Digital Forensic Report Superior Bicycles

Lab 3

Prepared by: Dennis Keritsis
IT SECURITY DEPARTMENT

Table of Contents

1. Forensic Copies

The Hash value for each image has been computed to show that the instant expert has maintained integrity during investigation from the original sourced computer. No alterations or substitutions have been made in any way, shape, or form to the images examined. Four digital images were used in this examination.

1.1. Statement of Compliance

I Examiner Keritsis assets that I am sufficiently skilled in digital forensics. I understand that my opinions are based on fact. I have no financial interest in the manner. The facts in this report are recorded to the best of my knowledge and ability. I attest these to be true in accordance with company policy.

1.2. Tools

∞ **AccessData FTK Imager –** Version 3.1.1.8

This forensic software allows for the imaging of files in order to preserve file integrity from a source path to a destination path with a corresponding unique code called a hash value (e.g., MD5)

1.3. Image Verifications

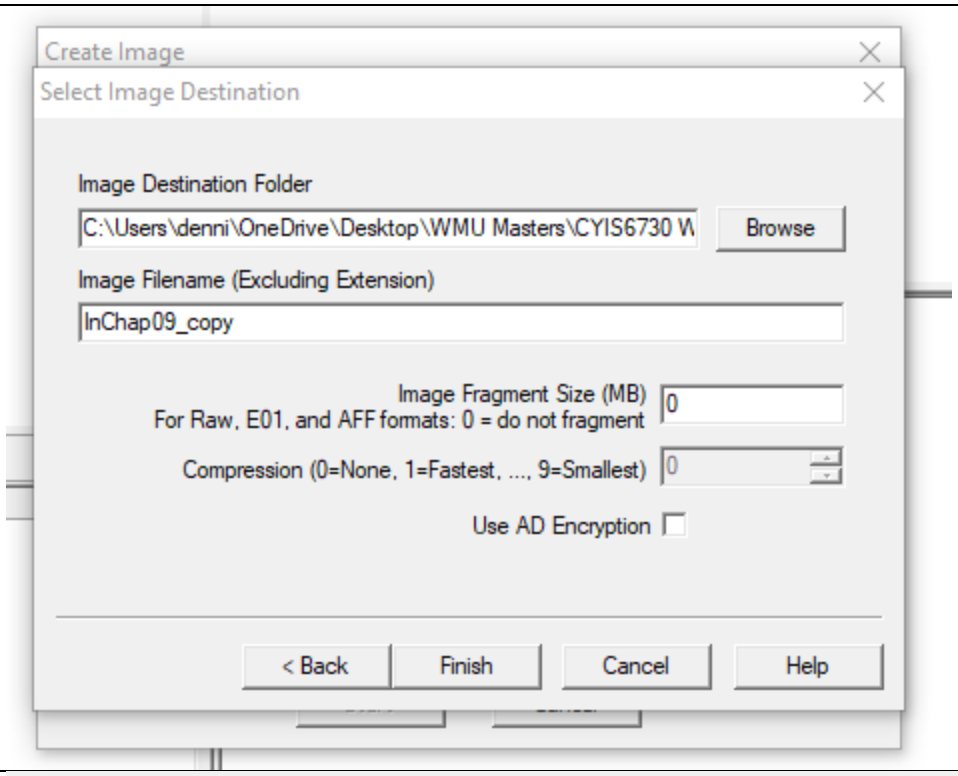
This section outlines Exhibits 3-A to 3-D of the four digital images used in this investigation. Two pieces of corresponding evidence are shown for each. First, Destination Folder is shown along with the Copied Image's file name. Additionally, the instant Examiner utilized no fragmentation which is set with zero "0". Second, the Verify Result page is created showing the corresponding matching hashes. MD5 is preferred and is a widely accepted standard. SHA1 was also computed alongside and is also widely accepted standard.

1.3.1. Matching of Forensic Copies

EXHIBIT 3-A

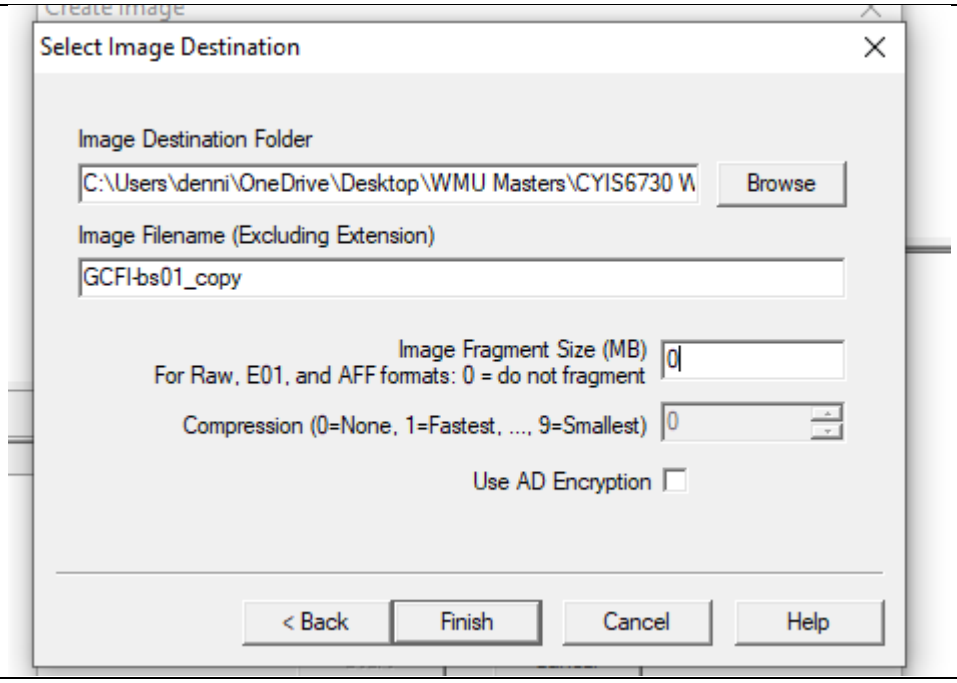
Original Image	**InChap09.dd**
Copied Image	**InChap09_copy.001**
Source Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Downloaded\Lab3-1
Destination Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Downloaded\Forensic Copies
Creation Time	6/9/2022 11:59 PM
Hash (MD5)	**db945a7e3589743923237c0518ababe1**
Hash (SHA1)	**6d87a3665d756b7e22de3d0b087c6ab9ec3f8bf7**

Evidence



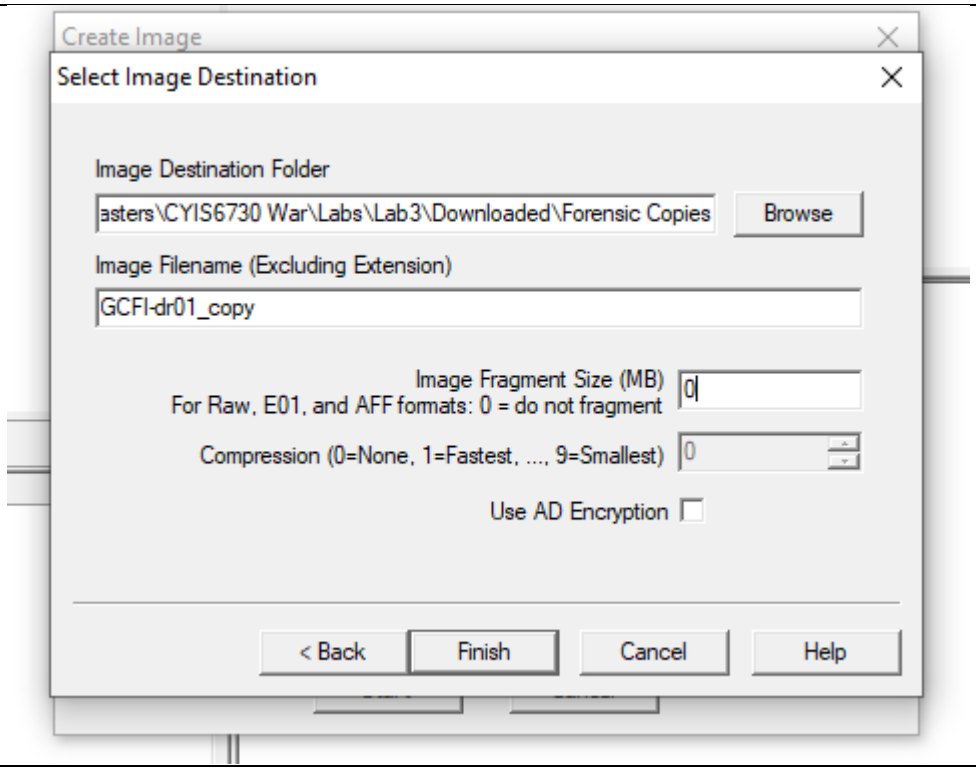
Name	InChap09_copy.001
Sector count	3074048
MD5 Hash	
Computed hash	db945a7e3589743923237c0518ababe1
Report Hash	db945a7e3589743923237c0518ababe1
Verify result	Match
SHA1 Hash	
Computed hash	6d87a3665d756b7e22de3d0b087c6ab9ec3f8bf7
Report Hash	6d87a3665d756b7e22de3d0b087c6ab9ec3f8bf7
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found

EXHIBIT 3-B

Original Image	**GCFI-bs01.E01**
Copied Image	**GCFI-bs01_copy.001**
Source Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Downloaded\Lab3-2
Destination Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Downloaded\Forensic Copies
Creation Time	6/10/2022 12:31 AM
Hash (MD5)	**7ccdac04e1ee276fdd6f435ca538c24a**
Hash (SHA1)	**ef4d1386b6122156b3af55c77e939b109bc89828**
Evidence	

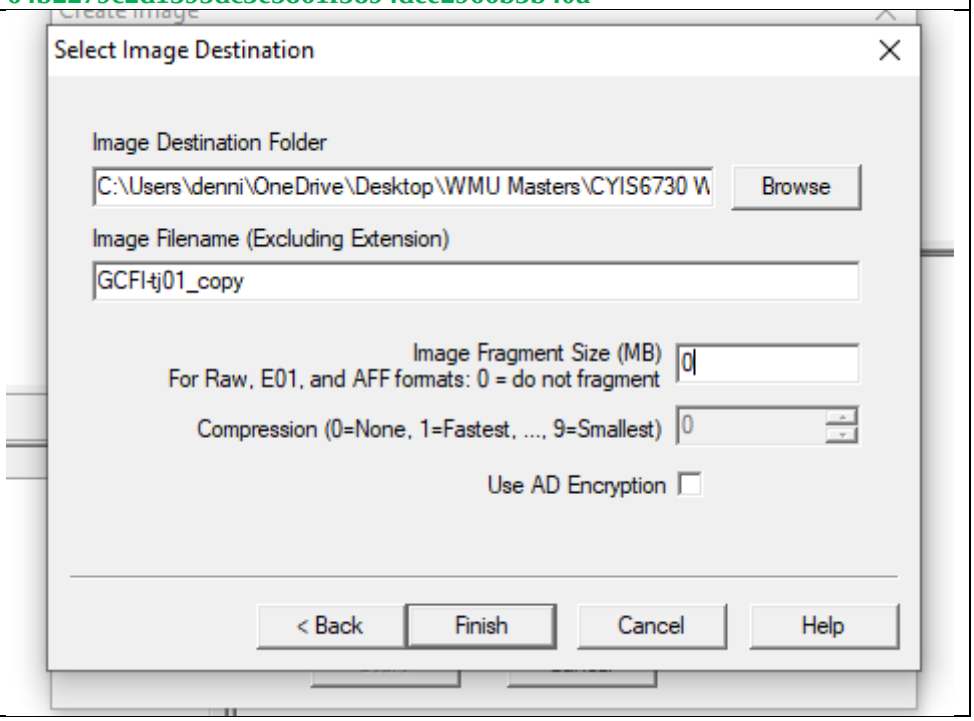
Name	GCFI-bs01_copy.001
Sector count	3074048
MD5 Hash	
Computed hash	7ccdac04e1ee276fdd6f435ca538c24a
Report Hash	7ccdac04e1ee276fdd6f435ca538c24a
Verify result	Match
SHA1 Hash	
Computed hash	ef4d1386b6122156b3af55c77e939b109bc89828
Report Hash	ef4d1386b6122156b3af55c77e939b109bc89828
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found

EXHIBIT 3-C

Original Image	**GCFI-dr01.E01**
Copied Image	**GCFI-dr01_copy.001**
Source Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Downloaded\Lab3-2
Destination Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Downloaded\Forensic Copies
Creation Time	6/10/2022 10:02 PM
Hash (MD5)	**30c3fac1e085e25f1734e7d469c5e2af**
Hash (SHA1)	**5012409fd17c2ec547d1ef703fddee605097689b**
Evidence	

Name	GCFI-dr01_copy.001
Sector count	12288000
MD5 Hash	
Computed hash	30c3fac1e085e25f1734e7d469c5e2af
Report Hash	30c3fac1e085e25f1734e7d469c5e2af
Verify result	Match
SHA1 Hash	
Computed hash	5012409fd17c2ec547d1ef703fddee605097689b
Report Hash	5012409fd17c2ec547d1ef703fddee605097689b
Verify result	Match

EXHIBIT 3-D

Original Image	**GCFI-tj01.001**
Copied Image	**GCFI-tj01_copy.001**
Source Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Downloaded\Lab3-3
Destination Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Downloaded\Forensic Copies
Creation Time	6/10/2022 11:47 PM
Hash (MD5)	**6e3b90b4c41e9b9c262343ff8c0c3008**
Hash (SHA1)	**64b2279c2d1395dc3e5861f5894dee2966b3b40a**
Evidence	

Name	GCFI-tj01_copy.001
Sector count	12285952
MD5 Hash	
Computed hash	6e3b90b4c41e9b9c262343ff8c0c3008
Report Hash	6e3b90b4c41e9b9c262343ff8c0c3008
Verify result	Match
SHA1 Hash	
Computed hash	64b2279c2d1395dc3e5861f5894dee2966b3b40a
Report Hash	64b2279c2d1395dc3e5861f5894dee2966b3b40a
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found

2. HoP 9-2

The purpose of this section is twofold. First the instant Examiner is to set up a hash database that will be used later to perform forensic investigation. Each of the sensitive files will be associated with a unique hash to be uploaded to said hash database. The image of said hard drive herein is InChap09_copy.dd which has had its integrity verified at **Exhibit 3A**, supra.

Second, After set up of the hash database, A Mr. Bob Swartz, an engineering manager at Superior Bicycles, and Mr. Swartz's hard drive with sensitive files is to be forensically and programmatically examined using an Autopsy module. Mr. Swartz's hard drive is associated with GCFI-bs01_copy.E01 which has had its integrity verified at **Exhibit 3B**, supra.

1.4. Tools

∞ **Autopsy on Windows–** Version 4.19.3

According to Sleuthkit.org: "Autopsy® is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools." Further , the instant Examiner utilized a hash database herein to upload MD5 hash values for forensic and programmatic searching of files within large images files. Further still, Autopsy was used to generate an Excel report to extract MD5 hash values.

∞ **Microsoft Excel**

∞ **Microsoft Notepad**

1.5. Deliverables

An excel file was programmatically generated by Autopsy. The screenshots within Exhibit A show a zoomed out view and a zoomed in view, wherein the zoomed in view shows the series of hashes (four (4) unique hashes total). Further, it can be seen that the hashes are accordingly sorted using a multilevel sort. This allows for the viewing of groups and to determine unique number of hashes. Excel's green dotted boarder shows the copying and pasting of values. These values were ultimately entered into a hash database back into Autopsy for programmatic searching.

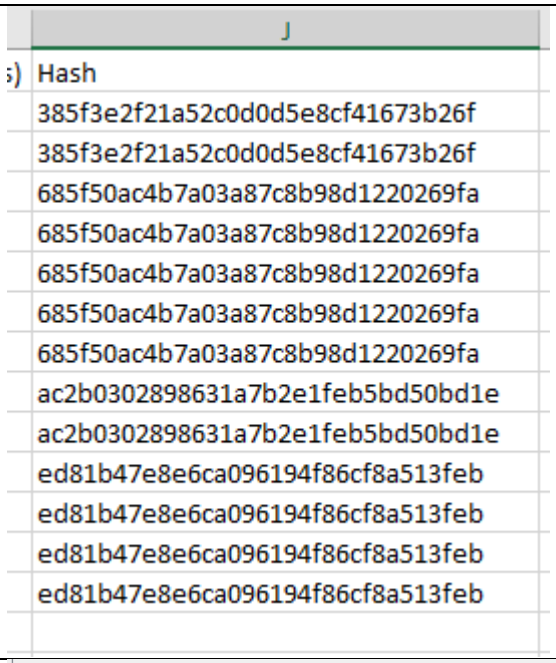
EXHIBIT A Setup and Extraction of Hash Values

File Name	**Excel Set up Hashes**
File Type	 Excel Set up Hashes.xlsx
File Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 1\HoP9-2

Evidence Excel

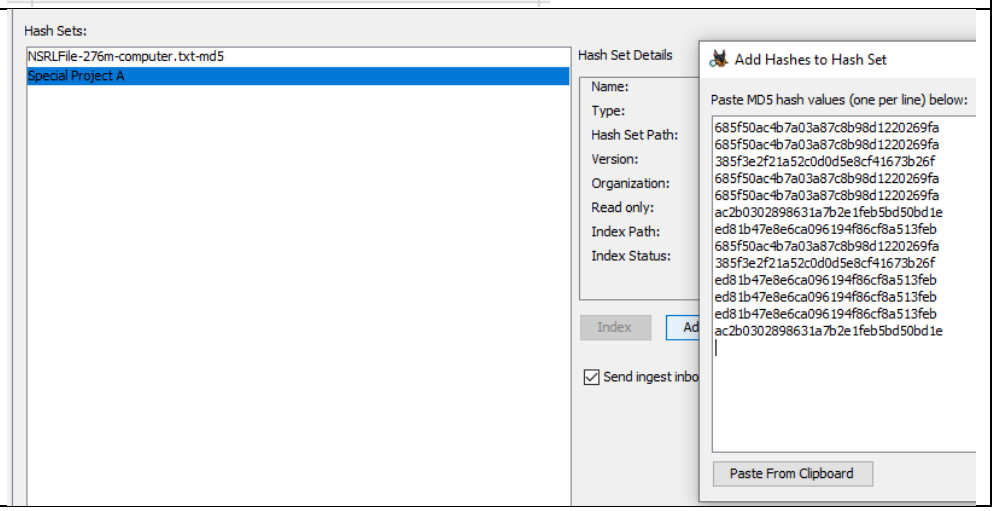
Tag	File	Comment	User Name	Modified Time	Changed Time	Accessed Time	Created Time	Size (Bytes)	Hash
Special Project A	/img_InChap09_copy.001/Users/Bob Swartz/Documents/Outlook Files/bs-superior@outlook.com.pst/Special Project-A (1).JPG		denni	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	55805	68575bac4b7a03a87c6b98d1220206f1a
Special Project A	/img_InChap09_copy.001/Users/Bob Swartz/Documents/Outlook Files/bs-superior@outlook.com.pst/Special Project-A (1).JPG		denni	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	55805	68575bac4b7a03a87c6b98d1220206f1a
Special Project A	/img_InChap09_copy.001/Users/Bob Swartz/Documents/Outlook Files/bs-superior@outlook.com.pst/Special Project-A (2).bmp		denni	2017-06-29 18:41:18 EDT	0000-00-00 00:00:00	2017-07-18 20:14:08 EDT	2017-06-29 18:41:18 EDT	1612854	3835fe2f21a52c0d0d5e8cf41673b26f
Special Project A	/img_InChap09_copy.001/Users/Bob Swartz/Documents/Test/Special Project-A (1).JPG		denni	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	55805	68575bac4b7a03a87c6b98d1220206f1a
Special Project A	/img_InChap09_copy.001/Users/Bob Swartz/Documents/Outlook Files/bs-superior@outlook.com.pst/Special Project-A (1).JPG		denni	2017-04-27 11:18:50 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2017-06-26 18:41:41 EDT	55805	68575bac4b7a03a87c6b98d1220206f1a
Special Project A	/img_InChap09_copy.001/Users/Bob Swartz/Documents/Test/Special Project-A (1).bmp		denni	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	1612854	ac2b0302898831a7b2a1feb5bc50bbd1e
Special Project A	/img_InChap09_copy.001/Users/Bob Swartz/Documents/Outlook Files/bs-superior@outlook.com.pst/Special Project-A (2).JPG		denni	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49519	ed081b47e8e6ca0961944f86cf8a513feb
Special Project A	/img_InChap09_copy.001/Users/Bob Swartz/Documents/Outlook Files/bs-superior@outlook.com.pst/Special Project-A (1).JPG		denni	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	55805	68575bac4b7a03a87c6b98d1220206f1a
Special Project A	/img_InChap09_copy.001/Users/Bob Swartz/Documents/Test/Special Project-A (2).bmp		denni	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	1612854	3835fe2f21a52c0d0d5e8cf41673b26f
Special Project A	/img_InChap09_copy.001/Users/Bob Swartz/Documents/Outlook Files/bs-superior@outlook.com.pst/Special Project-A (2).JPG		denni	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49519	ed081b47e8e6ca0961944f86cf8a513feb
Special Project A	/img_InChap09_copy.001/Users/Bob Swartz/Documents/Test/Special Project-A (2).JPG		denni	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	49519	ed081b47e8e6ca0961944f86cf8a513feb
Special Project A	/img_InChap09_copy.001/Users/Bob Swartz/Documents/Outlook Files/bs-superior@outlook.com.pst/Special Project-A (2).JPG		denni	2017-04-27 11:18:50 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2017-06-26 18:41:41 EDT	49519	ed081b47e8e6ca0961944f86cf8a513feb
Special Project A	/img_InChap09_copy.001/Users/Bob Swartz/Documents/Outlook Files/bs-superior@outlook.com.pst/Special Project-A (1).bmp		denni	2017-06-29 18:38:14 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2017-06-29 18:38:14 EDT	1612854	ac2b0302898831a7b2a1feb5bc50bbd1e

Evidence Zoomed Excel Hashes



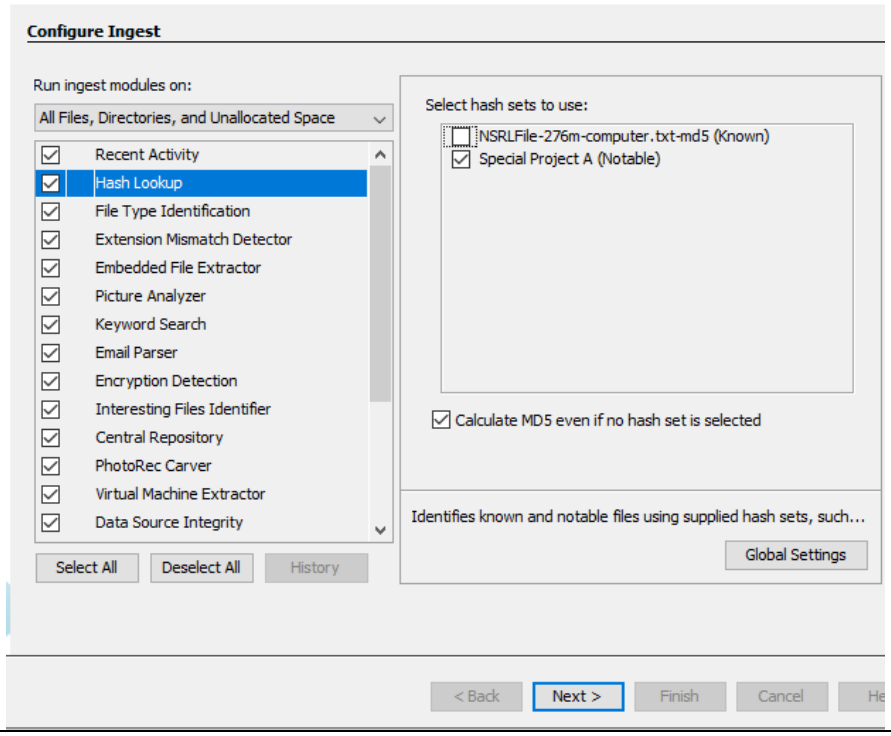
J
Hash
385f3e2f21a52c0d0d5e8cf41673b26f
385f3e2f21a52c0d0d5e8cf41673b26f
685f50ac4b7a03a87c8b98d1220269fa
685f50ac4b7a03a87c8b98d1220269fa
685f50ac4b7a03a87c8b98d1220269fa
685f50ac4b7a03a87c8b98d1220269fa
685f50ac4b7a03a87c8b98d1220269fa
ac2b0302898631a7b2e1feb5bd50bd1e
ac2b0302898631a7b2e1feb5bd50bd1e
ed81b47e8e6ca096194f86cf8a513feb
ed81b47e8e6ca096194f86cf8a513feb
ed81b47e8e6ca096194f86cf8a513feb
ed81b47e8e6ca096194f86cf8a513feb

Evidence Entry into Autopsy from Excel Copy/Paste



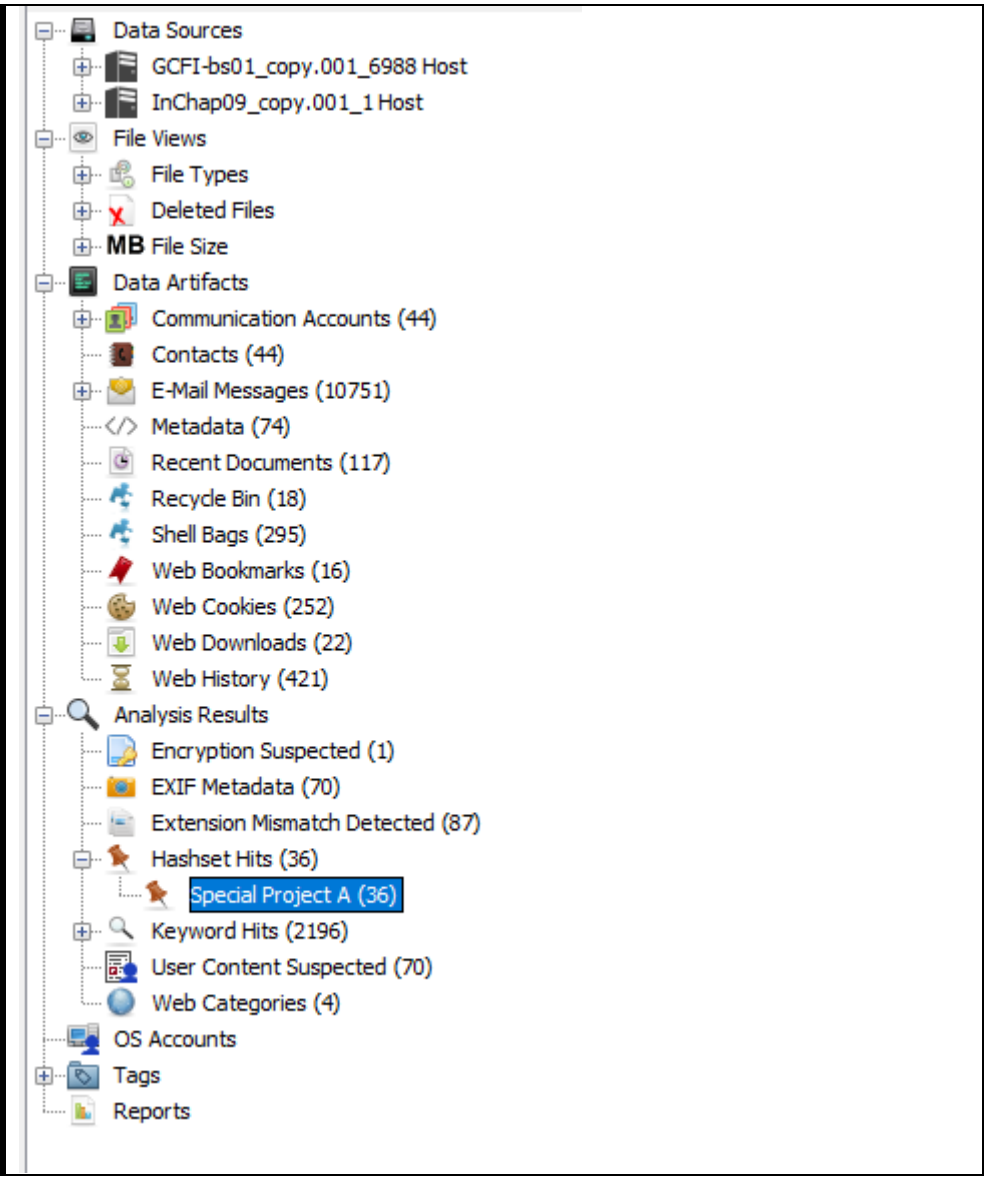
After entry into the hash database. The Examiner set ingest module to search for the sensitive material. The Hashes used were only associated with Special Project A (check), not NSRL (not check). After the module ran, 36 hits were discovered, each associated with only one unique hash.

EXHIBIT B Ingestion and Hits

Software	**Autopsy**
Evidence Ingest[1]	

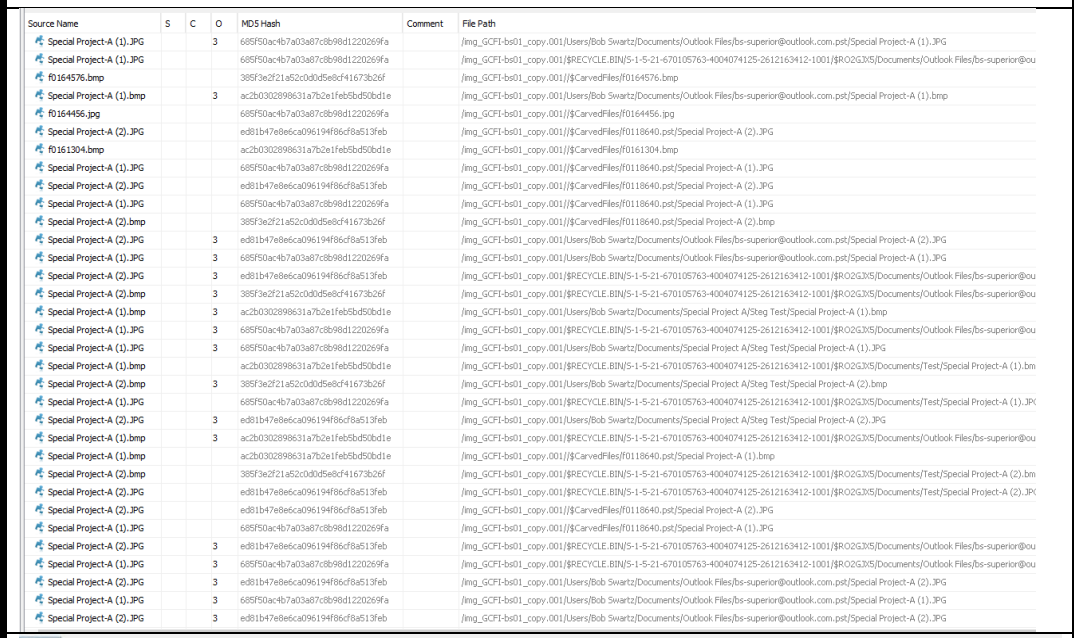
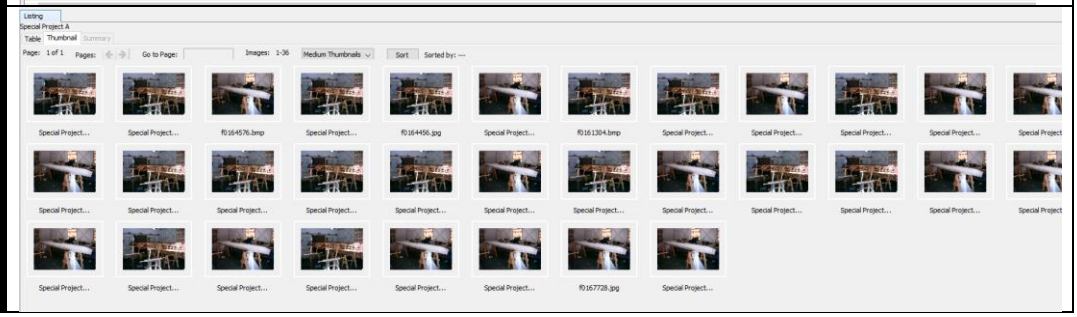
[1] The instant evidence shows all the check boxes check. However, all modules were not run as it was not needed.

Evidence
Hash Hits



The content can be found as listed. Additionally, a thumbnail view can be seen with a myriad of files, each of which match the hashes in the hash database with the sensitive information. Relevant information was extracted with a report generator in the form of Excel which is discussed in the next Exhibit.

EXHIBIT C Laundry List of Hit and Thumbnails (Fig. 3-1 and Step 4)

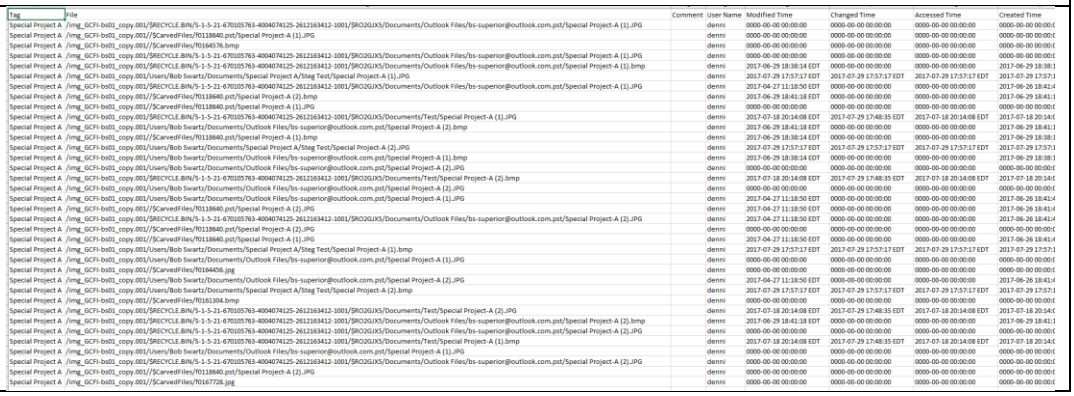
Software	**Autopsy**
Evidence Listing of Hits[2]	
Evidence Thumbnails	

Source Name	S	C	O	MD5 Hash	Comment	File Path
Special Project-A (1).JPG			3	685f50ac4b7a03a87c8b98d1220269fa		/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/Outlook Files/bs-superior@outlook.com.pst/Special Project-A (1).JPG
Special Project-A (1).JPG				685f50ac4b7a03a87c8b98d1220269fa		/img_GCFI-bs01_copy.001/$RECYCLE.BIN/S-1-5-21-670105763-4004074125-2612163412-1001/$RO2GJXS/Documents/Outlook Files/bs-superior@ou
f0164576.bmp				385f3e2f21a52c0d0d5e8cf41673b26f		/img_GCFI-bs01_copy.001/$CarvedFiles/f0164576.bmp
Special Project-A (1).bmp			3	ac2b0302898631a7b2e1feb5bd50bd1e		/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/Outlook Files/bs-superior@outlook.com.pst/Special Project-A (1).bmp
f0164456.jpg				685f50ac4b7a03a87c8b98d1220269fa		/img_GCFI-bs01_copy.001/$CarvedFiles/f0164456.jpg
Special Project-A (2).JPG				ed81b47e8e6ca096194f86cf8a513feb		/img_GCFI-bs01_copy.001/$CarvedFiles/f0118640.pst/Special Project-A (2).JPG
f0161304.bmp				ac2b0302898631a7b2e1feb5bd50bd1e		/img_GCFI-bs01_copy.001/$CarvedFiles/f0161304.bmp
Special Project-A (1).JPG				685f50ac4b7a03a87c8b98d1220269fa		/img_GCFI-bs01_copy.001/$CarvedFiles/f0118640.pst/Special Project-A (1).JPG
Special Project-A (2).JPG				ed81b47e8e6ca096194f86cf8a513feb		/img_GCFI-bs01_copy.001/$CarvedFiles/f0118640.pst/Special Project-A (2).JPG
Special Project-A (1).JPG				685f50ac4b7a03a87c8b98d1220269fa		/img_GCFI-bs01_copy.001/$CarvedFiles/f0118640.pst/Special Project-A (1).JPG
Special Project-A (2).bmp				385f3e2f21a52c0d0d5e8cf41673b26f		/img_GCFI-bs01_copy.001/$CarvedFiles/f0118640.pst/Special Project-A (2).bmp
Special Project-A (2).JPG			3	ed81b47e8e6ca096194f86cf8a513feb		/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/Outlook Files/bs-superior@outlook.com.pst/Special Project-A (2).JPG
Special Project-A (1).JPG			3	685f50ac4b7a03a87c8b98d1220269fa		/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/Outlook Files/bs-superior@outlook.com.pst/Special Project-A (1).JPG
Special Project-A (2).JPG			3	ed81b47e8e6ca096194f86cf8a513feb		/img_GCFI-bs01_copy.001/$RECYCLE.BIN/S-1-5-21-670105763-4004074125-2612163412-1001/$RO2GJXS/Documents/Outlook Files/bs-superior@ou
Special Project-A (2).bmp			3	385f3e2f21a52c0d0d5e8cf41673b26f		/img_GCFI-bs01_copy.001/$RECYCLE.BIN/S-1-5-21-670105763-4004074125-2612163412-1001/$RO2GJXS/Documents/Outlook Files/bs-superior@ou
Special Project-A (1).bmp			3	ac2b0302898631a7b2e1feb5bd50bd1e		/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/Special Project A/Steg Test/Special Project-A (1).bmp
Special Project-A (1).JPG			3	685f50ac4b7a03a87c8b98d1220269fa		/img_GCFI-bs01_copy.001/$RECYCLE.BIN/S-1-5-21-670105763-4004074125-2612163412-1001/$RO2GJXS/Documents/Outlook Files/bs-superior@ou
Special Project-A (1).JPG			3	685f50ac4b7a03a87c8b98d1220269fa		/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/Special Project A/Steg Test/Special Project-A (1).JPG
Special Project-A (1).bmp				ac2b0302898631a7b2e1feb5bd50bd1e		/img_GCFI-bs01_copy.001/$RECYCLE.BIN/S-1-5-21-670105763-4004074125-2612163412-1001/$RO2GJXS/Documents/Test/Special Project-A (1).bm
Special Project-A (2).bmp			3	385f3e2f21a52c0d0d5e8cf41673b26f		/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/Special Project A/Steg Test/Special Project-A (2).bmp
Special Project-A (1).JPG				685f50ac4b7a03a87c8b98d1220269fa		/img_GCFI-bs01_copy.001/$RECYCLE.BIN/S-1-5-21-670105763-4004074125-2612163412-1001/$RO2GJXS/Documents/Test/Special Project-A (1).JP(
Special Project-A (2).JPG			3	ed81b47e8e6ca096194f86cf8a513feb		/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/Special Project A/Steg Test/Special Project-A (2).JPG
Special Project-A (1).bmp			3	ac2b0302898631a7b2e1feb5bd50bd1e		/img_GCFI-bs01_copy.001/$RECYCLE.BIN/S-1-5-21-670105763-4004074125-2612163412-1001/$RO2GJXS/Documents/Outlook Files/bs-superior@ou
Special Project-A (1).bmp				ac2b0302898631a7b2e1feb5bd50bd1e		/img_GCFI-bs01_copy.001/$CarvedFiles/f0118640.pst/Special Project-A (1).bmp
Special Project-A (2).bmp				385f3e2f21a52c0d0d5e8cf41673b26f		/img_GCFI-bs01_copy.001/$RECYCLE.BIN/S-1-5-21-670105763-4004074125-2612163412-1001/$RO2GJXS/Documents/Test/Special Project-A (2).bm
Special Project-A (2).JPG				ed81b47e8e6ca096194f86cf8a513feb		/img_GCFI-bs01_copy.001/$RECYCLE.BIN/S-1-5-21-670105763-4004074125-2612163412-1001/$RO2GJXS/Documents/Test/Special Project-A (2).JP(
Special Project-A (2).JPG				ed81b47e8e6ca096194f86cf8a513feb		/img_GCFI-bs01_copy.001/$CarvedFiles/f0118640.pst/Special Project-A (2).JPG
Special Project-A (1).JPG				685f50ac4b7a03a87c8b98d1220269fa		/img_GCFI-bs01_copy.001/$CarvedFiles/f0118640.pst/Special Project-A (1).JPG
Special Project-A (2).JPG			3	ed81b47e8e6ca096194f86cf8a513feb		/img_GCFI-bs01_copy.001/$RECYCLE.BIN/S-1-5-21-670105763-4004074125-2612163412-1001/$RO2GJXS/Documents/Outlook Files/bs-superior@ou
Special Project-A (1).JPG			3	685f50ac4b7a03a87c8b98d1220269fa		/img_GCFI-bs01_copy.001/$RECYCLE.BIN/S-1-5-21-670105763-4004074125-2612163412-1001/$RO2GJXS/Documents/Outlook Files/bs-superior@ou
Special Project-A (2).JPG			3	ed81b47e8e6ca096194f86cf8a513feb		/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/Outlook Files/bs-superior@outlook.com.pst/Special Project-A (2).JPG
Special Project-A (1).JPG			3	685f50ac4b7a03a87c8b98d1220269fa		/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/Outlook Files/bs-superior@outlook.com.pst/Special Project-A (1).JPG
Special Project-A (2).JPG			3	ed81b47e8e6ca096194f86cf8a513feb		/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/Outlook Files/bs-superior@outlook.com.pst/Special Project-A (2).JPG

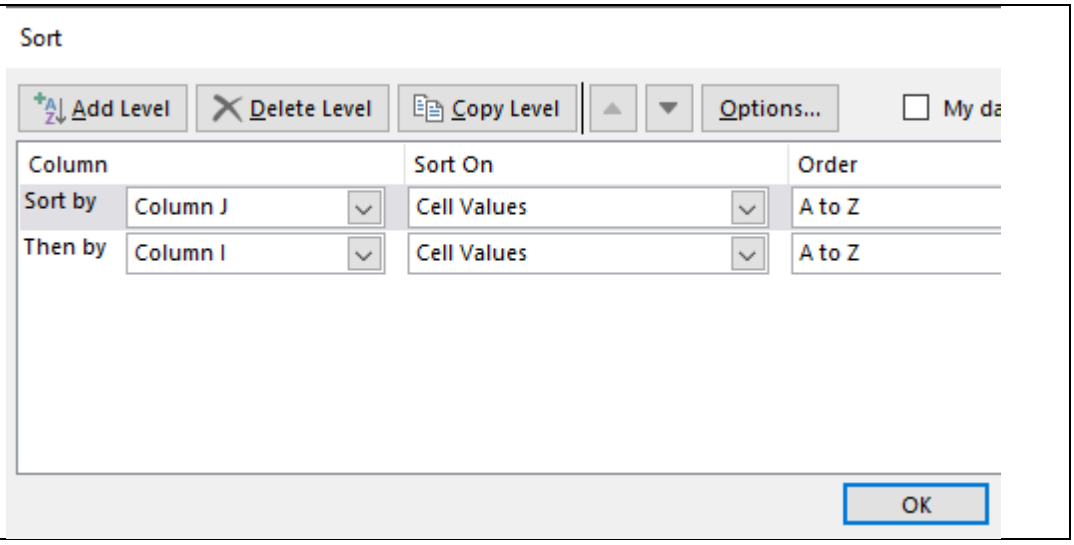
[2] The instant evidence shows all the check boxes check. However, all modules were not run as it was not needed.

After report generation into Excel, the first piece of evidence shows a zoomed out view of Excel prior to sorting. The second piece of evidence shows a sorting. The third piece of evidence is a zoomed in sorted Excel by at least hash value, which allows us to count the total number of unique hashes.

EXHIBIT D Excel Sorting and Confirmation (Fig. 3-2 and Step 7)

Software	**Autopsy** **Excel**
File Name **File Type**	**Proj0902-Report** Proj0902-Report.xlsx
File Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 1\HoP9-2
Evidence Excel Overview	

Evidence Excel Sort



Evidence Excel after Sorting; Ordering Hashes; and Showing 4 Unique Hashes

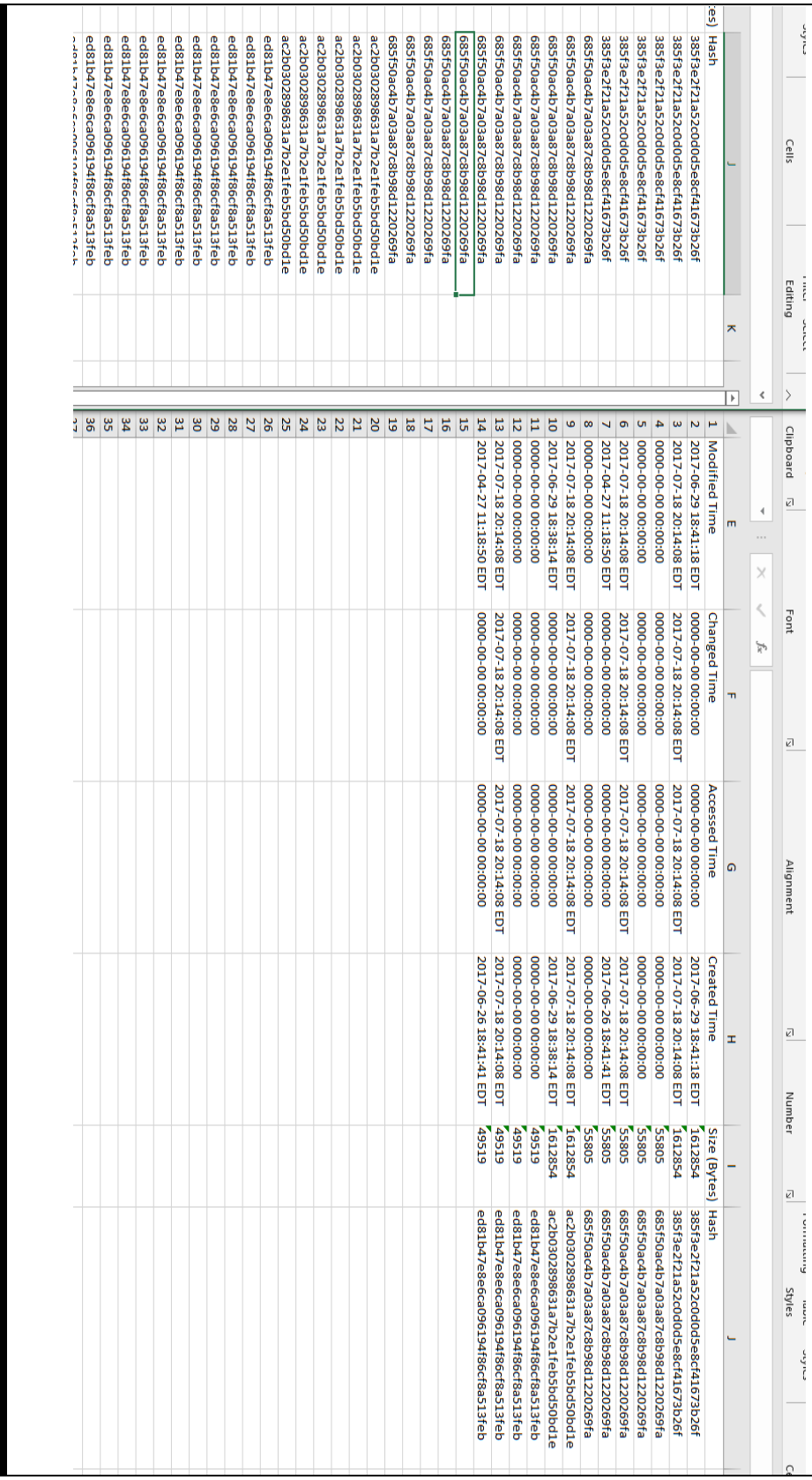
Hash
385f3e2f21a52c0d0d5e8cf41673b26f
385f3e2f21a52c0d0d5e8cf41673b26f
385f3e2f21a52c0d0d5e8cf41673b26f
385f3e2f21a52c0d0d5e8cf41673b26f
385f3e2f21a52c0d0d5e8cf41673b26f
385f3e2f21a52c0d0d5e8cf41673b26f
685f50ac4b7a03a87c8b98d1220269fa
685f50ac4b7a03a87c8b98d1220269fa
685f50ac4b7a03a87c8b98d1220269fa
685f50ac4b7a03a87c8b98d1220269fa
685f50ac4b7a03a87c8b98d1220269fa
685f50ac4b7a03a87c8b98d1220269fa
685f50ac4b7a03a87c8b98d1220269fa
685f50ac4b7a03a87c8b98d1220269fa
685f50ac4b7a03a87c8b98d1220269fa
685f50ac4b7a03a87c8b98d1220269fa
685f50ac4b7a03a87c8b98d1220269fa
685f50ac4b7a03a87c8b98d1220269fa
ac2b0302898631a7b2e1feb5bd50bd1e
ac2b0302898631a7b2e1feb5bd50bd1e
ac2b0302898631a7b2e1feb5bd50bd1e
ac2b0302898631a7b2e1feb5bd50bd1e
ac2b0302898631a7b2e1feb5bd50bd1e
ac2b0302898631a7b2e1feb5bd50bd1e
ed81b47e8e6ca096194f86cf8a513feb
ed81b47e8e6ca096194f86cf8a513feb
ed81b47e8e6ca096194f86cf8a513feb
ed81b47e8e6ca096194f86cf8a513feb
ed81b47e8e6ca096194f86cf8a513feb
ed81b47e8e6ca096194f86cf8a513feb
ed81b47e8e6ca096194f86cf8a513feb
ed81b47e8e6ca096194f86cf8a513feb
ed81b47e8e6ca096194f86cf8a513feb
ed81b47e8e6ca096194f86cf8a513feb
ed81b47e8e6ca096194f86cf8a513feb
ed81b47e8e6ca096194f86cf8a513feb

This exhibit compares and contrasts the two excel files. The excel file on the left side is the report from the suspects drive whereas the excel file on the right is from the set up. The evidence presented is a screenshot of both side by side showing the name number of unique hash values—4 total.

EXHIBIT E Sanity Check

Software	**Autopsy** **Excel**
File Name(s)	**Proj0902-Report; Excel Set up Hashes**
File Type(s)	 Proj0902-Report.xlsx **(Left)**  Excel Set up Hashes.xlsx **(Right)**
File Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 1\HoP9-2

Evidence Side by Side



	J	E	F	G	H	I	J
1	Hash	Modified Time	Changed Time	Accessed Time	Created Time	Size (Bytes)	Hash
2	385f3e2f21a52c0d0d5e8cf41673b26f	2017-06-29 18:41:18 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2017-06-29 18:41:18 EDT	1612854	385f3e2f21a52c0d0d5e8cf41673b26f
3	385f3e2f21a52c0d0d5e8cf41673b26f	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	1612854	385f3e2f21a52c0d0d5e8cf41673b26f
4	385f3e2f21a52c0d0d5e8cf41673b26f	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	55805	685f50ac4b7a03a87c8b98d1220269fa
5	385f3e2f21a52c0d0d5e8cf41673b26f	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	55805	685f50ac4b7a03a87c8b98d1220269fa
6	385f3e2f21a52c0d0d5e8cf41673b26f	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	55805	685f50ac4b7a03a87c8b98d1220269fa
7	385f3e2f21a52c0d0d5e8cf41673b26f	2017-04-27 11:18:50 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2017-06-26 18:41:41 EDT	55805	685f50ac4b7a03a87c8b98d1220269fa
8	685f50ac4b7a03a87c8b98d1220269fa	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	55805	685f50ac4b7a03a87c8b98d1220269fa
9	685f50ac4b7a03a87c8b98d1220269fa	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	1612854	ac2b0302898631a7b2e1feb5bd50bd1e
10	685f50ac4b7a03a87c8b98d1220269fa	2017-06-29 18:38:14 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2017-06-29 18:38:14 EDT	1612854	ac2b0302898631a7b2e1feb5bd50bd1e
11	685f50ac4b7a03a87c8b98d1220269fa	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49519	ed81b47e8e6ca096194f86cf8a513feb
12	685f50ac4b7a03a87c8b98d1220269fa	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	49519	ed81b47e8e6ca096194f86cf8a513feb
13	685f50ac4b7a03a87c8b98d1220269fa	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	2017-07-18 20:14:08 EDT	49519	ed81b47e8e6ca096194f86cf8a513feb
14	685f50ac4b7a03a87c8b98d1220269fa	2017-04-27 11:18:50 EDT	0000-00-00 00:00:00	0000-00-00 00:00:00	2017-06-26 18:41:41 EDT	49519	ed81b47e8e6ca096194f86cf8a513feb
15	685f50ac4b7a03a87c8b98d1220269fa						
16	685f50ac4b7a03a87c8b98d1220269fa						
17	685f50ac4b7a03a87c8b98d1220269fa						
18	685f50ac4b7a03a87c8b98d1220269fa						
19	685f50ac4b7a03a87c8b98d1220269fa						
20	ac2b0302898631a7b2e1feb5bd50bd1e						
21	ac2b0302898631a7b2e1feb5bd50bd1e						
22	ac2b0302898631a7b2e1feb5bd50bd1e						
23	ac2b0302898631a7b2e1feb5bd50bd1e						
24	ac2b0302898631a7b2e1feb5bd50bd1e						
25	ac2b0302898631a7b2e1feb5bd50bd1e						
26	ed81b47e8e6ca096194f86cf8a513feb						
27	ed81b47e8e6ca096194f86cf8a513feb						
28	ed81b47e8e6ca096194f86cf8a513feb						
29	ed81b47e8e6ca096194f86cf8a513feb						
30	ed81b47e8e6ca096194f86cf8a513feb						
31	ed81b47e8e6ca096194f86cf8a513feb						
32	ed81b47e8e6ca096194f86cf8a513feb						
33	ed81b47e8e6ca096194f86cf8a513feb						
34	ed81b47e8e6ca096194f86cf8a513feb						
35	ed81b47e8e6ca096194f86cf8a513feb						
36	ed81b47e8e6ca096194f86cf8a513feb						

This exhibit shows **four unique** files extract even though the files **appear** to be duplicates. The instant Examiner selected four files each associated with a unique hash for inspection. These files were saved locally. The next four thumbnails **appear** to show only two pictures. However, each are different based on file types of .bmp/.jpg.

EXHIBIT F Extraction and Inspection

Software	**Autopsy**
File Name(s)	**15746-Special Project-A (1)** **15825-Special Project-A (1)** **20303-f0164576** **20727-Special Project-A (2)**
File Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 1\HoP9-2\Pictures HoP9-2
File Type(s)	**.jpg and .bmp**
Evidence Selection from Autopsy	

Source Name	S	C	O	MD5 Hash
f0164576.bmp			3	385f3e2f21a52c0d0d5e8cf41673b26f
Special Project-A (2).bmp			3	385f3e2f21a52c0d0d5e8cf41673b26f
Special Project-A (2).bmp			3	385f3e2f21a52c0d0d5e8cf41673b26f
Special Project-A (2).bmp			3	385f3e2f21a52c0d0d5e8cf41673b26f
Special Project-A (2).bmp				385f3e2f21a52c0d0d5e8cf41673b26f
Special Project-A (2).bmp			3	385f3e2f21a52c0d0d5e8cf41673b26f
Special Project-A (1).JPG			3	685f50ac4b7a03a87c8b98d1220269fa
Special Project-A (1).JPG			3	685f50ac4b7a03a87c8b98d1220269fa
f0164456.jpg			3	685f50ac4b7a03a87c8b98d1220269fa
Special Project-A (1).JPG			3	685f50ac4b7a03a87c8b98d1220269fa
Special Project-A (1).JPG			3	685f50ac4b7a03a87c8b98d1220269fa
Special Project-A (1).JPG			3	685f50ac4b7a03a87c8b98d1220269fa
Special Project-A (1).JPG			3	685f50ac4b7a03a87c8b98d1220269fa
Special Project-A (1).JPG			3	685f50ac4b7a03a87c8b98d1220269fa
Special Project-A (1).JPG				685f50ac4b7a03a87c8b98d1220269fa
Special Project-A (1).JPG			3	685f50ac4b7a03a87c8b98d1220269fa
Special Project-A (1).JPG			3	685f50ac4b7a03a87c8b98d1220269fa
Special Project-A (1).JPG			3	685f50ac4b7a03a87c8b98d1220269fa
Special Project-A (1).bmp			3	ac2b0302898631a7b2e1feb5bd50bd1e
f0161304.bmp			3	ac2b0302898631a7b2e1feb5bd50bd1e
Special Project-A (1).bmp			3	ac2b0302898631a7b2e1feb5bd50bd1e
Special Project-A (1).bmp				ac2b0302898631a7b2e1feb5bd50bd1e
Special Project-A (1).bmp			3	ac2b0302898631a7b2e1feb5bd50bd1e
Special Project-A (1).bmp			3	ac2b0302898631a7b2e1feb5bd50bd1e
Special Project-A (2).JPG			3	ed81b47e8e6ca096194f86cf8a513feb
Special Project-A (2).JPG			3	ed81b47e8e6ca096194f86cf8a513feb

15746-Special Project-A (1).jpg	
15825-Special Project-A (1).bmp	

20303-f0164576.bmp	
20727-Special Project-A (2).jpg	

This exhibit, which is the Examiner's personal notes, shows the through process of the differing hash values associated with all four photos, wherein there appears to only be two photos to the human eye.

EXHIBIT G Extraction and Inspection

Software	**Microsoft Notepad**
File Name(s)	**HoP9-2 notes**
File Type	 HoP9-2 notes.txt
File Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 1\HoP9-2

```
.LOG

12:08 AM 6/10/2022 just added hashes to data set from excel
12:25 AM 6/10/2022 examine hard drive from Bob Swartz's who is
engineering man.
12:25 AM 6/10/2022 Calculate md5 hashes while using the custom hash
database
12:45 AM 6/10/2022 Ran ingest and created excel report
12:45 AM 6/10/2022 Performed sorting and found 4 unique hash values
(multilevel sort)
12:45 AM 6/10/2022 Opened up my original excel and also counted 4
unique hashes as sanity check.

12:48 AM 6/10/2022 took picture of side by side
12:56 AM 6/10/2022 tooked at the actual pictures by the human eye
there are only 2 but there are 4 hashes
12:56 AM 6/10/2022 That is, 2 are two pictures but each pictures
has some variant
12:57 AM 6/10/2022 The variant could include stenographic data or
was prepended/postpended attacked in order to preclude hash
searching.
12:59 AM 6/10/2022 Further investigation shows that the 2 photos
are bmp/jpg files That is why the hashes are different at least.
1:00 AM 6/10/2022 Further investigation shows this is correct since
all the bmps for (2) share same hash
       and all the JPG for (1) share the same hash
       and all the (1) for the bmp share the same hash
       and all the (2) for the JPG share the same hash.

1:01 AM 6/10/2022 further investigation is warranted with respect
to the file type of JPG. Is it lossless of lossy compression.
```

1.6. Discussion

The instant files in this investigation represent files that were found on Mr. Bob Swartz's hard drive. Importantly, these files are sensitive files. Four digitally unique files were found, wherein each of the four are associated with a unique digital fingerprint called a hash. Further, to the human eye there appeared to be only two pictures; however, digitally, there were four unique photos given .jpg and .bmp formats. While both .jpg and .bmp are raster-based file types, .jpg has lossy compression methods thereby making the stream of bits different.

As such, since the stream of bits for both files of .jpg/.bmp are different **even though they are derived from the same picture source**, each will produce a different hash value. Foreneisc investigation should not parochially limit hash searches to singular hash values as, during photo transfer and file type conversion, the corresponding hash value **will** change.

For evidence research, hash values not only provide a powerful way to unique identify evidence, but they also allow for computational processing time to be markedly decrease. This is because a hash function is a compression function.[3] That is, for example, SHA-256 will take variable length input, and output a fix length output of 256-bits (hench the name). This compression allows for marked bitwise comparison as it is **not** necessary to do a bitwise comparison over the whole image.

[3] .jpg is compressed. As such, the hash value correspondingly is a compression of compressed data.

3. HoP 9-3

This section will further investigate Mr. Swartz's hard drive is associated with GCFI-bs01_copy.E01 which has had its integrity verified at **Exhibit 3B**, supra. Similar to the previous investigation on his drive, the Examiner will extract hash values and load **additional** hash values for further investigation for Superior Bicycles files of interest.

1.7. Tools

∞ **Autopsy on Windows–** Version 4.19.3

According to Sleuthkit.org: "Autopsy® is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools." Further , the instant Examiner utilized a hash database herein to upload MD5 hash values for forensic and programmatic searching of files within large images files. Further still, Autopsy was used to generate an Excel report to extract MD5 hash values.

∞ **Microsoft Excel**

∞ **Microsoft Notepad**

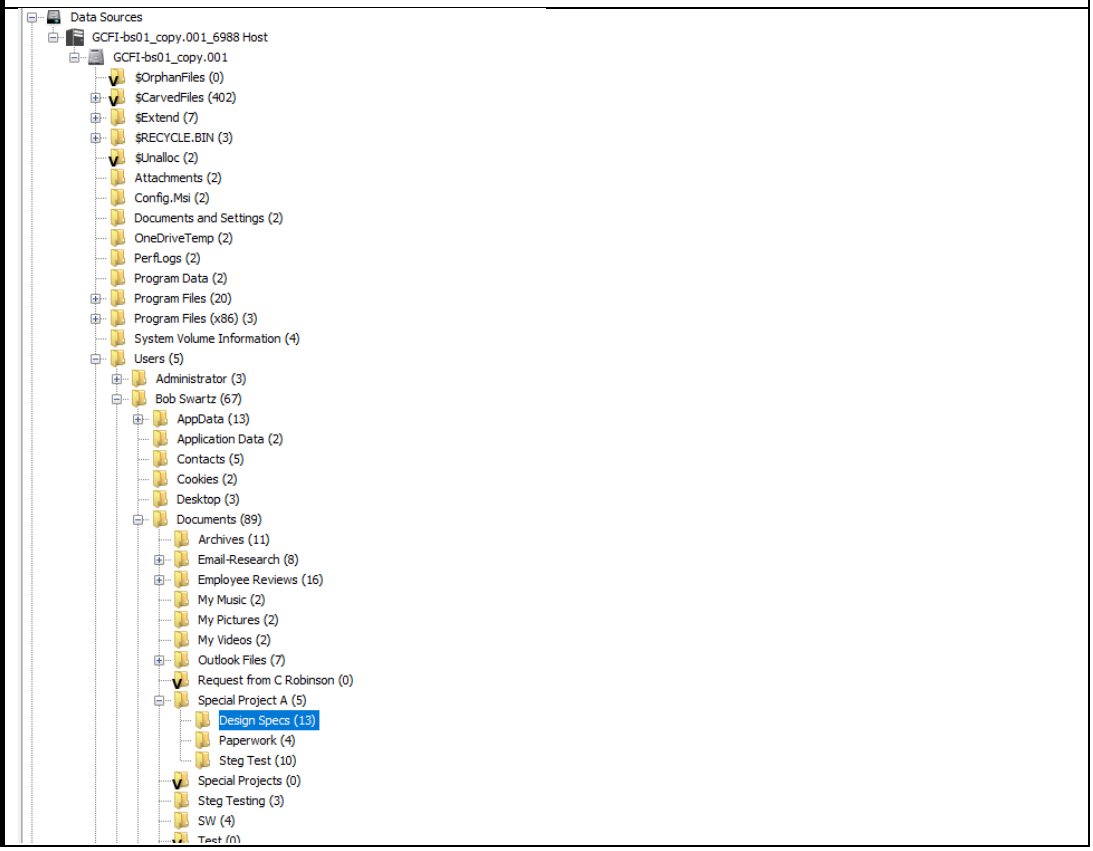
∞ **Kali Linux Subsystem on Windows**

According to Microsoft: "The Windows Subsystem for Linux lets developers run a GNU/Linux environment -- including most command-line tools, utilities, and applications -- directly on Windows, unmodified, without the overhead of a traditional virtual machine or dualboot setup."

1.8. Deliverables

Exhibit below shows the navigation to the important directory associated with Design Specs. Evidence will show the number of files in Design Specs; the contents as a whole; and a zoomed in of said contents with file selection for extraction to Excel via report generation in Autopsy. The files' hashes were associated with, for example, Microsoft Office Word.

EXHIBIT A Gathering Hashes (Fig. 3-3 and Step 4)

Software	**Autopsy**
Evidence File Tree	

Evidence of Contents

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash	SHA-256 Hash	N…
Special Project A-Whiskey-rev01.docx			0	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	15887	Allocated	Allocated	unknown	/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/S…	8854b5688ee27425575f5386224e0c74	a1a52d4a6c36f1cfb751647867ff9eddcb56b3b3b6b435bbe…	a
Special Project A-Whiskey-rev01.docx-slack			0	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	497	Allocated	Allocated	unknown	/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/S…	835977829ed7e5d4eda983e33dc7868e	eb83e1aef91b5a2ef84074c7d4470d7a7b142df740989613…	a
Special Project A-Xray1-rev01.docx			0	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	15854	Allocated	Allocated	unknown	/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/S…	886208c35f54e880282abc11fd707942	7e62163c8c492002a3128800d850a9900b27ce3ac2363c0b…	a
Special Project A-Xray1-rev01.docx-slack			0	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	530	Allocated	Allocated	unknown	/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/S…	120bc01b4688cadcaf28acca2edc6497	e98e4a1c4f8fd13a613808f1f7c6ee826b997d657966542e3…	a
Special Project A-Yankee1-rev01.docx			0	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	15836	Allocated	Allocated	unknown	/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/S…	bc0f267cda949a9a5a44d9b540d3022b	973a3a63ffdb7517314670800da3e8d968c1b9fc6464d6bc…	a
Special Project A-Yankee1-rev01.docx-slack			0	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	548	Allocated	Allocated	unknown	/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/S…	1dc439aca90bbdf4c4c9a31543252fe3	73f10e16a57e80fcd212b6629685e2e19a1d19bf13d34dda…	a
Special Project A-Zebra1-rev01.docx			0	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	15809	Allocated	Allocated	unknown	/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/S…	6f4db27056c7922657babce5fcc7c624	491b4a445e0874f9727cd128a2ec56d64bdb08f64273d0e9…	a
Special Project A-Zebra1-rev01.docx-slack			0	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	575	Allocated	Allocated	unknown	/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/S…	85fe01dd2811e29936f2c71c00ce2217	162f2b3728d3c90944d8db52c2a868628cf5bf629954eede…	a
[current folder]				2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	56	Allocated	Allocated	unknown	/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/S…			
[parent folder]				2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	368	Allocated	Allocated	unknown	/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/S…			
~$ecial Project A-Xray1-rev01.docx				2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	0	Allocated	Allocated	unknown	/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/S…	d41d8cd98f00b204e9800998ecf8427e	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca…	a
~WRL0206.tmp				2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	0	Allocated	Allocated	unknown	/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/S…	d41d8cd98f00b204e9800998ecf8427e	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca…	a
~WRL3521.tmp				2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	2017-07-29 17:57:17 EDT	0	Allocated	Allocated	unknown	/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/S…	d41d8cd98f00b204e9800998ecf8427e	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca…	a

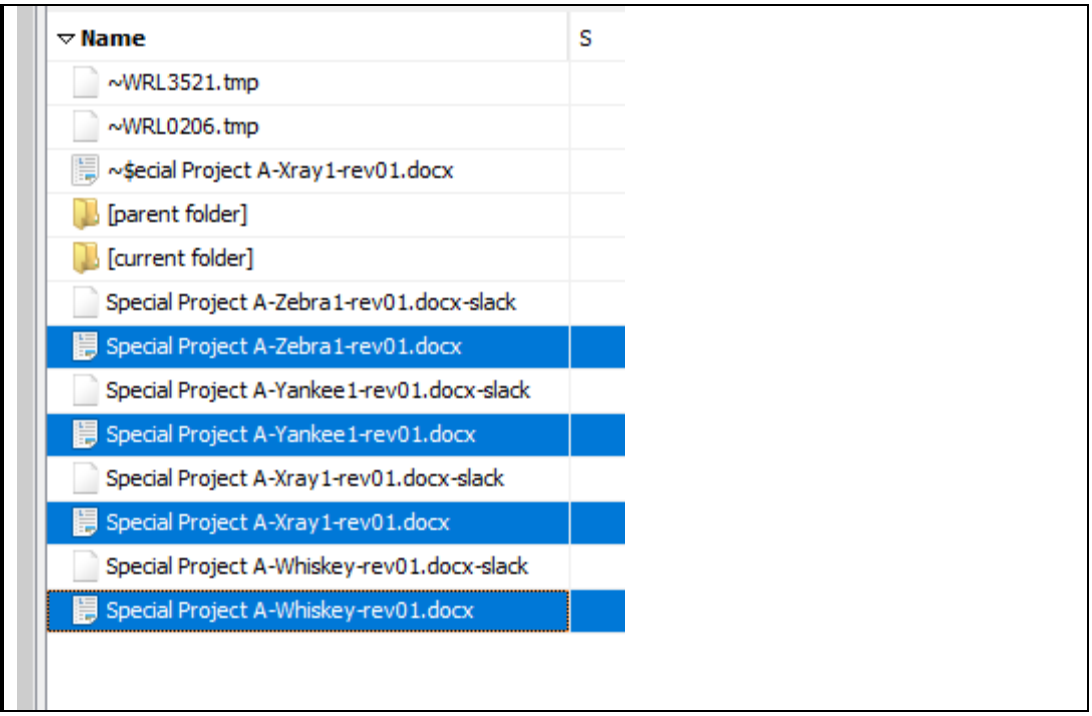
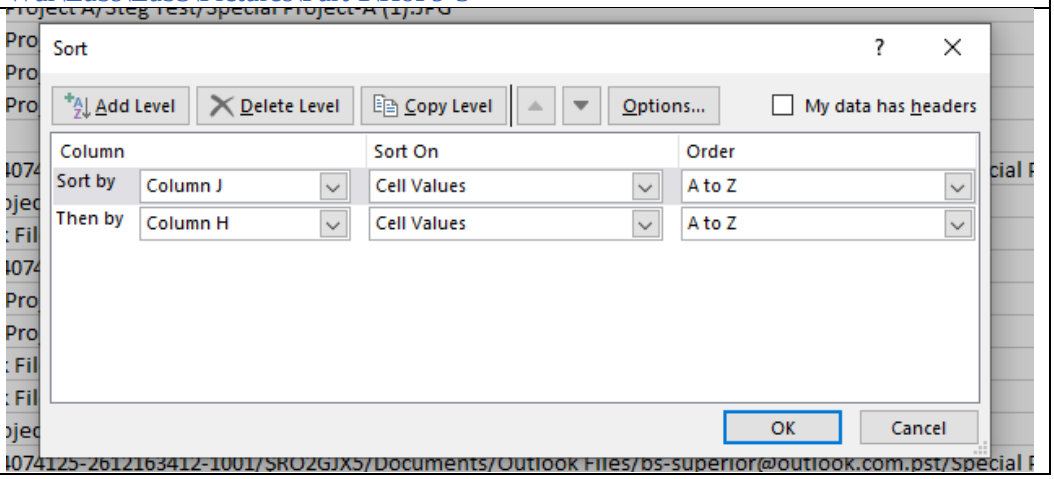
Evidence Selection of Contents for Extraction	

Exhibit below shows the series of steps after extraction within the generated file of Excel from Autopsy. This involves multi-level sorting for viewability and segmentation of hashes. The hash values are ultimately sent to .txt file for further sorting in the next Exhibit.

EXHIBIT B Hash Inspection and Sorting (Fig. 3-4 and Step 7)

Software	**Excel**
File Name(s) **File Type**	**Proj0903-Report** Proj0903-Report.xlsx
File Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 1\HoP9-3
Evidence Excel Sorting	

Evidence After Sorting Hash Column

Size (Bytes)	Hash
1612854	385f3e2f21a52c0d0d5e8cf41673b26f
1612854	385f3e2f21a52c0d0d5e8cf41673b26f
1612854	385f3e2f21a52c0d0d5e8cf41673b26f
1612854	385f3e2f21a52c0d0d5e8cf41673b26f
1612854	385f3e2f21a52c0d0d5e8cf41673b26f
1612854	385f3e2f21a52c0d0d5e8cf41673b26f
55805	685f50ac4b7a03a87c8b98d1220269fa
55805	685f50ac4b7a03a87c8b98d1220269fa
55805	685f50ac4b7a03a87c8b98d1220269fa
55805	685f50ac4b7a03a87c8b98d1220269fa
55805	685f50ac4b7a03a87c8b98d1220269fa
55805	685f50ac4b7a03a87c8b98d1220269fa
55805	685f50ac4b7a03a87c8b98d1220269fa
55805	685f50ac4b7a03a87c8b98d1220269fa
55805	685f50ac4b7a03a87c8b98d1220269fa
55805	685f50ac4b7a03a87c8b98d1220269fa
55805	685f50ac4b7a03a87c8b98d1220269fa
55805	685f50ac4b7a03a87c8b98d1220269fa
15809	6f4db27056c7922657babce5fcc7c624
15887	8854b5688ee27425575f5386224e0c74
15854	886208c35f54e880282abc11fd707942
1612854	ac2b0302898631a7b2e1feb5bd50bd1e
1612854	ac2b0302898631a7b2e1feb5bd50bd1e
1612854	ac2b0302898631a7b2e1feb5bd50bd1e
1612854	ac2b0302898631a7b2e1feb5bd50bd1e
1612854	ac2b0302898631a7b2e1feb5bd50bd1e
1612854	ac2b0302898631a7b2e1feb5bd50bd1e
15836	bc0f267cda949a9a5a44d9b540d3022b
49519	ed81b47e8e6ca096194f86cf8a513feb
49519	ed81b47e8e6ca096194f86cf8a513feb
49519	ed81b47e8e6ca096194f86cf8a513feb
49519	ed81b47e8e6ca096194f86cf8a513feb
49519	ed81b47e8e6ca096194f86cf8a513feb
49519	ed81b47e8e6ca096194f86cf8a513feb
49519	ed81b47e8e6ca096194f86cf8a513feb
49519	ed81b47e8e6ca096194f86cf8a513feb
49519	ed81b47e8e6ca096194f86cf8a513feb
49519	ed81b47e8e6ca096194f86cf8a513feb
49519	ed81b47e8e6ca096194f86cf8a513feb
49519	ed81b47e8e6ca096194f86cf8a513feb

Evidence Copied Excel values into Notepad for .txt analysis

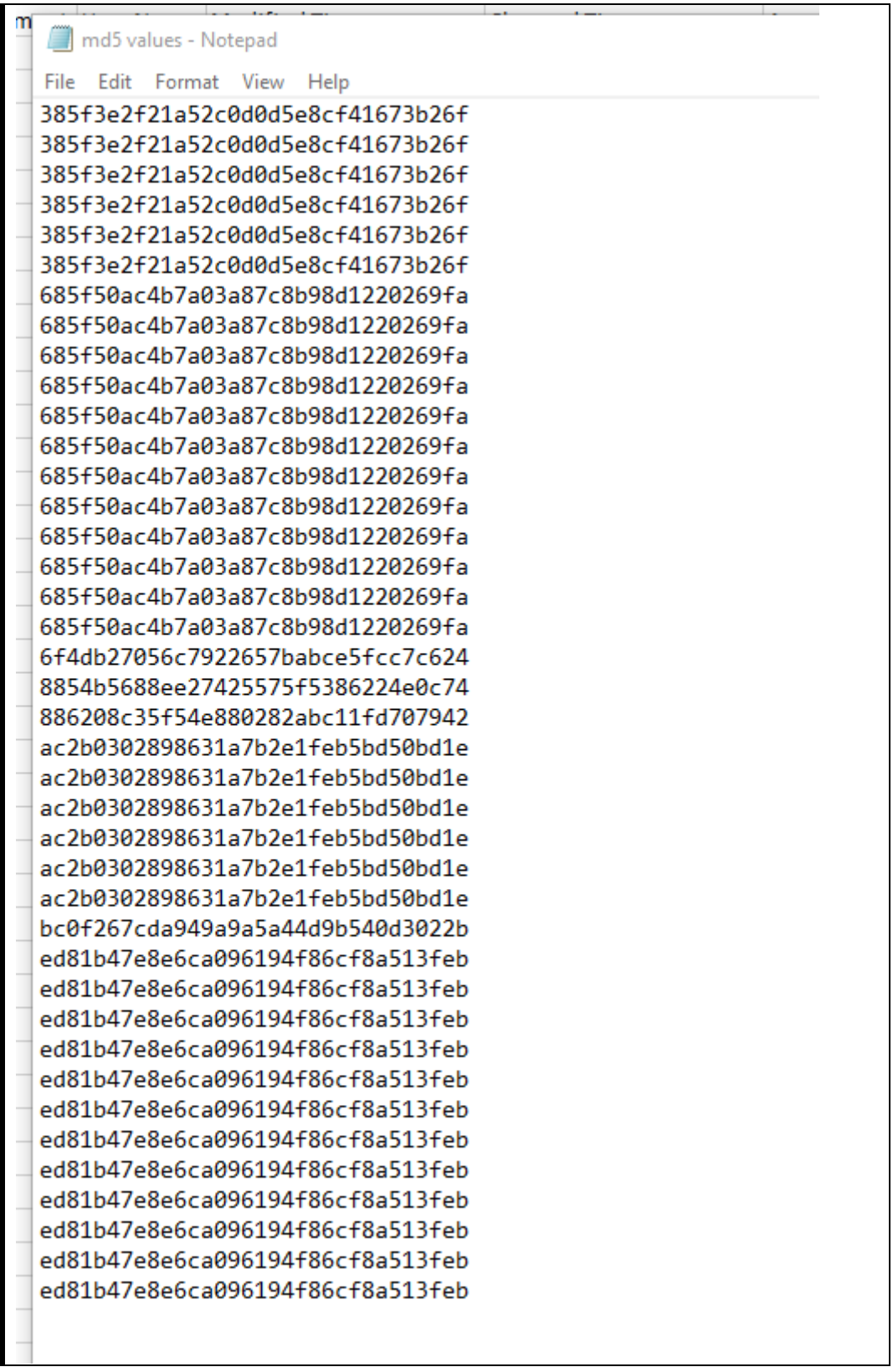
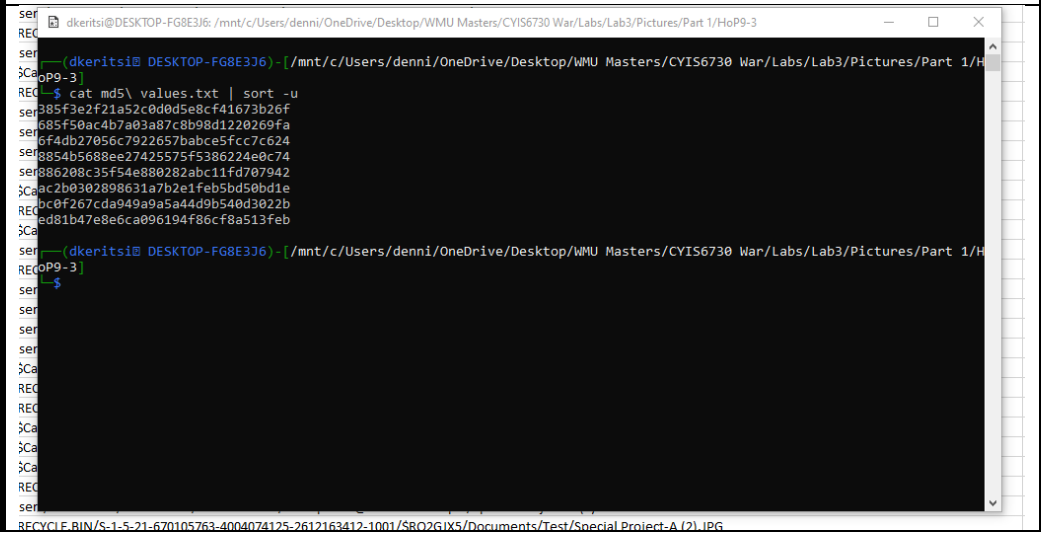
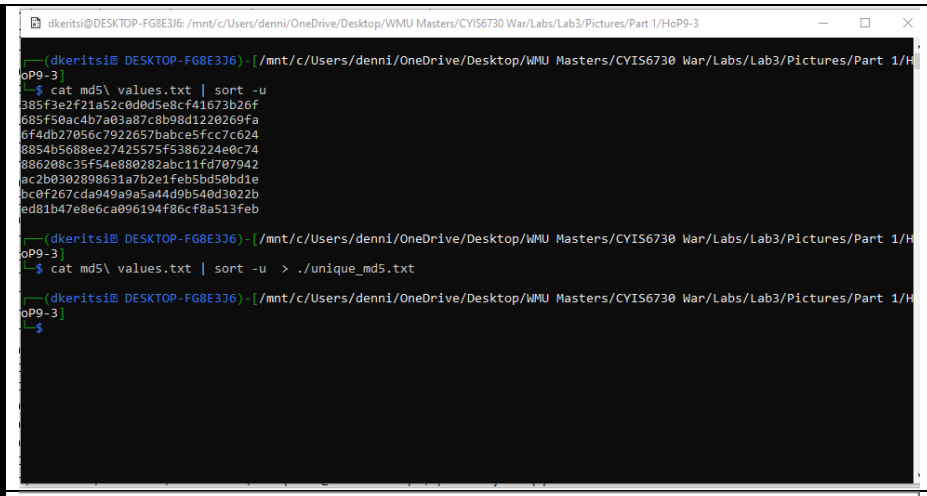
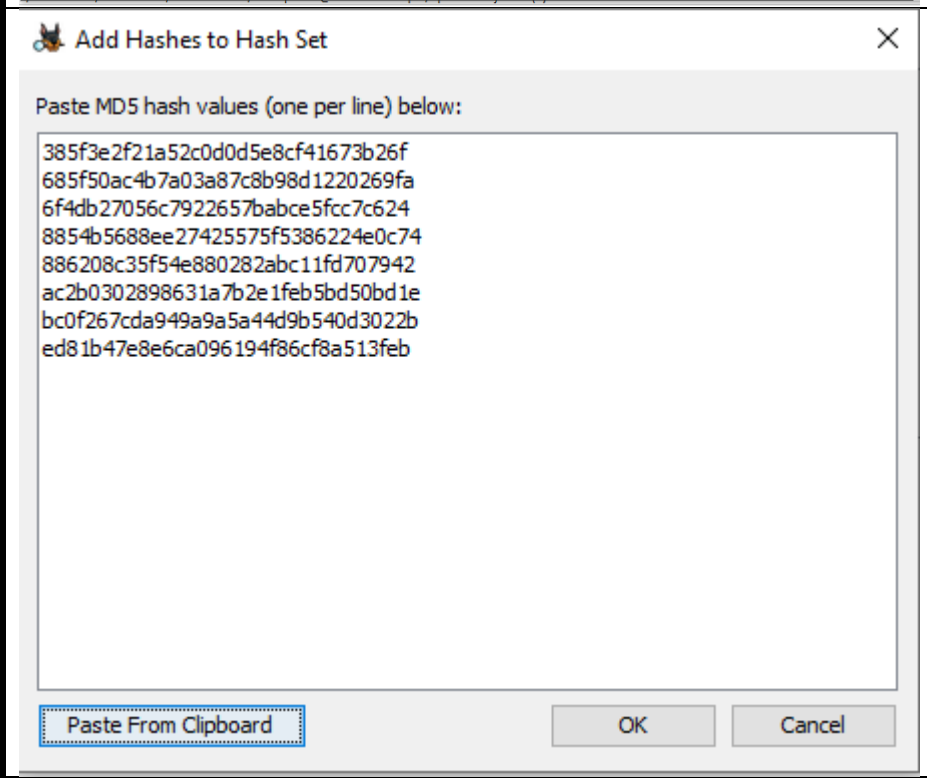


Exhibit below shows the copied excel values in a .txt file for duplication reduction as this will help with a sanity check since it is critical to ensure the database is loaded property for our investigation. The sort -u command allows for sorting with unique only values. This will remove duplicates. The cat command outputs the file .txt contents that is piped to sorting, wherein pipe is represented though a vertical bar "|". Pipe allows for the chaining of commands. Lastly, after ensuring proper output, the redirect and create file command is used ">" with a name of "unique_md5.txt"

EXHIBIT C Removing Duplicates and Adding Hashes (Fig. 3-4 and Step 7)

Software	**Kali Linux Subsystem on Windows; Autopsy**
File Name(s) **File Type**	**md5 values unique_md5**  md5 values.txt  unique_md5.txt
File Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 1\HoP9-3
Evidence Linux Command for Rm of Duplication	

Evidence Linux Command for New File	
Evidence Copy and Paste to Autopsy for DB Load	

After coming across the .jpg and .bmp images, I wanted to check how and why the hash values were different. In the instant case, the files were associated with Word documents. Now, the contents of the Word document (or word processing doc) could be the same whereas the header may be different. This was not the case. The contents were different. But as investigators, we should be aware that a corresponding hash **will** change if we moved from docx format to another word processing format. Importantly, the next Exhibit Shows, at the top, "**Confidential and Trade Secret Information**" in the Word document. (Emphasis added.)

EXHIBIT D Deep Dive

Software	**Autopsy**
Evidence Showing Different Contents at the Top and Header Information at Bottom	

Ultimately, what should be loaded into the database is a total of 8 hash values. According to my sanity check after my Kali Linux processing, this is what the Examiner found.

EXHIBIT E Examiner Forensic Notes

Software	**Microsoft Notepad**
File Name(s)	**Forensic Notes HoP9-3**
File Type	Forensic Notes HoP9-3.txt
File Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 1\HoP9-3

```
.LOG

9:20 PM 6/10/2022 Start time
9:21 PM 6/10/2022 Add hash values to our DB
9:35 PM 6/10/2022 It wants us to add the md5 values now
9:35 PM 6/10/2022 instructions now deviate from the book since Dr.
Rea (our client) doesn't want us to start more projects
9:35 PM 6/10/2022 after sorting need to filter out string of unique
values
9:40 PM 6/10/2022 Used Kali linux to CAT my output (since I really
hate windows)
9:41 PM 6/10/2022 But First saved the hashes to .txt and CAT that
.txt with a sort -u
9:43 PM 6/10/2022 showing unique MD5
9:44 PM 6/10/2022 need to do sanity check with number of md5 they
asked for four (4) so I should have (8), which I do.

--Deep Dive
9:50 PM 6/10/2022 Need to do some research as to why the hashes
differ
9:57 PM 6/10/2022 they differ because they are very unique files
```

1.9. Discussion

These files represent sensitive information since the emails represented above relate to Confidential and Secret information associated with bicycles. Accordingly, a forensic investigator will be able to save a corresponding hash value for future tracking. However, as noted above, if and when the file format changes the hash **will** change too. Also as noted above, the hash values allow for unique file identification, but most importantly, since hash functions are compression functions, they will allow significate computation increase of time since that the number of bits is much smaller than the total file's number of bits. This will allow forensic investigator to traverse large swaths of data over many images.

4. HoP 9-4

This section will further investigate a different image that is associated with GCFI-dr01.E01, which has had its integrity verified at **Exhibit 3C**, supra. The investigation continues to be centered around Superior Bicycles Inc. However, in this case personal files with PII will be discussed. Some file formats include PDF, ODS (which is similar to Excel), and ODT file types (which is similar to Microsoft Word). As to the contents, some emails in Memorandum Form[4] discussed firing Mr. Jim Shu per the request of Sam Clemens.

1.10. Tools

∞ **Autopsy on Windows–** Version 4.19.3

According to Sleuthkit.org: "Autopsy® is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools." Further , the instant Examiner utilized a hash database herein to upload MD5 hash values for forensic and programmatic searching of files within large images files. Further still, Autopsy was used to generate an Excel report to extract MD5 hash values.

∞ **Microsoft Excel**

∞ **Microsoft Word**

∞ **Microsoft Notepad**

∞ **Kali Linux Subsystem on Windows**

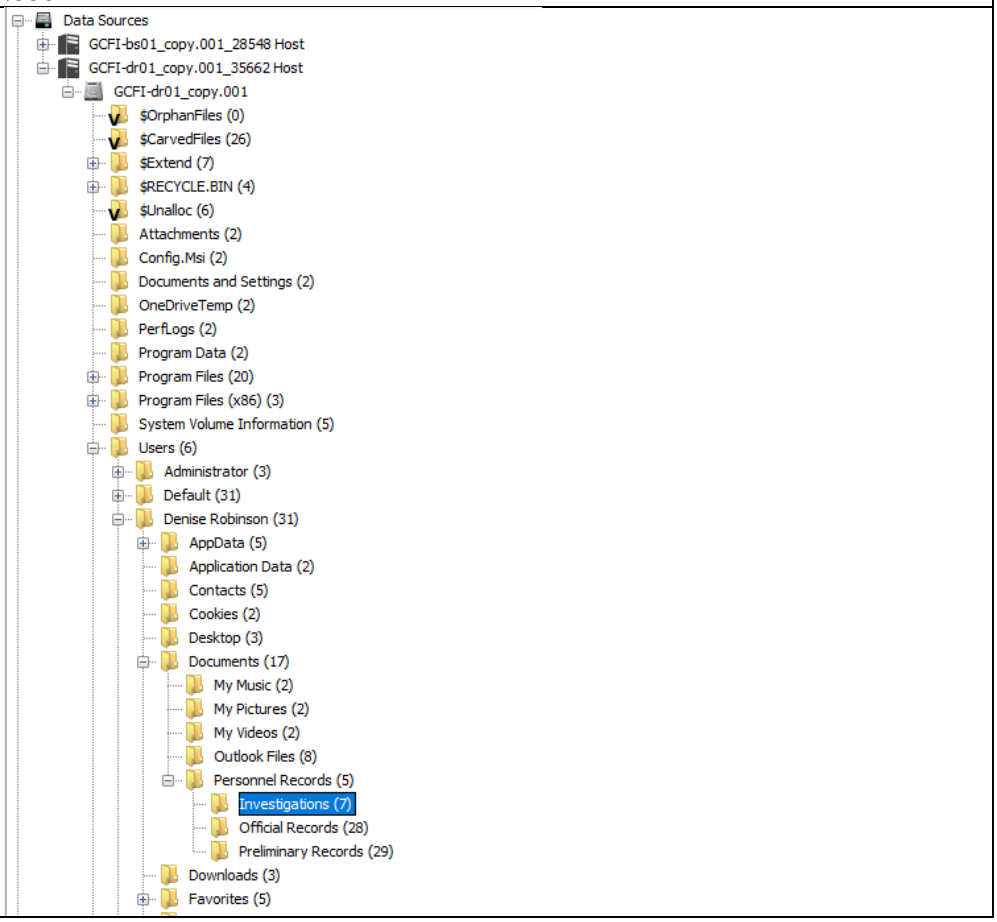
According to Microsoft: "The Windows Subsystem for Linux lets developers run a GNU/Linux environment -- including most command-line tools, utilities, and applications -- directly on Windows, unmodified, without the overhead of a traditional virtual machine or dualboot setup."

[4] These were extracted on to Windows Local machine. Accordingly, file format saved was Word from ODT.

1.11. Deliverables

This Exhibit shows the Investigations subdirectory and .odt files therein. The .odt files were extracted to examine the contents therein. Said contents includes the Termination of Jim Shu for lying per the request of Sam Clemens. Ultimately, these files were extracted and are discussed in the next Exhibit.

EXHIBIT A Investigations Sub Directory (Fig. 3-5 and Step 5)

Software	**Autopsy**
File Name(s)	**43716-Memo-Clemens; 43720-Memo-CRobinson**
File Type	**.odt**
Evidence Tree View	

Evidence
.odt files

Name	S	C	O	Modified Time	Change
[parent folder]				2017-07-30 16:05:44 EDT	2017-07
[current folder]				2017-07-29 18:01:14 EDT	2017-07
Memo-Clemens.odt			0	2017-07-29 18:01:14 EDT	2017-07
Memo-Clemens.odt-slack			0	2017-07-29 18:01:14 EDT	2017-07
Memo-CRobinson.odt			0	2017-07-29 18:01:14 EDT	2017-07
Memo-CRobinson.odt-slack			0	2017-07-29 18:01:14 EDT	2017-07
~$mo-Clemens.odt				2017-07-29 18:01:14 EDT	2017-07

This Exhibit shows .odt files and discussions from Sam Clemens and then from CEO Chris Robinson with respect to Jim Chu; his conduct; and his termination. Interestingly, the Memos are dated Dec. 1st 2016 whereas the Header data in each is dated in 2017. Files were added to the Hash DB.

EXHIBIT B Extraction and Investigation of ODT files

Software	**Autopsy**
File Name(s)	**43716-Memo-Clemens; 43720-Memo-CRobinson;**
File Type	 43716-Memo-Clemens.odt  43720-Memo-CRobinson.odt  5-Memo_clemens.odt.  6-Mem-robinson.odt.t
File Path	For ODT in Word: C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 1\HoP9-4 For ODT: C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 1\HoP9-4\Pictures
Evidence 43716-Memo-Clemens	**Memorandum** To: Chris Robinson, CEO & President of Superior, Inc. CC: Ralph Benson, General Counsel, Superior, Inc. Denise Robinson, HR Manager, Superior, Inc. From: Sam Clemens, Senior Advertising & Marketing Manager, Superior, Inc. Date: December 1, 2016 Subject: Termination of Jim Shu On November 20th of this year it was reported that Jim Shu had lied about our delivery schedule to our largest client. When I was contacted by our client, he was very upset that Jim had made promises to him that we would not be able to keep. In addition to this incident I have had three other similar incidents that I've documented with Jim's behavior. Each previous incident I counseled him on the matter. At this time I recommend that we terminate Jim Shu for this and previous problems with customers. We can not afford an employee to violate the trust of our customers.

Evidence 43720-Memo-CRobinson

Memorandum

To: Denise Robinson, HR Manager, Superior, Inc.
CC: Ralph Benson, General Counsel, Superior, Inc.
Sam Clemens, Senior Advertising & Marketing Manager, Superior, Inc.
From: Chris Robinson, CEO & President of Superior, Inc.
Date: December 1, 2016
Subject: RE: Termination of Jim Shu

Please proceed with the recommendation from Sam the termination of Jim Shu.

Evidence 5-Memo_clemens.odt

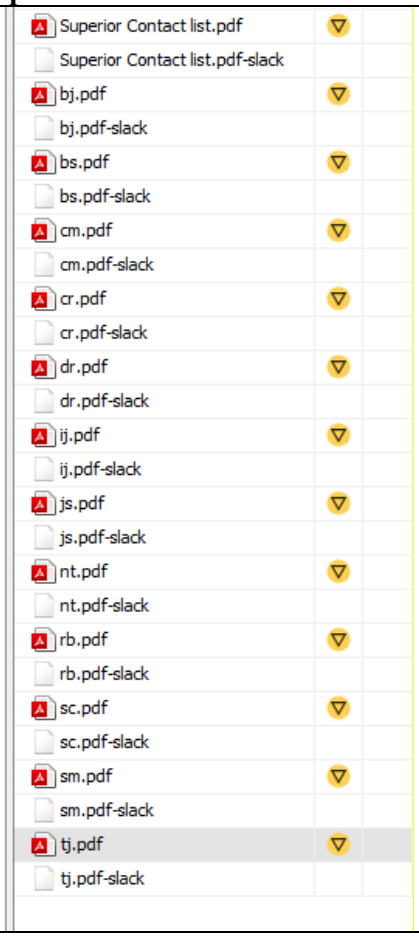
```
-------------------------------METADATA-------------------------------
---

Character Count: 863
Content-Type: application/vnd.oasis.opendocument.text
Creation-Date: 2017-07-29T14:15:35.767846957
Edit-Time: PT11M44S
Image-Count: 0
Last-Modified: 2017-07-29T14:27:19.663195014
Last-Save-Date: 2017-07-29T14:27:19.663195014
Object-Count: 0
Page-Count: 1
Paragraph-Count: 12
Table-Count: 0
Word-Count: 147
X-Parsed-By: org.apache.tika.parser.DefaultParser
date: 2017-07-29T14:27:19.663195014
dcterms:created: 2017-07-29T14:15:35.767846957
dcterms:modified: 2017-07-29T14:27:19.663195014
editing-cycles: 1
generator: LibreOffice/5.1.6.2$Linux_X86_64
LibreOffice_project/10m0$Build-2
meta:character-count: 863
meta:creation-date: 2017-07-29T14:15:35.767846957
meta:image-count: 0
meta:object-count: 0
meta:page-count: 1
meta:paragraph-count: 12
meta:save-date: 2017-07-29T14:27:19.663195014
meta:table-count: 0
meta:word-count: 147
modified: 2017-07-29T14:27:19.663195014
nbCharacter: 863
nbImg: 0
nbObject: 0
```

Evidence 6- Mem-robinson.odt Metadata	nbPage: 1 nbPara: 12 nbTab: 0 nbWord: 147 xmpTPg:NPages: 1 ----------METADATA---------- --- Character Count: 369 Content-Type: application/vnd.oasis.opendocument.text Creation-Date: 2017-07-29T14:15:35.767846957 Edit-Time: PT15M47S Image-Count: 0 Last-Modified: 2017-07-29T14:31:22.811987491 Last-Save-Date: 2017-07-29T14:31:22.811987491 Object-Count: 0 Page-Count: 1 Paragraph-Count: 8 Table-Count: 0 Word-Count: 55 X-Parsed-By: org.apache.tika.parser.DefaultParser date: 2017-07-29T14:31:22.811987491 dcterms:created: 2017-07-29T14:15:35.767846957 dcterms:modified: 2017-07-29T14:31:22.811987491 editing-cycles: 2 generator: LibreOffice/5.1.6.2$Linux_X86_64 LibreOffice_project/10m0$Build-2 meta:character-count: 369 meta:creation-date: 2017-07-29T14:15:35.767846957 meta:image-count: 0 meta:object-count: 0 meta:page-count: 1 meta:paragraph-count: 8 meta:save-date: 2017-07-29T14:31:22.811987491 meta:table-count: 0 meta:word-count: 55 modified: 2017-07-29T14:31:22.811987491 nbCharacter: 369 nbImg: 0 nbObject: 0 nbPage: 1 nbPara: 8 nbTab: 0 nbWord: 55 xmpTPg:NPages: 1

This Exhibit shows the subdirectory of Official Records. The files were opened. The Superior Contact List has important information for Forensic reconnaissance as it has a list of emails that may be used in the future. Files were added to the hash DB.

EXHIBIT C Official Records Sub Directory (Fig. 3-6 and Step 7)

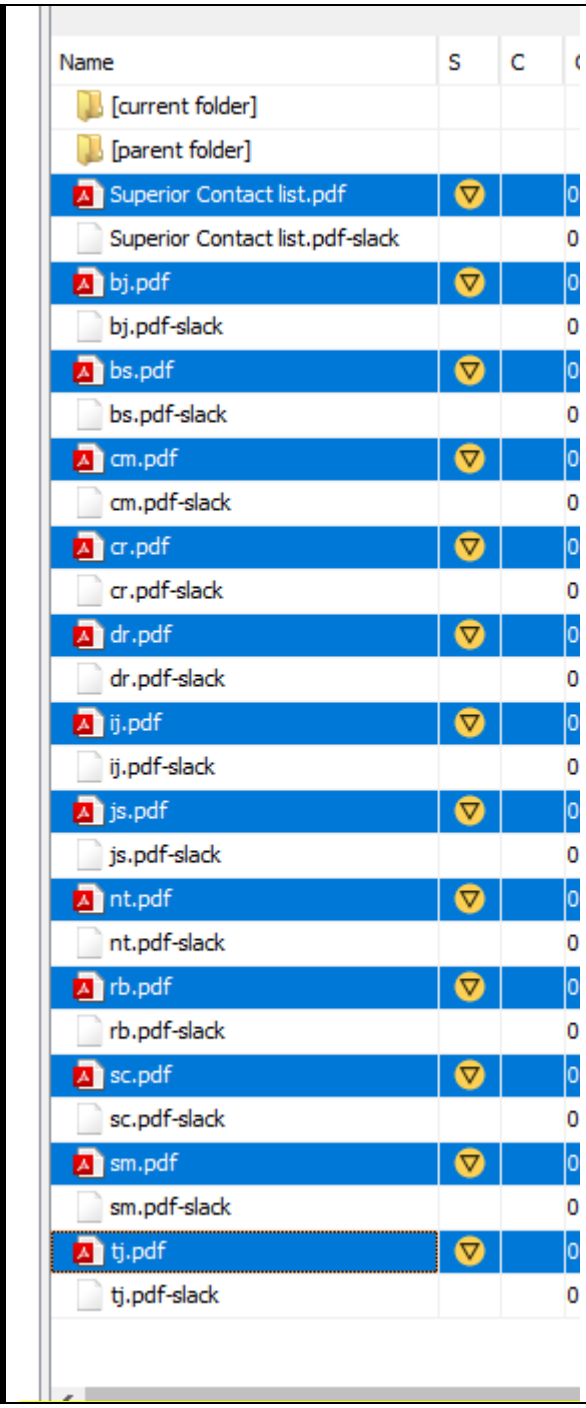
Software	**Autopsy**
File Name(s)	**E.g. Superior Contact list.pdf**
File Type	**.pdf**
Evidence Showing Files in Directory	

Evidence Opened PDF of Superior Contact List

Superior Contact list

First Name	Last Name	Company	Job Title	E-mail Address
Bart	Jones	Superior	Sales Manager	bj-superior@outlook.com
Bob	Swartz	Superior	Engineering Manager	bs-superior@outlook.com
Chris	Murphy	Superior	Marketing Manager	cm-superior@outlook.com
Chris	Robinson	Superior	President	cr-superior@outlook.com
Denise	Robinson	Superior	Personnel Manager	dr-superior@outlook.com
Ileen	Johnson	Superior	Controller	ij-superior@outlook.com
Tom	Johnson	Superior	Sales Rep	tj-superior@mail.com
Nau	Tjeriko	Superior	Regional Marketing Manager	nt-superior@outlook.com
Ralph	Benson	Superior	General Counsel	rb-superior@outlook.com
Sam	Clemens	Superior	Advertising & Marketing	sc-superior@outlook.com
Sebastian	Mwaqngonde	Superior	International Sales Rep	sm-superior@outlook.com

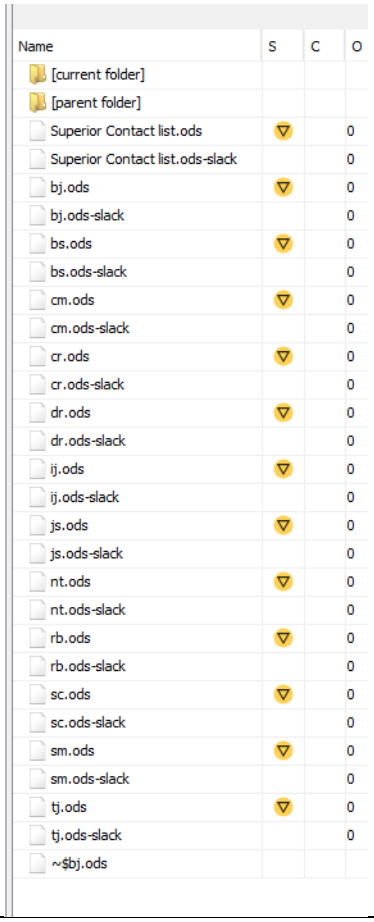
Evidence Selecting File for Report Generation for Hash DB



This Exhibit shows the subdirectory of Preliminary Records. The files were opened. The Superior Contact List has important information for Forensic reconnaissance as it has a list of emails that may be used in the future. The .ods extension is very similar to Excel. Files were added to the hash DB.

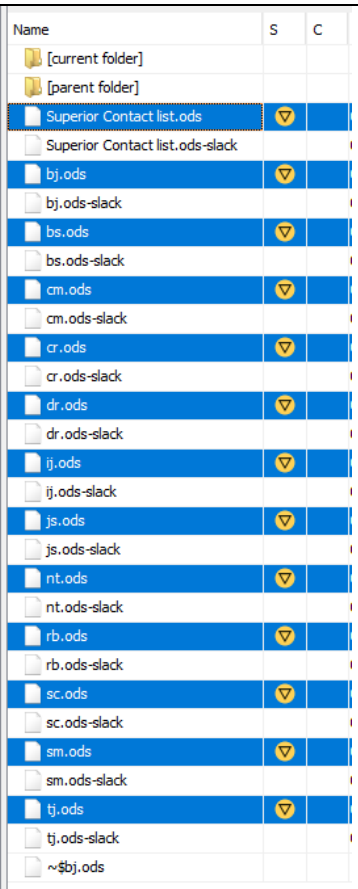
EXHIBIT D Preliminary Records Sub Directory (Fig. 3-7 and Step 9)

Software	**Autopsy**
File Name(s)	**Superior Contact list.ods**
File Type	 Superior Contact list.ods
File Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 1\HoP9-4



Name	S	C	O
[current folder]			
[parent folder]			
Superior Contact list.ods			0
Superior Contact list.ods-slack			0
bj.ods			0
bj.ods-slack			0
bs.ods			0
bs.ods-slack			0
cm.ods			0
cm.ods-slack			0
cr.ods			0
cr.ods-slack			0
dr.ods			0
dr.ods-slack			0
ij.ods			0
ij.ods-slack			0
js.ods			0
js.ods-slack			0
nt.ods			0
nt.ods-slack			0
rb.ods			0
rb.ods-slack			0
sc.ods			0
sc.ods-slack			0
sm.ods			0
sm.ods-slack			0
tj.ods			0
tj.ods-slack			0
~$bj.ods			

Evidence Selecting for Extraction



Evidence .ods extension after Extraction

First Name	Last Name	Company	Job Title	E-mail Address
Bart	Jones	Superior	Sales Manager	bj-superior@outlook.com
Bob	Swartz	Superior	Engineering Manager	bs-superior@outlook.com
Chris	Murphy	Superior	Marketing Manager	cm-superior@outlook.com
Chris	Robinson	Superior	President	cr-superior@outlook.com
Denise	Robinson	Superior	Personnel Manager	dr-superior@outlook.com
Ileen	Johnson	Superior	Controller	ij-superior@outlook.com
Tom	Johnson	Superior	Sales Rep	tj-superior@mail.com
Nau	Tjeriko	Superior	Regional Marketing Manager	nt-superior@outlook.com
Ralph	Benson	Superior	General Counsel	rb-superior@outlook.com
Sam	Clemens	Superior	Advertising & Marketing	sc-superior@outlook.com
Sebastian	Mwaqngonde	Superior	International Sales Rep	sm-superior@outlook.com

This Exhibit shows the subdirectory of Preliminary Records. The files were opened. The Superior Contact List has important information for Forensic reconnaissance as it has a list of emails that may be used in the future. The .ods extension is very similar to Excel. Files were added to the hash DB. The .xls file that is locally on the Examiner's machine has a "Tagged Files" tab with all the corresponding hashes.

EXHIBIT E Excel Generation (Fig. 3-8 and Step 11)

Software	**Excel**
File Name(s)	**Proj0904-Report**
File Type	 Proj0904-Report.xlsx
File Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 1\HoP9-4
Evidence Confirming 28 Rows Records with 29 Rows including Tag	

	A
1	Tag
2	Superior-Personnel-Records /
3	Superior-Personnel-Records /
4	Superior-Personnel-Records /
5	Superior-Personnel-Records /
6	Superior-Personnel-Records /
7	Superior-Personnel-Records /
8	Superior-Personnel-Records /
9	Superior-Personnel-Records /
10	Superior-Personnel-Records /
11	Superior-Personnel-Records /
12	Superior-Personnel-Records /
13	Superior-Personnel-Records /
14	Superior-Personnel-Records /
15	Superior-Personnel-Records /
16	Superior-Personnel-Records /
17	Superior-Personnel-Records /
18	Superior-Personnel-Records /
19	Superior-Personnel-Records /
20	Superior-Personnel-Records /
21	Superior-Personnel-Records /
22	Superior-Personnel-Records /
23	Superior-Personnel-Records /
24	Superior-Personnel-Records /
25	Superior-Personnel-Records /
26	Superior-Personnel-Records /
27	Superior-Personnel-Records /
28	Superior-Personnel-Records /
29	Superior-Personnel-Records /
30	

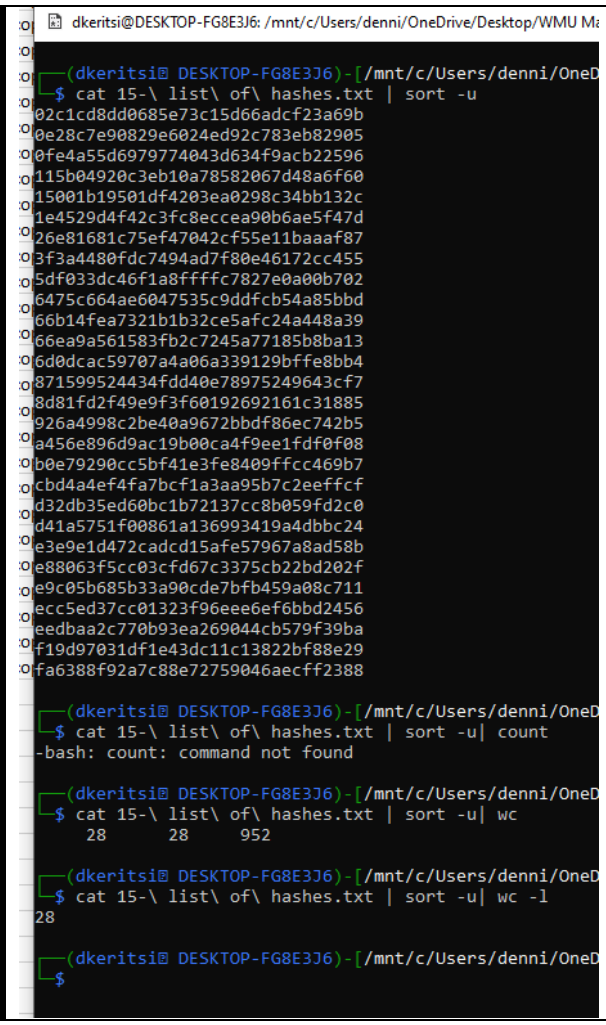
Evidence Showing all the Hash Values that are to be Loaded

	I	J
	Size (Bytes)	Hash
	11846	115b04920c3eb10a78582067d48a6f60
	14810	6475c664ae6047535c9ddfcb54a85bbd
	29994	e88063f5cc03cfd67c3375cb22bd202f
	28917	1e4529d4f42c3fc8eccea90b6ae5f47d
	30040	02c1cd8dd0685e73c15d66adcf23a69b
	31540	926a4998c2be40a9672bbdf86ec742b5
	54301	d32db35ed60bc1b72137cc8b059fd2c0
	30331	e9c05b685b33a90cde7bfb459a08c711
	29751	15001b19501df4203ea0298c34bb132c
	28714	cbd4a4ef4fa7bcf1a3aa95b7c2eeffcf
	29515	66ea9a561583fb2c7245a77185b8ba13
	28766	e3e9e1d472cadcd15afe57967a8ad58b
	33081	66b14fea7321b1b32ce5afc24a448a39
	30677	d41a5751f00861a136993419a4dbbc24
	30870	a456e896d9ac19b00ca4f9ee1fdf0f08
	17710	5df033dc46f1a8ffffc7827e0a00b702
	16476	8d81fd2f49e9f3f60192692161c31885
	17064	b0e79290cc5bf41e3fe8409ffcc469b7
	17675	fa6388f92a7c88e72759046aecff2388
	15899	26e81681c75ef47042cf55e11baaaf87
	23145	0fe4a55d6979774043d634f9acb22596
	17717	eedbaa2c770b93ea269044cb579f39ba
	16710	ecc5ed37cc01323f96eee6ef6bbd2456
	17788	6d0dcac59707a4a06a339129bffe8bb4
	17319	3f3a4480fdc7494ad7f80e46172cc455
	17044	871599524434fdd40e78975249643cf7
	17570	f19d97031df1e43dc11c13822bf88e29
	17444	0e28c7e90829e6024ed92c783eb82905

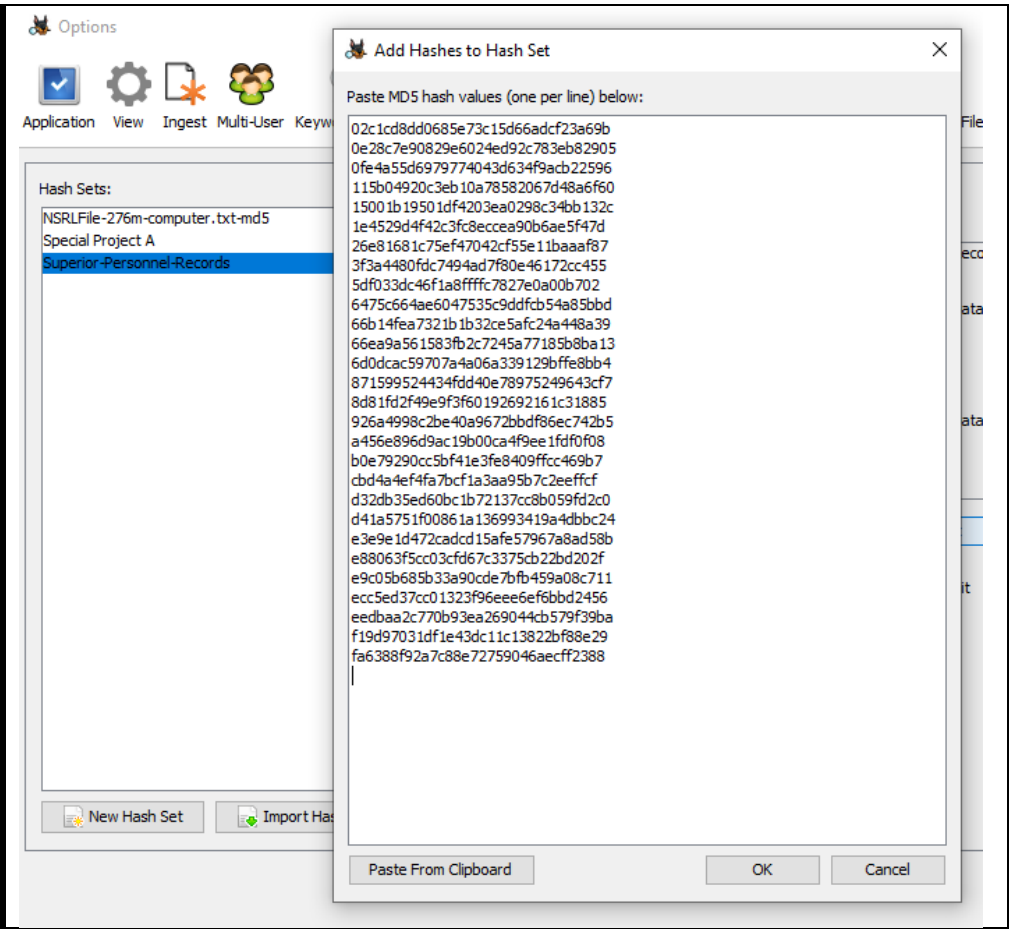
This Exhibit picks up from Excel whereby the Examiner copies and pastes the hashes to a .txt and uses Kali Linux to confirm 28 unique hashes since it is very hard to comb through line-by-line and to ensure this. The "cat" command outputs the file called "15- list of hashes.txt." And linking the "sort" command with "cat" is the pipe "|" as a vertical bar. The "sort" with the "-u" allows for duplicates to be removed. There is an additional pipe with "wc" for word count with a trigger of "-l" for lines. 28 was confirmed. After confirmation, the hashes were entered in the appropriate autopsy DB.

EXHIBIT F MD5 Hashes to DB (Fig. 3-9 and Step 17)

Software	**Autopsy; Kali Linux**
File Name(s)	**15- list of hashes**
File Type	 15- list of hashes.txt
File Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 1\HoP9-4\Pictures
Evidence List of Hashes to be Counted	02c1cd8dd0685e73c15d66adcf23a69b 0e28c7e90829e6024ed92c783eb82905 0fe4a55d6979774043d634f9acb22596 115b04920c3eb10a78582067d48a6f60 15001b19501df4203ea0298c34bb132c 1e4529d4f42c3fc8eccea90b6ae5f47d 26e81681c75ef47042cf55e11baaaf87 3f3a4480fdc7494ad7f80e46172cc455 5df033dc46f1a8ffffc7827e0a00b702 6475c664ae6047535c9ddfcb54a85bbd 66b14fea7321b1b32ce5afc24a448a39 66ea9a561583fb2c7245a77185b8ba13 6d0dcac59707a4a06a339129bffe8bb4 871599524434fdd40e78975249643cf7 8d81fd2f49e9f3f60192692161c31885 926a4998c2be40a9672bbdf86ec742b5 a456e896d9ac19b00ca4f9ee1fdf0f08 b0e79290cc5bf41e3fe8409ffcc469b7 cbd4a4ef4fa7bcf1a3aa95b7c2eeffcf d32db35ed60bc1b72137cc8b059fd2c0 d41a5751f00861a136993419a4dbbc24 e3e9e1d472cadcd15afe57967a8ad58b e88063f5cc03cfd67c3375cb22bd202f e9c05b685b33a90cde7bfb459a08c711 ecc5ed37cc01323f96eee6ef6bbd2456 eedbaa2c770b93ea269044cb579f39ba f19d97031df1e43dc11c13822bf88e29 fa6388f92a7c88e72759046aecff2388

Evidence Kali Linux Commands	

Evidence Adding to DB of "Superior-Personnel-Records



Some notes during forensic examination. The most important note being the emails/memos ordering the firing of Jim Shu.

EXHIBIT G Forensic Examiner Notes

Software	**Autopsy**
File Name(s)	**Digital Forensic Notes HoP 9-4**
File Type	 Digital Forensic Notes HoP 9-4.txt
File Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 1\HoP9-4
	.LOG 9:58 PM 6/10/2022 Set up folder 9:58 PM 6/10/2022 found that new image is required and need to do verification 10:04 PM 6/10/2022 hashes match 10:18 PM 6/10/2022 imported data and ingest n.b. there is no E01 ingest module in my autopsy 10:19 PM 6/10/2022 I imported wrong data source. Redo. 10:21 PM 6/10/2022 Ingest 10:33 PM 6/10/2022 Found ODT file type which is similar to docx file type 10:33 PM 6/10/2022 Observed emails about Mr. Jim Shu and Sam recommending them be fired. 10:39 PM 6/10/2022 Went to official records and a lot of PDFS 10:43 PM 6/10/2022 went to preliminary records and it shows the ods file type which is like Excel 10:46 PM 6/10/2022 Did file extraction

1.12. Discussion

These files represent a myriad of different file types such as PDF, ODS, and ODT files. The contents therein represent important business information that may be associated with regular and ordinary business, and therefore, not subject to the hearsay doctrine. That is, ordinarily the memorandum via email about Mr. Chu being terminate **would** be hearsay. However, given that it is in memorandum form, it is important to parlay this information to an attorney and explain the significance such that it may not be subject to heresy doctrine given its circulation through ordinary business operations. Secondly, the contents also had value PII associated with workers. These emails may be used in the future to forensically search emails associated with specific individuals.

Lastly, there were a series of tags and extractions. 28 unique hashes were found and are able to be used in future investigation associated with this company. As stated before, hashes not only provide integrity, but they also allow for fast computational time since bitwise operations can be readily performed given the relatively small number of bits relative to the file's bits.

5. HoP 14-1 Memorandum

Computer Forensic Analysis Report

MEMORANDUM FOR Harry Mudd, IT Department Manager

IT Department of Superior Bicycles

Jun 11th 2022

FROM: Dennis Keritsis, Digital Forensic Investigator

IT Security Department of Superior Bicycles

SUBJECT: Forensic Media Analysis Report

Subject(s) Tom Johnson

Introduction

It has come to the attention of Mr. Harry Mudd that Tom Johnson has violated policies more than once including the use of unauthorized applications. In accordance with company policy, to ensure equity and fairness of all employees, Tom Johnson's actions warrant an investigation of his device. Pending review and conclusions herein, a full audit may be issued, through Supervisory authority, accordingly in accordance with company policies.

1.13. Support Requested

Mr. Harry Mudd as instructed in the instant Examiner, Examiner Keritsis, to conduct an investigation as to whether Mr. Johnson has any files associated with Superior Bicycles' Special Project-A.

1.14. Statement of Compliance

I Examiner Keritsis assets that I am sufficiently skilled in digital forensics. I understand that my opinions are based on fact. I have no financial interest in the manner. The facts in this report are recorded to the best of my knowledge and ability. I attest these to be true in accordance with company policy. Forensic media image GCFI-tj01.001 has been duplicated and verified with hashes for integrity. *See* Exhibit 3-D, supra.

1.15. Tools

∞ **Autopsy on Windows**– Version 4.19.3

According to Sleuthkit.org: "Autopsy® is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools." Further , the instant Examiner utilized a hash database herein to upload MD5 hash values for forensic and programmatic searching of files within large images files. Further still, Autopsy was used to generate an Excel report to extract MD5 hash values.

∞ **Microsoft Excel**

∞ **Microsoft Notepad**

1.16. Findings

This section is providing evidentiary support, in accordance with company policies. That is, company policy prohibits a full audit without just cause as such actions may undermine equity and fairness in accordance with the company's vision and mission statements. Accordingly, the findings, through the use of hash-matching, represent a fast but focus forensic analysis of Mr. Johnson's computer.

1.16.1. Discussion on Exhibits

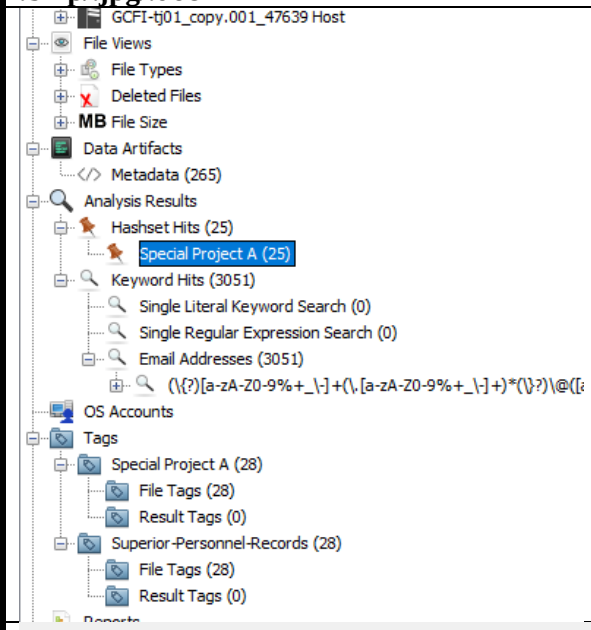
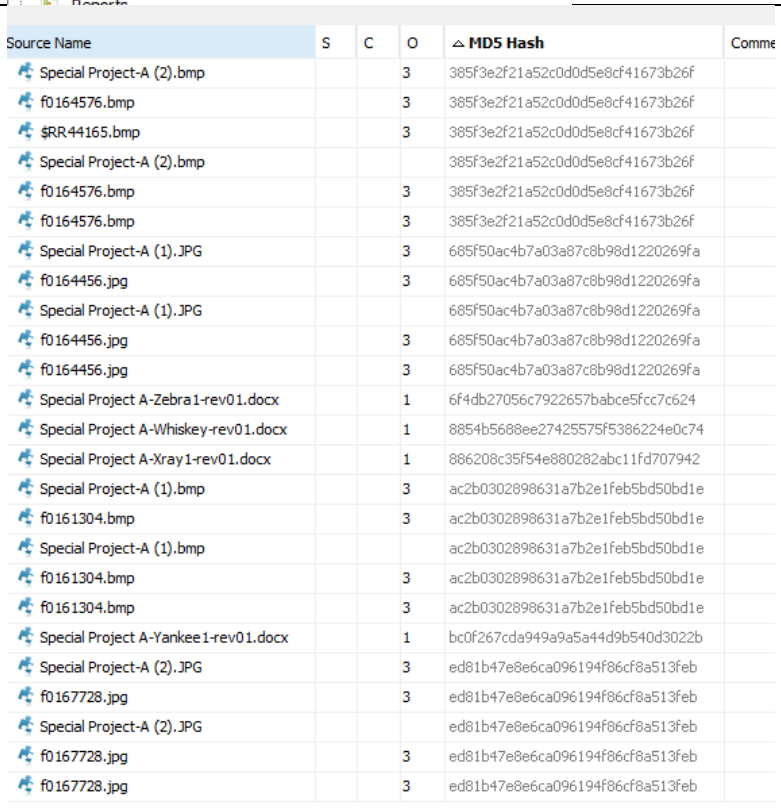
Exhibit below represents the total hits associated with the hashes found with Special Project A. Important: All his do not represent media associated with Mr. Johnson's device. That is, all twenty five (25) hits are not associated with Mr. Johnson's device as multiple images have been loaded in Autopsy herein per the instruction of CEO Dr. Alan Rea.[5] Further, the hashset hits allow the Examiner to comport with company policy with a fast but focused search as a full audit is not yet found warranted. The second piece of evidence with the below Exhibit is the list of files returned. The third piece of evidence within the below Exhibit is the list of three (3) files[6] showing, on the third column, directory of img:

"/img_GCFI-tj01_copy.0001/"

Accordingly, while .docx, .jpg, and .bmp files were in the return list, only bmp was associated with Mr. Johnson's device as seen in the third piece of evidence for the first Exhibit.

[5] As discussed in the Examiner's Forensic Notes in the last Exhibit, this was discovered at a later point of time. That is, it was believe that all eight (8) hashes were hit (timestamp 11:54 PM 6/10/2022). At a later point in time, about ten minutes later, the different in media analyzed was discovered (timestamps 11:59 ("Correction.")).
[6] Under careful inspection, the third piece of evidence has only two unique files as the last item is a duplicate. As such, extraction to Examiner's local machine consisted of two extractions.

EXHIBIT A Hash Hits (Fig. 3-10 Step 6)

Software	**Autopsy**
File Types	**.bmp/.jpg/.docx**[7]
Evidence Tree View Showing Hash Hits from Loaded DB	
Evidence Showing Laundry List of Files	

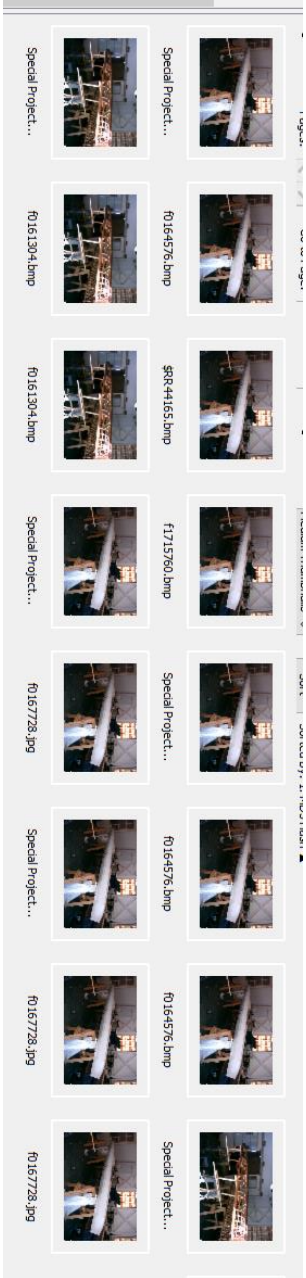
Source Name	S	C	O	MD5 Hash	Comme
Special Project-A (2).bmp			3	385f3e2f21a52c0d0d5e8cf41673b26f	
f0164576.bmp			3	385f3e2f21a52c0d0d5e8cf41673b26f	
$RR44165.bmp			3	385f3e2f21a52c0d0d5e8cf41673b26f	
Special Project-A (2).bmp				385f3e2f21a52c0d0d5e8cf41673b26f	
f0164576.bmp			3	385f3e2f21a52c0d0d5e8cf41673b26f	
f0164576.bmp			3	385f3e2f21a52c0d0d5e8cf41673b26f	
Special Project-A (1).JPG			3	685f50ac4b7a03a87c8b98d1220269fa	
f0164456.jpg			3	685f50ac4b7a03a87c8b98d1220269fa	
Special Project-A (1).JPG				685f50ac4b7a03a87c8b98d1220269fa	
f0164456.jpg			3	685f50ac4b7a03a87c8b98d1220269fa	
f0164456.jpg			3	685f50ac4b7a03a87c8b98d1220269fa	
Special Project A-Zebra1-rev01.docx			1	6f4db27056c7922657babce5fcc7c624	
Special Project A-Whiskey-rev01.docx			1	8854b5688ee27425575f5386224e0c74	
Special Project A-Xray1-rev01.docx			1	886208c35f54e880282abc11fd707942	
Special Project-A (1).bmp			3	ac2b0302898631a7b2e1feb5bd50bd1e	
f0161304.bmp			3	ac2b0302898631a7b2e1feb5bd50bd1e	
Special Project-A (1).bmp				ac2b0302898631a7b2e1feb5bd50bd1e	
f0161304.bmp			3	ac2b0302898631a7b2e1feb5bd50bd1e	
f0161304.bmp			3	ac2b0302898631a7b2e1feb5bd50bd1e	
Special Project A-Yankee1-rev01.docx			1	bc0f267cda949a9a5a44d9b540d3022b	
Special Project-A (2).JPG			3	ed81b47e8e6ca096194f86cf8a513feb	
f0167728.jpg			3	ed81b47e8e6ca096194f86cf8a513feb	
Special Project-A (2).JPG				ed81b47e8e6ca096194f86cf8a513feb	
f0167728.jpg			3	ed81b47e8e6ca096194f86cf8a513feb	
f0167728.jpg			3	ed81b47e8e6ca096194f86cf8a513feb	

[7] .docx, while associated with the hash hit list, was not associated with Mr. Johnson's device.

Evidence Showing IMG for GCFI-tj01.0001 And Showing Three Files

This Exhibit is an extension of the laundry list view, but for images in thumbnail view.

EXHIBIT B Thumbnail Images (Fig. 3-11 Step 9)

Software	**Autopsy**
File Type	**.bmp/.jpg**
Evidence Thumbnails	

Images extracted were exact duplicates. However, the naming was different and they were located in different areas. Metadata, which is part of the image is reproduced accordingly. Importantly, one of the images has a timestamp which helps provide a timeframe of a violation at or around 2017-06 to 2017-10. Lastly, each set of metadata has the same hash.

EXHIBIT C Extracted Images and Meta Data

Software	**Autopsy**
File Type	**.bmp**
Hash (MD5)	**385f3e2f21a52c0d0d5e8cf41673b26f**
Evidence (LEFT) 7- f1715760 **(RIGHT) 8- $RR44165**	
	
Meta Data 7- f1715760	Metadata Name: /img_GCFI-tj01_copy.001/$RECYCLE.BIN/S-1-5-21-670105763-4004074125-2612163412-1001/$RR44165.bmp Type: File System MIME Type: image/bmp Size: 1612854 File Name Allocation: Allocated Metadata Allocation: Allocated Modified:

	2017-06-29 18:41:18 EDT Accessed: 2017-10-25 18:13:02 EDT Created: 2017-10-25 18:13:02 EDT Changed: 2017-10-27 13:30:30 EDT MD5: 385f3e2f21a52c0d0d5e8cf41673b26f SHA-256: dea936e195f6de93366dfa20758c166f9a0644e240add9a7ae900f01f7669f0b Hash Lookup Results: BAD Internal ID: 58962 From The Sleuth Kit istat Tool: MFT Entry Header Values: Entry: 5767 Sequence: 1 $LogFile Sequence Number: 63038778 Allocated File Links: 1 $STANDARD_INFORMATION Attribute Values: Flags: Archive Owner ID: 0 Security ID: 270 (S-1-5-21-670105763-4004074125-2612163412-1001) Created: 2017-10-25 18:13:02.134730000 (EDT) File Modified: 2017-06-29 18:41:18.761536500 (EDT) MFT Modified: 2017-10-27 13:30:30.732113900 (EDT) Accessed: 2017-10-25 18:13:02.134730000 (EDT) $FILE_NAME Attribute Values: Flags: Archive Name: $RR44165.bmp Parent MFT Entry: 39 Sequence: 3 Allocated Size: 1613824 Actual Size: 1612854 Created: 2017-10-25 18:13:02.134730000 (EDT) File Modified: 2017-06-29 18:41:18.761536500 (EDT) MFT Modified: 2017-10-26 19:09:21.535225900 (EDT) Accessed: 2017-10-25 18:13:02.134730000 (EDT) $OBJECT_ID Attribute Values: Object Id: 6ae93190-b9d7-11e7-9c18-708bcd80a043 Attributes: Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72 Type: $FILE_NAME (48-6) Name: N/A Resident size: 90 Type: $OBJECT_ID (64-5) Name: N/A Resident size: 16 Type: $DATA (128-1) Name: N/A Non-Resident size: 1612854 init_size: 1612854 Starting address: 327510, length: 394
Meta Data **8-** **$RR44165**	Metadata Name: /img_GCFI-tj01_copy.001//$CarvedFiles/f1715760.bmp Type: Carved

[redacted]

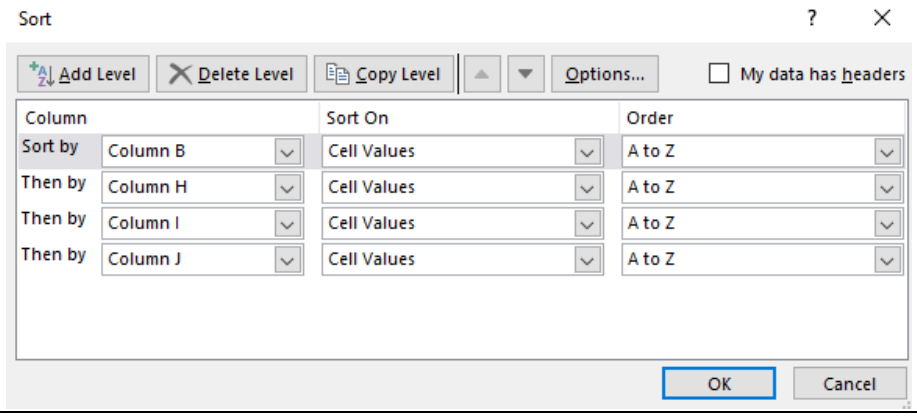
MIME Type:
image/bmp
Size:
1612854
File Name Allocation:
Unallocated
Metadata Allocation:
Unallocated
Modified:
0000-00-00 00:00:00
Accessed:
0000-00-00 00:00:00
Created:
0000-00-00 00:00:00
Changed:
0000-00-00 00:00:00
MD5:
385f3e2f21a52c0d0d5e8cf41673b26f
SHA-256:
dea936e195f6de93366dfa20758c166f9a0644e240add9a7ae900f01f7669f0b
Hash Lookup Results:
BAD
Internal ID:
78413

The forensic items were exported to excel via report generation. Applying a multi-tier sort, the files were organized. As seen by the primary sort, Column (B) was chosen as first since it is the IMG media that is creating unwanted hits. Important: All his do not represent media associated with Mr. Johnson's device. Exhibit with the last evidence (Right) shows directory of img:

"/img_GCFI-tj01_copy.0001/"

EXHIBIT D Excel from Report Generation (Fig. 3-12 Step 11)

Software	**Excel**
File Name(s)	**Proj1401-Report**
File Type	Proj1401-Report.xlsx
File Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 2\HoP14-1



54	Special Project A	/img_GCFI-tj01_copy.001/$RECYCLE.BIN/S-1-5-21-670105763-4004074125-2612163412-1001/$RR44165.bmp	2017-06-29 18:41:18 EDT	0000-00-00 00:00:00	2017-10-25 18:13:02 EDT	0000-00-00 00:00:00	1612854	385f3e2f21a52c0d0d5e8cf41673b26f
55	Special Project A	/img_GCFI-tj01_copy.001//$CarvedFiles/f1715760.bmp	2017-10-27 13:30:30 EDT	0000-00-00 00:00:00	2017-10-25 18:13:02 EDT	0000-00-00 00:00:00	1612854	385f3e2f21a52c0d0d5e8cf41673b26f

Evidence Showing Zoom on Hashes (Left) and Zoom on names (Right) for Both Files

These notes are critical as they represent the important Correction within the record that not all files hit represent files on Mr. Johnson's device. Additionally, files were carved (i.e., "$CarvedFiles") and in the $RECYCLE BIN. Accordingly, Mr. Johnson may have tried to hide this media. Only one (1) out of the eight (8) hashes for the images of the hashes was found.

EXHIBIT E Examiner's Forensic Notes

Software	**Notepad**
File Name(s)	**Forensic Examiner NOtes HoP14-1**[8]
File Type	 Forensic Examiner NOtes HoP14-1.txt
Hash (MD5)	**385f3e2f21a52c0d0d5e8cf41673b26f**
File Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 2\HoP14-1

```
.LOG

11:43 PM 6/10/2022 Need to add GCFI-tj001 but need copy first
11:48 PM 6/10/2022 copy verified
11:50 PM 6/10/2022 Ingesting and reading about Tom Johnson
11:51 PM 6/10/2022 Got hits on the hashes
11:53 PM 6/10/2022 Of the original 8 hashes
11:54 PM 6/10/2022 We have all hits on all hashes!
11:55 PM 6/10/2022 26+28 tags now 56 tags on "Special Project A"
11:59 PM 6/10/2022 Correction. Actually, many of those come from
bs01.
11:59 PM 6/10/2022 Looking at how many we really have we have ONLY
2!!! BOth are Bmps. Both have same hash. But different names.
12:02 AM 6/11/2022 Interesting. One of them was in RECYCLE BIN.
Other one was hidden because it was "carved"

$RR44165.bmp  org.sleuthkit.datamodel.Score@42145a3c  TAG_NO_COMMENT
       3      385f3e2f21a52c0d0d5e8cf41673b26f        /img_GCFI-
tj01_copy.001/$RECYCLE.BIN/S-1-5-21-670105763-4004074125-
2612163412-1001/$RR44165.bmp
f1715760.bmp  org.sleuthkit.datamodel.Score@42145a3c  TAG_NO_COMMENT
       -1     385f3e2f21a52c0d0d5e8cf41673b26f        /img_GCFI-
tj01_copy.001//$CarvedFiles/f1715760.bmp

12:12 AM 6/11/2022 Got metadata for both files
12:13 AM 6/11/2022 Extracted files
```

[8] Typographic error of capital "O" in original. Instant Examiner will note modify notes.

1.17. Conclusions

Dear Mr. Mudd,

the instant Examiner has comported with company policy by performing a focused but fast search without a full audit. With the limited analysis performed via our hash set of eight hashes, Mr. Johnson has sensitive company information associated with Special Project A, namely, a single image associated with a floatation device. This image (.bmp) has been duplicated and was located in at least two location within Mr. Johnson's device. A first duplicate associated with a RECYCLE BIN and a second duplicate associated with carved information. Both suggest that Mr. Johnson was aware of the sensitive information and attempted to hide said sensitive information and deleted sensitive information. Some events may have occurred at or around 2017-06 to 2017-10.

With Regards,

/s/ Dennis Keritsis.

6. HoP 14-2 Memorandum

Computer Forensic Analysis Report

RE: MEMORANDUM FOR Harry Mudd, IT Department Manager of IT Department of Superior Bicycles

FOR Bob Swartz Chief Engineer of Superior Bicycles

Jun 11th 2022

FROM: Dennis Keritsis, Digital Forensic Investigator

IT Security Department of Superior Bicycles

SUBJECT: Forensic Media Analysis Report

Subject(s) Tom Johnson

Introduction

This memo is in reply to the most recent memorandum sent to Mr. Harry Mudd who forwarded said most recent memorandum to Bob Swartz. Per the request of Mr. Swartz, through Harry Mudd, this report will perform a fast but focused search of Mr. Johnson's device. Important: Authorization for a full audit has not been given. Accordingly, the search of Mr. Johnson's device will be narrow per company policy.

1.18. Supplemental Support Search

Mr. Harry Mudd as instructed in the instant Examiner, Examiner Keritsis, to conduct an investigation as to whether Mr. Johnson has *additional* files. Support request will incorporate additional files for a supplemental search. Files include Special Project A and bicycle components. No full audit will be conducted.

1.19. Statement of Compliance

I Examiner Keritsis assets that I am sufficiently skilled in digital forensics. I understand that my opinions are based on fact. I have no financial interest in the manner. The facts in this report are recorded to the best of my knowledge and ability. I attest these to be true in accordance with company policy. Forensic media image GCFI-tj01.001 has been duplicated and verified with hashes for integrity. *See* Exhibit 3-D, supra.

1.20. Tools

∞ **Autopsy on Windows**– Version 4.19.3

According to Sleuthkit.org: "Autopsy® is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools." Further , the instant Examiner utilized a hash database herein to upload MD5 hash values for forensic and programmatic searching of files within large images files. Further still, Autopsy was used to generate an Excel report to extract MD5 hash values.

∞ **Microsoft Excel**

∞ **Microsoft Notepad**

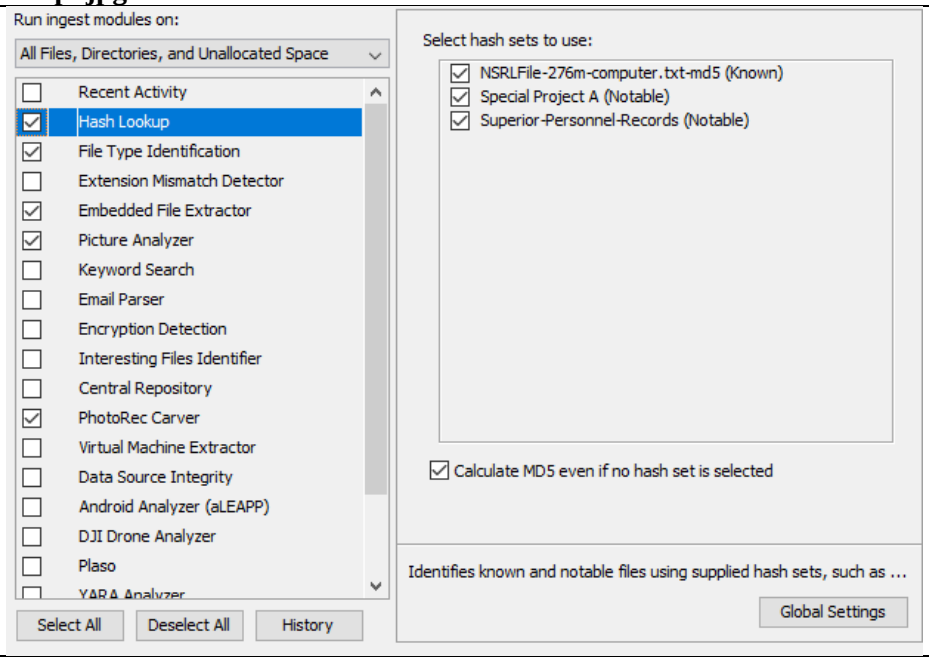
1.21. Findings

The following section will involve tagging kayaks and bicycles components as supplemental images that tagged and examined.

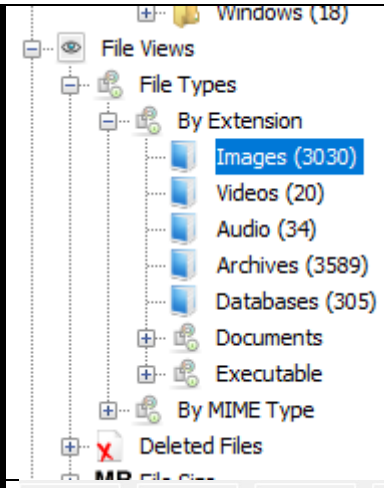
1.21.1. Discussion on Exhibits

This exhibit starts off with selecting the proper ingest modules. Different from the other forensic activities, this requires the Picture Analyzer module. Following ingest, the proper directory of "Images" was navigated to. Then the thumbnail tab was select which showed at least .jpg's and .bmp's. The last two pieces of evidence for this exhibit shows thumbnails of Kayaks and Bicycles, respectively.

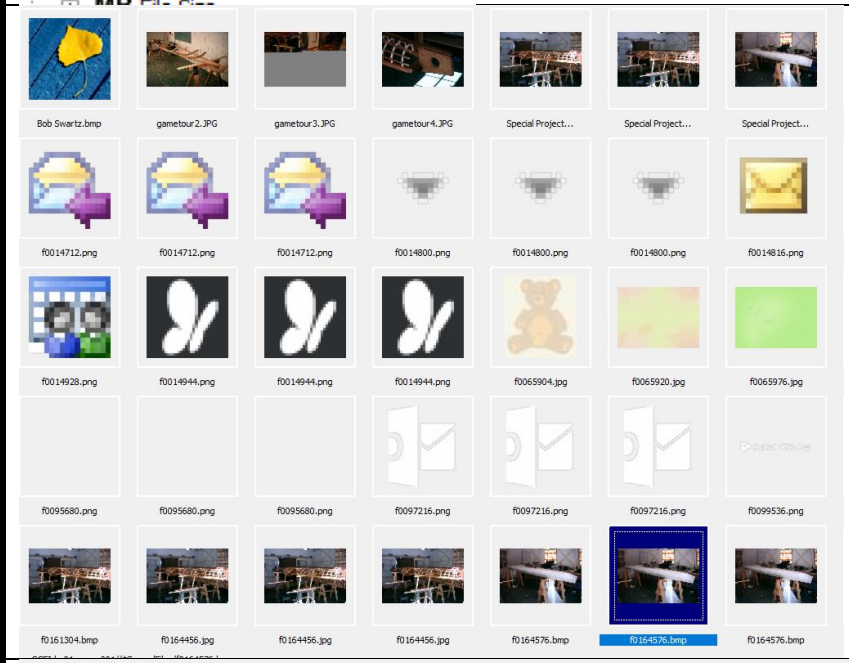
EXHIBIT A Autopsy Screen Shot of Directory (Fig. 3-13 Step 6)

Software	**Autopsy**
File Type	**.bmp/.jpg**
Evidence	
Picture Analyzer	
Required During Ingest	

Evidence Tree Viewer of Images



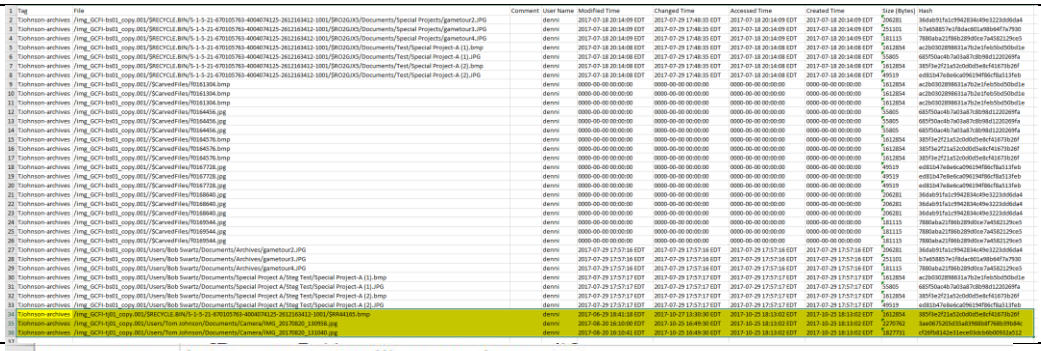
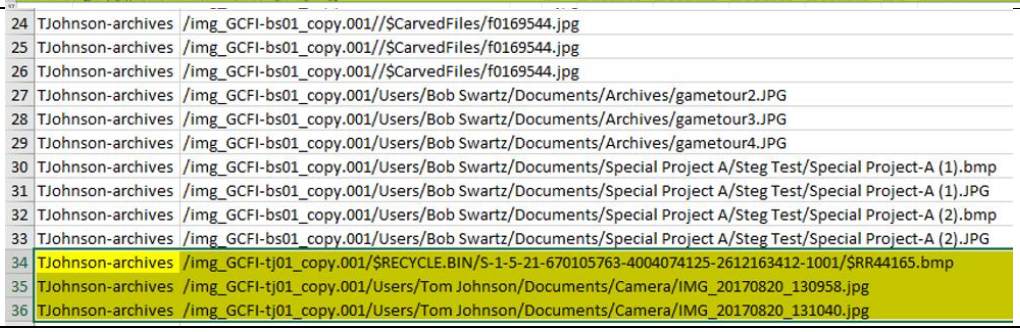
Evidence Thumbnail View of Kayaks



Evidence Thumbnail View of Bicycles

After tagging the files under TJohnson-photos, which can be seen below as "TJohnson-archives", the Examiner extracted the files via a report in Excel form and saved the data locally. The first piece of evidence is a zoomed out version. The second, and more material piece, shows a zoomed in version of the last three files. Two of which are .jgp's and one of which is a .bmp., wherein the .jpg's are bicycles and wherein the .bmp is a kayak. Important: While there are at least 36 rows in the extracted excel file, only files with img/GCFI-tj01_copy0001/ directory are relevant for this analysis. This can be seen in the second piece of evidence that is zoomed in within the 2nd column.

EXHIBIT B Excel Extraction (Fig. 3-14 Step 11)

Software	**Excel**
File Name(s)	**Proj1402**
File Type	Proj1402.xlsx
File Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 2\HoP14-2
Evidence Zoomed Out	
Evidence Zoomed In	

24	TJohnson-archives	/img_GCFI-bs01_copy.001//$CarvedFiles/f0169544.jpg
25	TJohnson-archives	/img_GCFI-bs01_copy.001//$CarvedFiles/f0169544.jpg
26	TJohnson-archives	/img_GCFI-bs01_copy.001//$CarvedFiles/f0169544.jpg
27	TJohnson-archives	/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/Archives/gametour2.JPG
28	TJohnson-archives	/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/Archives/gametour3.JPG
29	TJohnson-archives	/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/Archives/gametour4.JPG
30	TJohnson-archives	/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/Special Project A/Steg Test/Special Project-A (1).bmp
31	TJohnson-archives	/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/Special Project A/Steg Test/Special Project-A (1).JPG
32	TJohnson-archives	/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/Special Project A/Steg Test/Special Project-A (2).bmp
33	TJohnson-archives	/img_GCFI-bs01_copy.001/Users/Bob Swartz/Documents/Special Project A/Steg Test/Special Project-A (2).JPG
34	TJohnson-archives	/img_GCFI-tj01_copy.001/$RECYCLE.BIN/S-1-5-21-670105763-4004074125-2612163412-1001/$RR44165.bmp
35	TJohnson-archives	/img_GCFI-tj01_copy.001/Users/Tom Johnson/Documents/Camera/IMG_20170820_130958.jpg
36	TJohnson-archives	/img_GCFI-tj01_copy.001/Users/Tom Johnson/Documents/Camera/IMG_20170820_131040.jpg

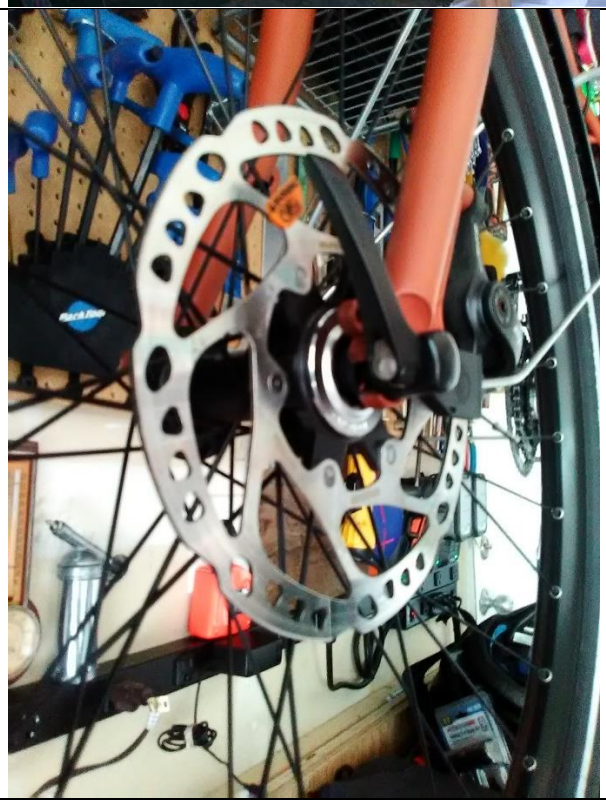
The exhibit below shows three (3) relevant files. All three were extracted from Autopsy and saved locally on the Examiner's device. Additionally, metadata was copied and pasted and saved accordingly in the same directory as three (3) .txt's for each respective image. One image was a .bmp (kayak) whereas the other two were .jpgs (bicycles). Interestingly, the bicycles appear to zoom in on the hub and spoke intersection as a possible critical component.

The kayak date ranges from 2017-06 to 2017-10 whereas the bicycles, similarly, are from 2017-08 to 2017-10 which suggests concurrent activities in disparate areas. Indeed, the both bicycle photos are on the same days for 2017-08, 2017-10, 2017-10, and 2017-10 for Modified, Accessed, Created, and Changed, respectively. This suggests that the photo is of the *same* bicycle. To the eye, this appears to be the case

EXHIBIT C Metadata of Files Extracted and Photos Themselves

Software	
File Name(s)	**4- $RR44165; 9- 58764-IMG_20170820_130958; 10- 58766-IMG_20170820_131040**[9]
File Type	 5- file meta data.txt  11 meta data.txt  12 meta data.txt **.jpg/.bmp;**
File Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 2\HoP14-2\Pictures

[9] During extraction and saving locally, the Examiner renamed the files with a number value and dash to save chronology and for organization.

Evidence **4- $RR44165**	
Evidence **9- 58764-** **IMG_20170820_130958**	

Evidence 10- 58766- IMG_20170820_131040	
Evidence 5- file meta data for $RR44165.bmp	Metadata Name: /img_GCFI-tj01_copy.001/$RECYCLE.BIN/S-1-5-21-670105763-4004074125-2612163412-1001/$RR44165.bmp Type: File System MIME Type: image/bmp Size: 1612854 File Name Allocation: Allocated Metadata Allocation: Allocated Modified: 2017-06-29 18:41:18 EDT Accessed: 2017-10-25 18:13:02 EDT Created: 2017-10-25 18:13:02 EDT Changed: 2017-10-27 13:30:30 EDT MD5: 385f3e2f21a52c0d0d5e8cf41673b26f SHA-256: dea936e195f6de93366dfa20758c166f9a0644e240add9a7ae900f01f7669f0b Hash Lookup Results: BAD

	Internal ID: 58962 From The Sleuth Kit istat Tool: MFT Entry Header Values: Entry: 5767 Sequence: 1 $LogFile Sequence Number: 63038778 Allocated File Links: 1 $STANDARD_INFORMATION Attribute Values: Flags: Archive Owner ID: 0 Security ID: 270 (S-1-5-21-670105763-4004074125-2612163412-1001) Created: 2017-10-25 18:13:02.134730000 (EDT) File Modified: 2017-06-29 18:41:18.761536500 (EDT) MFT Modified: 2017-10-27 13:30:30.732113900 (EDT) Accessed: 2017-10-25 18:13:02.134730000 (EDT) $FILE_NAME Attribute Values: Flags: Archive Name: $RR44165.bmp Parent MFT Entry: 39 Sequence: 3 Allocated Size: 1613824 Actual Size: 1612854 Created: 2017-10-25 18:13:02.134730000 (EDT) File Modified: 2017-06-29 18:41:18.761536500 (EDT) MFT Modified: 2017-10-26 19:09:21.535225900 (EDT) Accessed: 2017-10-25 18:13:02.134730000 (EDT) $OBJECT_ID Attribute Values: Object Id: 6ae93190-b9d7-11e7-9c18-708bcd80a043 Attributes: Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72 Type: $FILE_NAME (48-6) Name: N/A Resident size: 90 Type: $OBJECT_ID (64-5) Name: N/A Resident size: 16 Type: $DATA (128-1) Name: N/A Non-Resident size: 1612854 init_size: 1612854 Starting address: 327510, length: 394
Evidence 11 meta data for IMG_20170820_131040.jpg	Metadata Name: /img_GCFI-tj01_copy.001/Users/Tom Johnson/Documents/Camera/IMG_20170820_131040.jpg Type: File System MIME Type: image/jpeg Size: 1827731 File Name Allocation: Allocated Metadata Allocation: Allocated Modified: 2017-08-20 16:10:41 EDT Accessed:

	2017-10-25 18:13:02 EDT Created: 2017-10-25 18:13:02 EDT Changed: 2017-10-25 16:49:30 EDT MD5: cf26fb8142e31ece03dcb6b00932a512 SHA-256: f932364022f5ae38f76405993dd44d4db12fc3acad3733039bfae159c2a7d2c0 Hash Lookup Results: UNKNOWN Internal ID: 58766 From The Sleuth Kit istat Tool: MFT Entry Header Values: Entry: 5771 Sequence: 1 $LogFile Sequence Number: 63038668 Allocated File Links: 1 $STANDARD_INFORMATION Attribute Values: Flags: Archive Owner ID: 0 Security ID: 266 (S-1-5-21-670105763-4004074125-2612163412-1001) Created: 2017-10-25 18:13:02.450516400 (EDT) File Modified: 2017-08-20 16:10:41.000000000 (EDT) MFT Modified: 2017-10-25 16:49:30.449417200 (EDT) Accessed: 2017-10-25 18:13:02.450516400 (EDT) $FILE_NAME Attribute Values: Flags: Archive Name: IMG_20170820_131040.jpg Parent MFT Entry: 5769 Sequence: 1 Allocated Size: 1830912 Actual Size: 0 Created: 2017-10-25 18:13:02.450516400 (EDT) File Modified: 2017-10-25 18:13:02.450516400 (EDT) MFT Modified: 2017-10-25 18:13:02.450516400 (EDT) Accessed: 2017-10-25 18:13:02.450516400 (EDT) Attributes: Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72 Type: $FILE_NAME (48-2) Name: N/A Resident size: 112 Type: $DATA (128-1) Name: N/A Non-Resident size: 1827731 init_size: 1827731 Starting address: 327063, length: 447
Evidence **12 meta data for IMG_20170820_130958.jpg**	Metadata Name: /img_GCFI-tj01_copy.001/Users/Tom Johnson/Documents/Camera/IMG_20170820_130958.jpg Type: File System MIME Type: image/jpeg Size:

[redacted]

```
2270762
File Name Allocation:
Allocated
Metadata Allocation:
Allocated
Modified:
2017-08-20 16:10:00 EDT
Accessed:
2017-10-25 18:13:02 EDT
Created:
2017-10-25 18:13:02 EDT
Changed:
2017-10-25 16:49:30 EDT
MD5:
3ae0675205d35a83988b8f768b39b84c
SHA-256:
94bd4031d8b00367b872e7e53caf5e65e7f4a0502e3e6c971257e9ad6329
c84a
Hash Lookup Results:
UNKNOWN
Internal ID:
58764
From The Sleuth Kit istat Tool:
MFT Entry Header Values:
Entry: 5770 Sequence: 1
$LogFile Sequence Number: 63022833
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 266 (S-1-5-21-670105763-4004074125-2612163412-
1001)
Created: 2017-10-25 18:13:02.281142100 (EDT)
File Modified: 2017-08-20 16:10:00.000000000 (EDT)
MFT Modified: 2017-10-25 16:49:30.320106300 (EDT)
Accessed: 2017-10-25 18:13:02.281142100 (EDT)

$FILE_NAME Attribute Values:
Flags: Archive
Name: IMG_20170820_130958.jpg
Parent MFT Entry: 5769 Sequence: 1
Allocated Size: 2273280 Actual Size: 0
Created: 2017-10-25 18:13:02.281142100 (EDT)
File Modified: 2017-10-25 18:13:02.281142100 (EDT)
MFT Modified: 2017-10-25 18:13:02.281142100 (EDT)
Accessed: 2017-10-25 18:13:02.281142100 (EDT)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size:
72
Type: $FILE_NAME (48-2) Name: N/A Resident size: 112
Type: $DATA (128-1) Name: N/A Non-Resident size: 2270762
init_size: 2270762
Starting address: 271164, length: 555
```

The below exhibit is the Examiner's notes which were saved locally on his machine. Number of points. First, "Exif module" was not found in the latest version of Autopsy 4.19.3. It is now called "Picture Analyzer". Second, Examiner, as the behest of CEO Dr. Alan Rea, cases were not to be closed. Accordingly, when investigating, the proper directory for the right IMG needs to be noted. Third and last, the Examiner missed the bicycles components the first go around, but this error was remedied and did not affect the integrity of his evidence and conclusion.

EXHIBIT D Forensic Examiner Notes

Software	**Notepad**
File Name(s)	**Examiner Forensics Notes HoP14-2**
File Type	 Examiner Forensics Notes HoP14-2.txt
File Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 2\HoP14-2
Evidence[10]	.LOG 6:03 AM 6/11/2022 Harvey Mudd need mem to Bob Swartz 6:03 AM 6/11/2022 Find potential photos related to Project A and bicycle components 6:03 AM 6/11/2022 Source already loaded 6:06 AM 6/11/2022 Exif module is not "Picture Analyzer" 6:14 AM 6/11/2022 Some files are in part in thumbnail 6:17 AM 6/11/2022 Got to be careful though since we are looking at tj01_copy ONLY! 6:18 AM 6/11/2022 In listing, only 1 file was found. 6:18 AM 6/11/2022 GOing to extract this 6:19 AM 6/11/2022 Got file metadata too 6:20 AM 6/11/2022 Now generate report 6:26 AM 6/11/2022 I need to get bicycle components too. I missed that. 6:26 AM 6/11/2022 Now I see three total files. 6:29 AM 6/11/2022 Extract the two other photos 6:30 AM 6/11/2022 Got meta data for the other two photos

[10] Typos are in original (e.g., "GOing"). They are not fixed for the sake of authenticity and integrity.

1.22. Conclusion

Dear Mr. Mudd, please inform Mr. Swartz that:

Three important images were retrieved. A first image associated with a kayak and two other images associated with, more likely than not, a single bicycle. Additionally, suspect appears to be focused on the hub and spoke part of the single bicycle. Dates are critical. Suspect appears to be concurrently exploring or infiltrating both kayak Special Project A and bicycle components as the dates are running concurrently from at or around 2017-06 to 2017-08 to 2017-10. Details can be found in the metadata above.

With Regards,

/s/ Dennis Keritsis.

7. HoP 14-3 Memorandum

Computer Forensic Analysis Report

Attorney Work Product

Attorney-Client Privilege

INTERNAL MEMORANDUM FOR Mr. Ralph Benson

Office of General Counsel

Jun 11th 2022

FROM: Dennis Keritsis, Digital Forensic Investigator

IT Security Department

RE: Pending Legal Matters and Email Forensic Analysis

Subject(s) Jim Shu; Tom Johnson

Introduction

The most recent memorandum covered sensitive material associated with kayak and bicycles at or around 2017-06 to 2017-10. Said memorandum was forwarded to Mr. Swartz of engineering who corresponded with CEO Mr. Robinson who is working with general counsel Ralph Benson on pending legal matters.

1.23. Support Requested

Mr. Ralph Benson has requested the instant Examiner to investigate email correspondence of suspicious email addresses not within the company registry.

1.24. Statement of Compliance

I Examiner Keritsis assets that I am sufficiently skilled in digital forensics. I understand that my opinions are based on fact. I have no financial interest in the manner. The facts in this report are recorded to the best of my knowledge and ability. I attest these to be true in accordance with company policy.

1.25. Tools

∞ **Autopsy on Windows–** Version 4.19.3

According to Sleuthkit.org: “Autopsy® is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools.” Further , the instant Examiner utilized a hash database herein to upload MD5 hash values for forensic and programmatic searching of files within large images files. Further still, Autopsy was used to generate an Excel report to extract MD5 hash values.

∞ **Microsoft Excel**

∞ **Microsoft Notepad**

∞ **Kali Linux Subsystem on Windows**

According to Microsoft: “The Windows Subsystem for Linux lets developers run a GNU/Linux environment -- including most command-line tools, utilities, and applications -- directly on Windows, unmodified, without the overhead of a traditional virtual machine or dualboot setup.”

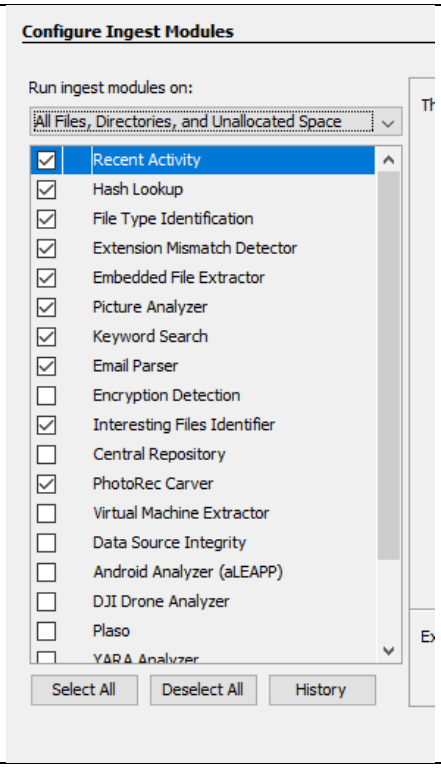
1.26. Findings

This section will be directed towards the data wrangling of emails that are not within our company's registry as these are suspect. Additionally, looking at the contents of respective emails, suspect language is used between parties to obfuscating their respective identities.

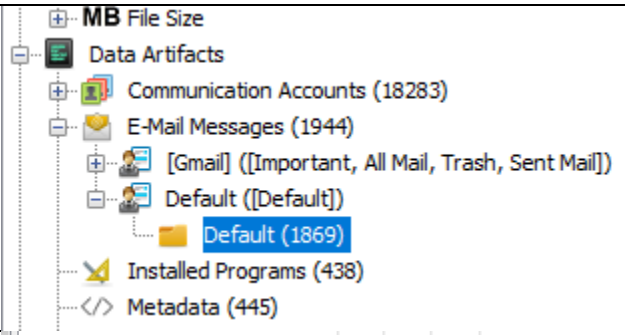
1.26.1. Discussion on Exhibits

The below exhibit will cover the ingestion of modules; analysis of .mbox files; and analysis of contents with respect to said .mbox files. .mbox files are associated with mailboxes. A suspect email address of ruth.wonderly@zoho.com outside our company's registry. Additionally, a number of other emails were tagged with "Non-SB-Email-Address." Further, when looking at the content of the emails, the corresponder and correspondee are anonymizing their names (e.g., "Your secret admirer."). However, inferentially, a device with an owner can be associated with the respective email addresses.

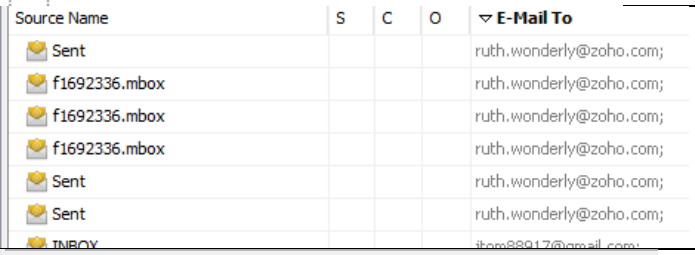
EXHIBIT A Autopsy Result (Fig. 3-15 Step 10)

Software	**Autopsy**
File Name(s)	**f1692336.mbox**
File Type	**.mbox**
Evidence Covering at least 10 Modules for Ingest	

Evidence Tree Viewer

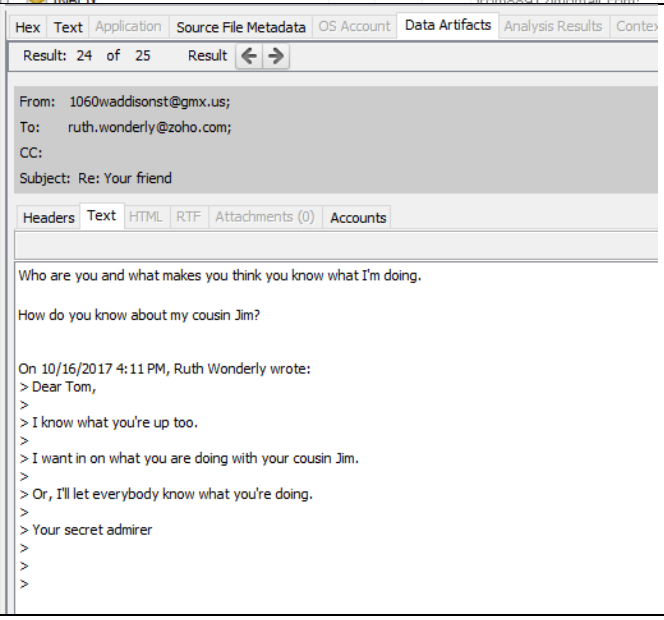


Evidence Requiring Examiner to Find Non-SB-Emails



Source Name	S	C	O	E-Mail To
Sent				ruth.wonderly@zoho.com;
f1692336.mbox				ruth.wonderly@zoho.com;
f1692336.mbox				ruth.wonderly@zoho.com;
f1692336.mbox				ruth.wonderly@zoho.com;
Sent				ruth.wonderly@zoho.com;
Sent				ruth.wonderly@zoho.com;

Evidence Content inside Suspect Email

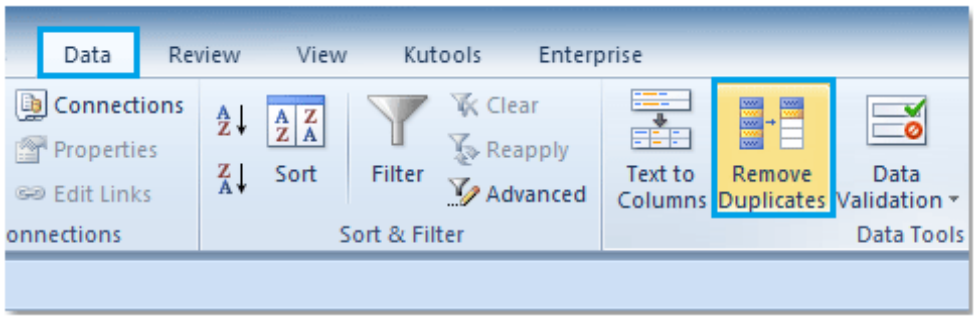


There was a great deal of emails. Per the instructions on p. 585 Step 12 ("ignoring any redundant messages"), the Examiner decided to filter on the backend instead of the front end to save time. The generate excel file from Autopsy shows 514 rows, with a total of 513 emails. Methods for filing in excel include, filtering by email header and filtering by plaintext. Ultimately, Examiner made a determination that around 26-28 unique emails exist which is a reasonable number to forward to general counsel for review. Excel generated at least two tabs called "E-Mail Messages" and "Tagged Results."

EXHIBIT B Excel Report (Fig. 3-16 Step 14)

Software	**Excel**
File Name(s)	**Proj1403-Report**
File Type	Proj1403-Report.xlsx
File Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 2\HoP14-3
Evidence Showing 514 rows with 513 Emails with Duplicates	
Evidence	

500	TSK_EMAIL_MSG	Non-SB-Email-Address		f1691712.mbox	denni
501	TSK_EMAIL_MSG	Non-SB-Email-Address		f1675784.txt	denni
502	TSK_EMAIL_MSG	Non-SB-Email-Address		Re Need to talk to you ASAP-3.eml	denni
503	TSK_EMAIL_MSG	Non-SB-Email-Address		Re Need to talk to you ASAP-2.eml	denni
504	TSK_EMAIL_MSG	Non-SB-Email-Address		Re Need to talk to you ASAP-1.eml	denni
505	TSK_EMAIL_MSG	Non-SB-Email-Address		Re Need to talk to you ASAP-2.eml	denni
506	TSK_EMAIL_MSG	Non-SB-Email-Address		Sent	denni
507	TSK_EMAIL_MSG	Non-SB-Email-Address		Sent	denni
508	TSK_EMAIL_MSG	Non-SB-Email-Address		f1675784.txt	denni
509	TSK_EMAIL_MSG	Non-SB-Email-Address		Sent	denni
510	TSK_EMAIL_MSG	Non-SB-Email-Address		Sent	denni
511	TSK_EMAIL_MSG	Non-SB-Email-Address		Sent	denni
512	TSK_EMAIL_MSG	Non-SB-Email-Address		You might be interested.eml	denni
513	TSK_EMAIL_MSG	Non-SB-Email-Address		Re Sample 1.eml	denni
514	TSK_EMAIL_MSG	Non-SB-Email-Address		Sent	denni



Evidence Showing "Tagged Results" TAB after Filtering by Source File Name Reduce 513 E-mails to 26 E-mails

	Result Type	Tag	Comment	Source File	User Name
2	TSK_EMAIL_MSG	Non-SB-Email-Address		Sent	denni
3	TSK_EMAIL_MSG	Non-SB-Email-Address		f1692336.mbox	denni
4	TSK_EMAIL_MSG	Non-SB-Email-Address		f1675784.txt	denni
5	TSK_EMAIL_MSG	Non-SB-Email-Address		Re Sample 1-1.eml	denni
6	TSK_EMAIL_MSG	Non-SB-Email-Address		Re Sample 1-2.eml	denni
7	TSK_EMAIL_MSG	Non-SB-Email-Address		Re Test message.eml	denni
8	TSK_EMAIL_MSG	Non-SB-Email-Address		Re Need to talk to you ASAP-3.eml	denni
9	TSK_EMAIL_MSG	Non-SB-Email-Address		Re You might be interested.eml	denni
10	TSK_EMAIL_MSG	Non-SB-Email-Address		Re Sample 1.eml	denni
11	TSK_EMAIL_MSG	Non-SB-Email-Address		Fwd You might be interested.eml	denni
12	TSK_EMAIL_MSG	Non-SB-Email-Address		Sample 1.eml	denni
13	TSK_EMAIL_MSG	Non-SB-Email-Address		You might be interested.eml	denni
14	TSK_EMAIL_MSG	Non-SB-Email-Address		f1705064.mbox	denni
15	TSK_EMAIL_MSG	Non-SB-Email-Address		INBOX	denni
16	TSK_EMAIL_MSG	Non-SB-Email-Address		Sent-1	denni
17	TSK_EMAIL_MSG	Non-SB-Email-Address		Money & Training.eml	denni
18	TSK_EMAIL_MSG	Non-SB-Email-Address		Re Money available.eml	denni
19	TSK_EMAIL_MSG	Non-SB-Email-Address		Re Need to talk to you ASAP.eml	denni
20	TSK_EMAIL_MSG	Non-SB-Email-Address		Re Need to talk to you ASAP-1.eml	denni
21	TSK_EMAIL_MSG	Non-SB-Email-Address		Re Need to talk to you ASAP-2.eml	denni
22	TSK_EMAIL_MSG	Non-SB-Email-Address		Trash	denni
23	TSK_EMAIL_MSG	Non-SB-Email-Address		f1670656.mbox	denni
24	TSK_EMAIL_MSG	Non-SB-Email-Address		f1670088.mbox	denni
25	TSK_EMAIL_MSG	Non-SB-Email-Address		f1670704.mbox	denni
26	TSK_EMAIL_MSG	Non-SB-Email-Address		f1675752.mbox	denni
27	TSK_EMAIL_MSG	Non-SB-Email-Address		f1691712.mbox	denni

Evidence "Email-Messages" TAB and Filtered by Header 35 total

	A	B	C	Headers
1	E-Mail To	E-Mail From	Subject	Headers
2	j-shu@gmx.com;	1060waddisonst@gmx.us;	Money	-----HEADERS-----X-Mozilla-Status: 1009X-Mozilla-Status2: 00800
3	j-shu@gmx.com;	1060waddisonst@gmx.us;	Money	-----HEADERS-----X-Mozilla-Status: 1001X-Mozilla-Status2: 00800
4	j-shu@gmx.us;	1060waddisonst@gmx.us;	Fwd: Money	-----HEADERS-----Content-Type: text/html; charset=utf-8Content
5	j-shu@gmx.us;	jtom88917@gmail.com;	New cell phone	-----HEADERS-----DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/r
6	j-shu@gmx.us;	jtom88917@gmail.com;	New cell phone	-----HEADERS-----To: j-shu@gmx.usFrom: Tom Johnson <jtom889
7	j-shu@gmx.us;	jtom88917@gmail.com;	New cell phone	-----HEADERS-----X-Mozilla-Status: 0001X-Mozilla-Status2: 00000
8	j_shu@gmx.us;	1060waddisonst@gmx.us;	Money & Training	-----HEADERS-----X-Mozilla-Status: 0001X-Mozilla-Status2: 00800
9	j_shu@gmx.us;	1060waddisonst@gmx.us;	New Announcement	-----HEADERS-----X-Mozilla-Status: 0009X-Mozilla-Status2: 00800
10	j_shu@gmx.us;	1060waddisonst@gmx.us;	Re: Money available	-----HEADERS-----X-Mozilla-Status: 0001X-Mozilla-Status2: 00800
11	j_shu@gmx.us;	1060waddisonst@gmx.us;	Re: Need to talk to you ASAP	-----HEADERS-----X-Mozilla-Status: 0001X-Mozilla-Status2: 00800
12	j_shu@gmx.us;	1060waddisonst@gmx.us;	Re: Need to talk to you ASAP	-----HEADERS-----X-Mozilla-Status: 0001X-Mozilla-Status2: 00800
13	j_shu@gmx.us;	1060waddisonst@gmx.us;	Re: Need to talk to you ASAP	-----HEADERS-----X-Mozilla-Status: 0001X-Mozilla-Status2: 00800
14	j_shu@gmx.us;	1060waddisonst@gmx.us;	Re: Need to talk to you ASAP	-----HEADERS-----X-Mozilla-Status: 0001X-Mozilla-Status2: 00800
15	j_shu@gmx.us;	1060waddisonst@gmx.us;	Re: Sample 1	-----HEADERS-----X-Mozilla-Status: 0001X-Mozilla-Status2: 00800
16	j_shu@gmx.us;	1060waddisonst@gmx.us;	Re: Sample 1	-----HEADERS-----X-Mozilla-Status: 0001X-Mozilla-Status2: 00800
17	j_shu@gmx.us;	1060waddisonst@gmx.us;	Re: Sample 1	-----HEADERS-----X-Mozilla-Status: 0001X-Mozilla-Status2: 00800
18	j_shu@gmx.us;	1060waddisonst@gmx.us;	Re: You might be interested	-----HEADERS-----X-Mozilla-Status: 0001X-Mozilla-Status2: 00800
19	j_shu@gmx.us;	1060waddisonst@gmx.us;	Sample 1	-----HEADERS-----Content-Type: text/plain; charset=utf-8; format
20	j_shu@gmx.us;	jtom88917@gmail.com;	Lab items	-----HEADERS-----Content-Type: text/plain; charset=utf-8; format
21	j_shu@gmx.us;	jtom88917@gmail.com;	Lab photo	-----HEADERS-----Content-Type: text/html; charset="UTF-8"---EN
22	j_shu@gmx.us;	jtom88917@gmail.com;	New cell phone	-----HEADERS-----Subject: New cell phoneReferences: <a5043050
23	j_shu@gmx.us;	jtom88917@gmail.com;	New job	-----HEADERS-----To: Jim Shu <j_shu@gmx.us>From: Tom Johnso
24	j_shu@gmx.us;	jtom88917@gmail.com;	Re: Lab items	-----HEADERS-----Content-Type: text/plain; charset=utf-8Content
25	j_shu@gmx.us;	jtom88917@gmail.com;	Re: Lab items	-----HEADERS-----X-Mozilla-Status: 0001X-Mozilla-Status2: 00000
26	j_shu@gmx.us;	jtom88917@gmail.com;	Re: New cell phone	-----HEADERS-----X-Mozilla-Status: 0001X-Mozilla-Status2: 00000
27	j_shu@gmx.us;	jtom88917@gmail.com;	Re: New cell phone	-----HEADERS-----Subject: Re: New cell phoneTo: Jim Shu <j_shu
28	jtom88917@gmail.com;	14582063432.15416399518.JAZJlhKstk@txt.voice.google.com;	New text message from Jim Shu (541) 639-9518	-----HEADERS-----Content-Type: text/html; charset="UTF-8"Cont
29	jtom88917@gmail.com;	j_shu@gmx.us;	Re: Lab items	-----HEADERS-----X-Mozilla-Status: 0001X-Mozilla-Status2: 00000
30	jtom88917@gmail.com;	j_shu@gmx.us;	Re: New cell phone	-----HEADERS-----X-Mozilla-Status: 0001X-Mozilla-Status2: 00000
31	jtom88917@gmail.com;	j_shu@gmx.us;	Re: New cell phone	-----HEADERS-----Content-Type: text/plain; charset=utf-8Content
32	jtom88917@gmail.com;	j_shu@gmx.us;	Re: New cell phone	-----HEADERS-----X-Mozilla-Status: 0001X-Mozilla-Status2: 00000
33	jtom88917@gmail.com;	j_shu@gmx.us;	Re: New job	-----HEADERS-----X-Mozilla-Status: 0001X-Mozilla-Status2: 00000
34	jtom88917@gmail.com;	no-reply@app.lookout.com;	Breach Report in Review: Anthem breach shows how personal data can leak in seconds	-----HEADERS-----Content-Transfer-Encoding: quoted-printableC
35	jtom88917@gmail.com;	team@lookout.com;	Lookout Found Your Device's Last Location	-----HEADERS-----Content-Type: text/html; charset=utf-8Content
36	ruth.wonderly@zoho.com;	1060waddisonst@gmx.us;	Re: Your friend	-----HEADERS-----X-Mozilla-Status: 0001X-Mozilla-Status2: 00800

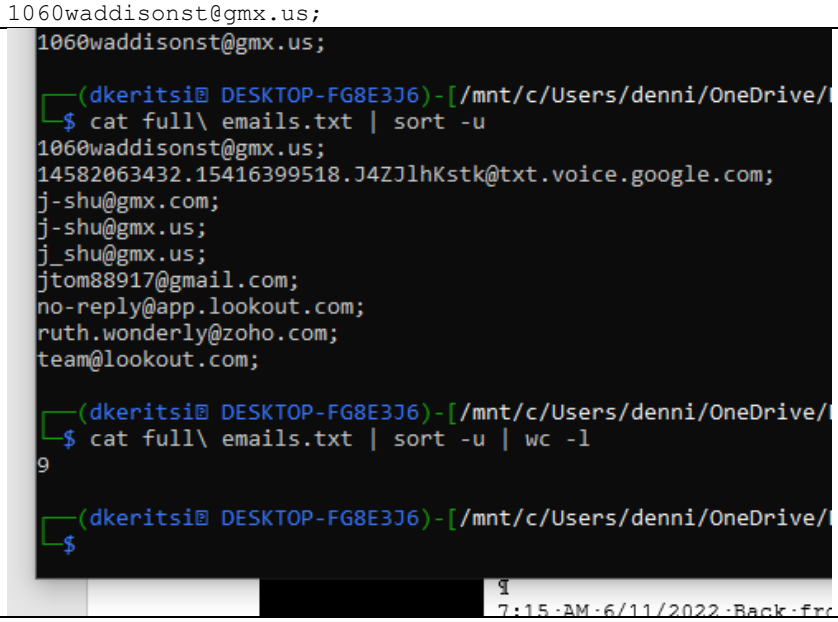
Evidence "Email-Messages" TAB and Filtered by Body of email 28 total

	A	B	C	Headers
1	E-Mail To	E-Mail From	Subject	Headers
2	j_shu@gmx.com;	1060waddisonst@gmx.us;	Money	----HEADERS----X-Mozilla-Status: 1009X-Mozilla-Status2
3	j_shu@gmx.us;	1060waddisonst@gmx.us;	Fwd: Money	----HEADERS----Content-Type: text/html; charset=utf-8
4	j_shu@gmx.us;	jtom88917@gmail.com;	New cell phone	----HEADERS----DKIM-Signature: v=1; a=sa-sha256; c=re
5	j_shu@gmx.us;	1060waddisonst@gmx.us;	New Announcement	----HEADERS----X-Mozilla-Status: 0009X-Mozilla-Status2
6	j_shu@gmx.us;	1060waddisonst@gmx.us;	Re: Money available	----HEADERS----X-Mozilla-Status: 0001X-Mozilla-Status2
7	j_shu@gmx.us;	1060waddisonst@gmx.us;	Re: Need to talk to you ASAP	----HEADERS----X-Mozilla-Status: 0001X-Mozilla-Status2
8	j_shu@gmx.us;	1060waddisonst@gmx.us;	Re: Need to talk to you ASAP	----HEADERS----X-Mozilla-Status: 0001X-Mozilla-Status2
9	j_shu@gmx.us;	1060waddisonst@gmx.us;	Re: Need to talk to you ASAP	----HEADERS----X-Mozilla-Status: 0001X-Mozilla-Status2
10	j_shu@gmx.us;	1060waddisonst@gmx.us;	Re: Need to talk to you ASAP	----HEADERS----X-Mozilla-Status: 0001X-Mozilla-Status2
11	j_shu@gmx.us;	1060waddisonst@gmx.us;	Re: Sample 1	----HEADERS----X-Mozilla-Status: 0001X-Mozilla-Status2
12	j_shu@gmx.us;	1060waddisonst@gmx.us;	Re: Sample 1	----HEADERS----X-Mozilla-Status: 0001X-Mozilla-Status2
13	j_shu@gmx.us;	1060waddisonst@gmx.us;	Re: Sample 1	----HEADERS----X-Mozilla-Status: 0001X-Mozilla-Status2
14	j_shu@gmx.us;	1060waddisonst@gmx.us;	Re: You might be interested	----HEADERS----X-Mozilla-Status: 0001X-Mozilla-Status2
15	j_shu@gmx.us;	1060waddisonst@gmx.us;	Sample 1	----HEADERS----Content-Type: text/plain; charset=utf-8
16	j_shu@gmx.us;	jtom88917@gmail.com;	Lab items	----HEADERS----Content-Type: text/plain; charset=utf-8
17	j_shu@gmx.us;	jtom88917@gmail.com;	Lab photo	----HEADERS----Content-Type: text/html; charset="UTF
18	j_shu@gmx.us;	jtom88917@gmail.com;	New job	----HEADERS----To: Jim Shu <j_shu@gmx.us>From: Tom
19	j_shu@gmx.us;	jtom88917@gmail.com;	Re: Lab items	----HEADERS----Content-Type: text/plain; charset=utf-8
20	j_shu@gmx.us;	jtom88917@gmail.com;	Re: New cell phone	----HEADERS----X-Mozilla-Status: 0001X-Mozilla-Status2
21	jtom88917@gmail.com;	14582063432.15416399518.J4ZJhkstk@txt.voice.google.com;	New text message from Jim Shu (541) 639-9518	----HEADERS----Content-Type: text/html; charset="UTF
22	jtom88917@gmail.com;	j_shu@gmx.us;	Re: Lab items	----HEADERS----X-Mozilla-Status: 0001X-Mozilla-Status2
23	jtom88917@gmail.com;	j_shu@gmx.us;	Re: New cell phone	----HEADERS----X-Mozilla-Status: 0001X-Mozilla-Status2
24	jtom88917@gmail.com;	j_shu@gmx.us;	Re: New cell phone	----HEADERS----Content-Type: text/plain; charset=utf-8
25	jtom88917@gmail.com;	j_shu@gmx.us;	Re: New cell phone	----HEADERS----X-Mozilla-Status: 0001X-Mozilla-Status2
26	jtom88917@gmail.com;	j_shu@gmx.us;	Re: New job	----HEADERS----X-Mozilla-Status: 0001X-Mozilla-Status2
27	jtom88917@gmail.com;	no-reply@app.lookout.com;	Breach Report in Review: Anthem breach shows how personal data can leak in seconds	----HEADERS----Content-Transfer-Encoding: quoted-pri
28	jtom88917@gmail.com;	team@lookout.com;	Lookout Found Your Device's Last Location	----HEADERS----Content-Type: text/html; charset=utf-8
29	ruth.wonderly@zoho.com;	1060waddisonst@gmx.us;	Re: Your friend	----HEADERS----X-Mozilla-Status: 0001X-Mozilla-Status2

The instant Examiner unitized Kali Linux Subsystem to clear out duplicates and provide a clean list for attorney. “cat” command is the output command. The vertical bar “|” is pipe that yokes the “sort -u” which sorts and remove duplicates with the -u trigger. As can been seen with that first command, these outputs a list of non-duplicated emails. Then a wc -l is utilized to count, wherein the -l trigger stands for number of lines as each email corresponds to one line. There are 9 total. These results were saved to “unique_list.txt.”

EXHIBIT C Remove Duplicates and List

Software	**Kali Linux Windows Subsystem; Notepad**
File Name(s)	**full emails; unique_list**
File Type	 unique_list.txt  full emails.txt
File Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 2\HoP14-3
Evidence from “full emails.txt” with duplications	j-shu@gmx.com; j-shu@gmx.us; j-shu@gmx.us; j_shu@gmx.us; j_shu@gmx.us; j_shu@gmx.us; j_shu@gmx.us; j_shu@gmx.us; j_shu@gmx.us; j_shu@gmx.us; j_shu@gmx.us; j_shu@gmx.us; j_shu@gmx.us; j_shu@gmx.us; j_shu@gmx.us; j_shu@gmx.us; j_shu@gmx.us; j_shu@gmx.us; jtom88917@gmail.com; jtom88917@gmail.com; jtom88917@gmail.com; jtom88917@gmail.com; jtom88917@gmail.com; jtom88917@gmail.com; jtom88917@gmail.com; jtom88917@gmail.com; ruth.wonderly@zoho.com; 1060waddisonst@gmx.us; 1060waddisonst@gmx.us; jtom88917@gmail.com;

	1060waddisonst@gmx.us; 1060waddisonst@gmx.us; 1060waddisonst@gmx.us; 1060waddisonst@gmx.us; 1060waddisonst@gmx.us; 1060waddisonst@gmx.us; 1060waddisonst@gmx.us; 1060waddisonst@gmx.us; 1060waddisonst@gmx.us; 1060waddisonst@gmx.us; 1060waddisonst@gmx.us; jtom88917@gmail.com; jtom88917@gmail.com; jtom88917@gmail.com; jtom88917@gmail.com; jtom88917@gmail.com; 14582063432.15416399518.J4ZJlhKstk@txt.voice.google.com; j_shu@gmx.us; j_shu@gmx.us; j_shu@gmx.us; j_shu@gmx.us; j_shu@gmx.us; no-reply@app.lookout.com; team@lookout.com; 1060waddisonst@gmx.us;
Evidence Kali Linux Subsystem Commands	
Evidence of Unique List in “unique_list.txt”	1060waddisonst@gmx.us; 14582063432.15416399518.J4ZJlhKstk@txt.voice.google.com; j-shu@gmx.com; j-shu@gmx.us; j_shu@gmx.us; jtom88917@gmail.com; no-reply@app.lookout.com; ruth.wonderly@zoho.com; team@lookout.com;

Notes reminding Examiner to Label Internal Memo accordingly for Confidentiality Purposes as this may be subject to discovery under Rule 26. As of now, instant Examiner is working in a consulting capacity.

EXHIBIT D Forensic Examiner Notes

Software	**Notepad**
File Name(s)	**HoP14-3 Forensic Notes**
File Type	 HoP14-3 Forensic Notes.txt
File Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 2\HoP14-3
Evidence	.LOG 6:32 AM 6/11/2022 Mr. Benson is lawyer and sent me memo. 6:32 AM 6/11/20226:33 AM 6/11/2022 NEED TO LABEL ATTORNEY WORK PRODUCT!!! 6:34 AM 6/11/2022 Also note that "Picture Analyzer" is to be used. 7:15 AM 6/11/2022 Back from Break. Ingest Module is at 99.99% and isn't finishing for some reason. 7:19 AM 6/11/2022 Done tagging. 7:21 AM 6/11/2022 Alot of emails! About 513. 7:38 AM 6/11/2022 Removed all the duplicates and found 26 unique emails 8:49 PM 6/11/2022

1.27. Conclusion

Dear Mr. Benson:

Here is a list of suspect emails below that are not register to our system. Methodologies are sound and can be substantiated above. Further, looking into the contents of emails, email-ers and email-ees are using pseudo names to obfuscate tracking; however, trackability can be done per your request as needed but is beyond of scope.

1060waddisonst@gmx.us;

14582063432.15416399518.J4ZJlhKstk@txt.voice.google.com;

j-shu@gmx.com;

j-shu@gmx.us;

j_shu@gmx.us;[11]

jtom88917@gmail.com;

no-reply@app.lookout.com;

ruth.wonderly@zoho.com;

Note Well

N.B.: The j-shu, more likely than not, may be associated a Mr. Jim Shu who is a former employee that was terminated for poor conduct. Additionally, jtom88917, more likely than not, may be associated with Tom Johnson who is currently under a limited scope of investigation for policy violations. As of now, Mr. Johnson has not had a full audit of his device.

With Regards,

/s/ Dennis Keritsis.

[11] Duplicate emails were removed; however, this is a duplicate to the human eye. This is part of the final results and as such should not be removed. Invisible characters can meddle with sort -u possibly. Sanity check was done and the result continued to appear.

8. HoP 14-4 Memorandum

Computer Forensic Analysis Report

Attorney Work Product

Attorney-Client Privilege

INTERNAL MEMORANDUM FOR Mr. Ralph Benson

Office of General Counsel

Jun 11th 2022

FROM: Dennis Keritsis, Digital Forensic Investigator

IT Security Department

SUBJECT: Acquisition of Email

Subject(s) Jim Shu (aka. j_shu); Tom Johnson

Introduction

Following the most recent memo, which comprised of a list of unique nine (9) emails, wherein said nine (9) emails may be associated with a Mr. Tom Johnson and a Mr. Jim Shu, Mr. Benson from the Office of General Counsel has corresponded with the instant Examiner for email retrieval.

1.28. Support Requested

Mr. Ralph Benson has requested a specific email with subject line “Sample 1” and sent to j_shu@gmx.us and from 1060waddisonst@gmx.us account.

1.29. Statement of Compliance

I Examiner Keritsis assets that I am sufficiently skilled in digital forensics. I understand that my opinions are based on fact. I have no financial interest in the manner. The facts in this report are recorded to the best of my knowledge and ability. I attest these to be true in accordance with company policy.

1.30. Tools

∞ **Autopsy on Windows–** Version 4.19.3

According to Sleuthkit.org: "Autopsy® is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools." Further , the instant Examiner utilized a hash database herein to upload MD5 hash values for forensic and programmatic searching of files within large images files. Further still, Autopsy was used to generate an Excel report to extract MD5 hash values.

∞ **Microsoft Excel**

∞ **Microsoft Notepad**

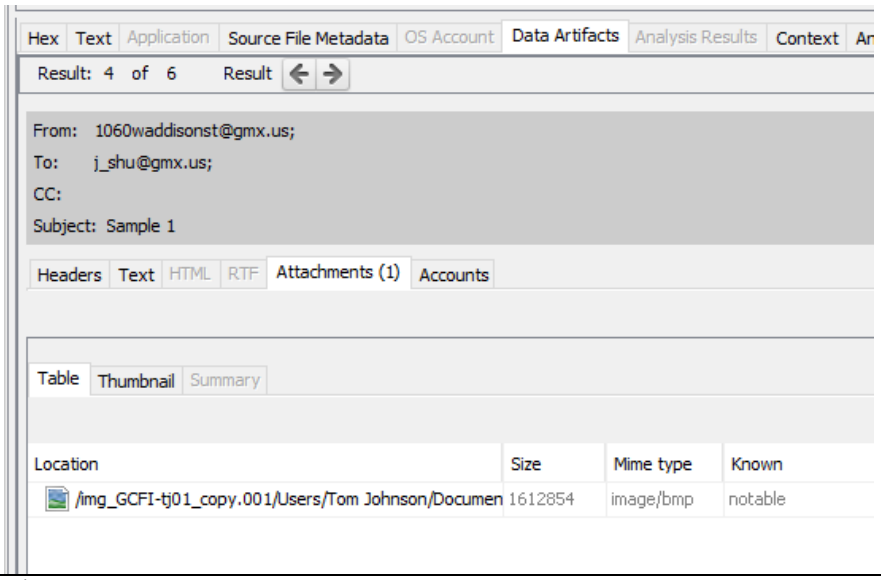
1.31. Findings

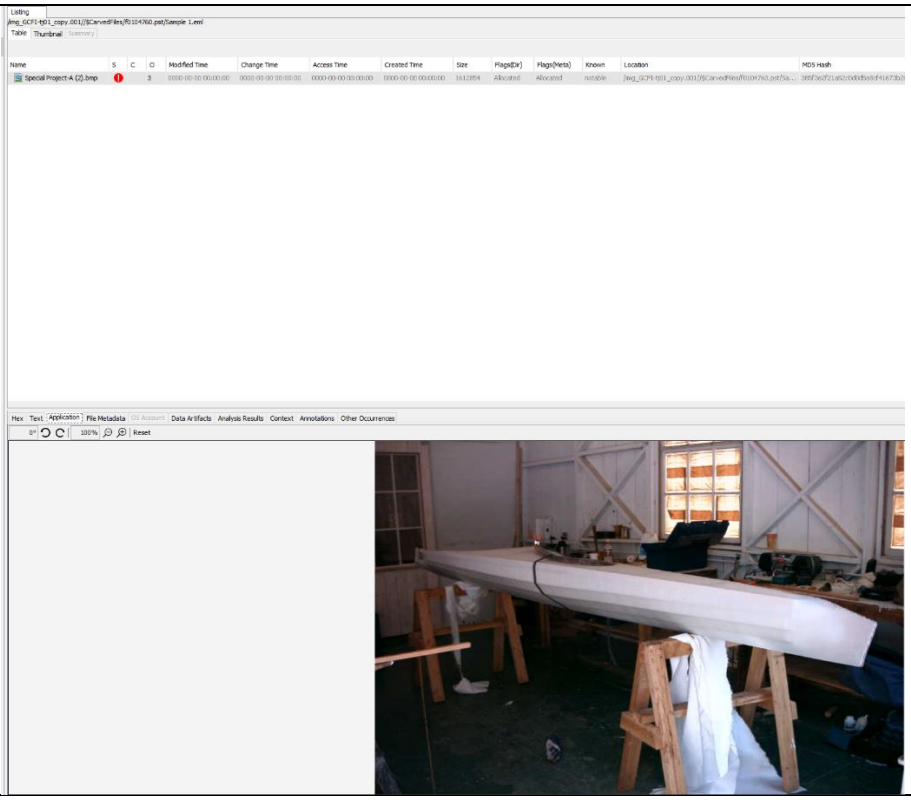
This section will explore the relationship between Mr. Shu and Mr. Johnson. Further, through a retroactive analysis of memo's past, a link will be determined.

1.31.1. Matching of Forensic Copies

Step 3 instructs Examiners to navigate to Views, By Extension, and Images. This is not needed as an Examiner may right-click on the file in the "Location" column in the exhibit below and directly hyperlink to the image attached to the respective email. This is seen in the first screen shot. The second screen shot is the respective attachment. The last screen shot is an extracted file.

EXHIBIT A Autopsy Screen Shot (Fig. 3-17 Step 3)

Software Evidence Showing "Location" Column with Hyperlink to IMG Attached	**Autopsy** 
Evidence Showing Contents of Email in Plaintext	Jim, Here's sample for the investor. Tell him or her that I'll need cash if they want any more information. Tom

Evidence Hyperlinked to Attachment	

After hyperlinking and viewing the photo, the instant Examiner extracted the file and saved it locally on his machine. Hash (**385f3e2f21a52c0d0d5e8cf41673b26f)** is a well-known hash associated with Special Project A that was found on Mr. Tom Johnson's device back in the First Memorandum addressed to Mr. Harry Mudd. Indeed, this was determined (earlier) to be hidden by Mr. Johnson as this was originally found in the /$RECYCLE.BIN and //$CarvedFiles. As such, there is a link between Mr. Shu and Mr. John with respect to kayak and Special Project A.[12]

EXHIBIT B Extracted File and Metadata

Software	**Autopsy**
File Name(s)	**3 - Special Project-A (2)**
File Type	**.bmp**
Hash (MD5)	**385f3e2f21a52c0d0d5e8cf41673b26f**
File Path	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Pictures\Part 2\HoP14-4\Pictures
Evidence Picture as .bmp	
Evidence Metadata	Metadata Name: /img_GCFI-tj01_copy.001//$CarvedFiles/f0104760.pst/Sample 1.eml/Special Project-A (2).bmp Type: Derived MIME Type:

[12] Further consideration is required for a link between bicycles and Mr. Shu.

[redacted]	image/bmp Size: 1612854 File Name Allocation: Allocated Metadata Allocation: Allocated Modified: 0000-00-00 00:00:00 Accessed: 0000-00-00 00:00:00 Created: 0000-00-00 00:00:00 Changed: 0000-00-00 00:00:00 MD5: 385f3e2f21a52c0d0d5e8cf41673b26f SHA-256: dea936e195f6de93366dfa20758c166f9a0644e240add9a7ae900f01f7669f0b Hash Lookup Results: BAD Internal ID: 424582

An HTML report was generated with all the IMGs attached.

EXHIBIT C HTML Screenshot from Generator (Fig. 3-18 Step 5)

Software Evidence	**Autopsy**

Autopsy Forensic Report

HTML Report Generated on 2022/06/11 08:29:20

Case:	Special Project A-1
Number of data sources in case:	3
Examiner:	Dennis Keritsis

Image Information:

GCFI-bs01_copy.001

Timezone:	America/New_York
Path:	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Downloaded\Forensic Copies\GCFI-bs01_copy.001

GCFI-dr01_copy.001

Timezone:	America/New_York
Path:	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Downloaded\Forensic Copies\GCFI-dr01_copy.001

GCFI-tj01_copy.001

Timezone:	America/New_York
Path:	C:\Users\denni\OneDrive\Desktop\WMU Masters\CYIS6730 War\Labs\Lab3\Downloaded\Forensic Copies\GCFI-tj01_copy.001

Software Information:

Autopsy Version:	4.19.3
Data Source Integrity Module:	4.19.3
Email Parser Module:	4.19.3
Embedded File Extractor Module:	4.19.3
Extension Mismatch Detector Module:	4.19.3
File Type Identification Module:	4.19.3
Hash Lookup Module:	4.19.3
Interesting Files Identifier Module:	4.19.3
Keyword Search Module:	4.19.3
PhotoRec Carver Module:	7.0
Picture Analyzer Module:	4.19.3
Recent Activity Module:	4.19.3

1.32. Conclusion

Dear Mr. Benson:

Important: Before reviewing the contents herein in detail, please review a first memorandum addressed to Mr. Harry Mudd of the IT Department. Mr. Mudd is a Manager there and should have a corresponding Memorandum TITLED "Computer Forensic Analysis Report […] MEMORADUM FOR Harry Mudd…" Please review corresponding Exhibit C and E and note the MD5 hash of **385f3e2f21a52c0d0d5e8cf41673b26f** accordingly.

Upon review, the instant Examiner has come to the conclusion that, Mr. Johnson is more likely than not, colluding Mr. Shu, Mr. Shu being a disgruntled employee for being readily terminated. In the past, Mr. Shu has had behavioral problems associated with clients. Mr. Shu was recommended to be fired at or around Dec. 1st 2016. Come now, in 2017, he continues to be embroiled in the affairs with our company. Primarily, he is associated with meddling in the company's affirms with our kayaks and Special Project A.

No strong determination has been made with bicycles and Mr. Shu however.

With Regards,

/s/ Dennis Keritsis.

9. Connections on Investigation for Full Audit

To CEO Sam Clemens, Mr. Ralph Benson, and to whom this may concern:

Our company as a respect for personal privacy, integrity, and equity. We are not ones to pry into the private lives of our employees which may include the reading of private mails. We waive this right for our employees out of respect. As such, this why we limit the scope of our investigations in a limited capacity when there is cause for concern. The question presented before our is:

Whether a Full Audit of Mr. Tom Johnson's Computer is Justified?

In chronological order, the facts will be distilled. Originally in Memo #1, Mr. Harry Mudd of the IT department gave cause for concern was Mr. Tom Johnson had violated some company policies. In a limited scope investigation, there was a determination that Mr. Johnson was associated with sensitive company information and attempted to hide said sensitive information at or around 2017-06 to 2017-10. It was found that Mr. Johnson was associated with our company's kayak project of Special Project A.

At Memo #2, and at the behest of Mr. Swartz, Mr. Mudd wished for the instant Examiner to make a further, supplemental determination on Special Project A again and further include bicycling material. At the end of this investigation, it was determined by the instant Examiner that Mr. Johnson harbored more material with Special Project A, and harbored *additional* biking material. These dates ran concurrent with the findings in Memo #1.

At Memo #3, and working in conjunction with legal counsel, a list of unique non-registered suspect email was presented to counsel. Additionally, the instant Examiner noted that emails in the list appear to be, more likely than note, associated with both (i) Mr. Johnson, and now (ii) Mr. Shu.

At Memo #4, and again working with legal counsel, an alarming connection was made as a whole. Mr. Shu and Mr. Johnson appear to be, more likely than note, colluding with one

another with an external investor. Further, Mr. Shu was terminated on Dec. 2016 but even 6 months to one year later, he is still in communication with at least one individual working at our company—Mr. Johnson. The instant Examiner noted, in a retroactive analysis, that Mr. Benson, primary legal counsel of whom the instant Examiner is working with, should review a corresponding MD5 of associated our company's kayak and Special Project A. Put another way, come now full circle, Memo #1 and Memo #4, when viewed as a whole, show an alarming pattern.

Simply put, Mr. Johnson is most likely colluding with Mr. Shu a disgruntled employee and possibly forwarding Mr. Shu sensitive material for an external investor. This Examiner has found this determination good and herein proper.

With Regards,

/s/ Dennis Keritsis.

10. Determination of Full Audit being Warranted

To CEO Sam Clemens

WHEREFORE, I Mr. Ralph Benson, upon review of the Forensic Examiner's determination, HEREBY advise this company to perform a full audit of Mr. Tom Johnson's computer.

/s/ Ralph Benson