A COMPREHENSIVE FORENSIC CASE REPORT WITH THE UNIVERSITY OF SINGAPORE TEAM #6

UNIVERSITY OF SINGAPORE CASE #2: NARCOS

By

Investigator Name	Matric Number	Contact Information
Haziq Hakim Bin Abdul Rahman	A0216481H	e0540038@u.nus.edu
Musfirah Wani Bte Abdul Rahim	A0221404Y	e0556596@u.nus.edu
Ng Jong Ray, Edward	A0216695U	e0540252@u.nus.edu
Sim Ting Yu Emily	A0221094N	e0556286@u.nus.edu

April 2023

Contribution Details

All team members contributed equally to this case.

Table of Contents

1. Executive Summary

In this report, our forensics team will go through the provided evidence belonging to a suspect, Steve. In this case, we looked through all of the evidence which consists of the suspect's image file and memory dump. After a thorough analysis of the evidence provided, the team have come up with a hypothesis, in this case, John and Steve are guilty while we are unable to conclude the stance for Jane. In order to find out what exactly Jane's role is in this case, more information is needed to come to a concise conclusion and the truth for the case.

2. Objectives

2.1. Case Description

Jane Esteban and John Fredricksen are suspected by the Intel to be involved in illegal activity. Hence, their belongings were searched by customs officers. Upon searching John's suitcase, 1KG of drug identified as Methamphetamine was found in John's suitcase which led to both Jane and John being interrogated.

The interrogation revealed that the suitcase was meant to be delivered to "Eastbourne Library" and to "666 Rewera Avenue" as an alternative. Upon raiding the address, incriminating objects such as guns, drugs and a desktop computer were found. This desktop computer was seized and its drive image (Narcos-1) and memory dump (Narcos-Mem-1) was obtained and given to our team for further analysis.

2.2. Hypothesis

Upon analysing the evidence, we hypothesised that John Fredrickson and the suspect, Steve Kowhai are guilty of drug-related activities whereby Steve could possibly be a drug distributor and will contact John to buy new drugs to sell. Their future intention is to mix the drug substances with other components, hence increasing the amount of drugs to be distributed to the market.

3. Evidence Analysed

In the forensics investigation, the following evidence files were given to the team. The respective image and memory files were combined and then analysed for this case:

Evidence Number	Evidence Name	Hash Values (MD5)	Size
00	Narcos-Combined.img	c63a3d19e9c9495b573f45be544e50f9	30 GB
01	Narcos-Mem-Combined.raw	9ca08c17b4a359d61f6f8f7bb6328c1c	4 GB

4. Steps Taken

As the suspect's desktop computer drive image and memory dump was acquired by the customs officers and provided to us, it was not acquired by our team. Hence, we are not able to determine if the acquisition process is performed in a way that ensures the integrity of the data being collected.

Both the drive image and memory dump were split into multiple files, hence before conducting the investigation, the team combined the files using some commands and ensured the file integrity by checking the hash values provided by the other customs officers who provided the team with the evidence files.

The commands used are

1. copy /b Narcos-Mem-1.001+Narcos-Mem-1.002+Narcos-Mem-1.003 Narcos-Mem-Combined.raw
2. cat Narcos-1.* > Narcos-Combined.img

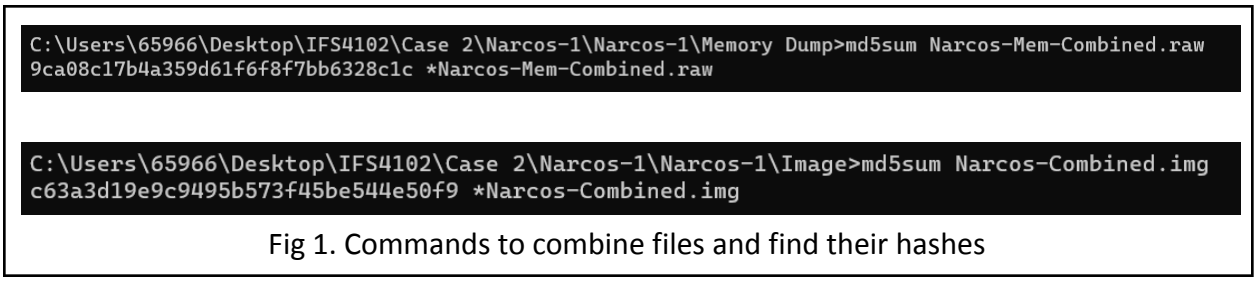


Fig 1. Commands to combine files and find their hashes

We computed the hash values of each of the files and created copies of them so that the team members would be able to analyse the evidence separately. To ensure the integrity of the

evidence, we conducted hash value checks every time we worked with the copied files, thus preventing any potential modification or compromise of the original data.

The following is a list of software tools that were used to analyse the evidence:

Software Used	Version Numbers
Autopsy	4.20.0
AccessData FTK Imager	4.7.1.2
Windows Registry Recovery x64 (WRR64)	3.1.1.0

Autopsy was mainly used to analyse the drive image file while FTKImager was used to analyse the memory dump file via running the strings command. It is noted that the Volatility tool was considered to be used on the memory dump file for analysis, however, the tool can't seem to be employed to analyse this memory dump file.

Additionally, based on the case description and looking through the evidence, we have come up with a keyword list to help us better identify and locate potentially relevant information. This keyword list is used in Autopsy to extract data that is relevant to the investigation:

Keyword List:

1. John
2. Jane
3. Drugs
4. Gun
5. Methamphetamine
6. Steganography
7. 666 Rewera Avenue
8. Eastbourne Library

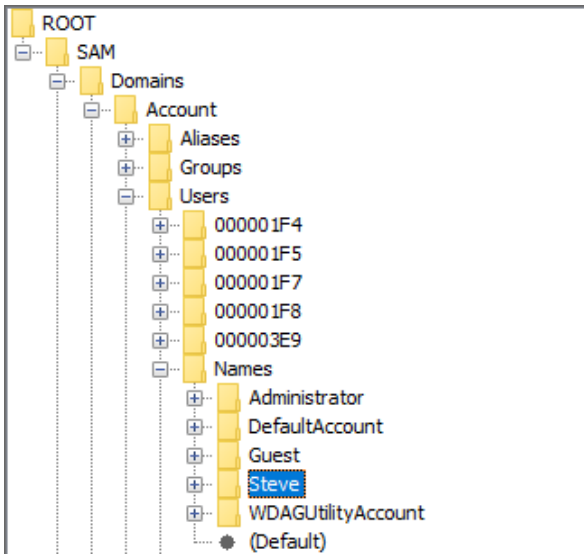
5. Relevant Findings

This section will examine and subsequently analyse the different evidence found by the team.

5.1. The Suspect

5.1.1. Name Of The Suspect

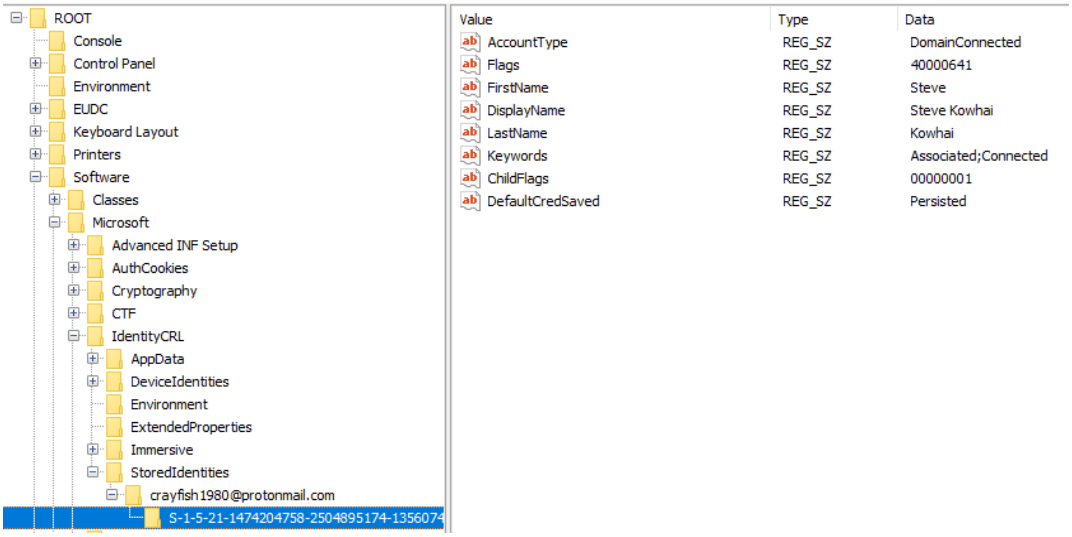
The given image (Evidence 00) and memory dump (Evidence 01) retrieved come from a suspect named Steve Kowhai. From the given image (Evidence 00), we are able to find the SAM registry hive from and from there we have found a key named “Steve”. Hence, we are able to determine that the evidence belongs to Steve.



/img_Narcos-1.001/vol_vol7/Windows/System32/config/SAM

Fig 2. Steve Key found in SAM Registry Hive

From the DEFAULT registry hive , we are also able to find the value “Display Name” with the corresponding data “Steve Kowhai” from the key. Furthermore, we performed a dual-tool technique to ensure that our findings are consistent. We used WRR64 and managed to obtain the same finding:



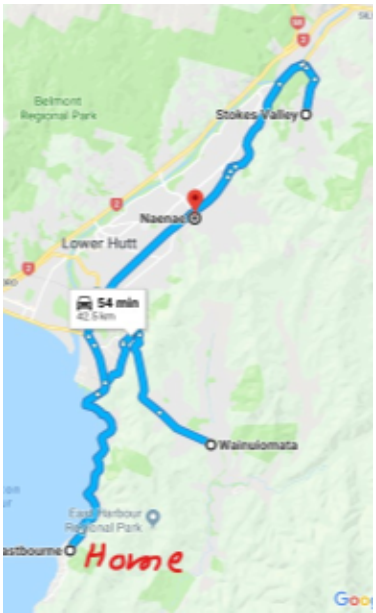
/img_Narcos-1.001/vol_vol7/Windows/System32/config/DEFAULT

Fig 3. Display name Steve Kowhai found in DEFAULT registry hive

From this information, we are able to determine that the suspect is called Steve Kowhai.

5.1.2. Where Does The Suspect Stay

Steve Kohwai seems to be currently staying in New Zealand. From the given image (Evidence 00), a picture named “Method run.jpg” was found under Steve’s personal “Documents” folder. The word “Home” was handwritten onto the image near Eastbourne.



/img_Narcos-1/vol_vol7/Users/Steve/Documents/Misc

Fig 4. Handwritten word home on a google maps route

Moreover, from the interrogation, we know that Steve wanted the initial dropoff point for drug collection to be Eastbourne Library. These 2 key pieces of information, when taken together, strongly indicate that Steve stays in Eastbourne, New Zealand.

5.1.3. What Does The Suspect Do

Steve has a multitude of drug-related searches in his web browsing history. Ranging from "What is Methamphetamine" to "drug paraphernalia". Moreover, Steve has downloaded images regarding recent drug busts. With this knowledge, we can know that Steve could have conducted activities closely related to the drugs industry, be it either consuming or selling.

History			2	https://www.google.com/search?q=crystal+meth&oq=cry...	2019-01-31 10:56:07 SGT	https://www.google.com/search?q=crystal+meth&oq=cry...	crystal meth - Google Search	Google Chrome	google.com
History			2	https://www.drugfreeworld.org/drugfacts/crystalmeth.html	2019-01-31 10:55:01 SGT	https://www.drugfreeworld.org/drugfacts/crystalmeth.html	What is Methamphetamine? What is Crystal Meth? How is ...	Google Chrome	drugfreeworld.org
History	History		2	https://www.drugfreeworld.org/drugfacts/crystalmeth.html	2019-01-31 10:55:01 SGT	https://www.drugfreeworld.org/drugfacts/crystalmeth.html	What is Methamphetamine? What is Crystal Meth? How is ...	Google Chrome	drugfreeworld.org
History			2	https://www.google.com/search?q=crystal+meth&oq=cry...	2019-01-31 10:56:07 SGT	https://www.google.com/search?q=crystal+meth&oq=cry...	crystal meth - Google Search	Google Chrome	google.com
History			2	https://www.google.com/search?q=crystal+meth&source...	2019-01-31 10:56:24 SGT	https://www.google.com/search?q=crystal+meth&source...	crystal meth - Google Search	Google Chrome	google.com
History			2	https://www.google.com/search?q=crystal+meth&source...	2019-01-31 10:56:24 SGT	https://www.google.com/search?q=crystal+meth&source...	crystal meth - Google Search	Google Chrome	google.com
History			2	https://www.google.com/search?q=crystal+meth&source...	2019-01-31 10:56:24 SGT	https://www.google.com/search?q=crystal+meth&source...	crystal meth - Google Search	Google Chrome	google.com
History			2	https://www.google.com/search?q=crystal+meth&source...	2019-01-31 10:56:30 SGT	https://www.google.com/search?q=crystal+meth&source...	crystal meth - Google Search	Google Chrome	google.com
History			2	https://www.google.com/search?q=crystal+meth&source...	2019-01-31 10:56:33 SGT	https://www.google.com/search?q=crystal+meth&source...	crystal meth - Google Search	Google Chrome	google.com

/img_Narcos-1.001/vol_vol7/Users/Steve/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat

"/img_Nacros-Combined.img/vol_vol7/$Recycle.Bin/S-1-5-21-1474204758-2504895174-135607821-1001"

Fig 5. Steve's Google searches for "Crystal Meth" and downloaded images of drug bust

History			2	https://www.google.com/search?q=drug+paraphernalia&o...	2019-01-31 10:57:16 SGT	https://www.google.com/search?q=drug+paraphernalia&o...	drug paraphernalia - Google Search	Google Chrome	google.com
History			2	https://www.google.com/search?q=drug+paraphernalia&s...	2019-01-31 10:57:21 SGT	https://www.google.com/search?q=drug+paraphernalia&s...	drug paraphernalia - Google Search	Google Chrome	google.com
History			2	https://www.google.com/search?q=drug+paraphernalia&s...	2019-01-31 10:57:21 SGT	https://www.google.com/search?q=drug+paraphernalia&s...	drug paraphernalia - Google Search	Google Chrome	google.com
History			2	https://www.google.com/search?q=drug+paraphernalia&s...	2019-01-31 10:57:21 SGT	https://www.google.com/search?q=drug+paraphernalia&s...	drug paraphernalia - Google Search	Google Chrome	google.com
History			2	https://www.google.com/search?q=drug+paraphernalia&s...	2019-01-31 10:57:26 SGT	https://www.google.com/search?q=drug+paraphernalia&s...	drug paraphernalia - Google Search	Google Chrome	google.com
History			2	https://www.google.com/search?q=drug+paraphernalia&s...	2019-01-31 10:57:30 SGT	https://www.google.com/search?q=drug+paraphernalia&s...	drug paraphernalia - Google Search	Google Chrome	google.com
History			2	https://www.google.com/search?q=drug+paraphernalia&s...	2019-01-31 10:57:37 SGT	https://www.google.com/search?q=drug+paraphernalia&s...	drug paraphernalia - Google Search	Google Chrome	google.com
History			2	https://www.google.com/search?biw=1916&bih=767&tbm...	2019-01-31 10:57:50 SGT	https://www.google.com/search?biw=1916&bih=767&tbm...	drug paraphernalia meth - Google Search	Google Chrome	google.com
History			2	https://www.google.com/search?biw=1916&bih=767&tbm...	2019-01-31 10:57:50 SGT	https://www.google.com/search?biw=1916&bih=767&tbm...	drug paraphernalia meth - Google Search	Google Chrome	google.com
History			2	https://www.google.com/search?biw=1916&bih=767&tbm...	2019-01-31 10:57:50 SGT	https://www.google.com/search?biw=1916&bih=767&tbm...	drug paraphernalia meth - Google Search	Google Chrome	google.com
History			2	https://www.google.com/search?biw=1916&bih=767&tbm...	2019-01-31 10:58:03 SGT	https://www.google.com/search?biw=1916&bih=767&tbm...	drug paraphernalia meth - Google Search	Google Chrome	google.com

/img_Narcos-1.001/vol_vol7/Users/Steve/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat

/img_Narcos-1.001/vol_vol7/Users/Steve/AppData/Local/Google/Chrome/User Data/Default/Cache/data_3/

Fig 6. Steve's Google searches for "drug paraphernalia" stored in his web's history and cache

In Steve's web browser history, we are also able to find multiple searches relating to "cutting drugs". Drug cutting is the practice of diluting the purity of illicit drugs with other adulterants such as aspirin or even coffee powder. Drug cutting is typically done by drug dealers to bulk up the original drug, allowing them to earn more profits.

WebCacheV		2	https://www.google.com/search?source=hp&ei=JolPXNbGA82_rQHw06rICw&q=cutting+drugs&btnK=Google+Search&oq...	2019-01-28 22:58:52 SGT
WebCacheV		2	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=2ahUKEwi0vtT2yZHgAhX...	2019-01-28 22:59:04 SGT
WebCacheV		1	https://en.wikipedia.org/wiki/Cutting_agent	2019-01-28 22:59:05 SGT
WebCacheV		1	https://en.wikipedia.org/	2019-01-28 22:59:04 SGT
WebCacheV		2	https://www.google.com/search?q=cutting+drugs&source=lnms&tbm=vid&sa=X&ved=0ahUKEwi0vtT2yZHgAhXaTn0KHTf...	2019-01-28 22:59:54 SGT
WebCacheV		2	https://www.google.com/search?q=cutting+drugs&tbm=isch&source=lnms&sa=X&ved=0ahUKEwjtmYKUypHgAhXUeX0KH...	2019-01-28 23:00:21 SGT
WebCacheV		2	https://www.google.com/search?q=cutting+drugs&source=lnms&sa=X&ved=0ahUKEwjy3dWgypHgAhWCeysKHVJfDXkQ_...	2019-01-28 23:00:22 SGT
WebCacheV		2	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=2ahUKEwi0vtT2yZHgAhX...	2019-01-28 23:00:38 SGT
WebCacheV		1	https://sunrisehouse.com/cause-effect/cutting-agents-drug-manufacturing/	2019-01-28 23:00:41 SGT
WebCacheV		1	https://sunrisehouse.com/	2019-01-28 23:00:38 SGT
WebCacheV		2	https://www.google.com/search?ei=LIlPXLT4Bdqd9QO3sq-4AQ&q=cutting+agents+for+ice&oq=cutting+drugs&gs_l=psy-...	2019-01-28 23:02:00 SGT

/img_Narcos-1.001/vol_vol7/Users/Steve/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat

Fig 7. Recent web searches relating to "Cutting drugs"

In addition to learning about the act of cutting drugs, Steve had recent searches regarding Money Laundering. Money Laundering is the illegal practice of concealing the origin of money obtained from illicit activities such as selling drugs. This can be done by converting it through a legitimate source and thus obtaining the "cleaned money".

WebCacheV		2	https://www.google.com/search?ei=6IlPXJ6AF8TJrQHt7bWABQ&q=how+to+launder+money&oq=how+to+launder+money&gs_l=psy-ab.3...106593...	2019-01-28 23:03:51 SGT
WebCacheV		2	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=2ahUKEwiMiKCFy5HgAhUPTn0KHZ66CfcQFjACegQI...	2019-01-28 23:03:57 SGT
WebCacheV		1	https://www.businessinsider.com.au/beginners-guide-to-money-laundering-2014-10?r=US&IR=T	2019-01-28 23:03:57 SGT
WebCacheV		1	https://www.businessinsider.com.au/	2019-01-28 23:03:57 SGT
WebCacheV		2	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=13&cad=rja&uact=8&ved=2ahUKEwiMiKCFy5HgAhUPTn0KHZ66CfcQFjAMegQ...	2019-01-28 23:04:00 SGT
WebCacheV		1	https://en.wikipedia.org/wiki/Money_laundering	2019-01-28 23:04:01 SGT

/img_Narcos-1.001/vol_vol7/Users/Steve/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat

Fig 8. Recent web searches relating to “Money Laundering”

Moreover, Steve has had a recent search for New Zealand drug gangs. The image below, which was downloaded after his Google search, was recovered from his computer image (Evidence 00).

History	2	https://www.google.com/search?q=gangs+nz+drugs&oq...	2019-01-31 10:59:17 SGT	https://www.google.com/search?q=gangs+nz+drugs&oq...	gangs nz drugs - Google Search	Google Chrome	google.com	C
History	2	https://www.google.com/search?q=gangs+nz+drugs&sou...	2019-01-31 10:59:32 SGT	https://www.google.com/search?q=gangs+nz+drugs&sou...	gangs nz drugs - Google Search	Google Chrome	google.com	C
History	2	https://www.google.com/search?q=gangs+nz+drugs&sou...	2019-01-31 10:59:32 SGT	https://www.google.com/search?q=gangs+nz+drugs&sou...	gangs nz drugs - Google Search	Google Chrome	google.com	C
History	2	https://www.google.com/search?q=gangs+nz+drugs&sou...	2019-01-31 10:59:32 SGT	https://www.google.com/search?q=gangs+nz+drugs&sou...	gangs nz drugs - Google Search	Google Chrome	google.com	C

/img_Narcos-1.001/vol_vol7/Users/Steve/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat

/img_Narcos-1.001/vol_vol7/Users/Steve/Pictures/eight_col_patches_crp.jpg

Fig 9. Search history and downloaded image regarding “NZ gangs”

Our team has also found evidence of Steve downloading software which can help evade digital forensic techniques. The softwares are CCleaner v5.52, TrueCrypt v.6.1a and Image Steganography 1.5.2. Below are the descriptions of the software:

Software	Description
CCleaner	This software is a system cleaner used to help clean or remove unwanted files and even unwanted Windows Registry values. Using CCleaner allows an individual to securely remove files, web history and registry values.
TrueCrypt	This software is used to create a virtual encrypted disk within a file, or encrypt a partition or the whole storage device. Using TrueCrypt supports a concept known as plausible deniability. This concept is the ability to deny knowledge or responsibility for an action that has occurred, typically by another person. TrueCrypt can support claims

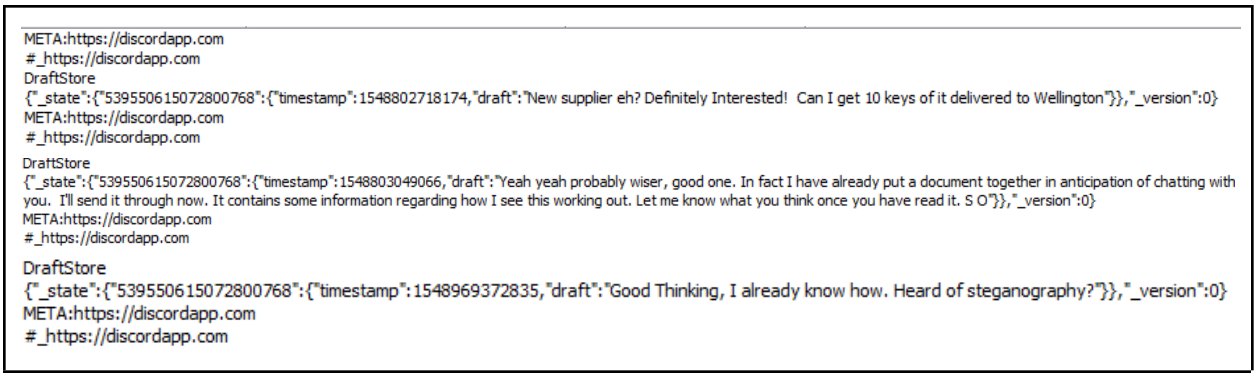
	to plausible deniability by aiding a single "hidden volume" to be created within another volume (TrueCrypt, 2015).
Image Steganography	This software is used to help apply image steganography techniques onto a chosen image. Image Steganography is the practice of concealing and obfuscating data within an image in a way that it is not visibly altered (Great Learning, n.d.). Using image steganography can help covertly pass a message to the recipient as anyone other than the intended recipient would not suspect that the image contains information.

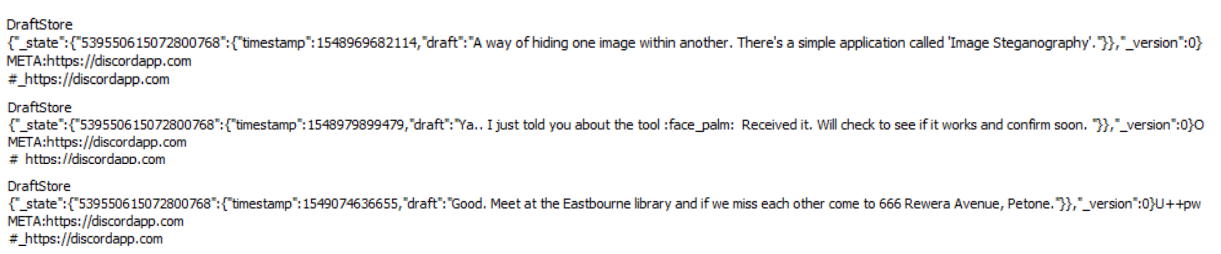
With the above evidence, we have strong evidence to believe that Steve Kohwai is an **experienced New Zealander drug dealer**. Evidence relating to his searches on cutting drugs and money laundering are signs that Steve is a drug dealer instead of a drug consumer as these actions are about manipulating drug products to be sold and how to “clean” his profits. Moreover, Steve’s knowledge about digital forensics software could indicate that he is experienced. His knowledge of covert ways to send information through Image Steganography, as well as knowing about software to encrypt his disk image and secure deleting of his files and registry, indicates that Steve puts in the effort to evade detection.

5.2. The Trip

5.2.1. Communication

The team have found that Steve and John might have communicated via the Discord application. We found evidence of communications in a Discord log file and also a file we carved using Autopsy.

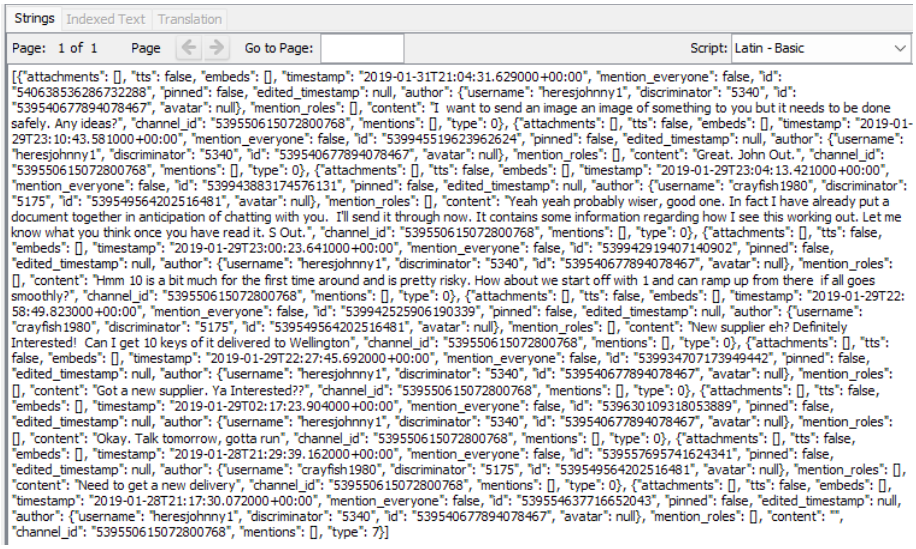




/img_Nacros-Combined.img/vol_vol7/Users/Steve/AppData/Roaming/Discord/Local Storage/leveldb/00000006.log

Fig 10. Steve's draft messages were captured on Discord logs

Since the above texts are found under the draft entry in DraftStore, these text messages suggest that it is a partial conversation and we were only able to observe Steve's response.



/img_Nacros-Combined.img/vol_vol7/$CarvedFiles/1/f0644226.gz

Fig 11. Carved text messages between John and Steve

However, the carved file found shows the conversation between Steve and John, giving our team high confidence that he has indeed sent out these messages. By combining both pieces of evidence, we are able to piece together the conversation between Steve and John. The content matches Jane's confession. The time stated is in UTC format and the extracted messages are the exact messages exchanged between John and Steve.

Steve (January 28, 2019, 9:29 PM): Need to get a new delivery

John (January 29, 2019, 5:23 PM): Okay. Talk tomorrow, gotta run

John(January 29, 2019, 10:27 PM): Got a new supplier. Ya Interested??

Steve(January 29, 2019, 10:58 PM): New supplier eh? Definitely Interested! Can I get 10 keys of it delivered to Wellington

John (January 29, 2019, 11:00 PM): Hmm 10 is a bit much for the first time around and is pretty risky. How about we start off with 1 and can ramp up from there if all goes smoothly?

Steve (January 29, 2019, 11:04 PM): 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 Out.

John (January 29, 2019, 11:10 PM): Great. John Out.

John (January 31, 2019, 9:04 PM): I want to send an image an image of something to you but it needs to be done safely. Any ideas?

Steve (January 31, 2019, 9:16 PM): Good Thinking, I already know how. Heard of steganography?

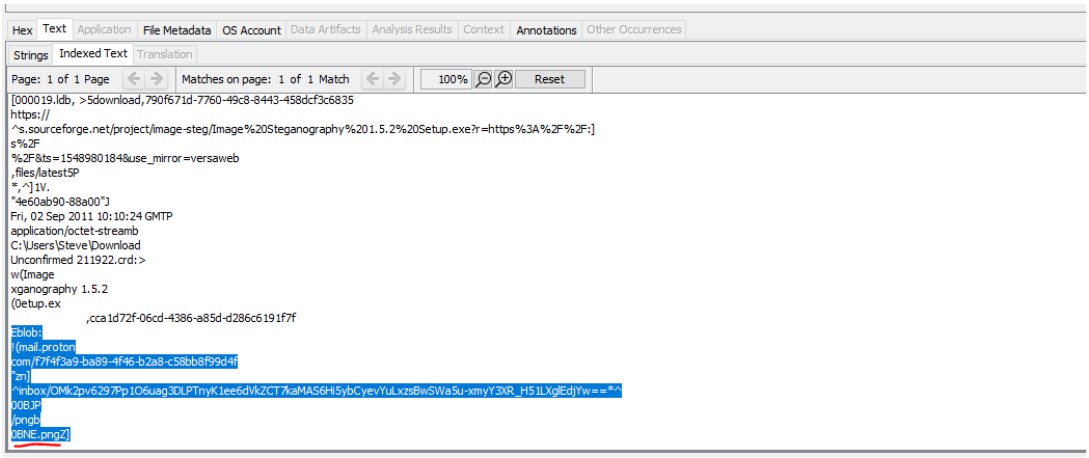
Steve (January 31, 2019, 9:21 PM): A way of hiding one image within another image. There's a simple application called 'Image Steganography'.

Steve (February 1, 2019, 12:11 AM): Ya.. I just told you about the tool :face_palm: Received it. Will check if it works and confirm soon.

Steve (February 2, 2019, 2:30 AM): Good. Meet at the Eastbourne library and if we miss each other come to 666 Rewera Avenue, Petone.

The text messages imply that Steve (crayfish1980) is getting drugs from John (heresjohnny1) and wanted them to be delivered to New Zealand, after which, they either meet at Eastbourne Library or 666 Rewera Avenue. It is also revealed that Steve has some basic knowledge of digital forensics (Steganography) and had suggested the tool to his partner, John for communication purposes.

John had made use of image steganography to create an image and later sent it to Steve via email. We found that Steve had downloaded a suspicious image (BNE.png) from his protonmail that fits within this timeframe:



/img_Nacros-Combined.img/vol_vol7/Users/Steve/AppData/Local/Google/Chrome/User Data/Default/000019.ldb

Fig 12. BNE image file downloaded from protonmail

Upon analysing the image file (BNE.png), we found that the image file is compressed. Thus, we suspect that there might be other files hidden inside this image file. By looking at the hex of the file (using CyberChef), we are able to find some other file header signatures.

/img_Nacros-Combined.img/vol_vol7/Users/Steve/Downloads/Misc/BNE.png

Fig 13. BNE image file used for steganography

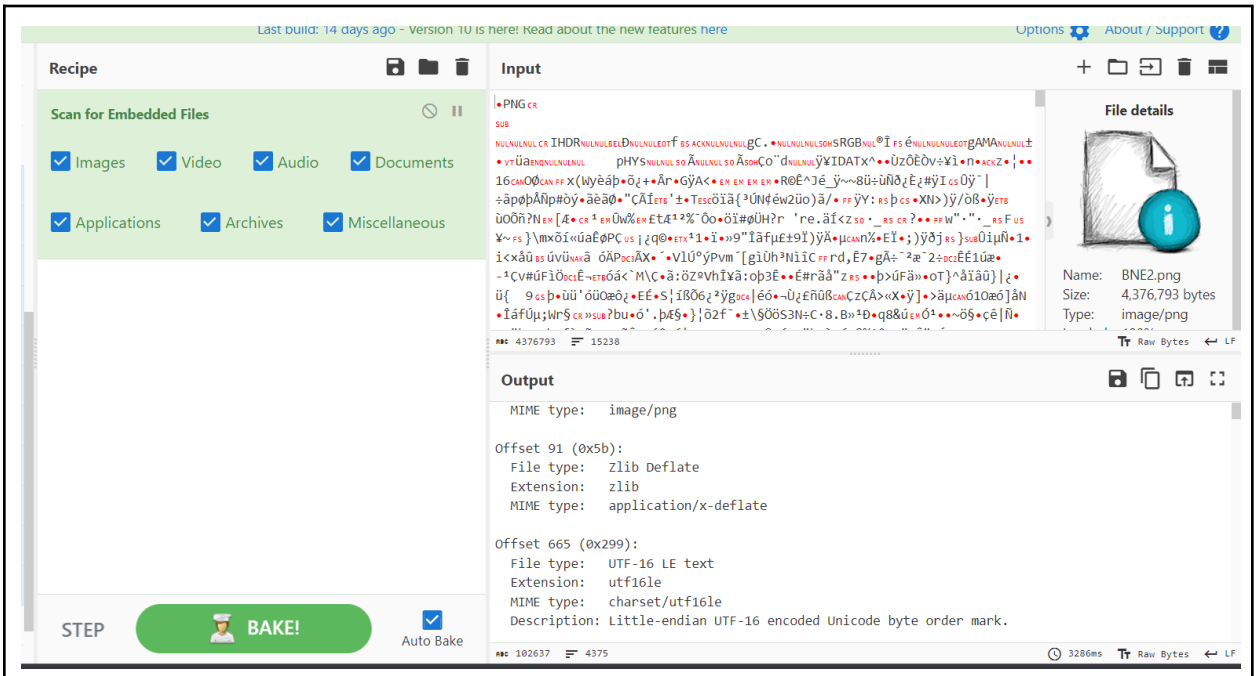


Fig 14. Proof that BNE.png has embedded files within itself

Furthermore, we performed a dual-tool technique to ensure that our findings are consistent. We used Binwalk, a tool to search images for embedded files, and managed to obtain similar findings that BNE.png has another file embedded in it:

```
nnythingy@Nnythingy:/mnt/c/Users/ngjon/Desktop$ binwalk BNE.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 2000 x 1126, 8-bit/color RGBA, non-interlaced
91            0x5B            Zlib compressed data, compressed
```

Fig 15. The output of running Binwalk on BNE.png

Running the command *"Binwalk -Mre BNE.png"*, we are then able to extract both the PNG image and the Zlib compressed data. However, after decompressing the Zlib file, we are unable to comprehend or extract any further information.

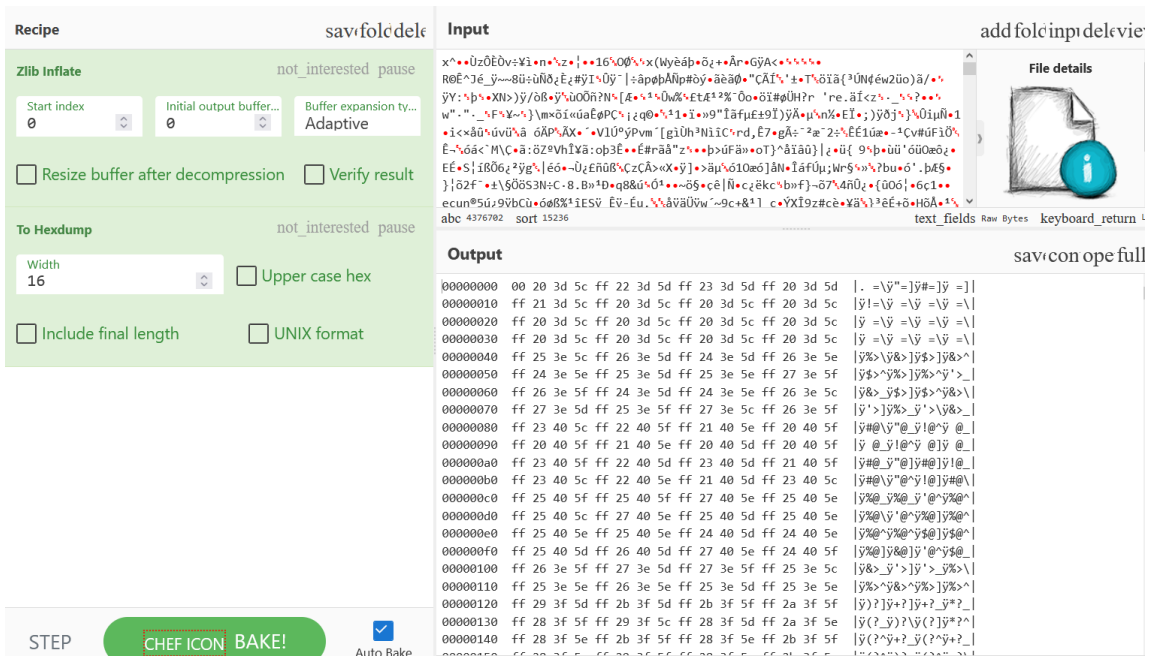
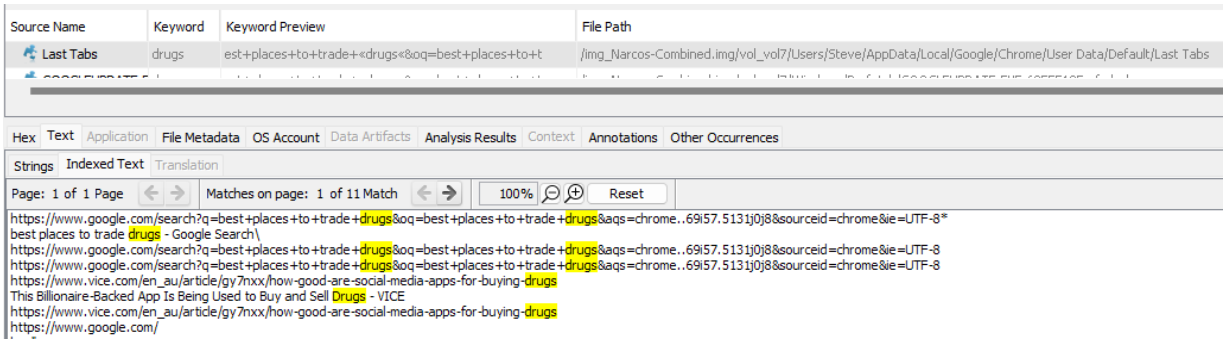


Fig 16. The content of the decompressed Zlib file

Lastly, the text messages also indicate the initial meeting point was set to be at “Eastbourne Library” and the alternative location is “666 Rewera Avenue, Petone”. This information corresponds to Janes’ confession during the interrogation.

5.2.2. Destination Selection

Upon conducting a keyword search for "drugs", we discovered that Steve had performed a Google search for "best places to trade drugs", indicating that he had carefully planned the meeting with John for dealing drugs at a specific location. This relevant information contained details of the last set of tabs open in Steve's Google Chrome browser.



/img_Nacros-Combined.img/vol_vol7/Users/Steve/AppData/Local/Google/Chrome/User Data/Default/Last Tabs

Fig 17. Steve searched for places to trade drugs

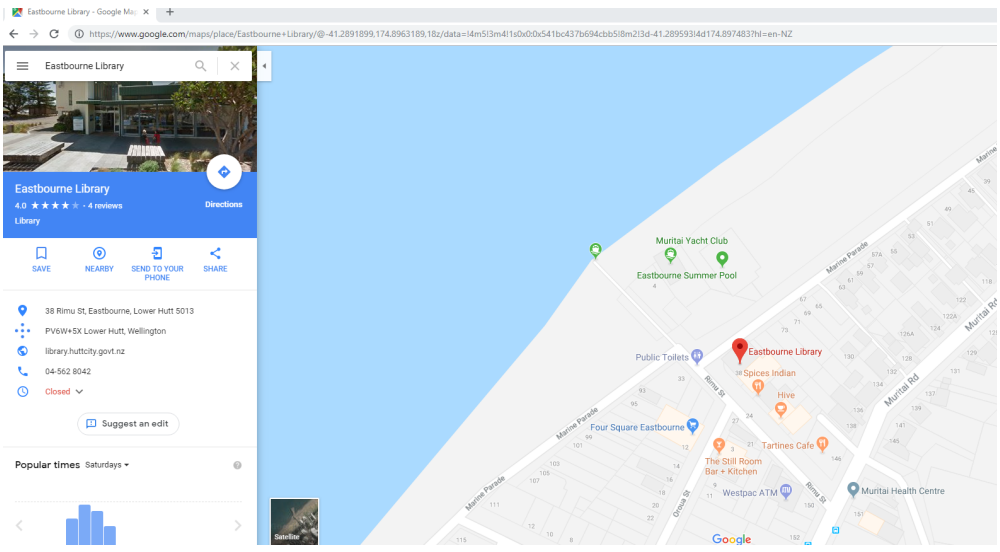
Looking through Steve's web search history, revealed more evidence of him planning for the meeting.

History	google.com	best places to trade drugs	Google Chrome	2019-02-02 09:01:34 SGT	Narcos-Combined.img
History	google.com	best places to trade drugs	Google Chrome	2019-02-02 09:01:34 SGT	Narcos-Combined.img
History	google.com	best places to trade drugs	Google Chrome	2019-02-02 09:01:34 SGT	Narcos-Combined.img
History	google.com	wellington libraries	Google Chrome	2019-02-02 09:01:51 SGT	Narcos-Combined.img
History	google.com	courteney place	Google Chrome	2019-02-02 09:02:51 SGT	Narcos-Combined.img
History	google.com	eastbourne library	Google Chrome	2019-02-02 09:04:36 SGT	Narcos-Combined.img
History	google.com	eastbourne	Google Chrome	2019-02-02 09:05:05 SGT	Narcos-Combined.img
History	google.com	eastbourne library	Google Chrome	2019-02-02 09:05:11 SGT	Narcos-Combined.img
WebCacheV01.dat	google.co.nz	drug routes in wellington	Microsoft Edge Analyzer	2019-01-29 01:02:39 SGT	Narcos-Combined.img
WebCacheV01.dat	google.co.nz	drug routes in wellington	Microsoft Edge Analyzer	2019-01-29 01:02:52 SGT	Narcos-Combined.img
WebCacheV01.dat	google.co.nz	drug routes in around wellington	Microsoft Edge Analyzer	2019-01-29 01:03:42 SGT	Narcos-Combined.img
WebCacheV01.dat	google.co.nz	drug routes in around wellington	Microsoft Edge Analyzer	2019-01-29 01:03:47 SGT	Narcos-Combined.img
WebCacheV01.dat	google.co.nz	international drug routes	Microsoft Edge Analyzer	2019-01-29 01:04:12 SGT	Narcos-Combined.img
WebCacheV01.dat	google.co.nz	international drug routes	Microsoft Edge Analyzer	2019-01-29 01:04:16 SGT	Narcos-Combined.img

Fig 18. Steve's Web History and Search

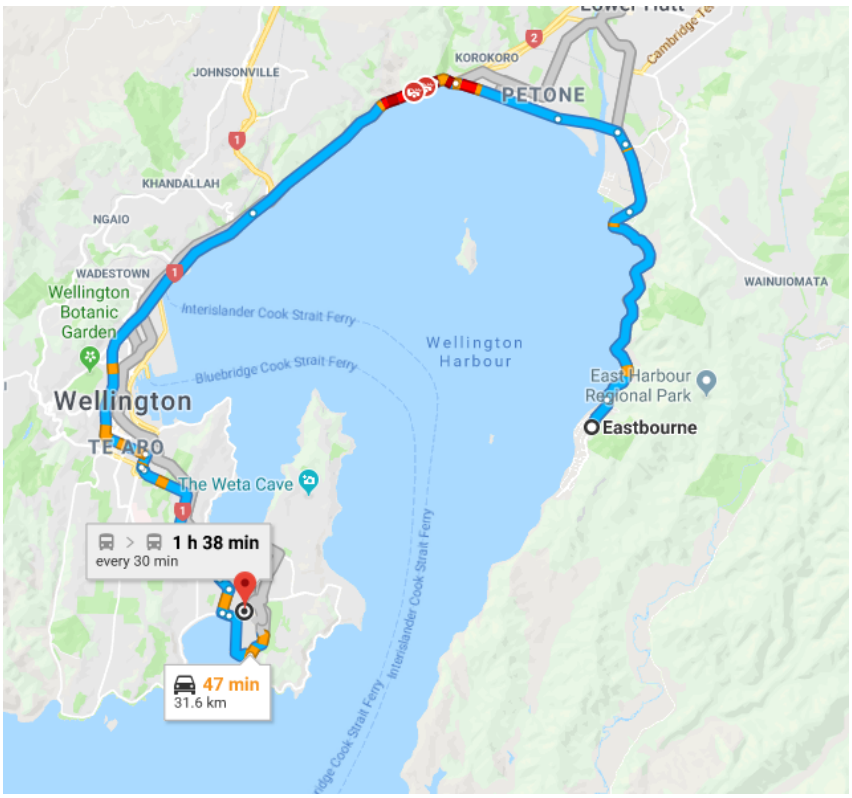
This provides further support to the notion that Steve had pre-planned the drug transaction with John.

In addition, we have discovered route images located in Steve's "Documents/Misc" folder. These images are named in a way that indicates their purpose, providing further insight into the nature of the routes being planned.



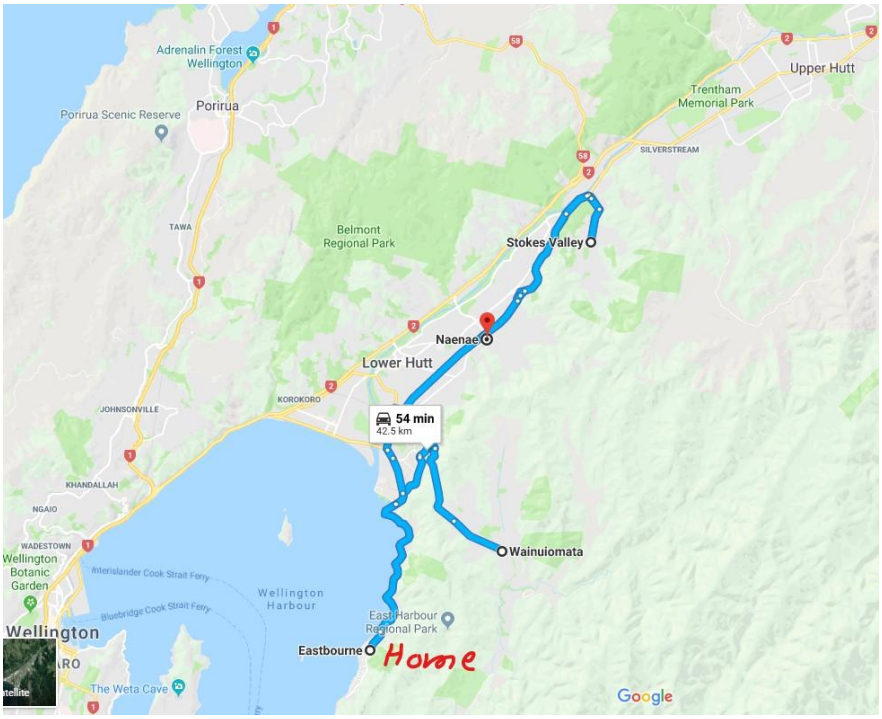
/img_Narcos-Combined.img/vol_vol7/Users/Steve/Documents/Misc/dropoff.jpg

Fig 19. dropoff.jpg



/img_Narcos-Combined.img/vol_vol7/Users/Steve/Documents/Misc/airport crystal.jpg

Fig 20. airport crystal.jpg



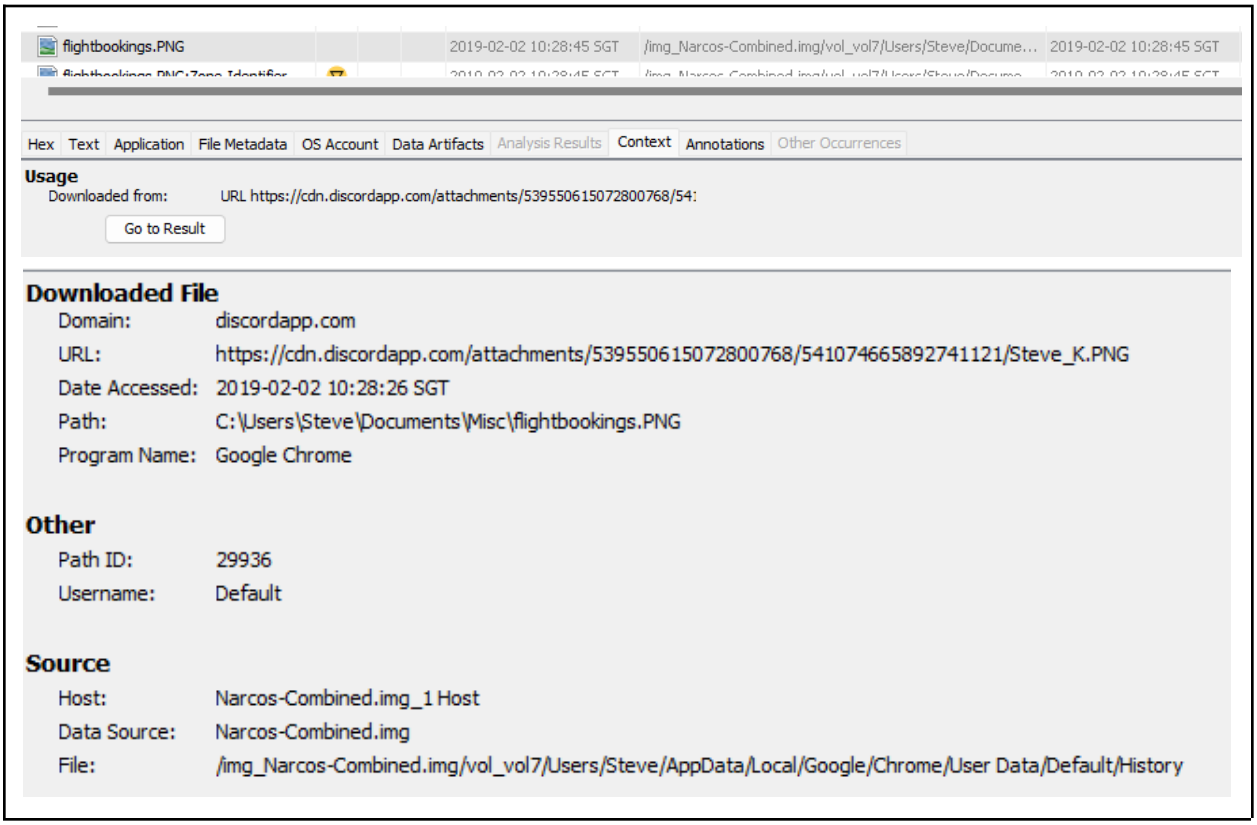
/img_Narcos-Combined.img/vol_vol7/Users/Steve/Documents/Misc/Method run.jpg

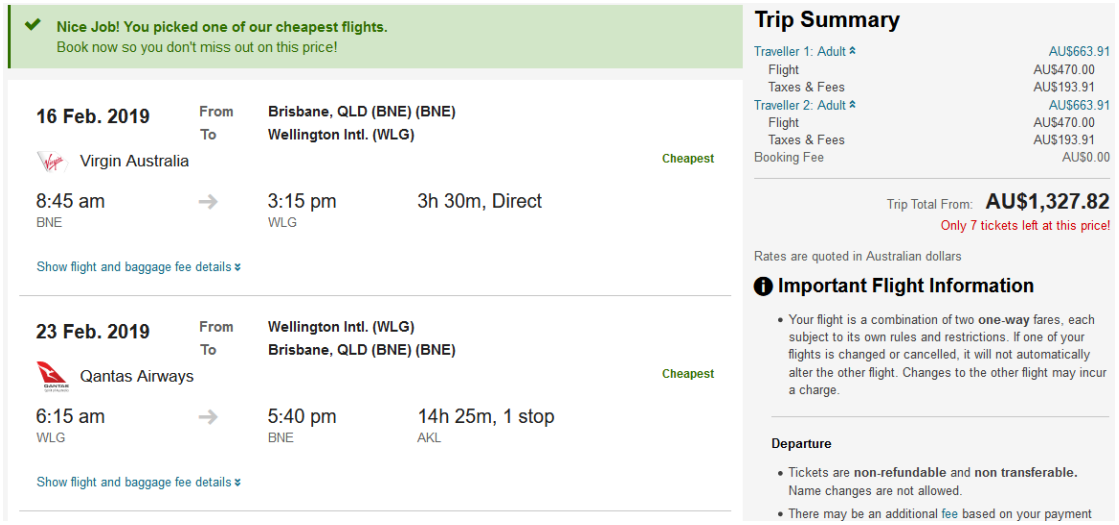
Fig 21. Method run.jpg

The image file named "dropoff.jpg" (Fig 19) reveals the predetermined meeting place at the Eastbourne library which was revealed in the conversation between Steve and John. "airport crystal.jpg" (Fig 20) indicates the estimated arrival time for John to reach the meeting point from the airport. Lastly, the file "Method run.jpg" (Fig 21) suggests the possible route Steve would take after receiving the drugs from John.

5.2.3. Flight Details

We noticed that flight booking details were stored on Steve's computer, which appeared to have been downloaded from Discord. This implies that it is likely that the details were sent during John and Steve's conversation, as the download timestamp of the image is just a few minutes after Steve's last message in Discord, on February 2, 2019, at 2:28 AM.





/img_Narcos-Combined.img/vol_vol7/Users/Steve/Documents/Misc/flightbookings.PNG

Fig 22. flightbookings.PNG

With the flight schedule information, Steve can plan his meeting and drug deal more effectively and accurately to minimise the risk of getting caught.

5.2.4. Purpose

Steve and John are probably involved in an illicit drug transaction. The previous section's analysis implies that Steve had planned the trip with the intention of purchasing drugs from John, who is the dealer.

5.3. Future Plans and Intention

Based on the above evidence in Section 5.2.1, we can see that their communication on Discord has revealed that Steve had the initial intention of buying "10 keys". After this current trip of only 1 key, if "all goes smoothly", John will attempt to bring more for Steve to sell.

Meanwhile, Steve has plans to choose his preferred Cutting Agents to mix with the new drug John will be bringing in, for the purpose of selling them, as explained in Section 5.1.3.

5.4. Role Of John

Our team's hypothesis is that John could be a middleman to purchase and bring drugs from presumably Brisbane, Australia. Steve will contact John to bring drugs from Australia to New Zealand for Steve to sell. John will then contact the drug suppliers and deliver the drugs from them to Steve at the designated dropoff point. Moreover, based on their communication in Section 5.2.1, they might have already been acquainted with each other and possibly have done some type of drug trafficking together in the past.

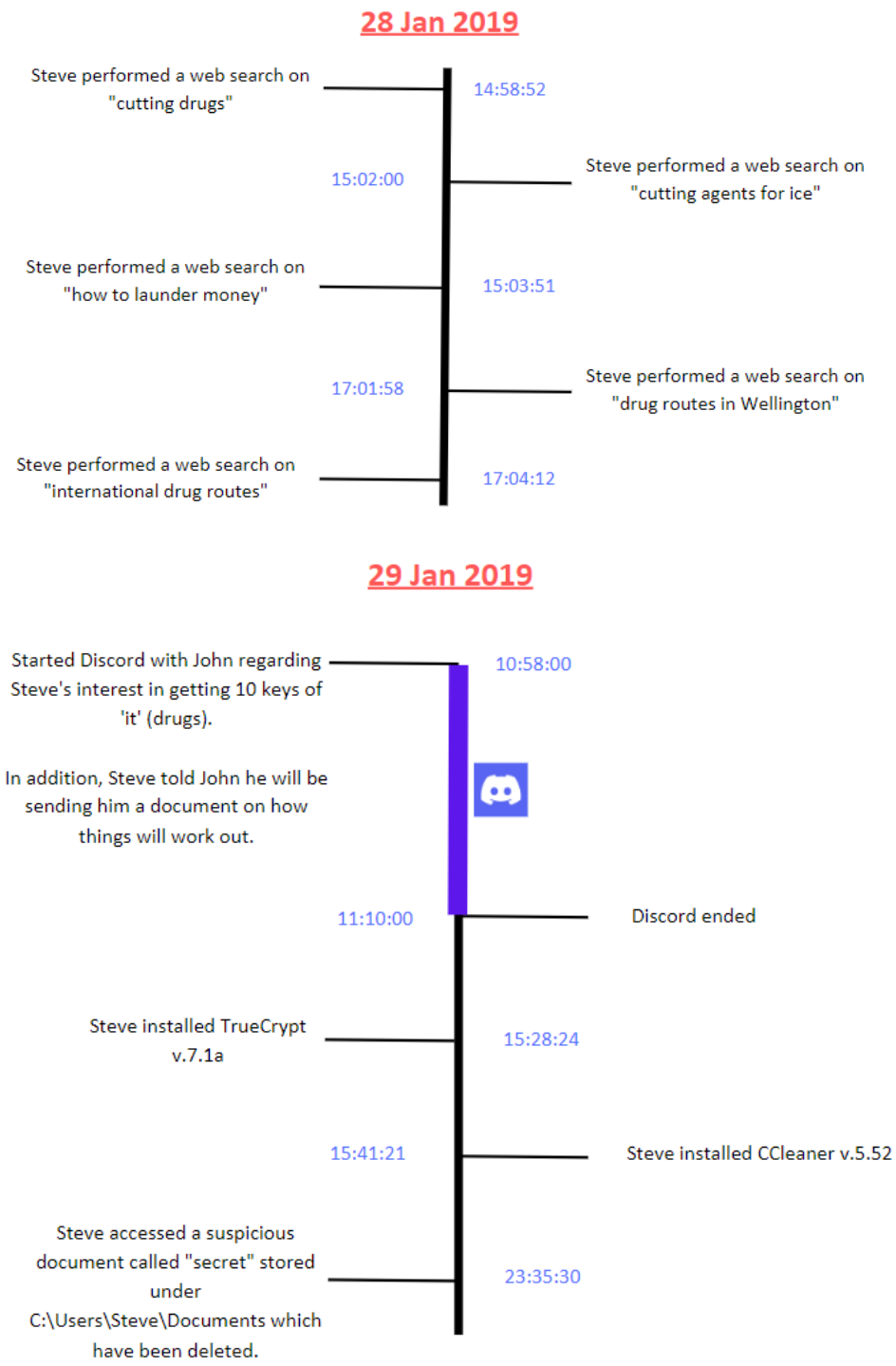
5.5. Role Of Jane

From both Evidence 00 and Evidence 01, we are unable to find substantial evidence which could imply the role of Jane Esteban.

However, as previously discussed in Section 5.2.3, the flight booking (Fig 22) was for 2 adults, which from the case could be for both John and Jane. Moreover, as stated in the case description, Jane was quick to give up the information told to her by John. Hence, this leads our team to conclude that Jane could be helping John. Her presence could possibly help make them both look less suspicious at the airport.

6. Timeline

The timeline of events in UTC time is shown below and the activities are split by their dates:



30 Jan 2019

Edited a relevant image with ScreenSketch on the routes to Eastbourne. Image name is "**Method run.jpg**", stored under C:\Users\Steve\Documents\Misc — 21:20:52

21:25:18 — Edited another relevant image on routes called "**airport crystals.jpg**" stored under C:\Users\Steve\Documents\Misc

31 Jan 2019

Steve performed a web search on "crystal meth" — 02:56:07

02:56:56 — Downloaded a drug image called "**620x349.jpg**" which is stored at C:\Users\Steve\Pictures

Moved "620x349.jpg" to the Recycle Bin. — 02:57:04

02:57:16 — Steve performed a web search on "drug paraphernalia". Some images stored in web cache.

Performed a web search on "drug paraphernalia meth" and downloaded an image called "price-meth-bust-4.jpg" stored at C:\Users\Steve\Pictures and deleted it. — 02:57:50

02:59:17 — Performed a web search on "gang nz drugs" and downloaded an image called "eight_col_patches_crp.jpg" stored at C:\Users\Steve\Pictures

1TB drive called "Seagate RSS LLC" attached to Steve's desktop. — 03:04:08

21:21:00 — Started Discord with John whereby Steve recommended the image steganography to John.

1 Feb 2019

00:11:00 — Started Discord with John whereby Steve received something from John as "Received it" text was seen.

00:13:19 — Download of suspicious "**BNE.png**" from Steve's mail (protonmail). File stored at C:\Users\Steve\Downloads\Misc

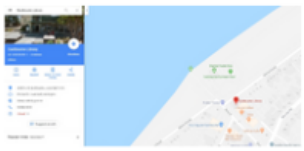
00:15:04 — Steve performed a web search on "Image Steganography"

00:16:32 — Downloaded Image Steganography tool from Sourceforge.net and ran it.

02:49:18 — Accessed a file called "**package.jpg**" stored at C:\Users\Steve\Downloads\Misc which has been deleted already.

2 Feb 2019

01:06:05 — Accessed an image called "**dropoff.jpg**" stored at C:\Users\Steve\Documents\Misc. This is a route image to Eastbourne library.



02:28:16 — Steve accessed an attachment from discord, "Steve_K.PNG".

This is a flight booking ticket that is also found in his own desktop called "**flightbookings.PNG**" stored at C:\Users\Steve\Documents\Misc

02:28:44 — Accessed "**flightbookings.PNG**"

02:30:00 — Discord communication with John started whereby Steve mentioned about meeting at Eastbourne Library or at 666 Rewera as an alternative.

7. Other Diagrams

7.1. Relationship Diagram (Entity Diagram)

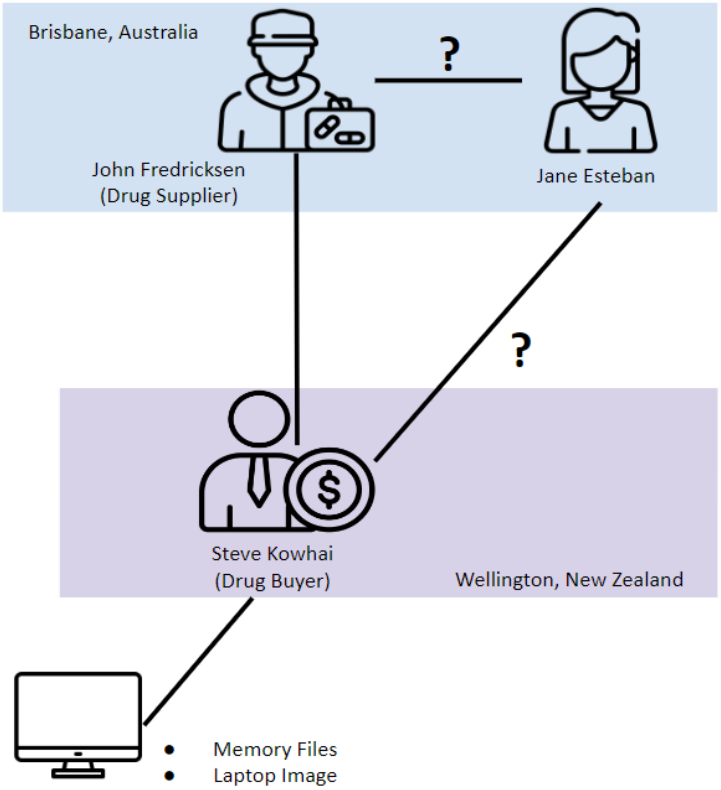


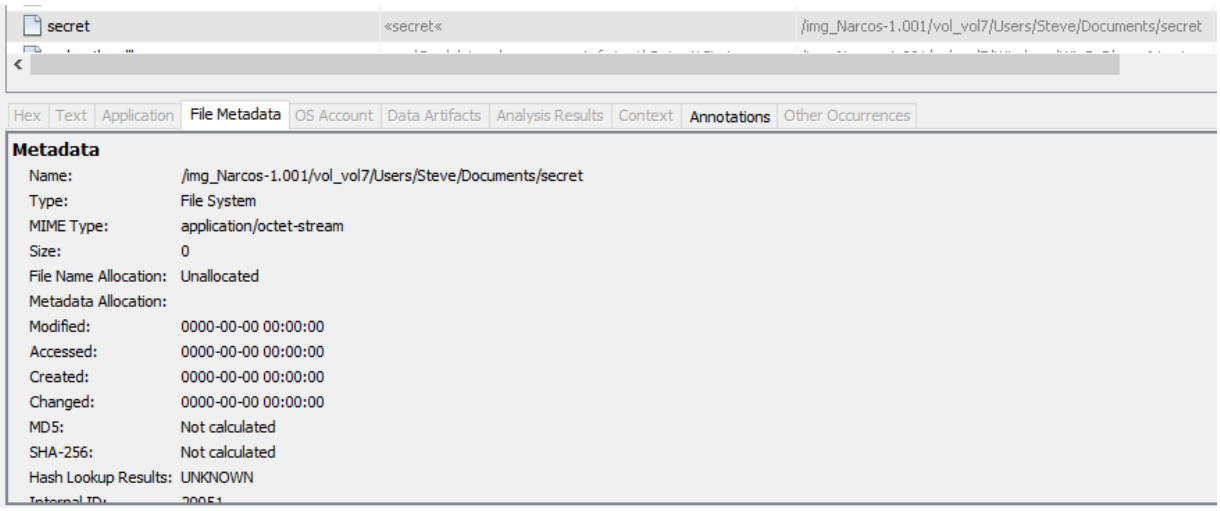
Fig 23. Entity diagram for the case

Based on several pieces of evidence, it is clear that Steve is involved in purchasing drugs from John. However, the available evidence that was provided for the team to analyse is not sufficient to establish the involvement of Jane in this case or her relationship with John and Steve.

8. Other Interesting Findings

8.1 Document File Named “secret”

There exists an unallocated file named “secret” that can be found in Steve’s Documents folder.



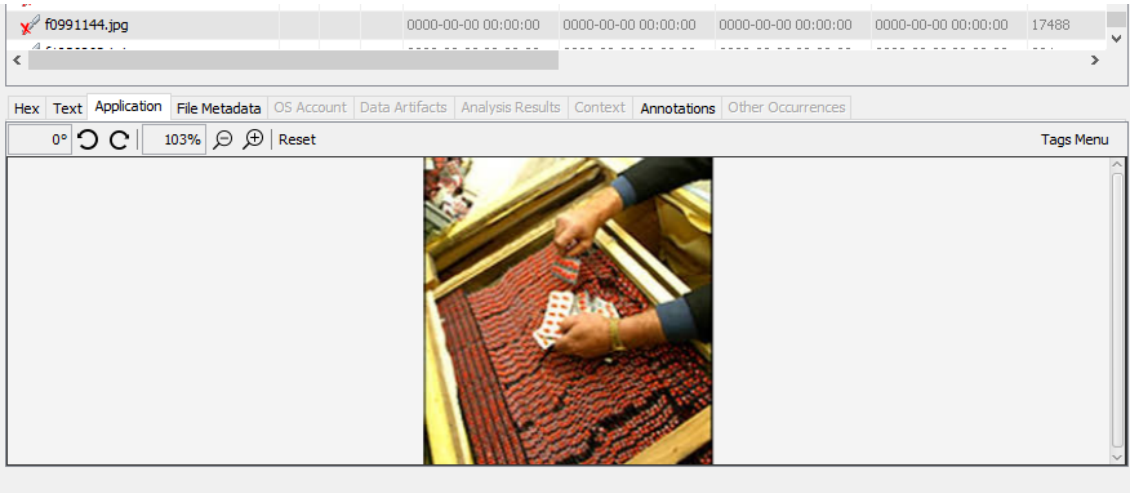
/img_Narcos-1.001/vol_vol7/Users/Steve/Documents/secret

Fig 24. The file named “secret”

The naming of this file is interesting as a file with this naming normally contains confidential and important information. However, we were unable to find much information on this file such as extensions, MAC times and data. Furthermore, as stated in the timeline, Steve has also accessed this file hence we felt that this file might hold information that could provide useful insights into the investigation. We believe that this file could have been removed when Steve ran CCleaner.

8.2 Other Drugs

While going through the files in Autopsy, our team came across the photo below which looks like a crate filled with what seems to be pills.



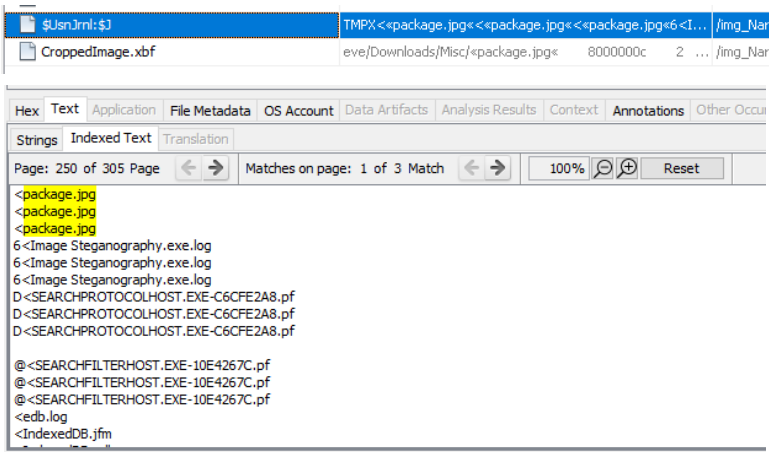
/img_Narcos-1.001/vol_vol7/$CarvedFiles/2/f0991144.jpg

Fig 25. Crate containing a large amount of what seems to be pills

Considering the main drug in this case is meth, and from prior knowledge of what meth looks like (white crystal substance), we can safely assume that the pills here are not meth. These pills could be another drug altogether. While it may not be the important evidence here, these pills (if they were illegal drugs) could indicate that Steve has not only purchased meth to distribute but also possibly other drug types.

8.3 Package.jpg

Another file that has piqued our interest is the file called“package.jpg”. While we cannot find the exact content of this image file, some metadata files have suggested this image being used for in the segment of image steganography:



/img_Narcos-1.001/vol_vol7/$Extend/$UsnJrnl:$

Fig 26. Package.jpg followed by the Steganography exe log file in UsnJrnlJ

This **$UsnJrnl:$J** contains information about changes to the filesystem. Following the timeline above, package.jpg was accessed before using the image steganography application. This means that package.jpg may have been used in the steganography. However, we cannot find package.jpg anywhere in the given image so we cannot determine whether it was or was not used in steganography or what the exact photo even is.

9. Conclusion

In conclusion, there is evidence that John and Steve are definitely guilty of drug trafficking. Our team has strong evidence that Steve is the main culprit behind this trafficking operation. The evidence shows that Steve is the person requesting and later having plans on mixing and selling these drugs. Steve's web searches and history of drug cutting and money laundering dispel any hypothesis that he is innocent in this case.

Our team also has strong evidence that John is a main player in this trafficking operation. All of the communication found is between the known culprit Steve and John. Moreover, their communication history shows that John was the person suggesting to Steve that there is a new supplier for the drugs which Steve wants to purchase. Hence, John's knowledge of drug suppliers as well as his communication history on Discord and email exchange with Steve suggests that John is guilty as well as he is an active collaborator in this trafficking operation.

However, the team is uncertain about Jane's role in this case, hence, we cannot conclude that she is guilty unless more evidence is given as stated in Section 10. Recommendations. Thus, if we are able to determine the role of Jane, we would be able to have a bigger and better picture of the case.

10. Recommendations

10.1 Evidence from John or Jane

As our team could not conclude what Jane's role is in the case and her relationship with John and Steve, we would need more evidence files to draw a conclusion. Evidence such as John or Jane's computer image/memory.

It is possible that having John's computer image would be useful as we can then find out how and what he communicated with Jane. Furthermore, we would be able to find more evidence to

strengthen our hypothesis on the relationship between John and Steve such as finding the BNE.png file from John's side or any communication evidence within the people involved in the case (e.g. email exchange, discord log from John's side).

Since Jane's Windows laptop was found during the search, performing the acquisition of her laptop image can allow our team to perform similar checks to find web history, communication logs, downloaded files and other evidence. The evidence found can better expose what Jane's role is regarding the drug trafficking.