

Digital Forensic and Investigation:

Digital Corpora 2019 Narcos Case Solution

Solved by:

Khubab Ahmed and Muhammad Saim

Table of Contents

1. <i>Executive Summary</i>	4
1.1 Story	4
1.2 Our Task	4
1.3 Tools Usage	4
1.3 Evidence collection	5
2. <i>Methodology</i>	6
2.1 Evidence Verification:	6
2.1.1 Method to verify evidence	7
2.1 Case Preservation	10
2.1.1 Method to preserve evidence	11
2.2 Case Tools	15
2.3 Case Main Suspects	17
2.4 Case Artifacts	18
3. <i>Finding and Description</i>	19
3.1 User Account Profiles and Computer Names	19
3.2 Web Activity	23
3.2.1 Steve Kowhai:	23
3.2.2 Jane Esteban:	25
3.2.3 John Fredricksen:	27
3.3 Behavioral Images	29
3.3.1 Steve Kowhai	29
3.3.2 Jane Esteban	38
3.3.3 John Fredricksen	42
3.4 Binary Files	49
3.4.1 Steve Kowhai:	49
3.4.2 Jane Esteban:	50
3.4.3 John Fredricksen:	51
3.5 Content and Communication between Suspects	52
3.5.1 John Fredricksen and Steve Kowhai:	52
3.5.2 John Fredricksen and Jane Esteban:	53

3.5.3	Jane Esteban Mail:	54
3.6	Documents	56
3.6.1	Steve Kowhai:	56
3.6.2	John Fredricksen	58
3.6.3	Jane Esteban	62
3.7	Obfuscation Methods	64
3.8	Encryption Methods	64
3.9	Malware used	65
3.10	Vulnerability exploited for Malware	66
3.11	Corroborative evidence	67
3.11.1	Steve Kowhai:	67
3.11.2	John Fredricksen:	68
3.11.3	Jane Esteban:	68
3.12	Artifact changes across different windows 10 Builds	69
3.13	Suspects Roles	69
3.12.1	Steve Kowhai	69
3.12.2	John Fredricksen	69
3.12.3	Jane Esteban	69
4.	<i>Summary and Conclusion</i>	70
4.1	User Accounts:	70
4.2	Web History and Images:	70
4.3	Communication	70
4.4	Documents	71
4.5	Conclusion	71
5.	<i>Appendix</i>	72
5.1	Description of persons of interest	72
5.2	Association Diagram of persons of interest	73
5.3	Evidence Listing	74
5.4	Software and tools used in the investigation	81
6.	<i>References</i>	83

1. Executive Summary

1.1 Story

The operation began with intelligence from the Australian government, which flagged two passengers, Jane Esteban and John Fredricksen, as potential suspects involved in illegal activities. Upon their arrival in Wellington, New Zealand, from Brisbane, Australia, customs officials intercepted the two individuals. A thorough search of their luggage revealed clothing, toiletries, a Windows laptop, and one kilogram of methamphetamine hidden in the lining of Jane Esteban's suitcase. Both suspects were immediately taken into custody and interrogated separately.

During interrogation, John Fredricksen refused to cooperate, providing no information or answers. In contrast, Jane Esteban admitted that she was instructed by John to deliver the suitcase to the Eastbourne library. If that plan failed, she was to deliver it to 666 Rewera Avenue, Petone. Acting on this lead, customs and police officers raided the Rewera Avenue address, where they discovered additional drugs, firearms, and a desktop computer. However, no individuals were present at the time of the raid.

1.2 Our Task

As a customs forensic investigators, We have the task of conducting a forensic examination of the digital devices recovered during the operation. These devices include laptops and memory dumps belonging to John Fredricksen, Jane Esteban, and an unknown suspect. The objective is to uncover the suspects' motives, goals, and objectives through a thorough analysis of the digital evidence.

1.3 Tools Usage

To carry out the forensic investigation, the following tools will be utilized:

FTK Imager: This tool will be used to create forensic copies of the digital images provided. Creating a copy is essential to ensure that the original evidence remains unaltered during the investigation, preserving the integrity of the evidence for future use in court.

Autopsy: This digital forensics tool will be employed to analyze the forensic images. Autopsy is instrumental in extracting data artifacts from the system, differentiating between relevant and irrelevant data, and identifying potential evidence that could link the suspects to illegal activities.

Registry Viewer: This tool will be used to examine the system's registry values. The registry is a critical area for investigation as it is often exploited in malware attacks and may contain crucial evidence related to the suspects' activities.

1.3 Evidence collection

The handling and collection of evidence is one of the most crucial components of the rapidly developing science of computer forensics. It is necessary to make use of digital forensic tools to gather the evidence, as they will be of assistance in locating deleted data, tracking image exploitation and steganography, gaining access to encrypted files, and gathering more evidence.

In the given scenario no hint is provided to a hidden files or data but since it's a common practice with criminal with knowledge of the data hiding on compute e.g. steganography, we would make use of autopsy in uncovering these files and data.

Then after gathering this evidence, we would separate the evidence which would lead to the suspects being guilty or their innocence proven. This evidence will also be documented as it is a crucial part of investigation and losing it can be a big blow to the case.

Depending upon the evidence clarity it would be moved forward to other organizations for further confirmation of the evidence, or a verdict would be given in court to close the case indefinitely.

2. Methodology

2.1 Evidence Verification:

From the evidence provided after calculating it hashtes to come over that the provided evidence is verified and correct.

Drive Images:

Actor	File Name	Provided MD5	Calculated MD5
Steve Kowhai	Narcos-1a.001-021	c63a3d19e9c9495b573f45be544e50f9	c63a3d19e9c9495b573f45be544e50f9
Jane Estaban	Narcos-3a.001-021	6265dbaa16a354daddba311334484660	6265dbaa16a354daddba311334484660
John Fredricksen	Narcos-2a.001-021	B66ca567bec6b0a195b99c57dfa0919f0919f	B66ca567bec6b0a195b99c57dfa0919f0919f

Memory Images:

Actor	File Name	Provided MD5	Calculated MD5
Steve Kowhai	Narcos-1a.001-021	9ca08c17b4a359d61f6f8f7bb6328c1c	9ca08c17b4a359d61f6f8f7bb6328c1c
Jane Estaban	Narcos-3a.001-021	0f7e7be4d2844457e2111eaffa1e77ec	0f7e7be4d2844457e2111eaffa1e77ec
John Fredricksen	Narcos-2a.001-021	8e8a3a91eb89fe6c3cd10231f13141fe	8e8a3a91eb89fe6c3cd10231f13141fe

2.1.1 Method to verify evidence

Below are the steps taken to verify the evidence by matching hashes.

- Open FTK Imager tool.

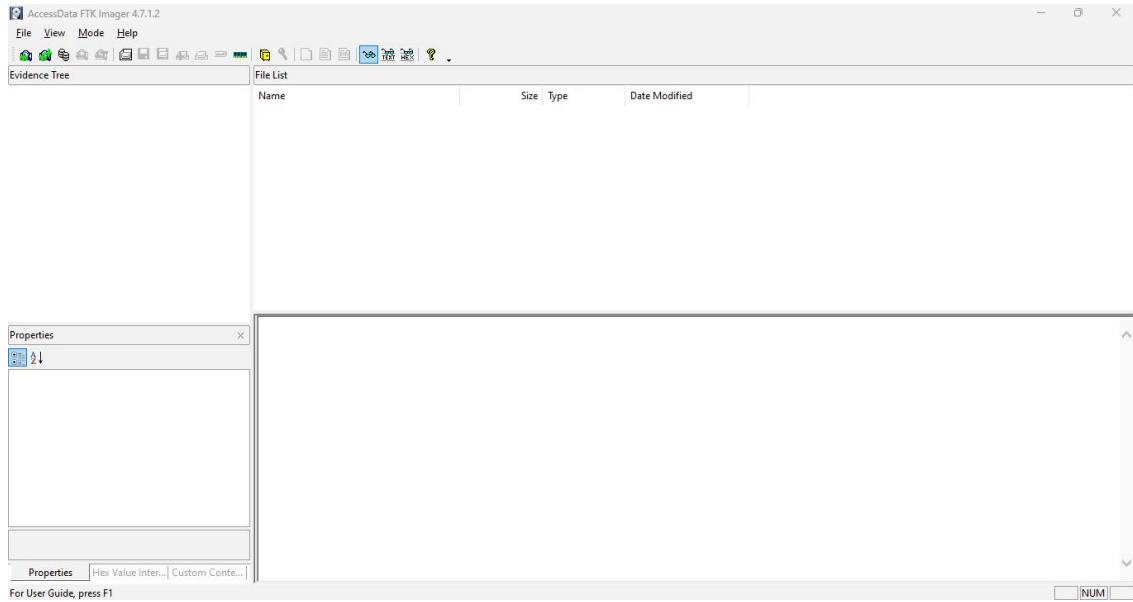


Figure 1 Open FTK Imager tool.

- Add Evidence Item and Select Image file option.

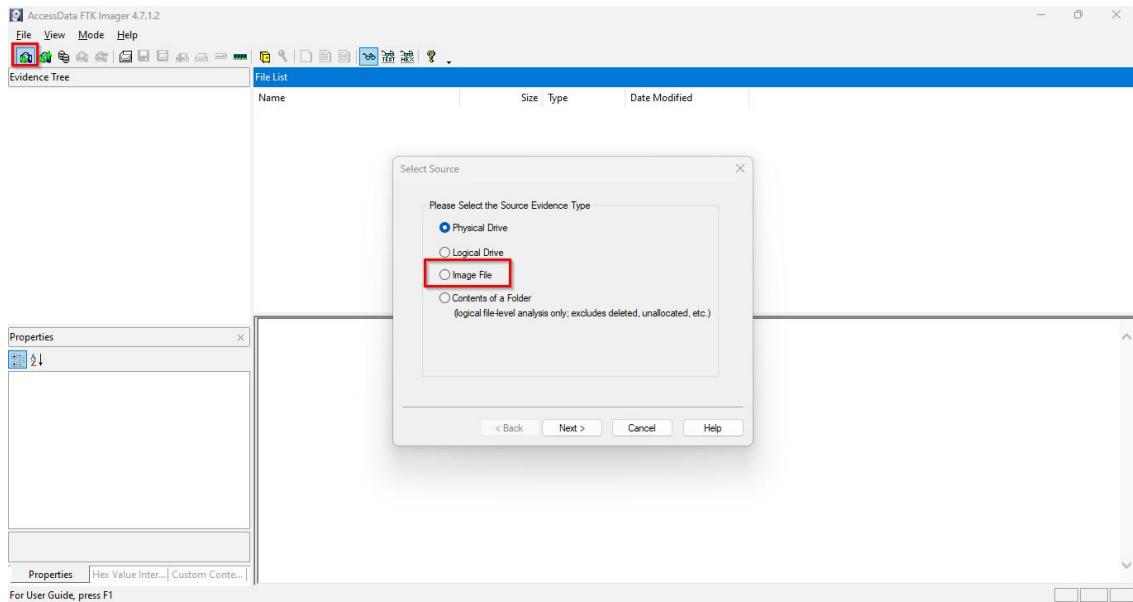


Figure 2 Add Evidence Item and Select Image file option.

- Add an Image file.

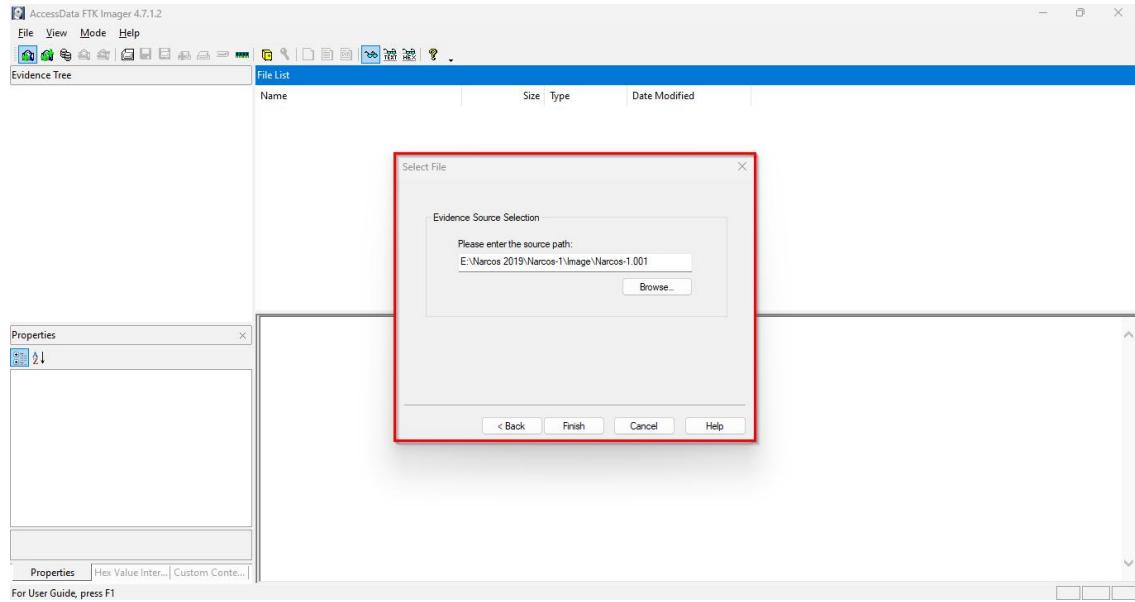


Figure 3 Add an Image file.

- Now right-click on evidence and verify the disk image.

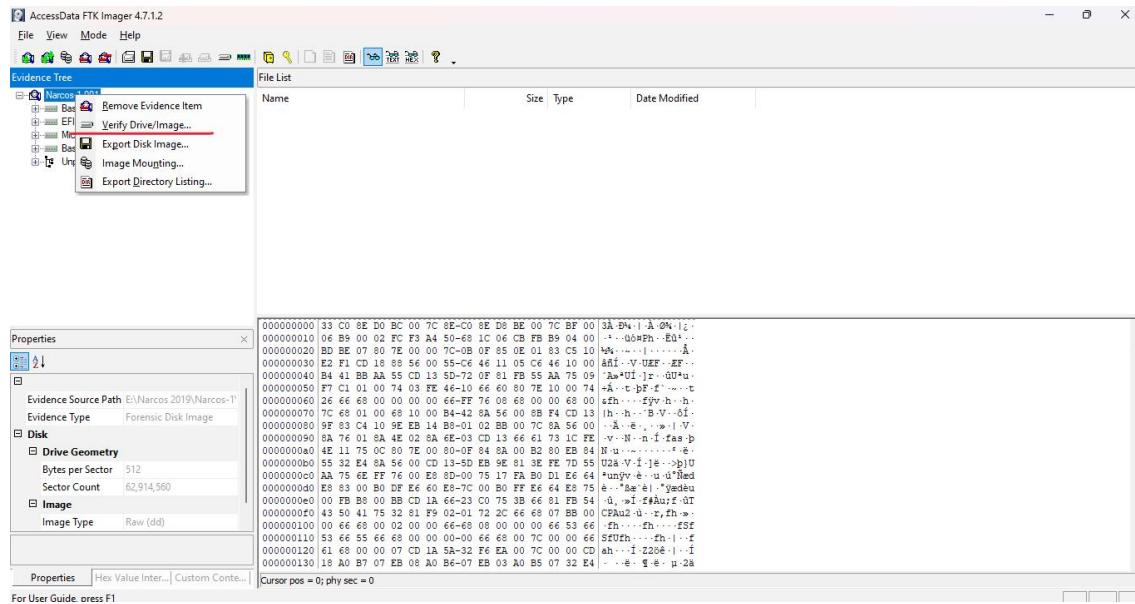


Figure 4 verify the disk image.

- Started verifying the Image.

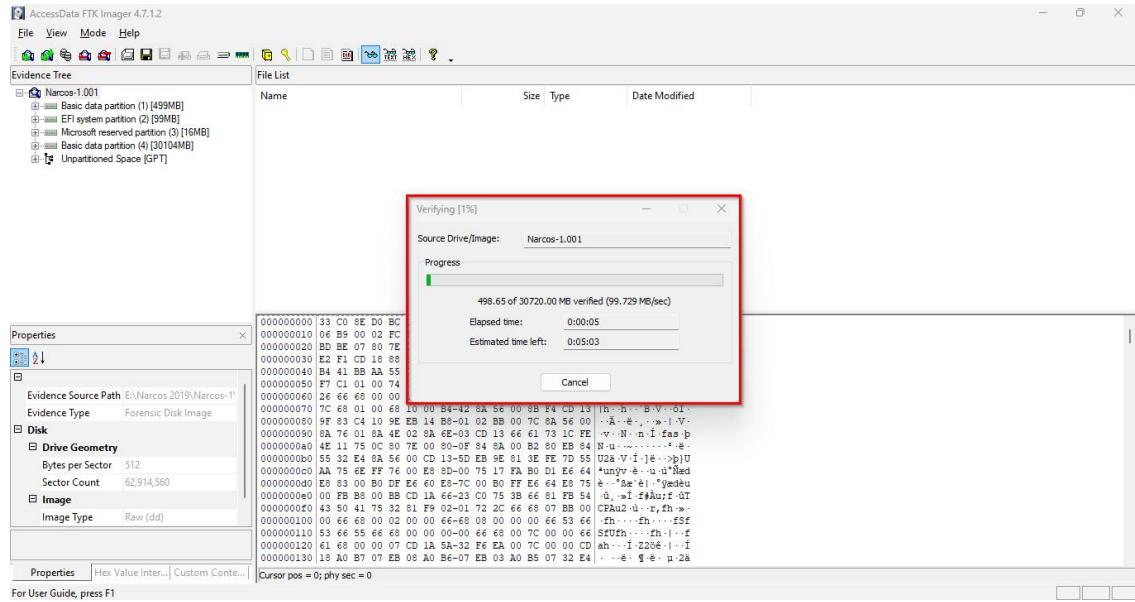


Figure 5 verifying the Image.

- Verification done and hashes is calculated.

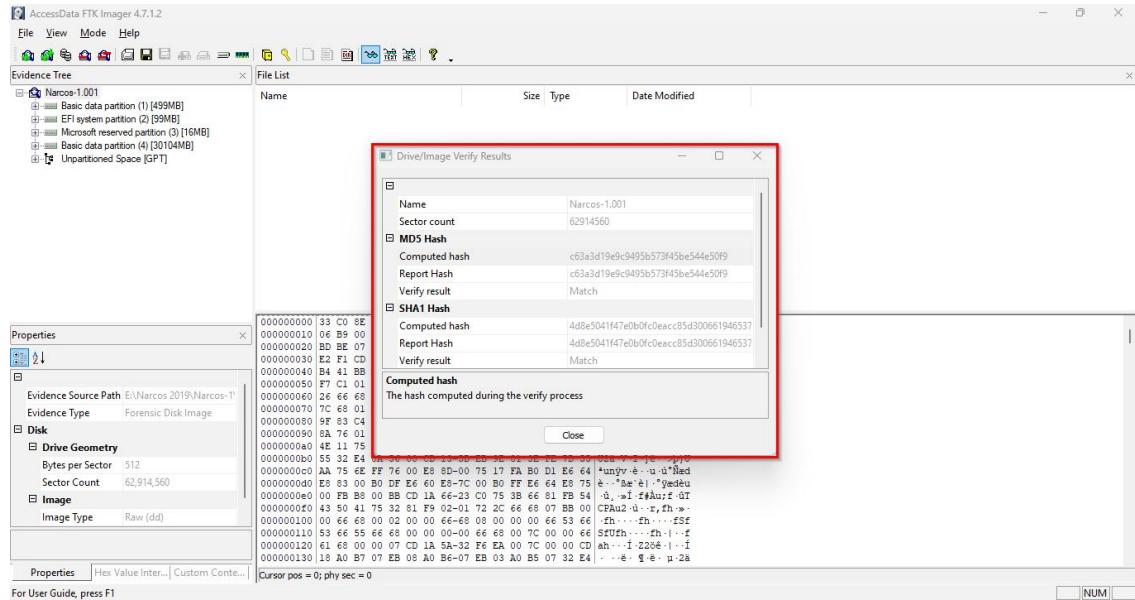


Figure 6 Verification done and hashes is calculated.

2.1 Case Preservation

Firstly, we match the MD5 hash of the image provided this is done to ensure that correct image has been received by the investigator and that the image hasn't gone through some change during movement.

Now, before starting the working on the image we would use the tool FTK imager to create a copy image of the original image. This is done to ensure that the original image doesn't go through some permanent change, or the original image doesn't suffer from some changes during the working. As this would degrade the credibility of the discovered evidence moving forward with the case. All the working moving forward for this case is done upon this copy image.

Next, the hash of that copy image is also compared to ensure that the image hasn't gone through some changes.

Drive Images:

Actor	File Name	Provided MD5	Calculated MD5
Steve Kowhai	Narcos-1a.001-021	c63a3d19e9c9495b573f45be544e50f9	c63a3d19e9c9495b573f45be544e50f9
Jane Esteban	Narcos-3a.001-021	6265dbaa16a354daddba311334484660	6265dbaa16a354daddba311334484660
John Fredricksen	Narcos-2a.001-021	B66ca567bec6b0a195b99c57dfa0919f0919f	B66ca567bec6b0a195b99c57dfa0919f0919f

Memory Images:

Actor	File Name	Provided MD5	Calculated MD5
Steve Kowhai	Narcos-1a.001-021	9ca08c17b4a359d61f6f8f7bb6328c1c	9ca08c17b4a359d61f6f8f7bb6328c1c
Jane Esteban	Narcos-3a.001-021	0f7e7be4d2844457e2111eaffa1e77ec	0f7e7be4d2844457e2111eaffa1e77ec
John Fredricksen	Narcos-2a.001-021	8e8a3a91eb89fe6c3cd10231f13141fe	8e8a3a91eb89fe6c3cd10231f13141fe

2.1.1 Method to preserve evidence

To preserve the evidence, I used FTK imager tool to make a copy of the original image file.

- Open FTK Imager tool.

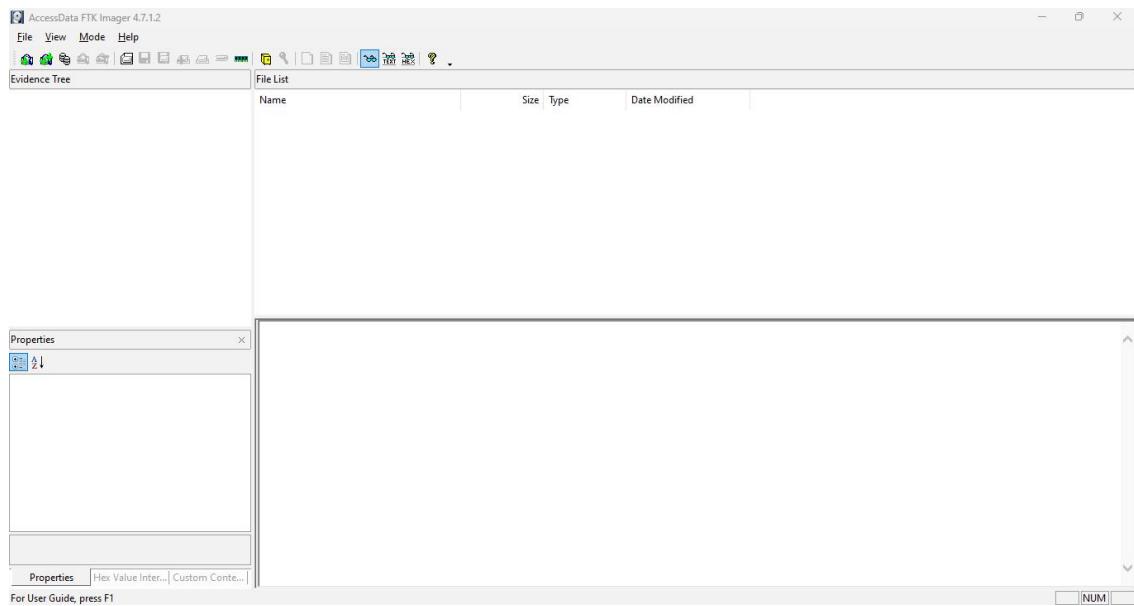


Figure 7 FTK Imager tool

[SPACE INTENTIONALLY LEFT BLANK]

- Go to File --> Create Disk Image

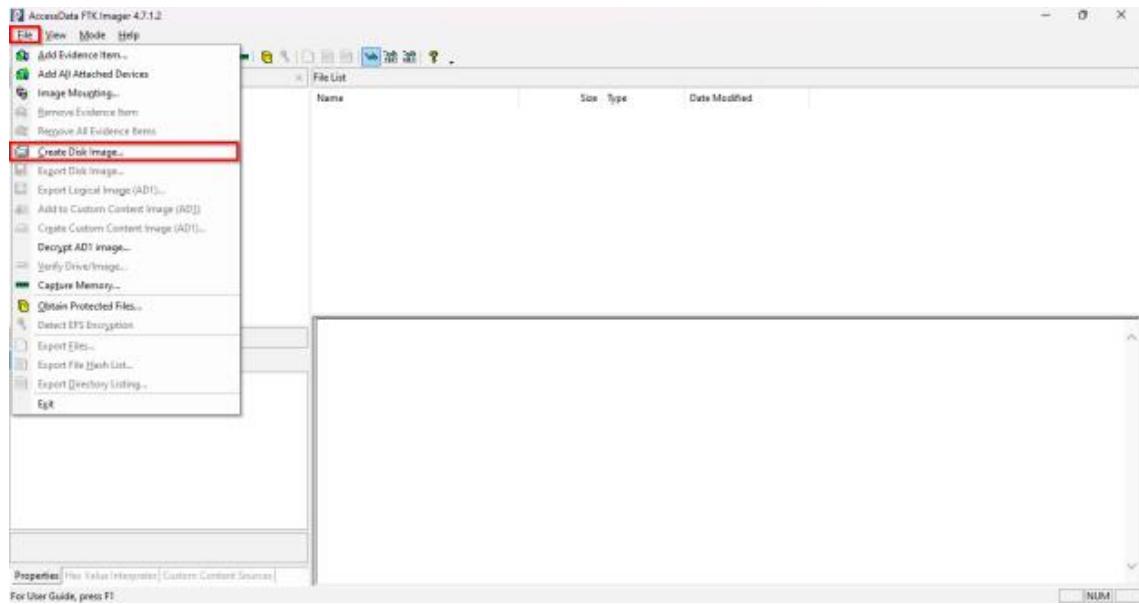


Figure 8 Create Disk Image

- Select Image File option

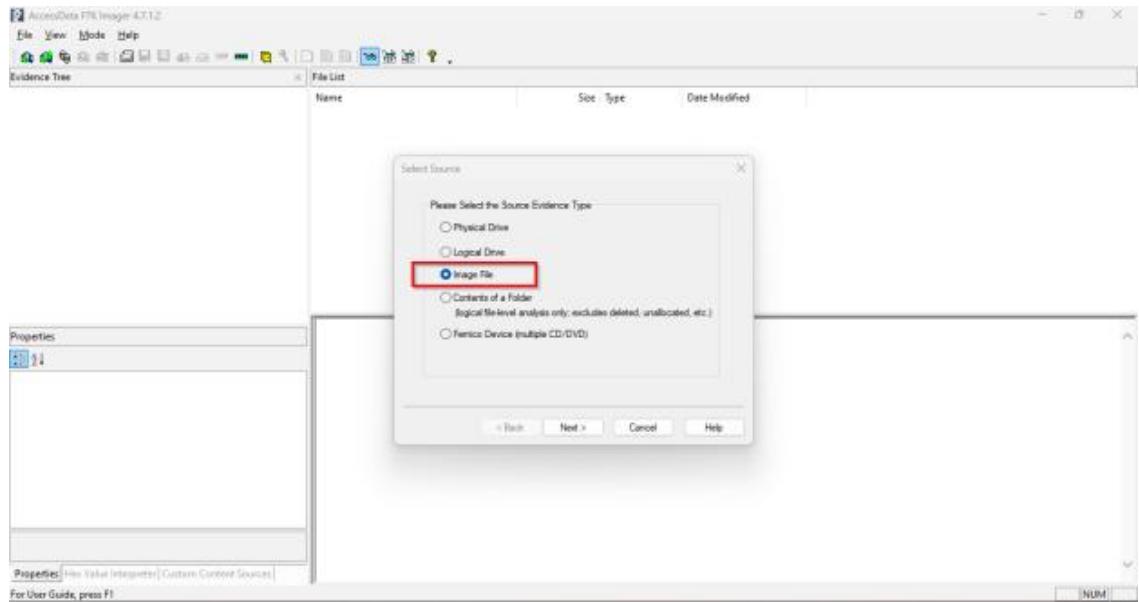


Figure 9 Image File option

- Add the original Image file

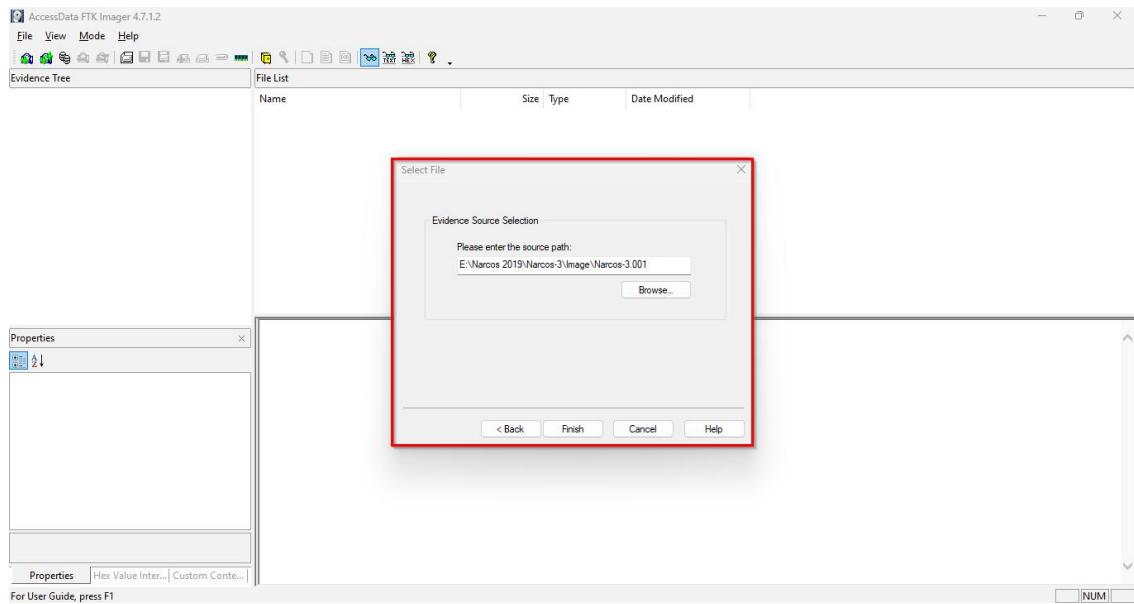


Figure 10 add the original Image file

- Add the important necessary information.

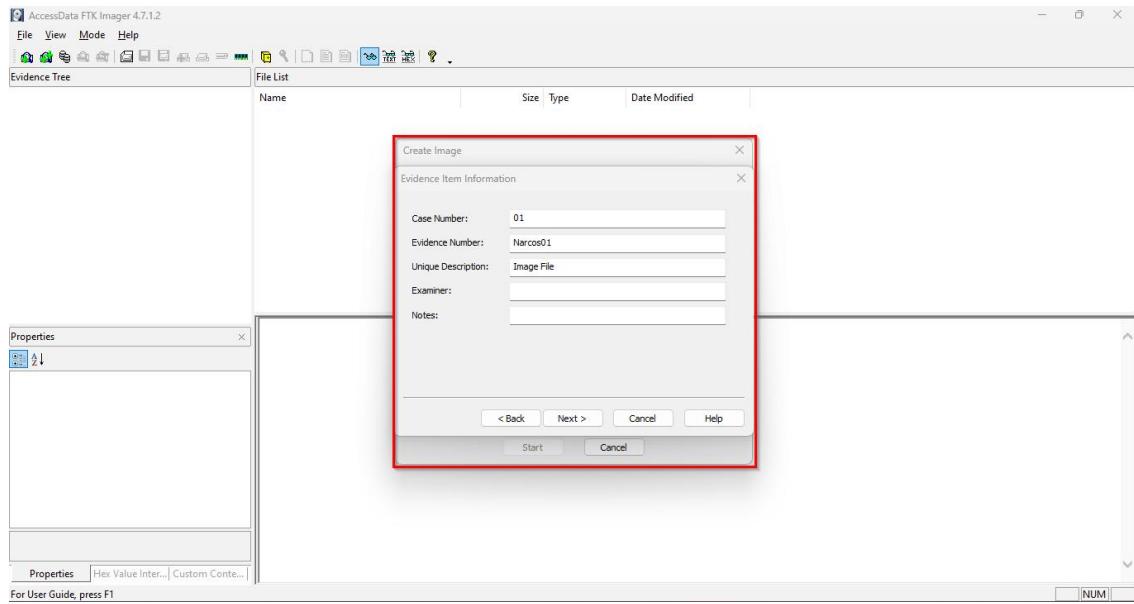


Figure 11 Add the important necessary information.

- Add image destination file

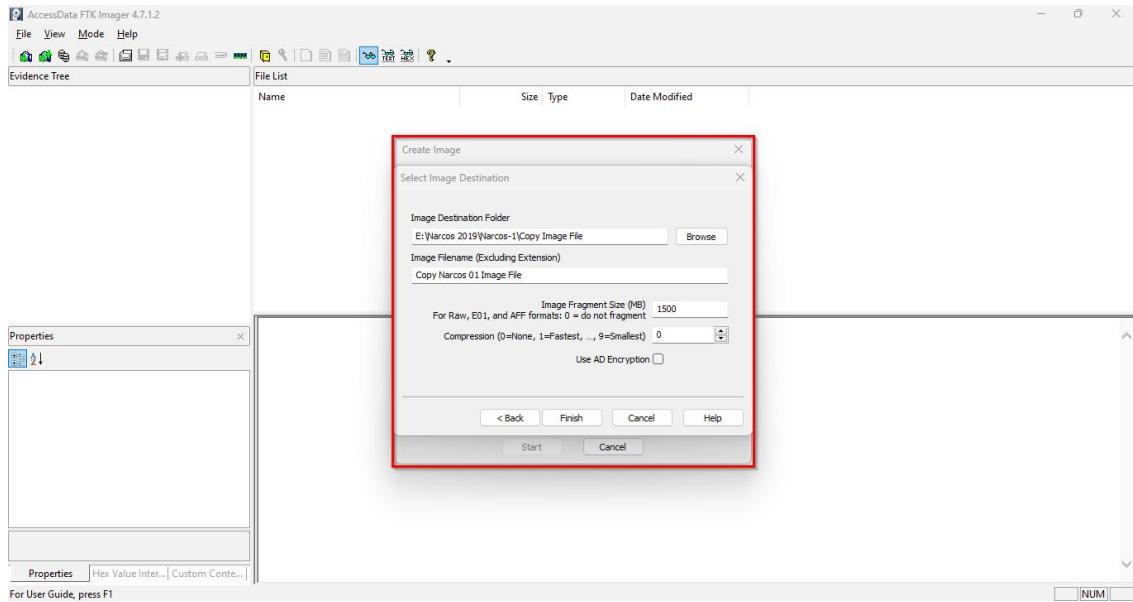


Figure 12 Add image destination file

- Start copying the image.

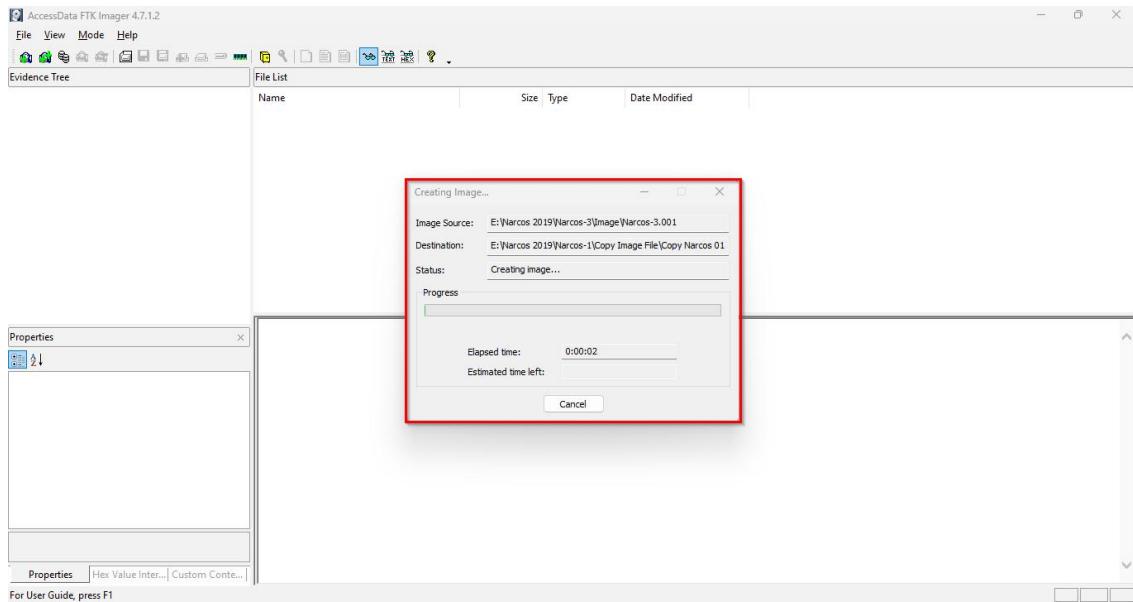


Figure 13 copying the image.

- Copying of the image hash file is done

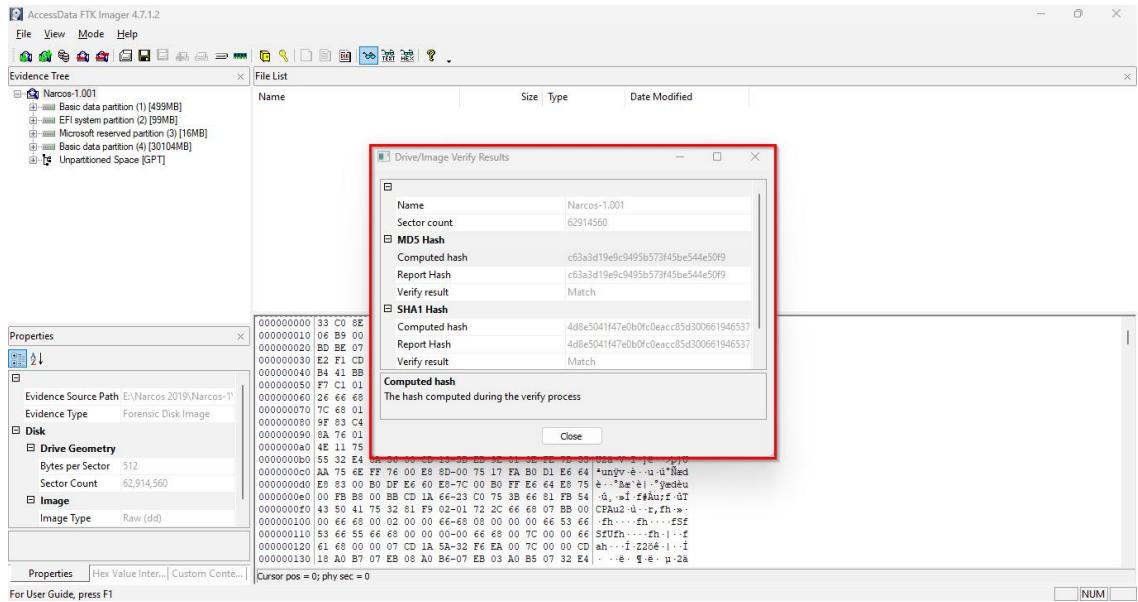


Figure 14 Copying of the image hash file is done

2.2 Case Tools

Moving forward with the case after all the previous work is done of preserving the evidence. We start working on analyzing the evidence for this purpose we utilize 2 tools

1. Autopsy
2. Registry Viewer

We use autopsy for analyzing the images. We used it since its user-friendly interface and extensibility makes it a popular choice among forensic examiners and investigators worldwide used for analyzing disk images, extracting data, and uncovering evidence in various investigative scenarios. As compared to some other tools, namely Magnet AXIOM. Also, this tool is recognized by many countries' courts so there is no issue on the credibility of evidence gathered from Autopsy. There is a personal preference here as well in this case.

Next, I would use FTK imager provided registry file and then use that file in registry viewer. Registry viewer would give us a much better Gui view of the systems registry as compared to tools like RegScanner.

FTK Imager:

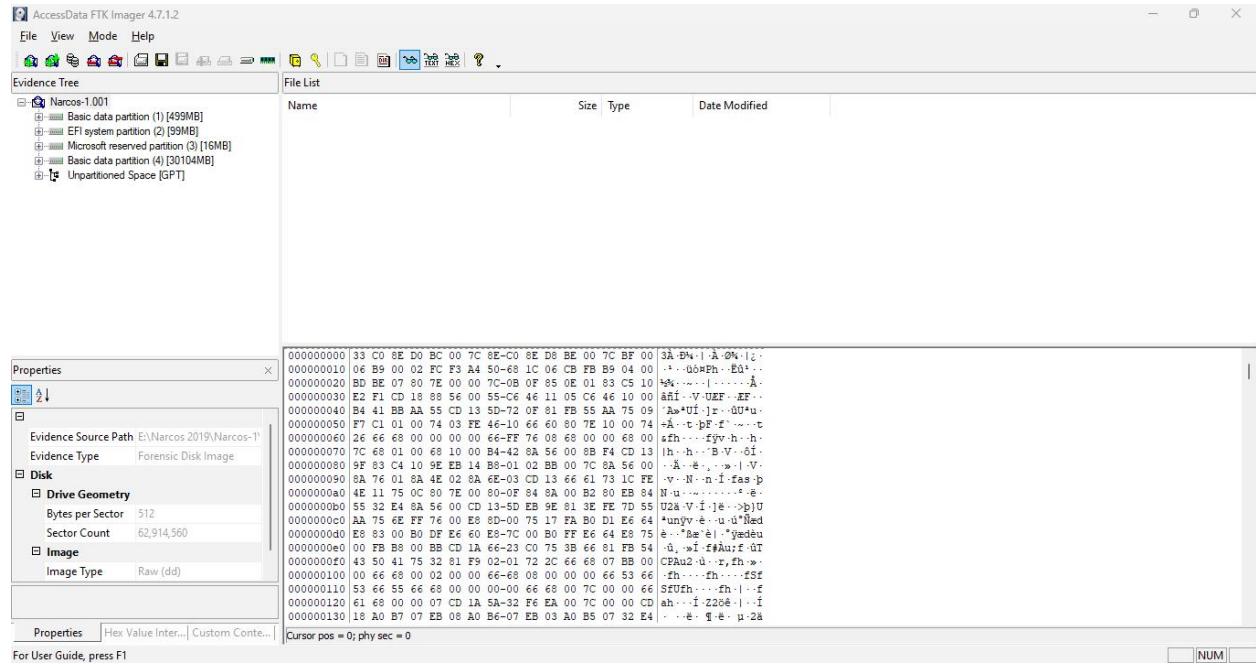


Figure 15 FTK Imager

Autopsy:

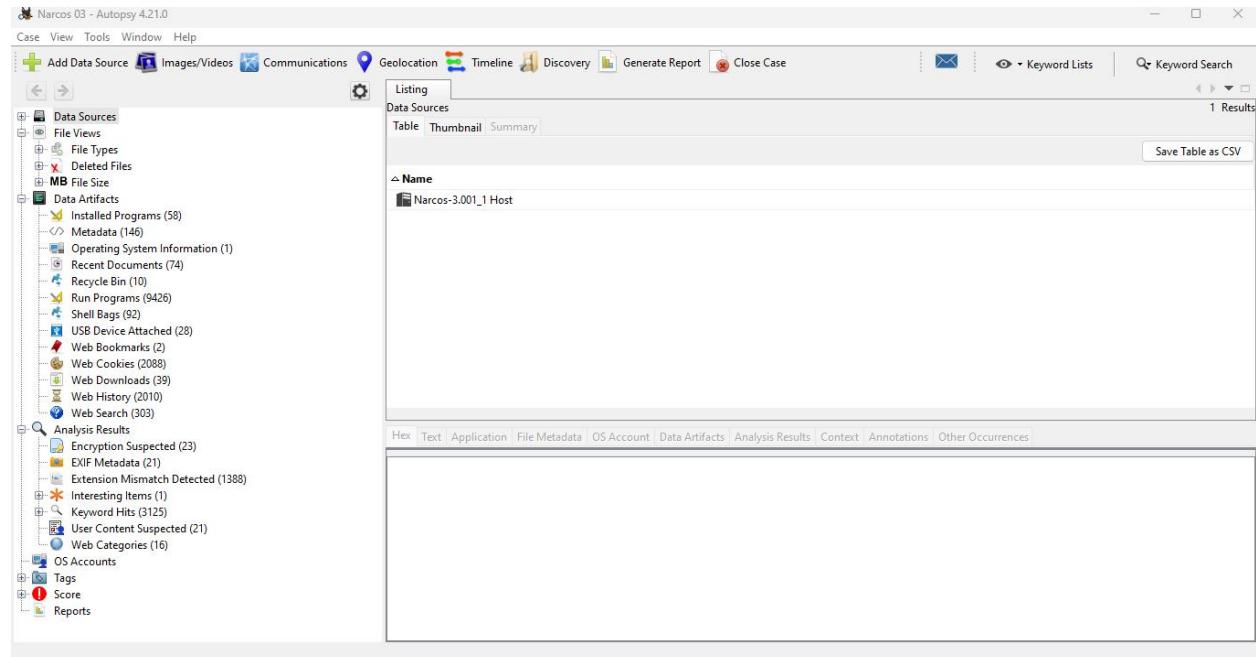


Figure 16 Autopsy

Registry Viewer:

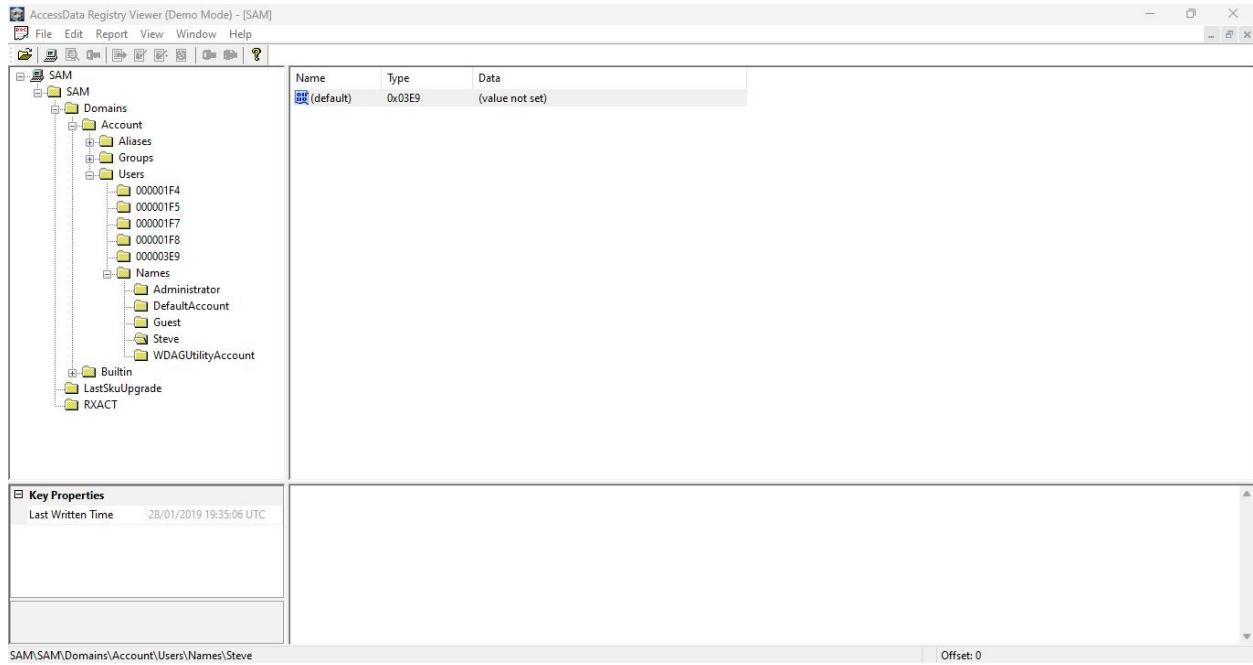


Figure 17 Registry Viewer

2.3 Case Main Suspects

Steve Kowhai: Is New Zealand based drug dealer wanting to find quality products for his drug empire.

Jane Esteban: Jane is an undercover Australian Federal Police (AFP) officer tasked with gathering evidence about a drug ring involving John Fredricksen and his associate Steve Kowhai in New Zealand.

John Fredricksen: John has been asset of Steve Kowhai (NZ dealer) as a smuggler with Jane Esteban as her smuggling partner/ mule.

2.4 Case Artifacts

After all the previous work has been done, we move on to the most important part of the investigation. That is extracting evidence whether the person is guilty or innocent. The data extracted from forensic analysis is known as ‘artifacts’ which in turn is used as evidence.

Normally there are a lot of artifacts present on a system. Some of these are not as usable as evidence may seem. Some help in building timelines of crimes and some are used to uncover the hidden motives or objectives of a person.

In our case we are doing a specific analysis of the system image following all the rules provided above and utilizing all the tools as well. We are trying to gather specific evidence related to the list of suspects provided to us. So mainly we are trying to get some documents, some chats or some emails which can be used to say that the crime this individual is accused of is what he is guilty of as well. This would mainly be done using autopsy and volatility.

Standard information like time zone, system os etc. Isn't relevant as to this report.

[SPACE INTENTIONALLY LEFT BLANK]

3. Finding and Description

3.1 User Account Profiles and Computer Names

These users were found on the systems confiscated from the scene.

Actor	Computer Name	Usernames
Steve Kowhai	SK-DESKTOP	Steve
Jane Esteban	JELAPTOP	JaneE
John Fredricksen	JOHNFLAPTOP1	JohnF

Paths:

For Computer Name:

The computer name can be found in the following registry key:

HKEY_LOCAL_MACHINE - SYSTEM - CurrentControlSet - Control - ComputerName -
ComputerName

For Usernames:

The user account profiles are in the following registry key:

HKEY_LOCAL_MACHINE - SOFTWARE - Microsoft - Windows NT -CurrentVersion -
ProfileList

Steve Kowhai Computer Name:

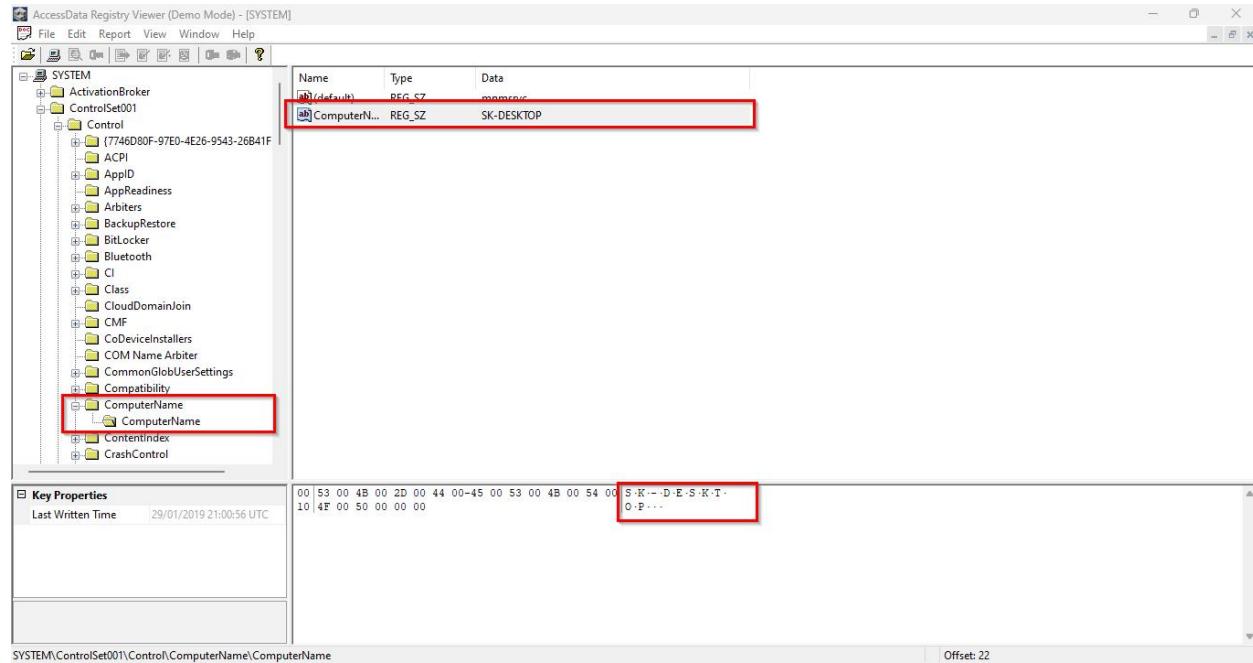


Figure 18 Steve Kowhai Computer Name

Steve Kowhai Username:

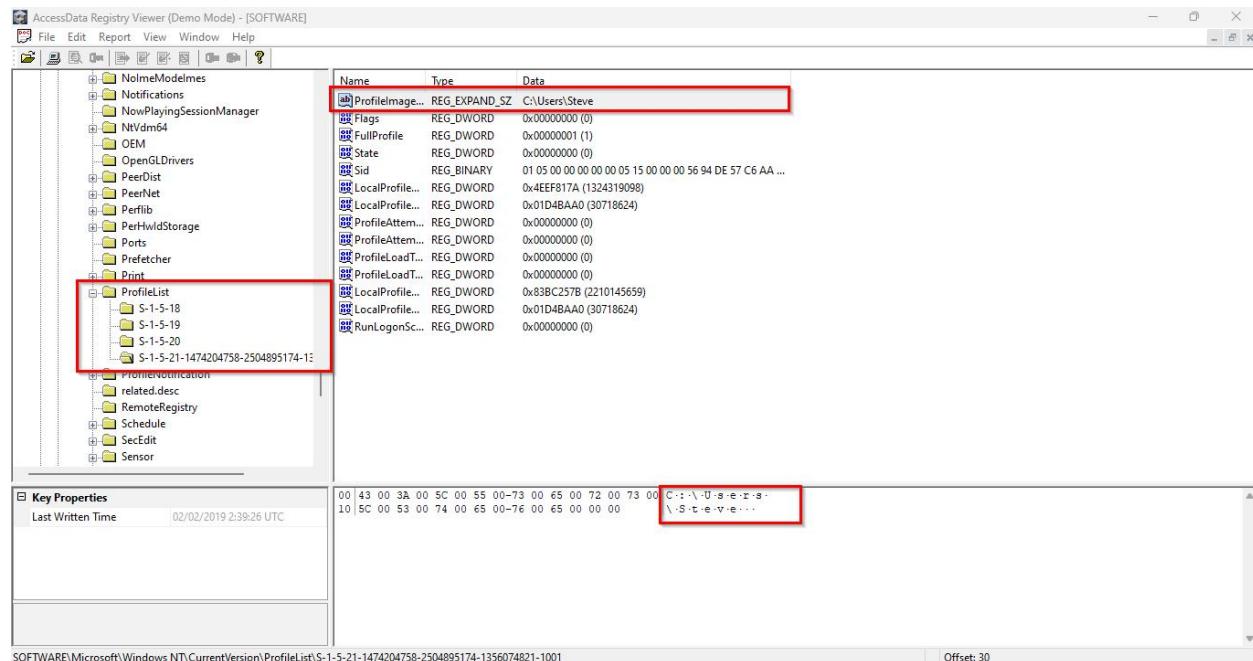


Figure 19 Steve Kowhai Username

John Fredricksen Computer Name:

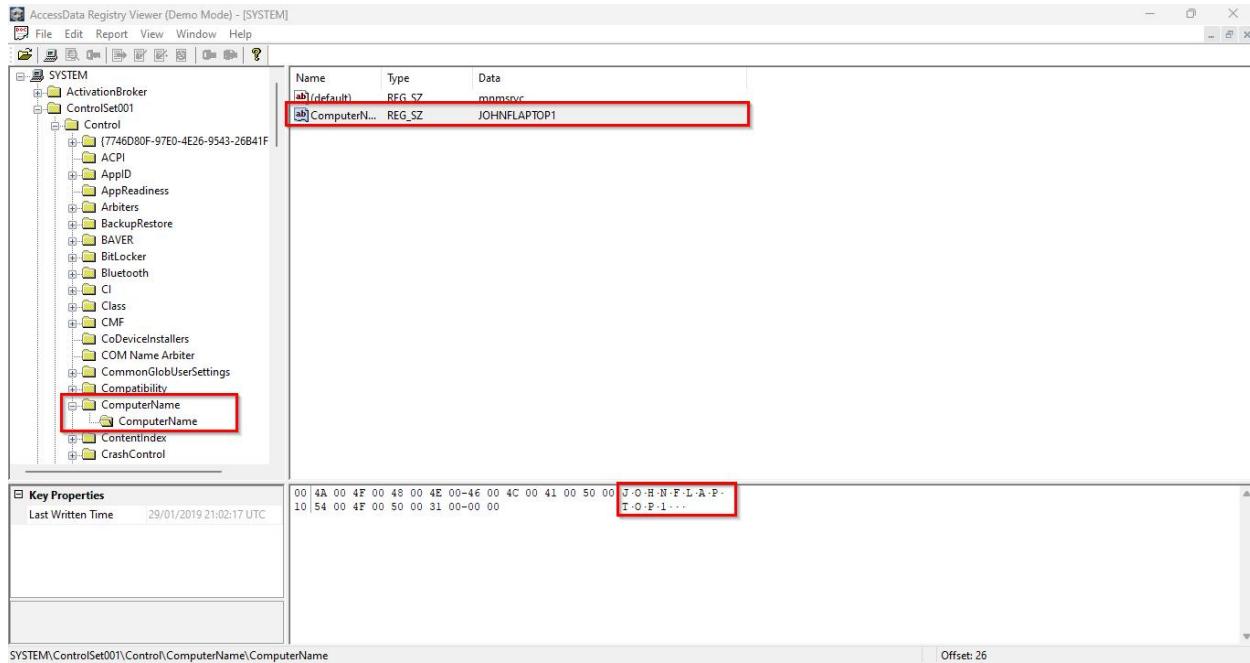


Figure 20 John Fredricksen Computer Name

John Fredricksen Username:

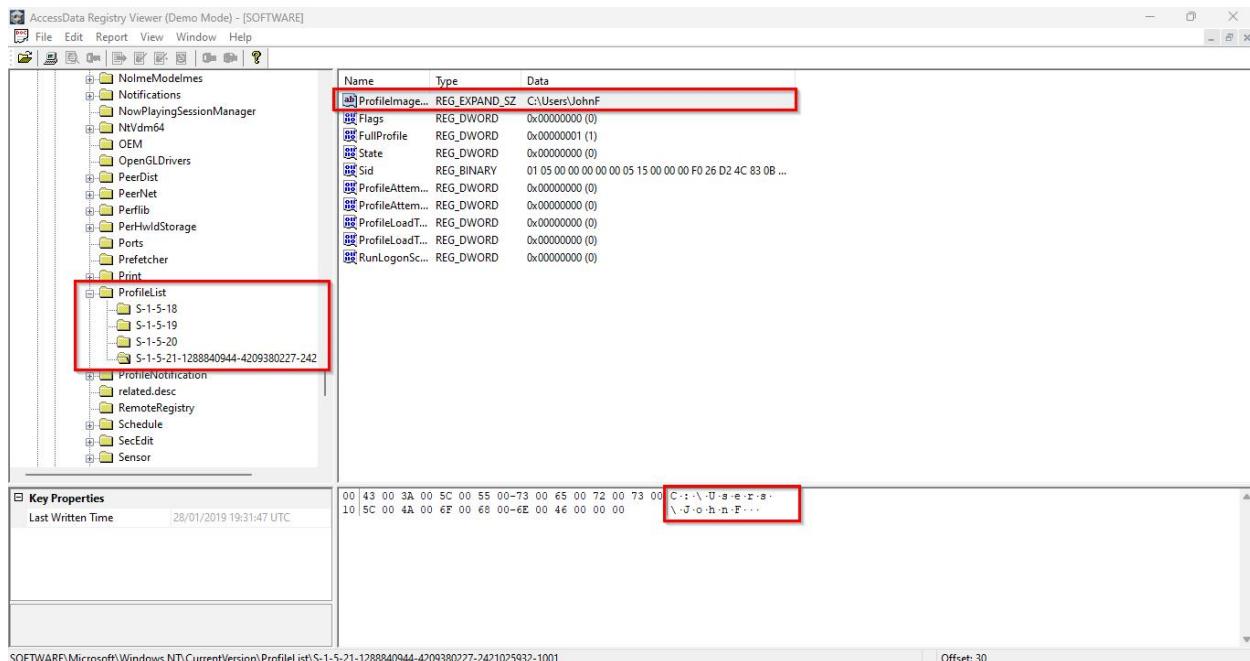


Figure 21 John Fredricksen Username

Jane Esteban Computer Name:

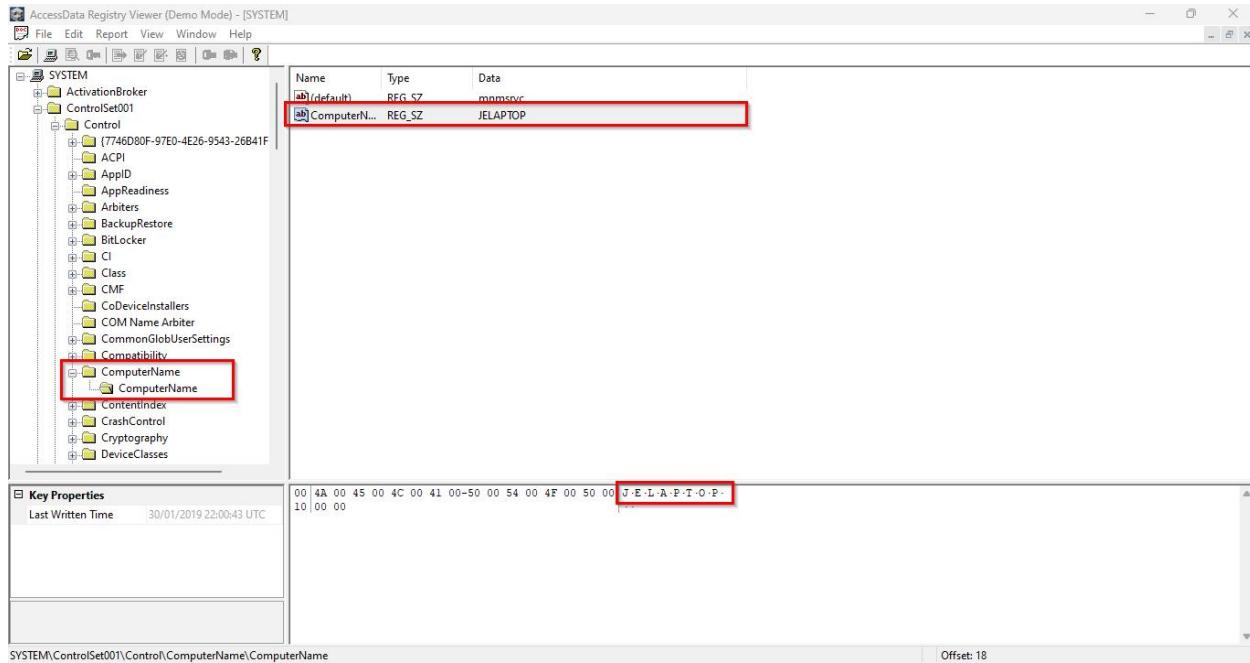


Figure 22 Jane Esteban Computer Name

Jane Esteban Username:

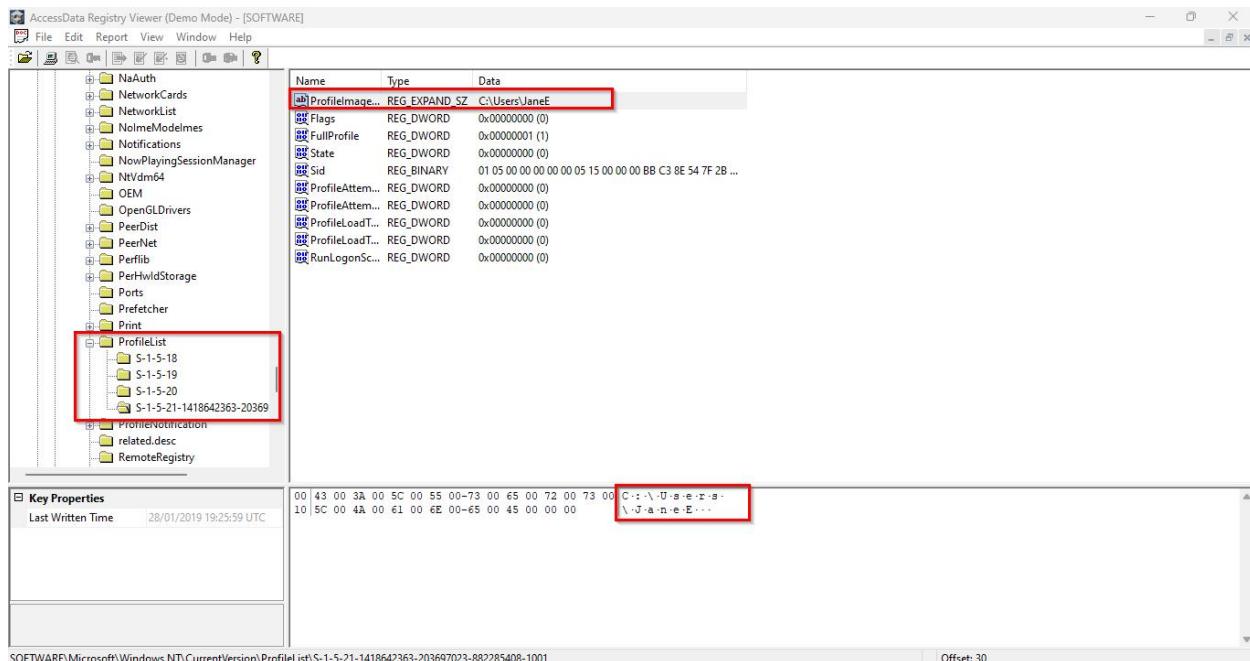


Figure 23 Jane Esteban Username

3.2 Web Activity

Relevant web activity on each suspect's computer.

3.2.1 Steve Kowhai:

In Steve Kowhai web history multiple searches related to drug use, distribution, and trafficking were discovered. He seems to be searching for 'crystal meth', 'drug paraphernalia', 'drug paraphernalia meth', 'best places to trade drugs', 'cutting drugs', 'cutting agent for ice' and 'drug routes in Wellington'. Additionally, he seems to be searching for 'how to launder money'. This all suggests Steve Kowhai being a drug dealer rather than user and possibly him distributing it and laundering the money to stay safe from IRS.

Moreover, he is seen searching for software's to encrypt and possibly hide his working on the system.

ccleaner: Software often used to clean up evidence on a computer.

truecrypt: Encryption software that could be used to hide illegal activities.

protonmail: An encrypted email service that could be used for private communications related to illegal activities.

Web Search:

- crystal meth
- drug paraphernalia
- drug paraphernalia meth
- gangs nz drugs
- best places to trade drugs
- cutting drugs
- cutting agents for ice
- how to launder money
- drug routes in Wellington
- international drug routes
- image steganography download
- ccleaner

- truecrypt
- protonmail

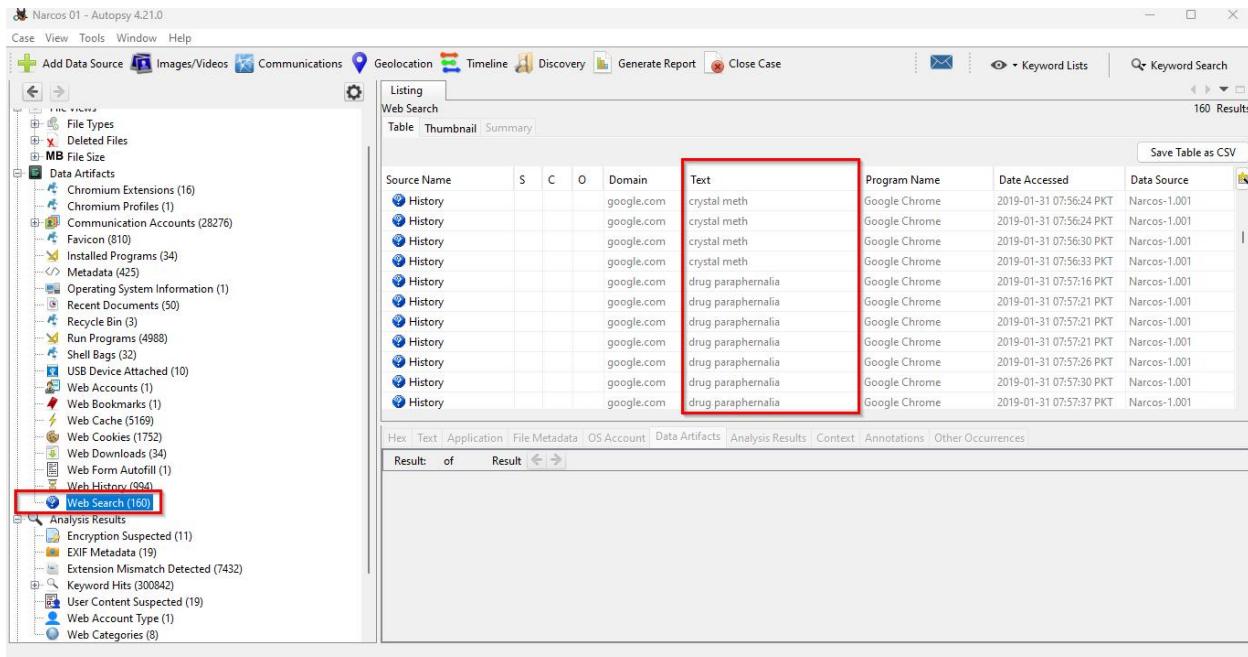


Figure 24 Steve Kowhai Web Search

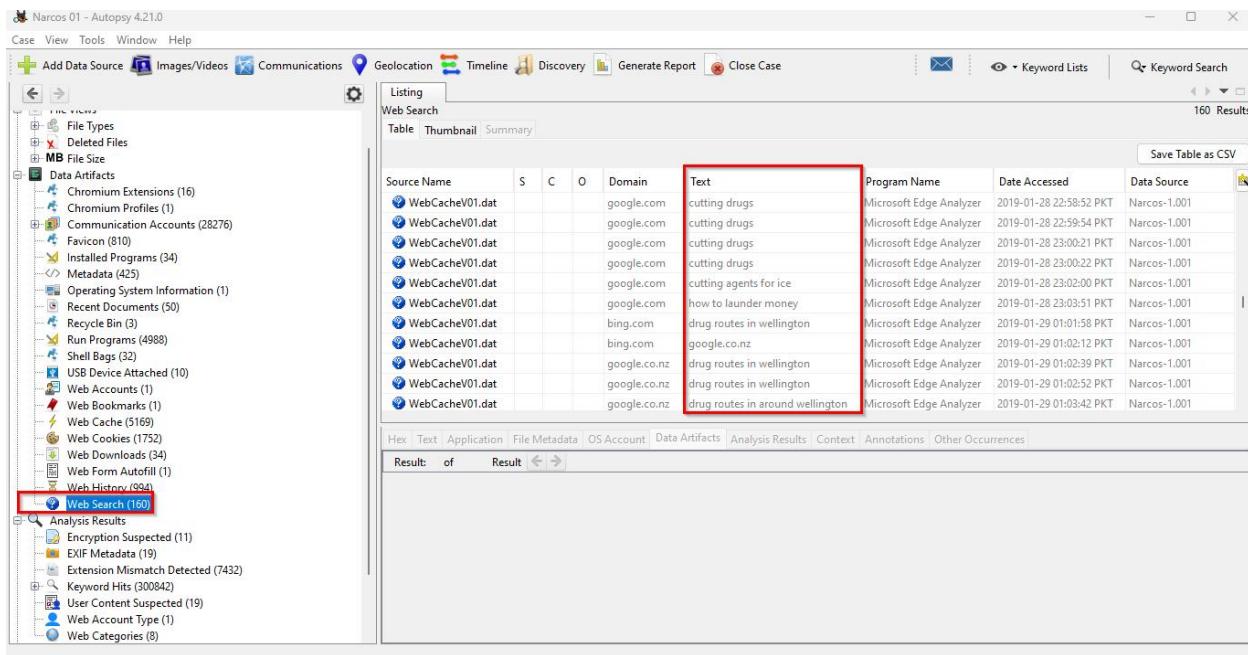


Figure 25 Steve Kowhai Web Search

3.2.2 Jane Esteban:

In Jane Esteban, web history multiple searches related to federal agency such as ‘federal agent badge’, ‘federal agent badge au’, ‘discord’, ‘micro voice recorder’, ‘micro voice recorder’, ‘how to act like a meth addict’, ‘how to look like a meth addict’, ‘news9’, ‘theguardian’, ‘reddit’, ‘how to pretend to be desperate’, ‘survival tips for undercover cop’, ‘undercover cop survival’.

All this led us to believe the Jane is possible an undercover cop. Who's acting as mole for possibly police. This is believed by all the searches about acting like a drug addict and how to survive as a mole.

Web Search:

- federal agent badge
- federal agent badge au
- disocrd
- micro voice recorder
- Micro voice recorder au
- How to act like a meth addict
- How to look like a meth addict
- News9
- Theguardian
- Reddit
- How to pretend to be desparate
- Survival tips for an undercover cop
- Undercover cop survival

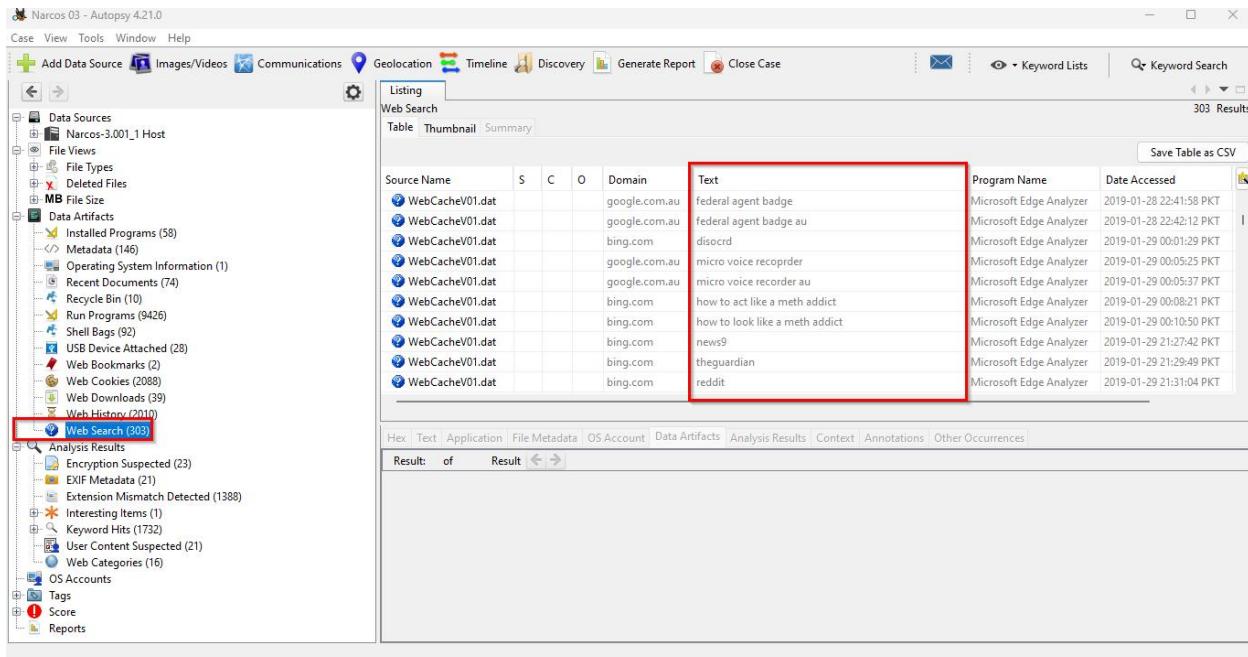


Figure 26 Jane Esteban Web Search

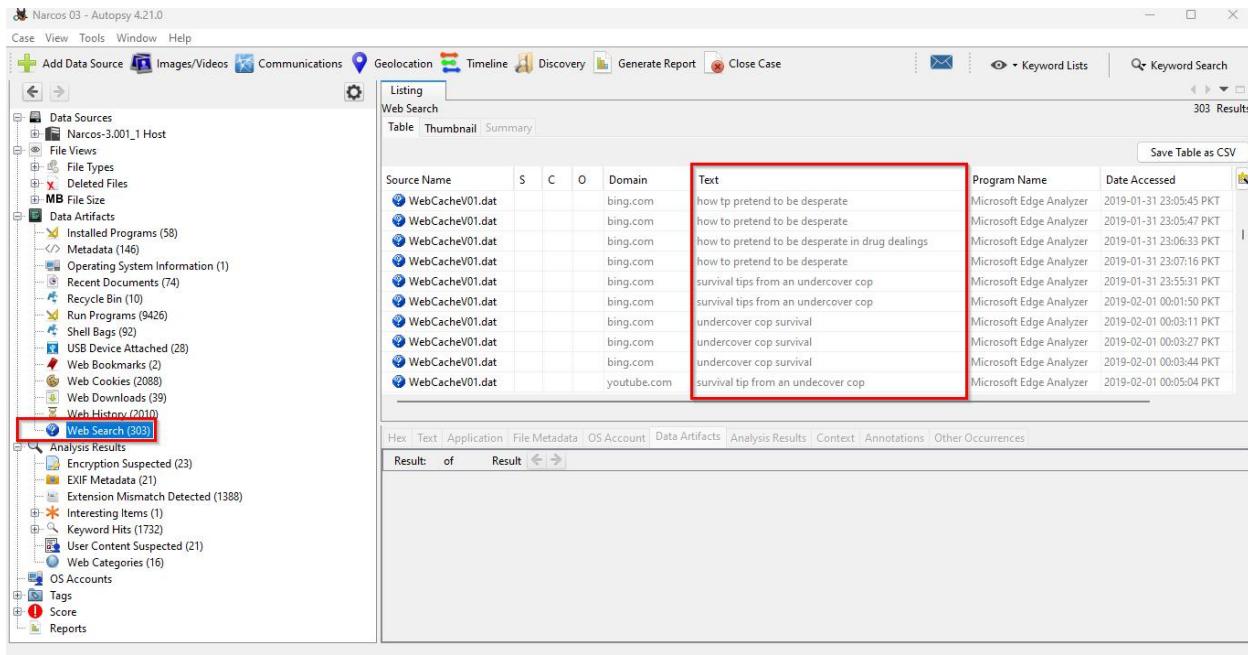


Figure 27 Jane Esteban Web Search

3.2.3 John Fredricksen:

In John Fredricksen, web history multiple searches related to ‘pablo escobar’, ‘body packing’, ‘suitcase concealment’, ‘suitcase concealment for drugs’, ‘cutting drugs’, ‘drugs subreddit’ leads us to believe that John is a drug user and is looking for ways to hide drugs in suitcase.

Not only that he is seen searching for ‘steganography’, ‘steganography image download’, ‘image steganography’ which leads us to believe that John is hiding something behind his images.

Also, he is seen looking for flights to Wellington, New Zealand.

Web Search:

- drug memes
- pablo escobar
- baidu antivirus download
- openoffice
- discord
- encryption methods youtube
- suitcase concealments
- suitcase concealments for drugs
- new zealand to wellington
- Flight brisbane to WLG return
- cutting drugs
- how to launder money
- drugs subreddit
- suitcase concealments
- how to cut drugs
- steganography
- steganography image download
- tutorial on image steganography
- image steganography

- protonmail
- discord
- openoffice

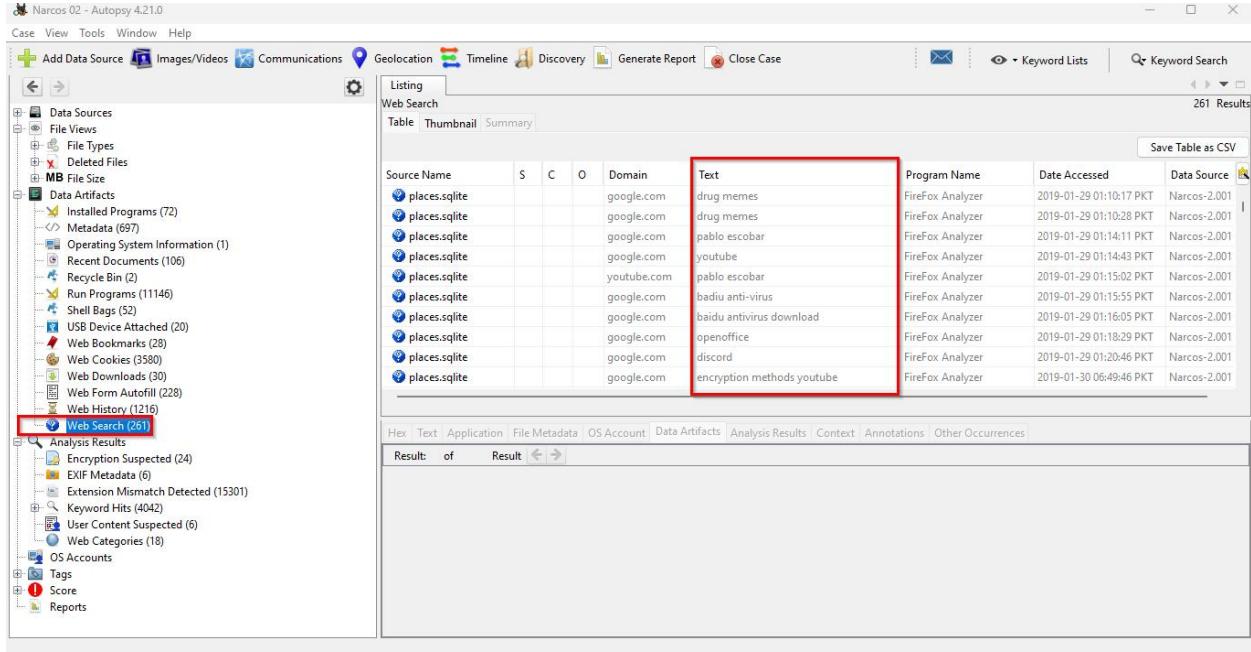


Figure 28 John Fredricksen Web Search

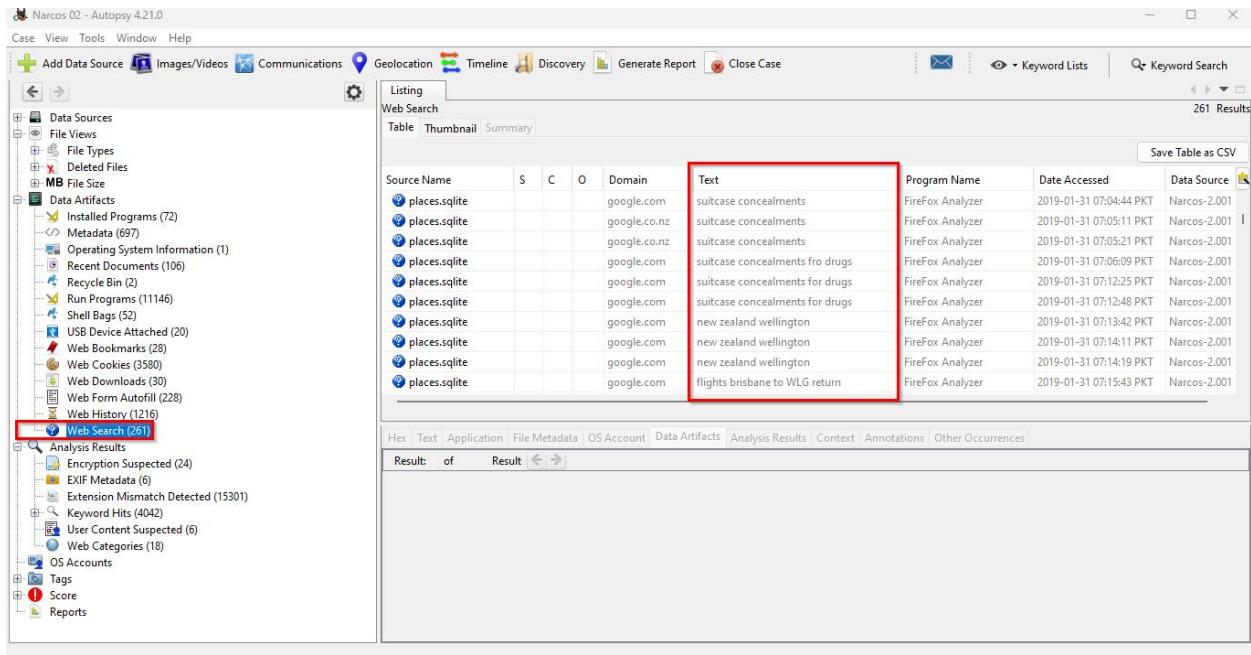


Figure 29 John Fredricksen Web Search

3.3 Behavioral Images

3.3.1 Steve Kowhai

airport crystals.jpg

From the images we can gather that Steve had a route planned out from Eastbourne to his location. And the image name suggests that its crystal and airport hinting to Steve being a drug dealer receiving crystals from airport from John who's looking to hide them.

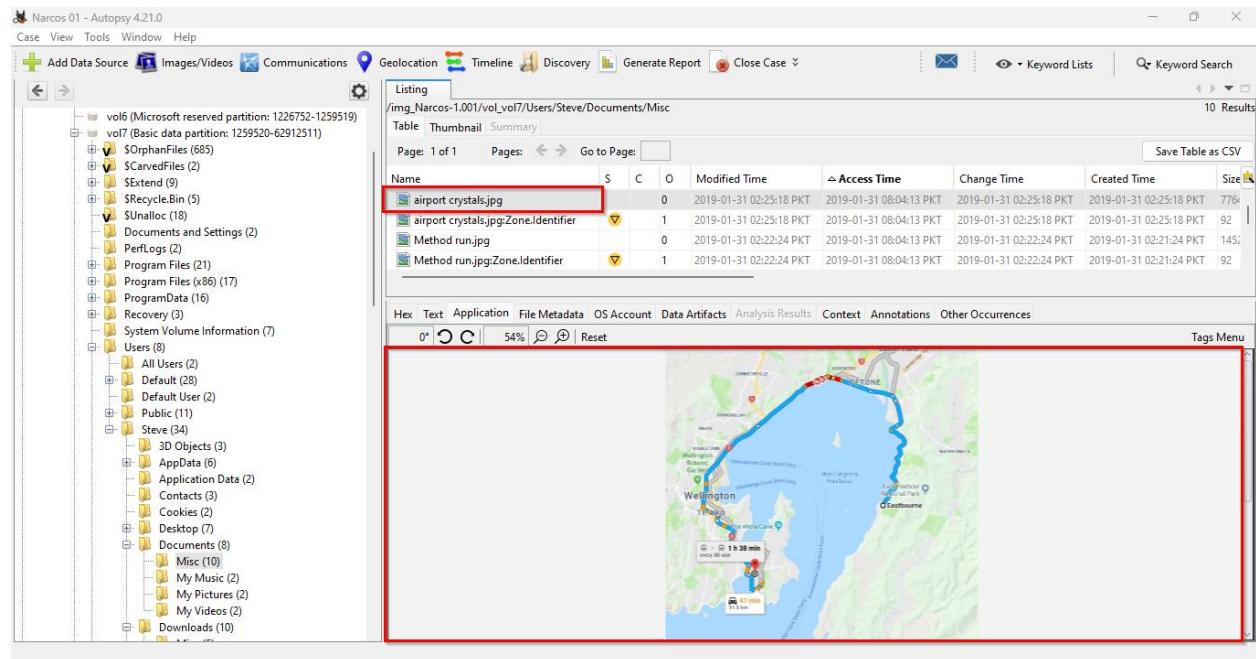


Figure 30 airport crystals.jpg

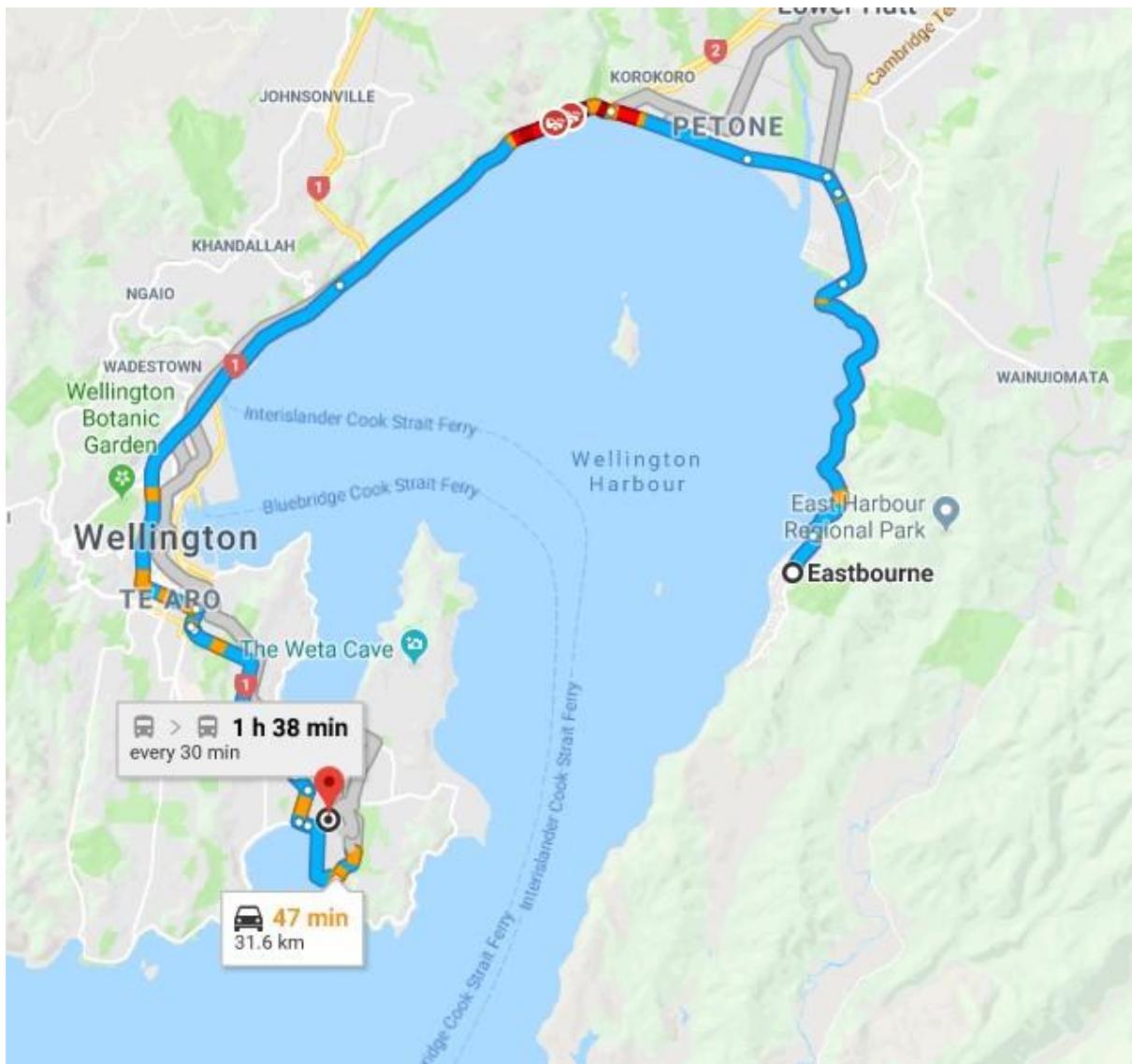


Figure 31 airport crystals.jpg

Methodrun.jpg

In these images it is hinted that Steve had an escape path already done from his home in Eastbourne stocks valley hinted from the image name.

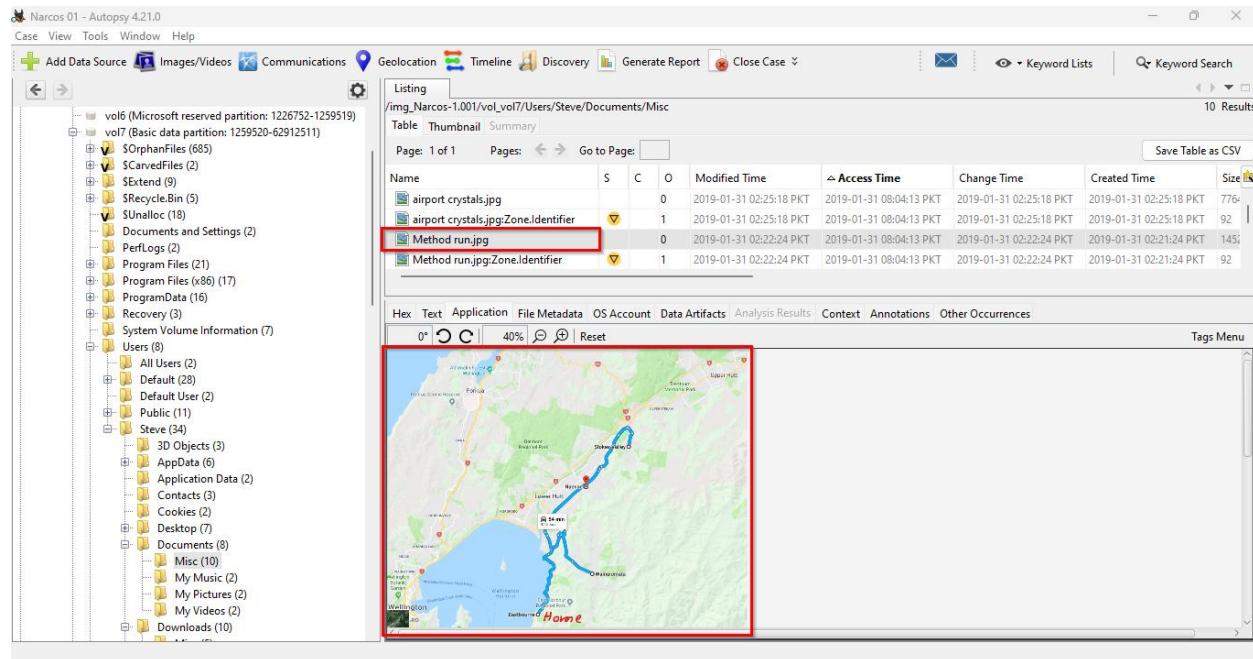


Figure 32 Methodrun.jpg

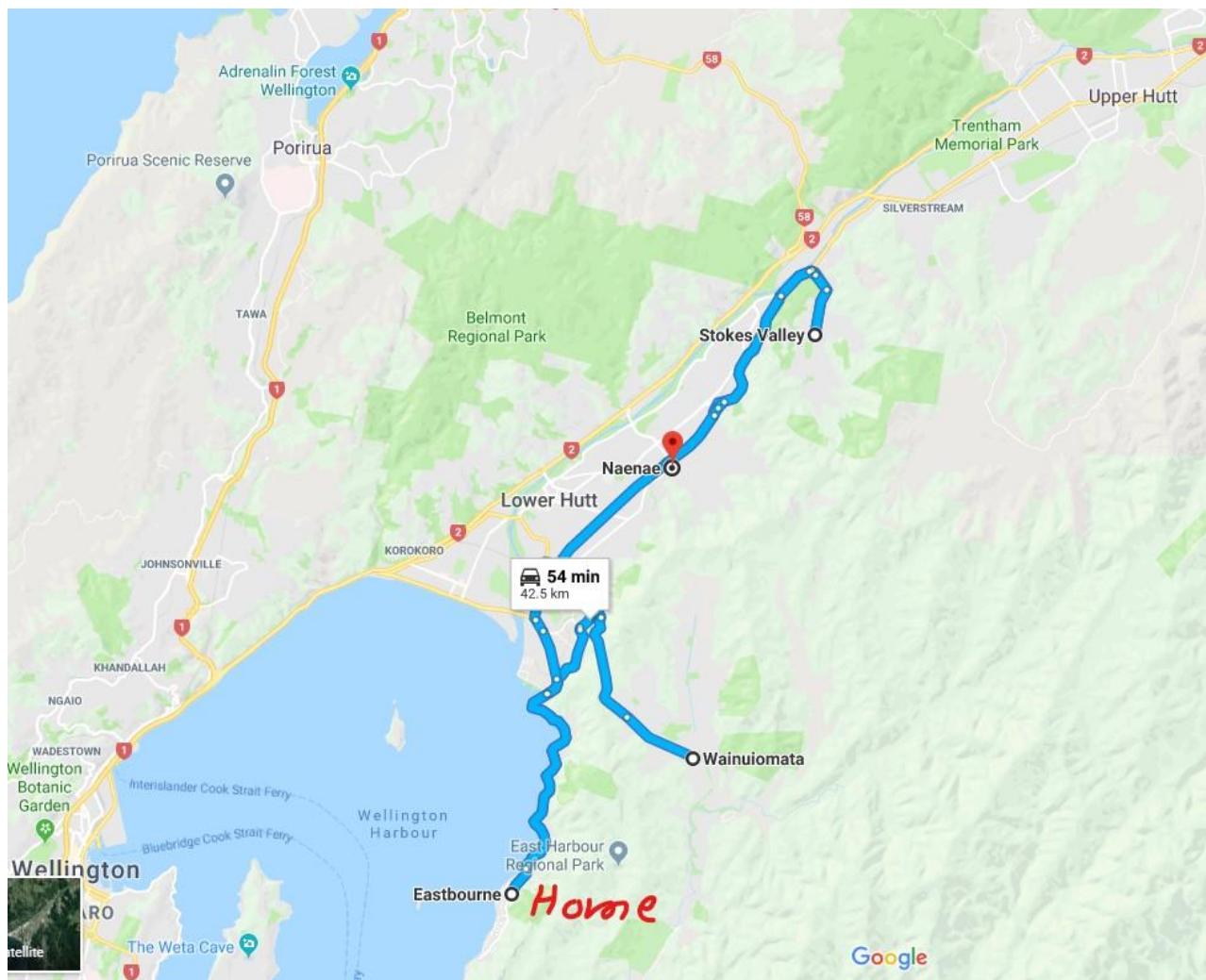


Figure 33 Methodrun.jpg

Dropoff.jpg

This image hints towards a possible dropoff location possibly for his drugs which are being smuggled by John as suggested by image name.

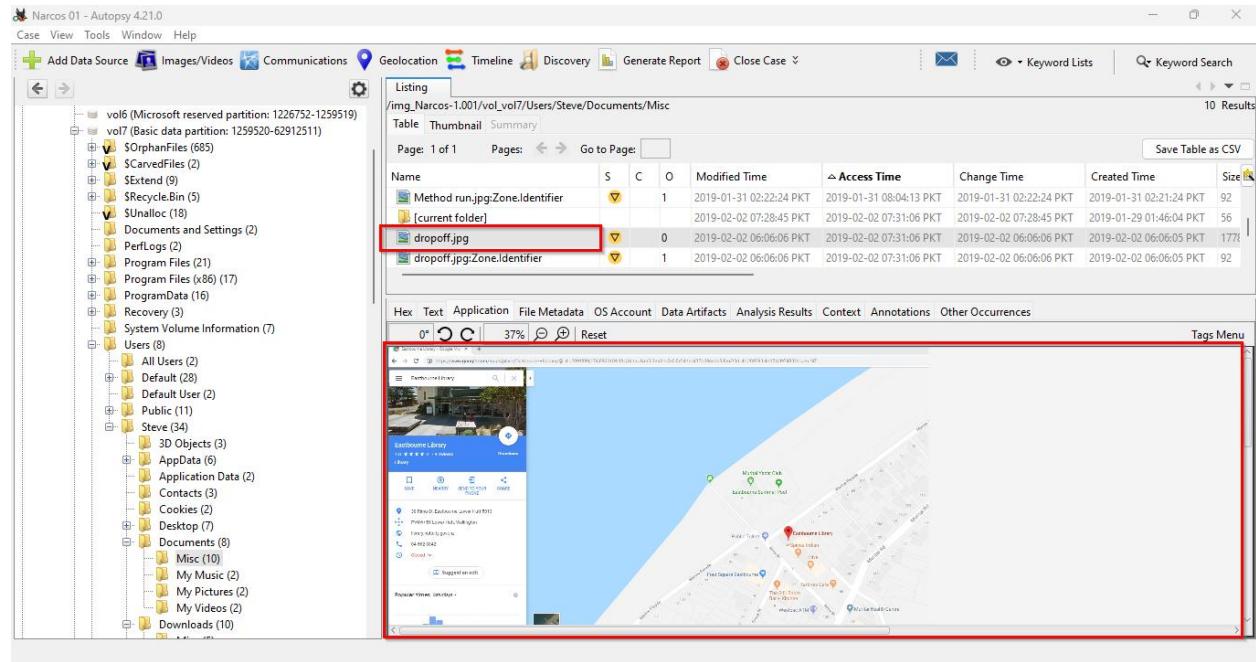


Figure 34 Dropoff.jpg

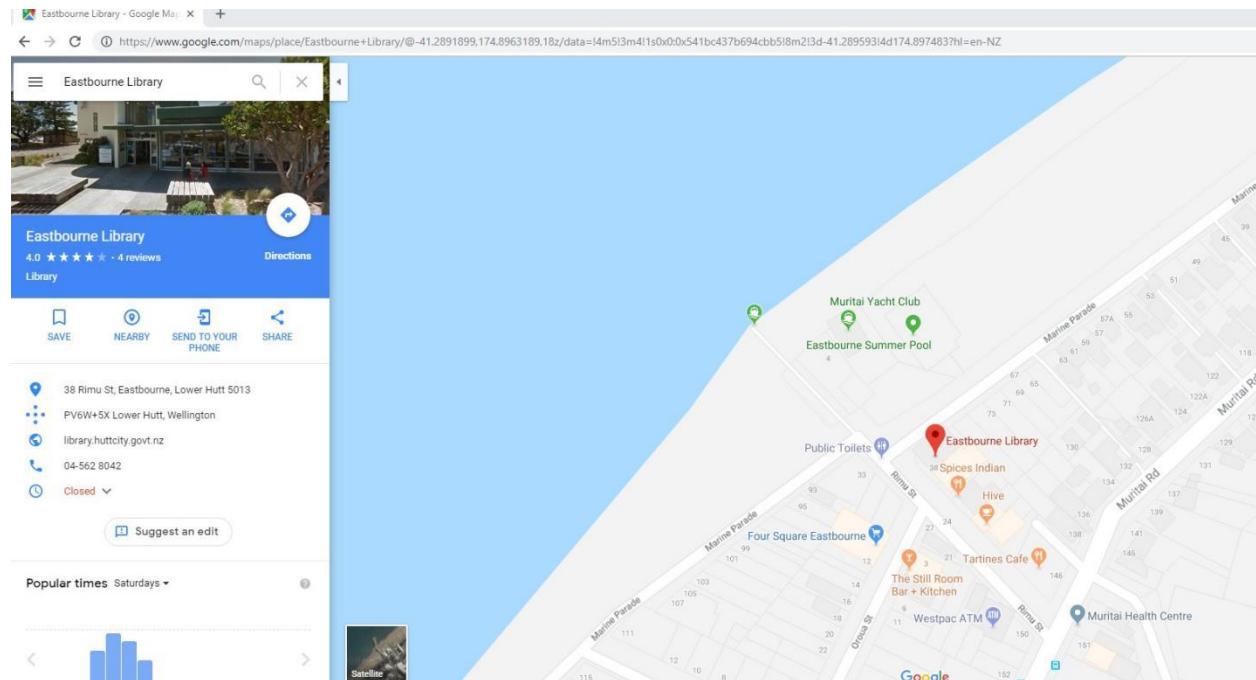


Figure 35 Dropoff.jpg

Flightbookings.PNG

In this image we can see the flight bookings of Steve from Brisbane to Wellington and flight back to Brisbane from Wellington.

The screenshot shows the Narcos 4.21.0 software interface. The left pane displays a file tree with various partitions and user folders. The right pane shows a table of files in the 'Misc' folder, with 'flightbookings.PNG' highlighted. Below the table, a 'Trip Summary' and 'Important Flight Information' section is displayed, also highlighted with a red box. The 'Trip Summary' section shows two flights: one from Brisbane to Wellington on 16 Feb. 2019 and another from Wellington to Brisbane on 23 Feb. 2019. The 'Important Flight Information' section contains a list of bullet points regarding flight rules and fees.

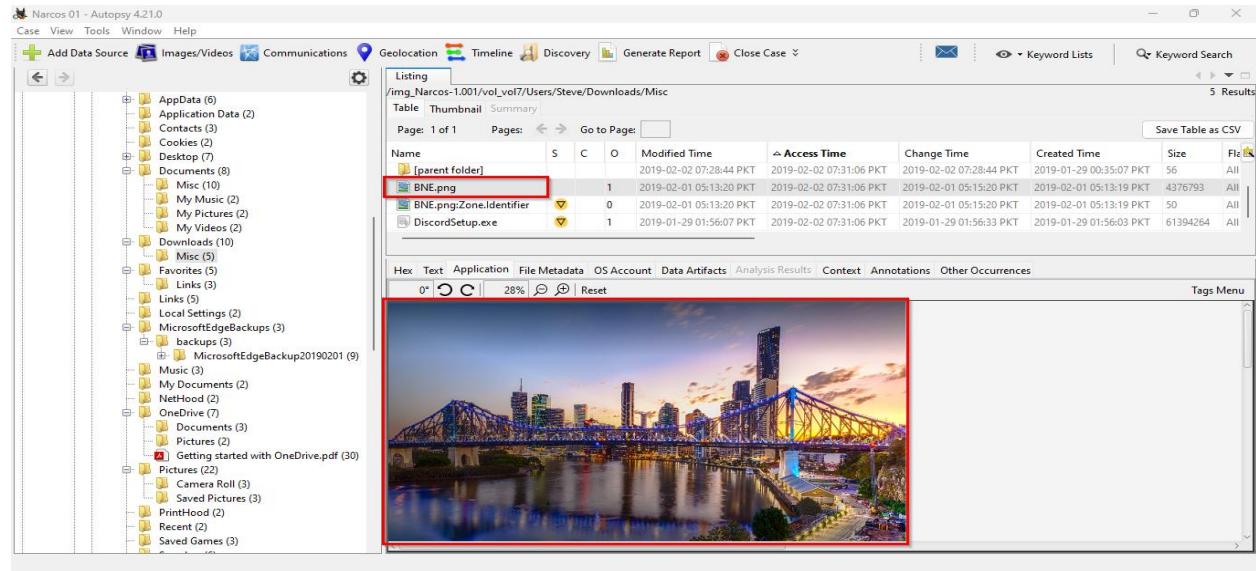
Figure 36 Flightbookings.PNG

The screenshot shows the Flightbookings website. It displays two flight bookings for Steve. The first booking is for a flight from Brisbane to Wellington on 16 Feb. 2019, operated by Virgin Australia. The second booking is for a flight from Wellington to Brisbane on 23 Feb. 2019, operated by Qantas Airways. The website includes a 'Trip Summary' section with a breakdown of fares and fees, and an 'Important Flight Information' section with a list of bullet points. The 'Departure' section includes a note about non-refundable and non-transferable tickets.

Figure 37 Flightbookings.PNG

BNE.png

In this image we can see a bridge. Goggle image search reveals it to be Australia Houses Rivers Bridges Roads Brisbane Night.

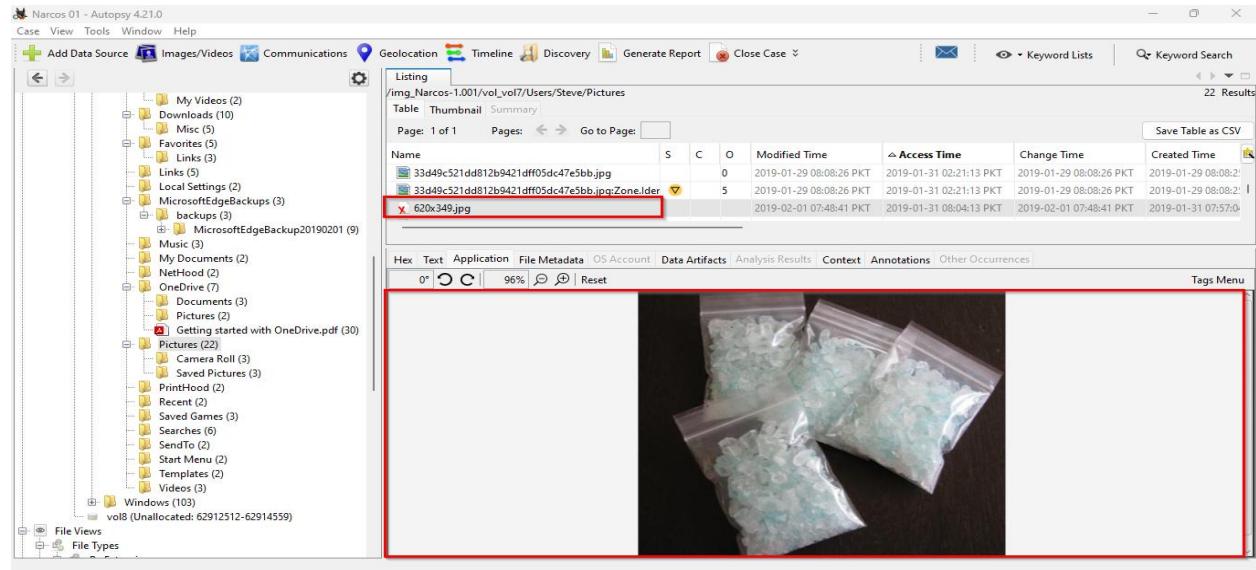


The screenshot shows the Autopsy 4.21.0 interface. The left sidebar shows a file tree with various folders and files. The main area displays a table titled 'Listing' with the path '/img_Narcos-1.001/vol_vol7/Users/Steve/Downloads/Misc'. The table has columns for Name, S, C, O, Modified Time, Access Time, Change Time, Created Time, Size, and File. There are 5 results. The file 'BNE.png' is highlighted with a red box in the table. Below the table is a preview area showing a thumbnail of a bridge at night, which is also highlighted with a red box. The preview area includes tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences.

Figure 38 BNE.png

620x349.jpg(Deleted Pic)

A deleted image of crystal meth was found on Steve's system maybe hinting to his involvement in drugs as seen previously.



The screenshot shows the Autopsy 4.21.0 interface. The left sidebar shows a file tree with various folders and files. The main area displays a table titled 'Listing' with the path '/img_Narcos-1.001/vol_vol7/Users/Steve/Pictures'. The table has columns for Name, S, C, O, Modified Time, Access Time, Change Time, and Created Time. There are 22 results. The file '620x349.jpg' is highlighted with a red box in the table. Below the table is a preview area showing a thumbnail of two ziplock bags filled with white crystalline methamphetamine, which is also highlighted with a red box. The preview area includes tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences.

Figure 39 620x349.jpg(Deleted Pic)

price-meth-bust-4.jpg (Deleted Pic)

This deleted image possibly hints to the meth bust by official possibly his meth and his money lost.

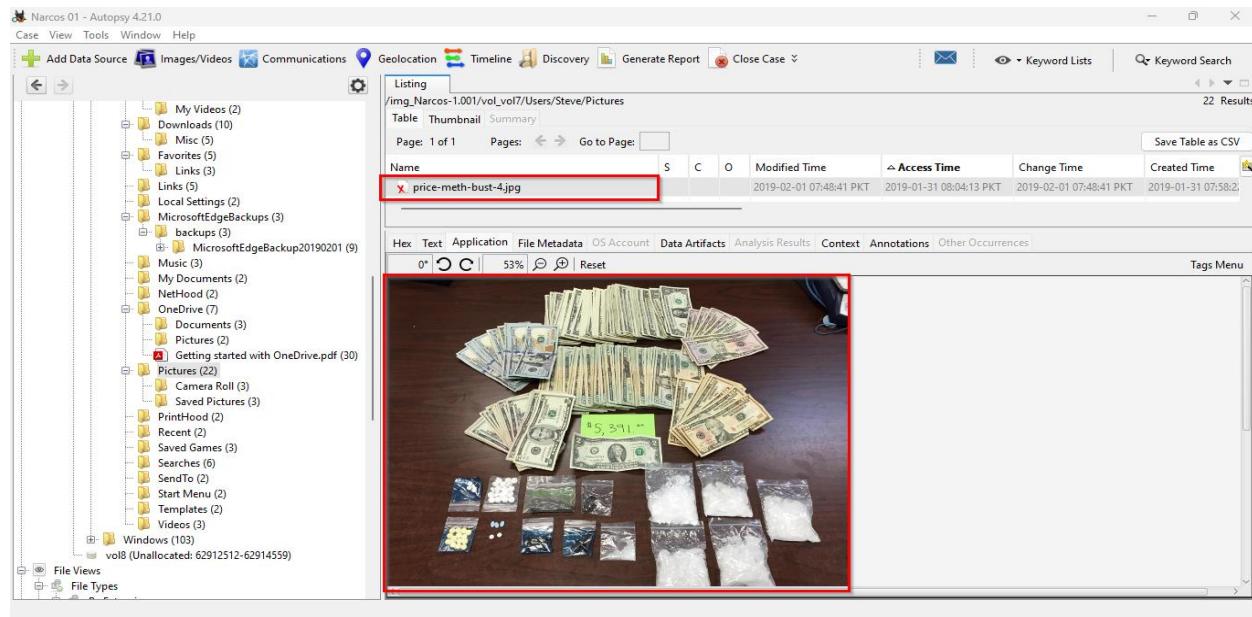


Figure 40 price-meth-bust-4.jpg (Deleted Pic)

eight_col_patches_crp.jpg (Deleted Pic)

This deleted image hints towards possible gang affiliations for Steve to 'Mongrel Mob'

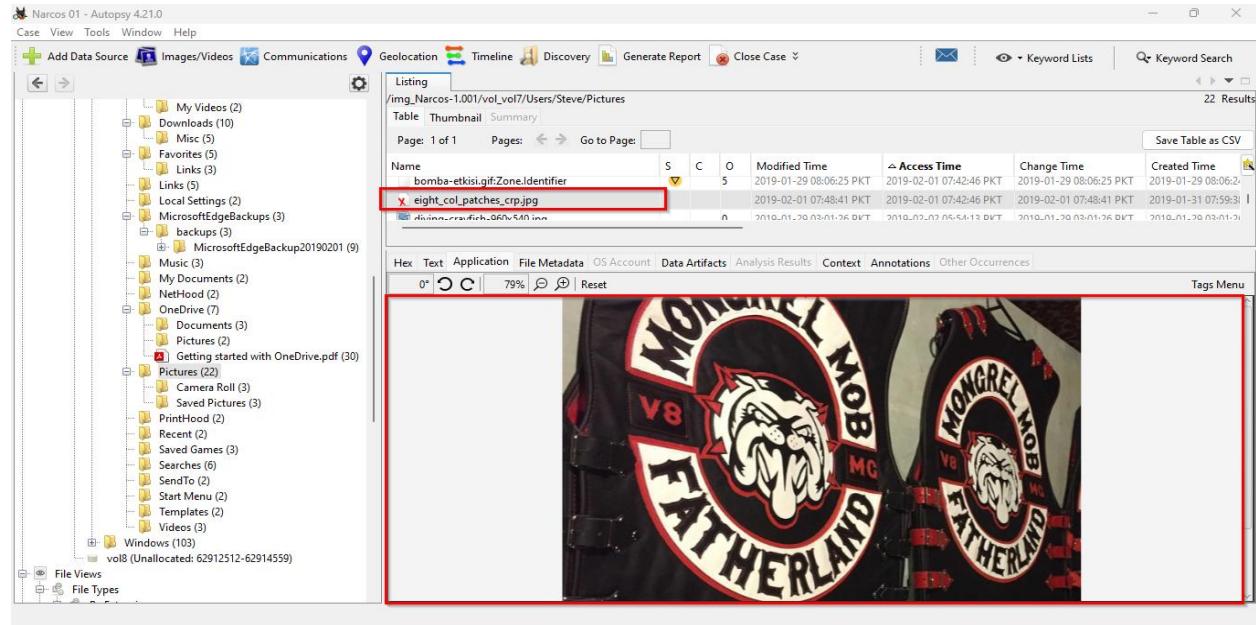


Figure 41 eight_col_patches_crp.jpg (Deleted Pic)

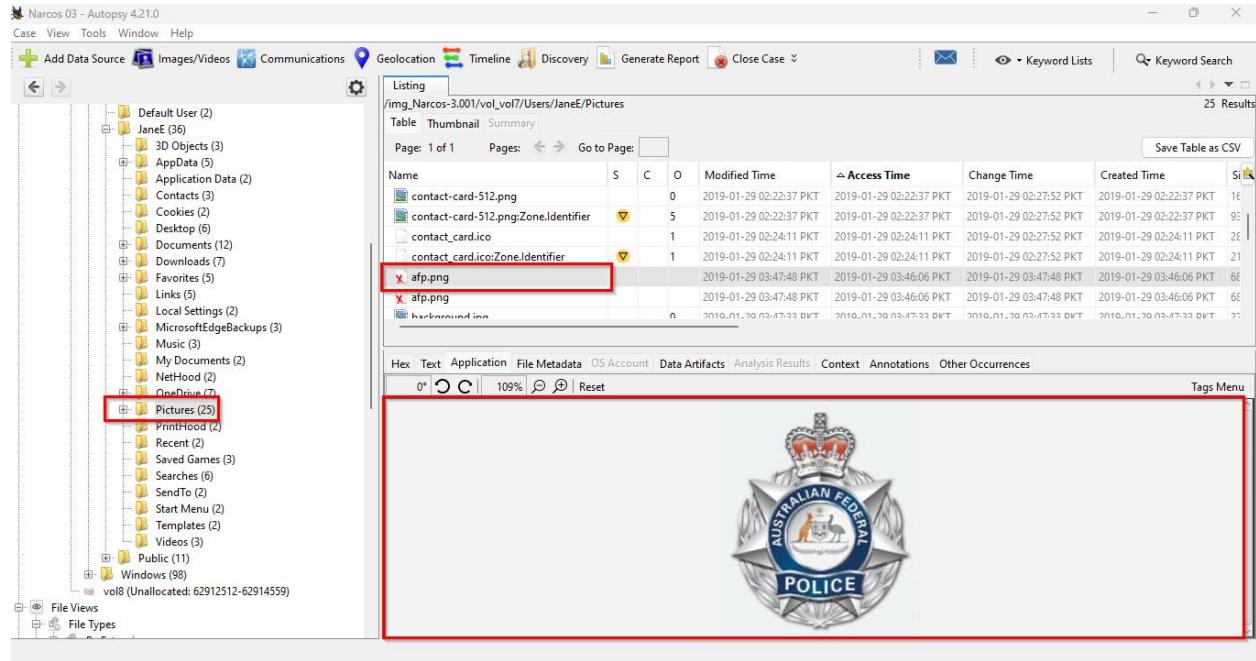
Summary:

From all the images we can see that Steve is a gang affiliated drug dealer with multiple plans of escaping and is also following all the drug busts to maybe identify the prices/ profit margin in this business.

3.3.2 Jane Esteban

Deleted Pic (afp.png)

This image is the logo of Australian Federal Police further cementing Jane as an undercover cop.



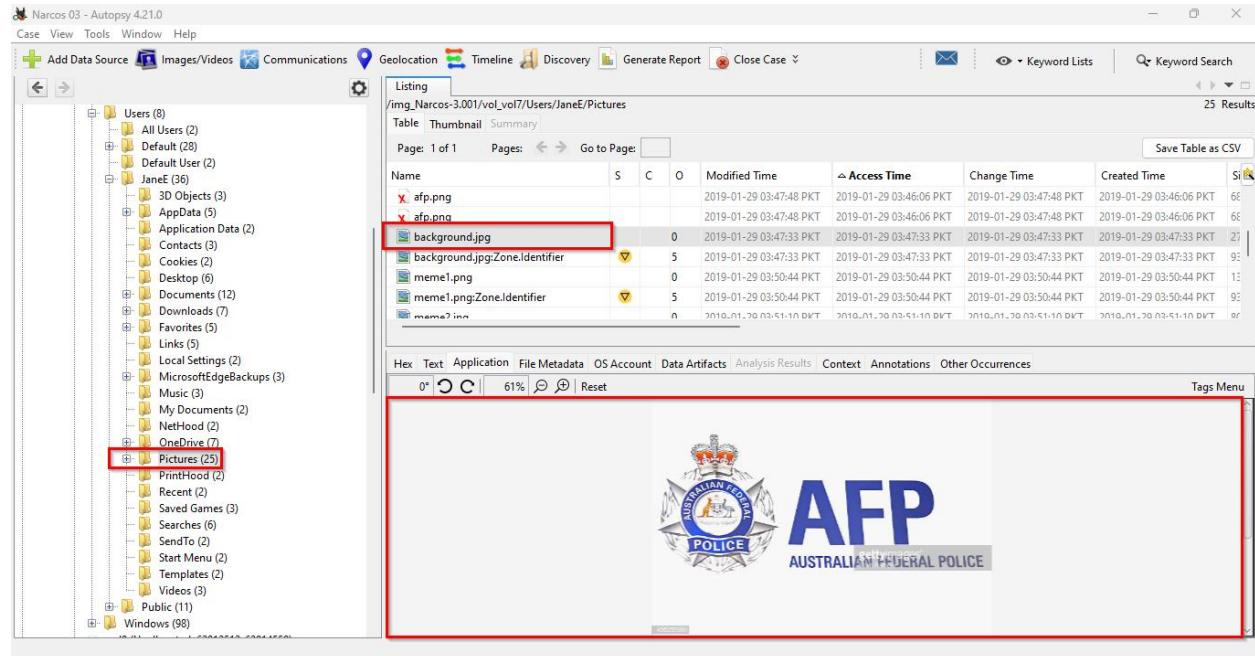
The screenshot shows the Narcos 03 - Autopsy 4.21.0 interface. The left sidebar shows a file tree with various folders like Default User, JaneE, AppData, Application Data, Contacts, Cookies, Desktop, Documents, Downloads, Favorites, Links, Local Settings, MicrosoftEdgeBackups, Music, My Documents, NetHood, OneDrive, Pictures, Public, and Windows. The 'Pictures' folder is highlighted with a red box. The main pane shows a table of files in the '/img_Narcos-3.001/vol1/vol7/Users/JaneE/Pictures' directory. The table has columns: Name, S, C, O, Modified Time, Access Time, Change Time, Created Time, and Size. Several files are listed, including 'contact-card-512.png', 'contact-card-512.png:Zone.Identifier', 'contact_card.ico', 'contact_card.ico:Zone.Identifier', 'afp.png', and 'afp.png'. The 'afp.png' file is highlighted with a red box. Below the table is a preview window showing the Australian Federal Police logo. The preview window has a red border and is also highlighted with a red box. The bottom of the preview window shows the file's metadata: '2010-01-20 02:47:22 DKT', '2010-01-20 02:47:22 DKT', '2010-01-20 02:47:22 DKT', and '2010-01-20 02:47:22 DKT'.

Name	S	C	O	Modified Time	Access Time	Change Time	Created Time	Size
contact-card-512.png	0			2019-01-29 02:22:37 PKT	2019-01-29 02:27:52 PKT	2019-01-29 02:22:37 PKT	2019-01-29 02:22:37 PKT	16
contact-card-512.png:Zone.Identifier	5			2019-01-29 02:22:37 PKT	2019-01-29 02:27:52 PKT	2019-01-29 02:22:37 PKT	2019-01-29 02:22:37 PKT	95
contact_card.ico	1			2019-01-29 02:24:11 PKT	2019-01-29 02:27:52 PKT	2019-01-29 02:24:11 PKT	2019-01-29 02:24:11 PKT	28
contact_card.ico:Zone.Identifier	1			2019-01-29 02:24:11 PKT	2019-01-29 02:27:52 PKT	2019-01-29 02:24:11 PKT	2019-01-29 02:24:11 PKT	21
afp.png				2019-01-29 03:47:48 PKT	2019-01-29 03:46:06 PKT	2019-01-29 03:47:48 PKT	2019-01-29 03:46:06 PKT	68
afp.png				2019-01-29 03:47:48 PKT	2019-01-29 03:46:06 PKT	2019-01-29 03:47:48 PKT	2019-01-29 03:46:06 PKT	68
background.jpg	0			2010-01-20 02:47:22 DKT	2010-01-20 02:47:22 DKT	2010-01-20 02:47:22 DKT	2010-01-20 02:47:22 DKT	27

Figure 42 afp.png

Pic (Background.jpg)

This image is the logo of Australian Federal Police further cementing Jane as an undercover cop.



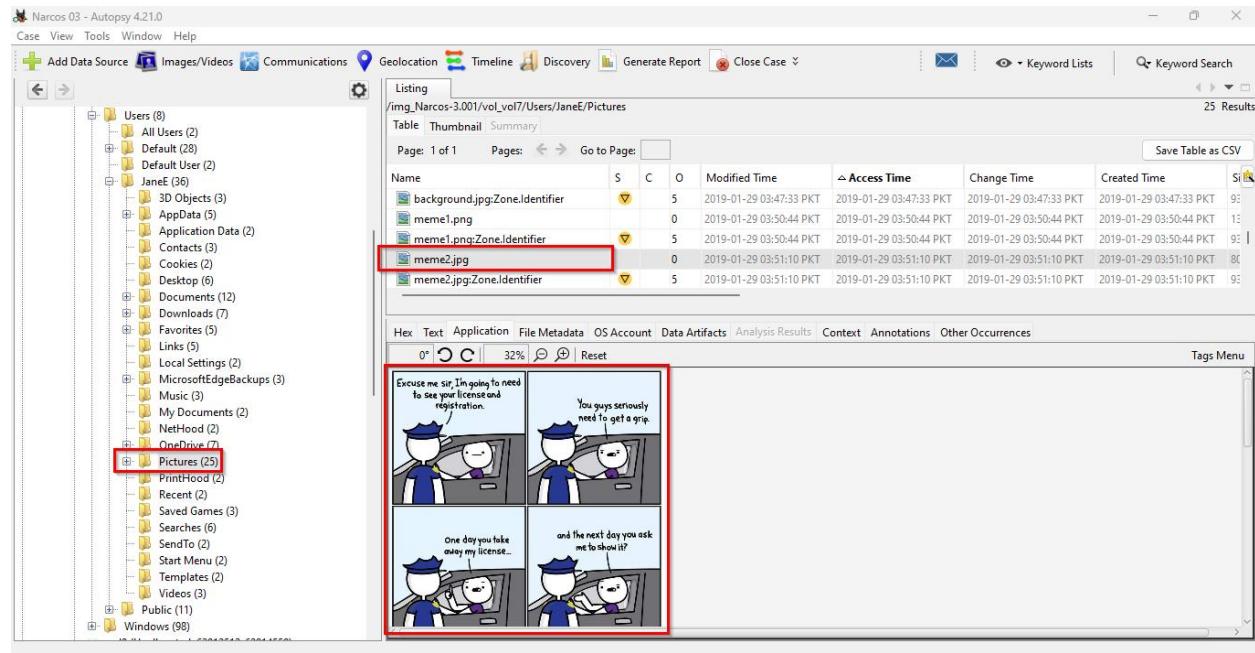
The screenshot shows the Autopsy 4.21.0 interface. The left sidebar shows a file tree with a red box highlighting the 'Pictures (25)' folder. The main area is a table view with a red box highlighting the file 'background.jpg'. The file details are as follows:

Name	S	C	O	Modified Time	Access Time	Change Time	Created Time	Size
background.jpg	0			2019-01-29 03:47:33 PKT	2019-01-29 03:47:33 PKT	2019-01-29 03:47:33 PKT	2019-01-29 03:47:33 PKT	27

The file viewer on the right shows the Australian Federal Police logo with the text 'AUSTRALIAN FEDERAL POLICE' and 'AFP'.

Figure 43 Pic (Background.jpg)

Pic (meme2.jpg):



The screenshot shows the Autopsy 4.21.0 interface. The left sidebar shows a file tree with a red box highlighting the 'Pictures (25)' folder. The main area is a table view with a red box highlighting the file 'meme2.jpg'. The file details are as follows:

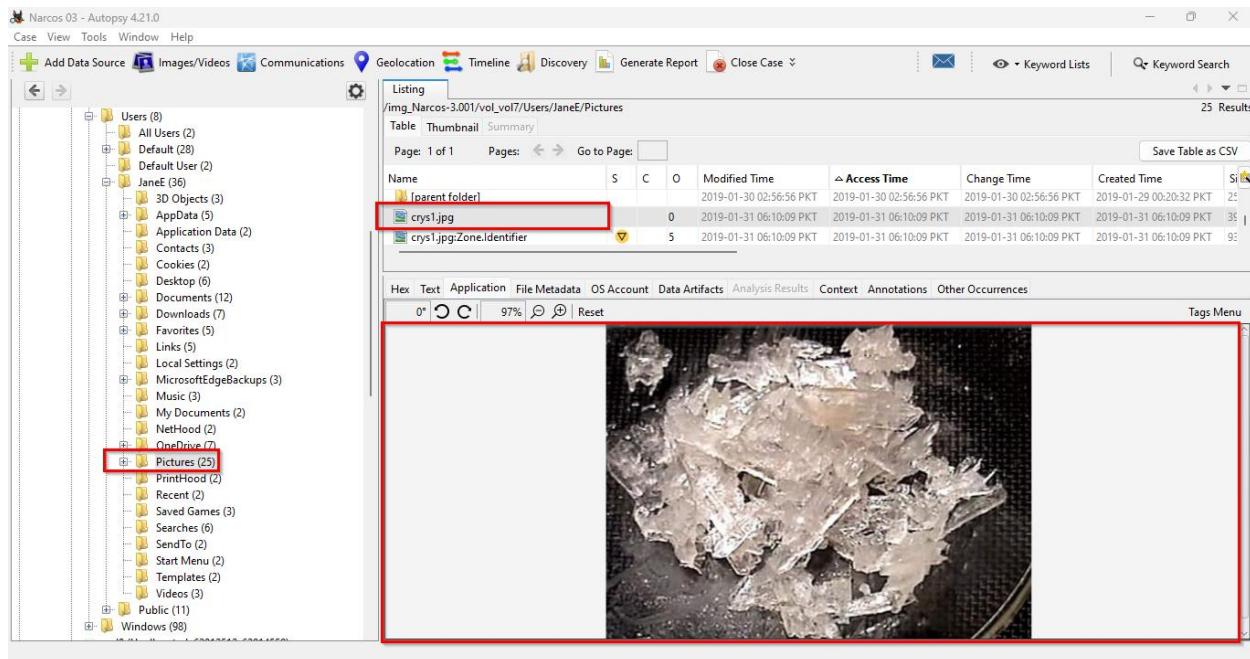
Name	S	C	O	Modified Time	Access Time	Change Time	Created Time	Size
meme2.jpg	0			2019-01-29 03:51:10 PKT	2019-01-29 03:51:10 PKT	2019-01-29 03:51:10 PKT	2019-01-29 03:51:10 PKT	80

The file viewer on the right shows a meme image with two police officers in a car. The top panel of the meme has the following text: 'Excuse me sir, I'm going to need to see your license and registration.' and 'You guys seriously need to get a grip.' The bottom panel has the following text: 'One day you take away my license...' and 'and the next day you ask me to show it?'.

Figure 44 Pic (meme2.jpg):

Pic (crys1.jpg):

A bunch of images of different looking crystals.

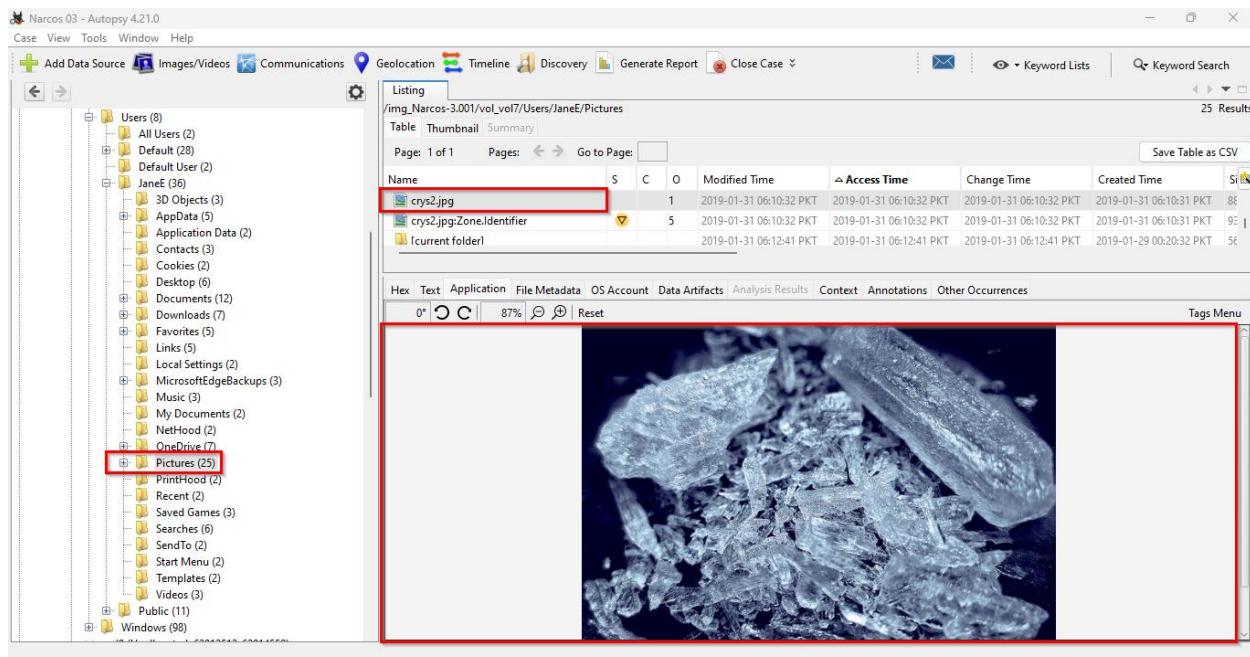


The screenshot shows the Autopsy 4.21.0 interface. The left sidebar shows a tree view of the file system, with the 'Pictures' folder under 'JaneE' highlighted with a red box. The main pane shows a table of files in the '/img_Narcos-3.001/vol_vol7/Users/JaneE/Pictures' directory. The file 'crys1.jpg' is selected and highlighted with a red box. The thumbnail view on the right shows a cluster of light-colored, translucent, crystalline structures.

Name	S	C	O	Modified Time	Access Time	Change Time	Created Time	Size
parent folder				2019-01-30 02:56:56 PKT	2019-01-30 02:56:56 PKT	2019-01-30 02:56:56 PKT	2019-01-29 00:20:32 PKT	25
crys1.jpg	0			2019-01-31 06:10:09 PKT	2019-01-31 06:10:09 PKT	2019-01-31 06:10:09 PKT	2019-01-31 06:10:09 PKT	35
crys1.jpgZone.Identifier	5			2019-01-31 06:10:09 PKT	2019-01-31 06:10:09 PKT	2019-01-31 06:10:09 PKT	2019-01-31 06:10:09 PKT	95

Figure 45 crys1.jpg

Pic (crys2.jpg):



The screenshot shows the Autopsy 4.21.0 interface. The left sidebar shows a tree view of the file system, with the 'Pictures' folder under 'JaneE' highlighted with a red box. The main pane shows a table of files in the '/img_Narcos-3.001/vol_vol7/Users/JaneE/Pictures' directory. The file 'crys2.jpg' is selected and highlighted with a red box. The thumbnail view on the right shows a cluster of large, sharp, light-colored crystalline structures.

Name	S	C	O	Modified Time	Access Time	Change Time	Created Time	Size
crys2.jpg	1			2019-01-31 06:10:32 PKT	2019-01-31 06:10:32 PKT	2019-01-31 06:10:32 PKT	2019-01-31 06:10:31 PKT	86
crys2.jpgZone.Identifier	5			2019-01-31 06:10:32 PKT	2019-01-31 06:10:32 PKT	2019-01-31 06:10:32 PKT	2019-01-31 06:10:31 PKT	95
{current folder}				2019-01-31 06:12:41 PKT	2019-01-31 06:12:41 PKT	2019-01-31 06:12:41 PKT	2019-01-29 00:20:32 PKT	56

Figure 46 crys2.jpg

Pic(crys3.jpg):

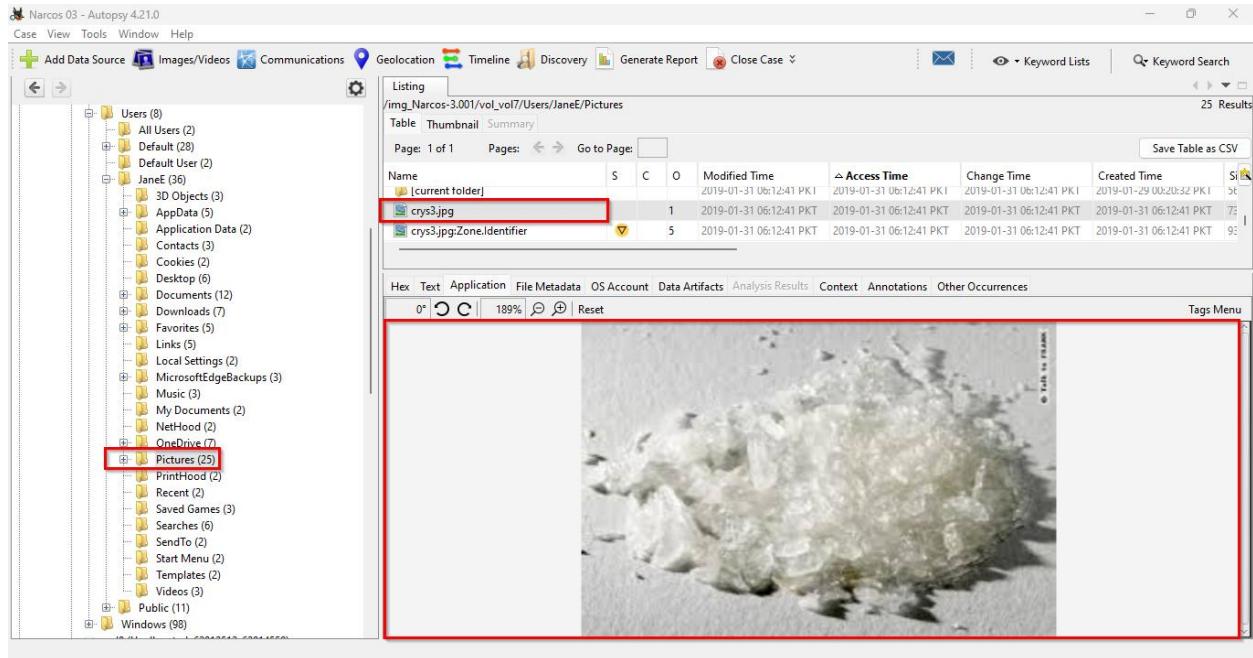


Figure 47 crys3.jpg

Summary:

From the images we can see that Jane has an Australian police badge and is following some meme for possibly dogging sharing her information and is looking into how different drugs look like.

[SPACE INTENTIONALLY LEFT BLANK]

3.3.3 John Fredricksen shipping.PNG

This image shows a DHL courier service image in which we can see that John is sending something on an address in New Zealand. Possibly sending something to Steve.

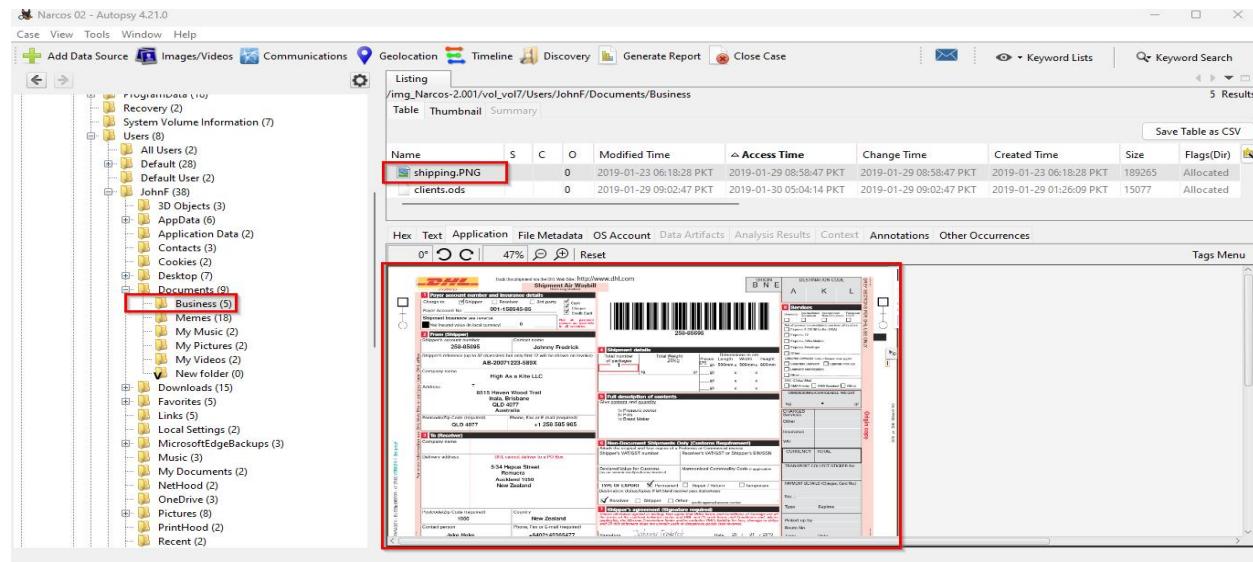


Figure 48 shipping.PNG

Figure 49 shipping.PNG

Steve K.PNG

Below is the flights schedule which was present on Steve's system. This hints toward John and Steve being in communication and possibly planning the drug smuggling together.

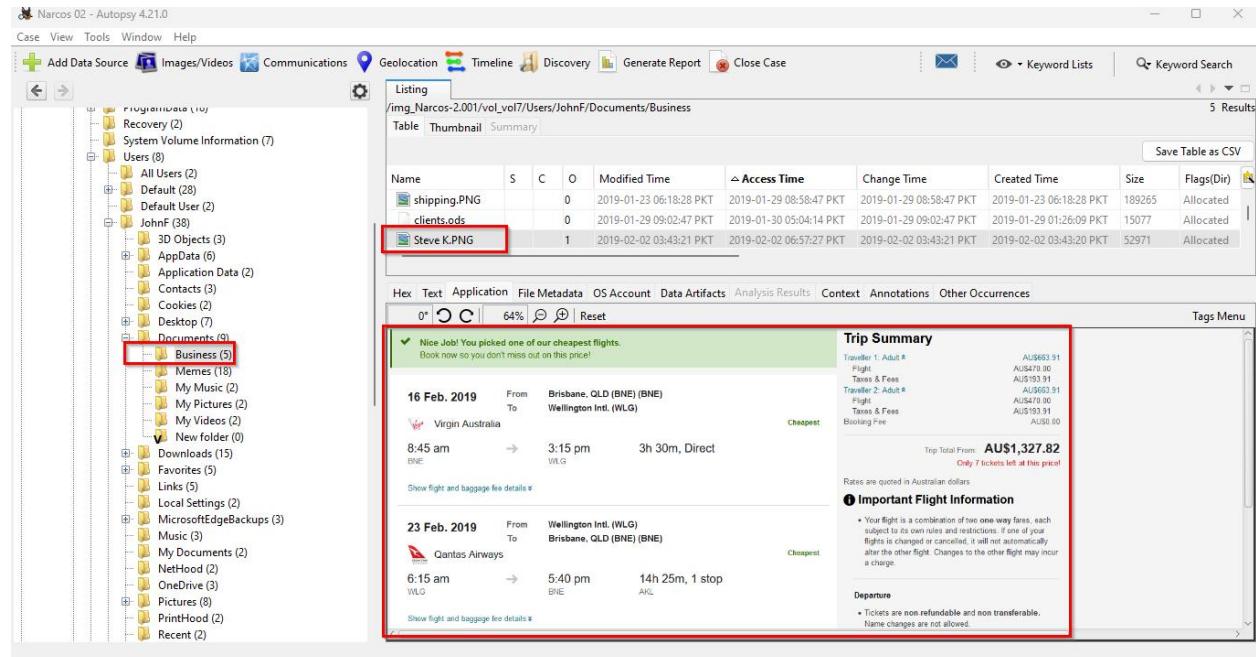


Figure 50 Steve K.PNG

The screenshot shows a flight booking interface. It displays two flight trips: one on 16 Feb. 2019 from Brisbane to Wellington, and another on 23 Feb. 2019 from Wellington to Brisbane. The 16 Feb. 2019 trip is labeled as the 'Cheapest' and is booked with Virgin Australia. The 23 Feb. 2019 trip is also labeled as the 'Cheapest' and is booked with Qantas Airways. The interface includes a 'Trip Summary' table at the bottom right showing flight details and costs for both travellers. The summary table includes columns for Traveller, Flight, Taxes & Fees, and Booking Fee. The total trip cost is listed as AU\$1,327.82.

Figure 51 Steve K.PNG

durg meme 7.jpg

Below are some of the drug memes which John has been following.

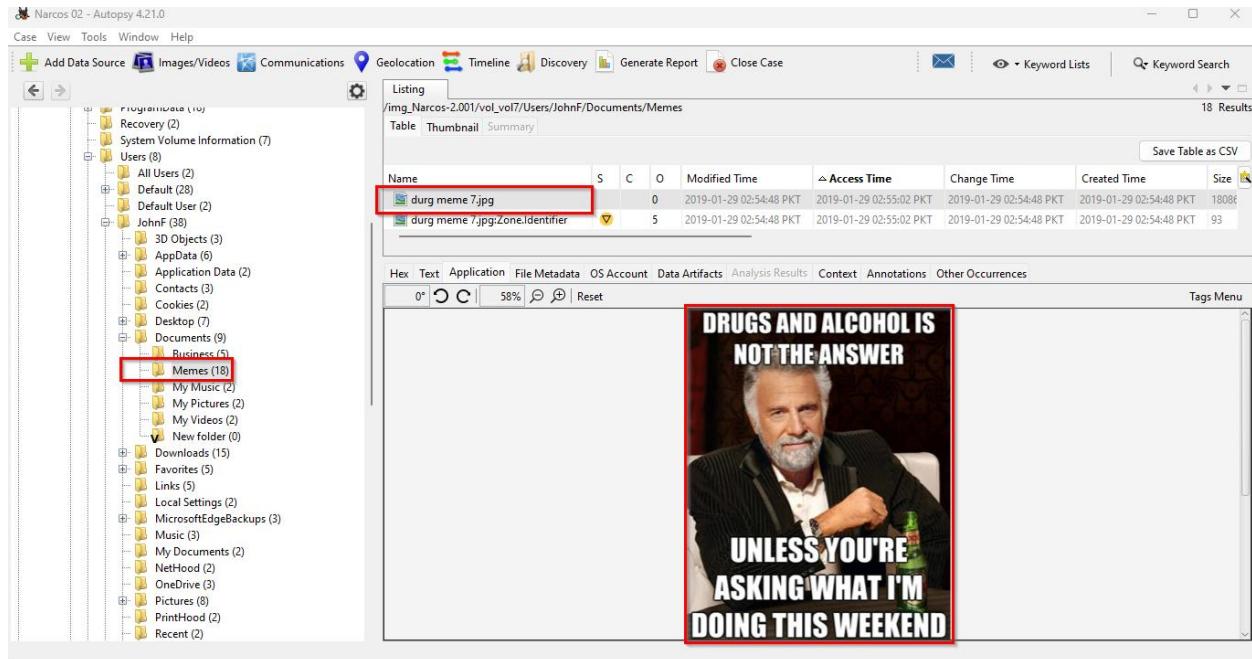


Figure 52 durg meme 7.jpg

drug wallpaper.jpg

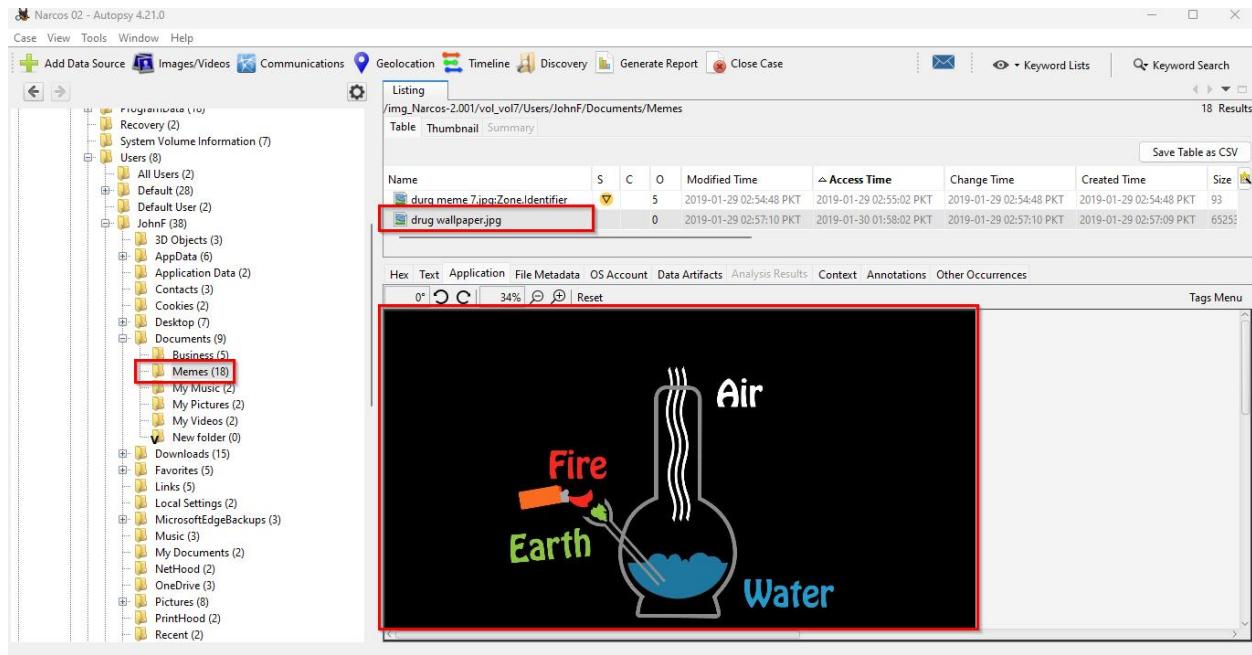


Figure 53 drug wallpaper.jpg

drugmeme3.jif

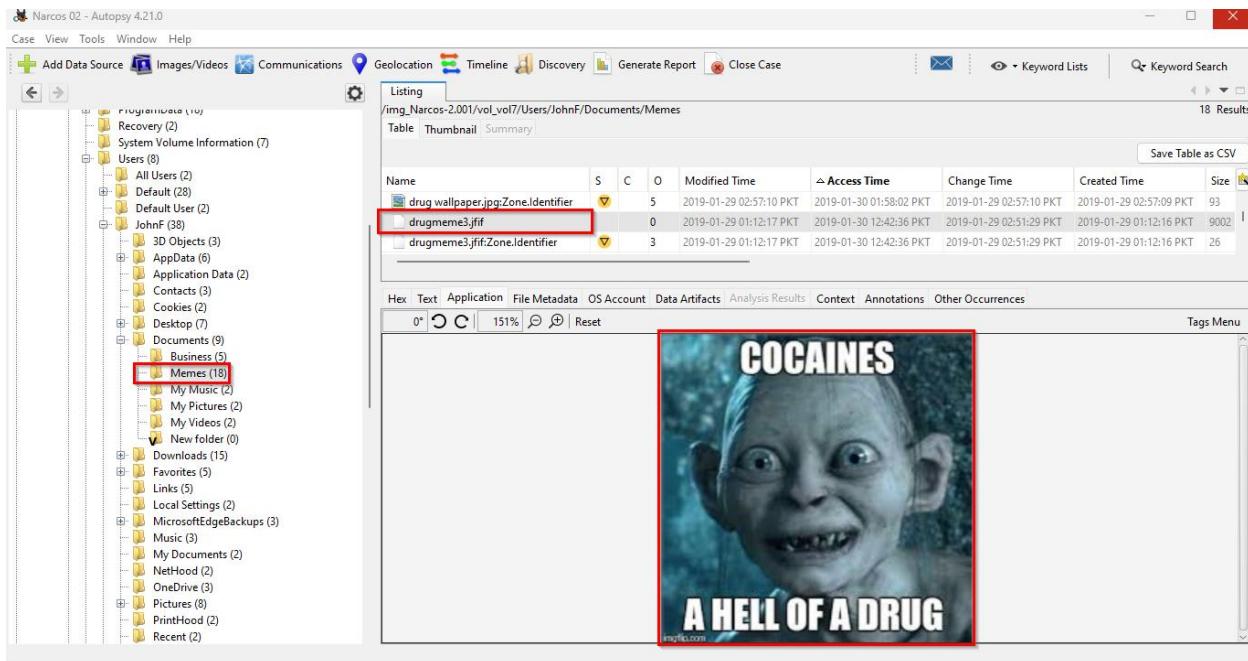


Figure 54 drugmeme3.jif

drugmeme4.jif

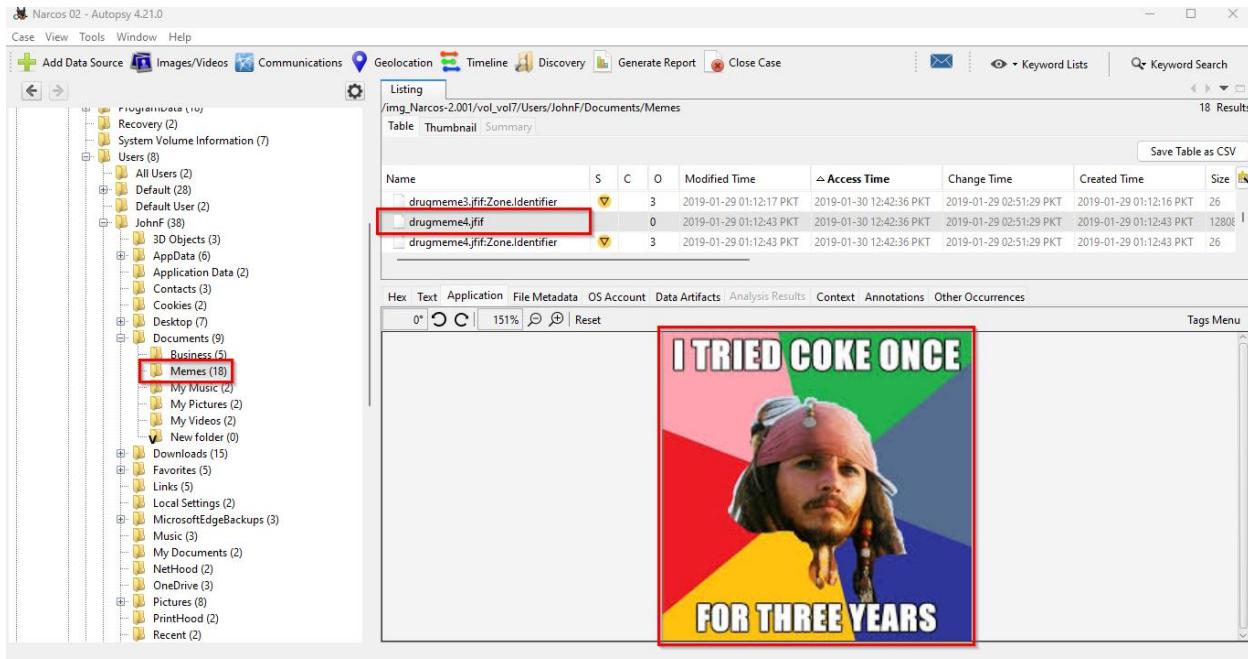


Figure 55 drugmeme4.jif

drugmeme5.jif

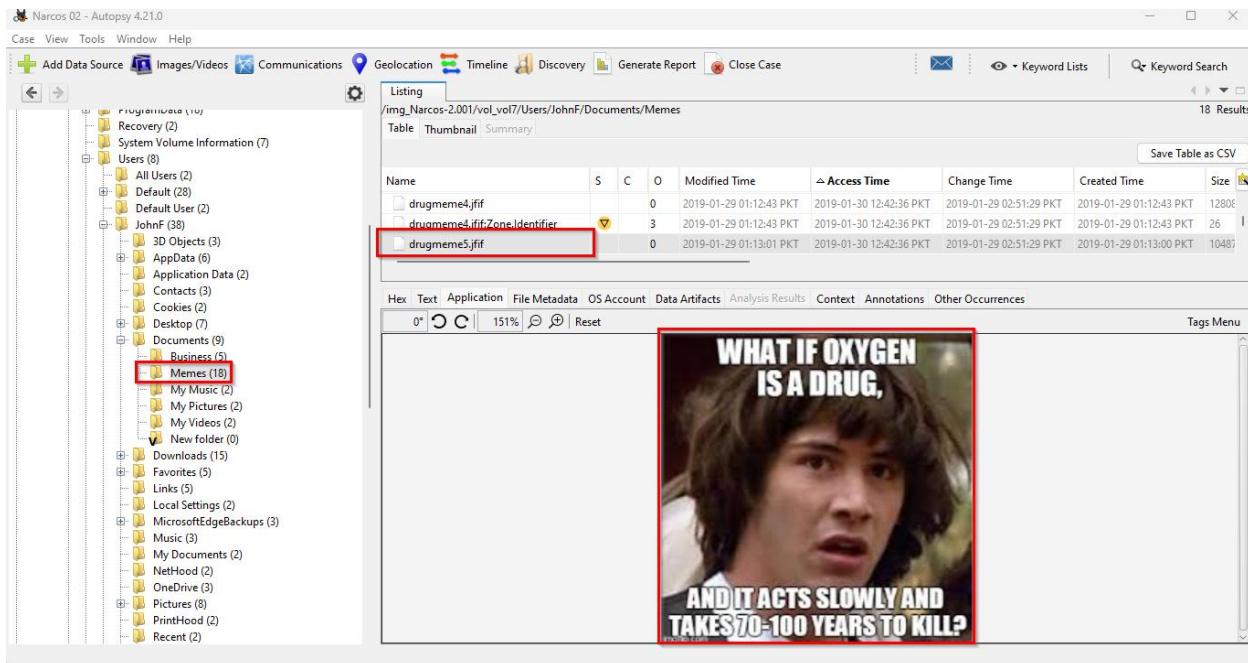


Figure 56 drugmeme5.jif

drugmeme6.jif

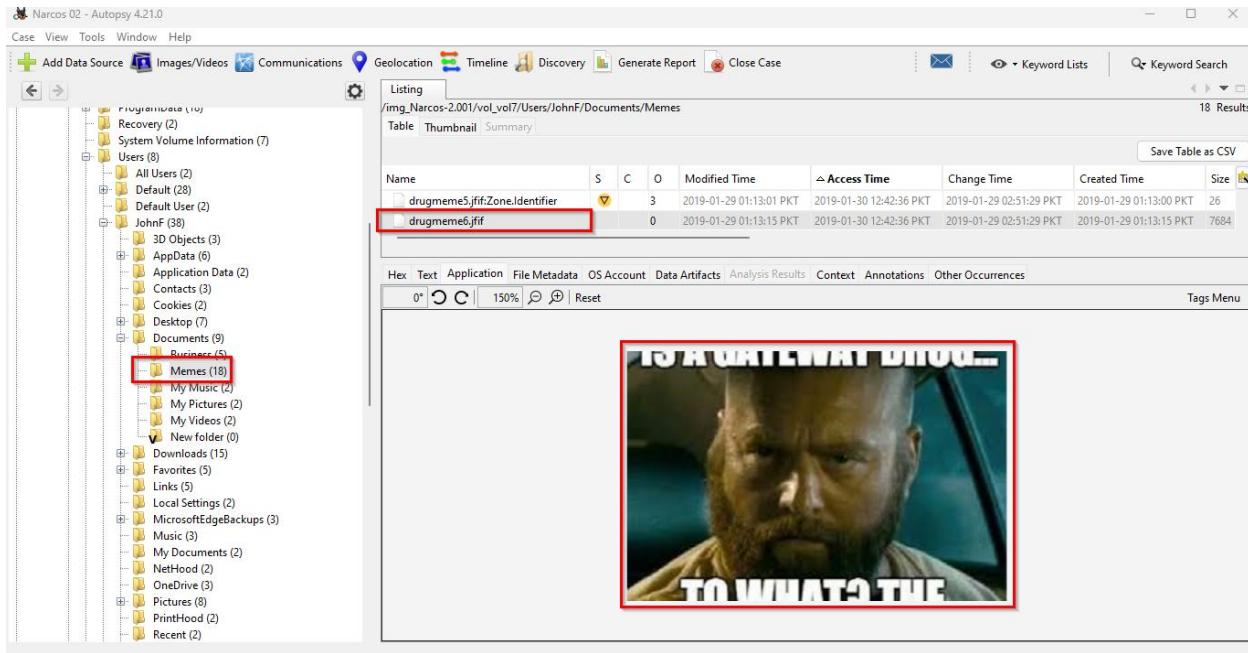


Figure 57 drugmeme6.jif

drugmeme2.jif

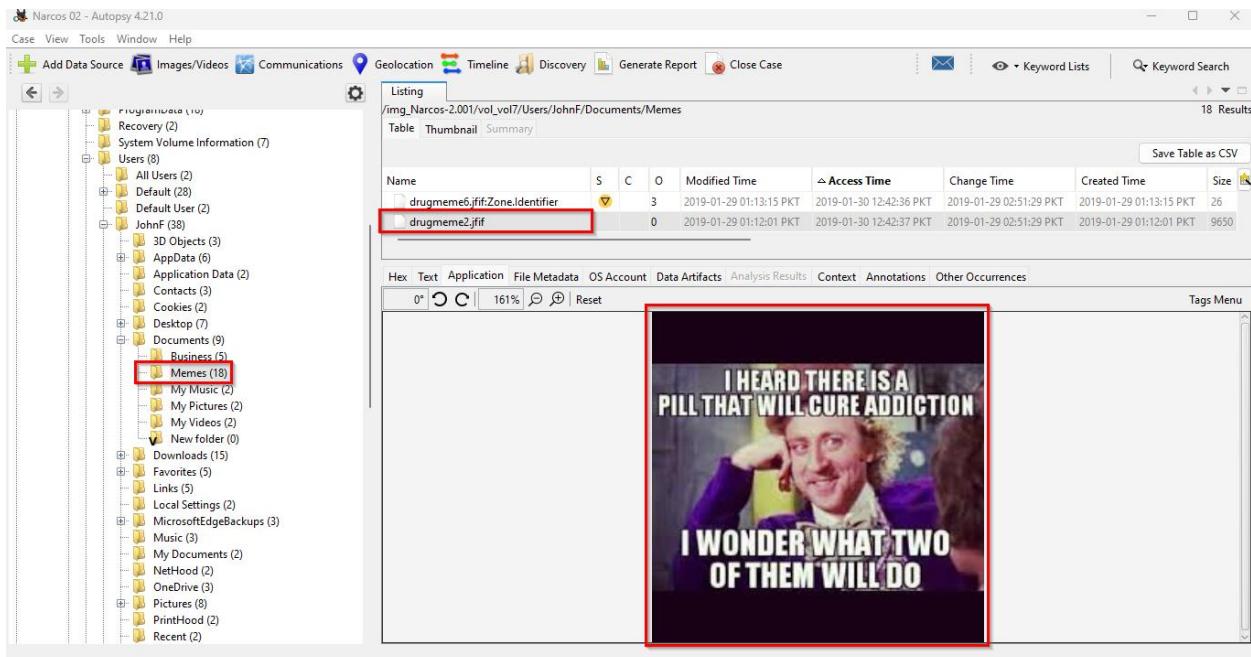


Figure 58 drugmeme2.jif

drugmeme 1.jif

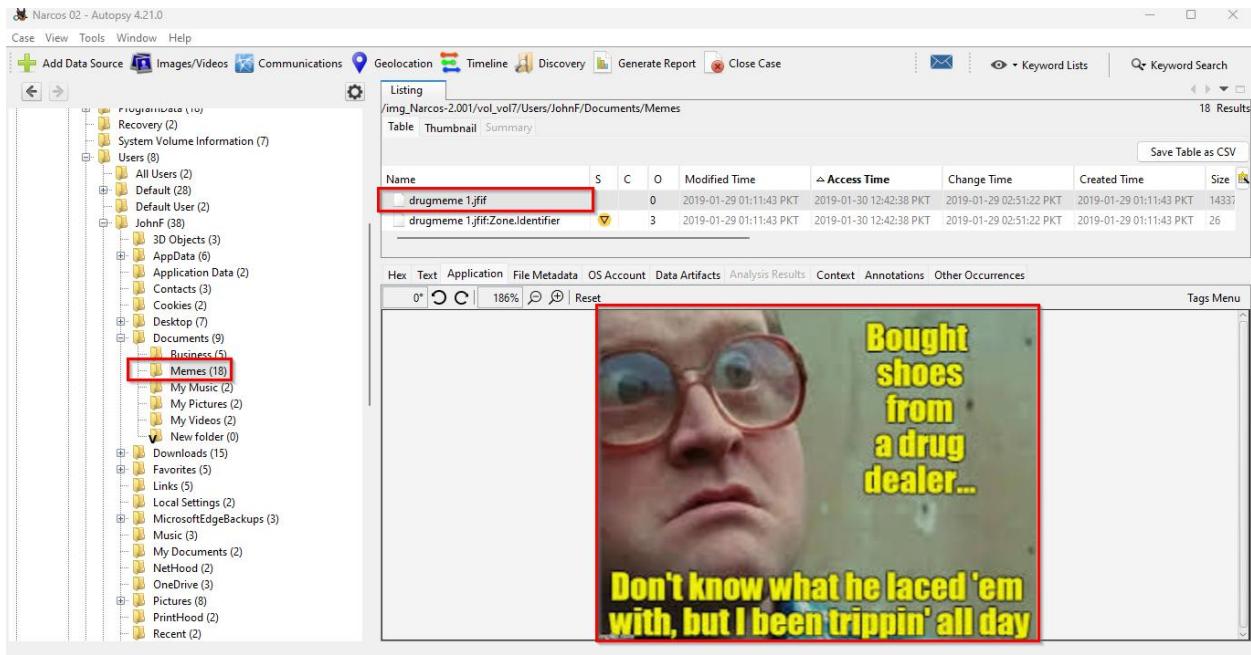


Figure 59 drugmeme 1.jif

1540752698-brisbane.jpg

Below is the same bridge image which was found on the Steve systems. This again cements this idea that Steve and John are in communication with each other

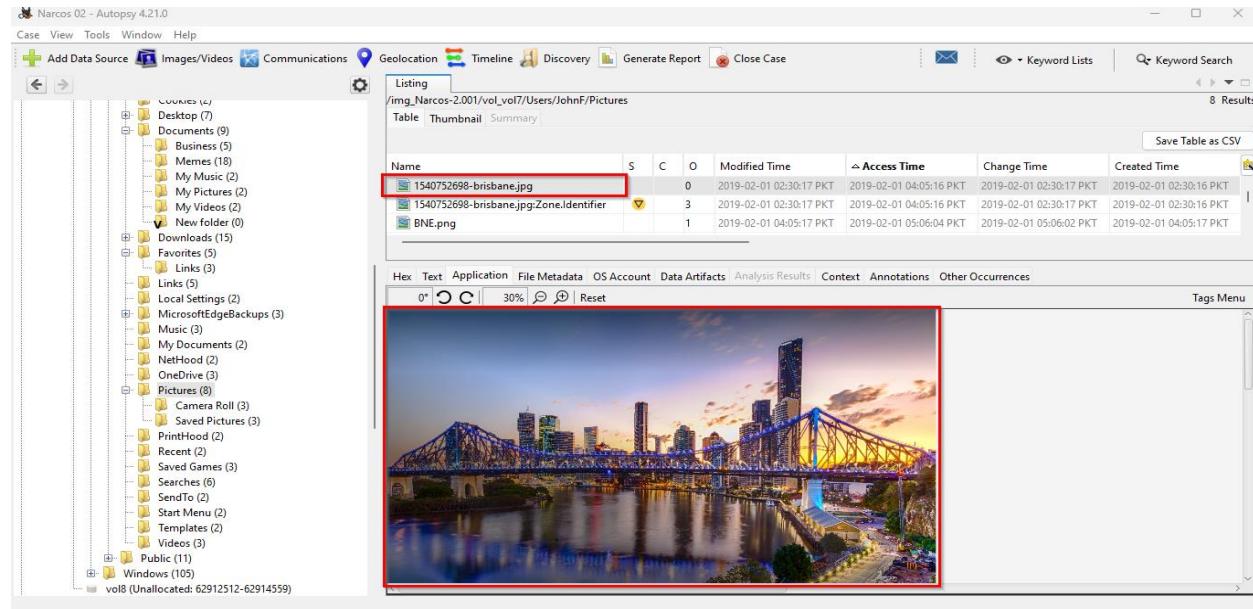


Figure 60 1540752698-brisbane.jpg

BNE.png

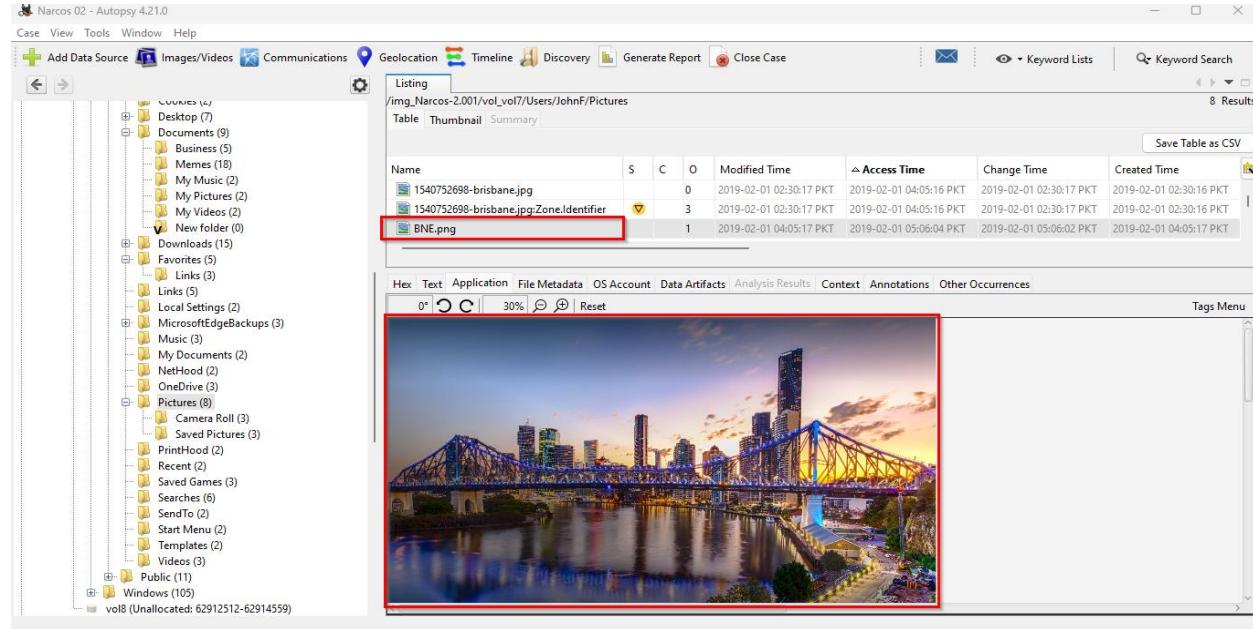


Figure 61 BNE.png

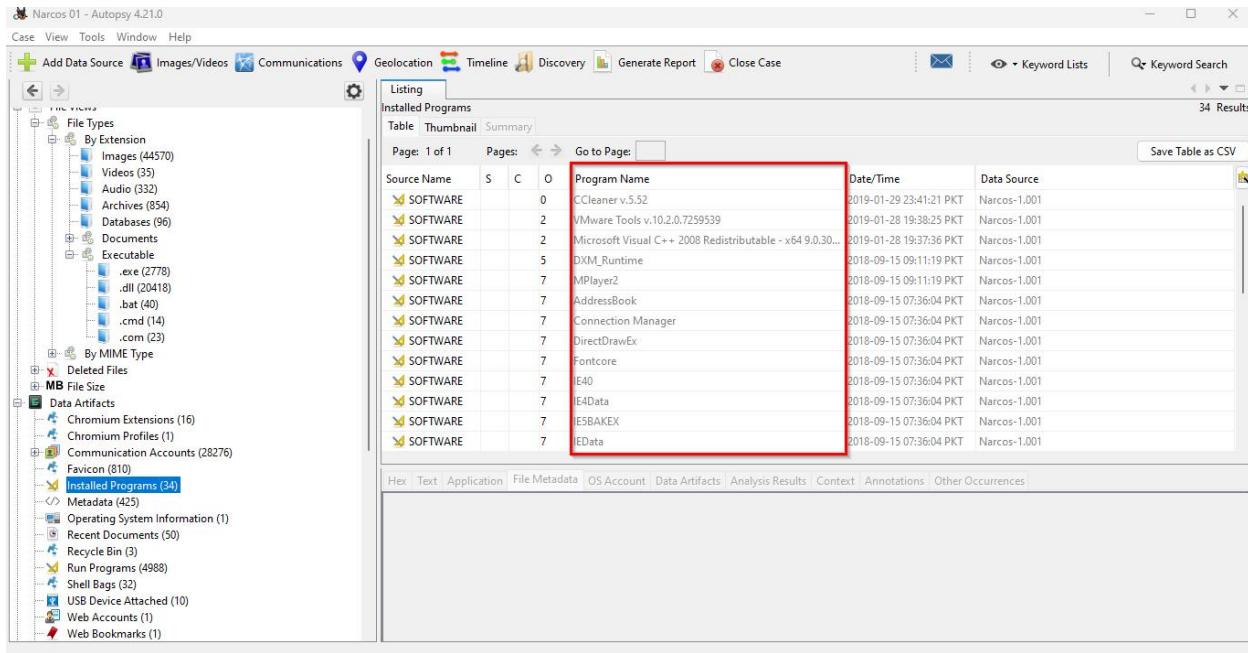
3.4 Binary Files

Executable files tend to be binary files. Some of the suspect's binary file which were discovered are given below.

3.4.1 Steve Kowhai:

Possible Binary Files present on Johns System.

1. CCleaner v.5.52
2. VMware Tools v.10.2.0.7259539
3. TrueCrypt v.7.1a
4. Discord
5. Image Steganography



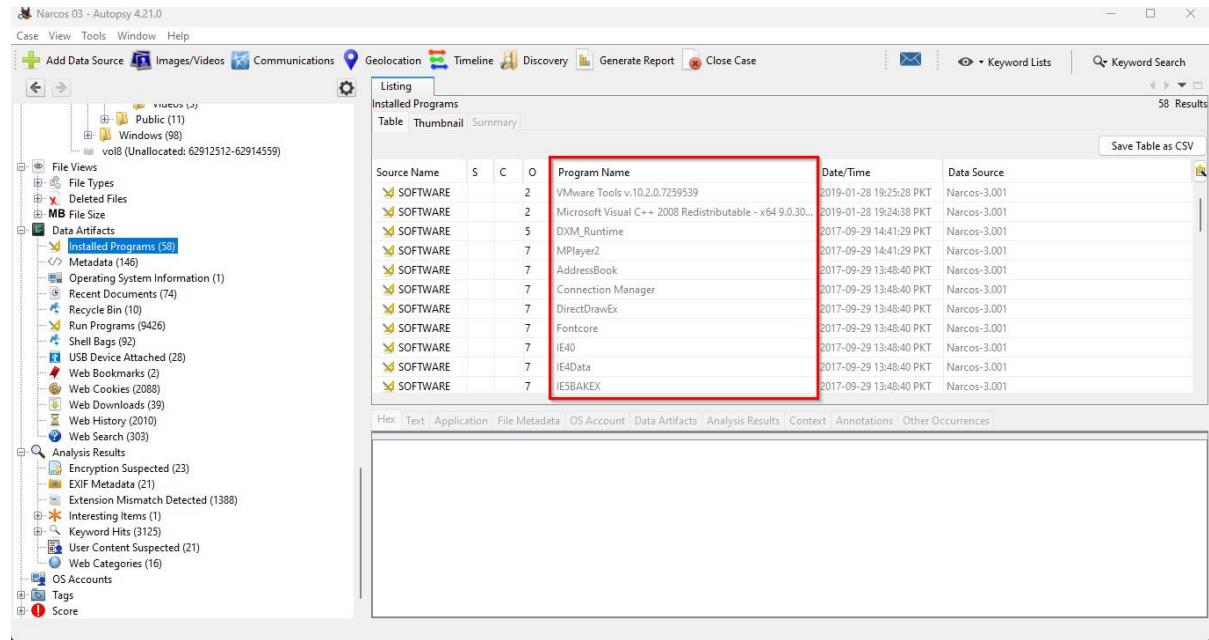
Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE	0			CCleaner v.5.52	2019-01-29 23:41:21 PKT	Narcos-1.001
SOFTWARE	2			VMware Tools v.10.2.0.7259539	2019-01-28 19:38:25 PKT	Narcos-1.001
SOFTWARE	2			Microsoft Visual C++ 2008 Redistributable - x64 9.0.30...	2019-01-28 19:37:36 PKT	Narcos-1.001
SOFTWARE	5			DXM_Runtime	2018-09-15 09:11:19 PKT	Narcos-1.001
SOFTWARE	7			MPlayer2	2018-09-15 09:11:19 PKT	Narcos-1.001
SOFTWARE	7			AddressBook	2018-09-15 07:36:04 PKT	Narcos-1.001
SOFTWARE	7			Connection Manager	2018-09-15 07:36:04 PKT	Narcos-1.001
SOFTWARE	7			DirectDrawEx	2018-09-15 07:36:04 PKT	Narcos-1.001
SOFTWARE	7			Fontcore	2018-09-15 07:36:04 PKT	Narcos-1.001
SOFTWARE	7			E40	2018-09-15 07:36:04 PKT	Narcos-1.001
SOFTWARE	7			E4Data	2018-09-15 07:36:04 PKT	Narcos-1.001
SOFTWARE	7			E5BAKEX	2018-09-15 07:36:04 PKT	Narcos-1.001
SOFTWARE	7			EData	2018-09-15 07:36:04 PKT	Narcos-1.001

Figure 62 Steve Kowhai Binary Files

3.4.2 Jane Esteban:

Possible Binary Files present on Johns System

1. VMware Tools v.10.2.0.7259539.
2. Discord



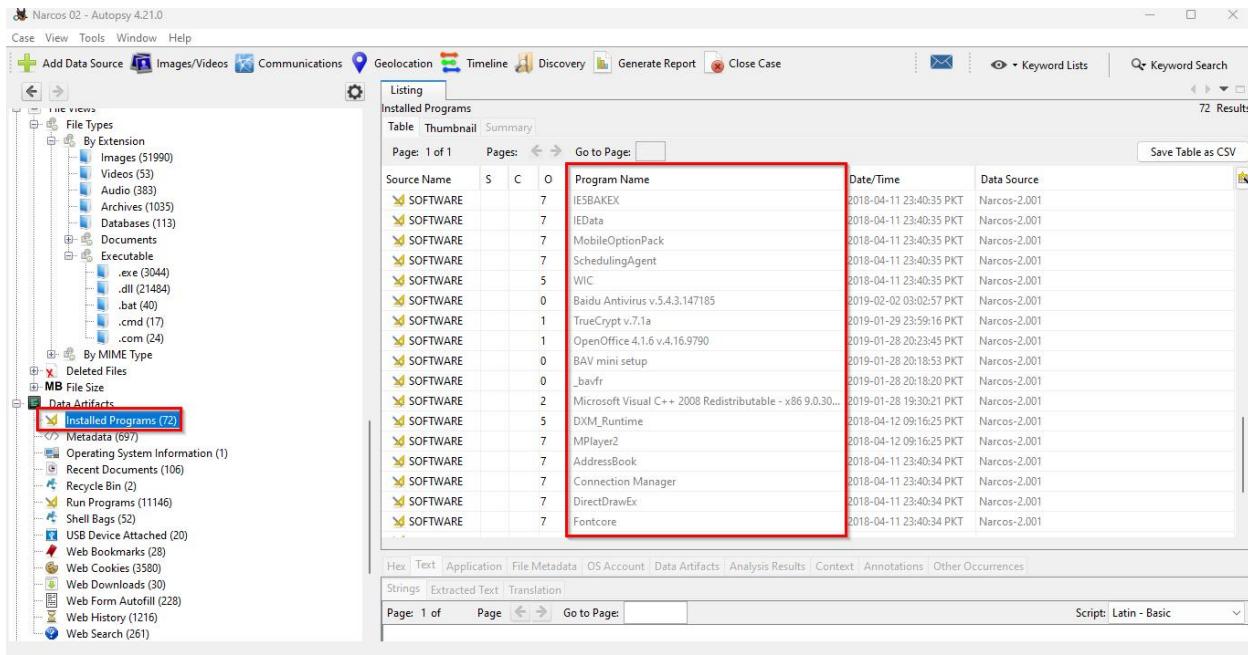
Source Name	Program Name	Date/Time	Data Source
2	VMware Tools v.10.2.0.7259539	2019-01-28 19:25:28 PKT	Narcos-3.001
2	Microsoft Visual C++ 2008 Redistributable - x64 9.0.30...	2019-01-28 19:24:38 PKT	Narcos-3.001
5	DXM_Runtime	2017-09-29 14:41:29 PKT	Narcos-3.001
7	MPlayer2	2017-09-29 14:41:29 PKT	Narcos-3.001
7	AddressBook	2017-09-29 13:48:40 PKT	Narcos-3.001
7	Connection Manager	2017-09-29 13:48:40 PKT	Narcos-3.001
7	DirectDrawEx	2017-09-29 13:48:40 PKT	Narcos-3.001
7	Fontcore	2017-09-29 13:48:40 PKT	Narcos-3.001
7	IE40	2017-09-29 13:48:40 PKT	Narcos-3.001
7	IE4Data	2017-09-29 13:48:40 PKT	Narcos-3.001
7	IESBAKEX	2017-09-29 13:48:40 PKT	Narcos-3.001

Figure 63 Jane Esteban Binary Files

3.4.3 John Fredricksen:

Possible Binary Files present on Johns System

3. VMware Tools v.10.2.0.7259539
4. TrueCrypt v.7.1a
5. Baidu Antivirus v.5.4.3.147185
6. OpenOffice 4.1.6 v.4.16.9790
7. BAV mini setup / _bavfr



Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE	7			I5BAKEX	2018-04-11 23:40:35 PKT	Narcos-2.001
SOFTWARE	7			IEData	2018-04-11 23:40:35 PKT	Narcos-2.001
SOFTWARE	7			MobileOptionPack	2018-04-11 23:40:35 PKT	Narcos-2.001
SOFTWARE	7			SchedulingAgent	2018-04-11 23:40:35 PKT	Narcos-2.001
SOFTWARE	5			WIC	2018-04-11 23:40:35 PKT	Narcos-2.001
SOFTWARE	0			Baidu Antivirus v.5.4.3.147185	2019-02-02 03:02:57 PKT	Narcos-2.001
SOFTWARE	1			TrueCrypt v.7.1a	2019-01-29 23:59:16 PKT	Narcos-2.001
SOFTWARE	1			OpenOffice 4.1.6 v.4.16.9790	2019-01-28 20:23:45 PKT	Narcos-2.001
SOFTWARE	0			BAV mini setup	2019-01-28 20:18:55 PKT	Narcos-2.001
SOFTWARE	0			_bavfr	2019-01-28 20:18:20 PKT	Narcos-2.001
SOFTWARE	2			Microsoft Visual C++ 2008 Redistributable - x86 9.0.30...	2019-01-28 19:30:21 PKT	Narcos-2.001
SOFTWARE	5			DXIM_Runtime	2018-04-12 09:16:25 PKT	Narcos-2.001
SOFTWARE	7			MPlayer2	2018-04-12 09:16:25 PKT	Narcos-2.001
SOFTWARE	7			AddressBook	2018-04-11 23:40:34 PKT	Narcos-2.001
SOFTWARE	7			Connection Manager	2018-04-11 23:40:34 PKT	Narcos-2.001
SOFTWARE	7			DirectDrawEx	2018-04-11 23:40:34 PKT	Narcos-2.001
SOFTWARE	7			Fontcore	2018-04-11 23:40:34 PKT	Narcos-2.001

Figure 64 John Fredricksen Binary Files

3.5 Content and Communication between Suspects

Some chats were discovered from the systems. These chats were discovered in discord a platform where people can have voice chat and message each other with the ability to share your system screen as well. Some chats were encrypted but we were able to decrypt them.

Below are some chats which were discovered.

3.5.1 John Fredricksen and Steve Kowhai:

John: New supplier eh? Definitely Interested! Can I get 10 keys of it delivered to Wellington

Steve: Yeah yeah probably wiser, good one. In fact I have already put a document together in anticipation of chatting with you. I'll send it through now. It contains some information regarding how I see this working out. Let me know what you think once you have read it. S O

John: Good Thinking, I already know how. Heard of steganography?

Steve: A way of hiding one image within another. There's a simple application called 'Image Steganography'.

John: Ya.. I just told you about the tool :face_palm: Received it. Will check to see if it works and confirm soon.

Steve: Good. Meet at the Eastbourne library and if we miss each other come to 666 Rewera Avenue, Petone.

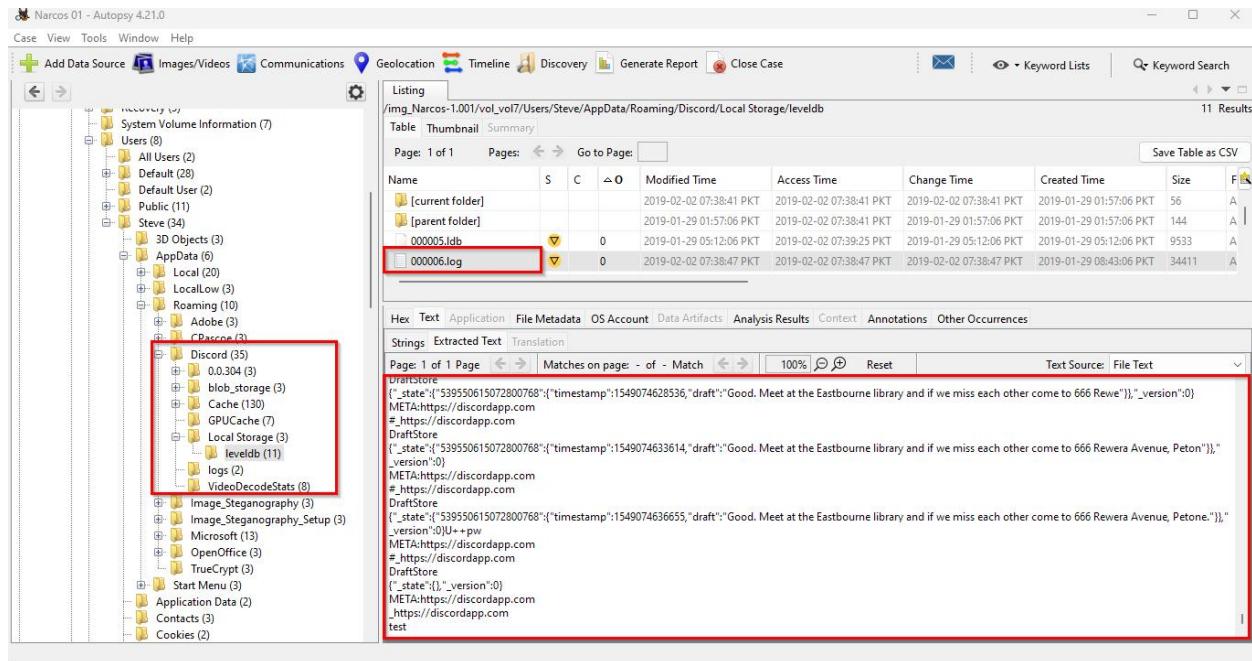


Figure 65 John Fredricksen and Steve Kowhai Discord Chat

3.5.2 John Fredricksen and Jane Esteban:

John: Planning a shipment within the next month. Shut up and wait. How much do you want?

John: Good, now that's what I wanted to hear. Here is the plan. You and I will be acting like a couple travelling on a holiday to New Zealand. This is what I want you to do: Look the part, act normal, and don't tell anyone about what we're doing. Understood?

John: Good. Talk tomorrow at 3PM or else

John: ah bugger wrong person, disregard

Jane: I want to send an image of something to you but it needs to be done safely. Any ideas?

John: No what's that?

Jane: Okay, I'll have a look and see if I can get it to work and then send the image through

Jane: It worked, sending it and the password via email now. I used a tool called image steganography..

John: Right. What's your full name and date of birth? I need it for booking the flights ASAP.

John: Flights booked. I'll pick you up from the Woolworths (133 Oxley Station Rd, Oxley QLD 407, Australia) at ... Just bring yourself I'll cover everything else

John: See you soon. John out

3.5.3 Jane Esteban Mail:

Proton Mail: becomingjane@protonmail.com

Below are all the mail that Jane had sent. Looking at all the evidence gathered till now it seems they were sent to John.

1. Got any of that ice??
2. Also I've got some friends that want to score too. Here's their contact card
3. The usual
4. What is it...
5. Umm I don't know, sounds pretty risky
6. Err nah I'm not keen
7. WHAT! Please, I swear whatever you need I'll do it... I've put them through enough as it is. What do you want from me??
8. Yes John got it
9. My full name is Jane Esteban and my birthday is 13/07/1992
10. I'll be there

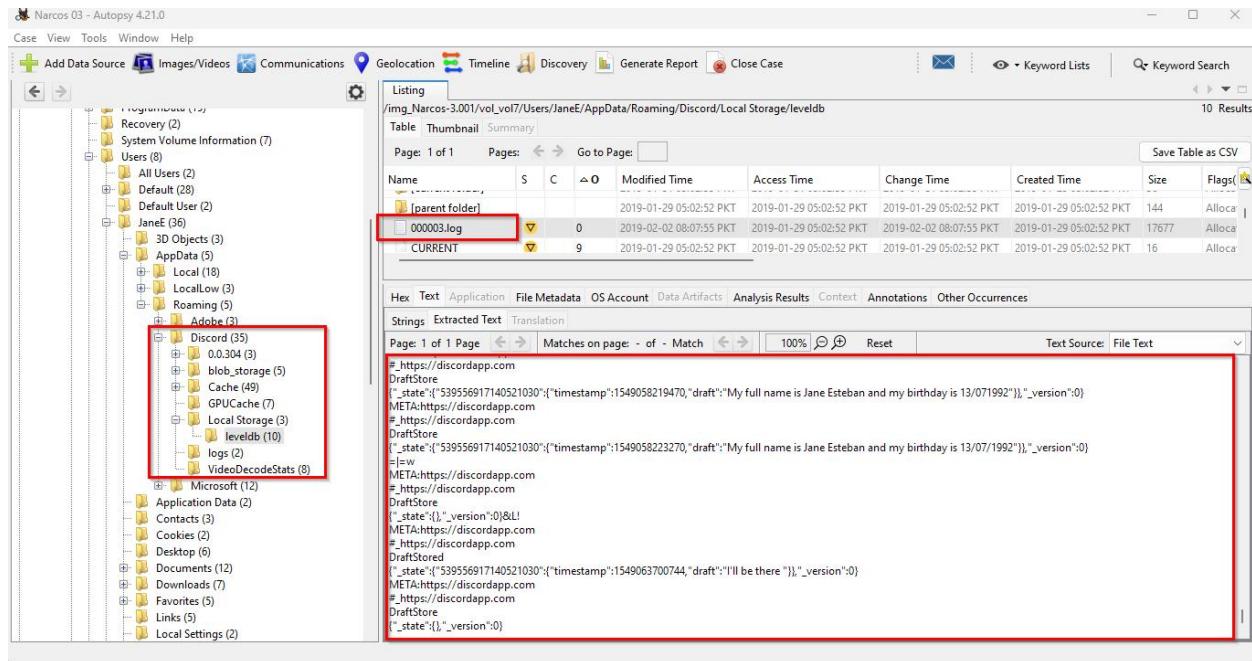


Figure 66 John Fredricksen and Jane Esteban Discord Chat

[SPACE INTENTIONALLY LEFT BLANK]

3.6 Documents

3.6.1 Steve Kowhai:

These documents were discovered on Steve Kowhai's system.

TrueCrypt User Guide.pdf

Below is the user guide for a software named TrueCrypt. TrueCrypt can create a virtual encrypted disk within a file, encrypt a partition, or encrypt the whole storage device. Hinting towards Steve probably encrypting bunch of suspicious files.



Figure 67 TrueCrypt User Guide.pdf

Getting started with OneDrive.pdf

A OneDrive starting document which was discovered on Steve's system. Hinting to maybe Steve hiding something on his drives.

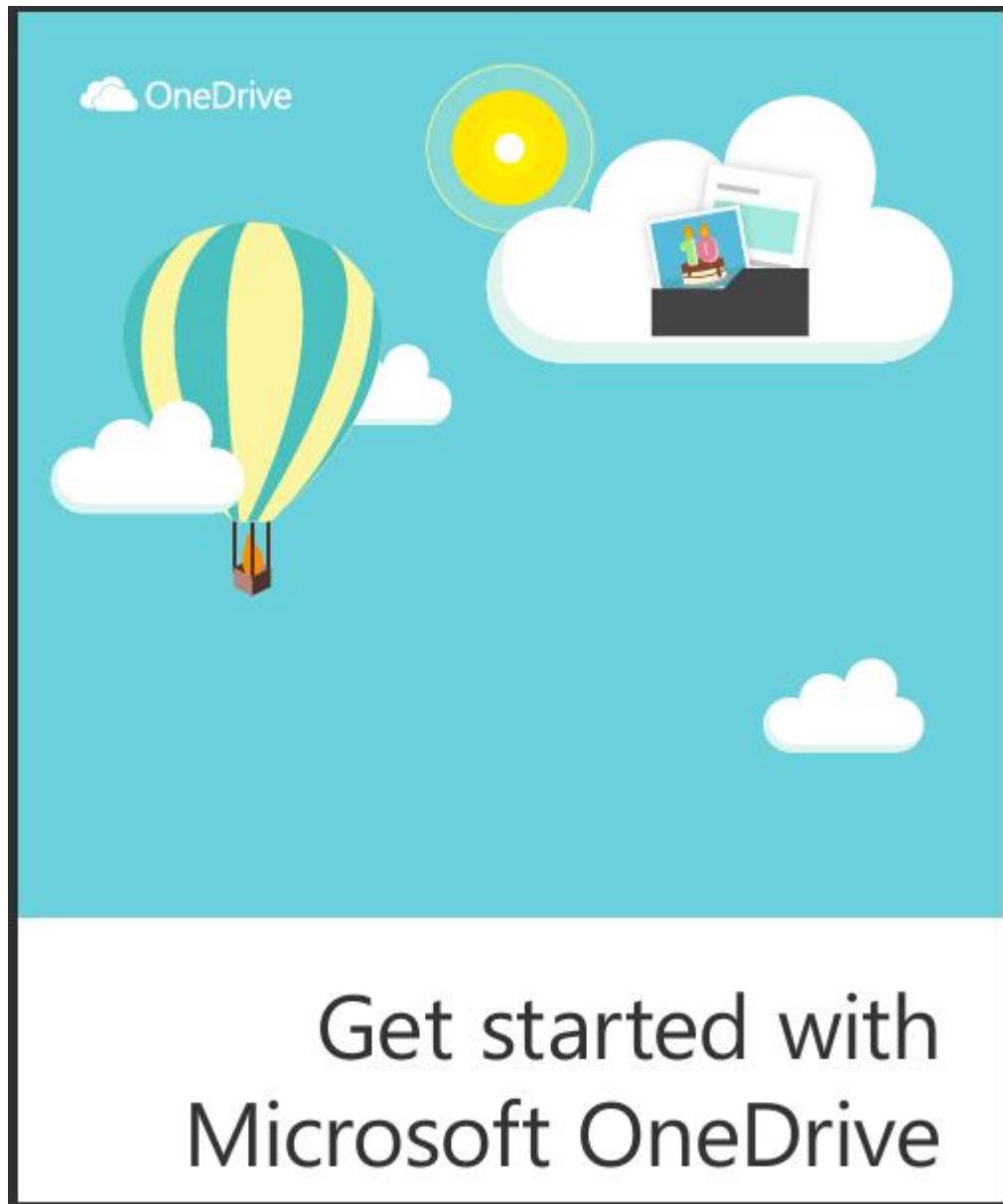


Figure 68 Getting started with OneDrive.pdf

3.6.2 John Fredricksen

client.ods

On John Fredricksen system there was an excel sheet discovered. This sheet lists people's names, Location, Product, Amount and Delivery period was discovered. We can see Jake Heke whose DHL shipment detail was discovered previously by the images. Also, Steve Kowhai and Jane Estebane were also discovered. This also makes us believe Steve is also a drug distributor like Steve Kowhai.

	A	B	C	D	E	F
1	Name	Location	Product	Amount	Delivery	
2	Ricky Ross	Los Angeles	Mama Coca	20kg	Monthly	
3	Frank Lucas	New York, USA	Ferry Dust	15kg	Quarterly	
4	Chris Coke	Kingston Jamaica	Coke	20kg	Monthly	
5	Steve Kowhai	Wellington, New Zealand	Crank	15kg	Monthly	
6	Don Cholito	Puerto Rico	Snow	25kg	Quarterly	
7	Manuel Noriega	Panama	Smack	15kg	Monthly	
8	Joaquin Guzman	Guadalajara, Mexico	China White	15kg	Monthly	
9	Leroy Barnes	New York, USA	Load pack	15kg	Quarterly	
10	AL Capone	Sicily, Italy	Silly putty	25kg	Monthly	
11	Jane Esteban	Brisbane, Australia	Uppers	1 gram	On demand	
12	Pablo Escobar	Colombia	White horse	15kg	Quarterly	
13	Franz Sanchez	Isthmus City	Mary Jane	20kg	Quarterly	
14	Jake Heke	Auckland	Tweak	10kg	Monthly	
15						
16						

Figure 69 client.ods

f0240272.odt

On John's system a word file discovered in this file we can see the actual planning done by John before going to Wellington, New Zealand.

We can see that he thinks between the road and sea. From previous evidence we know that he settles on air as he thinks the sea is much more vulnerable than it looks. He contemplates that shipping the product might be safer but costs higher for a small package. He also mentions this is a quality test for the product. Depending on this he might do future business. Then we can see that he settles for air as it is much cheaper for all the parties involved. Then he shows map of main drug trafficking and a inter regional map for drug trafficking.

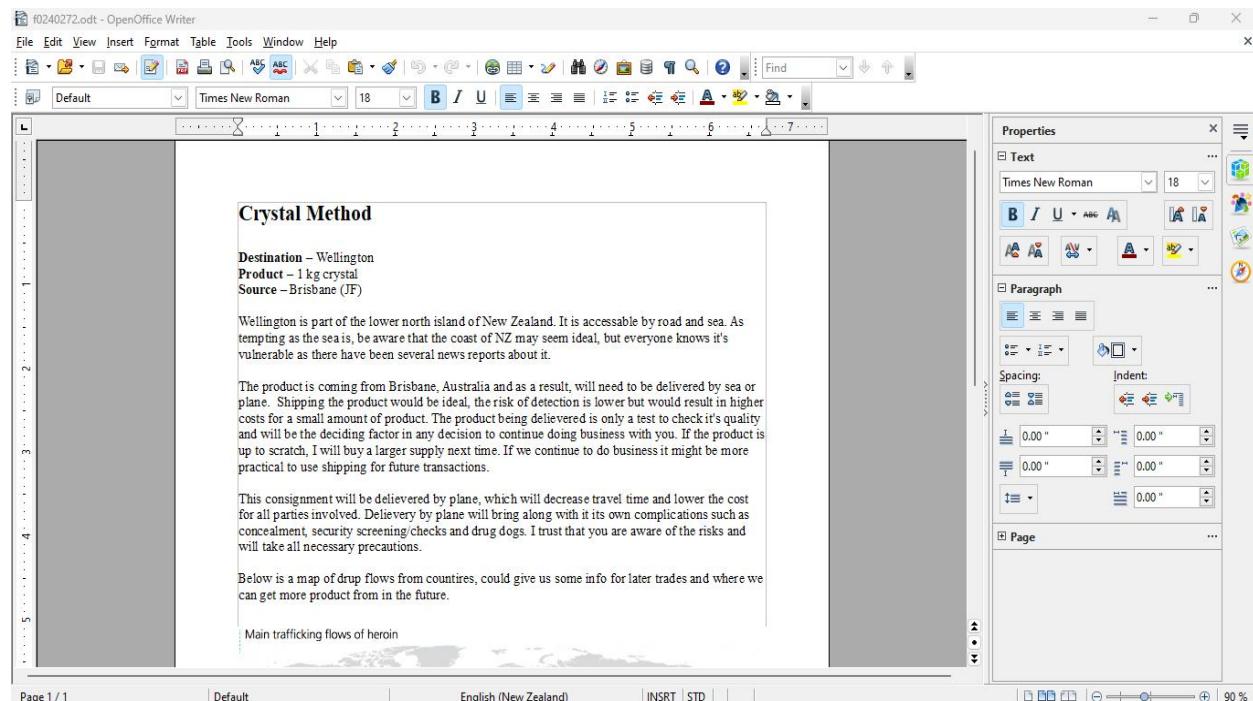


Figure 70 f0240272.odt

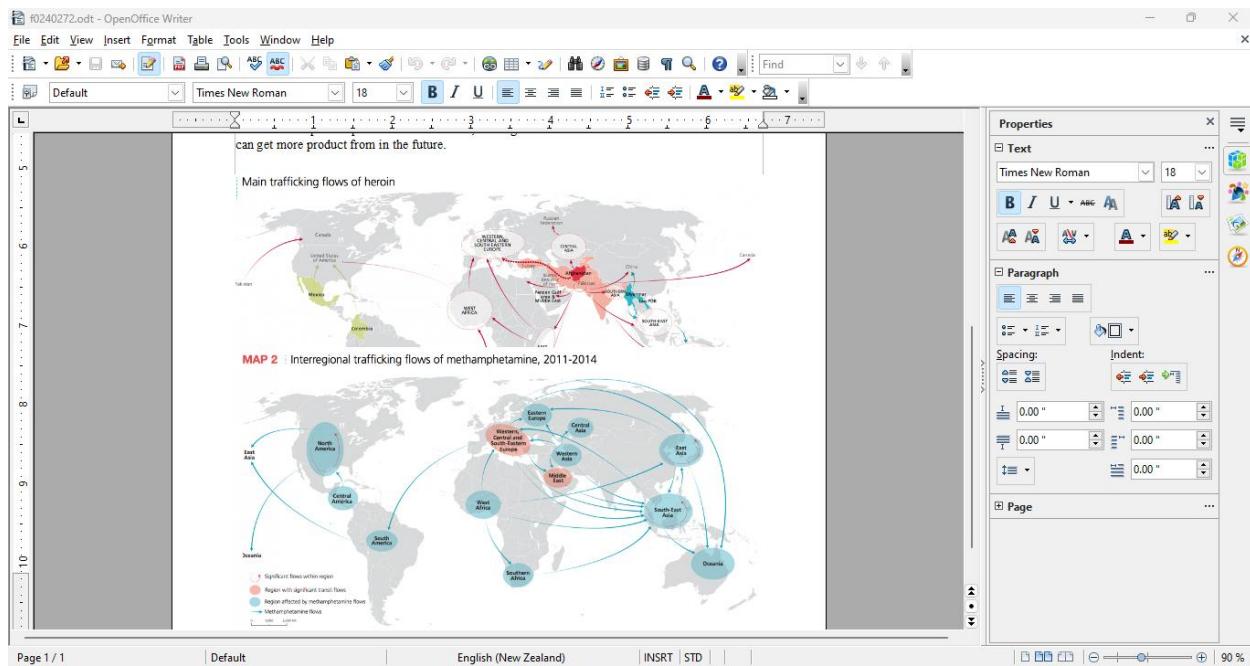


Figure 71 f0240272.odt

[SPACE INTENTIONALLY LEFT BLANK]

TrueCrypt User Guide.pdf

Same TrueCrypt encryption guide which was found on Steve Kowhai's System was found.

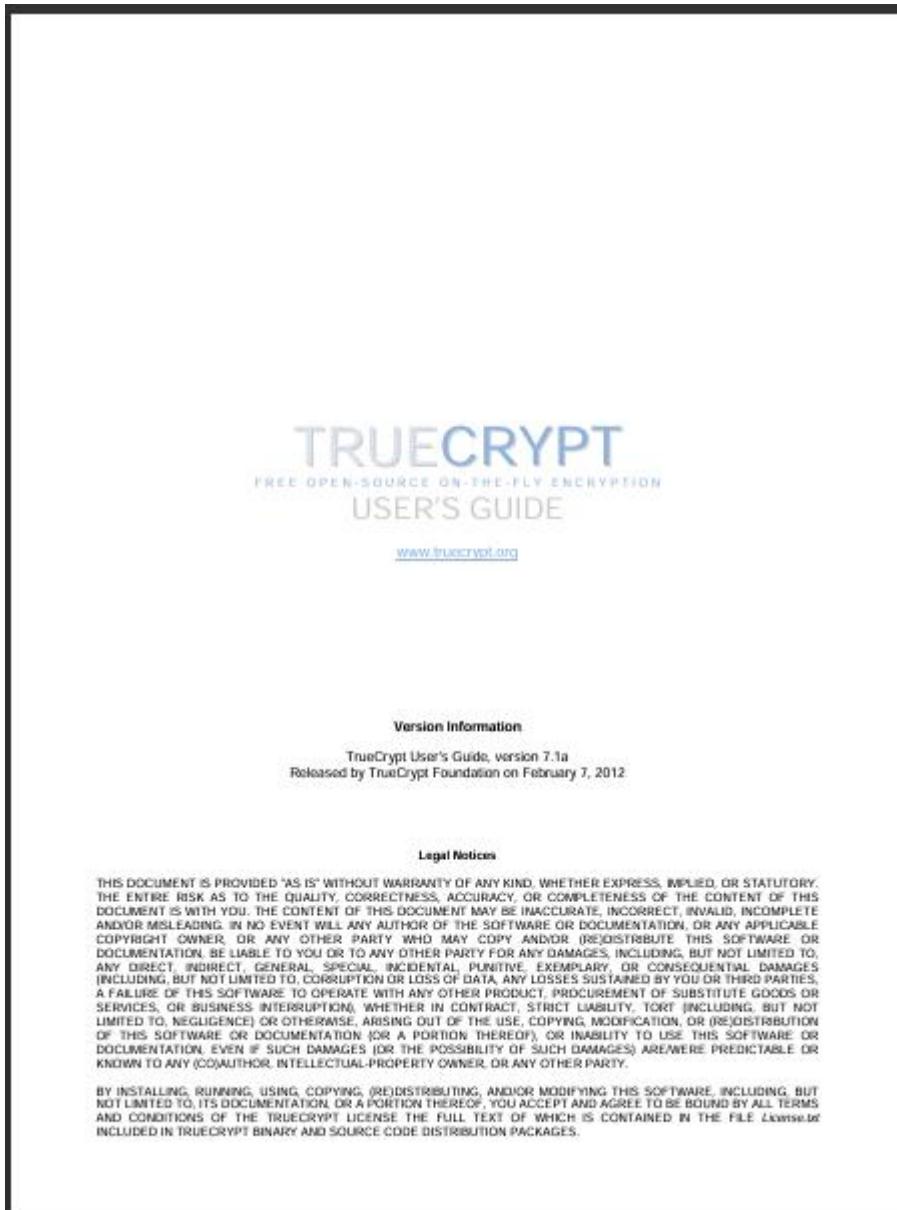


Figure 72 TrueCrypt User Guide.pdf

3.6.3 Jane Esteban

course-undercover-survival.pdf

On Jane Esteban System this undercover cop survival course pamphlet was discovered. Looking at the previous evidence this cements Jane as an undercover cop.

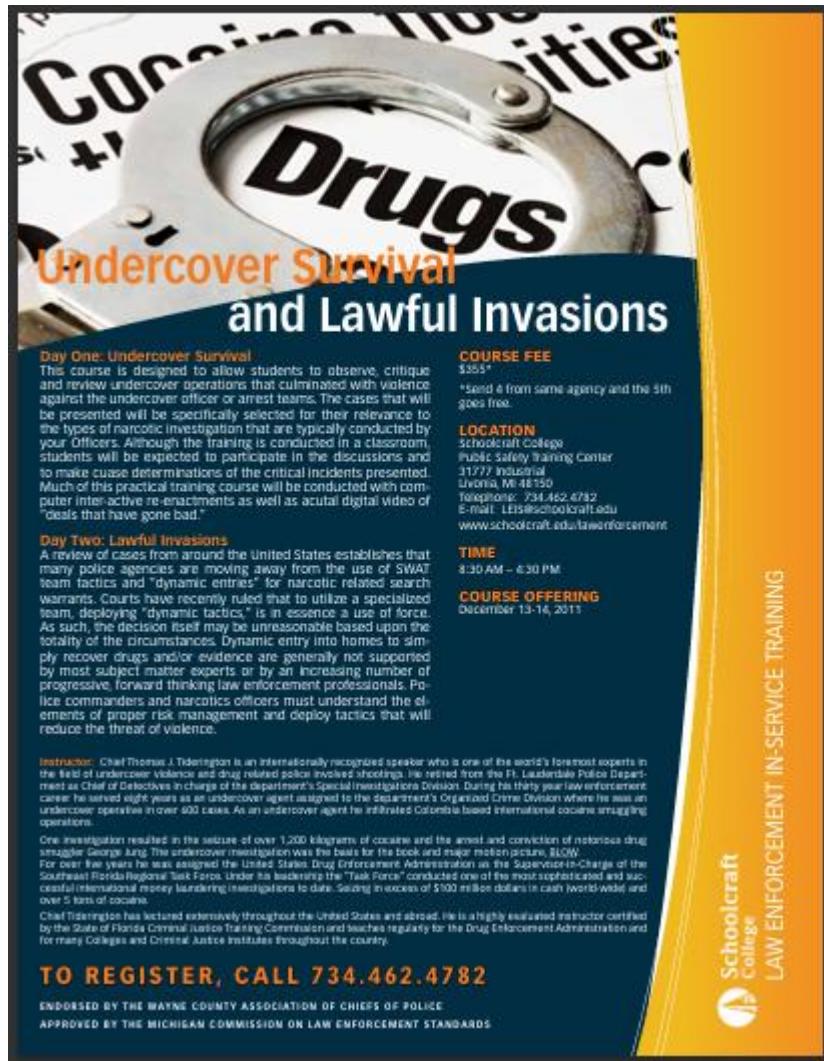


Figure 73 course-undercover-survival.pdf

Getting started with OneDrive.pdf

Same OneDrive pdf like Steve Kowhai was discovered.

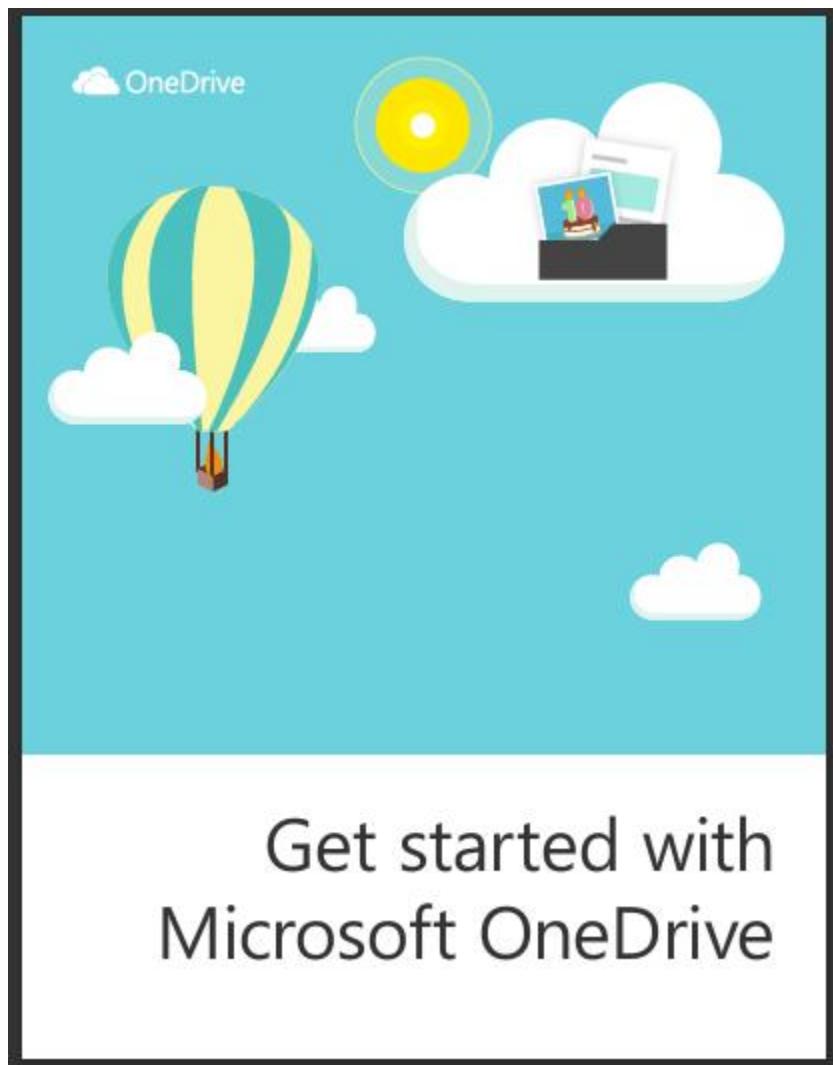


Figure 74 Getting started with OneDrive.pdf

3.7 Obfuscation Methods

Obfuscation refers to transforming the regular code into a human unreadable form which causes more complexity in static detection and analysis. Here we can see bunch of files with nonsensical data which is sign of obfuscation.

In this case a bunch of web history relating to image steganography was discovered with many starting guides for tools were discovered in the systems of suspects. This can be seen by going through the documents and the discord chats where image steganography was mentioned

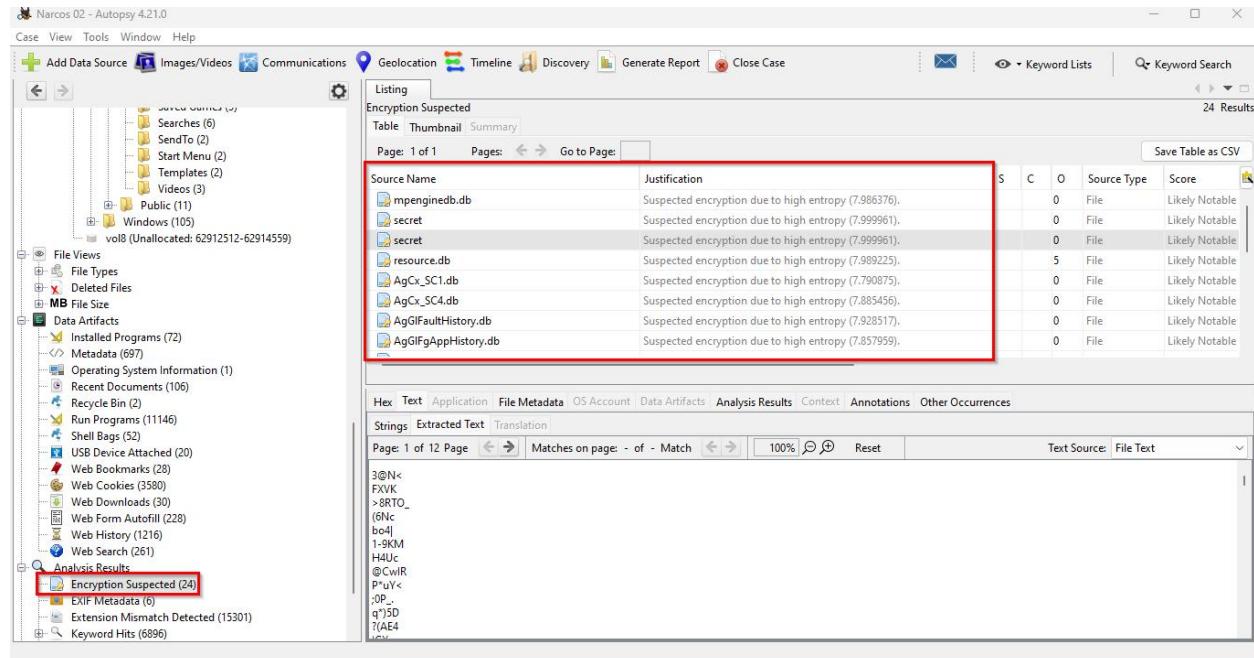


Figure 75 Obfuscated Files

3.8 Encryption Methods

There was only 1 type of encryption methods discovered during this evidence gathering which is:

- Truecrypt

TrueCrypt is a discontinued open-source utility used for on-the-fly disk encryption. Although it is no longer maintained, it is still widely used in legacy systems.

These encryption standard documents were also discovered previously.

Two methods to circumvent the encryption used by TrueCrypt are:

- Brute Force Attack:** This involves systematically trying all possible combinations until the correct one is found. This is often impractical due to the time required but can be feasible with weak passwords.
- Forensic Analysis and Password Guessing:** Using sophisticated tools like Passware Kit or Elcomsoft Forensic Disk Decryptor can exploit weaknesses in password creation or potential keyloggers on the suspect's machine.

3.9 Malware used

A malware was discovered on John Fredricksen's system. From the previous binary files this file turned out to be malware. For confirmation we used virus total which consists of backlog of large amount of malware which are discovered around the world.

It's a trojan which is used to steal banking credentials. Hinting towards John being much more of a computer man then he seemed before.

Name: Contact Card.exe

MD5 Hash: 409b88b2b275353f2ca05983cef1abf5

SHA-256 Hash: d56dd549736bda8fd1ebc8ae17c0b642c1df0fb5ce5e824b723d9b3f29da38c3

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
Contact Card.exe	2			2019-01-29 07:25:08 PKT				385024	Allocated	Allocated

Figure 76 Contact Card.exe

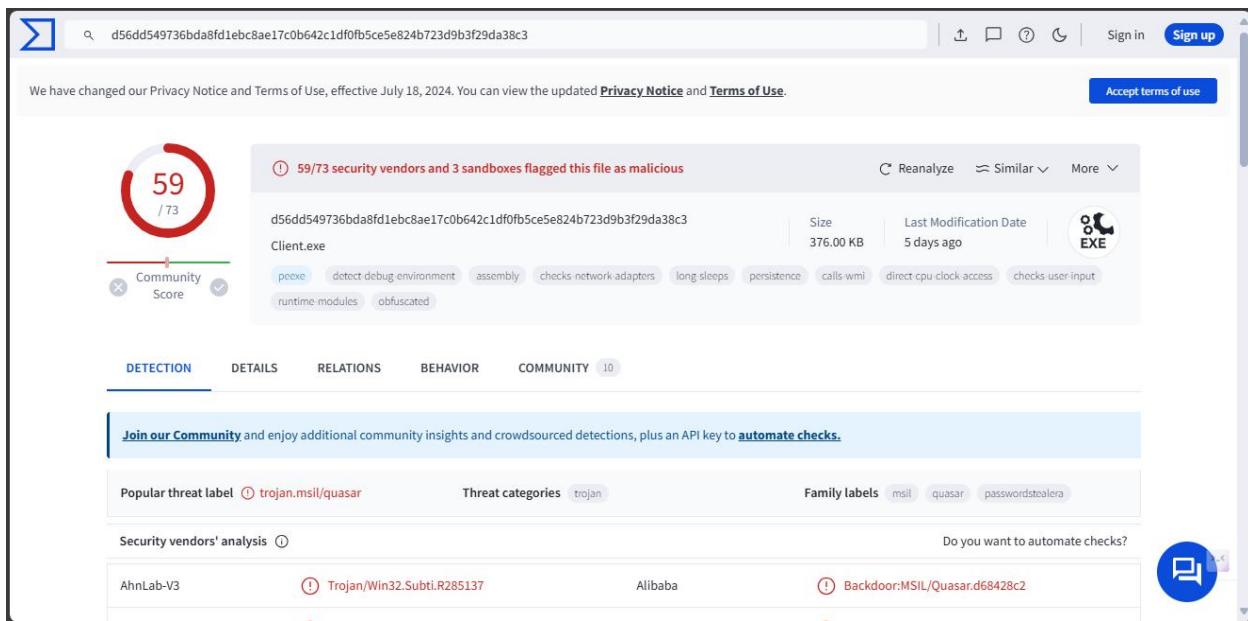


Figure 77 Virus Total Contact Card.Client.exe output

3.10 Vulnerability exploited for Malware

The malware was spread by Jane through discord. When she said that she would be sharing the list of people who wants to buy the drugs in discord she shared this Malware with John. The possible use for this malware is to infect John's system and get credentials from him.

[SPACE INTENTIONALLY LEFT BLANK]

3.11 Corroborative evidence

I used Autopsy's Timeline tool to help me to visualize and analyze system and user activities over time. This timeline can be matched with any testimony to confirm their validity of case timeline.

3.11.1 Steve Kowhai:

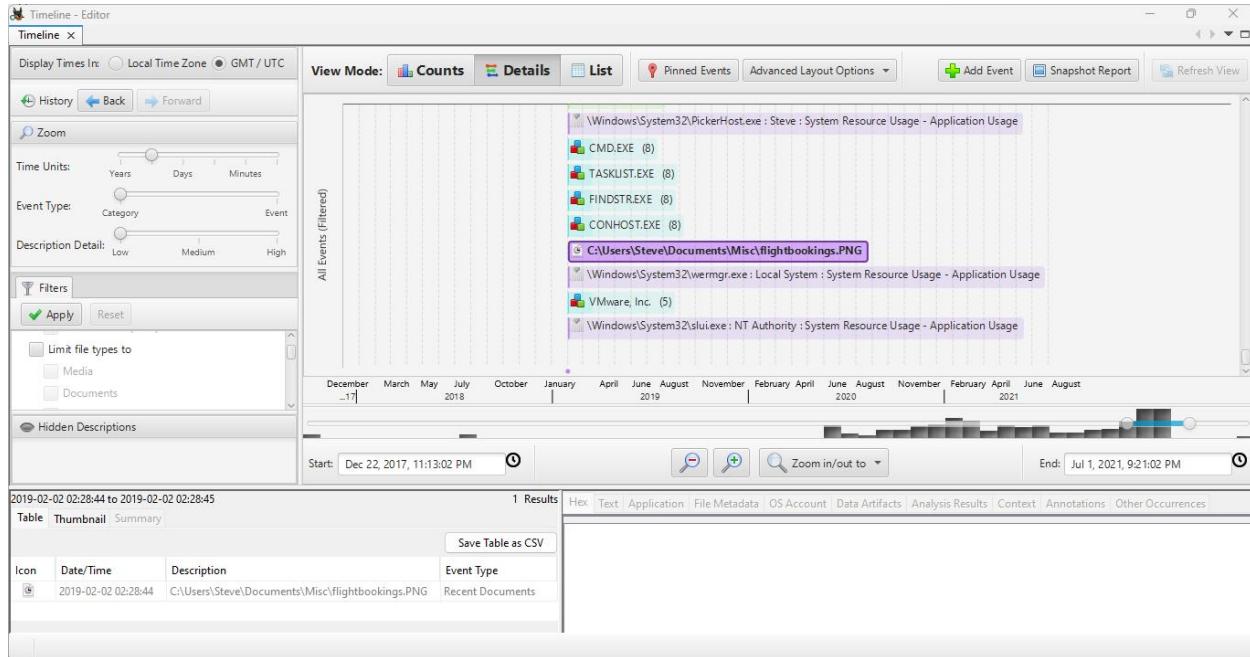


Figure 78 Steve Kowhai Timeline

[SPACE INTENTIONALLY LEFT BLANK]

3.11.2 John Fredricksen:

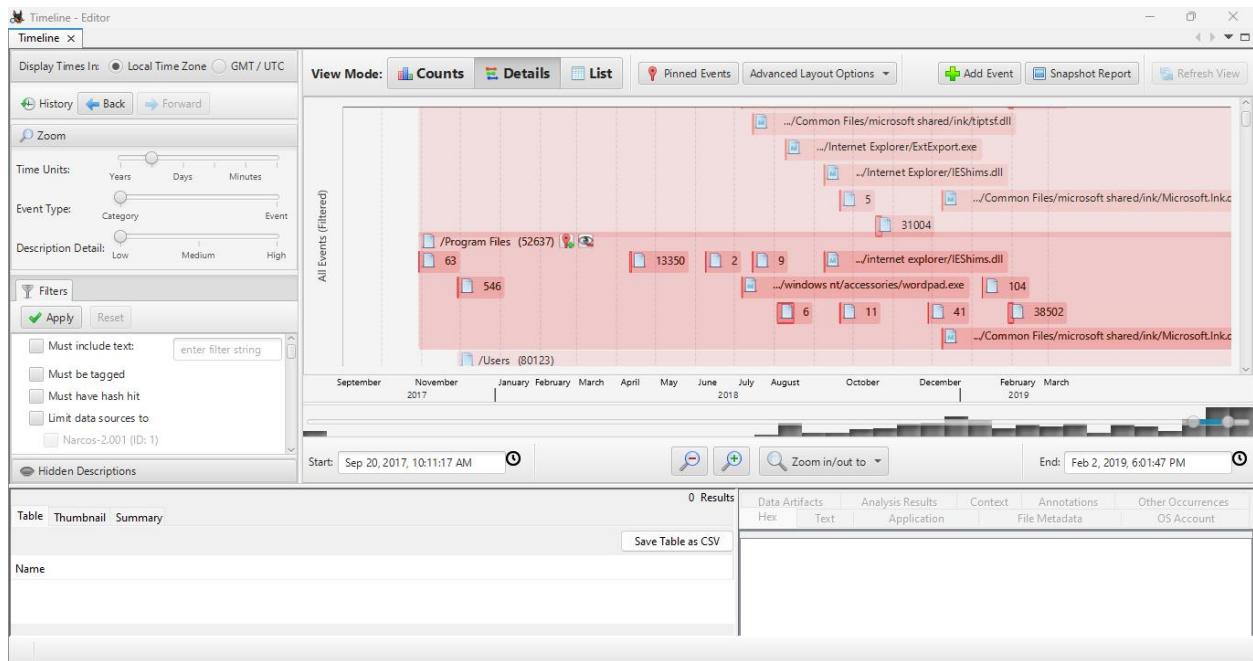


Figure 79 John Fredricksen Timeline

3.11.3 Jane Esteban:

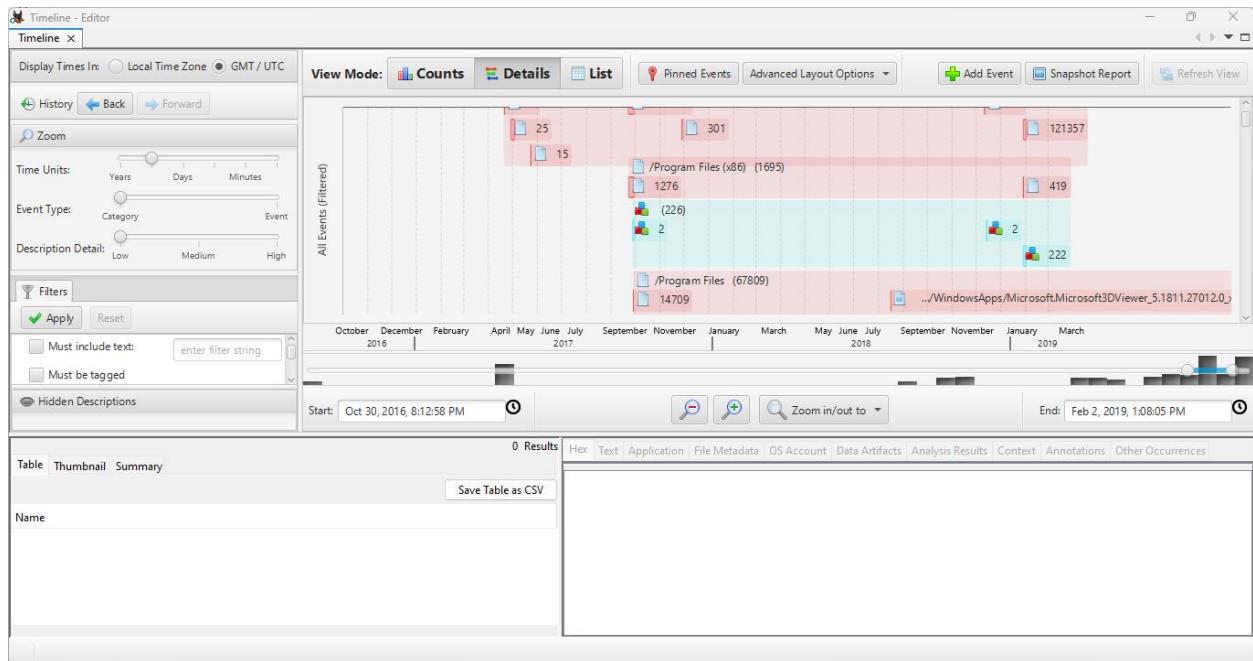


Figure 80 Jane Esteban Timeline

3.12 Artifact changes across different windows 10 Builds

The analysis revealed that there are significant changes in the windows artifacts across the system.

For Example:

- The Flight Booking Detail Picture has accessed date on Steve is 2019-02-02 02:31:06 UTC while on John accessed date is 2019-02-02 01:57:27 UTC.
- The BNE image which shows Australia Houses Rivers Bridges Roads Brisbane Night Cities photo present in both Steve and John have different accessed time. The John accessed date is 2019-02-01 12:06:04 UTC and Steve accessed date is 2019-02-02 02:31:06 UTC.

Likewise, there are a lot of artifacts which have significant changes in windows artifacts.

3.13 Suspects Roles

Below are the suspects' roles discovered in this forensic investigation.

3.12.1 Steve Kowhai

Steve Kowhai role has become clear from this investigation as a gang affiliated drug dealer who was the one buying some drugs from 'John Fredricksen' to further his business in New Zealand.

3.12.2 John Fredricksen

John Fredricksen role has become clear as a drug dealer in his country. Form the images and from all the files discovered we can see that John had also planned to deliver a drug sample to Wellington, New Zealand.

3.12.3 Jane Esteban

Jane Esteban role has become clear as an undercover cop which is acting like a drug addict to get information from John Fredricksen. Possibly she was the who leaked the delivery information and led to their arrest at the airport.

4. Summary and Conclusion

In Summary this report represents a detailed forensics investigation conducted by us into the activates and digital evidence related to the suspects involved namely Steve Kowhai, John Fredricksen, Jane Esteban involved in the drug smuggling operation intercepted by custom officials. Some Main points, Findings and recommendations.

Some digital evidence was gathered which can be used to identify the guilty and innocent in this case.

4.1 User Accounts:

Only one user account was discovered on all the systems leading us to believe there was only one user present on the system. Meaning no one else was secretly using their systems.

4.2 Web History and Images:

From the Web history, it was discovered that Steve Kowhai was a gang-affiliated drug dealer with John Fredricksen, who was also a drug distributor. John was also following many drug trends such as many drug memes and following many drugs related sub reddit's. John's web history showed that he was planning to hide the sample in a suitcase and was also shown to be looking for flights from Brisbane, Australia to Wellington, New Zealand. John was also shown to have mapped out his plan with all the flights already planned. While Jane was discovered to be an undercover cop trying to find ways to infiltrate this network and try to survive this operation.

4.3 Communication

There was some communication between Steve and John in which it was uncovered that John was planning on selling some drugs to Steve namely 'Crystal'. The Communication between John and Jane was also uncovered in which he talked to Jane like she was a courier for the package meaning on the day of arrest she was in possession of the drugs.

4.4 Documents

From the documents discovered we can see that John and Steve have implemented some kind of encryption to hide their wrongdoings and that they were actively searching for image steganography tools as well. On both Steve and Johns system the ‘Vera crypt’ user guide was discovered. On Johns, an excel sheet was discovered, listing the buyers and location with their name.

In this sheet Jane and Steves name were also written cementing that John was a drug Distributor.

Once again, Jane was discovered to be looking for a course with survival tips for undercover cops.

4.5 Conclusion

In conclusion, it was discovered that John Fredricksen was an active drug user and distributor with interregional and international connections and Steve was a gang-affiliated drug dealer. The digital evidence and analysis provide us with enough substantial evidence against these two individuals of being guilty. As for Jane Esteban it was made evident that she was an undercover cop trying to bust this drug trade and possibly was the one who relied the information for the arrest on the airport making her innocent of any crime and deserving of medal for her hard work and bravery in face of such dangers.

5. Appendix

5.1 Description of persons of interest

Actors	Description
Steve Kowhai	<ul style="list-style-type: none">• Images retrieved.• Discord chat intercepted.• Web search Intercepted.• Was buying drug sample from John.• Had plans for drop off and escape.• Gang affiliated.• Drug Dealer/ Distributor.
Jane Esteban	<ul style="list-style-type: none">• Images retrieved.• Discord chat intercepted.• Web search Intercepted.• Undercover cop.• Acted as a partner with John.• Hid samples in her suitcase.• Shared malware file with John.
John Fredricksen	<ul style="list-style-type: none">• Images retrieved.• Discord chat intercepted.• Web search Intercepted.• Very active in drugs sub reddit.• Drug user and distributor.• Regional and inter regional distributor.• Sold the drug sample to Steve.• Planned to use Jane as mule.

5.2 Association Diagram of persons of interest

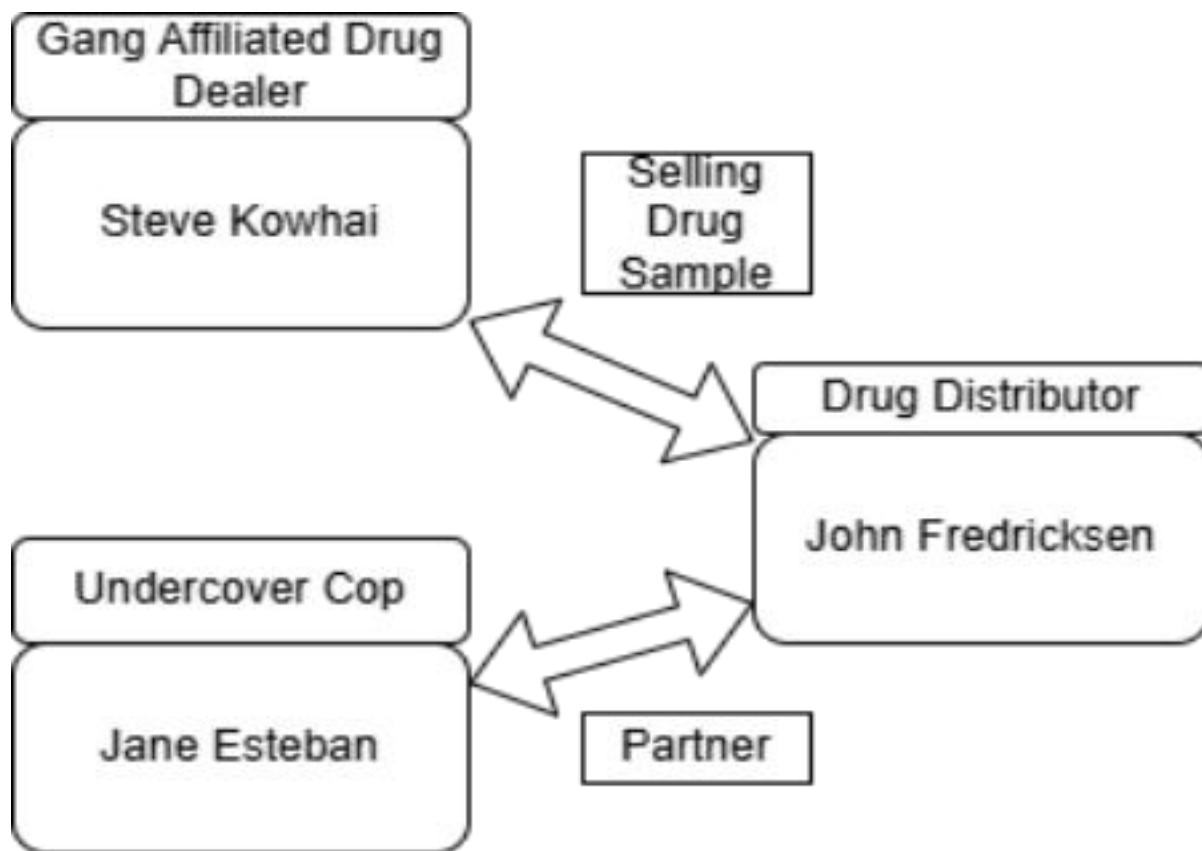
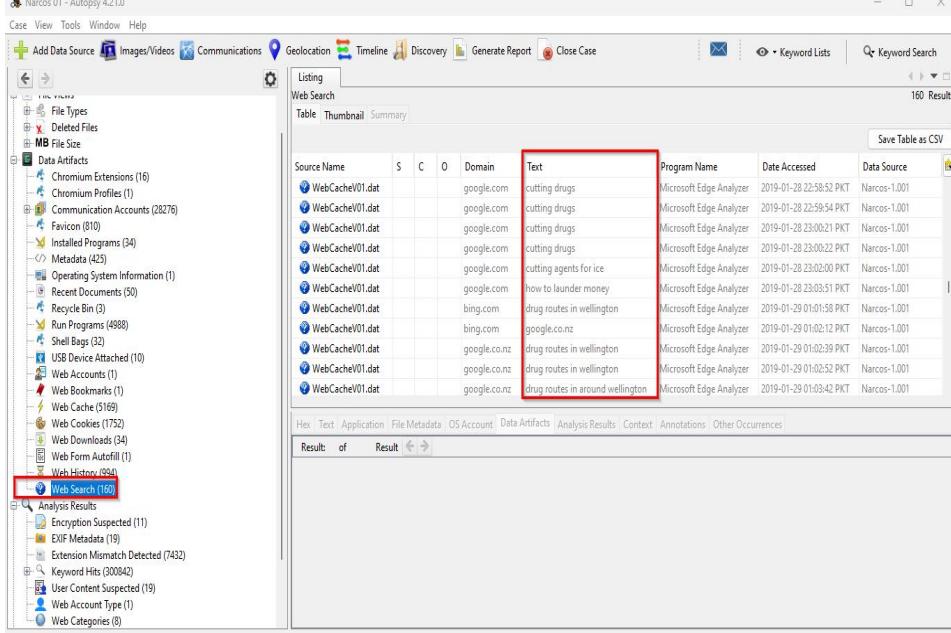
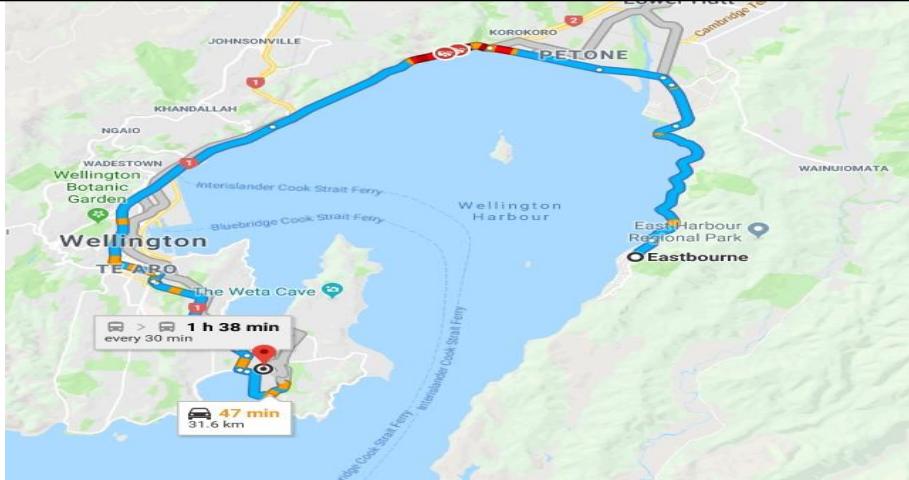
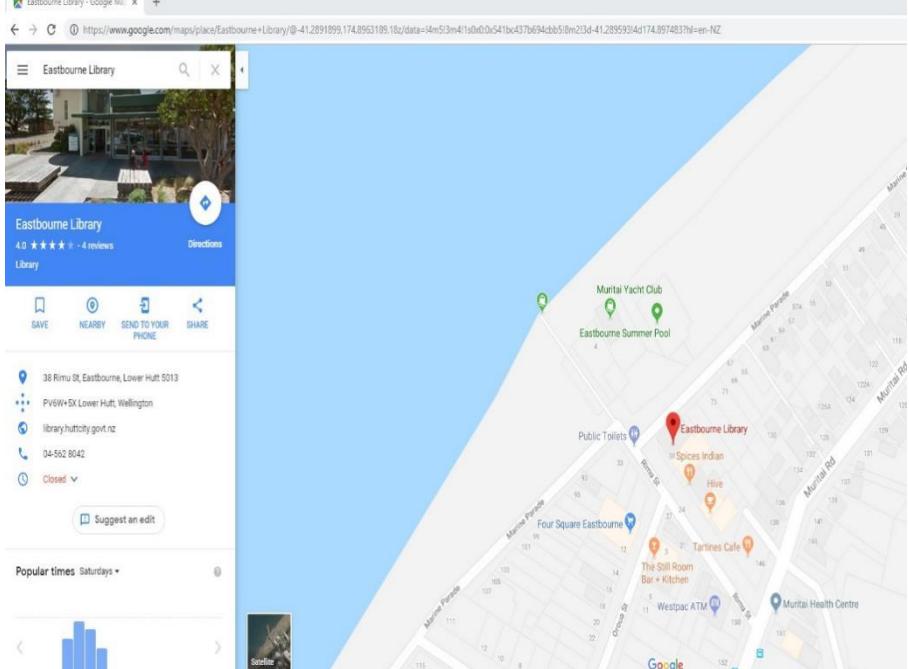
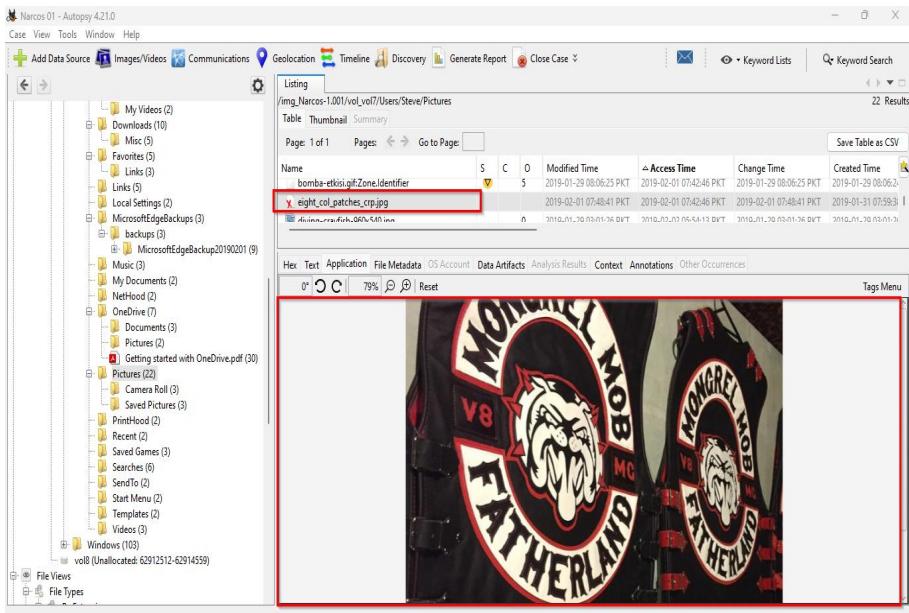


Figure 81 Association Diagram of persons of interest

5.3 Evidence Listing

Actor Name	Evidence type	Evidence Image
Steve Kowhai	Web History	 <p>Autopsy 01 - Autopsy 4.21.0</p> <p>Case View Tools Window Help</p> <p>Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case</p> <p>Keyword Lists Keyword Search</p> <p>160 Results</p> <p>Save Table as CSV</p> <p>Source Name S C O Domain Text Program Name Date Accessed Data Source</p> <p>WebCacheV01.dat google.com cutting drugs Microsoft Edge Analyzer 2019-01-28 22:58:52 PKT Narcos-1.001</p> <p>WebCacheV01.dat google.com cutting drug Microsoft Edge Analyzer 2019-01-28 22:59:54 PKT Narcos-1.001</p> <p>WebCacheV01.dat google.com cutting drug Microsoft Edge Analyzer 2019-01-28 23:00:21 PKT Narcos-1.001</p> <p>WebCacheV01.dat google.com cutting drug Microsoft Edge Analyzer 2019-01-28 23:00:22 PKT Narcos-1.001</p> <p>WebCacheV01.dat google.com cutting drug Microsoft Edge Analyzer 2019-01-28 23:02:00 PKT Narcos-1.001</p> <p>WebCacheV01.dat google.com cutting drug Microsoft Edge Analyzer 2019-01-28 23:03:51 PKT Narcos-1.001</p> <p>WebCacheV01.dat bing.com how to launder money Microsoft Edge Analyzer 2019-01-29 01:01:58 PKT Narcos-1.001</p> <p>WebCacheV01.dat google.co.nz drug routes in wellington Microsoft Edge Analyzer 2019-01-29 01:02:12 PKT Narcos-1.001</p> <p>WebCacheV01.dat google.co.nz drug routes in wellington Microsoft Edge Analyzer 2019-01-29 01:02:52 PKT Narcos-1.001</p> <p>WebCacheV01.dat google.co.nz drug routes in around wellington Microsoft Edge Analyzer 2019-01-29 01:03:42 PKT Narcos-1.001</p> <p>Web Search (160)</p> <p>Analysis Results</p> <ul style="list-style-type: none"> Encryption Suspected (11) EXIF Metadata (19) Extension Mismatch Detected (7432) Keyword Hits (300842) User Content Suspected (19) Web Account Type (1) Web Categories (8)
	Images	





Narcos 01 - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing /img/Narcos-1.001/vol_volt7/Users/Steve/Pictures 22 Results

Table Thumbnail Summary

Page: 1 of 1 Pages: Go to Page

Name S C O Modified Time Access Time Change Time Created Time

33d49c521dd812b9421dff05dc47e5bb.jpg	0	2019-01-29 08:08:26 PKT	2019-01-31 02:21:13 PKT	2019-01-29 08:08:22	2019-01-31 02:21:13 PKT	2019-01-29 08:08:22
33d49c521dd812b9421dff05dc47e5bb.jpgZone.Identifier	5	2019-01-29 08:08:26 PKT	2019-01-31 02:21:13 PKT	2019-01-29 08:08:22	2019-01-31 02:21:13 PKT	2019-01-29 08:08:22
620x349.jpg						

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Tags Menu

File Views File Types



Discord Chat

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing /img/Narcos-1.001/vol_volt7/Users/Steve/AppData/Roaming/Discord/Local Storage/levels 11 Results

Table Thumbnail Summary

Page: 1 of 1 Pages: Go to Page

Name S C O Modified Time Access Time Change Time Created Time Size F

[current folder]				2019-02-02 07:38:41 PKT	2019-02-02 07:38:41 PKT	2019-02-02 07:38:41 PKT	2019-01-29 01:57:06 PKT	56	A
[parent folder]				2019-01-29 05:12:06 PKT	2019-02-02 07:38:41 PKT	2019-01-29 05:17:06 PKT	2019-01-29 01:57:06 PKT	144	A
000005.jbb				2019-01-29 05:12:06 PKT	2019-02-02 07:39:25 PKT	2019-01-29 05:12:06 PKT	2019-01-29 05:12:06 PKT	9533	A
000006.jpg				2019-02-02 07:38:47 PKT	2019-02-02 07:38:47 PKT	2019-02-02 07:38:47 PKT	2019-01-29 08:43:06 PKT	34411	A

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation

Page: 1 of 1 Page: Matches on page: - of - Match: 100% Reset Text Source: File Text

```

chatstore
('state': '539550615072800768', 'timestamp': '1549074628536', 'draft': 'Good. Meet at the Eastbourne library and if we miss each other come to 666 Rewera Avenue, Petone'), 'version': 0)
META:https://discordapp.com
# https://discordapp.com
DraftStore
('state': '539550615072800768', 'timestamp': '1549074633814', 'draft': 'Good. Meet at the Eastbourne library and if we miss each other come to 666 Rewera Avenue, Petone'), 'version': 0)
META:https://discordapp.com
# https://discordapp.com
DraftStore
('state': '539550615072800768', 'timestamp': '1549074636655', 'draft': 'Good. Meet at the Eastbourne library and if we miss each other come to 666 Rewera Avenue, Petone'), 'version': 0)
META:https://discordapp.com
# https://discordapp.com
DraftStore
('state': '539550615072800768', 'timestamp': '1549074638711', 'draft': 'Good. Meet at the Eastbourne library and if we miss each other come to 666 Rewera Avenue, Petone'), 'version': 0)
META:https://discordapp.com
# https://discordapp.com
test

```

Jane
Esteba
n

Images/
web
history

Narcos 03 - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing /img/Narcos-3.001/vol.v017/Users/JaneE/Pictures

Table Thumbnail Summary

Page: 1 of 1 Pages: Go to Page: Save Table as CSV

Name	S	C	O	Modified Time	Access Time	Change Time	Created Time	Size
contact-card-512.png	0			2019-01-29 02:22:37 PKT	2019-01-29 02:22:37 PKT	2019-01-29 02:22:37 PKT	2019-01-29 02:22:37 PKT	16
contact-card-512.pngZone.Identifier	5			2019-01-29 02:22:37 PKT	2019-01-29 02:22:37 PKT	2019-01-29 02:22:37 PKT	2019-01-29 02:22:37 PKT	95
contact_card.ico	1			2019-01-29 02:24:11 PKT	2019-01-29 02:24:11 PKT	2019-01-29 02:27:52 PKT	2019-01-29 02:24:11 PKT	26
contact_card.ico.Zone.Identifier	1			2019-01-29 02:24:11 PKT	2019-01-29 02:24:11 PKT	2019-01-29 02:27:52 PKT	2019-01-29 02:24:11 PKT	21
afp.png				2019-01-29 03:47:48 PKT	2019-01-29 03:46:06 PKT	2019-01-29 03:47:48 PKT	2019-01-29 03:46:06 PKT	66
afp.png				2019-01-29 03:47:48 PKT	2019-01-29 03:46:06 PKT	2019-01-29 03:47:48 PKT	2019-01-29 03:46:06 PKT	66
background.jpg	6			2010-01-10 00:47:32 DWT	2010-01-10 00:47:32 DWT	2010-01-10 00:47:32 DWT	2010-01-10 00:47:32 DWT	27

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

0% 100% 10% Reset Tags Menu

Narcos 03 - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing Web Search

Table Thumbnail Summary

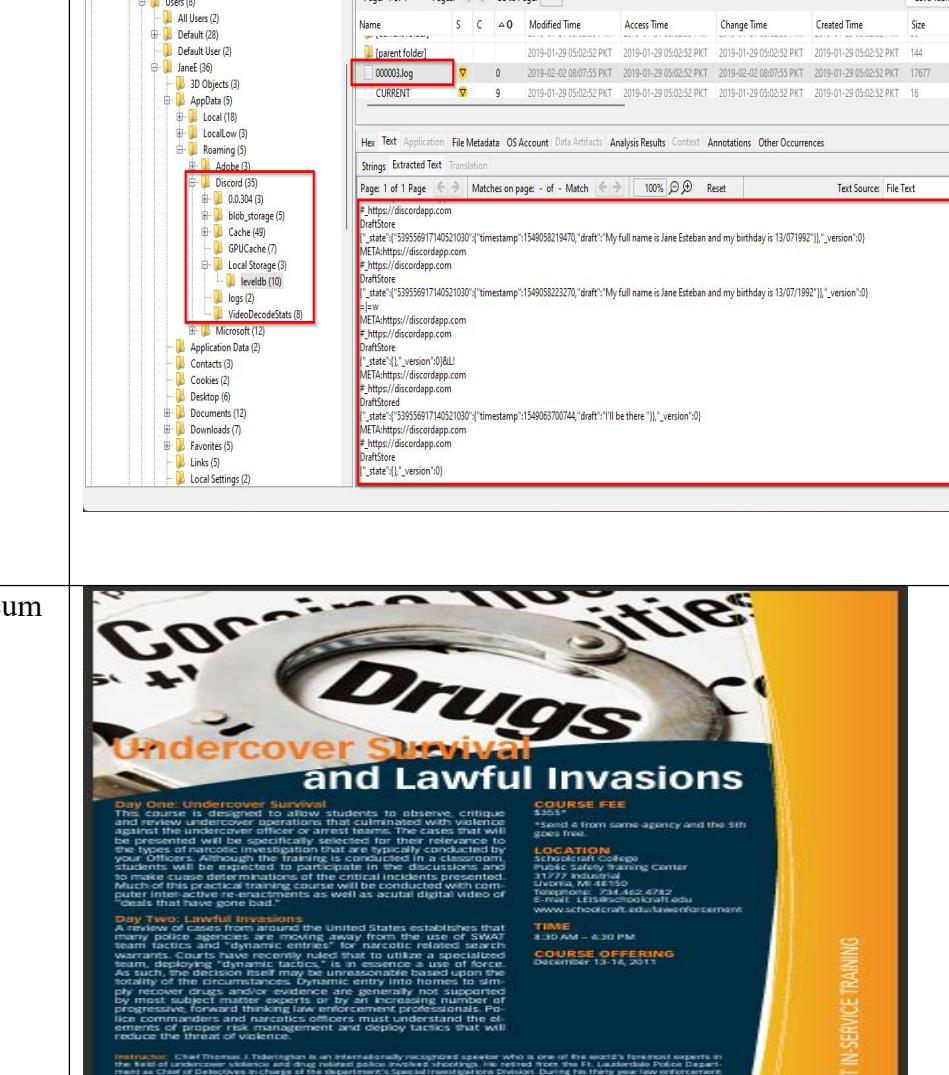
303 Results

Save Table as CSV

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed
WebCacheV01.dat				bing.com	how to pretend to be desperate	Microsoft Edge Analyzer	2019-01-31 22:05:45 PKT
WebCacheV01.dat				bing.com	how to pretend to be desperate	Microsoft Edge Analyzer	2019-01-31 23:05:47 PKT
WebCacheV01.dat				bing.com	how to pretend to be desperate in drug dealings	Microsoft Edge Analyzer	2019-01-31 23:06:33 PKT
WebCacheV01.dat				bing.com	how to pretend to be desperate	Microsoft Edge Analyzer	2019-01-31 23:07:16 PKT
WebCacheV01.dat				bing.com	survival tips from an undercover cop	Microsoft Edge Analyzer	2019-01-31 23:55:31 PKT
WebCacheV01.dat				bing.com	survival tips from an undercover cop	Microsoft Edge Analyzer	2019-02-01 00:01:50 PKT
WebCacheV01.dat				bing.com	undercover cop survival	Microsoft Edge Analyzer	2019-02-01 00:03:11 PKT
WebCacheV01.dat				bing.com	undercover cop survival	Microsoft Edge Analyzer	2019-02-01 00:03:27 PKT
WebCacheV01.dat				youtube.com	survival tip from an undercover cop	Microsoft Edge Analyzer	2019-02-01 00:03:44 PKT
WebCacheV01.dat				youtube.com	survival tip from an undercover cop	Microsoft Edge Analyzer	2019-02-01 00:05:04 PKT

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result of Result

<h1>Discord</h1>	
Document	

John
Fredri
ck

Images/
web
history

DHL EXPRESS

Shipment Air Waybill
(Non negotiable)

1 **Payer account number and insurance details**

Charge to Shipper Receiver 3rd party Cash Cheque Credit Card

Payer Account No. 001-158545-85

Shipment Insurance see reverse
Yes Insured value (in local currency) 0 Not all payment options are available in all countries.

2 **From (Shipper)**

Shipper's account number 258-85695 Contact name Johnny Fredrick

Shipper's reference (up to 32 characters but only first 12 will be shown on invoice) AB-20071223-589X

Company name High As a Kite LLC

Address 8515 Haven Wood Trail Inala, Brisbane QLD 4077 Australia

Postcode/Zip Code (required) QLD 4077 Phone, Fax or E-mail (required) +1 258 585 965

3 **To (Receiver)**

Company name

Delivery address DHL cannot deliver to a PO Box

5/34 Hapua Street Remuera Auckland 1050 New Zealand

Postcode/Zip Code (required) 1050 Country New Zealand

Contact person Jake Heke Phone, Fax or E-mail (required) +6402145365477

4 **Shipment details**

Total number of packages 1	Total Weight 20kg	Dimensions in cm 575 @ 500mm x 500mm x 600mm
	kg	gr @ x x
	kg	gr @ x x
	kg	gr @ x x

5 **Full description of contents**

Give content and quantity

1x Pressure cooker
3x Pots
1x Bread Maker

6 **Non-Document Shipments Only (Customs Requirement)**

Attach the original and five copies of a Proforma or Commercial invoice. Shipper's VAT/GST number Receiver's VAT/GST or Shipper's EIN/SSN

Declared Value for Customs (as on commercial/proforma invoice) Harmonised Commodity Code if applicable

TYPE OF EXPORT Permanent Repair / Return Temporary

Destination duties/taxes if left blank receiver pays duties/taxes

Receiver Shipper Other specify approved account number

7 **Shipper's agreement (Signature required)**

Unless otherwise agreed in writing, we agree that DHL's Terms and Conditions of carriage are all the terms of the contract between ourselves and DHL, and (1) such terms and conditions and, where applicable, the DHL Standard Terms and Conditions for loss, damage or delay, and (2) this shipment does not contain cash or dangerous goods (see overall).

Signature Johnny Fredrick Date 29 / 01 / 2019

ORIGIN B N E DESTINATION CODE A K L

GREY SECTIONS FOR DHL USE ONLY

DHL EXPRESS - 139501

Narcos 02 - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing Web Search 261 Results

Table Thumbnail Summary

Save Table as CSV

Source Name S C O Domain Text Program Name Date Accessed Data Source

places.sqlite	google.com		suitcase concealments	Firefox Analyzer	2019-01-31 07:04:44 PKT	Narcos-2.001
places.sqlite	google.co.nz		suitcase concealments	Firefox Analyzer	2019-01-31 07:05:17 PKT	Narcos-2.001
places.sqlite	google.co.nz		suitcase concealments	Firefox Analyzer	2019-01-31 07:05:21 PKT	Narcos-2.001
places.sqlite	google.com		suitcase concealments for drugs	Firefox Analyzer	2019-01-31 07:06:09 PKT	Narcos-2.001
places.sqlite	google.com		suitcase concealments for drugs	Firefox Analyzer	2019-01-31 07:12:25 PKT	Narcos-2.001
places.sqlite	google.com		suitcase concealments for drugs	Firefox Analyzer	2019-01-31 07:12:48 PKT	Narcos-2.001
places.sqlite	google.com		new zealand wellington	Firefox Analyzer	2019-01-31 07:13:42 PKT	Narcos-2.001
places.sqlite	google.com		new zealand wellington	Firefox Analyzer	2019-01-31 07:14:11 PKT	Narcos-2.001
places.sqlite	google.com		new zealand wellington	Firefox Analyzer	2019-01-31 07:14:19 PKT	Narcos-2.001
flights brisbane to VLG return				Firefox Analyzer	2019-01-31 07:15:43 PKT	Narcos-2.001

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result of Result

Name	S	C	O	Modified Time	Access Time	Change Time
drugmeme3.jif;Zone.Identifier	3			2019-01-29 01:12:17 PKT	2019-01-30 12:42:36 PKT	2019-01-29 02:43:23 PKT
drugmeme4.jif	0			2019-01-29 01:12:43 PKT	2019-01-30 12:42:36 PKT	2019-01-29 02:43:23 PKT
drugmeme4.jif;Zone.Identifier	3			2019-01-29 01:12:43 PKT	2019-01-30 12:42:36 PKT	2019-01-29 02:43:23 PKT

Document	A	B	C	D	E	F
1 Name	Location	Product	Amount	Delivery		
2 Ricky Ross	Los Angeles	Mama Coca	20kg	Monthly		
3 Frank Lucas	New York, USA	Ferry Dust	15kg	Quarterly		
4 Chris Coke	Kingston Jamaica	Coke	20kg	Monthly		
5 Steve Kowhai	Wellington, New Zealand	Crank	15kg	Monthly		
6 Don Cholito	Puerto Rico	Snow	25kg	Quarterly		
7 Manuel Noriega	Panama	Smack	15kg	Monthly		
8 Joaquin Guzman	Guadalajara, Mexico	China White	15kg	Monthly		
9 Leroy Barnes	New York, USA	Load pack	15kg	Quarterly		
10 AL Capone	Sicily, Italy	Silly putty	25kg	Monthly		
11 Jane Esteban	Brisbane, Australia	Uppers	1 gram	On demand		
12 Pablo Escobar	Colombia	White horse	15kg	Quarterly		
13 Franz Sanchez	Isthmus City	Mary Jane	20kg	Quarterly		
14 Jake Heke	Auckland	Tweak	10kg	Monthly		
15						
16						

5.4 Software and tools used in the investigation

FTK Imager:

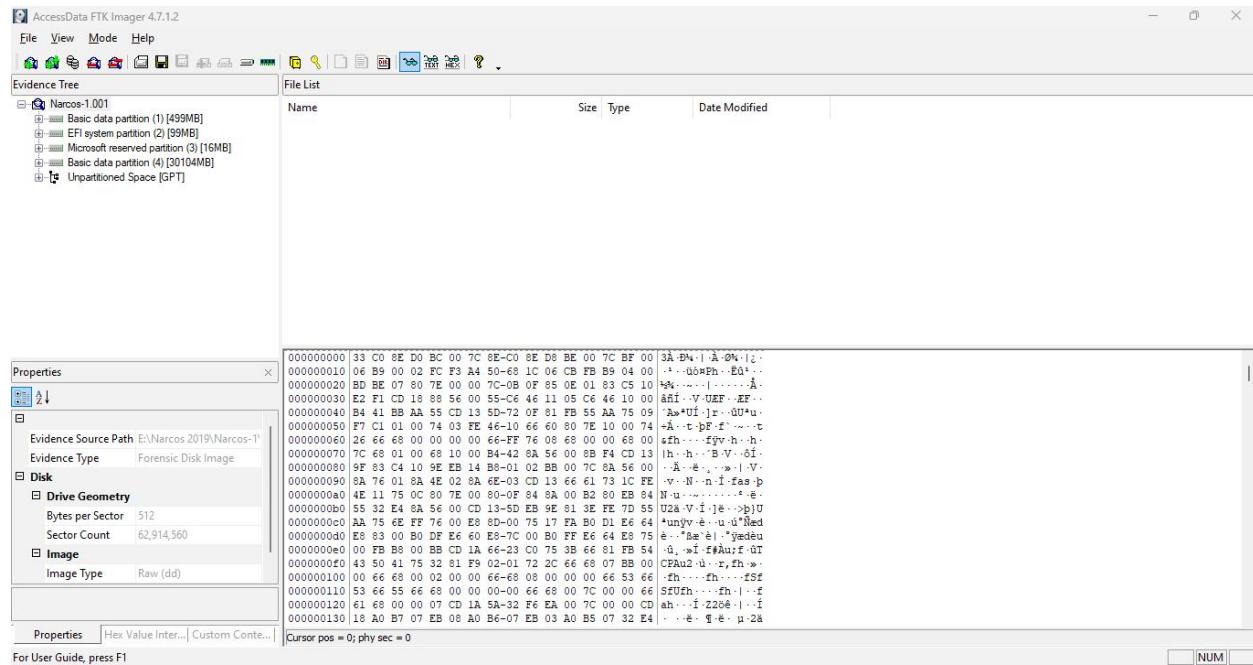


Figure 15 FTK Imager

Autopsy:

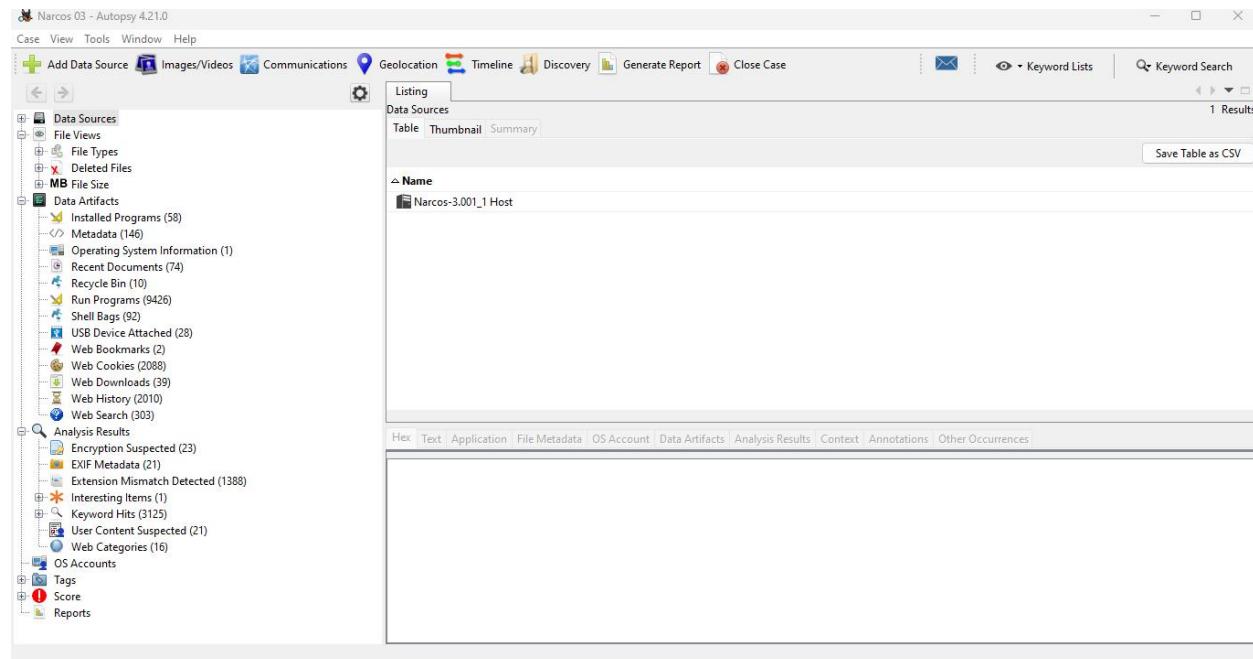


Figure 16 Autopsy

Registry Viewer:

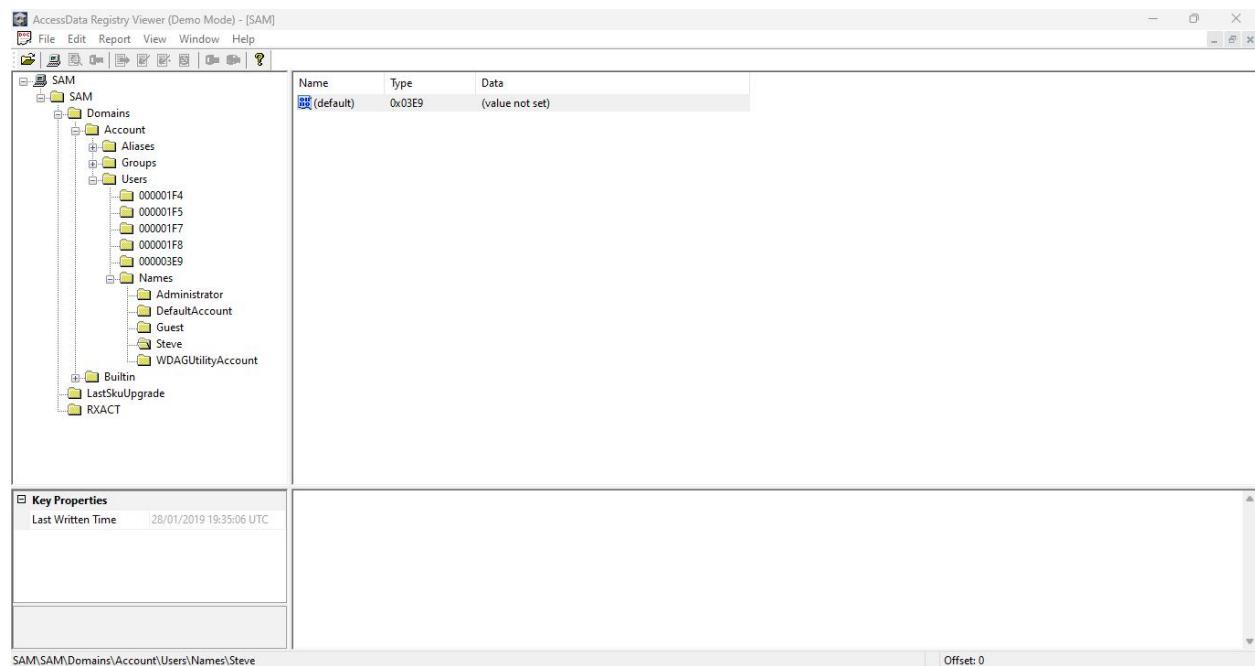


Figure 17 Registry Viewer

[SPACE INTENTIONALLY LEFT BLANK]

6. References

- Sleuth Kit. (n.d.). *Autopsy User Documentation 4.12.0*. Retrieved from <https://sleuthkit.org/autopsy/docs/user-docs/4.12.0/index.html>
- Williams, O. W. (n.d.). *Internet Browser Forensics with Autopsy*. LinkedIn. Retrieved from https://www.linkedin.com/pulse/internet-browser-forensics-autopsy-octavious-w--rq7be#:~:text=To%20view%20the%20data%20in,visits%2C%20keyword_search_terms%2C%20downloads
- Cyberspace Security. (2019, February 12). *Autopsy Internet History Analysis - Open-Source Digital Forensics*. [Video]. YouTube. <https://www.youtube.com/watch?v=wU5hHPuf1Lo>
- AccessData. (2012). *Registry Viewer User Guide*. Scribd. Retrieved from <https://www.scribd.com/document/144984450/Registry-Viewer-User-Guide>
- GeeksforGeeks. (n.d.). *Analysis of Data Source Using Autopsy*. Retrieved from <https://www.geeksforgeeks.org/analysis-of-data-source-using-autopsy/>
- GeeksforGeeks. (n.d.). *How to Create a Forensic Image with FTK Imager*. Retrieved from <https://www.geeksforgeeks.org/how-to-create-a-forensic-image-with-ftk-imager/>
- DFIRScience. (Feb 15, 2022). *Autopsy Tutorial for Windows - Digital Forensics* [Video]. YouTube. <https://www.youtube.com/watch?v=5SHB4HwkX28>

[END]