Forensic Investigation

Forensic Investigation Overview -

Prepared for: Lard Lad donuts in Springfield
Prepared by: Mohammed Kashem, Forensic Officer at Police Specialist Unit Springfield
CaseNo: Lard Lad donuts, PenelopOlsen
Evidence: USB.EvergreenTerrace.POlsen

CASE BRIEF

Springfield Police Specialist Unit approached Mohammed Kashem - Forensic Officer. To investigate the USB device that was recovered from Ms. Penelope Olsen, a employee of Lard Lad Donuts.

Lard Lad Donuts, believe that Ms.Olsen has stolen the companies high prized assets, the secret recipe for 'Honey Duff Donuts' and Ms. Olsen is a under cover agent working for their competitor. Lard Lad Donuts provided two IM packets that was captured when sending messages over the companies network.

Objective

A brief was supplied to Mohammed Kashem - Forensic Officer with questions to be answered when carrying out the forensic investigation.

1. Find anyone else that is implicated (if so, who?)
2. Where was Ms.Olsen travelling too
3. Find the secret recipe
4. how was this hidden and how it was recovered
5. What steps were taken to hide the evidence

Tools Included

A clean copy of Linux Mint Operating System running on Virtual Box
Autopsy, forensics examination tool from The Sleuth Kit

Investigation

1. Find anyone else is implicated

Found that three people was implicated from the evidence

- Unknown person
- A second person 'Lisa' in a secret message to 'dad', the author of the document appears to be 'Mike'
- Another person is 'dad'

2. Where was Ms. Olsen travelling too

She was planning to travel to **Hawaii**, from the evidence found in the to IM packets (Exhibit B).

3. Find the secret recipe

The secret ingredients was recovered from the USB image drive, this shows the ingredients to the donut recipe.

4. How was the file hidden and how it was recovered

The file was hidden using steganography, a Jar file needed to be executed in order to recover the secret ingredients. This was then protected with a password. The password was recovered instructions from the message to Dad from 'Lisa' This was also hidden using steganography.

5. What steps were taken to hide the evidence
A number of techniques was used to hide the evidence, such as deleting the evidence, hiding evidence in deep within folders, hiding evidence in the same folders with huge numbers of non-important files. There were some duplicates making the process recovering evidence difficult.

Conclusion

From the evidence we found that Lisa is the daughter of Mr H.J. Simpson at 742 Evergreen Terrace.

Investigation Process

In order to start the investigation, the details of the USB was required. Mohammed Kashem - Forensic Officer at Springfield used commands in Terminal such as file, fsstat and fls to get more details about the USB image.

File Type: FAT16 (16 bits)
Smallest cluster size: 4075 [bits] / 4kb
The root of the disk, there were 5 items

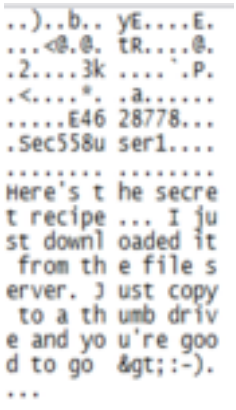
In order to make sure that the disk that was being analysed and maintained integrity, the hash value was used. This was done twice, once in terminal command md5sum and in Autopsy's MD5 function.

`ef3eb472a6338e426e19cfd6266a1b18`

The hash value makes sure no evidence has been changed in anyway, if the data was changed the hash value would change, in this forensic investigation no data was changed and the hash value was the same in both.

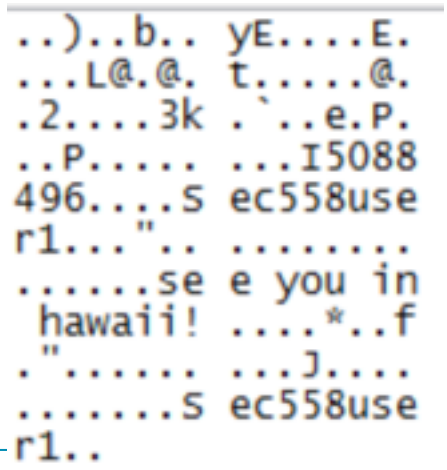
IM packets Investigation

The first priority was to review the given IM packets Exhibits A and B provided by Lard Lad Donuts captured by their company network. The IM packets sent from Ms Olsen's computer IP address, 192.168.1.158. There was an unknown host IP address 64.12.24.50. The detailed message contained is shown below.



Here on the left you can see the secret recipe being transmitted to a unknown person.

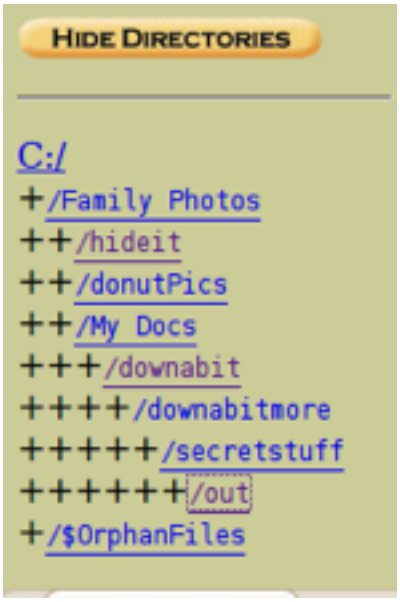
On the right Ms Olsen says to the unknown person, see you in Hawaii. This indicates the two people would meet up Hawaii and Ms.Olsen was planning to travel there.



Investigation of USB Image

This process is the full analysis of the USB image in detail using the tools provided, Autopsy. The evidence from what gathered in Exhibit A and B shows that there is a hidden recipe.

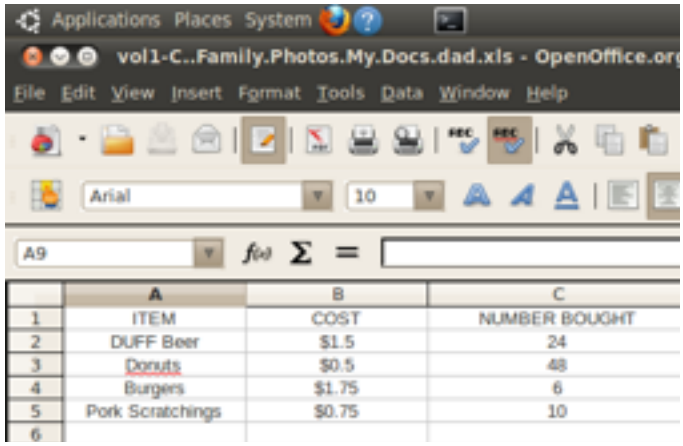
The initial start of the process was to review the USB image and create a timeline.txt from the period of the incident took place. This would then be sorted in timeline of when the incident took place.



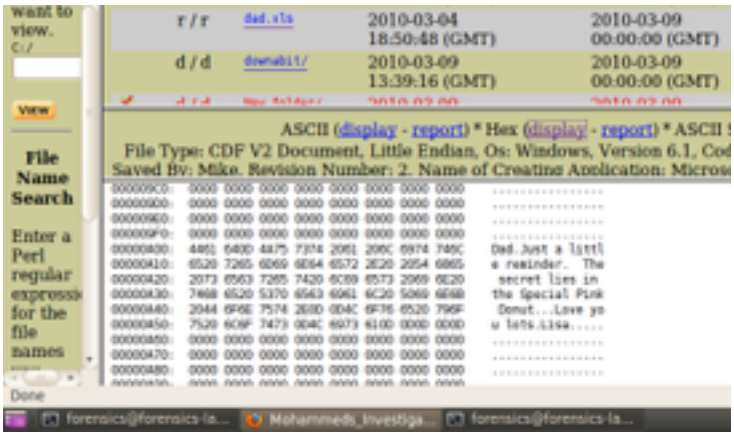
There were some interesting files and folders that was used to hide the evidence, there was one file deleted that was recovered successfully. This was a Jar file. This needed to be executed in order to see how it works. This was a stenography file used to encrypt a file inside a file. This was easy to find as it was hidden in a folder called hideIt. It was a software downloaded from http://stegoshare.sf.net. This allows the user to hide a file inside another image with a password without any user knowing that there is a hidden file inside it.

Another file was buried deep down in multiple-folders, this was an image png file. While exporting the png file, its file size was big. This made sure that something was hidden in the image file.

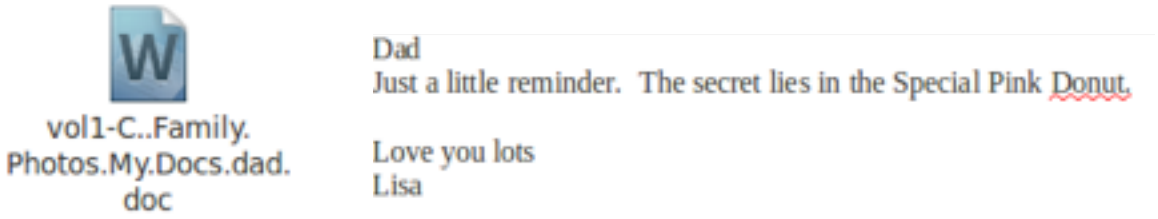
There was a recipe found but this was a basic donuts, this was not the secret recipe. Upon our continuous analysis of the USB image, a .xls file was exported, a message showed to dad from Lisa when viewed in Autopsy but when exported. The file was a excel document containing a list of ingredients. The hidden message was hidden in the file using stenography. The file was changed from **.xls** to **.doc** to view the hidden cryptic message.



The file contained a list of items, when viewed the file in Autopsy it showed a hidden message. Once you changed the file type to .doc the secret cryptic message was able to be read.



This shows there is a message in the excel document.



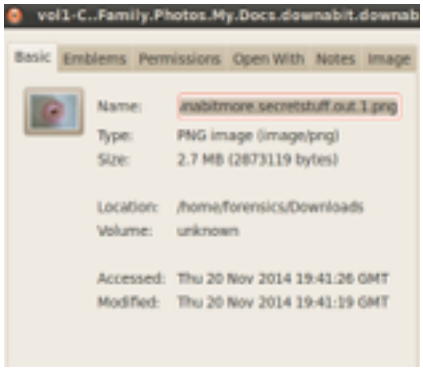
documents Category

C:/Family Photos/My Docs/dad.xls
CDF V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Title: Dad, Author: Mike, Template: Normal, Last Saved By: Mike, Revision Number: 2, Name of Creating Application: Microsoft Office Word, Total Editing Time: 06:00, Create Time/Date: Sat Feb 6 14:12:00 2010, Last Saved Time/Date: Wed Mar 3 16:42:00 2010, Number of Pages: 1, Number of Words: 14, Number of Characters: 82, Security: 0
Image: /var/lib/autopsy/Mohammeds_Investigation/SuspectUSB/images/usbimage.dd Inode: 114184

C:/Family Photos/My Docs/Basic Donuts.doc
CDF V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Title: Basic Donuts, Author: Mike, Template: Normal, Last Saved By: Mike, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Total Editing Time: 01:00, Create Time/Date: Sat Feb 6 14:07:00 2010, Last Saved Time/Date: Sat Feb 6 14:08:00 2010, Number of Pages: 1, Number of Words: 36, Number of Characters: 207, Security: 0
Image: /var/lib/autopsy/Mohammeds_Investigation/SuspectUSB/images/usbimage.dd Inode: 114187

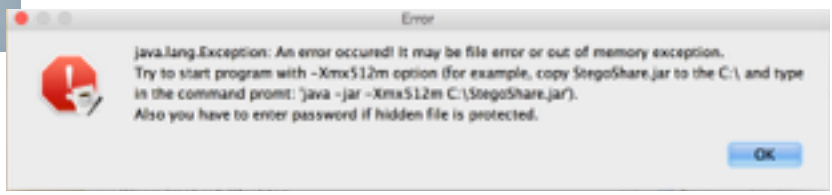
Some of the files was recovered using the 'documents category' function in Autopsy. It gave the locations to the files where it was stored on the USB image. Any files that was changed in different formats.

Finding the secret recipe. The recipe was hidden in a cryptic stenography in a png file. The file was executed in the Jar file that was recovered when deleted. Upon running the file, it required a password.

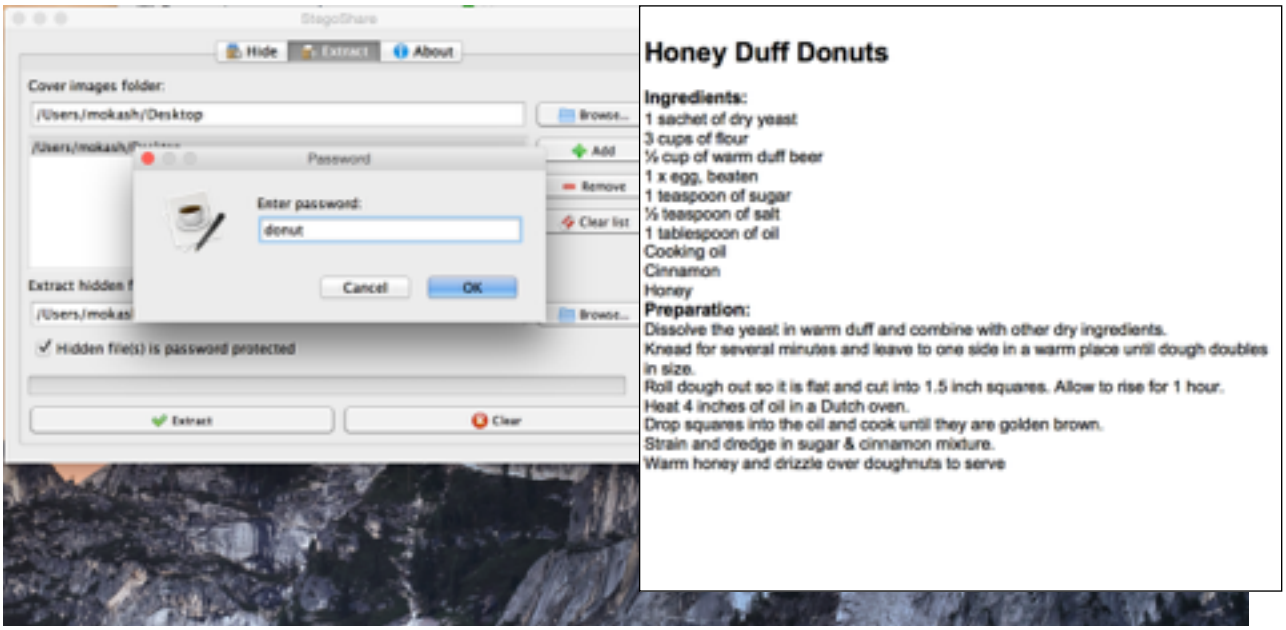


The password was located in the images in the donut folder, there were identical images. The password was found on the 'special pink donut'. The cryptic message that 'Lisa' sent to her 'dad' contained vital information of where the password was located.

These images that was recovered, had identical images. First you won't notice anything different. One of the images had the password to decode the encrypted png image needed to recover the secret ingredient



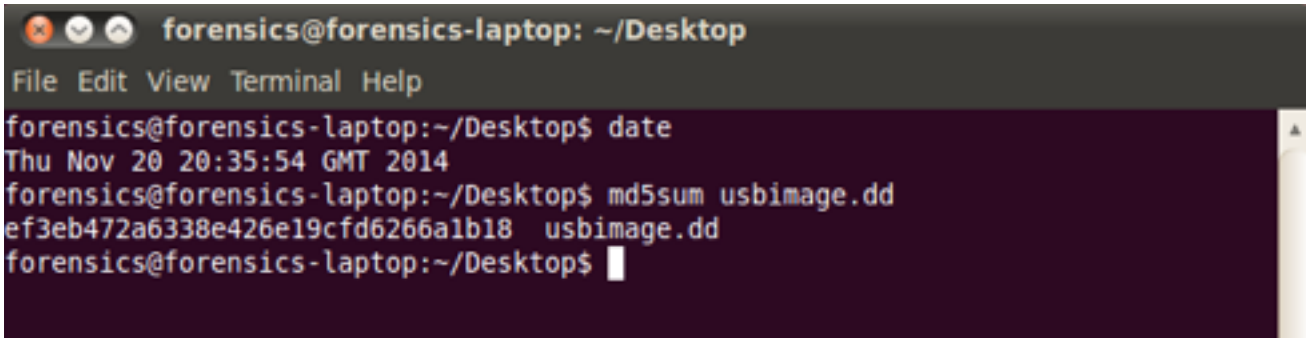
Now the password was recovered we were able to decode the stolen ‘secret recipe’. To decode the ‘secret recipe’ we needed to run the ‘jar’ file and enter the password as donut and extract it to view the secret recipe.



Summary

The secret recipe was recovered successfully using the forensics techniques, Mohammed Kashem - Forensic Officer was able to recover the files.

To make sure the integrity of this investigation report, the hash value was recalculated on 20/11/2014. This shows no data was changed and the hash value is still the same.



Including in the investigation report, you will find the following files:

- Evidence folder[1] - containing all evidence found and duplicates.
- Text files[2] - containing file.txt, fsstat.txt, fls.txt, fls.txt, dirtywords.txt and timeline.txt.

[1] Inside Evidence Folder, folder called Evidence

[2] Inside Evidence Folder, folder called Text_Files