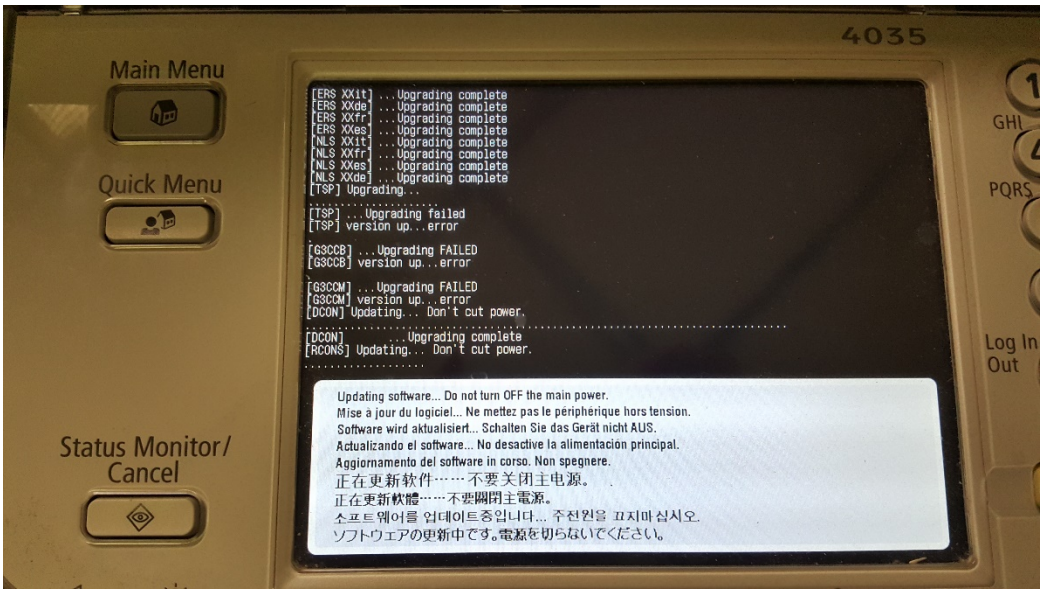

Figure 6: Final process of downloading the OS.

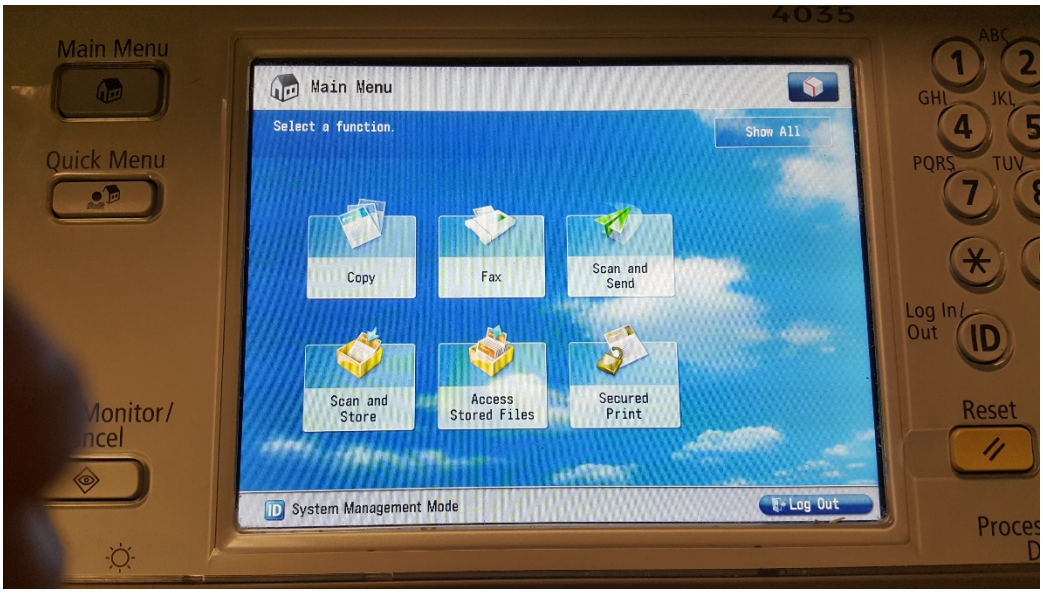

Figure 7: Still of the installed OS.

Generating/Populating Data:

The Canon® ImageRUNNER ADVANCE 4035 photocopier was tested for 9 functions: copying, printing, scanning to email, scanning to file, scanning to mail box, printing to mail box, sending a fax, receiving a fax, and secure printing. To use the email and mail box functions, the photocopier was connected to the Internet using an Ethernet cable. Also, the fax functions needed a phone line attached; so, a phone cable was connected to the machine. The documents used to generate the data were produced in the file, MU Forensic Test File.doc, which can be found in Appendix A. The file consisted of 10 pages that corresponded to the function being performed, i.e. the page being copied contained the word "COPY1." As mentioned, only 9 functions were tested. The secure printing function enables a user to print and release the document or print and store it on the photocopier until released. Once all the data was generated, the photocopier hard drive was removed, and two forensic clones were created.

Initializing the Photocopier:

Canon® photocopiers have a built in function that enables resale companies to delete all stored files on the machine and initialize it back to its default mode. This is done via the path: System/Registration\System Management Mode\Data Management\Initialize All Data/Settings. A white pop up screen appeared and prompted the user for a specified deletion method. There were five options: once with null (0) data, once with random data, 3 times with random data, 7 times with random data (the DoD (Department of Defense) standard), and 9 times with random data. For this project, the once with null (0) data option was selected. A message prompt asked if the user was sure they wanted to perform the action, and after clicking OK a display box appeared estimating the duration. The process took 15 minutes to complete, and the machine restarted itself after completion. After the machine restarted, it appeared the same as when

powdered on with just OS installed; it was ready to use. The hard drive was removed from the photocopier, and two forensic clones were created. Images for the described process can be found in Figures 8 through 11.

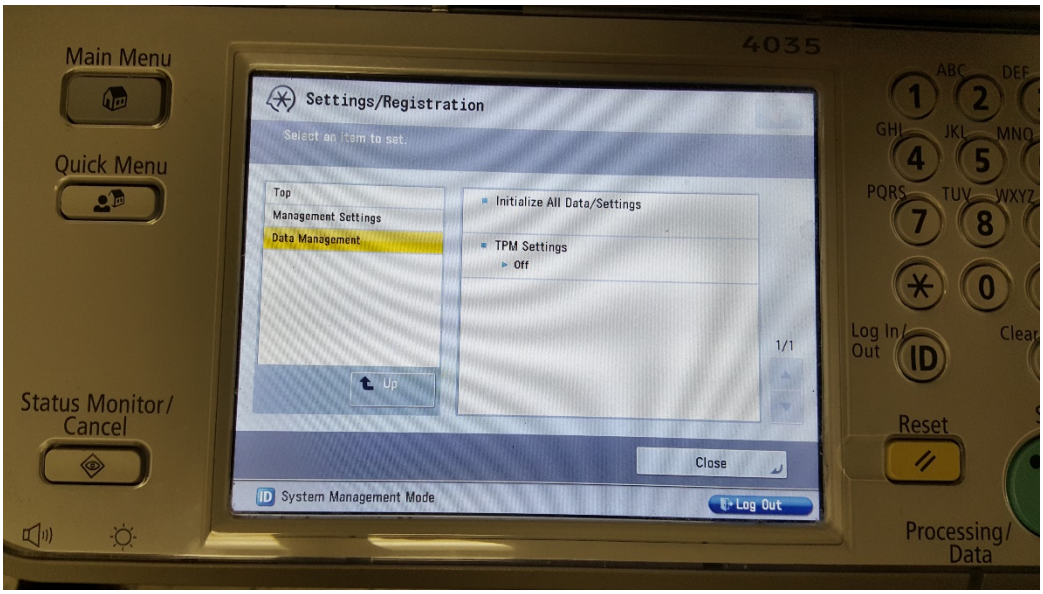

Figure 8: Main screen/path to utilize the initialize function.

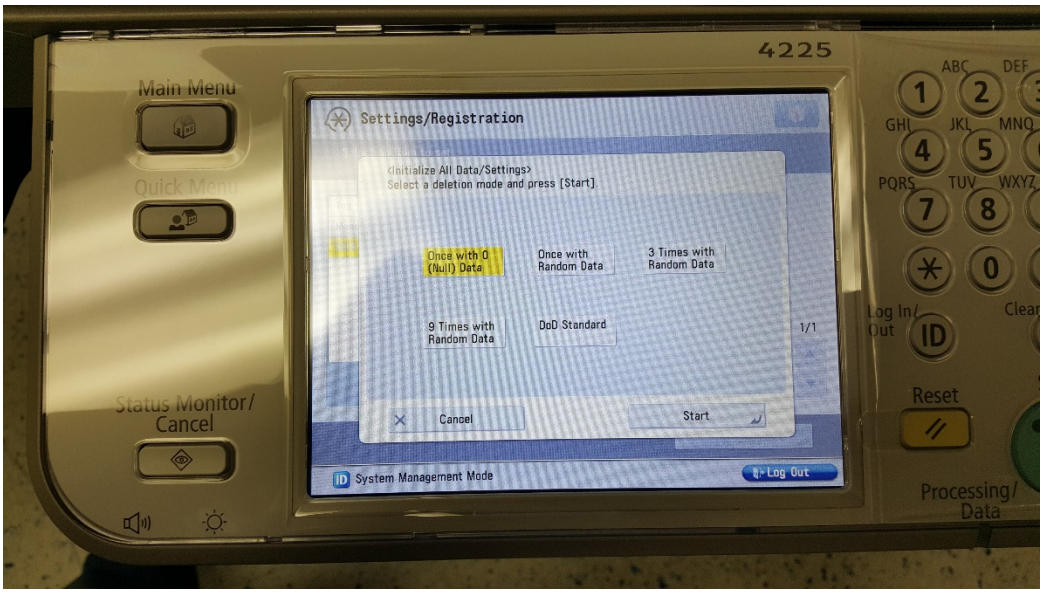

Figure 9: The five options for how the deletion process will occur.

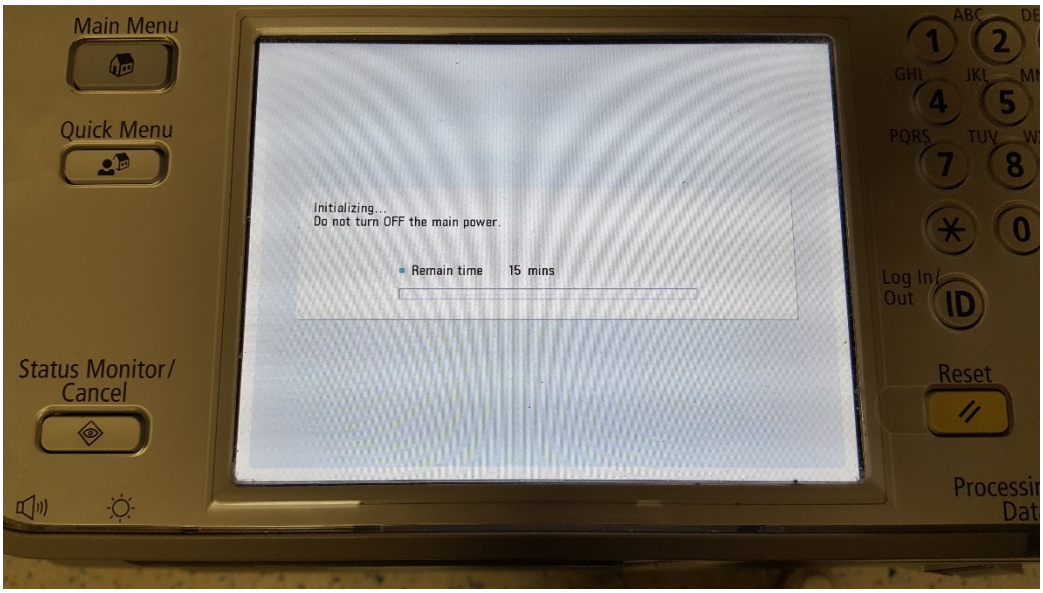

Figure 10: Progress bar with the displayed estimated time remaining.

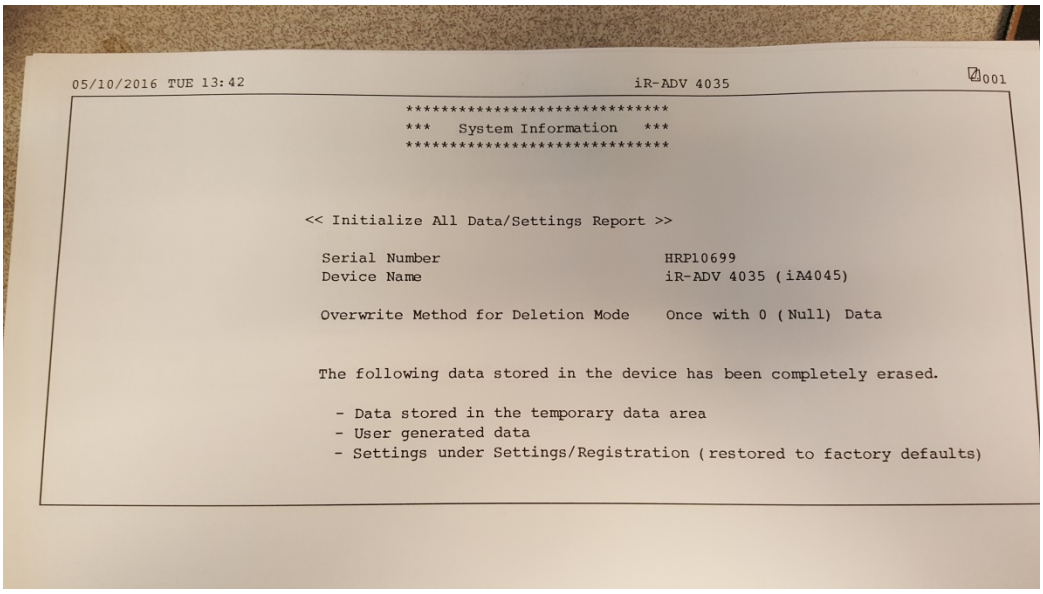

Figure 11: Confirmation report printed after machine initialized.

Producing the Workable Images:

The hard drives were connected one at a time to the computer via the StarTech.com Switching Adapter. The adapter was connected to the IDE pins on the hard drive, and the USB cable was inserted into the computer. (see Figure 12) Once connected, Access Data FTK Imager® 3.4.0.1 was opened and used to make a forensic image of the hard drive. The images

were created as .E01 files (EnCase® Image files) with a 1500 MB size limit and a compression rate of 6 (1 being the fastest compression and 9 being the slowest). The size and compression rates were the default options and appropriate for this research.

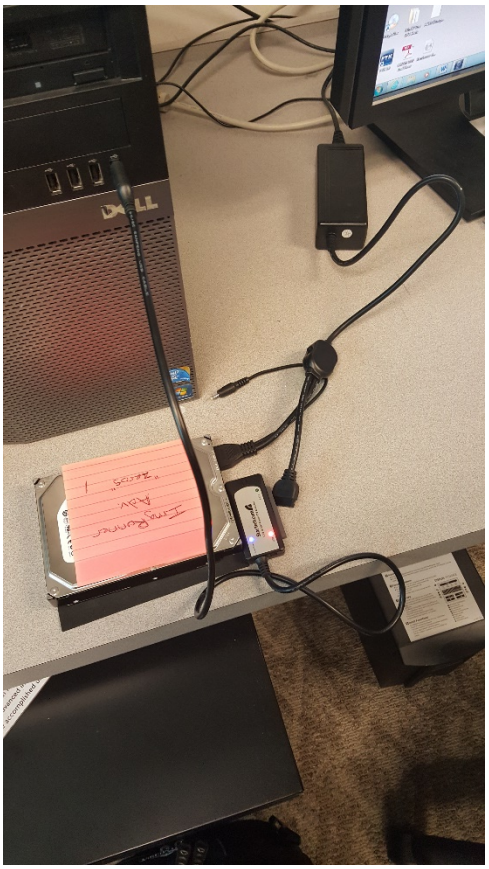

Figure 12: Set up for connecting the hard drives to the computer to produce forensic images.

After the images were created, FTK Imager® verified the images and produced MD5 and SHA1 hash values. Hash values are a string of numbers and characters that uniquely identify a large amount of digital information.[10] These values are created using mathematical algorithms such as MD5 and SHA1. The hash values were examined to ensure that both hard drives contained the same contents. The hash values for the similar hard drive should be identical. If the hash values differed, the hard drives were re-imaged and verified again. The .E01 files were stored in the folder Internship HD Images in the Internship folder on the Desktop. Six hard

drives produced two image files, an .E01 and an .E02, while the hard drives containing all zeros only produced one .E01 file. The time to create the images averaged 4 hours and 7 minutes with an additional 45 minutes to verify it.

Analyzing the Hard Drive Images:

FTK® 5.6.13 was used and four cases were created, one for each photocopier stage. Both images were added to the same case file because they contained the same content, based on the matching hash values. In FTK®, the image files were examined for JPEGs, PNGs, and PDFs. Some manual data carving, cutting out hidden information, had to be performed to obtain the desired files from the unallocated space on the hard drive. Also, spooling (.SPL) and shadow files (.SHD) were carved out of the image to see if any more information could be obtained.

Autopsy® 4.0.0 was used in a similar manner to FTK® 5.6.13. In Autopsy®, the image files were added to a case folder containing a proper name, such as PhotocopierDataHD02. The image file was then examined. Autopsy® automatically carved out PDFs, JPEGs, PNGs, Plain Text files, and Email addresses.

Results:

Partitions:

The photocopier hard drive appeared to have 15 partitions when observed in FTK®. The partitions were labeled “dev\sdb#” with the numbers ranging from 1-15. (see Figure 13) However, partitions 4 and 6 were not present. In Autopsy®, the partitions were displayed differently. The software had broken the hard drive into 27 volumes with the numbers ranging from 1 to 49. (see Figure 14) This time, several numbers were missing and out of order.

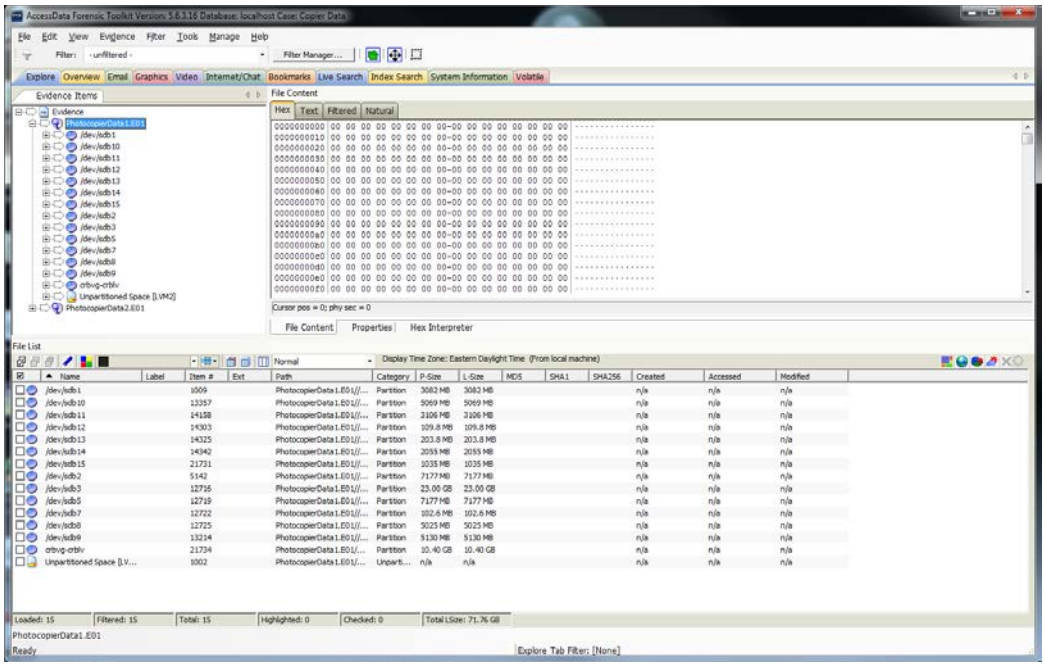

Figure 13: Partitions found and ordered while analyzing in FTK®.

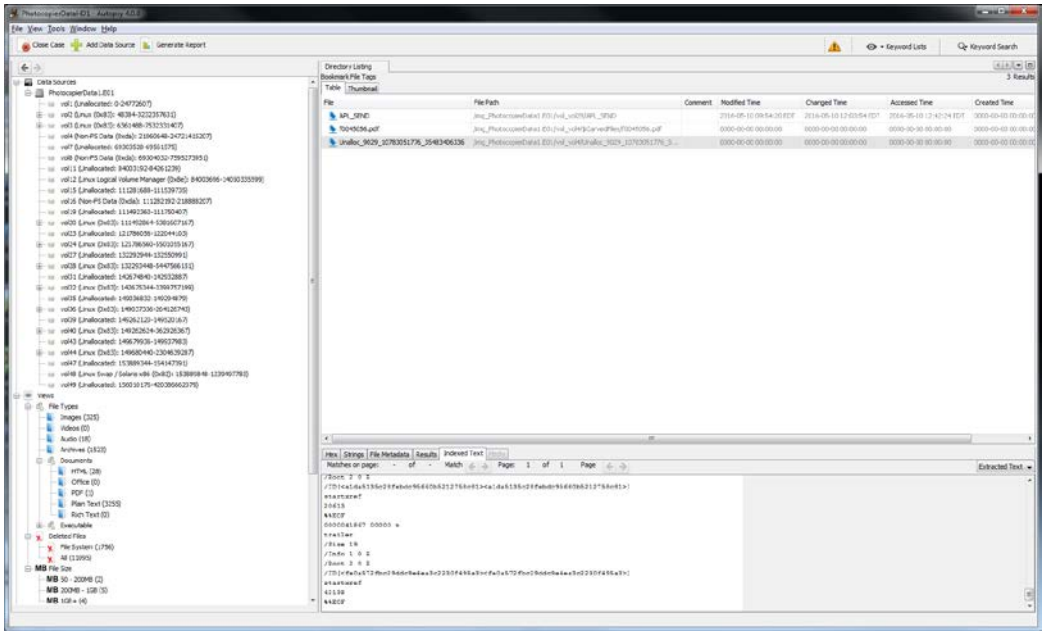

Figure 14: Partitions found and ordered while analyzing in Autopsy®.

The hard drives were cloned from a 160 GB Toshiba hard drive; thus, it was expected that the image size would be 160 GB. However, the image files were read as 71.76 GB with 391.6 GB of unallocated space. This is due to cloning the 160 GB hard drive to a 500 GB hard

drive and imaging the 500 GB hard drive. For instance, there was only 71.76 GB of data present on both hard drives. However, when the larger disk was imaged, it contained more unallocated space which is why the amount of unallocated space is twice as large as the original hard drive size.

Zero Hard Drive:

The hard drive that contained zeros produced the expected results. There were 3 partitions on the drive that were labeled: Unrecognizable file system. Nothing was found in FTK® or Autopsy® because the hard drive was, indeed, all zeros. (see Figure 15)

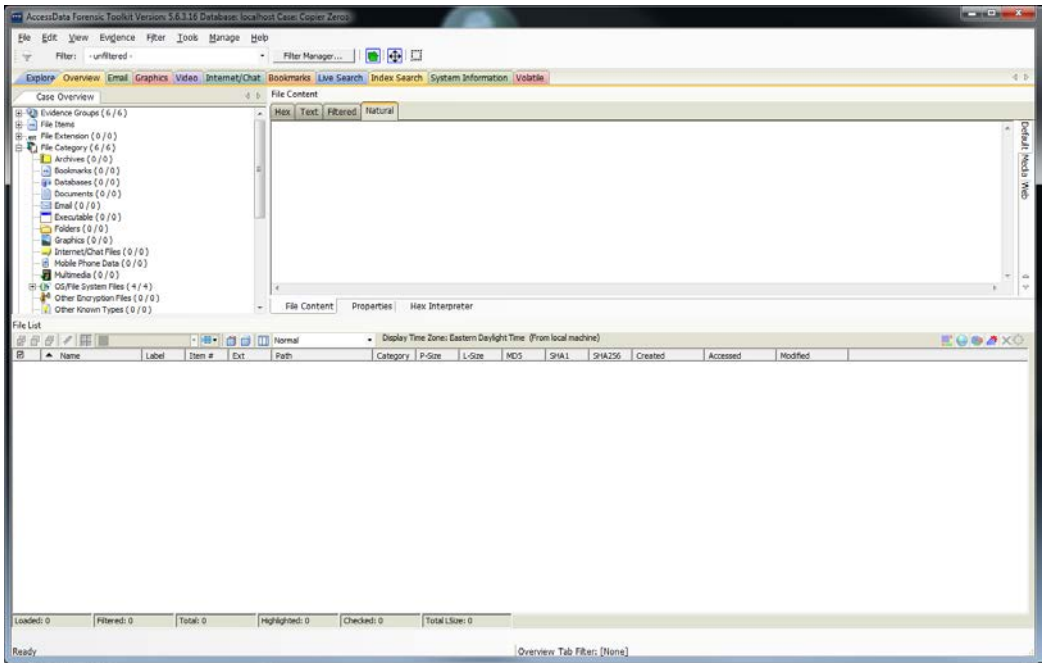

Figure 15: Results after carving the zero hard drive for files in FTK®.

OS Hard Drive:

The OS hard drive exhibited the partition labeling described previously, and information about the operating system was found on the machine. It was a Unix OS with a form of bootable Java. A Linux debugger, i686 Montavista Linux GNU, and information about the processor (2.6.18 pro500 x86 Pentium 3) were found. Also, there were several PNG image files and Plain

Text files found. However, the images consisted of the navigation icons for the various functions, and other style images such as: borders, backgrounds, loading screens, etc. (see Figure 16)

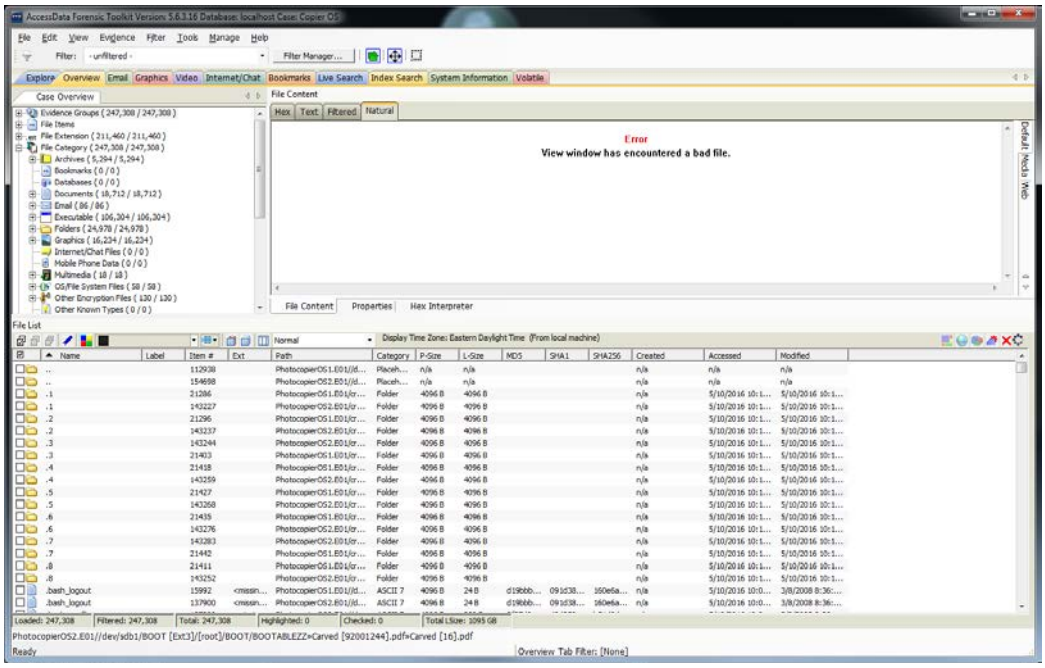

Figure 16: Results after carving the OS hard drive for files in FTK®.

Data Hard Drive:

In FTK®, various PNG and JPEG image files were found along with a few PDF files. One PDF file matched the exact document that was used for the scan to file function. (see Figure 17) Information about all of the functions performed on the machine was present. For instance: date and time stamps for the scans, the phone number associated with faxing, and print records illustrating that the job printed successfully. The email address that performed the scan to Email function was recovered as well, displaying that there was an attached image with it. (see Figure 18)

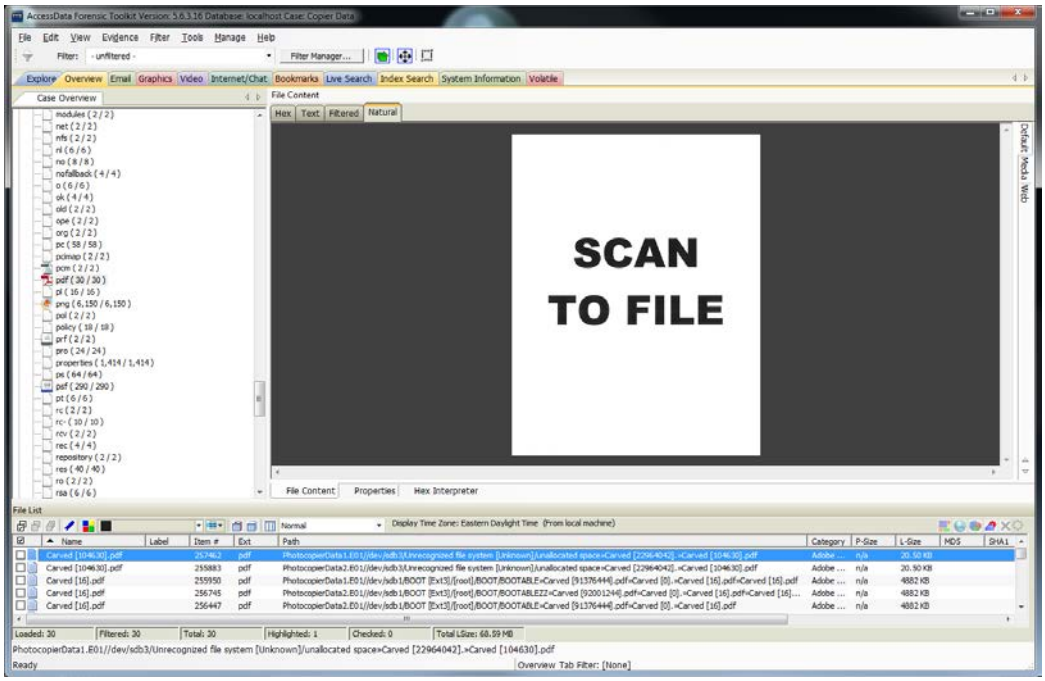

Figure 17: PDF of an actual document recovered during analysis.

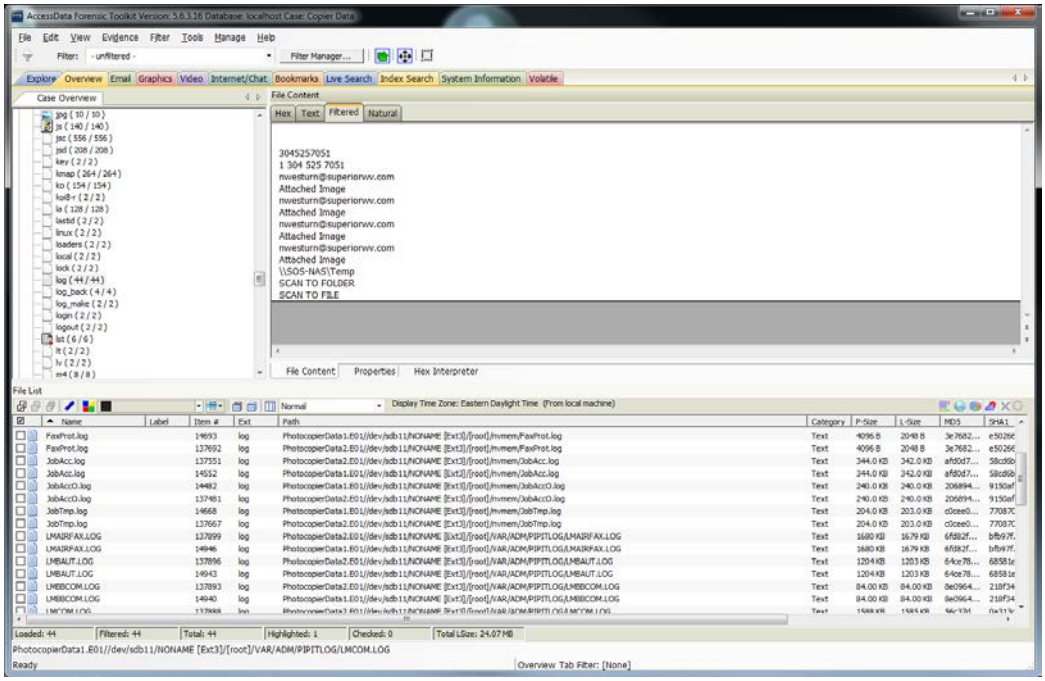

Figure 18: File describing a few scan functions performed on the photocopier with Emails.

Autopsy® found the same files that FTK® found. For example, the same PDF file was recovered, and the time stamps, phone number, and JPEGs and PNGs were all observed.

However, Autopsy® recovered several more Email addresses than the one that had only performed the scan functions. There were several .edu, .com, and .org email addresses listed, which were determined to be Email addresses for individuals or organizations involved with supplying source code to the machine and OS. (see Figure 19)

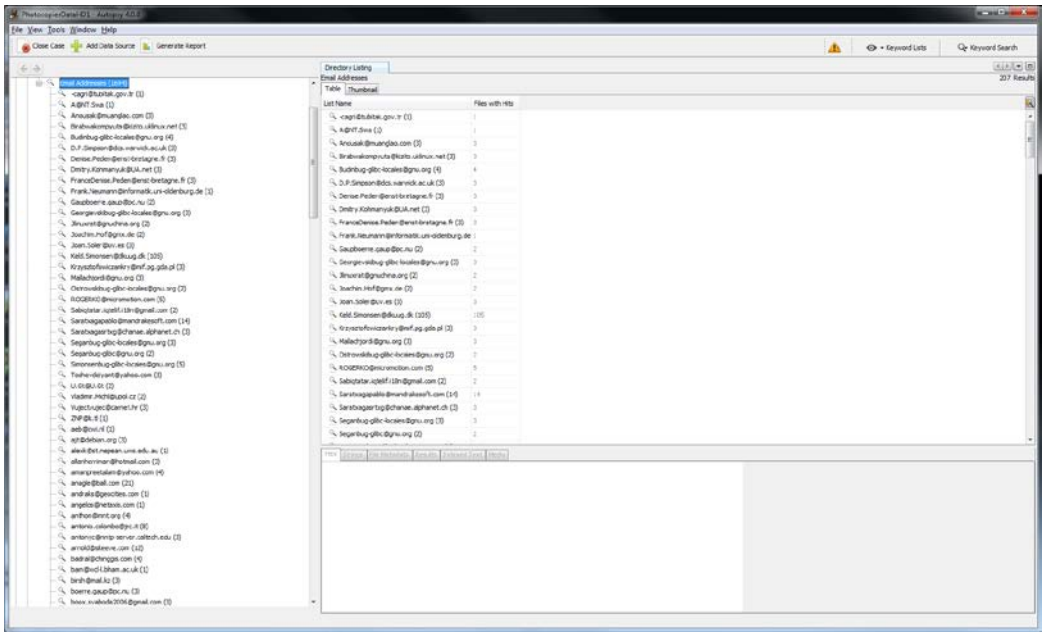

Figure 19: Email addresses recovered using Autopsy®.

Initialized Hard Drive:

The initialized hard drives appeared to contain the same data as the OS only hard drives. For instance, the drives contained images of the navigation icons for the operating software and Plain Text files that appeared to be source code for the machine. (see Figure 20)

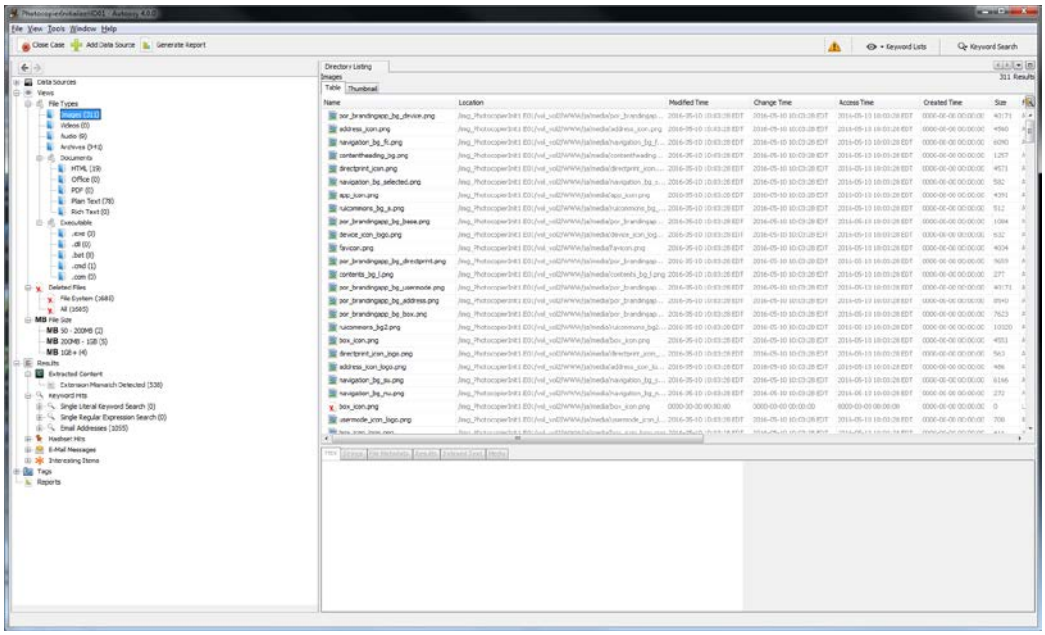

Figure 20: List of images found analyzing the Initialize hard drive.

A general breakdown of the number of files observed in both FTK® and Autopsy® is outlined in Table 1.

Table 1: Number of recovered files and file types during data analysis.

Forensic Software	File Type	Zero HD	OS HD	Data HD	Initialize HD
FTK® 5.6.13	Log	0	44	44	44
	Graphics	0	8117	10749	8285
	PDF	0	54	30	54
Autopsy® 4.0.0	Images	0	325	325	311
	Archives	0	1523	1523	941
	PDF	0	0	1	0
	Plain Text	0	3248	3255	78
	Deleted Items	0	10913	11095	1685
	Email	0	1686	1694	1055

Discussion:

Several relevant items were found while analyzing the photocopier hard drive through the various stages. For example, all of the metadata for most of the performed functions was recovered. This was expected because previous studies have shown that the hard drives serve as an actual storage media in the machines.[2,3,4,5] One issue with the results was what wasn't recovered. For instance, the secure print function was used, and the password to release the document was never inserted. Thus, the document was presumed to be on the hard drive, but it was unable to be recovered as a JPG, PDF, or any other file format listed as a file extension. However, an audit log was found containing metadata that implied that the file exists. For instance, the file contained the password used to hold the document (7654321) and the words, Attached Image. (see Figure 21)

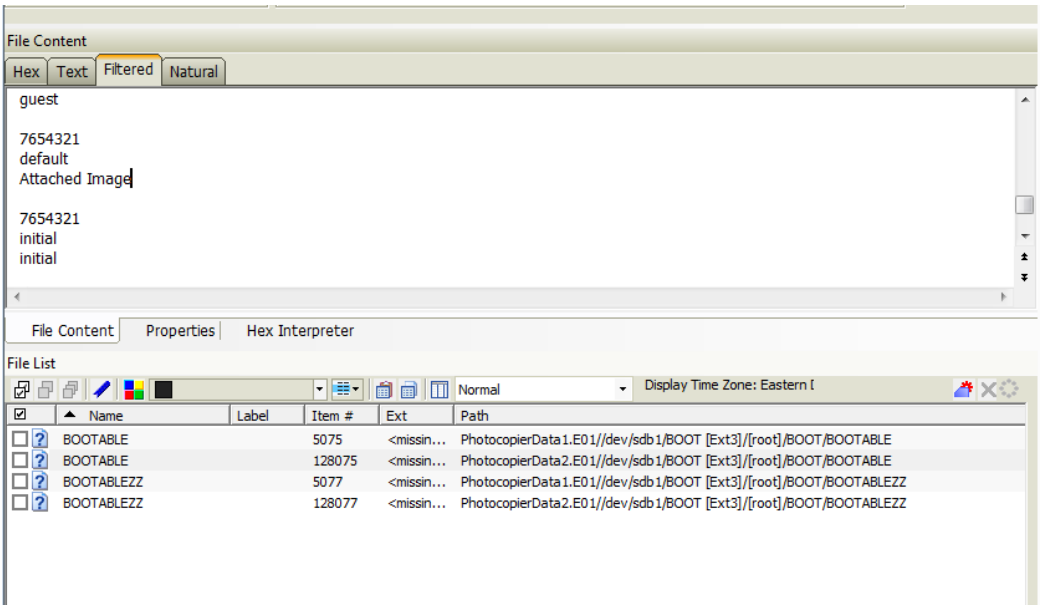

Figure 21: Potential metadata from the secure print function.

The total amount of data recovered was likely due to there not being enough data populated on the original hard drive. To overcome this issue, a hard drive from a current working photocopier was removed and imaged. However, the hard drive exhibited a firmware password

as part of the new security features with newer models. Thus, the hard drive could not be imaged without the password removed, and there was no mechanism or software available to remove the password.

Limitations:

There were several issues that occurred during the project. The first was trying to install the OS on the photocopier hard drive. The process took several attempts and three different photocopiers before it was successfully added to the machine. According to Western Digital's Data LifeGuard Diagnostics software, the hard drive reported as being wiped; however, the photocopier could not detect that the drive was attached. Thus, trying to hold down the 2 and 8 buttons resulted in the error code illustrated in Figure 22.

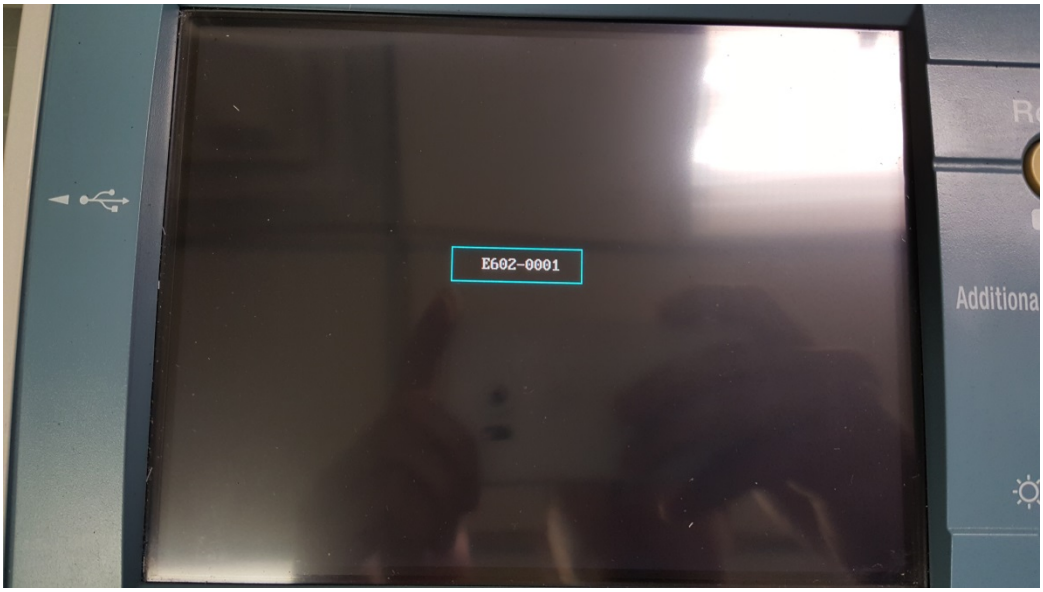

Figure 22: Error code observed due to the machine not recognizing the USB flash drive.

Another issue occurred when trying to produce the forensic image in FTK Imager®. Both hard drives were created via the Disk Jockey Pro using the option for a bit-by-bit copy. However, only the two Zero hard drives initially contained the same hash values. The other six hard drives

had to be recopied and reimaged/rehashed before they reported as being identical. This process was time consuming because the hard drives each took 5 hours to completely image and verify.

A third issue observed was when trying to view potentially pertinent files. Files were exported from the software program, FTK® or Autopsy®, to the Desktop and opened with Adobe Reader®, Adobe Illustrator®, Microsoft Word®, Notepad®, Paint®, etc. However, most file extensions, such as .CP, .PS, and .PSF, could not be opened. Even changing the file extension through the command line or trying to view the files in programs downloaded from the Internet (Ghostscript™ 9.19, File Viewer Plus, and PDFOnline converter) could not open the files. When opening the files was attempted, the program displayed an error message saying, "The file you are trying to view is corrupt or doesn't exist," or "There is no image to view." Thus, it is unknown if any of those files contained relevant information for the project.

Conclusion:

As hypothesized, forensically relevant data was recovered from a photocopier hard drive. The recovered data took the form of JPGs, PDFs, and Log files. Those files consisted of time stamps and information as to what jobs were performed. Email addresses and telephone numbers were found, and a direct copy of a scanned document was recovered.

When the wiping process was performed, the photocopier was initialized to a bare bone machine with nothing but the OS applied to it. No previous files, such as JPGs, PDFs, and Log files were able to be carved from the hard drive image. This suggests that companies are taking steps to make their machines more secure from privacy breeches.

Future Work:

Future work should be adjusted to incorporate more data for the data generation portion and include images to scan in or print rather than just text files. Also, photocopiers with firmware

passwords should be tested. However, the machine would need to be fully populated with filler data to ensure that important information is not lost during the acquisition process.

Acknowledgements:

- Reviewers:
    - Ian Levstein, M.S.
    - Nevin Westurn
    - Terry Fenger, Ph.D.
- Superior, Inc.:
    - Barry Ballard
    - Jim Childers
    - Sam Webb
- Marshall University Forensic Science Center:
    - Celia Whelan
    - Adam Cervellone
    - Cpl. Robert Boggs
    - Wes Gibson
    - Tiffany Hussell

References:

[1] http://www.copierguide.com/help-advice/hard-drive-security/

[2] http://www.cbsnews.com/news/digital-photocopiers-loaded-with-secrets/

[3] Lee K, Lee C, Park N, Kim S, Won D. An analysis of multi-function peripheral with a digital forensics perspective. First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering 2011 doi:10.1109/cnsi.2011.24

[4] Marcella A. Digital multifunctional devices: forensic value and corporate exposure. Edpacs 2010 41(1), 1-11.

[5] https://digital-forensics.sans.org/blog/2014/09/03/copier-forensics-in-2014-the-good-the-bad-and-the-ugly

[6] Rackley CC, Griffin SE. Multifunction device security awareness. Proceedings of the 5th Annual Conference on Information Security Curriculum Development - InfoSecCD 2008.

[7] Serapiglia A. Data storage forensics–what is really left after I hit the delete button, and how can I actually make sure it's gone? Information Systems Education Journal 2014 12(5), 23-36.

[8] http://bucks.blogs.nytimes.com/2010/06/01/why-photocopiers-have-hard-drives/?_r=1

[9] https://msdn.microsoft.com/en-us/library/f9ax34y5(v=vs.110).aspx

Appendix A:

Word Document Used to Generate Data:

COPY1

SCAN TO EMAIL

SCAN TO FILE

PRINT TO MAILBOX

COPY TO MAILBOX

FAX

SEND

FAX

RECIEVE

PRINT

SECURE

PRINT

HOLD

SECURE PRINT RELEASE