**RICK AND MATENSON CASE FILE**

**Forensic Investigators: Jerin Verghese, Yash Shrivastava, Vedant Kale**

**A picture containing text, clipart, sign, flag

Description automatically generated**

**Cover Sheet**

**Confidential Material Enclosed**

**Only Authorized Individuals Should View Beyond This Cover Sheet**

# Summation

The case begins with an investigation of a black USB thumb drive provided by Mr. David Smith (owner of the warehousing company). Recently, Mr. Smith received complaints from the female employees that the male employees of the organization are involved in watching pornography during office hours. As per the Access Use policy, viewing pornography and getting involved in sexual harassment is prohibited. Mr. Smith believes that the culprit is from the Information Technology (IT) department and is trying his best to cover their tracks. He later mentioned two names Bob Masterson (IT Director) and Rick Bell (the Director of the Accounting Department) who he thinks are the possible offenders and had provided the media data of these users to examine for evidence.

Mr. Smith hand-delivered the USB thumb drive to me. As soon as I received the drive I made my way to the forensics lab and preserved the thumb drive in a safe. Then, I made an exact copy of the thumb drive using an FTK imager tool. Later, I verified the hash values of the original drive, and a copy of the same to check if it is verifying or not, and it was matched successfully. The proof for matching the hashes has been provided in Figure 3. The data was examined using two forensics tools namely Autopsy and FTK Imager. Copies of the files found in the Autopsy were generated for examination. The files retrieved using Autopsy were cross verified using an FTK imager and we got the exact count of files in both tools.

A deep investigation of the thumb drive reveals some significant files and evidence that certainly corroborate Mr. Smith’s concerns about Male employees in the IT department (Bob Matenson and Rick Bell) being involved in viewing pornography and sexual harassment during office hours which is against User Access Policy. Along with that, the three Microsoft Word files were password protected. This directs toward the fact that they were very aware of the consequences of the same, and hence they were very good at covering their tracks. Along with this, a total of six images mixed with cats and dogs were retrieved from the thumb drive. There are a total of 5 jpeg files and a single gif file. This contained proof of graphic pornography that was dug out from the USB drive. This proves that Mr. Bob Matenson and Rick Bell were watching adult as well as child porn. To further notice, the metadata of the Word files shows that the files were created in a period of a longer interval. This concludes that this misconduct happened somewhere within a timeframe of 5 years from 2001 to 2006. All three Microsoft Word files, namely 00001.doc, 00002.doc, and 00003.doc were created by Mr. Matenson and he also modified them last. Also, the files were password protected, and Mr. Matenson set “modify password” on the file as well. This indicates that he did not want any other person to access/change that file.

The \_0001-word document consisted of the following message “**Ricardo mi amigo, I sent you some specal pix. I sepcally love abby we have spent good times together. There are also some older” ones.** This clarifies Bob was involved in sexual harassment with a female employee named abby. Since he had sent it to Rick, it makes it clear that Rick too is involved in these activities along with Bob. The Word file was password protected which implies Bob didn’t want anyone to view the contents of this file. Furthermore, if you concentrate on the last line in Word file 00001.doc, he mentioned “**Older ones**”. This indicates that some older female employees are potential victims of sexual harassment. This document was password protected and it was reserved for modification by Mr. Matenson only. This means that he did not want any other person to access or view or change the content of the file. Another clear indication of **covering the tracks**.

The \_00002 words consisted of the following message “**Ricco, more do you want more. Do you want younger or older”.** This message was written for Mr. Rick Bell. The options young and old show that Mr. Matenson is asking Rick Bell for his choice if he wants younger or older. This is a clear indication that Mr. Robert Matenson was engaged in sexual harassment activities with his fellow female coworkers of different age groups (young and old). This document was password protected and it could only be modified by Robert Matenson. This indicates that Robert Matenson did not wish other people to access or view the same.

The \_0003-word document consisted of the following message “**Rick, I am sending these with codewords because I don’t trust emails. The FBI can see it. What do you think of them”.** He didn't want the FBI to find out, Bob was sending Rick photographs with codes. Bob said he doesn't believe in emails as they could be intercepted or accessed by the FBI. Also, Bob asked Rick for his thoughts on the images he had forwarded to Rick. This document was password-protected and reserved by Robert Mastenson for editing, indicating that he did not want others to have access to or examine its contents—yet another blatant example of "covering his tracks.”

Moreover, six photos and files 000004-000009 were recovered during the media recovery and examination process. Files 000004, 000005, and 000008 were JPEG files and each had a cat which is considered “kiddie porn” as defined in the state of Illinois. Files 000006, 000007, and 000009 each had a photo of a dog which is considered “adult pornography” as defined in the state of Illinois.

The obtained six photo files represent clear proof that Bob Mastenson and Rick Bell were involved in exchanging child as well as adult pornography graphical images. This evidence goes in coordination with the evidence obtained from the three MS Word documents referred to in the previous section of this report. This provides a clue into the MS Word document (000001 doc) authored by Bob Mastenson and referenced “Abbey” as the female employee victim of sexual harassment. This leads to the conclusion that Bob Mastenson was engaged in sexual harassment with female employees in the warehousing firm. The rest of the photos represent proof that Bob Mastenson had sent photos of adult as well as child pornography to Rick Bell.

To conclude, the proofs obtained and analyzed from all three Word documents that were authored by Mr. Matenson and sent to Rick Bell, along with the six graphical images of child and adult porn provide concrete evidence that Bob and Rick were involved in viewing porn and sexual harassment during office hours. As the thumb drive was formatted, this shows that Bob and Rick know how they should cover their tracks. With all these, it can be concluded that Mr. Smith’s concerns are valid, and Bob and Rick were involved in viewing pornography and sexual harassment.

There were some files which do not provide any links that can be used to prove two employees Bob and Rick guilty. The rest of the files were safely returned to David Smith, owner of the warehousing firm.

**Table of Contents**

[1. Summation 2](#_Toc132415278)

[2. Analysis 7](#_Toc132415279)

[a. Media 7](#_Toc132415280)

[Fig 1- Posterior view of USB thumb drive 8](#_Toc132415281)

[Fig 2- Anterior view of USB thumb drive 9](#_Toc132415282)

[Fig 3- Hashes of original and backed-up media. 10](#_Toc132415283)

[b. Files 10](#_Toc132415284)

[3. Documents 11](#_Toc132415285)

[a. File1- 00001.doc 11](#_Toc132415286)

[Fig 4- A message from Bob to Rick 12](#_Toc132415287)

[Figure 5 - Metadata Information of \_000001 doc 13](#_Toc132415288)

[b. File2- \_00002.doc 13](#_Toc132415289)

[Fig 6: A message from Rob Matenson to Rick Bell 14](#_Toc132415290)

[Fig 7: Metadata of 00002.doc file 15](#_Toc132415291)

[c. File3- \_00003.doc 16](#_Toc132415292)

[Fig 8: Message from Robert to Rick 17](#_Toc132415293)

[Fig 9: Metadata of \_00003.doc file 18](#_Toc132415294)

[4. Photographic Images: 19](#_Toc132415295)

[a. File001- 000004.jpg: 19](#_Toc132415296)

[Fig 10 - Image of Cat referring to Child Pornography 20](#_Toc132415297)

[Fig 11- Metadata of Fig 10 20](#_Toc132415298)

[b. File002- 000005.jpg: 20](#_Toc132415299)

[Fig 12 - Image of Cat referring to Child Pornography 21](#_Toc132415300)

[Fig 13- Metadata of Fig 11 21](#_Toc132415301)

[c. File003- 000006.jpg: 22](#_Toc132415302)

[Fig 14: Showing the image related to adult pornography. 22](#_Toc132415303)

[Fig 15: Metadata showcasing the MD5, SHA-256 values along with Modification dates 23](#_Toc132415304)

[d. File004- 000007.jpg: 23](#_Toc132415305)

[Fig 16: Showing the image related to adult pornography. 24](#_Toc132415306)

[Fig 17: Metadata showcasing the MD5, SHA-256 values along with Modification dates 24](#_Toc132415307)

[e. File005- 000008.jpg: 24](#_Toc132415308)

[Fig 18- Photo of Cat “Child Pornography” 25](#_Toc132415309)

[Fig 19- Metadata of Fig 17 26](#_Toc132415310)

[f. File006- 000009.gif: 26](#_Toc132415311)

[Fig 20- Photo of Dog “Adult Pornography” 26](#_Toc132415312)

[Fig 21- Metadata of Fig 19 27](#_Toc132415313)

[Appendix A: Full Report 28](#_Toc132415314)

[Appendix B: Policy on Collection of Evidence 28](#_Toc132415315)

[Appendix C: Policy on forensically sterile media 28](#_Toc132415316)

[Appendix D: Glossary 28](#_Toc132415317)

[Appendix E: Credentials 29](#_Toc132415318)

[Technical Aspects of Data Retrieval 29](#_Toc132415319)

[Software used during the forensic examination and procedures: 30](#_Toc132415320)

# **Analysis**

Forensic Examiner: Jerin Verghese, Yash Shrivastava, Vedant Kale

## **Media**

Mr. David Smith, the owner of the warehousing firm handed me the USB thumb drive, which he thinks was used by two of his employees in the firm to get involved in sexual harassment and in watching pornography on their computers provided by the company during work hours. The USB thumb drive was transparent and shaded dark gray from the front. The size of the drive is 16GB and has serial number BL174326240W. The thumb drive can be accessed both on traditional computer devices and mobile devices as it has a mini-USB-C port that can be connected to mobile devices. An actual photograph of the thumb drive is provided in the figure below with anterior and posterior views.

A picture containing text, indoor, case

Description automatically generated

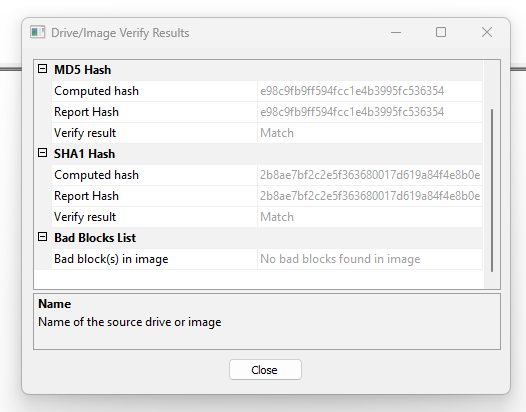
### Fig 1- Posterior view of USB thumb drive

A picture containing weapon

Description automatically generated

### **Fig 2- Anterior view of USB thumb drive**

As soon as I received a thumb drive from Mr. Smith, I created a backup image of the same using an FTK imager and started working on the backup image. The resulting copy was named CS\_1.001. The computed MD5 checksum was e98c9fb9ff594fcc1e4b3995fc536354 and the reported hash was the same resulting in MD5 in the match. Similarly, the computed hash was 2b8ae7bf2c2e5f363680017d619a84f4e8b0e and resulted in the same. Both were produced during the creation of the backup, and both were matched. The below figure shows the same.



### **Fig 3- Hashes of original and backed-up media.**

### **Files**

The USB backup drive CS\_1.001 contained a total of 28 files. All the files were deleted to cover the tracks; however, I retrieved all the files using Autopsy version 4.20.0 and FTK Imager 4.7.1.2 and found the exact same count of deleted files. There was a total of 5 .jpg files named 000004 to 000009. A total of 6-word files are named from 000001 to 000003 and similar files are exhibited as prefixes.

### **Documents**

### **File1- 00001.doc**

This file is a Microsoft Word document file. It was generated by using Microsoft Word 97-2003. It was stored under the file name 000001.doc on the given USB thumb drive. The file was password protected and cracked using the Passware tool and the password decrypted was “special”. The size of the Word file is 19KB and it was created and modified by Robert Mastenson on 09-04-2002 at 4:32 PM.

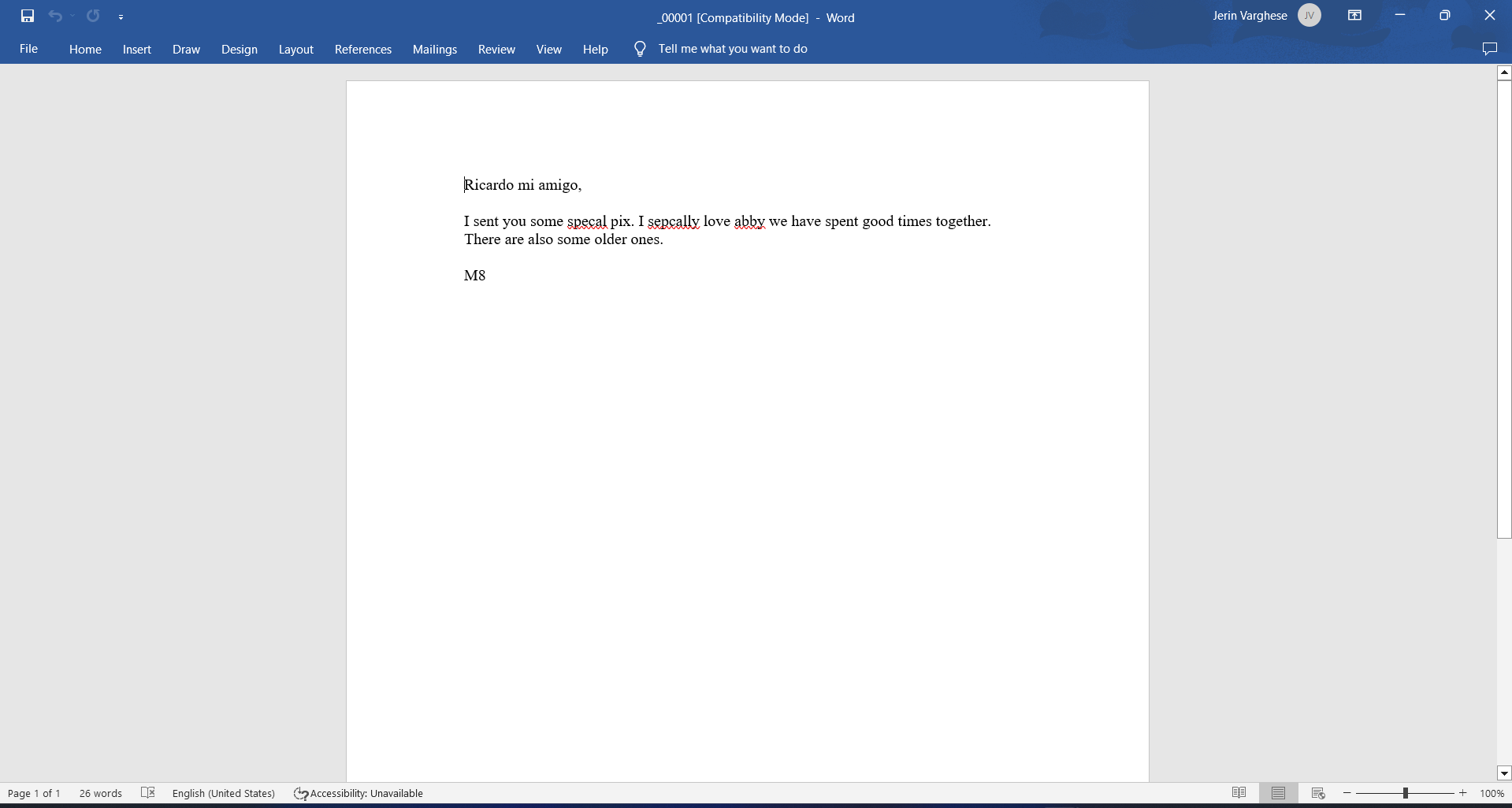
The Word document \_0001 contained the following message sent by BOB to Rick.

**“Ricardo mi amigo,**

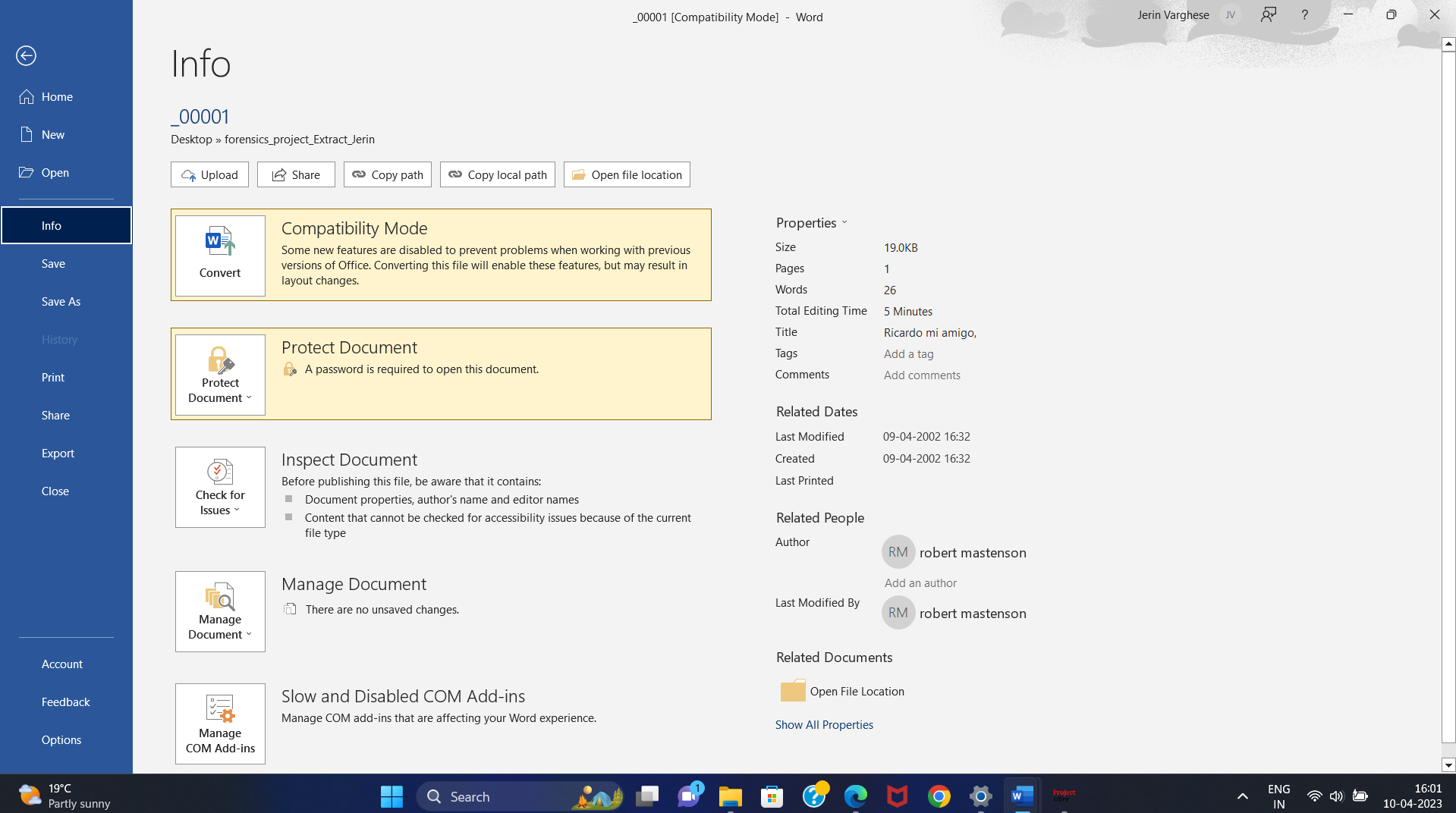
**I sent you some specal pix. I sepcally love abby we have spent good times together.**

**There are also some older ones.”**

This indicated that Bob had sent some pics to Rick. Bob specifies he loved “abby” and had spent a great time together. This clarifies Bob was involved in sexual harassment with a female employee named abby. He also mentions there are some older ones which could be the pics of other female employees who would have been the victim of this harassment. Since he had sent it to Rick, it makes it clear that Rick too is involved in these activities along with Bob. The Word file was password protected which implies Bob didn’t want anyone to view the contents of this file.



### **Fig 4- A message from Bob to Rick**



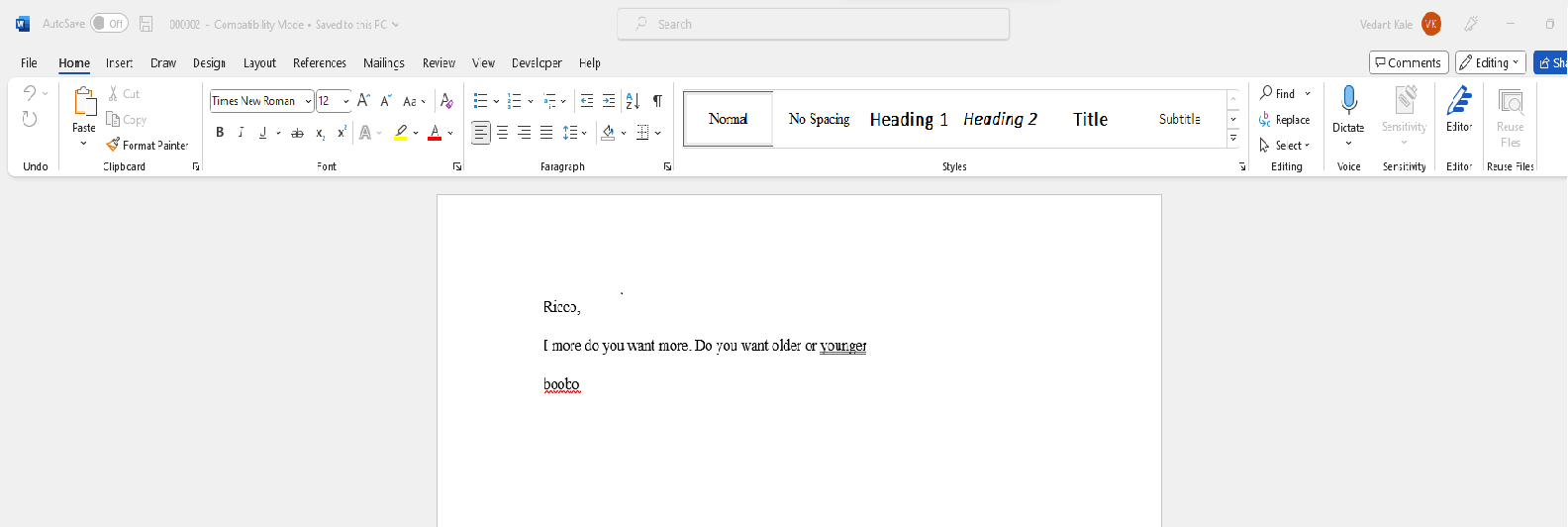
### **Figure 5 - Metadata Information of \_000001 doc**

### **File2- \_00002.doc**

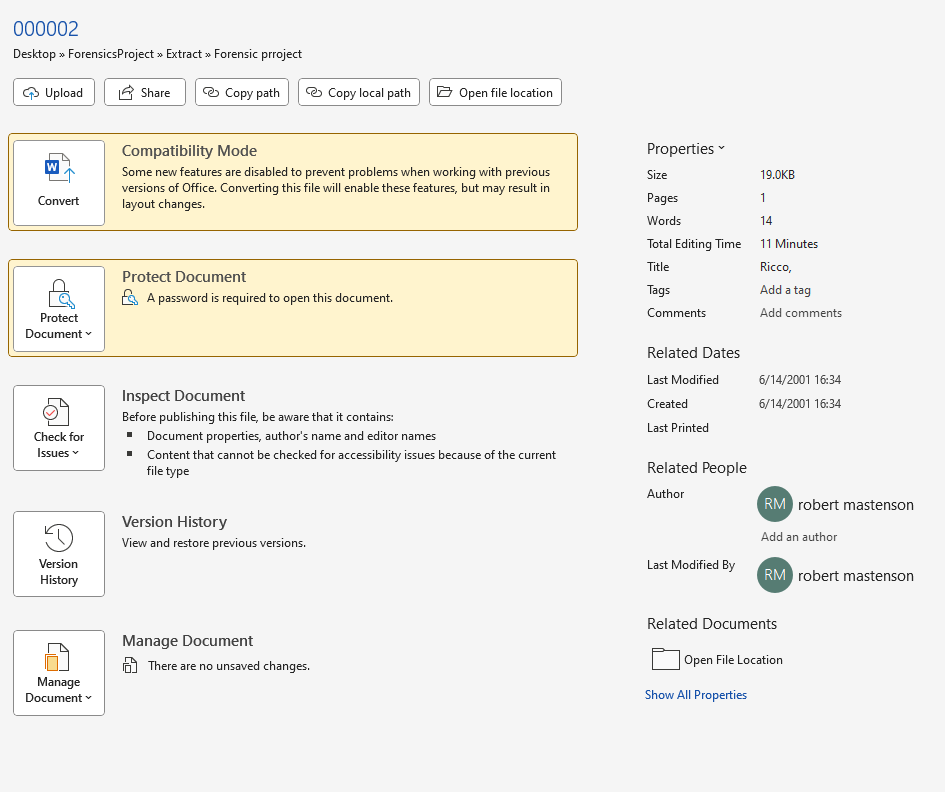
This file is a Microsoft Word document file. It was generated by using Microsoft Word 97-2003. It was stored under the file name 000002.doc on the given USB thumb drive.

The contents of the file are recorded below in the below Figure (fig number). Furthermore, the details include metadata of the said word file in the below figure (fig number). This file was encrypted with a password and the size of the file is 19K. The creator of this file is Robert Matenson and the date of creation is 14th June 2001 at 16:34:00. Additionally, the file was last modified by Robert Matenson on 14th June 2001 at 16:34:00.

As the file was encrypted with a password, I cracked a password “picture” with the Passware tool successfully. The file was included with a message concluding that Robert has more cat and dog pictures if Rick is asking for more. This message was specifically written for Rick Bell. Robert was asking if Rick wants older or younger ones. This is a clear indication that Mr. Robert Matenson was engaged in sexual harassment activities with his fellow female coworkers of different age groups (young and old). This document was password protected and it could only be modified by Robert Matenson. This clearly indicates that Robert Matenson did not wish other people to access or view the same. This is a crystal-clear indication of Covering his tracks. The password for both opening and modifying the document is “picture” all spelled in lowercase. The file appears to have been deleted by Bob from the thumb drive. Another indication of hiding and covering the tracks. The file was successfully retrieved using Autopsy and has a hexadecimal string associated with it “DOCF11E0A1B11AE1”.



### **Fig 6: A message from Rob Matenson to Rick Bell**



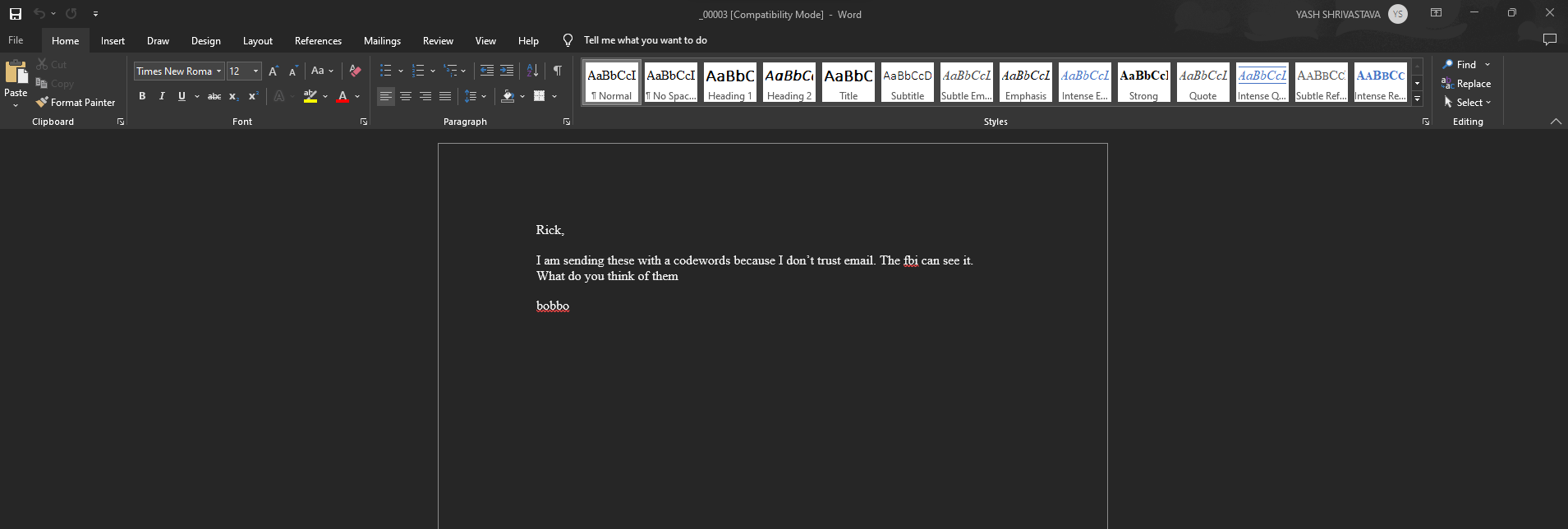
### **Fig 7: Metadata of 00002.doc file**

### **File3- \_00003.doc**

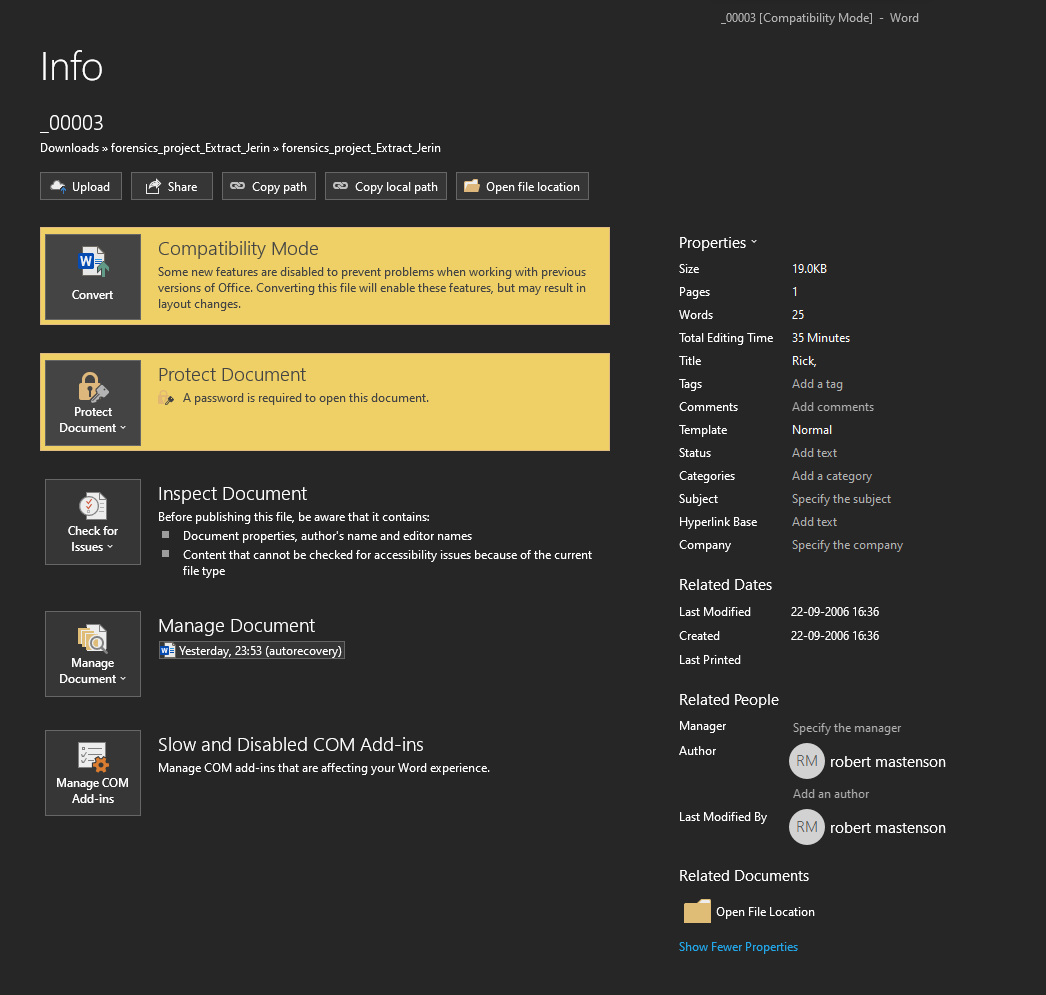
This is a Microsoft Word document. It was generated using Microsoft Word 97-2003. It was stored with the filename **\_00003.doc** on the given USB thumb drive.

The content of the file is below in the figure attached. Furthermore, the details include metadata of the said word file in the figure below. The file was encrypted with the password with a file size of 19 KB. The file was created by **Robert Mastenson on 22 September 2006 at 16:36:00.** Additionally, the file was last modified by **Robert Mastenson on 22 September 2006 at 16:36:00.**

As the file was protected with a password, I used the ***Passware tool*** to successfully crack the password. The password happens to be **“collect”.** The file contained a message from Robert Mastenson which was along the lines that because he didn't want the FBI to find out, Bob was sending Rick photographs with codes. Bob said he doesn't believe in emails as they could be intercepted or accessed by the FBI. Also, Bob asked Rick for his thoughts on the images he had forwarded to Rick. This document was password-protected and reserved by Robert Mastenson for editing, indicating that he did not want others to have access to or examine its contents—yet another blatant example of "covering his tracks." The password is "collect" in all lowercase and can be used to access and edit the document. The file was then deleted from the USB thumb drive which is a clear indication of covering his tracks. It was received using Autopsy and has a hexadecimal string value of **DOCF11E0A1B11AE1**

****

### **Fig 8: Message from Robert to Rick**

****

### **Fig 9: Metadata of \_00003.doc file**

### **Photographic Images:**

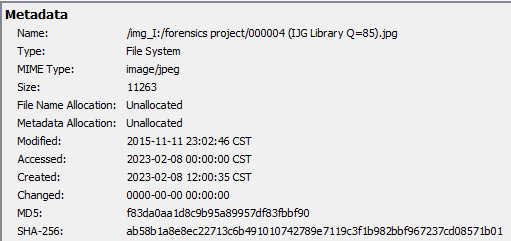
### **File001- 000004.jpg:**

File001, which is saved as 000004 is an Image file with a JPEG extension. The file was found under the RecycleBin/Forensics/Project/pics directory. The size of the file is 11KB with a resolution of 196x210. It was stored in the following path in my PC: C:\Users\Jerin\Desktop\forensics\_project\_Extract\_Jerin\000004 (IJG Library Q=85).jpg

The image contained a photo of a cat. Cat image refers to “child pornography” as per the law defined in the state of Illinois. This provides conclusive evidence that BOB and Rick were involved in the viewing of pornography during office hours. Apart from that the message retrieved from the word documents \_000001, \_000002, \_000003 clarifies that these were the images that were exchanged between them. Also, it was mentioned in the letter \_000003 as they were worried about being caught by the FBI, they were not sending those images via emails and were using code words for exchanging data. All this evidence gives solid proof that Bob and Rick were involved in viewing pornography as well as sexual harassment activities during working hours.



### **Fig 10 - Image of Cat referring to Child Pornography**

****

### **Fig 11- Metadata of Fig 10**

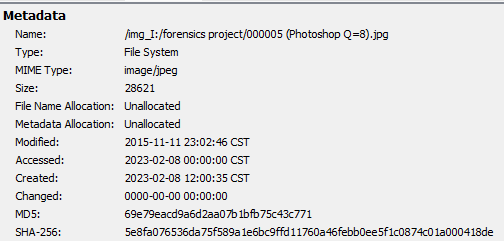
### **File002- 000005.jpg:**

File002, which is saved as 000005 is an Image file with a JPEG extension. The file was found under the RecycleBin/Forensics/Project/pics directory. The size of the file is 28KB with a resolution of 256x372. It was stored in the following path on my PC: C:\Users\Jerin\Desktop\forensics\_project\_Extract\_Jerin\000005 (Photoshop Q=8).jpg.

The image contained the photo of a cat. Cat image refers to “child pornography” as per the law defined in the state of Illinois. This provides conclusive evidence that BOB and Rick were involved in viewing pornography during office hours. Apart from that the message retrieved from the word documents \_000001, \_000002, \_000003 clarifies that these were the images that were exchanged between them. Also, it was mentioned in the letter \_000003 as they were worried about being caught by the FBI, they were not sending those images via emails and were using code words for exchanging data. All this evidence gives solid proof that Bob and Rick were involved in viewing pornography as well as sexual harassment activities during working hours.



### **Fig 12 - Image of Cat referring to Child Pornography**

****

### **Fig 13- Metadata of Fig 11**

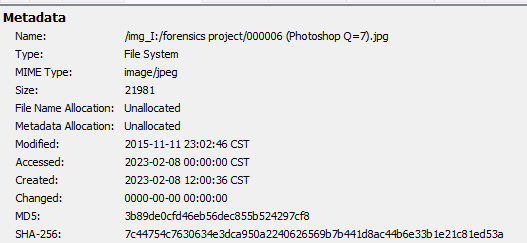
### **File003- 000006.jpg:**

File 003, which is saved as 000006.jpg, is a typical photographic image file. The Recycle Bin/Forensics Project/pics directory is included in this file. It has a 22 KB file size with a resolution of 320x240. It was last modified on 2015-11-11 at 23:02:46 CST.

It contains a picture of a dog which is classified as adult pornography in the state of Illinois. And is a clear indication that Robert was involved in adult pornography. When Robert mentioned that he was going to send some older images and that he did not trust email for delivering those photos, it appears that this photo was sent along with the letter (\_00003.doc). Mastenson also mentioned in his letter to Rick Bell that he would send photographs with code words because he was concerned the FBI would be able to view them. This confirms that he indulged in "adult pornography," which is why he did not want the FBI to view the images.



### **Fig 14: Showing the image related to adult pornography.**



### **Fig 15: Metadata showcasing the MD5, SHA-256 values along with Modification dates**

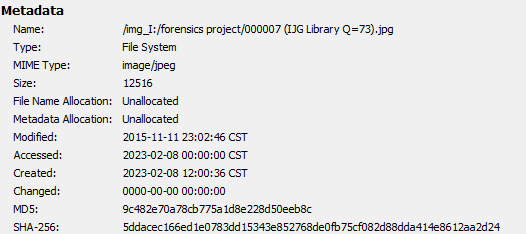
### **File004- 000007.jpg:**

File 004, which is saved as 000007.jpg, is a typical photographic image file. The Recycle Bin/Forensics Project/pics directory is included in this file. It has a 13 KB file size with a resolution of 320x240. It was last modified on 2015-11-11 at 23:02:46 CST.

It contains a picture of a dog which is classified as adult pornography in the state of Illinois. And is a clear indication that Robert was involved in adult pornography. When Robert mentioned that he was going to send some older images and that he did not trust email for delivering those photos, it appears that this photo was sent along with the letter (\_00003.doc). Mastenson also mentioned in his letter to Rick Bell that he would send photographs with code words because he was concerned the FBI would be able to view them. This confirms that he indulged in "adult pornography," which is why he did not want the FBI to view the images.

****

### **Fig 16: Showing the image related to adult pornography.**

****

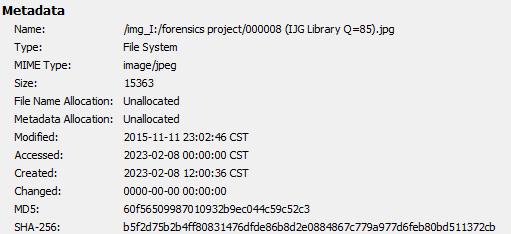
### **Fig 17: Metadata showcasing the MD5, SHA-256 values along with Modification dates**

### **File005- 000008.jpg:**

This file is a standard photographic image file that is stored as 000008. jpg. This file was stored under the Recycle Bin/Forensics Project/pics directory. It contains a hexadecimal header, it has a .jpg extension and the size of the file is 15KB. It is a regular image with a resolution of 264\*269 and it is a standard photographic image file. The image contains a picture of a cat. This strongly indicates that Mr. Matenson was involved in viewing pornography at the workplace. In the \_00003.doc file, Mr. Matenson clearly stated that he will not send these pictures over email as the FBI can see them. Also, in letter 00001.doc Mr. Matenson stated that it was Matenson’s willingness, and in the end, he sent this photo. This indicates solid evidence of engagement in child pornography. The file was created and last modified on 11th November 2015 at 23:02:46 Central time. The image has been inserted below.



### **Fig 18- Photo of Cat “Child Pornography”**

****

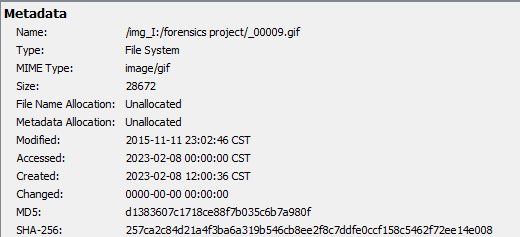
### **Fig 19- Metadata of Fig 17**

### **File006- 000009.gif:**

This file is a standard graphical image file that is stored as 000009. This file was stored under the Recycle Bin/Forensics Project/pics directory. It contains a hexadecimal header, it has a .gif extension and the size of the file is 28KB. It is a regular image with a resolution of 240\*143 and it is a graphical photographic image file. The image contains a picture of a dog. This strongly indicates that Mr. Matenson was involved in viewing pornography at the workplace. In the \_00003.doc file, Mr. Matenson clearly stated that he will not send these pictures by email as the FBI can see them. When looking at \_00002.doc, Mr. Matenson asked Rick Bell, “I have a few more pictures, do you want those? This as well clearly indicates solid evidence of engagement in adult pornography. Additionally, this file was last modified on 11th November 2015 at 23:02 Central time. The image has been inserted below.



### **Fig 20- Photo of Dog “Adult Pornography”**



### **Fig 21- Metadata of Fig 19**

### **Appendix A: Full Report**

Please see the submitted original pen drive entitled with the name labeled as Matenson case file.

### **Appendix B: Policy on Collection of Evidence**

Obtained evidence is labeled with a case number. Once a case number has been assigned to the evidence, a log of that evidence begins, and it is maintained throughout the investigation process. All evidence related to the case is logged and maintained including physical and logical images. All the pieces of evidence are stored safely in the fire-safe locker and are secured by a key. Keys are only issued when, and only when evidence is signed out of evidence lockup. All sign-outs are also stored and maintained on a chain of custody logs which are also stored in a fire safe.

### **Appendix C: Policy on forensically sterile media**

All media used for case investigations is forensically sterile. All media, before its use in a case (i.e., imaging and storage), is sterilized in compliance with the Department of Defense’s disk scrubbing utility. Media considered “new” or “never been used” is not immune from this process. In addition, all used media is sterilized again when it becomes dissociated with a case.

### **Appendix D: Glossary**

Data Carving: A process involving the examination of media for content relating to multiple types of space (i.e., slack space, unused space, unallocated space).

Deleted Files: Files that are removed from the storage space of a piece of media. In most cases and depending on the type of deletion, deleted files can be recovered using computer forensic tools.

USB Drive/Thumb drive/Pen drive: A Universal Serial Bus drive that is pocket size and portable and contains higher storage capacity. https://en.wikipedia.org/wiki/USB\_flash\_drive

Free Space: Unused, but not empty, space on a piece of storage media.

Hash: any well-defined procedure or mathematical function for turning some kind of data into a relatively small integer, that may serve as an index.

JPEG: Joint Photographic Experts Group. A commonly used method of compression for photographic images.

Metadata: Metadata is data about data. Metadata may describe an individual piece of data, content, or a collection of data including multiple content items.

Password-protected files: Many software programs include the ability to protect a file using a password. One type of password protection is sometimes called “access denial.” If this feature is used, the data will be present on the disk in the normal manner, but the software program will not open or display the file without the user entering the password. In many cases, forensic examiners can bypass this feature. Many of the files also contain modified passwords as the owner does not want to allow others to modify them.

### **Appendix E: Credentials**

### **Technical Aspects of Data Retrieval**

1. All equipment and software used in all the procedures in this report have been tested and validated to ensure they are in proper working order and continue to produce the most accurate results. All test media is hashed before and after each validation.
2. When deemed necessary, data examination, retrieval, and data carving are done with the use of two separate but forensically sound methods to validate any findings during the examination.
3. I ran a hash on the original media and noted the value, I then wiped and verified the wipe of the target media.
4. I made an exact copy of the original media to the wiped and verified media. I ran a hash on the original media again and it matched the original value.

### **Software used during the forensic examination and procedures:**

1. Autopsy 4.20.0- Open-source software, free and available for public use.
2. FTK Imager 4.7.1.2- Open-source software, free and available for public use.
3. Passware Kit