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:

<u>Materials</u>:

- MHDDTM with Fast Disk Eraser v4.4
- Western Digital® Data
 LifeGuardTM 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

<u>Scope</u>:

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 MHDDTM 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.

		4225	ABC DEF
	Settings/Registration		GHI JKL MNQ
Quick Menu	cinitialize All Data/Settings> Select a deletion mode and press [Start]		PQRS TUV WXYZ
	Once with 0 (Null) Deta Date With Rendom Date Sandom Date		
	9 Times with Random Data DoD Standard	1/1	Out D
Status Monitor/ Cancel	× Cancel Start		Reset
	D System Management Made	trag Out	Processing/ Data
47 X.	and the second second	14 N. 64	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

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



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

***************	11 ADV 4033	
*** System Info *******************	mation ***	
<< Initialize All Data/Settin	ngs Report >>	
Serial Number	HRP10699	
Device Name	iR-ADV 4035 (iA4045)	
Overwrite Method for Delet:	ion Mode Once with 0 (Null) Data	
The following data stored :	in the device has been completely erase	d.
- Data stored in the tem	porary data area	
- User generated data		
- Settings under Setting	s/Registration (restored to factory def	aults

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:

<u>Partitions</u>:

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.

	rensk Topikit Ve	rsion: 5.6.3.16 Database: lo	calhost Cese: Copier Data									
Ele Edit Vie	w Evidence	Filter Tools Manage	Пер									
T Filter:	· unfiltered ·		Filter Hanager									
Explore Over	wew Email Gr	aphics Video Internet/C	hat Bookmarks Live Search	Index Search Sys	em Informati	on Volatile						4.1
Evidence It	ems		b File Content									
D Evidenci			Hex Text Fitered	Natural								
000 m	tocopierOwth1.E01		0000000000 00 00 0	0 00 00 00 00 00	-00 00 00	00 00 00 00 00						1
B-C-O-1	/dev/sdb1		000000010 00 00 0	0 00 00 00 00 00	-00 00 00	00 00 00 00 00						1
BCO.	/dev/sdb10		000000020 00 00 0	0 00 00 00 00 00	-00 00 00 1	00 00 00 00 00						
BCO	/dev/sdb11		000000030 00 00 0	0 00 00 00 00 00	-00 00 00	00 00 00 00 00						
B-C-C-	/dev/sdb12		000000040 00 00 0		-00 00 00	00 00 00 00 00 -						
	/Dev/9001.3		0000000000 00 00 00		-00 00 00 1	00 00 00 00 00						
600	/dev.lade t C		0000000070 00 00 0	0 00 00 00 00 00	-00 00 00	00 00 00 00 00 00						
ADA.	(dev/ads2		0000000000 00 00 0	0 00 00 00 00 00	-00 00 00	00 00 00 00 00						
-	/dev/adb3		0000000000 00 00 0	0 00 00 00 00 00	-00 00 00	00 00 00 00 00						
BOO.	/dev/sdb5		00 00 040000000	0 00 00 00 00 00	-00 00 00	00 00 00 00 00						
100 B	/dev/sdb7		000000000000000000000000000000000000000	0 00 00 00 00 00	-00 00 00	00 00 00 00 00 -						
\$C0.	/dev/sdb8				-00 00 00 1							
8-CO/	/dev/edb9		000000000000000000000000000000000000000		-00 00 00 00	00 00 00 00 00 00						
#CQ4	arbvg-arblv		C0000000f0 00 00 0	0 00 00 00 00 00	-00 00 00	00 00 00 00 00						
0 C 2 C	Unpartitioned Space	e [LVM2]										
H-C-Y Phot	tocopierData2.E01		Cursor pos = 0; phy sec =	0								
			File Content Pro	perties Hex Inte	preter							
e List			File Content Pro	perties Hex Inte	preter							
list		· · · · · · ·	File Content Pro	perties Hex Inte	preter Eastern Daylg	ht Time (From local ma	achine)			La se s		E 0 0 4 X0
List		Label Item Ext	File Content Pro	Display Time Zone Category P-Size	Eastern Daylig	ht Time (Prom local ma MDS SHA1	achine) SHA256	Created	Accessed	Nodified	1	E @ @ # XQ
List A A Ame A Name A Very(rdb1		Label Iten # Ext	File Content Pro	Display Time Zone Category P-Size Partion 3082 N	Eastern Daylig	ht Time (Prom local ma MD5 SHA1	achine) SHA256	Created	Accessed	Nodified	Į	E @ 0 4 X0
List A A Anne A Iane A	•		File Content Pro	Perties Hex Inte Display Time Zone Category P-Size Partition 3082 N Pertition 3082 N	Eastern Daylig L-Size 3082 MB 5069 MB	ht Time (From local ma MD5 SHA1	schine) SHA256	Created n/s n/s	Accessed n/a n/a	Nodified n/a n/a		₹ @ ● 2 ש
List A Name A Na	0		Pile Content Pro	Perties Hex Inte Display Time Zone Category P-Size Partition 3082 N Partition 3069 N Partition 3106 N	Eastern Daylig L-Size 3 3082 HB 5 5069 HB 8 3106 HB	ht Time (Prom local ma MD5 SHA1	achine) SHA256	Created n/s n/s n/s	Accessed n/in n/in n/in	Modified n/a n/a		E002×0
List A Name Jdev/sdb1 Jdev/sdb1 Jdev/sdb1 Jdev/sdb1 Jdev/sdb1 Jdev/sdb1 Jdev/sdb1 Jdev/sdb1	0		File Content Pro	Perties Hex Inte Display Time Zone Category P-Size Partition 3062 N Partition 3064 N Partition 3106 M	Eastern Daylig L-Size 0 3082 MB 5 5069 MB 0 3106 MB 8 109.8 MB 9 203.8 MB	ht Time (Prom local ma MD5 SHA1	shine) SHA256	Created n/a n/a n/a n/a	Accessed n/is n/is n/is n/is	Modified n/a n/a n/a e la		E @ 0 # ×0
List Name Jókv/sdb1 Jókv/sdb1 Jókv/sdb1 Jókv/sdb1 Jókv/sdb1 Jókv/sdb1 Jókv/sdb1 Jókv/sdb1	0		File Content Pro	Perties Hex Inte Display Time Zone Category P-Size Partition 2002 N Partition 2008 N Partition 1008 N Partition 2008 N Partition 2008 N	Eastern Daylig L-Size 0 3082 HB 5 5069 HB 0 3396 HB 0 109.8 HB 109.8 HB 0 203.8 HB	ht Time (From local ma MDS SHA1	schine) SHA256	Created n/s n/s n/s n/s n/s	Accessed n/is n/is n/is n/is n/is	Modified n/a n/a n/a n/a n/a	1	EG04×0
List Name /dev/sdb1 /dev/sdb1 /dev/sdb1 /dev/sdb1 /dev/sdb1 /dev/sdb1 /dev/sdb1 /dev/sdb1	0		File Content Pro	Perties Hex Inte Display Time Zone Category P-Size Partion 3002 M Partion 3000 M Partion 3008 M Partion 2013 R Partion 2013 R Partion 2013 R	Eastern Daylig L-Size 3082 HB 5 5069 HB 8 3326 HB 8 109.8 MB 8 203.8 MB 8 203.8 MB 9 203.8 MB 9 203.8 MB	ht Time (Prom local ma MDS SHA1	schine) SHA256	Created n/s n/s n/s n/s n/s n/s	Accessed n/is n/is n/is n/is n/is	Modified n/a n/a n/a n/a n/a	1	E004x0
List	0 1 2 3 4 5	tem # t	File Content Pro	Perties Hex Inte Display Time Zone Category P-Size Pertion 3002 N Pertion 3009 N Pertion 3009 N Pertion 203.81 Partion 203.81 Partion 2035 N Pertion 2035 N	Eastern Daylig L-Size 5 5062 MB 5 3206 MB 8 109.8 MB 8 109.8 MB 8 203.8 MB 8 2055 MB 8 2055 MB 8 2055 MB 8 2055 MB 8 2055 MB	ht Time (Prom local ma MDS SHA1	schine) SHA256	Created n/s n/s n/s n/s n/s n/s	Accessed n/is n/is n/is n/is n/is n/is	Modified n/a n/a n/a n/a n/a n/a	1	E004 X0
List	0 1 2 3 4 5	- (# -) (# -) Label Tren # Ext 1009 12337 14158 1403 14325 14342 21731 5142 21731	Pile Content Pro	Perties Hex Inte Display Time Zone Category P-Size Partition 3002 N Partition 3002 N Partition 3004 Partition 2003 R Partition 2003 R Partition 2035 N Partition 2035 N Partition 3005 N	Eastern Daylig L-Size 3082 HB 5 5069 HB 3 306 HB 8 1013 8 HB 8 1035 HB 8 1035 HB 8 1035 HB 8 1035 HB 9 1036 HB	ht Time (Prom local ma MDS SHA1.	schine) SHA256	Created n/s n/s n/s n/s n/s n/s n/s n/s	Accessed n/s n/s n/s n/s n/s n/s n/s n/s n/s	Modified n/a n/a n/a n/a n/a n/a n/a	1	E00 2×0
List / Mame /dev/sdb1 /dev/sdb1 /dev/sdb1 /dev/sdb1 /dev/sdb1 /dev/sdb1 /dev/sdb1 /dev/sdb1	0	Ext 1000 1003 14128 1403 1403 1403 14025 14025 14025 14025 14025 14025 14025 14025 14025 1402 1403 1402 1403 1403 1403 1405 1005 1	Pie Content Pro Press P	Perties Hex Inte Display Time Zone Category P-Size Partition 3062 M Partition 3064 M Partition 203.81 Partition 203.81 Partition 203.81 Partition 203.81 Partition 203.81 Partition 203.81 Partition 203.81 Partition 203.91 Partition 203.91 Partition 203.91 Partition 203.91	Eastern Daylig L-Size 5 5069 MB 5 3026 MB 8 109.8 MB 8 2055 MB 8 2055 MB 8 1035 MB 8 1035 MB 8 1035 MB 8 23.00 GB 8 23.00 GB	ht Time (Prom local m MD5 SHA1	schine)	Created n/s n/s n/s n/s n/s n/s n/s n/s	Accessed n/a n/a n/a n/a n/a n/a n/a n/a n/a	Modified n/a n/a n/a n/a n/a n/a n/a n/a n/a	1	E002X0
List	0	- (#-) (*) Label Iten a Ext 1009 10337 14158 14033 14033 14025 1442 2175 1442 2175 14275 1479 12725	File Content Pro Pro Protectoper Ceta L 50-1/, Photocoper	Perties Hex Inte Dipolay Time Zone Category P-Size Partison 3062 M Partison 3062 M Partison 3050 P Partison 203.81 Partison 2035 M Partison 2035 M	Eastern Dayls; L.Size 0 3082 H8 5 5069 H9 0 3296 H8 8 109.8 H8 8 103.8 H8 8 1035 H8 8 1035 H8 8 1035 H8 8 1035 H8 8 23.00 08 8 112.6 M8	ht Time (from local nu I MDS SHA1	schine) SHA256	Created n/a n/a n/a n/a n/a n/a n/a n/a n/a n/a	Accessed n/s n/s n/s n/s n/s n/s n/s n/s n/s n/s	Modified n/a	1	E 0 0 4 × 0
List A Name Adev/edb I Adev	0	- 100 Etem # Ext 1000 11337 14128 14033 14025 1442 12715 1422 12719 12729 12725	Pie Content Pro PretroperGela LEGU/ ProtocoperGela LEGU/	Perties Hex Inte Doplay Time Zone Category IP -Size Partition 3062 H Partition 3062 H Partition 3062 H Partition 3062 H Partition 3063 H Partition 3063 H Partition 203.8 H Partition 203.8 H Partition 203.8 H Partition 203.7 H Partition 2127 H Partition 2127 H Partition 2127 H Partition 2026 H Partition 2027 H Partition 2026 H	Lister Daylig Lister 3082 HB 3082 HB 3082 HB 5069 MB 3086 HB 8005 MB 2038 MB 8005 MB 2055 MB 9005 MB 2055 MB 9005 MB 2005 MB 9005 MB 2005 MB 9005 MB 23.00 GB 9005 MB 20.00 GB 9005 MB 20.00 GB	frit Time (From local nu MDS SHA1	schine) 944255	Created n/s n/s n/s n/s n/s n/s n/s n/s	Accessed n/is n/i	Modified n/a	T	E 6 6 4 ×0
List	0		File Content Pro	Dipolary Time Zone Dipolary Time Zone Category P-Size Perton 3000 H Perton 3000 H Perton 3000 H Perton 2003 H Perton 2004 H Perton 2005 H Perton 5020 H Perton 5020 H	Eastern Daylig L-Size 1 3062 MB 5 5069 MB 8 3306 MB 8 3306 MB 8 3035 MB 8 2355 MB 8 2355 MB 8 2355 MB 8 2355 MB 8 2355 MB 8 2350 MB 5 3025 MB 5 3025 MB	ht Time (from local nu MDS SHA1 -	schine) 944256	Created n/s n/s n/s n/s n/s n/s n/s n/s	Accessed nja nja nja nja nja nja nja nja nja nja	Modified n/a n/a n/a	I	E004×0
List A Name /dev/ddb 1 /dev/ddb	0 1 2 3 4 5	tabel them a tabel them a tabel them a tabel	File Content Pro Port	Depictus Hex Inte Doplay Time Zone Category P-Size Partition 3062 H Partition 3062 H Partition 2033 H Partition 2033 H Partition 2033 H Partition 2035 H Partition 2037 H Partition 2037 H Partition 2030 H Partition 2037 H Partition 2037 H Partition 2037 H Partition 2030 H Partition 2037 H	Eastern Daylig L-Sze 0 3062 H6 5 S069 H6 0 3266 H6 0 3266 H6 0 3205 H6 0 203,8 H6 0 203,8 H6 0 203,8 H6 0 203,8 H6 0 203,9 H6 1 2177 H0 8 23,00 G8 0 225, H6 1 2177 H0 8 10,26,7 H6 1 502,5 H6 1 510 H6 8 10,40,7 H	ht Time (From local nu IMD5 SHA1	schine) 944256	Created n/a n/a n/a n/a n/a n/a n/a n/a	Accessed n/s n/s n/s n/s n/s n/s n/s n/s n/s n/s	Modified r/l0 r/l0	I	E G G A XO
List I and J devyldob J dev	0 1 2 2 3 4 4 5 5	- 19- 2014 1000 - 1000 1000 -	File Content Pro	Display Time Zone Display Time Zone Category P-Size Perston 3004 M Perston 3035 M Perston 23.04 M Perston 32.04 M	Eastern Davis L-Sze 1-Sze 3-2062 MB 5-5069 MB 5-2056 MB 5-205	ht Time (From local nu MDS SHA1	schine) 94A256	Стельтея п.ба п	Accessed ruja ruja ruja ruja ruja ruja ruja ruja	Modified n/e n/e n/e	F	E C O 2 × C
List Arrow Construction Arrow Construction	0 1 2 3 3 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	- 19 - 10 - 10 Label Dam # Ett 1000 100	File Content Pro	Display Time Zone Display Time Zone Category P-Sze Partton 3020 H Partton 3020 H Partton 3020 H Partton 3020 H Partton 2033 H Partton 2033 H Partton 2024 H Partton 2027 H Partton 2026 H Partton 2024 H Partton 203 N Partton 203 N Partton 204 H Partton 203 N Partton 203 N Partton 203 N	Dastern Daylig Eastern Daylig 1.52x 0 3062.46 5 5069.46 8 109.8 MB 8 2055.46 8 2055.46 9 2054.46 8 2055.46 9 2105.46 9 2107.40 9 2025.5 MB 9 102.6 MB 9 102.5 MB 9 102.6 MB	ht Time (From local mu	achine) SHA256	Стеаted л/а л/а л/а л/а л/а л/а л/а л/а	Accessed n/s n/s n/s n/s n/s n/s n/s n/s	Modified n/s n/s	T	E @ @ ×0
List	0 1 2 3 4 4 5 5 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7	(19) (19)	File Content Pro	Display Time Zone Display Time Zone Category (P-See Partison 3002 / Pertson 3002 / Pertson 3002 / Pertson 2003 / Pertson 2003 / Pertson 2003 / Pertson 2003 / Pertson 2003 / Pertson 2004 / Pertson 302 / Pertson 302 / Pertson 302 / Pertson 302 / Pertson 302 / Pertson 2004	Preter Eastern Daylog 1-Size 3-3042 MB 5-5069 MB 8-3064 MB 8-3065 MB 8-3055 MB 8-2035 MB 8-2035 MB 8-2035 MB 8-2035 MB 8-2035 MB 8-2035 MB 8-2035 MB 8-300 CB 9-7127 MB 8-5130 MB 8-5100 MB 8-	ht Time (from local ma	echine) 944256	Created n/a n/a n/a n/a n/a n/a n/a n/a	Accessed n/k n/k n/k n/k n/k n/k n/k n/k n/k n/k	Modified n/a n/a	T	
List	Pitered: 15 Pitered: 15	Control Contro Control Control Control Control Control Control Control Control Co	File Content Pro	Operations Hers: bits Obdrigs Them Zone Devices Them Zone Catagory IP determined Persition Partition 3009 NP Partition 2004 NP Partition 2004 NP Partition 2014 NP Partition 2015 NP Partition 2015 NP Partition 2014 NP Partono 2014 NP	Preter Eastern Daylog 1.63m 3.062.46 5.069.M6 3.236.46 8.109.8 M6 3.235.46 8.235.5 M6 8.235.5 M6 8.23.5 M6 8.23.00 G8 1.277.16 8.510.46 5.00.5 M6 5.10.46 5.10.46 5.00.6 M6 5.10.46 5.10.46 5.00.6 M6 5.10.46 5.10.46 5.10.46 5.00.6 M6 5.10.46 5.00.6 M6 5.10.46 5.00.6 M6 5.10.46 5.00.6 M6 5.10.46 5.10.46 5.10.46 5.00.6 M6 5.10.46	(ht Time (hten local ma	schine) 944256	Created n/a n/a n/a n/a n/a n/a n/a n/a	Accessed n/b n/b n/b n/b n/b n/b n/b n/b	Modified n/s n/s n/a n/a	I	
e List	P 1 2 3 4 5 5 5 5 5 5 5 5 5 5 5 5 5	- 18 - 11 - 12 Label Dam # Est 10300 1030 1030 1030 1030 1030 10	File Content Pro	perties Hex bits - Deploy The Zone - Particlo	Preter Eastern Dayle 1-Size 3 3082 HB 3 3085 HB 3 2035 HB 3 2036 HB 3 2037 HB 3 2036 HB 3 2036 HB 3 2036 HB 3 2036 HB 3 2036 HB 3 2036 HB 3 2037 HB 3	Pri Time (Prom local ma	schne) SHA256	Created n/a n/a n/a n/a n/a n/a n/a n/a	Accessed n/h n/h n/h n/h n/h n/h n/h n/h n/h n/h	Modified n/b n/b	1	

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

* PhotoseperData D1 - Autopy 40.8							A-10-100
file Xew Joo's Window Help							
👩 Oose Case 🌵 Add Data Source 👔 Generate Report					4	⊙ • Keyword Lists	2 Keyword Search
4.0	Directory Listing						(11) (C
🖬 🖾 Ceta Sources	Bookmark File Tags						3 Read
😑 🛄 PhotocapierData 1.001	Table Thursteal						
vol: (unalocated: 0-24772607)	Fit	File Path	Conment	Modified Time	Charged Tine	Accessed Time	Created Time
i = · · · · · · · · · · · · · · · · · ·	NRLSIND	ing_PhotocoseData(10)(vii_vo29044_SIND		2114-05-10 09:54:20 807	2016-05-10 12:02:54	(D7 2044-05-10 12:42:24 ID	0000-00-00 00-00-0
iii iii vol3 0.mm (0x85): 6361488-75323314075	NO45/56.007	and Photocomplanat Photod vol4/BCarvedPley/0044056.pdf		0000-00-00 00:00:00	0000-00-00.00.00.00	0000-00-00-00-00-00	3000-00-03 00.00.0
— isi vol4 (hon-PS Oata (hoda): 21860648-24721415207)	Index 0020 10283051236 15483406136	her Betweensthatat Fit had weldt hader inte unterbierthe it		000-05-00-00-00-00	0000-00-00-00-00-00	0000-00-00-00-00-00	2000-00-00-00-00-
vol7 (J.relaceted: 69303528 49501575)		had an					
- 10 Volt (Norr#5 Data (Ixda): 69304032-7595173951)							
 In total Environment (E4001/02/04/01/209) 							
 Weitz (Linkx Logical Volime Manager (280e): PR020005-24030320299) Weitz (Linkx Logical Volime Manager (280e): PR020005-24030320299) 							
and the set of the set							
Finance webb Lawy Carbon 111402064-53805671670							
- in vol23 fundocated: 121786058-1220+4103							
H- 10 V024 Emax (2x03): 121796560-5500015167)							
will? (Jnalocated: 132292944-132550991)							
⊕ w vol38 Linux (2x83): 132253448-5447566151)							
- 10 vol31 (Unallocated: 142574840-342532887)	12						
1436 28344-1399 757199	13						
 wei35 (Jnaforateil: 149334833: 149294879) 							
() wold (Linux (0x03): 149027336-264126740)							
 wo09 (Unalocated: 149262129-149320167) 							
8-18 r040 (Jmax (2x83): 149262624-362926367)							
- III V043 (JRIBOGRINI: 1496 /9038-14963/903)							
 III V204 LPAX (2453): 1493040-2304639287) III V204 LPAX (2453): 1493044 (24047201) 							
is vote (indexate) (50010176-60039662120							
vest							
(P. d). Fie Types							
- images (325)							
- Videos (0)							
- L Audio (18)	×	- F					
Andrewes (1823)	Hex Stings File Metadata Results Indeved	Text Photos					
© 🖏 Documenta	Natches on pages - of - Hatch	6 a Pages 1 of 1 Page 6 a					Extracted Text
нтия, (20)	72oct 2 0 1	The second second second second					
Office (D)	/TD1ca16a5135e28fabde9566005212768	013-ca1da6135-20fabd0-9560786212*58-01>)					
PDF (3)	etarturef						
Plan Text (3253)	20615						
A Contraction	648CF						
Deleted Dira	trailer						
Plie System (1756)	/2Lem 18						
4 (12)99	/Infe 1 0 I						
B MB File Sze	/base 2 # 2						
MB 50 - 20048 (2)	/IDIefs0a512fbe28ddeBeiss3e2220f4W	LaTerfa0x572fbe29odeRaLaxTe2230f455aTe1					
MR source and left							
10 10 10 10 10 10 10 10 10 10 10 10 10 1	5 / L / F						1.0

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

AccessData Forensic Toolkit Version S	.6.3.16 Database	s localhos	A Cesel Copier 05										
Ele Edit View Evidence Filter	Tools Manag	е Нер				-							
Filter: - unfiltered -			Filter Manager		CI								
Deplace Opening Empl Crapher	Midao Intoine	t/Chat	Danimaria This Cours	Index Car	reh Eusta	um lafarmatic	a Habib						4.5
Contract of the local designed	and et all all etter		Ele Cantant	Didex see	Contraction of the local division of the loc		and a contra	51					
Case Overview		0.0	File Content	(and a second									
■ Nicketse Gradge (247,0000 (247,0000 (247,000 (247,000) (247,000 (247,000 (247,000 (247	2		Hex Text Hitered	matural			3	View win	l dow has e	Error Encountered	a bad file.		e *
🕀 📲 Multimedia (18 / 18)													* A
H A Other Encryption Files (130 / 130	a.		e										1 4
Other Known Types (0/0)	,	-	File Content P	operties	Hex Interp	orețer							
File List													
888/1			Normal	Display	Time Zone: I	Eastern Dayligi	ht Time (Fra	om local mad	hine)				E G & A XC
E A Name Label	Iten #	Dat	Path	Category	P-Size	L-Sze	MDS	\$1A1	9HA256	Created	Accessed	Modified.	
00.	112938		PhotocopierOS1.001//d	Placeh	n/a	nja				n/a	n/a	n/a	
	154698		PhotocopierO62.E01//d	Placeh	n/a	nla				nla	n/a	n/a	
- i	21286		PhotocopierOG1.E01/cr.	Folder	4096 B	4096.0				nja	\$/10/2016 10:1	\$/10/2016 10:1	
.1	143227		PhotocopierOS2.E01/cr	Folder	4096.8	-9096 B				n/a	5/10/2016 10:1	5/10/2016 10:1	
.2	21296		PhotocopierOS1.E01/cr	Folder	4096 B	4096 B				n/a	5/10/2016 10:1	5/10/2016 10:1	
Dia .2	143237		PhotocopierOS2.601/cr.	Folder	4096.8	4096 B				n/s	5/10/2016 10:1	5/10/2016 30:1	
.3	143244		PhotocopierO52.E01/cr.	Folder	4096 B	4096 B				n/a	5/10/2016 10:1	5/10/2016 10:1	
	21403		PhotocopierOS1.E01/cr.	Folder	4096 8	4096 8				n/s	5/10/2016 10:1	\$/10/2016 10:1	
	21418		Photocopier061.601/cr	Folder	4096 B	4096 B				n/a	5/10/2016 10:1	5/10/2016 10:1	
	143259		Photocopier062.801/cr	Folder	4096 B	4096 B				n/a	5/10/2016 10:1	\$/10/2016 10:1	
.5	21427		PhotocopierOS1.E01/or	Folder	4096.8	4096.8				n/a	5/10/2016 10:1	5/10/2016 10:1	
.s	143268		PhotocopierOS2.E01/cr	Folder	4096 B	4096 B				n/a	5/10/2016 10:1	5/10/2016 10:1	
.6	21435		PhotocopierOS1.601/cr.	Folder	4096.8	4096 B				nia	5/10/2016 10:1	\$/10/2016 10:1	
.6	143276		PhotocopierOS2.E01/cr	Folder	4096 B	4096 B				n/a	5/10/2016 10:1	5/10/2016 10:1	
.7	143283		PhotocopierOS2.E01/cr	Folder	4096.8	4096 8				n/is	5/10/2016 10:1	\$/10/2016 10:1	
.7	21442		Photocopier061.E01/cr	Folder	4096 B	4096 B				n/a	5/10/2016 10:1	5/10/2016 10:1	
.8	21411		PhotocopierOG1.E01/or.	Folder	4096.0	4096 B				n/a	5/10/2016 10:1	5/10/2016 10:1	
.8	143252		PhotocopierOS2.601/or.	Folder	4096 B	4096 B				n/9	5/10/2016 10:1	5/10/2016 10:1	
.bash_logout	15992	cmssin	PhotocopierOS1.E01//d	ASCII 7	4096 B	248	d19bbb	091d38	150e5a	n/a	5/10/2016 10:0	3/8/2008 8:36:	
🗋 📄 .bash_logout	137900	cmissin	PhotocopierOS2.801//d	ASCII 7	4096 8	248	d19000	091538	160e6a	n/a	5/10/2016 10:0	3/8/2008 8:36:	-
Loaded: 247,308 Filtered: 247,308	Total: 247,308	H	phighted: 0 Che	sked: 0	Total	Size: 1095 G8			1.010.00				
PhotoconierOS2 E01//dev/sdb1/BOOT	Ext 31/Iroot 1/80	007/800	TAR E77sCarved 1920	01244] ndfa	Carned F1r	al ndf							
Based.			Construction Construction	are dibute		1.0.0	In.	the Tab To	on films				
							- WARKY	med 1862 P.F	AND DESCRIPTION OF				

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)

AccessData Forensic Toolkit Version Ele Edit Vew Evidence Fijte	r 56316 Databese lox rToolsBanage	alhost Case: Copier D Help	ata						-	- x
Pilter: - unfiltered -		Filter Manager	···· 📄 🔂							
Explore Overview Email Graphic	video Internet/Ch	at Bookmarks Live	Search Index Sea	arch System Information	volatile					4
Case Overview	4	File Content								
modules (2/2)		Hex Text Fit	ered Natural							
mit(1/2) mit(1/2) m(5/5) m(5/5) m(5/5) m(5/5) m(5/5) m(5/5) m(5/7) m(5/7) <t< th=""><th></th><th><</th><th>Properties </th><th>ex.Interpreter</th><th>SCAN TO FIL</th><th>l .E</th><th></th><th></th><th></th><th></th></t<>		<	Properties	ex.Interpreter	SCAN TO FIL	l .E				
File List										
888 / 1 1		Normal	 Display 	Time Zone: Eastern Daylight Tir	ne (From local machine)		975 0			∂ ×○
2 A Name Labe	Item # Ext	Path					Category	P-Size L-Size	MDS	2441 -
Carved [104630].pdf	257462 pdf	PhotocopierDista	1.E01//dev/edb3/Unv	ecognized file system [Unknown	[Analocated space+Carved [22964042]. H	Carved [104630] pdf	Adobe	n/a 20.50 K	0.	-
Carved [16].pdf	255950 pdf	PhotocopierData	1.E01//dev/sdb1/800	OT [Ext3]/[root]/BOOT/BOOTAE	LE+Carved [91376444].odf+Carved [0].+C	arved [16].pdf=Carved [16].pdf	Adobe	n/a 4382 KE		
Carved [16].pdf	256745 pdf	PhotocopierData	2.801//dev/sdb1/800	DT [Ext3]/[root]/BOOT/BOOTAS	LEZZ+Carved (92001244).pdf+Carved (0).	Carved [16].pdf+Carved [16]	Adobe	n/a 4882 KE	1	
Carved [16].pdf	256447 pdf	PhotocopierData	2.E01//dev/sdb1/800	DT [Ext3]/[root]/BOOT/BOOTAL	LE+Carved (91376444).pdf+Carved (0).+C	arved [16].pdf	Adobe	n/a 4882.KZ	K.	-
•		20 C	10		191 - 191 - 198 - 198 - 198 - 198 - 198 - 198 - 198 - 198 - 198 - 198 - 198 - 198 - 198 - 198 - 198 - 198 - 198					
Loaded: 30 Filtered: 30	Total: 30	Highlighted; 1	Checked: 0	Total LSize: 60.59 MD						
rhotocopierData1.E01//dev/sdb3/Unr	ecognized file system	Unknown]/unallocat	ed space>Carved [3	22964042].>Carved [10463	0].pdf					
xady				0/	erview Tab Filter: [None]					_

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

Effe Ext Level First Undited Parter				Contraction of the
Next until resolution Plane Manager Image Control Image Contro Image Contro Image Control <th></th> <th></th> <th></th> <th></th>				
Splitp Overview Email Graphen Video Internet/Char Bookmarks Like Search System In Care Overview 4 FAR Context FAR Context Maturel Maturel <th></th> <th></th> <th></th> <th></th>				
Cite Overview File Content Part (10) / 100 /	mation Volatie			
Note Note <th< th=""><th></th><th></th><th></th><th></th></th<>				
Price (16) (16) 2045257051 Price (16) (16) 20557051 Price (16) (16) 2055				
A Nexe Labor Text Path Diplay Time Zone: Exclore A Nexe Labor Text Path Pointogenetation: 160 U/dir/w/db:11A0XARE Enclore Avantex.log 13992 None Pointogenetation: 200 U/dir/w/db:11A0XARE Enclore JobAcc.log 13992 None Pointogenetation: 200 U/dir/w/db:11A0XARE Enclore JobAcc.log 13992 None Pointogenetation: 200 U/dir/w/db:11A0XARE Enclore JobAcc.log 13993 None Pointogenetation: 200 U/dir/w/db:11A0XARE Enclore JobAcc.log 13993 None Pointogenetation: 200 U/dir/w/db:11A0XARE Enclore JobAcc.log 13993 None Pointogenetation: 200 U/dir/w/db:11A0XARE Enclore JobAcc.log 13995 Nonecose/etabacl.200 U/dir/w/db:11A0XARE Enclore Enclore JobAcc.log 13995 Nonecose/etabacl.200 U/dir/w/db:11A0XARE Enclore Enclore JobTm.log 13995 Nonecose/etabacl.200 U/dir/w/db:11A0XARE Enclore Enclore UMABPALLOG 13995 N				
Image: Control of the second				
▲ Name Label Test Petrospectros ■ Name Label Test Petrospectros Entrospectros ■ Name Label Test Petrospectros Entrospectros Entrospectros ■ Subscr. log 13992 Hog Petrospectros Entrospectros Entrospectros > Subscr. log 13992 Hog Petrospectros Entrospectros Entrospectros > Subscr. log 14952 Hog Petrospectros Entrospectros Entrospectros > Subscr. log 14952 Hog Petrospectros Entrospectros Entrospectros > Subscr. log 14952 Hog Petrospectros Entrospectros Entrospectros > Subscr. log 14958 Hog Petrospectros Entrospectros Entrospectros Entrospectros > Subscr. log 13967 Hos Petrospectros Entrospectros Ent	Daylight Time (From local machine)			IT CO DO A
Fashmatikg 1493 Leg Photospectralsa: EXIV/Lev/dbit /LNOWME_EXIV/Lev/dbit /LNOWME		Category	P-Size L-Size	MD5 S
FainPetchig 12792 bit Photosperficial.201/Wryde 1LX0/Wreff EXCI/pro- babic.clg 12793 Bit Photosperficial.201/Wryde 1LX0/Wreff EXCI/pro- babic.clg	invmem/FaxProt.log	Text	4096.8 2048.8	3e7682 e5
JAAACLOB 137351 top Photospechasil.201//wr/db11/Wr/WE [2:17]/po JAAACLOB 1492 top Photospechasil.201//wr/db11/Wr/WE [2:17]/po JAAACLOB 14942 top Photospechasil.201//wr/db11/Wr/WE [2:17]/po JAAACLOB 137951 top Photospechasil.201//wr/db11/Wr/WE [2:17]/po JAAACLOB 137951 top Photospechasil.201//wr/db11/Wr/WE [2:17]/po JAAFTA JO 137956 top Photospechasil.201//wr/db11/Wr/WE [2:17]/po JAABTA LOG 137956 top Photospechasil.201//wr/db11/Wr/WE [2:17]/po JAABTA LOG 137956 top Photospechasil.201//wr/db11/Wr/WE [2:17]/po JABARA LOG 137956 top Photospechasil.201//wr/db11/Wr/WE [2:17]/po JUBARA LOG 137956 top Photospechasil.201//wr/db11/Wr/WE [2:17]/po JUBARA LOG 137958 top Photospechasil.201//wr/db11/Wr/WE [2:17]/po JUBECCHLOG 137958 top Photospechasil.201//wr/db11/Wr/WE [2:17]/po JUBECCHLOG 137958 top Photospechasil.201//wr/db11/Wr/WE [2:17]/po JUBECCHLOG 137958	hvmem/FaxProt.log	Text	4096 B 2048 B	3e7682 e!
JAMACLÓG 1452 log Photospechas LLO //ev/ds 11/AC/WHE [LOL]/po JAMACLÓ Jay 1442 log Photospechas LLO //ev/ds 11/AC/WHE [LOL]/po JAMACLÓ Jay 1474 log Photospechas LLO //ev/ds 11/AC/WHE [LOL]/po JAMACLÓ Jay 13741 log Photospechas LLO //ev/ds 11/AC/WHE [LOL]/po JAMACLÓ Jay 13747 log Photospechas LLO //ev/ds 11/AC/WHE [LOL]/po JAMACLÓ Jay 13747 log Photospechas LLO //ev/ds 11/AC/WHE [LOL]/po JAMACLÓ JAY LOLAY	hvmen/JobAcc.log	Text	344.0 KB 342.0 KB	afd0d7 Si
Jahaco.Dag 14482 kg Protocome Class L50 ///w/dx1 //KOR44E [15:1]/group Jahco.Dag 13745 kg Protocome Class L50 //w/dx1 //KOR44E [15:1]/group Jahco.Dag 14668 kg Protocome Class L50 //w/dx1 //KOR44E [15:1]/group Jahron bg 14667 Kg Protocome Class L50 //w/dx1 //KOR44E [15:1]/group Jahron bg 13767 Kg Protocome Class L50 //w/dx1 //KOR44E [15:1]/group JAHRAYALOG 13797 Kg Protocome Class L50 //w/dx1 //KOR44E [15:1]/group JUHERYALOG 137976 Kg Protocome Class L50 //w/dx1 //KOR44E [15:1]/group JUHERYALOG 137976 Kg Protocome Class L50 //w/dx1 //KOR44E [15:1]/group JUHERYALOG 137976 Kg Protocome Class L50 //w/dx1 //KOR44E [15:1]/group JUHERYALOG 137976 Kg Protocome Class L50 //w/dx1 //KOR44E [15:1]/group JUHERYALOG 137978 Kg Protocome Class L50 //w/dx1 //KOR44E [15:1]/group JUHERYALOG 137987 Kg Protocome Class L50 //w/dx1 //KOR44E [15:1]/group JUHERYALOG 14798 Kg Protocome Class L50 //w/dx1 //KOR44E [15:1]/group	hvmen/JobAcc.log	Text	344.0 KB 342.0 KB	afd0d7 Si
JableCO.Jog 137415 kg PrintcogerChabL201/khr/sht 11/GNUME [Ex13]/get JableTo.Jog JableTo.Jog 14564 50 PrintcogerChabL201/khr/sht 11/GNUME [Ex13]/get JableTo.Jog JableTo.Jog 137667 50 PrintcogerChabL201/khr/sht 11/GNUME [Ex13]/get JableTo.Jog JableTo.Jog 137667 50 PrintcogerChabL201/khr/sht 11/GNUME [Ex13]/get JableTo.Jog JubeTo.Jog 137967 60 PrintcogerChabL201/khr/sht 11/GNUME [Ex13]/get JableTo.Jog PrintcogerChabL201/khr/sht 11/GNUME [Ex13]/get JableTo.Jog JubeTo.Jog 14944 60 PrintcogerChabL201/khr/sht 11/GNUME [Ex13]/get JableTo.Jog PrintcogerChabL201/khr/sht 11/GNUME [Ex13]/get JableTo.Jog JubeTo.Jog 13793 Sig PrintcogerChabL201/khr/sht 11/GNUME [Ex13]/get JableTo.Jog PrintcogerChabL201/khr/sht 11/GNUME [Ex13]/get JableTo.Jog JMERCORLOG 14949 Sig PrintcogerChabL201/khr/sht 11/GNUME [Ex13]/get JableTo.Jog PrintcogerChabL201/khr/sht 11/GNUME [Ex13]/get JableTo.Jog JMERCORLOG 14949 Sig PrintcogerChabL201/khr/sht 11/GNUME [Ex13]/get JableTo.Jog PrintcogerChabL201/khr/sht 11/GNUME [Ex13]/get JableTo.Jog JMERCORLOG 14949 Sig PrintcogerChabL201/khr/sht 11/GNUME [Ex13]/get JableTo.Jog	hvmen/JobAccO.log	Text	240.0 KB 240.0 KB	206894 9
Johns Jog 14668 kg ProtocogeCatal.201//ev/dbt 1/KCNME [Exc]/goo Johns Jog J3567b Jog ProtocogeCatal.201//ev/dbt 1/KCNME [Exc]/goo JABJYALOG 12797b Jog ProtocogeCatal.201//ev/dbt 1/KCNME [Exc]/goo JUARFXALOG 12797b Jog ProtocogeCatal.201//ev/dbt 1/KCNME [Exc]/goo JUARFXALOG 12797b Jog ProtocogeCatal.201//ev/dbt 1/KCNME [Exc]/goo JUBRFXALOG 13797b Jog ProtocogeCatal.201//ev/dbt 1/KCNME [Exc]/goo JUBRFXALOG 13797b Jog ProtocogeCatal.201//ev/dbt 1/KCNME [Exc]/goo JUBRFXALOG 13797b Jog ProtocogeCatal.201//ev/dbt 1/KCNME [Exc]/goo JUBRCKALOG 13797b Jog ProtocogeCatal.201//ev/dbt 1/KCNME [Exc]/goo JUBRCKALOG 13797b Jog ProtocogeCatal.201//ev/dbt 1/KCNME [Exc]/goo JUBRCKALOG 1474b Jog ProtocogeCatal.201//ev/dbt 1/KCNME [Exc]/goo JURCKALOG 1474b Jog ProtocogeCatal.201//ev/dbt 1/KCNME [Exc]/goo JURCKALOG 1474b Jog ProtocogeCatal.201//ev/dbt 1/KCNME [Exc]/goo JURCKALOG 1474b Jog ProtocogeCatal.201//ev/dbt 1/KCNME [Exc]/goo	hvmen/JobAccO.log	Text	240.0 KB 240.0 KB	205894 9
Johns bg 13767 bg PhotospecTeable 201/(kr/whot I)/KV/WHE [D:12]/(br JUMB/XLOG 13797 bg PhotospecTeable 201/(kr/whot I)/KV/WHE [D:12]/(br JUMB/XLOG 14946 bg PhotospecTeable 201/(kr/whot I)/KV/WHE [D:12]/(br JUMB/XLOG 14946 bg PhotospecTeable 201/(kr/whot I)/KV/WHE [D:12]/(br JUMB/XLOG 14946 bg PhotospecTeable 201/(kr/whot I)/KV/WHE [D:12]/(br JUMB/XLOG 14943 bg PhotospecTeable 201/(kr/whot I)/KV/WHE [D:12]/(br JUMB/XLOG 13983 bg PhotospecTeable 201/(kr/whot I)/KV/WHE [D:12]/(br JUMB/XLOG 14944 bg PhotospecTeable 201/(kr/whot I)/KV/WHE [D:12]/(br JUMI/XLOG 14944 bg PhotospecTeable 201/(kr/whot I)/KV/WHE [D:12]/(br JUMI/XLOG 14944 bg PhotospecTeable 201/(kr/whot I)/KV/WHE [D:12]/(br	hvmem/JobTmp.log	Test	204.0 KB 203.0 KB	clicee0 7
UNUERVALOG 12709 big Photospechasi.20.1//ev./dbi.11.V/CNME_[0.21]/pig. UNUERVALOG 1494-big Photospechasi.20.1//ev./dbi.11.V/CNME_[0.21]/pig. UNUERVALOG 1494-big Photospechasi.20.1//ev./dbi.11.V/CNME_[0.21]/pig. UNUERVALOG 13976 big Photospechasi.20.1//ev./dbi.11.V/CNME_[0.21]/pig. UNERVALOG 1494-big Photospechasi.20.1//ev./dbi.11.V/CNME_[0.21]/pig. Legi.20.1/20.1/20.1/20.1/20.1/20.1/20.1/20.1	nvmem/JobTmp.log	Text	204.0 KB 203.0 KB	c0cee0 7
UAUERALLOG 1444 Ioo Photocoperbasis 160 (Mev/dot 11/KOVME) [Exc1] (Ioo UPBUT.LOG 13784 Ioo Photocoperbasis 201 (Mev/dot 11/KOVME) [Exc1] (Ioo UPBUT.LOG 14943 Ioo Photocoperbasis 201 (Mev/dot 11/KOVME) [Exc1] (Ioo UPBUT.LOG 14943 Ioo Photocoperbasis 201 (Mev/dot 11/KOVME) [Exc1] (Ioo UPBCONLOG 13783 Ioo Photocoperbasis 201 (Mev/dot 11/KOVME) [Exc1] (Ioo UPBCONLOG 14744 Ioo Photocoperbasis 201 (Mev/dot 11/KOVME) [Exc1] (Ioo UPBCONLOG 14744 Ioo Photocoperbasis 201 (Mev/dot 11/KOVME) [Exc1] (Ioo UPBCONLOG 14744 Ioo Photocoperbasis 201 (Mev/dot 11/KOVME) [Exc1] (Ioo UPBCONLOG 14744 Ioo Photocoperbasis 201 (Mev/dot 11/KOVME) [Exc1] (Ioo	VAR/ADM/PIPITLOG/LMAIRFAX.LOG	Text	1680 KB 1679 KB	6fd82f b
UBBL/TLDG 1379% log PhotospecTedLE 201/W-r/dx11K04WE [Ex13] (po UBBL/TLDG 1494 / 120 UBBL/TLDG 1494 / 120 Sep PhotospecTedLE 201/Wr/dx11K04WE [Ex13] (po UBBL/TLDG 1494 / 120 UBBL/TLDG 1494 / 120 Sep PhotospecTedLE 201/Wr/dx11K04WE [Ex13] (po UBBL/TLDG 1494 / 120 UBBL/TLDG 1494 / 120 Sep PhotospecTedLE 201/Wr/dx11K04WE [Ex13] (po UBBL/TLDG 1494 / 120 UBBL/TLDG 1494 / 120 Sep PhotospecTedLE 201/Wr/dx11K04WE [Ex13] (po UBBL/TLDG 1494 / 120 UBBL/TLDG 1494 / 120 Sep PhotospecTedLE 201/Wr/dx11K04WE [Ex13] (po UBBL/TLDG 1494 / 120 UBBL/TLDG 1494 / 120 Sep PhotospecTedLE 201/Wr/dx11K04WE [Ex13] (po UBBL/TLDG 1494 / 120 UBBL/TLDG 1494 / 120 Sep PhotospecTedLE 201/Wr/dx11K04WE [Ex13] (po UBBL/TLDG 1494 / 120 UBBL/TLDG 1494 / 120 Sep PhotospecTedLE 201/Wr/dx11K04WE [Ex13] (po UBBL/TLDG 1494 / 120 UBBL/TLDG 1494 / 120 Sep PhotospecTedLE 201/Wr/dx11K04WE [Ex13] (po UBBL/TLDG 1494 / 120 UBBL/TLDG 1494 / 120 Sep PhotospecTedLE 201/Wr/dx11K04WE [Ex13] (po UBBL/TLDG 1494 / 120 UBBL/TLDG 1494 / 120 Sep PhotospecTedLE 201/Wr/dx11K04WE	VAR/ADM/PIPTILOG/LMAIRFAX.LOG	Text	1680 KB 1679 KB	6fd82f bi
UBBLCNLCG 14943 bg Photospectrals.100/(#vr/db:1/MCVME_B021) UBBCCNLCG 13993 bg Photospectrals.100/(#vr/db:1/MCVME_B021) UBBCCNLCG 14940 bg Photospectrals.100/(#vr/db:1/MCVME_B021) UBBCCNLCG 14940 bg Photospectrals.100/(#vr/db:1/MCVME_B021) UBBCCNLCG 14940 bg Photospectrals.100/(#vr/db:1/MCVME_B021)	VAR/ADM/PIPTLOG/LMBAUT.LOG	Text	1204 KB 1203 KB	64ce78 68
DMBCOMLOG 137893 log PhotocoperDist3.E01/(dev/lob11)/E01/WEE [Src1]/(for UMBCOMLOG 14940 log PhotocoperDist3.E01/(dev/lob11)/(dev/lob11)/(for UMCOMLOG 14940 log PhotocoperDist3.E01/(dev/lob11)/(for UMCOMLOG 117898 log log <td< td=""><td>VAR/ADM/PIPITLOG/LMBAUT.LOG</td><td>Text</td><td>1204 KB 1203 KB</td><td>64ce78 6</td></td<>	VAR/ADM/PIPITLOG/LMBAUT.LOG	Text	1204 KB 1203 KB	64ce78 6
UNIDCONLOG 14940 log Protocoper/Data.101/(de/u/de11)/101/UNIANI [0:17]/(for INC/041/02 173888 lon Binteroneir/Data.261/(de/u/de11)/101/UNIANE.261/01/for	VAR/ADM/PIPITLOG/LMBBCOM.LOG	Text	84.00 KB 84.00 KB	8e0964 21
INCOM LOG INCOM LOG IN INCOM LOG IN IN INCOM LOG IN	VAR/ADM/PIPITLOG/LMBBCOM.LOG	Text	84.00 KB 84.00 KB	Be0954 21
the second data and the se	VAR /ann.PIPITI OG 8 MCOM 1 OG	Test	15RR.KR 15R5.KR	Section ina
di 44 Filteredi 44 Total: 44 Highlightedi 1 Checkedi 0 Total LSize: 2	07 MB			
ocopierData1.E01//dev/sdb11/NONAME [Ext3]/[root]/VAR/ADM/PIPITLOG/LMCOM.LOG				

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)

Operation Description Description <thdescription< th=""> <thdescription< th=""> <</thdescription<></thdescription<>	Order Description Order Description Description Order Description Description Description Description Description Order Description								
Description Test Note:	Image: control intervent interven	€ →	Drectory Listing						100
View Control C	View Units Loch Model Tra Oway Tra Kennet Tra Model Tra Model Tra Model Tra	Ceta Sources	Table Thumboal						
implementation impleme	image: space	 Vevs d. ReTures 	Name	Lecation	Mudified Time	Change Time	Access Time	Created Time	Ser 1
	• Marcial State • Marcial State > Marcial	Theres (21.0	ar brandingson be device and	Jac Putocopyber FOL/vii udDWWW/ja/neda/oor brandmast	2016-05-10 (0.03 (9) 807	2016-05-10 10-01-26 FDT	2014-05-10 10:00.09 FDT	0000-00-00.00:00:00	47:71 4
Note 00 Note 00	• More 00 • Note 00 • N	Videos (00	W address kon one	And Photocoperints E0: And wild/WWW/Jalmedia/address.com.prg	2016-05-10 10.03.28 807	2010-07-10 10:00.00.00 2017	2010-05-10 10:00:24 607	mon-or-or oc.or.oc	+510
Second State Second State<	Note of the second se	- Audio (2)	The very sector be filling	Ing Photocopiedrit1 E01/vil +o02WWW/Jahredia/vavautors bg f.	2016-25-10 10:43:29 601	2016-05-10 10:00 09 EDT	2015-05-10 10:03:28 601	0000-00-00-00-00-00	6010
Perspective	Profile Profile <t< td=""><td>And And And And And And And And And And</td><td>Torter/Heading bg.prg</td><td>And PhotocoperDilli E0(And volDWWA/Ja/media/content/wadrog</td><td>2014-25-10 10-61-28 607</td><td>2016-05-10 10:00:09 807</td><td>2011-05-10 10-01-24 607</td><td>0006-06-08 00-00-00</td><td>1277</td></t<>	And	Torter/Heading bg.prg	And PhotocoperDilli E0(And volDWWA/Ja/media/content/wadrog	2014-25-10 10-61-28 607	2016-05-10 10:00:09 807	2011-05-10 10-01-24 607	0006-06-08 00-00-00	1277
	No. Control Name No. Not-control No. No. No. Not-control No. Not-contro <td>NTM (19)</td> <td>g drectprint, ican ang</td> <td>ing Potneceint1E01/vst vol2WWW/wineda/devetarte con</td> <td>2016-05-10 (0-03-20 007</td> <td>2016-05-10 10:03:20 807</td> <td>2011-05-13 10:01:24 807</td> <td>1005-01-00 00-00-00</td> <td>4571 4</td>	NTM (19)	g drectprint, ican ang	ing Potneceint1E01/vst vol2WWW/wineda/devetarte con	2016-05-10 (0-03-20 007	2016-05-10 10:03:20 807	2011-05-13 10:01:24 807	1005-01-00 00-00-00	4571 4
Prof DB Proj DB <t< td=""><td>Part (FIG) Part (F</td><td>- Crfice (0)</td><td>Travisation be selected and</td><td>Into Photocopyrolit1 E0: And vol2/WWW/Ja/meda/www.aton. bt +</td><td>2016-05-10 10:03:26 EDT</td><td>2016-05-10 10-03:26 (017</td><td>2014-05-10 10:00:29 207</td><td>1000-00-00 00-00-00</td><td>885 4</td></t<>	Part (FIG) Part (F	- Crfice (0)	Travisation be selected and	Into Photocopyrolit1 E0: And vol2/WWW/Ja/meda/www.aton. bt +	2016-05-10 10:03:26 EDT	2016-05-10 10-03:26 (017	2014-05-10 10:00:29 207	1000-00-00 00-00-00	885 4
Locare Statistic Machine Statistic <thmachine statistic<="" th=""> Machine Statistic</thmachine>	Luczsowar, Na, 240 Nach Sett (20) Luczsowar, Na, 240 Nach Sett (20) Luczsowar, Nach 240 Nach	- V PDP (0)	E an konung	Jass Wetscoperbill (0)/vid vid/WWWJa/media/app kompre	2010-25-10 10:43-00 607	1010-03-10 10:00 20 201	2011-03-13 10:03 20 207	0000-00-00-00-00-00	4351 4
No. Marcing Proj. Strateging Jung Marcy Proj. Strategi	Part Jan Aller Part Ja	Plan Text (28)	E sacamente bo a oto	Inc. Petrocene/bit1001/vii volDWWW/admeda/uccommone.htt	2016-35-10 10:03 19 601	2016-05-10 10:03:28 837	2014-05-10 10:00.28 EDT	0006-06-06 00:00:00	512
	Benerg (am)	- Side Text (2)	the new brandware by have new	Inter Petropartitit El: And -sil2/APMA/Ja/meda/oor frankram	2016-35-10 10-03-29 EDF	2016-05-10 10-09-29 201	2014-06-13 10-03-28 607	0000-00-00 00-00-00	1004
Intercorp Processing Processi	Interse Implementation	() ees ()	Truce and honory	Java divisor and bits FOL/and and/W/Waltabarda/dears and bet-	2016-25-10 10 (21-25) [01	2016-PS-ID 10-01-08-F11	2014-05-10 10-00-28 FDT	000-00-00-00-00-00	837 8
in the January B, J	Art 01 Bar Janobago Japatestra Mag Mag Managest B (10 /m 2017m) (2017m) (2017	- Leii (0)	The factory and	line References/set IN Ad with/Webshedellares me	2016-05-10 (0-01-06-01-0	2016-05-10 10:03:09:07	2014-05-10 10-02-24 EDT	000-01-01-01-01-01	4004
	Model Market Station Market Station </td <td>- Lut (0)</td> <td>an encoderate he destand and</td> <td>And Networket 1711 at additional and a second</td> <td>2010-15-10 (0.01-06-007</td> <td>2016-05-10-10-02-09-02-0</td> <td>2011-05-13-16-05-26-05-7</td> <td>0000-01-01-00-00-01</td> <td>-</td>	- Lut (0)	an encoderate he destand and	And Networket 1711 at additional and a second	2010-15-10 (0.01-06-007	2016-05-10-10-02-09-02-0	2011-05-13-16-05-26-05-7	0000-01-01-00-00-01	-
Bits Bits <th< td=""><td>Control 00 par/screentype/</td><td>- a .ond (1)</td><td>The second secon</td><td>Jaw Mctromechitt Ett for antibiotechilametalogenetation has been</td><td>- 2016-25-10 (D-03-26-FDF</td><td>2016-05-10 10-09-20-007</td><td>2014-05-13 10-20-24 207</td><td>0000-00-00-00-00-00-00-00-00-00-00-00-0</td><td>222</td></th<>	Control 00 par/screentype/	- a .ond (1)	The second secon	Jaw Mctromechitt Ett for antibiotechilametalogenetation has been	- 2016-25-10 (D-03-26-FDF	2016-05-10 10-09-20-007	2014-05-13 10-20-24 207	0000-00-00-00-00-00-00-00-00-00-00-00-0	222
A Stratem (148) And Stratem (148)	Strate Strate<	Deleter Dire	are brandingare by upgrands and	liser the terrestable to the second s	2016-35-10 10-53-36-507	2014-05-10 10-Ch 38 EVT	MILES IN ISOMOUTINEST	0000-00-00-00-00-00	-
• # 1003 • # 2004 (space	L L <thl< th=""> L L L</thl<>	File Explain (2681)		line determinent mit fall until and and a fall of the second	2016-20-10-00-00-00-00	0116_PE_101100-0-00.011	THE ME IN MOUTH AND		imate a
Mile Feine And Antonio Columnation Mile Feine	Mile Feision Mile Peison	All (1585)	a to be to get by an and	Inc. Between hit for hit collected and hands have been been been been been been been be	1014-35-10 (0.83-10 EDF	Marchel in the state and	WHILE AN AD AD AD AD AD	1000-00-00-00-00-00-00-	3445 1
Image: Space (g) Image: Space (g)<	Here 50: 2006 (C) Registration (C) <thregistration (c)<="" th=""> <thregistration (c)<="" <="" td=""><td>MB File Sole</td><td>The second secon</td><td>here an an</td><td>2016-05-10 10101038 601</td><td>2016-05-10 10:00 12 (01</td><td>2013-00-11 10-01-20 ED1</td><td>000000000000000000000000000000000000000</td><td>1013</td></thregistration></thregistration>	MB File Sole	The second secon	here an	2016-05-10 10101038 601	2016-05-10 10:00 12 (01	2013-00-11 10-01-20 ED1	000000000000000000000000000000000000000	1013
Operation Operation <t< td=""><td>Bits Bits <th< td=""><td>MB 50 - 20046 (2)</td><td>a contract gate of</td><td>Ins. Reference Mill Tor And and Million Andread adverses of the</td><td>This of its there is stor</td><td>2014 05 10 10 01 20 20 10 1</td><td>2012-00-10-10-00-00-00</td><td>0000-00-00-00-00-00-</td><td></td></th<></td></t<>	Bits Bits <th< td=""><td>MB 50 - 20046 (2)</td><td>a contract gate of</td><td>Ins. Reference Mill Tor And and Million Andread adverses of the</td><td>This of its there is stor</td><td>2014 05 10 10 01 20 20 10 1</td><td>2012-00-10-10-00-00-00</td><td>0000-00-00-00-00-00-</td><td></td></th<>	MB 50 - 20046 (2)	a contract gate of	Ins. Reference Mill Tor And and Million Andread adverses of the	This of its there is stor	2014 05 10 10 01 20 20 10 1	2012-00-10-10-00-00-00	0000-00-00-00-00-00-	
No. Procession Procession <td>Instrument Instrument Instrum</td> <td>- MB 20040 - 150 (S)</td> <td>a sox_cor.prg</td> <td>lad"-ucrocobecters to the "rothward to segregation" row bud</td> <td>2016-35-10 10:13:25 601</td> <td>2016-05-10 10103 28 601</td> <td>2019-05-10 10:01:20 001</td> <td>0000-00-00 00 00 0000</td> <td>4553</td>	Instrument Instrum	- MB 20040 - 150 (S)	a sox_cor.prg	lad"-ucrocobecters to the "rothward to segregation" row bud	2016-35-10 10:13:25 601	2016-05-10 10103 28 601	2019-05-10 10:01:20 001	0000-00-00 00 00 0000	4553
Bondschart Mater. J. Schart	Botest Order 1 Botest	Results	Tank (and) can job (an)	lad"unitedea.prg. pp. (eif"region.org/resemption.perifical"	2016-05-10 10:021-09 FDT	.mie-es-to to-ch.26.251		more-de-de de-de-de-	563
Construction Memory Set (a), proved (a), proved (a), provide and provide a	Construction Medgebringt, pure Megebringt, pure <td>Extracted Content</td> <td>agg.ess_coul_pdortad</td> <td>lind"uproche.peri portika"ingue.ek/houegreagaun"con"m</td> <td>2016-95-10 (DIRELOBEDT</td> <td>2018/69-10 10:03/35/697</td> <td>2019-06-13 10:01-28 EDT</td> <td>0000-06-00-00-00-00</td> <td>406 4</td>	Extracted Content	agg.ess_coul_pdortad	lind"uproche.peri portika"ingue.ek/houegreagaun"con"m	2016-95-10 (DIRELOBEDT	2018/69-10 10:03/35/697	2019-06-13 10:01-28 EDT	0000-06-00-00-00-00	406 4
A report Int A report Int<	A report Ins Projection (Streep Starts (St)) Projection (Streep Starts (Streep Starts (Streep Starts (Streep Starts (St))) Projection (Streep Starts (Streep St	🖙 🕍 Extension Manalch Detected (\$38)	Tandagou" p6"an bud	And "upported that the loss way the predamand the "pd"?"	. 2016-25-19 (0:03:29 ED1	2010-02-10 10:00:09:001	2014-05-10 10:00.28 001	0000-00-00:00:00:00	0106 3
Specified (specified (specif	Spright (set of streed Stards [2]) 1 Spright (set of streed Stards [2]) 000000000000000000000000000000000000	A Reynord Hts	andergouil performed	Jeeg_TestumperSHLEG(/ve_veQV/VV/)Emeila/savgeline_bg_e-	2016-26-10 (D-63-28 821	2014-05-10 10-09-09-801	2014-06-10 10-00-26 80 1	0000-00-00-00-00-00-	274 4
Service Concernmental and a service of the ser	 A set of the set of	Single Literal Reyword Search (0) Single Taxa for Engenerating Search (0)	X pox_courted	/mg_hitocoperant1.b0(/ml_vol2w/wv/)annelia.bov_kon.phg	0000-00-00-00-00100	0000-00-00 00:00.00	(000-01-01-00.00.00	0000-00-00 00:00:00	8. B
Marine Marine Marine Marine Marine Marine Marine Ma	Hadar He	E S Inge Repair Expression and Convy	atemode_kcm_logo.pnp	Jing_Photocoperbit1.001/vii_vi/07WWW/jw/media/juerrode_jcon_l.	2016-05-10 10:01:09 /07	3016-05-10 10:00 UN EDT	1011-05-10 10-01-20 FDT	0000-00-00-00-00-00	700 8
Ideal Message Transformed International Internationa International International International International Internatio		F Hadset Hits	A	The Arter and the Market Market Science and American	L. NOLADALIN, PLAN IN MICH.	2114-26-10.01/7110.017	THE PROPERTY OF THE PROPERTY.		
A Price sing Store	🙆 E-Mid Neuroper	🔮 E-Mal Messages	PEN Group Instants Incasts [24						
185	/ 🌮 Prioresing Roma	/ 🧚 Interesting Itone							
	a Tap	Teps							
kperts	k Rovb	k Reports							

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	File Type	Zero HD	OS HD	Data HD	Initialize HD
Software					
	Log	0	44	44	44
FTK® 5.6.13	Graphics	0	8117	10749	8285
	PDF	0	54	30	54
	Images	0	325	325	311
	Archives	0	1523	1523	941
Autopsy®	PDF	0	0	1	0
4.0.0	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)

File Co	ntent										
Hex	Text Filtere	d Natural									
gues	t										*
7654 defau Attac	321 ult :hed Image										
7054											
/654 initia	321 I										-
initia	i										±
											Ŧ
										P	
File	Content	Properties	Hex In	terpreter							
File List	:										
₽₽	8 🖊 🔒			•	i i i i i i i i i i i i i i i i i i i	Normal		•	Display Time Zone: Eastern [🗕 🍊 🗙 🔿	ł
V	 Name 		Label	Item #	Ext	Path					
	BOOTABLE			5075	<missin< td=""><td>PhotocopierD</td><td>ata 1.E0 1//de</td><td>ev/s</td><td>sdb1/BOOT [Ext3]/[root]/BOOT/BOOTABLE</td><td></td><td></td></missin<>	PhotocopierD	ata 1.E0 1//de	ev/s	sdb1/BOOT [Ext3]/[root]/BOOT/BOOTABLE		
	BOOTABLE			128075	<missin< td=""><td>PhotocopierD</td><td>ata2.E01//de</td><td>ev/s</td><td>sdb1/BOOT [Ext3]/[root]/BOOT/BOOTABLE</td><td></td><td></td></missin<>	PhotocopierD	ata2.E01//de	ev/s	sdb1/BOOT [Ext3]/[root]/BOOT/BOOTABLE		
	BOOTABLEZZ			5077	<missin< td=""><td>PhotocopierD</td><td>ata 1.E0 1//de</td><td>ev/s</td><td>sdb1/BOOT [Ext3]/[root]/BOOT/BOOTABLEZZ</td><td></td><td></td></missin<>	PhotocopierD	ata 1.E0 1//de	ev/s	sdb1/BOOT [Ext3]/[root]/BOOT/BOOTABLEZZ		
	BOOTABLEZZ			128077	<missin< td=""><td>PhotocopierD</td><td>ata2.E01//de</td><td>ev/s</td><td>sdb1/BOOT [Ext3]/[root]/BOOT/BOOTABLEZZ</td><td></td><td></td></missin<>	PhotocopierD	ata2.E01//de	ev/s	sdb1/BOOT [Ext3]/[root]/BOOT/BOOTABLEZZ		



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.





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