Harsimran Kaur V00879358

Maninder Singh V00879900

ELEC 570 – Project II: Investigating Blackmailing

(Weight: 30%; Due: July 13, 2017)

Case Description

Alicia Peabody is a key executive for a major retailer who had been contacted by an unknown person that stated he had in his possession some compromising pictures and letters of her and her exboyfriend. Alicia is married and had had an affair with that boyfriend. The suspect provided proof of possession of the documents by sending by email a copy of the handwritten signature of Alicia that she usually uses to sign her correspondences. The suspect then threatened Alicia with exposing the letters and pictures, unless she would pay a ransom. Alicia who is concerned not only with her reputation at work, but also with protecting her marriage, reported in confidence the threat to the police. In her police report, she indicated that she suspected that the blackmailer was none other than the exboyfriend himself, since the relationship didn't end up well. She indicated that she believes that the compromising material in possession of the ex-boyfriend consist of 2 love letters and 1 compromising picture of both of them.

The police invited for an interview the suspected boyfriend, whose name is John Lewis. Mr. Lewis denied being the blackmailer, and also claimed that he has even deleted from his computer all letters and pictures about Alicia immediately after the breakup. He also indicated that he doesn't know anything about Jekyll.hyde@yahoo.com, the email address used by the suspected blackmailer. As the answers provided by Mr. Lewis raised more suspicion, he was asked and agreed to take a polygraph examination. He failed the polygraph examination, which prompted the police to obtain a search warrant and seize his PC. The disk image of the computer was acquired as part of the evidentiary items.

The blackmail email, and sample regular emails exchanged between Ms. Peabody and Mr. Lewis, were collected and added to the evidence.

Task

As forensic expert, you are tasked with investigating whether there is enough evidence to support the claim that John Lewis is the blackmailer.

The disk image with corresponding hashes and additional evidence can be downloaded here:

The size of the uncompressed folder is 59.8 Gb. Therefore, it is expected that download would take several hours. It took about 37hrs to upload the image to Google drive with high speed Internet.

https://drive.google.com/file/d/0B1xnRxT-Y8DMMnZhRUs3YzI0RWs/view?usp=sharing

Your task is to analyze the evidence, and extract all the relevant data for the investigation. You are expected to document your findings in a forensic report to be given to the police (and submitted as your answer to the assignment). A forensic report is a step-by-step list of everything you have done and what the results were. You don't need to actually list all of the failed attempts or crowd it with non-relevant facts. Keep it accurate, relevant and simple.

Ensure that you answer in particular the following questions that the police are interested in:

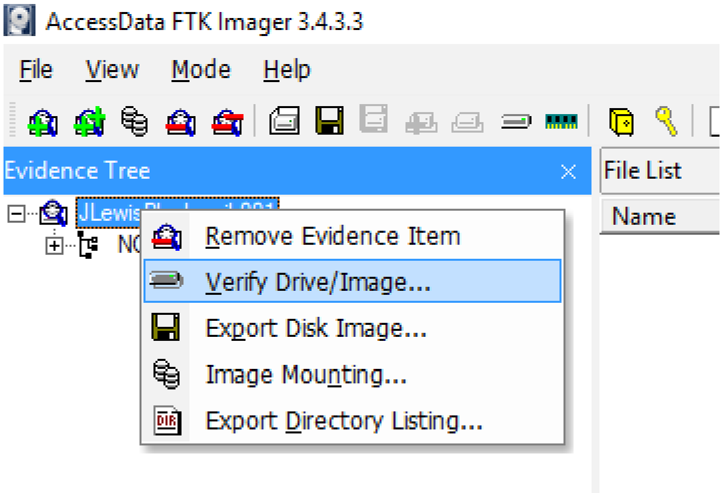
1. Check the validity of the forensic image using the supplied hashes. [1%]

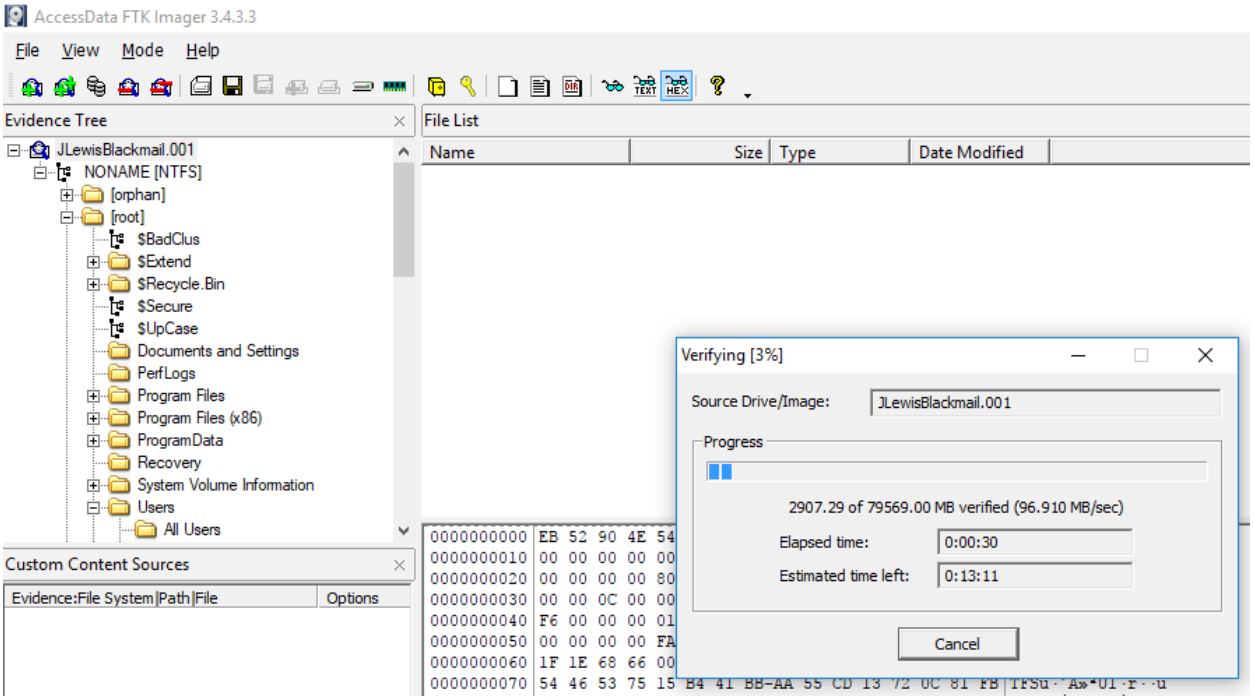
   Answer:

   To check the validity of forensic image we need to verify that the computed hash and reported hash values should match for MD5 Hash and SHA1 Hash and verify the result as match.

   We can do this as follows:

   Right click on the image we want to verify as valid.





```
0000000000 EB 52 90 4E 54
0000000010 00 00 00 00 00
0000000020 00 00 00 00 80
0000000030 00 00 0C 00 00
0000000040 F6 00 00 00 01
0000000050 00 00 00 00 FA
0000000060 1F 1E 68 66 00
0000000070 54 46 53 75 15 B4 41 BB-AA 55 CD 13 72 0C 81 FB TFSu·´A»ªU1·r··u
```

Verifying [3%]

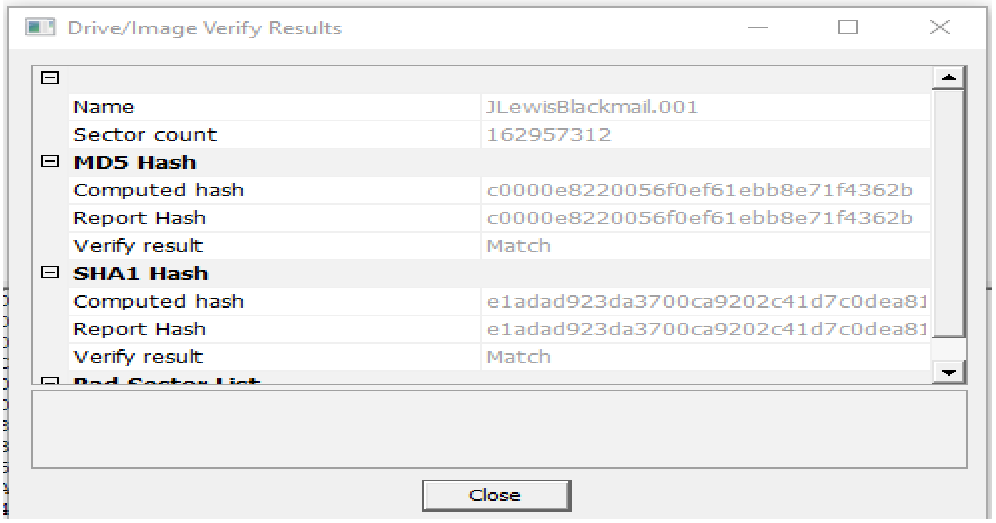
Source Drive/Image: JLewisBlackmail.001

Progress

2907.29 of 79569.00 MB verified (96.910 MB/sec)

Elapsed time: 0:00:30

Estimated time left: 0:13:11



⊟	
Name	JLewisBlackmail.001
Sector count	162957312
⊟ **MD5 Hash**	
Computed hash	c0000e8220056f0ef61ebb8e71f4362b
Report Hash	c0000e8220056f0ef61ebb8e71f4362b
Verify result	Match
⊟ **SHA1 Hash**	
Computed hash	e1adad923da3700ca9202c41d7c0dea81
Report Hash	e1adad923da3700ca9202c41d7c0dea81
Verify result	Match
⊟ **Bad Sector List**	

From the image above it is seen that the MD5 and SHA1 Hash values are matched for hash values. So the disk image acquired is valid.

2. What crucial data are available on the seized device? Indicate the specific files that contain such data and explain the importance of the different pieces of information for the investigation. All relevant information must be identified. Explain what processes did you (the investigator) used to successfully examine the image and uncover the evidence, by highlighting explicitly the logical process or thought that led to the discovery of the relevant information. [15%]

Answer:

We have used AccessData's FTK Imager to do disk imaging.

Step 1: run FTK Imager.exe to start the tool. Then upload the image and we can see all the files in the evidence tree on the left hand side of the FTK imager window.

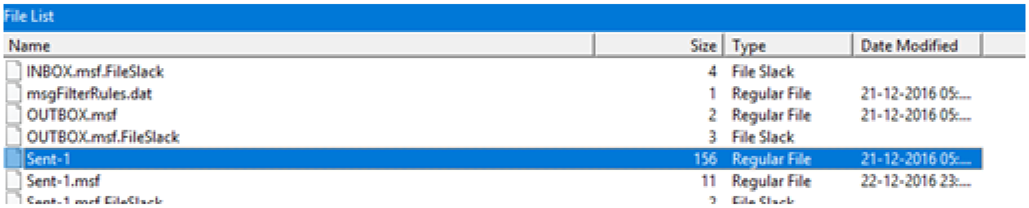
As given in the assignment as HINT we are focusing on the deleteme folder which is suspects home folder as follows

Root-> users->deleteme

Evidence 1:

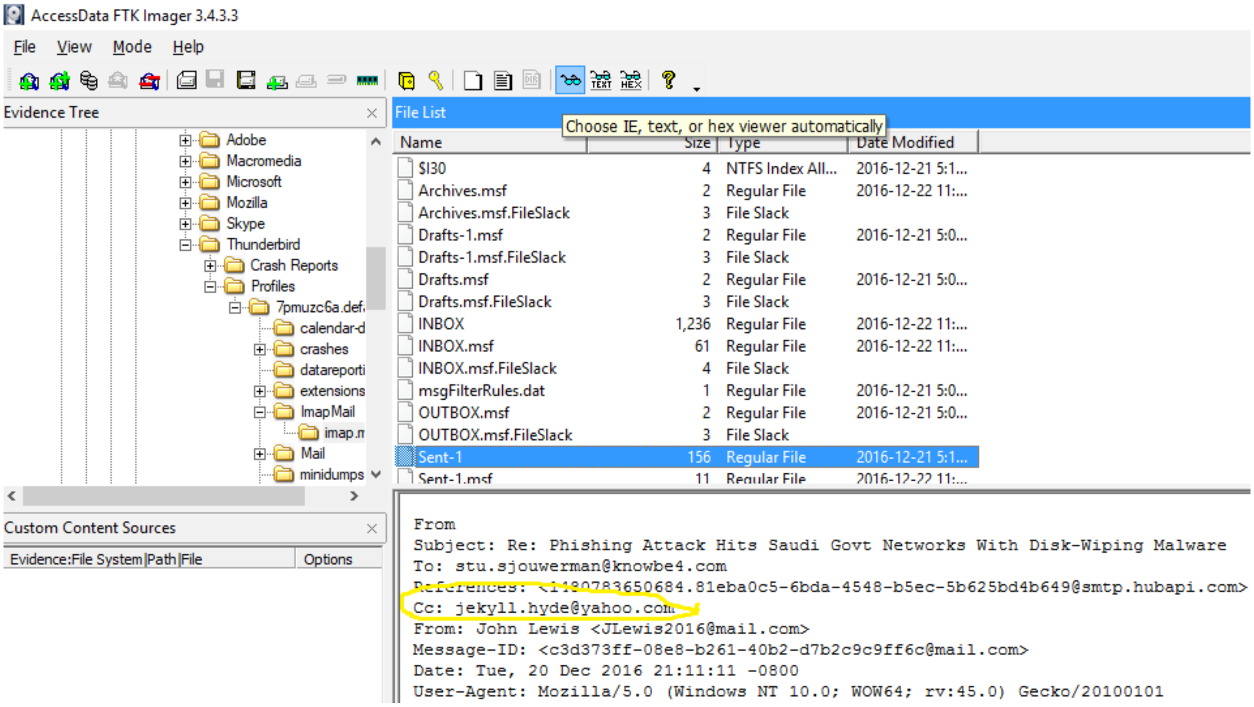
Root->users->Deleteme->AppData->Roaming->Thunderbird->Profiles->7pmuzc6a.default->ImapMail->imap.mail.com->Sent-1

When we viewed this file in automatic (IE) mode we found that the blackmailer has put Jekyll.hyde@yahoo.com in the CC and the original sender is Mr Lewis with email Id jlewis2016@mail.com and when he was investigated he told that he doesn't know anything about the Jekyll.hyde@yahoo.com email id . From here we can illustrate blackmailer might be Mr. Lewis because he put this email in the cc first then used the same email id to send Ms. Alicia the blackmailing email just to hide him, or it is a close or hired person but for sure to whom he sent the love letters and compromised picture of both of them so that he can blackmail Ms. Alicia, Mr. Lewis is for sure involved.



File List

Name	Size	Type	Date Modified
INBOX.msf.FileSlack	4	File Slack	
msgFilterRules.dat	1	Regular File	21-12-2016 05:...
OUTBOX.msf	2	Regular File	21-12-2016 05:...
OUTBOX.msf.FileSlack	3	File Slack	
Sent-1	156	Regular File	21-12-2016 05:...
Sent-1.msf	11	Regular File	22-12-2016 23:...
Sent-1.msf.FileSlack	2	File Slack	



File List

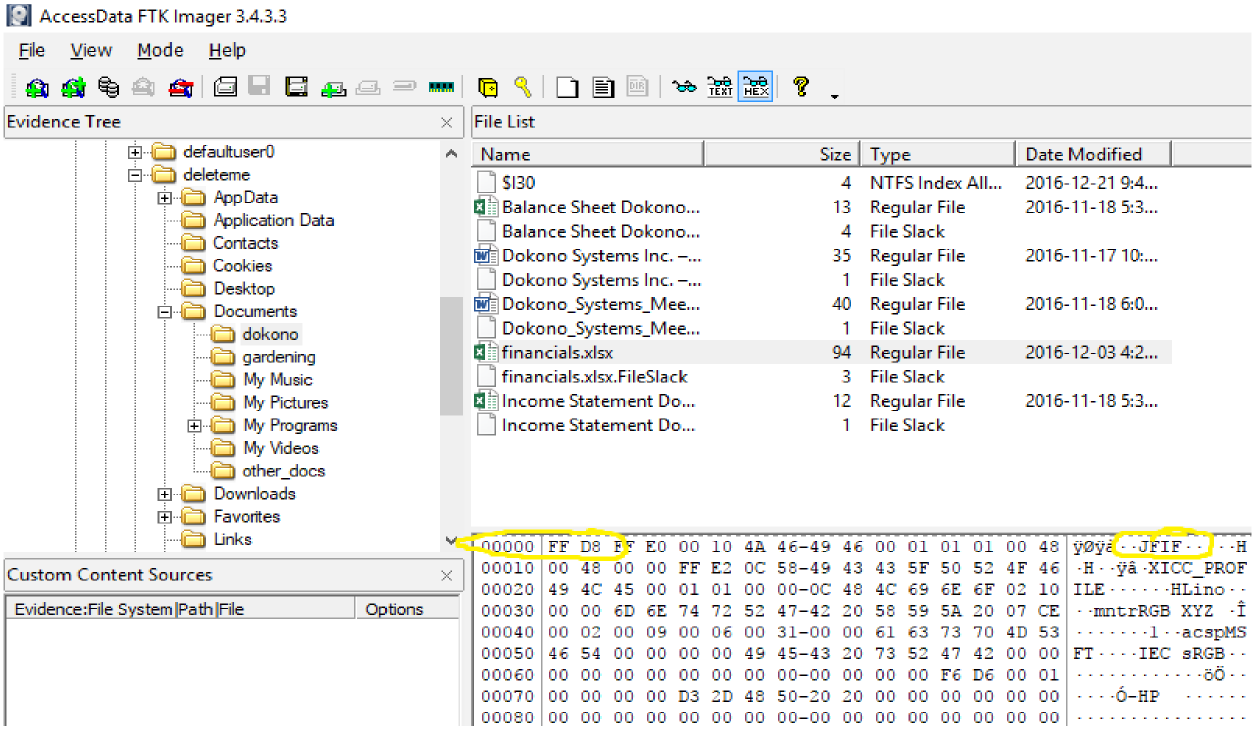
Name	Size	Type	Date Modified
$I30	4	NTFS Index All...	2016-12-21 5:1...
Archives.msf	2	Regular File	2016-12-22 11:...
Archives.msf.FileSlack	3	File Slack	
Drafts-1.msf	2	Regular File	2016-12-21 5:0...
Drafts-1.msf.FileSlack	3	File Slack	
Drafts.msf	2	Regular File	2016-12-21 5:0...
Drafts.msf.FileSlack	3	File Slack	
INBOX	1,236	Regular File	2016-12-22 11:...
INBOX.msf	61	Regular File	2016-12-22 11:...
INBOX.msf.FileSlack	4	File Slack	
msgFilterRules.dat	1	Regular File	2016-12-21 5:0...
OUTBOX.msf	2	Regular File	2016-12-21 5:0...
OUTBOX.msf.FileSlack	3	File Slack	
Sent-1	156	Regular File	2016-12-21 5:1...
Sent-1.msf	11	Regular File	2016-12-22 11:...

```
From
Subject: Re: Phishing Attack Hits Saudi Govt Networks With Disk-Wiping Malware
To: stu.sjouwerman@knowbe4.com
References: <1480783650684.81eba0c5-6bda-4548-b5ec-5b625bd4b649@smtp.hubapi.com>
Cc: jekyll.hyde@yahoo.com
From: John Lewis <JLewis2016@mail.com>
Message-ID: <c3d373ff-08e8-b261-40b2-d7b2c9c9ff6c@mail.com>
Date: Tue, 20 Dec 2016 21:11:11 -0800
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:45.0) Gecko/20100101
```

Evidence 2:

deleteme->documents->dokono->financials.xlsx

When we browsed the financial.xlsx in the HEX mode which is saved as .xlsx which is the extension of EXCEL, then we noticed the “JFIF” tag which is characteristic of JPEG file. Also at the beginning of the file constant byte values 0xFF D8 which always mark the start of the image (SOI) of a JPEG file as shown in the figure below.

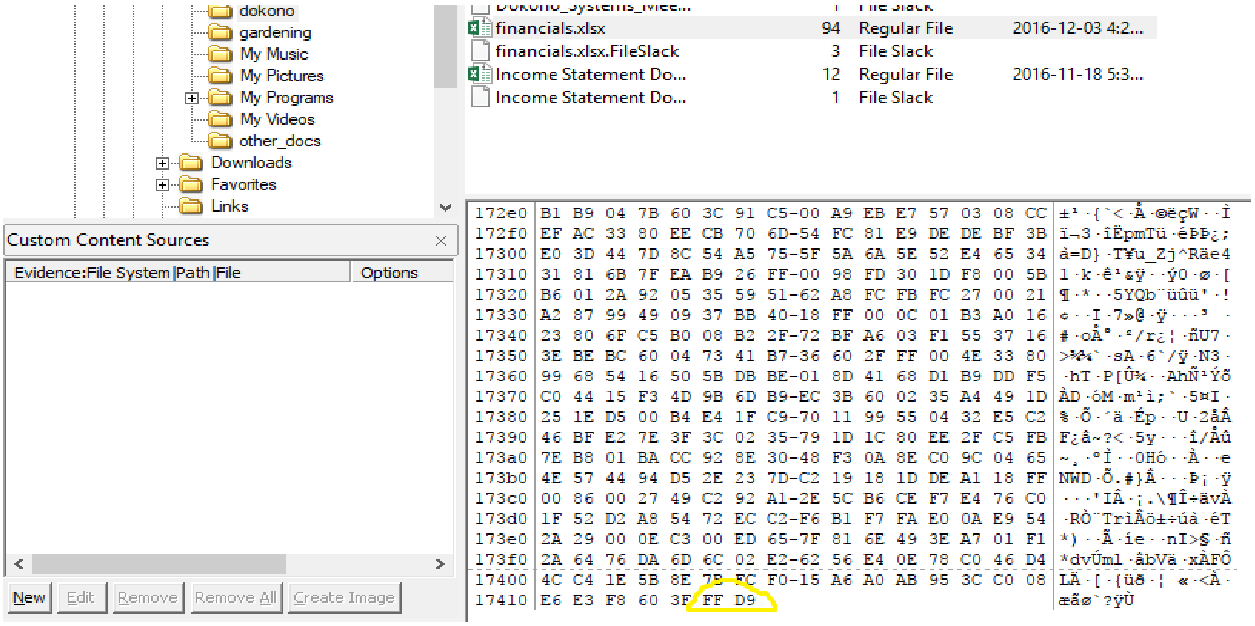


File List

Name	Size	Type	Date Modified
$I30	4	NTFS Index All...	2016-12-21 9:4...
Balance Sheet Dokono...	13	Regular File	2016-11-18 5:3...
Balance Sheet Dokono...	4	File Slack	
Dokono Systems Inc. –...	35	Regular File	2016-11-17 10:...
Dokono Systems Inc. –...	1	File Slack	
Dokono_Systems_Mee...	40	Regular File	2016-11-18 6:0...
Dokono_Systems_Mee...	1	File Slack	
financials.xlsx	94	Regular File	2016-12-03 4:2...
financials.xlsx.FileSlack	3	File Slack	
Income Statement Do...	12	Regular File	2016-11-18 5:3...
Income Statement Do...	1	File Slack	

```
00000 FF D8 FF E0 00 10 4A 46-49 46 00 01 01 01 00 48  ÿØÿà··JFIF··  ··H
00010 00 48 00 00 FF E2 0C 58-49 43 43 5F 50 52 4F 46  ·H··ÿâ·XICC_PROF
00020 49 4C 45 00 01 01 00 00-0C 48 4C 69 6E 6F 02 10  ILE······HLino··
00030 00 00 6D 6E 74 72 52 47-42 20 58 59 5A 20 07 CE  ··mntrRGB XYZ ·Î
00040 00 02 00 09 00 06 00 31-00 00 61 63 73 70 4D 53  ·······1··acspMS
00050 46 54 00 00 00 00 49 45-43 20 73 52 47 42 00 00  FT····IEC sRGB··
00060 00 00 00 00 00 00 00 00-00 00 00 00 F6 D6 00 01  ············öÖ··
00070 00 00 00 00 D3 2D 48 50-20 20 00 00 00 00 00 00  ····Ó-HP  ······
00080 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
```

Similarly we noticed that the JPEG file ends with the constant byte values 0xFF D9 which always mark the end of a JPEG file.

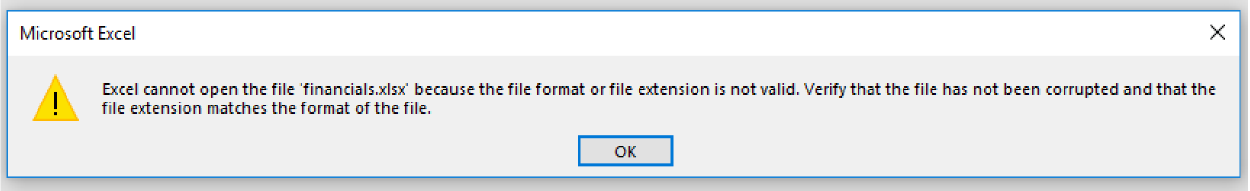


financials.xlsx	94	Regular File	2016-12-03 4:2...
financials.xlsx.FileSlack	3	File Slack	
Income Statement Do...	12	Regular File	2016-11-18 5:3...
Income Statement Do...	1	File Slack	

```
172e0 B1 B9 04 7B 60 3C 91 C5-00 A9 EB E7 57 03 08 CC ±¹·{`<·Å·©ëçW··Ì
172f0 EF AC 33 80 EE CB 70 6D-54 FC 81 E9 DE DE BF 3B ï¬3·îËpmTü·éÞÞ¿;
17300 E0 3D 44 7D 8C 54 A5 75-5F 5A 6A 5E 52 E4 65 34 à=D}·T¥u_Zj^Räe4
17310 31 81 6B 7F EA B9 26 FF-00 98 FD 30 1D F8 00 5B 1·k·ê¹&ÿ··ý0·ø·[
17320 B6 01 2A 92 05 35 59 51-62 A8 FC FB FC 27 00 21 ¶·*··5YQb¨üûü'·!
17330 A2 87 99 49 09 37 BB 40-18 FF 00 0C 01 B3 A0 16 ¢··I·7»@·ÿ···³ ·
17340 23 80 6F C5 B0 08 B2 2F-72 BF A6 03 F1 55 37 16 #·oÅ°·²/r¿¦·ñU7·
17350 3E BE BC 60 04 73 41 B7-36 60 2F FF 00 4E 33 80 >¾¼`·sA·6`/ÿ·N3·
17360 99 68 54 16 50 5B DB BE-01 8D 41 68 D1 B9 DD F5 ·hT·P[Û¾··AhÑ¹Ýõ
17370 C0 44 15 F3 4D 9B 6D B9-EC 3B 60 02 35 A4 49 1D ÀD·óM·m¹ì;`·5¤I·
17380 25 1E D5 00 B4 E4 1F C9-70 11 99 55 04 32 E5 C2 %·Õ·´ä·Ép··U·2åÂ
17390 46 BF E2 7E 3F 3C 02 35-79 1D 1C 80 EE 2F C5 FB F¿â~?<·5y···î/Åû
173a0 7E B8 01 BA CC 92 8E 30-48 F3 0A 8E C0 9C 04 65 ~¸·ºÌ··0Hó··À··e
173b0 4E 57 44 94 D5 2E 23 7D-C2 19 18 1D DE A1 18 FF NWD·Õ.#}Â···Þ¡·ÿ
173c0 00 86 00 27 49 C2 92 A1-2E 5C B6 CE F7 E4 76 C0 ···'IÂ·¡.\¶Î÷ävÀ
173d0 1F 52 D2 A8 54 72 EC C2-F6 B1 F7 FA E0 0A E9 54 ·RÒ¨TrìÂö±÷úà·éT
173e0 2A 29 00 0E C3 00 ED 65-7F 81 6E 49 3E A7 01 F1 *)··Ã·íe··nI>§·ñ
173f0 2A 64 76 DA 6D 6C 02 E2-62 56 E4 0E 78 C0 46 D4 *dvÚml·âbVä·xÀFÔ
17400 4C C4 1E 5B 8E 7B FC F0-15 A6 A0 AB 95 3C C0 08 LÄ·[·{üð·¦ «·<À·
17410 E6 E3 F8 60 3F FF D9                            æãø`?ÿÙ
```

The constant values 0xFF D8 and 0xFF D9 are called magic numbers. And these tell us that the file is truly a JPEG image not a EXCEL file.

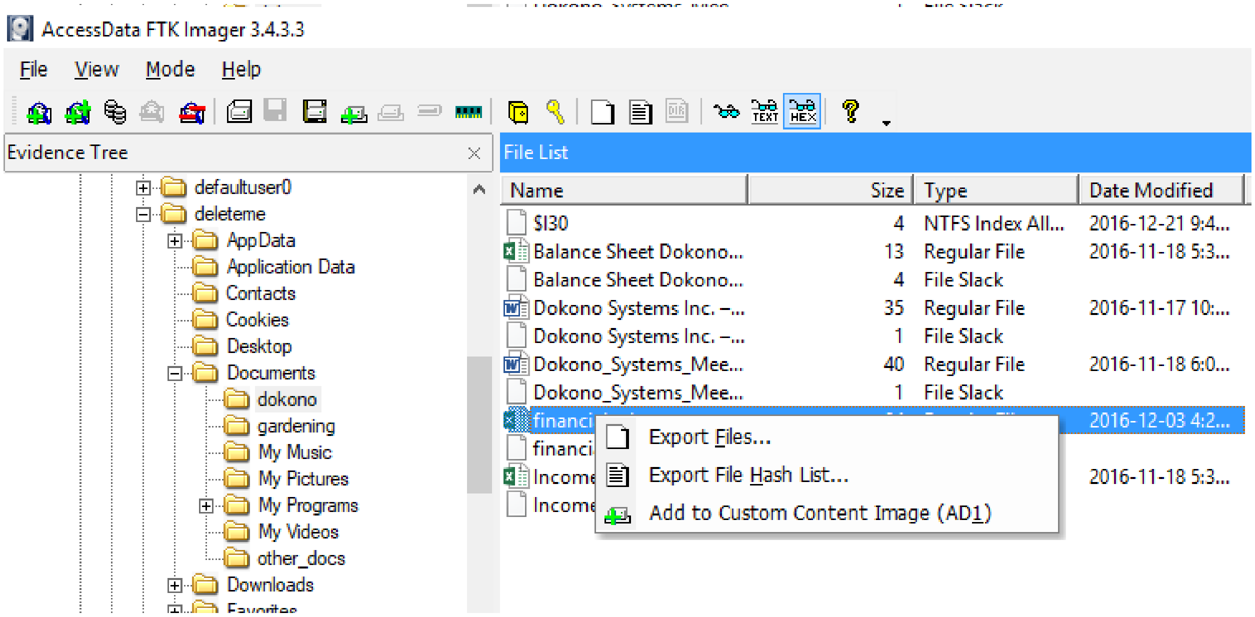
To further make sure that if it is excel file we tried opening it and got this msg.



Microsoft Excel

Excel cannot open the file 'financials.xlsx' because the file format or file extension is not valid. Verify that the file has not been corrupted and that the file extension matches the format of the file.

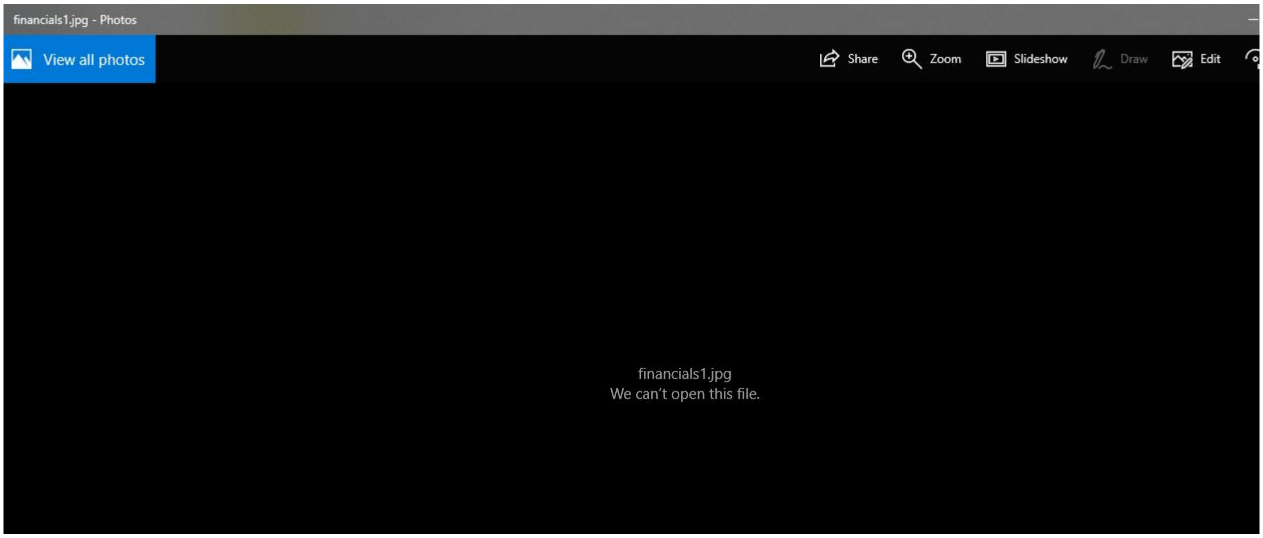
So we have exported the file on the desktop to do further analysis to reconstruct the image further.



AccessData FTK Imager 3.4.3.3

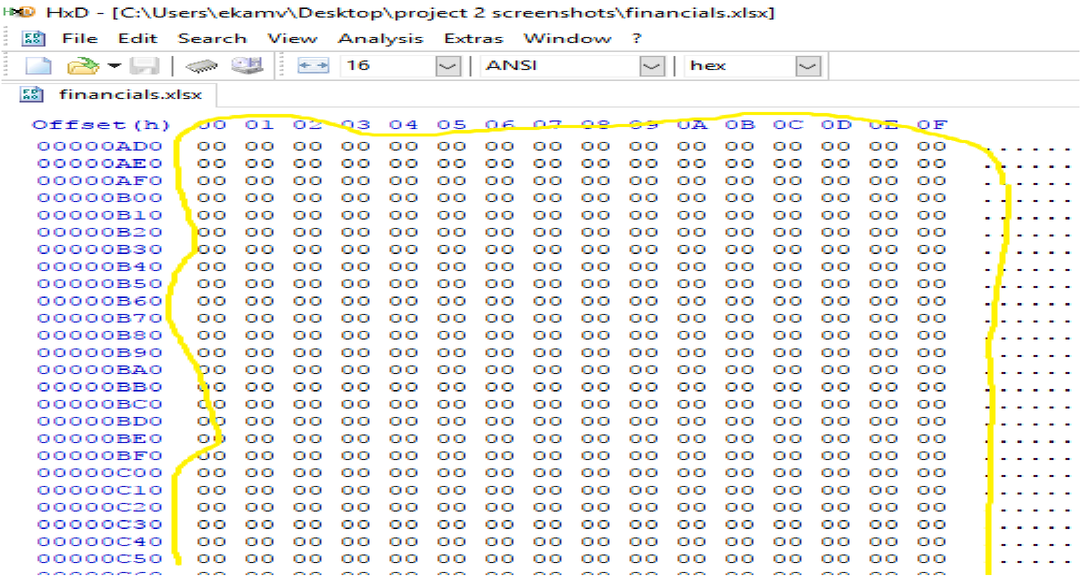
Name	Size	Type	Date Modified
$I30	4	NTFS Index All...	2016-12-21 9:4...
Balance Sheet Dokono...	13	Regular File	2016-11-18 5:3...
Balance Sheet Dokono...	4	File Slack	
Dokono Systems Inc. –...	35	Regular File	2016-11-17 10:...
Dokono Systems Inc. –...	1	File Slack	
Dokono_Systems_Mee...	40	Regular File	2016-11-18 6:0...
Dokono_Systems_Mee...	1	File Slack	
financi			2016-12-03 4:2...
financi			
Income			2016-11-18 5:3...
Income			

Then we have used HxD Hexeditor which has the basic hex editing, capabilities for searching and replacing the deleting of byte patterns to open the **financials.xlsx.** After changing the file extension to .jpg instead of .xlsx it was not still opening.



financials1.jpg
We can't open this file.

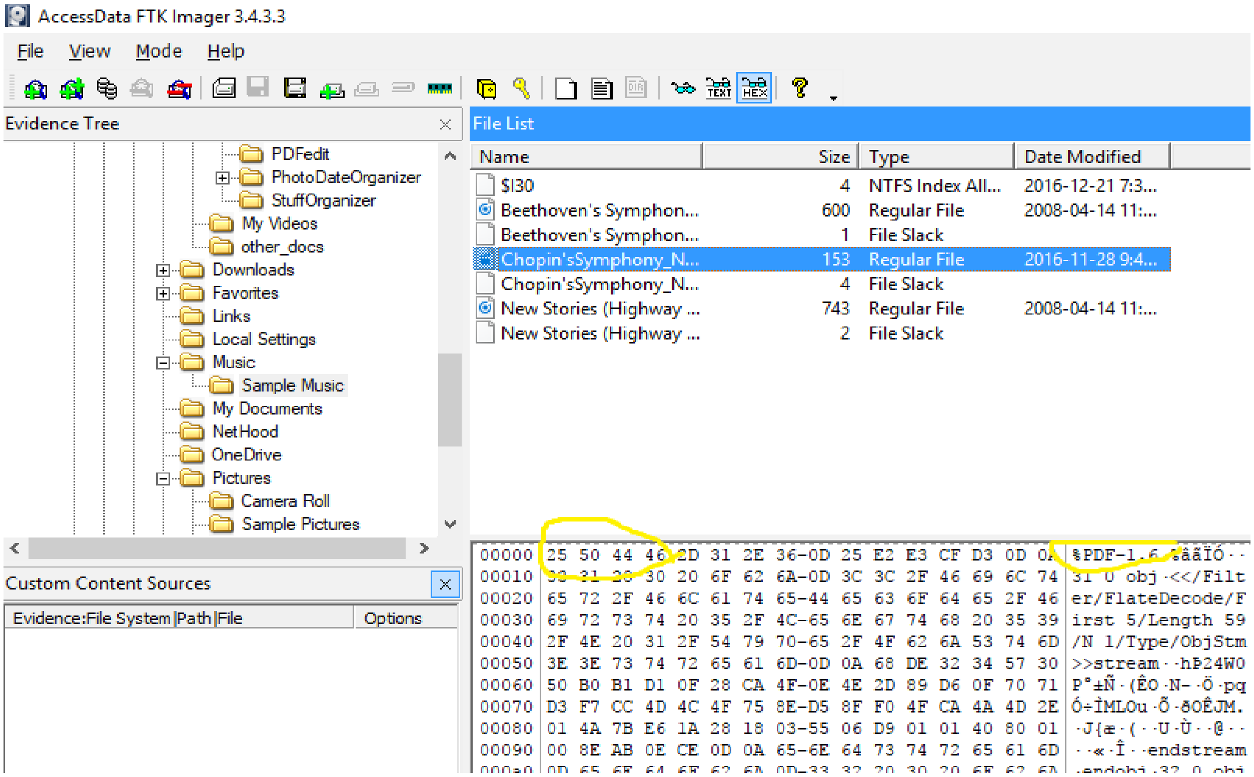
Upon exploring the byte patterns we found that there are **a large number of zeros which are embedded to corrupt the image intentionally Upon removing the zeros and saving it in .JPEG format, we found a compromising image of Mr. Lewis and Ms. Alicia.** So, this is the first evidence that Mr. Lewis is the person who is trying to black mail Ms. Alicia Peabody. The compromised image is shown below.


HxD - [C:\Users\ekamv\Desktop\project 2 screenshots\financials.xlsx]
File
Edit
Search
View
Analysis
Extras
Window
?
16
ANSI
hex
financials.xlsx

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000AD0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000AE0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000AF0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000B00   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000B10   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000B20   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000B30   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000B40   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000B50   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000B60   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000B70   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000B80   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000B90   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000BA0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000BB0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000BC0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000BD0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000BE0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000BF0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000C00   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000C10   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000C20   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000C30   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000C40   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
00000C50   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......
```

Evidence 3:

Signatures: When we browsed the Music->sample music-> Chopin'sSymphony_N we found that there is a %PDF tag and the binary of the image is starting with 25 50 44 46 this means that the image is PDF file which is saved using different extension. Also we tried to play it but it gives us error.


AccessData FTK Imager 3.4.3.3

Name	Size	Type	Date Modified
$I30	4	NTFS Index All...	2016-12-21 7:3...
Beethoven's Symphon...	600	Regular File	2008-04-14 11:...
Beethoven's Symphon...	1	File Slack	
Chopin'sSymphony_N...	153	Regular File	2016-11-28 9:4...
Chopin'sSymphony_N...	4	File Slack	
New Stories (Highway ...	743	Regular File	2008-04-14 11:...
New Stories (Highway ...	2	File Slack	

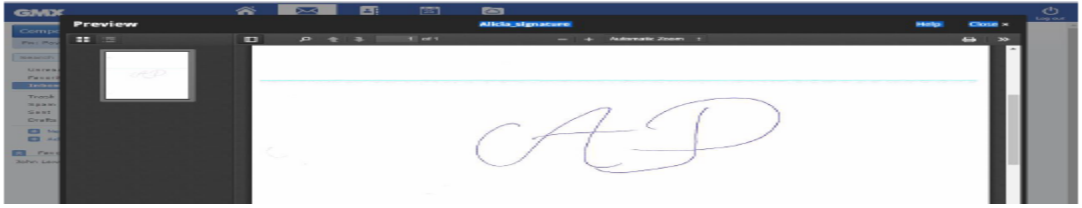
```
00000  25 50 44 46 2D 31 2E 36-0D 25 E2 E3 CF D3 0D 0A  %PDF-1.6·%âãÏÓ··
00010  33 31 20 30 20 6F 62 6A-0D 3C 3C 2F 46 69 6C 74  31 0 obj·<</Filt
00020  65 72 2F 46 6C 61 74 65-44 65 63 6F 64 65 2F 46  er/FlateDecode/F
00030  69 72 73 74 20 35 2F 4C-65 6E 67 74 68 20 35 39  irst 5/Length 59
00040  2F 4E 20 31 2F 54 79 70-65 2F 4F 62 6A 53 74 6D  /N 1/Type/ObjStm
00050  3E 3E 73 74 72 65 61 6D-0D 0A 68 DE 32 34 57 30  >>stream··hÞ24W0
00060  50 B0 B1 D1 0F 28 CA 4F-0E 4E 2D 89 D6 0F 70 71  P°±Ñ·(ÊO·N-·Ö·pq
00070  D3 F7 CC 4D 4C 4F 75 8E-D5 8F F0 4F CA 4A 4D 2E  Ó÷ÌMLOu·Õ·ðOÊJM.
00080  01 4A 7B E6 1A 28 18 03-55 06 D9 01 01 40 80 01  ·J{æ·(··U·Ù··@··
00090  00 8E AB 0E CE 0D 0A 65-6E 64 73 74 72 65 61 6D  ··«·Î··endstream
000a0  0D 65 6E 64 6F 62 6A 0D-33 32 20 30 20 6F 62 6A  ·endobj·32 0 obj
```

Then we exported it to the desktop, then upon saving the file using .pdf we found same signatures which the blackmailer sent her as the proof of having love letter possession. As shown follows in the figures.

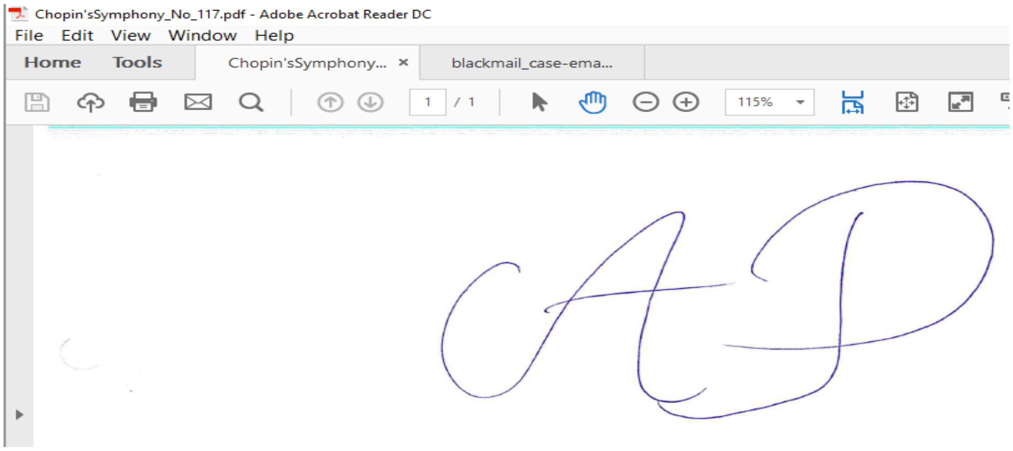
Attached as proof is your favorite signature apposed at the bottom of the letters. Unless you pay $10,000, I'll send the pictures to your husband and at your workplace. Payment must be done in the next 10 days. Instructions for payment will follow. Stay tuned.

Jekyll Hyde.

Attachment (file Alicia_signature.pdf)

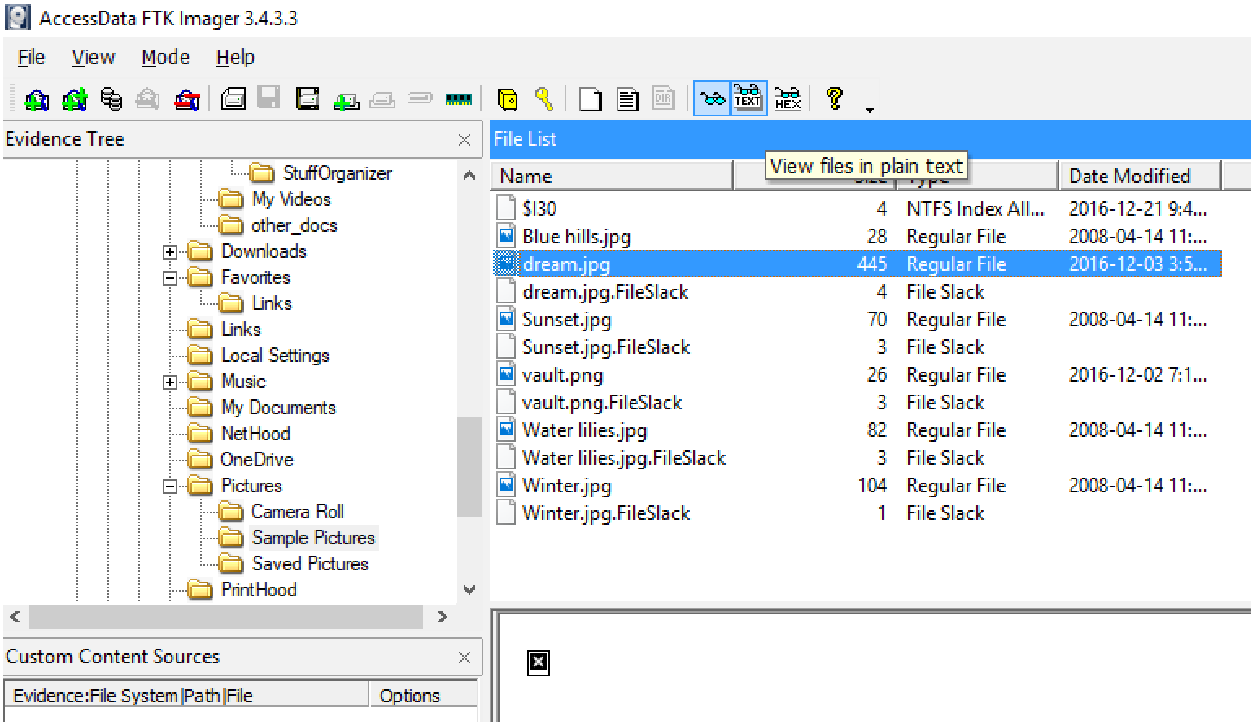


The figure shown below shows the same signatures when we converted the image into .pdf file. This confirms that Mr. John has made these signatures himself to use as integrity for the mails to send to Ms. Alicia.

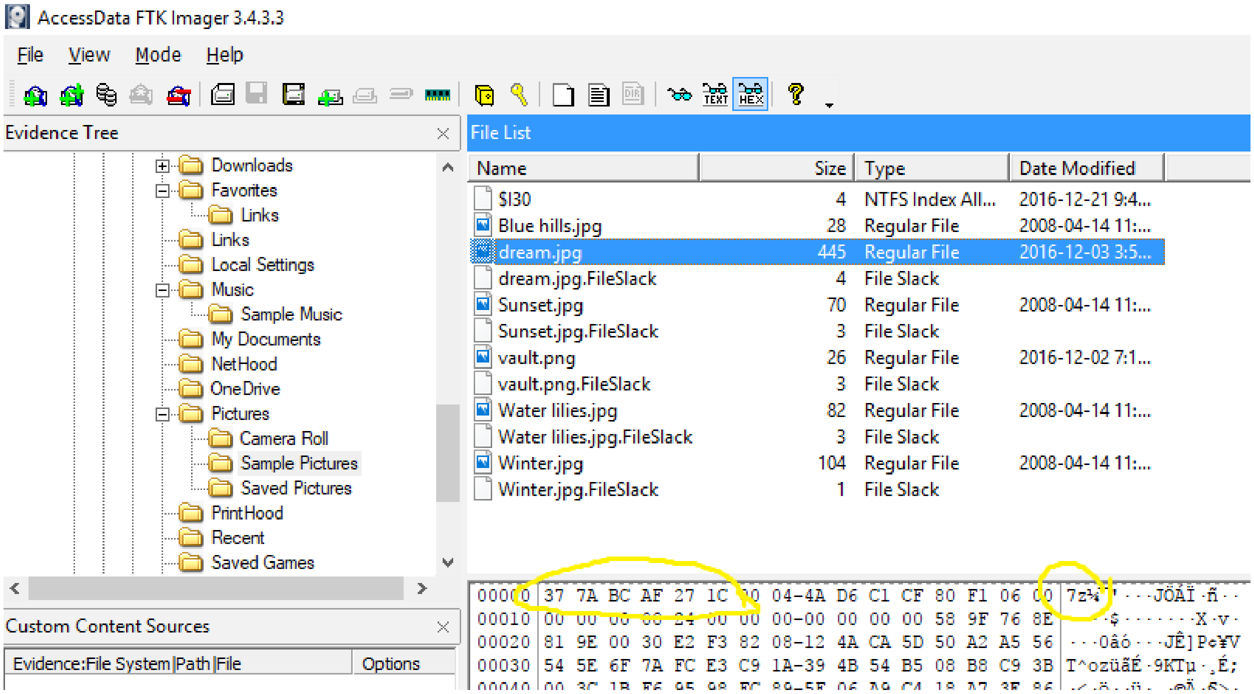


Evidence 4:

Upon browsing **Pictures-> Sample Pictures->dream.jpg** we found that in automatic (IE) mode there was a cross. All other files were opening fine for example Bluehills.jpg, Sunset.jpg. Then upon seeing the hex mode we again found that the extension had been changed to jpg but the image is having 7z signature and magic number 37 7A BC AF 27 1C as shown in the figure so this is confirmed that it is 7z file.



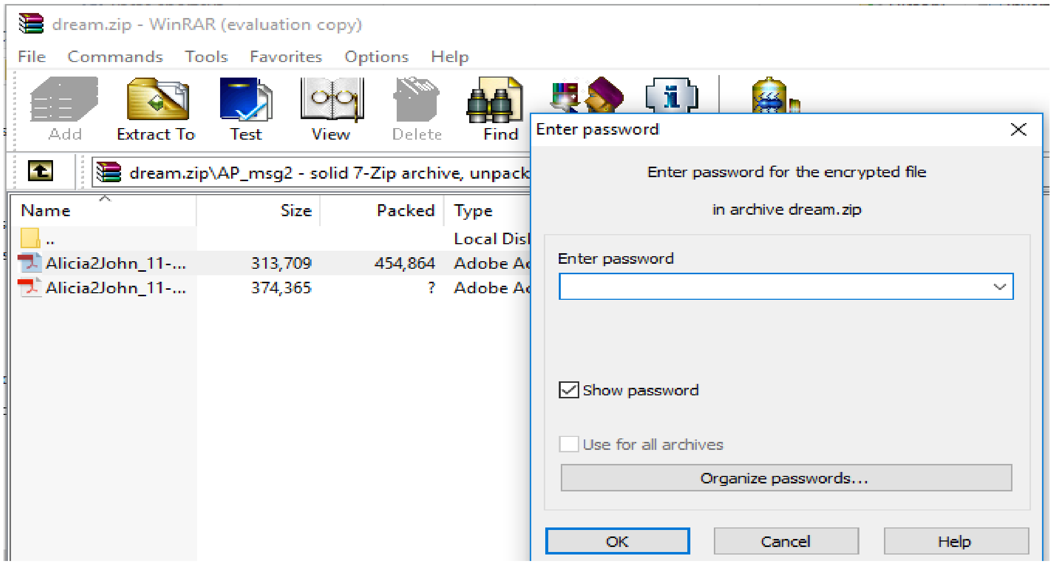
Name	Size	Type	Date Modified
$I30	4	NTFS Index All...	2016-12-21 9:4...
Blue hills.jpg	28	Regular File	2008-04-14 11:...
dream.jpg	445	Regular File	2016-12-03 3:5...
dream.jpg.FileSlack	4	File Slack	
Sunset.jpg	70	Regular File	2008-04-14 11:...
Sunset.jpg.FileSlack	3	File Slack	
vault.png	26	Regular File	2016-12-02 7:1...
vault.png.FileSlack	3	File Slack	
Water lilies.jpg	82	Regular File	2008-04-14 11:...
Water lilies.jpg.FileSlack	3	File Slack	
Winter.jpg	104	Regular File	2008-04-14 11:...
Winter.jpg.FileSlack	1	File Slack	



Name	Size	Type	Date Modified
$I30	4	NTFS Index All...	2016-12-21 9:4...
Blue hills.jpg	28	Regular File	2008-04-14 11:...
dream.jpg	445	Regular File	2016-12-03 3:5...
dream.jpg.FileSlack	4	File Slack	
Sunset.jpg	70	Regular File	2008-04-14 11:...
Sunset.jpg.FileSlack	3	File Slack	
vault.png	26	Regular File	2016-12-02 7:1...
vault.png.FileSlack	3	File Slack	
Water lilies.jpg	82	Regular File	2008-04-14 11:...
Water lilies.jpg.FileSlack	3	File Slack	
Winter.jpg	104	Regular File	2008-04-14 11:...
Winter.jpg.FileSlack	1	File Slack	

```
00000 37 7A BC AF 27 1C 00 04-4A D6 C1 CF 80 F1 06 00 7z¼'' ···JÖÁÏ·ñ··
00010 00 00 00 00 24 00 00 00-00 00 00 00 58 9F 76 8E ····$·······X·v·
00020 81 9E 00 30 E2 F3 82 08-12 4A CA 5D 50 A2 A5 56 ···0âó···JÊ]P¢¥V
00030 54 5E 6F 7A FC E3 C9 1A-39 4B 54 B5 08 B8 C9 3B T^ozüãÉ·9KTµ·¸É;
```

Then we converted the file into 7z. It was having two further files, while trying to open the files we found that there is a password on the files.



dream.zip\AP_msg2 - solid 7-Zip archive, unpack

Name	Size	Packed	Type
..			Local Disl
Alicia2John_11-...	313,709	454,864	Adobe Ac
Alicia2John_11-...	374,365	?	Adobe Ac

Enter password

Enter password for the encrypted file

in archive dream.zip

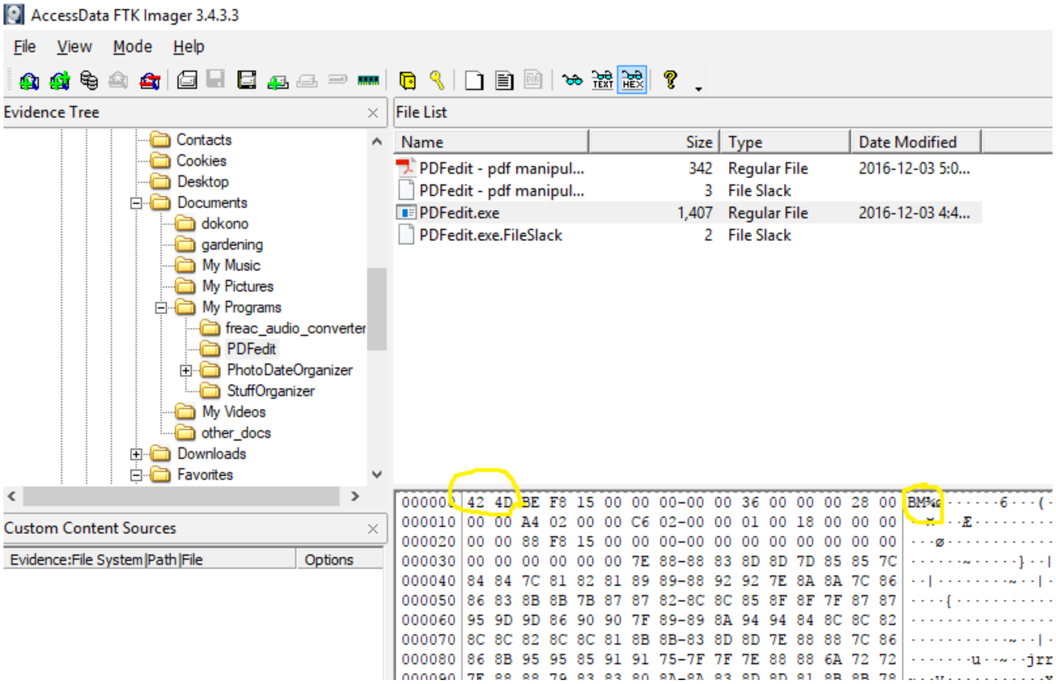
Enter password

☑ Show password

□ Use for all archives

Then we tried to find the password of this file so we browsed

My programs-> PDFedit->PDFedit.exe and we found that the file is BMP file with magic number 42 4D. so then we converted it into .BMP file. Then we become suspicious about the file.



Name	Size	Type	Date Modified
PDFedit - pdf manipul...	342	Regular File	2016-12-03 5:0...
PDFedit - pdf manipul...	3	File Slack	
PDFedit.exe	1,407	Regular File	2016-12-03 4:4...
PDFedit.exe.FileSlack	2	File Slack	

```
000000 42 4D BE F8 15 00 00 00-00 00 36 00 00 00 28 00  BM¾ø······6···(·
000010 00 00 A4 02 00 00 C6 02-00 00 01 00 18 00 00 00  ··¤···Æ·········
000020 00 00 88 F8 15 00 00 00-00 00 00 00 00 00 00 00  ···ø············
000030 00 00 00 00 00 00 7E 88-88 83 8D 8D 7D 85 85 7C  ······~·····}··|
000040 84 84 7C 81 82 81 89 89-88 92 92 7E 8A 8A 7C 86  ··|········~··|·
000050 86 83 8B 8B 7B 87 87 82-8C 8C 85 8F 8F 7F 87 87  ····{···········
000060 95 9D 9D 86 90 90 7F 89-89 8A 94 94 84 8C 8C 82  ················
000070 8C 8C 82 8C 8C 81 8B 8B-83 8D 8D 7E 88 88 7C 86  ···········~··|·
000080 86 8B 95 95 85 91 91 75-7F 7F 7E 88 88 6A 72 72  ·······u··~··jrr
000090 7F 88 88 79 83 83 80 8A-8A 83 8D 8D 81 8B 8B 78
```

As why would someone changed the extension of a bmp file to .exe so, then we opened the file

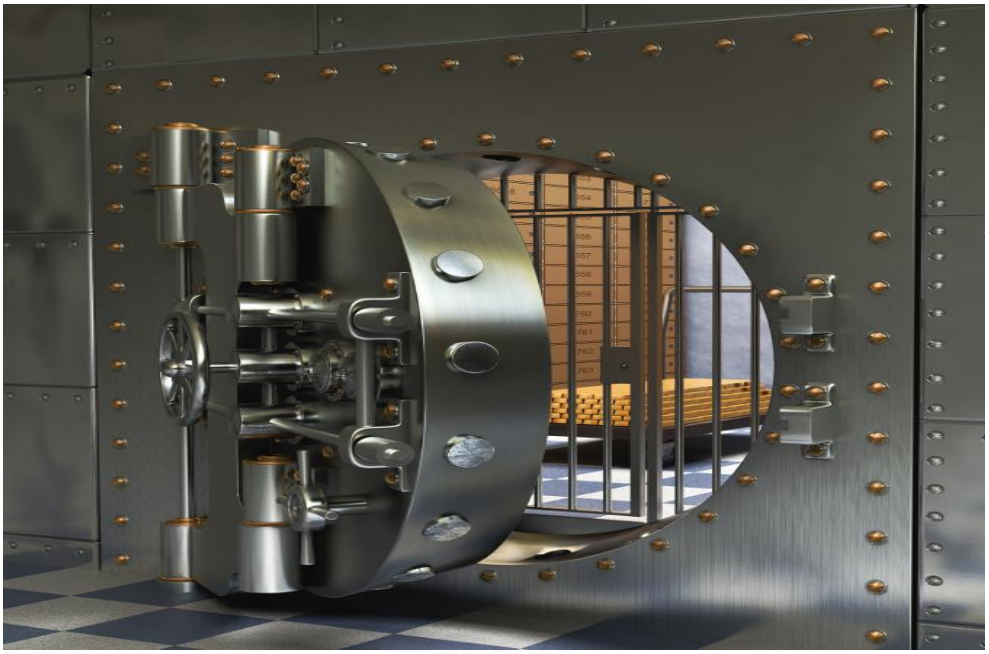
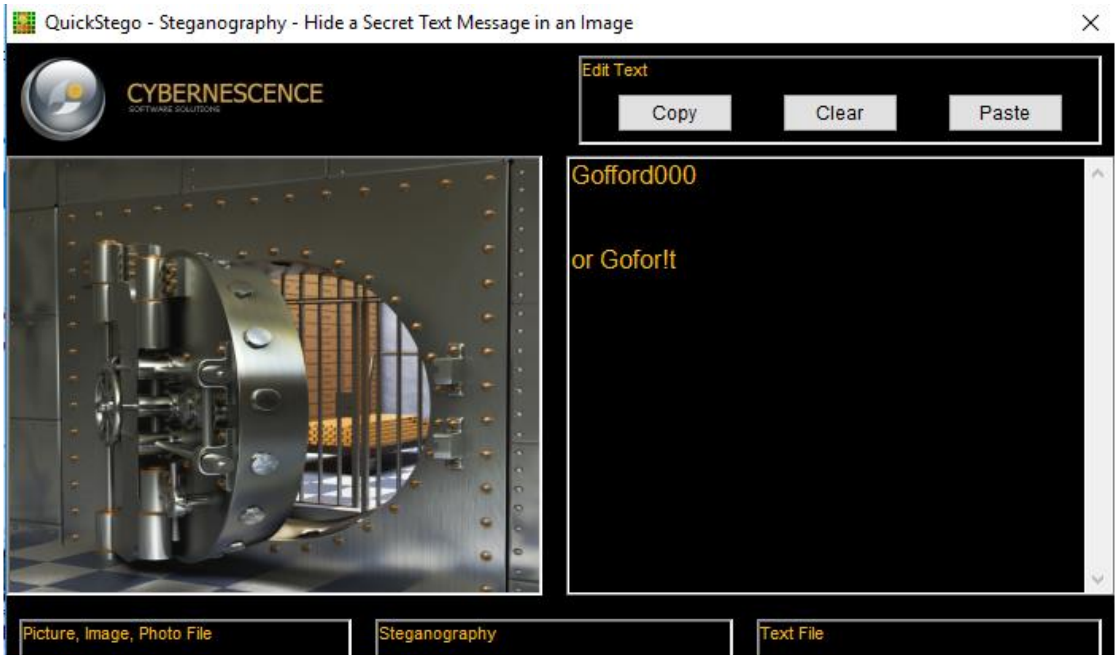


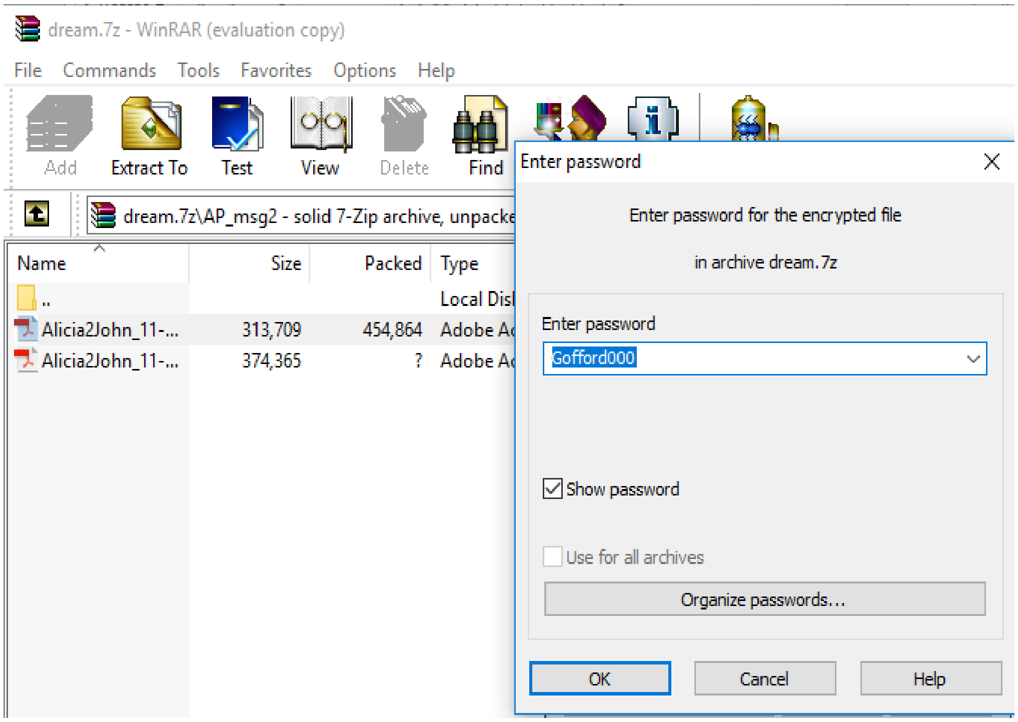
Image does not have anything but since to find the reason of changing the file extension, we tried using QuickStego and we found that there are again two passwords hidden in the image. So we tried the passwords.


QuickStego - Steganography - Hide a Secret Text Message in an Image
CYBERNESCENCE
SOFTWARE SOLUTIONS
Edit Text
Copy
Clear
Paste
Picture, Image, Photo File
Steganography
Text File

Gofford000

or Gofor!t

When we tried the password Gofford000 we are able to retrieve the letters the blackmailer was talking about in the email.


dream.7z - WinRAR (evaluation copy)
File Commands Tools Favorites Options Help
Add
Extract To
Test
View
Delete
Find

dream.7z\AP_msg2 - solid 7-Zip archive, unpacke

Name	Size	Packed	Type
..			Local Disl
Alicia2John_11-...	313,709	454,864	Adobe Ac
Alicia2John_11-...	374,365	?	Adobe Ac

Enter password

Enter password for the encrypted file

in archive dream.7z

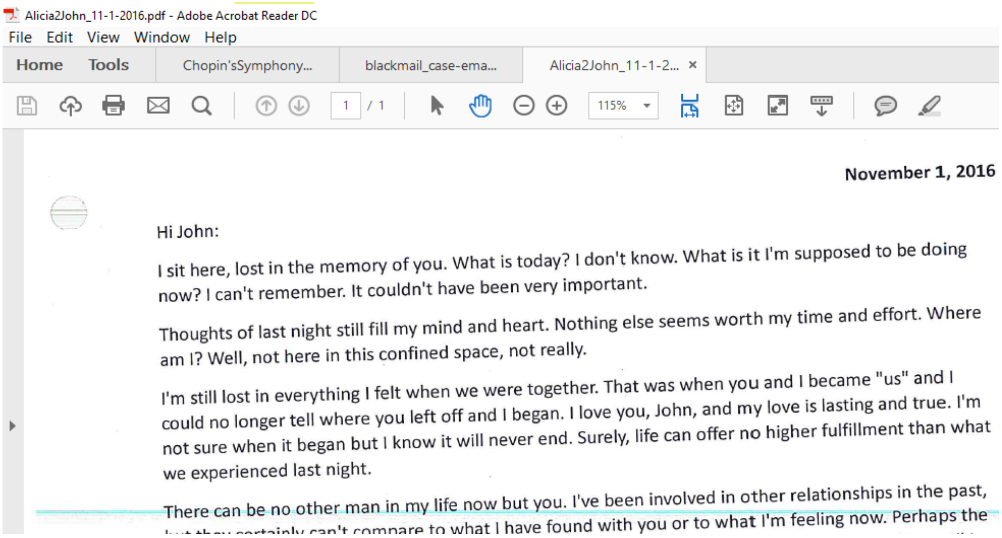
Enter password

Gofford000

☑ Show password

☐ Use for all archives

Organize passwords...
OK
Cancel
Help



November 1, 2016

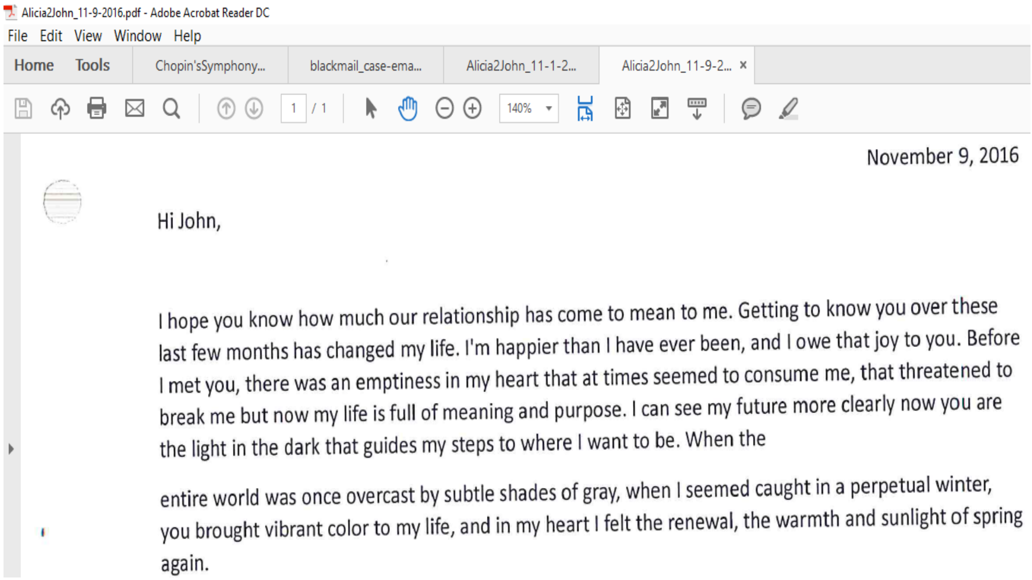
Hi John:

I sit here, lost in the memory of you. What is today? I don't know. What is it I'm supposed to be doing now? I can't remember. It couldn't have been very important.

Thoughts of last night still fill my mind and heart. Nothing else seems worth my time and effort. Where am I? Well, not here in this confined space, not really.

I'm still lost in everything I felt when we were together. That was when you and I became "us" and I could no longer tell where you left off and I began. I love you, John, and my love is lasting and true. I'm not sure when it began but I know it will never end. Surely, life can offer no higher fulfillment than what we experienced last night.

There can be no other man in my life now but you. I've been involved in other relationships in the past, but they certainly can't compare to what I have found with you or to what I'm feeling now. Perhaps the



November 9, 2016

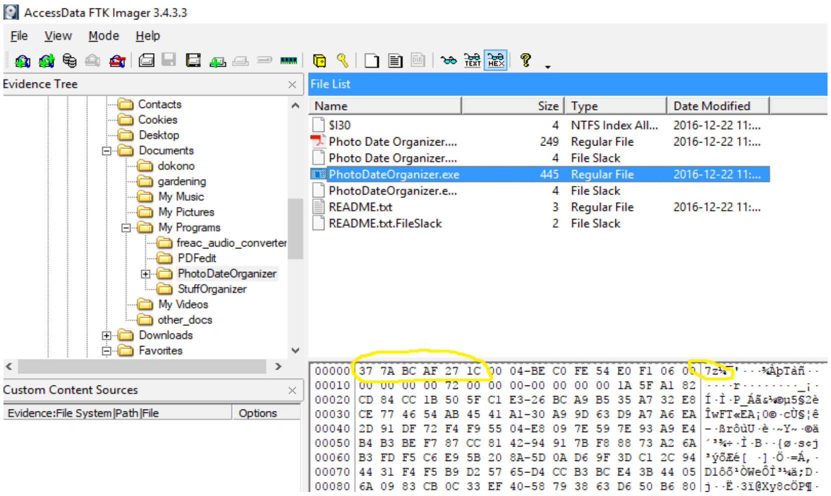
Hi John,

I hope you know how much our relationship has come to mean to me. Getting to know you over these last few months has changed my life. I'm happier than I have ever been, and I owe that joy to you. Before I met you, there was an emptiness in my heart that at times seemed to consume me, that threatened to break me but now my life is full of meaning and purpose. I can see my future more clearly now you are the light in the dark that guides my steps to where I want to be. When the

entire world was once overcast by subtle shades of gray, when I seemed caught in a perpetual winter, you brought vibrant color to my life, and in my heart I felt the renewal, the warmth and sunlight of spring again.

Evidence 5:

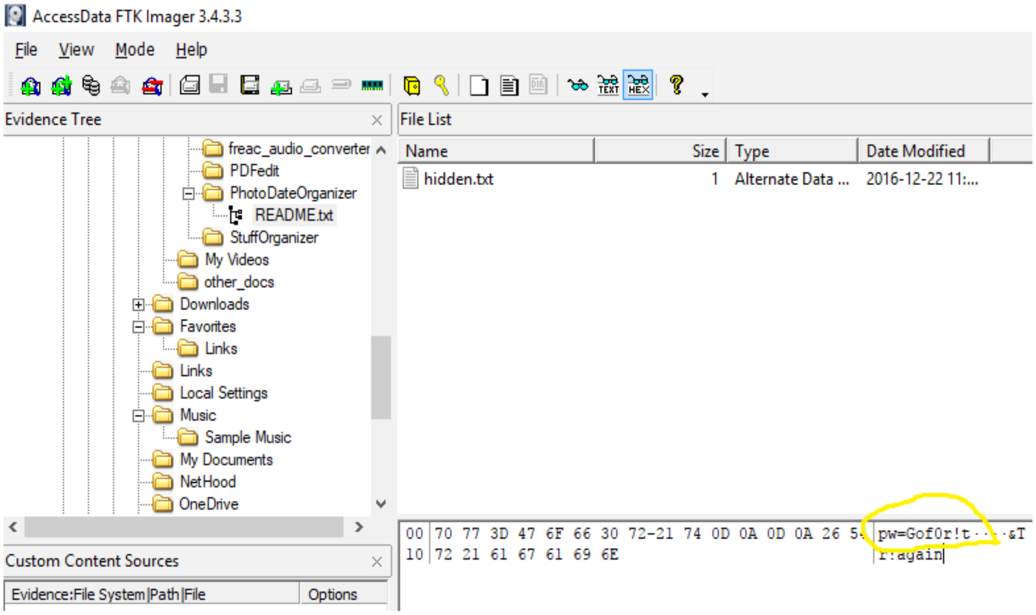
When we browsed the folder My Programs->PhotoDateOrganizer then again we found that there is a file named PhotoDateOrganizer.exe. Upon opening this file in hex mode we found that it is also a 7z file and have magic number 37 7A BC AF 27 1C. So we exported the file then when we tried opening it, again a password is there. Then we tried the second password we found in the PDFedit.bmp but it was not working. So we tried to find password in some other file.



Name	Size	Type	Date Modified
$I30	4	NTFS Index All...	2016-12-22 11:...
Photo Date Organizer....	249	Regular File	2016-12-22 11:...
Photo Date Organizer....	4	File Slack	
PhotoDateOrganizer.exe	445	Regular File	2016-12-22 11:...
PhotoDateOrganizer.e...	4	File Slack	
README.txt	3	Regular File	2016-12-22 11:...
README.txt.FileSlack	2	File Slack	

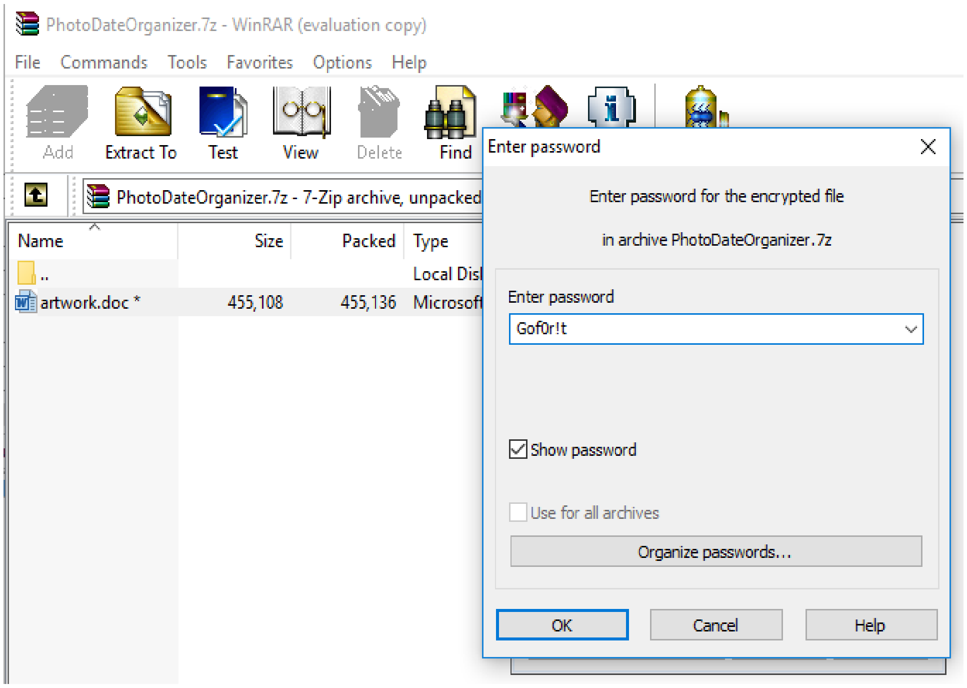
```
00000 37 7A BC AF 27 1C 00 04-BE C0 FE 54 E0 F1 06 00 7z¼¯'···¾ÀþTàñ··
00010 00 00 00 00 72 00 00 00-00 00 00 00 1A 5F A1 82 ····r·······_¡·
00020 CD 84 CC 1B 50 5F C1 E3-26 BC A9 B5 35 A7 32 E8 Í·Ì·P_Áã&¼©µ5§2è
00030 CE 77 46 54 AB 45 41 A1-30 A9 9D 63 D9 A7 A6 EA ÎwFT«EA¡0©·cÙ§¦ê
00040 2D 91 DF 72 F4 F9 55 04-E8 09 7E 59 7E 93 A9 E4 -·ßrôùU·è·~Y~·©ä
00050 B4 B3 BE F7 87 CC 81 42-94 91 7B F8 88 73 A2 6A ´³¾÷·Ì·B··{ø·s¢j
00060 B3 FD F5 C6 E9 5B 20 8A-5D 0A D6 9F 3D C1 2C 94 ³ýõÆé[ ·]·Ö·=Á,·
00070 44 31 F4 F5 B9 D2 57 65-D4 CC B3 BC E4 3B 44 05 D1ôõ¹ÒWeÔÌ³¼ä;D·
00080 6A 09 83 CB 0C 33 EF 40-58 79 38 63 D6 50 B6 80 j··Ë·3ï@Xy8cÖP¶·
```

When we tried opening PhotoDateOrganizer.7z there was a password and we found its password in the same loaction PhotodateOrganizer->README.txt->hidden.txt. When we tried the password it was working.



Name	Size	Type	Date Modified
hidden.txt	1	Alternate Data ...	2016-12-22 11:...

```
00 70 77 3D 47 6F 66 30 72-21 74 0D 0A 0D 0A 26 54 pw=Gof0r!t····&T
10 72 21 61 67 61 69 6E                            r!again
```


PhotoDateOrganizer.7z - WinRAR (evaluation copy)
File Commands Tools Favorites Options Help
Add Extract To Test View Delete Find
PhotoDateOrganizer.7z - 7-Zip archive, unpacked
Name Size Packed Type
Local Disk
Enter password
OK Cancel Help
Organize passwords...

Name	Size	Packed	Type
..			Local Disl
artwork.doc *	455,108	455,136	Microsoft

Enter password for the encrypted file

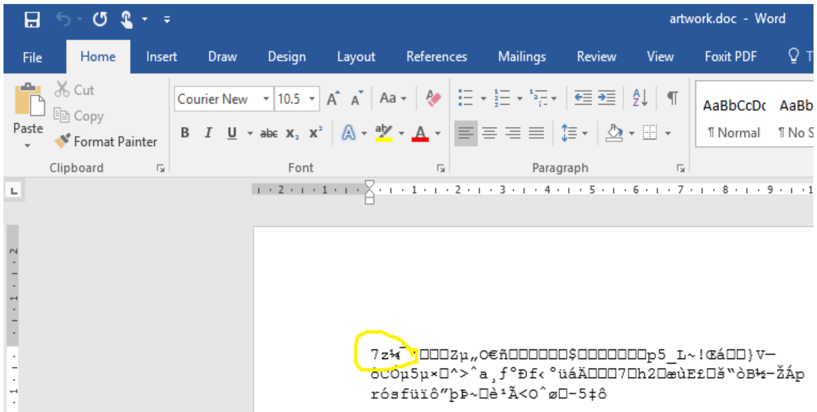
in archive PhotoDateOrganizer.7z

Enter password: Gof0r!t

☑ Show password

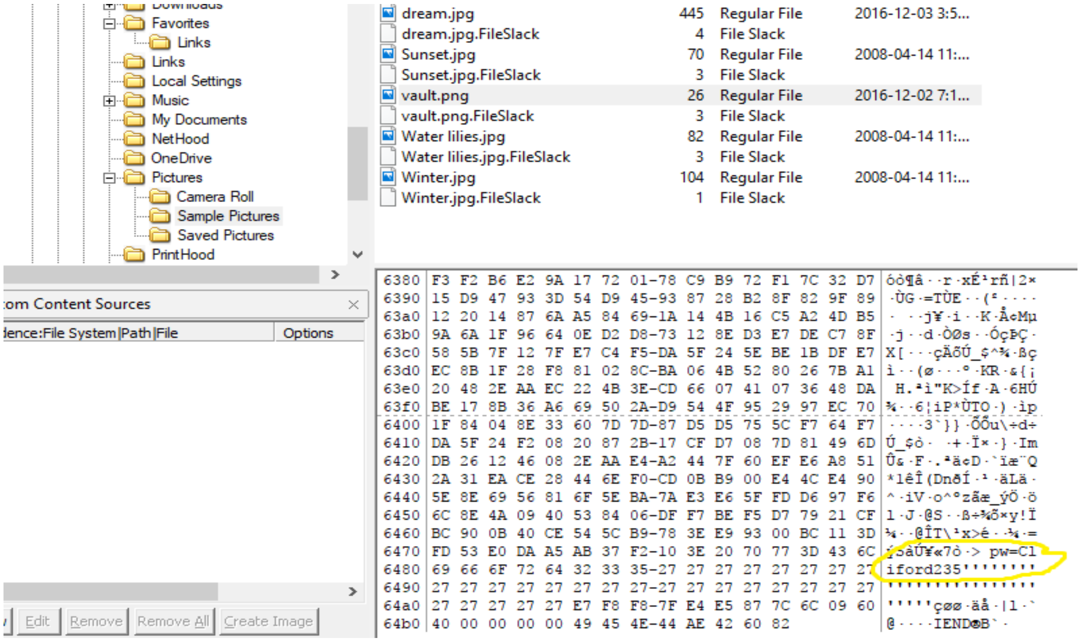
□ Use for all archives

Upon opening the file, it was again zip file, and we came to know it when we tried opening artwork.doc. again it was starting from 7z as shown follows. Then we converted it again into artwork.7z


artwork.doc - Word
File Home Insert Draw Design Layout References Mailings Review View Foxit PDF
Paste Cut Copy Format Painter
Courier New 10.5
AaBbCcDc AaBb
¶ Normal ¶ No S
Clipboard Font Paragraph

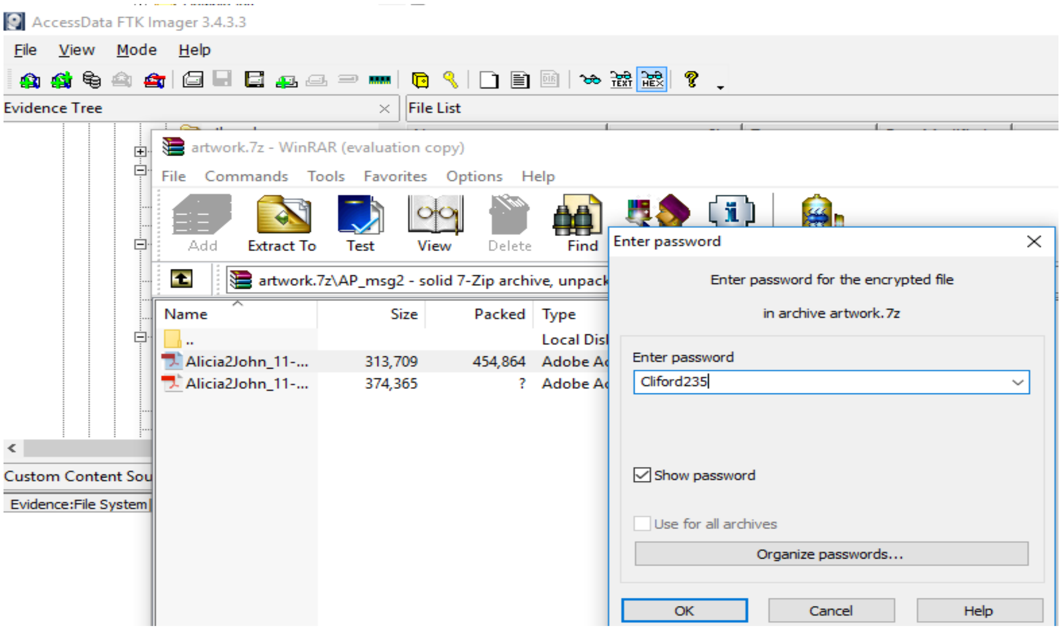
```
7z¼¯'□□□Zµ„O€ñ□□□□□□□$□□□□□□□□p5_L~!Œá□□}V—
ōCOµ5µ×□^>ˆa¸ƒ°Ðf‹°üáÄ□□□7□h2□æùE£□š"òB½–ŽÁp
rósfüïô”þÞ~□è¹Ã<Oˆø□–5‡ô
```

Then we found one more picture vault.png and upon browsing the end of the hex file there was written pw=Cliford235 then we tried this password to open PhotoDateOrganizer.7z and it was opened.



dream.jpg	445	Regular File	2016-12-03 3:5...
dream.jpg.FileSlack	4	File Slack	
Sunset.jpg	70	Regular File	2008-04-14 11:...
Sunset.jpg.FileSlack	3	File Slack	
vault.png	26	Regular File	2016-12-02 7:1...
vault.png.FileSlack	3	File Slack	
Water lilies.jpg	82	Regular File	2008-04-14 11:...
Water lilies.jpg.FileSlack	3	File Slack	
Winter.jpg	104	Regular File	2008-04-14 11:...
Winter.jpg.FileSlack	1	File Slack	

```
6380 F3 F2 B6 E2 9A 17 72 01-78 C9 B9 72 F1 7C 32 D7  óò¶â··r·xÉ¹rñ|2×
6390 15 D9 47 93 3D 54 D9 45-93 87 28 B2 8F 82 9F 89  ·ÙG·=TÙE··(²····
63a0 12 20 14 87 6A A5 84 69-1A 14 4B 16 C5 A2 4D B5  · ··j¥·i··K·Å¢Mµ
63b0 9A 6A 1F 96 64 0E D2 D8-73 12 8E D3 E7 DE C7 8F  ·j··d·ÒØs··ÓçÞÇ·
63c0 58 5B 7F 12 7F E7 C4 F5-DA 5F 24 5E BE 1B DF E7  X[···çÄõÚ_$^¾·ßç
63d0 EC 8B 1F 28 F8 81 02 8C-BA 06 4B 52 80 26 7B A1  ì··(ø···º·KR·&{¡
63e0 20 48 2E AA EC 22 4B 3E-CD 66 07 41 07 36 48 DA   H.ªì"K>Íf·A·6HÚ
63f0 BE 17 8B 36 A6 69 50 2A-D9 54 4F 95 29 97 EC 70  ¾··6¦iP*ÙTO·)·ìp
6400 1F 84 04 8E 33 60 7D 7D-87 D5 D5 75 5C F7 64 F7  ····3`}}·ÕÕu\÷d÷
6410 DA 5F 24 F2 08 20 87 2B-17 CF D7 08 7D 81 49 6D  Ú_$ò· ·+·Ï×·}·Im
6420 DB 26 12 46 08 2E AA E4-A2 44 7F 60 EF E6 A8 51  Û&·F·.ªä¢D·`ïæ¨Q
6430 2A 31 EA CE 28 44 6E F0-CD 0B B9 00 E4 4C E4 90  *1êÎ(DnðÍ·¹·äLä·
6440 5E 8E 69 56 81 6F 5E BA-7A E3 E6 5F FD D6 97 F6  ^·iV·o^ºzãæ_ýÖ·ö
6450 6C 8E 4A 09 40 53 84 06-DF F7 BE F5 D7 79 21 CF  l·J·@S··ß÷¾õ×y!Ï
6460 BC 90 0B 40 CE 54 5C B9-78 3E E9 93 00 BC 11 3D  ¼··@ÎT\¹x>é··¼·=
6470 FD 53 E0 DA A5 AB 37 F2-10 3E 20 70 77 3D 43 6C  ýSàÚ¥«7ò·> pw=Cl
6480 69 66 6F 72 64 32 33 35-27 27 27 27 27 27 27 27  iford235''''''''
6490 27 27 27 27 27 27 27 27-27 27 27 27 27 27 27 27  ''''''''''''''''
64a0 27 27 27 27 27 E7 F8 F8-7F E4 E5 87 7C 6C 09 60  '''''çøø·äå·|l·`
64b0 40 00 00 00 00 49 45 4E-44 AE 42 60 82           @····IEND®B`·
```



artwork.7z\AP_msg2 - solid 7-Zip archive, unpack

Name	Size	Packed	Type
..			Local Disk
Alicia2John_11-...	313,709	454,864	Adobe Ac
Alicia2John_11-...	374,365	?	Adobe Ac

Enter password

Enter password for the encrypted file

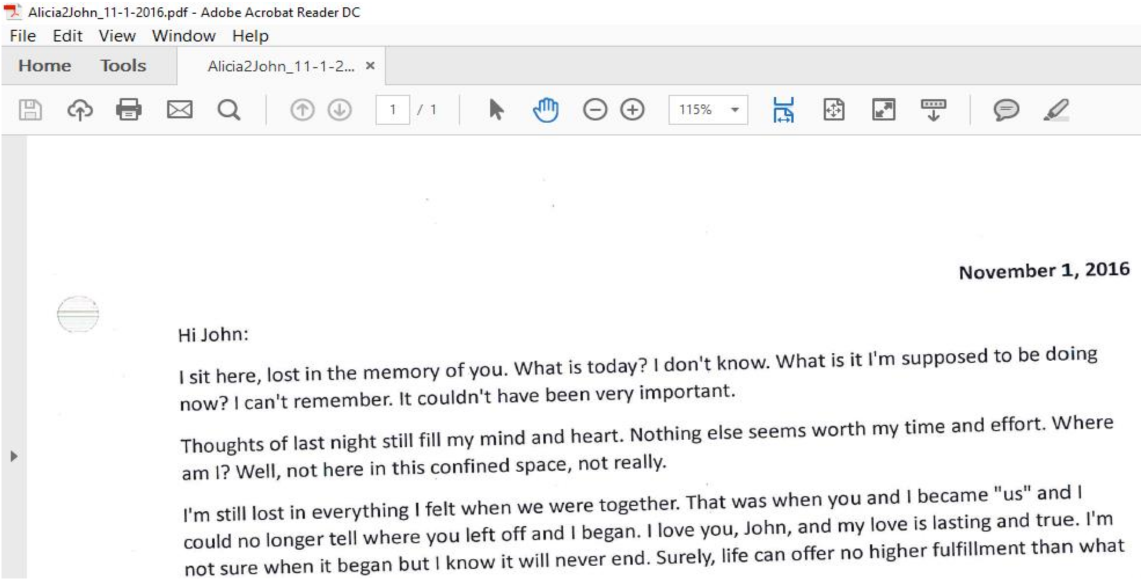
in archive artwork.7z

Enter password: Cliford235

☑ Show password

□ Use for all archives

Then we found two more love letters



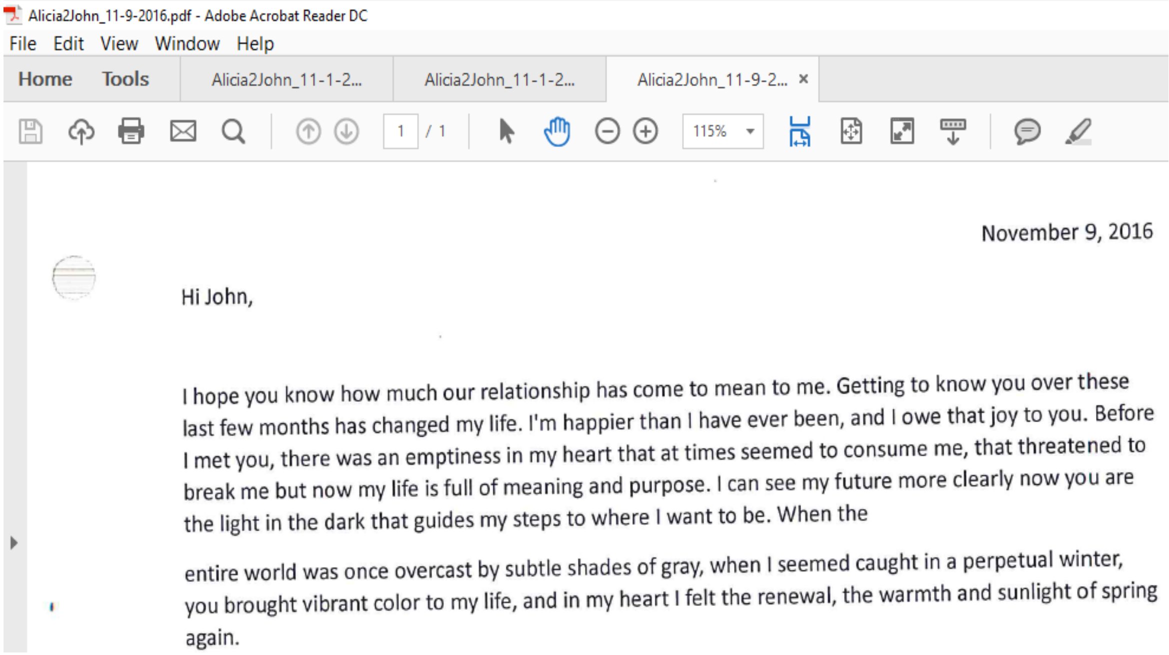
November 1, 2016

Hi John:

I sit here, lost in the memory of you. What is today? I don't know. What is it I'm supposed to be doing now? I can't remember. It couldn't have been very important.

Thoughts of last night still fill my mind and heart. Nothing else seems worth my time and effort. Where am I? Well, not here in this confined space, not really.

I'm still lost in everything I felt when we were together. That was when you and I became "us" and I could no longer tell where you left off and I began. I love you, John, and my love is lasting and true. I'm not sure when it began but I know it will never end. Surely, life can offer no higher fulfillment than what



November 9, 2016

Hi John,

I hope you know how much our relationship has come to mean to me. Getting to know you over these last few months has changed my life. I'm happier than I have ever been, and I owe that joy to you. Before I met you, there was an emptiness in my heart that at times seemed to consume me, that threatened to break me but now my life is full of meaning and purpose. I can see my future more clearly now you are the light in the dark that guides my steps to where I want to be. When the

entire world was once overcast by subtle shades of gray, when I seemed caught in a perpetual winter, you brought vibrant color to my life, and in my heart I felt the renewal, the warmth and sunlight of spring again.

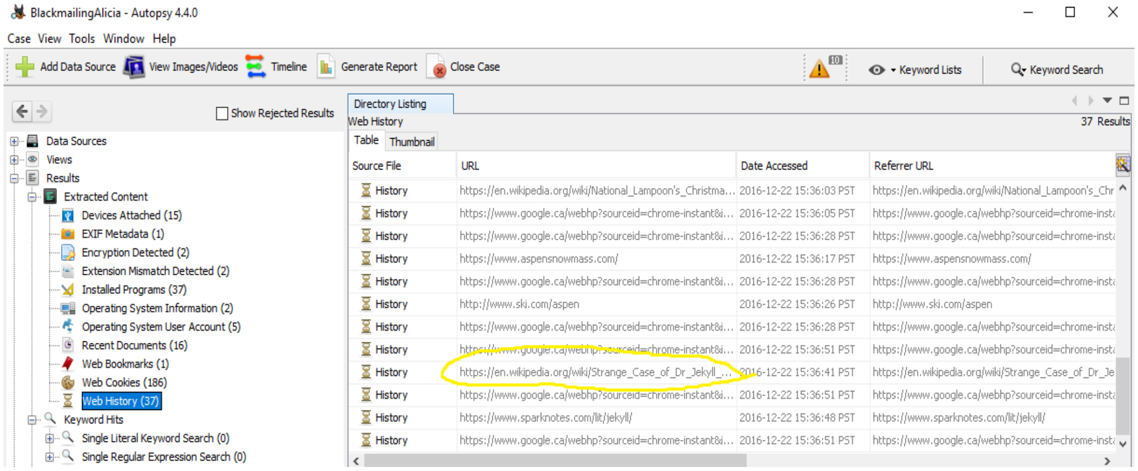
So we found that there are two locations where Mr. John. Has kept the letters which Ms. Alicia sent to Mr. John.

Evidence 6:

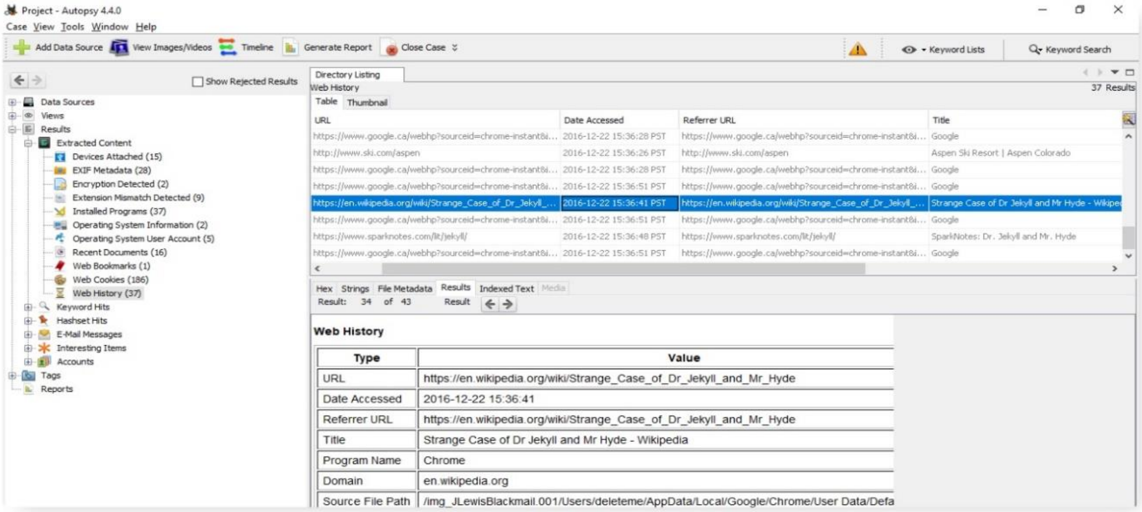
When we uploaded the investigation file in Autopsy, and we looked into cookies:

Results-> Web History

Then we found that Mr. John had visited a page from Wikipedia to read the strange case of Dr Jekyll. This gives a strong evidence that Mr. John is the original blackmailer who was blackmailing Ms. Alicia, and might be using his name.



Source File	URL	Date Accessed	Referrer URL
History	https://en.wikipedia.org/wiki/National_Lampoon's_Christma...	2016-12-22 15:36:03 PST	https://en.wikipedia.org/wiki/National_Lampoon's_Chr
History	https://www.google.ca/webhp?sourceid=chrome-instant&i...	2016-12-22 15:36:05 PST	https://www.google.ca/webhp?sourceid=chrome-insta
History	https://www.google.ca/webhp?sourceid=chrome-instant&i...	2016-12-22 15:36:28 PST	https://www.google.ca/webhp?sourceid=chrome-insta
History	https://www.aspensnowmass.com/	2016-12-22 15:36:17 PST	https://www.aspensnowmass.com/
History	https://www.google.ca/webhp?sourceid=chrome-instant&i...	2016-12-22 15:36:28 PST	https://www.google.ca/webhp?sourceid=chrome-insta
History	http://www.ski.com/aspen	2016-12-22 15:36:26 PST	http://www.ski.com/aspen
History	https://www.google.ca/webhp?sourceid=chrome-instant&i...	2016-12-22 15:36:28 PST	https://www.google.ca/webhp?sourceid=chrome-insta
History	https://www.google.ca/webhp?sourceid=chrome-instant&i...	2016-12-22 15:36:51 PST	https://www.google.ca/webhp?sourceid=chrome-insta
History	https://en.wikipedia.org/wiki/Strange_Case_of_Dr_Jekyll_...	2016-12-22 15:36:41 PST	https://en.wikipedia.org/wiki/Strange_Case_of_Dr_Je
History	https://www.google.ca/webhp?sourceid=chrome-instant&i...	2016-12-22 15:36:51 PST	https://www.google.ca/webhp?sourceid=chrome-insta
History	https://www.sparknotes.com/lit/jekyll/	2016-12-22 15:36:48 PST	https://www.sparknotes.com/lit/jekyll/
History	https://www.google.ca/webhp?sourceid=chrome-instant&i...	2016-12-22 15:36:51 PST	https://www.google.ca/webhp?sourceid=chrome-insta



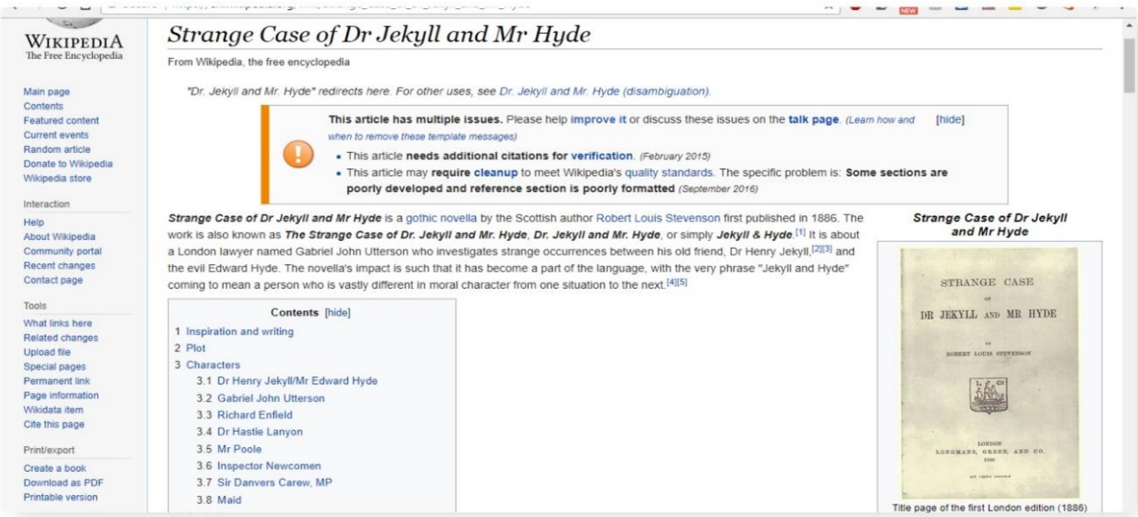
Web History 37 Results

URL	Date Accessed	Referrer URL	Title
https://www.google.ca/webhp?sourceid=chrome-instant&i...	2016-12-22 15:36:28 PST	https://www.google.ca/webhp?sourceid=chrome-instant&i...	Google
http://www.ski.com/aspen	2016-12-22 15:36:26 PST	http://www.ski.com/aspen	Aspen Ski Resort | Aspen Colorado
https://www.google.ca/webhp?sourceid=chrome-instant&i...	2016-12-22 15:36:28 PST	https://www.google.ca/webhp?sourceid=chrome-instant&i...	Google
https://www.google.ca/webhp?sourceid=chrome-instant&i...	2016-12-22 15:36:51 PST	https://www.google.ca/webhp?sourceid=chrome-instant&i...	Google
https://en.wikipedia.org/wiki/Strange_Case_of_Dr_Jekyll_...	2016-12-22 15:36:41 PST	https://en.wikipedia.org/wiki/Strange_Case_of_Dr_Jekyll_...	Strange Case of Dr Jekyll and Mr Hyde - Wikiped
https://www.google.ca/webhp?sourceid=chrome-instant&i...	2016-12-22 15:36:51 PST	https://www.google.ca/webhp?sourceid=chrome-instant&i...	Google
https://www.sparknotes.com/lit/jekyll/	2016-12-22 15:36:48 PST	https://www.sparknotes.com/lit/jekyll/	SparkNotes: Dr. Jekyll and Mr. Hyde
https://www.google.ca/webhp?sourceid=chrome-instant&i...	2016-12-22 15:36:51 PST	https://www.google.ca/webhp?sourceid=chrome-instant&i...	Google

Result: 34 of 43 Result

Web History

Type	Value
URL	https://en.wikipedia.org/wiki/Strange_Case_of_Dr_Jekyll_and_Mr_Hyde
Date Accessed	2016-12-22 15:36:41
Referrer URL	https://en.wikipedia.org/wiki/Strange_Case_of_Dr_Jekyll_and_Mr_Hyde
Title	Strange Case of Dr Jekyll and Mr Hyde - Wikipedia
Program Name	Chrome
Domain	en.wikipedia.org
Source File Path	/img_JLewisBlackmail.001/Users/deleteme/AppData/Local/Google/Chrome/User Data/Defa



Strange Case of Dr Jekyll and Mr Hyde

From Wikipedia, the free encyclopedia

"Dr. Jekyll and Mr. Hyde" redirects here. For other uses, see Dr. Jekyll and Mr. Hyde (disambiguation).

This article has multiple issues. Please help **improve it** or discuss these issues on the **talk page**. *(Learn how and when to remove these template messages)* [hide]

- This article **needs additional citations for verification**. *(February 2015)*
- This article may **require cleanup** to meet Wikipedia's quality standards. The specific problem is: **Some sections are poorly developed and reference section is poorly formatted** *(September 2016)*

Strange Case of Dr Jekyll and Mr Hyde is a gothic novella by the Scottish author Robert Louis Stevenson first published in 1886. The work is also known as ***The Strange Case of Dr. Jekyll and Mr. Hyde***, ***Dr. Jekyll and Mr. Hyde***, or simply ***Jekyll & Hyde***.[1] It is about a London lawyer named Gabriel John Utterson who investigates strange occurrences between his old friend, Dr Henry Jekyll,[2][3] and the evil Edward Hyde. The novella's impact is such that it has become a part of the language, with the very phrase "Jekyll and Hyde" coming to mean a person who is vastly different in moral character from one situation to the next.[4][5]

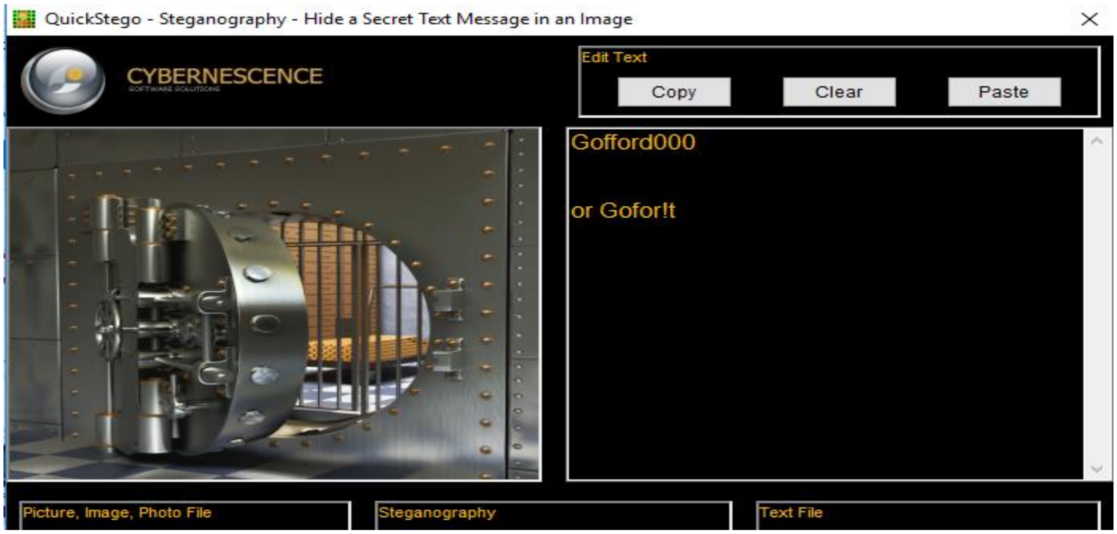
Contents [hide]

Strange Case of Dr Jekyll and Mr Hyde

Title page of the first London edition (1886)

From all the 6 evidences we found, confirm that Mr. John was lying that he deleted all the data related to the relationship of Ms. Alicia and Mr. John.

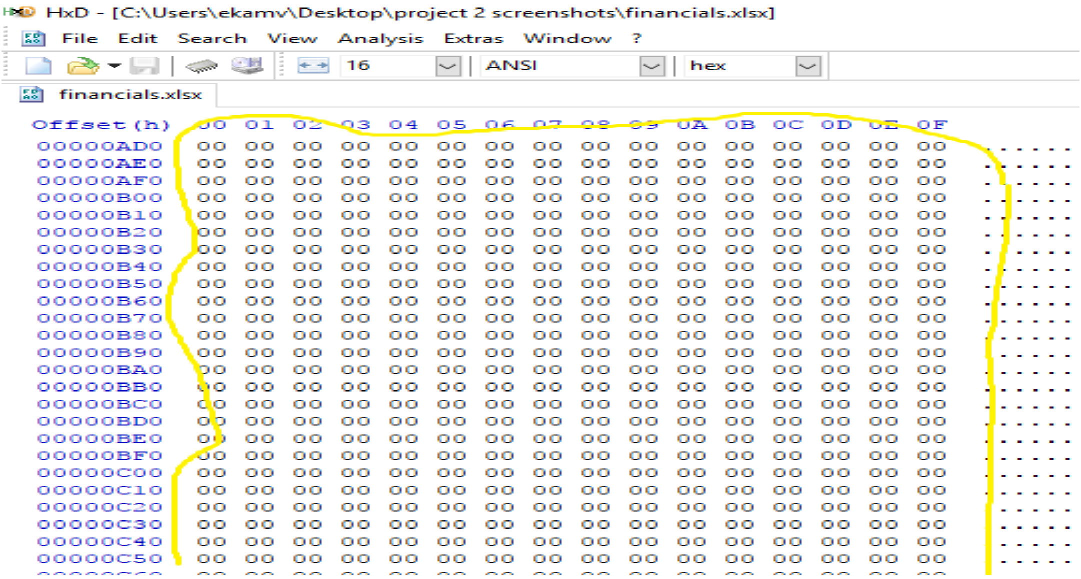
3. For each file, what processes were taken by the suspect to mask them from others? All masking processes used for relevant information must be identified, even redundant ones. [5%]
Answer:
Following are the masking processes used by the suspect:
    1. Steganography: Suspect used this technique to hide the passwords which were required to open the 2 love letters. The tool used is Quickstego.


QuickStego - Steganography - Hide a Secret Text Message in an Image
CYBERNESCENCE
SOFTWARE SOLUTIONS
Edit Text
Copy
Clear
Paste
Picture, Image, Photo File
Steganography
Text File

Gofford000

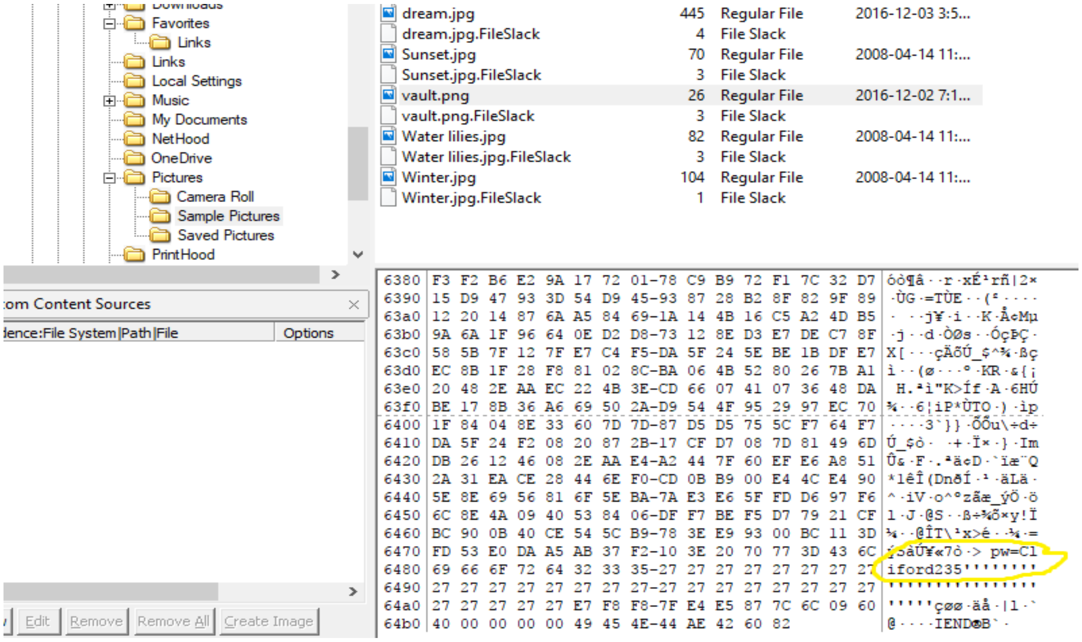
or Gofor!t

2. Hex editor: He has used this tool to corrupt the files, changed the extensions while saving the pictures, hide the passwords as shown follows.


HxD - [C:\Users\ekamv\Desktop\project 2 screenshots\financials.xlsx]
File
Edit
Search
View
Analysis
Extras
Window
?
16
ANSI
hex
financials.xlsx

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000AD0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000AE0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000AF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000B00  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000B10  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000B20  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000B30  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000B40  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000B50  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000B60  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000B70  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000B80  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000B90  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000BA0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000BB0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000BC0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000BD0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000BE0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000BF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000C00  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000C10  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000C20  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000C30  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000C40  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
00000C50  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ......
```

In this screen shot it is shown that extra zeros are added to make sure that the image cannot be retrieved.



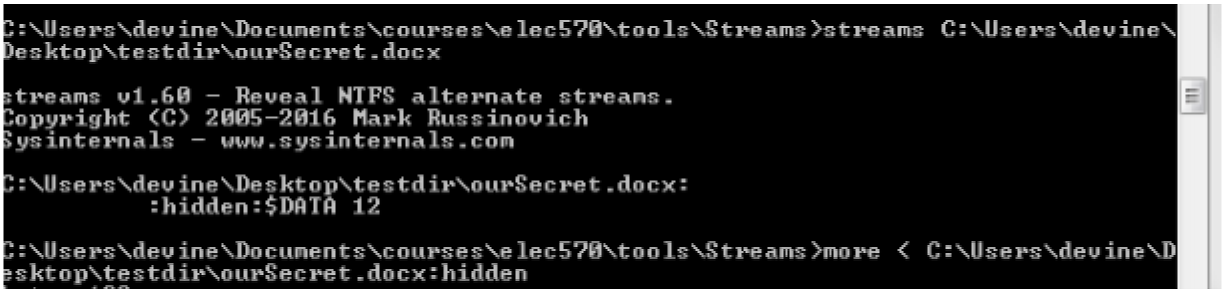
dream.jpg	445	Regular File	2016-12-03 3:5...
dream.jpg.FileSlack	4	File Slack	
Sunset.jpg	70	Regular File	2008-04-14 11:...
Sunset.jpg.FileSlack	3	File Slack	
vault.png	26	Regular File	2016-12-02 7:1...
vault.png.FileSlack	3	File Slack	
Water lilies.jpg	82	Regular File	2008-04-14 11:...
Water lilies.jpg.FileSlack	3	File Slack	
Winter.jpg	104	Regular File	2008-04-14 11:...
Winter.jpg.FileSlack	1	File Slack	

```
6380 F3 F2 B6 E2 9A 17 72 01-78 C9 B9 72 F1 7C 32 D7 óò¶â··r·xÉ¹rñ|2×
6390 15 D9 47 93 3D 54 D9 45-93 87 28 B2 8F 82 9F 89 ·ÙG·=TÙE··(²····
63a0 12 20 14 87 6A A5 84 69-1A 14 4B 16 C5 A2 4D B5 · ··j¥·i··K·Å¢Mµ
63b0 9A 6A 1F 96 64 0E D2 D8-73 12 8E D3 E7 DE C7 8F ·j··d·ÒØs··ÓçÞÇ·
63c0 58 5B 7F 12 7F E7 C4 F5-DA 5F 24 5E BE 1B DF E7 X[···çÄõÚ_$^¾·ßç
63d0 EC 8B 1F 28 F8 81 02 8C-BA 06 4B 52 80 26 7B A1 ì··(ø···º·KR·&{¡
63e0 20 48 2E AA EC 22 4B 3E-CD 66 07 41 07 36 48 DA  H.ªì"K>Íf·A·6HÚ
63f0 BE 17 8B 36 A6 69 50 2A-D9 54 4F 95 29 97 EC 70 ¾··6¦iP*ÙTO·)·ìp
6400 1F 84 04 8E 33 60 7D 7D-87 D5 D5 75 5C F7 64 F7 ····3`}}·ÕÕu\÷d÷
6410 DA 5F 24 F2 08 20 87 2B-17 CF D7 08 7D 81 49 6D Ú_$ò· ·+·Ï×·}·Im
6420 DB 26 12 46 08 2E AA E4-A2 44 7F 60 EF E6 A8 51 Û&·F·.ªä¢D·`ïæ¨Q
6430 2A 31 EA CE 28 44 6E F0-CD 0B B9 00 E4 4C E4 90 *1êÎ(DnðÍ·¹·äLä·
6440 5E 8E 69 56 81 6F 5E BA-7A E3 E6 5F FD D6 97 F6 ^·iV·o^ºzãæ_ýÖ·ö
6450 6C 8E 4A 09 40 53 84 06-DF F7 BE F5 D7 79 21 CF l·J·@S··ß÷¾õ×y!Ï
6460 BC 90 0B 40 CE 54 5C B9-78 3E E9 93 00 BC 11 3D ¼··@ÎT\¹x>é··¼·=
6470 FD 53 E0 DA A5 AB 37 F2-10 3E 20 70 77 3D 43 6C ýSàÚ¥«7ò·> pw=Cl
6480 69 66 6F 72 64 32 33 35-27 27 27 27 27 27 27 27 iford235''''''''
6490 27 27 27 27 27 27 27 27-27 27 27 27 27 27 27 27 ''''''''''''''''
64a0 27 27 27 27 27 E7 F8 F8-7F E4 E5 87 7C 6C 09 60 '''''çøø·äå·|l·`
64b0 40 00 00 00 00 49 45 4E-44 AE 42 60 82          @····IEND®B`·
```

In this screen shot it is seen that password is hidden in the vault.png file which is an image and the password can be found either using hex editor or HEX code which can be viewed using FTK Imager.

3. Alternate data stream

This is used to hide the password using alternate data stream in hidden.txt which is further embedded into README.txt. one example is shown in the following screen shot as described in the tutorial



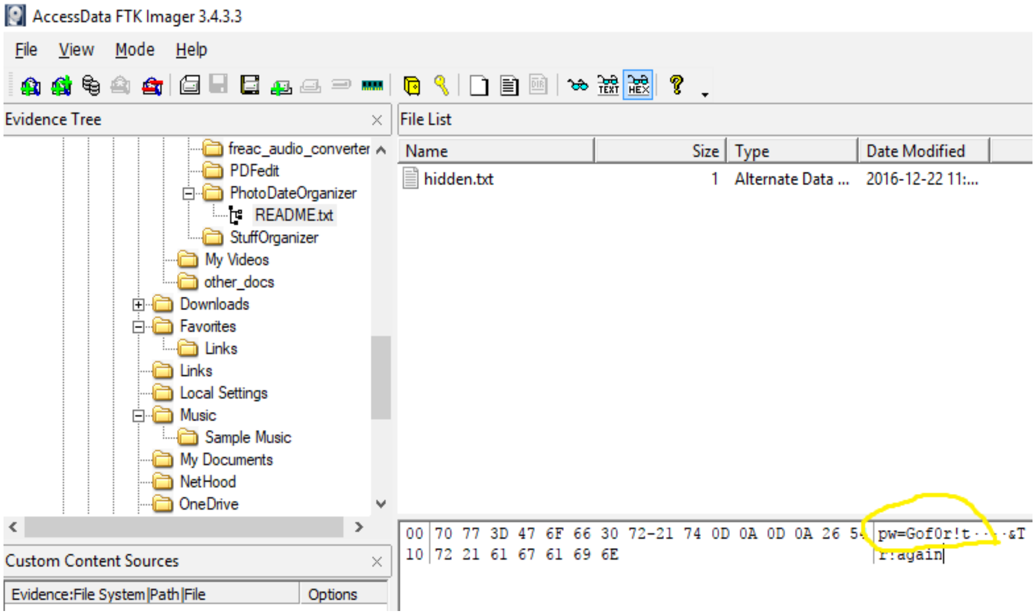
```
C:\Users\devine\Documents\courses\elec570\tools\Streams>streams C:\Users\devine\
Desktop\testdir\ourSecret.docx

streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users\devine\Desktop\testdir\ourSecret.docx:
         :hidden:$DATA 12

C:\Users\devine\Documents\courses\elec570\tools\Streams>more < C:\Users\devine\D
esktop\testdir\ourSecret.docx:hidden
```

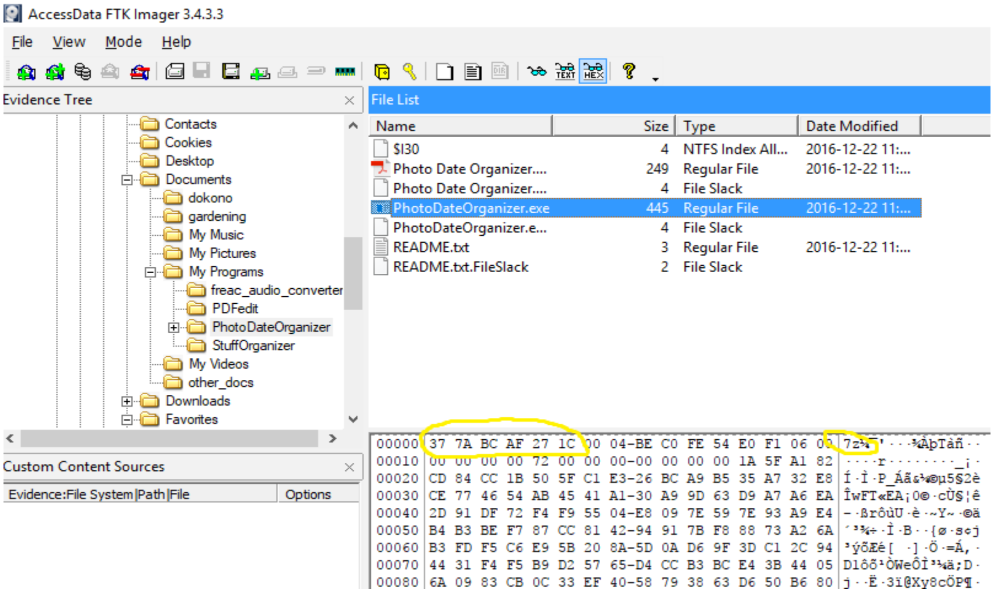
And then we found that the password is hidden in this hidden file.



Name	Size	Type	Date Modified
hidden.txt	1	Alternate Data ...	2016-12-22 11:...

```
00 70 77 3D 47 6F 66 30 72-21 74 0D 0A 0D 0A 26 54 pw=Gof0r!t····&T
10 72 21 61 67 61 69 6E                            r!again
```

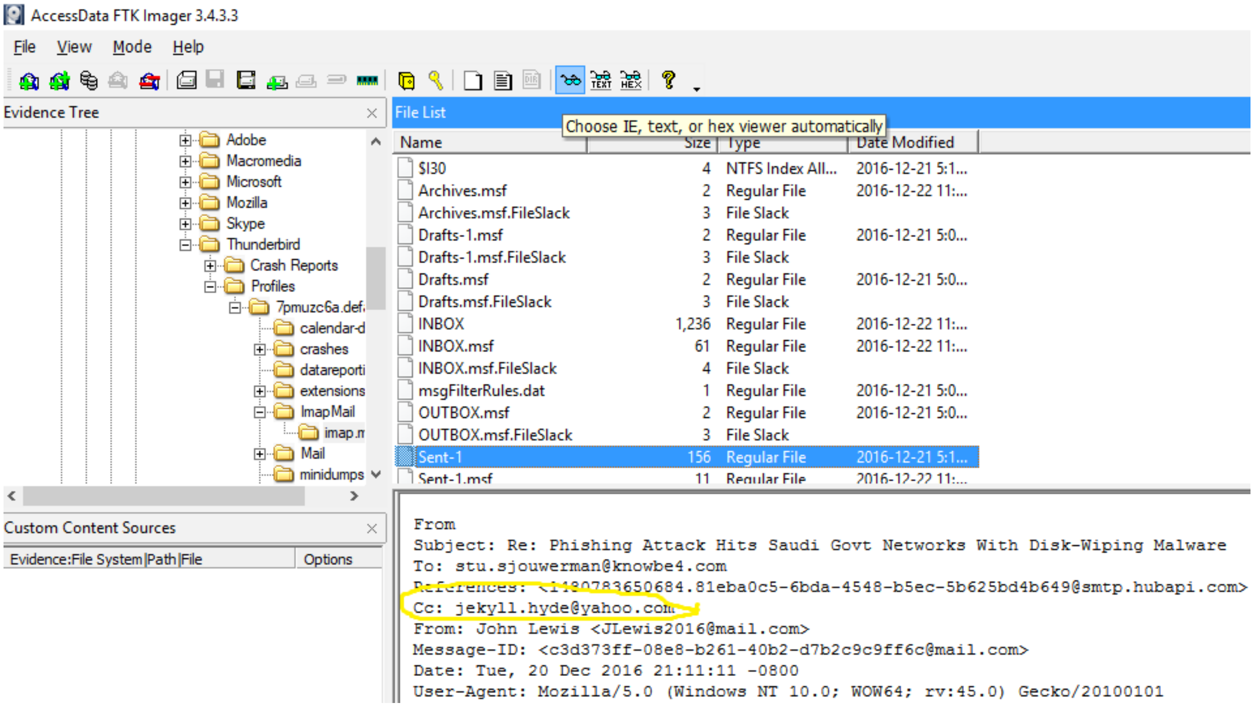
4. FTK imager
We have used this tool to analyze the whole suspect machine. This tool helps to view the files in three modes named automatic, text and HEX from where we can see the images and there content and investigate the suspicious files. For example, the screen shot below shows that the file PhotoDateOrganizer is saved as .exe but it is a .7z folder and there are various other examples.



Name	Size	Type	Date Modified
$I30	4	NTFS Index All...	2016-12-22 11:...
Photo Date Organizer....	249	Regular File	2016-12-22 11:...
Photo Date Organizer....	4	File Slack	
PhotoDateOrganizer.exe	445	Regular File	2016-12-22 11:...
PhotoDateOrganizer.e...	4	File Slack	
README.txt	3	Regular File	2016-12-22 11:...
README.txt.FileSlack	2	File Slack	

```
00000 37 7A BC AF 27 1C 00 04-BE C0 FE 54 E0 F1 06 00 7z¼¯'···¾ÀþTàñ··
00010 00 00 00 00 72 00 00 00-00 00 00 00 1A 5F A1 82 ····r········_¡·
00020 CD 84 CC 1B 50 5F C1 E3-26 BC A9 B5 35 A7 32 E8 Í·Ì·P_Áã&¼©µ5§2è
00030 CE 77 46 54 AB 45 41 A1-30 A9 9D 63 D9 A7 A6 EA ÎwFT«EA¡0©·cÙ§¦ê
00040 2D 91 DF 72 F4 F9 55 04-E8 09 7E 59 7E 93 A9 E4 -·ßrôùU·è·~Y~·©ä
00050 B4 B3 BE F7 87 CC 81 42-94 91 7B F8 88 73 A2 6A ´³¾÷·Ì·B··{ø·s¢j
00060 B3 FD F5 C6 E9 5B 20 8A-5D 0A D6 9F 3D C1 2C 94 ³ýõÆé[ ·]·Ö·=Á,·
00070 44 31 F4 F5 B9 D2 57 65-D4 CC B3 BC E4 3B 44 05 D1ôõ¹ÒWeÔÌ³¼ä;D·
00080 6A 09 83 CB 0C 33 EF 40-58 79 38 63 D6 50 B6 80 j··Ë·3ï@Xy8cÖP¶·
```

4. Investigate and discuss whether or not the email evidence helps in making the case against the suspect. [5%]
The first evidence we found about the emails was in the sent folder of Mr. John where he did CC to Mr. Jekyll. So, it can be predicted that Mr. John is the person who is sending the email and is using name of someone else. But at the same time this cannot be ruled out that he can be his friend to whom he is using to send Ms. Alicia blackmailing email.



Name	Size	Type	Date Modified
$I30	4	NTFS Index All...	2016-12-21 5:1...
Archives.msf	2	Regular File	2016-12-22 11:...
Archives.msf.FileSlack	3	File Slack	
Drafts-1.msf	2	Regular File	2016-12-21 5:0...
Drafts-1.msf.FileSlack	3	File Slack	
Drafts.msf	2	Regular File	2016-12-21 5:0...
Drafts.msf.FileSlack	3	File Slack	
INBOX	1,236	Regular File	2016-12-22 11:...
INBOX.msf	61	Regular File	2016-12-22 11:...
INBOX.msf.FileSlack	4	File Slack	
msgFilterRules.dat	1	Regular File	2016-12-21 5:0...
OUTBOX.msf	2	Regular File	2016-12-21 5:0...
OUTBOX.msf.FileSlack	3	File Slack	
Sent-1	156	Regular File	2016-12-21 5:1...
Sent-1.msf	11	Regular File	2016-12-22 11:...

```
From
Subject: Re: Phishing Attack Hits Saudi Govt Networks With Disk-Wiping Malware
To: stu.sjouwerman@knowbe4.com
References: <1480783650684.81eba0c5-6bda-4548-b5ec-5b625bd4b649@smtp.hubapi.com>
Cc: jekyll.hyde@yahoo.com
From: John Lewis <JLewis2016@mail.com>
Message-ID: <c3d373ff-08e8-b261-40b2-d7b2c9c9ff6c@mail.com>
Date: Tue, 20 Dec 2016 21:11:11 -0800
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:45.0) Gecko/20100101
```

According to our investigation we can say that Mr. John has definitely lied that he has deleted all the personal content of both of them, But only email evidence shows that they both know each other but definitely not that he has send that blackmailing email to Ms. Alicia.

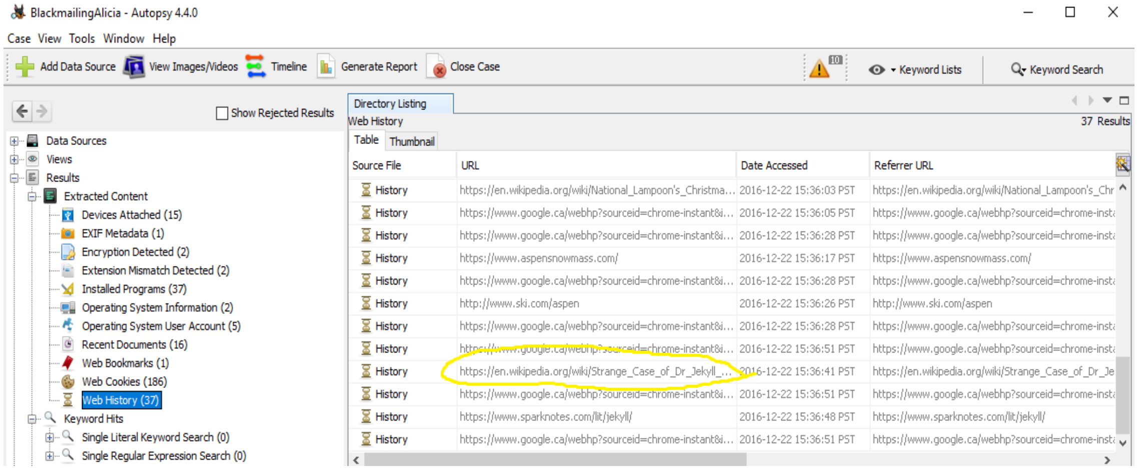
The second evidence we found against him was Ms. Alicia's signature, but question was not asked about those signatures by the investigators.

But there is no strong evidence available, which can definitely establish relation between Mr. John and Mr. Jekyll which can prove it that these both names are of the same person.

But as he denied that he does not have any evidence about their relation, and we found a lot of evidences which are encrypted in so many ways so that no one see them. Or he is making sure that even police will not be able to find it that he is in possession of anything which blackmailer was talking about makes the evidences stronger against him.

5. Discuss and justify whether or not the overall evidence is enough to conclude blackmailing by the suspect. [4%]

Answer: Overall evidence is enough for Mr. John to be a suspect because he browsed the strange case of Dr. Jekyll from where Ms. Alicia got the blackmailing email, may be used this search to find a name which can act as blackmailer.

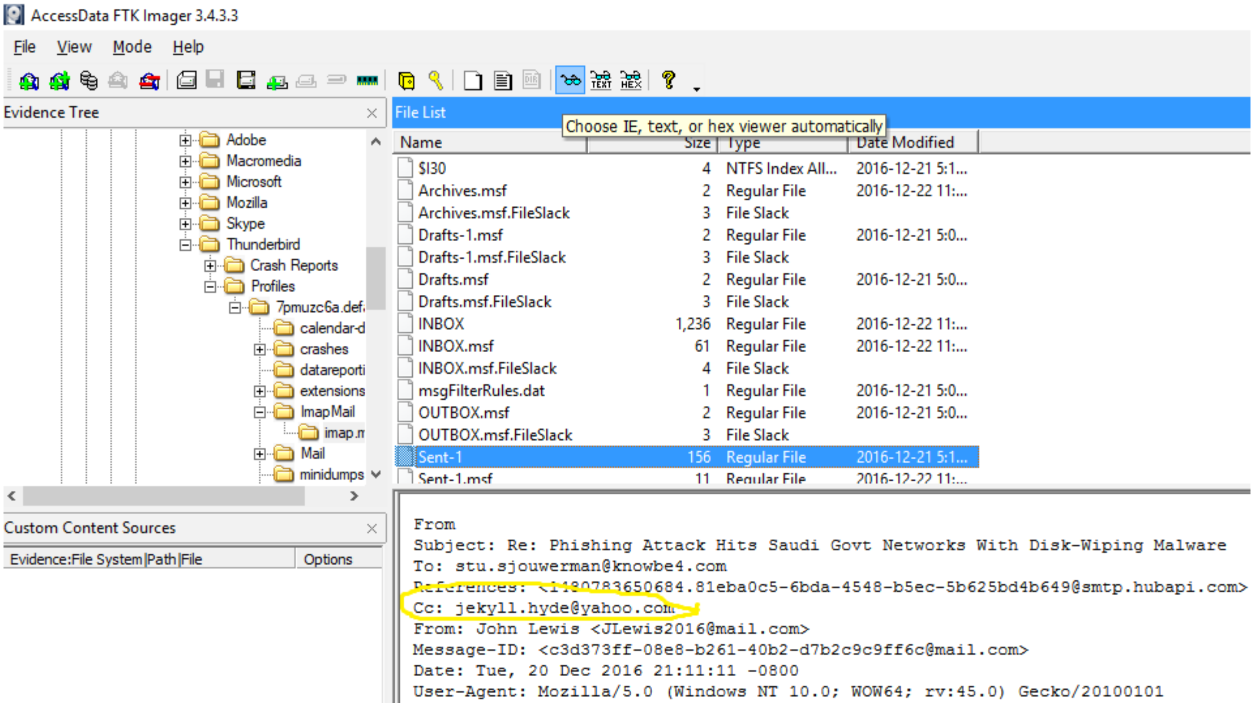


Web History 37 Results

Source File	URL	Date Accessed	Referrer URL
History	https://en.wikipedia.org/wiki/National_Lampoon's_Christma...	2016-12-22 15:36:03 PST	https://en.wikipedia.org/wiki/National_Lampoon's_Chr
History	https://www.google.ca/webhp?sourceid=chrome-instant&i...	2016-12-22 15:36:05 PST	https://www.google.ca/webhp?sourceid=chrome-insta
History	https://www.google.ca/webhp?sourceid=chrome-instant&i...	2016-12-22 15:36:28 PST	https://www.google.ca/webhp?sourceid=chrome-insta
History	https://www.aspensnowmass.com/	2016-12-22 15:36:17 PST	https://www.aspensnowmass.com/
History	https://www.google.ca/webhp?sourceid=chrome-instant&i...	2016-12-22 15:36:28 PST	https://www.google.ca/webhp?sourceid=chrome-insta
History	http://www.ski.com/aspen	2016-12-22 15:36:26 PST	http://www.ski.com/aspen
History	https://www.google.ca/webhp?sourceid=chrome-instant&i...	2016-12-22 15:36:28 PST	https://www.google.ca/webhp?sourceid=chrome-insta
History	https://www.google.ca/webhp?sourceid=chrome-instant&i...	2016-12-22 15:36:51 PST	https://www.google.ca/webhp?sourceid=chrome-insta
History	https://en.wikipedia.org/wiki/Strange_Case_of_Dr_Jekyll_...	2016-12-22 15:36:41 PST	https://en.wikipedia.org/wiki/Strange_Case_of_Dr_Je
History	https://www.google.ca/webhp?sourceid=chrome-instant&i...	2016-12-22 15:36:51 PST	https://www.google.ca/webhp?sourceid=chrome-insta
History	https://www.sparknotes.com/lit/jekyll/	2016-12-22 15:36:48 PST	https://www.sparknotes.com/lit/jekyll/
History	https://www.google.ca/webhp?sourceid=chrome-instant&i...	2016-12-22 15:36:51 PST	https://www.google.ca/webhp?sourceid=chrome-insta

Then we found that Mr. John send an email to the someone with CC as Jekyll.hyde@yahoo.com.

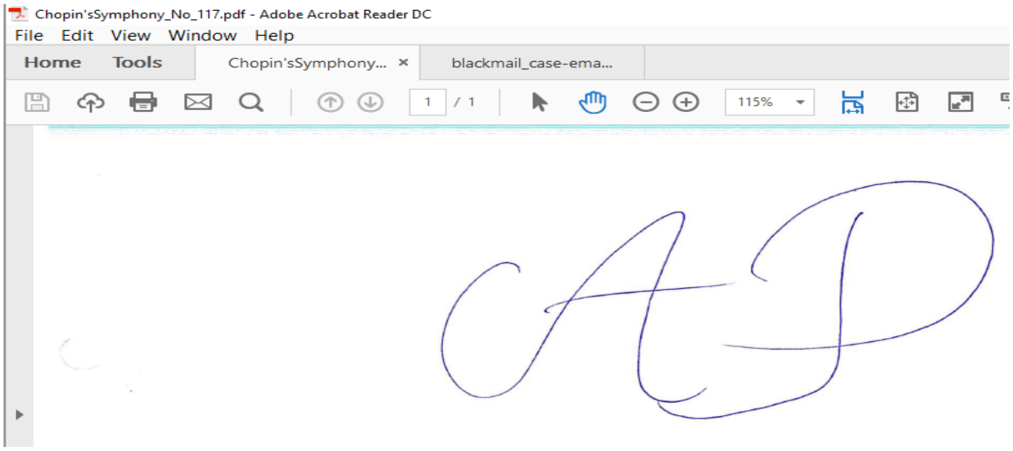
This person can be his friend whom he has asked to blackmail Ms. Alicia. And in the investigation he denied that he does not know anything about this email Is and the person.



Name	Size	Type	Date Modified
$I30	4	NTFS Index All...	2016-12-21 5:1...
Archives.msf	2	Regular File	2016-12-22 11:...
Archives.msf.FileSlack	3	File Slack	
Drafts-1.msf	2	Regular File	2016-12-21 5:0...
Drafts-1.msf.FileSlack	3	File Slack	
Drafts.msf	2	Regular File	2016-12-21 5:0...
Drafts.msf.FileSlack	3	File Slack	
INBOX	1,236	Regular File	2016-12-22 11:...
INBOX.msf	61	Regular File	2016-12-22 11:...
INBOX.msf.FileSlack	4	File Slack	
msgFilterRules.dat	1	Regular File	2016-12-21 5:0...
OUTBOX.msf	2	Regular File	2016-12-21 5:0...
OUTBOX.msf.FileSlack	3	File Slack	
Sent-1	156	Regular File	2016-12-21 5:1...
Sent-1.msf	11	Regular File	2016-12-22 11:...

```
From
Subject: Re: Phishing Attack Hits Saudi Govt Networks With Disk-Wiping Malware
To: stu.sjouwerman@knowbe4.com
References: <1480783650684.81eba0c5-6bda-4548-b5ec-5b625bd4b649@smtp.hubapi.com>
Cc: jekyll.hyde@yahoo.com
From: John Lewis <JLewis2016@mail.com>
Message-ID: <c3d373ff-08e8-b261-40b2-d7b2c9c9ff6c@mail.com>
Date: Tue, 20 Dec 2016 21:11:11 -0800
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:45.0) Gecko/20100101
```

We found signatures od Ms. Alicia which are used in the blackmailing email.



Chopin'sSymphony_No_117.pdf - Adobe Acrobat Reader DC
File Edit View Window Help
Home
Tools
Chopin'sSymphony...
blackmail_case-ema...
1 / 1
115%

He used Steganography to hide the passwords to open the files. He kept love letters at two different locations and have used different passwords to open these files. He tried to hide everything from the investigators to prove himself as innocent. But if would have deleted the files then also with the help of FTK imager investigators could have come to know that he has deleted the files at the time of break up. But he was in procession of everything the black mailer was talking about and that too hidden. So, he is definitely involved in blackmailing Ms. Alicia