IFS4102 Digital Forensics

AY2023/24 Semester 2

Case 1 Analysis Report

Team 6	
Ang Yong Ming	A0216990X
Hrithie Menon	A0244277Y
Ibrahim Sharul	A0225864X
Teo Chuan Kai	A0174217H

Table of Contents

1. Executive Summary

This case analysis report details the forensic analyses of potential illegal activities related to Jane Esteban and John Fredricksen. When searched by Customs officers in Wellington Airport after arriving from Brisbane, Australia, one kilogram of Methamphetamine was located in the lining of John Fredricksen's suitcase. This report focuses on a desktop computer seized from 666 Rewera Avenue, an address revealed by Jane Esteban after questioning.

This report will present a detailed description of the case and the background, along with the tools employed by the team in the process of forensic analysis of the acquired evidence. We subsequently believe that the main suspect is a man named Steve Kowhai, who also goes by the username "crayfish1980" on several online platforms. Steve Kowhai had communicated with John Fredricksen to arrange for a delivery of Methamphetamine to Eastbourne Library or alternatively, 666 Rewera Avenue. We believe that Kowhai intends to process and re-distribute the drugs received from Fredricksen, and also scale up operations subject to a successful first delivery. However, through available evidence, we are unable to definitively conclude the role of Jane Esteban in the case and her guilt.

2. Case Overview

2.1. Case Description and Background

Due to intelligence provided by the Australian government, two passengers were intercepted by Customs upon arriving at Wellington, New Zealand from Brisbane. The Intel provided stated that Jane Esteban and John Fredricksen may be involved in illegal activity. The suspects were searched by a customs officer. John Fredricksen's baggage consisted of clothing, toiletries and a Windows laptop. Jane Esteban's baggage also consisted of clothing, toiletries and a small Windows laptop.

Upon further search of the lining of John Fredricksen's suitcase, one kilogram of Methamphetamine was located. Both suspects were taken into separate interview rooms where they were interrogated. John Fredricksen refused to answer any questions.

Jane Esteban, meanwhile, stated all she knew and that she had to deliver the suitcase to the "Eastbourne library" but if all else failed then they were to deliver it to 666 Rewera Avenue, Petone as told by John Fredricksen. Customs and police subsequently raided that address. There was nobody present at the address. Customs did, however, find drugs, guns and a desktop computer in the living room of the suspect's house.

This case will be considered from the perspective of Customs forensics investigators with the purpose of determining the relationship between John Fredrickson and the suspect, their future intentions and any other supporting evidence that pertains to the case.

2.2. Evidence Analysed

The process of evidence acquisition was not performed by the team, but was instead performed by Customs officers as part of the raid on 666 Rewera Avenue. We, as Customs forensics officers, were delivered the drive image and memory dump of the suspect's desktop computer.

Both the drive image and memory dump were delivered as split files, thus, the team used the following Windows Powershell commands to combine the files and confirmed its integrity by checking the file hashes against the values reported by the Customs officers who performed the acquisition.

1. Combining the split drive image files: `cmd /c copy /b Narcos-1.* Narcos-1.img`
2. Combining the split memory dump files: `cmd /c copy /b Narcos-Mem-1.* Narcos-Mem-1.raw`
3. Generating SHA1 checksum for drive image: `Get-FileHash Narcos-1.img -Algorithm SHA1`
4. Generating SHA1 checksum for memory dump: `Get-FileHash Narcos-Mem-1.raw -Algorithm SHA1`

No	File Name	SHA1 Checksum	Size
1	Narcos-1.img	4d8e5041f47e0b0fc0eacc85d300661946537418	30.0 GB
2	Narcos-Mem-1.raw	191a10f54e04ad05d9d6a430e01ef6203406accb	4.0 GB

2.3. Tools Used

Name	Version
Autopsy	4.21.0
Volatility 3 Framework	2.7.0
Windows Powershell	5.1.22621.2506
ChromeHistoryViewer	1.53
TheSleuthKit	4.12.1
Image Steganography	1.5.2

3. Evidence and Findings

3.1. System Information

3.1.1. Operating System Information

Name: SK-DESKTOP
Version: Windows 10 Pro
Processor Architecture: AMD64
Product ID: 00330-80000-00000-AA502
Owner: Steve

3.1.2. Drive Information

Type: Image
Size: 32212254720 bytes (30.0 GB)
Sector Size: 512 bytes
Device ID: 029f7256-1e4a-4810-82f0-6844f30f6169
Layout:

Name	Description	Starting Sector	Ending Sector	Length in Sectors	Flags
vol1	Unallocated	0	2048	2048	Unallocated
vol4	Basic data partition	2048	1023999	1021952	Allocated
vol5	EFI System partition	1024000	1226751	202752	Allocated
vol6	Microsoft reserved partition	1226752	1259519	23768	Allocated
vol7	Basic data partition	1259520	62912511	61652992	Allocated
vol8	Unallocated	62912512	62914559	2048	Unallocated

3.2. User-Installed Programs

After analysing the drive image obtained from the suspect's computer, we were able to identify several programs that were installed by the suspect, ones which are not packaged into Windows operating systems by default. The presence of these programs along with their intended functions provides an insight into potential actions performed by the suspect on the seized computer.

3.2.1. Apache OpenOffice 4.1.6

Apache OpenOffice is an open-source office software suite for word processing, spreadsheets, presentations.

- Installer Location: /img_Narcos-1/vol_vol7/Users/Steve/Downloads/Apache_OpenOffice_4.1.6_Win_x86_install_en-US.exe
- Executable Location: /img_Narcos-1/vol_vol7/Program Files (x86)/OpenOffice 4/program/soffice.exe

3.2.2. CCleaner 5.5.2

CCleaner is a utility commonly used to clean potentially unwanted files and invalid Windows Registry entries from a computer.

- Installer Location: /img_Narcos-1/vol_vol7/Users/Steve/Downloads/ccsetup552.exe
- Executable Location: /img_Narcos-1/vol_vol7/Program Files/CCleaner/CCleaner64.exe

3.2.3. Discord 0.0.304

Discord is an instant messaging and voice over IP (VoIP) social platform which allows communications through voice calls, video calls, text messaging and media and files.

- Installer Location: /img_Narcos-1/vol_vol7/Users/Steve/Downloads/Misc/DiscordSetup.exe
- Executable Location: /img_Narcos-1/vol_vol7/Users/Steve/AppData/Local/Discord/app-0.0.304/Discord.exe

3.2.4. Google Chrome 72.0.3626.81

Google Chrome is a widely used web browser

- Installer Location: /img_Narcos-1/vol_vol7/Users/Steve/Downloads/ChromeSetup.exe
- Executable Location: /img_Narcos-1.img/vol_vol7/Program Files (x86)/Google/Chrome/Application/chrome.exe

3.2.5. Image Steganography 1.5.2

Image Steganography is a program which allows users to embed text and files in images, in a process called steganography

- Installer Location: /img_Narcos-1/vol_vol7/Users/Steve/Downloads/Image Steganography 1.5.2

- Executable Location: /img_Narcos-1/vol_vol7/Users/Steve/AppData/Roaming/CPascoe/Image Steganography/ProgData/Image Steganography.exe

3.2.6. TrueCrypt 7.1a

TrueCrypt is an open-source utility used for on-the-fly encryption, which can be employed to create virtual encrypted disks enclosed within a file, or to encrypt a partition or the whole storage device.

- Installer Location: /img_Narcos-1/vol_vol7/Users/Steve/Downloads/TrueCrypt Setup 7.1a.exe
- Executable Location: /img_Narcos-1/vol_vol7/Program Files/TrueCrypt/TrueCrypt.exe

3.3. Images

3.3.1. Exhibit 1 (620x349.jpg)

File Name	620x349.jpg
File Path	/img_Narcos-1/vol_vol7/Users/Steve/Pictures/620x349.jpg
File Size	19342 bytes
Hash Value	MD5: 60398A8EC59753CE5AADB99A566844D7 SHA1: 03AF3A8D88DE94880180514ADD4A39BAAD5A660F
Modified Time	2019-02-01 10:48:41 SGT
Accessed Time	2019-01-31 11:04:13 SGT
Created Time	2019-01-31 10:57:04 SGT
Status	Unallocated (deleted)
Content	

This image depicts several bags of white crystalline material. Based on the case background, we infer that the picture depicts bags of Methamphetamine, which corresponds with the substances confiscated by the Customs in Wellington Airport.

3.3.2. Exhibit 2 (price-meth-bust-4.jpg)

File Name	price-meth-bust-4.jpg
File Path	/img_Narcos-1/vol_vol7/Users/Steve/Pictures/price-meth-bust-4.jpg

File Size	118136 bytes
Hash Value	MD5: 480DA4FF5734C6D20787AF08FC9DA46E SHA1: F3D9972DE1D08104BF395E76E7642CC4A5779519
Modified Time	2019-02-01 10:48:41 SGT
Accessed Time	2019-01-31 11:04:13 SGT
Created Time	2019-01-31 10:58:22 SGT
Status	Unallocated (deleted)
Content	

This image, together with its time, shows a meth bust operation and the total money found. Doing an image reverse search on TinyEye reveals that it's from an operation in Prince, Utah, the United States. It was deleted, indicating the possible covering of tracks but it is unsure exactly how this image would aid the suspect, except by serving as drug trade gone wrong.

3.3.3. Exhibit 3 (eight_col_patches_crp.jpg)

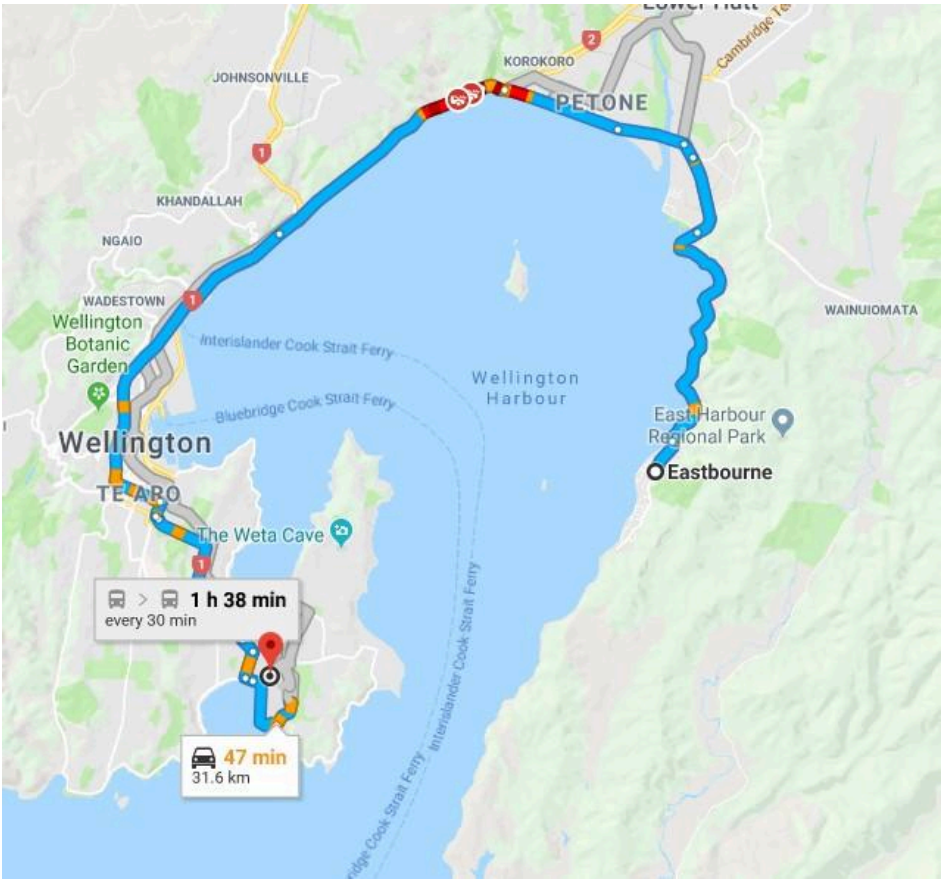
File Name	eight_col_patches_crp.jpg
File Path	/img_Narcos-1/vol_vol7/Users/Steve/Pictures/eight_col_patches_crp.jpg
File Size	86240 bytes
Hash Value	MD5: EA016DB23A40F61C10CE802692DF7C0C SHA1: 4E41EA7351BCFA5667958A5397A81B58E602D8C7

Modified Time	2019-02-01 10:48:41 SGT
Accessed Time	2019-02-01 10:42:46 SGT
Created Time	2019-01-31 10:59:38 SGT
Status	Unallocated (deleted)
Content	

This image depicts the logo of an organised street and prison gang in New Zealand. Based on the web history of places to sell drugs and gangs in New Zealand, we can infer it to be one of the possible avenues to trade or sell the drugs.The fact that it was deleted could be indicative of the suspect trying to cover their tracks

3.3.4. Exhibit 4 (airport crystals.jpg)

File Name	airport crystals.jpg
File Path	/img_Narcos-1/vol_vol7/Users/Steve/Documents/Misc/airport crystals.jpg
File Size	77643 bytes
Hash Value	MD5: F938F92D9DBAEDA2E92246DEEEBE830A SHA1: 52F2D5EBD27AF489C7B112344EC86788B6AC105A
Modified Time	2019-01-31 05:25:18 SGT
Accessed Time	2019-01-31 05:25:18 SGT
Created Time	2019-01-31 05:25:18 SGT
Status	Allocated

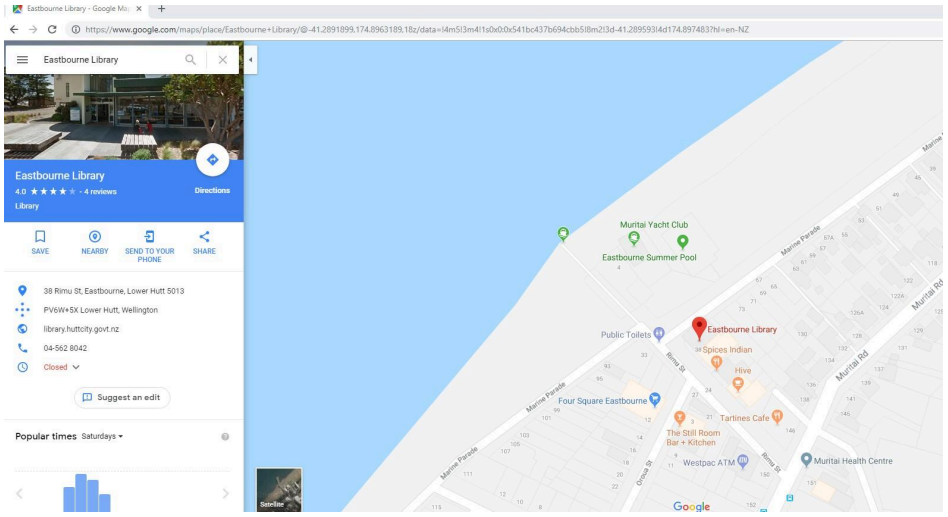
Content	

This image is labelled “airport crystals.jpg”, indicating that there might be potential links to the Methamphetamine that was seized by customs at the airport from Jane Esteban and John Fredricksen. It is a screen capture of Google Maps showing directions from Wellington International Airport to a town named Eastbourne.

The destination of this route appears to correlate with the location depicted in Exhibit 5 (dropoff.jpg). Thus, it is likely that this route was intended for either one or both of Jane Esteban and John Fredricksen to take after having landed at Wellington International Airport, with the purpose of delivering the Methamphetamine that was seized by Customs from John Fredricksen’s suitcase. This image could have been circulated to Jane Esteban and/or John Fredricksen to inform them of the route to take to deliver the suitcase with the Methamphetamine, as stated by Jane Esteban in her confession. The recipient is thus likely to be the suspect.

3.3.5. Exhibit 5 (dropoff.jpg)

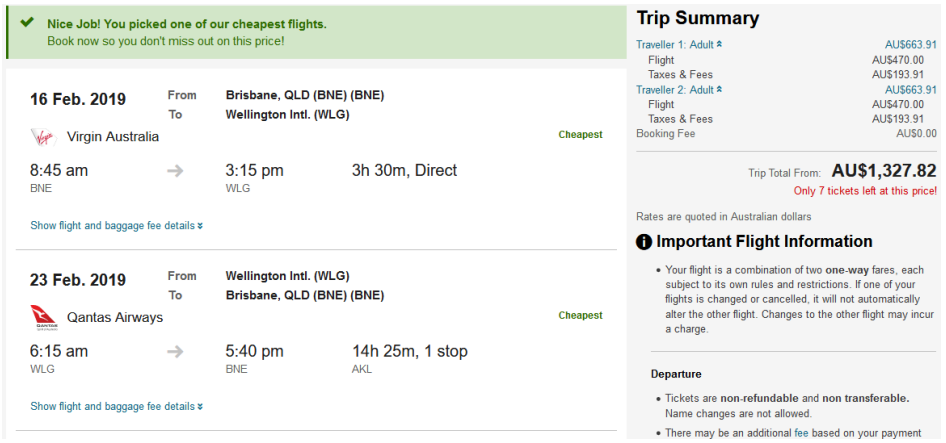
File Name	dropoff.jpg
File Path	/img_Narcos-1/vol_vol7/Users/Steve/Documents/Misc/dropoff.jpg
File Size	177888 bytes
Hash Value	MD5: 7FEB763BEBE42C3A3464C9EE3BB1D3E8

	SHA1: 47EA895261F5B0F6775B0E2C66891067BC816F92
Modified Time	2019-01-31 05:25:18 SGT
Accessed Time	2019-01-31 05:25:18 SGT
Created Time	2019-01-31 05:25:18 SGT
Status	Allocated
Content	

This image is a window capture of Google Maps highlighting Eastbourne Library located in 38 Rimu Street, Eastbourne, Lower Hutt, Wellington, New Zealand, labelled dropoff.jpg. This suggests that it was understood by the suspect to be a location to potentially drop off drugs for someone else to collect. This location corresponds to the confession by Jane Esteban - for Methamphetamine to be delivered to “Eastbourne Library". This image could have been circulated to one or both of Jane Estaban and John Fredricksen, along with Exhibit 4 (airport crystals.jpg) to clarify the intended location for them to deliver the suitcase that contained the Methamphetamine seized by Customs.

3.3.6. Exhibit 6 (flightbookings.PNG)

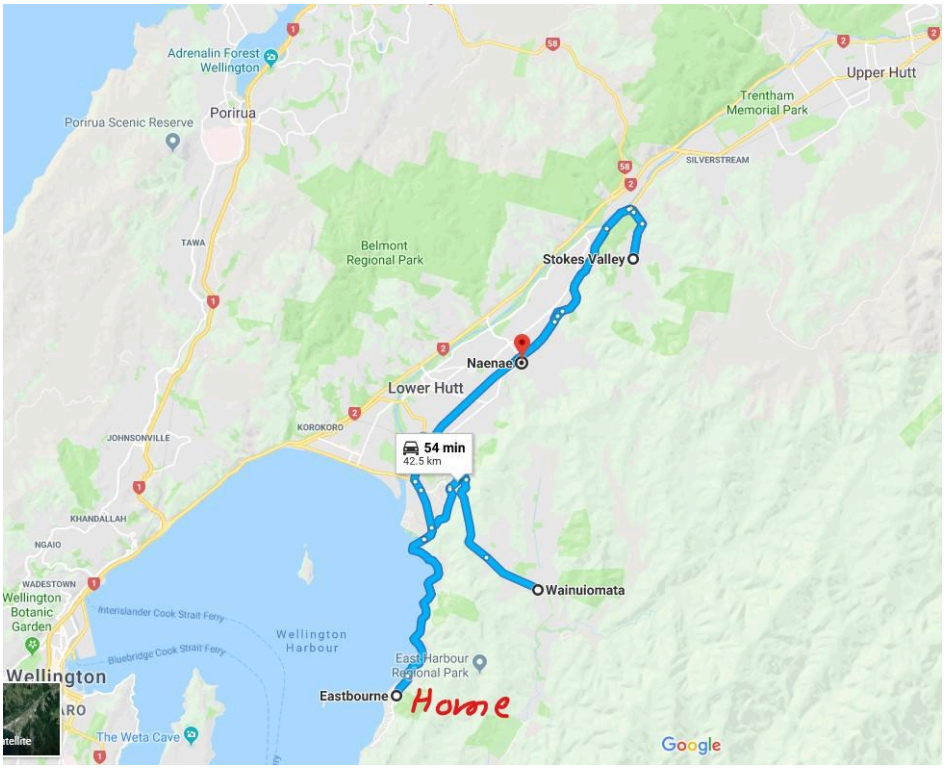
File Name	flightbookings.PNG
File Path	/img_Narcos-1/vol_vol7/Users/Steve/Documents/Misc/flightbookings.PNG
File Size	52971 bytes
Hash Value	MD5: D1B21A1CDDCB3494D637F2424CC5F0F1 SHA1: 856E13E9C8E8B46DE1C1DD35B5FF49F6537EB870
Modified Time	2019-01-31 05:25:18 SGT
Accessed Time	2019-01-31 05:25:18 SGT
Created Time	2019-01-31 05:25:18 SGT

Status	Allocated
Content	

This image is a screen capture of a trip summary for return flights from Brisbane, Australia to Wellington, New Zealand on 2019-02-16 and from Wellington, New Zealand to Brisbane, Australia with a stopover in Auckland, New Zealand on 2019-02-23. Both flights were booked for two adults, and the fares were charged as Australian dollars. Considering the background of the case, it is very likely that these were the flights that Jane Esteban and John Fredricksen took when they arrived in Wellington.

3.3.7. Exhibit 7 (Method run.jpg)

File Name	Method run.jpg
File Path	/img_Narcos-1/vol_vol7/Users/Steve/Documents/Misc/Method run.jpg
File Size	145213 bytes
Hash Value	MD5: 69B225BC0EF5A0C003F1E2A6646AAF92 SHA1: 2F9CEFCBA4F8735BDC852BAF572266B32F05EF93
Modified Time	2019-01-31 05:25:18 SGT
Accessed Time	2019-01-31 05:25:18 SGT
Created Time	2019-01-31 05:25:18 SGT
Status	Allocated

Content	

This image is a screen capture of a Google Maps page, showing the directions between multiple locations, while the locations cannot be clearly seen through the picture, the path hints at the suggested route for navigating from

1. A town named Wainuiomata
2. A junction in Eastbourne
3. A junction in Stokes Valley

Several further observations can be made from this image.

1. All the locations specified are located in and around Wellington, New Zealand, specifically a region known as Lower Hutt.
2. The location pinned at Eastbourne is labelled “Home”. This indicates that the suspect likely resides in the town of Eastbourne, New Zealand.

The presence of this charted path, along with it being labelled “Method run” indicates that this was a route that either the suspect or someone they were communicating with were intending to take. The town of Eastbourne that is correlated with the confession from Jane Esteban, and Exhibit 5 (dropoff.jpg), indicates that this route of travel may be involved in transporting the Methamphetamine.

3.3.8. Exhibit 8 (BNE.png)

File Name	BNE.png
File Path	/img_Narcos-1/vol_vol7/Users/Steve/Downloads/Misc/BNE.png
File Size	4376793 bytes
Hash Value	MD5: DFFA98BDD7371D1806ADB09DB27BA283

	SHA1: 0897FAA06FBB6E0D678A9497B6F5D330F231362F
Modified Time	2019-02-01 08:13:20 SGT
Accessed Time	2019-02-02 10:31:06 SGT
Created Time	2019-02-02 10:31:06 SGT
Status	Allocated
Content	

This image appears to depict the skyline of a developed city, based on reverse image searches, we were able to identify it as a stock image of the city of Brisbane, Australia, available from the link here. Furthermore, its file name of “BNE” also lends credence to this as it is the airport code for Brisbane Airport. This also hints at the correlation between this image and the contents of Exhibit 6 (flightbookings.PNG) which shows tickets for a flight from Brisbane to Wellington.

An interesting observation is that the created time is after the modified time, meaning that the file did not originate from the file system. Additionally, this image has a size of approximately 4MB, which is significantly larger than that of other images found so far. Further analysis of this artefact in Exhibit 17 shows that there exists content hidden within this image.

3.4. Communications

3.4.1. Exhibit 9 (Discord Outgoing Message Cache)

File Name	000006.log
File Path	/img_Narcos-1/vol_vol7/Users/Steve/AppData/Roaming/Discord/Local Storage/leveldb/000006.log
File Size	34411 bytes
Hash Value	MD5: 19DA7FC1B8DA010F787B4671AAD2570F SHA1: 689B8EF85FF9C48EC17A336BA277FA19A1234F23
Modified Time	2019-02-02 10:38:47 SGT
Accessed Time	2019-02-02 10:38:47 SGT
Created Time	2019-02-02 10:38:47 SGT
Status	Allocated
Relevant Contents	Timestamp: 1548802718174 (2019-01-30 06:58:38 SGT) Message: New supplier eh? Definitely Interested! Can I get 10 keys of it delivered to Wellington Timestamp: 1548803049066 (2019-01-30 07:04:09.066 SGT) Message: 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 Timestamp: 1548969372835 (2019-02-01 05:16:12.835 SGT) Message: Good Thinking, I already know how. Heard of steganography? Timestamp: 1548969682114 (2019-02-01 05:21:22.144 SGT) Message: A way of hiding one image within another. There's a simple application called 'Image Steganography'. Timestamp: 1548979899479 (2019-02-01 08:11:39.479 SGT) Message: Ya.. I just told you about the tool :face_palm: Received it. Will check to see if it works and confirm soon. Timestamp: 1549074636655 (2019-02-02 10:30:36.655 SGT) Message: Good. Meet at the Eastbourne library and if we miss each other come to 666 Rewera Avenue, Petone.

Analysis and research of this artefact shows that it is a segment of a log file generated by the LevelDB data store. It is an on-disk key-value store developed by Google that is often used by programs as a database or for caching. Discord uses LevelDB as a cache for several forms of information, one of which is to store the messages typed by users.

This specific segment of the LevelDB log file appears to contain data pertaining to messages sent by the user logged into Discord on the drive image. Based on the case background along with evidence obtained so far, it is very likely that these messages were typed and sent by the suspect via the Discord program. The intended recipient and any responses to these messages were not able to be ascertained via this artefact alone. Despite this, based on the contents of the messages sent by the suspect, several pieces of information can be obtained from the logs:

- Contact with a new supplier, whom suspect requests “10 keys” of objects delivered to Wellington (correlating with the case background, the “10 keys” is likely to refer to shipments of Methamphetamine)
- Suspect sends further information through a document to recipient (based on installed programs, this document is likely to be created with OpenOffice)
- Discussions about hiding information through image steganography, also highlighting that information might have been exchanged between the suspect and the other individual in contact. (this confirms that the Image Steganography program was used to hide information)
- Instructions to meet at Eastbourne Library, and 666 Rewera Avenue as a secondary meeting point (this corresponds to the information provided by Jane Esteban during the interrogation)

3.4.2. Exhibit 10 (Discord Chat Logs)

File Name	f0644226
File Path	/img_Narcos-1.img/vol_vol7/$CarvedFiles/1/f0644226.gz/f0644226
File Size	4345 bytes
Hash Value	MD5: 12EF289C0A890E64527127F8121339F9 SHA1: 22F796EDD428C94D78663F4348354509843D190C
Modified Time	N/A
Accessed Time	N/A
Created Time	N/A
Status	Allocated (Carved from deleted files)
Relevant Contents	Timestamp: 2019-01-29 05:29:39.162 SGT Username: crayfish1980 Message: Need to get a new delivery Timestamp: 2019-01-29 10:17:23.904 SGT Username: heresjohnny1

	Message: Okay. Talk tomorrow, gotta run Timestamp: 2019-01-30 06:27:45.692 SGT Username: heresjohnny1 Message: Got a new supplier. Ya Interested?? Timestamp: 2019-01-30 06:58:49.823 SGT Username: crayfish1980 Message: New supplier eh? Definitely Interested! Can I get 10 keys of it delivered to Wellington Timestamp: 2019-01-30 07:00:23.641 SGT Username: heresjohnny1 Message: 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? Timestamp: 2019-01-30 07:04:13.421 SGT Username: crayfish1980 Message: 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. Timestamp: 2019-01-30 07:10:43.581 SGT Username: heresjohnny1 Message: Great. John Out. Timestamp: 2019-02-01 05:04:31.629 SGT Username: heresjohnny1 Message: I want to send an image an image of something to you but it needs to be done safely. Any ideas?

Further examination of files used by the Discord program, along with string analyses of the files present on the file system with references to the message found in Exhibit 9 revealed a file with JSON-structured data containing chat logs from discord. This file was retrieved through Autopsy's file carving feature, indicating that it has already been deleted, either automatically by Discord when cleaning old logs, or manually by the suspect.

There are two usernames mentioned within the logs: crayfish1980 and heresjohnny1. Based on case background information along with context from Exhibit 9, we posit that heresjohnny1 is a Discord account belonging to John Fredricksen due to the similarities in naming, while crayfish1980 belongs to the suspect based on the matching content from Exhibit 9. The information adds further context to the information obtained from Exhibit 9 (Discord Outgoing Message Cache).

Several further pieces of information can be obtained from the chat logs:

- The suspect (crayfish1980) actively requests for a “new delivery” from John Fredricksen (heresjohnny1) (the object in question likely refers to Methamphetamine).
- The suspect initially requests for “10 keys” of the drugs, but John Fredricksen instead proposes to start with “1 key” to assess the feasibility of the delivery first.
- John Fredricksen intends to send an image to the suspect, but wants it to be done in a safe manner. The conversation seems to continue towards the messages shown in Exhibit 9.

3.5. Web Data

3.5.1. Exhibit 11 (Google Chrome Autofill)

File Name	Web Data
File Path	/img_Narcos-1.img/vol_vol7/Users/Steve/AppData/Local/Google/Chrome/User Data/Default/Web Data
File Size	69632 bytes
Hash Value	MD5: 5D56ECB5F42590BF79CAB34BEE1C6832 SHA1: D6F795CEDE8D4C0D089464402625C4A02F25CFAD
Modified Time	2019-02-02 10:28:16 SGT
Accessed Time	2019-02-02 10:28:16 SGT
Created Time	2019-01-30 05:05:55 SGT
Status	Allocated
Content	Name: username Value: crayfish1980 Count: 3 Date Created: 2019-01-30 07:34:33 SGT Date Accessed: 2019-02-01 08:22:00 SGT Username: Default Program Name: Google Chrome Data Source: Narcos-1.img

Autofill is a feature provided by Google Chrome which allows users to fill up forms automatically with stored information, it is most commonly used in the context of login forms. The list of saved autofills for Google Chrome show that there is a record of the value “crayfish1980” being saved for a field titled “username”. This indicates that the suspect could be active on multiple platforms or services under the username “crayfish1980”. It should be noted that the created and accessed dates for the entry are different than that of the file:

- Autofill date created: 2019-01-30 07:34:33 SGT
- Autofill date accessed: 2019-02-01 08:22:00 SGT

3.5.2. Exhibit 12 (Google Chrome Saved Web Accounts)

File Name	Login Data
File Path	/img_Narcos-1.img/vol_vol7/Users/Steve/AppData/Local/Google/Chrome/User Data/Default/Login Data
File Size	18432 bytes
Hash Value	MD5: D1CCD48044B6A8D1B9A5E2F21C29DA70 SHA1: 3DDAED3D23F0C247715B18D9257DC5D99485E521
Modified Time	2019-02-02 10:28:16 SGT
Accessed Time	2019-02-02 10:28:16 SGT
Created Time	2019-01-30 05:05:55 SGT

Status	Allocated
Content	URL: https://mail.protonmail.com/login; Date Created: 2019-02-01 08:12:51 SGT; Decoded URL: protonmail.com; Username: Default; Realm: https://mail.protonmail.com/; Domain: protonmail.com; Program Name: Google Chrome

In addition to autofills, Google Chrome also provides a feature to store web accounts for different applications or websites, speeding up users ability to login to them. In the list of saved accounts from the drive image, there is an entry for the email provider protonmail, with the URL listed as “protonmail.com”. In combination with Exhibit 10 (Google Chrome Autofill) we are able to ascertain that the suspect owns and likely uses the email address crayfish1980@protonmail.com.

3.5.3. Exhibit 13 (Google Chrome History)

File Name	History
File Path	/img_Narcos-1.img/vol_vol7/Users/Steve/AppData/Local/Google/Chrome/User Data/Default/History
File Size	360448 bytes
Hash Value	MD5: F3F979C6DEE9FBB7CBDF5818AAA4B723 SHA1: 178C6170CF55E649C7CEDD201B4A9EA51A976B0F
Modified Time	2019-02-02 10:28:48 SGT
Accessed Time	2019-02-02 10:28:48 SGT
Created Time	2019-01-30 05:05:55 SGT
Status	Allocated

The History file is an SQLite3 on-disk SQL database which is used by Google Chrome to store a list of URLs along with metadata about the links which the user has visited.

Items of Interest in Search History

truecrypt (via Google)

- 2 instances (2019-01-30 07:26:30 SGT, 2019-01-30 07:26:53 SGT)
- Related to download and install of TrueCrypt program, installer was downloaded from the URL https://www.softpedia.com/get/Security/Encrypting/TrueCrypt.shtml

protonmail (via Google)

- 2 instances (2019-01-30 07:34:09 SGT, 2019-02-01 08:12:20 SGT)
- Potentially logged in using credentials stated in Exhibits 10 and 11

ccleaner (via Google)

- 1 instance (2019-01-30 07:40:35 SGT)
- Related to download and install of CCleaner program, installer was downloaded from the URL https://www.ccleaner.com/ccleaner/download/standard

crystal meth (via Google)

- 7 instances (between 2019-01-31 10:56:07 SGT and 2019-01-31 10:56:33 SGT)

drug paraphernalia (via Google)
- 7 instances (between 2019-01-31 10:57:16 SGT to 2019-01-31 10:57:37 SGT)

drug paraphernalia meth (via Google)
- 4 instances (between 2019-01-31 10:57:50 SGT to 2019-01-31 10:58:03 SGT)

gangs nz drugs (via Google)
- 4 instances (between 2019-01-31 10:59:17 SGT to 2019-01-31 10:59:32 SGT)

image steganography download (via Google)
- 1 instance (2019-02-01 08:15:04 SGT)
- Could be related to download and install of the Image Steganography program

best places to trade drugs (via Google)
- 3 instances (2019-02-02 09:01:34 SGT)

wellington libraries (via Google)
- 1 instance (2019-02-02 09:01:51 SGT)

courteney place (via Google)
- 1 instance (2019-02-02 09:02:51 SGT)

eastbourne library (via Google)
- 2 instances (2019-02-02 09:05:11 SGT)

3.5.4. Exhibit 14 (Google Chrome Logs)

File Name	000019.ldb
File Path	/img_Narcos-1.img/vol_vol7/Users/Steve/AppData/Local/Google/Chrome/User Data/Default/000019.ldb
File Size	2115 bytes
Hash Value	MD5: 2AFA4BE8B333D4231A6D7B008A1EF4BA SHA1: CCB2F480C820948262A038861D94836260461F25
Modified Time	2019-02-01 10:39:51 SGT
Accessed Time	2019-02-02 10:28:16 SGT
Created Time	2019-02-01 10:39:51 SGT
Status	Allocated

Relevant Contents	C:\Users\Steve\Download Unconfirmed 211922.crd:> w(Image xganography 1.5.2 (0etup.ex cca1d72f-06cd-4386-a85d-d286c6191f7f Eblob: !(mail.proton com/f7f4f3a9-ba89-4f46-b2a8-c58bb8f99d4f *zn] ^inbox/OMk2pv6297Pp1O6uag3DLPTnyK1ee6dVkZCT7kaMAS6Hi5ybCyevYuLxzsBwSWa5u-xmyY3XR_H51LXglEdjYw==*^ 00BJP /pngb 0BNE.pngZ

The 000019.ldb is likely a Microsoft Access lock information file. Considering the location of where the file was found, it is likely that this file was used by Google Chrome as a lock file, which aims to prevent concurrent access to critical information which could result in data inconsistencies. Analysing the snippets of text that can be seen within the file, the area highlighted in red shows a URL from the mail.proton.com domain. The subsequent lines contain the filename “BNE.png”, which is referring to the similarly named file as stated in Exhibit 8. Thus, we can conclude that the BNE.png image was downloaded by the suspect from the protonmail email platform.

When further considering the Discord conversations between crayfish1980 and heresjohnny1 in Exhibits 9 and 10, it can be concluded that this image is likely the one that heresjohnny1 wanted to send to crayfish1980 over a safe channel, to which the latter suggested the use of the Image Steganography software. Further considering the relatively large size of the BNE.png file found in Exhibit 8, we conclude that this image contains a hidden file within.

3.5.5. Exhibit 15 (Microsoft Edge History)

File Name	WebCacheV01.dat
File Path	/img_Narcos-1.img/vol_vol7/Users/Steve/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat
File Size	42991616 bytes
Hash Value	MD5: D69B6EA8E6A1C05C57C4B0523BB37AC0 SHA1: E0A49F019F4F543A8026850666CEFE96C3B9BDA9
Modified Time	2019-02-02 10:39:26 SGT
Accessed Time	2019-02-02 10:39:26 SGT
Created Time	2019-02-02 10:39:26 SGT
Status	Allocated

WebCacheV01.dat is an Extensible Storage Engine database also known as the Jet Blue engine. When a site is visited with the Microsoft Edge browser, it will write the history into this file.

Items of Interest in Search History

download open office (via bing.com)

- 2 instances (2019-01-28 20:42:24 SGT)
- Related to the download and install of the OpenOffice program, suspect eventually downloaded installer from the URL https://versaweb.dl.sourceforge.net/project/openofficeorg.mirror/4.1.6/binaries/en-US/Apache_OpenOffice_4.1.6_Win_x86_install_en-US.exe

download discord (via bing.com)

- 2 instances (2019-01-28 20:55:46 SGT)
- Related to download and install of the Discord program used as communications platform, suspect eventually downloaded installer from the URL URL https://dl.discordapp.net/apps/win/0.0.304/DiscordSetup.exe

protnmail (via bing.com)

- 2 instances (2019-01-28 21:02:11 SGT)
- A misspelling of “protonmail”, potentially logged in using credentials stated in Exhibits 10 and 11

cutting drugs (via google.com)

- 8 instances (between 2019-01-28 22:58:52 SGT and 2019-01-28 23:00:22 SGT)

cutting agents for ice (via google.com)

- 2 instances (2019-01-28 23:02:00 SGT, 2019-01-28 23:02:01 SGT)
- “Ice” is a common synonym used to refer to methamphetamine

how to launder money (via google.com)

- 2 instances (2019-01-28 23:03:51 SGT)

drug routes in wellington (via bing.com)

- 2 instances (2019-01-29 01:01:58 SGT)

drug routes in wellington (via google.co.nz)

- 5 instances (between 2019-01-29 01:02:39 SGT and 2019-01-29 01:03:27 SGT)

drug routes in around wellington (via google.co.nz)

- 5 instances (between 2019-01-29 01:03:42 SGT and 2019-01-29 01:03:55 SGT)

international drug routes (via google.co.nz)

- 4 instances (between 2019-01-29 01:04:12 SGT and 2019-01-29 01:11:15 SGT)

install chrome (via bing.com)

- 2 instances (2019-01-29 21:04:35 SGT, 2019-01-29 21:04:44 SGT)
- Related to the download and install of the Google Chrome browser, suspect proceed to download the installer from https://www.google.com/chrome/

3.6. Other Data

3.6.1. Exhibit 16: Microsoft OneNote

File Name	settings.dat.LOG2
File Path	/img_Narcos-1.img/vol_vol7/Users/Steve/AppData/Local/Packages/Microsoft.Office.OneNote_8wekyb3d8bbwe/Settings/settings.dat.LOG2
File Size	73728 bytes
Hash Value	MD5: 96367D55A827156444F47DD35643165E SHA1: 36862414307FC4F3D0B7813CCD5DE16ABE776BA1
Modified Time	2019-02-01 08:26:05 SGT
Accessed Time	2019-02-01 08:26:05 SGT
Created Time	2019-02-01 08:26:05 SGT
Status	Allocated
Contents	ProviderId 2418c0082017486a SigninName 00037FFE1E74C1EA FederationProvider EmailAddress crayfish1980@protonmail.com FirstName Steve Initials LastName Kowhai FriendlyName Steve Kowhai ProfileUrl Picture

While there is no official documentation stating the purpose of files named settings.dat, it is accepted as a commonly used file in which Windows applications store configurations or settings. In many cases, these files are Windows registry files, which are used to store parts of the Windows Registry specific to the application in question. The overall path of this settings.dat indicates that it is used by the OneNote program as part of Microsoft Office.

The contents of the file indicate that it was previously configured with an authenticated user bearing the email address of "crayfish1980@protonmail.com", first name of "Steve" and last name of "Kowhai". Based on Exhibits 10 (Google Chrome Autofills) and 11 (Google Chrome Saved Accounts), we conclude that this account is associated with the suspect. Furthermore, it also shows evidence that the suspect is named Steve Kowhai.

Additionally, the presence of the “LOG2” suffix in the file name, when combined with additional research, indicate that this file is effectively a truncated log of changes that have been made to registry hives. This behaviour could be due to several actions, such as the user logging out of the OneDrive account, or registry hives being specifically deleted or modified by programs such as CCleaner.

3.6.2. Exhibit 17: Image Hidden With Steganography

In an attempt to extract the hidden contents within Exhibit 8 (BNE.png), we utilised the same version of Image Steganography to extract the hidden file. However, we were unable to obtain any valid files from this process.

File Name	00000006.bin
File Path	/img_Narcos-1.img/vol_vol7/Users/Steve/AppData/Local/Packages/Microsoft.Office.OneNote_8wekyb3d8bbwe/LocalState/AppData/Local/OneNote/16.0/cache/00000006.bin
File Size	32768 bytes
Hash Value	MD5: 9F155752AA87A273D6F943A32121D698 SHA1: 7FC2D09B53523FFA032134277B660F681161B0A7
Modified Time	2019-02-01 08:26:04 SGT
Accessed Time	2019-02-01 08:26:04 SGT
Created Time	2019-02-01 08:24:48 SGT
Status	Allocated
Relevant Contents	Stego The location = C:\Users\Steve\Downloads\Misc \BNE Pass equals Elchapo2 Success

Further search within the drive image revealed a potential password utilised in the steganography process. Autopsy was able to retrieve the 00000006.bin file within the application cache for Microsoft OneNote. It appears to contain contents of a document in OneNote which states that a password was used in relation to the file BNE.png along with the word “Stego”. Attempting to use this password to also decrypt the hidden contents, we were able to retrieve an image named package.jpg.

File Name	package.jpg
File Path	N/A (hidden within BNE.png)
File Size	83871 bytes

Hash Value	MD5: 8BA9265A1563FF871A471C552BAB0B67 SHA1: 69BBE11C8646E5E1633C0C1772D88A520C9E1C11
Modified Time	N/A
Accessed Time	N/A
Created Time	N/A
Status	N/A
Contents	

This image shows a suitcase with its base layer revealed, along with three rectangular shaped objects wrapped in brown tape. Considering the context in which this image was sourced including Exhibits 9 (Discord Outgoing Message Cache), 10 (Discord Chat Logs), 14 (Google Chrome Logs) and the Methamphetamine was found in the lining of John's Fredricksen's suitcase, we can understand that this photo was sent from Fredricksen to the suspect embedded in Exhibit 8 (BNE.png). The suspect was informed of Fredricksen's intention to send this file through messages on Discord. The suspect then received the image from his protonmail email account, before using the password "Elchapo2" to extract and decrypt the image using the Image Steganography program. We conclude that the purpose of this photo was for Fredricksen to communicate where the drugs would be hidden within the suitcase, such that the suspect may be able to successfully retrieve it later.

4. Analysis

Based on the list of evidence and their associated considerations as stated in section 3 along with prior background information on the case, our holistic and comprehensive analysis of the available evidence will seek to establish the relationship between John Fredricksen and the suspect, and any possible future intentions based on the following questions, in the position of forensics investigators acting on behalf of the Customs.

- Who was the suspect?
- What did the suspect want from John Fredricksen during the latter's trip?
- What where the future plans and intentions of the suspect and John Fredricksen
- What was the role of Jane Esteban in the case and is she guilty?

This section of the case analysis report will seek to establish answers to the questions above to identify the suspect and to analyse the possible actions and intentions of John Fredricksen and Jane Esteban, along with supporting evidence for our claims.

4.1. Identity of the Suspect

We believe the suspect to be a man named Steve Kowhai. This is based on the firstly, the details obtained from analysing the system information found in the drive image, which stated the owner as "Steve", and the system name as "SK-DESKTOP". Secondly, from Exhibit 16 (Microsoft OneNote Data), records of an authenticated user with the first and last names of Steve and Kowhai respectively were found. Thus, we conclude that the suspect in this case is a man named Steve Kowhai.

Steve Kowhai frequently utilised the username "crayfish1980" for accounts on web platforms and services. We were able to ascertain that he is associated with the email address "crayfish1980@protonmail.com", and that he has also actively used Discord as an online communications platform under the username "crayfish1980". Steve Kowhai has also previously used Microsoft services under the same email address, evident from Exhibit 16 which shows prior authentications under the email address.

He is likely to reside in or within the vicinity of the town of Eastbourne, New Zealand. This is primarily supported by several mentions of the surrounding regions in search engine queries such as "wellington library", "eastbourne library", "drug routes in wellington" and "drug routes in around wellington". Furthermore, many of the images found in the drive image (Exhibits 4, 5, 6 and 7) refer to the region around Wellington.

While we have strong evidence to suggest that Steve Kowhai resides or operates in the vicinity of Eastbourne, New Zealand, we are unable to determine whether this is his permanent base of operations. He could have alternatively travelled specifically to the Wellington region for the purpose of dealing with drugs.

4.2. Suspect's Intentions Relating to John Fredricksen

Our investigation has led us to believe that there is strong evidence pointing to Steve Kowhai communicating with John Fredricksen with the purpose of obtaining or purchasing

Methamphetamine. In this case, we believe John Fredricksen to be acting in the role of the dealer, while the suspect Steve Kowhai was the buyer of the drugs.

4.2.1. Initial Communication

With reference to Exhibits 9 (Discord Outgoing Message Cache) and 10 (Discord Chat Logs), we believe that Steve Kowhai (crayfish1980) first initiated communications with John Fredricksen (heresjohnny1) through the discord communications platform on 2019-01-29 05:29:39.162 SGT.

Steve Kowhai begins by requesting for a “new delivery”, to which John Fredricksen replies that he has a “new supplier” and seeks to confirm Steve Kowhai’s interest. When combined with images such as Exhibits 1 and 2, and search terms such as “cutting agents for ice” in Exhibit 15, we strongly believe that the “delivery” and “supplier” were referring to Methamphetamine. This corresponds to the Methamphetamine seized by Customs officers at Wellington Airport

4.2.2. Destination Selection and Subsequent Communications

Based on the search engine queries from Exhibits 13 (Google Chrome History) and 15 (Microsoft Edge History), it can be observed that Kowhai had performed prior research into topics such as “best places to trade drugs” and potential meeting points such as “courteney place”, “wellington libraries" and “eastbourne library”. The intended meeting location was communicated to John Fredricksen over Discord on 2019-02-02 10:30:36.655 SGT to meet at the Eastbourne Library, and alternatively 666 Rewera Avenue if they missed each other, evident from Exhibit 9 (Discord Outgoing Message Cache). This information is corroborated by Jane Esteban when she was questioned by Customs officers after being arrested at Wellington Airport. In addition, it is extremely likely that specific directions were provided to John Fredricksen and Jane Esteban in the means of Exhibits 4 (airport crystals.jpg) and 5 (dropoff.jpg) in order to assist them in navigating to the location to deliver the drugs.

We also conclude that Fredricksen subsequently sent an image to Kowhai. This intention was communicated by a message sent by Fredricksen through Discord to Kowhai on 2019-02-01 05:04:31.629 SGT, asking Kowhai for suggestions on methods to send “an image of something ... to be done safely”, referencing Exhibit 10 (Discord Chat Logs). Our further analyses of the information present on the drive image revealed that the Image Steganography program was suggested to Fredricksen by Kowhai, which the former had used to hide the package.jpg image (Exhibit 17 - Image Hidden With Steganography) within the BNE.png image (Exhibit 8), protected with the password “Elchapo2” (Exhibit 17). The BNE.png image was then sent via email to Kowhai to his account crayfish1980@protonmail.com, which Kowhai then downloaded to his computer, before retrieving the hidden image with the same software. The hidden image was highly likely intended to depict how Fredricksen had hidden the Methamphetamine within the lining of the suitcase he brought to Wellington and which was discovered by Customs at the airport. The purpose of this communication was to inform Kowhai on where he could find the drugs within the suitcase.

Thus we conclude that based on the evidence available to us, Kowhai had approached Fredricksen with the main purpose of obtaining a shipment of Methamphetamine delivered to Eastbourne Library with 666 Rewera Avenue as an alternative destination. They further communicated with each other to exchange details about how the drugs were packaged, along with means of navigation to the meeting points.

4.3. Suspect's Future Plans and Intentions

Based on the available evidence, we believe that Steve Kowhai's intentions after receiving the Methamphetamine include further processing of the drugs and distribution, subsequently also involving the scaling up of operations

4.3.1. Processing and Distribution of Methamphetamine

Assuming that Steve Kowhai would have been able to successfully retrieve the suitcase containing the Methamphetamine from either Eastbourne Library or 666 Rewera Avenue, we believe that his subsequent intentions were to first process the drugs. This is supported by Exhibit 15 (Microsoft Edge History), where Kowhai had searched up terms such as "cutting drugs" and "cutting agents for ice". Research has led us to believe that the process of cutting drugs involves diluting the substance's purity or enhancing its effects, often being a step in processing before distribution of drugs.

Additionally, search terms from Exhibit 13 (Google Chrome History) such as "best places to trade drugs" show that Kowhai may have had further intentions to either trade or sell the drugs in his possession. Search terms such as "international drug routes" also further support the possibility of Kowhai seeking to distribute the drugs in his possession.

Steve Kowhai may have also been planning routes that may be associated with the processing and distribution of the Methamphetamine. Exhibit 7 (Method run.jpg) indicates one possible route, with the area of Eastbourne marked as "Home", also potentially demonstrating Kowhai's intention to base his operations out of Eastbourne.

4.3.2. Money Laundering

Referring to Exhibit 15, there were searches made for "how to launder money". This lends credence to the possibility that Steve Kowhai was primarily intending to sell the drugs in his possession, before considering potential ways to launder this profits from the sale.

4.3.3. Expanding Scale of Operations

Exhibit 10 (Discord Chat Logs) indicates that Steve Kowhai initially indicated to John Fredricksen that he wanted "10 keys" of what we now understand to be Methamphetamine in a message on 2019-01-30 06:58:49.823 SGT. However, Fredricksen then replied, suggesting that they reduce the size of the delivery to "1 key" to ensure that it can be delivered successfully first, before increasing the scale of deliveries. This gives us evidence that Kowhai harboured the intention to use this meeting between him and Fredricksen as a scaled-down trial-run, ensuring its success before scaling up their operations - increasing the amount of Methamphetamine delivered to Kowhai by Fredricksen. Additionally, while Exhibits 3 (eight_col_patches_crp.jpg) and 13 (Google Chrome History) contain potential

links to gang-related activities, we are hesitant to make such conclusions as we were unable to locate definitive links between Kowhai and active gangs in the evidence available to us.

4.4. Role of Jane Esteban

Based on the evidence available thus far, while there does seem to be some form of association between Jane Esteban, John Fredricksen and the suspect Steve Kowhai, the team is unable to ascertain with confidence the role of Jane Esteban in this case. The team is only able to show that the information provided by Jane Estaben through her questioning corresponds to the information that is found from the seized computer, such as the primary and secondary meeting locations. Additionally, there is likely some premeditated intention to include Jane Esteban in some manner with regards to the transaction of the Methamphetamine, primarily supported by Exhibit 6 (flightbookings.PNG), which indicates that the flights to and from Wellington were booked for 2 adults. Therefore, while we believe that Jane Esteban was involved to a certain extent in the dealings of Methamphetamine between John Fredricksen and Steve Kowhai, based on the currently available acquired evidence, we are unable to ascertain her exact role and her guilt in this case.

4.5. Other Interesting Findings

4.5.1. Possible Presence of Encrypted Contents

Thus far, we have been able to associate several of the evidence artefacts with the list of user-installed programs stated in Section 3.2, one exception being TrueCrypt. We are confident that Steve Kowhai had intentionally installed the program in order to encrypt or decrypt contents to ensure its confidentiality, however we were not able to locate with confidence any files that may have undergone this process within the drive image.

However, there is a file named “secret” with the path of /img_Narcos-1.img/vol_vol7/Users/Steve/Documents/secret and size of 0 bytes which has been deleted (currently unallocated). We were unable to retrieve any useful information or content of this file, thus we suspect that a program such as CCleaner may have been used to wipe the contents and metadata from the entire file from the file system of the drive. Further considering the name of the file, we suspect that this file may have been associated with the use of TrueCrypt to ensure its confidentiality via encryption, although this cannot be definitively proven by the team.

4.5.2. Deleted Open Document Format File

File Name	Memo Things.lnk
File Path	/img_Narcos-1.img/vol_vol7/Users/Steve/AppData/Roaming/Microsoft/Windows/Recent/Memo Things.lnk
File Size	757 bytes

Hash Value	MD5: 05585385F29613AF82B1EF02834015DD SHA1: C718176DF630D199B16202A865A44536CAFA7DF2
Modified Time	2019-01-30 07:44:49 SGT
Accessed Time	2019-01-30 07:44:49 SGT
Created Time	2019-01-29 04:55:19 SGT
Status	Allocated
Target Path	C:\Users\Steve\Documents\Misc\Memo Things.odt

In the list of recently accessed documents we were able to locate an entry that pointed to the directory C:\Users\Steve\Documents\Misc\Memo Things.odt. In searching for the file, we were unable to find any signs of its presence, likely indicating that the contents and metadata of the file had already been completely deleted from the file system. Despite this, from the file extension within the link file, we are able to ascertain that it is an Open Document Text (.odt) file. Furthermore, we believe this document to be of interest as “Memo Things.odt” is not expected to be a default file for OpenOffice installations. This, combined with the presence of the OpenOffice program installed by Steve Kowhai on the computer, shows that he likely used it to open Memo Things.odt. However, we are unable to ascertain the contents of this text document.

5. Conclusion

Following our comprehensive analysis on this case, we can conclude that the suspect is an individual named Steve Kowhai, who is likely based out of the vicinity of Eastbourne, New Zealand.

Kowhai's relationship with John Fredricksen, who was one of the individuals searched and arrested by Customs at Wellington Airport, was that he intended to purchase Methamphetamine from Friedrickson as indicated by their Discord communications (Exhibits 9 and 10). Kowhai and Fredricksen had further communications over Discord regarding how the drugs were packaged into the linings of the suitcase (Exhibit 17), primary and secondary meeting points (Exhibits 4 and 5), and the itinerary of Fredricksen and Jane Esteban (Exhibit 6).

The evidence available to us leads us to believe that Kowhai had intentions of further processing and distribution of Methamphetamine in the future, and potentially for money laundering purposes, as evidenced by Steve's web history data (Exhibits 13 and 15).

Lastly, with the currently available information, we are unable to determine with certainty the role of Jane Esteban in this case. While the evidence points that she likely intended to travel with Fredricksen (Exhibit 6), and that the information revealed during the process of questioning largely corroborates with our analysis of the evidence, our stance is that there exists insufficient evidence to pass judgement on Jane Esteban regarding her guilt in the case.

6. Appendix

6.1. Autopsy String Search Terms

John
Jane
Methamphetamine
Drugs
Eastbourne
666 Rewera
Wellington
crayfish1980
Steve kowhai
heresjohnny1