Technical Report

CM3111

21050251

Theodor Baur

Content

1 Introduction

1.1 Background

1.1.1 Scenario

Security staff at *Lard&land Donuts*, a doughnut making company in Springfield, are worried that one of their employees, Ms. Taurus Smith, has been working with their competitor, *Diggity Doughnuts*, and has leaked the recipe for *Lard&land Donuts* prized assets, the "Honey Duff Donuts".

1.1.2 Events

Prior to any investigation, the *Lard&land Donuts* security staff had been monitoring Ms. Taurus Smith's activity, however they did not find anything suspicious.

An unexpected laptop appeared on *Lard&land Donuts* wireless network and Ms. Taurus Smith's computer sent instant message packets over this network to the laptop. Security staff claim that there were no strangers seen at the company, therefore they believe that the laptop resided in the carpark. From the analysis of these packets, *Lard&land Donuts* believe they are a victim of a computer misuse attack and that Ms. Taurus Smith is planning to leave shortly, at which point they decided to call the police.

Subsequent investigations into Ms. Taurus Smith indicated that the name was an alias and that Taurus' real name was Mrs Mona Simpson. Mona Simpson is a wanted woman whose last known address was with her son Mr H.J. Simpson at 742 Evergreen Terrace. The police searched 742 Evergreen Terrace and found a liquid damaged phone and a USB stick containing a disk image.

1.2 Evidence

1.2.1 Exhibit A - Liquid damaged phone

This phone was found during the search of 742 Evergreen Terrace. It appears that this phone will not yield any information.

1.2.2 USB stick

This USB stick was found during the search of 742 Evergreen Terrace. It contains an image of a laptop hard drive.

1.2.3 Exhibit B,C,D,E - PCAP files

Packets sent when Taurus's computer (192.168.1.158) sent instant message packets to an unexpected laptop.

1.3 Objectives

1.3.1 Ensure proper handling of evidence

Any evidence chosen to be analysed must follow the Association of Chief Police Officers (ACPO) guidelines.

- Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
- Principle 2: In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
- Principle 3: An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
- Principle 4: The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

1.3.2 Recover evidence relating to the alleged illegal activities involving Taurus Smith

Uncover evidence (if any) linking Taurus Smith or her accomplice to the alleged computer misuse incident involving *Lard&land Doughnuts*.

1.3.3 Identify potential accomplices

Uncover evidence linking other parties to Taurus Smith's illegal activities (if any exist) and establish the nature of this relationship.

1.3.4 Assess Taurus Smith's intentions and plans

Uncover any evidence (if any) showing where Taurus Smith plans to travel and what her future plans are.

1.3.5 Uncover all recipes

Uncover all instances of recipes that Taurus Smith may or may not have sent.

1.3.6 Uncover any hidden/deleted user accounts

Uncover all instances of user accounts that may be deleted/hidden.

1.3.7 Establish timeline of events

Present timeline of all relevant events relating to Taurus Smith's alleged computer misuse.

2 Methodology

2.1 Procedure Outline

The procedure followed in this investigation aims to preserve the integrity of the evidence, whilst performing a thorough and encompassing analysis of the system, keeping each sub procedure repeatable and sound.

1. Preparation: Establish a secure environment to perform forensic analysis and gather the necessary analysis tools
2. Acquisition: Create exact copies of digital media and record the hashes of each piece of digital media to check the integrity after analysis.
3. Analysis: Conduct analysis on digital evidence in the following areas:
    a. Email
    b. Web Activity
        i. History
        ii. Cookies
        iii. Searches
    c. Chat Logs/Communication Data
    d. Network
    e. Attached Devices
    f. Programs Installed
    g. Deleted Files
    h. Encrypted Files
    i. EXIF metadata
    j. Registry
    k. Unallocated files
4. Verification: Gather the hashes of each piece of digital media post-analysis and compare to the hashes of each piece of digital media recorded in the acquisition phase.

2.2 Preparation

2.2.1 Tools

Kali Linux + VMware

Kali Linux Version: 2023.4

VMware Version: VMWare Workstation 17 Player

To maintain security and isolation, all stages of the investigation has been run inside of virtual machines using VMWare. The forensic tool Autopsy (see more details below) has a graphical interface for Windows therefore one virtual machine has been set up inside a Windows 10 environment inside VMWare. Parts of the investigation also took place inside a virtual machine running on Kali Linux as many forensic tools come preinstalled on the system, such as John the Ripper. This helps the legal admissibility of evidence as Kali Linux contains many standard and recognized forensic tools.

Using a virtual machine provides a secure and isolated environment. This is crucial in digital forensics, where handling sensitive data and potentially malicious files is common. The isolation ensures that if the forensic environment is compromised, the host system (in this case, Windows) remains unaffected.

Autopsy

Version: 4.21.0

Autopsy is a standard open-source tool used to analyse disk images and recover files from them. It contains a collection of command line tools that can perform:

- File system analysis
- Data recovery
- Timeline analysis
- Keyword searching
- Report generation
- Web artifact analysis

Autopsy also has a graphical interface which can simplify the process of forensic investigation, whilst also providing the same detailed analysis as the collection of tools found inside it. A browser-based version of this tool is installed

on Kali Linux, however for the purposes of this investigation the desktop version of this tool will be installed.

John the Ripper

Version: 1.9.0

John the Ripper is an open-source password cracking tool pre-installed into Kali Linux. It is useful specifically in a forensic scenario to help crack password protected files. John the Ripper is also able to utilize multiple cores, making the password-cracking process more optimized.

Wireshark

Version: 4.2.0

Wireshark is an open-source tool that can be used for network analysis. It can be used in a forensic setting to inspect large amounts of network traffic and network packets in a user-friendly interface. This tool is pre-installed on Kali Linux

Exiftool

Version: 12.70

Exiftool is an open-source tool used to analyse, write, and display EXIF metadata found in images, audio, videos and PDFs. This tool can be used on both *Kali Linux* and *Windows 10*.

2.2.2 Setup

Date/Time	Action	Outcome
2023-12-17 14:10:45 UTC	Install *VMWare Workstation 17 Player* and follow the setup instructions for you forensic machine. https://www.vmware.com/uk/products/workstation-player.html	*VMWare Workstation 17 Player* installed.
2023-12-17 14:15:54 UTC	Install *Windows 10* ISO and follow the installation instructions. https://www.microsoft.com/en-ca/software-download/windows10	*Windows 10* ISO installed.

2023-12-17 14:20:24 UTC	Install *Kali Linux* for *VMware* and follow the installation instructions. https://www.kali.org/get-kali/#kali-virtual-machines	*Kali Linux* for *VMware* installed.
2023-12-17 14:24:41 UTC	Install *Autopsy* on your *Windows 10* virtual machine using the following link. https://www.sleuthkit.org/autopsy/	*Autopsy* installed on virtual machine.
2023-12-17 14:25:22 UTC	Download all Exhibit files (*Taurus Laptop.001*, *pcap files.zip*, *Exhibit A_Back.jpg* and, *Exhibit B_Back.jpg*).	*Case* files installed
2023-12-17 14:27:11 UTC	Copy the files, the run your virtual machine and paste the files inside a directory on your virtual machine	*Case* files transported to virtual machine.

2023-12-17 14:27:31 UTC	Open the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\Taurus Smith.001" SHA256`
	Then record this hash
		`a2f49fa7ce6b111c6e198de2ca4a24a8e73d6d85291805db5bede4d60fab23be`
		`CertUtil: -hashfile command completed successfully.`
		`a2f49fa7ce6b111c6e198de2ca4a24a8e73d6d85291805db5bede4d60fab23be`
		SHA256 hash recorded.

2023-12-17 14:28:19 UTC	In the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\Taurus Smith.001" MD5`
	Then record this hash
		`56aeba1a708c5210c8728e5a2560f9ca`
		`CertUtil: -hashfile command completed successfully.`
		`56aeba1a708c5210c8728e5a2560f9ca`
		MD5 hash recorded.

2023-12-17 14:28:38 UTC	In the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\Exhibit A_Back.jpg" SHA256`
	Then record this hash
		`5290f3d34b9b8b37a608c4f51781ae324e9d9c39db9162557010005d01614854`
		`CertUtil: -hashfile command completed successfully.`
		`5290f3d34b9b8b37a608c4f51781ae324e9d9c39db9162557010005d01614854`
		SHA256 hash recorded.

2023-12-17 14:29:14 UTC	In the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\Exhibit A_Back.jpg" MD5`
	Then record this hash
		`480252b5de825054fb918cb08bb7030e`
		`CertUtil: -hashfile command completed successfully.`
		`480252b5de825054fb918cb08bb7030e`
		MD5 hash recorded.

2023-12-17 14:30:44 UTC	In the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\Exhibit A_Front.jpg" SHA256`
	Then record this hash
		`164a764b6386e7f4a04301048b6f5d962195193a61bc4b95750f7def3d8d2f8e`
		`CertUtil: -hashfile command completed successfully.`
		`164a764b6386e7f4a04301048b6f5d962195193a61bc4b95750f7def3d8d2f8e`
		SHA256 hash recorded.

2023-12-17 14:31:15 UTC	In the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\Exhibit A_Front.jpg" MD5`
	Then record this hash
		`321009e97b88f3178106ef2275f7ed19`
		`CertUtil: -hashfile command completed successfully.`
		`321009e97b88f3178106ef2275f7ed19`
		MD5 hash recorded.

2023-12-17 14:32:20 UTC	Extract all files in the *pcap files.zip* archive	Files in *pcap files.zip* extracted.

2023-12-17 14:32:49 UTC	In the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\ Exhibit B and Exhibit C.pdf" SHA256`
	Then record this hash
		`c6760229562f8c2bb47be38b90877624a72d89151dbaf5de108e73b5c9a7153f`
		`CertUtil: -hashfile command completed successfully.`
		`c6760229562f8c2bb47be38b90877624a72d89151db af5de108e73b5c9a7153f`
		SHA256 hash recorded.

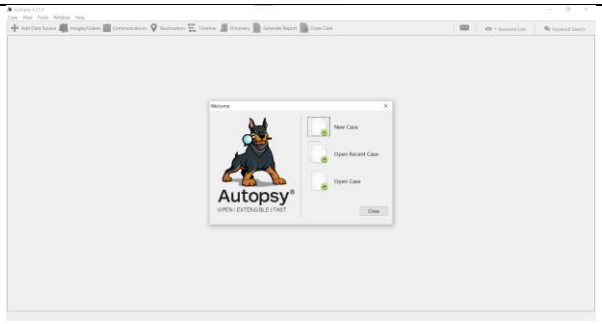
2023-12-17 14:33:51 UTC	In the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\ Exhibit B and Exhibit C.pdf" MD5`
	Then record this hash
		`321009e97b88f3178106ef2275f7ed19`
		`CertUtil: -hashfile command completed successfully.`
		`3a4ab9eba38ef8244cfaa44eec392a3e`
		MD5 hash recorded.

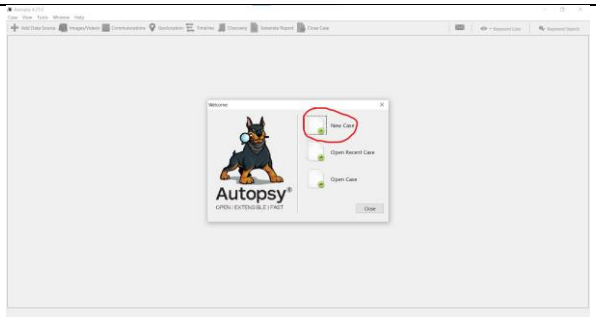
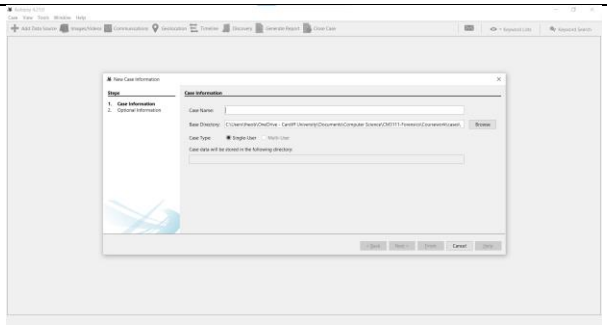
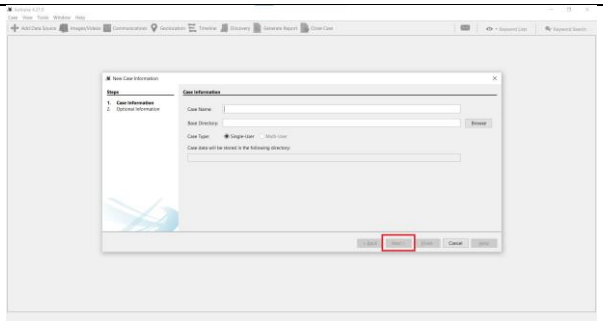
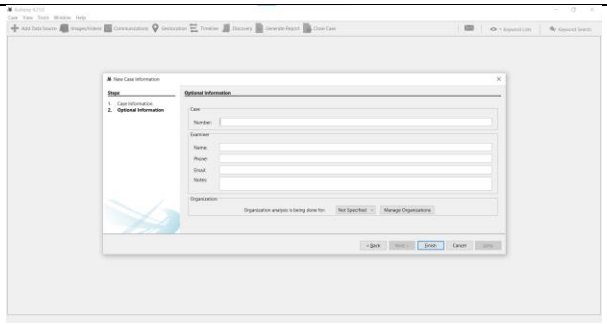
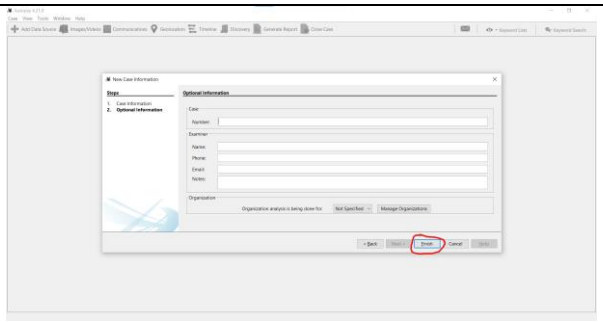
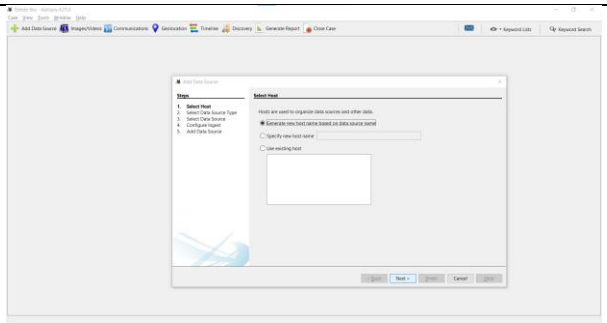
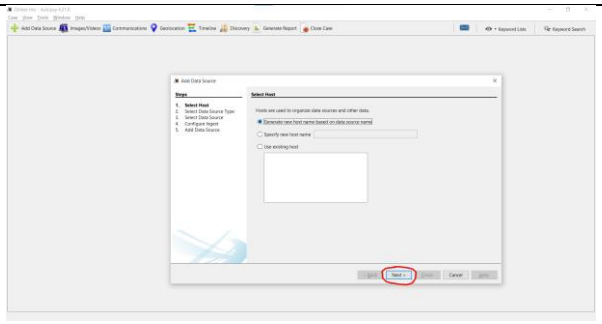
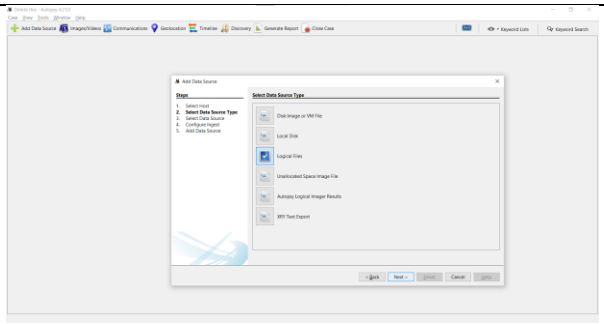
2023-12-17 14:34:29 UTC	In the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\ Exhibit D.pcapng" SHA256`
	Then record this hash
		`8f4b221f715c216d55b13089d325bec45ae5f4c143484bd0ad5c5c2d38f12292`
		`CertUtil: -hashfile command completed successfully.`
		`8f4b221f715c216d55b13089d325bec45ae5f4c1434 84bd0ad5c5c2d38f12292`
		SHA256 hash recorded.

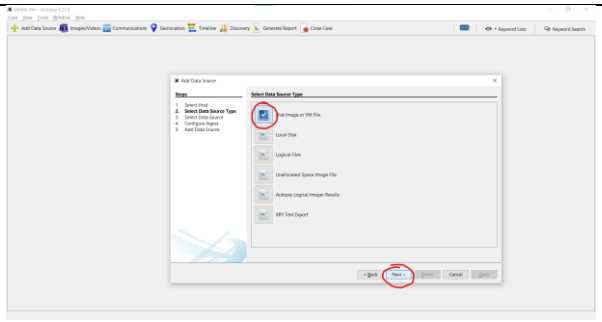
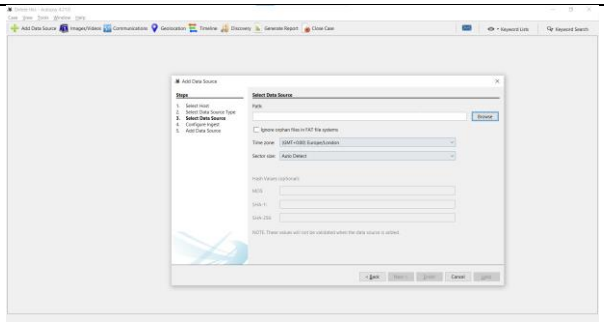
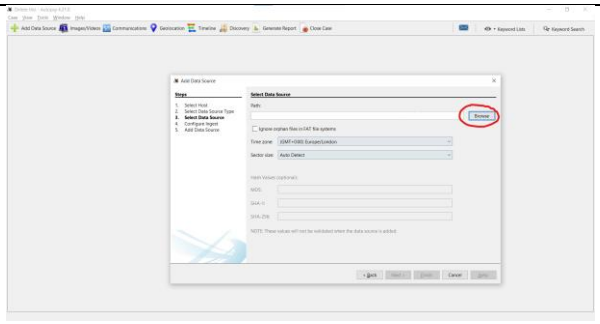
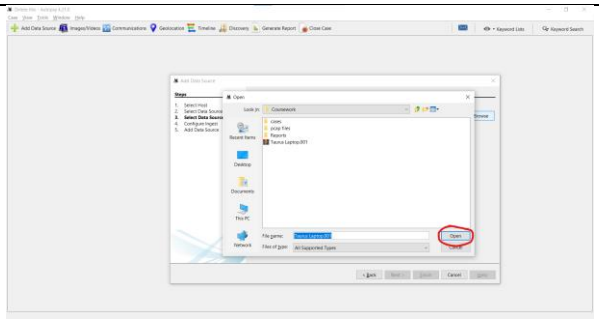
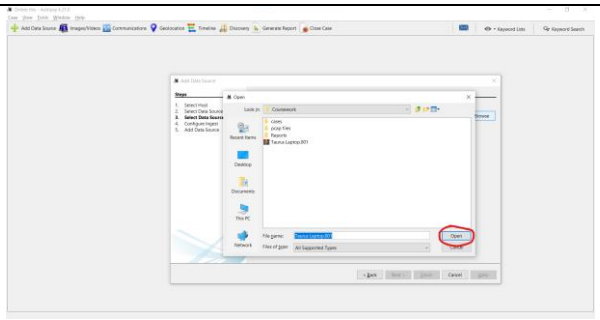
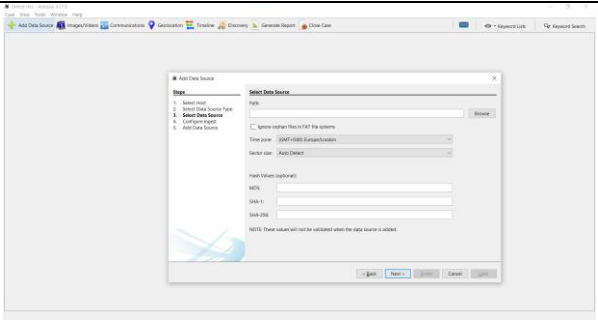
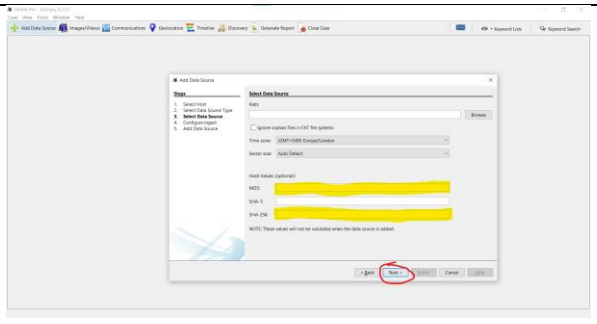
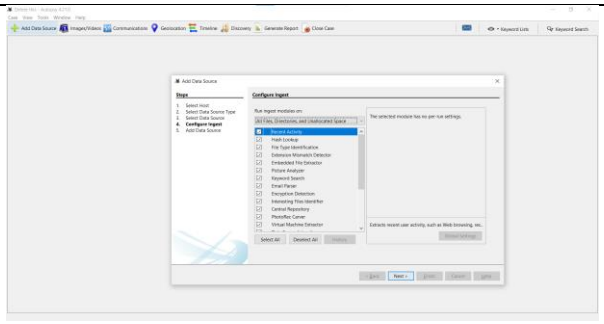
2023-12-17 14:35:15 UTC	In the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\ Exhibit D.pcapng" MD5`
	Then record this hash
		`251a1a9a8284397a70d06cadd1a5bfa6`
		`CertUtil: -hashfile command completed successfully.`
		`251a1a9a8284397a70d06cadd1a5bfa6`
		MD5 hash recorded.

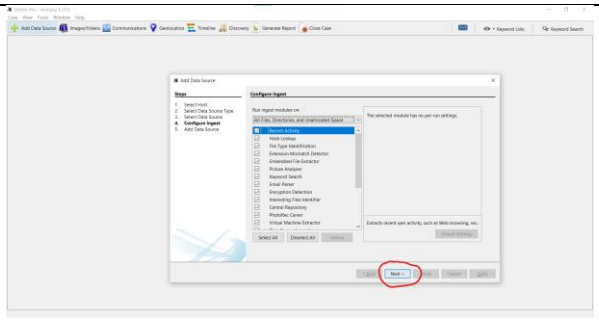
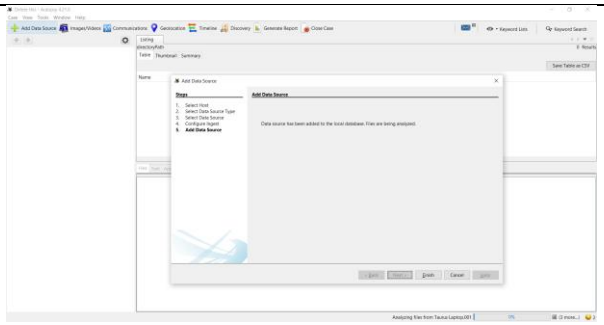
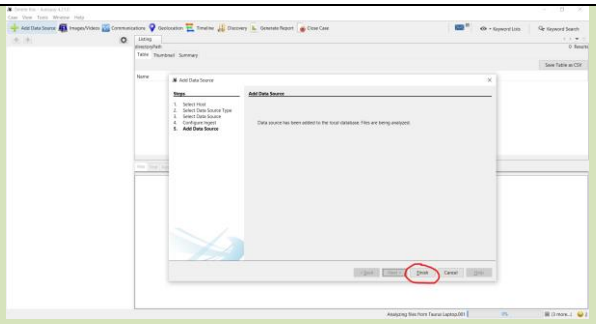
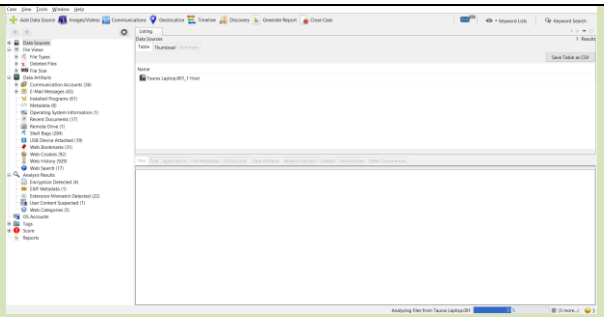
2023-12-17 14:36:12 UTC	In the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\ Exhibit E.pcapng" SHA256`
	Then record this hash
		`72359088a569ca213e92c79390a2fcebe0869c67073aae828d20f85cf76ae2ba`
		`CertUtil: -hashfile command completed successfully.`
		`72359088a569ca213e92c79390a2fcebe0869c67073 aae828d20f85cf76ae2ba`
		SHA256 hash recorded.

2023-12-17 14:36:59 UTC	In the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\ Exhibit E.pcapng" MD5`
	Then record this hash
		`756f6afcc9e40556947905ad0824b708`
		`CertUtil: -hashfile command completed successfully.`
		`756f6afcc9e40556947905ad0824b708`
		MD5 hash recorded.

2023-12-17 15:25:23 UTC	Run *Autopsy* your windows 10 virtual machine.	 *Autopsy* opened.

2023-12-17 15:26:55 UTC		
	Click *New Case* (circled in red).	*Case Information* opened.
2023-12-17 15:27:22 UTC		
	Enter case name and location and click *Next* (circled in red).	*Optional Information* opened.
2023-12-17 15:27:22 UTC		
	Enter case information (optional) and click *Finish* (circled in red).	*Add Data Source* opened.
2023-12-17 15:27:59 UTC		
	Click *Next* (circled in red).	*Select Data Source Type* opened.

2023-12-17 15:28:10 UTC	 Click *Disk Image or VM file* the click *Next* (both circled in red).	 *Select Data Source* opened.
2023-12-17 15:28:41 UTC	 Click *Browse* (circled in red).	 *File Explorer* opened.
2023-12-17 15:28:55 UTC	 Navigate to where your *Taurus Laptop.001* file is located and click *Open* (circled in red).	 *Select Data Source* opened.
2023-12-17 15:29:30 UTC	 Fill *MD5* box (highlighted) with the MD5 hash: `56aeba1a708c5210c8728e5a2560f9ca`	 *Configure Ingest* opened.

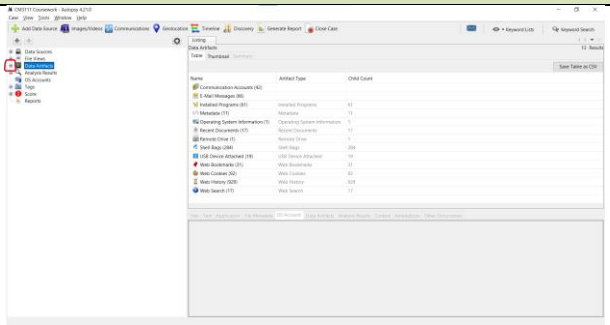
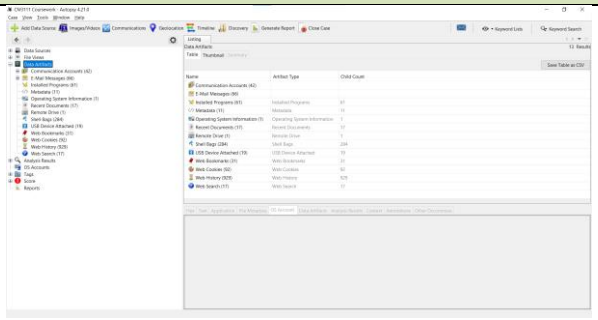
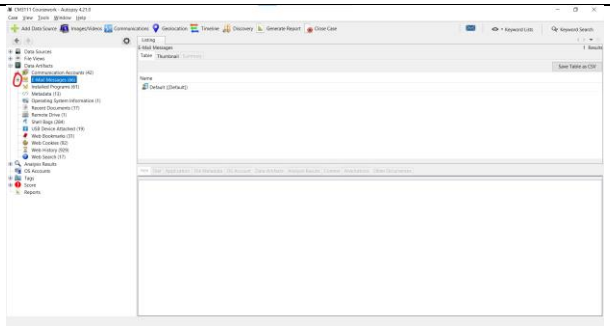
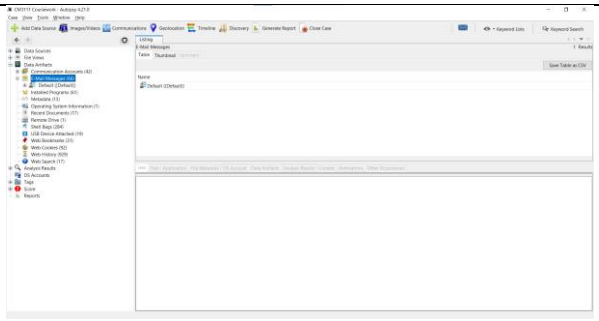
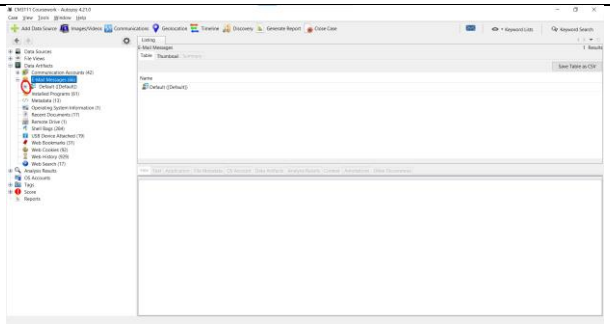
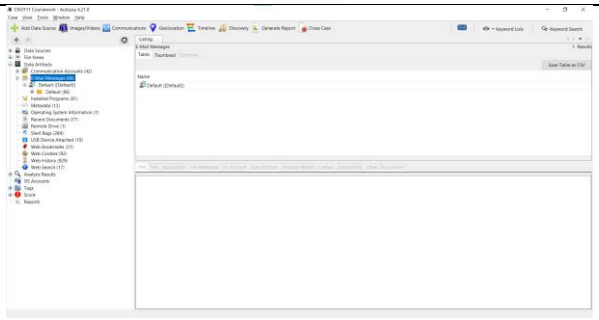
	Fill *SHA-256* box (highlighted) with SHA256 hash: `a2f49fa7ce6b111c6e198de2ca4a24a8e73d6d85291805db5bede4d60fab23be` Click *Next* (circled in red).	
2023-12-17 15:30:00 UTC	 Click *Next* (circled in red).	 *Add Data Source* opened.
2023-12-17 15:30:55 UTC	 Click *Finish* (circled in red).	 *Autopsy* setup complete.

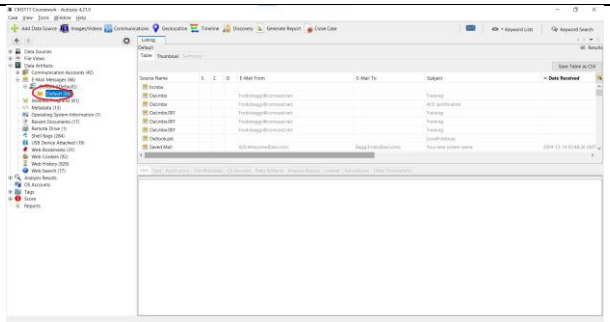
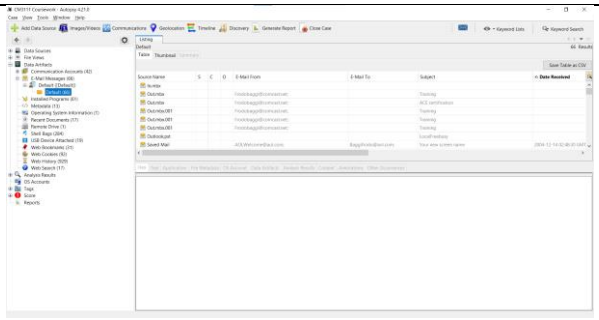
2.3 Investigation

A method for each of these areas will be provided to establish how any evidence pieces were obtained. This section's purpose is to demonstrate how to recreate the evidence collection, not to document every single file analysed, which would be too expansive for the scope of this technical report. Any notable files found through the analysis methods below will be expanded upon in *Section 4: Analysis and Findings*, and any additional steps needed beyond what is detailed in this section will also be expanded upon in *Section 4: Analysis and Findings*.

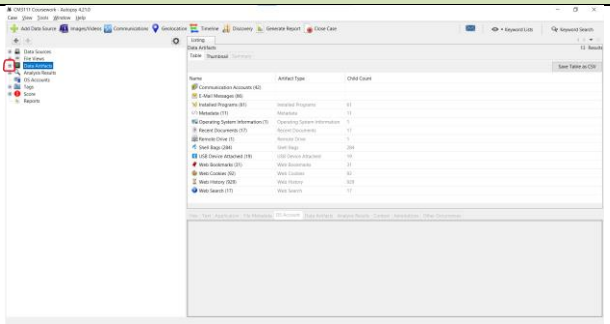
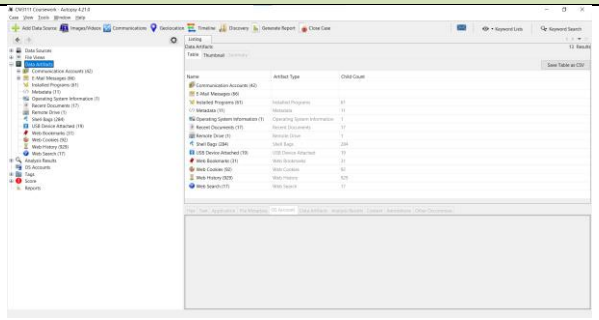
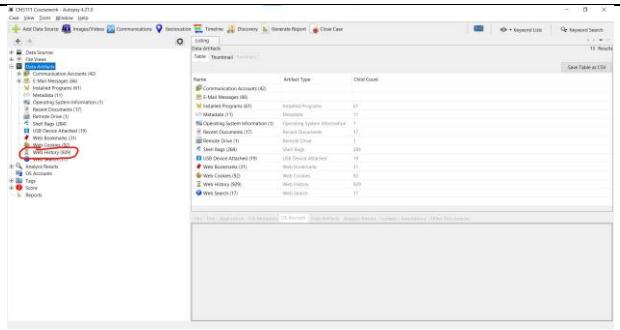
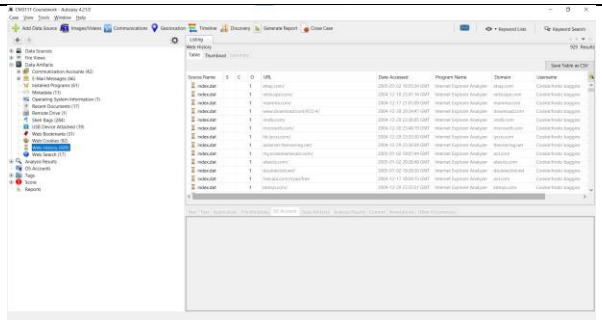
2.3.1 Email

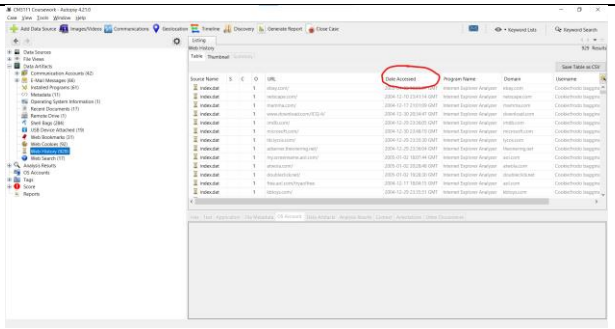
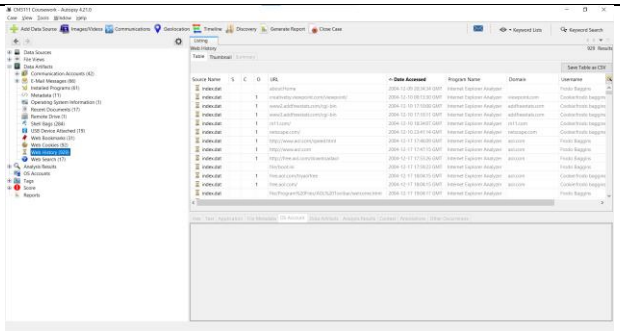
Date/Time	Action	Outcome

2023-12-28 09:20:11 UTC	Open *Autopsy* to view seen in section 3.2.2	*Autopsy* opened to view seen in section 3.2.2
2023-12-28 09:20:57 UTC	 Click the + box left of *Data Artifacts* (circled in red).	 *Data Artifacts* folder expanded.
2023-12-28 09:21:47 UTC	 Click the + box left of *E-Mail Messages* (circled in red).	 *E-Mail Messages* folder expanded.
2023-12-28 09:22:21 UTC	 Click the + box left of *Default* (circled in red).	 *Default* folder expanded.

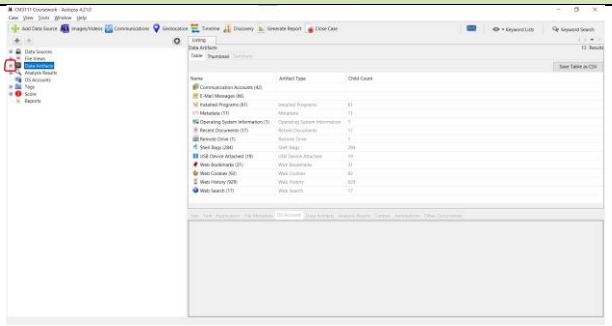
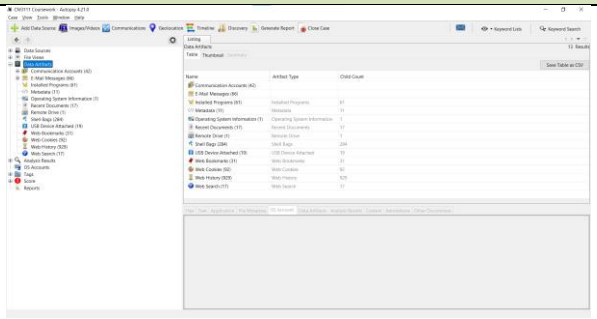
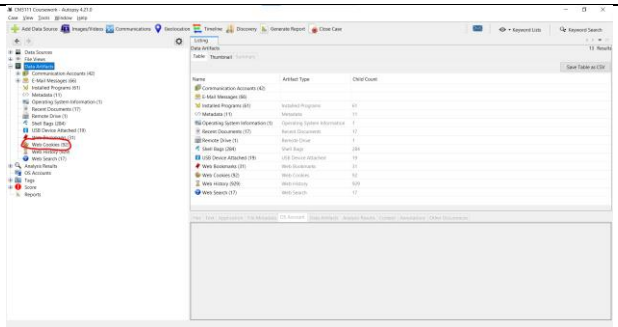
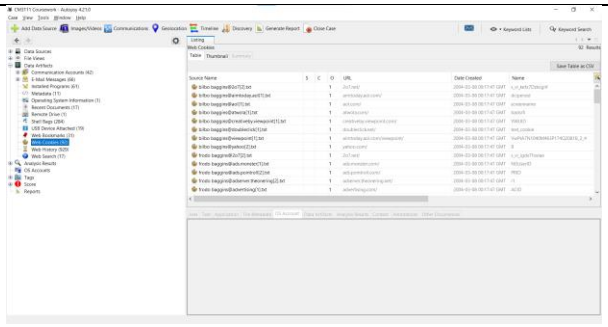
2023-12-28 09:22:27 UTC	 Click *Default* (circled in red).	 All email events from the image displayed on the right panel.

2.3.2 Web Activity History

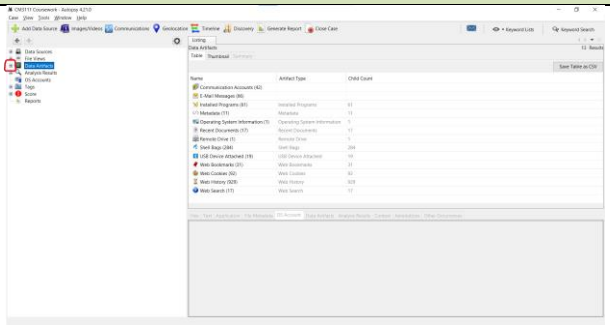
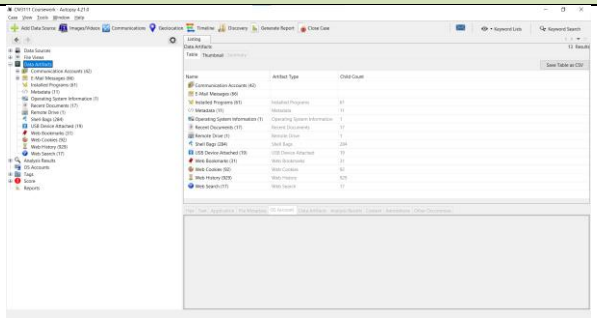
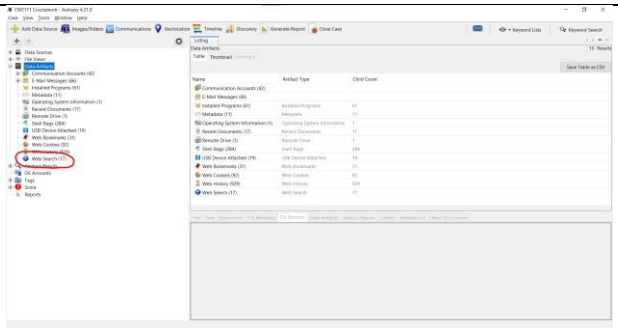
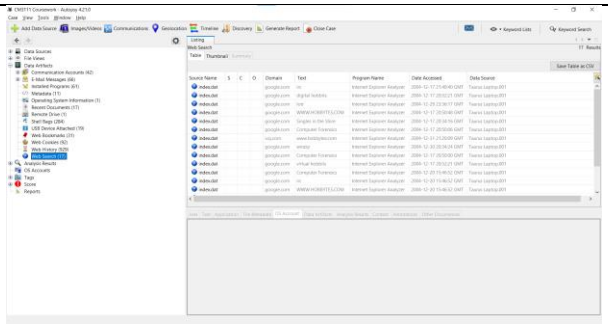
Date/Time	Action	Outcome
2023-12-20 15:20:55 UTC	Open *Autopsy* to view seen in section 3.2.2	*Autopsy* opened to view seen in section 3.2.2
2023-12-20 15:20:57 UTC	 Click the + box left of *Data Artifacts* (circled in red).	 *Data Artifacts* folder expanded.
2023-12-20 15:21:56 UTC	 Click *Web History* text (circled in red).	 All pages recorded in every browsers web history shown on right panel

2023-12-20 15:22:47 UTC	 Click the *Date Accessed* box (circled in red)	 Items in history sorted by date accessed

Cookies

Date/Time	Action	Outcome
2023-12-20 15:20:55 UTC	Open *Autopsy* to view seen in section 3.2.2	*Autopsy* opened to view seen in section 3.2.2
2023-12-20 15:30:09 UTC	 Click the + box left of *Data Artifacts* (circled in red).	 *Data Artifacts* folder expanded.
2023-12-20 15:31:40 UTC	 Click *Web Cookies* text (circled in red).	 All cookies recorded in every browsers web history shown on right panel

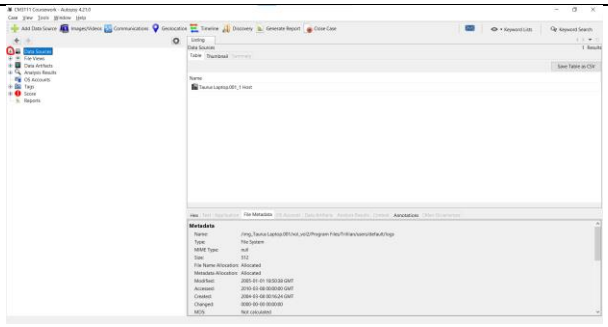
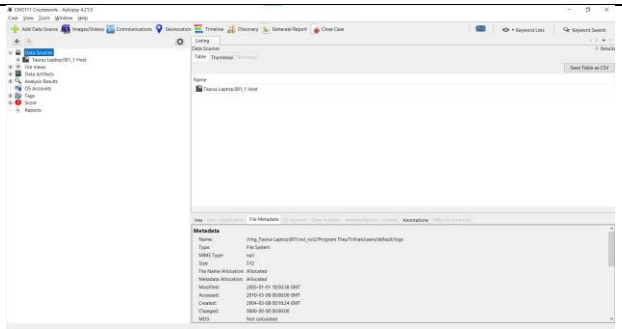
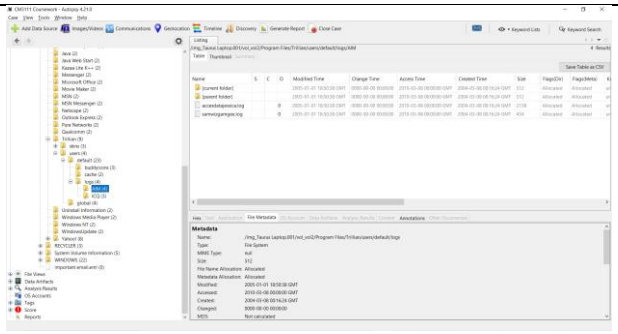
Searches

Date/Time	Action	Outcome
2023-12-20 15:20:55 UTC	Open *Autopsy* to view seen in section 3.2.2	*Autopsy* opened to view seen in section 3.2.2
2023-12-20 15:35:21 UTC	 Click the + box left of *Data Artifacts* (circled in red).	 *Data Artifacts* folder expanded.
2023-12-20 15:36:23 UTC	 Click *Web Search* text (circled in red).	 All cookies recorded in every browsers web history shown on right panel

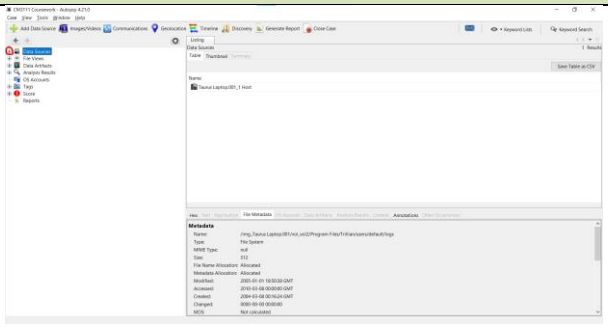
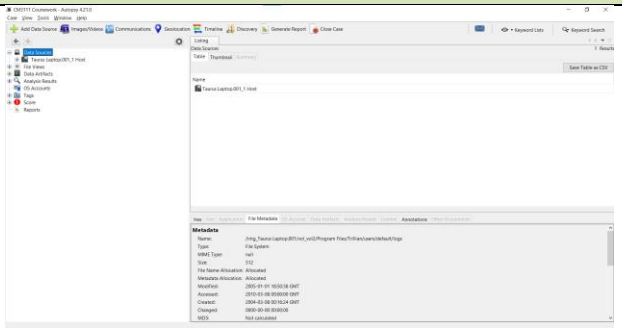
2.3.3 Chat Logs/Communication Data

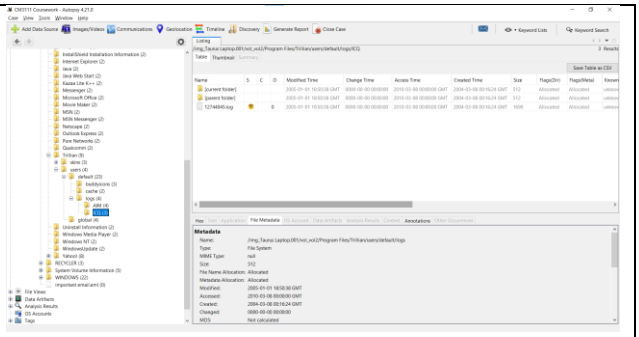
AIM Logs

Date/Time	Action	Outcome
2023-12-20 15:20:55 UTC	Open *Autopsy* to view seen in section 3.2.2	*Autopsy* opened to view seen in section 3.2.2

2023-12-20 16:04:57 UTC	 Click the + box to the left of *Data Sources* (circled in red).	 *Data* Source folder expanded to show *Taurus Laptop.001_ 1 Host*.
2023-12-20 16:06:17 UTC	Navigate to the following location in *Taurus Laptop.001_ 1 Host*: `/img_Taurus Laptop.001/vol_vol2/Program Files/Trillian/users/default/logs/AIM`	 *AIM* logs are shown in the right panel.

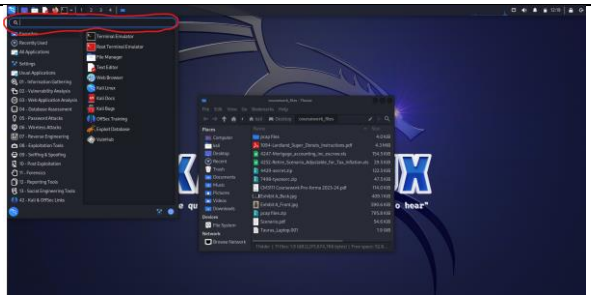
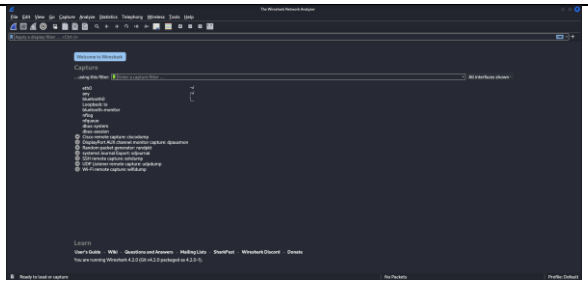
ICQ Logs

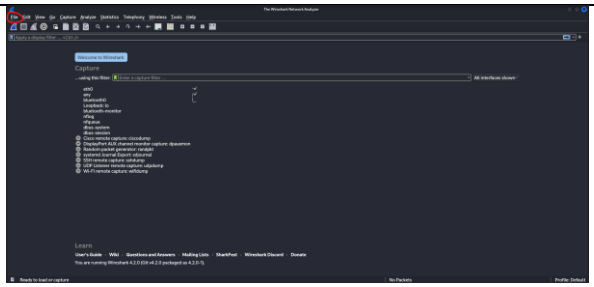
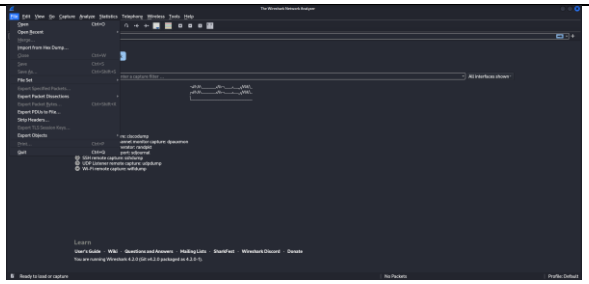
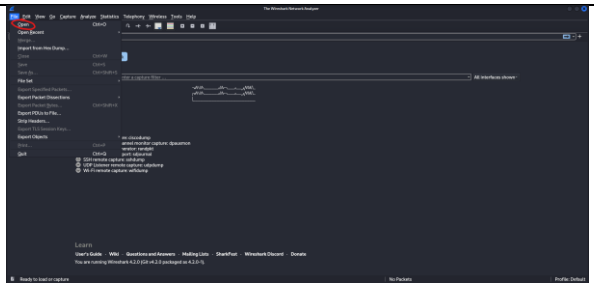
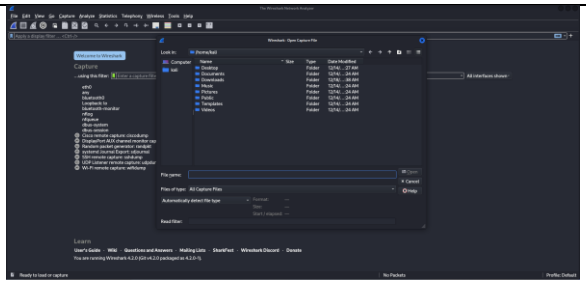
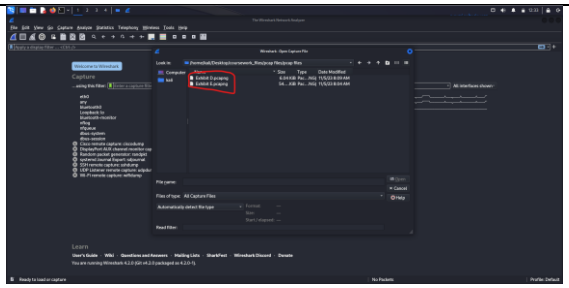
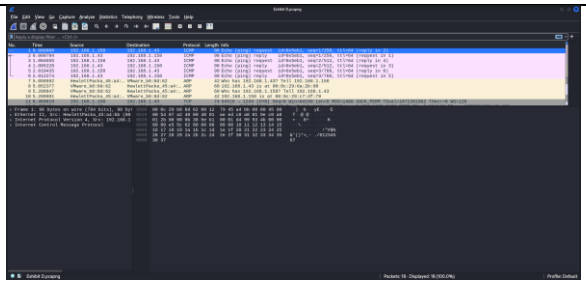
Date/Time	Action	Outcome
2023-12-20 15:20:55 UTC	Open *Autopsy* to view seen in section 3.2.2	*Autopsy* opened to view seen in section 3.2.2
2023-12-20 16:23:45 UTC	 Click the + box to the left of *Data Sources* (circled in red).	 *Data* Source folder expanded to show *Taurus Laptop.001_ 1 Host*.

2023-12-20 16:25:01 UTC	Navigate to the following location in *Taurus Laptop.001_1 Host*: `/img_Taurus Laptop.001/vol_vol2/Program Files/Trillian/users/default/logs/ICQ`	 *ICQ* logs are shown in the right panel.

2.3.4 Network

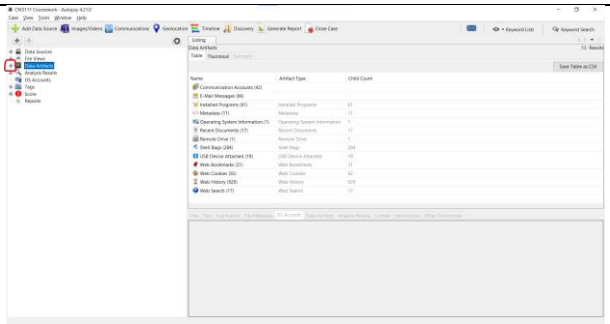
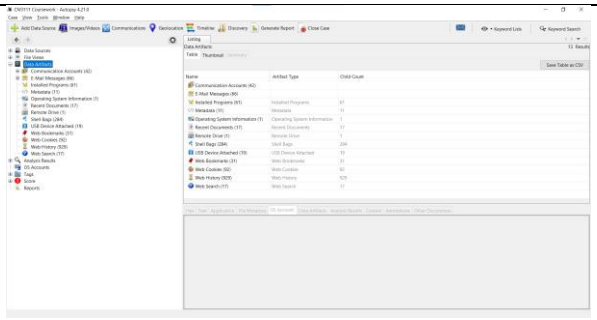
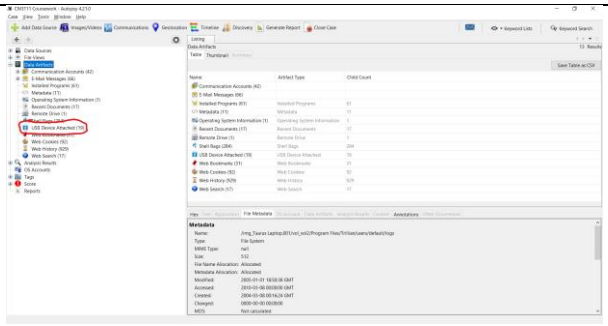
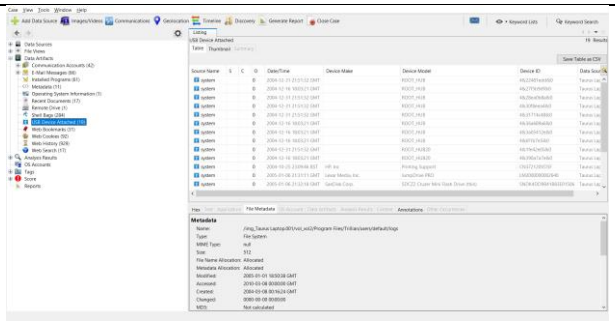
Date/Time	Action	Outcome
2023-12-20 17:05:20 UTC	Copy *pcap files.zip* into *VMware Kali Linux*.	*pcap files.zip* copied into *VMware Kali Linux*.
2023-12-20 17:05:43 UTC	 Open folder containing *pcap files.zip* (Exhibit B,C,D,E).	Folder containing *pcap files.zip* (Exhibit B,C,D,E) opened
2023-12-20 17:05:52 UTC	 Right-click *pcap files.zip* (Exhibit B,C,D,E).	 Options menu displayed for *pcap files.zip* (Exhibit B,C,D,E).

2023-12-20 17:12:01 UTC	 Click *Extract Here* (circled in red).	 Contents of *pcap files.zip* extracted to current directory inside folder *pcap files* (circled in red).
2023-12-20 17:16:59 UTC	 Click the *Kali Linux* logo (circled in red).	 Application search opened.
2023-12-20 17:20:04 UTC	 Inside the search bar (circled in red) type "wireshark".	 *Wireshark* appears in search results.
2023-12-20 17:20:50 UTC	 Click *Wireshark*.	 *Wireshark* opened.

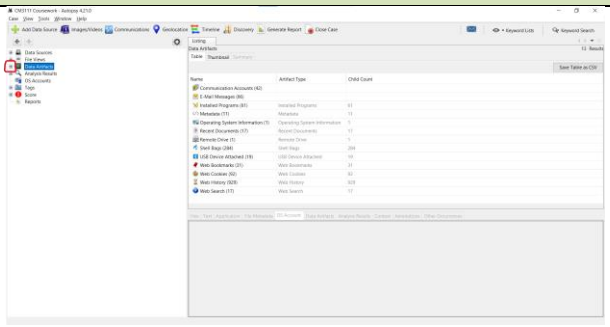
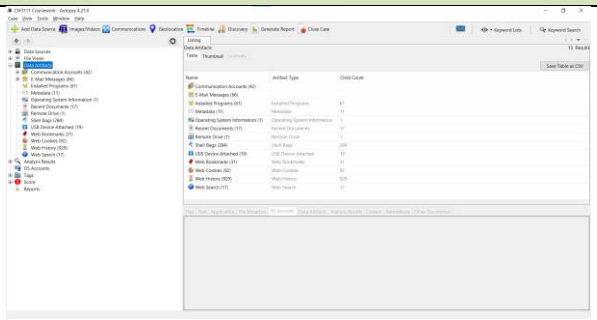
2023-12-20 17:24:14 UTC	 Click *File* (circled in red).	 *File* menu opened.
2023-12-20 17:26:52 UTC	 Click *Open* (circled in red).	 File explorer opened.
2023-12-20 17:27:23 UTC	 Navigate to the folder containing the *pcap files* folder and click either *Exhibit D.pcapng* or *Exhibit E.pcapng*.	 File opened in *Wireshark*.

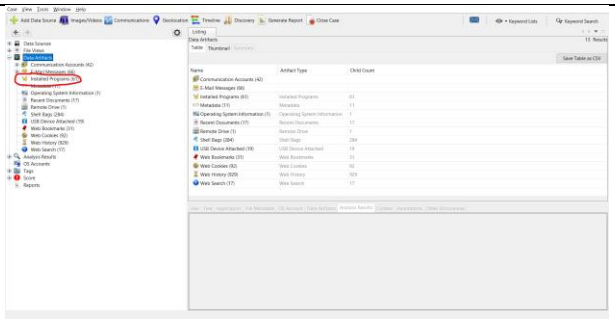
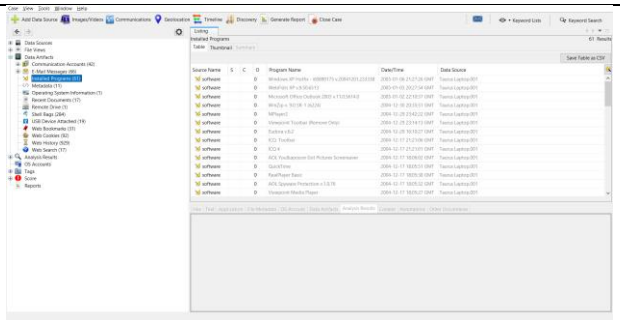
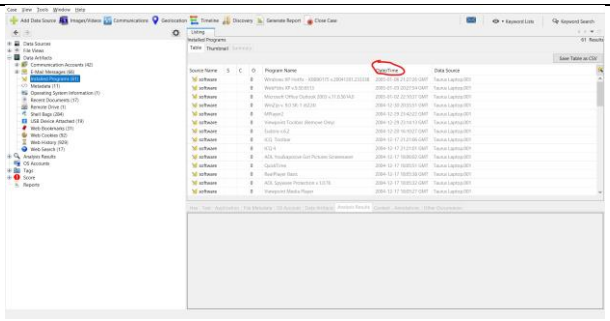
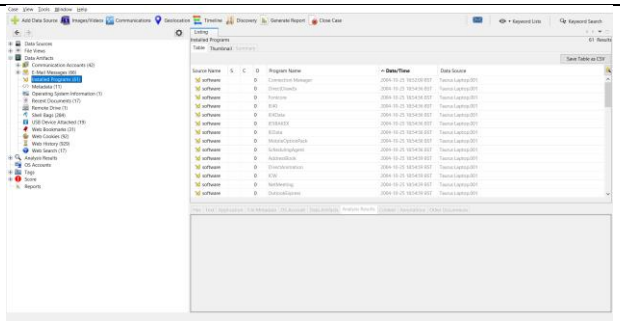
2.3.5 Attached Devices

Date/Time	Action	Outcome
2023-12-20 16:33:10 UTC	Open *Autopsy* to view seen in section 3.2.2	*Autopsy* opened to view seen in section 3.2.2

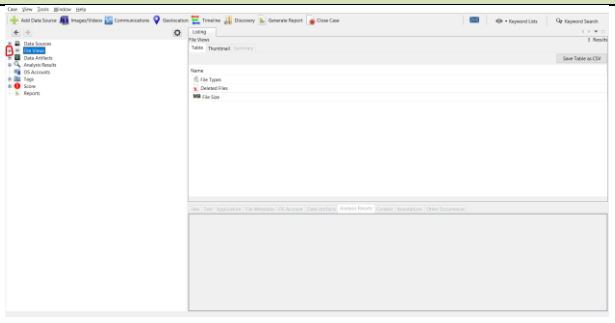
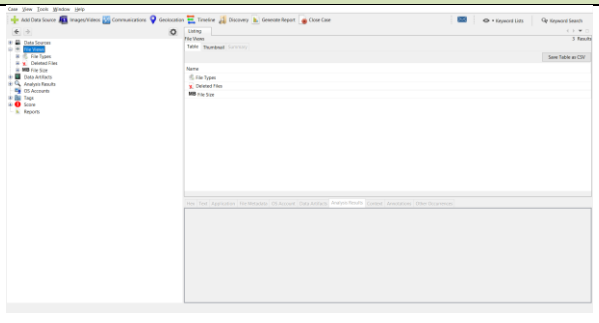
2023-12-20 16:33.22 UTC	 Click the + box left of *Data Artifacts* (circled in red).	 *Data Artifacts* folder expanded.
2023-12-20 16:34.19 UTC	 Click the *USB Device Attached* text (circled in red).	 All USB devices attached to the laptop are shown on right panel.

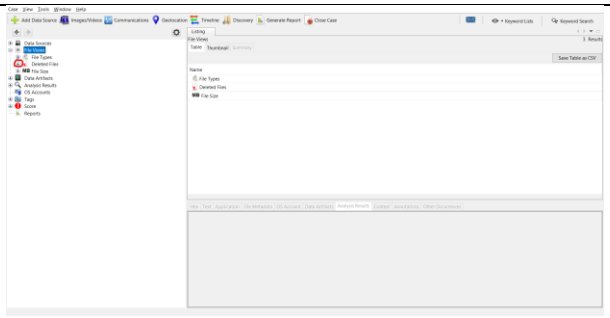
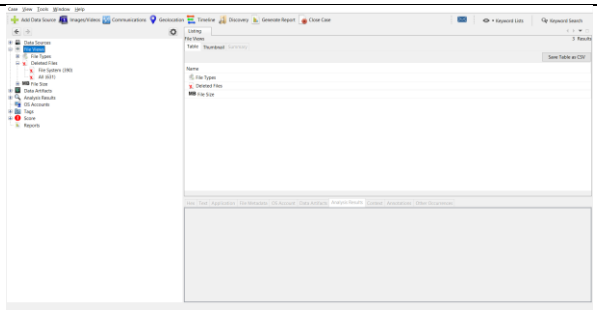
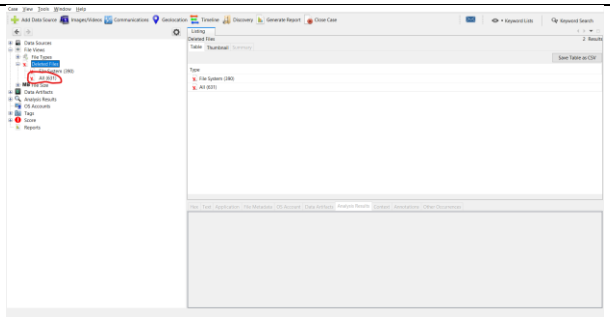
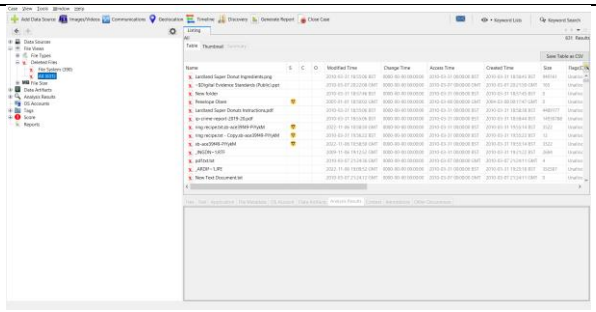
2.3.6 Programs Installed

Date/Time	Action	Outcome
2023-12-20 16:43:30 UTC	Open *Autopsy* to view seen in section 3.2.2	*Autopsy* opened to view seen in section 3.2.2
2023-12-20 16:44.22 UTC	 Click the + box left of *Data Artifacts* (circled in red).	 *Data Artifacts* folder expanded.

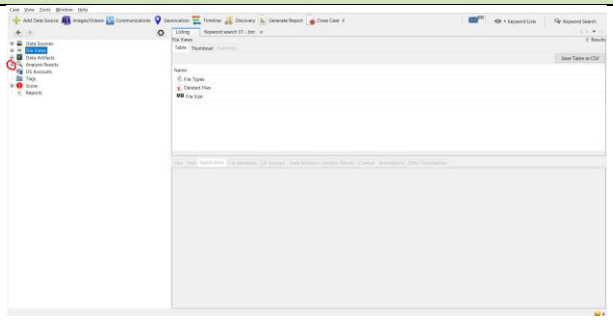
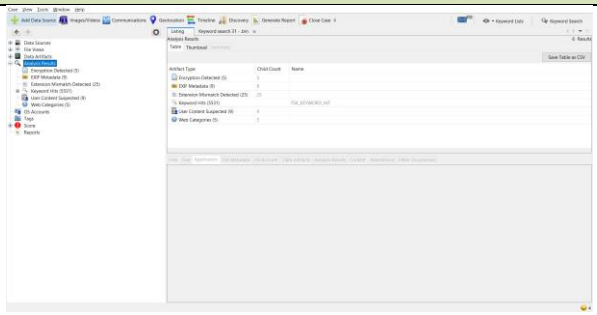
2023-12-20 16:45.43 UTC	 Click the *Installed Programs* text (circled in red).	 All installed programs attached to the laptop are shown on right panel.
2023-12-20 16:45.50 UTC	 Click the *Date/Time* text (circled in red).	 Installed programs are ordered from oldest to newest.

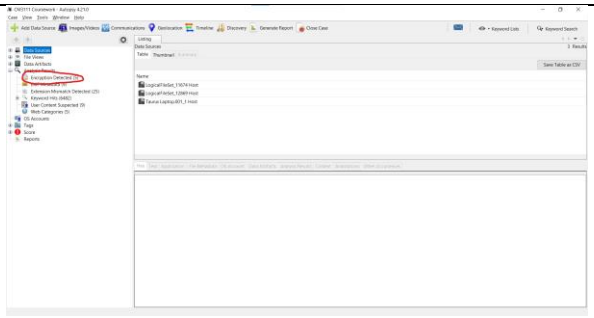
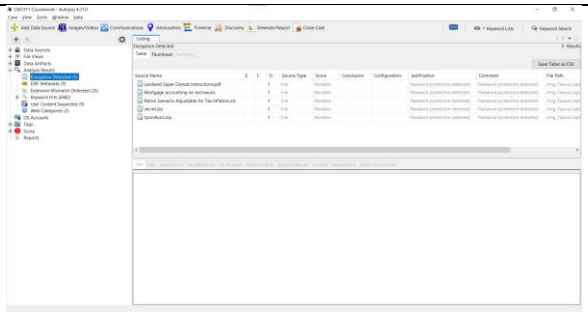
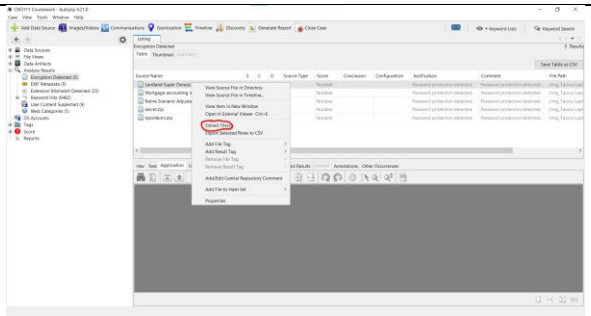
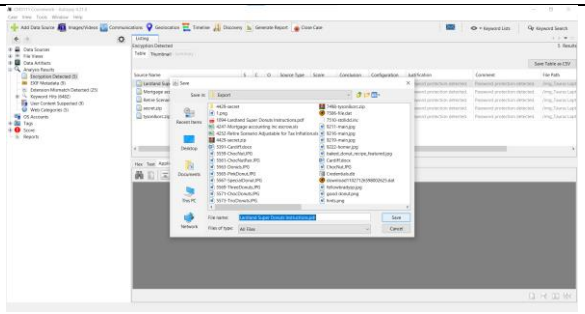
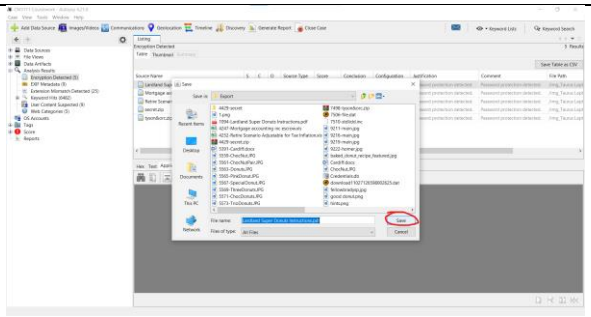
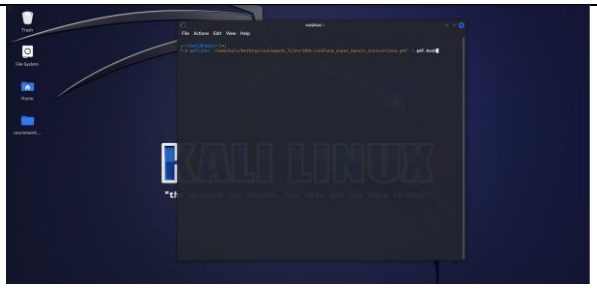
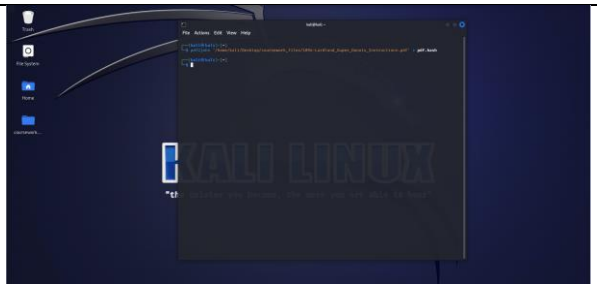
2.3.7 Deleted Files

Date/Time	Action	Outcome
2023-12-20 16:53:42 UTC	Open *Autopsy* to view seen in section 3.2.2	*Autopsy* opened to view seen in section 3.2.2
2023-12-20 16:55.12 UTC	 Click the + box left of *File Views* (circled in red).	 *File Views* folder expanded.

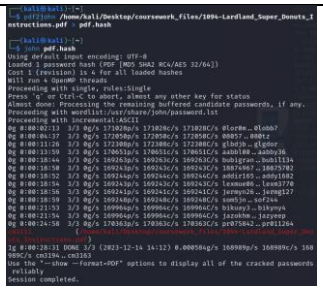
2023-12-20 16:55.27 UTC	 Click the + box left of *Deleted Files* (circled in red).	 *Deleted Files* folder expanded.
2023-12-20 16:57.05 UTC	 Click the *All* box (circled in red).	 All deleted files are shown in the right panel.

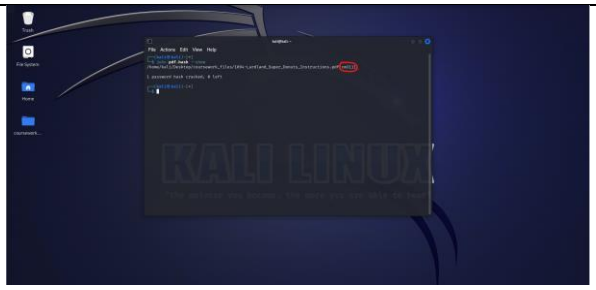
2.3.8 Encrypted Files

Date/Time	Action	Outcome
2023-12-29 19:15:03 UTC	Open *Autopsy* to view seen in section 3.2.2	*Autopsy* opened to view seen in section 3.2.2
2023-12-29 19:16.25 UTC	 Click the + box left of *Analysis Results* (circled in red).	 *Analysis Results* folder expanded.

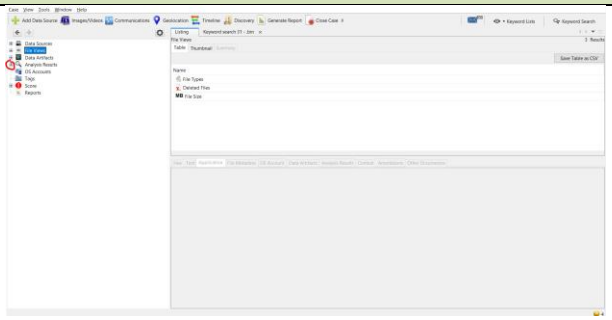
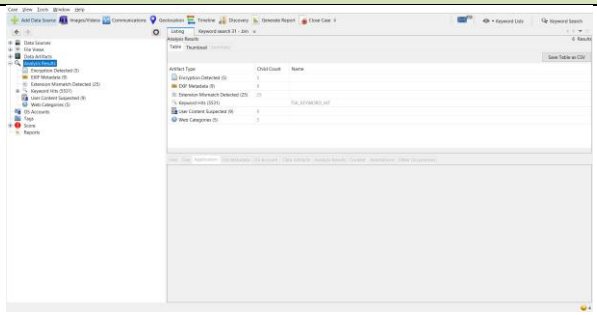
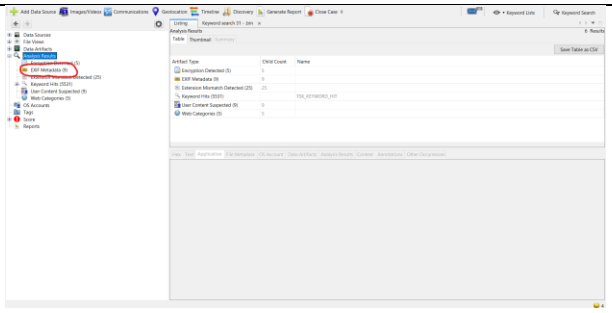
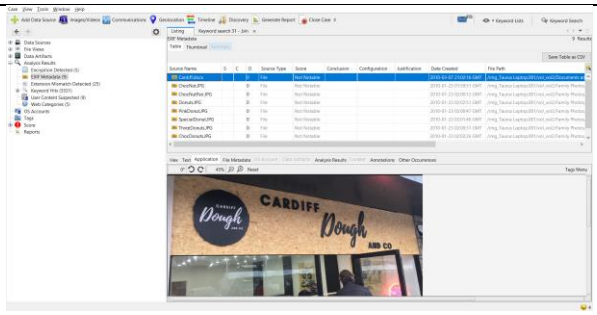
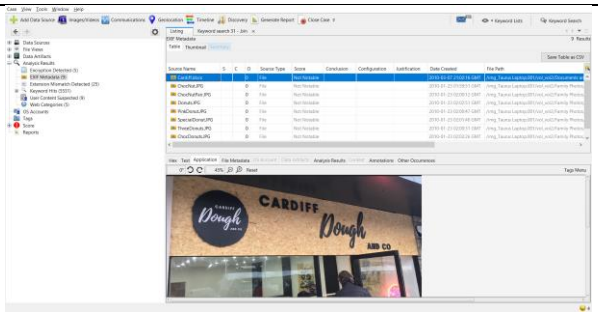
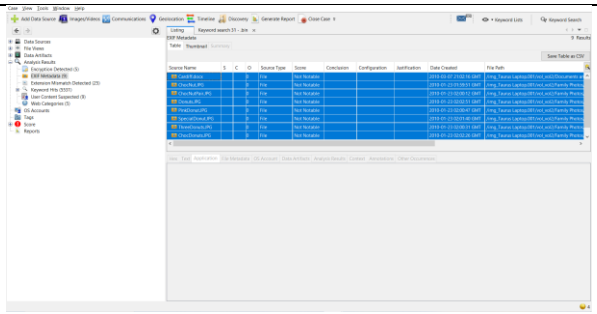
2023-12-29 19:16.30 UTC	 Click *Encryption Detected* (circled in red).	 *Encryption Detected* folder expanded.
2023-12-29 19:16.46 UTC	 Right click on a file and click *Extract File(s).*	 *File Explorer* Opened.
2023-12-29 19:16.59 UTC	 Click *Save*.	Encrypted file extracted.
2023-12-29 19:17.08 UTC	Copy exported file into *Kali Linux* virtual machine.	File with encryption copied into *Kali Linux* virtual machine.
2023-12-29 19:17.31 UTC	 If the encrypted file is a PDF then the following into to the terminal:	 Password hash generated.

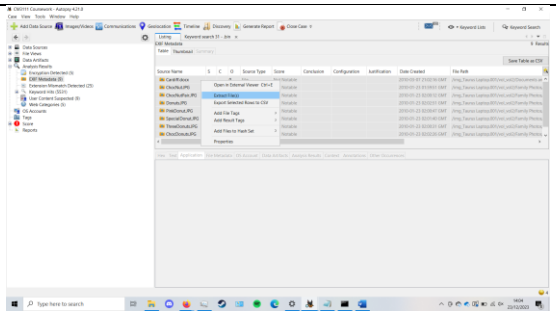
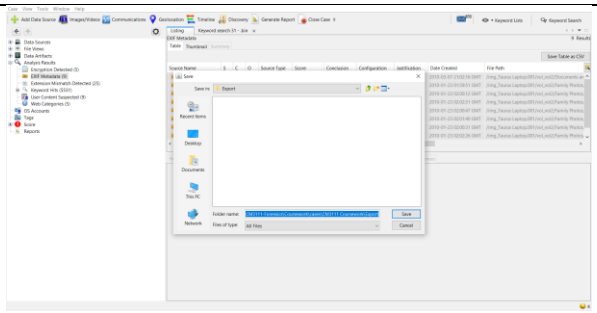
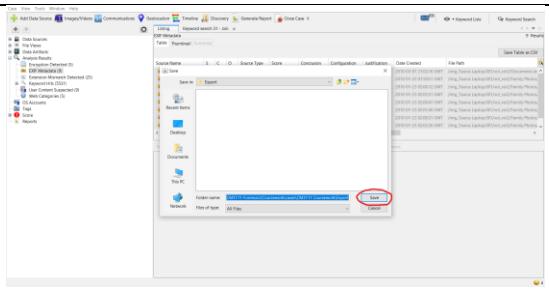
	`pdf2john "PATH TO ENCRYPTED PDF" > pdf.hash`
	If the encrypted file is a ZIP then type:
	`zip2john "PATH TO ENCRYPTED ZIP" > zip.hash`
	If the encrypted file is a *Microsoft Office* document then type:
	`office2john "PATH TO ENCRYPTED OFFICE FILE" > office.hash`	

2023-12-29
19:17.44 UTC
	
	If the encrypted file is a PDF then the following into to the terminal:
	`john pdf.hash`
	If the encrypted file is a ZIP then type:
	`john zip.hash`
	If the encrypted file is a *Microsoft Office* document then type:
	`john office.hash`
		
		John the Ripper program begins to test passwords on encrypted file.

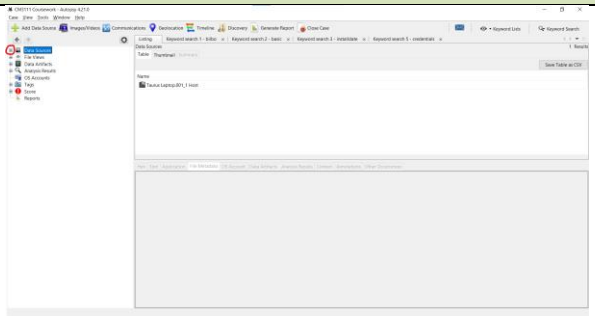
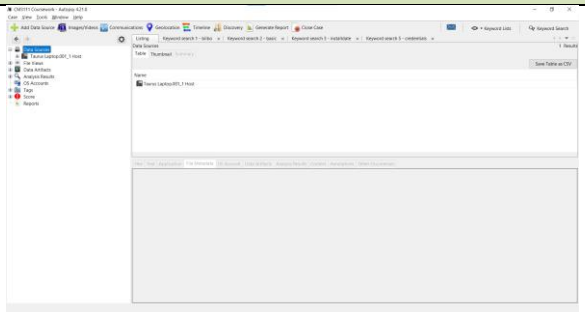
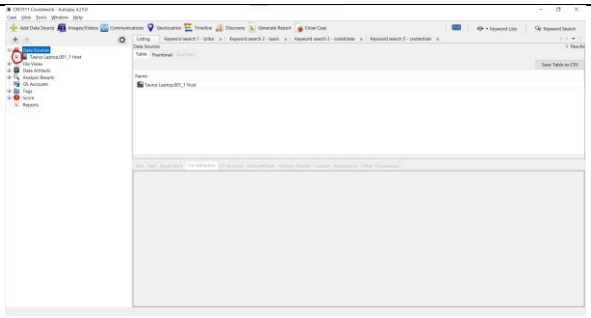
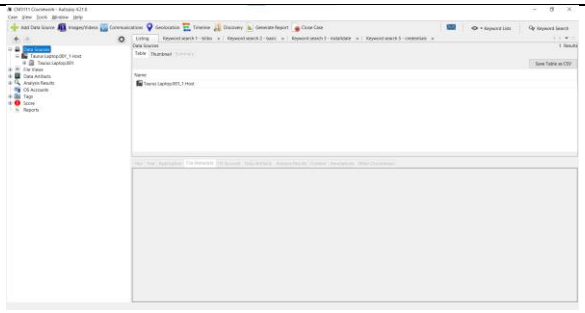
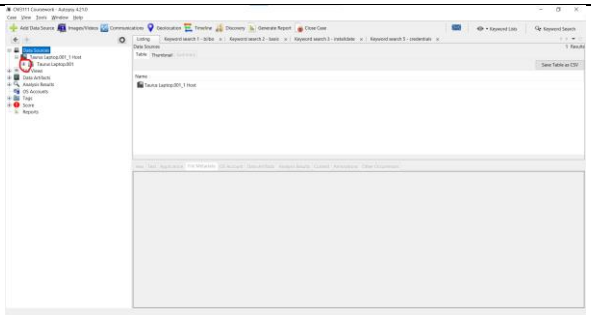
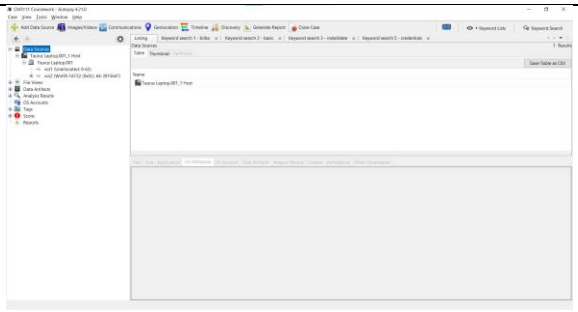
2023-12-29
19:46.12 UTC
	
	If the encrypted file is a PDF then the following into to the terminal:
	`john pdf.hash --show`
	If the encrypted file is a ZIP then type:
	`john zip.hash --show`
	If the encrypted file is a *Microsoft Office* document then type:
	`john office.hash --show`
		
		Password for encrypted file shown (circled in red).

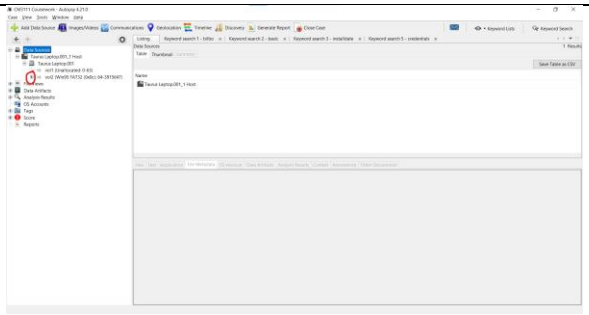
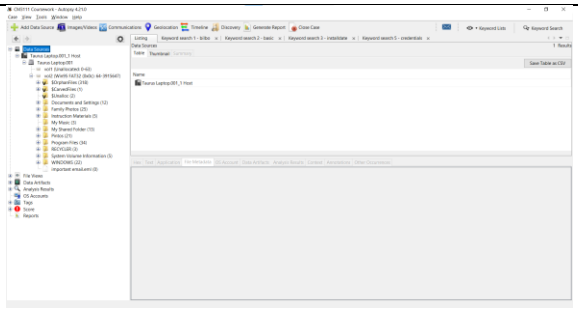
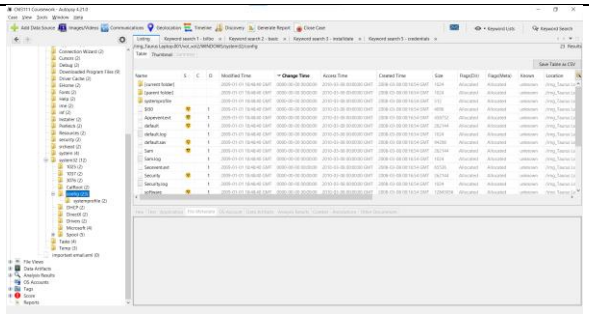
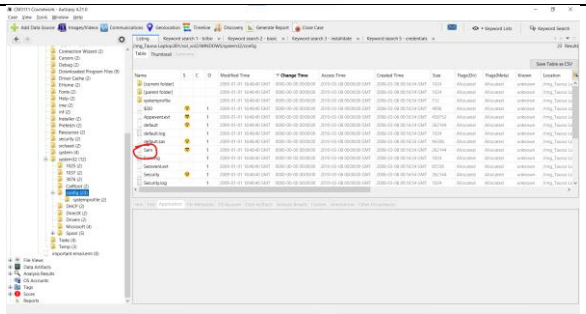
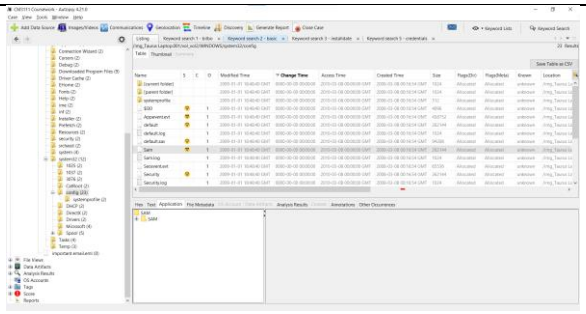
2.3.9 EXIF Metadata

Date/Time	Action	Outcome
2023-12-23 13:58:03 UTC	Open *Autopsy* to view seen in section 3.2.2	*Autopsy* opened to view seen in section 3.2.2
2023-12-23 13:59.29 UTC	 Click the + box left of *Analysis Results* (circled in red).	 *Analysis Results* folder expanded.
2023-12-23 13:59.43 UTC	 Click the *EXIF Metadata* box (circled in red).	 *EXIF Metadata* folder expanded.
2023-12-23 14:00:12 UTC	 Click *ctrl+a*.	 All files with *EXIF Metadata* selected.

2023-12-23 14:02:36 UTC	 *Right click* + *Extract Files(s)*	 File explorer opened in *export* folder.
2023-12-23 14:06:40 UTC	 Click *Save* (circled in red)	Files with *EXIF metadata* exported.
2023-12-23 14:07:42 UTC	Copy exported file into *Kali Linux* virtual machine.	File with EXIF metadata copied into *Kali Linux* virtual machine.
2023-12-23 14:09:24 UTC	 In the terminal type: `sudo apt-get install exiftool`	 *Exiftool* installed.
2023-12-23 14:09:59 UTC	 In the terminal type: `exiftool "{PATH TO FILE}".`	 Observe EXIF metadata.

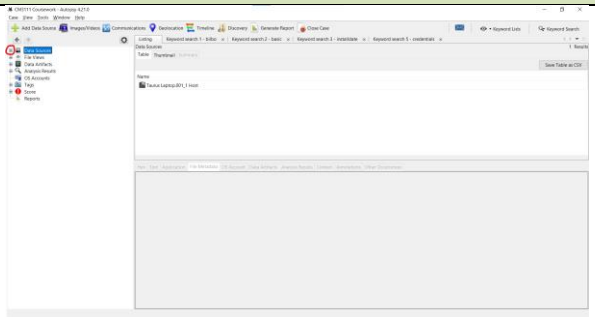
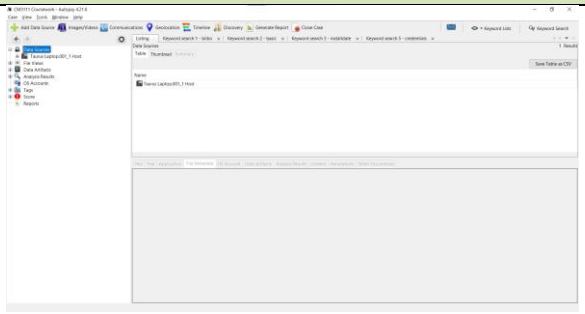
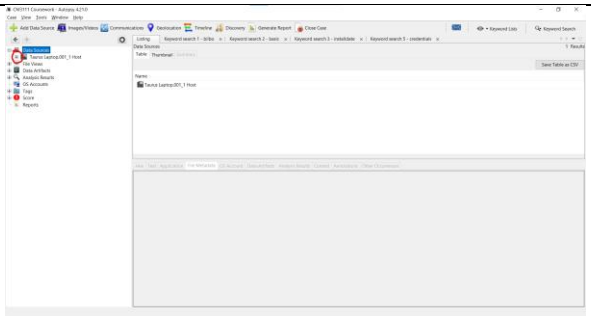
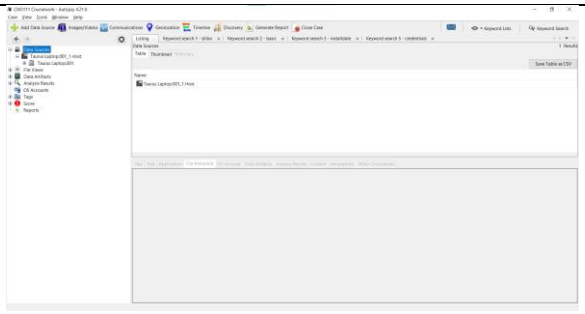
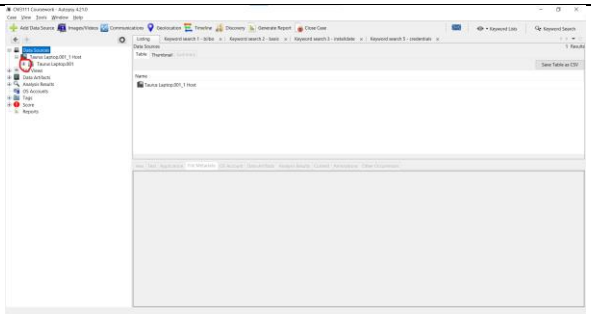
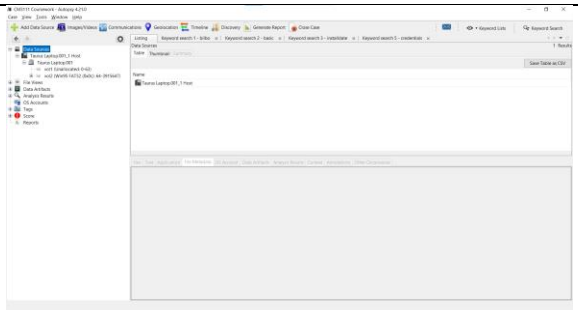
2.3.10 Registry

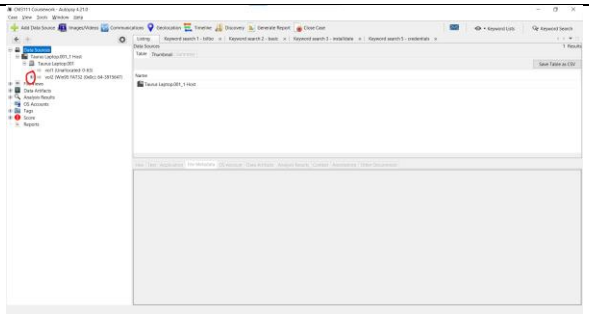
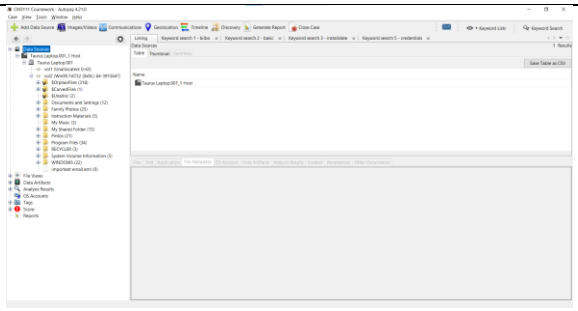
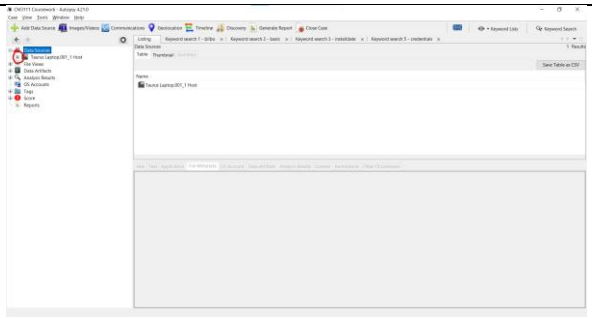
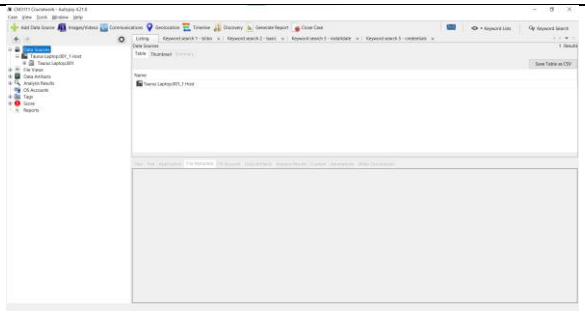
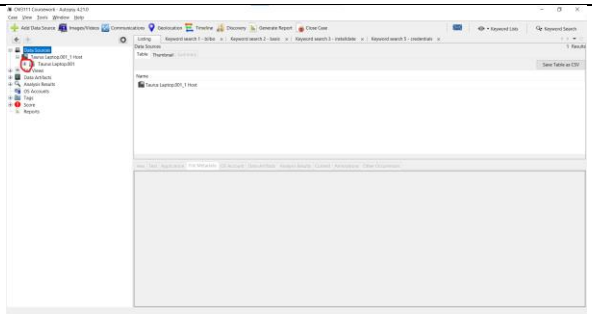
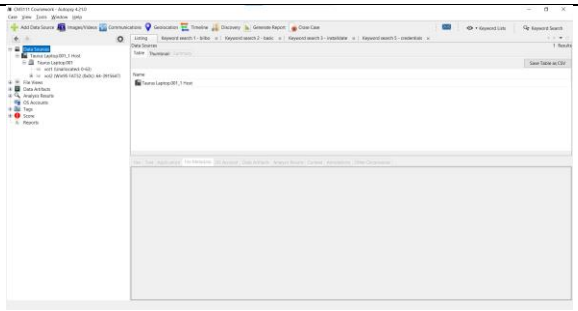
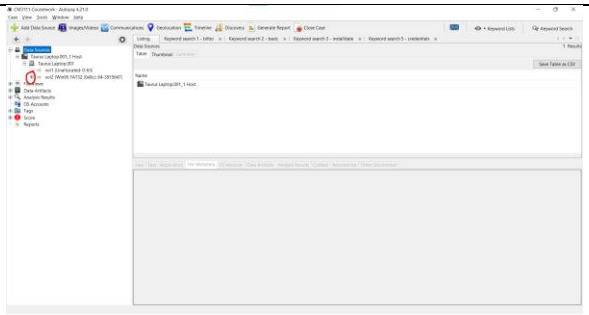
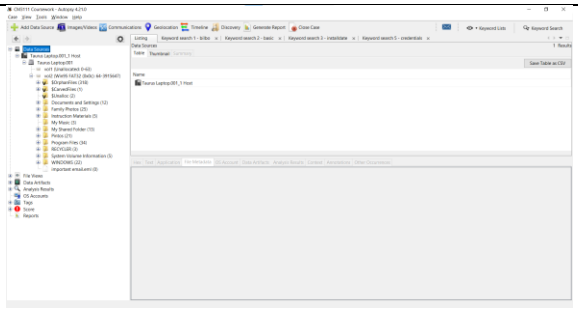
Date/Time	Action	Outcome
2024-01-06 21:59:13 UTC	Open *Autopsy* to view seen in section 3.2.2	*Autopsy* opened to view seen in section 3.2.2
2024-01-06 21:59:40 UTC	 Click the + box left of *Data Sources* (circled in red).	 *Data Sources* folder expanded.
2024-01-06 22:00:12 UTC	 Click the + box left of *Taurus Laptop.001_ 1 Host* (circled in red).	 *Taurus Laptop.001_ 1 Host* folder expanded.
2024-01-06 22:00:56 UTC	 Click the + box left of *Taurus Laptop.001* (circled in red).	 *Taurus Laptop.001* folder expanded.

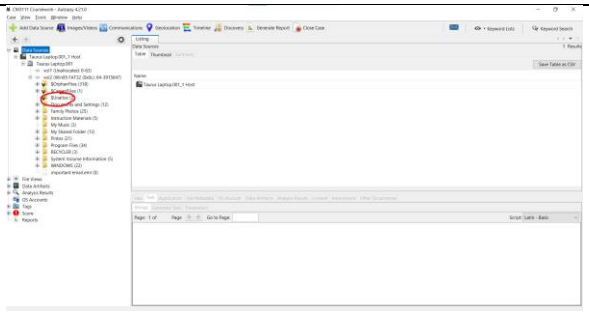
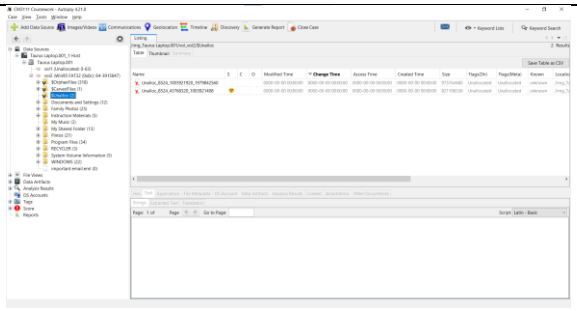
2024-01-06 22:01:19 UTC	 Click the + box left of *vol2* (circled in red).	 *vol2* folder expanded.
2024-01-06 22:01:31 UTC	 Navigate to *WINDOWS/system32/config*.	*config* folder expanded.
2024-01-06 22:02:05 UTC	 Select a registry hive out of the following (SAM is circled in red in this case): - default - Sam - Security - software - system - userdiff	 Registry hive shown in bottom right tab.

2.3.11 Unallocated Files

Date/Time	Action	Outcome

2024-01-10 19:42:09 UTC	Open *Autopsy* to view seen in section 3.2.2	*Autopsy* opened to view seen in section 3.2.2
2024-01-10 19:42:30 UTC	 Click the + box left of *Data Sources* (circled in red).	 *Data Sources* folder expanded.
2024-01-10 19:42:59 UTC	 Click the + box left of *Taurus Laptop.001_ 1 Host* (circled in red).	 *Taurus Laptop.001_ 1 Host* folder expanded.
2024-01-10 19:43:15 UTC	 Click the + box left of *Taurus Laptop.001* (circled in red).	 *Taurus Laptop.001* folder expanded.

2024-01-10 19:46:23 UTC	 Click the + box left of *vol2* (circled in red).	 *vol2* folder expanded.
2024-01-10 19:46:45 UTC	 Click the + box left of *Taurus Laptop.001_ 1 Host* (circled in red).	 *Taurus Laptop.001_ 1 Host* folder expanded.
2024-01-10 19:47:01 UTC	 Click the + box left of *Taurus Laptop.001* (circled in red).	 *Taurus Laptop.001* folder expanded.
2024-01-10 19:47:46 UTC	 Click the + box left of *vol2* (circled in red).	 *vol2* folder expanded.

2024-01-10 19:48:00 UTC	 Click on *$Unalloc* (circled in red).	 *$Unalloc* displayed on the top right pane. Unallocated files are inside *$Unalloc*.

2.4 Verification

In order to verify the integrity of all evidence items, the MD5 and SHA-256 hash of the initial exhibits given must match the copy examined by the forensic investigator post-examination. This ensures that none of the content of the image (including files, metadata, or indeed any other content) has been altered.

Date/Time	Action	Outcome

29-12-23
16:23:18 UTC
	Open the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\Taurus Smith.001" SHA256`
	Then record this hash
		`a2f49fa7ce6b111c6e198de2ca4a24a8e73d6d85291805db5bede4d60fab23be`
		`CertUtil: -hashfile command completed successfully.`
		`a2f49fa7ce6b111c6e198de2ca4a24a8e73d6d8529 1805db5bede4d60fab23be`
		SHA256 hash recorded.

29-12-23
16:24:07 UTC
	In the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\Taurus Smith.001" MD5`
	Then record this hash
		`56aeba1a708c5210c8728e5a2560f9ca`
		`CertUtil: -hashfile command completed successfully.`
		`56aeba1a708c5210c8728e5a2560f9ca`
		MD5 hash recorded.

29-12-23
16:24:39 UTC
	In the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\ Exhibit A_Back.jpg" SHA256`
	Then record this hash
		`5290f3d34b9b8b37a608c4f51781ae324e9d9c39db9162557010005d01614854`
		`CertUtil: -hashfile command completed successfully.`
		`5290f3d34b9b8b37a608c4f51781ae324e9d9c39db 9162557010005d01614854`
		SHA256 hash recorded.

29-12-23
16:25:14 UTC
	In the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\ Exhibit A_Back.jpg" MD5`
	Then record this hash
		`480252b5de825054fb918cb08bb7030e`
		`CertUtil: -hashfile command completed successfully.`
		`480252b5de825054fb918cb08bb7030e`
		MD5 hash recorded.

29-12-23 16:26:05 UTC	In the command prompt type: `certutil -hashfile "{CASE FILE LOCATION}\ Exhibit A_Front.jpg" SHA256`	`164a764b6386e7f4a04301048b6f5d962195193a61bc4b95750f7def3d8d2f8e` `CertUtil: -hashfile command completed successfully.`

	Then record this hash	`164a764b6386e7f4a04301048b6f5d962195193a61bc4b95750f7def3d8d2f8e` SHA256 hash recorded.

29-12-23
16:26:59 UTC
	In the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\Exhibit A_Front.jpg" MD5`
	Then record this hash
		`321009e97b88f3178106ef2275f7ed19`
		`CertUtil: -hashfile command completed successfully.`
		`321009e97b88f3178106ef2275f7ed19`
		MD5 hash recorded.

29-12-23
16:27:30 UTC
	In the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\Exhibit B and Exhibit C.pdf" SHA256`
	Then record this hash
		`c6760229562f8c2bb47be38b90877624a72d89151dbaf5de108e73b5c9a7153f`
		`CertUtil: -hashfile command completed successfully.`
		`c6760229562f8c2bb47be38b90877624a72d89151dbaf5de108e73b5c9a7153f`
		SHA256 hash recorded.

29-12-23
16:28:20 UTC
	In the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\Exhibit B and Exhibit C.pdf" MD5`
	Then record this hash
		`321009e97b88f3178106ef2275f7ed19`
		`CertUtil: -hashfile command completed successfully.`
		`3a4ab9eba38ef8244cfaa44eec392a3e`
		MD5 hash recorded.

29-12-23
16:28:55 UTC
	In the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\Exhibit D.pcapng" SHA256`
	Then record this hash
		`8f4b221f715c216d55b13089d325bec45ae5f4c143484bd0ad5c5c2d38f12292`
		`CertUtil: -hashfile command completed successfully.`
		`8f4b221f715c216d55b13089d325bec45ae5f4c143484bd0ad5c5c2d38f12292`
		SHA256 hash recorded.

29-12-23
16:29:30 UTC
	In the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\Exhibit D.pcapng" MD5`
	Then record this hash
		`251a1a9a8284397a70d06cadd1a5bfa6`
		`CertUtil: -hashfile command completed successfully.`
		`251a1a9a8284397a70d06cadd1a5bfa6`
		MD5 hash recorded.

29-12-23
16:30:24 UTC
	In the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\Exhibit E.pcapng" SHA256`
	Then record this hash
		`72359088a569ca213e92c79390a2fcebe0869c67073aae828d20f85cf76ae2ba`
		`CertUtil: -hashfile command completed successfully.`
		`72359088a569ca213e92c79390a2fcebe0869c67073aae828d20f85cf76ae2ba`
		SHA256 hash recorded.

29-12-23
16:30:40 UTC
	In the command prompt type:
	`certutil -hashfile "{CASE FILE LOCATION}\Exhibit E.pcapng" MD5`
	Then record this hash
		`756f6afcc9e40556947905ad0824b708`
		`CertUtil: -hashfile command completed successfully.`
		`756f6afcc9e40556947905ad0824b708`
		MD5 hash recorded.

29-12-23 16:31:16 UTC	Open terminal on *Kali Linux* virtual machine in *VMware*.	 Terminal opened

29-12-23 16:31:51 UTC	 In the terminal type: `sha256sum "{PATH TO EXTRACTED PCAP FILES}/pcap files/Exhibit B and Exhibit C.pdf"` Then record this hash	 `c6760229562f8c2bb47be38b90877624a72d89151dbaf5de108e73b5c9a7153f` SHA256 hash recorded.
29-12-23 16:32:34 UTC	 In the terminal type: `md5sum "{PATH TO EXTRACTED PCAP FILES}/pcap files/Exhibit B and Exhibit C.pdf"` Then record this hash	 `3a4ab9eba38ef8244cfaa44eec392a3e` MD5 hash recorded.
29-12-23 16:33:05 UTC	 In the terminal type: `sha256sum "{PATH TO EXTRACTED PCAP FILES}/pcap files/Exhibit D.pcapng"` Then record this hash	 `8f4b221f715c216d55b13089d325bec45ae5f4c143484bd0ad5c5c2d38f12292` SHA256 hash recorded.

29-12-23 16:33:40 UTC	 In the terminal type: `md5sum "{PATH TO EXTRACTED PCAP FILES}/pcap files/ Exhibit D.pcapng"` Then record this hash	 `251a1a9a8284397a70d06cadd1a5bfa6` MD5 hash recorded.
29-12-23 16:34:35 UTC	 In the terminal type: `sha256sum "{PATH TO EXTRACTED PCAP FILES}/pcap files/Exhibit E.pcapng"` Then record this hash	 `72359088a569ca213e92c79390a2fcebe0869c67073aae828d20f85cf76ae2ba` SHA256 hash recorded.
29-12-23 16:35:18 UTC	 In the terminal type: `md5sum "{PATH TO EXTRACTED PCAP FILES}/pcap files/ Exhibit E.pcapng"` Then record this hash	 `756f6afcc9e40556947905ad0824b708` MD5 hash recorded.

3 Analysis and Findings

3.1 Evidence Overview

3.1.1 System Overview

The following information has been extracted from the image using *Autopsy*.

Name	FRODO1
Operating System	Microsoft Windows XP Service Pack 2
Registered Owner	ADXP
Install Date	2004-10-25 18:58:20
Number of Accounts	8
Time Zone	Europe/London

3.1.2 Evidence Hashes

The following MD5 and SHA256 hashes were generated for each evidence file. This included:

- *Taurus Laptop.001*
- *Exhibit A_ Back.jpg*
- *Exhibit A_ Front.jpg*
- *Exhibit B and Exhibit C.pdf*
- *Exhibit D.pcapng*
- *Exhibit E.pcapng*

The hashes were generated before conducting the investigation and after conducting the investigation. The files contained in *pcap files.zip* (*Exhibit B and Exhibit C.pdf*, *Exhibit D.pcapng*, and *Exhibit E.pcapng*) were analysed inside the *Kali Linux* machine in *VMware* as well as in the *Windows 10* machine in *VMware* hence both the Linux and Windows versions of these files had their hashes checked post-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	5290f3d34b9b8b37a608c4f51781ae32 4e9d9c39db9162557010005d01614854
Exhibit A_Front.jpg (pre-investigation)	321009e97b88f3178106ef2275f7ed19	164a764b6386e7f4a04301048b6f5d96 2195193a61bc4b95750f7def3d8d2f8e
Exhibit A_Front.jpg (post-investigation)	321009e97b88f3178106ef2275f7ed19	164a764b6386e7f4a04301048b6f5d96 2195193a61bc4b95750f7def3d8d2f8e
Exhibit B and Exhibit C.pdf (pre-investigation)	3a4ab9eba38ef8244cfaa44eec392a3e	c6760229562f8c2bb47be38b90877624 a72d89151dbaf5de108e73b5c9a7153f
Exhibit B and Exhibit C.pdf (post-investigation windows)	3a4ab9eba38ef8244cfaa44eec392a3e	c6760229562f8c2bb47be38b90877624 a72d89151dbaf5de108e73b5c9a7153f
Exhibit B and Exhibit C.pdf (post-investigation linux)	3a4ab9eba38ef8244cfaa44eec392a3e	c6760229562f8c2bb47be38b90877624 a72d89151dbaf5de108e73b5c9a7153f
Exhibit D.pcapng (pre-investigation)	251a1a9a8284397a70d06cadd1a5bfa6	8f4b221f715c216d55b13089d325bec4 5ae5f4c143484bd0ad5c5c2d38f12292
Exhibit D.pcapng (post-investigation windows)	251a1a9a8284397a70d06cadd1a5bfa6	8f4b221f715c216d55b13089d325bec4 5ae5f4c143484bd0ad5c5c2d38f12292
Exhibit D.pcapng (post-investigation linux)	251a1a9a8284397a70d06cadd1a5bfa6	8f4b221f715c216d55b13089d325bec4 5ae5f4c143484bd0ad5c5c2d38f12292
Exhibit E.pcapng (pre-investigation)	756f6afcc9e40556947905ad0824b708	72359088a569ca213e92c79390a2fceb e0869c67073aae828d20f85cf76ae2ba
Exhibit E.pcapng (post-investigation windows)	756f6afcc9e40556947905ad0824b708	72359088a569ca213e92c79390a2fceb e0869c67073aae828d20f85cf76ae2ba
Exhibit E.pcapng (post-investigation linux)	756f6afcc9e40556947905ad0824b708	72359088a569ca213e92c79390a2fceb e0869c67073aae828d20f85cf76ae2ba

As shown in the table above, both the MD5 and SHA256 hashes remained the same pre-investigation and post-investigation on both machines when applicable. This verifies that the file contents have remained the same.

3.2 Key Findings

3.2.1 Recipes

Recipes 1 & 2: Steganography – Deleted Data

The image contains a deleted email file (*Exhibit H*), sent at 2010-03-04 10:11:46 UTC. Inside the contents of this email file is a string of text reading "Expected Results: you need to decode the contents." and a *Base64* encoded message. When decoded the message produces the following:

Encoded	Decoded

<table>
<tr>
<td>VGhpcyBpcyBhIG11bHRpLXBhcnQgbWVzc2FnZSBpbiBNSU1
FIGZvcm1hdC4KCi0tLS0tLT1fTmV4dFBhcnRfMDAwXzAwMj
NfMDFDNzEyMTQuRDNENDlBMDAKQ29udGVudC1UeXBlOiB0Z
Xh0L3BsYWluOwoJY2hhcnNldD0iaXNvLTg4NTktMSIKQ29u
dGVudC1UcmFuc2Zlci1FbmNvZGluZzogcXVvdGVkLXByaW5
0YWJsZQoKUGxlYXNlIGdvIHRvIHRoZSB3ZWJzaXRlIGFuZC
BkZWNvZGUgdGhlIHR3byBwbmcgZmlsZXMsIHlvdSB3aWxsI
HNlZSB0aGUgZGV0YWlsczogaHR0cHM6Ly9zdHlsZXN1eHgu
Z2l0aHViLmlvL3N0ZWdhbm9ncmFwaHkvCgotLS0tLS09X05
leHRQYXJ0XzAwMF8wMDIzXzAxQzcxMjE0LkQzRDQ5QTAwCk
NvbnRlbnQtVHlwZTogdGV4dC9odG1sOwoJY2hhcnNldD0ia
XNvLTg4NTktMSIKQ29udGVudC1UcmFuc2Zlci1FbmNvZGlu
ZzogcXVvdGVkLXByaW50YWJsZQoKPCFET0NUWVBFIEhUTUw
gUFVCTElDICItLy9XM0MvL0RURCBIVE1MIDQuMCBUcmFuc2
l0aW9uYWwvL0VOIj4KPEhUTUw+PEhFQUQ+CjxNRVRBIGh0d
HAtZXF1aXY9M0RDb250ZW50LVR5cGUgY29udGVudD0zRCJ0
ZXh0L2h0bWw7ID0KY2hhcnNldD0zRGlzby04ODU5LTEiPgo
8TUVUQSBjb250ZW50PTNEIk1TSFRNTCA2LjAwLjI5MDAuMj
k2MyIgbmFtZT0zREdFTkVSQVRPUj4KPFNUWUxFPjwvU1RZT
EU+CjwvSEVBRD4KPEJPRFkgYmdDb2xvcj0zRCNmZmZmZmY+
CkhlcmUgdGhlcmUgaXMgaHRtbCBjb250ZW50CjwvQk9EWT4
8L0hUTUw+CgotLS0tLS09X05leHRQYXJ0XzAwMF8wMDIzXz
AxQzcxMjE0LkQzRDQ5QTAwLS0=</td>
<td>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

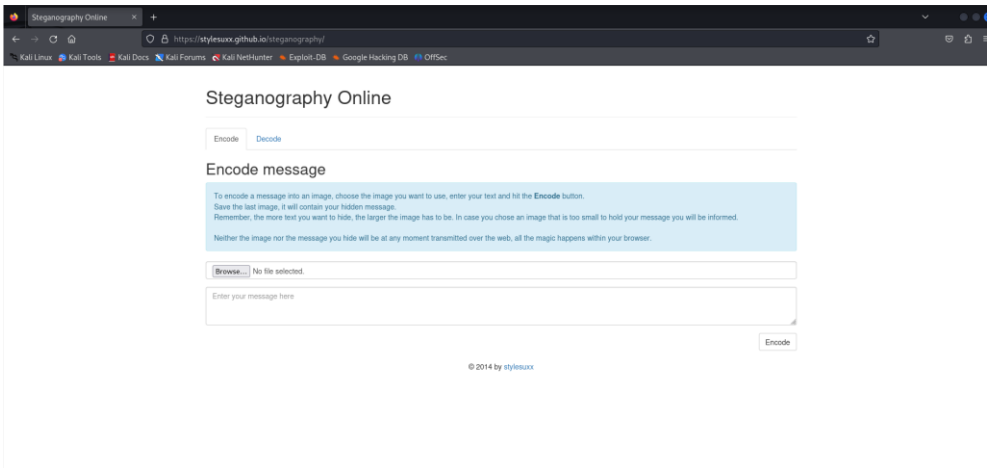
Please go to the website and decode the two png files, you will see the details: https://stylesuxx.github.io/steganography/

------=_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--</td>
</tr>
</table>

The decoded message contains a link 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 website is a tool used to encode or decode a message into a .png file which the user is able to upload to the website. If *Exhibit F* is uploaded to this website and decoded, what appears to be a doughnut recipe can be found. This recipe is shown below:

```
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.

Similarly, if *Exhibit G* is uploaded into this website and decoded, what appears to be another recipe appears as follows:

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.

Recipe 3: Password Protected Files

The encrypted file Lardland Super Donuts Instructions.pdf (*Exhibit 1*) is a password protected .pdf file. After running the tool *John the Ripper* 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 encrypted file appears to have a baked doughnut recipe inside. The first 2 images on the recipe sheet are visually identical to a pair of images (*Exhibit J* and *Exhibit K*) found in *Taurus Smith's* directory 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`

This recipe appears to be intentionally hidden (password protected). The recipe also appears to have been created with the images *Exhibit J* and *Exhibit K* found on the laptop in *Taurus Smith's* user account. This raises the question of whether *Taurus Smith* helped to create this recipe file.

The instructions (*Exhibit I*) are actually found on *Bilbo Baggins'* user account, not on *Taurus Smith's* user account, however a deleted file with an identical name (*Exhibit V*) can be found on *Taurus Smith's* user account. 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. 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 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 *Exhibit J* and *Exhibit K* (*Exhibit W* and *X* respectively) can be found inside *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*. 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 (Taurus) 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.

Recipe 4: Network Packets

Exhibit D.pcapng is a PCAP file revealing a short exchange of 18 packets between 192.168.1.158 (*Taurus's* computer) and 192.168.1.43, an unexpected laptop that appeared briefly on *Lardland Doughnuts* network. At 2010-03-07 12:19:38.625569 UTC *Taurus's* computer sends 192.168.1.43 what appears to be a recipe for a doughnut in the network packet *Exhibit L*.

```
## **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 192.168.1.158 (*Taurus's* computer) and 192.168.1.43, the unexpected laptop, with a length of 509 packets, 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 *Taurus's* work computer to the unexpected laptop. The conversation above shows that *Taurus* is in communication with the laptop, and *Taurus* 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 *Exhibit F* and *Exhibit G*), some of which have been sent over a secure channel. The user operating the unexpected laptop then thanks *Taurus*, at which point *Taurus* says "see you in hawaii!" which could indicate that *Taurus* and the user behind the unexpected laptop plan to meet in Hawaii. *Taurus* then claims that she has another file, she then says "this is something useful".

The traffic travels between two devices, *Taurus'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)*.

Exhibit B and *Exhibit C* show a conversation between *Taurus Smith's* laptop (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 *Taurus Smith'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 >:-)	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 >:-)” is only visible in one conversation.

Recipe 5: Family Photos

A recipe was found in the *Family Photos* folder inside a subfolder *My Docs* inside a document file (*Exhibit Y*) containing the recipe for “Basic Donuts”. This file does not appear to conceal the recipe in any form.

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. Inside the metadata of this file, it can be observed that the author of the document is called Mike, which could potentially implicate 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 does appear to have been created, modified, and accessed around 3 days before Taurus exchanged packets with her accomplice and one the same day that the deleted email concerning the two encoded .png files was sent (*Exhibit H*) which is a time period of relevance to the investigation.

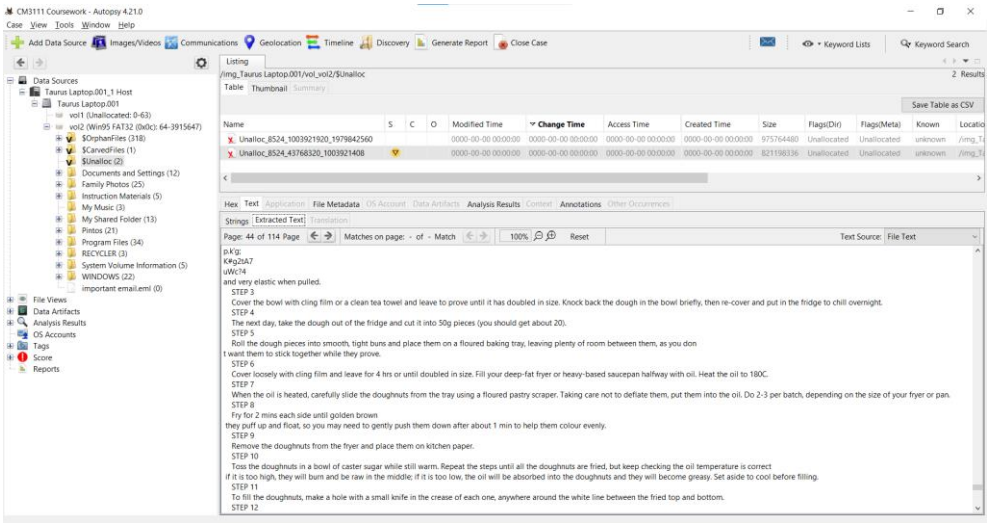
Recipe 6: Ring Recipe

A deleted file called *ring recipe.txt.sb-ace39f49-PiYykM* (*Exhibit Z*) 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.

Recipe 7: Unallocated Files

The unallocated space file *Unalloc_8524_43768320_1003921408* (*Exhibit AE*) contains a recipe on the 44th page of extracted text.



The recipe has only been partially recovered as steps 1 and 2 are missing, however the remainer of the recipe appears to be intact:

```
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, one likely explanation for this recipe being in unallocated space is that it was deleted and not overwritten. Files can also be found in unallocated space if the space has been reformatted or if the file system has been corrupted.

3.2.2 Travel Plans

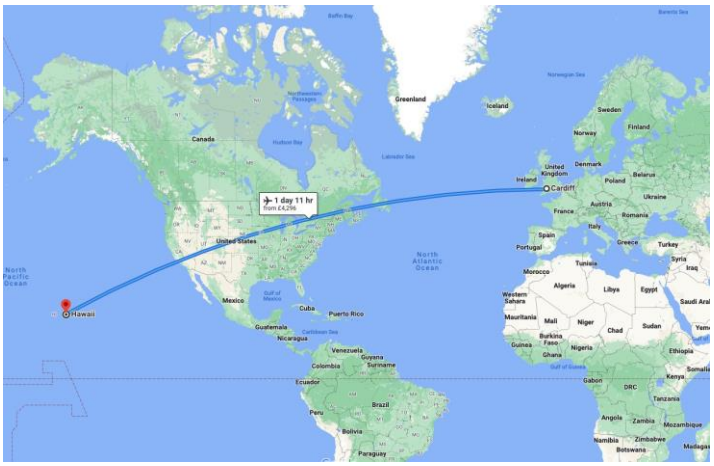
There are multiple pieces of evidence indicating that Taurus Smith is planning on travelling to Hawaii. These include a network packet coming from her laptop and a carved file.

Network

Exhibit P is a packet sent from *Taurus'* computer (192.168.1.158) to the unexpected laptop (192.168.1.43) at 2010-03-07 12:29:44.400196 UTC. The payload inside that packet 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.

Carved File

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



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 Taurus 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 *Taurus'* 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" (*Exhibit U*). There is also an *Microsoft Word* document containing an image of a doughnut shop in Cardiff named "Cardiff Dough and Co" (*Exhibit T*). Interestingly this file has a MIME type of a .jpeg image and contains EXIF metadata. These files were found inside a *SendTo* folder, indicating that they are intended to be sent to another location on the laptop.

The fact that Taurus has an interest in the Cardiff area is made more significant when in conjunction with *Exhibit S* and *Exhibit P*. These evidence items indicated that Taurus has an interest in Cardiff, Hawaii, and potentially the travel from Cardiff to Hawaii, and would provide some justification that Taurus is planning to travel from Cardiff to Hawaii.

3.2.3 Implicated Individuals

There appears to be an accomplice that is implicated along with Taurus, though the identity of this individual is unclear. It can be ascertained that Taurus 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*. Taurus (192.168.1.158) first sends a message communicating to the recipient that she has "sent a few files" using steganography. The recipient (192.168.1.43) then responds "thanks", confirming that she has received the files containing the recipes. This creates a situation where it is likely that the recipient knew that Taurus was sending encoded files, and the recipient also was actively expecting these files. Taurus then sends the message "see you in hawaii!!!", which would indicate that she expects to see the recipient. If Taurus' word is to be taken at face value, it would indicate that Taurus and the recipient have already communicated about these encoded files and have communicated about travelling to Hawaii together, showing some form of relationship between the two. Importantly, it shows that Taurus and the recipient have been collaborating to traffic encoded doughnut recipes.

3.2.4 Deleted/Hidden User Accounts

Inside the *Sam* registry (*Exhibit AA*), 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* (*Exhibit AB*). 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). This can be seen for the *Bilbo Baggins* account in *Exhibit AC* and the *Taurus Smith* account in *Exhibit AD*.

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* (*Exhibit AA*). Regarding the *Taurus Smith* account, 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.

3.3 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 (*Exhibit AB*).
2010-01-03 00:16:20 UTC	file.dat	File Created	Image with a hidden encoded message containing a doughnut recipe (*Exhibit F*) created.
2010-01-03 00:16:20 UTC	stdlidd.inc	File Created	Image with a hidden encoded message containing a doughnut recipe (*Exhibit G*) created.
2010-02-02 12:02:26 UTC	file.dat	File Modified	Image with a hidden encoded message containing a doughnut recipe (*Exhibit F*) modified.

2010-02-02 12:02:26 UTC	stdlidd.inc	File Modified	Image with a hidden encoded message containing a doughnut recipe (*Exhibit G*) modified.
2010-03-04 00:06:49	Basic donuts.doc	File Created	File containing the recipe for "Basic donuts" *(Exhibit Y)* 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 (*Exhibit H*).
2010-03-04 13:35:24 UTC	Basic donuts.doc	File Modified	File containing the recipe for "Basic donuts" *(Exhibit Y)* modified.
2010-03-07 00:00:00 UTC	Basic donuts.doc	File Accessed	File containing the recipe for "Basic donuts" *(Exhibit Y)* accessed.
2010-03-07 00:00:00 UTC	maps.png	File Accessed	File containing map of Cardiff (*Exhibit U*) accessed.
2010-03-07 00:00:00 UTC	Lardland Super Donuts Instructions.pdf	File Accessed	Lardland Super Donuts Instructions (*Exhibit I*) 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 (*Exhibit L*).
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" (*Exhibit M*).
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." (*Exhibit N*).
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" (*Exhibit O*).
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!" (*Exhibit P*).
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" (*Exhibit R*).
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." (*Exhibit Q*).
2010-03-07 21:03:08 UTC	Cardiff.docx	File Modified	File containing image of "Cardiff Dough and Co" (*Exhibit T*) modified.
2010-03-08 00:00:00 UTC	file.dat	File Accessed	Image with a hidden encoded message containing a doughnut recipe (*Exhibit F*) accessed.
2010-03-08 00:00:00 UTC	stdlidd.inc	File Accessed	Image with a hidden encoded message containing a doughnut recipe (*Exhibit G*) accessed.
2010-03-08 00:00:00 UTC	Lardland Super Donut Ingredients.png	File Accessed	Lardland Super Donuts Ingredients image (*Exhibit J*) accessed.
2010-03-08 00:00:00 UTC	baked_donut_recipe_featured.jpg	File Accessed	Baked Donut Recipe image (*Exhibit K* and *X*) accessed.
2010-03-08 00:06:26 UTC	_REGISTRY_MACHINE_SAM	File Modified	Registry hive found in snapshot showing user account information modified (*Exhibit AB*).
2010-03-31 00:00:00 BST	ring recipe.txt.sb-ace39f49-PiYykM	File Accessed	Deleted file which could potentially contain a recipe accessed (*Exhibit Z*).
2010-03-31 18:55:06 BST	Lardland Super Donuts Instructions.pdf	File Modified	Deleted file suspected to be Lardland Super Donuts Instructions.pdf (*Exhibit V*) 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 (*Exhibit W*) 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 (*Exhibit W*) 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 (*Exhibit V*) 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 (*Exhibit Z*).

4 Conclusion

4.1 Recipes

It does appear as if Taurus Smith a.k.a. Ms Mona Simpson has intentionally encoded/hidden and sent 4 secret doughnut recipes. 1 other doughnut recipe (*Basic donut.doc*) was found on Taurus Smith's laptop image however this recipe

is not hidden and it is not clear if it was a secret recipe belonging to *Lard&land Donuts*, or if it was ever sent. A deleted file that is suspected to have contained a recipe due to its name (ring recipe.txt.sb-ace39f49-PiYykM) was also found on the laptop image, however the contents were not recoverable therefore it not clear if it was a secret recipe, if the recipe was belonging to *Lard&land Donuts*, or if it was ever sent. A recipe was also found in unallocated space, the majority of this recipe was recoverable, however some steps were missing and it had no metadata attached. No recipe for "Honey Duff Donuts" have been recovered.

Recipes 1 and 2 were hidden by encoding a recipe each into 2 .png files using the website *https://stylesuxx.github.io/steganography/*, then changing the file extensions of these .png files. An email was found on Taurus' laptop image communicating to a recipient that two .png files have been sent and that the website *https://stylesuxx.github.io/steganography/*, should be used to decode the contents. These were confirmed by to have been sent by Taurus to an accomplice as later in a captured instant message packet with an accomplice, Taurus writes "I have sent you a few files using different way, some of them are steged and some of them used secure ways/channel.".

A third recipe was found on the laptop image inside the *Bilbo Baggins* user account for "Lardland Super Donuts". This recipe was a .pdf file that was intentionally hidden using password-protection. It is also likely that Taurus created this .pdf file herself as the .pdf file contained two images that are visually identical to two images also found on the *Taurus Smith* user account, and a deleted file using the same name can also be found on the *Taurus Smith* user account. It is also suspected that the *Bilbo Baggins* account and the *Taurus Smith* account are both being operated under by the same person.

A fourth recipe was found inside the PCAP files given as *Exhibit D*. This file showed captured instant message packets being sent between Taurus' work computer and an unexpected laptop in the *Lard&land Donuts* car park. The exchange of packets revealed that Taurus first sent the accomplice a recipe for a custard doughnut, at which the accomplice confirmed their involvement in *Exhibit E* by replying "thanks".

Another recipe was found in the unallocated space of the laptop (*Exhibit AE*). This was likely deleted from the laptop and not yet overwritten, it has no metadata attached to it, therefore it is difficult to prove if Taurus wrote or distributed the recipe, or if it even was from *Lard&land Donuts*. 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.

4.2 Travel Plans

The extracted evidence strongly suggests that Taurus is planning to travel to Hawaii.

An intercepted network packet (*Exhibit P*) sent from Taurus' work computer to her accomplice in the *Lard&land Donuts* car park contained the explicit message "see you in hawaii!" implying a possible meeting between Taurus and her accomplice in Hawaii.

In addition, a carved file can be found displaying a screenshot of a flight route from Cardiff to Hawaii. The absence of metadata for this file means that it cannot be used to show a definitive link to Taurus, however, it does show that the user of the laptop has interest in the flight path, and is also notable as the laptop contains other files relating Taurus to both Cardiff and Hawaii.

There are also two files inside the *SendTo* folder in the *Taurus Smith* user account that suggest Taurus has an interest in the Cardiff area. One is a file called *Cardiff.docx* containing and image of a doughnut shop in Cardiff. The other is an image of a map of Cardiff, containing an added red marker and a label reading *Lard&land Donuts*.

4.3 Deleted/Hidden User Accounts

There are several complexities surround the *Taurus Smith* user account. Inside the registry the list of 8 accounts can be observed, with 4 user accounts. Interestingly the *Taurus Smith* account is not present in the registry, despite being present in the *Documents and Settings* folder of the image. A snapshot of the system was also taken at a restore point showing only 1 user account named *user1*. The only evidence of the *Taurus Smith* user accounts existence is in the *Documents and Settings* folder. However, upon analysis of this folder it appears as if the *Cookies* folder found inside, and the *Local Settings* folder are directly duplicated from the *Bilbo Baggins* account, even containing the same cookie MD5

hash and the same SID. While no conclusive evidence has been extracted, the most likely explanations are these:

1. The *Taurus Smith* user account never existed formally. This means the *Taurus Smith* folder inside *Documents and Settings* was manually created using files from the *Bilbo Baggins* account. This is supported by the fact that the *Taurus Smith* user account is not in the registry and contains several duplicated files from the *Bilbo Baggins* account.
2. The *Taurus Smith* user account existed (potentially as the *user1* account) but was deleted. This would mean that the *Taurus Smith* folder in *Documents and Settings* was from the previously existing account, however it would require the manual copying and replacing of some of *Bilbo Baggins'* files into this folder.
3. The *Taurus Smith* user account is hidden from the registry while retaining the user profile folder. Similar to the deletion scenario, data copying from Bilbo Baggins would be required.

5 Appendix

5.1 Exhibit F

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	

5.2 Exhibit G

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	

5.3 Exhibit H

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 VGhpcyBpcyBhIG11bHRpLXBhcnQgbWVzc2FnZSBpbiBNSU1FIGZvcm1hdC 4KCi0tLS0tLT1fTmV4dFBhcnRfMDAwXzAwMjNfMDFDNzEyMTQuRDNENDlB MDAKQ29udGVudC1UeXBlOiB0ZXh0L3BsYWluOwoJY2hhcnNldD0iaXNvLT g4NTktMSIKQ29udGVudC1UcmFuc2Zlci1FbmNvZGluZzogcXVvdGVkLXBy aW50YWJsZQoKUGxlYXNlIGdvIHRvIHRoZSB3ZWJzaXRlIGFuZCBkZWNvZG UgdGhlIHR3byBwbmcgZmlsZXMsIHlvdSB3aWxsIHNlZSB0aGUgZGV0YWls czogaHR0cHM6Ly9zdHlsZXN1eHguZ2l0aHViLmlvL3N0ZWdhbm9ncmFwaH kvCgotLS0tLS09X05leHRQYXJ0XzAwMF8wMDIzXzAxQzcxMjE0LkQzRDQ5 QTAwCkNvbnRlbnQtVHlwZTogdGV4dC9odG1sOwoJY2hhcnNldD0iaXNvLT g4NTktMSIKQ29udGVudC1UcmFuc2Zlci1FbmNvZGluZzogcXVvdGVkLXBy aW50YWJsZQoKPCFET0NUWVBFIEhUTUwgUFVCTElDICItLy9XM0MvL0RURC BIVE1MIDQuMCBUcmFuc2l0aW9uYWwvL0VOIj4KPEhUTUw+PEhFQUQ+CjxN RVRBIGh0dHAtZXF1aXY9M0RDb250ZW50LVR5cGUgY29udGVudD0zRCJ0ZX h0L2h0bWw7ID0KY2hhcnNldD0zRGlzby04ODU5LTEiPgo8TUVUQSBjb250 ZW50PTNEIk1TSFRNTCA2LjAwLjI5MDAuMjk2MyIgbmFtZT0zREdFTkVSQV RPUj4KPFNUWUxFPjwvU1RZTEU+CjwvSEVBRD4KPEJPRFkgYmdDb2xvcj0z RCNmZmZmZmY+CkhlcmUgdGhlcmUgaXMgaHRtbCBjb250ZW50CjwvQk9EWT 48L0hUTUw+CgotLS0tLS09X05leHRQYXJ0XzAwMF8wMDIzXzAxQzcxMjE0 LkQzRDQ5QTAwLS0=------ =_NextPart_000_0023_01C71214.D3D49A00-- Expected Results: you need to decode the contents.

5.4 Exhibit I

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!  **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. 6

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 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!

5.5 Exhibit J

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	

5.6 Exhibit K

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	

5.7 Exhibit L

File Name	`Exhibit D.pcapng`
Packet Number	`14`
Timestamp	`2010-03-07 12:19:38.625569 UTC`
Source IP Address	`192.168.1.158`
Destination IP Address	`192.168.1.43`
Source Port	`54516`
Destination Port	`1234`
Packet Length	`4604`
Protocol	`TCP`
Hash Value (MD5)	

Payload (ASCII)	`## **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 JustinsÂ [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.

5.8 Exhibit M

File Name	Exhibit E.pcapng
Packet Number	8
Timestamp	2010-03-07 12:27:18.788496
Source IP Address	192.168.1.158
Destination IP Address	192.168.1.43
Source Port	54516
Destination Port	1234
Packet Length	94
Protocol	TCP
Hash Value (MD5)	
Payload (ASCII)	I have sent you a few files

5.9 Exhibit N

File Name	Exhibit E.pcapng
Packet Number	10
Timestamp	2010-03-07 12:27:48.632271 UTC
Source IP Address	192.168.1.158
Destination IP Address	192.168.1.43
Source Port	54516
Destination Port	1234
Packet Length	154
Protocol	TCP
Hash Value (MD5)	
Payload (ASCII)	using different way, some of them are steged and some of them used secure ways/channel.

5.10 Exhibit O

File Name	Exhibit E.pcapng
Packet Number	16
Timestamp	2010-03-07 12:28:07.506722 UTC
Source IP Address	192.168.1.43
Destination IP Address	192.168.1.158
Source Port	1234
Destination Port	54516
Packet Length	73
Protocol	TCP

Hash Value (MD5)	
Payload (ASCII)	Thanks

5.11 Exhibit P

File Name	Exhibit E.pcapng
Packet Number	99
Timestamp	2010-03-07 12:29:44.400196 UTC
Source IP Address	192.168.1.158
Destination IP Address	192.168.1.43
Source Port	54516
Destination Port	1234
Packet Length	85
Protocol	TCP
Hash Value (MD5)	
Payload (ASCII)	see you in hawaii!

5.12 Exhibit Q

File Name	Exhibit E.pcapng
Packet Number	417
Timestamp	2010-03-07 12:32:07.614208 UTC
Source IP Address	192.168.1.158
Destination IP Address	192.168.1.43

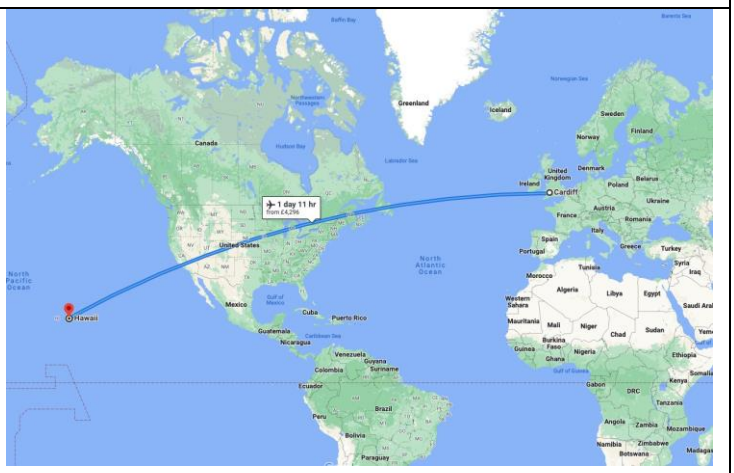
Source Port	54516
Destination Port	1234
Packet Length	93
Protocol	TCP
Hash Value (MD5)	
Payload (ASCII)	this is something useful.

5.13 Exhibit R

File Name	Exhibit E.pcapng
Packet Number	321
Timestamp	2010-03-07 12:31:25.042577 UTC
Source IP Address	192.168.1.158
Destination IP Address	192.168.1.43
Source Port	54516
Destination Port	1234
Packet Length	86
Protocol	TCP
Hash Value (MD5)	
Payload (ASCII)	i have another file

5.14 Exhibit S

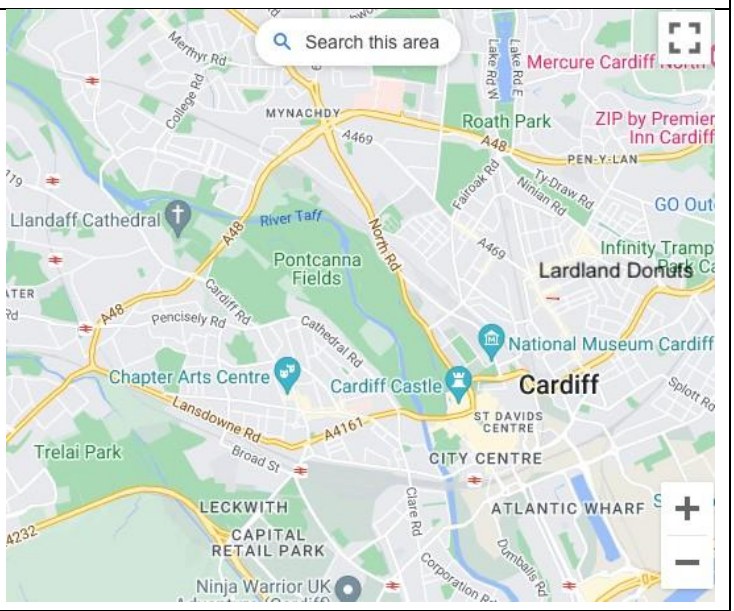
File Name	f0066494.png
File Path	/img_Taurus Laptop.001/vol_vol2/$CarvedFiles/1/f0066494.png
Hash Value (MD5)	0c9dac13c42678ceda658b21507e9156

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	

5.15 Exhibit T

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	

5.16 Exhibit U

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	

5.17 Exhibit V

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	

5.18 Exhibit W

File Name	Lardland Super Donut Ingredients.png
File Path	/img_Taurus Laptop.001/vol_vol2/Documents and Settings/Bilbo Baggins/My Documents/Lardland Lardland Super Donut Ingredients.png
Hash Value (MD5)	e8566c5389e4e15a9cb0e29caaf19637
Modified	2010-03-31 18:55:06 BST
Accessed	2010-03-31 00:00:00 BST
Created	2010-03-31 18:56:43 BST
MIME Type	application/octet-stream
Content	

5.19 Exhibit X

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

Content	

5.20 Exhibit Y

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.

5.21 Exhibit Z

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

5.22 Exhibit AA

File Name	Sam
File Path	/img_Taurus Laptop.001/vol_vol2/WINDOWS/system32/config/Sam
Hash Value (MD5)	3f6c3c0ce0a27bf07e33fec310b30123
Modified	2009-01-01 18:48:40 UTC
Accessed	2010-03-08 00:00:00 UTC
Created	2008-03-08 00:16:54 UTC
MIME Type	application/x.windows-registry
Content	

5.23 Exhibit AB

File Name	_REGISTRY_MACHINE_SAM

File Path	/img_Taurus Laptop.001/vol_vol2/System Volume Information/_restore{B1217314-DDCC-46C9-BF49-2DA9C85265A0}/RP27/snapshot/_REGISTRY_MACHINE_SAM
Hash Value (MD5)	3785693b7db690238ef04997228fc049
Modified	2010-03-08 00:06:26 UTC
Accessed	2010-03-08 00:00:00 UTC
Created	2009-03-08 00:06:24 UTC
MIME Type	application/x.windows-registry
Content	

5.24 Exhibit AC

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	

5.25 Exhibit AD

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	

5.26 Exhibit AE

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