Digital Forensics Technical Report

November 27, 2018

Summary

A Company named Lard Lad Donuts in Springfield believed that one of their employees , Ms Penelope Olsen is a secret agent and has access to the Company's secret recipe. They also believed that she has leaked the secret recipe to a Company named "Dunkin' Donuts" which happened to be their competitors. This led Lard Lad Donuts to file a Police complaint against Ms Penelope Olsen.

Moreover, Investigations into Ms Penelope Olsen indicate that the name is an alias and the she is Mrs Mona Simpson and is a wanted woman. After several investigations, Police found out that her last known address was with her son Mr. H.J.Simpson. at 742 Evergreen Terrace. Also, they found a USB device from the same address.

As a forensics analyst, my objective is to perform an analysis of the digital image provided by the local police.

Evidence Acquisition processing procedures

I will be using industry standard tools and techniques throughout handling, processing, and analysis of the evidence.

Local Police removed the USB drive for a forensic analysis. A working copy of the image was created for the examination. All subsequent analysis will be performed on a working copy of forensic image, not on the original media or the digital forensic image acquisition.

I will be using a tool named Autopsy which is a Digital Forensics platform to investigate what happened on a computer and to recover all the data from the digital image.

Analysis

- *Analysing instant messaging packets.*

The security staff of the company monitored Penelope's activity when they encountered a laptop which appeared on company's wireless network.

The security staff used the tool named Wireshark which enabled to track Penelope's computer network address. (192.168.1.158)

Below are the instant messaging packets which shows :-

1. Exhibit A.

No.	Time	Source	Destination	Protocol	Info
9	4.680216	192.168.1.10	192.168.1.255	NTP	NTP broadcast
10	8.181469	Vmware_69:e6:2b	Vmware_b0:8d:62	ARP	Who has 192.168.1.10? Tell 192.168.1.30
11	8.181738	Vmware_b0:8d:62	Vmware_69:e6:2b	ARP	192.168.1.10 is at 00:0c:29:b0:8d:62
12	11.909351	Vmware_c0:00:02	Broadcast	ARP	Who has 192.168.1.157? Tell 192.168.1.2
13	11.911114	192.168.1.2	192.168.1.157	TCP	54419 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=
14	11.911119	Vmware_1f:f8:1a	Vmware_c0:00:02	ARP	192.168.1.157 is at 00:0c:29:1f:f8:1a
15	11.912003	192.168.1.2	192.168.1.157	TCP	54419 > http [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSV=499
16	11.912007	192.168.1.157	192.168.1.2	TCP	http > 54419 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MS
17	11.913000	192.168.1.2	192.168.1.157	TCP	54419 > http [FIN, ACK] Seq=1 Ack=1 Win=5888 Len=0 TS
18	11.947402	192.168.1.157	192.168.1.2	TCP	http > 54419 [ACK] Seq=1 Ack=2 Win=5792 Len=0 TSV=185
19	11.977411	192.168.1.2	192.168.1.157	TCP	[TCP ACKed lost segment] 54419 > http [ACK] Seq=2 Ack
20	11.977416	192.168.1.157	192.168.1.2	TCP	http > 54419 [FIN, ACK] Seq=1 Ack=2 Win=5792 Len=0 TS
21	13.674543	Vmware_b0:8d:62	Vmware_69:e6:2b	ARP	Who has 192.168.1.30? Tell 192.168.1.10
22	13.674786	Vmware_69:e6:2b	Vmware_b0:8d:62	ARP	192.168.1.30 is at 00:0c:29:69:e6:2b
23	18.870898	192.168.1.158	64.12.24.50	SSL	Continuation Data
24	18.871477	64.12.24.50	192.168.1.158	TCP	https > 51128 [ACK] Seq=1 Ack=7 Win=64240 Len=0
25	33.914966	192.168.1.158	64.12.24.50	SSL	Continuation Data
26	33.915486	64.12.24.50	192.168.1.158	TCP	https > 51128 [ACK] Seq=1 Ack=196 Win=64240 Len=0

```
0000  00 0c 29 b0 8d 62 00 12  79 45 a4 bb 08 00 45 00   ..)..b.. yE....E.
0010  00 e5 ab 3c 40 00 40 06  74 52 c0 a8 01 9e 40 0c   ...<@.@. tR....@.
0020  18 32 c7 b8 01 bb 33 6b  d2 c9 07 e9 60 db 50 18   .2....3k ....`.P.
0030  f5 3c d0 8c 00 00 2a 02  00 61 00 b7 00 04 00 06   .<....*. .a......
0040  00 00 00 00 00 45 34 36  32 38 37 37 38 00 00 01   .....E46 28778...
0050  0b 53 65 63 35 35 38 75  73 65 72 31 00 02 00 8f   .Sec558u ser1....
0060  05 01 00 04 01 01 01 02  01 01 00 83 00 00 00 00   ........ ........
0070  48 65 72 65 27 73 20 74  68 65 20 73 65 63 72 65   Here's t he secre
0080  74 20 72 65 63 69 70 65  2e 2e 2e 20 49 20 6a 75   t recipe ... I ju
0090  73 74 20 64 6f 77 6e 6c  6f 61 64 65 64 20 69 74   st downl oaded it
00a0  20 66 72 6f 6d 20 74 68  65 20 66 69 6c 65 20 73    from th e file s
00b0  65 72 76 65 72 2e 20 4a  75 73 74 20 63 6f 70 79   erver. J ust copy
00c0  20 74 6f 20 61 20 74 68  75 6d 62 20 64 72 69 76    to a th umb driv
00d0  65 20 61 6e 64 20 79 6f  75 27 72 65 20 67 6f 6f   e and yo u're goo
00e0  64 20 74 6f 20 67 6f 20  26 67 74 3b 3a 2d 29 00   d to go  &gt;:-).
00f0  03 00 00                                           ...
```

2. Exhibit B.

No.	Time	Source	Destination	Protocol	Info
205	88.495741	192.168.1.159	192.168.1.255	BROWSER	Get Backup List Request
206	88.496757	192.168.1.159	192.168.1.255	NBNS	Name query NB WORKGROUP<1b>
207	89.247375	192.168.1.159	192.168.1.255	NBNS	Name query NB WORKGROUP<1b>
208	89.998917	192.168.1.159	192.168.1.255	NBNS	Name query NB WORKGROUP<1b>
209	90.000408	192.168.1.157	192.168.1.255	NBNS	Name query NB SANS<1d>
210	90.788876	192.168.1.158	64.12.24.50	SSL	Continuation Data
211	90.789489	64.12.24.50	192.168.1.158	TCP	https > 51128 [ACK] Seq=1254 Ack=414 Win=64240 Len=0
212	90.816866	192.168.1.158	64.12.24.50	SSL	Continuation Data
213	90.817354	64.12.24.50	192.168.1.158	TCP	https > 51128 [ACK] Seq=1254 Ack=524 Win=64240 Len=0

```
0000  00 0c 29 b0 8d 62 00 12  79 45 a4 bb 08 00 45 00   ..)..b.. yE....E.
0010  00 96 ab 4c 40 00 40 06  74 91 c0 a8 01 9e 40 0c   ...L@.@. t.....@.
0020  18 32 c7 b8 01 bb 33 6b  d4 60 07 e9 65 c0 50 18   .2....3k .`..e.P.
0030  f5 16 50 dd 00 00 00 00  00 00 00 49 35 30 38 38   ..P..... ...I5088
0040  34 39 36 00 00 01 0b 53  65 63 35 35 38 75 73 65   496....S ec558use
0050  72 31 00 02 00 22 05 01  00 04 01 01 01 02 01 01   r1..."... ........
0060  00 16 00 00 00 00 73 65  65 20 79 6f 75 20 69 6e   ......se e you in
0070  20 68 61 77 61 69 69 21  00 03 00 00 2a 02 00 66    hawaii! ....*..f
0080  00 22 00 04 00 14 00 00  00 00 00 4a 00 00 00 00   ."...... ...J....
0090  00 00 00 00 00 01 0b 53  65 63 35 35 38 75 73 65   .......S ec558use
00a0  72 31 00 00                                        r1..
```

(HEX CONTENT VIEWER)

Penelope's Computer network address could be seen as a source which means she was sending some messages to some other user whose network address is 64.12.24.50.

Hex Content Viewer shows you the raw and exact contents of a file and the decoded group of ASCII characters shows the message which Penelope sent to the user. The message could be read as :

"Here's the secret recipe…I just downloaded it from the file's server. Just copy to a thumb drive and you're good to go &gt ; :-)."

This indicates Penelope had an access to the Company's secret recipe.
Also, The Hex Content Viewer of Exhibit B shows the message :

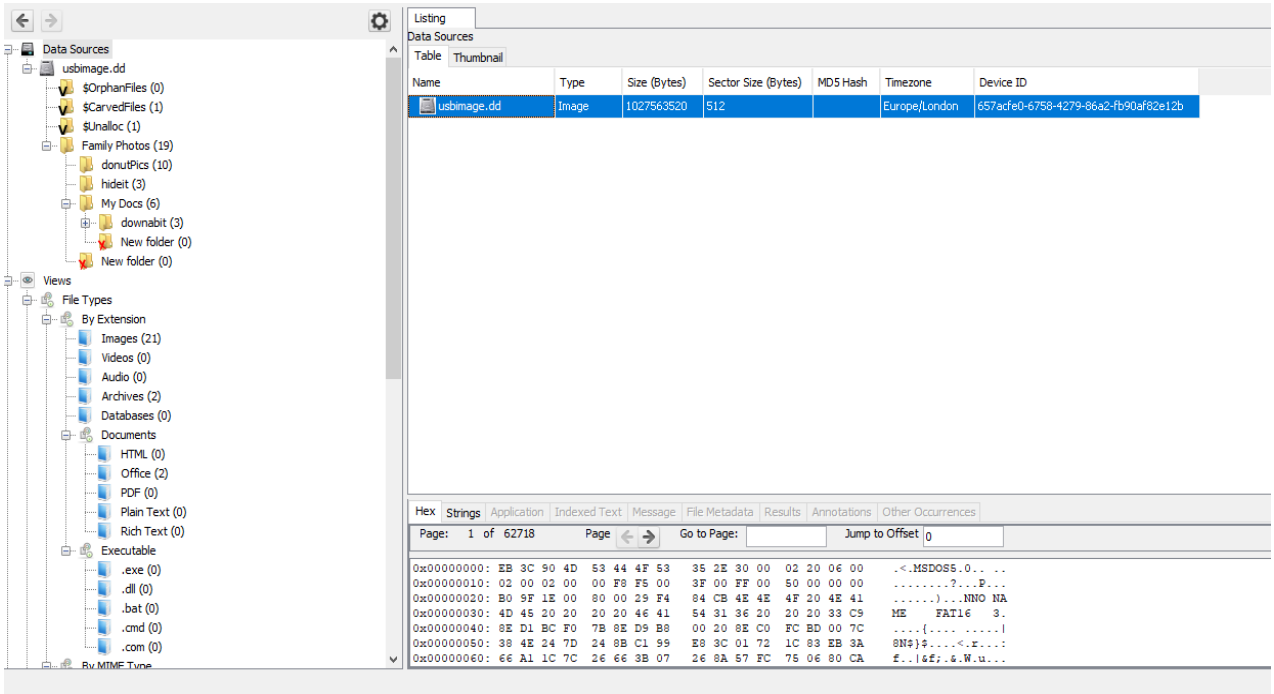
"see you in hawaii!"

Which was sent from the same source to the same destination.
This indicates Penelope was planning to travel to Hawaii.

This is the data which was recovered from the messaging packets.

- *Analysing Forensic image.*

To examine the forensic image provided by the local police, I extracted the image in the tool named Autopsy. It was a copy of the original USB drive in a .dd format.



There were multiple files and folders residing in it and each of the folder shows a modified, accessed and created date with time stamps.

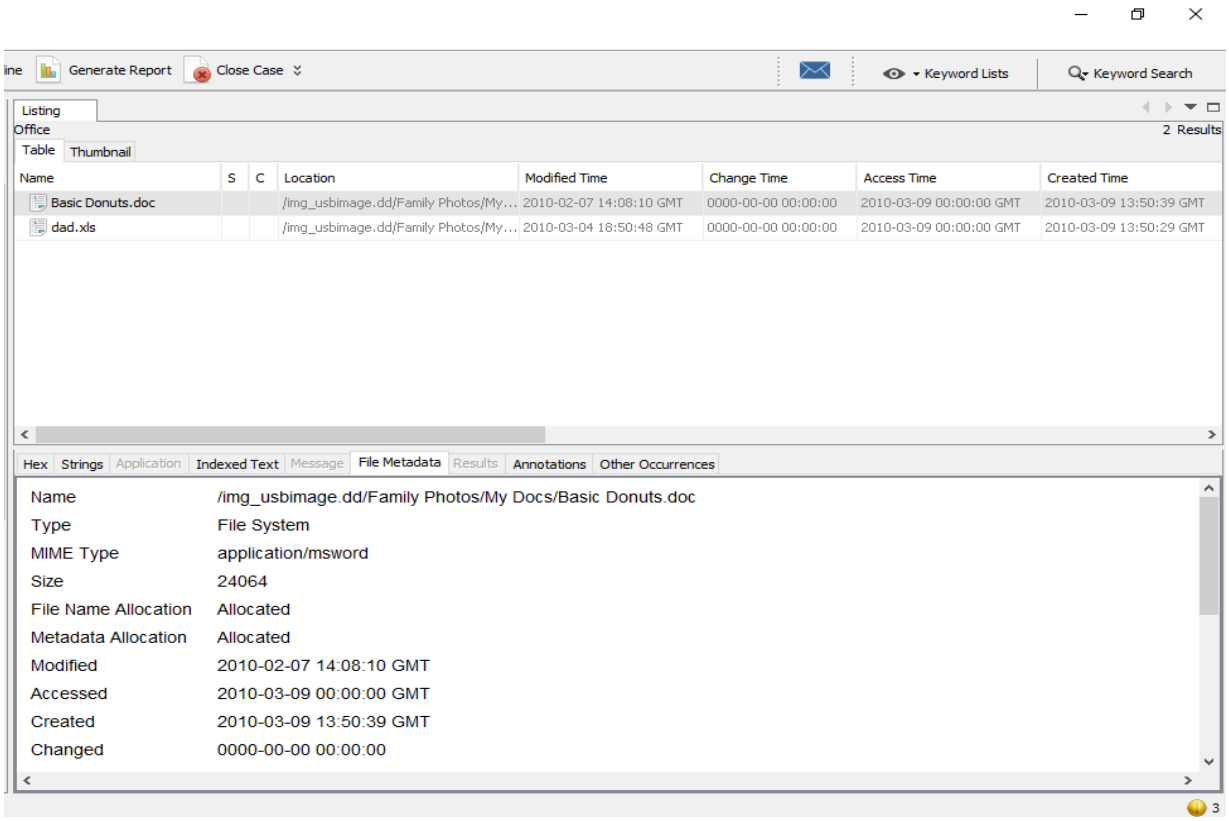
Examining each file and folder, steps were taken to recover the evidence which led to the file consisting a secret recipe which was hidden.

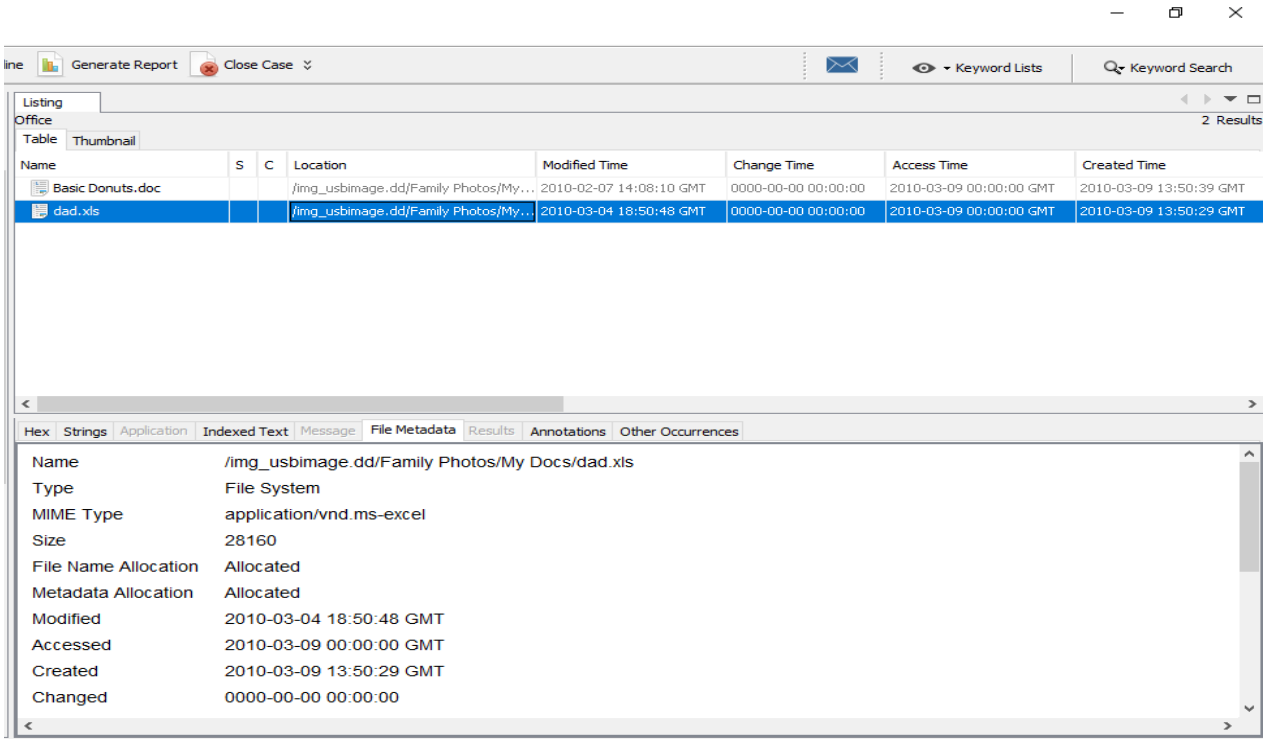
Going through the folders, some family photos were found which may belong to Penelope and also some images of donuts made by the company.

Also, there were four deleted files residing in the image. One file in the deleted section was erased from folder named “hideit”.

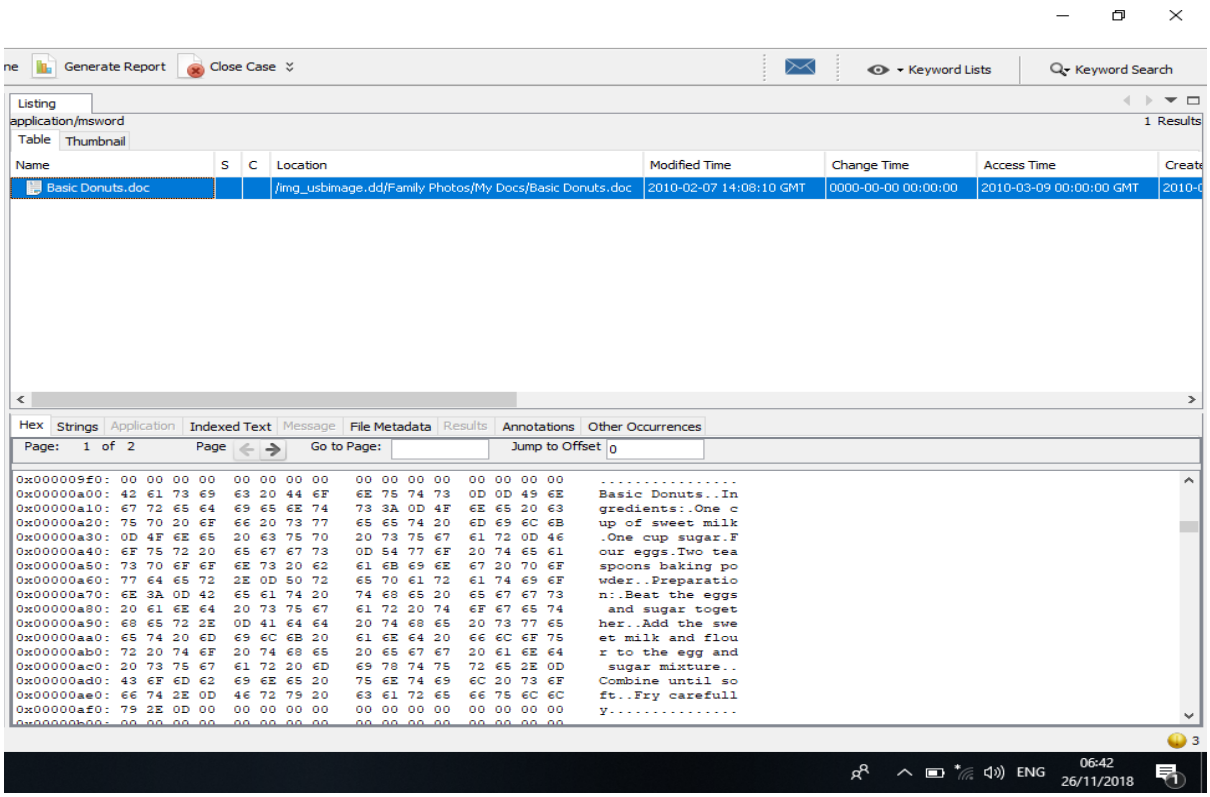
Furthermore, the “hideit” folder consisted of two office files which were named :-

1. BasicDonuts.doc
2. Dad.xls





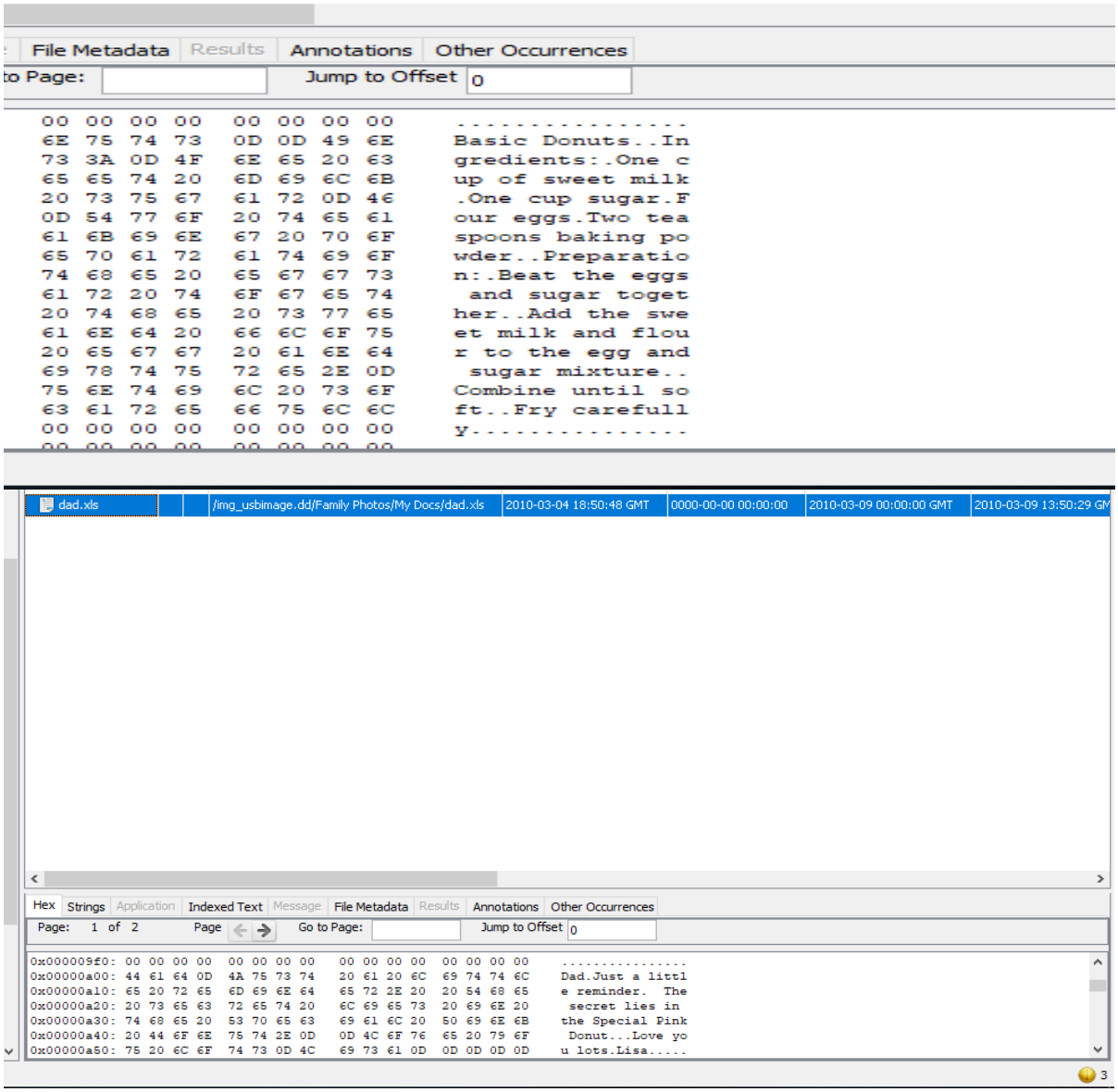
These two files gave the evidence of the secret recipe being leaked and who else was involved.



(BasicDonuts.doc)

- BasicDonuts.doc
- Dad.xls

Examining these files, the decoded ASCII characters of the Hex Content Viewer gave the basic recipe which was used by Lard Lad Donuts company to make donuts.



The file BasicDonuts.doc indicates that there is third person named Lisa who was sending some secret information to someone named dad.

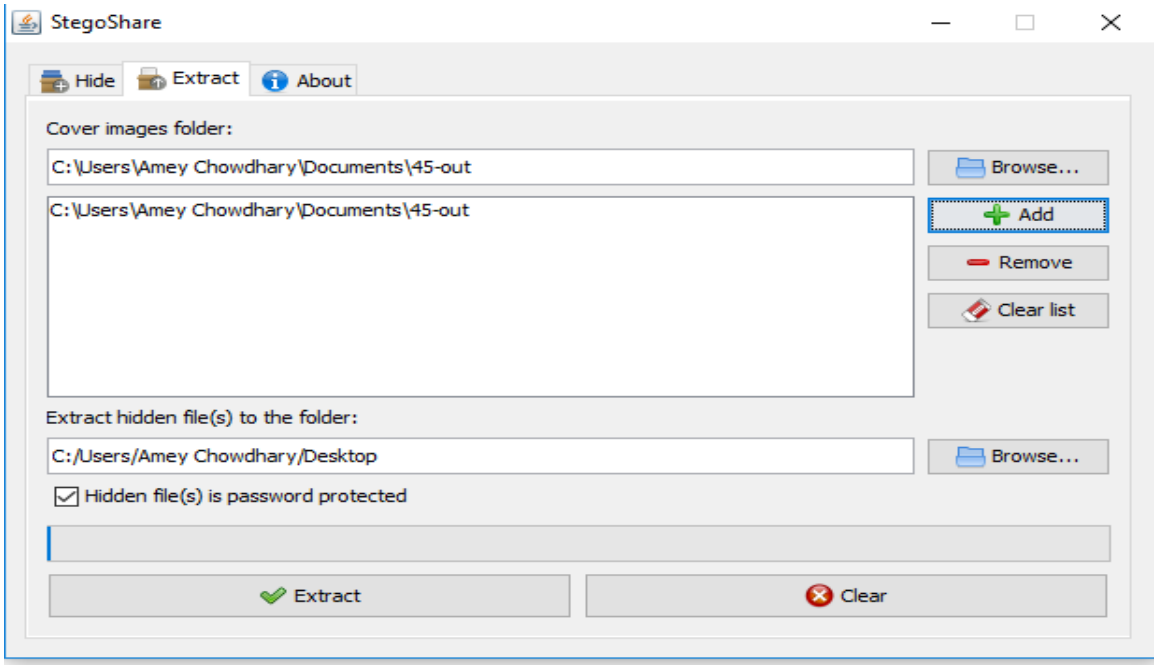
“Dad, just a little reminder. The secret lies in the special pink donut…Love you lots, Lisa.”

Name	S	C	Location	Modified Time	Change Time	Access Time	Created Time
New folder			/img_usbimage.dd/Family Photos/New folder	2010-03-09 13:35:50 GMT	0000-00-00 00:00:00	2010-03-09 00:00:00 GMT	2010-03-09 13:35:
StegoShare.jar			/img_usbimage.dd/Family Photos/hideit/StegoShare.jar	2008-12-08 12:11:08 GMT	0000-00-00 00:00:00	2010-03-09 00:00:00 GMT	2010-03-09 13:48:
New folder			/img_usbimage.dd/Family Photos/My Docs/New folder	2010-03-09 13:39:16 GMT	0000-00-00 00:00:00	2010-03-09 00:00:00 GMT	2010-03-09 13:39:
f0000000.zip			/img_usbimage.dd//$CarvedFiles/f0000000.zip	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:

Analysing the deleted files folder, I extracted all the deleted files in Autopsy where I found the a clue about the location of the file where the secret was.

```
his$0
LMain/Form1;
init>
(LMain/Form1;)V
Code
ctionPerformed
Ljava/awt/event/ActionEvent;)V
tackMapTable
nclosingMethod
java/lang/Exception
An error occured! It may be file error or out of memory exception.
ry to start program with -Xmx512m option (for example, copy StegoShare.jar to the C:\ and type
in the command promt: 'java -jar -Xmx512m C:\StegoShare.jar').
lear
he file was successfully hided in the cover images (cover images dir/out)!
Please do not add or remove any files from the 'out' folder (you can only rename
files and this folder), otherwise it will be imposible to extract hidden file.
peration complete
Error
Main/Form1$1
nnerClasses
java/lang/Object
ava/awt/event/ActionListener
ain/Form1
jProgressBar1
Ljavax/swing/JProgressBar;
LMain/Stego;
ain/Stego
```

The hex viewer shows that the file was hid in the folder cover images dir/out where I found the image file 1.png.



I also found a file name Stego.jar which is a tool for steganography to hide files and send the information. Using this tool, I extracted the hidden file named 1.png which was password protected.

One of the messages in the file BasicDonuts.doc shows that the secret recipe lies in the special pink donut.

This image of the special pink donut gave the clue that the password for extracting the secret recipe is nothing but “donut”.

Honey Duff Donuts

Ingredients:
1 sachet of dry yeast
3 cups of flour
½ cup of warm duff beer
1 x egg, beaten
1 teaspoon of sugar
½ teaspoon of salt
1 tablespoon of oil
Cooking oil
Cinnamon
Honey
Preparation:
Dissolve the yeast in warm duff and combine with other dry ingredients.
Knead for several minutes and leave to one side in a warm place until dough doubles in size.
Roll dough out so it is flat and cut into 1.5 inch squares. Allow to rise for 1 hour.
Heat 4 inches of oil in a Dutch oven.
Drop squares into the oil and cook until they are golden brown.
Strain and dredge in sugar & cinnamon mixture.
Warm honey and drizzle over doughnuts to serve

This is the recovered secret recipe which was hidden in the file 1.png extracted using the tool stego.jar.

Above report recovers all the evidence from the digital image

Conclusions

- The instant messaging packets Exhibit A and Exhibit B proves that Penelope had the secret recipe and she was planning to travel to Hawaii

- The file BasicDonuts.doc proves that the secret recipe is the special pink donut and someone named Lisa and dad was also involved in this.

- The secret recipe was hid in the image file 1.png.

- The steganography tool Stego.jar was used to hide the secret recipe.