IFS4102 Digital Forensics Case Presentation

Group 6

By: Wellington Customs Forensic Department
Investigators: Ang Yong Ming, Hrithie Menon, Ibrahim Sharul, Teo Chuan Kai

Table of contents

Our Role

- Analyse evidence of the seized laptops
- Further understand motives, goals and objectives of
  - John Fredricksen
  - Suspect, who is determined to be Steve Kowhai
  - Jane Esteban
- Present case findings to Customs' management and in court

Questions pending answers

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

Brief answers to questions

Question	Brief Answer
1. Who was Jane actually?	An undercover Australian Police Officer
2. What did John think of Jane, and what did he want from her?	A vulnerable individual who could be used to orchestrate a facade of a couple on holiday to evade detection
3. Who were the guilty parties in the overall case based on the extra evidence given?	Steve Kowhai and John Fredricksen
4. What were the guilty parties' future plans and intentions based on the extra evidence	Steve Kowhai - Scaling up deliveries of Meth John Fredricksen - Continue trafficking drugs

Overview of case

- Intelligence from the Australian government led to the interception of John Fredricksen and Jane Esteban upon their arrival in Wellington, New Zealand from Brisbane.
- During a search, **one kilogram of Methamphetamine** was found in John Fredricksen's suitcase.
- Additional evidence provided by Customs officers: images and memory dumps of two seized laptops.
- Initial uncertainty regarding Jane Esteban's role and guilt.
- Further forensic examination of the new evidence to understand the motives, relationship and future intentions of Fredricksen, Esteban, and Kowhai.

Findings from Case 1

- Steve Kowhai, our suspect, who goes by the username “crayfish1980” communicated with John Fredricksen via discord to arrange for a delivery of Methamphetamine to Eastbourne Library or alternatively, 666 Rewera Avenue.
- Many evidence found pointing to Steve’s intention to buy and resell drugs on a larger scale and money launder
- Potential presence of encrypted contents and a unrecoverable deleted memo document found

Methodology

- **Evidence Acquisition:** Obtained computer drive images from customs officers.
- **Chain of Custody Management:** Signed and maintained a chain of custody form for each acquired drive image.
- **Integrity Verification:** Combined the acquired drive image files and verified their hash values using powershell to ensure integrity and detect any potential tampering
- **Examination Utilizing Forensic Tools**: Employed forensic tools such as Autopsy to systematically analyze the entire drive image for suspicious files, artifacts, and potential evidence.

Evidence Analysed

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

Overview of 2 computers seized

John Fredricksen

Operating System	Drive
Name: JOHNFLAPTOP1 Version: Windows 10 Pro Processor Architecture: AMD64 Product ID: 00330-80000-00000-AA310 Owner: JohnF	Type: Image Size: 32212254720 bytes (30.0GB) Sector Size: 512 bytes Device ID: b6ef7f3b-8930-4671-8133-d8a69df8774e

Jane Esteban

Operating System	Drive
Name: JELAPTOP Version: Windows 10 Pro Processor Architecture: AMD64 Product ID: 00330-80000-00000-AA263 Owner: Windows User	Type: Image Size: 32212254720 bytes (30.0GB) Sector Size: 512 bytes Device ID: 016e41e0-c13e-453c-9b95-a886aa80fb28

Drive Information

John Fredricksen

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

Drive Information

Jane Esteban

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

Forensic 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

Search Terms used in Autopsy

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

John Fredricksen’s computer

Narcos-2

User Installed Programmes

Apache OpenOffice

Open-source word processing application

Baidu Antivirus

Host-based anti-malware solution offered by Baidu.

Discord

Instant messaging and voice over IP (VoIP) social platform

Image Steganography

Program which allows users to embed text and files in images

Mozilla Firefox

Web browser by Mozilla Foundation

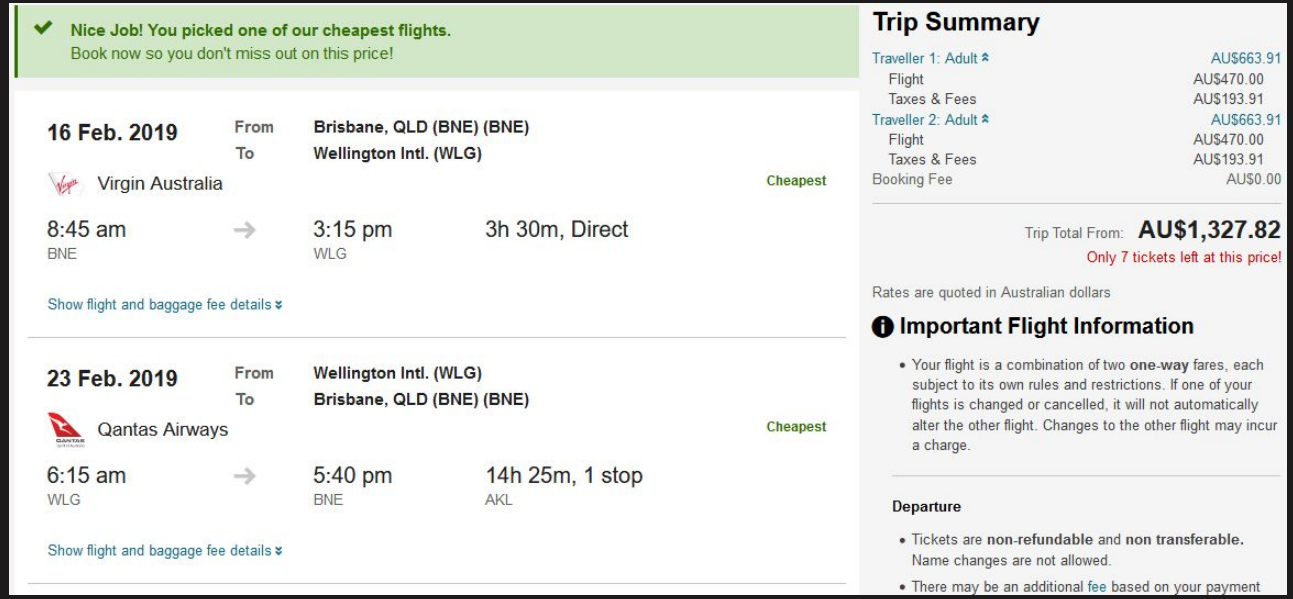
TrueCrypt

Open-source utility to encrypt partitions or whole storage devices

Exhibit A1: BNE.png

Same picture as in Case 1 of Brisbane sent from John to Steve; Image hidden inside with password “Elchapo2” titled “Package.jpg” (Exhibit A5)

Exhibit A2 (Steve K.PNG)



Nice Job! You picked one of our cheapest flights.
Book now so you don't miss out on this price!

16 Feb. 2019
From Brisbane, QLD (BNE) (BNE)
To Wellington Intl. (WLG)
Virgin Australia — Cheapest
8:45 am BNE → 3:15 pm WLG — 3h 30m, Direct
Show flight and baggage fee details

23 Feb. 2019
From Wellington Intl. (WLG)
To Brisbane, QLD (BNE) (BNE)
Qantas Airways — Cheapest
6:15 am WLG → 5:40 pm BNE — 14h 25m, 1 stop AKL
Show flight and baggage fee details

Trip Summary

Traveller 1: Adult	AU$663.91
Flight	AU$470.00
Taxes & Fees	AU$193.91
Traveller 2: Adult	AU$663.91
Flight	AU$470.00
Taxes & Fees	AU$193.91
Booking Fee	AU$0.00

Trip Total From: **AU$1,327.82**
Only 7 tickets left at this price!

Rates are quoted in Australian dollars

Important Flight Information

- Your flight is a combination of two **one-way** fares, each subject to its own rules and restrictions. If one of your flights is changed or cancelled, it will not automatically alter the other flight. Changes to the other flight may incur a charge.

Departure

- Tickets are **non-refundable** and **non transferable.** Name changes are not allowed.
- There may be an additional fee based on your payment

Trip summary of return flights booking from Brisbane for 2 (Same as in Case 1); John and Jane. Fredricksen communicated this to Steve and Jane

Exhibit A3 (shipping.PNG)

Different name

Likely fake company name

Inala address - John is from here

1 of John's clients in client list

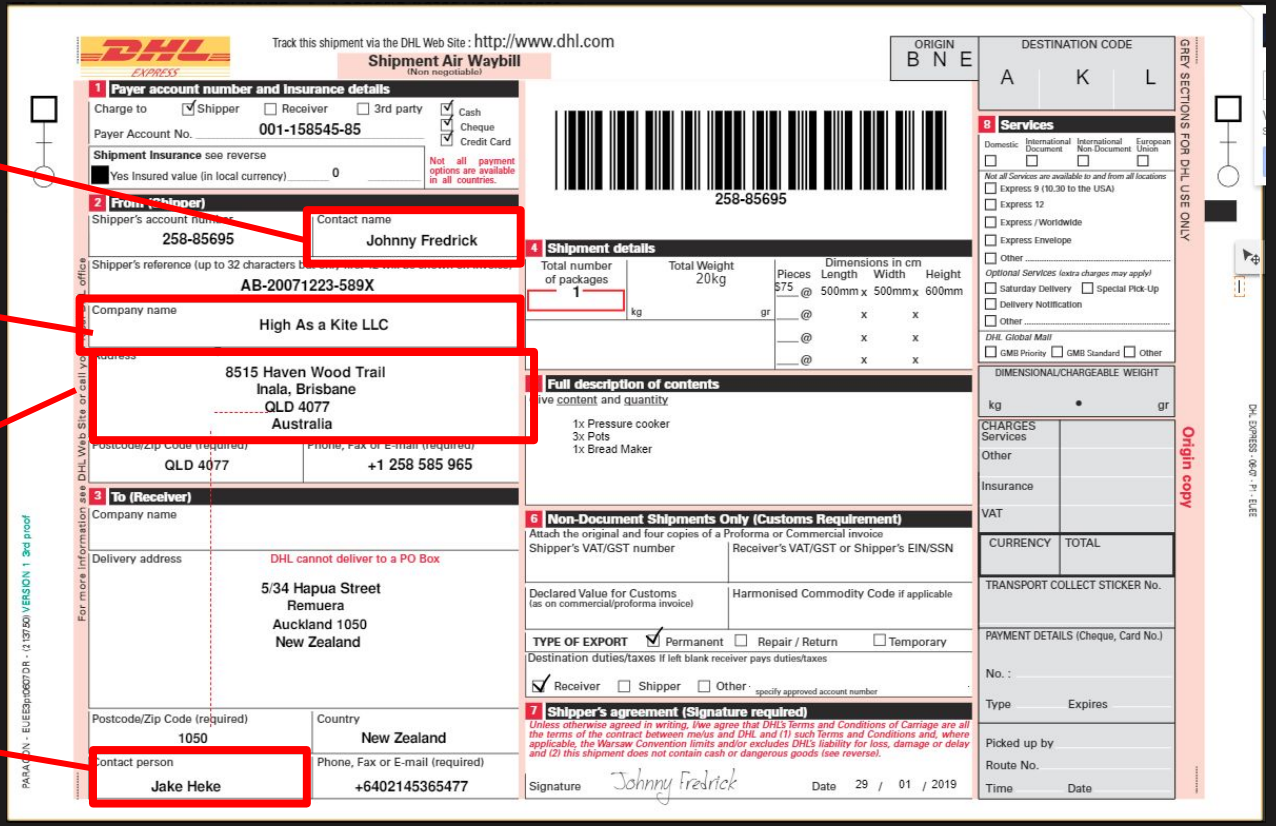


Exhibit A4 (Janes Kids.jpg)

A picture of Jane Esteban Kids, used to blackmail her in Exhibit A12 (Discord Chat Logs)

Exhibit A5 (package.jpg)

Picture hidden in Exhibit A1: BNE.png showing where drugs will be hidden, sent to Steve for him to retrieve “the package” later

Exhibit A6 (clients.ods)

	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

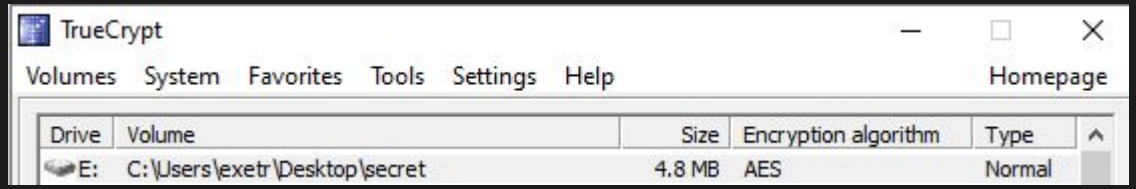
Different types of drugs

Under his business folder is this document contains the name of several individuals, their locations, products, amounts and frequency of delivery; The products seem to be colloquial terms for different type of drugs

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

Downloads folder of John, downloaded as an attachment from John Fredricksen's ProtonMail account, as elaborated in Exhibit A13 (ProtonMail Account), title indicative of something substantial

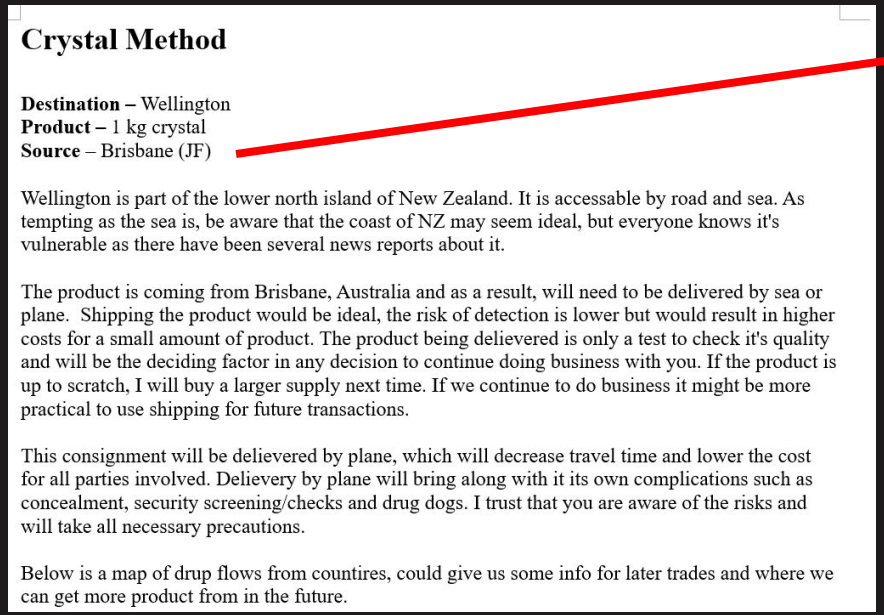
Exhibit A8 (secret)



File found in zip archive, similar name to Possible Presence of Encrypted Contents in Case 1. Found to be encrypted file using password “ilovediving”. Steve sent it to John and deleted it immediately (Case 1)

Exhibit A9 (Memo Things.odt)

John Fredricksen



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.

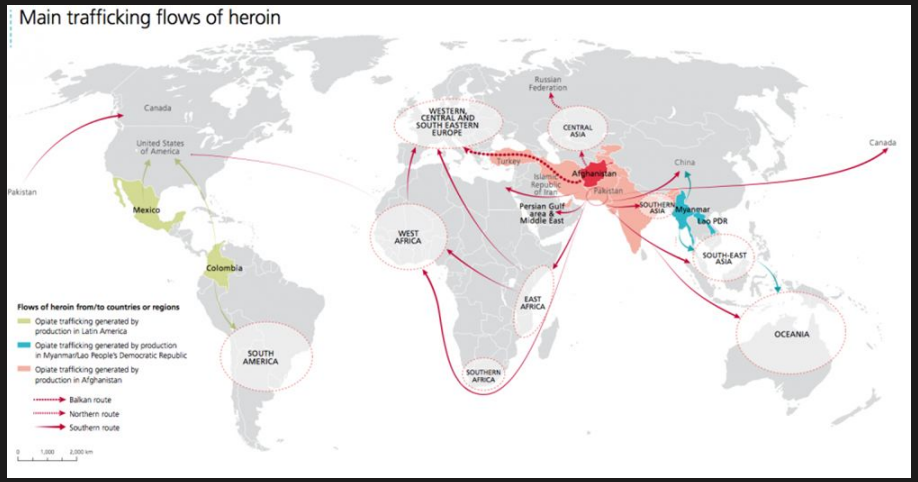
The product is coming from Brisbane, Australia and as a result, will need to be delivered by sea or plane. Shipping the product would be ideal, the risk of detection is lower but would result in higher costs for a small amount of product. The product being delievered is only a test to check it's quality 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.

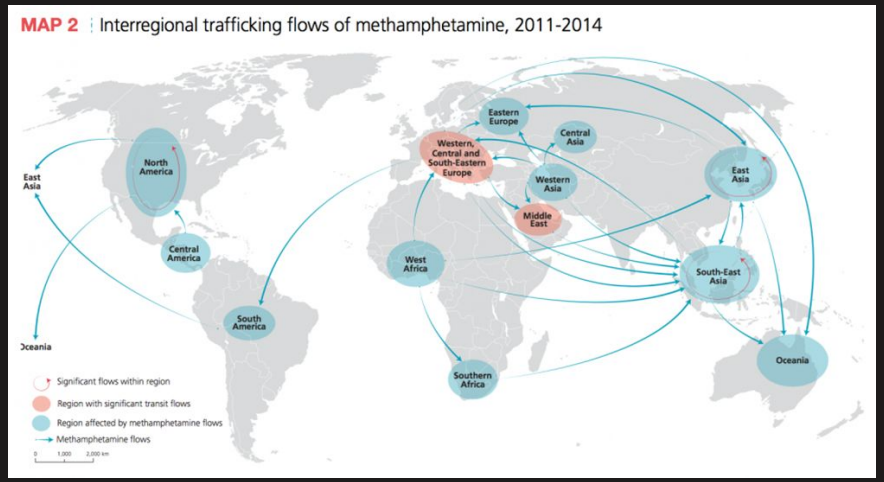
This consignment will be delievered by plane, which will decrease travel time and lower the cost for all parties involved. Delievery by plane will bring along with it its own complications such as concealment, security screening/checks and drug dogs. I trust that you are aware of the risks and will take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

Extracted from secret encrypted volume; Tells details of operation to transport 1kg of crystal (ice) from Brisbane to Wellington.

Exhibit A9 (Memo Things.odt)



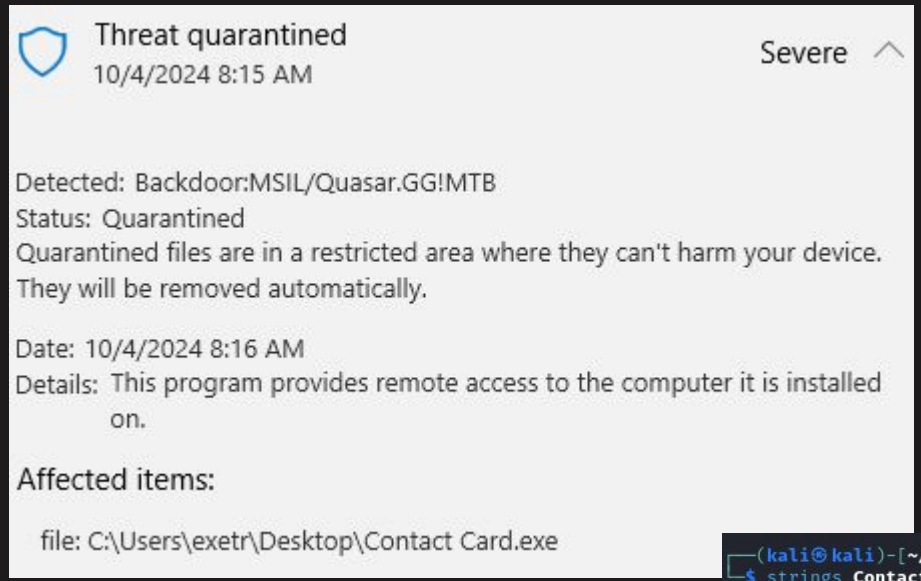


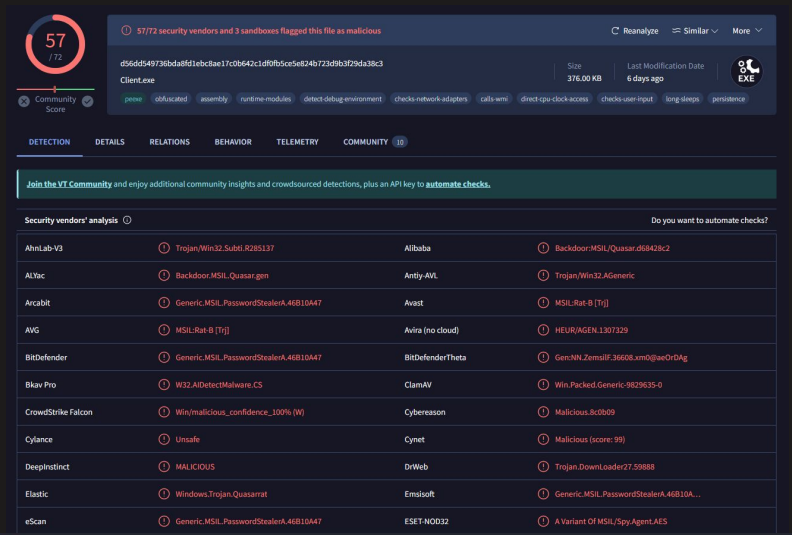
Shows details of how their drug trafficking operations worldwide

Exhibit A10 (Contact_Card.zip)

Found in Downloads folder, sent by Jane Esteban via Discord from Exhibit A12 (Discord Chat Logs) and downloaded by John

Exhibit A11 (Contact Card.exe)





A known malware with Remot Administration tool (with keylogger) activated

```
┌──(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
```

Exhibit A12 (Discord Chat Logs) - Deleted

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

Conversation between John and Jane, Contact_Card zip sent

Exhibit A12 (Discord Chat Logs)

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??

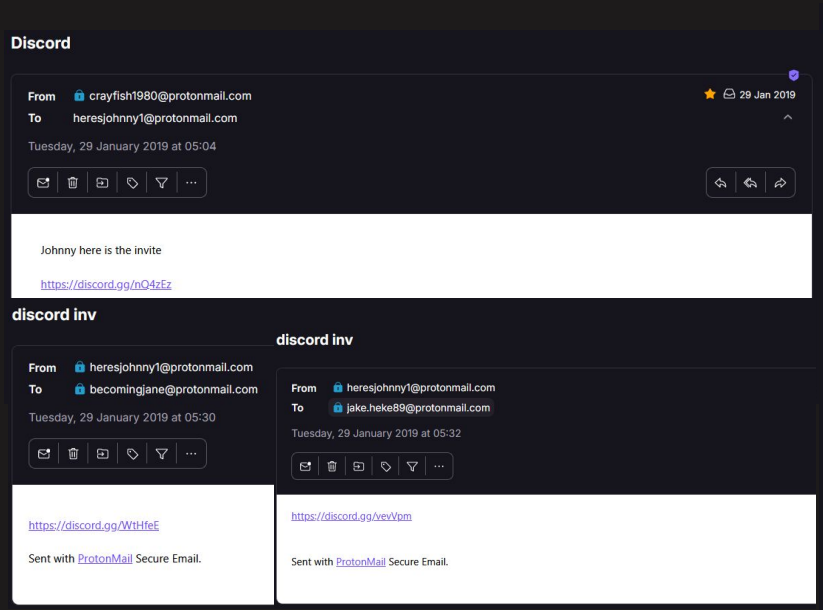
Timestamp: 2019-01-31 08:28:17.127 SGT
Username: heresjohnny1
Message: Good, now that's what I wanted to hear. Here is the plan. You and I will be acting like a couple travelling on a holiday to New Zealand. This is what I want you to do: Look the part, act normal, and don't tell anyone about what we're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

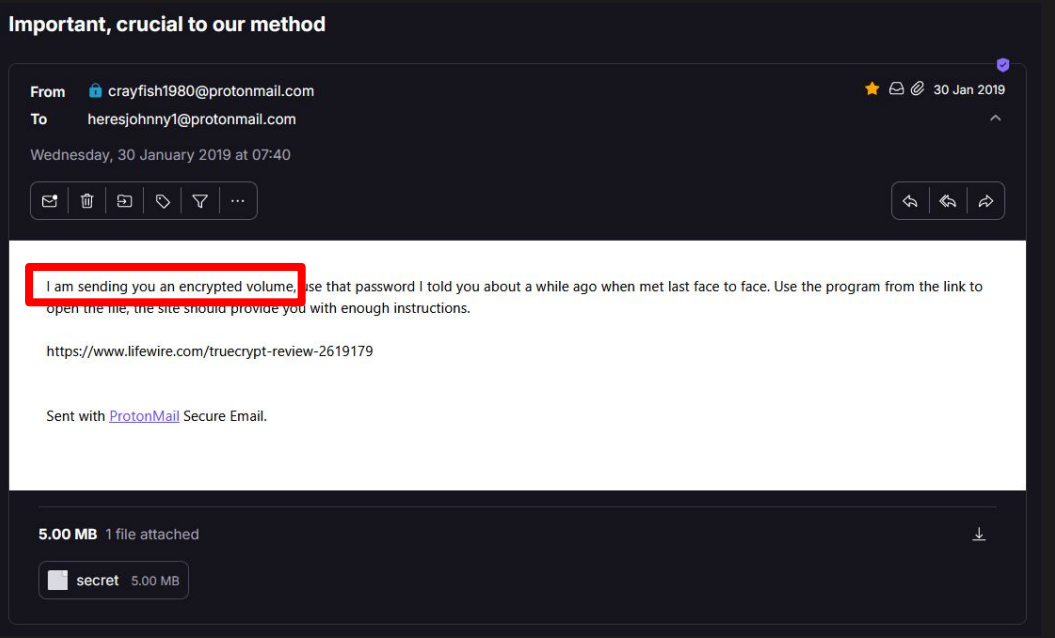
Timestamp: 2019-01-31 08:29:00.666 SGT
Username: becomingjane
Message: Yes John... I got it

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

Blackmailed Jane and being forced to follow her as a cover

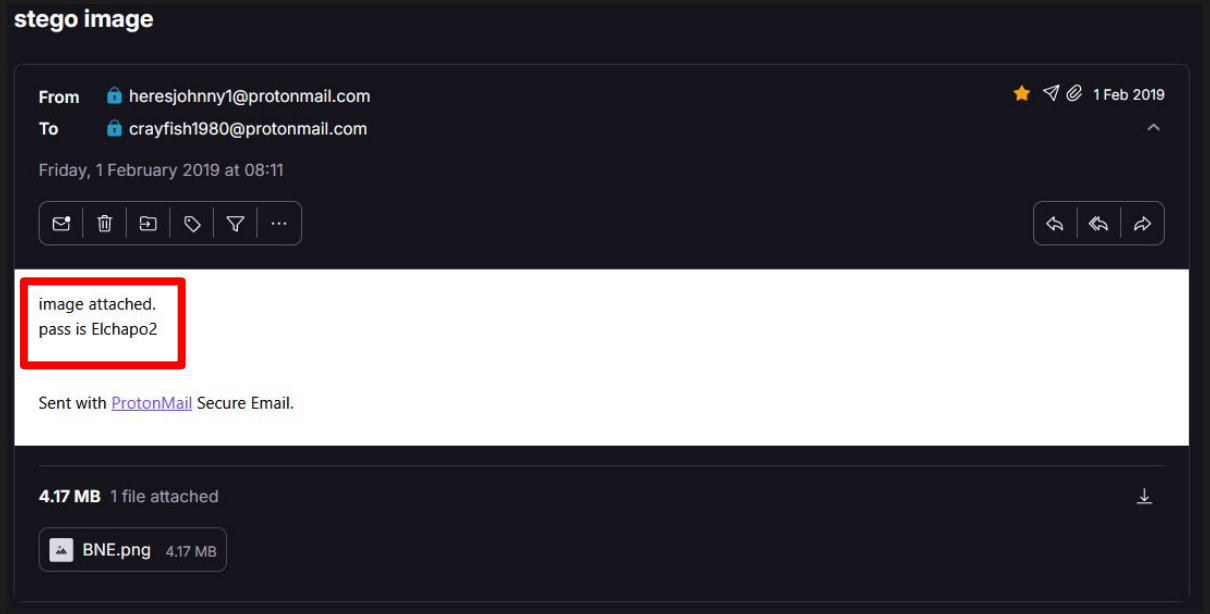
Exhibit A13 (ProtonMail Account)





Sent route and encrypted volume, as in Exhibit A8

Exhibit A13 (ProtonMail Account)



Password to the Image Steganography in Exhibit A1 (BNE.png)

Exhibit A14 (Microsoft Edge History)

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)

protonmail (via bing.com)
6 instances (between 2019-01-28 21:12:28 SGT and 2019-01-29 02:10:47 SGT)

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)

Exhibit A14 (Microsoft Edge History)

Items of Interest in Search History:
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)

Exhibit A14 (Microsoft Edge History)

Items of Interest in Search History:
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)

Exhibit A14 (Microsoft Edge History)

Items of Interest in Search History:
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)

Exhibit A15 (Mozilla Firefox 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

Exhibit A15 (Mozilla Firefox History)

Items of Interest in Search History
encryption methods youtube (via google.com)
1 instance (2019-01-29 04:49:46 SGT)

Research to evade crime

drug detector dogs (via google.com)
1 instance (2019-01-31 10:01:30 SGT)

suitcase concealments (via google.com)
3 instances (2019-01-31 10:04:44 SGT to 2019-01-31 10:05:21 SGT)

suitcase concealments for drugs (via google.com)
3 instances (2019-01-31 10:06:09 SGT to 2019-01-31 10:12:48 SGT)

Exhibit A15 (Mozilla Firefox History)

Items of Interest in Search History
flights brisbane to WLG return (via google.com)
1 instance (2019-01-31 10:15:43 SGT)

To hide package details of where drugs are stored

steganography image download (via google.com)
2 instances (2019-02-01 05:29:24 SGT, 2019-02-01 05:29:27 SGT)

Flights from brisbane to wellington au
1 instance (2019-02-02 06:40:45 SGT)

Shows where John might be from

directions from Inala to brisbane airport
1 instance (2019-02-02 10:46:16 SGT)

Jane Esteban Computer

Narcos-3

User installed Programmes

Quasar

Light-weight remote administration tool with RDP and keylogging features

Discord

Instant messaging and voice over IP (VoIP) social platform for communication

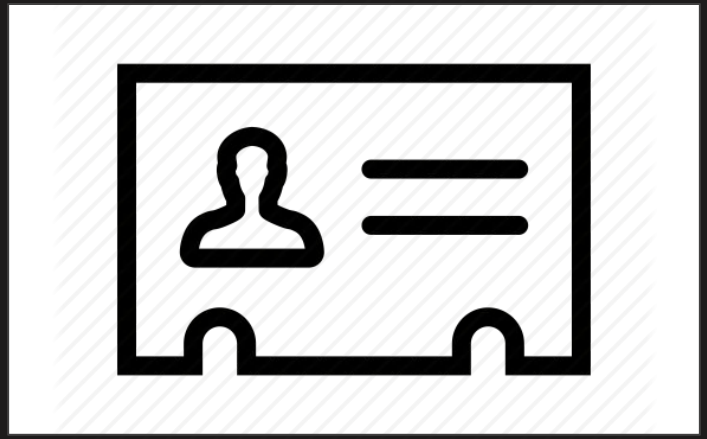
Exhibit B1 (afp.png) - Deleted

A badge of the Australian Federal Police

Exhibit B2 (background.png)

A badge, along with the title of the Australian Federal Police

Exhibit B3 (contact-card-512.png)



A clip art of contact-card, used by Jane to change the icon of the Quasar Keylogger to this Contact card image so that John would unknowingly execute it

Exhibit B4 (crys1.jpg), B5 (crys2.jpg), B6 (crys3.jpg)

Image of what we suspect to be Methamphetamine crystals, likely used by Jane for her research into drug trafficking

Exhibit B7 (course-undercover-survival.pdf)

Found in her documents, outline for a law enforcement in-service training course offered by Schoolcraft College's Public Safety Training Center titled "Undercover Survival and Lawful Invasions".

Shows that she might be an undercover officer when combined with Police badge and with her search history

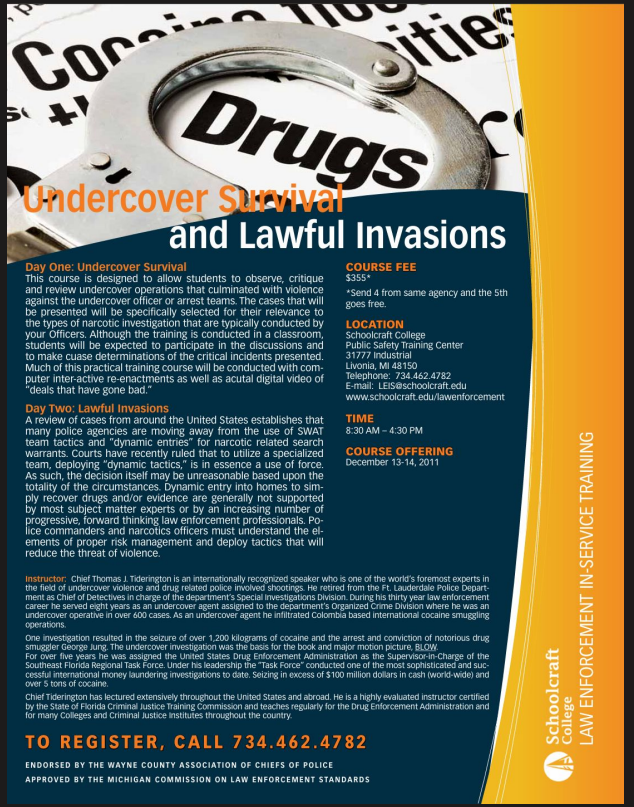


Exhibit B8 (01-30-2019.html) - Keylogger

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]

John's email details

Exhibit B8 (01-30-2019.html)

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]

Password to secre
encrypted content

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]

Exhibit B9 (01-31-2019.html)
Exhibit B10 (02-01-2019.html)

Repeated content as shown in Exhibit B8

Exhibit B11 (02-02-2019.html)

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]

His idea of packing the Meth crystals into a salt packaging to evade detection.

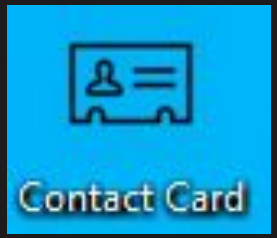
Event (Time): sunblock tan - Woolworths Online - Mozilla Firefox (12:45)
directions from Inala to brisbane airport[Enter]

Event (Time): Enter password for C:\Users\JohnF\Downloads\Attachments-Importa...\secret (12:50)
ilovediving

Exhibit B12 (Contact Card.zip)- Deleted

ZIP file with keylogger was sent as an attachment by Jane to John, passing it off as the “contact card” of individuals who were interested in obtaining drugs from John, who subsequently downloaded and extracted

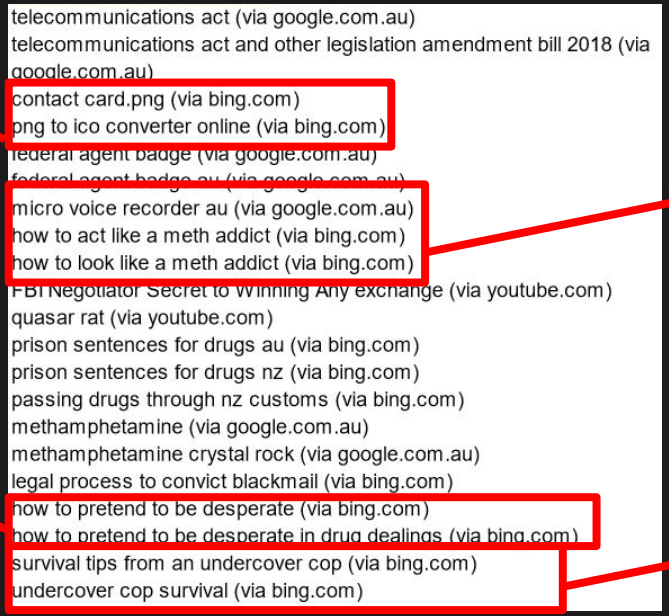
Exhibit B13 (Contact Card.exe) - Deleted



Same as Exhibit A11. Supports theory on keylogger generated to send John Fredricksen. Proceeded to delete the executable on her host

Exhibit B14 (Microsoft Edge History)

Preparation for contact with John by creating the keylogger



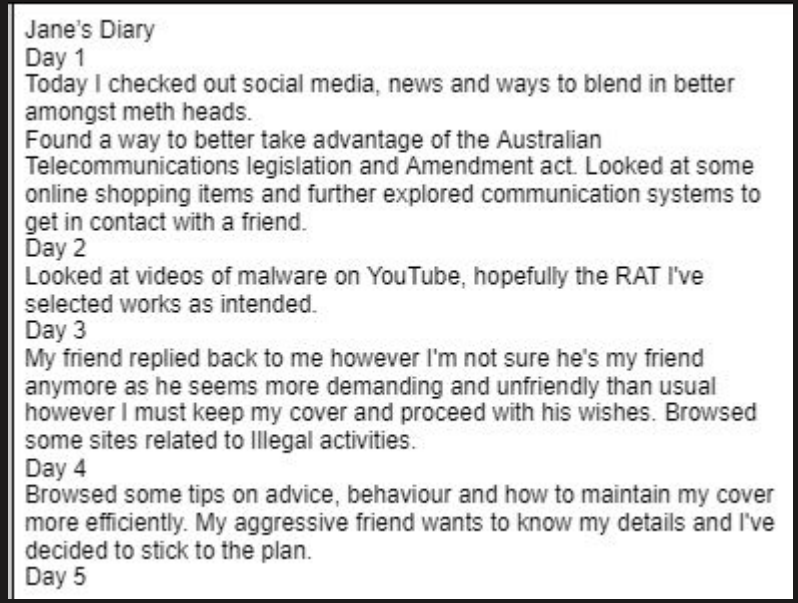
Preparation before the contact with John

Shows she was worried when John did not want new clients

Reaffirms her fear so she is searching for tips before she went on the trip

Jane's undercover role as a drug user allows her to gather vital information on John's illegal activities, aided by her use of deception and a micro voice recorder.

Exhibit B15 (Microsoft OneDrive Cache)



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

Her diary confirms her identity as a undercover officer taking cover

Analysis and Conclusion

1. Identity of Jane Esteban

Name: Jane Esteban
Suspected Role: Undercover Agent
Focus: Drug-related activities and crimes
Proficiency:
Despite some indications of uncertainty or inexperience, proficiency in using tools for information gathering.

The amount of information on her laptop and her handling of certain situations suggest competence beyond mere suspicion.

1. Identity of Jane Esteban

- Possibility that the evidence indicating her AFP allegiance could be planted to mislead investigators, but the amount of information on her laptop and her handling of certain situations suggest otherwise.

- Overall, the evidence strongly supports the conclusion that Jane Esteban is indeed an undercover agent for the AFP, tasked with uncovering and prosecuting individuals involved in drug-related activities.

2. What did John think of Jane? What did John want from Jane?

- Initially receptive to Jane Esteban's request for drugs but lost interest when she sent a file he couldn't open, indicating he viewed her as a potential drug buyer.
- Proposed that Esteban accompany him on a business trip to New Zealand, showing he viewed Jane as gullible and wanted to use her to mask the trip as a couple holiday
- Threatened harm to Jane Esteban's children when she refused, suggesting he saw her as vulnerable and manipulable.
- Booked flights for their trip to Wellington, indicating he expected her compliance.

3. Who were the guilty parties in the overall case?

1. Steve Kowhai:

- Guilty of intent to traffic controlled substances, as evidenced by his intended receipt and redistribution of methamphetamine from John Fredricksen.
- Suspected intent of manufacturing controlled substances, indicated by search history related to drug modification processes.
- Suspected intent to commit acts of money laundering in conjunction with drug distribution.

3. Who were the guilty parties in the overall case?

2. John Fredricksen:

- Guilty of trafficking in controlled substances, supported by evidence of his role as a supplier and distributor of drugs.
- Guilty of import and export of controlled substances, demonstrated by possession and transportation of methamphetamine from Australia to New Zealand.

3. Who were the guilty parties in the overall case?

3. Jane Esteban:

- Not assigned guilt based on evidence suggesting she provided intelligence to New Zealand Customs, leading to the apprehension of Fredricksen.
- Diminished responsibility due to coercion by Fredricksen into accompanying him to New Zealand.
- No direct possession of controlled substances and unclear awareness of Fredricksen's intentions.
- Uncertain legality and admissibility of evidence obtained through covert installation of a remote administration tool on Fredricksen's laptop.

4. Guilty parties' future plans and intentions based

1. Steve Kowhai:

- Intended to scale up deliveries of methamphetamine from John Fredricksen for future shipments.
- Planned to be involved in the process of "cutting" methamphetamine to enhance its effects or dilute its purity.
- Intended to distribute the processed drugs, likely within Wellington, New Zealand and worldwide
- Planned to engage in acts of money laundering with profits from drug sales, as indicated by his search history.

4. Guilty parties' future plans and intentions based

2. John Fredricksen:

- Likely to continue operations of supplying drugs
- Envisioned scaling up drug supply operations, as suggested by conversation with Jane Esteban about having "bigger fish to fry" in Exhibit A12 (Discord Chat Logs), which could refer to Steve's ambitious expansion plan seen in Exhibit A9 (Memo Things.odt)

Further action

- Find the thumb drive that was connected to John's laptop and analyse for further details of his drug trafficking empire, likely found in his address in Inala

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

- Obtain Mobile Device that was connected to Jane's laptop and analyse for further communication between Jane and John

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

Further action

- Access John's Protonmail using his login credentials found in Jane's Computer to find correspondences with his other clients

- Being able to run volatility properly on memory dump might yield us more info but the memory dump given was unusable

Timeline

Legend:
Events are highlighted based on their source/evidence

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

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

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

Timeline

Legend:
Events are highlighted based on their source/evidence

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

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

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

Timeline

Legend:
Events are highlighted based on their source/evidence

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

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

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

Timeline

Legend:
Events are highlighted based on their source/evidence

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

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

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

Any Questions?