IFS4102 Digital Forensics

AY2023/24 Semester 2

Case 2 Analysis Report

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

Table of Contents

Table of Contents **2**
1. Executive Summary **5**
2. Case Overview **6**
2.1. Case Description and Background 6
2.2. Evidence Analysed 6
2.3. Tools Used 7
3. Evidence and Findings (Narcos-2) **8**
3.1. System Information 8
3.1.1. Operating System Information 8
3.1.2. Drive Information 8
3.2. User Installed Programs 9
3.2.1. OpenOffice 4.1.6.9790 9
3.2.2. Baidu Antivirus 5.4.3.147185 9
3.2.3. Discord 0.0.304 9
3.2.4. Image Steganography 1.5.2 9
3.2.5. Mozilla Firefox 64.0.2 9
3.2.6. TrueCrypt 7.1a 9
3.3. Images 11
3.3.1 Exhibit A1 (BNE.png) 11
3.3.2 Exhibit A2 (Steve K.PNG) 12
3.3.3 Exhibit A3 (shipping.PNG) 12
3.3.4 Exhibit A4 (Janes Kids.jpg) 14
3.3.5 Exhibit A5 (package.jpg) 15
3.4. Documents & Files 16
3.4.1. Exhibit A6 (clients.ods) 16
3.4.2. Exhibit A7 (Attachments-Important, crucial to our method.zip) 16
3.4.3. Exhibit A8 (secret) 17
3.4.4. Exhibit A9 (Memo Things.odt) 18
3.4.5. Exhibit A10 (Contact_Card.zip) 20
3.4.6. Exhibit A11 (Contact Card.exe) 21
3.5. Communications 24
3.5.1. Exhibit A12 (Discord Chat Logs) 24
3.5.2. Exhibit A13 (ProtonMail Account) 27
Received Emails 27
Sent Emails 28
3.6. Web Data 30
3.6.1. Exhibit A14 (Microsoft Edge History) 30
Items of Interest in Search History 30
3.6.2. Exhibit A15 (Mozilla Firefox History) 31
Items of Interest in Search History 31
4. Evidence and Findings (Narcos-3) **33**

4.1. System Information 33
4.1.1. Operating System Information 33
4.1.2. Drive Information 33
4.2. User Installed Programs 34
4.2.1. Discord 0.0.304 34
4.2.2. Quasar v1.3.0.0 34
4.3. Images 35
4.3.1. Exhibit B1 (afp.png) 35
4.3.2. Exhibit B2 (background.png) 35
4.3.3. Exhibit B3 (contact-card-512.png) 36
4.3.4. Exhibit B4 (crys1.jpg) 37
4.3.5. Exhibit B5 (crys2.jpg) 38
4.3.6. Exhibit B6 (crys3.jpg) 39
4.4. Documents & Files 41
4.4.1. Exhibit B7 (course-undercover-survival.pdf) 41
4.4.2. Exhibit B8 (01-30-2019.html) 42
4.4.3. Exhibit B9 (01-31-2019.html) 44
4.4.4. Exhibit B10 (02-01-2019.html) 45
4.4.5. Exhibit B11 (02-02-2019.html) 47
4.4.6. Exhibit B12 (Contact Card.zip) 49
4.4.7. Exhibit B13 (Contact Card.exe) 50
4.5. Web Data 51
4.5.1. Exhibit B14 (Microsoft Edge History) 51
Items of Interest in Search History 51
4.5.2. Exhibit B15 (Microsoft OneDrive Cache) 53
5. Analysis **55**
5.1. Identity of Jane Esteban 55
5.2. Relations Between John Fredricksen and Jane Esteban 56
5.3. Guilty Parties in the Case 56
Steve Kowhai 56
John Fredricksen 57
Jane Esteban 57
5.4. Future Plans and Intentions of Guilty Parties 58
Steve Kowhai 58
John Fredricksen 58
5.5. Further Action 58
5.5.1. Thumbdrive Analysis 58
5.5.2. Mobile Device Examination 59
5.5.3. Protonmail Access 59
5.5.4. Memory Dump Analysis 59
6. Conclusion **60**
7. Appendix **61**
7.1. Combined Timeline of Events 61
2019-01-23 61

2019-01-28 61
2019-01-29 61
2019-01-30 61
2019-01-31 62
2019-02-01 62
2019-02-02 62
2019-02-16 62
2019-02-23 62
7.2. Autopsy String Search Terms 63

1. Executive Summary

Adding onto the conclusions drawn from our Case 1 Report, and combined with newly available evidence, our forensic analyses has led us to believe that Jane Esteban is part of the Australian Federal Police, serving as an undercover agent with the goal of discovering and prosecuting drug-related activities. She initially approached John Fredricksen attempting to purchase drugs, but was eventually threatened to accompany Fredricksen to Wellington to deliver the drugs to Kowhai, such that Fredricksen could reduce suspicion on him.

We thus believe two suspects to be guilty in light of the overall case and all available evidence - Steve Kowhai of intention to traffic and produce controlled drugs, and money laundering; and John Fredricksen of trafficking and import of controlled substances.

Considering their future plans and intentions, we believe that if Steve Kowhai was able to obtain the methamphetamine from John Fredricksen, he would continue to scale up subsequent shipments of the drug from Fredricksen, and to process and redistribute the drugs in his possession. We also believe that John Fredricksen is likely to continue supplying his current clients, and also is considering opportunities to seek new clients with larger orders.

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, John Fredricksen and Jane Esteban. 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. One kilogram of Methamphetamine was located in the lying of John Fredricksen's suitcase.

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 under instruction from John Fredricksen. Customs raided that address and seized a desktop computer in the living room of the suspect.

Through our forensic analysis of the drive image in the Case 1 report, we concluded that this desktop computer belonged to Steve Kowhai, who had communicated with John Fredricksen with the purpose of obtaining or purchasing Methamphetamine, and for both parties to meet at either Eastbourne Library or 666 Rewera Avenue for the exchange of the drugs. We highly suspect that Kowhai had the intention to further process and to sell the drugs, and intended to launder the proceeds from the sale, before scaling up his operations. At the time of concluding investigations of Case 1, we were unable to ascertain the role of Jane Esteban in the case and her guilt.

We have since been provided with extra evidence by Customs officers in the form of the images and memory dumps of two seized laptops. The purpose of this second case is to carry out further forensic examination on the newly available evidence, to further understand the motives, goals and objectives of John Fredricksen, Jane Esteban and Steve Kowhai. This report should be read in conjunction with the Case 1 report previously submitted.

2.2. Evidence Analysed

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 for the first laptop: `cmd /c copy /b Narcos-2.* Narcos-2.img`
2. Combining the split drive image files for the second laptop: `cmd /c copy /b Narcos-3.* Narcos-3.img`
3. Combining the split memory dump files for the first laptop: `cmd /c copy /b Narcos-Mem-2.* Narcos-Mem-2.raw`

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

No	File Name	SHA1 Checksum	Size
1	Narcos-2.img	576d20ffc835d98724e472c1714eaecff37f13d1	30 GB
2	Narcos-Mem-2.raw	3d6f1ff3e3d61b42837a7ebf0ffe058433c6282f	4 GB
3	Narcos-3.img	57c9a704b09fbb50118da57f62546824e062a73a	30 GB
4	Narcos-Mem-3.raw	90b3d8ba9e96373c96ee9460193c1b585eadb009	4 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
MZHistoryView	1.70
TheSleuthKit	4.12.1
Image Steganography	1.5.2
TrueCrypt	7.1a

3. Evidence and Findings (Narcos-2)

3.1. System Information

3.1.1. Operating System Information

Name: JOHNFLAPTOP1
Version: Windows 10 Pro
Processor Architecture: AMD64
Product ID: 00330-80000-00000-AA310
Owner: JohnF

3.1.2. Drive Information

Type: Image
Size: 32212254720 bytes (30.0GB)
Sector Size: 512 bytes
Device ID: b6ef7f3b-8930-4671-8133-d8a69df8774e
Layout:

Name	Description	Starting Sector	Ending Sector	Length in Sectors	Flags
vol1	Unallocated	0	2047	2048	Unallocated
vol4	Basic data partition	2048	1023999	1021952	Allocated
vol5	EFI System partition	1024000	1226751	202752	Allocated
vol6	Microsoft reserved partition	1226752	1259519	32768	Allocated
vol7	Basic data partition	1259520	62912511	61652992	Allocated
vol8	Unallocated	62912512	62914559	2048	Unallocated

3.2. User Installed Programs

3.2.1. OpenOffice 4.1.6.9790

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

- Installer Location: /img_Narcos-2/vol_vol7/Users/JohnF/Downloads/Apache_OpenOffice_4.1.6_Win_x86_install_en-US.exe
- Executable Location: /img_Narcos-2/vol_vol7/Program Files (x86)/OpenOffice 4/program/soffice.exe

3.2.2. Baidu Antivirus 5.4.3.147185

Baidu Antivirus is a host-based anti-malware solution offered by Baidu.

- Installer Location: /img_Narcos-2/vol_vol7/Users/JohnF/Downloads/BavPro_Setup_Mini_C1.exe
- Executable Location: /img_Narcos-2/vol_vol7/Program Files (x86)/Baidu Security/Baidu Antivirus/5.4.3.147185.0/Bav.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-2/vol_vol7/Users/JohnF/Downloads/DiscordSetup.exe

3.2.4. 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-2/vol_vol7/Users/JohnF/Downloads/Image Steganography 1.5.2 Setup.exe
- Executable Location: /img_Narcos-2/vol_vol7/Users/JohnF/AppData/Roaming/CPascoe/Image Steganography/ProgData/Image Steganography.exe

3.2.5. Mozilla Firefox 64.0.2

Firefox is an open-source web browser developed by the Mozilla Foundation.

- Installer Location: Unknown
- Executable Location: /img_Narcos-2/vol_vol7/Program Files/Mozilla Firefox/firefox.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-2/vol_vol7/Users/JohnF/Downloads/TrueCrypt Setup 7.1a.exe
- Executable Location: /img_Narcos-2/vol_vol7/Program Files/TrueCrypt/TrueCrypt.exe

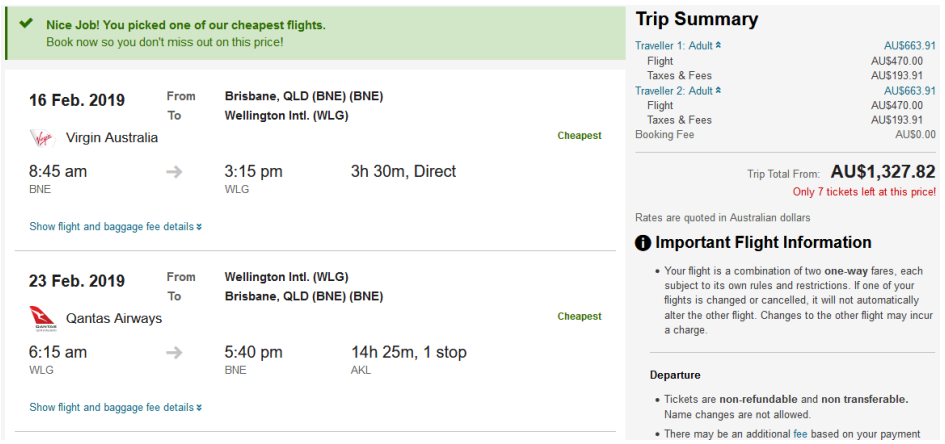
3.3. Images

3.3.1 Exhibit A1 (BNE.png)

File Name	BNE.png
File Path	/img_Narcos-2/vol_vol7/Users/JohnF/Pictures/BNE.png
File Size	4376793 bytes
Hash Value	MD5: DFFA98BDD7371D1806ADB09DB27BA283 SHA1: 0897FAA06FBB6E0D678A9497B6F5D330F231362F
Modified Time	2019-02-01 07:05:17 SGT
Accessed Time	2019-02-01 08:06:04 SGT
Created Time	2019-02-01 07:05:17 SGT
Status	Allocated
Content	

This image depicts the skyline of a developed city. Based on the file hashes, it is the same file as Exhibit 8 (BNE.png) from Case 1. Thus, we can conclude that this was the file sent from John Fredricksen to Steve Kowhai. This image file has an image, Exhibit 17 (Image Hidden With Steganography) hidden in the image and encrypted with the password “Elchapo2” with the Image Steganography software. From prior investigation in Case 1, we concluded that it contained an image (Exhibit 17 from Case 1 and Exhibit A5 from Case 2) titled package.jpg which shows packages of Methamphetamine and the exposed lining of a suitcase.

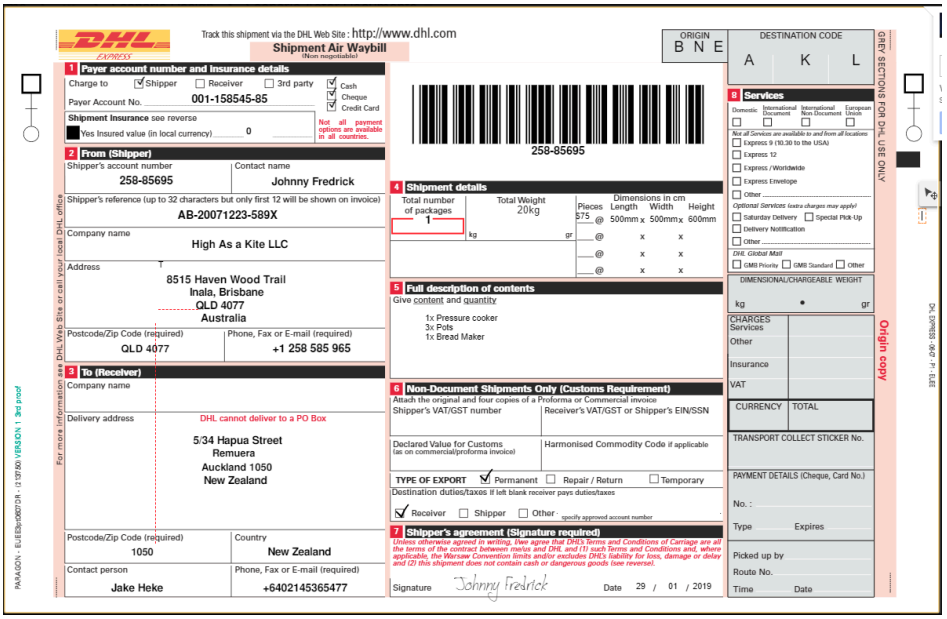
3.3.2 Exhibit A2 (Steve K.PNG)

File Name	Steve K.PNG
File Path	/img_Narcos-2/vol_vol7/Users/JohnF/Documents/Business/Steve K.PNG
File Size	52971 bytes
Hash Value	MD5: D1B21A1CDDCB3494D637F2424CC5F0F1 SHA1: 856E13E9C8E8B46DE1C1DD35B5FF49F6537EB870
Modified Time	2019-02-02 06:43:21 SGT
Accessed Time	2019-02-02 09:57:27 SGT
Created Time	2019-02-02 06:43:20 SGT
Status	Allocated
Content	

This screen capture of a trip summary of return flights booking 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. This image is the same as the image found on Steve Kowhai's drive image, stated as Exhibit 6 (flightbookings.PNG) in the Case 1 report. Current analysis of the two newly acquired images confirms to us that the second passenger was meant to be Jane Esteban. Thus, based on prevailing evidence available to us, we believe that Fredricksen had communicated this image to both Steve Kowhai and Jane Esteban.

3.3.3 Exhibit A3 (shipping.PNG)

File Name	shipping.PNG
File Path	/img_Narcos-2/vol_vol7/Users/JohnF/Documents/Business/shipping.PNG
File Size	bytes

Hash Value	MD5: 4FDF3DD6BAC6BA99F6EAFCEDD9A64EFA SHA1: E8D2D97BE5621EB02FD9438B4E907632CD2C607A
Modified Time	2019-01-23 09:18:28 SGT
Accessed Time	2019-01-29 11:58:47 SGT
Created Time	2019-01-23 09:18:28 SGT
Status	Allocated
Content	

This exhibit is a photo of a DHL Shipping label. The contact name is listed as Johnny Fredrick, which we observe to be a modified version of John Fredricksen, potentially in an attempt to reduce suspicion from the shipping company or Customs authorities, and to remove any possible connections tying the package back to Fredricksen. The sending company name is stated as “High As a Kite LLC”, which we believe is not an actual entity, but a word-play on the outcome of getting “high” from drugs. The sender address is stated as “8515 Haven Wood Trail, Inala, Brisbane, QLD 4077, Australia”, and the contact number is +1 258 585 965. This sending address is of significant importance to us, especially when combined with Exhibit A15 (Mozilla Firefox Search History), where Fredricksen had searched for “directions from Inala to brisbane airport”. This leads us to believe that Fredricksen is primarily based out of Inala, Brisbane Australia.

The receiver is stated as Jake Heke, with a contact number of +6402145365477 and an address of 5/34 Hapua Street, Remuera, Auckland 1050, New Zealand. This name and region can be found in Exhibig A6 (clients.ods). We thus believe that this is evidence of a separate transaction of drug trafficking from that of Steve Kowhai, likely including a shipment of 10 kilograms of “tweak”, which is a slang name used in place of Methamphetamine. Furthermore, considering that the second leg of flights stated in Exhibit A2 (Steve K.PNG) involves a stopover in Auckland, before completing the return flight to Brisbane, we strongly believe that Fredricksen, along with Esteban, had intended to complete two shipments of drugs to Steve Kowhai and Jake Heke in Wellington and Auckland respectively. The shipping

label was signed on 2019-01-29 which is almost one month before the flight that stops at Auckland on 2019-02-23. Thus, we are confident to conclude that Fredricksen visited Auckland in association with this transaction.

The contents of the shipment are stated as one pressure cooker, 3 pots and 1 bread maker, with a combined weight of 20 kilograms. Fredricksen could be observed searching for avenues to obtain these objects from Exhibit A15 (Mozilla Firefox Search History). We feel that it could be possible that Fredricksen intended for the Methamphetamine destined for Heke to be concealed within these objects. However, we do not have conclusive evidence to prove so. Furthermore, this could be a trial run to assess the feasibility of shipping drugs via DHL to Auckland, ensuring its success before commencing the shipment of actual drugs.

3.3.4 Exhibit A4 (Janes Kids.jpg)

File Name	Janes Kids.jpg
File Path	/img_Narcos-2/vol_vol7/Users/JohnF/AppData/Local/Temp/vmware-JohnF/VMwareDnD/2cce6695/Janes Kids.jpg
File Size	200136 bytes
Hash Value	MD5: 1B4BA1D430AB0F4A5F1698EC481A8F93 SHA1: 13E3EF512610EE36238BFAFF690D253CE39C5AF3
Modified Time	2019-01-23 10:29:42 SGT
Accessed Time	2019-01-31 08:20:56 SGT
Created Time	2019-01-23 10:29:41 SGT
Status	Allocated
Content	

The photo of two children is saved with the title of “Janes Kids”. There is significant reason for us to believe that these children are related to Jane Esteban, which John Fredricksen used in an attempt to blackmail her based on Exhibit A12 (Discord Chat Logs).

3.3.5 Exhibit A5 (package.jpg)

File Name	package.jpg
File Path	/img_Narcos-2/vol_vol7/Users/JohnF/AppData/Local/Temp/vmware-JohnF/VMwareDnD/770cd05f/package.jpg
File Size	83781 bytes
Hash Value	MD5: 8BA9265A1563FF871A471C552BAB0B67 SHA1: 69BBE11C8646E5E1633C0C1772D88A520C9E1C11
Modified Time	2019-02-01 07:02:24 SGT
Accessed Time	2019-02-01 07:04:37 SGT
Created Time	2019-02-01 07:02:24 SGT
Status	Allocated
Content	

This image shows a suitcase with its base layer revealed, along with three rectangular shaped objects wrapped in brown tape. Based on the file hash, it is the same image as found in Exhibit 17 (Image Hidden With Steganography) from Case 1. The presence of this file on Fredricksen’s laptop confirms our prior conclusion that the purpose of this photo was for Fredricksen to communicate where the drugs would be hidden within the suitcase, such that Steve Kowhai may be able to successfully retrieve it later.

3.4. Documents & Files

3.4.1. Exhibit A6 (clients.ods)

File Name	clients.ods
File Path	/img_Narcos-2/vol_vol7/Users/JohnF/Documents/Business/clients.ods
File Size	15077 bytes
Hash Value	MD5: DB804B47095901E20D6666B1E9A56003 SHA1: 4FB8EB9BD132B02EF413356FE9F3308155BAD977
Modified Time	2019-01-29 12:02:47 SGT
Accessed Time	2019-01-30 08:04:14 SGT
Created Time	2019-01-29 04:26:09 SGT
Status	Allocated
Content	

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

This is an OpenDocument spreadsheet document. Based on the name of the file, along with its contents, we strongly believe that John Fredricksen used this spreadsheet to track the list of clients he is serving. The spreadsheet contains the name of several individuals, their locations, products, amounts and frequency of delivery. Based on research of the product terms found in the spreadsheet, we understand them to be colloquial terms to refer to different types of drugs.

3.4.2. Exhibit A7 (Attachments-Important, crucial to our method.zip)

File Name	Attachments-Important, crucial to our method.zip
File Path	/img_Narcos-2/vol_vol7/Users/JohnF/Downloads/Attachments-Important, crucial to our method.zip

File Size	5242990 bytes
Hash Value	MD5: 7774E97391FE79E3CA91141CA36412AF SHA1: B32C52C3996F8DA4572419308541A374CC8AB9F0
Modified Time	2019-01-30 08:00:16 SGT
Accessed Time	2019-01-30 08:00:50 SGT
Created Time	2019-01-30 08:00:16 SGT
Status	Allocated

This ZIP file was found in the Downloads folder for the Windows user JohnF. It contains a single without extensions named “secret”, which is further elaborated as Exhibit A8. We believe that this ZIP file was downloaded as an attachment from John Fredricksen’s ProtonMail account, as elaborated in Exhibit A13 (ProtonMail Account).

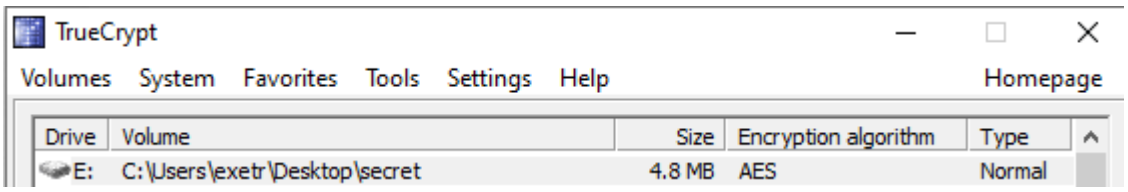
3.4.3. Exhibit A8 (secret)

File Name	secret
File Path	N/A (extracted from ZIP archive)
File Size	5242880 bytes
Hash Value	MD5: 173094089256DFA0BBF2C682DF261B5F SHA1: 5CC9A45816B689FEB43E62C36A4496411EC316E5
Modified Time	2019-01-29 23:59:50 SGT
Accessed Time	N/A (extracted from ZIP archive)
Created Time	N/A (extracted from ZIP archive)
Status	N/A (extracted from ZIP archive)

The “secret” file extracted from the ZIP archive previously mentioned as Exhibit A7 appears to bear some form of relation to the file with the same name we previously discovered in Case 1, which we labelled as a potentially interesting finding under “Possible Presence of Encrypted Contents”.

Further evidence retrieved from this case has confirmed our prior suspicion that this file was used as an encrypted volume under the TrueCrypt program, shown by the details from Exhibit B8 (01-30-2019.html). Effectively, John Fredricksen was observed to be active on the TrueCrypt program, where he attempted to enter the password for the file located at “C:\Users\JohnF\Downloads\Attachments-Importa...\secret” at 2019-01-30 10:04. The password he supplied to the program was “ilovediving”.

Subsequently, we used the same version of TrueCrypt and attempted to mount and decrypt this “secret” file to our forensics workstation. We were able to successfully mount a drive with a size of 4.8MB that was encrypted with the AES algorithm as shown below.



Furthermore, Exhibit A13 (ProtonMail Account) shows us that John Fredricksen (heresjohnny1@protonmail.com) had received an email from Steve Kowhai (crayfish1980@protonmail.com) on 2019-01-30 07:40:00 SGT with the “secret” file as an attachment. Kowhai confirmed the file as an encrypted volume, and suggested the use of TrueCrypt to decrypt it.

From the available evidence, we can confirm that the contents within the encrypted volume originated from Steve Kowhai and were intended for John Fredricksen. Furthermore, we believe that shortly after creating and sending the encrypted volume, Steve Kowhai had intentionally deleted all file contents and metadata related to this file. This confirms our suspicions of the possible presence of encrypted contents in Steve Kowhai’s desktop computers as stated in Section 4.5.1 of the Case 1 report.

3.4.4. Exhibit A9 (Memo Things.odt)

File Name	Memo Things.odt
File Path	N/A (extracted from TrueCrypt volume)
File Size	832662 bytes
Hash Value	MD5: 18302CE1440A264FDD66BA51E1DC9AC2 SHA1: B6C929EF7513C5F517FE0D71E6582038E9912EA7
Modified Time	2019-01-30 05:13:50 SGT
Accessed Time	N/A (extracted from TrueCrypt volume)
Created Time	N/A (extracted from TrueCrypt volume)
Status	N/A (extracted from ZIP archive)

Contents

Crystal Method

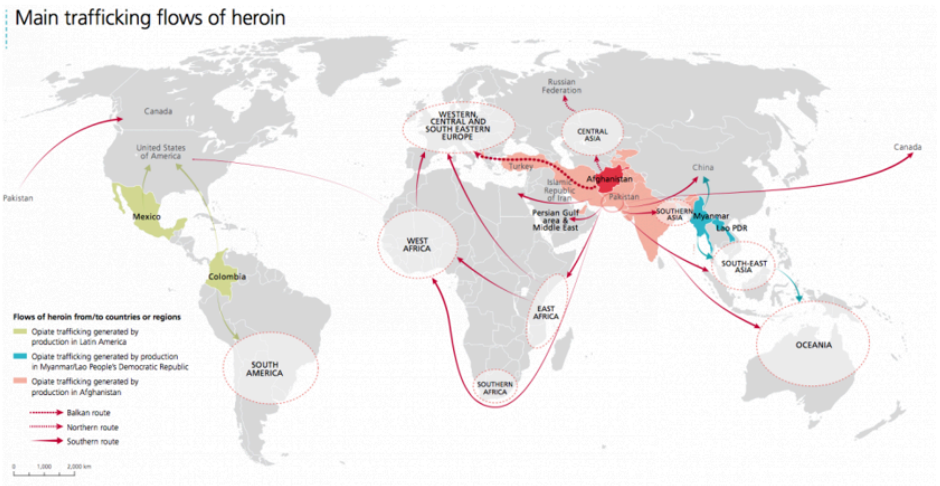
Destination – Wellington
Product – 1 kg crystal
Source – Brisbane (JF)

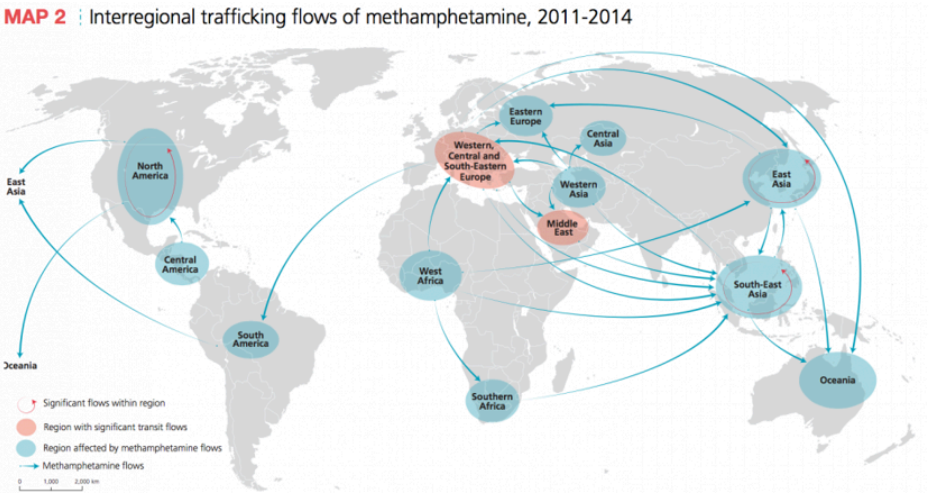
Wellington is part of the lower north island of New Zealand. It is accessable by road and sea. As tempting as the sea is, be aware that the coast of NZ may seem ideal, but everyone knows it's vulnerable as there have been several news reports about it.

The product is coming from Brisbane, Australia and as a result, will need to be delivered by sea or plane. Shipping the product would be ideal, the risk of detection is lower but would result in higher costs for a small amount of product. The product being delievered is only a test to check it's quality and will be the deciding factor in any decision to continue doing business with you. If the product is up to scratch, I will buy a larger supply next time. If we continue to do business it might be more practical to use shipping for future transactions.

This consignment will be delievered by plane, which will decrease travel time and lower the cost for all parties involved. Delievery by plane will bring along with it its own complications such as concealment, security screening/checks and drug dogs. I trust that you are aware of the risks and will take all necessary precautions.

Below is a map of drup flows from countires, could give us some info for later trades and where we can get more product from in the future.





Within the mounted drive from Exhibit A8, we were able to locate a single file named Memo things.odt. It is an OpenDocument Text file, which contains a document outlining “Crystal

Method". The contents of this document are presented as a proposal for the delivery of 1 kilogram of crystal (colloquial term used to refer to Methamphetamine) to Wellington originating from Brisbane. The source is stated along with "JF", which is also the initials for John Fredricksen. The contents of the document continue to elaborate on the implications, feasibility and possible modes of transport for delivering Methamphetamine into New Zealand from Brisbane. The contents of this file confirms our prior conclusions from the Case 1 report, that Steve Kowhai had requested for a shipment of 1 kilogram of Methamphetamine to be delivered to Wellington by John Fredricksen. Furthermore, this initial delivery had the purpose of validating the viability of such shipments, with intentions of scaling up future shipments. Considering that Kowhai had sent this file encrypted in a TrueCrypt volume to Fredricksen as observed from Exhibit A13 (ProtonMail Account), we can conclude that its purpose was for Kowhai to communicate both his current and future intentions to Fredricksen.

Similar to Exhibit A8 (secret), appears to bear some form of relation to the file with the same name we previously discovered in Case 1, which we labelled as a potentially interesting finding under "Deleted Open Document Format File".

Thus, we conclude that the following was the likely timeline of events:

- Steve Kowhai prepared the OpenDocument Text document with the OpenOffice software on his desktop computer and saved it as "Memo Things.odt". The contents of the word document acted as a proposal which outlined several details and considerations about the delivery of Methamphetamine to Wellington.
- Kowhai then created an AES encrypted volume named "secret" (Exhibit A8) with the TrueCrypt software with the password "ilovediving".
- Mounting this encrypted volume, he then stored the Memo Things.odt file within
- Kowhai attached the "secret" encrypted volume in an email and sent it to John Fredricksen, with instructions on accessing it with the TrueCrypt program and a pre-communicated password as seen in Exhibit A13 (ProtonMail Account)
- Fredricksen downloaded the attachment, decrypted the volume in TrueCrypt with the agreed password, and extracted the Memo Things.odt file

3.4.5. Exhibit A10 (Contact_Card.zip)

File Name	Contact_Card.zip
File Path	/img_Narcos-2/vol_vol7/Users/JohnF/Downloads/Contact_Card.zip
File Size	198604 bytes
Hash Value	MD5: B4526C58D6A1A6D6BD654474A1CE8823 SHA1: 7A5C5482D7B90A3A142695CF11A02C73CF2CAAF8
Modified Time	2019-01-30 06:01:31 SGT
Accessed Time	2019-01-30 06:03:04 SGT
Created Time	2019-01-30 06:01:31 SGT

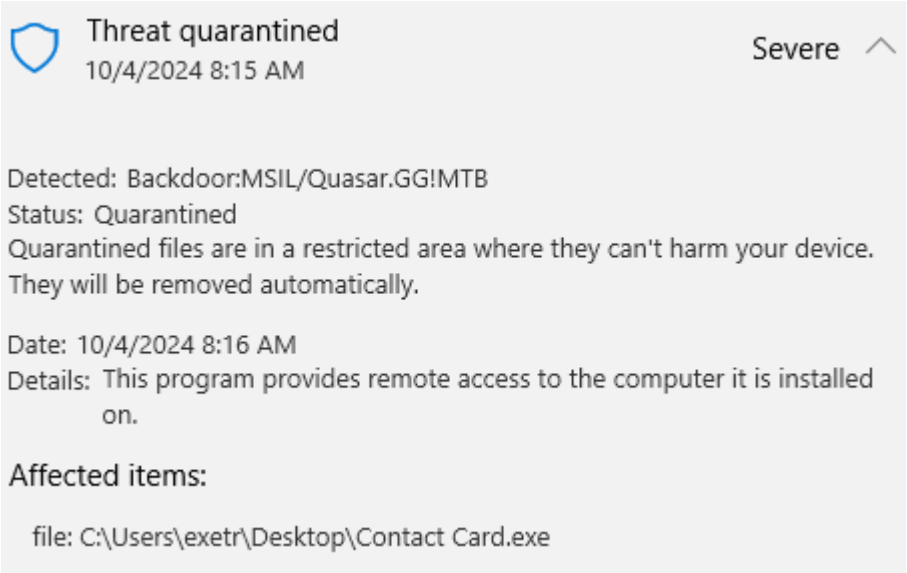
Status	Allocated

This ZIP file was found in the Downloads folder for the Windows user JohnF. It contains a single executable named “Contact Card.exe” (Exhibit A11). From Exhibit A12 (Discord Chat Logs), we can ascertain that this file was sent by Jane Esteban to John Fredricksen over Discord, attached to a message stating “Also I've got some friends that want to score too. Here's their contact card”, sent on 2019-01-29 11:32:45.151 SGT. Furthermore, from analysing Exhibit A14 (Microsoft Edge History), we can further conclude that Fredricksen upon receiving the message on Discord, he proceeded to access the URL https://cdn.discordapp.com/attachments/539556917140521030/539649072802299930/Contact_Card.zip on 2019-01-29 22:01:00 SGT with the Microsoft Edge browser from which this file was downloaded.

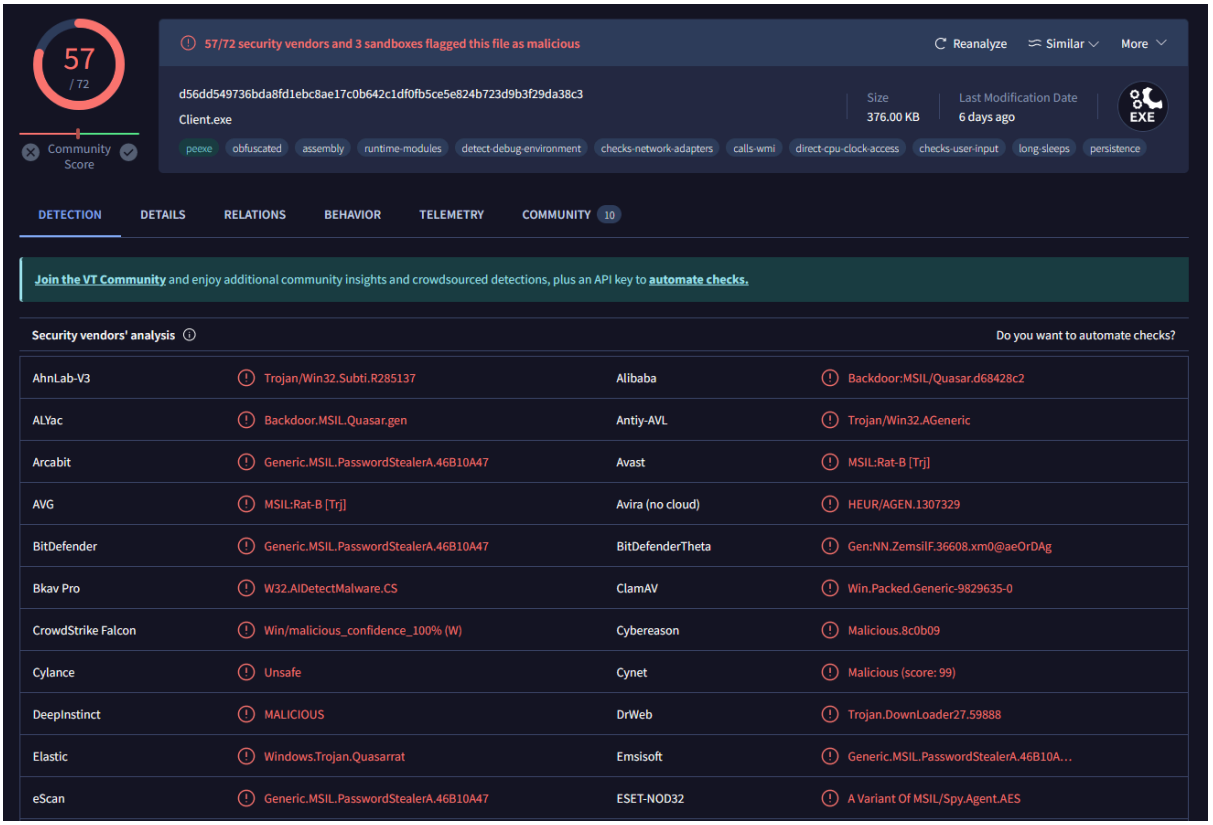
3.4.6. Exhibit A11 (Contact Card.exe)

File Name	Contact Card.exe
File Path	N/A (extracted from ZIP archive)
File Size	385024 bytes
Hash Value	MD5: 409B88B2B275353F2CA05983CEF1ABF5 SHA1: 2FC14E18C0B090D55360E60468489AA65E2375F2
Modified Time	2019-01-29 06:25:08 SGT
Accessed Time	N/A (extracted from ZIP archive)
Created Time	N/A (extracted from ZIP archive)
Status	N/A (extracted from ZIP archive)

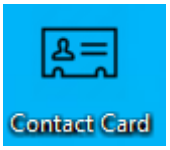
When extracting the contents of the ZIP archive, Windows automatically quarantined the resulting executable, highlighting that it was likely a malware named Backdoor:MSIL/Quasar.GG!MTB. Based on the list of user-installed programs found on the drive image acquired from Jane Esteban’s laptop, we posited that this executable was related to the Quasar 1.3 program found installed on her laptop.



Submitting the executable to Virustotal, we realised that many other anti-malware services reported similar results, that the program was likely a backdoor, and several identified as “Quasar”



When whitelisting the executable from Windows’ anti-malware service, we noted that the icon for the program was the same image as Exhibit B3 (contact-card-512.png).



When combining the facts regarding this executable, along with evidence available to us, we feel that it is extremely likely that this executable was created by Jane Esteban. She had intentionally changed the name to “Contact Card.exe” and changed the icon to one that resembles a contact card. She then compressed it as a ZIP archive, and sent it as an attachment to John Fredricksen over Discord, stating that it was contact information for more interested buyers for more drugs. All these actions were an attempt to masquerade the malicious intent, from both the Windows anti-malware service, and to mislead Fredricksen into running the executable. Based on Exhibit A12 (Discord Chat Logs), we believe that Fredricksen did run the executable, likely in an attempt to obtain the contact information as promised by Esteban, but did not see any feedback, later claiming that it “did not open”.

Further researching on the capabilities offered by Quasar, which is described as a remote administration tool, it operates on a client-server model, where a client will connect back to a server and send information recorded. A server is first initially set up, which can generate and build a standalone client with a set of pre-defined variables such as host name, IP address and port number. When executed, the client will initiate a connection back to the server.

We strongly believe that this executable was the standalone client generated by Esteban. She then sets up a server on her own laptop, and when Fredricksen runs the executable thinking it would show details about potential customers, the client would be set up and start sending information back to the server. One of the monitoring capabilities offered by Quasar is acting as a keylogger. Considering the information found in the Quasar “reports” shown in Exhibits B8 (01-30-2019.html), B9 (01-31-2019.html), B10 (02-01-2019.html) and B11 (02-02-2019.html), which appears to show keypresses, we can ascertain that Esteban had configured the client to act as a keylogger, and to send recorded keypresses back to the server.

Preliminary analysis of the binary by observing the strings found within supports this hypothesis, as we were able to locate the presence of calls to Windows API such as xClient.Core.MouseKeyHook.WinApi, which are present in third party libraries that allow for the monitoring of input devices.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ strings Contact\ Card.exe | grep Hook
xClient.Core.MouseKeyHook
System.Collections.Generic.IEnumerator<xClient.Core.MouseKeyHook.KeyPressEventArgsExt>.get_Current
System.Collections.Generic.IEnumerable<xClient.Core.MouseKeyHook.KeyPressEventArgsExt>.GetEnumerator
System.Collections.Generic.IEnumerator<xClient.Core.MouseKeyHook.KeyPressEventArgsExt>.Current
<keyboardHookStruct>5__4
idHook
CallNextHookEx
SetWindowsHookEx
UnhookWindowsHookEx
HookResult
xClient.Core.MouseKeyHook.WinApi
xClient.Core.MouseKeyHook.Implementation
```

3.5. Communications

3.5.1. Exhibit A12 (Discord Chat Logs)

File Name	f0095872
File Path	/img_Narcos-2/vol_vol7/$CarvedFiles/1/f0095872.gz/f0095872
File Size	11295 bytes
Hash Value	MD5: 20088C57ADEAEDB189B3465A060BD7AA SHA1: CA14444EE7EECD883052C2E036A64A5B37289688
Modified Time	N/A
Accessed Time	N/A
Created Time	N/A
Status	Allocated (Carved from deleted files)
Content	Timestamp: 2019-01-29 11:29:13.328 SGT Username: becomingjane Message: Got any of that ice?? Timestamp: 2019-01-29 11:32:45.151 SGT Username: becomingjane Message: Also I've got some friends that want to score too. Here's their contact card Attachment: Contact_Card.zip (downloaded from https://cdn.discordapp.com/attachments/539556917140521030/539649072802299930/Contact_Card.zip, found in file system as Exhibit A10) Timestamp: 2019-01-30 06:15:24.015 SGT Username: heresjohnny1 Message: Sweet thanks Timestamp: 2019-01-31 07:43:51.346 SGT Username: heresjohnny1 Message: Yo, what you after? Timestamp: 2019-01-31 07:45:17.505 SGT Username: heresjohnny1 Message: Also that contact card didn't open and I can't be bothered with new clients right now... Bigger fish to fry Timestamp: 2019-01-31 07:58:14.054 SGT Username: becomingjane Message: The usual Timestamp: 2019-01-31 08:01:24.337 SGT Username: heresjohnny1 Message: Aight cool, umm actually I have a proposition for ya

Timestamp: 2019-01-31 08:09:48.186 SGT
Username: becomingjane
Message: What is it... ?

Timestamp: 2019-01-31 08:14:25.248 SGT
Username: heresjohnny1
Message: I have a business dealing happening overseas and I need you to accompany me as cover. Everything will be paid for but you need to keep your trap shut

Timestamp: 2019-01-31 08:17:28.473 SGT
Username: becomingjane
Message: Umm I don't know, sounds pretty risky.

Timestamp: 2019-01-31 08:18:20.052 SGT
Username: heresjohnny1
Message: Yea I understand but ill make it worth your while

Timestamp: 2019-01-31 08:18:54.930 SGT
Username: heresjohnny1
Message: Err nah I'm not keen

Timestamp: 2019-01-31 08:21:35.695 SGT
Username: becomingjane
Message: I didn't want to do this but, you leave me no choice

Timestamp: 2019-01-31 08:22:19.809 SGT
Username: heresjohnny1
Message: You don't wanna see them hurt do ya
Attachment: Janes Kids.jpg (downloaded from https://cdn.discordapp.com/attachments/539556917140521030/540325927175979028/Janes_Kids.jpg, found in file system as Exhibit A4)

Timestamp: 2019-01-31 08:24.13.315 SGT
Username: becomingjane
Message: WHAT! Please, I swear whatever you need I'll do it... I've put them through enough as it is. What do you want from me??

Timestamp: 2019-01-31 08:28:17.127 SGT
Username: heresjohnny1
Message: Good, now that's what I wanted to hear. Here is the plan. You and I will be acting like a couple travelling on a holiday to New Zealand. This is what I want you to do: Look the part, act normal, and don't tell anyone about what we're doing. Understood?

Timestamp: 2019-01-31 08:29:00.666 SGT
Username: becomingjane
Message: Yes John... I got it

Timestamp: 2019-01-31 08:31:18.285 SGT
Username: heresjohnny1
Message: Good. Talk tomorrow at 3PM or else

	Timestamp: 2019-02-01 09:59:28.642 SGT Username: heresjohnny1 Message: Right. What's your full name and date of birth? I need it for booking the flights ASAP. Timestamp: 2019-02-02 05:58:11.994 SGT Username: becomingjane Message: My full name is Jane Esteban and my birthday is 13/07/1992 Timestamp: 2019-02-02 08:02:08.234 SGT Username: heresjohnny1 Message: Flights booked. I'll pick you up from the Woolworths (133 Oxley Station Rd, Oxley QLD 407, Australia) at ... Just bring yourself I'll cover everything else

Further examination of files used by the Discord program, along with string analyses of relevant keywords revealed a file with JSON-structured data containing chat logs from the Discord program. 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: heresjohnny1 and becomingjane. Based on case background, along with prior analyses from Case1, we understand heresjohnny1 to be an account used by John Fredricksen. Considering the username of becomingjane and the context of the communications, we conclude that becomingjane was the account used by Jane Esteban.

The communications between Fredricksen and Esteban reveal several further information about the relationship between both individuals and confirms their purpose for travelling to New Zealand

- Jane Esteban (becomingjane) initiates contact with John Fredricksen (heresjohnny1) by requesting for "ice", which is a term normally used to refer to Methamphetamine.
- Esteban further mentions she has friends who would also be interested in obtaining Methamphetamine or drugs, and attaches a ZIP archive to the message. Fredricksen proceeds to download this file, which is found in the file system as Exhibit A10 (Contact Card.zip). Fredricksen subsequently attempts to open the file, but comments that he was unable to do so
- Fredricksen proceeds to propose that Esteban accompany him on a "business dealing happening overseas", to which Esteban rejects. We believe that Fredricksen is referring to the meetup with Steve Kowhai at either Eastbourne Library or 666 Rewera Avenue that is previously elaborated in the report for Case 1.
- Fredricksen proceeds to send a message appearing to threaten Esteban, with an attached photo named "Janes Kids.jpg", suggesting that she would not want to "see them hurt". This image is found in the file system as Exhibit A4.
- Esteban relents and agrees to follow Fredricksen on the trip to Wellington. Fredricksen then further elaborates on his plan, that both of them will travel to New Zealand as a couple on holiday, and requests her to "act normal".

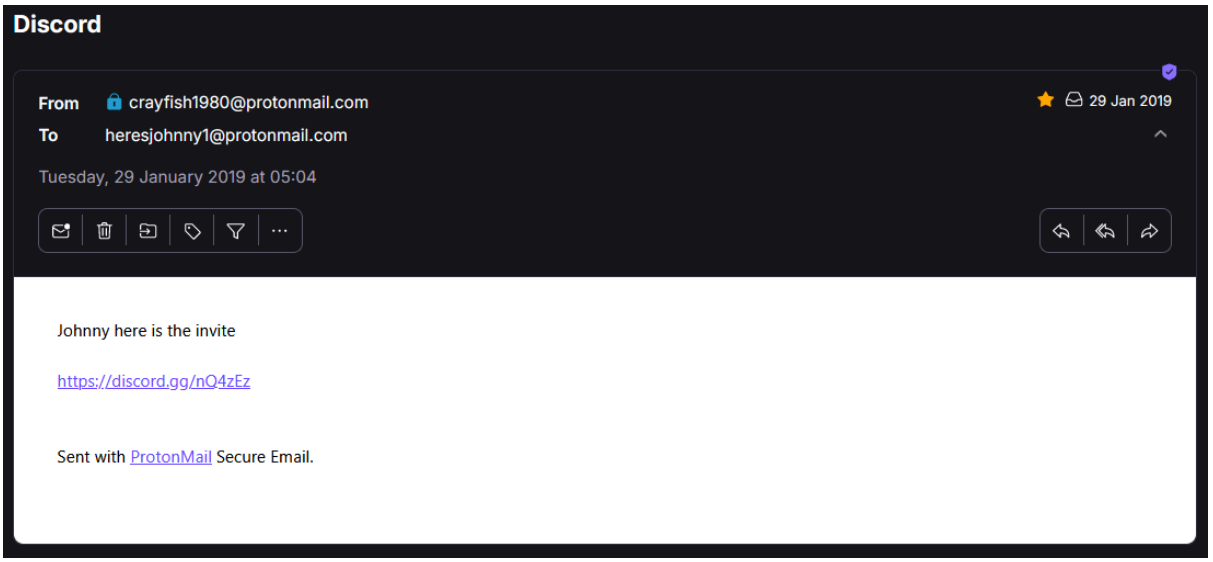
- Fredricksen then requests for Esteban's personal details so that he can book flights to Wellington, New Zealand. We strongly believe the flight in question to be that of the one depicted in Exhibit A2 (Steve K.PNG).
- Finally, Fredricksen requests Esteban to meet at the Woolworths located at 133 Oxley Station Rd, Oxley QLD 407, Australia before the flight.

3.5.2. Exhibit A13 (ProtonMail Account)

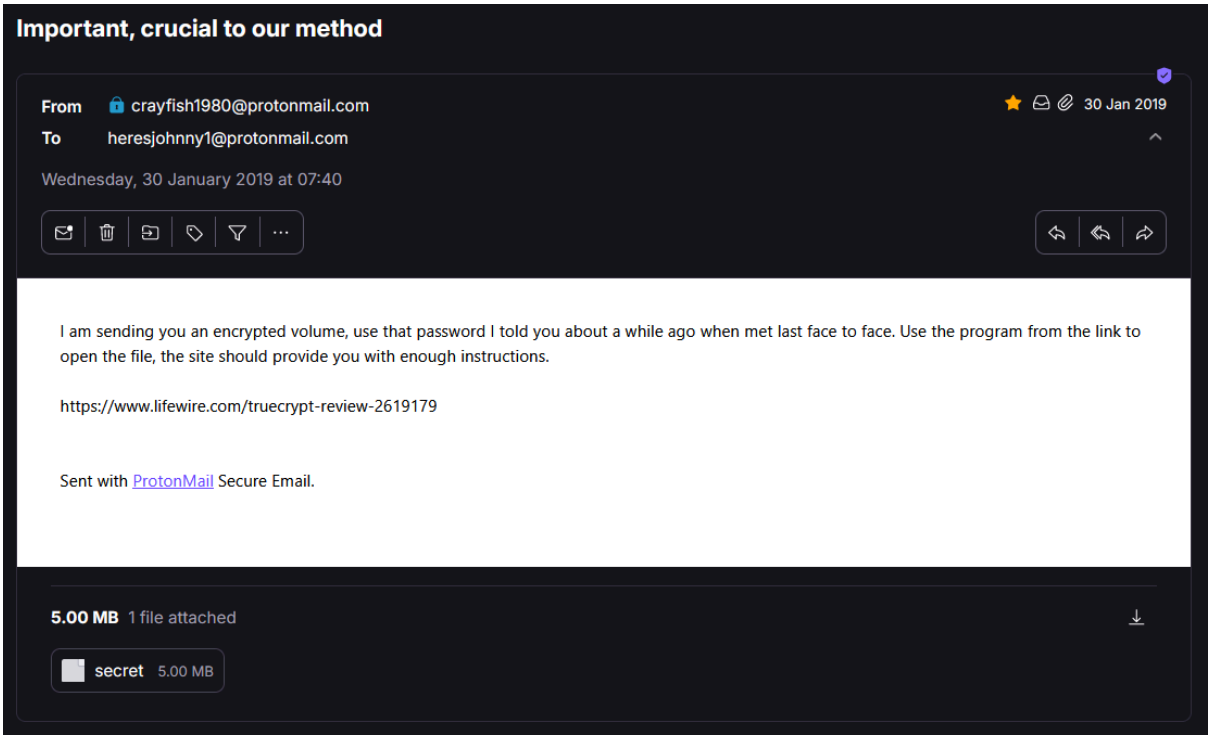
Thus far, we have been able to establish that John Fredricksen owns and uses a protonmail email address (heresjohnny1@protonmail.com). Based on information available from Exhibit B8 (01-30-2019.html), we could observe that John Fredricksen was observed to visit the login page of ProtonMail on 2019-01-30 09:56 via the Microsoft Edge web browser. He then entered the values heresjohnny1 and John1234, which we believe to be the username and password to his ProtonMail account. With this information, we attempted to log into his email account with these credentials and were successful in gaining access.

Received Emails

Within his email account, we found two messages that are of significant interest. Firstly on 2019-01-29 05:04 SGT, Fredricksen received an email from Steve Kowhai (crayfish1980@protonmail.com) titled "Discord", which contains a Discord invite link. We strongly believe that this private channel was used by both Kowhai and Fredricksen to communicate, with messages sent including the logs recovered as Exhibits 9 (Discord Outgoing Message Cache) and 10 (Discord Chat Logs) from the Case 1 report.

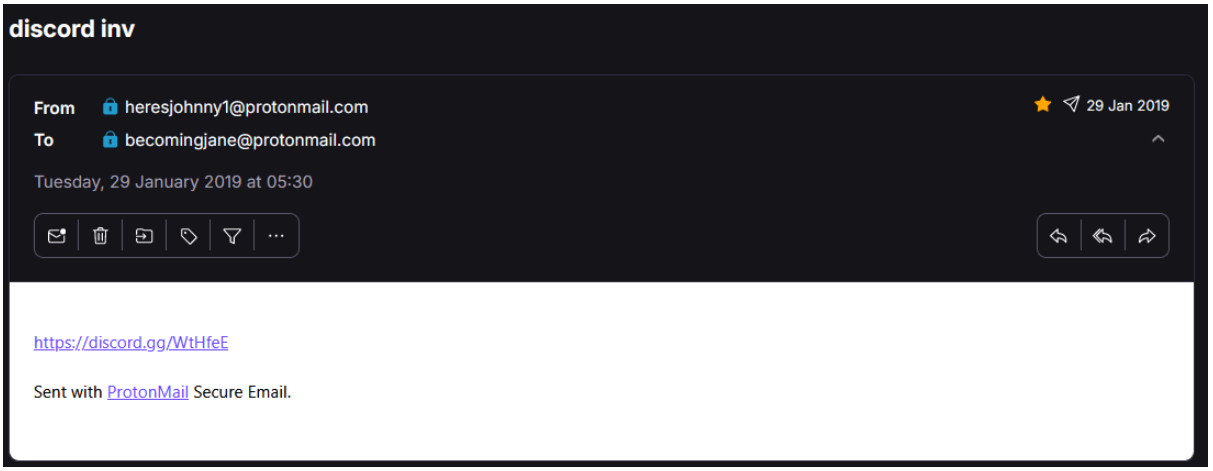


Secondly, on 2019-01-30 07:40 SGT, Kowhai sent Fredricksen an email titled "Important, crucial to our method". There is a single attachment titled "secret", which we confirm to be the same file as Exhibit A8 (secret), with instructions to open the encrypted volume with the TrueCrypt software and using a previously agreed password. We strongly believe that John Fredricksen downloaded the attachment as "Attachments-Important, crucial to our method.zip" shortly after receiving the email from Kowhai, which was then found within the file system as Exhibit A7.



Sent Emails

Under the sent emails, we found another 3 emails of interest. Firstly, on 2019-01-29 05:30 SGT, Fredricksen had sent Jane Esteban (becomingjane@protonmail.com) an email containing a Discord invite link. We believe that Fredricksen had used this email to invite Esteban to a private Discord channel before communications were initiated. Subsequently, the conversations that are shown in Exhibit A12 (Discord Chat Logs) would take place within this channel.



Secondly, we also discovered a similar email sent by Fredricksen to Jake Heke (jake.heke89@protonmail.com) on 2019-01-29 05:32, containing a Discord invite link. This email holds significance as Jake Heke was a name found in Exhibit A6 (clients.ods), whom we concluded was another individual involved with receiving Methamphetamine from Fredricksen. It was possible that Fredricksen did communicate with Heke over the private Discord channel, but we were unable to find any evidence that proves such messages were sent.

discord inv

From heresjohnny1@protonmail.com
To jake.heke89@protonmail.com
29 Jan 2019
Tuesday, 29 January 2019 at 05:32

https://discord.gg/vevVpm

Sent with ProtonMail Secure Email.

Lastly, John Fredricksen sent an email to Steve Kowhai on 2019-02-01 08:11 SGT with the image BNE.png attached, stating that the “pass is Elchapo2”. Analysing the attachment, we were able to confirm that it is the same file as found in Exhibit A1 (BNE.png). Furthermore, this confirms the activity as stated in Exhibit B10 (02-01-2019.html). We have previously proven that Fredricksen had hidden Exhibit A5 (package.jpg) with the Image Steganography program, which depicted the packages of Methamphetamine likely intended for Kowhai and a suitcase with its lining cut open, which we concluded was the same suitcase confiscated by Customs in Wellington Airport.

stego image

From heresjohnny1@protonmail.com
To crayfish1980@protonmail.com
1 Feb 2019
Friday, 1 February 2019 at 08:11

image attached.
pass is Elchapo2

Sent with ProtonMail Secure Email.

4.17 MB 1 file attached

BNE.png 4.17 MB

3.6. Web Data

3.6.1. Exhibit A14 (Microsoft Edge History)

File Name	WebCacheV01.dat
File Path	/img_Narcos-2/vol_vol7/Users/JohnF/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat
File Size	37748736 bytes
Hash Value	MD5: 8A812DEA96F1879C7746895BFF0FB5DD SHA1: F53482622C778B1960DE243EBD4362BAF098EA22
Modified Time	2019-02-02 11:17:47 SGT
Accessed Time	2019-02-02 11:17:47 SGT
Created Time	2019-01-29 03:26:34 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

firefox (via google.com.au)

- 2 instances (2019-01-28 20:08:33 SGT, 2019-01-28 20:08:34 SGT)
- Related to the download and installer of the Mozilla Firefox web browser, suspect eventually downloaded the installer from the URL https://www.mozilla.org/en-US/firefox/new/?f=138

protonmail (via bing.com)

- 6 instances (between 2019-01-28 21:12:28 SGT and 2019-01-29 02:10:47 SGT)
- Based on Exhibits A13 (ProtonMail Account) and B8 (01-30-2019.html), we can conclude that John Fredricksen had used the protonmail account of heresjohnny1@protonmail.com as a means of communication

how to cut drugs (via bing.com)

- 4 instances (between 2019-01-28 23:01:55 SGT and 2019-01-28 23:02:18 SGT)

how to cut drugs (via youtube.com)

- 2 instances (2019-01-28 23:03:06 SGT, 2019-01-28 23:03:07 SGT)

cutting drugs (via youtube.com)

- 2 instances (2019-01-28 23:04:24 SGT)

how to launder money (via bing.com)

- 2 instances (2019-01-28 23:07:36 SGT, 2019-01-28 23:10:30 SGT)

drugs subreddit (via bing.com)
- 4 instances (between 2019-01-28 23:13:20 SGT and 2019-01-28 23:17:29 SGT)

dhl (via bing.com)
- 2 instances (2019-01-29 03:43:19 SGT, 2019-01-29 03:49:16 SGT)
- Likely associated with shipping label found as part of Exhibit A3 (shipping.PNG)

shipping companies for packaging (via bing.com)
- 2 instances (2019-01-29 03:49:16 SGT)
- Likely associated with shipping label found as part of Exhibit A3 (shipping.PNG)

shipping companies for packaging au (via bing.com)
- 2 instances (2019-01-29 03:49:20 SGT, 2019-01-29 03:51:38 SGT)
- Likely associated with shipping label found as part of Exhibit A3 (shipping.PNG)

harvey norman pressure cooker au (via bing.com)
- 2 instances (2019-01-29 03:52:03 SGT)
- Likely associated with objects stated in shipping label found as part of Exhibit A3 (shipping.PNG)

3.6.2. Exhibit A15 (Mozilla Firefox History)

File Name	places.sqlite
File Path	/img_Narcos-2/vol_vol7/Users/JohnF/AppData/Roaming/Mozilla/Firefox/Profiles/fj248tbu.default/places.sqlite
File Size	5242880 bytes
Hash Value	MD5: 50A698FFF857F00065E7B6B0CEEE2188 SHA1: BBECE011AE08634A9D02A1CDB5FEC1E44AD39879
Modified Time	2019-02-02 10:47:52 SGT
Accessed Time	2019-02-02 10:47:52 SGT
Created Time	2019-01-29 04:09:54 SGT
Status	Allocated

Firefox uses an on-drive SQL database named places.sqlite as a database to store browsing history.

Items of Interest in Search History

baidu anti-virus download (via google.com)
- 1 instance (2019-01-29 04:15:55 SGT)
- Related to download and install of the Baidu AntiVirus program

openoffice (via google.com)

- 1 instance (2019-01-29 04:18:29 SGT)
- Related to download and install of the OpenOffice program

discord (via google.com)

- 1 instance (2019-01-29 04:20:46 SGT)
- Related to download and install of Discord, linked to Exhibit A12 (Discord Chat Logs)

encryption methods youtube (via google.com)

- 1 instance (2019-01-29 04:49:46 SGT)
- Likely subsequent related to use of Image Steganography, which is associated with image found hidden in Exhibit A1 (BNE.png)

drug detector dogs (via google.com)

- 1 instance (2019-01-31 10:01:30 SGT)
- Related to research on the capabilities drug detector dogs possess to prevent detection

suitcase concealments (via google.com)

- 2 instances (2019-01-31 10:04:44 SGT to 2019-01-31 10:05:21 SGT)
- Initial search of suitcase concealments but not helpful because it showed what happens when a body is concealed in a suitcase

suitcase concealments for drugs (via google.com)

- 3 instances (2019-01-31 10:06:09 SGT to 2019-01-31 10:12:48 SGT)
- Related to research of best place to store drugs in suitcase without being found out, prior to committing crime, associated with Exhibit A5 (package.jpg)

flights brisbane to WLG return (via google.com)

- 1 instance (2019-01-31 10:15:43 SGT)
- Related to flight trip searched, and tickets bought in Exhibit A2 (Steve K.PNG)

steganography image download (via google.com)

- 2 instances (2019-02-01 05:29:24 SGT, 2019-02-01 05:29:27 SGT)
- Associated with software download to do image steganography hidden in Exhibit A1 (BNE.png)

Flights from brisbane to wellington au

- 1 instance (2019-02-02 06:40:45 SGT)
- Related to flight trip searched, and tickets bought in Exhibit A2 (Steve K.PNG)

directions from Inala to brisbane airport

- 1 instance (2019-02-02 10:46:16 SGT)
- Corresponds to sender address of John Fredricksen's found on Exhibit A3 (shipping.PNG), indicating he is from Inala and searching the way to embark on a trip

4. Evidence and Findings (Narcos-3)

4.1. System Information

4.1.1. Operating System Information

Name: JELAPTOP
Version: Windows 10 Pro
Processor Architecture: AMD64
Product ID: 00330-80000-00000-AA263
Owner: Windows User

4.1.2. Drive Information

Type: Image
Size: 32212254720 bytes (30.0GB)
Sector Size: 512 bytes
Device ID: 016e41e0-c13e-453c-9b95-a886aa80fb28
Layout:

Name	Description	Starting Sector	Ending Sector	Length in Sectors	Flags
vol1	Unallocated	0	2047	2048	Unallocated
vol4	Basic data partition	2048	1023999	1021952	Allocated
vol5	EFI System partition	1024000	1226751	202752	Allocated
vol6	Microsoft reserved partition	1226752	1259519	32768	Allocated
vol7	Basic data partition	1259520	62912511	61652992	Allocated
vol8	Unallocated	62912512	62914559	2048	Unallocated

4.2. User Installed Programs

4.2.1. 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: Unknown
- Executable Location: /img_Narcos-3/vol_vol7/Users/JaneE/AppData/Local/Discord/app-0.0.304/Discord.exe

4.2.2. Quasar v1.3.0.0

Quasar is a fast and light-weight remote administration tool coded in C#. The usage ranges from user support through day-to-day administrative work to employee monitoring. It supports features such as remote desktop connections and keylogging.

- Installer Location: /img_Narcos-3/vol_vol7/Users\JaneE\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\Quasar.v1.3.0.0.zip
- Executable Location: /img_Narcos-3/vol_vol7/Users/JaneE/Downloads/Quasar v1.3.0.0/Quasar.exe

4.3. Images

4.3.1. Exhibit B1 (afp.png)

File Name	afp.png
File Path	/img_Narcos-3/vol_vol7/Users/JaneE/Pictures/afp.png
File Size	68697 bytes
Hash Value	MD5: SHA1:
Modified Time	2019-01-29 06:47:48 SGT
Accessed Time	2019-01-29 06:46:06 SGT
Created Time	2019-01-29 06:46:06 SGT
Status	Unallocated
Content	

This image depicts the badge of the Australian Federal Police. It has been deleted by a user from the file system, however its contents are still retained.

4.3.2. Exhibit B2 (background.png)

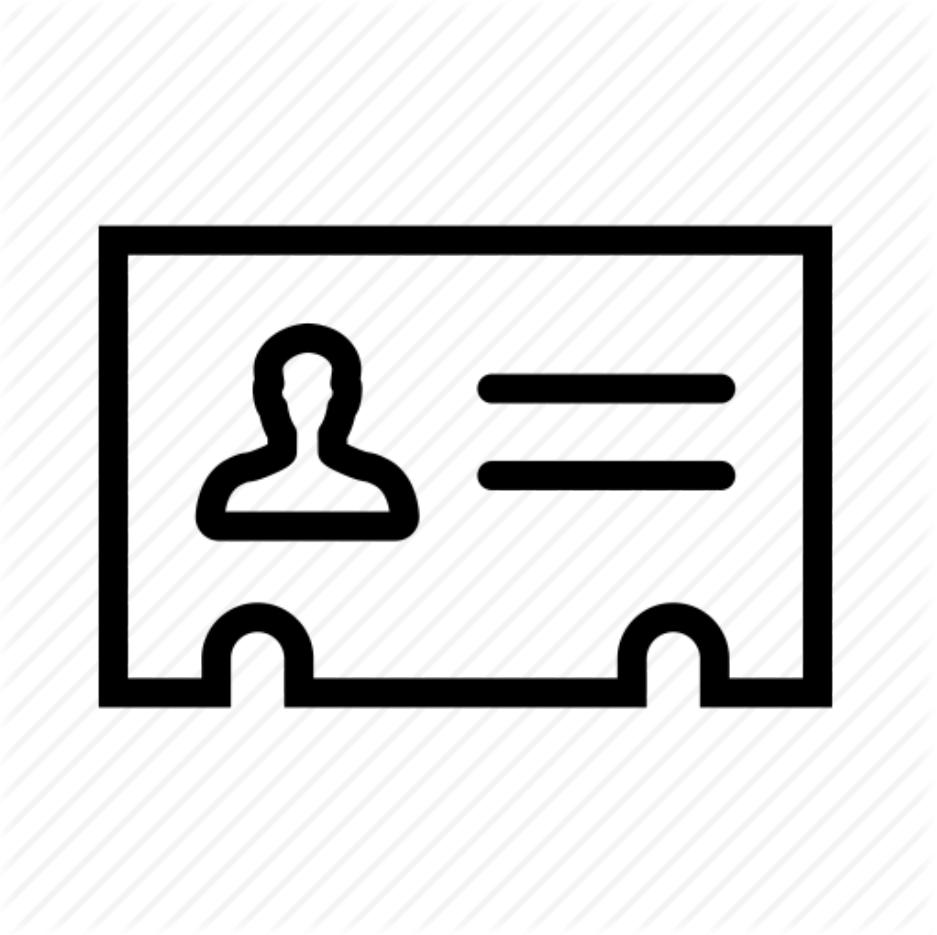
File Name	background.jpg
File Path	/img_Narcos-3/vol_vol7/Users/JaneE/Pictures/background.jpg
File Size	27438 bytes
Hash Value	MD5: SHA1:
Modified Time	2019-01-29 06:47:33 SGT

Accessed Time	2019-01-29 06:47:33 SGT
Created Time	2019-01-29 06:47:33 SGT
Status	Allocated
Content	

This image depicts the badge, along with the title of the Australian Federal Police.

4.3.3. Exhibit B3 (contact-card-512.png)

File Name	contact-card-512.png
File Path	/img_Narcos-3/vol_vol7/Users/JaneE/Pictures/contact-card-512.png
File Size	16953 bytes
Hash Value	MD5: 90ecfb62803906854fa9543751edc3c2 SHA1: 10401559ec02aac225bfa24be6bc29c10f18ebd320c093e849a094275b531e66
Modified Time	2019-01-29 05:22:37 SGT
Accessed Time	2019-01-29 05:22:37 SGT
Created Time	2019-01-29 05:22:37 SGT
Status	Allocated

Content	

This image appears to be a clipart of an icon of a contact card. We observe this to be the same image as the icon that was set for A11 (Contact Card.exe) and B13 ($RHZPX06.exe). We further note that Jane Esteban had converted this image to a Contact Card.ico file, which is an extension for images used as Icons for files on Windows. This was likely done via an online service, as we observed web searches for “png to ico converter” in Exhibit 14 (Microsoft Edge History). We thus conclude that there is strong evidence to support our prior hypothesis that Jane masqueraded the Quasar client with keylogging capabilities as a contact detail file or program, in hopes that John Fredricksen would be mistaken into launching it.

4.3.4. Exhibit B4 (crys1.jpg)

File Name	crys1.jpg
File Path	/img_Narcos-3/vol_vol7/Users/JaneE/Pictures/crys1.jpg
File Size	39684 bytes
Hash Value	MD5: 5C580E37403CC6138497A23E9B0B9464 SHA1: C0A936CF0C6313035C6FBE4CB263277345C32CD9
Modified Time	2019-01-31 09:10:09 SGT

Accessed Time	2019-01-31 09:10:09 SGT
Created Time	2019-01-31 09:10:09 SGT
Status	Allocated
Content	

This is an image of what we suspect to be Methamphetamine crystals. From the Microsoft Edge search history of this system (Exhibit B12), we believe that Jane Esteban had downloaded this image from Google images as part of her research into drug trafficking.

4.3.5. Exhibit B5 (crys2.jpg)

File Name	crys2.jpg
File Path	/img_Narcos-3/vol_vol7/Users/JaneE/Pictures/crys2.jpg
File Size	88579 bytes
Hash Value	MD5: 9D005F3905B24B628F5EB076C8524BCF SHA1: 575AAE72954FEC4A92199B315DE4D1D07AD5E449
Modified Time	2019-01-31 09:10:32 SGT
Accessed Time	2019-01-31 09:10:32 SGT
Created Time	2019-01-31 09:10:31 SGT
Status	Allocated

Content	

This is an image of what we suspect to be Methamphetamine crystals. From the Microsoft Edge search history of this system (Exhibit B12), we believe that Jane Esteban had downloaded this image from Google images as part of her research into drug trafficking.

4.3.6. Exhibit B6 (crys3.jpg)

File Name	crys3.jpg
File Path	/img_Narcos-3/vol_vol7/Users/JaneE/Pictures/crys3.jpg
File Size	7330 bytes
Hash Value	MD5: 4EB61426BAF813858640533599816096 SHA1: 6228F5048AE8DA89F2FB5ECBF175A7CC36B149F0
Modified Time	2019-01-31 09:12:41 SGT
Accessed Time	2019-01-31 09:12:41 SGT
Created Time	2019-01-31 09:12:41 SGT
Status	Allocated

This is an image of what we suspect to be Methamphetamine crystals. From the Microsoft Edge search history of this system (Exhibit B12), we believe that Jane Esteban had downloaded this image from Google images as part of her research into drug trafficking.

4.4. Documents & Files

4.4.1. Exhibit B7 (course-undercover-survival.pdf)

File Name	course-undercover-survival.pdf
File Path	/img_Narcos-3/vol_vol7/Users/JaneE/Documents/course-undercover-survival.pdf
File Size	bytes
Hash Value	MD5: FA714F0AAD66BF3953D061ADF2457F86 SHA1: F164D9C1E77D4D17ED85D594801BA1C12F0A151E
Modified Time	2019-02-01 08:04:19 SGT
Accessed Time	2019-02-01 08:04:19 SGT
Created Time	2019-02-01 08:04:19 SGT
Status	Allocated

Contents	

This PDF document is an outline for a law enforcement in-service training course offered by Schoolcraft College's Public Safety Training Center titled "Undercover Survival and Lawful Invasions". It provides further details regarding the schedule and outline of the two day course, along with a phone number to contact for registration. The course is dated 2011-12-13 to 2011-12-14.

4.4.2. Exhibit B8 (01-30-2019.html)

File Name	01-30-2019.html
File Path	/img_Narcos-3/vol_vol7/Users/JaneE/Downloads/Quasar v1.3.0.0/Clients/JohnF@JOHNFLAPTOP1_4DD90B0/Logs/01-30-2019.html

File Size	2777 bytes
Hash Value	MD5: FD3A044BEE4D5AF72FABA9630867D4FD SHA1: BD91FCC9D02C0CA41C769B8944530EBDB6346886
Modified Time	2019-02-02 10:52:34 SGT
Accessed Time	2019-01-30 09:41:16 SGT
Created Time	2019-01-30 09:41:16 SGT
Status	Allocated
Relevant Contents	**Event (time): #general - Discord (08:14)** Sweet thanks [Enter] Got a new supplier. Ya Interested??[Enter] Hmm 10 is abit 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?[Enter] **Event (time): Start - Microsoft Edge (09:56)** protonmail.com[Enter] **Event (time): Login | ProtonMail - Microsoft Edge (09:56)** heresjohnny1John1234[Enter] **Event (time): Inbox | heresjohnny1@protonmail.com | ProtonMail - Microsoft Edge (09:57)** [Control + C] **Event (time): New tab and 1 more page - Microsoft Edge (09:57)** [Control + V][Enter] **Event (time): Enter password for C:\Users\JohnF\Downloads\Attachments-Importa...\secret (10:04)** ilovediving **Event (time): Mozilla Firefox (11:49)** decryption methods [Back]encryption methods youtube[Enter]

This HTML contains a list of events, formatted with a title and associated contents. Considering the full file path of this file, we strongly believe that it is a report generated by the Quasar program, which is an open-source remote administration tool for Windows systems. Thus, we can conclude that the HTML file contains logs of keypresses from the laptop of John Fredricksen, the associated timestamps and what programs or windows the input was entered into. Based on the file name, this report contains captured data from 2019-01-30.

The events can be summarised as follows:

- (2019-30-01 08:14) John Fredricksen communicates over Discord. The contents match the ones found in Exhibit 10 (Discord Chat Logs) from the Case 1 report. Thus, we conclude that he is communicating with Steve Kowhai at this time. The

contents of the conversation include Fredricksen suggesting that Kowhai starts small shipments of drugs, assessing its viability before scaling up transactions

- (2019-30-01 09:56) Fredricksen navigates to protonmail.com and logs in with the username “heresjohnny1” and password “John1234”. We were able to gain access to this account as further documented in Exhibit A13 (ProtonMail Account).
- (2019-30-01 10:04) Fredricksen enters the password “ilovediving” into a program that references the secret file (Exhibit A8). We are confident that he likely referenced the instructions from Kowhai and is using TrueCrypt to decrypt the volume sent by Kowhai.

4.4.3. Exhibit B9 (01-31-2019.html)

File Name	01-31-2019.html
File Path	/img_Narcos-3/vol_vol7/Users/JaneE/Downloads/Quasar v1.3.0.0/Clients/JohnF@JOHNFLAPTOP1_4DD90B0/Logs/01-31-2019.html
File Size	6485 bytes
Hash Value	MD5: 948B4C559B944D6C0F2E1DA8E285D835 SHA1: 8C1AA410A535904E237628EA44160F32694282E8
Modified Time	2019-02-02 10:52:34 SGT
Accessed Time	2019-02-02 10:52:34 SGT
Created Time	2019-02-02 10:52:34 SGT
Status	Allocated
Relevant Contents	**Event (time): #general - Discord (09:43)** Yo, what you after?[Enter] Also that contact card didn't open and I can't be bothered with new clients got bigger fishj to fry right now... [Enter] Aight cool, umm actually I have a proposition for ya[Enter] I have a business dealing happening overseas and I need you to accompany me as cover. Everything will be paid for but you need to keep your trap shut[Enter] Yea I understand but ill make it worth your while[Enter] I did't want to do this but, you leave me no choice[Enter] You don't wanna see them hurt do yaGood, now that's what I wanted to hear. Here is the plan. You will and I will be acting like a couple travelling on a holiday to New Zealand. This is what I want you to do: Look the part, act normal, and don't tell anyone about what you and I will be acting like a couple travelling on a holiday to New Zealand. This is what I want you to do: Look the part, act normal, and don't tell anyone about what we're doing. Understood? [Enter] Good talk tommorrow at 3PM or else[Enter] **Event (time): Google - Mozilla Firefox (11:59)** drug detectector dogs[Enter]

	Event (time): drug detector dogs - Google Search - Mozilla Firefox (12:01) body packing[Enter] **Event (time): body packing - Google Search - Mozilla Firefox (12:04)** suitcase concealments[Enter] **Event (time): suitcase concealments - Google Search - Mozilla Firefox (12:06)** fro drugs[Enter] **Event (time): suitcase concealments fro drugs - Google Search - Mozilla Firefox (12:13)** new zealand wellington[Enter] **Event (time): new zealand wellington - Google Search - Mozilla Firefox (12:15)** flights to brisbane to WLG return[Enter]

This HTML contains a list of events, formatted with a title and associated contents. Considering the full file path of this file, we strongly believe that it is a report generated by the Quasar program, which is an open-source remote administration tool for Windows systems. Thus, we can conclude that the HTML file contains logs of keypresses from the laptop of John Fredricksen, the associated timestamps and what programs or windows the input was entered into. Based on the file name, this report contains captured data from 2019-01-31.

The events can be summarised as follows:

- (2019-01-31 09:43): John Fredricksen communicates over Discord. Based on the contents captured, and cross-referencing with Exhibit A12 (Discord Chat Logs), we believe that he is communicating with Jane Esteban. He attempts and is successful in threatening Esteban to accompany him on a trip to New Zealand.
- (2019-01-31 11:59 to 12:06): Fredricksen performs multiple searches on Google related to transportation and hiding of drugs such as “drug detector dogs”, “body packing” and “suitcase concealments”.
- (2019-01-31 12:13 to 12:15): Fredricksen performs searches on Google for “new zealand wellington” and “flights to brisbane to WLG return”.

4.4.4. Exhibit B10 (02-01-2019.html)

File Name	02-01-2019.html
File Path	/img_Narcos-3/vol_vol7/Users/JaneE/Downloads/Quasar v1.3.0.0/Clients/JohnF@JOHNFLAPTOP1_4DD90B0/Logs/02-01-2019.html
File Size	5733 bytes

Hash Value	MD5: F51AA5754E54915E93D329A3EEFDC042 SHA1: F7AF9CA41B1C9ABFFAF3ACBB520E533D29152616
Modified Time	2019-02-02 10:52:34 SGT
Accessed Time	2019-02-02 10:52:34 SGT
Created Time	2019-02-02 10:52:34 SGT
Status	Allocated
Relevant Contents	**Event (Time): #general - Discord (07:02)** ah bugger wrong person, disregard messageI want to send an image of something to you but it needs to be done safely. Any ideas?[Enter] No what's that?[Enter] Okay I'll have a look and see if I can get it to work and then send the image through[Enter] **Event (Time): steganography - Google Search - Mozilla Firefox (07:29)** Image download[Enter] **Event (Time): steganography image download - Google Search - Mozilla Firefox (07:29)** beach[Enter] **Event (Time): beach - Google Search - Mozilla Firefox (07:30)** brisbane[Enter] **Event (Time): brisbane - Google Search - Mozilla Firefox (07:30)** tutorial on image steganography[Enter] **Event (Time): Save As (09:04)** BNE **Event (Time): Enter Password (09:05)** Elchapo2 **Event (Time): #general - Discord (09:59)** It worked, sending it via email now. I used a tool called image steganography and the password.[Enter] **Event (Time): Mozilla Firefox (10:04)** protonmail[Enter] **Event (Time): Login | ProtonMail - Mozilla Firefox (10:04)** heresjohnny1John1234 **Event (Time): (4) Inbox | heresjohnny1@protonmail.com | ProtonMail - Mozilla Firefox (10:05)** crayfish1980@protstego imageimage attached.[Enter] pass is Elchapo2 **Event (Time): #general - Discord (11:58)**

	Right. What's your full name and date of birth? I need it for booking flights ASAP.[Enter]

This HTML contains a list of events, formatted with a title and associated contents. Considering the full file path of this file, we strongly believe that it is a report generated by the Quasar program, which is an open-source remote administration tool for Windows systems. Thus, we can conclude that the HTML file contains logs of keypresses from the laptop of John Fredricksen, the associated timestamps and what programs or windows the input was entered into. Based on the file name, this report contains captured data from 2019-02-01.

The events can be summarised as follows:

- (2019-02-01 07:02): John Fredricksen communicates over Discord. The contents match the ones found in Exhibit 10 (Discord Chat Logs) from the Case 1 report. He has a conversation over Discord seeking suggestions for sending images in a safe manner
- (2019-02-01 07:29): Fredricksen searches terms related to image steganography. It is likely he downloaded and installed the Image Steganography program around this time
- (2019-02-01 09:04 to 09:05): A file is noted to be saved as "BNE" and a password "Elchapo2" is supplied to a certain program. Referencing Exhibit 17 (Image Hidden With Steganography) from our Case 1 report, we are confident that at this time Fredricksen utilised the Image Steganography program to hide the package.jpg file (Exhibit A5) within another image to obtain the BNE.png file (Exhibit A1).
- (2019-02-01 09:59): Communicates with Steve Kowhai over Discord to report that he was successful in hiding the image safely using Image Steganography and is sending it to Kowhai over email.
- (2019-02-01 10:04 to 10:05): Fredricksen logs into his protonmail account and sends Steve Kowhai (crayfish1980@protonmail.com) an email with the image containing hidden content, stating the password as "Elchapo2"
- (2019-02-01 11:58): Fredricksen asks Jane Esteban over Discord for her full name and date of birth for booking the flights as shown in Exhibit A2 (Steve K.PNG). This message can also be found within Exhibit A12 (Discord Chat Logs).

4.4.5. Exhibit B11 (02-02-2019.html)

File Name	02-02-2019.html
File Path	/img_Narcos-3/vol_vol7/Users/JaneE/Downloads/Quasar v1.3.0.0/Clients/JohnF@JOHNFLAPTOP1_4DD90B0/Logs/02-02-2019.html
File Size	5014 bytes
Hash Value	MD5: 7EDEA768C94997ED685BF7BC51CC325A SHA1: EF05486F35E9110F34DD8F31418A57B64E1A2C52
Modified Time	2019-02-02 10:52:34 SGT

Accessed Time	2019-02-02 10:52:34 SGT
Created Time	2019-02-02 10:52:34 SGT
Status	Allocated
Relevant Contents	**Event (Time): Mozilla Firefox (08:29)** flights from brisbane to wlG[Enter] **Event (Time): flights from brisbane to wlG - Google Search - Mozilla Firefox (08:29)** flights from brisbane to wlG au[Enter] **Event (Time): flights from brisbane to wlG au - Google Search - Mozilla Firefox (08:34)** flights from brisbane to wlG jetstar[Enter] **Event (Time): flights from brisbane to wlG jetstar - Google Search - Mozilla Firefox (08:40)** flights from brisbane to wellington au[Enter] **Event (Time): Cortana (08:42)** snip[Enter] **Event (Time): Save As (08:42)** Steve K **Event (Time): #general - Discord (09:00)** Flights booked. I'll pick you up from the Woolworths (133 Oxley Station Rd, Oxley QLD 4075, Austraila) at … Just bring yourself I'll cover everything else[Enter] **Event (Time): Mozilla Firefox (12:40)** woolworths[Enter] **Event (Time): Woolworths Supermarket - Buy Groceries Online - Mozilla Firefox (12:41)** travel[Enter] **Event (Time): travel - Woolworths Online - Mozilla Firefox (12:41)** suitcase[Enter] **Event (Time): toilet - Woolworths Online - Mozilla Firefox (12:43)** sanitary **Event (Time): Foam Hand Wash Rose & Cherry In Bloom 250ml | Woolworths - Mozilla Firefox (12:43)** bars[Enter] **Event (Time): Help At Hand Epsom Salt 1kg | Woolworths - Mozilla Firefox (12:44)** sunblock[Enter] **Event (Time): sunblock tan - Woolworths Online - Mozilla Firefox**

	(12:45) directions from Inala to brisbane airport[Enter] **Event (Time): Enter password for C:\Users\JohnF\Downloads\Attachments-Importa...\secret (12:50)** ilovediving

This HTML contains a list of events, formatted with a title and associated contents. Considering the full file path of this file, we strongly believe that it is a report generated by the Quasar program, which is an open-source remote administration tool for Windows systems. Thus, we can conclude that the HTML file contains logs of keypresses from the laptop of John Fredricksen, the associated timestamps and what programs or windows the input was entered into. Based on the file name, this report contains captured data from 2019-02-02.

The events can be summarised as follows:

- (2019-02-02 08:29 to 08:40): John Fredricksen performs multiple searches on Google for flights from Brisbane, Australia to Wellington, New Zealand. We believe that during this time, he likely booked the flights as stated in Exhibit A2 (Steve K.PNG)
- (2019-02-02 08:42): Launches Microsoft Cortana and searches for “snip”, afterwards launching the Snipping Tool program, and captures some portion of his screen, saving the resulting file as “Steve K”, which was how Exhibit A2 was generated. From the contents of Exhibit A2, we can conclude he captured the details of the flight he booked from Brisbane to Wellington.
- (2019-02-02 09:00): Fredricksen sends a message to Jane Esteban over Discord, reminding her to meet at the woolworths at 133 Oxley Station Road
- (2019-02-02 12:40 to 12:45): Performs multiple searches on Woolworths, an online supermarket based in Australia, for several travel essentials such as suitcases and hand wash. It is likely that Fredricksen had intended to use a suitcase purchased here as the avenue to hide the packages of Methamphetamine in, as shown in Exhibit A5 (package.jpg). The unusual search of Help At Hand Epsom Salt might indicate his idea of packing the Meth crystals into a salt packaging to evade detection.

4.4.6. Exhibit B12 (Contact Card.zip)

File Name	Contact Card.zip
File Path	/img_Narcos-3/vol_vol7/Users/JaneE/Documents/Contact Card.zip
File Size	bytes
Hash Value	MD5: B4526C58D6A1A6D6BD654474A1CE8823 SHA1: 7A5C5482D7B90A3A142695CF11A02C73CF2CAAF8
Modified Time	2019-01-29 05:20:23 SGT
Accessed Time	2019-01-29 05:09:29 SGT

Created Time	2019-01-29 05:09:29 SGT
Status	Unallocated

Observing the file hashes, we noted that this ZIP archive is the same as Exhibit A10 (Contact_Card.zip). Based on prior analysis of Exhibit A10, we noted that this ZIP file was sent as an attachment by Jane Esteban to John Fredricksen on 2019-01-29 11:32:45.151 SGT, passing it off as the “contact card” of individuals who were interested in obtaining drugs from Fredricksen. We understand that Fredricksen eventually downloaded the attachment and extracted its contents on his laptop.

4.4.7. Exhibit B13 (Contact Card.exe)

File Name	Contact Card.exe
File Path	/img_Narcos-3/vol_vol7/Users/JaneE/Desktop/Contact Card.exe
File Size	385024 bytes
Hash Value	MD5: 409B88B2B275353F2CA05983CEF1ABF5 SHA1: 2FC14E18C0B090D55360E60468489AA65E2375F2
Modified Time	2019-01-29 05:25:06 SGT
Accessed Time	2019-01-29 05:28:02 SGT
Created Time	2019-01-29 05:28:02 SGT
Status	Unallocated

Observing the file hashes, we noted that this executable is the same as Exhibit A11 (Contact Card.exe). The presence of the same executable on Jane Esteban’s laptop further supports our initial theory, that Esteban had generated this executable as a Quasar client, which was configured to act as a keylogger. She had then compressed this executable into a ZIP archive as Exhibit B12 (Contact Card.zip), before sending it as an attachment in a Discord message to John Fredricksen as shown in Exhibit A12 (Discord Chat Logs). Afterwards, Esteban proceeded to delete the executable, resulting in its presence in the recycle bin and being flagged as unallocated.

4.5. Web Data

4.5.1. Exhibit B14 (Microsoft Edge History)

File Name	WebCacheV01.dat
File Path	/img_Narcos-3/vol_vol7/Users/JaneE/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat
File Size	45613056 bytes
Hash Value	MD5: 1911BBD11DC5C49EFD4D1AD37263FAB3 SHA1: 685A19AB3DA7A5A2B72D6596B79B3A120287F245
Modified Time	2019-02-02 11:09:39 SGT
Accessed Time	2019-01-29 03:21:55 SGT
Created Time	2019-01-29 03:21:55 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

Telecommunications Act (via google.com.au)

- Likely to research on laws governing telecommunications, which could be relevant to monitoring or intercepting communications related to drug dealings.

Telecommunications Act and Other Legislation Amendment Bill 2018 (via google.com.au)

- Further research on legislative changes related to telecommunications, possibly to understand any updates or amendments that could affect investigations.

Contact card.png (via bing.com)

- Downloaded contact card to be used as an icon for keylogger that is sent to John as seen in Exhibit A10.

PNG to ICO Converter Online (via bing.com)

- Potentially to convert an image file format for use in creating cover materials, in this case the keylogger.

Federal Agent Badge (via google.com.au) and Federal Agent Badge AU (via google.com.au)

- Searched and downloaded as seen in Exhibit B1 and Exhibit B2.

Micro Voice Recorder AU (via google.com.au)

- Looking for a discreet recording device, likely for covertly capturing conversations related to drug dealings or any suspicious behaviour.

How to Act Like a Meth Addict (via bing.com) and How to Look Like a Meth Addict (via bing.com)

- Research on behaviour and appearance to adopt a convincing persona as a drug user during undercover work.

FBI Negotiator Secret to Winning Any Exchange (via youtube.com)

- Could be seeking strategies for effective communication and negotiation during interactions with John in case the situation arises.

Quasar RAT (via youtube.com)

- Research on a remote access tool, possibly for technical aspects of surveillance or investigation, and was used as the keylogger sent to John.

Prison Sentences for Drugs AU (via bing.com) and Prison Sentences for Drugs NZ (via bing.com)

- Possibly to understand the legal consequences of drug-related offences in Australia and New Zealand, likely for background knowledge or potential charges against John.

Passing Drugs Through NZ Customs (via bing.com)

- Investigating methods and risks associated with smuggling drugs through customs, potentially to understand John's operation better and cover all bases of what could happen.

Methamphetamine (via google.com.au) and Methamphetamine Crystal Rock (via google.com.au)

- Research on the drug itself, likely to familiarise with its appearance, effects, and usage patterns for better undercover performance.

Legal Process to Convict Blackmail (via bing.com)

- Understanding legal procedures for prosecuting blackmail offences, possibly for broader knowledge or to anticipate legal strategies.

How to Pretend to Be Desperate (via bing.com) and How to Pretend to Be Desperate in Drug Dealings (via bing.com)

- Exploring strategies to feign desperation, likely to gain trust or sympathy from John during undercover interactions.

Survival Tips from an Undercover Cop (via bing.com) and Undercover Cop Survival (via bing.com)

- Seeking advice on staying safe and effective while operating undercover, indicating a focus on maintaining cover and personal safety during the investigation.

These specifics offer further confirmation backing the claim that Jane is functioning as an undercover law enforcement agent, posing as a drug user to monitor John and his illicit drug dealings. By feigning desperation, Jane can decrease John's suspicions, making it easier for her to gather vital information for law enforcement. The search for a micro voice recorder

implies Jane's intention to secretly record John's conversations, assisting in the collection of potentially damning evidence.

4.5.2. Exhibit B15 (Microsoft OneDrive Cache)

File Name	{7795B737-5C97-416D-B996-72FE146BF12A}{12}.db
File Path	/img_Narcos-3/vol_vol7/Users/JaneE/AppData/Local/Packages/Microsoft.Office.OneNote_8wekyb3d8bbwe/LocalState/AppData/Local/OneNote/16.0/FullTextSearchIndex/{7795B737-5C97-416D-B996-72FE146BF12A}{12}.db
File Size	167936 bytes
Hash Value	MD5: 0E7ABA03A3F9AF493681E16E5304B5F6 SHA1: 27679C2F0EB557ABCEC8C61695C5740377B84BC9
Modified Time	2019-02-02 07:29:02 SGT
Accessed Time	2019-01-29 08:19:36 SGT
Created Time	2019-01-29 08:19:36 SGT
Status	Allocated
Relevant Content	Jane’s Diary Day 1 Today I checked out social media, news and ways to blend in better amongst meth heads. Found a way to better take advantage of the Australian Telecommunications legislation and Amendment act. Looked at some online shopping items and further explored communication systems to get in contact with a friend. Day 2 Looked at videos of malware on YouTube, hopefully the RAT I've selected works as intended. Day 3 My friend replied back to me however I'm not sure he's my friend anymore as he seems more demanding and unfriendly than usual however I must keep my cover and proceed with his wishes. Browsed some sites related to Illegal activities. Day 4 Browsed some tips on advice, behaviour and how to maintain my cover more efficiently. My aggressive friend wants to know my details and I've decided to stick to the plan. Day 5

This file is an on-drive database in the SQLite3 format, and was used by the Microsoft OneDrive program as a cache which stores snapshots of notebooks accessed, created or modified by the user. This specific cache file contains entries pertaining to a document named “Jane’s Diary”. The contents document what appear to be Jane Esteban’s thoughts regarding her activities, across 4 days, with the fifth day lacking any associated entry. We

understand her thoughts to refer to John Fredricksen as the “friend”. Based on the contents, we understand this to refer to the period between 2019-01-29 to 2019-02-01 after cross referencing events such as the “friend” wanting to know her details from Exhibit A12 (Discord Chat Logs) and her searches on the internet from Exhibit B14 (Microsoft Edge History).

5. 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 further establish the identities of John Fredricksen and Jane Esteban, in addition to the conclusions derived from our report on Case 1. Furthermore, we seek to understand more about their respective motives, goals and objectives. Our analysis will be based on the following questions:

- Who was Jane actually?
- What did John think of Jane, and what did he want from her?
- Who were the guilty parties in the overall case based on the extra evidence given?
- What were the guilty parties' future plans and intentions based on the extra evidence given?

5.1. Identity of Jane Esteban

Given the evidence available to us, we believe that Jane Esteban is acting as an undercover agent as part of the Australian Federal Police (AFP). Initial clues such as Exhibit B1 (afp.png) and B2 (background.png) hinted at a potential association with the AFP. Her role as an undercover agent was further backed by the presence of domain-specific documents such as Exhibit B7 (course-undercover-survival.pdf), which hint at prior training in the field of undercover operations.

Based on Exhibit B14 (Microsoft Edge History), we observed a number of searches for drug related activities such as the behaviour of drug addicts, details on methamphetamine, likely indicating that her scope of undercover operations is on drug-related activities and crimes. Within the same exhibit, we also observe web searches for Australian legislation and "prison sentences for drugs" in both Australia and New Zealand. However, based on her web searches on topics such as "how to act like a meth addict" and "survival tips from an undercover cop" show that she may be uncertain or inexperienced in the role of an undercover police officer. Despite this, from the successful deployment of a remote administration tool Exhibits B12 (Contact Card.zip) and B13 (Contact Card.exe), she has shown to be well versed in the tools that may be available to her in terms of gathering information. Thus, we conclude that Jane Esteban is an undercover agent associated with the Australian Federal Police, working to uncover and prosecute individuals involved in drug-related activities.

However, there is a remote possibility that the signs indicating her allegiance to the AFP could be intentionally planted to mislead potential investigators. However, assessing the amount of information and evidence still present on the laptop, her uncertainties in handling complications such as being threatened by John Fredricksen to accompany him to New Zealand, and attempting to search for terms such as "undercover cop survival " lead us to believe that she may not have acted with that level of sophistication in mind. Lastly, we have significant reason to believe that the

5.2. Relations Between John Fredricksen and Jane Esteban

In assessing how John Fredricksen viewed Jane Esteban, we have based our analyses primarily off Exhibit A12 (Discord Chat Logs), which show the majority of the communications between the two individuals. When Esteban first approached Fredricksen over a request for drugs, John was initially receptive to follow through with the transaction. However, after Esteban sent a contact card masquerading as a remote administration tool client to log the inputs Fredricksen made to his laptop, and being unable to open the file, his interest cooled off, stating that he is not looking for “new clients”.

However, Fredricksen subsequently offers a proposition to Esteban, for her to accompany him on a “business dealing” to New Zealand. We understand this event to refer to his intention to deliver a shipment of Methamphetamine to Steve Kowhai in Wellington, New Zealand, as stated in our conclusions from the Case 1 report. When Esteban refuses, Fredricksen sends her an image of what we believe to be her children, threatening them with harm if she does not comply. Eventually, Esteban relents and agrees to accompany Fredricksen on the trip to New Zealand. Fredricksen proceeds to obtain her personal details and books the flights to Wellington.

We conclude that through his demands, John Fredricksen viewed Jane Esteban as a vulnerable individual which he could threaten to act on his behalf or in his interest. We also conclude that the purpose of Fredricksen’s communication with Esteban was mainly to avoid travelling to Wellington alone, instead opting to have a facade of a couple on holiday so as to reduce potential suspicion from authorities while carrying Methamphetamine concealed in his suitcase.

However, due to lack of available evidence, we are unsure of how Jane Esteban was able to find out about the occupation of John Fredricksen and to be aware of his business in the trafficking of illicit substances. Additionally, we are uncertain as to how John Fredricksen came into possession of a photo of Jane Esteban’s children, which he used to threaten Jane Esteban into accompanying him to New Zealand.

5.3. Guilty Parties in the Case

Combining the available evidence across Cases 1 and 2, along with our prior conclusions from the Case 1 report, we believe that the guilty parties in the overall case are as follows. However, we highlight that the exact violation of laws are subject to the jurisdiction where the individuals may be tried or prosecuted.

Steve Kowhai

- Intention in Trafficking of Controlled Substances: From our analyses and the case background, we were able to confirm that the Methamphetamine found in the suitcase lining of John Fredricksen were intended for Steve Kowhai. Additionally, it is also reasonable to believe that Kowhai had intended to further redistribute the drugs to other parties within the region of Wellington. Thus, we believe that he should be guilty of intent to traffic controlled drugs.

- Intention of Manufacturing of Controlled Substances: Based on available evidence, primarily the search history of Steve Kowhai, we have significant reason to believe that Steve Kowhai intended to further modify the contents of the Methamphetamine to be received from John Fredricksen, such as the process of “cutting” drugs.
- Intention to Commit Acts of Money Laundering: Analyses of available evidence has given us reason to believe that in combination of processing and further distribution of Methamphetamine, Steve Kowhai harboured intentions, or was in consideration of potential ways of laundering any proceeds gained from any future sale of drugs in his possession.

While we are certain that Steve Kowhai actively intended to be in possession of the Methamphetamine found in the suitcase of John Fredricksen and also intended to further process and distribute the drugs, we feel that that subject to prevailing legislation, it may be difficult of proving Steve Kowhai to be definitively guilty of the offences stated above, since he was not actually in possession of the Methamphetamine.

John Fredricksen

- Trafficking in Controlled Substances: Our analysis of available evidence has provided strong support for John Fredricksen’s role as a supplier and distributor of drugs, with Exhibit A6 (clients.ods) indicating him as the supplier. Furthermore, the overall case has shown Fredricksen to be in possession of a controlled substance (Methamphetamine in the lining of his suitcase). Thus, John Fredricksen would be guilty of trafficking in controlled drugs as he was in the possession of such drugs for the purpose of trafficking
- Import and Export of Controlled Substances: With regards to the overall case, we further believe that John Fredricksen is guilty of the import and export of controlled drugs. He was proven to be in possession of Methamphetamine which he brought into New Zealand from Australia. Furthermore, through analyses of available evidence in both cases, we are able to show that he was in possession of these drugs for the purpose of delivering it to a location in New Zealand.

Jane Esteban

We believe that in consideration of all available evidence, no guilt should be assigned to Jane Esteban. This is founded on our belief that Jane Esteban was the individual behind the intel provided to New Zealand Customs which alerted them to both her and John Fredricksen as suspicious individuals. Subsequently, when questioned, Esteban had provided answers which were able to be corroborated against information obtained from both Steve Kowhai and John Fredricksen’s computers.

While Jane Esteban could be argued to have abetted in the trafficking or import of controlled substances, we feel that there would be diminished responsibility on her part as she was threatened by Fredricksen into accompanying him to New Zealand, and that she was not the individual in direct possession of any controlled substances, since the Methamphetamine was found in the suitcase of John Fredricksen. Additionally, we find no evidence to support that Jane Esteban was definitely aware of the purpose of Fredricksen’s trip to New Zealand.

We however are uncertain about the legality and admissibility of the arguments presented regarding Jane Esteban thus far. Mainly, Jane had covertly installed a remote administration tool in order to log the inputs made by John Fredricksen on his laptop. This presents potential issues in whether the evidence such as Exhibits B8 (01-30-2019.html), B9 (01-31-2019.html), B10 (02-01-2019.html) and B11 (02-02-2019.html) would be potentially rendered inadmissible as evidence due to how it was obtained.

5.4. Future Plans and Intentions of Guilty Parties

With the available information and evidence, we believe that in the case where John Fredricksen and Jane Esteban had not been stopped and questioned by Customs officers at Wellington Airport, they would have continued with their future plans.

Steve Kowhai

Assuming that he would be able to successfully obtain the Methamphetamine that was discovered by Customs, we believe that Steve Kowhai had the intention to scale up deliveries of Methamphetamine from John Fredricksen for future shipments, as outlined in Exhibit A9 (Memo Things.odt). Additionally, Kowhai had harboured intentions of being involved in the “cutting” of the methamphetamine, which involves diluting the substance’s purity or enhancing its effects. Having processed the drugs, we also believe that he intended to further distribute the drugs, likely within the vicinity of Wellington, New Zealand. With the profits from the sale of the drugs, Kowhai also likely intended to perform acts of money laundering, as evident from his search history, thus supporting our initial conclusions from the Case 1 report.

John Fredricksen

Despite the available evidence and our analyses, we are less certain about the future plans and intentions of John Fredricksen. However, we strongly believe that Fredricksen is likely to continue his operations of supplying drugs as per the information found in Exhibit A6 (client.ods). Similarly, it is also likely that Fredricksen envisions scaling up the operations of supplying drugs, evident from his conversation with Jane Esteban about having “bigger fish to fry”, seen in Exhibit A12 (Discord Chat Logs).

5.5. Further Action

While our evidence outlined in this report is detailed, we have also identified further areas that could be done to ensure comprehension in the investigation, should there be a need and if the resources permit.

5.5.1. Thumbdrive Analysis

It is crucial to analyse the thumbdrive previously connected to John's laptop, the Kingston DataTraveler, to uncover evidence related to his drug trafficking activities, particularly focusing on potential leads at his Inala address, found in the shipping details in Exhibit A3.

Type	Value
Date/Time	2019-01-29 12:01:20 SGT
Device Make	Toshiba Corp.
Device Model	Kingston DataTraveler 102/2.0 / HEMA Flash Drive 2 GB / PNY Attache 4GB Stick
Device ID	408D5C142849B0C159D753A3
Source File Pat	/img_Narcos-2.001/vol_vol7/Windows/System32/config/SYSTEM

5.5.2. Mobile Device Examination

Obtain and examine the mobile device linked to Jane's laptop to uncover any relevant communications between Jane and John, which could provide insights into their collaboration or illegal dealings.

Type	Value
Date/Time	2019-01-31 13:40:22 PST
Device Make	Samsung Electronics Co., Ltd
Device Model	Galaxy A5 (MTP)
Device ID	83f14a4a384d4c51
Source File Path	/img_Narcos-3.001/vol_vol7/Windows/System32/config/SYSTEM
Artifact ID	-9223372036854775688

5.5.3. Protonmail Access

Access John's Protonmail account using the login credentials found on Jane's computer to further examine communications with other individuals involved in illicit activities, aiming to gather incriminating evidence.

5.5.4. Memory Dump Analysis

Attempting to run Volatility on the memory dump could provide valuable insights; however, the memory dump provided was unusable, hindering our ability to extract further information from it.

6. Conclusion

In concluding our overall findings between Case 1 and Case 2, we believe that firstly, an individual likely based out of Wellington, New Zealand named Steve Kowhai is the primary suspect of the case. He intended to obtain methamphetamine supplied by John Fredricksen, which was discovered by Customs upon arriving in Wellington Airport. There is also strong evidence to believe that Kowhai had intentions of further expanding the scale of operations related to processing, selling of drugs, and laundering the proceeds from their sale.

Secondly, we believe Jane Esteban to be part of the Australian Federal Police, serving as an undercover agent with the goal of discovering and prosecuting drug-related activities. She initially approached John Fredricksen attempting to purchase drugs, but was eventually threatened to accompany Fredricksen to Wellington to deliver the drugs to Kowhai.

We thus believe two suspects to be guilty in light of the overall case and all available evidence - Steve Kowhai of intention to traffic and produce controlled drugs, and money laundering; and John Fredricksen of trafficking and import of controlled substances.

Considering their future plans and intentions, we believe that if Steve Kowhai was able to obtain the methamphetamine from John Fredricksen, he would continue to scale up subsequent shipments of the drug from Fredricksen, and to process and redistribute the drugs in his possession. We also believe that John Fredricksen is likely to continue supplying his current clients, and also is considering opportunities to seek new clients with larger orders.

7. Appendix

7.1. Combined Timeline of Events

All dates and times in the timeline of events will be stated in SGT (GMT+8)

Legend:
Events are highlighted based on their source/evidence

- Case Background/Information
- Evidence/Conclusion from Case 1
- Evidence/Conclusion from Case 2

2019-01-23

09:18:28 - John Fredricksen creates image of DHL shipping label, showing a package intended for Jake Heke in Auckland

2019-01-28

23:00:00: Steve Kowhai performs multiple searches on the internet relating the “cutting drugs”, and money laundering

2019-01-29

01:00:00 - Steve Kowhai performs multiple searches related to drug routes in Wellington and internationally
05:29:39 - Steve Kowhai initiates contact with John Fredricksen over Discord, with the message “Need to get a new delivery”
05:09:29 - Jane Esteban creates and compresses Quasar client as Contact Card.zip
11:29:13 - Jane Esteban initiates contact with John Fredricksen over Discord, with the message “Got any of that ice??”
11:32:45 - Jane Esteban sends Contact Card.zip to John
22:01:00 - John Fredricksen Downloads ZIP file

2019-01-30

Before 06:14:00 - John Fredricksen extracts and runs Contact Card.exe, the Quasar client connects to the server and starts recording key and mouse input information for the next 4 days
Before 07:40:00 - Steve Kowhai composes the Memo Things.odt file, creates an AES encrypted volume with TrueCrypt with the password “ilovediving”, and stores the word document within
07:40:00 - Steve Kowhai sends John Fredricksen the encrypted volume with instructions on how to access files within over email
08:00:16 - John Fredricksen downloads the attached encrypted volume from his email
08:04:00 - John Fredricksen decrypts the downloaded volume with TrueCrypt and accesses the Memo Things.odt contained within

2019-01-31

05:00:00 - Steve Kowhai searches for multiple routes on Google maps (Wellington Airport to Eastbourne, location of Eastbourne Library, Wainuiomata to Eastbourne to Stokes Valley), and creates screenshots of each route.
08:22:19 - John Fredricksen threatens Jane Esteban with photos of her children, demanding that she follows him New Zealand to reduce suspicion on Fredricksen
09:59:00 - John Fredricksen performs multiple searches for terms relating to hiding of drugs and travel to Wellington
10:57:00 - Steve Kowhai performs multiple searches for drug paraphernalia

2019-02-01

07:02:24 - John Fredricksen takes photo of suitcase and packaged drugs, saved as package.jpg
07:05:17 - John Fredricksen creates image (BNE.png) hidden with package.jpg using the Image Steganography program
08:11:00 - John Fredricksen sends image hidden with packaged drugs and suitcase (BNE.png) to Steve Kowhai over email

2019-02-02

06:29:00 - John Fredricksen searches for flights from Brisbane to Wellington
08:02:08 - John Fredricksen books flights to Wellington, New Zealand and instructs Jane Esteban to meet at 133 Oxley Station Road on the day of the flight
10:30:36 - Steve Kowhai informs John Fredricksen to meet at Eastbourne Library or alternatively 666 Rewera Avenue

2019-02-16

06:45:00 - Jane Esteban and John Fredricksen departs on a flight from Brisbane bound for Wellington
11:15:00 - Jane Esteban and John Fredricksen arrive in Wellington, subsequently arrested and questioned by Customs

2019-02-23

02:15:00 - John Fredricksen and Jane Esteban are scheduled to depart Wellington, New Zealand en route to Brisbane, Australia, with a stopover at Auckland, New Zealand

7.2. Autopsy String Search Terms

John
Jane
Methamphetamine
Drugs
Eastbourne
666 Rewera
Wellington
crayfish1980
Steve kowhai
heresjohnny1
Elchapo2
crayfish1980
becomingjane