Mastenson Case File

Forensic Investigation Report

Forensic Investigators: Lekhana Kikkeri Ramesh (A20526217)
lkikkeriramesh@hawk.iit.edu

Surendar Venkatachalam (A20525010)
svenkatachalam@hawk.iit.edu

Cover Sheet
Confidential Material Enclosed
Only Authorized Individuals Should View Beyond This Cover Sheet

I. Summation

This case involves the examination of a silver USB thumb drive of size 64GB that was obtained from David Smith, the owner of a warehousing firm. Mr. Smith has received reports from female employees alleging that male employees were accessing pornography and participating in sexual harassment during work hours.
Smith stated that his company has an Acceptable Use Policy that restricts how computers are used by employees. The AUP forbids computer users from viewing pornography or engaging in sexual harassment.
Smith is concerned that the offending employee(s) work in his company's Information Technology Division and are familiar with "covering their tracks" when engaged in this type of behavior. The IT Director's name is Robert Mastenson, and he is believed to be talking with Rick Bell, the Accounting Department Director. The major goal, in this case, was to gather any information and evidence that could aid in assessing if Robert Mastenson (director of IT) and Rick Bell (director of accounting) were accessing pornography and engaging in sexual harassment during working hours.
Mr. Smith hand-delivered the USB thumb drive to us. To preserve the original media and avoid making any changes or wiping contents from the USB thumb drive Mr. Smith handed us, we obtained a fresh one and duplicated the original media from it. Then, after establishing a hash value for the original media and noting it, we determined the hash value for the duplicated media and discovered that both the original media's and the copied media's hash values were identical. Further examinations were done only on the copied media.

The USB thumb drive image reveals numerous crucial files that undoubtedly support Mr. Jenkins' worries regarding male workers (Robert Mastenson and Rick Bell) viewing pornography and engaging in sexual harassment during work hours. The three MS Word papers authored by "Robert Mastenson" in particular contained lines of communication between Robert Mastenson and Rick Bell that indicated that they were involved in sexual harassment during working hours. Interestingly, the three MS Word files were password secured, proving that those two directors were skilled at "covering their tracks." Furthermore, the five JPG images and one GIF file containing visual pornography that was extracted from the formatted USB thumb drive demonstrate that Robert Masterson and Rick Bell were viewing adult as well as child pornography. It's worth noting that metadata examination of the three MS Word documents revealed that their creation dates were separated by a few years. This hints at the period of this misconduct, which occurred over five years. Furthermore, Robert Mastenson created Doc 000001 on April 9, 2002. Robert created Doc 000002 once more on June 14, 2001, and Doc 000003 once more on September 22, 2006. All three documents were written for Rick Bell and were saved last by Robert Mastenson. In addition, six photographs were extracted from the formatted USB thumb drive.

The first MS Word document, 000001.doc, had text in it that was addressed to Rick Bell and called him "Ricardo mi amigo," which translates to "Ricardo my friend" in English. It also mentioned that Robert had sent Rick some special pictures. In the same document, Robert added, "I love Abbey and we have spent good times together." He added that he "has some older ones" in his remarks. According to this document, Robert sexually harassed an employee named "Abbey" who was 'maybe' working for the company. Since Rick was the target of the letter or text, it is clear that both engaged in sexual harassment. Additionally, the phrase "older ones" in the final line of the text implies that there may be older female employees who are the targets of sexual harassment. Robert is telling Rick about this so that he can also indulge in this conduct. Another clear example of Robert Mastenson "covering his tracks" is the password-protected document he reserved for modification. This suggests he did not want anyone to access or examine the document's content.

The second MS Word document, 000002. Doc, contains text written for Rick Bell again, this time addressing him as "Ricco" and stating that Robert has more photographs if Rick wants more. Robert inquired whether Rick preferred older or younger children. This plainly shows that Robert is engaging in workplace sexual harassment with female employees of various ages (young and old). This also demonstrates that Robert is offering Rick the option of sexually harassing older or younger female colleagues. This document was password secured and reserved for modification by Robert Mastenson, indicating that he did not want anybody to access or examine the content, yet another clear sign of "covering his tracks."

The third and last MS Word document, 000003. The doc contains text written for Rick. The text indicates that Robert was sending images with code phrases to Rick to avoid detection by the FBI. Robert stated that he does not trust the e-mail. In addition, Robert asked for Rick's feedback on the images he had provided him. This document was password secured and reserved for modification by Robert Mastenson, indicating that he did not want anybody to access or examine the content, yet another clear sign of "covering his tracks."

Moreover, throughout the media recovery and examination process, six photographs, files 000004-000009, were retrieved. JPEG files 000004, 000005, and 000008 each contained a cat, which is considered "kiddie porn" in the state of Florida. Files 000006, 000007, and 000009 all contained a photograph of a dog, which is considered "adult pornography" in the state of Florida. Only file 000009 is a GIF, while the rest are JPEGs.

The evidence from obtaining six photo files shows that Robert Mastenson and Rick Bell were exchanging child and adult pornographic images. This evidence supports the evidence gathered from the three MS Word documents mentioned in the previous section of this study. It's worth noting that the photo file 000009 contains "adult pornography" depicting two individuals having "intercourse." This hints at the MS Word document (000001 doc)

prepared by Robert Mastenson, which mentioned "Abbey" as the female employee who was sexually harassed. This leads to the conclusion that Robert Mastenson engaged in sexual harassment of female warehousing employees.

In conclusion, the evidence obtained and analyzed from three MS Word documents authored by Robert Mastenson and sent to Rick Bell, as well as the six "child and adult pornography" provide solid evidence that Robert Mastenson (IT director) and Rick Bell (director of accounting) were engaged in viewing pornography and engaging in sexual harassment during working hours. Furthermore, the thumb drive media was prepared, confirming David Smith's suspicion that Robert Mastenson and Rick Bell were well-versed in "covering their tracks." Furthermore, metadata examination of the three MS Word documents revealed that they were created by Robert Mastenson over five years, indicating that this type of conduct was occurring for a long period. Furthermore, Mastenson indicated in one letter to Rick Bell that he didn't use e-mail for communication with Rick Bell because he was concerned that the FBI could access the contents of his letters. This demonstrates that Mastenson engaged in illegal behavior, in this case, sexual harassment and child and adult pornography. Based on the evidence thus far, we can definitively state that David Smith's worries were justified in that Robert Mastenson and Rick Bell were engaged in watching pornography as well as sexual harassment at the warehousing firm during working hours.

There were no additional pieces of evidence in the media that were thoroughly examined and returned to Mr. Smith along with this report.

Table of Contents

II. Analysis

Forensic Examiners: Lekhana Kikkeri Ramesh
Surendar Venkatachalam

A. Media

We extracted all the recoverable files from the thumb drive by mounting them into the Standard FTK Imager file as a physical drive. The recovered files' hash values were then exported and saved as a CSV file with the name hash values. We then got the hash value of the whole folder(MD5 checksum: E077C92BE247450B0BD754FBA99A00C5, SHA1 checksum: 248E78C0F0DBF4A702ED2D53F0676E9A9644A1B4). For each file in the folder, we obtained MD5 and SHA1 hash values. Following the hashing, we made a copy of the recovered files and used the copy for further examination. The files' uniqueness will be verified afterward by comparing the beginning and final hash values of the files in the cloned folder. The FTK imager creates an exact bitwise replica of the source disk, which we shall examine. The original folder was titled Project, and the duplicated version was named project1. Further investigations will be conducted on the project1 contents, but the project folder will be kept unaltered.

Examining the thumb drive revealed that it had been formatted because it only displayed the root directory folder. There were no files to be found. We can deduce that the media was formatted at this point. To recover all potentially recoverable files, we used Disk Digger and FTK imager. We analyzed the files retrieved by both applications and found that they were nearly similar. FTK imager gave us the deleted files and their respective folders, so it was easy to process those files. Since the files were in the root directory which required them to be recovered directly from unallocated space, we could render the opinion that data was placed on the device, and then formatted. We found a certain

number of files that validates the concern about company employees watching pornography and engaging in sexual harassment.

Figure 1: 3.5 USB Thumb drive of size 64 GB

B. Files

From the pen drive, we were able to retrieve 9 files that are related to this case. Three of the files were Word documents and they are password protected. To break the password, we used John the Ripper password cracking tool and brute-forced the password for all the files. We also used Metadata++ to further analyze the documents and determine the author, creation, modification date, and any other important information to help with the case.

Documents

File 001: 000001.doc

The file is a Microsoft Word document that was password protected and was created on 2002:04:09 20:32:00(4:32 PM) by Robert Mastenson using Microsoft Word 9.0. We analyzed the metadata of the file using metadata++, a Metadata analysis software and discovered that it is only one page long, titled 'Ricardo mi amigo,' and contains only 20 words. Those with the password were granted read and write access to the file. The file was last edited on 2002:04:09 20:32:00(8.32 PM) by Robert Mastenson.

To brute force the password, we employed John the Ripper, a strong password brute-forcing tool. We were fortunate in locating the special password and were able to open

the document and read its contents. The paper had a message to Ricardo, which could be rick bell, saying "I love Abbey and we have spent good times together," which could indicate that they engaged in sexual harassment with a female employee named Abbey. There is also a note that says, 'There are also some old ones,' which may indicate that there have been several incidents involving older personnel.

Another obvious example of Robert Mastenson "covering his tracks" is the password-protected document he reserved for updating and that was password-protected, implying that he did not want anyone accessing or examining the document's content. The password is "special," and it consists of all lowercase letters. It can be used to access and edit documents.

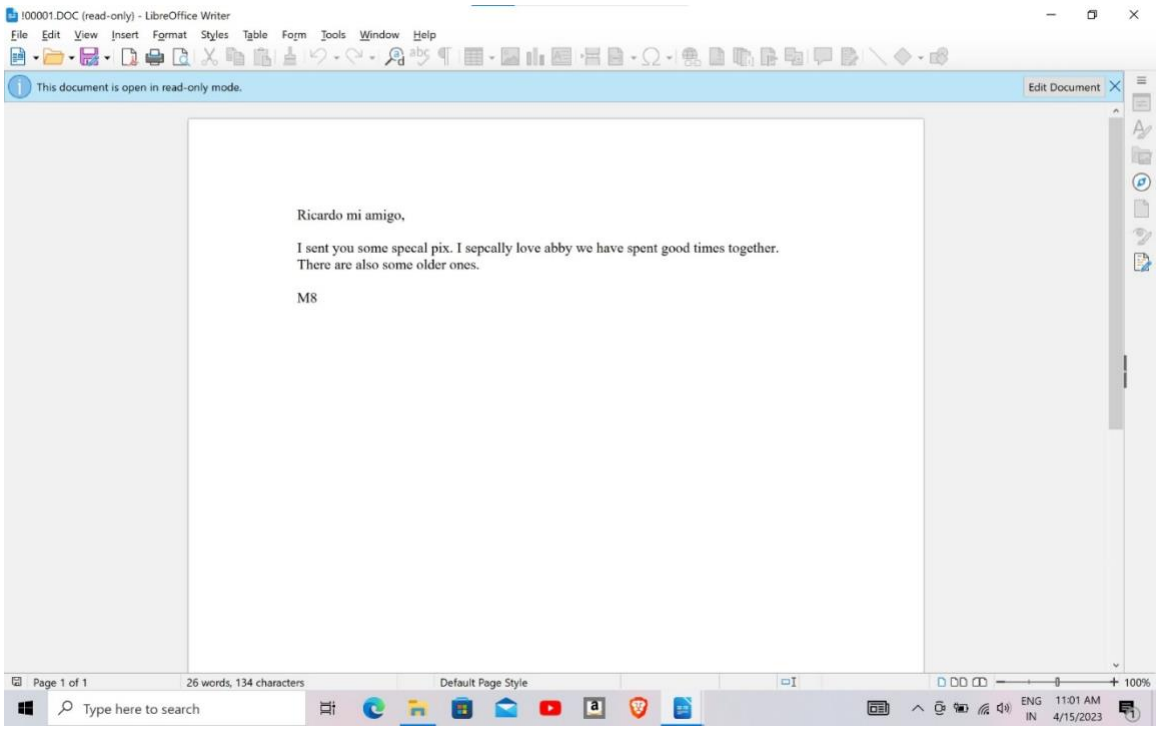

Figure 2- Letter from Robert Mastenson to Rick Bell

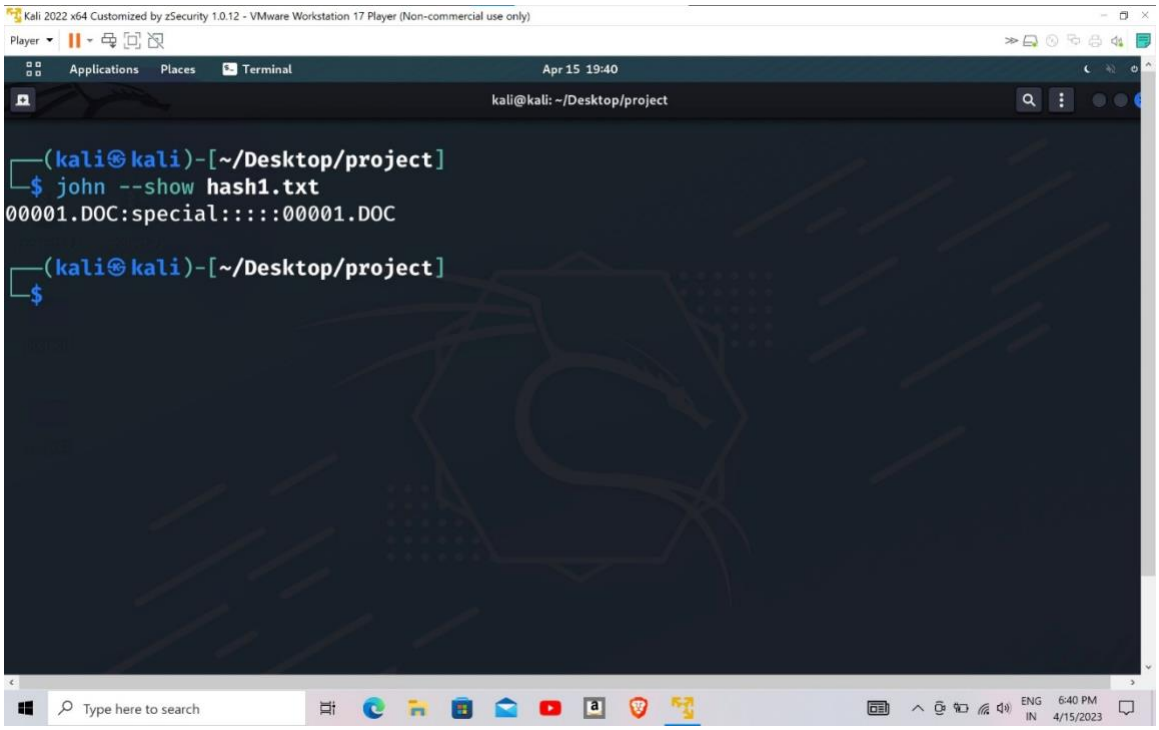

Figure 3: John cracks the !00001.doc password

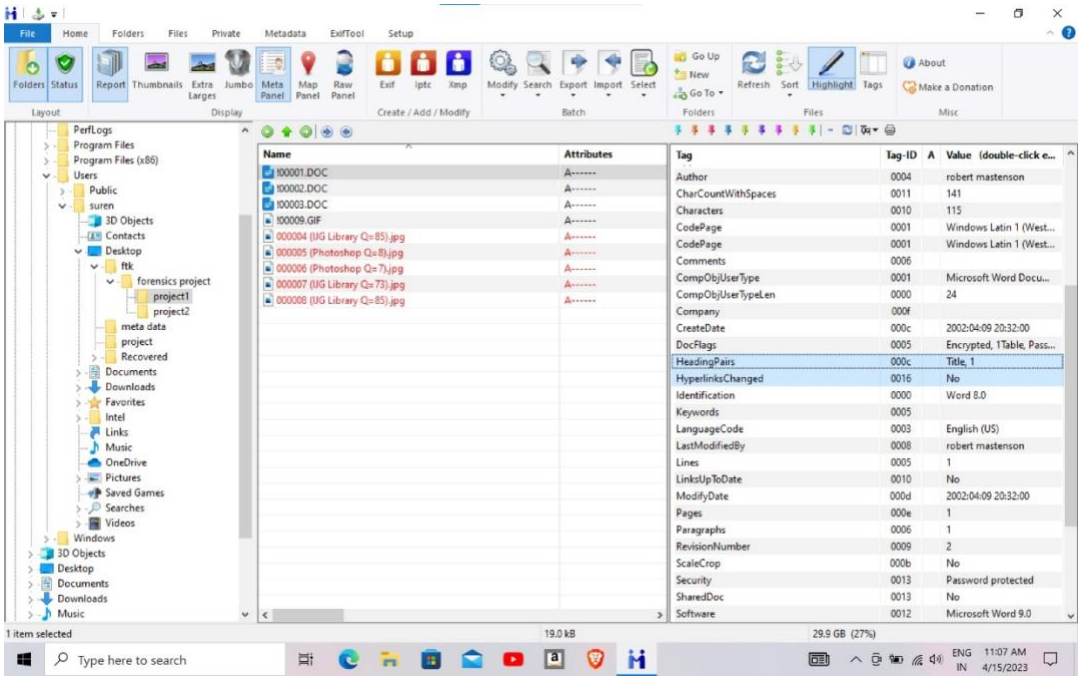

Figure 4: Metadata showing "Bob Mastenson 000001 doc"

File 002: 000002.doc

File 002 is a Microsoft Office Document that was created using Microsoft Word 97-The second file, 00002.DOC, is also a Microsoft Word document that was password secured and was created on 2001:06:14 20:34:00(8.34 PM) by Robert Mastenson. The file's metadata reveals that it is one page long and contains ten words titled 'Ricco,'. Those with the password were granted read and write access to the file. Robert Mastenson last updated the file on 2001:06:14 20:34:00(8.34 PM).

The second file contained a note to Ricco, which might alternatively be seen as a reference to Rick Bell. Robert mentions "I more do you want more" in this document, which could indicate more images of employees that are tied to sexual harassment. In the second sentence, he asks Ricco, "Do you want younger or older?" This could suggest that he is providing Ricco with photos of staff based on the age category he prefers. This also demonstrates that Robert is allowing Rick the option of choosing between older and younger female colleagues to engage in sexual harassment. This document was similarly password protected, and we discovered the password was an 'image' by using the John the Ripper program. The password-protected file indicates that he wishes to conceal anything in it that he does not want others to view. The password to open and change the document is "picture" in all lowercase letters.

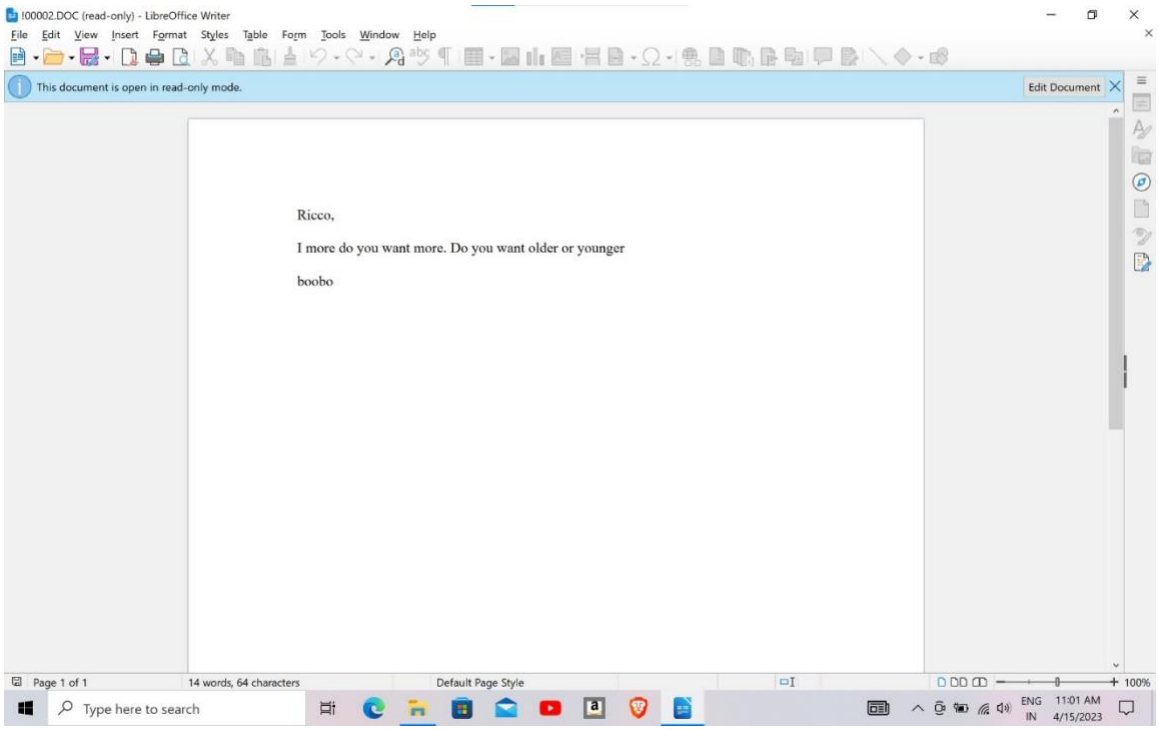

Figure 5: Letter from Bob Mastenson to Rick Bill

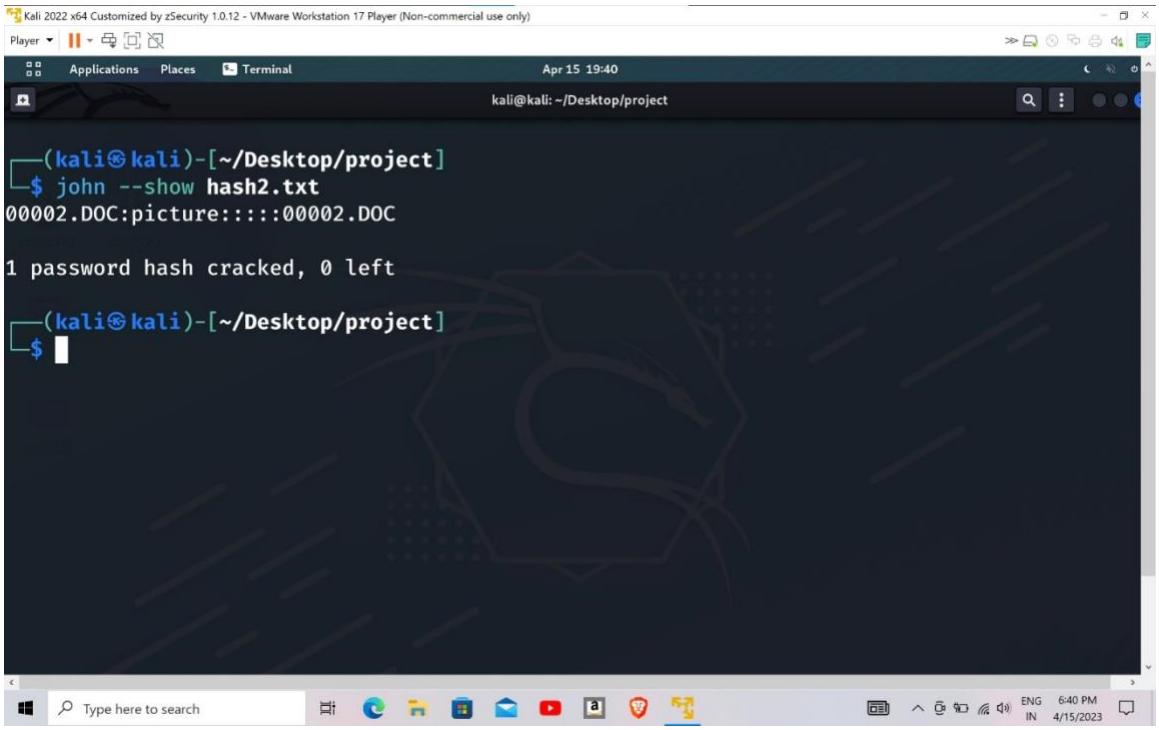

Figure 6: John cracks the !00002.doc password

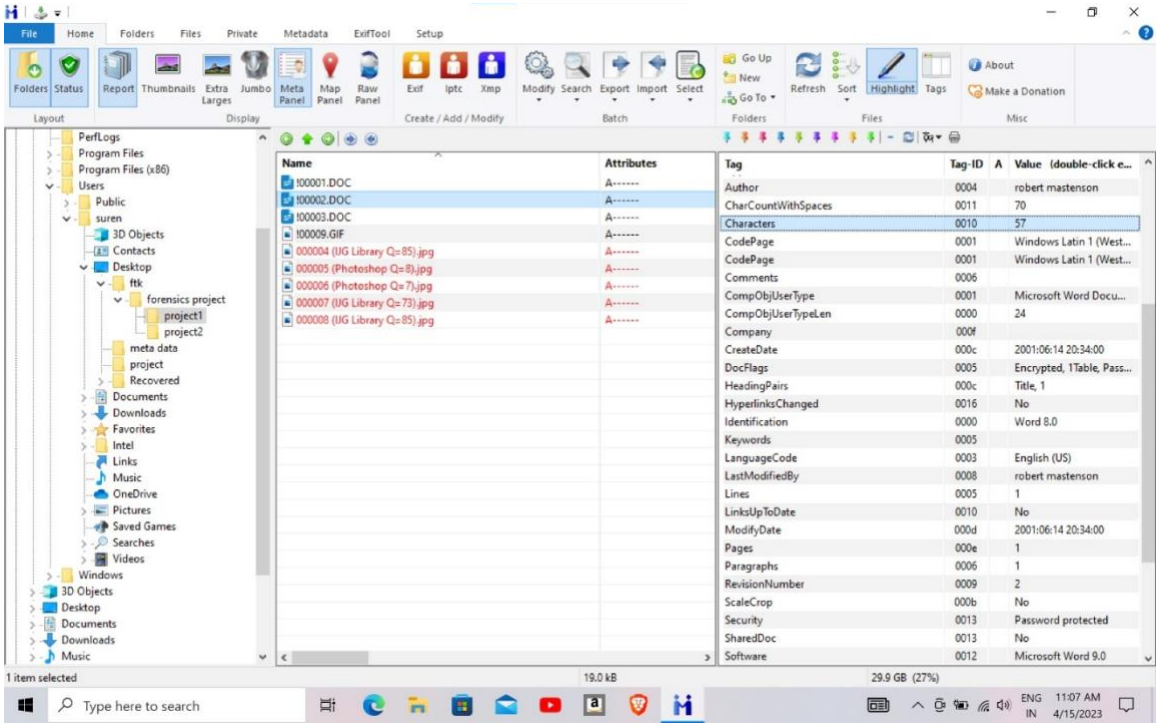

Figure 7: Metadata showing "000002.doc

File 003: 000003.doc

The third file is found to be a Word file created by Microsoft Word and is named!00003.DOC created on 2006:09:22 20:36:00(8.36 pm) by Robert Mastenson and is password protected. The metadata indicates that the file is 1 page long and contains 18 words with the title "Rick,". The file was allotted both read and write permission for those who had the password. The file was last modified by Robert Mastenson on 2006:09:22 20:36:00(8.36 PM).

The third file contained a note from Rick that stated, "I am sending these with codewords because I don't trust email." The FBI is aware of it. "What do you think of them?" written by Robert Mastenson. We can deduce from the message that he is sending something to Rick, which in this case could be illicit photographs of female employees, using code phrases to avoid raising suspicion, and that he is not using any formal means of communication, such as email, which the FBI could easily detect. He also inquires as to Rick's thoughts on the photographs. This was likewise password secured, which we broke using John the Ripper. All lowercase "collect" is the password for both opening and editing the document.

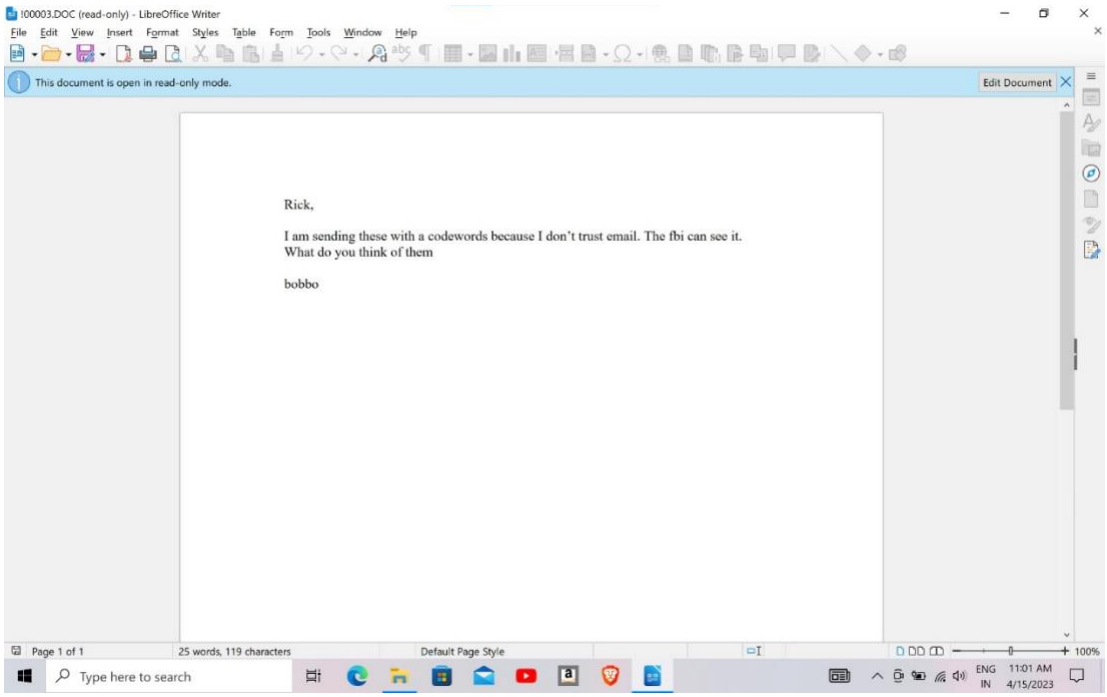

Figure 8: Letter from Bob Mastenson to Rick Bill

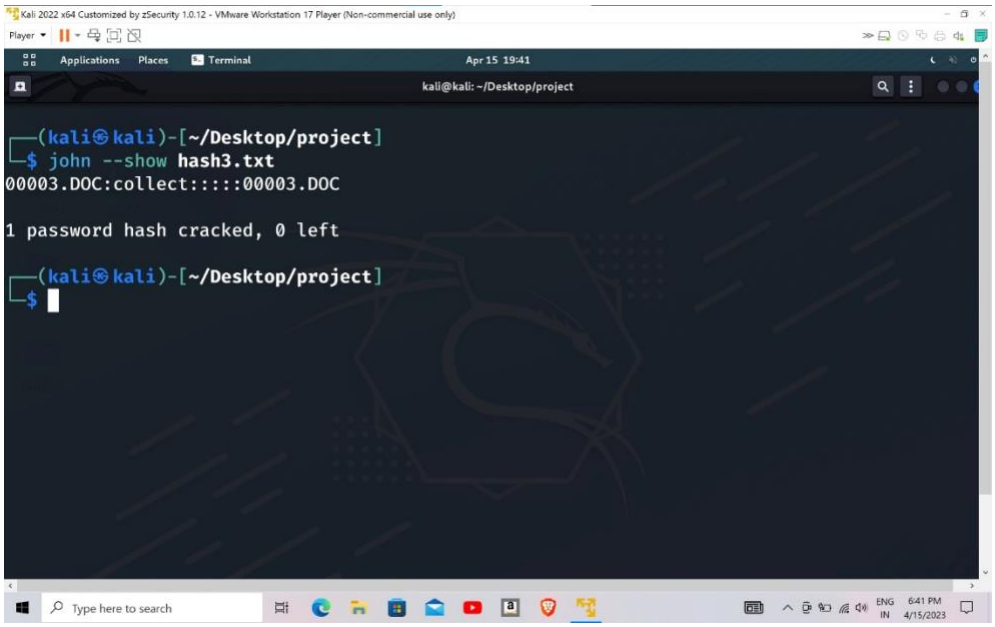

Figure 9: John cracks the !00003.doc password

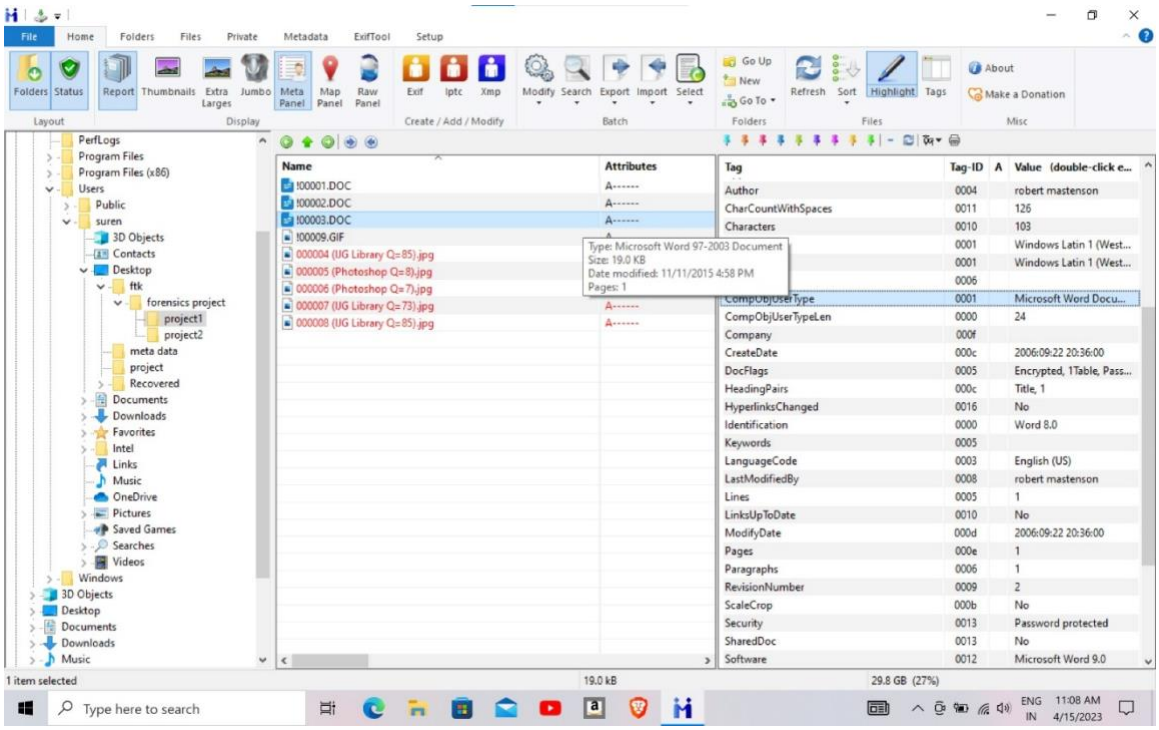

Figure 10: Metadata showing "000002.doc

File 000004.JPEG

File 000004 is a JPEG file containing a photo of a cat that has been defined as "kiddie porn" in the state of Florida. This photograph provides strong evidence that Mastenson was involved in child pornography. This is also obvious in Rick Bell's letter (000001 pdf) concerning Mastenson's willingness and the fact that he sent images to Rick Bell. The image is included below:

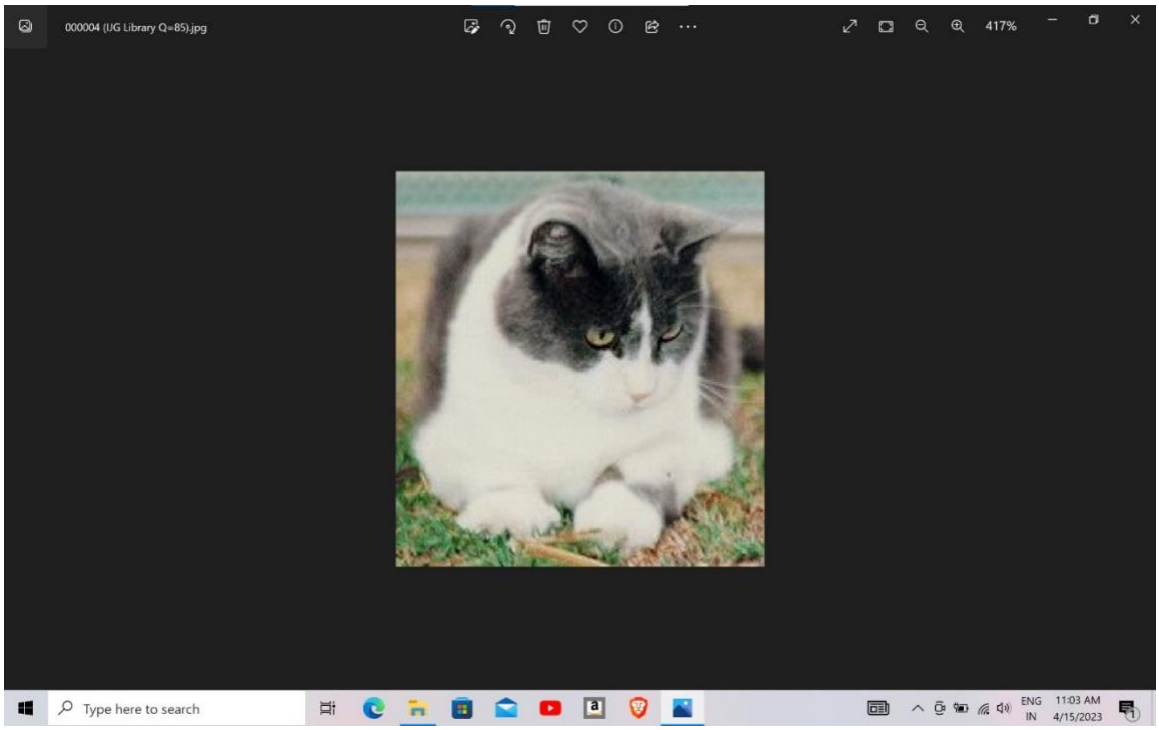

Figure 11- Photo of a cat "child pornography"

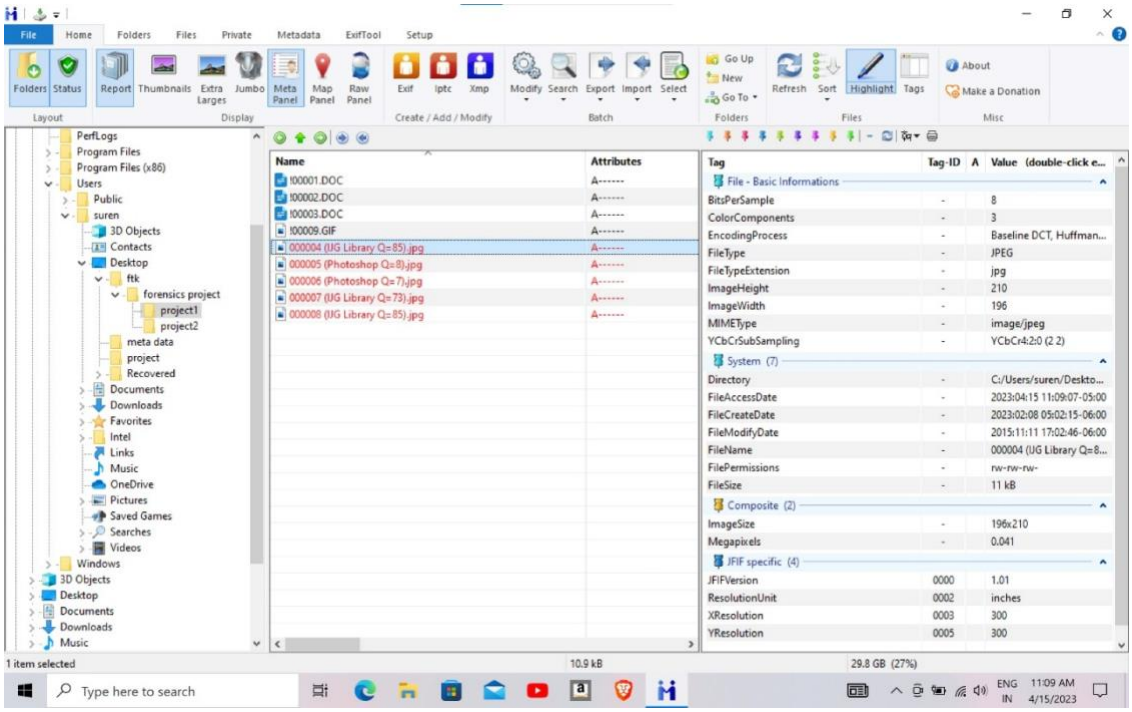

Figure 12: Metadata showing "000004"

File 000005.JPEG

File 000005 is also a JPEG file that contains a photo of a cat that is classified as "kiddie porn" in the state of Florida. This photograph provides strong evidence that Mastenson was involved in child pornography. This is also obvious in Rick Bell's letter (000001 pdf) regarding Mastenson's willingness and the fact that he sent images to Rick Bell. The image is included below:

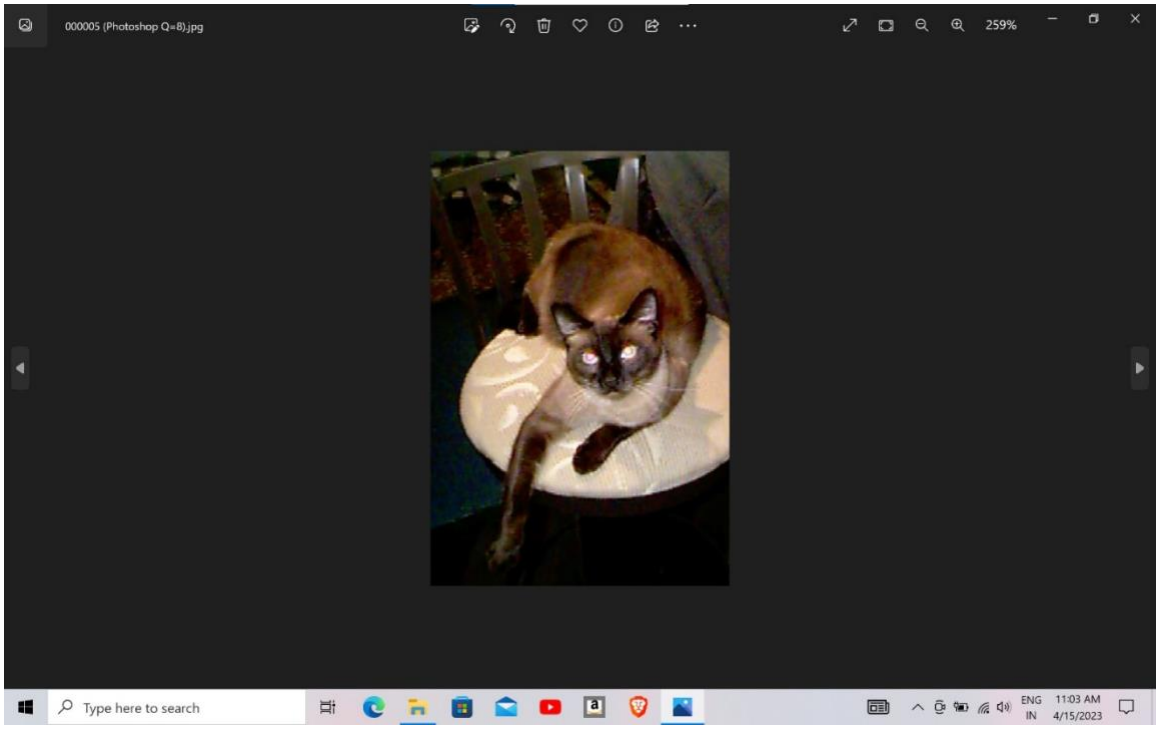

Figure 13- Photo of a cat "child pornography"

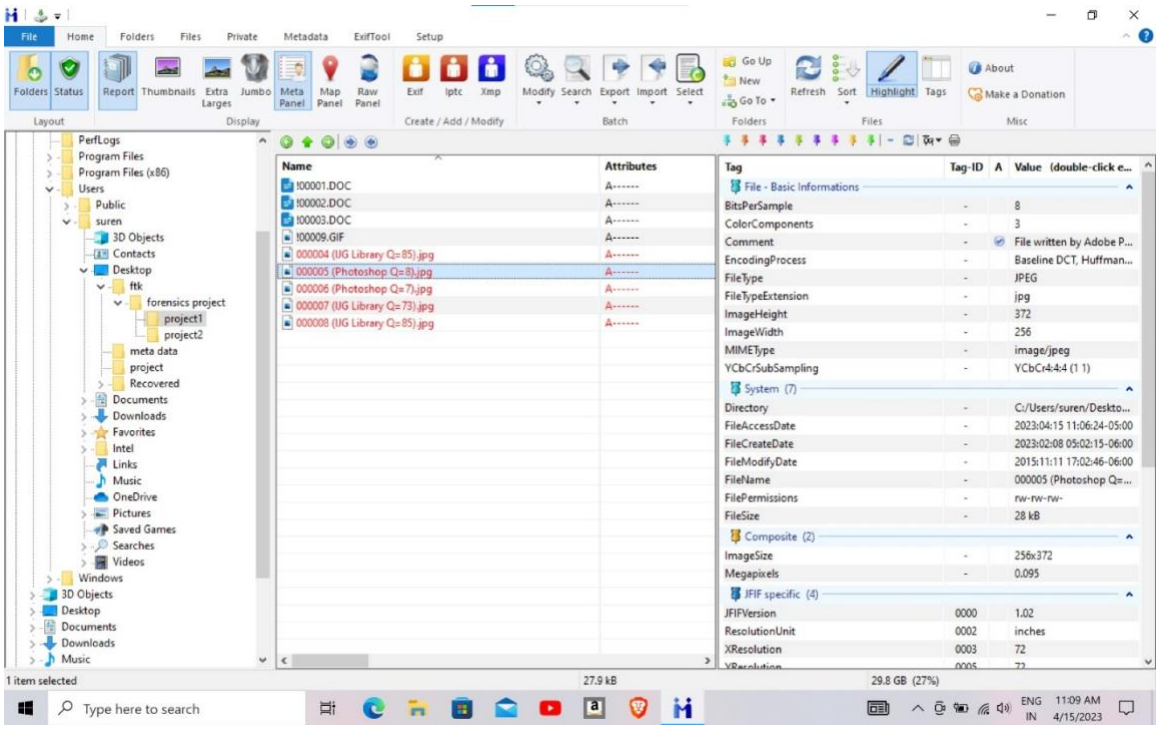

Figure 14: Metadata showing "000005"

File 000006.JPEG

File 000006 is also a JPEG file that includes a photo of a dog that is considered "adult pornography" under Florida law. This shot is conclusive proof that Mastenson was involved in adult pornography. This photo appears to have been sent together with the letter (000003. doc) when Mastenson mentioned that he was going to send some older photos and that he did not trust email for doing so. Furthermore, in his letter to Rick Bell, Mastenson indicated that he would send photos with code phrases because he was scared the FBI would view the photos. This confirms his involvement in "adult pornography," which is why he did not want the FBI to examine the video. The photo is inserted below:

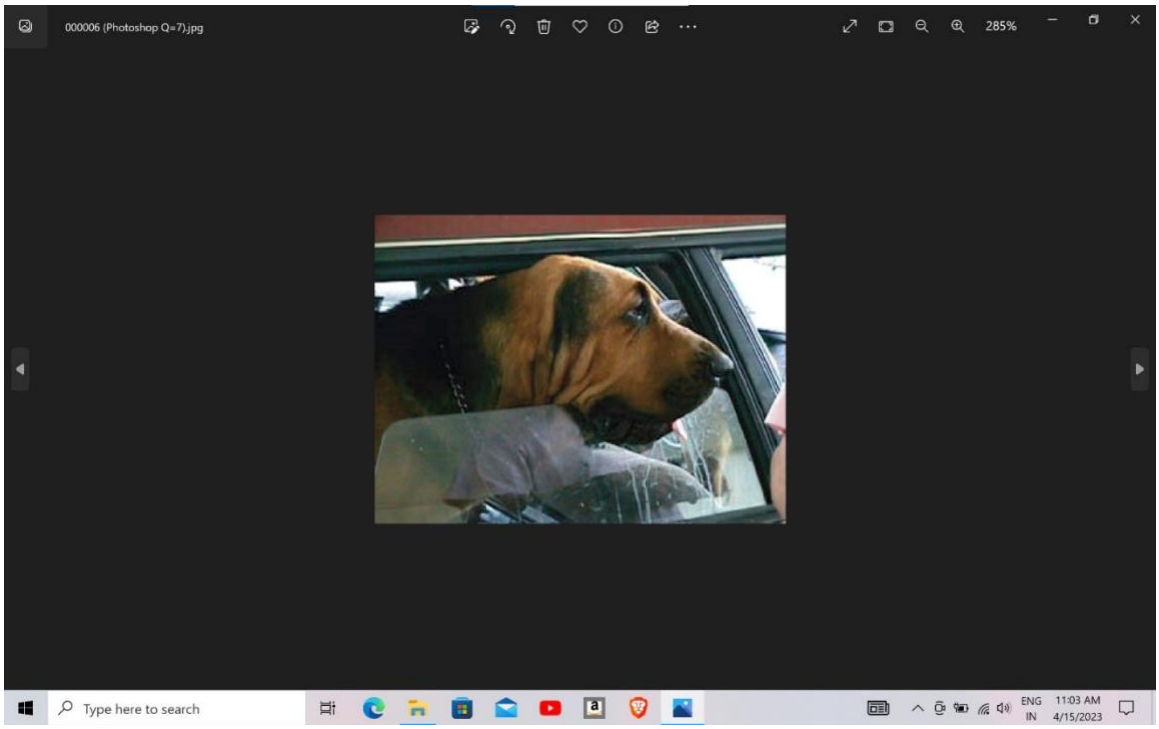

Figure 15 – Photo of a dog "adult pornography"

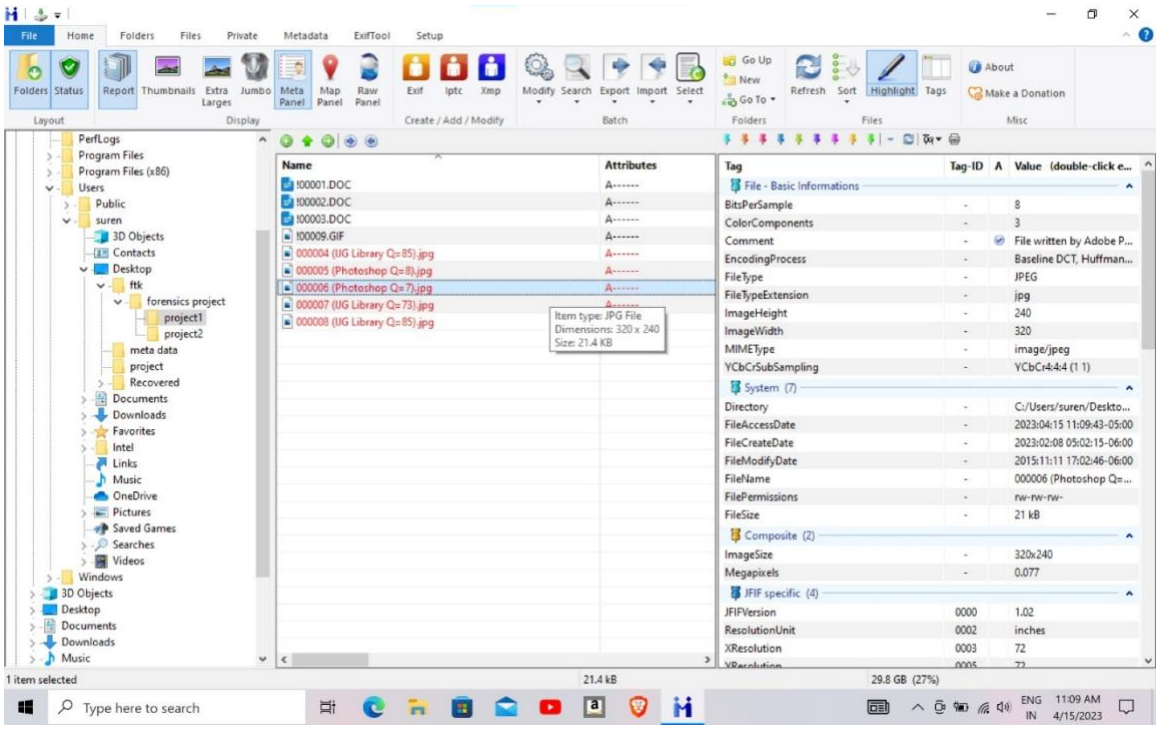

Figure 16: Metadata showing "000006"

File 000007.JPEG

File 000007 is also a JPEG file that includes a photo of a dog that is considered "adult pornography" under Florida law. This shot is conclusive proof that Mastenson was involved in adult pornography. This photo appears to have been sent together with the letter (000003. doc) when Mastenson mentioned that he was going to provide some older photos and that he did not trust email for doing so. Furthermore, in his letter to Rick Bell, Mastenson showed that he would send photos with code words because he was scared the FBI would view the photos. This confirms his involvement in "adult pornography," which is why he did not want the FBI to examine the video. The photo is inserted below:

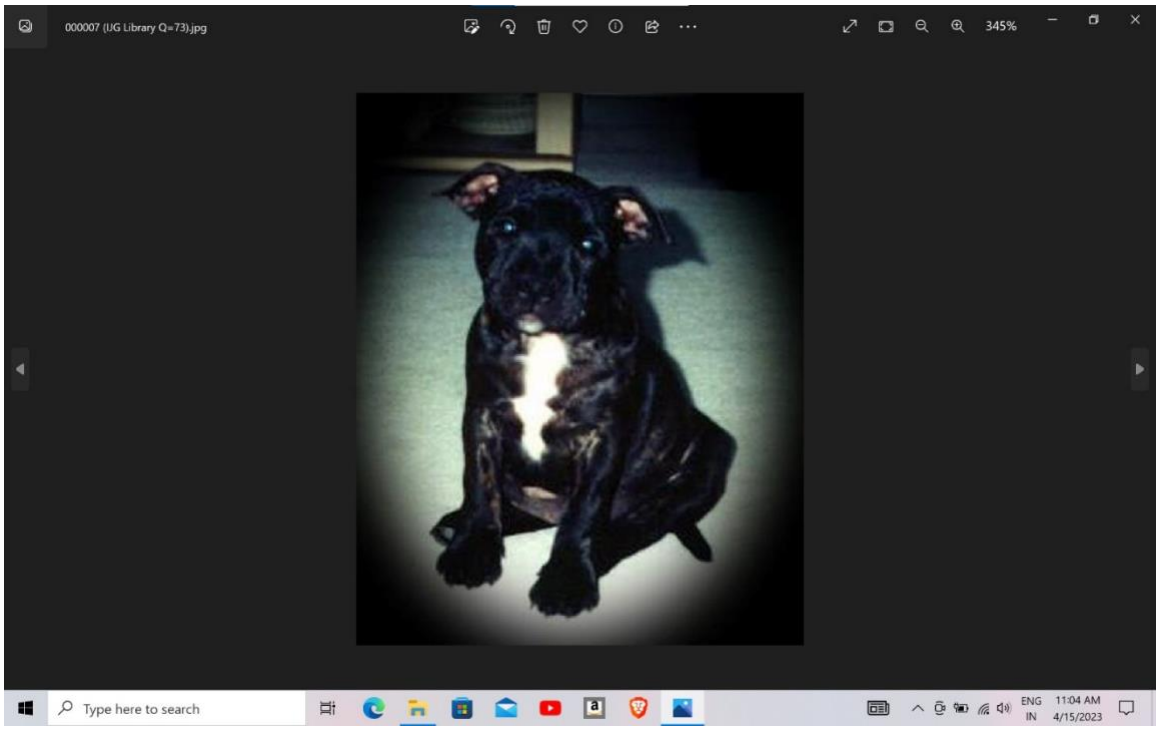

Figure 17– Photo of a dog "adult pornography"

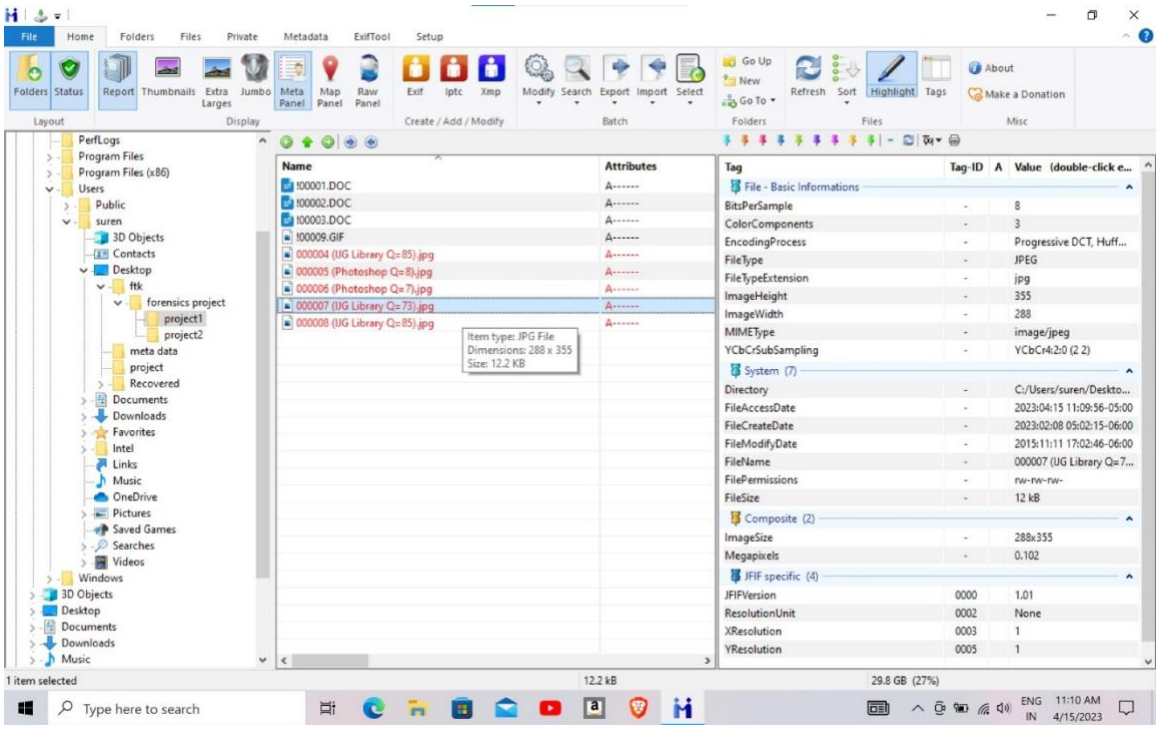

Figure 18: Metadata showing "000007"

File 000008.JPEG

File 000008 is also a JPEG file that contains a photo of a cat that is classified as "kiddie porn" in the state of Florida. This photograph provides strong evidence that Mastenson was involved in child pornography. This is also obvious in Rick Bell's letter (000001 pdf) regarding Mastenson's willingness and the fact that he supplied images to Rick Bell. The image is included below:

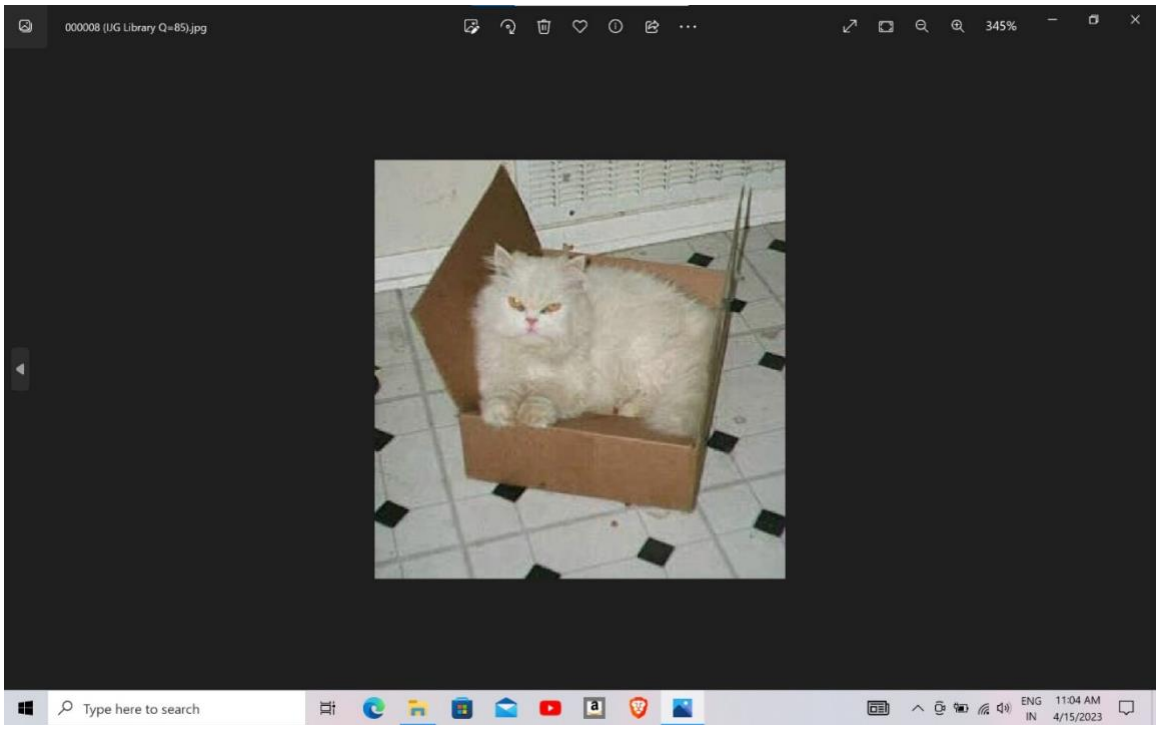

Figure 19- Photo of a cat "child pornography"

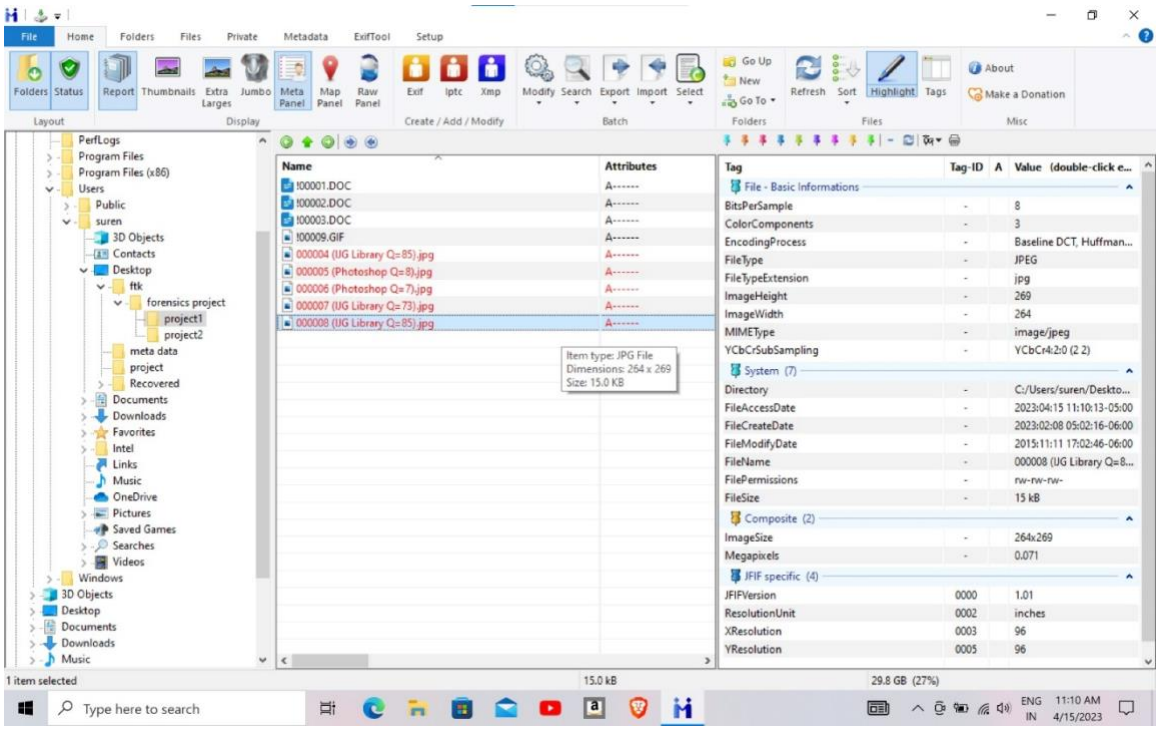

Figure 20: Metadata showing "000008"

File 000009.GIF

File 000009 is a GIF file that contains an image of a dog that is classified as "adult pornography" in the state of Florida. This image is conclusive proof that Mastenson was involved in adult pornography. It's worth mentioning that his distinctive photograph is linked to doc 00001 since Mastenson mentioned in that document that he loved "Abbey" and that they had spent good times together. This photo appears to be a reference to Mastenson's involvement in workplace sexual harassment during working hours, and that "Abbey" was one of his victims. The image is included below:

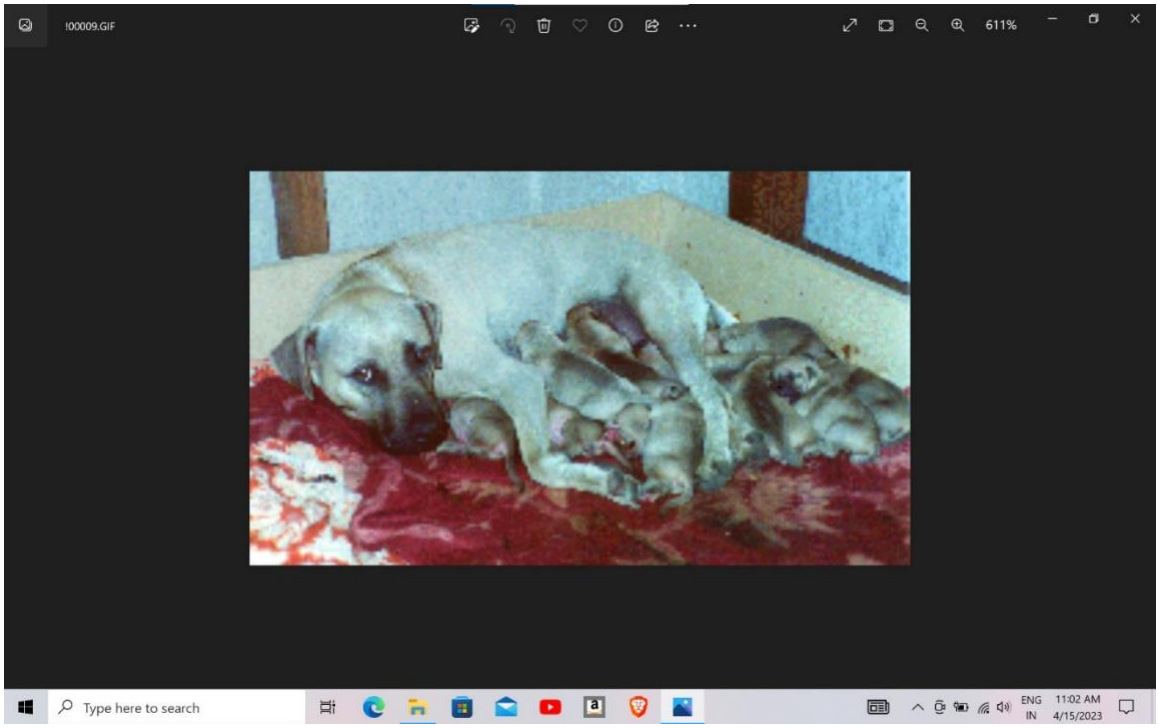

Figure 21– Photo of a dog "adult pornography"

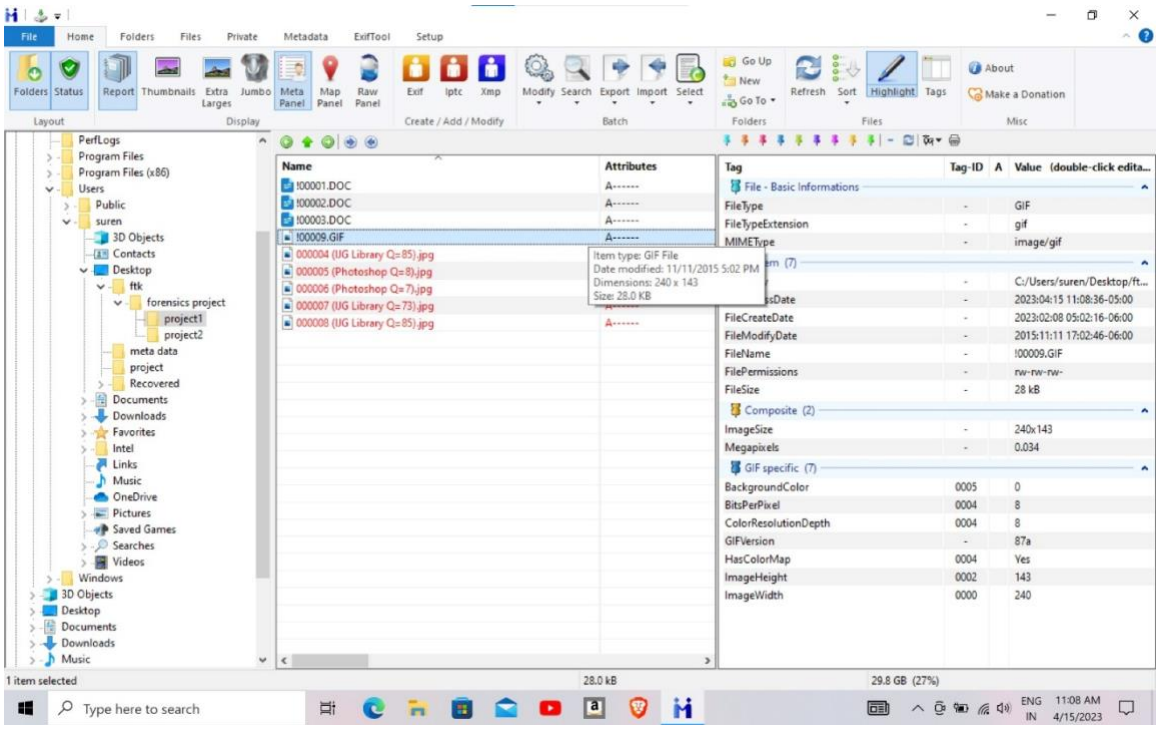

Figure 22: Metadata showing "000009"

Appendix A: Full File Report

See enclosed CD-ROM entitled Robert Mastenson Case – Full File Report.

Appendix B: Policy on Evidence Collection

A case number, which is a unique identifying number, will be assigned to the thumb drive. A concise description of the pen drive, including its type, size, and color, should be provided. The label should include the date and time the evidence was gathered. All evidence in the case, including physical evidence and photos, is meticulously recorded and safely stored. The evidence is kept in a secure lockup that requires a key to open. Keys are only given out when evidence is checked out of the jail. A chain of custody form, which is also locked in the fire-safe lockup, keeps a complete record of all checkouts. Other changes in custody of the evidence, including the name of the person who received the evidence, the date and time of transfer, and other pertinent information regarding the transfer, should be documented on the label.

Appendix C: Policy on Forensically Sterile Media

By the Department of Defense's (DOD) disk scrubbing utility, media used in a forensic investigation should be forensically sterile. According to DOD regulation, forensically sterile media must be obtained from a reliable source and adequately documented, including the manufacturer, model, and serial number. To avoid unwanted access or tampering, media must be stored in a secure environment. This technique does not exclude "new" or "never been used" media. Furthermore, when used media becomes separated from a case, it is sterilized anew. To guarantee the integrity of the evidence collected and evaluated in forensic investigations, forensically sterile media must be used. The use of forensically sterile media preserves the integrity of the evidence and ensures its admissibility in court.

Appendix D: Glossary

Hash values: A hash value is a fixed-length numeric value that uniquely identifies data. Hash values can also be used to validate the integrity of data received through unsecured channels. To establish whether data was altered, compare the hash value of received data to the hash value of data as it was transmitted. As long as the evidence is properly collected and processed, any third party evaluating the hash value independently will find the same number string. Hash values are an important tool in digital forensics because they allow for the verification of the integrity and validity of digital evidence, the identification of known harmful files, and the establishment of a chain of custody for evidence.

Brute force: A brute force attack use trial and error to guess login information, encryption keys, or the location of a hidden web page. Hackers try every potential combination in the hopes of making the right guess. Although this is an ancient attack method, it is still effective and popular among hackers. Because cracking a password can take anything from a few seconds to several years, depending on its length and complexity. The hacker attempts a variety of usernames and passwords, frequently using a computer to try a large number of combinations until they uncover the correct login credentials. The term "brute force" refers to attackers who employ excessive force to gain access to user accounts.

Metadata is information that describes other data. It's useful for identifying, locating, and describing digital objects including files, photos, movies, and web pages. It has the same value as data, and experts appreciate its potential to help users find, organize, and utilize information. Metadata is defined as data that describes and explains itself. It gives context by providing facts such as the source, kind, owner, and relationships to other data sets, allowing you to grasp the significance of a certain data set and guide you on how to use it.

Root: A root directory in a Unix-like operating system holds all of the system's directories and files. There is no one root directory in MS-DOS and various versions of Microsoft Windows since these operating systems employ a separate root directory for each storage device and partition.

Formatted: Formatting a hard disk implies erasing all data on the device and creating a file system to make room for the operating system. Most individuals format a hard disk to remove the contents of the device. Formatting a drive erases all of the data on it, making it an efficient method of ensuring that all data is deleted from the device.

Unallocated space: Unallocated space, commonly known as "free space," is the space on a hard disk that can be used to store new files. In contrast, allocated space is the space on a hard drive where files already exist. Consider "allocated" storage space to be already

filled with data that will not be replaced by newer data, but "unallocated" space is accessible to store new data even if it contains old data that will be overwritten by new data. When a file is deleted from a storage device, the space it occupied is not necessarily immediately overwritten with new data. Instead, the file system marks the space as unallocated, indicating that it is available for use. Until new data is written to that space, the original data may still be recoverable using forensic techniques.

Encryption: Encryption is a method of encrypting data so that only authorized parties can decipher it. It is the process of transforming human-readable plaintext to incomprehensible text, also known as ciphertext, in technical terms. To put it simply, encryption modifies readable data so that it appears random.

Compressed files: A file that has been decreased in size by using a compression algorithm, which is widely used to save disk space. When a file is compressed, it becomes unreadable to most programs until it is decompressed. A compressed file is any file that contains one or more smaller files or directories than their original file size. These files facilitate speedier downloads and enable more data to be stored on portable media.

Digital evidence: Any information or data that may be taken from digital devices such as computers, smartphones, tablets, and other electronic devices and utilized as evidence in legal or investigative procedures is referred to as digital evidence. Emails, text messages, pictures, videos, audio recordings, internet surfing history, social media activity, and metadata are all examples of digital evidence. When electronic devices are seized and secured for examination, this evidence can be obtained.

Appendix E: Credentials

a. Technical Aspects of Data Retrieval

- All original data files were copied to other forensically sterile media.
- All recoverable deleted files with potential evidence value were restored or recovered and copied to forensically sterile media.
- All recoverable deleted files with potential evidentiary value were restored or recovered and copied to forensically sterile media.
- Our write blockers are tested quarterly. We analyzed the unallocated and slack space for potentially important lost or concealed data, and any potentially relevant data/files were forensically copied out to other media.
- A list of all the files found on the inspected media was created, regardless of whether they included possible evidence or not.

- A forensic bitstream (exact) replica of the USB Drive on the subject media was created for another identical USB Drive. The examination was carried out on a copy of the original material. Another Forensic bitstream copy has been made and is being kept elsewhere.
- No examination was ever performed on the original media.
- All the equipment and software used in the procedures in this report have been tested and validated to guarantee that they are in proper working condition and continue to give the most accurate findings. Before and after each validation, all test media is hashed.
- When necessary, data inspection, retrieval, and carving are performed using two distinct but forensically sound approaches to validate any results made throughout the investigation.
- We performed a hash on the original media and recorded the value before wiping and verifying the wipe of the target media.
- We copied the original media exactly to the deleted and certified media.

Software used during the forensic examination and procedures:

1. **Disk Digger**: a tool that can help you recover deleted photos and videos from your computer or memory card, even if you've accidentally deleted them or reformatted your device.
2. **FTK imager:** public domain, open-source software, free and available for public use.
3. **John the Ripper:** open-source software, free and available for public use.
4. **Metadata++:** free software that allows you to view, edit, and copy metadata from different file formats in a user-friendly way.