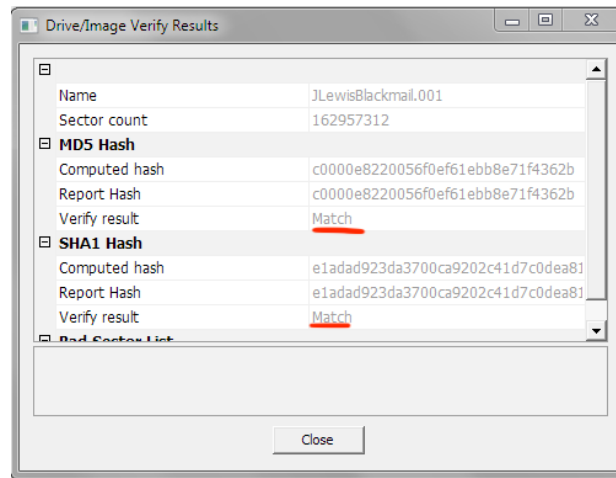


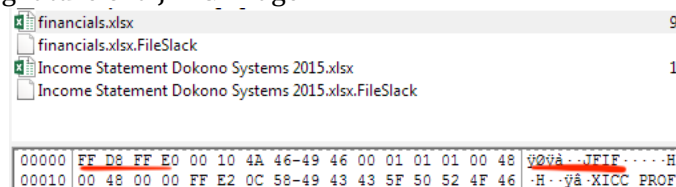
Assignment 2

1. I checked the validity of the supplied hashes using FTK Imager and did not notice any differences and the software confirmed this by indicating "Match" as shown below.

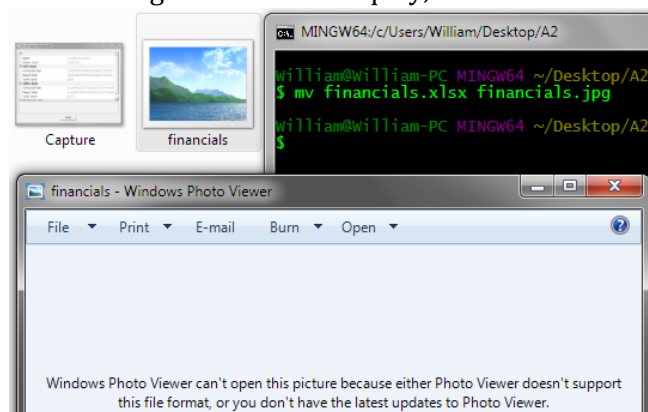


2. To examine the image I used FTK Imager and focused on the deleteme folder as per the hint in the assignment. I noticed that the only folders which contained files were AppData, Documents, Downloads, Music and Pictures. Because AppData was so large I decided to save it for last and examined the other folders in the order listed.
 - a. Documents: The first folder I examined was Documents, which contained several more folders, four of which contained more files.

The first, dokono, contained five files, all of which had the correct magic numbers, when examining their contents in hexadecimal, and displayed correctly when exported and opened on my computer, except for one. financials.xlsx contained the hexadecimal signature of a JPEG image.



This led me to assume the file was actually a JPEG with the extension changed to disguise it as something uninteresting. So I renamed the file with the proper extension, however the image still did not display, as shown below.



I tried opening the file again with photo editing software GIMPshop and received the error messaged shown below which gave me a clue as to why the file was not opening.

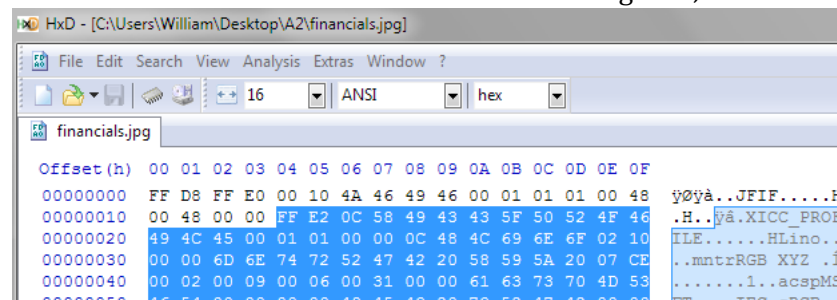


This led me to examine the hex data further as well as reference the JPEG specification to determine the significance of different markers. I noticed that the file had some “reserved for application” markers (according to the specification) and this led me to believe the JPEG has some application specific markers that are responsible for the error.

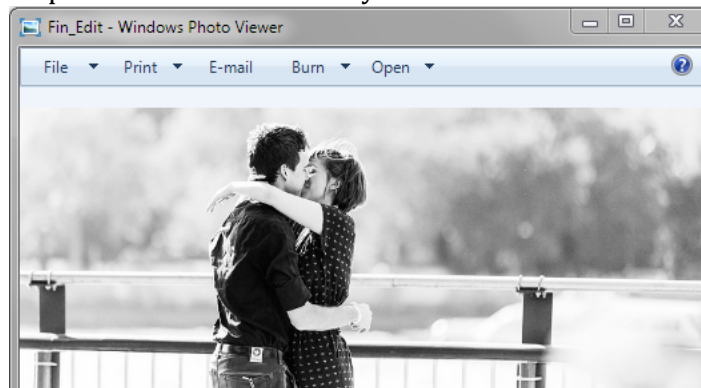
XFFD8'	SOI*	Start of image
XFFD9'	EOI*	End of image
XFFDA'	SOS	Start of scan
XFFDB'	DQT	Define quantization table(s)
XFFDC'	DNL	Define number of lines
XFFDD'	DRI	Define restart interval
XFFDE'	DHP	Define hierarchical progression
XFFDF'	EXP	Expand reference component(s)
XFFEO' through XFFEF'	APP	Reserved for application segments
XFFFO' through XFFFD'	JPG	Reserved for JPEG extensions
XFFFE'	COM	Comment

00000	FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 48	y0yà..JFIF....H
00010	00 48 00 00 FF E2 0C 58 49 43 43 5F 50 52 4F 46	.H..yà.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	..mnrRGB XYZ .f
00040	00 02 00 09 00 06 00 31 00 00 61 63 73 70 4D 531..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 00 00 018Ö..
00070	00 00 00 00 D3 2D 48 50 20 20 00 00 00 00 00	...Ô-HP
● ● ●		
01380	65 E7 66 3D 66 92 66 E8 67 3D 67 93 67 E9 68 3F	eçf=f..fëg=g.géh?
01390	68 96 68 EC 69 43 69 9A 69 F1 6A 48 6A 9F 6A F7	h.hiCi.iñHj.j+
013a0	6B 4F 6B A7 6B FF 6C 57 6C AF 6D 08 6D 60 6D B9	kOk\$ky1Wl~m~m~m~
013b0	6E 12 6E 6B 6E C4 6F 1E 6F 78 6F D1 70 2B 70 86	n.nknAo .oxoNp+p.
● ● ●		
01610	F6 FB F7 8A F8 19 F8 A8 F9 38 F9 C7 FA 57 FA E7	ôû+æ~û8ûCûWûç
01620	FB 77 FC 07 FC 98 FD 29 FD BA FE 4B FE DC FF 6D	ûwû.û.ý)ý~pKpÛym
01630	FF FF FF DB 00 43 00 01 01 01 01 01 01 01 01	ýýýÛ~C.....
01640	01 01 01 01 02 02 03 02 02 02 02 04 03 03 02
01650	03 05 04 05 05 05 04 04 04 05 06 07 06 05 07
● ● ●		

I also noticed that the non-default markers appeared in one contiguous chunk and that the default markers expected in every JPEG file precede and follow this chunk. So, I deleted the entire chunk of non-default markers using HxD, a hex editor.

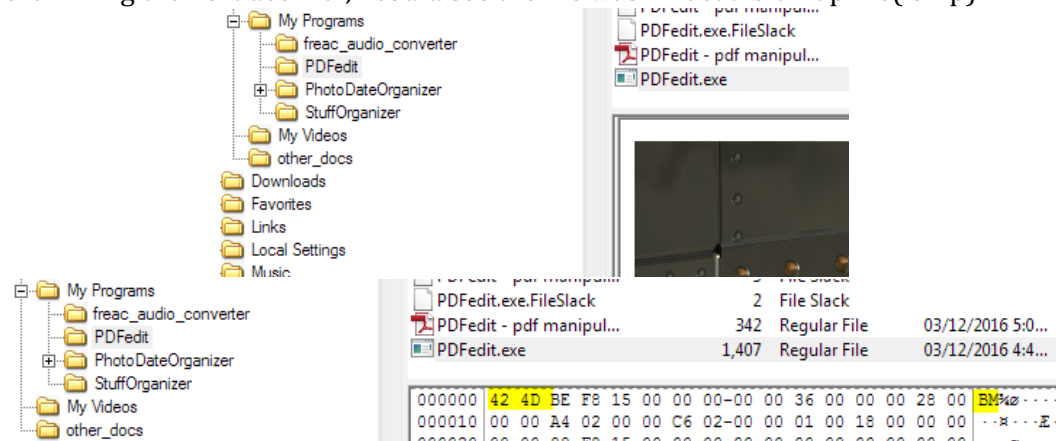


I tried opening the image one last time, and finally it worked, obtaining the following piece of evidence. A photo of Alicia kissing John Lewis, who is not her husband. Perfect material to attempt to black mail somebody with.

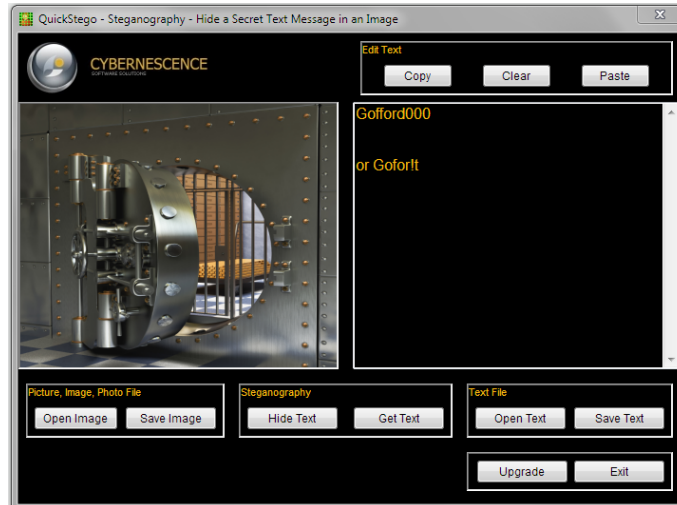


I moved onto the next folder contained in the Documents folders, labeled Gardening. This folder contained several images and pdfs, all of which had the correct hexadecimal signatures. It was possible to view all the files with FTK Imager in Auto mode and there was nothing suspicious, so I moved on.

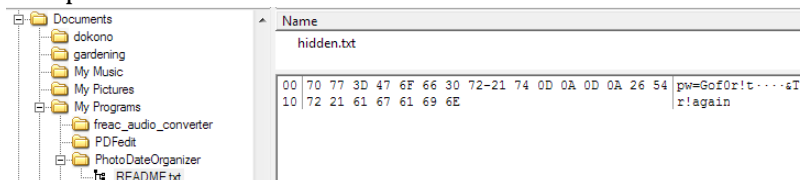
The next folder which contained more folders was My Programs. In it were 4 folders. The first, freak_audio_converter contained no suspicious files. The two text files were readable, and the exe file had the correct magic numbers for an executable, 4D 5A, and even ran when exported onto my machine. Moving onto the next folder PDFedit, it contained a manual for a PDF manipulator which could be viewed from within FTK Imager and did not seem suspicious. However it also contained a file called PDF.exe but when viewed in FTK Imager with Auto mode, an image displayed, and when examining the hexadecimal, I could see the file was in fact a bit map file(.bmp).



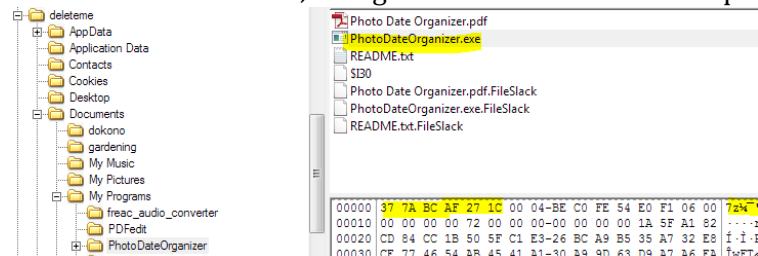
The image was a vault which is related to security and it in and of itself contained no sensitive information, so I asked myself "why hide an image of a vault by changing its' extension". I considered the possibility that using steganography, some information was hidden inside of the image. Using a free program called Quick Stego, I discovered the string "Gofford000 or Gofor!t" was hidden within the image. I was not sure the significance of this string but I assumed it could be passwords.



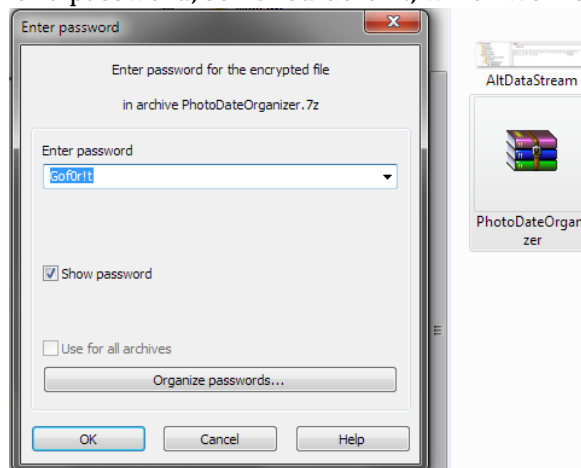
The next folder within My Programs was PhotoDateOrganizer, which contained 3 files. The first was a pdf with correct signature which displayed correctly. There was a file called README.txt that had an alternate data stream called hidden.txt. The alternate data stream contained the string “pw=Gof0r!t &Tr!again” which I again assumed were passwords.



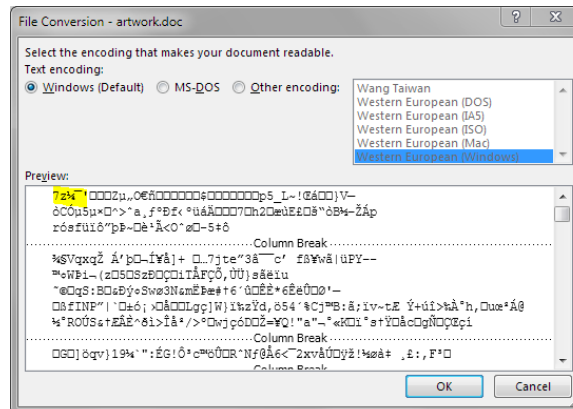
The last file called PhotoDateOrganizer.exe had an exe extension but the signature of a 7zip archive. So I extracted the file, changed the extension and attempted to open it.



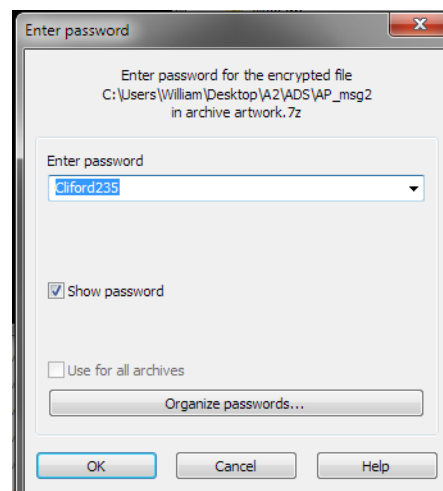
The archive asked for a password, so I tried Gof0r!t, which worked.



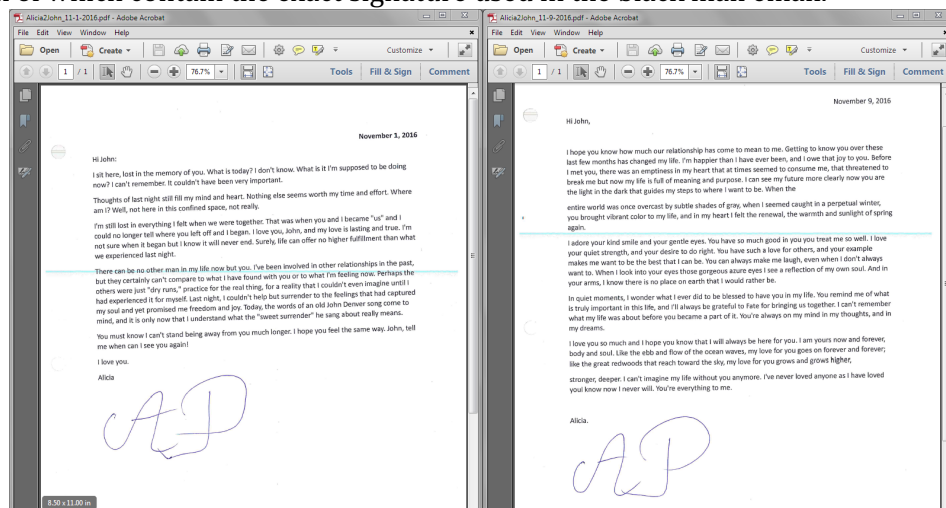
The archive contained a word document but when I attempted to open it, I got the following error message and a preview which contained the ASCII representation of the 7zip file signature.



This led me to believe the file was a 7zip archive, so I changed the signature again and once again was asked for a password. The passwords discovered so far did not work. However, later on I discovered another password hidden in a PNG file which I discuss later in the report.



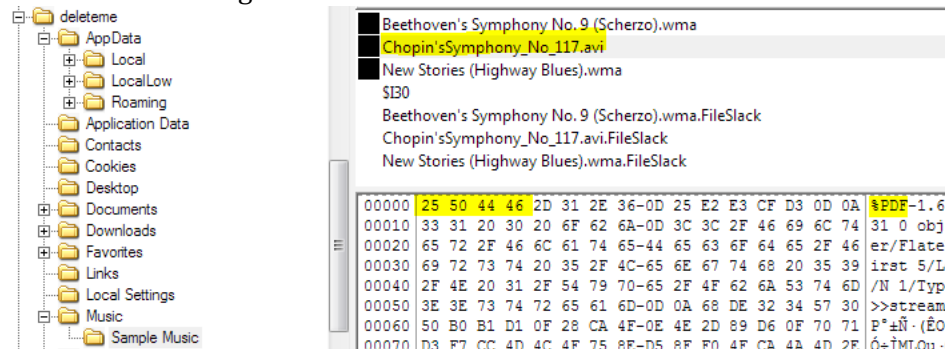
This password worked and I obtained two love letters written from John to Alicia, both of which contain the exact signature used in the black mail email.



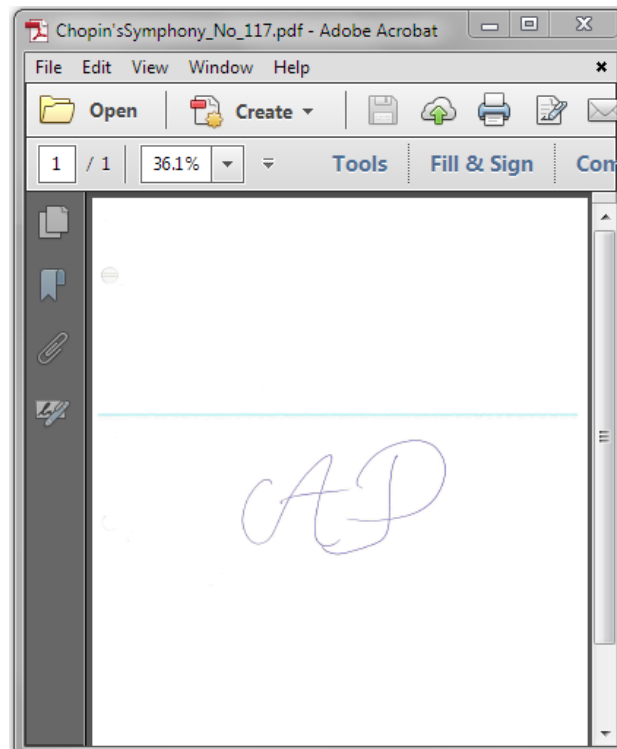
Moving on to the last folder contained in My Programs, StuffOrganizer, I examined the files and both had correct signatures and did not seem suspicious.

The last folder contained in Documents was called other_docs, but the files contained within had correct file signatures and opened correctly when exported so I did not deem them suspicious and moved on

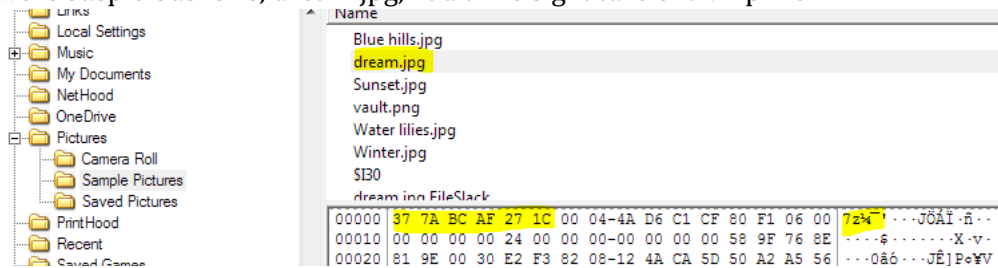
- b. After Documents I examined the Downloads folder. The folder contained two installation executables which did not seem suspicious. However, it was noteworthy that the user downloaded Chrome and an email client, Thunderbird, about two weeks after the black mail email was sent. If he was the black mailer, he may have uninstalled and reinstalled these programs in an attempt to destroy evidence.
- c. Next, I examined the Music folder. This folder contained three audio files but one of them had the file signature of a PDF.



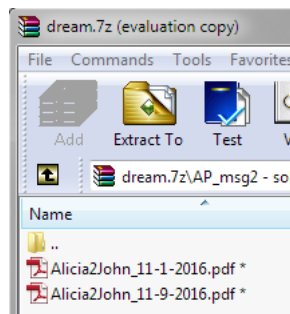
I exported the file, changed the extension, and this revealed a PDF of the exact signature used in the black mail email.



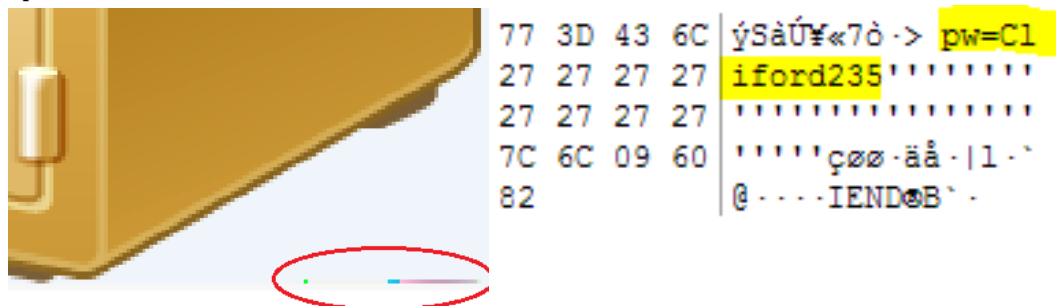
- d. Next was the Pictures folder which contained one folder inside with more files, Sample Pictures. There were several images contained within this folder but two were suspicious. One, dream.jpg, had a file signature of a 7zip file.



So I extracted the file, changed the extension, and was asked for a password, this time, the password I found earlier "Gofford000" worked and I obtained copies of the love letters I found earlier.

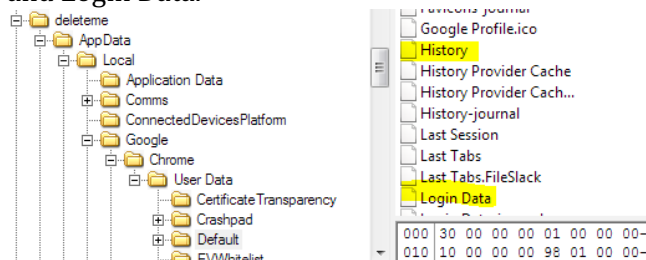


Second there was a file, vault.png, which stuck out to me because it was a vault like the other image which contained a password. I examined the image and noticed discoloured pixels in the bottom right hand corner. I examined the corresponding area in ASCII and found a password, "Cliford235". This is the password I used to open the nested archive discussed earlier.

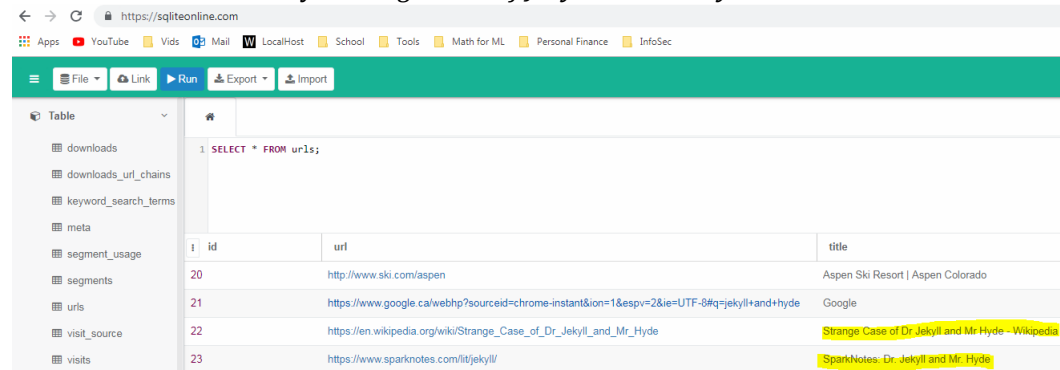


- e. Lastly, I examined the AppData folder. Because of the size of the folder I looked for two specific folders.

Firstly, the Google Chrome User Data folder, which contained two SQLite files of interest, History and Login Data.

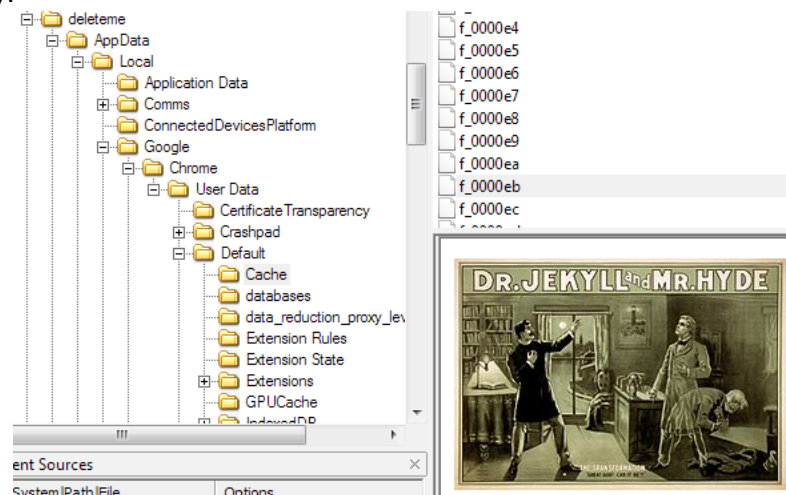


Using sqliteonline.com, I was able to examine the contents of these databases. I did not find anything of interest in the Login Data file (I was hoping to find jeekyll.hyde@yahoo.com as a saved username). However, in the History database I found that the user of this computer searched Spark Notes and Wikipedia for information on the story "*Strange Case of Jekyll and Mr. Hyde*".

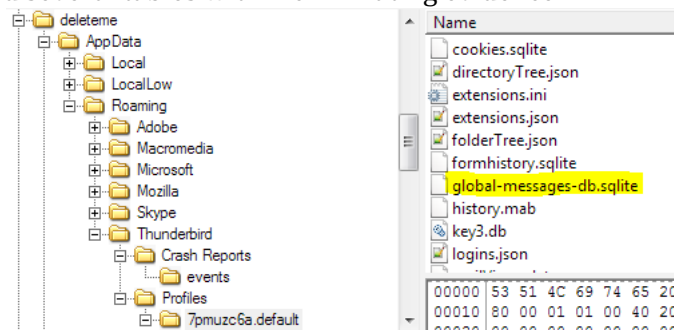


id	url	title
20	http://www.ski.com/aspen	Aspen Ski Resort Aspen Colorado
21	https://www.google.ca/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8&q=jeekyll+and+hyde	Google
22	https://en.wikipedia.org/wiki/Strange_Case_of_Dr_Jekyll_and_Mr_Hyde	Strange Case of Dr Jekyll and Mr Hyde - Wikipedia
23	https://www.sparknotes.com/lit/jeekyll/	SparkNotes: Dr. Jekyll and Mr. Hyde

I also checked the Google Chrome Cache folder and found the following image, perhaps from when the user visited the sites pertaining to Jekyll and Hyde found in his history.



Lastly, I examined the Thunderbird profiles folder and found an sqlite database file which contained several tables with incriminating evidence.



One table contained emails which were in his inbox. The only interesting record was for an email the user received from forensicsfocus.com, a site which discusses digital forensics. The email states the user has signed up for their emailing list. This could indicate the user was attempting to learn how to hide his digital trail.


```
1 SELECT * FROM messagesText_content;
```

i	docid	c0body	c1subject	c2attachmentNames
96		TechTarget Today's Top White Papers: Social customer service is ...	Social customer service is the way...	
97		Welcome to Forensic Focus! You or someone else has used your ...	User Account Application	

Another Table contained the user's contacts and one record contained the email address which sent the black mail email.

```
1 SELECT * FROM contacts;
```

i	id	directoryUUID	contactUUID	popularity	frecency	name
17		Null	Null	0	0	Teresa Bernardos
18		Null	Null	0	0	jekyll.hyde@yahoo.com
19		Null	Null	0	0	John Lewis

Finally, and perhaps the most incriminating, one of the files contained sent emails from the user's account. Using FTK Imager's search function, I was able to find that an email sent from John Lewis Cc'd Jekyll.hyde@yahoo.com. This means that the user of the thunderbird account on this machine, JLewis2016@mail.com, intentionally Cc'd the same email account that was responsible for the black mail.

3. The following table summarized the steps taken to mask the evidence files from others.

Love Letters	The love letters where hidden in encrypted archives which had their extensions renamed to appear as different uninteresting files. Furthermore, the passwords used to decrypt these archives were hidden using steganography as well alternate data streams.
Signature	The Signature was hidden by simply changing the file extension
Picture of John and Alicia Kissing	The photo was hidden by changing the file extension. The file was also only openable with a specific application, but it is unclear weather this was on purpose or if photo had application specific markers from the software used by the camera the photo was taken with.
Search History and Email Client Databases	The evidence gathered from App Data for Thunderbird and chrome was not hidden any more then it usually is, however given that the suspect reinstalled Chrome and Thunderbird after the blackmail incident I suspect this was gone in an attempt to destroy this evidence.

4. The email evidence does help in making a case against the suspect since it provides an email address to link the suspect to the crime, as well as provides proof that the suspect and the black mailer are in possession of the same scan of Alicia's signature. Additionally it helps

establish a time line which allows us to postulate why the suspect reinstalled Thunderbird and Google Chrome.

5. The overall evidence is most likely enough to conclude blackmailing. Although we cannot assume that John Lewis hid the photo of him kissing Alicia, love letters, and the signature because he planned to black mailer her. He could make the defense that he was hiding them because she was cheating and didn't want anyone to find out. He did say he deleted these files right after the break up. Therefore we caught him on one lie. Even though the signature is a direct match, they are the same on both love letters so it appears Alicia scanned her signature and may have sent it to many people. However, John did send an email to a colleague where he Cc'd the email address of the black mailer. This means that the prosecution can ask John why he Cc'd that address and how he knows the owner of the address. Additionally, he stated that he doesn't know anything about this email address which is clearly not the case since he Cc'd it. Thus we caught John on two lies. Depending on how he responds to questioning related to this evidence, the prosecution is extremely likely to get a guilty verdict.