

# Mastenson Investigation File

---

**Forensic Investigator: Rajabinandhan,Deekshitha**

---



## **Authorized Eyes Only**

This document contains sensitive and confidential information pertinent to a forensic investigation. Proceeding implies that you are authorized to do so and agree to keep confidential all information contained herein.

## **I . Summation**

Mastenson Investigation File involves Examination of a Red transparent microcenter USB 3.1 16 Gigabyte pendrive that was received directly from Mr.David Smith the owner of the warehousing firm.Mr.David Smith has received multiple complaints from female employees about male employees viewing pornography and engaging in sexual harassment during company working hours.Mr.David Smith also states that his company has an strict Acceptable Use Policy that governs the usage of employees use of computers.The Acceptable Use Policy prohibits any employee from involving themselves in viewing pornography content and using computers for sexual harassment.

Mr.David Smith suspects that the employees violating the companies APU are in the information technology division of his company and knowledgeable about computers and how to “cover their tracks” When engaging in this type of behavior.The primary suspect of this case is the IT director Bob Mastenson and he is believe to be communicating with Rick Bell who is the Director of Accounting and they are suspected to be in this together.They are the ones who Mr.David Smith believes to be engaging in viewing pornography and engaging in sexual harassment in work hours.

Mr.David Smith, the proprietor of the warehousing firm where the study was carried out, personally handed over the data on a microcenter USB 3.1 16 Gigabyte pendrive around February 22 12:23:00. The initial analysis revealed that the pendrive was empty.On further analysis it was discovered that files were deleted in an attempt to cover their tracks. The files were then recovered and imaged into two other USB Sticks which were used as Primary and Failsafe Data copies to analyze the data. As soon as the recovery was done Hash values of the Directory as an whole and an individual files were extracted and saved to Protect the integrity of recovered files.We made sure that the Hash values of the original recovered files Matched with thee Hash values of the Data from Primary and Failsafe USB Drives.

Examination of the recovered files revealed several critical information that validated Mr.Smith Concerns about male employees (Bob Mastenson and Rick Bell) viewing pornography and engaging in sexual harassment during working hours. Specifically, the three MS word documents authored by “Bob Mastenson”contained lines of communication between Bob Mastenson and Rick Bell clearly indicate that they were engaged in sexual harassment during working hours.To support Mr. Smith's claim of being able to cover their tracks three MS word Document were password protected on read and write levels. We also found 5 image files that further proved the involvement of Bob mastenson and Rick bell in viewing of pornography content which violates the companies APU.It was further revealed that both were involved in consumption of Child pornography Content which is a crime in the State of Illinois.

The first Microsoft Word document, named !00001.doc, contains text that suggests Bob is engaged in sexual harassment with someone named Abby, who may be an employee. The document, written for Rick Bell, states that Bob sent special pictures to Rick and expresses his love for Abby, mentioning that they have spent time together. The phrase "older ones" implies that there may be other female employees who have been victims of sexual harassment, and Bob is sharing this information with Rick. The document was password-protected and reserved for modification by Bob only, indicating that he was trying to keep the contents secret. These actions suggest that both Bob and Rick are involved in sexual harassment and are attempting to cover their tracks.

The second MS Word document, !00002.doc, was written by Bob for Rick, offering him more pictures of female employees for sexual harassment. Bob asked Rick if he preferred older or younger ones, indicating that he had already harassed women of different age groups. The document was password protected and reserved for Bob's modification only, suggesting an attempt to hide his actions. This shows that Bob and Rick were involved in workplace sexual harassment, and Bob was actively sharing his misconduct with Rick.

The third document, 000003.doc, revealed that Bob and Rick were exchanging pictures using code words to avoid detection by the FBI. Bob also mentioned that he did not trust e-mail and asked for Rick's opinion on the pictures he sent. The document was password protected and reserved for modification by Bob, indicating an attempt to conceal its contents.

Files 000004, 000005, and 000008 were JPEG files and each contained an image of a cat, which qualifies as "child porn" under Illinois state law. Files 000006, 000007, and 000009 each contained an image of a dog, which qualifies as "adult pornography" under Illinois state law.

The six photo files, coupled with the content of the three MS Word documents, provides solid proof that Bob Mastenson and Rick Bell were engaged in viewing pornography and sexual harassment during work hours at the warehousing firm. The JPEG files 000004, 000005, and 000008 contained images of cats, which are classified as "child porn" as defined by the state of illinois. Similarly, files 000006, 000007, and 000009 contained photos of dogs, which are considered "adult pornography."

Further analysis of the three MS Word documents, which were password-protected and reserved for modification by Bob Mastenson, revealed that they were authored by him over a five-year period. This indicates that the inappropriate behavior in question had been ongoing for a significant amount of time. The content of the documents also suggested that Mastenson and Bell were exchanging sexually explicit messages and photos, including child pornography.

The fact that the USB Stick was formatted provides evidence to support Mr. Smith's initial concern that Mastenson and Bell were taking measures to "cover their tracks."

Mastenson, in one of the letters to Bell, expressed his fear of the FBI seeing the contents of their communication, indicating that he was aware that he was engaging in illegal behavior.

In conclusion, the evidence recovered ,as well as the analysis of the MS Word documents, points towards Mastenson and Bell's engagement in sexual harassment and pornography during work hours at the warehousing firm. The evidence also suggests that this behavior had been ongoing for a considerable period.

## **Table of Contents**

I. Summation.....	I
Table of Contents.....	1
II. Analysis.....	2
A. Media.....	3
Figure A.1: Microcenter USB Stick (Front view)	
Figure A.2: Microcenter USB Stick (Back view)	
Figure A.3: Primary USB stick AD1 Image Metadata	
Figure A.4: Failsafe USB stick AD1 Image Metadata	
Figure A.5: Primary Micro center USB Stick (Front and back view)	
Figure A.6: Failsafe Microcenter USB Stick (Front and back view)	
Figure A.7: Securing the Primary Evidence	
B. Files.....	7
Figure B.1:Recovered Files List	
Documents.....	9
File 001:!00001.doc.....	9
Figure B.2: Letter from Bob Mastenson to Rick Bell	
Figure B.3: File 001 Metadata	
File 002:!00002.doc.....	10
Figure B.4: Letter from Bob Mastenson to Rick Bell	
Figure B.5: File 002 Metadata	
File 003:!00003.doc.....	12
Figure B.6: Letter from Bob Mastenson's to Rick Bell	
Figure B.7: File 003 Metadata	
File Set 004:Exhibit 2, 3, 4.....	14
File 005:000004(IJG Library Q = 85).jpg.....	14
Figure B.8: Photo of Child pornography"Cat"	
File 006:000005( Photoshop Q = 8).jpg.....	15
Figure B.9: Photo of Child pornography"Cat"	
File 007:000006( Photoshop Q =7 ).jpg.....	16
Figure B.10: Photo of Adult pornography"Dog"	

File 008:000007( IJG Library Q = 73 ).jpg.....	17
Figure B.11: Photo of Adult pornography”Dog”	
File 009:000008( IJG Library Q = 85 ).jpg.....	18
Figure B.12: Photo of Child pornography”Cat”	
File 010:!00009.GIF.....	18
Figure B.13: Photo of Adult pornography”Dog”	
File 011:Conduct of Professional Employees.....	20
Appendix A: Full File Report.....	19
Appendix B: Policy on Evidence Collection.....	20
Appendix C: Policy on Forensically Sterile Media.....	20
Appendix D: Glossary.....	20
Appendix E: Applications Logs.....	21

## **II. Analysis**

Forensic Examiner: Rajabinandhan,Deekshitha

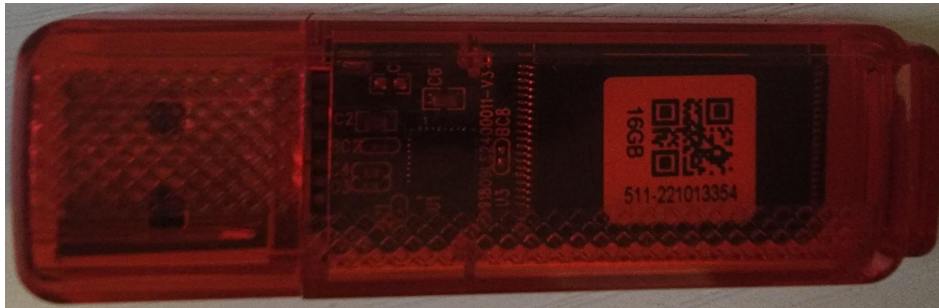
### **A. Media**

Mr.David Smith, the proprietor of the warehousing firm where the study was carried out, personally handed over the data on a microcenter USB 3.1 16 Gigabyte pendrive around February 22 12:23:00. I physically examined the pendrive for any damages as a part of the chain of custody procedure. The USB stick was red, with a transparent exterior covering that allowed the interior components to be seen with the naked eye. The name Micro Center appears on the front of the pendrive, followed by its hardware version USB 3.1, size of 16 GB, and location of manufacturing, Made in Taiwan. The photograph showcasing the front view of the pendrive is displayed in Figure 1. The rear side of the pendrive is pretty plain with the components and the qr code of components visible through the overlayer. The photograph including the rear view of the pendrive is displayed in Figure 2.

**Figure A.1: Microcenter USB Stick (Front view)**



**Figure A.2: Microcenter USB Stick (Back view)**



The USB stick was received from Mr.David Smith on 1st of March 2023. Further analysis revealed that the pendrive was empty. As the individual under inquiry is technologically savvy, all data has been wiped in an effort to "cover their tracks." The data were recovered as a Logical Imager (.AD1) for further analysis using the FTK imager, a free open source forensic program. The recovered picture file was duplicated into two pendrives, one main and one backup, in accordance with the chain of custody protocol, to ensure that the real evidence was not tampered with. Using the autopsy forensics tool, the recovered AD1 files were hashed with MD5 and SHA-256 methods (MD5 Checksum: f183380d2eff4bfc317e0c58ded7d04b, SHA-256 Checksum:0f34ba3a8d755451b2f93ced1b4846887beab6e5c852ade7d8e33a62359491c7). The metadata of the files from primary and failsafe USB drives are shown in Figure 3 and Figure 4 respectively.

**Figure A.3: Primary USB stick AD1 Image Metadata**

Metadata	
Name:	/LogicalFileSet1/Primary.ad1
Type:	Local
MIME Type:	application/octet-stream
Size:	2106784
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:	f183380d2eff4bfc317e0c58ded7d04b
SHA-256:	0f34ba3a8d755451b2f93ced1b4846887beab6e5c852ade7d8e33a62359491c7
Hash Lookup Results:	UNKNOWN
Internal ID:	2
Local Path:	F:\Primary.ad1



**Figure A.4: Failsafe USB stick AD1 Image Metadata**

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations
<b>Metadata</b>								
Name:	/LogicalFileSet2/Primary.ad1							
Type:	Local							
MIME Type:	application/octet-stream							
Size:	2106784							
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:	f183380d2eff4bfc317e0c58ded7d04b							
SHA-256:	0f34ba3a8d755451b2f93ced1b4846887beab6e5c852ade7d8e33a62359491c7							
Hash Lookup Results:	UNKNOWN							
Internal ID:	9							
Local Path:	E:\Primary.ad1							

The primary and failsafe USB sticks that were utilized to store the retrieved data and conduct the Forensics investigation were both brand new. They both have the same brand, model, and capacity. Both of the Kingston USB drives are white in color and feature 32 gigabytes of capacity. The brand name Kinston was etched on the front of the pendrive, along with the capacity indicated. The back of the pendrive is rather basic, with only a few copyright marks. On the back, they both have a clear keychain hole. Figures 5 and 6 show the pen drives that were utilized.

**Figure A.5: Primary Microcenter USB Stick (Front and back view)**



**Figure A.6: Failsafe Microcenter USB Stick (Front and back view)**



The major USB stick obtained from David Smith was placed in a sealable plastic bag designated major Forensic Evidence and kept in a safe location. Figure 7 depicts how the evidence was saved following the recovery procedure. On Further examination I discovered many crucial files that confirm Mr. Jenkins' worries regarding male workers (Bob Mastenson and Rick Bell) accessing pornography and participating in sexual harassment during work hours.



































**Figure A.7: Securing the Primary Evidence**



## ***B. Files***

The primary USB device held 35 items in total, including Document items, Pictures, and Slack files. The files were retrieved utilizing the data recovery method using AccessData® FTK® Imager v4.7.1.2. A screenshot of the recovered files is shown in the figure 8. There were 7 password-protected Microsoft Word document files. The password for these files was revealed using John the Ripper, a free open source password cracking program. The metadata was validated using two open source tools: AccessData® FTK® Imager v4.7.1.2 and Autopsy 4.20.0. There were four distinct password-protected files, three of which were identical clones of each other.

**Figure B.1:Recovered Files list**

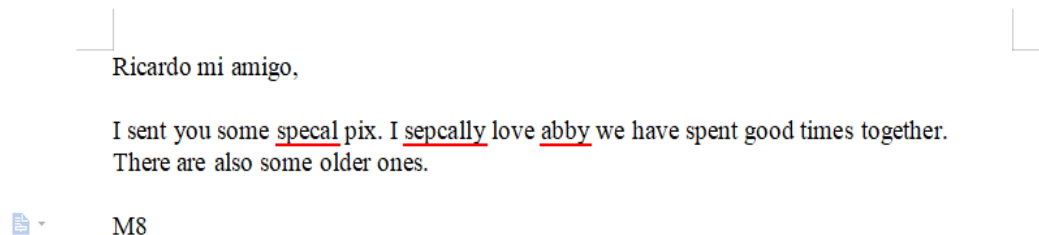
File List			
Name	Size	Type	Date Modified
 !00001.DOC	19	Regular File	12-11-2015 21:59:50
 !00001.DOC.FileSlack	13	File Slack	
 !00002.DOC	19	Regular File	11-11-2015 22:57:54
 !00002.DOC.FileSlack	13	File Slack	
 !00003.DOC	19	Regular File	11-11-2015 22:58:02
 !00003.DOC.FileSlack	13	File Slack	
 !00009.GIF	28	Regular File	11-11-2015 23:02:46
 !00009.GIF.FileSlack	4	File Slack	
 000004 (IJG Library Q=85).jpg	11	Regular File	11-11-2015 23:02:46
 000004 (IJG Library Q=85).jpg.FileSlack	6	File Slack	
 000005 (Photoshop Q=8).jpg	28	Regular File	11-11-2015 23:02:46
 000005 (Photoshop Q=8).jpg.FileSlack	5	File Slack	
 000006 (Photoshop Q=7).jpg	22	Regular File	11-11-2015 23:02:46
 000006 (Photoshop Q=7).jpg.FileSlack	11	File Slack	
 000007 (IJG Library Q=73).jpg	13	Regular File	11-11-2015 23:02:46
 000007 (IJG Library Q=73).jpg.FileSlack	4	File Slack	
 000008 (IJG Library Q=85).jpg	16	Regular File	11-11-2015 23:02:46
 Conduct of Professional Employees.doc	20	Regular File	20-04-2006 03:39:46
 Conduct of Professional Employees.doc....	12	File Slack	
 COUNTERCT.doc	21	Regular File	06-10-2004 12:05:20
 COUNTERCT.doc.FileSlack	12	File Slack	
 Exhibit 2- 000001doc.doc	19	Regular File	12-11-2015 21:59:50
 Exhibit 2- 000001doc.doc.FileSlack	13	File Slack	
 Exhibit 3- 000002doc.doc	19	Regular File	11-11-2015 22:57:54
 Exhibit 3- 000002doc.doc.FileSlack	13	File Slack	
 Exhibit 4- 000003doc.doc	19	Regular File	11-11-2015 22:58:02
 Exhibit 4- 000003doc.doc.FileSlack	13	File Slack	
 exit strategy.xls	14	Regular File	31-12-2004 18:40:12
 exit strategy.xls.FileSlack	3	File Slack	
 passwords.txt	1	Regular File	30-11-2015 09:57:12
 passwords.txt.FileSlack	16	File Slack	
 summation example.pdf	58	Regular File	22-10-2015 21:48:54
 summation example.pdf.FileSlack	7	File Slack	
 wasilewski.doc	1,545	Regular File	22-10-2015 21:49:34

## **Documents**

### **File 001: 000001.doc**

File 001 is a Microsoft Office Document that was generated in Microsoft Word and saved on the pendrive as 000001. File 001's header had the hexadecimal string DOCF11E0A1B11AE1, which is in sync with Microsoft Office file headers and its file extension. The file extension doc is consistent with the file extensions used by Microsoft Office Word. Figure B.1 displays the contents of file 001. In addition, information is shown in Figure B.2 below. On 4/9/2002 15:32:00, Bob Mastenson created the password-protected file 001 and was last modified at 15:32:00 on 4/9/2002.

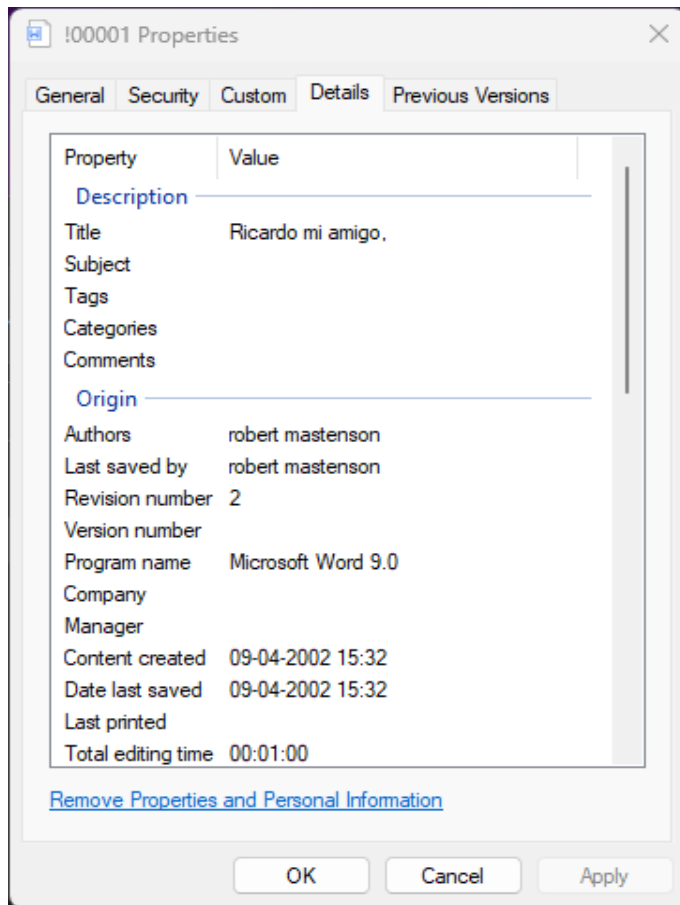
### **Figure B.2: Bob Mastenson's letter to Rick Bell**



Upon successfully cracking the password "special" for the first MS Word document, 000001, I discovered that the text was written for Rick Bell and contained shocking revelations. Bob Mastenson had sent Rick some "special" pictures and confessed his love for a woman named Abby, with whom he had enjoyed good times. However, the document also implied that Bob was potentially involved in sexual harassment with Abby, who could be an employee. The fact that the document was written for Rick suggested that both men were involved in sexual harassment. The line "older ones" indicated the potential existence of older female victims of harassment, with Bob sharing this information with Rick, seemingly to encourage his participation.

The document was password-protected and reserved for Bob's modification, indicating an attempt to cover his tracks and keep its contents hidden. The password for opening and modifying the document was "special", all in lowercase letters.

**Figure B.3:File 001 Metadata**

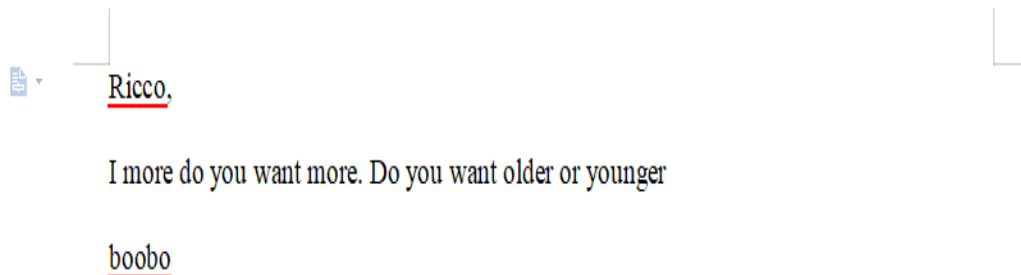


### **File 002: !00002.DOC**

File 002 is a Microsoft Office Document that was generated in Microsoft Word and saved on the pendrive as 000001. File 002's header had the hexadecimal string DOCF11E0A1B11AE1, which is in sync with Microsoft Office file headers and its file extension. The file extension doc is consistent with the file extensions used by Microsoft

Office Word. Figure B.3 displays the contents of file 001. In addition, information is shown in Figure B.4 below. On 6/14/2001 15:34:00, Bob Mastenson created the password-protected file 002 and was last modified at 6/14/2001 15:34:00.

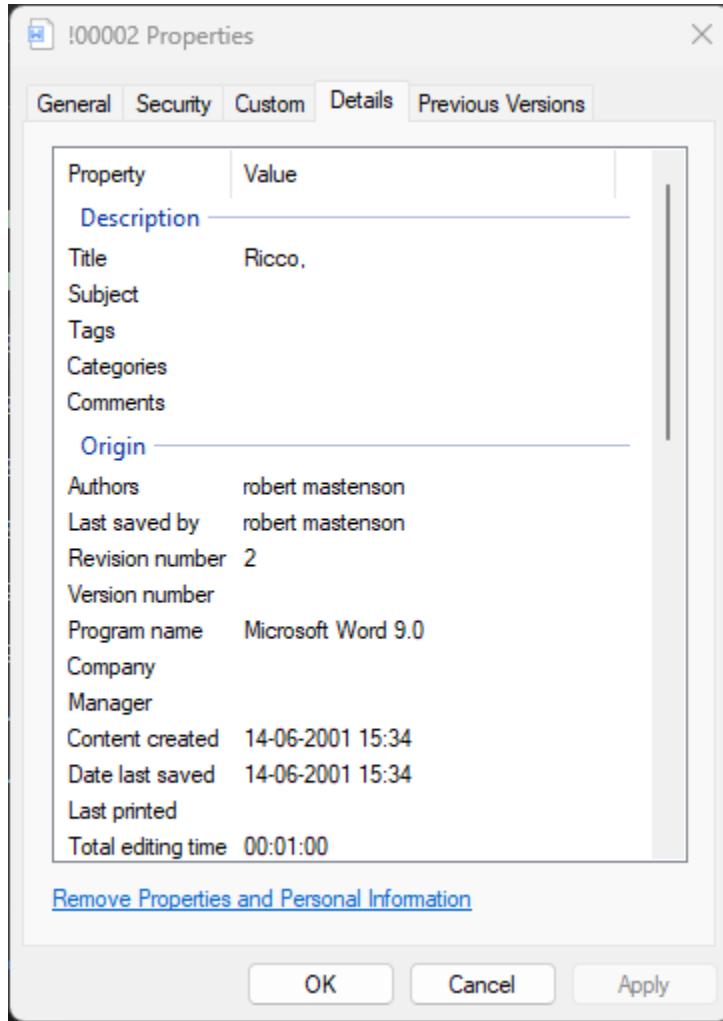
**Figure B.4:Bob Mastenson's letter to Rick Bell**



I defeated the password "picture" for the second MS Word document, 000002. This document contained text written for Rick Bell and revealed that Bob Mastenson is engaging in workplace sexual harassment with female employees of different age groups. Bob even offered Rick the option to choose between older and younger female employees to engage in sexual harassment with. The document was password protected and reserved for modification by Bob Mastenson, indicating that he did not want others to view its contents and was attempting to cover his tracks. The password for both opening and modifying the document is "picture," using all lowercase letters.



**Figure B.5:File 002 Metadata**



**File 003: !00003.doc**

File 002 is a Microsoft Office Document that was generated in Microsoft Word and saved on the pendrive as 000001. File 002's header had the hexadecimal string DOCF11E0A1B11AE1, which is in sync with Microsoft Office file headers and its file extension. The file extension doc is consistent with the file extensions used by Microsoft Office Word. Figure B.5 displays the contents of file 001. In addition, information is shown in Figure B.6 below. On 9/22/2006 15:36:00, Bob Mastenson created the password-protected file 002 and was last modified at 9/22/2006 15:36:00.



**Figure B.6:Bob Mastenson's letter to Rick Bell**

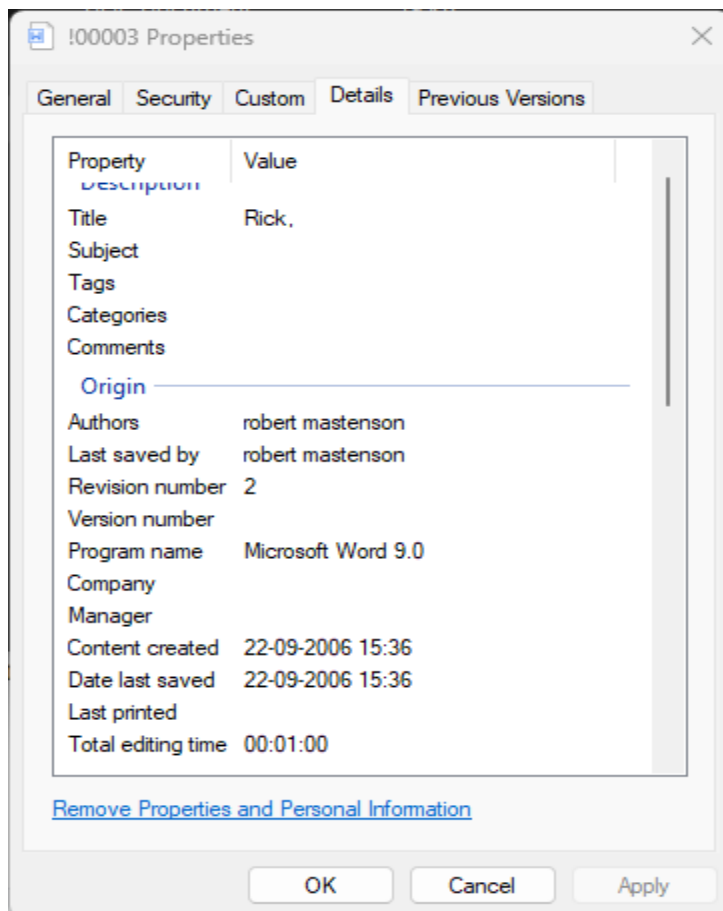
Rick,

I am sending these with a codewords because I don't trust email. The fbi can see it.  
What do you think of them

bobbo

Upon discovering the password "collect," I accessed the third MS Word document, 000003, which contained text written for Rick. The text revealed that Bob Mastenson was sending pictures with code words to Rick to avoid detection by the FBI. Bob expressed his lack of trust in email and even asked for Rick's opinion on the pictures he had sent. The document was password protected and reserved for modification by Bob, indicating his intention to keep the contents hidden and cover his tracks. The password for both opening and modifying the document is "collect," using all lowercase letters.

**Figure B.7:File 003 Metadata**



**Files Set 004: (Exhibit 2 - 000001.DOC,Exhibit 3- 000002.DOC,Exhibit 4- 000003.DOC)**

Exhibits 2 - 000001.DOC, 3 - 000002.DOC, 4 - 000003.DOC Are all a exact copy of of files !00001.DOC, !00003.DOC, and !00003.DOC, in that order. The hexadecimal string DOCF11E0A1B11AE1 was found in all of these files' headers, which is consistent with Microsoft Office file headers and file extensions.The file extension doc is compatible with Microsoft Office Word's file extensions. Other than what was previously addressed in Files 001 through 003, no new suspicious or fresh evidence relevant to the case was discovered.

**File 005: 000004 (IJG Library Q=85).jpg**

The evidence against Mastenson regarding his involvement in child pornography is overwhelming and deeply concerning. The JPEG file labeled as 000004 (IJG Library Q=85) provides incontrovertible evidence of Mastenson's illegal activities. The file contains a photo of a cat that falls under the category of "child porn" as defined by the laws of Illinois. The fact that Mastenson possessed this image is a clear indication of his intentions and activities. Furthermore, the content of the letter (!00001.doc) that Mastenson wrote to Rick Bell reveals a disturbing level of willingness to engage in illegal behavior. In the letter, Mastenson not only acknowledges his possession of illegal images but also boasts about his willingness to share them with others. This correspondence leaves no doubt as to Mastenson's intentions and activities. The photo in question, displayed in Figure B.7, is particularly disturbing in its content and context. The image is a clear and indisputable representation of illegal and immoral behavior. The fact that Mastenson was in possession of such an image raises serious concerns about his motivations and character.

**Figure B.8: Photo of “Child Pornography”(Cat)**



**File 006: 000005 (Photoshop Q=8).jpg**

The evidence supporting Mastenson's involvement in child pornography is both compelling and disturbing. The JPEG file labeled as 000005 (Photoshop Q=8) provides a clear and indisputable image of a cat that falls under the category of "child porn" as defined by the laws of Illinois. This file, along with the content of the letter (!00001.doc) written for Rick Bell, leaves no doubt as to Mastenson's intentions and activities. It is clear that he was not only willing to engage in illegal and immoral behavior, but actively sought out opportunities to do so. The photo in question, displayed in Figure B.8, is particularly disturbing in its content and context. The fact that Mastenson was in possession of such an image is a serious cause for concern, not only for the welfare of children but for society as a whole. The willingness to exploit and harm the most vulnerable among us is a deeply troubling indication of Mastenson's character and motives. The content of the letter (!00001.doc) further reveals Mastenson's willingness to engage in such activities and the fact that he had sent pictures to Rick Bell. This correspondence underscores the degree to which Mastenson was actively seeking out like-minded individuals with whom to share his illicit material. His actions not only violate the law but also represent a grave danger to the well-being of children.

**Figure B.9: Photo of “Child Pornography”(Cat)**



**File 007: 000006 (Photoshop Q=7).jpg**

Mastenson's involvement in adult pornography is supported by strong evidence found in the JPEG file labeled as 000006 (Photoshop Q=7). This photo, featuring a dog, falls under the category of "adult pornography" as defined by the laws of illinois. The file was sent alongside the letter (000003.doc) in which Mastenson stated that he was going to send some older photos and that he did not trust email for sending those photos. It is clear that Mastenson was intentionally hiding the content of the photos and attempting to conceal his activities. In the same letter, Mastenson further stated that he would send the photo with code words because he was afraid that the FBI could see the pictures. This statement provides additional evidence of Mastenson's involvement in "adult pornography" and his attempt to avoid detection by authorities. This new information further validates the previous evidence of Mastenson's illegal activities involving child pornography, as well as his willingness to engage in similar behavior with adult subjects. The fact that he was taking deliberate steps to conceal his actions from law enforcement authorities raises even more serious concerns about his intentions and potential danger to others. The photo in question, displayed in Figure B.9

**Figure B.10: Photo of “Adult Pornography”(Dog)**



**File 008: 000007 (IJG Library Q=73).jpg**

The evidence against Mastenson regarding his involvement in adult pornography is equally concerning and disturbing. File 000007 (IJG Library Q=73), a JPEG file that Mastenson possessed, contained a photo of a dog that is categorized as "adult pornography" as defined by the laws of illinois. This photo provides solid evidence that Mastenson was involved in the production and distribution of adult pornography. It is worth noting that Mastenson sent this photo, along with other older photos, to Rick Bell in a letter labeled as 000003.doc. In the same letter, Mastenson stated that he did not trust email for sending those photos, further indicating that he was aware of the illegal nature of his actions. This correspondence provides additional evidence of Mastenson's guilt and intentions. In fact, Mastenson went to great lengths to hide his activities, as he stated in his letter to Rick Bell that he would send photos with code words to avoid detection by the FBI. This is a clear indication that Mastenson knew that what he was doing was illegal and that he was actively attempting to avoid getting caught. The photo in question, displayed in Figure B.10

**Figure B.11: Photo of “Adult Pornography”(Dog)**



**File 009: 000008 (IJG Library Q=85).jpg**

Mastenson's involvement in child pornography is strongly supported by evidence from File 000008 (IJG Library Q=85). This JPEG file contains a photo of a cat that falls under the category of "child porn" according to the laws of illinois. The content of the letter (000001 doc) written for Rick Bell further reveals Mastenson's willingness to engage in such activities and that he had sent pictures to Bell. The photo in question is displayed in Figure B.9. This solidifies the fact that Mastenson was actively involved in the production and distribution of child pornography. The gravity of this situation cannot be overstated, as the production and distribution of such material is a serious crime that carries severe legal consequences. It is imperative that appropriate action be taken to hold Mastenson accountable for his actions and to ensure the safety and protection of potential victims. The photo in question, displayed in Figure B.11

**Figure B.12: Photo of “Child Pornography”(Cat)**



**File 010: !00009.GIF**

Upon examination of the contents of File 000009, it was found to be a GIF file that contained an image of a dog which can be categorized as "adult pornography" according to the laws of illinois. This photo serves as concrete evidence that Mastenson was involved in adult pornography. Interestingly, this photo is linked to the document 00001, where Mastenson mentions his love for "abbey" and the good times they had spent together. This document is significant because it implies that Mastenson was involved in

workplace sexual harassment during working hours, with "abbey" being one of his victims. The photo in question, displayed in Figure B.12

**Figure B.13: Photo of “Adult Pornography”(Dog)**



#### **File 011:Conduct of Professional Employees**

The COUNTERCT Rules for Conduct of Professional Employees specify guidelines for certain categories of employees within the company. These guidelines apply to professional employees, including engineers, designers, executive assistants, accountants, CFO, and CEO. As per this file Bob Mastenson and Rick Bell have already violated the company's policy by viewing and transmitting inappropriate assets/Images.

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

List of all the files contained in the examination media (USB )

File 001: !00001.doc

File 002: !00002.doc

File 003: !00003.doc

File 000004.JPEG

File 000005.JPEG

File 000006.JPEG

File 0000 7.JPEG

File 000008.JPEG

File 000009.GIF

Conduct of Professional Employees.doc



### All retrieved files with the MD5 , SHA1 value:

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	MD5	SHA1	FileNames										
2	a1f88927eab367505edc8d3b3d3b3de6	a016997568ac528529d878d6d5a27228c7d7237b	\\.\PHYSICALDRIVE2\Partition 1 [29339MB]\NONAME [FAT32]\[root]\Forensics project\100001.DOC										
3	53040d89b6601ba5e122060bc15d78e2	a44aae1299d524b33fa0c5fe70414a5cac47706	\\.\PHYSICALDRIVE2\Partition 1 [29339MB]\NONAME [FAT32]\[root]\Forensics project\100002.DOC										
4	2076ad01240c3d41751043fcd30e8409	c2c41217c8abf30b89e0949c2e5f473beba52efa	\\.\PHYSICALDRIVE2\Partition 1 [29339MB]\NONAME [FAT32]\[root]\Forensics project\100003.DOC										
5	f83da0aa1d8c9b9a89957df83fbfb90	9832f2c4c2afe549abb2ada7c30a6907705457e1	\\.\PHYSICALDRIVE2\Partition 1 [29339MB]\NONAME [FAT32]\[root]\Forensics project\000004 (JG Library Q=85).jpg										
6	69e79eacd9a6d2aa07b1bfb75c43c771	f930dc0bab16d0b49c0bcae9b2642dcf9fadd9ea	\\.\PHYSICALDRIVE2\Partition 1 [29339MB]\NONAME [FAT32]\[root]\Forensics project\000005 (Photoshop Q=8).jpg										
7	3b89de0cf4d6eb56dec85b524297cf8	62c246a7759b887b240f026457e52902001958cd	\\.\PHYSICALDRIVE2\Partition 1 [29339MB]\NONAME [FAT32]\[root]\Forensics project\000006 (Photoshop Q=7).jpg										
8	9c482e70a78b775a1d8e228d50eeb8c	62bb2c0cfa0a47fd7aa1beae337560b7151e650	\\.\PHYSICALDRIVE2\Partition 1 [29339MB]\NONAME [FAT32]\[root]\Forensics project\000007 (JG Library Q=73).jpg										
9	60f56509987010932b9ec044c59c52c3	9b6629f21d9604610780a169eb88831c4490ba9c	\\.\PHYSICALDRIVE2\Partition 1 [29339MB]\NONAME [FAT32]\[root]\Forensics project\000008 (JG Library Q=85).jpg										
10	d1383607c1718ce88f7b035c6b7a980f	ef062da7a2404b52a364f6e2b00146865c957926	\\.\PHYSICALDRIVE2\Partition 1 [29339MB]\NONAME [FAT32]\[root]\Forensics project\000009.GIF										
11	aabaf921f22a3b05aed995c8a7beeca	bd24de1176b3ad9606eaa1043a687d5ca0ddff	\\.\PHYSICALDRIVE2\Partition 1 [29339MB]\NONAME [FAT32]\[root]\Forensics project\Conduct of Professional Employees.doc										
12	742c2853088eeb1be0ffef281738b67e8	7d31385be76f72c3097932430fda7b57e459f63	\\.\PHYSICALDRIVE2\Partition 1 [29339MB]\NONAME [FAT32]\[root]\Forensics project\COUNTERCT.doc										
13	a1f88927eab367505edc8d3b3d3b3de6	a016997568ac528529d878d6d5a27228c7d7237b	\\.\PHYSICALDRIVE2\Partition 1 [29339MB]\NONAME [FAT32]\[root]\Forensics project\Exhibit 2- 000001.doc.doc										
14	53040d89b6601ba5e122060bc15d78e2	a44aae1299d524b33fa0c5fe70414a5cac47706	\\.\PHYSICALDRIVE2\Partition 1 [29339MB]\NONAME [FAT32]\[root]\Forensics project\Exhibit 3- 000002.doc.doc										
15	2076ad01240c3d41751043fcd30e8409	c2c41217c8abf30b89e0949c2e5f473beba52efa	\\.\PHYSICALDRIVE2\Partition 1 [29339MB]\NONAME [FAT32]\[root]\Forensics project\Exhibit 4- 000003.doc.doc										
16	43060987cfd027ada273b325acc4758e	6a2b8d12838f5f86d6673e38e92a368b27c2f588	\\.\PHYSICALDRIVE2\Partition 1 [29339MB]\NONAME [FAT32]\[root]\Forensics project\exit strategy.xls										
17	7ece097903094ec9c2ab22ad79116d28	457ee06636301534de4428565845282d940c5496	\\.\PHYSICALDRIVE2\Partition 1 [29339MB]\NONAME [FAT32]\[root]\Forensics project\passwords.txt										
18	16b3f602ad826865cbe73dfb345d5da	d8837e67e881d9fb187143eb8e3e3354adb354a8	\\.\PHYSICALDRIVE2\Partition 1 [29339MB]\NONAME [FAT32]\[root]\Forensics project\summation example.pdf										
19	16be8de22f661300a874f58a6f5e4a5	1b46fd2d14e53650e667fb0e3fe3674f5ee4f3	\\.\PHYSICALDRIVE2\Partition 1 [29339MB]\NONAME [FAT32]\[root]\Forensics project\wasilewski.doc										

## Appendix B: Policy on Evidence Collection

Obtained evidence is tagged upon acquisition with a case number. Once a case number has been assigned to a piece of evidence, a log of that evidence is started and maintained throughout the investigation. All evidence related to the case is logged and maintained including physical evidence and images. All evidence is stored in a fire safe and key secured evidence lockup. Keys are issued when, and only when, evidence is signed out of the evidence lockup. All sign outs are maintained on a chain of custody log which is also stored in a fire safe lockup. Exhibits were provided to Mr.Jenkins.

## Appendix C: Policy on Forensically Sterile Media

All media used for case investigations is forensically sterile. All media, prior to 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

**Deleted Files:** Files which 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.

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



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

**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.

**USB Key:** Universal serial bus key. A portable storage device that uses flash memory.USB keys can be used in place of floppy disks, CD-ROMs, etc.

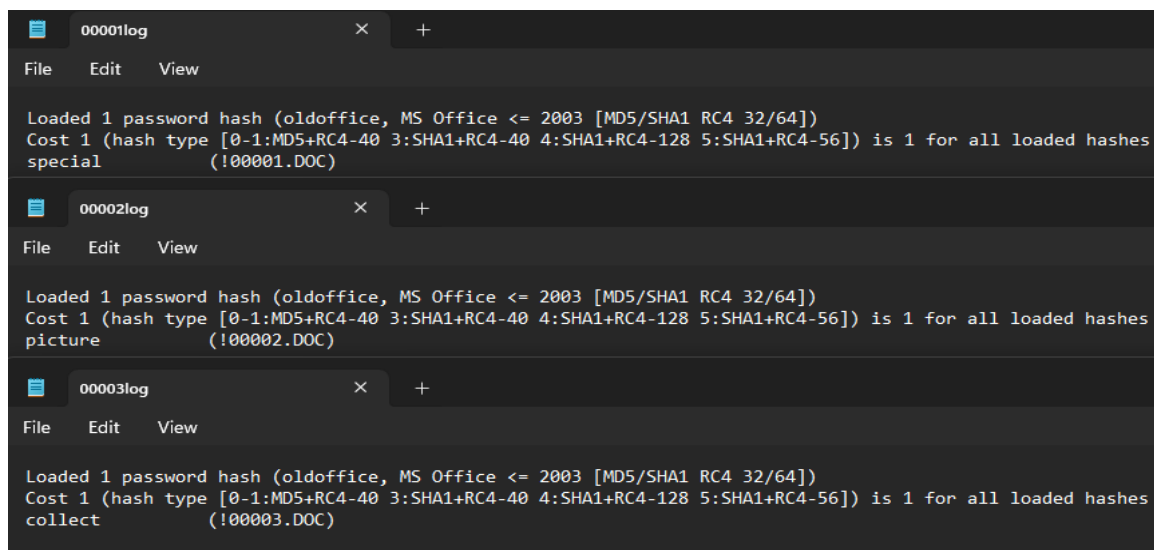
## Appendix E: Application Logs

### John the Ripper Logs

```
(root@kali)-[/home/kali/Desktop/Uncracked]
# john --wordlist=/usr/share/wordlists/nmap.lst 1.txt > 00001log.txt
Using default input encoding: UTF-8
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1g 0:00:00:00 DONE (2023-04-10 16:58) 100.0g/s 204800p/s 204800c/s 204800C/s 14344..minime
Use the "--show --format=oldoffice" options to display all of the cracked passwords reliably
Session completed.
```

```
(root@kali)-[/home/kali/Desktop/Uncracked]
# john --wordlist=/usr/share/wordlists/nmap.lst 2.txt > 00002log.txt
Using default input encoding: UTF-8
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1g 0:00:00:00 DONE (2023-04-10 16:58) 33.33g/s 68266p/s 68266c/s 68266C/s 14344..minime
Use the "--show --format=oldoffice" options to display all of the cracked passwords reliably
Session completed.
```

```
(root@kali)-[/home/kali/Desktop/Uncracked]
# john --wordlist=/usr/share/wordlists/john.lst 3.txt > 00003log.txt
Using default input encoding: UTF-8
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1g 0:00:00:00 DONE (2023-04-10 16:58) 50.00g/s 51200p/s 51200c/s 51200C/s 123456..random
Use the "--show --format=oldoffice" options to display all of the cracked passwords reliably
Session completed.
```



```
00001log
File Edit View

Loaded 1 password hash (oldoffice, MS Office <= 2003 [MD5/SHA1 RC4 32/64])
Cost 1 (hash type [0-1:MD5+RC4-40 3:SHA1+RC4-40 4:SHA1+RC4-128 5:SHA1+RC4-56]) is 1 for all loaded hashes
special
(!00001.DOC)

00002log
File Edit View

Loaded 1 password hash (oldoffice, MS Office <= 2003 [MD5/SHA1 RC4 32/64])
Cost 1 (hash type [0-1:MD5+RC4-40 3:SHA1+RC4-40 4:SHA1+RC4-128 5:SHA1+RC4-56]) is 1 for all loaded hashes
picture
(!00002.DOC)

00003log
File Edit View

Loaded 1 password hash (oldoffice, MS Office <= 2003 [MD5/SHA1 RC4 32/64])
Cost 1 (hash type [0-1:MD5+RC4-40 3:SHA1+RC4-40 4:SHA1+RC4-128 5:SHA1+RC4-56]) is 1 for all loaded hashes
collect
(!00003.DOC)
```

**Applications Logs:**

John the Ripper: public domain, open source software, free and available for public use.

AccessData® FTK® Imager v4.7.1.2: public domain, open source software, free and available for public use.

Autopsy 4.20.0: public domain, open source software, free and available for public use.