Court Report

CM3111

21050251

Theodor Baur

Content

1 Background and Objectives

1.1 Background

Mrs Mona Simpson (also referred to by her alias Ms. Taurus Smith) is being investigated as her former employer *Lard&land Donuts*, a doughnut making company in Springfield, suspect that Mona Simpson has leaked doughnut recipes to their competitor *Diggity Doughnuts*. *Lard&land Donuts* had been monitoring Mona Simpson's activity but had found nothing suspicious previously.

An unexpected laptop then briefly connected to the *Lard&land Donuts* network, exchanging a number of instant message packets with Mona Simpson's work computer. Instant message packets are small segments of a digital message that are sent across a network. *Lard&land Donuts* then analysed these packets and suspected that they had been involved in a computer misuse attack. At which point the police were called.

The police then conducted an investigation and discovered that her legal name was Mrs Mona Simpson (a wanted woman) and that Taurus Smith (the name she had been known as working at *Lard&land Donuts*) was an alias. The police then conducted a search on her last known address, 742 Evergreen Terrace, where she had lived with her son, Mr H.J Simpson. At this address they found a USB stick containing a system image of a laptop hard drive and a liquid damaged phone. A system image is a snapshot of a devices operating system, such as *Windows* or *Linux*, including installed programs, settings and data.

Succeeding these events, this forensic examination attempted to extract information relevant to the case from the following evidence items:

Exhibit code	File name	Description

Exhibit A	`Exhibit A_Back.jpg`
	`Exhibit A_Front.jpg`
		The liquid damaged phone found at 742 Evergreen Terrace.

Exhibit B	`Exhibit B and Exhibit C.pdf`	A screenshot of a program displaying one of the instant message packets intercepted at *Lard&land Donuts*.
Exhibit C		A screenshot of a program displaying one of the instant message packets intercepted at *Lard&land Donuts*.

Exhibit D	`Exhibit D.pcapng`	A *.pcapng* file containing a number of the instant message packets intercepted at *Lard&land Donuts* (a *.pcapng* file is a file format that is used to record captured packets)
Exhibit E	`Exhibit E.pcapng`	A *.pcapng* file containing a number of the instant message packets intercepted at *Lard&land Donuts*.
Exhibit F	`Taurus Laptop.001`	The USB stick containing a laptop hard drive image found at 742 Evergreen Terrace.

1.2 Objectives

This forensic investigation was conducted with the following objectives:

1. Ensure proper handling of evidence – Any evidence analysed should not be modified in any way, and should have its integrity verified after the investigation. The investigation should follow the Association of Chief Police Officers (ACPO) guidelines.
2. Recovery of any evidence pertaining to the alleged illegal activities of Mrs Mona Simpson – Uncover evidence (if any) pertaining to the alleged computer misuse incident at *Lard&land Donuts*.
3. Identify potential accomplices – Uncover evidence linking other parties to Mrs Mona Simpson's illegal activities (if any exist) and establish the nature of this relationship.
4. Assess Mrs Mona Simpson's future intentions and plans - Uncover any evidence (if any) showing where Mona Simpson plans to travel and what her future plans are.
5. Uncover evidence pertaining to the alleged leaked recipes – Uncover all evidence relating to the *Lard&land Donuts* alleged leaked recipes.
6. Uncover any hidden/deleted user accounts - Uncover all instances of user accounts that may be deleted/hidden.
7. Establish timeline of events

2 Methodology

2.1 Preparation

Firstly, a secure environment was created to perform forensic analysis. This was achieved by using a virtual machine, a simulation of an operating system that can be run on a computer. This operating system works just like a normal operating system, therefore forensic analysis can be performed on it. For this investigation, a virtual machine software called *VMware* was used. Inside *VMware* a *Windows 10* machine and a *Kali Linux* machine were ran. The *Windows 10* machine was the primary machine used to conduct the analysis, whilst the *Kali Linux* machine was used for specialized analysis as the operating system has specialized forensic tools preinstalled.

All pieces of digital evidence, *Exhibit A-F*, had working copies created for analysis, meaning that none of the original media was analysed. These working copies were transferred into the virtual machine.

2.2 Tools

Below shows what tools are installed inside each virtual machine on the forensic workstation.

Forensic workstation	
VMware Workstation 17 Player	
Windows 10	Kali Linux 2023.4
Autopsy 4.21.0	John the Ripper 1.9.0
	Wireshark 4.2.0
	Exiftool 12.70

Manually installed program	Pre-installed program

2.3 Procedure

Analysis was conducted on the network packet files as well as the following areas of the laptop image:

a. Email – Emails sent by users on the laptop

b. Web Activity
    i. History – Websites that the users on the laptop have visited.
    ii. Cookies – Small file downloaded when certain websites are visited, these are used by websites to remember preferences, or data entered into the website.
    iii. Searches – Search queries made using a search engine on a browser. For example, a *Google search*.

c. Chat Logs/Communication Data – Records of chat messages sent by users.

d. Attached Devices – Physical devices that have been connected to the machine, for example a USB stick.

e. Programs Installed

f. Deleted Files – Files that have been deleted by the user can still be recovered.

g. Encrypted Files – Files that have some sort of password-protection preventing anyone from accessing them without the password.

h. EXIF metadata – Data contained inside an image telling us what device and settings were used to take it. For example, the camera model and lens aperture.

i. Registry – Collection of settings and preferences for the *Windows* operating system. It can contain information like the number of users on a machine.

After analysis was conducted, an MD5 and SHA256 check was conducted on each version of each copy of the evidence files to ensure they matched the values recorded in the preparation stage.

2.3.1 Integrity Check

In order to ensure that the working copies were identical to the original media, MD5 and SHA256 hash values for each of the pieces of digital evidence were calculated for the original media (on the forensic workstation) and the working copies (inside the virtual machine). MD5 and SHA256 hash values are values that are computed on a file, two files that have the same MD5 or SHA256 hash are normally identical, and minor changes to any file will result in a very different MD5 or SHA256 hash.

As shown in the table below, both the MD5 hash and the SHA256 hash matches before and after the forensic investigation. This means that the files before and after the investigation are identical, verifying the files have not been altered, modified or tampered with in the process of the investigation.

Evidence	MD5 Hash	SHA256 Hash
Taurus Laptop.001 (pre-investigation)	56aeba1a708c5210c8728e5a2560f9ca	a2f49fa7ce6b111c6e198de2ca4a24a8e73d6d85291805db5bede4d60fab23be
Taurus Laptop.001 (post-investigation)	56aeba1a708c5210c8728e5a2560f9ca	a2f49fa7ce6b111c6e198de2ca4a24a8e73d6d85291805db5bede4d60fab23be
Exhibit A_Back.jpg (pre-investigation)	480252b5de825054fb918cb08bb7030e	5290f3d34b9b8b37a608c4f51781ae324e9d9c39db9162557010005d01614854
Exhibit A_Back.jpg (post-investigation)	480252b5de825054fb918cb08bb7030e	5290f3d34b9b8b37a608c4f51781ae324e9d9c39db9162557010005d01614854
Exhibit A_Front.jpg (pre-investigation)	321009e97b88f3178106ef2275f7ed19	164a764b6386e7f4a04301048b6f5d962195193a61bc4b95750f7def3d8d2f8e
Exhibit A_Front.jpg (post-investigation)	321009e97b88f3178106ef2275f7ed19	164a764b6386e7f4a04301048b6f5d962195193a61bc4b95750f7def3d8d2f8e
Exhibit B and Exhibit C.pdf (pre-investigation)	3a4ab9eba38ef8244cfaa44eec392a3e	c6760229562f8c2bb47be38b90877624a72d89151dbaf5de108e73b5c9a7153f
Exhibit B and Exhibit C.pdf (post-investigation windows)	3a4ab9eba38ef8244cfaa44eec392a3e	c6760229562f8c2bb47be38b90877624a72d89151dbaf5de108e73b5c9a7153f
Exhibit B and Exhibit C.pdf (post-investigation linux)	3a4ab9eba38ef8244cfaa44eec392a3e	c6760229562f8c2bb47be38b90877624a72d89151dbaf5de108e73b5c9a7153f
Exhibit D.pcapng (pre-investigation)	251a1a9a8284397a70d06cadd1a5bfa6	8f4b221f715c216d55b13089d325bec45ae5f4c143484bd0ad5c5c2d38f12292
Exhibit D.pcapng (post-investigation windows)	251a1a9a8284397a70d06cadd1a5bfa6	8f4b221f715c216d55b13089d325bec45ae5f4c143484bd0ad5c5c2d38f12292
Exhibit D.pcapng (post-investigation linux)	251a1a9a8284397a70d06cadd1a5bfa6	8f4b221f715c216d55b13089d325bec45ae5f4c143484bd0ad5c5c2d38f12292
Exhibit E.pcapng (pre-investigation)	756f6afcc9e40556947905ad0824b708	72359088a569ca213e92c79390a2fcebe0869c67073aae828d20f85cf76ae2ba
Exhibit E.pcapng (post-investigation windows)	756f6afcc9e40556947905ad0824b708	72359088a569ca213e92c79390a2fcebe0869c67073aae828d20f85cf76ae2ba
Exhibit E.pcapng (post-investigation linux)	756f6afcc9e40556947905ad0824b708	72359088a569ca213e92c79390a2fcebe0869c67073aae828d20f85cf76ae2ba

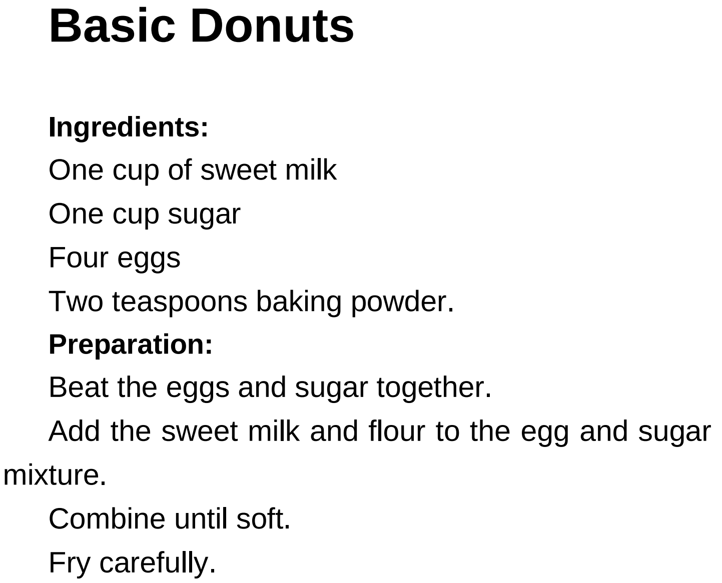
3 Findings and Results

3.1 Recipes

Four recipes were found with various concealing techniques applied to them another one was found with no attempt to conceal it, and a final one was found but the contents were unrecoverable.

3.1.1 Basic Donuts

A recipe was found in the *Family Photos* folder inside a subfolder *My Docs* inside a .doc file (a type of document file) containing the recipe for "Basic Donuts":

File Name	`Basic Donuts.doc`
File Path	`/img_Taurus Laptop.001/vol_vol2/Family Photos/My Docs/Basic Donuts.doc`
Hash Value (MD5)	`b4ffc53f767f121ef1d8914d46540cf0`
Modified	`2010-03-04 13:35:24 GMT`
Accessed	`2010-03-07 00:00:00 GMT`
Created	`2010-03-04 00:06:49 GMT`
MIME Type	`application/msword`
Content	 **Basic Donuts** **Ingredients:** One cup of sweet milk One cup sugar Four eggs Two teaspoons baking powder. **Preparation:** Beat the eggs and sugar together. Add the sweet milk and flour to the egg and sugar mixture. Combine until soft. Fry carefully.

It is unclear whether this doughnut recipe originated from *Lard&Land Doughnuts* or not as it does just appear to be a very simple recipe for a standard doughnut that can be found online. A person called "Mike" was found to be the author of this inside the file metadata, potentially implicating this person if the recipe is indeed a private *Lard&Land Doughnuts* recipe and found to have been sent around with knowledge of its secrecy. This file was created, modified, and accessed at a time period of relevance to the investigation.

3.1.2 Ring Recipe

A deleted file called *ring recipe.txt.sb-ace39f49-PiYykM* could potentially contain a doughnut recipe inside its contents, therefore has the potential to be of significant interest, however no such recipe could be recovered. One word, “method”, was able to be extracted from the contents. The files name itself would suggest that at some point it could have contained a doughnut recipe, the contents also suggest that it might have contained a recipe.

File Name	`ring recipe.txt.sb-ace39f49-PiYykM`
File Path	`/img_Taurus Laptop.001/vol_vol2/Documents and Settings/Taurus Smith/Desktop/ring recipe.txt.sb-ace39f49-PiYykM`
Hash Value (MD5)	`d88d6b11e3a615b557264440515ce772`
Modified	`2022-11-06 10:58:50 GMT`
Accessed	`2010-03-31 00:00:00 BST`
Created	`2010-03-31 19:55:14 BST`
MIME Type	`application/octet-stream`
Content	`method`

3.1.3 Method 1: Deleted Emails and Steganography

The laptop image contains the deleted email file shown below:

File Name	`Important email.eml`
File Path	`/img_Taurus Laptop.001/vol_vol2/Family Photos/Important email.eml`
Hash Value (MD5)	`a0dc0b235a4e35b123a78bd1a2ce5bee`
Modified	`2010-03-04 10:43:50 UTC`
Accessed	`2022-03-08 00:00:00 UTC`
Created	`2022-03-08 00:13:38 UTC`
MIME Type	`message/rfc822`

Content	X-Account-Key: account3 Return-Path: <useram@domaingal.com> Received: from cluster.serviceorg.com (cluster.serviceorg.com [10.213.4.42]) by mail.serviceorg.com (8.12.11.20100614/8.12.11) with ESMTP id kARABqg0023308 for <userpf@domaingal.com>; Thu, 04 Mar 2010 11:11:54 +0100 Received: from cluster.serviceorg.com (localhost.localdomain [127.0.0.1]) by localhost.serviceorg.com (Postfix) with ESMTP id 30C6248047 for <userpf@domaingal.com>; Thu, 04 Mar 2010 11:11:52 +0100 (CET) Received: from spiderwall.localdomain (gateway-gal.domaingal.com [10.10.254.4])by cluster.serviceorg.com (Postfix) with SMTP id 5530848056for <userpf@domaingal.com>; Thu, 04 Mar 2010 11:11:48 +0100 (CET) Received: (qmail 27268 invoked from network); 27 Nov 2010 10:11:48 -0000 Received: from pc-seg.dominio.locale (HELO PCSEG) (10.10.0.100) by 12.45.87.123 with SMTP; 27 Nov 2010 10:11:47 -0000 Message-ID: <002601c7120c$7220d3d0$6400670a@dominio.locale> From: "name surname" <useram@domaingal.com> To: <destuser@domaingal.com> Subject: determ- iter Date: Thu, 04 Mar 2010 11:11:46 +0100 MIME-Version: 1.0 Content-Type: multipart/alternative; boundary="----=_NextPart_000_0023_01C71214.D3D49A00" X-Priority: 3 X-MSMail-Priority: Normal X-Mailer: Microsoft Outlook Express 6.00.2900.2869 X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2962 X-imss-version: 2.044 X-imss-result: Passed X-imss-scanInfo: M:P L:E SM:0 X-imss-tmaseResult: TT:0 TS:0.0000 TC:00 TRN:0 TV:3.6.1039(14838.003)

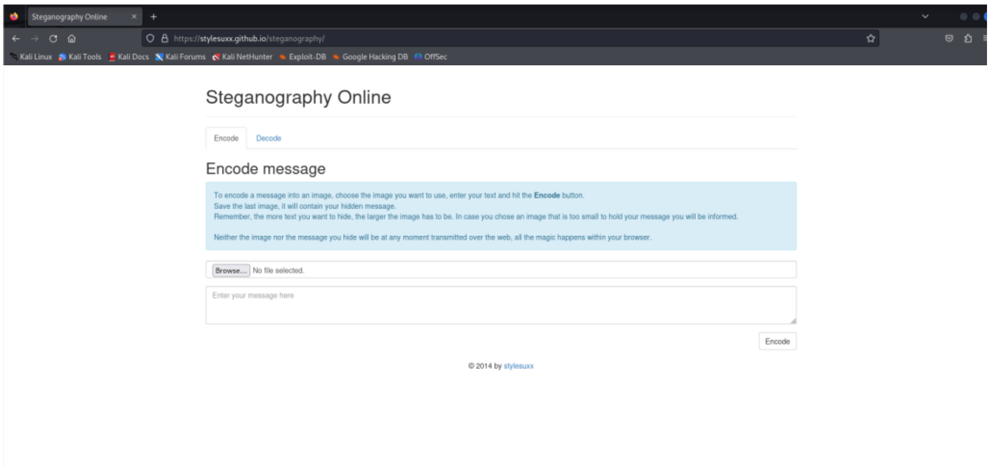
	X-imss-scores: Clean:64.23839 C:2 M:3 S:5 R:5 X-imss-settings: Baseline:1 C:4 M:4 S:4 R:4 (0.0000 0.0000) X-Scanned-By: MIMEDefang 2.54 on 10.213.4.47 VGhpcyBpcyBhIG11bHRpLXBhcnQgbWVzc2FnZSBpbiBNSU1FIGZvcm 1hdC4KCi0tLS0tLT1fTmV4dFBhcnRfMDAwXzAwMjNfMDFDNzEyMTQu RDNENDlBMDAKQ29udGVudC1UeXBlOiB0ZXh0L3BsYWluOwoJY2hhcn NldD0iaXNvLTg4NTktMSIKQ29udGVudC1UcmFuc2Zlci1FbmNvZGlu ZzogcXVvdGVkLXByaW50YWJsZQoKUGxlYXNlIGdvIHRvIHRoZSB3ZW JzaXRlIGFuZCBkZWNvZGUgdGhlIHR3byBwbmcgZmlsZXMsIHlvdSB3 aWxsIHNlZSB0aGUgZGV0YWlsczogaHR0cHM6Ly9zdHlsZXN1eHguZ2 l0aHViLmlvL3N0ZWdhbm9ncmFwaHkvCgotLS0tLS09X05leHRQYXJ0 XzAwMF8wMDIzXzAxQzcxMjE0LkQzRDQ5QTAwCkNvbnRlbnQtVHlwZT ogdGV4dC9odG1sOwoJY2hhcnNldD0iaXNvLTg4NTktMSIKQ29udGVu dC1UcmFuc2Zlci1FbmNvZGluZzogcXVvdGVkLXByaW50YWJsZQoKPC FET0NUWVBFIEhUTUwgUFVCTElDICItLy9XM0MvL0RURCBIVE1MIDQu MCBUcmFuc2l0aW9uYWwvL0VOIj4KPEhUTUw+PEhFQUQ+CjxNRVRBIG h0dHAtZXF1aXY9M0RDb250ZW50LVR5cGUgY29udGVudD0zRCJ0ZXh0 L2h0bWw7ID0KY2hhcnNldD0zRGlzby04ODU5LTEiPgo8TUVUQSBjb2 50ZW50PTNEIk1TSFRNTCA2LjAwLjI5MDAuMjk2MyIgbmFtZT0zREdF TkVSQVRPUj4KPFNUWUxFPjwvU1RZTEU+CjwvSEVBRD4KPEJPRFkgYm dDb2xvcj0zRCNmZmZmZmY+CkhlcmUgdGhlcmUgaXMgaHRtbCBjb250 ZW50CjwvQk9EWT48L0hUTUw+CgotLS0tLS09X05leHRQYXJ0XzAwMF 8wMDIzXzAxQzcxMjE0LkQzRDQ5QTAwLS0=------ =_NextPart_000_0023_01C71214.D3D49A00-- Expected Results: you need to decode the contents.

Inside the contents section of the email, highlighted in yellow is a *Base64* encoded message, and below it is a message "you need to decode the contents". *Base64* encoding in this context is a method of converting a string of letters into a coded message that needs to be decoded to read. When decoded the message appears as follows:

Encoded	VGhpcyBpcyBhIG11bHRpLXBhcnQgbWVzc2FnZSBpbiBNSU1FIGZvcm1h dC4KCi0tLS0tLT1fTmV4dFBhcnRfMDAwXzAwMjNfMDFDNzEyMTQuRDNE NDlBMDAKQ29udGVudC1UeXBlOiB0ZXh0L3BsYWluOwoJY2hhcnNldD0i aXNvLTg4NTktMSIKQ29udGVudC1UcmFuc2Zlci1FbmNvZGluZzogcXVv dGVkLXByaW50YWJsZQoKUGxlYXNlIGdvIHRvIHRoZSB3ZWJzaXRlIGFu ZCBkZWNvZGUgdGhlIHR3byBwbmcgZmlsZXMsIHlvdSB3aWxsIHNlZSB0 aGUgZGV0YWlsczogaHR0cHM6Ly9zdHlsZXN1eHguZ2l0aHViLmlvL3N0 ZWdhbm9ncmFwaHkvCgotLS0tLS09X05leHRQYXJ0XzAwMF8wMDIzXzAx QzcxMjE0LkQzRDQ5QTAwCkNvbnRlbnQtVHlwZTogdGV4dC9odG1sOwoJ Y2hhcnNldD0iaXNvLTg4NTktMSIKQ29udGVudC1UcmFuc2Zlci1FbmNv ZGluZzogcXVvdGVkLXByaW50YWJsZQoKPCFET0NUWVBFIEhUTUwgUFVC TElDICItLy9XM0MvL0RURCBIVE1MIDQuMCBUcmFuc2l0aW9uYWwvL0VO Ij4KPEhUTUw+PEhFQUQ+CjxNRVRBIGh0dHAtZXF1aXY9M0RDb250ZW50 LVR5cGUgY29udGVudD0zRCJ0ZXh0L2h0bWw7ID0KY2hhcnNldD0zRGlz by04ODU5LTEiPgo8TUVUQSBjb250ZW50PTNEIk1TSFRNTCA2LjAwLjI5 MDAuMjk2MyIgbmFtZT0zREdFTkVSQVRPUj4KPFNUWUxFPjwvU1RZTEU+

	CjwvSEVBRD4KPEJPRFkgYmdDb2xvcj0zRCNmZmZmZmY+CkhlcmUgdGhl cmUgaXMgaHRtbCBjb250ZW50CjwvQk9EWT48L0hUTUw+CgotLS0tLS09 X05leHRQYXJ0XzAwMF8wMDIzXzAxQzcxMjE0LkQzRDQ5QTAwLS0=
Decoded	This is a multi-part message in MIME format. ------=_NextPart_000_0023_01C71214.D3D49A00 Content-Type: text/plain; charset="iso-8859-1" Content-Transfer-Encoding: quoted-printable Please go to the website and decode the two png files, you will see the details: https://stylesuxx.github.io/steganography/ ------=_NextPart_000_0023_01C71214.D3D49A00 Content-Type: text/html; charset="iso-8859-1" Content-Transfer-Encoding: quoted-printable <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"> <HTML><HEAD> <META http-equiv=3DContent-Type content=3D"text/html; = charset=3Diso-8859-1"> <META content=3D"MSHTML 6.00.2900.2963" name=3DGENERATOR> <STYLE></STYLE> </HEAD> <BODY bgColor=3D#ffffff> Here there is html content </BODY></HTML> ------=_NextPart_000_0023_01C71214.D3D49A00--

The decoded message contains a link (highlighted in yellow) to a website called *Steganography Online* pictured below and indicates that the recipient has 2 .png files that need to be decoded using the website. The term steganography refers to the technique of hiding data within an ordinary, non-secret file or message to avoid detection. In most cases this is an image, video, or audio file. A .png file refers to a common type of image file.



Steganography Online

Encode message

To encode a message into an image, choose the image you want to use, enter your text and hit the **Encode** button.
Save the last image, it will contain your hidden message.
Remember, the more text you want to hide, the larger the image has to be. In case you chose an image that is too small to hold your message you will be informed.

Neither the image nor the message you hide will be at any moment transmitted over the web, all the magic happens within your browser.

No file selected.

Enter your message here

© 2014 by stylesuxx

The website allows users to upload their own .png image files and uses steganography to encode a message into the .png files or decode an already encoded message from an uploaded .png file.

Using *Autopsy* two files that contain the .png MIME type can be found without the .png file extension. A MIME type in this context is a label used to identify the filetype of a certain file, and a file extension refers to the suffix after the "." in a file name. For example, in "image.png" the underlined part is the file extension. File extensions are also used to indicated the filetype of a file but they can be modified manually. The two files mentioned are shown below:

File Name	`file.dat`
File Path	`/img_Taurus Laptop.001/vol_vol2/My Shared Folder/file.dat`
Hash Value (MD5)	`a91d377ba346b0363a3c31fd4eaabd37`
Modified	`2010-02-02 12:02:26 UTC`
Accessed	`2010-03-08 00:00:00 UTC`
Created	`2010-01-03 00:16:20 UTC`
MIME Type	`image/png`

Content	

File Name	`stdlidd.inc`
File Path	`/img_Taurus Laptop.001/vol_vol2/My Shared Folder/stdlidd.inc`
Hash Value (MD5)	`f0440dd15ce0d70c0148ee7fdd83f208`
Modified	`2010-02-02 12:02:26 UTC`
Accessed	`2010-03-08 00:00:00 UTC`
Created	`2010-01-03 00:16:20 UTC`
MIME Type	`image/png`
Content	

These files contain the file extension .dat and .inc respectively however possess the MIME type as a .png. When these files are uploaded to https://stylesuxx.github.io/steganography/ and decoded using *Steganography Online's* decode method, the following recipes can be found:

```
file.dat
```

```
Ingredients


    2 2/3 cups (319g( unbleached all-purpose flour
    1 1/2 tsp baking powder
```

1/4 tsp baking soda
3/4 tsp salt
1/4 cup (56g) unsalted butter , melted
1/4 cup (55ml) vegetable oil
3/4 cup + 2 Tbsp (180g) granulated sugar
Seeds of 1 vanilla bean
2 large eggs
2 tsp vanilla extract
1 cup (235ml) milk
Softened butter , for tins

Glaze

1 1/2 cups (180g) powdered sugar
3 Tbsp (42g) unsalted butter , melted
1 tsp vanilla extract
1 small pinch salt
2 - 3 Tbsp milk
Food coloring and sprinkles (optional)

Instructions

Preheat oven to 425 degrees. Butter 14 holes of three doughnut tins and set aside. In a mixing bowl, whisk together flour, baking powder, baking soda and salt for 30 seconds, set aside.

In a separate mixing bowl, using an electric hand mixer, blend together melted butter, vegetable oil, sugar and vanilla bean seeds until smooth, about 1 minute. Blend in eggs one at a time then mix in vanilla extract.

Working in three separate batches, beginning and ending with flour mixture, add 1/3 of the flour mixture alternating with half of the milk and mix just until combined after each addition. Spoon batter into buttered doughnut wells, filling them about 1/4-inch from the rim.

Bake in preheated oven 7 - 8 minutes, or until toothpick inserted into doughnut comes out clean. Transfer to a wire rack to cool until lukewarm then dip in glaze and return to wire rack, immediately top with sprinkles if using and allow glaze to set at room temperature.

For the glaze:

In a flat bottomed bowl, whisk together powdered sugar, melted butter, vanilla and salt then stir in 2 Tbsp of milk, adding additional milk 1 tsp at a time to reach desired consistency and whisk until smooth. Tint with food coloring if desired.

Warm in microwave in 6 - 10 second intervals on HIGH power to warm as it begins to set while dipping doughnuts, as needed, whisking after heating.

stdlidd.inc

Ingredients

2 1/4 cups (320g) all-purpose flour (scoop and level to measure)
2 tsp baking powder
3/4 tsp salt
2/3 cup (140g) granulated sugar
1/4 cup (57g) unsalted butter, softened

```
    1/4 cup (60ml) vegetable oil or canola oil
    2 large eggs
    1 tsp real coconut extract
    1/2 tsp vanilla extract
    1 cup (235ml) canned light coconut milk
    1 Tbsp lemon juice

Glaze and topping

    1 1/2 cups (177g) powdered sugar
    3 Tbsp (45ml) milk, or as needed
    1 1/2 Tbsp (21g) salted butter, melted
    1/2 tsp real coconut extract
    3/4 cup (56g) finely shredded coconut, toasted or untoasted

Instructions

    Preheat oven to 400 degrees.
    In a mixing bowl whisk together flour, baking powder and salt for 20 seconds, set aside.
    In the bowl of an electric stand mixer fitted with the paddle attachment blend together
butter and sugar then mix in vegetable oil.
    Mix in one egg then mix in second egg, coconut extract, and vanilla extract.
    Add in 1/3 of the flour mixture then mix on low until combined, mix in 1/2 of the coconut
milk and the lemon juice.
    Mix in another 1/3 of the flour mixture followed by remaining 1/2 of the coconut milk. Mix
in last 1/3 of the flour, fold batter with a rubber spatula to ensure it's evenly incorporated.
    Spray donut pans with non-stick baking spray. Transfer batter to a gallon size resealable
bag.
    Cut a small corner from bag and pipe batter into donut pans, coming about 1/3-inch from the
top.
    Bake in preheated oven until donuts are set, about 8 - 11 minutes. Let cool in pan for about
3 minutes then invert onto a wire rack to cool.
    For the glaze, in a medium mixing bowl whisk together powdered sugar, milk, butter and
coconut extract until smooth.
    Place coconut in a bowl. Dip cooled donuts in glaze then let excess run off and dip glazed
portion in coconut.
    Return to wire rack to let glaze set. Store donuts in an airtight container at room
temperature.
    AD
    Recipe source: Cooking Classy
```

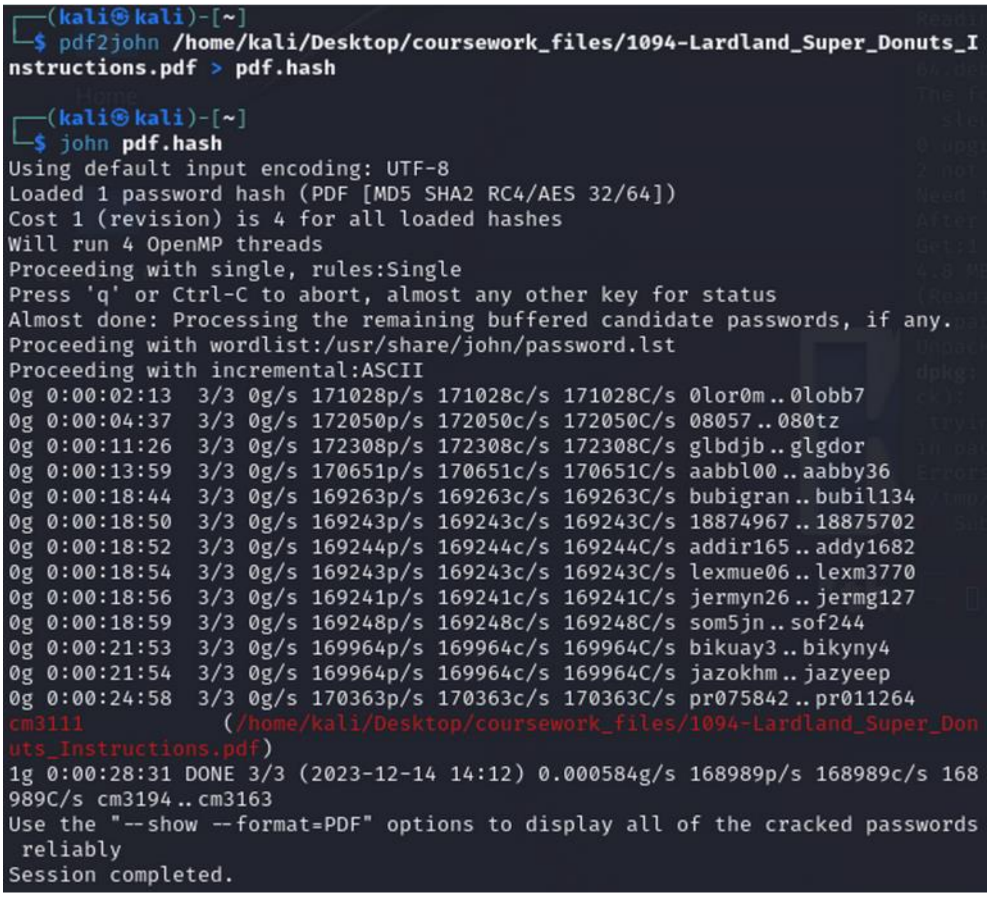
These recipes appear to be intentionally hidden inside the image. In addition the initial email that instructs the recipient to use *Steganography Online* appears to have its instructions intentionally hidden (encoded in *Base64*), and the initial email has been deleted from the laptop. This could imply that a party involved in either the sending or receiving of these recipes is intentionally trying to hide both the recipes, the method to decode the recipes, and the fact that these recipes have been encoded in the first place.

3.1.4 Method 2: Decrypting Password Protected Files

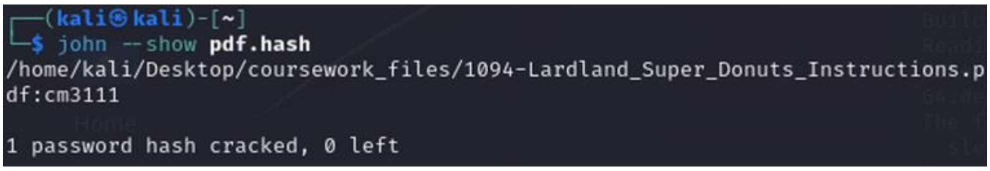
A password-protected file named *Lardland Super Donuts Instructions.pdf* can be found on the laptop image in the location:

```
/img_Taurus Laptop.001/vol_vol2/Documents and Settings/Bilbo
Baggins/My Documents/Lardland Super Donuts Instructions.pdf
```

After running the tool *John the Ripper*, a password cracking tool which contains the functionality to crack a .pdf file, for 28 minutes and 58 seconds the password was found to be “cm3111” as pictured below.

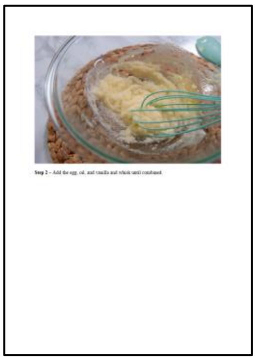
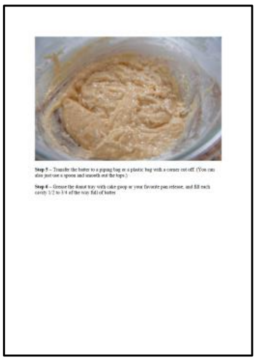
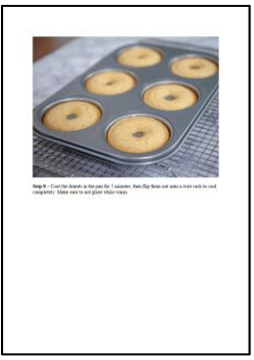


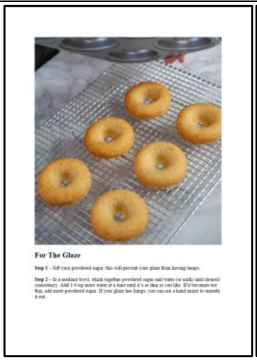
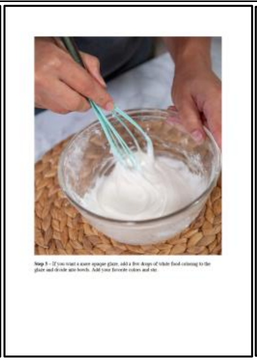
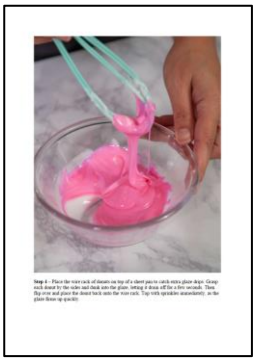
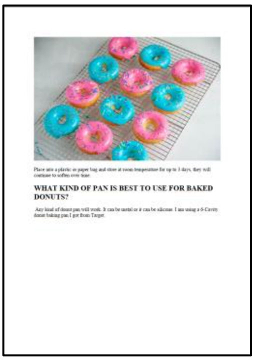
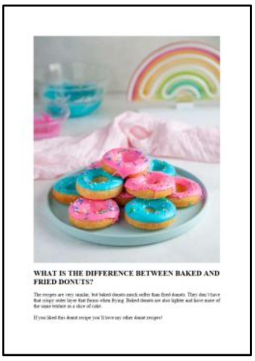
```
┌──(kali㉿kali)-[~]
└─$ pdf2john /home/kali/Desktop/coursework_files/1094-Lardland_Super_Donuts_I
nstructions.pdf > pdf.hash

┌──(kali㉿kali)-[~]
└─$ john pdf.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/64])
Cost 1 (revision) is 4 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
0g 0:00:02:13  3/3 0g/s 171028p/s 171028c/s 171028C/s 0lor0m..0lobb7
0g 0:00:04:37  3/3 0g/s 172050p/s 172050c/s 172050C/s 08057..080tz
0g 0:00:11:26  3/3 0g/s 172308p/s 172308c/s 172308C/s glbdjb..glgdor
0g 0:00:13:59  3/3 0g/s 170651p/s 170651c/s 170651C/s aabbl00..aabby36
0g 0:00:18:44  3/3 0g/s 169263p/s 169263c/s 169263C/s bubigran..bubil134
0g 0:00:18:50  3/3 0g/s 169243p/s 169243c/s 169243C/s 18874967..18875702
0g 0:00:18:52  3/3 0g/s 169244p/s 169244c/s 169244C/s addir165..addy1682
0g 0:00:18:54  3/3 0g/s 169243p/s 169243c/s 169243C/s lexmue06..lexm3770
0g 0:00:18:56  3/3 0g/s 169241p/s 169241c/s 169241C/s jermyn26..jermg127
0g 0:00:18:59  3/3 0g/s 169248p/s 169248c/s 169248C/s som5jn..sof244
0g 0:00:21:53  3/3 0g/s 169964p/s 169964c/s 169964C/s bikuay3..bikyny4
0g 0:00:21:54  3/3 0g/s 169964p/s 169964c/s 169964C/s jazokhm..jazyeep
0g 0:00:24:58  3/3 0g/s 170363p/s 170363c/s 170363C/s pr075842..pr011264
cm3111           (/home/kali/Desktop/coursework_files/1094-Lardland_Super_Don
uts_Instructions.pdf)
1g 0:00:28:31 DONE 3/3 (2023-12-14 14:12) 0.000584g/s 168989p/s 168989c/s 168
989C/s cm3194..cm3163
Use the "--show --format=PDF" options to display all of the cracked passwords
 reliably
Session completed.
```



```
┌──(kali㉿kali)-[~]
└─$ john --show pdf.hash
/home/kali/Desktop/coursework_files/1094-Lardland_Super_Donuts_Instructions.p
df:cm3111

1 password hash cracked, 0 left
```

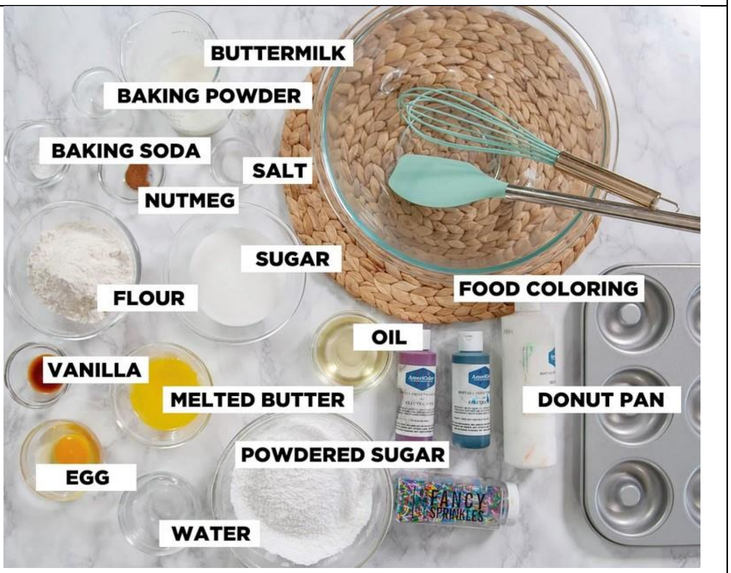
The contents of the password protected file appears to be a baked doughnut recipe:

File Name	`Lardland Super Donuts Instructions.pdf`
File Path	`/img_Taurus Laptop.001/vol_vol2/Documents and Settings/Bilbo Baggins/My Documents/Lardland Super Donuts Instructions.pdf`
Hash Value (MD5)	`66c0fd2bd4412be556df100b22d09647`
Modified	`2005-01-01 18:50:02 UTC`
Accessed	`2010-03-07 00:00:00 UTC`
Created	`2004-03-08 00:17:47 UTC`
MIME Type	`application/pdf`
Content	 A soft and tender baked donut recipe that only takes 15 minutes! These donuts are extremely easy to make, taste just like a piece of cake and look adorable with a bright colored glaze and fun sprinkles. Perfect for birthdays, a weekend treat or even a wedding, these donuts can be customized to be any flavor you like. Add some pumpkin puree and a cream cheese frosting, or some rosemary and a lemon glaze to make your favorite donut. No need to break out the deep fryer or fancy mixer for this recipe, all you'll need is a donut pan and a whisk. **BAKED DONUT INGREDIENTS** This recipe is adapted from my white velvet buttermilk cake. The main difference is the mixing, with donuts there is no special method. You will need some food coloring if you plan on coloring your glaze, and white food coloring to make the glaze more opaque. Don't forget the donut pan! BUTTERMILK BAKING POWDER BAKING SODA SALT NUTMEG SUGAR FLOUR FOOD COLORING OIL VANILLA MELTED BUTTER DONUT PAN POWDERED SUGAR EGG WATER **BAKED DONUT RECIPE STEP-BY-STEP** **Step 1** – Place the sugar and melted butter in a large bowl and combine with a whisk until it's smooth.  **Step 2** – Add the egg, oil, and vanilla and whisk until combined. **Step 3** – In a separate medium bowl, add the flour, baking powder, baking soda, nutmeg, and salt. Mix to gently combine. **Step 4** – Add half the dry mixture into the wet mixture, whisk gently until some of the flour remains, then add all the buttermilk, mix a little, and add the rest of the flour. *Mix until just combined, do not over mix. The batter will be very wet and there will be a few lumps.*  **Step 5** – Transfer the batter to a piping bag or a plastic bag with a corner cut off. (You can also just use a spoon and smooth out the tops.) **Step 6** – Grease the donut tray with cake goop or your favorite pan release, and fill each cavity 1/2 to 3/4 of the way full of batter. **Step 7** – Bake at 450°F (232°C) for 7-9 minutes. When the tops are firm and bounce back when you touch them, they're done.  **Step 8** – Cool the donuts in the pan for 5 minutes, then flip them out onto a wire rack to cool completely. Make sure to not glaze while warm.

	 **For The Glaze** **Step 1** – Sift your powdered sugar, this will prevent your glaze from having lumps. **Step 2** – In a medium bowl, whisk together powdered sugar and water (or milk) until desired consistency. Add 1/4 tsp more water at a time until it's as thin as you like. If it becomes too thin, add more powdered sugar. If your glaze has lumps, you can use a hand mixer to smooth it out.  **Step 3** – If you want a more opaque glaze, add a few drops of white food coloring to the glaze and divide into bowls. Add your favorite colors and stir.  **Step 4** – Place the wire rack of donuts on top of a sheet pan to catch extra glaze drips. Grasp each donut by the sides and dunk into the glaze, letting it drain off for a few seconds. Then flip over and place the donut back onto the wire rack. Top with sprinkles immediately, as the glaze firms up quickly.  Place into a plastic or paper bag and store at room temperature for up to 3 days, they will continue to soften over time. **WHAT KIND OF PAN IS BEST TO USE FOR BAKED DONUTS?** Any kind of donut pan will work. It can be metal or it can be silicone. I am using a 6-Cavity donut baking pan I got from Target.  **WHAT IS THE DIFFERENCE BETWEEN BAKED AND FRIED DONUTS?** The recipes are very similar, but baked donuts are much softer than fried donuts. They don't have that crispy outer layer that forms when frying. Baked donuts are also lighter and have more of the same texture as a slice of cake. If you liked this donut recipe you'll love my other donut recipes!

The first and second images in *Lardland Super Donuts Instructions.pdf* are visually identical to the following images:

File Name	`Lardland Super Donut Ingredients.png`

File Path	/img_Taurus Laptop.001/vol_vol2/Documents and Settings/Taurus Smith/ Lardland Super Donut Ingredients.png
Hash Value (MD5)	ea08eba4c5d296b2f52d169864fbfa39
Modified	2005-01-01 18:50:02 UTC
Accessed	2010-03-08 00:00:00 UTC
Created	2004-03-08 00:17:47 UTC
MIME Type	image/png
Content	 BUTTERMILK BAKING POWDER BAKING SODA SALT NUTMEG SUGAR FOOD COLORING FLOUR OIL VANILLA MELTED BUTTER DONUT PAN POWDERED SUGAR FANCY SPRINKLES EGG WATER

File Name	baked_donut_recipe_featured.jpg
File Path	/img_Taurus Laptop.001/vol_vol2/Documents and Settings/Taurus Smith/baked_donut_recipe_featured.jpg
Hash Value (MD5)	649fa6b2ba32786580f3707575641c1f
Modified	2005-01-01 18:50:02 UTC
Accessed	2010-03-08 00:00:00 UTC
Created	2004-03-08 00:17:47 UTC
MIME Type	image/png

Content	

These images appear in the *Taurus Smith* (alias of Mona Simpson) folder at the locations below:

- `/img_Taurus Laptop.001/vol_vol2/Documents and Settings/Taurus Smith/ Lardland Super Donut Ingredients.png`
- `/img_Taurus Laptop.001/vol_vol2/Documents and Settings/Taurus Smith/baked_donut_recipe_featured.jpg`

The password-protection on this document suggests that this recipe is intentionally hidden. The recipe also appears to have been created with the two images above found in *Taurus Smith's* user account. This raises the question of whether *Taurus Smith* helped to create this recipe file.

The recipe was actually found in the *Bilbo Baggins* user account, not on the *Taurus* user account however a deleted file with an identical name (shown below) can be found on *Taurus Smith's* user account.

File Name	`Lardland Super Donuts Instructions.pdf`
File Path	`/img_Taurus Laptop.001/vol_vol2/Documents and Settings/Taurus Smith/Lardland Super Donuts Instructions.pdf`
Hash Value (MD5)	`2ac7400ab842f347e6be5000b2bbfbe5`
Modified	`2010-03-31 18:55:06 BST`
Accessed	`2010-03-31 00:00:00 BST`
Created	`2010-03-31 18:58:38 BST`

MIME Type	application/octet-stream
Content	

Inside the metadata of this file we can observe that the file was last modified at 2010-03-31 18:55:06 BST, however it was actually created at 2010-03-31 18:58:38 BST, around 3 minutes later (metadata is data that describes other data, in this case it is a set of data that describes a file). This behavior can exist if a file has been copied into a new location. If the file is modified, then the file is copied into the new location, the modified timestamp (digital record of a time when an event occurs) will remain the same but the created date will be set to when it is copied over to the new location. This would indicate that the file was modified before being copied over to Taurus' account, at which point it was deleted. It is also worth noting that images with the same file names as the two images above (*Lardland Super Donut Ingredients.png* and *baked_ donut_ recipe_ featured.jpg*) can be found inside the *Bilbo Baggins* user account.

Timestamp (last accessed, modified, or created)	Bilbo Baggins	Taurus Smith
2010-03-07 00:00:00 UTC	Lardland Super Donuts Instructions.pdf - (Exhibit I)	
2010-03-07 00:00:00 UTC	baked_donut_recipe_featured.jpg - (Exhibit X)	
2010-03-08 00:00:00 UTC		baked_donut_recipe_featured.jpg - (Exhibit K)
2010-03-08 00:00:00 UTC		Lardland Super Donut Ingredients.png - (Exhibit J)
2010-03-31 18:56:43 BST	Lardland Super Donut Ingredients.png (deleted) - (Exhibit W)	
2010-03-31 18:58:38 BST		Lardland Super Donuts Instructions.pdf (deleted) - (Exhibit V)

From this view it is not clear in which account *Lardland Super Donuts Instructions.pdf* was created.

However there is reason to believe that the *Bilbo Baggins* account is also being used by Taurus. This is because both the *Bilbo Baggins* account and the

Taurus Smith account contain a cookies folder containing the exact same cookies for multiple web services under the account name *Bilbo Baggins*. Cookies are small files downloaded when certain websites are visited, these are used by websites to remember preferences, or data entered into the website. Each of these web services cookie files have the exact same MD5 hash, showing that the files are completely identical.

Cookie file name	Bilbo Baggins MD5	Taurus Smith MD5
bilbo baggins@2o7[2].txt	e7b1c1e1ffb78c98e6bb0587b58b5c25	e7b1c1e1ffb78c98e6bb0587b58b5c25
bilbo baggins@aimtoday.aol[1].txt	f21a48a9cdb7fc65127a4372e358c82f	f21a48a9cdb7fc65127a4372e358c82f
bilbo baggins@aol[1].txt	7e873b7109f50eecaafd991a80acfad8	7e873b7109f50eecaafd991a80acfad8
bilbo baggins@atwola[1].txt	28d25319ae891868a09c8c97c4fbe4aa	28d25319ae891868a09c8c97c4fbe4aa
bilbo baggins@creativeby.viewpoint[1].txt	06d09ceac68cd977c92ca9335c0eb11e	06d09ceac68cd977c92ca9335c0eb11e
bilbo baggins@doubleclick[1].txt	bilbo baggins@doubleclick[1].txt	bilbo baggins@doubleclick[1].txt
bilbo baggins@viewpoint[1].txt	737d9ec78a689ec9791ae121f4656113	737d9ec78a689ec9791ae121f4656113
bilbo baggins@yahoo[2].txt	08b23cbd2e1c528783d7631395672620	08b23cbd2e1c528783d7631395672620

This could indicate that the same user (Mona Simpson) is actually operating both accounts and has logged in to the *Bilbo Baggins* web accounts using both the *Taurus Smith* and *Bilbo Baggins* user account. This is because cookies store session information, login states, and user preferences, and if the user logs into the same web accounts on different user accounts, it is highly likely that these cookies will be identical. If we take the assumption that Taurus is operating both accounts, we can continue with the assumption that Taurus has created *Lardland Super Donuts Instructions.pdf* in one of the two accounts that are logged into by her, though it is not clear which one created *Lardland Super Donuts Instructions.pdf* first. This behaviour can also be explained if the cookie files have been manually copied over from one account to the other.

3.1.5 Method 3: Network Packet Analysis

Exhibit D.pcapng is a PCAP file revealing a short exchange of 18 packets between the IP address 192.168.1.158 (Mona Simpson's computer) and the IP address 192.168.1.43, an unexpected laptop that appeared briefly on *Lardland Doughnuts* network. A PCAP file is a file format that is used to record captured packets and IP addresses are a string of numbers used to identify devices over a network. At the timestamp 2010-03-07 12:19:38.625569 UTC Mona Simpson's computer sends 192.168.1.43 what appears to be a recipe for a doughnut in the network packet:

```
## **Ingredients**

### **For the dough**

- 500gÂ [strong white bread
flour](https://www.bbcgoodfood.com/glossary/flour-glossary)

- 60gÂ [golden caster
sugar](https://www.bbcgoodfood.com/glossary/sugar-glossary)

- 15gÂ [fresh yeast,](https://www.bbcgoodfood.com/glossary/yeast-
glossary)Â crumbled

- 4Â [eggs](https://www.bbcgoodfood.com/glossary/egg-glossary)

- [zest 1/2 lemon](https://www.bbcgoodfood.com/glossary/lemon-
glossary)

- 2 tspÂ fine sea salt

- 125gÂ [softened unsalted
butter](https://www.bbcgoodfood.com/glossary/butter-glossary)

- about 2 litresÂ [sunflower
oil,](https://www.bbcgoodfood.com/glossary/sunflower-oil-
glossary)Â for deep-frying

- [caster sugar,](https://www.bbcgoodfood.com/glossary/sugar-
glossary)Â for tossing



### **Method**

- **STEP 1**

    Put 150g water and all the dough ingredients, apart from the
butter, into the bowl of a mixer with a dough hook. Mix on a medium
speed for 8 mins or until the dough starts coming away from the
```

sides and forms a ball. Turn off the mixer and let the dough rest for 1 min.

- **STEP 2**

Start the mixer up again on a medium speed and slowly add the butter to the dough â□□ about 25g at a time. Once it is all incorporated, mix on high speed for 5 mins until the dough is glossy, smooth and very elastic when pulled.

- **STEP 3**

Cover the bowl with cling film or a clean tea towel and leave to prove until it has doubled in size. Knock back the dough in the bowl briefly, then re-cover and put in the fridge to chill overnight.

- **STEP 4**

The next day, take the dough out of the fridge and cut it into 50g pieces (you should get about 20).

- **STEP 5**

Roll the dough pieces into smooth, tight buns and place them on a floured baking tray, leaving plenty of room between them, as you donâ□□t want them to stick together while they prove.

- **STEP 6**

Cover loosely with cling film and leave for 4 hrs or until doubled in size. Fill your deep-fat fryer or heavy-based saucepan halfway with oil. Heat the oil to 180C.

- **STEP 7**

When the oil is heated, carefully slide the doughnuts from the tray using a floured pastry scraper. Taking care not to deflate them, put them into the oil. Do 2-3 per batch, depending on the size of your fryer or pan.

- **STEP 8**

Fry for 2 mins each side until golden brown â□□ they puff up and float, so you may need to gently push them down after about 1 min to help them colour evenly.

- **STEP 9**

Remove the doughnuts from the fryer and place them on kitchen paper.

- **STEP 10**

Toss the doughnuts in a bowl of caster sugar while still warm. Repeat the steps until all the doughnuts are fried, but keep checking the oil temperature is correct â□□ if it is too high, they will burn and be raw in the middle; if it is too low, the oil will be absorbed into the doughnuts and they will become greasy. Set aside to cool before filling.

- **STEP 11**

To fill the doughnuts, make a hole with a small knife in the crease of each one, anywhere around the white line between the fried top and bottom.

- **STEP 12**

Fill a piping bag with your filling and pipe into the doughnut until nicely swollen â□□ 20-50g is the optimum quantity, depending on the filling; cream will be less, because it is more aerated. After filling, the doughnuts are best eaten straight away, but will keep in an airtight tin.

- **STEP 13**

Fillings

Custard filling: Try out Justin'sÂ [custard filling](http://www.bbcgoodfood.com/recipes/custard-filling)Â and, if you like, add different flavours to the custard as follows...

Brown sugar: Replace the caster sugar with half soft dark brown sugar and half light brown sugar. You can add chopped stem ginger to the finished custard, or some hazelnut praline. Finish with half the quantity of cream.

Chocolate: Whisk 150g dark (70%) chocolate into the milk. Finish with half the cream.

Coffee: Add 4 tbsp of freshly ground strong coffee to the milk.

```
    Malt & vanilla: Mix 2 tbsp of powdered malt into the sugar, and
2 tbsp of liquid malt into the milk.

    Saffron: Add a good pinch of saffron to the milk. Finish with
half the quantity of cream.

    Violet custard: Add 3 tsp of violet extract and 3 tbsp of
violet liqueur to the finished custard. Sprinkle sugared violets
and crushed Parma Violet sweets over the top of the filled
doughnuts.
```

Examining *Exhibit E*, another PCAP file between the IP address 192.168.1.158 (Mona Simpson's computer) and the IP address 192.168.1.43, the unexpected laptop, the following conversation can be established:

Timestamp	Sender	Message	Recipient
2010-03-07 12:27:18.788496 UTC	192.168.1.158	I have sent you a few files	192.168.1.43
2010-03-07 12:27:48.632271 UTC	192.168.1.158	using different way, some of them are steged and some of them used secure ways/channel.	192.168.1.43
2010-03-07 12:28:07.506722 UTC	192.168.1.43	Thanks	192.168.1.158
2010-03-07 12:29:44.400196 UTC	192.168.1.158	see you in hawaii!	192.168.1.43
2010-03-07 12:31:25.042577 UTC	192.168.1.158	i have another file	192.168.1.43
2010-03-07 12:32:07.614208 UTC	192.168.1.158	this is something useful.	192.168.1.43

The recipe is clearly sent from Mona Simpson's work computer to the unexpected laptop. The conversation above shows that Mona Simpson is in communication with the laptop, and Mona Simpson claims she has sent multiple files, some of which are "steged", which is likely short for steganography (a technique employed to hide recipes inside files such as images as seen in *file.dat* and *stdlidd.inc*. The user operating the unexpected laptop then thanks Mona Simpson, at which point Mona Simpson says "see you in hawaii!" which could indicate that Mona Simpson and the user behind the unexpected laptop plan to meet in Hawaii. Mona Simpson then claims that she has another file, she then says "this is something useful".

The traffic travels between two devices, Mona Simpson's computer which has the MAC address *HewlettPacka_45:a4:bb (00:12:79:45:a4:bb)*, and the unexpected laptop which has the MAC address *vmware_b0:8d:62 (00:0c:29:b0:8d:62).* MAC addresses are also strings of characters that identify devices on a network, similar to IP addresses.

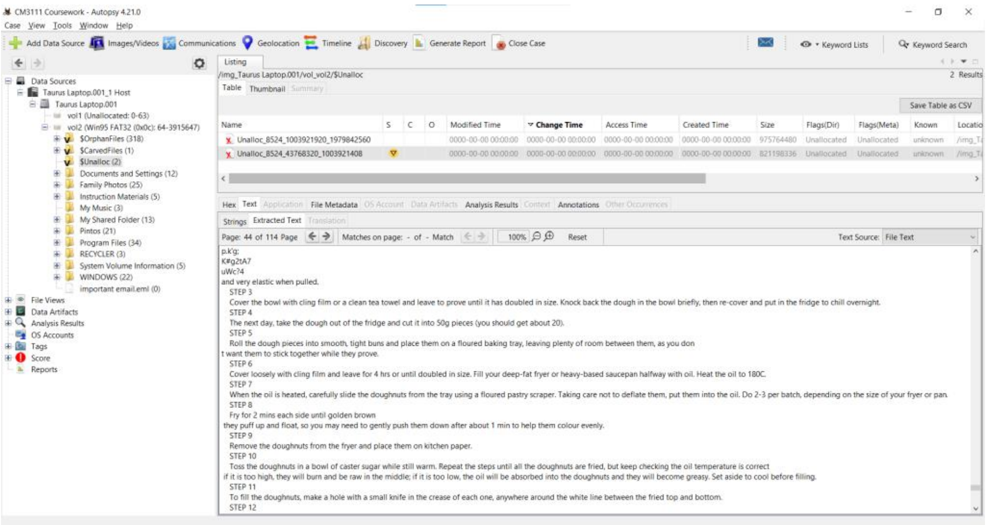
Exhibit B and *Exhibit C* show a conversation between Mona Simpson's computer (192.168.1.158) and the unexpected laptop (64.12.24.50), operating using a different IP address from what is displayed in *Exhibit D* and *Exhibit E* (192.168.1.43). This is the same device as the MAC address of Mona Simpson's computer and the unexpected laptop remains consistent between exhibits (*HewlettPacka_45:a4:bb (00:12:79:45:a4:bb)* and *vmware_b0:8d:62 (00:0c:29:b0:8d:62* respectively). Though the data given in *Exhibit B* and *Exhibit C* only consists of two screenshots, the following conversation can be established:

Timestamp	Sender	Message	Recipient
	192.168.1.158	Here's the secret recipe I just downloaded from the file server. Just copy to a thumb drive and you're good to go &gt;:-)	64.12.24.50
	192.168.1.158	see you in Hawaii!!	64.12.24.50

The exact timestamps of each message is not displayed in the exhibits. The message "see you in hawaii" appears to be sent in both conversations whereas the message "Here's the secret recipe I just downloaded from the file server. Just copy to a thumb drive and you're good to go &gt;:-)" is only visible in one conversation.

3.1.6 Method 4: Searching Unallocated Files

Unallocated files are files located in the space on a digital storage space that are not currently allocated to any files or directories. The space can contain remnants of previously deleted or lost files. *Autopsy* automatically extracts unallocated space files and displays any extracted text in a viewer. Inside the file *Unalloc_8524_43768320_1003921408* a recipe can be found in the 44th page of extracted text:



/img_Taurus Laptop.001/vol_vol2/$Unalloc

2 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Locatio
Unalloc_8524_1003921920_1979842560				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	975764480	Unallocated	Unallocated	unknown	/img_T
Unalloc_8524_43768320_1003921408	▽			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	821198336	Unallocated	Unallocated	unknown	/img_T

Page: 44 of 114 Page

Matches on page: - of - Match

100%

Text Source: File Text

```
p.k'g;
K#g2tA7
uWc?4
and very elastic when pulled.
   STEP 3
   Cover the bowl with cling film or a clean tea towel and leave to prove until it has doubled in size. Knock back the dough in the bowl briefly, then re-cover and put in the fridge to chill overnight.
   STEP 4
   The next day, take the dough out of the fridge and cut it into 50g pieces (you should get about 20).
   STEP 5
   Roll the dough pieces into smooth, tight buns and place them on a floured baking tray, leaving plenty of room between them, as you don
t want them to stick together while they prove.
   STEP 6
   Cover loosely with cling film and leave for 4 hrs or until doubled in size. Fill your deep-fat fryer or heavy-based saucepan halfway with oil. Heat the oil to 180C.
   STEP 7
   When the oil is heated, carefully slide the doughnuts from the tray using a floured pastry scraper. Taking care not to deflate them, put them into the oil. Do 2-3 per batch, depending on the size of your fryer or pan.
   STEP 8
   Fry for 2 mins each side until golden brown
 they puff up and float, so you may need to gently push them down after about 1 min to help them colour evenly.
   STEP 9
   Remove the doughnuts from the fryer and place them on kitchen paper.
   STEP 10
   Toss the doughnuts in a bowl of caster sugar while still warm. Repeat the steps until all the doughnuts are fried, but keep checking the oil temperature is correct
 if it is too high, they will burn and be raw in the middle; if it is too low, the oil will be absorbed into the doughnuts and they will become greasy. Set aside to cool before filling.
   STEP 11
   To fill the doughnuts, make a hole with a small knife in the crease of each one, anywhere around the white line between the fried top and bottom.
   STEP 12
```

The recipe is shown as follows:

File Name	`Unalloc_8524_43768320_1003921408`
File Path	`/img_Taurus Laptop.001/vol_vol2/$Unalloc/Unalloc_8524_43768320_1003921408`
Hash Value (MD5)	`Not calculated`
Modified	`0000-00-00 00:00:00`
Accessed	`0000-00-00 00:00:00`
Created	`0000-00-00 00:00:00`
MIME Type	`application/octet-stream`
Extracted Recipe	uWc?4 and very elastic when pulled. STEP 3 Cover the bowl with cling film or a clean tea towel and leave to prove until it has doubled in size. Knock back the dough in the bowl briefly, then re-cover and put in the fridge to chill overnight. STEP 4 The next day, take the dough out of the fridge and cut it into 50g pieces (you should get about 20). STEP 5 Roll the dough pieces into smooth, tight buns and place them on a floured baking tray, leaving plenty of room between them, as you don t want them to stick together while they prove. STEP 6 Cover loosely with cling film and leave for 4 hrs or until doubled in size. Fill your deep-fat fryer or heavy-based saucepan halfway with oil. Heat the oil to 180C. STEP 7

When the oil is heated, carefully slide the doughnuts from the tray using a floured pastry scraper. Taking care not to deflate them, put them into the oil. Do 2-3 per batch, depending on the size of your fryer or pan.

STEP 8

Fry for 2 mins each side until golden brown they puff up and float, so you may need to gently push them down after about 1 min to help them colour evenly.

STEP 9

Remove the doughnuts from the fryer and place them on kitchen paper.

STEP 10

Toss the doughnuts in a bowl of caster sugar while still warm. Repeat the steps until all the doughnuts are fried, but keep checking the oil temperature is correct if it is too high, they will burn and be raw in the middle; if it is too low, the oil will be absorbed into the doughnuts and they will become greasy. Set aside to cool before filling.

STEP 11

To fill the doughnuts, make a hole with a small knife in the crease of each one, anywhere around the white line between the fried top and bottom.

STEP 12

Fill a piping bag with your filling and pipe into the doughnut until nicely swollen 20-50g is the optimum quantity, depending on the filling; cream will be less, because it is more aerated. After filling, the doughnuts are best eaten straight away, but will keep in an airtight tin.

STEP 13

Fillings

Custard filling: Try out Justin's custard filling and, if you like, add different flavours to the custard as follows...

Brown sugar: Replace the caster sugar with half soft dark brown sugar and half light brown sugar. You can add chopped stem ginger to the finished custard, or some hazelnut praline. Finish with half the quantity of cream.

Chocolate: Whisk 150g dark (70%) chocolate into the milk. Finish with half the cream.

Coffee: Add 4 tbsp of freshly ground strong coffee to the milk.

Malt & vanilla: Mix 2 tbsp of powdered malt into the sugar, and 2 tbsp of liquid malt into the milk.

Saffron: Add a good pinch of saffron to the milk. Finish with half the quantity of cream.

Violet custard: Add 3 tsp of violet extract and 3 tbsp of violet liqueur to the finished custard. Sprinkle sugared violets and crushed Parma Violet sweets over the top of the filled doughnuts.

IHDR

When files are deleted the space that the files are stored in is marked as unallocated to be overwritten. However, the data itself remains intact until it is overwritten. The most likely explanation for this recipe being in unallocated space is that it was deleted and not currently overwritten. If the likely explanation that the file was deleted is to be taken, it can indicate that either the contents were intended to be hidden or that the file was not needed by the operator of the laptop. In conjunction with the other pieces of evidence it would look more likely that this recipe was intentionally deleted, however this is an assumption that cannot be fully supported. The file also contains no metadata therefore it is difficult to prove if Mona Simpson wrote or distributed the recipe, or if it even was from *Lard&land Donuts*.

3.2 Travel Plans

There are multiple pieces of evidence indicating that Taurus Smith is planning on travelling to Hawaii. These include a network packet coming from her laptop and a carved file.

Network

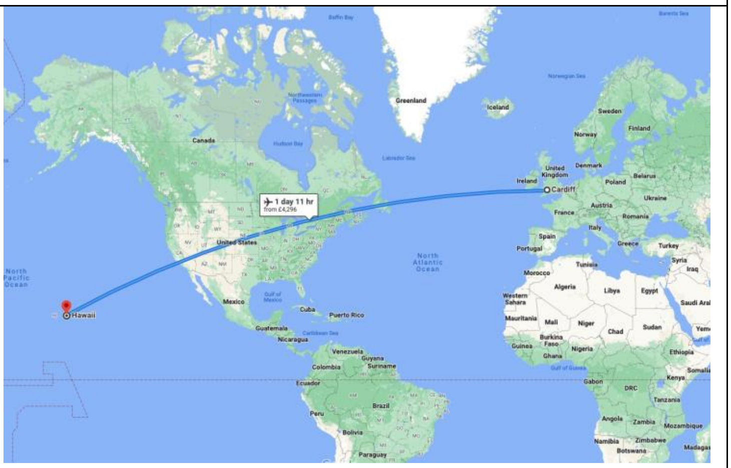
A packet found in *Exhibit E* (shown below) contains a message reading “see you in hawaii!”. This indicates that both Taurus and the accomplice operating the unexpected laptop may plan to meet in Hawaii, if Taurus is to be taken at her word.

Timestamp	Sender	Message	Recipient
2010-03-07 12:29:44.400196 UTC	192.168.1.158	see you in hawaii!	192.168.1.43

Carved File

On the laptop image inside a carved file, there is an image depicting a flight path from Cardiff to Hawaii.

File Name	f0066494.png
File Path	/img_Taurus Laptop.001/vol_vol2/$CarvedFiles/1/f0066494.png
Hash Value (MD5)	0c9dac13c42678ceda658b21507e9156
Modified	0000-00-00 00:00:00
Accessed	0000-00-00 00:00:00
Created	0000-00-00 00:00:00

MIME Type	`image/png`
Content	

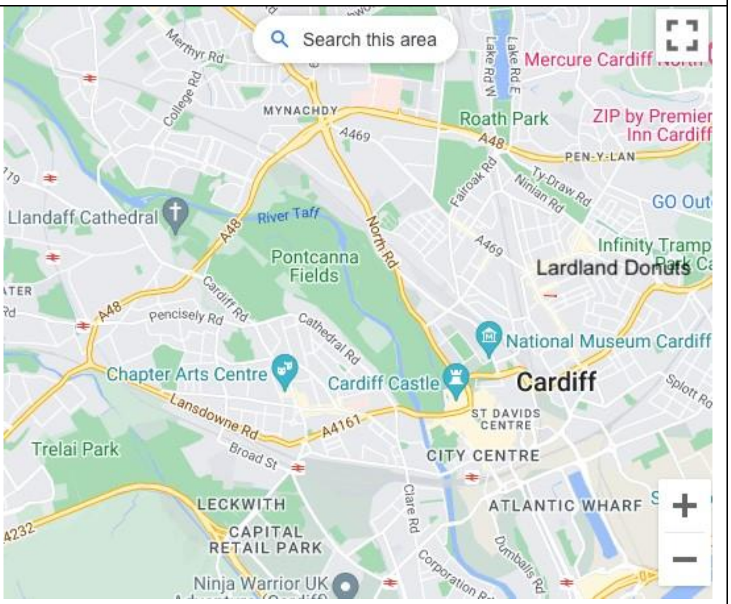
A carved file is a file that has been recovered from a storage medium (like a hard disk or USB drive) using a process that bypasses the file system originally used to manage it. This method, known as file carving, relies on identifying and extracting data based on content patterns and structural signatures inherent to specific file types. Since file carving does not depend on file system metadata, the recovered file often lacks associated information such as the original file name, directory structure, and timestamps. As a result, a carved file is typically a raw data segment that matches the format of a specific file type (like a JPEG image or PDF document) but without its original file system context.

In isolation this file itself cannot be attributed to Mona Simpson directly, as there are multiple users of this laptop who could have created the file and without any valid metadata we are unable to establish it is difficult to prove who created it. However, it does confirm that a user of the laptop had viewed flights from Hawaii to Cardiff on *Google Maps*.

In isolation this file itself cannot be attributed to Mona Simpson directly, as there are multiple users of this laptop who could have created the file and without any valid metadata we are unable to establish it is difficult to prove who created it. However, it does confirm that a user of the laptop had viewed flights from Hawaii to Cardiff on *Google Maps*.

SendTo Folder

Inside the *SendTo* folder on *Mona Simpson's* user account there are two files indicating an interest in Cardiff, Wales. There is a .png file containing a screenshot of a *Google* maps view of Cardiff, modified with a red line and a label reading "Lardland Donuts".

File Name	`maps.png`
File Path	`/img_Taurus Laptop.001/vol_vol2/Documents and Settings/Taurus Smith/SendTo/maps.png`
Hash Value (MD5)	`e101eed602496b694b5443cde5f28bc6`
Modified	`2005-01-01 18:50:02 GMT`
Accessed	`2010-03-07 00:00:00 GMT`
Created	`2004-03-08 00:17:47 GMT`
MIME Type	`image/png`
Content	

There is also an *Microsoft Word* document containing an image of a doughnut shop in Cardiff named "Cardiff Dough and Co"

File Name	`Cardiff.docx`
File Path	`/img_Taurus Laptop.001/vol_vol2/Documents and Settings/Taurus Smith/SendTo/Cardiff.docx`
Hash Value (MD5)	`9278c02e287f100ee1987b7e96811f82`
Modified	`2010-03-07 21:03:08 UTC`
Accessed	`2010-03-07 00:00:00 UTC`
Created	`2004-03-08 00:17:47 UTC`
MIME Type	`image/jpeg`

Content	

These files were found inside a *SendTo* folder, indicating that they are intended to be sent to another location on the laptop.

These evidence items indicated that Mona Simpson has an interest in Cardiff, Hawaii, and potentially the travel from Cardiff to Hawaii, and would provide some justification that Mona Simpson is planning to travel from Cardiff to Hawaii.

3.3 Implicated Individuals

There appears to be an accomplice that is implicated along with Mona Simpson, though the identity of this individual is unclear. It can be ascertained that Mona Simpson is sending secret doughnut recipes to a recipient who is aware of the secrecy of these files and is willingly accepting them. This can be assumed from the exchange seen in the *Exhibit E*. The exchange would indicate that Mona Simpson and the recipient have already communicated about the encoded files being sent and have communicated about travelling to Hawaii together, showing some form of relationship between the two.

3.4 Deleted/Hidden Accounts

3.4.1 Method 4: Registry Analysis

Terms:

- Registry – Collection of settings and preferences for the *Windows* operating system. It can contain information like the number of users on a machine.
- SAM – Security Account Manager. A registry hive that stores credentials and account information for local users.

- SID – Security Identifiers. A unique value that is used to identify a user account or computer account.
- RID – Relative Identifiers. The unique suffix of an SID used to identify a user account or computer account.

Inside the *SAM* registry found on Mona Simpson's laptop 8 user accounts can be found inside by navigating to *SAM>Domains>Account>Users*.

Account Name	RID	SID
Administrator	000001F4	S-1-5-21-1801674531-1177238915-725345543-500
Guest	000001F5	S-1-5-21-1801674531-1177238915-725345543-501
HelpAssistant	000003E8	S-1-5-21-1801674531-1177238915-725345543-1000
SUPPORT_388945a0	000003EA	S-1-5-21-1801674531-1177238915-725345543-1002
Frodo Baggins	000003EC	S-1-5-21-1801674531-1177238915-725345543-1004
Bilbo Baggins	000003ED	S-1-5-21-1801674531-1177238915-725345543-1005
Pippin	000003EE	S-1-5-21-1801674531-1177238915-725345543-1006
Sam	000003EF	S-1-5-21-1801674531-1177238915-725345543-1007

Two key takeaways can be found. Noticeably, the *Taurus Smith* user account is missing. Also, there appears to be a missing account with the SID ending with the suffix -1003.

There was a restore point taken containing a system snapshot, created at 2009-03-08 00:06:24 UTC and modified at 2010-03-08 00:06:26 UTC, containing a *SAM* registry hive called *_REGISTRY_MACHINE_SAM*. Inside this registry hive we can observe 5 user accounts by navigating to *SAM>Domains>Account>Users*.

Account Name	RID	SID
Administrator	000001F4	S-1-5-21-1801674531-1177238915-725345543-500
Guest	000001F5	S-1-5-21-1801674531-1177238915-725345543-501
HelpAssistant	000003E8	S-1-5-21-1801674531-1177238915-725345543-1000
SUPPORT_388945a0	000003EA	S-1-5-21-1801674531-1177238915-725345543-1002
user1	000003EB	S-1-5-21-1801674531-1177238915-725345543-1003

Notably, inside this snapshot there appears to be the missing user account with the SID suffix -1003 with the account name "user1".

The *Taurus Smith* user account would appear to have the same SID as the *Bilbo Baggins* account as inside the folders *Local Settings>Application Data>Microsoft>Credentials* for both accounts, there can be found a folder with the same SID (S-1-5-21-1801674531-1177238915-725345543-1005), shown below:

File Name	S-1-5-21-1801674531-1177238915-725345543-1005
File Path	/img_Taurus Laptop.001/vol_vol2/Documents and Settings/Bilbo Baggins/Application Data/Microsoft/Credentials/S-1-5-21-1801674531-1177238915-725345543-1005

Hash Value (MD5)	Not calculated
Modified	2005-01-01 18:50:02 UTC
Accessed	2010-03-08 00:00:00 UTC
Created	2004-03-08 00:17:47 UTC
MIME Type	null
Content	

File Name	S-1-5-21-1801674531-1177238915-725345543-1005
File Path	/img_Taurus Laptop.001/vol_vol2/Documents and Settings/Taurus Smith/Local Settings/Application Data/Microsoft/Credentials/S-1-5-21-1801674531-1177238915-725345543-1005
Hash Value (MD5)	Not calculated
Modified	2005-01-01 18:50:02 UTC
Accessed	2010-03-08 00:00:00 UTC
Created	2004-03-08 00:17:47 UTC
MIME Type	null
Content	

It is likely that the account *user1* has been deleted at some point as it is not present in the image or in the active registry *SAM*. There are several possibilities as to why it might not appear in the registry but has a folder inside *Documents and Settings*, and why it appears to have the same cookies and SID as the *Bilbo Baggins* account.

1. The *Taurus Smith* user account does not actually exist and never has existed, the only evidence of its existence is a folder inside *Documents and Settings* which could have very easily been created manually, by copying files from the *Bilbo Baggins* account folder such as the *Cookies* folder and the *Local Settings* folder, both of which contain identical files.
2. The *Taurus Smith* user account existed (potentially under the deleted *user1* profile) but was deleted at some point from the system, but the user's profile folder and associated data were not removed. At this point the *Cookies* folder and the *Local Settings* folder, would also need to be manually copied over from the *Bilbo Baggins* user account

in an attempt to conceal. This would also explain why the *Taurus Smith* account is not present in the registry.

3. The *Taurus Smith* user account existed (potentially as *user1*) but was hidden at some point from the registry, however the user account folder was kept. At this point the *Cookies* folder and the *Local Settings* folder, would also need to be manually copied over from the *Bilbo Baggins* user account. This also would explain why the *Taurus Smith* account is not present in the registry.

No evidence has been extracted that could conclusively confirm any of these possibilities.

3.5 Timeline

Date/Time	Description	Event Type	Analysis
2009-03-08 00:06:24 UTC	_REGISTRY_MACHINE_SAM	File Created	Registry hive found in snapshot showing user account information created.
2010-01-03 00:16:20 UTC	file.dat	File Created	Image with a hidden encoded message containing a doughnut recipe created.
2010-01-03 00:16:20 UTC	stdlidd.inc	File Created	Image with a hidden encoded message containing a doughnut recipe created.
2010-02-02 12:02:26 UTC	file.dat	File Modified	Image with a hidden encoded message containing a doughnut recipe modified.
2010-02-02 12:02:26 UTC	stdlidd.inc	File Modified	Image with a hidden encoded message containing a doughnut recipe modified.
2010-03-04 00:06:49	Basic donuts.doc	File Created	File containing the recipe for "Basic donuts" created.
2010-03-04 10:11:46 UTC	Important email.eml	Email	Email sent containing *Base64* encoded message instructing recipient to use the website https://stylesuxx.github.io/steganography/ to decode 2 .png files.
2010-03-04 13:35:24 UTC	Basic donuts.doc	File Modified	File containing the recipe for "Basic donuts" modified.
2010-03-07 00:00:00 UTC	Basic donuts.doc	File Accessed	File containing the recipe for "Basic donuts" accessed.
2010-03-07 00:00:00 UTC	maps.png	File Accessed	File containing map of Cardiff accessed.
2010-03-07 00:00:00 UTC	Lardland Super Donuts Instructions.pdf	File Accessed	Lardland Super Donuts Instructions accessed.

2010-03-07 12:19:38.625569 UTC	Exhibit D.pcapng	Packet Sent	Packet sent from 192.168.1.158 (*Taurus's* computer) to 192.168.1.43 containing a doughnut recipe.
2010-03-07 12:27:18.788496 UTC	Exhibit E.pcapng	Packet Sent	Packet sent from 192.168.1.158 (*Taurus's* computer) to 192.168.1.43 containing the message "I have sent you a few files".
2010-03-07 12:27:48.632271 UTC	Exhibit E.pcapng	Packet Sent	Packet sent from 192.168.1.158 (*Taurus's* computer) to 192.168.1.43 containing the message "using different way, some of them are steged and some of them used secure ways/channel.".
2010-03-07 12:28:07.506722 UTC	Exhibit E.pcapng	Packet Sent	Packet sent from 192.168.1.43 to 192.168.1.158 (*Taurus's* computer) containing the message "Thanks".
2010-03-07 12:29:44.400196 UTC	Exhibit E.pcapng	Packet Sent	Packet sent from 192.168.1.158 (*Taurus's* computer) to 192.168.1.43 containing the message "see you in hawaii!".
2010-03-07 12:31:25.042577 UTC	Exhibit E.pcapng	Packet Sent	Packet sent from 192.168.1.158 (*Taurus's* computer) to 192.168.1.43 containing the message "i have another file".
2010-03-07 12:32:07.614208 UTC	Exhibit E.pcapng	Packet Sent	Packet sent from 192.168.1.158 (*Taurus's* computer) to 192.168.1.43 containing the message "this is something useful.".
2010-03-07 21:03:08 UTC	Cardiff.docx	File Modified	File containing image of "Cardiff Dough and Co" modified.
2010-03-08 00:00:00 UTC	file.dat	File Accessed	Image with a hidden encoded message containing a doughnut recipe accessed.
2010-03-08 00:00:00 UTC	stdlidd.inc	File Accessed	Image with a hidden encoded message containing a doughnut recipe accessed.
2010-03-08 00:00:00 UTC	Lardland Super Donut Ingredients.png	File Accessed	Lardland Super Donuts Ingredients image accessed.
2010-03-08 00:00:00 UTC	baked_donut_recipe_featured.jpg	File Accessed	Baked Donut Recipe image accessed.
2010-03-08 00:06:26 UTC	_REGISTRY_MACHINE_SAM	File Modified	Registry hive found in snapshot showing user account information modified.
2010-03-31 00:00:00 BST	ring recipe.txt.sb-ace39f49-PiYykM	File Accessed	Deleted file which could potentially contain a recipe accessed.
2010-03-31 18:55:06 BST	Lardland Super Donuts Instructions.pdf	File Modified	Deleted file suspected to be Lardland Super Donuts Instructions.pdf modified.
2010-03-31 18:55:06 BST	Lardland Super Donut Ingredients.png	File Modified	Deleted file suspected to be Lardland Super Donuts Ingredients.png modified

2010-03-31 18:56:43 BST	Lardland Super Donut Ingredients.png	File Created (copied)	Deleted file suspected to be Lardland Super Donuts Ingredients.png copied into *Bilbo Baggins'* user account.
2010-03-31 18:58:38 BST	Lardland Super Donuts Instructions.pdf	Filed Created (copied)	Deleted file suspected to be Lardland Super Donuts Instructions.pdf copied into *Taurus Smith's* user account.
2010-03-31 19:55:14 BST	ring recipe.txt.sb-ace39f49-PiYykM	Filed Created (copied)	Deleted file which could potentially contain a recipe copied into *Taurus Smith's* desktop.

4 Conclusion

4.1 Recipes

From what we were able to extract, it appears as if Mona Simpson intentionally encoded/hid four secret doughnut recipes:

1. Vanilla Doughnuts - Hidden inside *file.dat* using steganography.
    a. Confirmed to have been sent by Mona Simpson to an accomplice in *Exhibit E.*
2. Coconut Doughnuts - Hidden inside *stdlidd.inc* using steganography.
    a. Confirmed to have been sent by Mona Simpson to an accomplice in *Exhibit E.*
3. Lardland Super Doughnuts - Hidden inside a password-protected PDF.
    a. Likely created by Taurus due to the presence of two images also found in the *Taurus Smith* account and a deleted file using the same name can also be found on the *Taurus Smith* user account.
4. Custard Doughnuts - Sent over a network packet.
    a. Accomplice confirmed their involvement by replying "thanks".

There are two recipes which could be related to this case however there is not sufficient evidence to know if they were secret recipes from *Lard&land Donuts*.

1. Basic Donut.doc – Did not appear to be sent anywhere
2. ring recipe.txt.sb-ace39f49-PiYykM – The only contents able to be extracted was the word "method"
3. Recipe found in unallocated space – In conjunction with other evidence, it would be likely that this recipe was intentionally deleted.
    a. No metadata to indicated that Mona Simpson wrote or distributed the recipe.
    b. No conclusive evidence to suggest that it was intentionally deleted or hidden.

No recipe for "Honey Duff Donuts" have been recovered.

4.2 Travel Plans

The extracted evidence strongly suggests that Mona Simpson is planning to travel to Hawaii:

1. Network Packet (Exhibit E) – "see you in hawaii!" packet sent from Mona Simpson's work computer to accomplice
2. Carved File – Screenshot of flight route from Cardiff to Hawaii
    a. Absence of metadata mean that it cannot be used to show a definitive link
3. Cardiff.docx – Image of doughnut shop in Cardiff.
4. maps.png – Image of a map of Cardiff, containing an added red marker and a label reading Lard&land Donuts.

4.3 Implicated Individuals

The existence of an accomplice can be confirmed by the packet exchanges in *Exhibit E*. No evidence was able to be extracted regarding the identity of the accomplice.

4.4 Deleted/Hidden Accounts

It is likely that the *Taurus Smith* account is a deleted/hidden account. We also know for sure that there was an account *user1* that was deleted/hidden, however no information other than its existence could be extracted.

There are three likely possibilities for the nature of the *Taurus Smith* account, none of which could be confirmed:

1. The account never existed formally and the *Taurus Smith* folder was manually created using files from the *Bilbo Baggins* account.
    a. *Taurus Smith* account is not in the registry.
    b. There are several duplicated files that are found in the *Bilbo Baggins* account.
2. The account existed (potentially as *user1*) but was deleted. The *Taurus Smith* folder were remnants of a deleted account.
    a. *Taurus Smith* account is not in the registry.
    b. Would require the manual copying and replacing of some of Bilbo Baggins' files into this folder.

3. The account existed (potentially as *user1*) but is hidden from the registry while retaining the user profile folder.
    a. *Taurus Smith* account is not in the registry.
    b. Would require the manual copying and replacing of some of Bilbo Baggins' files into this folder.

5 Glossary

Term	Definition
Base64	A method for encoding data, often used to transfer data over the internet. It converts binary data into text format.
Carved File	A file recovered from a digital storage space, typically extracted from areas not readily visible or accessible, like remnants found in unallocated disk space.
Cookie	Small pieces of data stored on your computer by websites you visit. They are used to remember your preferences and login information.
Directory	A folder or location on a computer or network where files are stored.
DOC File	A document file format used by Microsoft Word before 2007. Primarily used for text documents.
DOCX File	A document file format used by Microsoft Word since 2007. It is more efficient and secure than DOC.
Encrypted	Data that has been transformed into a secure format that prevents unauthorized access. Encryption requires a key to decode.
EXIF Metadata	Information embedded in images and videos, including details like camera settings, date, time, and sometimes location.
IP Address	A unique number assigned to each device on a network, like an address for your computer on the internet.
JPEG File	A common format for images, known for its balance of quality and file size.
MAC Address	A unique identifier assigned to network interfaces (like your computer's Ethernet or Wi-Fi card) for communications on a physical network.
MD5 Hash	A type of checksum used to ensure data integrity. It creates a unique, fixed-size hash value from data.
Metadata	Data that provides information about other data, like a summary or description.

MIME Type	A standard that indicates the nature and format of a file, document, or email attachment.
Network Packets	Small chunks of data sent over a computer network.
Open Source	Software with source code that anyone can inspect, modify, and enhance.
Password Cracking	The process of recovering passwords from data stored or transmitted by computer systems.
PCAP File	A file format used to capture and store network packets.
PDF File	A file format used to present documents in a manner independent of application software, hardware, and operating systems.
PNG File	An image file format known for its lossless compression and support of transparent backgrounds.
Registry	In computing, a database that stores configuration settings and options on Microsoft Windows operating systems.
RID	Relative Identifier, a part of a security identifier (SID) in Windows systems that identifies a user or group.
SAM Hive	Security Account Manager, a component of Microsoft Windows that stores user passwords in a secure format.
SHA256 Hash	A cryptographic hash function that produces a 256-bit (32-byte) hash value, widely used for security applications.
Screenshot	An image taken by a computer or mobile device to capture the visible items displayed on the screen.
SID	Security Identifier, a unique, immutable identifier of a user or group object in Microsoft Windows.
Steganography	The practice of hiding messages or information within other non-secret text or data.
Timestamp	A sequence of characters or encoded information identifying when a particular event occurred, usually giving date and time of day.
Unallocated Files	Files located in the space on a digital storage space that is not currently allocated to any files or directories. The space can contain remnants of previously deleted or lost files.
Virtual Machine	A software emulation of a physical computer that can run an operating system and applications like a real computer.