FORENSICS INVESTIGATION REPORT

BY

TILIJE UZU

TABLE OF CONTENT

Executive Summary:

This forensic investigation report focuses on the digital evidence collected from the devices of three suspects as follows:

1. Steve Kowhai (Narcos-1, unknown suspect)
2. John Fredrickson (Narcos-2)
3. Jane Esteban (Narcos-3)

The suspects are implicated in a transnational drug trafficking operation before they were intercepted at Wellington, New Zealand border. The investigation reveals a sophisticated network where John Fredrickson, identified as the primary supplier, coordinated with his new client Steve Kowhai, the buyer, through encrypted channels to arrange drug transactions.

Jane Esteban, a key accomplice, posed as John's wife to facilitate the transport of the illicit substances across borders. Evidence extracted from their devices includes detailed communication logs, encrypted documents, drug-related images, and digital evidence of flight bookings and delivery plans. The suspects employed various encryption techniques, such as steganography and TrueCrypt, to conceal the nature of their activities and protect sensitive information.

This report outlines the findings from the analysis of their devices and presents the critical evidence that links each suspect to the drug trafficking operation.

Key Evidence: 1. **John**

Fredrickson Drive:

- A folder named "**Attachments-Important, crucial to our method**" which contains an encrypted secret file of John Fredrickson and Steve Kowhai deal plans and future intentions.
- An Excel file named "**client.ods**" which contains the list of John Fredrickson customers (buyers of his drug product), location of the buyer, kind of product, amount, and delivery period.
- An image "**BNE.png**" that hides the main product to be delivered to Steve Kowhai using a steganography tool.
- Flight booking ticket of John Fredrickson and Jane Esteban to Steve Kowhai location.
- A DHL Shipping ticket named "**shipping.PNG**" that ships John Fredrickson's product (10kg of Tweak) to one of his clients Jake Heke in Auckland, New Zealand.

2. **Steve Kowhai Drive**:

- Multiple images of drug products and dollar cash.

- The "**BNE.png**" image that was encrypted and sent to him (Steve Kowhai) by John Fredrickson which hides the main product to be delivered to him.
- Images of the map for John Fredrickson travel planned route to transit the product and the destination address where the product is to be delivered to.
- The flight booking ticket of John Fredrickson and Jane Esteban from Brisbane, Australia, to Wellington, New Zealand.

3. **Jane Esteban Drive:**
   - A folder named "**Clients**" that contains a conversation transcript between John Fredrickson and Jane Esteban via discord. The chat log revealed the deal plans with Steve Kowhai, the encryption method used to hide their secret with password, and the destination address to meet Jane Esteban for take-off to Wellington, New Zealand.
   - A tool "**Quasar.exe**" used as a remote desktop to connect an external computer remotely. This is where the conversion transcripts between John Fredrickson and Jane Esteban, and the browser activities of John Fredrickson were downloaded from.
   - Various images of hard-drug substances.

Introduction

The purpose of this forensic investigation was to gather, analyze, and document evidence related to an alleged drug trafficking network involving three individuals: John Fredrickson, Steve Kowhai, and Jane Esteban.

John Fredrickson, the suspected supplier, orchestrated drug shipments from Brisbane, Australia, to Wellington, New Zealand, with Steve Kowhai as the intended recipient. Jane Esteban, acting as an accomplice, played a critical role by pretending to be John Fredrickson's wife to facilitate the smuggling operation. Law enforcement intercepted the suspects at the border, which led to a forensic examination of their digital devices for evidence.

The investigation uncovered a series of encrypted communications between John Fredrickson and Jane Esteban on Jane's device, which detailed drug deal arrangements with Steve Kowhai, methods of concealment, and plans for the next shipment. John Fredrickson's device contained extensive records, including secret files, client lists, order details, and travel

itineraries related to the upcoming smuggling. Steve Kowhai's device revealed images of drugs and other related content that John Fredrickson had sent. The suspects used steganography to obscure the primary package contents and TrueCrypt to hide sensitive documents, adding layers of encryption to evade detection.

This report provides an in-depth analysis of the evidence found on each suspect's device, detailing the communication methods, encryption techniques, and incriminating files discovered. The findings presented in this investigation will support the prosecution of the suspects for their involvement in the illegal drug distribution network.

Chapter One

Policy and Procedures for Handling Digital Evidence

The handling of digital evidence in this investigation followed strict protocols to ensure its integrity, reliability, and admissibility. The following policy and procedures outline the key steps: 1. **Evidence Collection:**

Digital evidence was collected from the suspects' devices in a manner that preserved the original state of each device. Standard forensic imaging tools(FTK Imager, Volatility) were used to create bit-by-bit copies of the drives from John Fredrickson, Jane Esteban, and Steve Kowhai(unknown suspect), ensuring that no data was altered during the acquisition process.

2. **Chain of Custody:**

A documented chain of custody was maintained from the time evidence was collected to its analysis and storage. This documentation records every individual who handled the evidence, the purpose for accessing it, and the date and time of each transfer. A proper chain of custody ensures accountability and helps prevent any questions regarding tampering or contamination. 3. **Evidence Hashing:**

To guarantee the integrity of each piece of digital evidence, a cryptographic hash (using algorithms like SHA-256, SHA-1 or MD5) was generated for each file or drive image at the time of acquisition. Hash values serve as unique digital fingerprints for the data, and any alteration to the files would result in a change in the hash value. The hash values were then securely recorded to verify the integrity of the evidence throughout the investigation process. 4. **Evidence Storage:**

All digital evidence was securely stored in a controlled-access forensic lab. Digital images, physical devices, and extracted artefacts were stored in a manner that prevents unauthorized access and environmental damage. 5. **Evidence Analysis:**

Forensic analysis was conducted on forensic copies rather than the original devices to prevent data alteration. Specialized tools (TrueCrypt, Steganography) were used to decrypt files, recover hidden data, and analyze encrypted communications while adhering to forensic best practices to maintain data authenticity. 6. **Documentation:**

Detailed documentation of all forensic steps taken including acquisition, hashing, analysis methods, and results was maintained as part of the investigation record. This documentation supports transparency, reproducibility, and reliability in the forensic findings.

Chapter Two
Evidence Assessment

1. Steve Kowhai Drive Image Analysis:

Starting with the image evidence Drive-One (Narcos-1), identified to be Steve Kowhai, the forensic image was uncompressed, the hash was verified for integrity and the image file was fully loaded with AccessData FTK Imager for analysis.

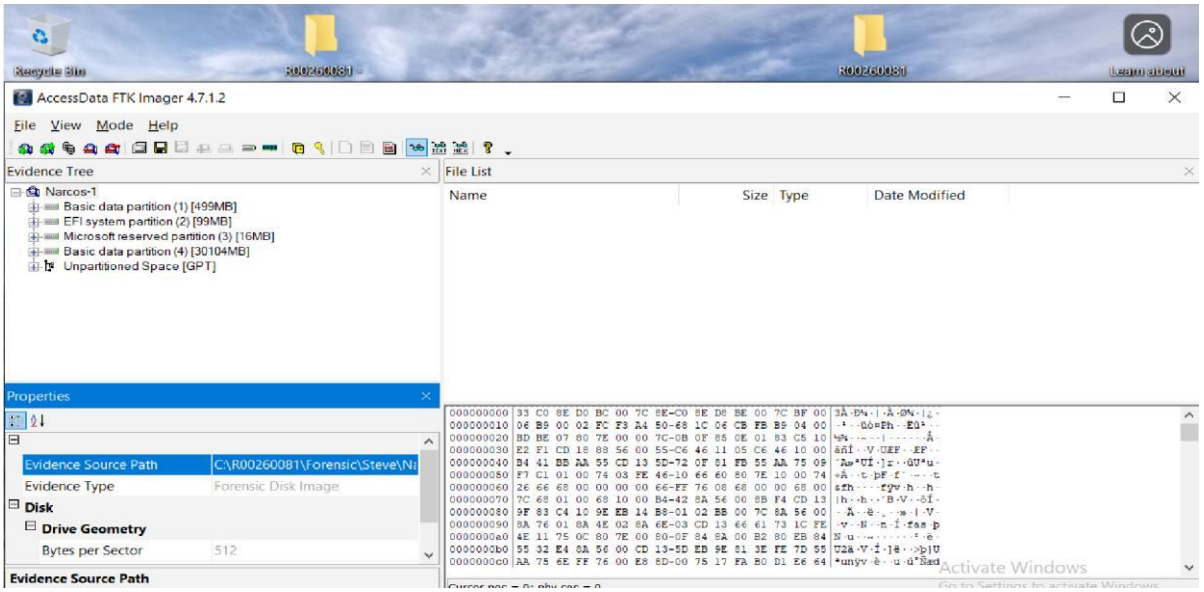


Fig 2.1 Steve Kowhai's Drive Image (Narcos-1)

a.) Analysis of evidence found in the suspect **Recycle.Bin** folder:

• **Narcos-1\NTFS\root\Recycle.Bin\S-1-5-21-1474204758-2504895174-13560748211001**

While investigating the suspect drive, multiple hard-drug images with loads of dollar cash were found in the Recycle.Bin directory: This is an indicator that the suspect is evidently involved in illicit drug trafficking as shown in the image below.

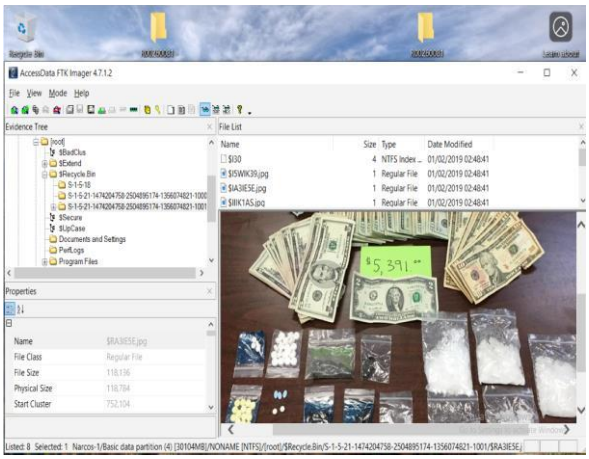


Fig 2.2 Image of dollar cash with illicit drugs

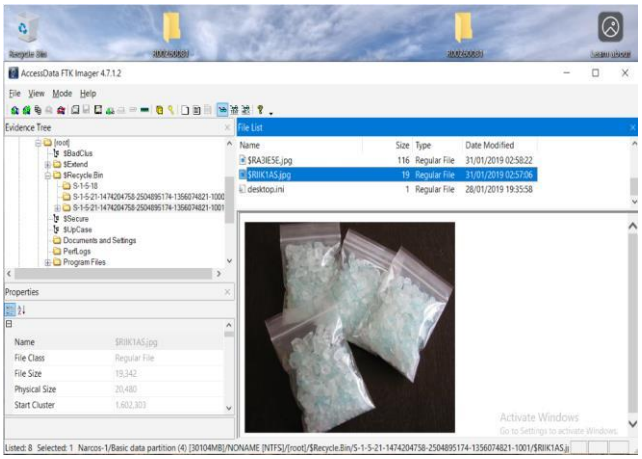


Fig 2.3 Image of illicit drugs

b.) Analysis of evidence found in the suspect's **Documents** folder:

• **Narcos-1\NTFS\Users\Steve\Documents\Misc**

Series of image evidence were found in the suspect Documents directory which includes a round-trip flight booking ticket (**flightbookings.PNG**) scheduled a take-off on 16th February, 2019 at 08:45 am from Brisbane airport, Australia to Wellington, New Zealand with a return trip scheduled on 23rd February, 2019 at 06:15 am from Wellington airport New Zealand back to Brisbane, Australia. And a secret file at **C:\Users\Steve\Documents\Misc\secret,** appeared as a deleted file.

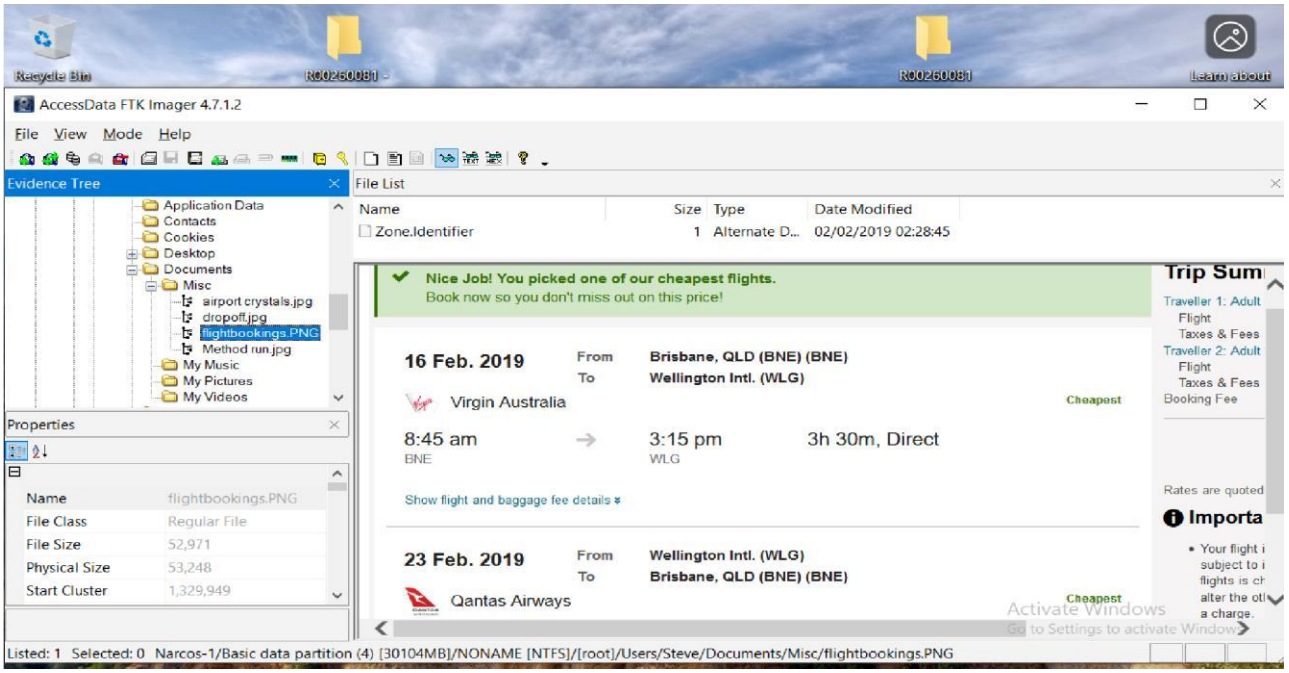


Fig 2.4 A flight booking ticket C:\Users\Steve\Documents\Misc\flightbooking.PNG

An image of a map "**airport crystals.jpg**" and "**Method run.jpg"** were found in the same Documents folder. These images indicated a direction of transit from the Wellington airport to the suspect home address which is pinpointed on the map. This confirmed that an accomplice which is expected to land in Wellington by 16th February will be visiting the suspect address for a yet unknown mission.

An image "**dropoff.jpg**" which indicated the exact address of the suspect was also found in the same Documents folder (**38 Rimu St, Eastbourne, Lower Hutt 5013**). As also indicated on the map that the suspect definitely lives in Eastbourne.

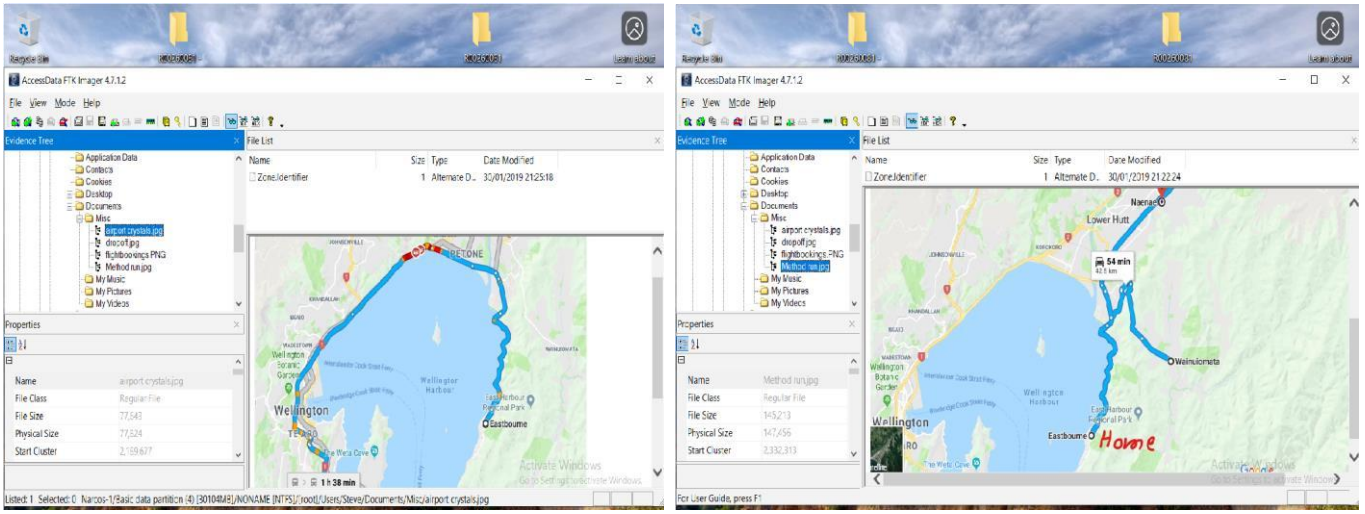


Fig 2.5 A map directions to Steve Kowhai home address

c.) Analysis of evidence found in the suspect's **Downloads** folder:

- **Narcos-1\NTFS\Users\Steve\Downloads**

Suspicious software was found in the suspect Downloads folder, this includes: "**Image Steganography 1.5.2 Setup.exe**" and "**TrueCrypt Setup 7.1a.exe**". These applications are mainly being used to hide and encrypt secret contents respectively. An image "**BNE.png**" and a discord application "**DiscordSetup.exe**" which is being used as a communication channel was also found in the Downloads folder: **Narcos-1\NTFS\Users\Steve\Downloads\Misc**

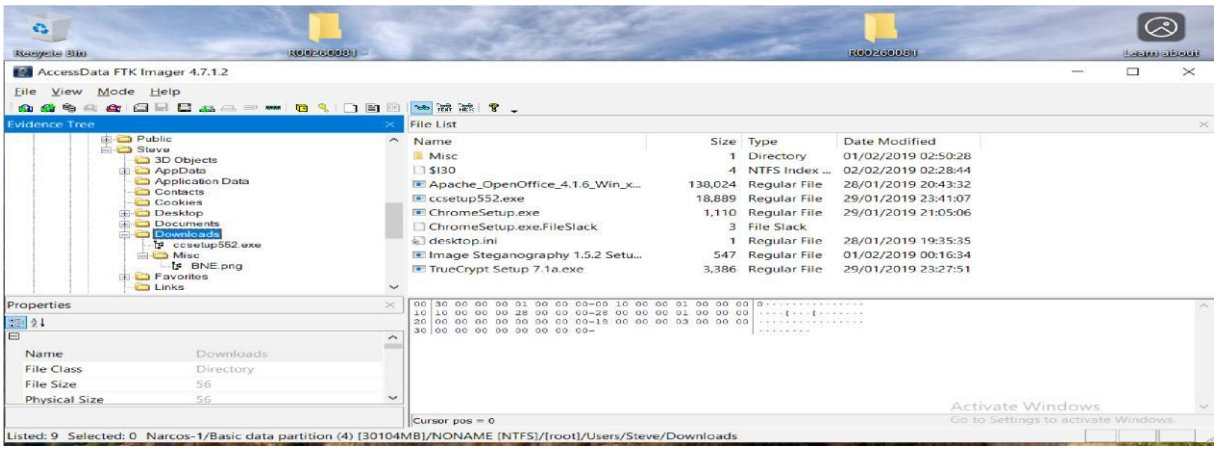


Fig 2.6 Steve Kowhai download folder: C:\Users\Steve\Downloads

d.) The Suspect Memory Image Analysis:

The memory image file was uncompressed, the hash was verified for integrity, and the splitted memory image file was merged into a volatility readable format and then analysed using Volatility3.

Volatility command (**sudo python3 vol.py Narcos-Mem-1.raw windows.info**) was executed to display information of the suspect machine (windows version 10) which was subjected to the forensic assessment as shown below.

```
┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility3]
└─$ sudo python3 vol.py -f Narcos-Mem-1.raw windows.info
[sudo] password for progress:
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0×f804432a9000
DTB     0×1ad000
Symbols file:///home/progress/Downloads/R00260081/Forensic/R00260081/Forensic/Memory%20Dump/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/6924731305
6076BBCB3411FD96428714-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0×f804436afdc0
Major/Minor     15.17763
MachineType     34404
KeNumberProcessors      4
SystemTime      2019-02-02 02:33:34+00:00
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Sun Apr 10 16:09:02 2044

┌──(progress㉿R00260081)-[~/…/R00260081/Forensic/Memory Dump/volatility3]
└─$
```

Fig 2.7 Steve Kohwai's machine information

Using the Volatility "psscan" (**sudo python3 vol.py Narcos-Mem-1.raw windows.psscan)** plugin to display the running process, various processes were found to be running on the suspect machine while one of the processes of interest is the **Discord.exe** which serves as a communication and documents sharing channel.

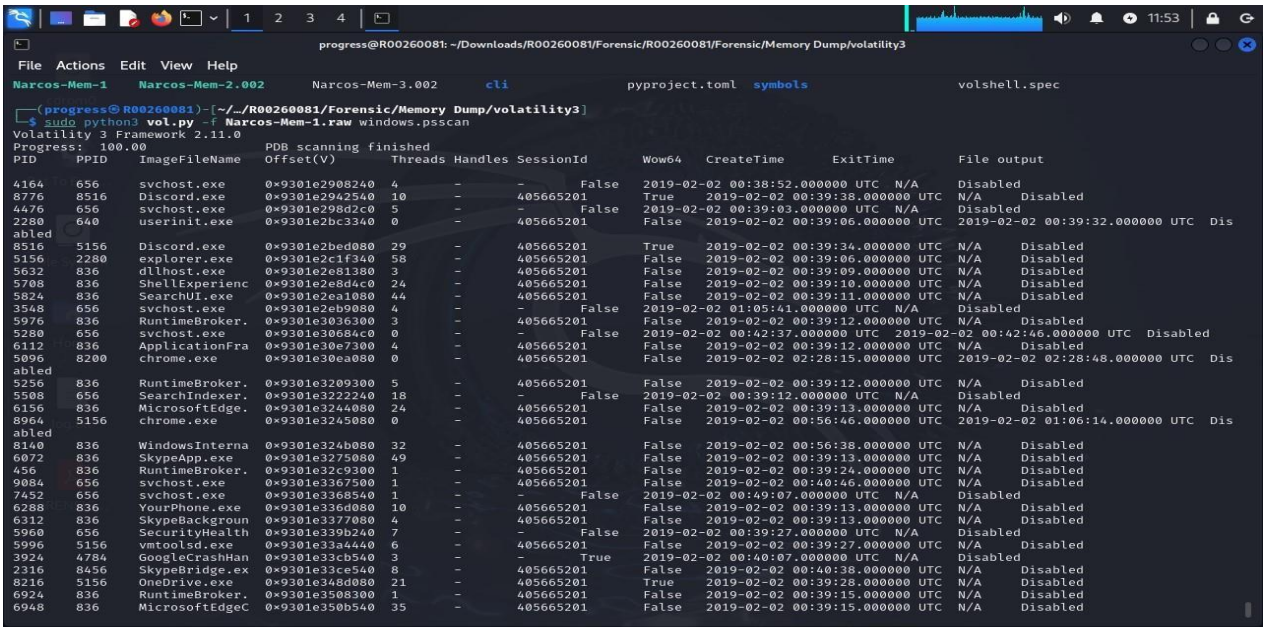


Fig 2.8 Steve Kohwai's machine running processes

2. John Fredrickson Drive Image Analysis

John Fredrickson (Narcos-2), one of the suspects that was intercepted by the law enforcement agency. John's forensic image was uncompressed, the hash was verified for integrity, and the image file was fully loaded with AccessData FTK Imager for analysis.

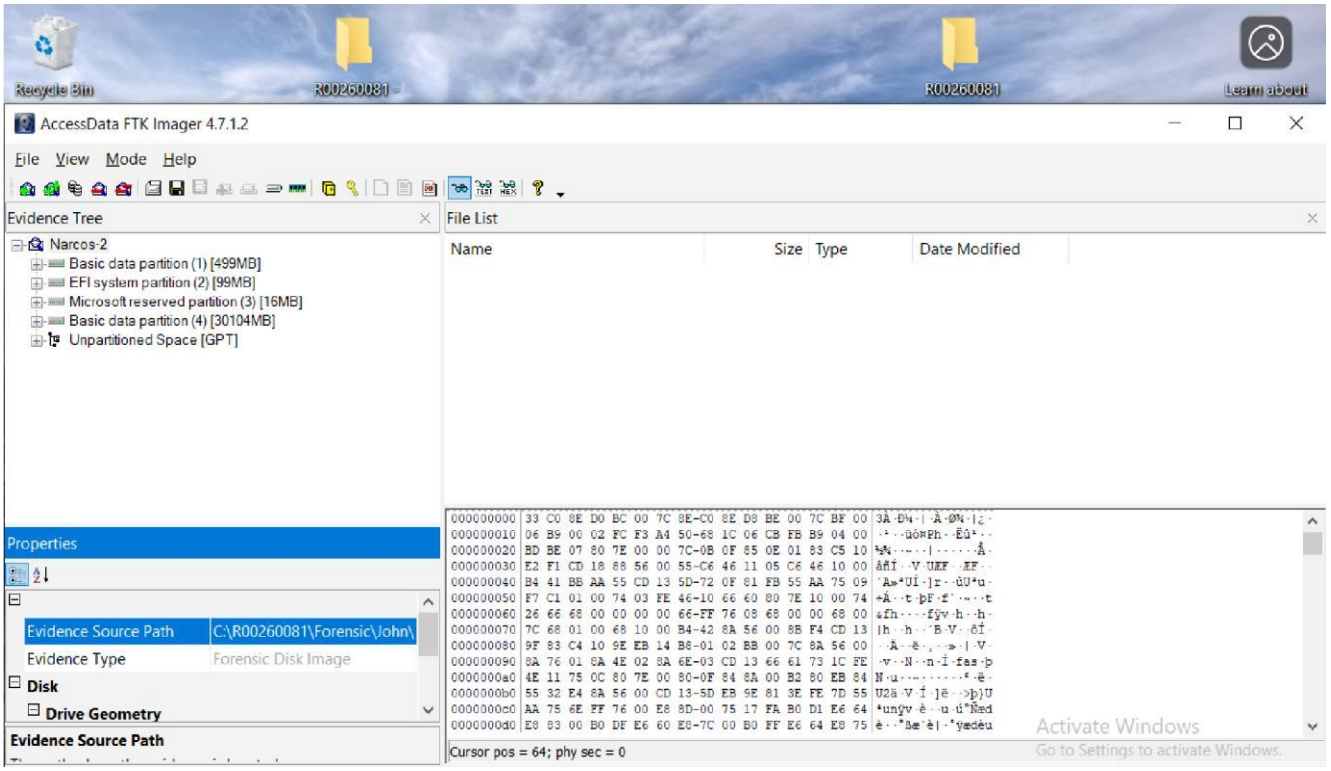


Fig 2.9 John Fredrickson's drive image (Narcos-2)

a.) Analysis of evidence found in the suspect **Business** folder

- **Narcos-2\NTFS\Users\JohnF\Documents\Business**

Among the evidence found in this folder includes: **clients.ods, shipping.PNG,** and **Steve K.PNG.** The "Steve K.PNG" is the image of the same flight booking ticket that was previously found on Steve Kowhai's machine. A round-trip flight booking ticket scheduled a take-off on 16th February, 2019 at 08:45 am from Brisbane airport, Australia to Wellington, New Zealand with a return trip scheduled on 23rd February, 2019 at 06:15 am from Wellington airport New Zealand back to Brisbane, Australia.

The **shipping.PNG** shows an image of a DHL delivery ticket transiting a product from a sender Johnny Fredrickson, address (8515 Haven Wood Trail Inala, Brisbane QLD 4077 Australia) to a receiver named Jake Heke, address (5/34 Hapua Street, Remuera Auckland 1050, New Zealand), dated on 29-01-2019 and signed by Johnny Fredrickson.

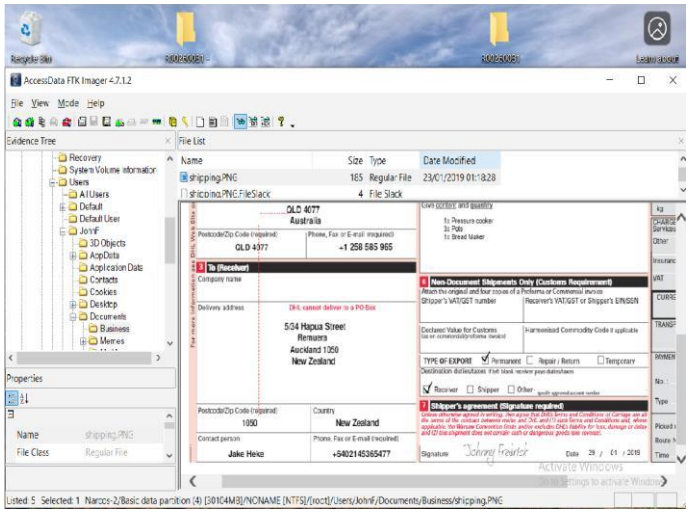


Fig 2.10 DHL Shipping

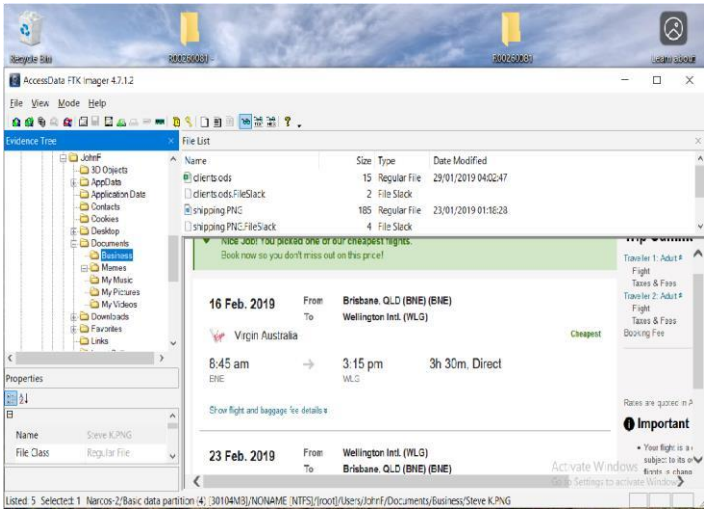
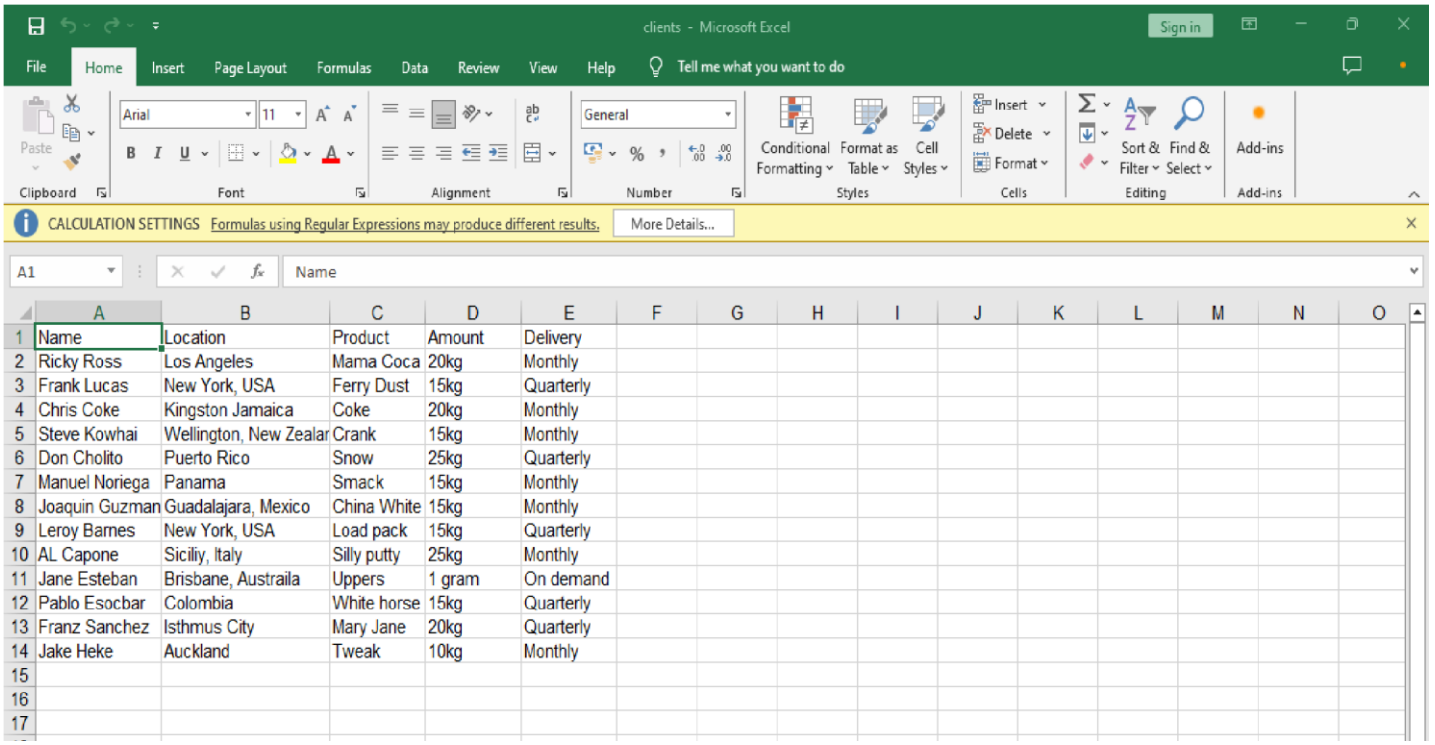


Fig 2.11 Flight Booking Ticket

- The clients.ods: **Narcos-2\NTFS\Users\JohnF\Documents\Business\clients.ods** is an excel document which contains the list of John Fredrickson product buyers (harddrugs). The name of each buyer, the location, the kind of product ordered, the amount (kg, gram), and every delivery period were all contained in this document which confirmed John Fredrickson is indeed involved in hard-drug trafficking with multiple accomplices including Steve Kowhai and Jane Esteban.



clients - Microsoft Excel

CALCULATION SETTINGS Formulas using Regular Expressions may produce different results. More Details...

A1 Name

	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 Zealar	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
15					
16					
17					

Fig 2.12 John Fredrickson's List of Clients C:\Users\JohnF\Documents\Business\clients.ods

b.) Analysis of evidence found in the suspect **Downloads** folder:

- **Narcos-2\NTFS\Users\JohnF\Downloads**

Various documents and applications were found in this folder which includes a very suspicious folder named "**Attachments-Important, crucial to our method**" that contains a file named "**secret**" which is encrypted. Others applications are **Contact Card.zip**, **TrueCrypt Setup.exe** which is being used for file encryption, and **Image Steganography 1.5.2 Setup.exe** which is also being used to hide a content inside an image, and **DiscordSetup.exe** which is being used for communication and documents sharing channel.

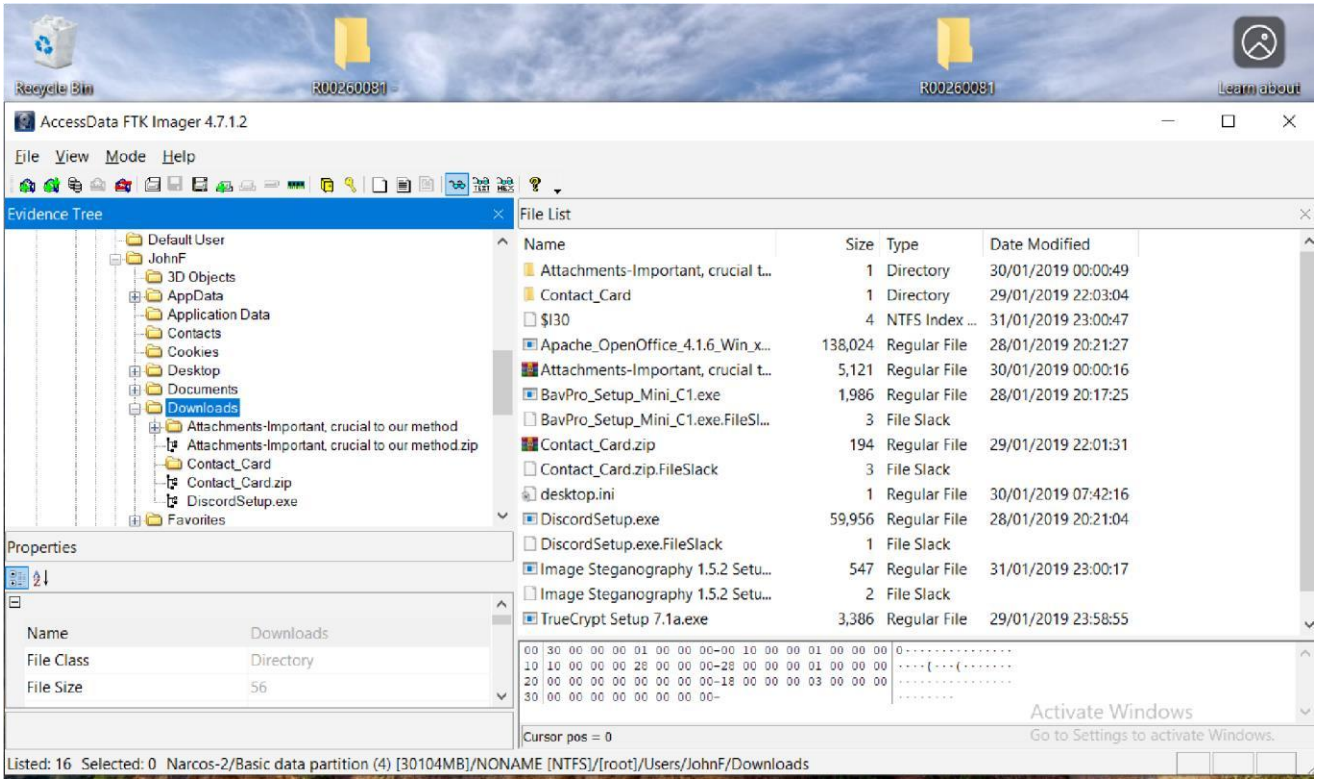


Fig 2.13 John Fredrickson's downloads folder: C:\Users\JohnF\Download

c.) Analysis of evidences found in the suspect **Pictures** folder:

- **Narcos-2\NTFS\Users\JohnF\Pictures**

An image "**BNE.png**" that was previously found on Steve Kowhai's drive was also found in John's folder with the same name attachment. A look alike image was found alongside in the same folder and with a different name attachment "**1540752698-brisbane.jpg**" and a different size. This hinted that a secret content has been hidden in the **BNE.png** image for anonymity.

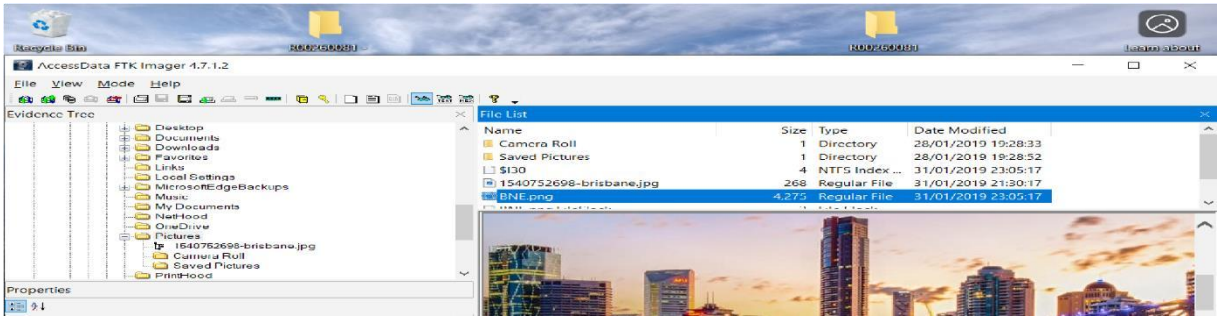


Fig 2.14 BNE.png image: C:\Users\JohnF\Pictures\BNE.png

d.) Analysis of evidence found in the suspect **Documents** folder:

- **Narcos-2\NTFS\Users\JohnF\Documents\Memes**

  Series of drug memes images were also found in the suspect's document directory all convey messages relating to drug trafficking and abuse of drugs which probably indicates the involvement of the suspect in illicit drug trafficking.

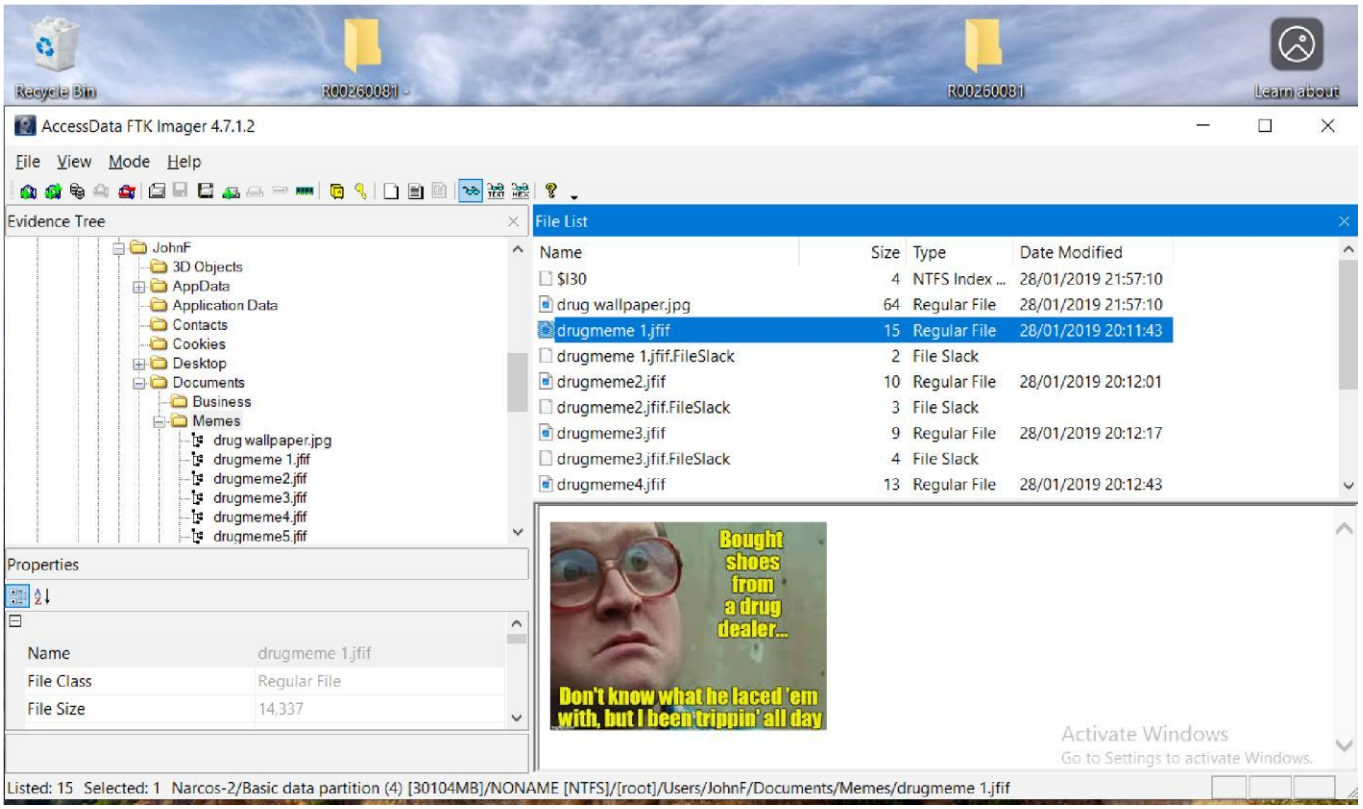


Fig 2.15 Hard-Drug Memes folder: C:\Users\JohnF\Documents\Memes

e.) The Suspect Memory Image Analysis:

The memory image file was uncompressed, the hash was verified for integrity, and the splitted memory image file was merged into a volatility readable format and analysed using Volatility3.

Volatility command (**sudo python3 vol.py Narcos-Mem-2.raw windows.info**) was executed to display information of the suspect machine (windows version 10) which was subjected to the forensic assessment as shown below.

Fig 2.16 John Fredrickson's machine information

Executing the Volatility "psscan" (**sudo python3 vol.py Narcos-Mem-2.raw windows.psscan)** plugin to display the running process, various processes were found to be running on the suspect machine. A process of interest is Discord.exe which has several processes running, the application that runs this process is a communication and documents sharing channel software. This software (Discord.exe) is now confirmed being used by John Fredrickson and Steve Kowhai.

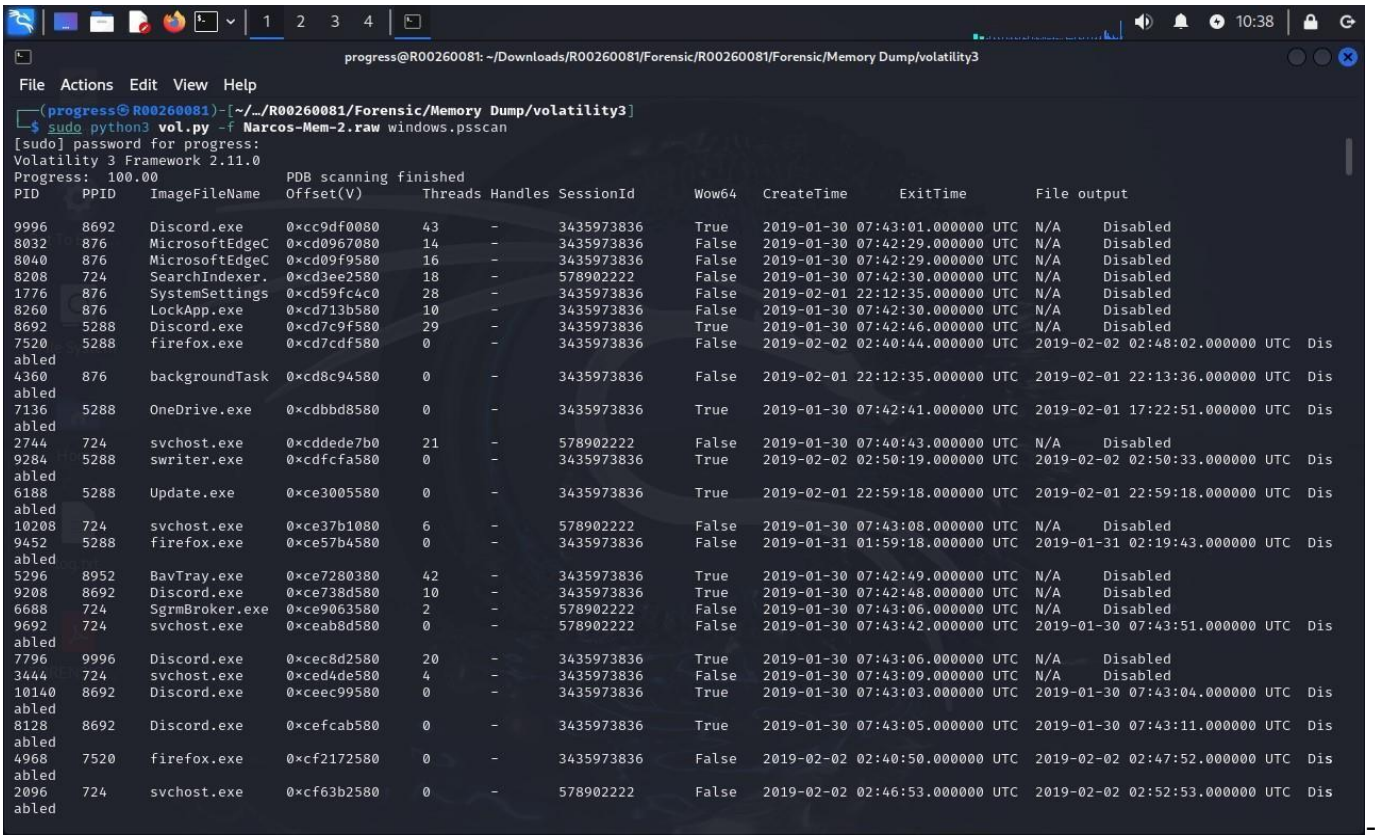


Fig 2.17 John Fredrickson's machine running processes

3.) Jane Esteban Drive Image Analysis:

Jane Esteban (Narcos-3), an undercover Australian Federal Police and one of the suspects intercepted by the law enforcement agency who is an accomplice of John Fredrickson.

Jane's forensic image was uncompressed, the hash was verified for integrity, and the image file was fully loaded with AccessData FTK Imager for analysis.

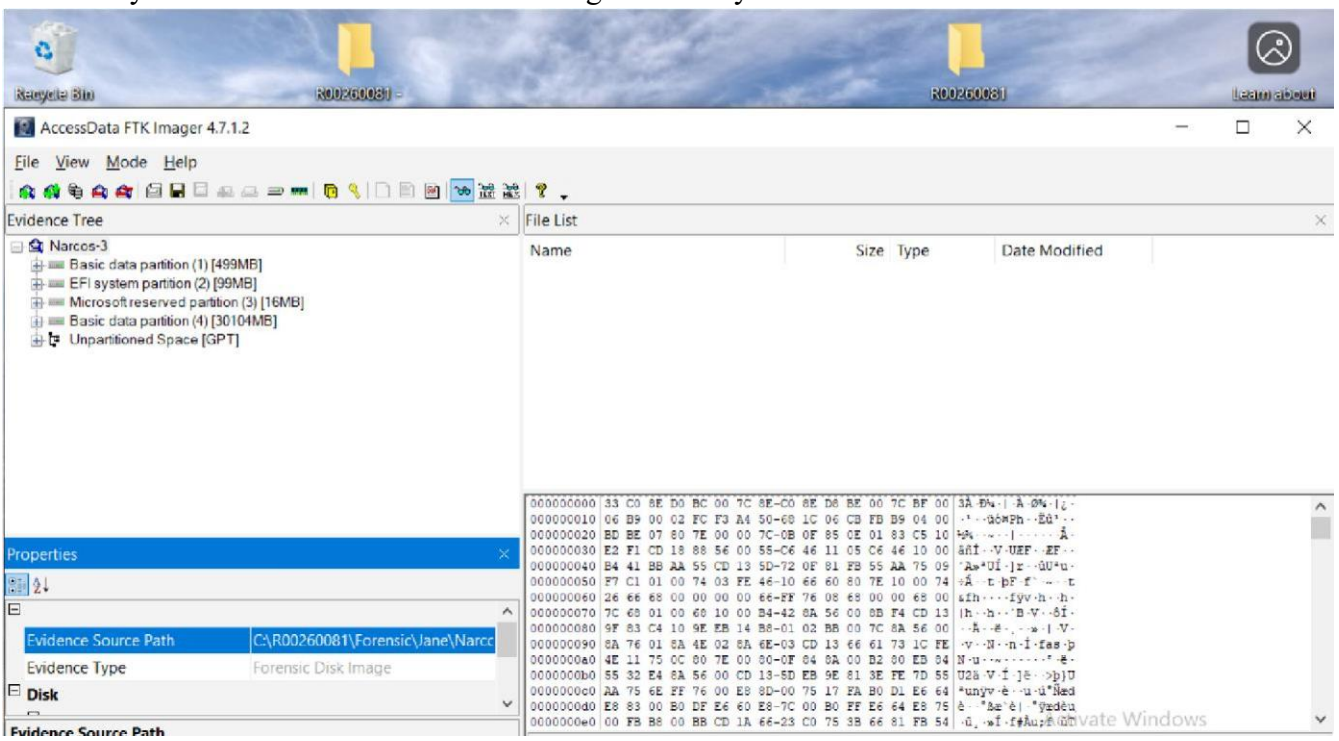


Fig 2.18 Jane Esteban's drive image (Narcos-3)

a.) Analysis of evidence found in the suspect **Downloads** folder:

- **Narcos-3\NTFS\Users\JaneE\Downloads**

Some software were found in the suspect downloads directory which includes: **Contact Card.exe**, the contact card is being used by Jane Esteban and John Fredricksion as a business card, other software found in the same folder is the **Quasar v 1.3.0.0.exe,** this application is being used by Jane to connect to an external computer remotely record all the activities and keystrokes of the connected computer. It was discovered that Jane connected to John's computer using this software and saved John's browser activities and keystrokes on her machine.

b.) Analysis of evidence found in the suspect **Logs** folder:

- **Narcos-3\NTFS\Users\JaneE\Downloads\Quasarv1.3.0.0\Clients\JohnF@JOHNFLAPTOP1_4DD90B0\Logs**

Inside this folder there are browser logs saved by Jane Esteban using the Quasar software which contains the communications between Stave Kowhai and John Fredricksion on their plans relating to drug trafficking while they also shared encrypted documents between them through the discord platform. The logs also include the communications between John Fredricksion and Jane Esteban as an accomplice.

- The suspects communications analysis:

On 30th January, 2019 at around 08:14, John Fredrickson was having a transaction conversation with a client who happens to be Steve Kowhai. Their initial deal was to deliver a product amount up to 10kg of hard-drug, however John had another thought to try to with 1kg due to the risk that might involve with the delivery and planned to proceed with more deals if everything goes well with the first deal.

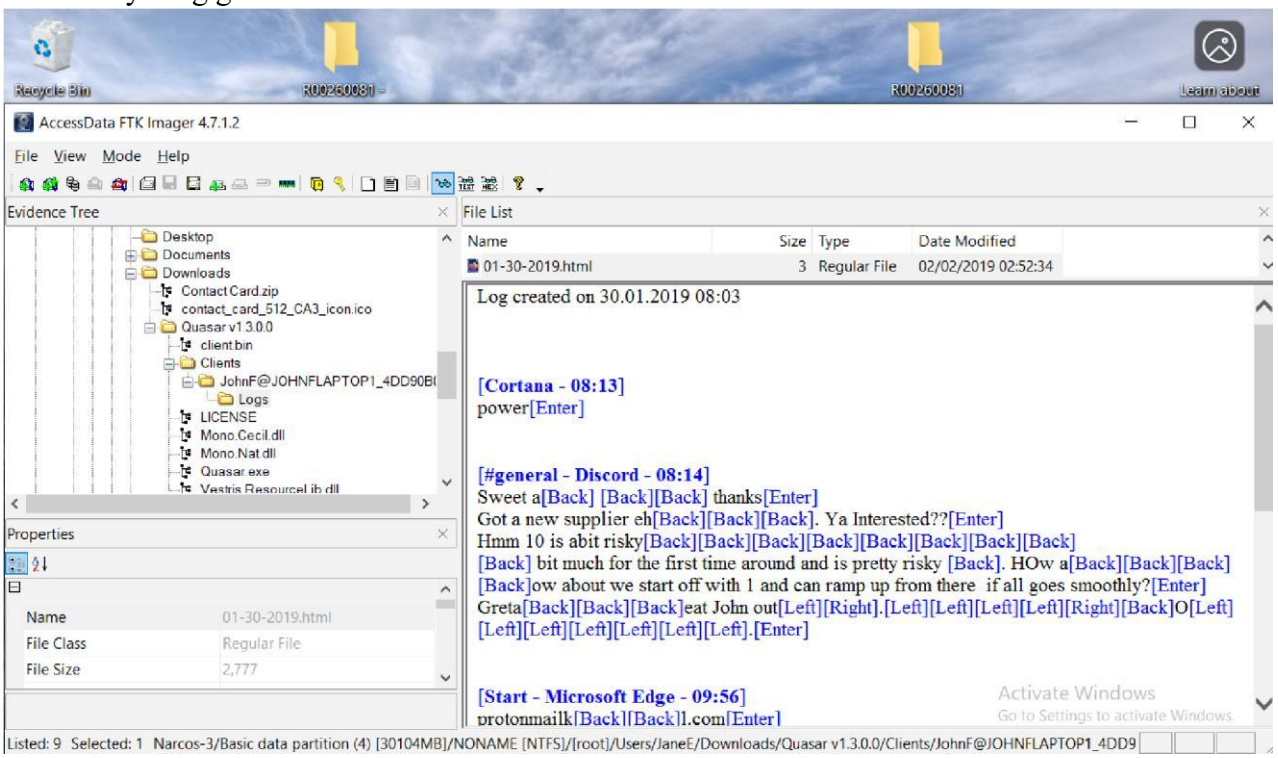


Fig 2.19 Communications 1.

On the same day 30th January, 2019 after the conversation, John logged in his email account (heresjohnny1@protonmail.com, Password:John1234) at around 09:56 to download and access a secret file with the password "**ilovediving**" from the directory: **C:\Users\JohnF\Downloads\Attachments-Important, crucial to our method\secret** at exactly 10:04. This secret file is confirmed to have been sent to him by Steve Kowhai as the same secret document was found on Steve Kowhai drive.

An attempt was made to access John Fredrickson email account in order to analyse the content of the mailbox, however, access could not be granted due to credentials invalid.

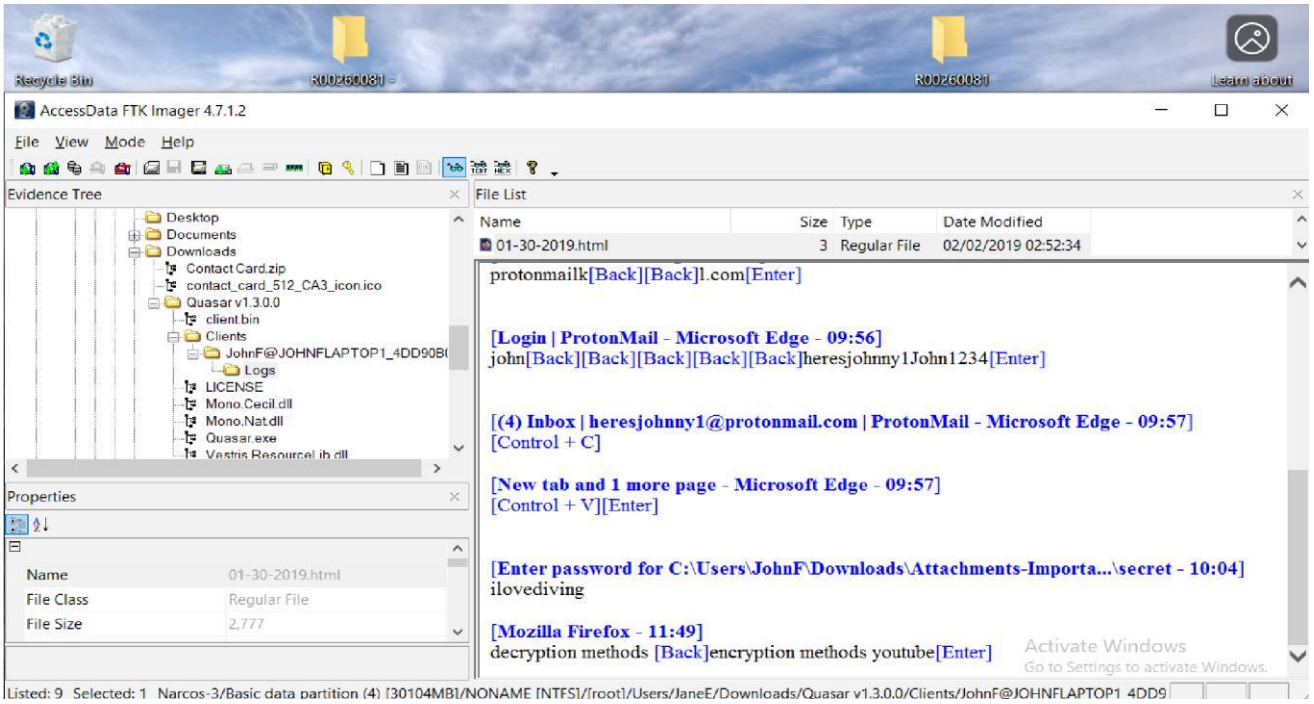


Fig 2.20 Communications 2.

On 31st January, 2019 at around 09:43, John was having a conversion with Jane on discord, the conversation involved making a request to Jane to accompany him as a cover up for smuggling of drugs to Steve Kowhai location in Wellington and promised to pay Jane for her part if she agrees with the deal. Jane was initially reluctant to agree with the offer, however, she had no choice than to accept. The plan is to act like couples travelling to New Zealand for holiday and told her not to reveal to anyone what they are actually there to do.

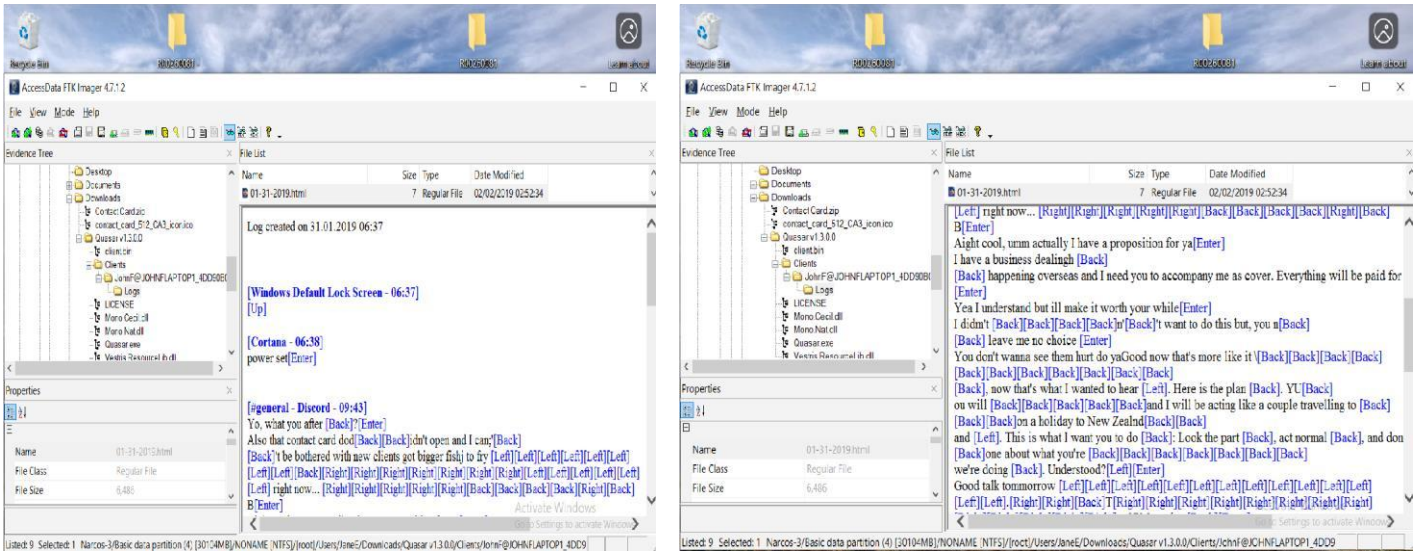


Fig 2.21 Communications 3.

On 1th February, 2019 at around 07:02, John was having a conversation with Steve Kowhai through discord, trying to send an image to Steve and looking for a way to hide the real content inside the image. He later resulted in using Steganography, he downloaded an image of brisbane tower and encrypted it with a password (**Elchapo2**) hiding a content in it, then saved as "**BNE.png**".

At around 10:05, John logged in his email account and sent the encrypted image to Steve Kowhai email address (**crayfish1980@protstego**).

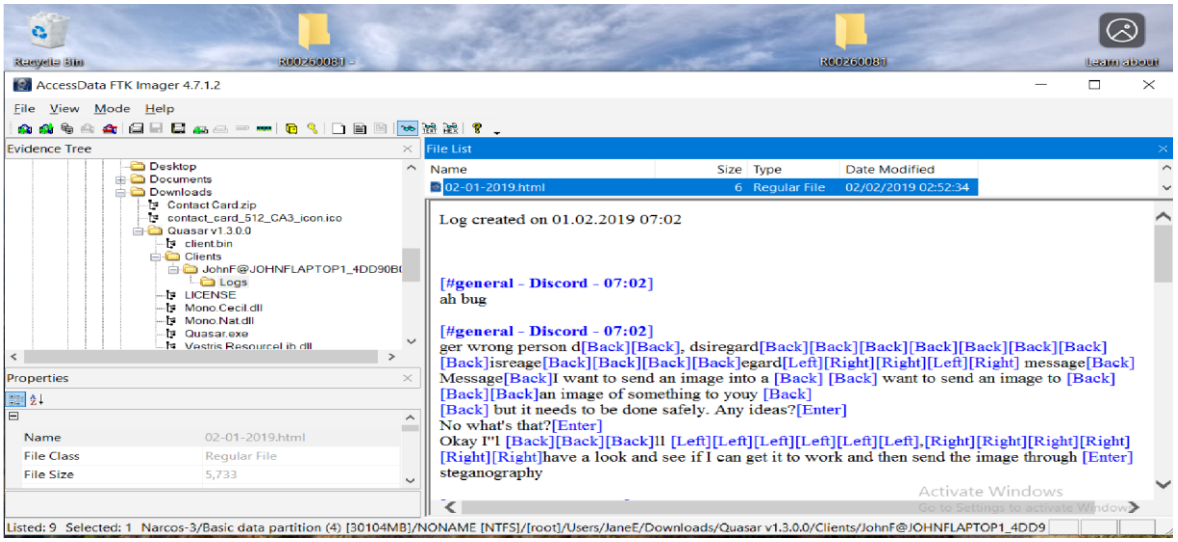


Fig 2.22 Communications 4.

On the same day 1st January, 2019 at around 09:59, John is confirming to Steve Kowhai on discord the method he used to hide the content and with the password. He sent the image to Steve's email address and included the password for decryption at around 10:05.

At around 11:58 on discord, John Fredrickson was requesting Jane Esteban's full name and date of birth to book a flight for both ahead of their mission.

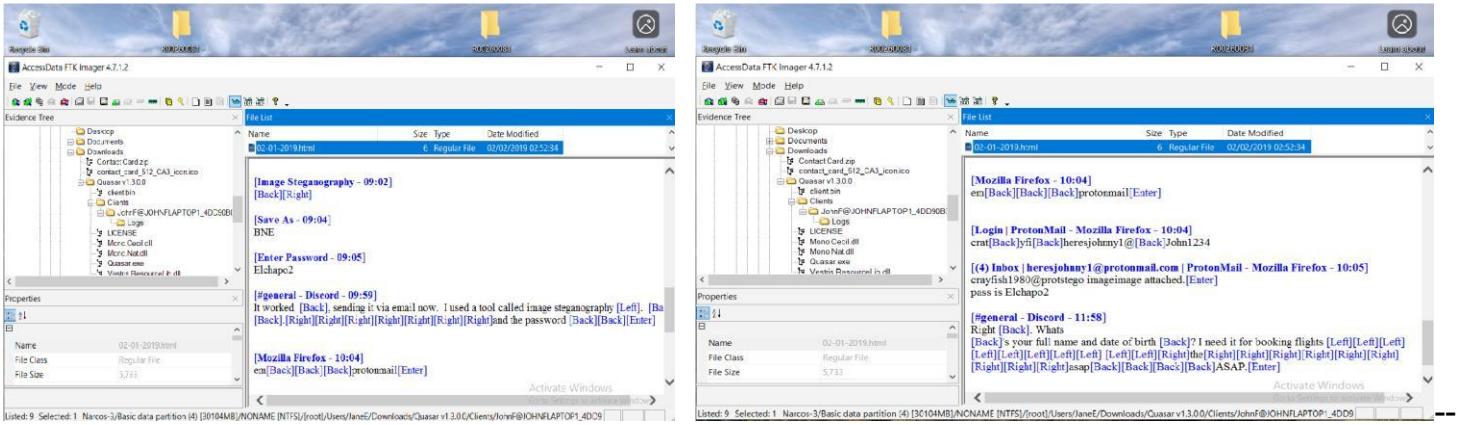


Fig 2.23 Communications 5.

On 2nd February, 2019 at around 08:29 to 08:42, John Fredricksion was booking a flight from Brisbane airport, Australia to Wellington, New Zealand, he booked the flight and saved the image as **Steve K**. He then confirmed to Jane Esteban on discord at around 09:00 about the flight and to pick her up at the address in "**Woolworth 133 Oxley Station Rd, Oxley QLD 4075 Australia**".

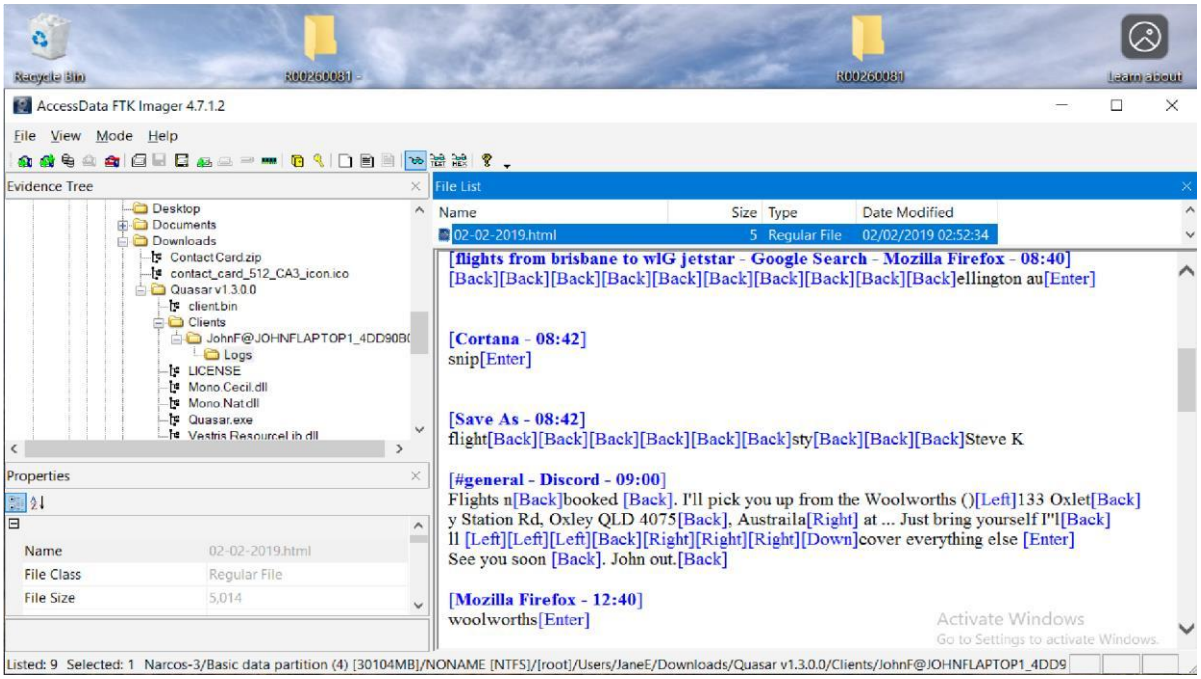


Fig 2.24 Communications 6.

It was also revealed on the same day 2nd February, 2019 at around 12:48, John used a TrueCrypt encryption/decryption software to decrypt and access the secret file from the directory:"**C:\Users\JohnF\Downloads\Attachments-Important, crucial to our method\secret"** with the password "**ilovediving**"**.** The file which was sent to him by Steve Kowhai.

Chapter Three

Fact and Clarification From The Forensic Investigation

1. The Encrypted Secret:

Upon identifying the encryption method used to encrypt the secret file with the password being revealed through their communication channel (discord). The secret file was recovered from John Fredrickson's drive and mounted into TrueCrypt to decrypt and read the content of the file. The file was decrypted with the password (**ilovediving**), and outputted to a word document file "**Memo Things.ods**".

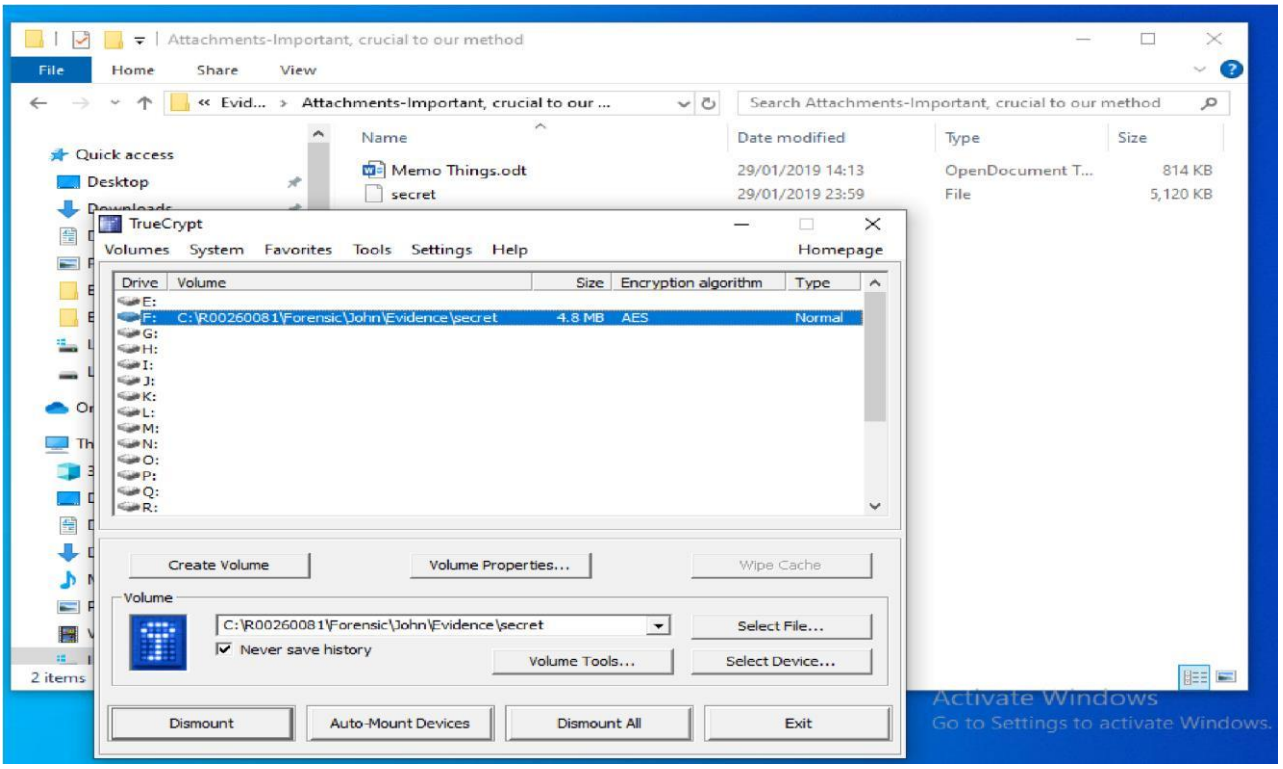
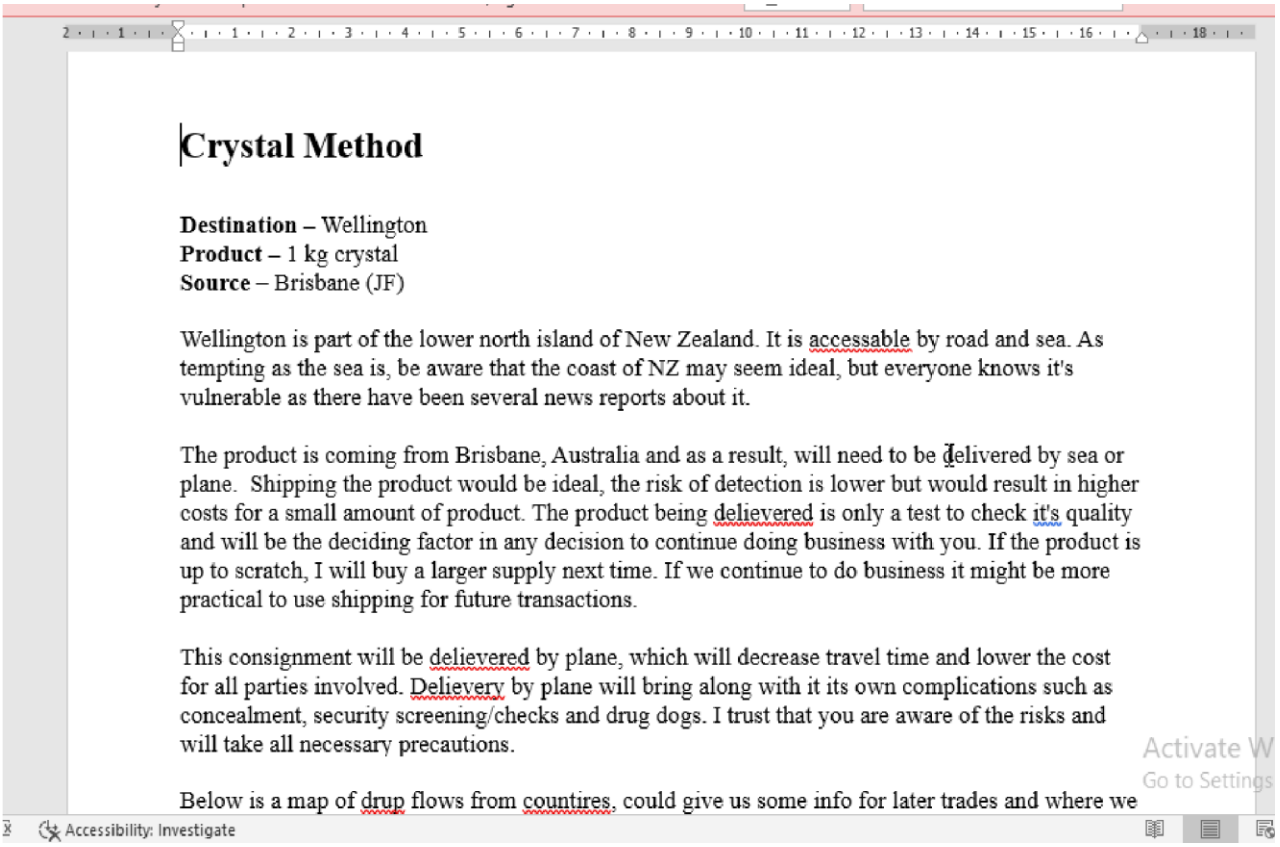


Fig 3.1 Using TrueCrypt to decrypt the secret file

The content of the decrypted file contains the plans from Steve Kowhai to guide John Fredrickson the travel itineraries related to the drug trafficking and smuggling within New Zealand and overseas. It contains their upcoming plans and future intentions mainly on smuggling the products safely.

It contains the name of the product (**Crystal**) which Steve Kowhai ordered from John Fredricksion, the amount to be initially delivered (1kg), the destination location to deliver to (Wellington), and the dealer (John Fredrickson) location which is in Brisbane.



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

Accessibility: Investigate

Fig 3.2 Their secret document (Memo Things.ods)

2. The Steganography Hidden Content:

Upon being discovered, John Fredrickson used an image Steganography software to hide a content inside the **BNG.png** image with the encryption password also being revealed through the communication channel (discord) and sent the image to Steve Kowhai email address. This image (BNG.png) was recovered from John's drive and was loaded into the Steganography software for decryption using the password found (**Elchapo2).** The result outputs an image (**package.jpg**) which shows the picture of the real product to be delivered to Steve Kowhai and how it is being hidden inside a suitcase.

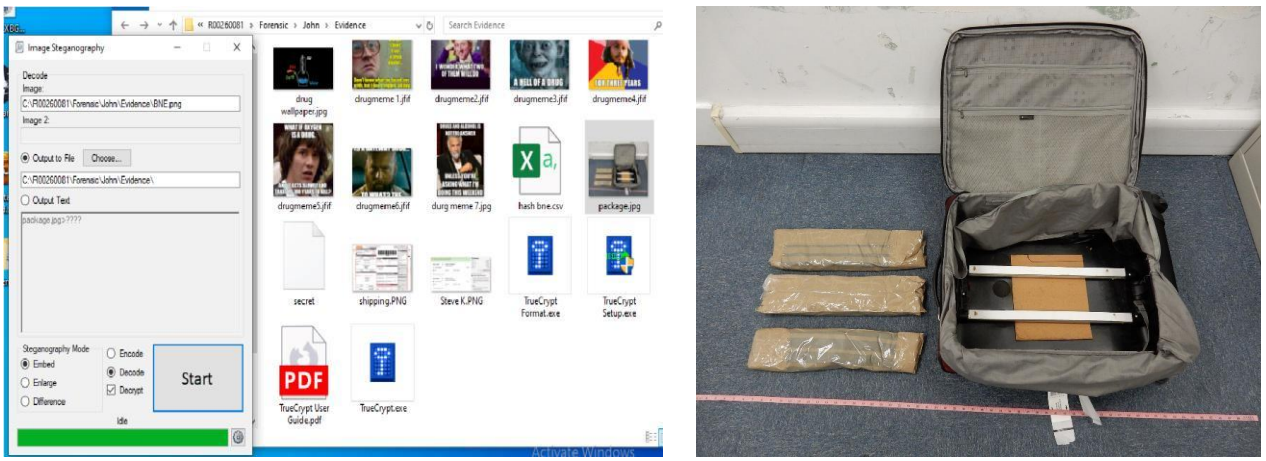
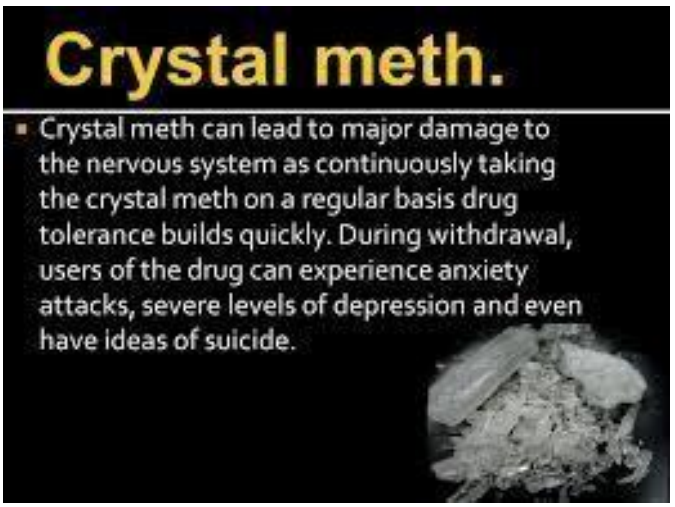


Fig 3.3 Steganography to uncover the hidden package. The (package.jpg)

From the secret file recovered and revealed, it was indicated that Steve Kowhai and

John Fredrickson were both in a transaction of the hard-drug product called **Crystal.** The Images that were recovered from Jane Esteban's drive which explains what this product looks like, how it is being inhaled and injected, and the damages it causes to the body nervous system.



3. **The Recovered Evidence:**

From the evidence assessment and with all evidence recovered, it proved that Steve Kowhai and John Fredrickson are both heavily involved in drug trafficking, while Steve Kowhai is a client who purchases hard-drugs across different dealers.

In relation to the ongoing investigation, evidence recovered from the Steve Kowhai drive which clearly indicates the suspect's involvement in drug trafficking and his relationship with the intercepted suspects (John Fredrickson and Jane Esteban). The evidence includes:

- The **BNG.png** image that was encrypted by John Fredrickson which was later recovered and decrypted to an image "**package.jpg"** that contains a hard-drug product expected to be delivered to Steve Kowhai location.
- A flight booking ticket of John Fredrickson and Jane Esteban from Brisbane Australia to Wellington New Zealand.
- A file named **secret** which was found to have contained plans of travel itineraries related to drug smuggling within New Zealand and overseas, and with their future intentions. It included the name of the drug product (**Crystal**) to be delivered to his location in Wellington by John Fredrickson, the amount (1 kg), and the location of the supplier (**Brisbane JF**) which is John Fredrickson.
- Various images of a map expected to direct a drug dealer enroute from the Wellington airport down to his home location in **Eastbourne.**
- Images of hard-drugs with dollar cash
- Some software applications are being used for encryption and hiding of illicit content to preserve anonymity of their activities. He used Steganography to the real product sent to him by John Fredricksion and also used TrueCrypt to encrypt a file that contained their secret and sent the file to John Fredrickson.

Steve Kowhai Operating System Information

Variable	Value
Kernel Base	0xf804432a9000
DTB	0x1ad000
Is64Bit	True
IsPAE	False
layer_name	0 WindowsIntel32e
memory_layer	1 FileLayer
KdVersionBlock	0xf804436afdc0
Major/Minor	15.17763
MachineType	34404
KeNumberProcessors	4
SystemTime	2019-02-02 02:33:34+00:00
NtSystemRoot	C:\Windows

NtProductType	NtProductWinNt
NtMajorVersion	10
NtMinorVersion	0
PE MajorOperatingSystemVersion	10
PE MinorOperatingSystemVersion	0
PE Machine	34404
PE TimeDateStamp	Sun Apr 10 16:09:02 2044

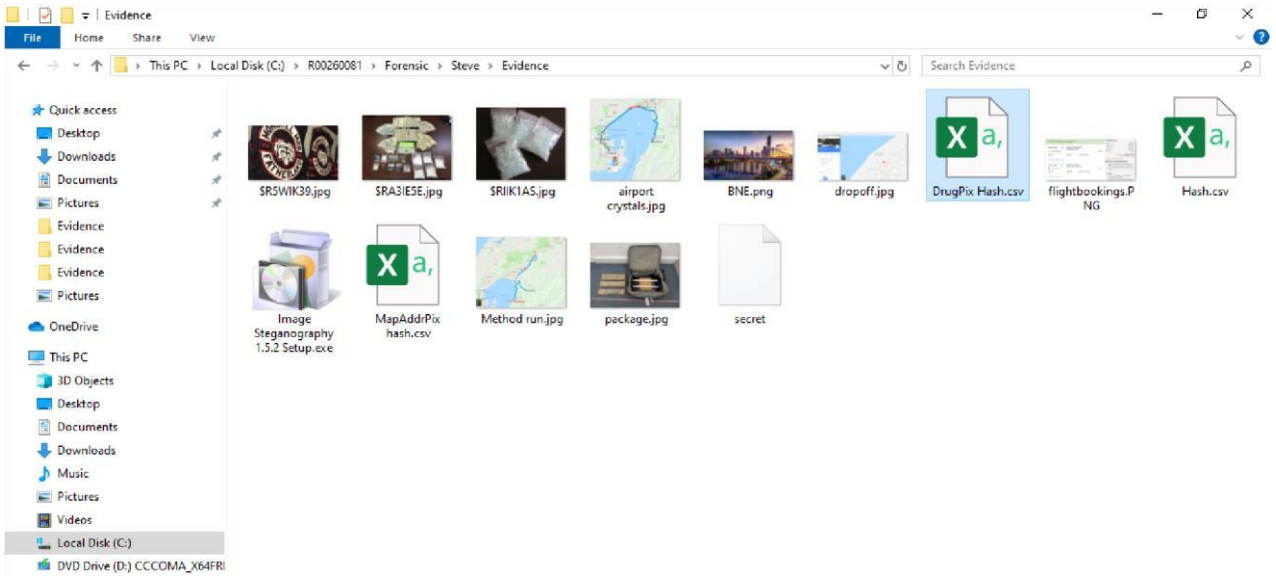


Fig 3.4 Evidence Recovered from Steve Kowhai's drive

Artefacts	Location	MD5-Hash	Timestamp

BNE.png	**C:\Users\Steve\Downloads\Misc\ BNE.png**	dffa98bdd7371d1806ad b09db27ba283	01/02/2019 00:13:25
package.jpg	**C:\Users\Steve\Downloads\Misc\ package.jpg**	8ba9265a1563ff871a47 1c552bab0b67	01/02/2019 00:13:25
secret	**C:\Users\Steve\Documents\secre t**	6c1b3daeda50ba945a7 6e1bf95ae9012	
dropoff.jpg	**C:\Users\Steve\Documents\Misc\ dropoff.jpg**	7feb763bebe42c3a3464 c9ee3bb1d3e8	02/02/2019 01:06:06
airport Crystals.jpg	**C:\Users\Steve\Documents\Misc\ airport Crystal.jpg**	f938f92d9dbaeda2e922 46deeebe830a	30/01/2019 21:25:18
Method run.jpg	**C:\Users\Steve\Documents\Misc\ Method run.jpg**	69b225bc0ef5a0c003f1e 2a6646aaf92	30/01/2019 21:22:24
flightbookings.PNG	**C:\Users\Steve\Documents\Misc\ flightbooking.PNG**	d1b21a1cddcb3494d637 f2424cc5f0f1	02/02/2019 02:28:45
$RA3IE5E.jpg	**C:\Recycle.Bin\S-1-5-21-1474204 758-2504895174-1356074821-100 1\RA3IE5E.jpg**	480da4ff5734c6d20787a f08fc9da46e	31/01/2019 02:58:22
$RIIK1AS.jpg	**C:\Recycle.Bin\S-1-5-21-1474204 758-2504895174-1356074821-100 1\$RIIK1AS.jpg**	60398a8ec59753ce5aad b99a566844d7	31/01/2019 02:56:06

John Fredrickson from Australia who is a drug dealer that supplies illicit drugs to Steve Kowhai and other various buyers. John Fredrickson concluded a deal with Steve Kowhai and was currently on the mission to deliver a product to Steve Kowhai before he was intercepted alongside his accomplice Jane Esteban by the law enforcement.

John Fredrickson traded in multiple products of hard-drug as found in his drive, he also recently shipped one of his products by DHL to a client (Jake Heke) in Auckland, New Zealand. Some of the evidence recovered from John Fredrickson's drive includes:

- A folder named "**Attachments-Important, crucial to our method"** which contains the secret file that was sent to him by Steve Kowhai.
- An excel document which contains the list of up to 13 clients that he regularly supplies the hard-drugs, including Steve Kowhai expected to receive a drug product Crank amounted up to 15kg to be delivered monthly, and Jane Esteban expected to receive a drug product Uppers amounted to 1 gram and to be delivered base on demand.
- A contact card (**Contact Card.exe**) used as a business card by John Fredrickson and Jane Esteban.
- An image (**BNE.png**) that contains hidden content. From the investigation it was discovered that John Fredrickson downloaded the original image **1540752698brisbane.jpg** and used a Steganography software to hide and encrypt the picture (**package.jpg)** of the product **Crystal** to be delivered to Steve Kowhai, he saved the encrypted image as BNE.png and then sent it to Steve Kowhai email address.
- A DHL shipping image **shipping.PNG** that John Fredrickson used to ship his drug product to one of his clients (Jake Heke) in Auckland, New Zealand dated on 29/01/2019 and signed by Johnny Fredrickson. Jake Heke's name is included in the document that contains the list of John Fredrickson clients found on John's drive "C:**Users\JohnF\Documents\Business\clients.ods"**. From the list, Jake Heke is expected to receive hard-drug product **Tweak**, amounting to **10 kg monthly** from John Fredrickson.
- A flight booking ticket saved as **Steve K.PNG.** The ticket was used to book a flight that transports John Fredrickson and Jane Esteban from Brisbane airport, Australia to Wellington New Zealand on their mission to deliver a drug product **Crystal** to Steve Kowhai home address.
- An **Image Steganography 1.5.2 Setup.exe** and **TrueCrypt.exe** that was used to carry out the encryption and hidden method of their transaction plans.
- A picture of Jane Esteban kids was also found on John Fredrickson drive **C:\Users\JohnF\AppData\Local\Temp\vmware-johnF\VMwareDnD\a7dfe1 09\Janes Kids.jpg**

John Fredrickson's Operating System Information

Variable	Value
Kernel Base	0xf800fd692000
DTB	0x1ad000
Is64Bit	True

IsPAE	False
layer_name	0 WindowsIntel32e
memory_layer	1 FileLayer
KdVersionBlock	0xf800fda2cd60
Major/Minor	15.17134
MachineType	34404
KeNumberProcessors	4
SystemTime	2019-02-02 02:54:03+00:00
NtSystemRoot	C:\Windows
NtProductType	NtProductWinNt
NtMajorVersion	10
NtMinorVersion	0
PE MajorOperatingSystemVersion	10
PE MinorOperatingSystemVersion	0

PE Machine	34404
PE TimeDateStamp	Tue Jan 1 06:44:13 2019

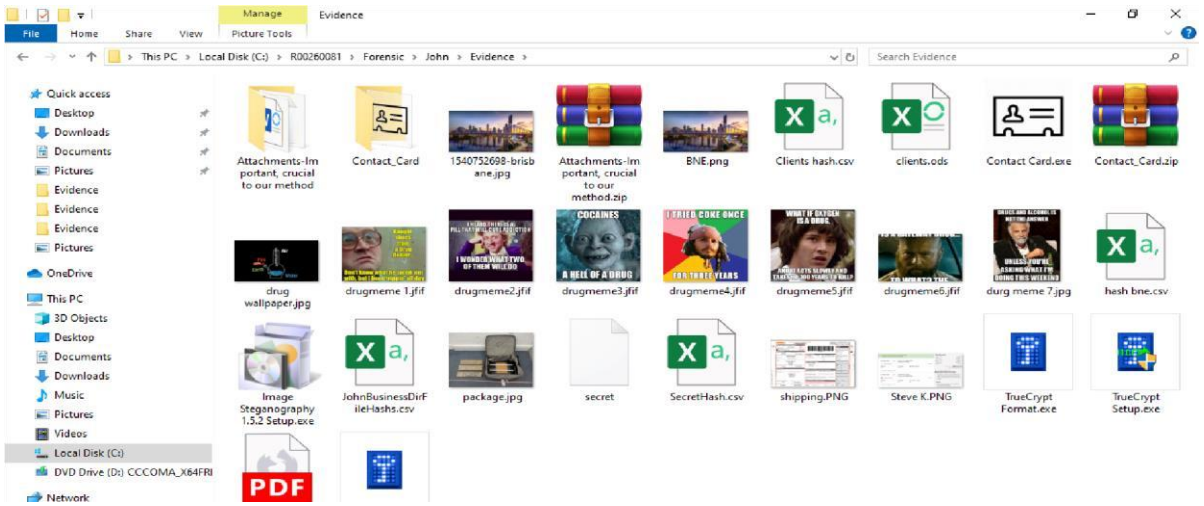


Fig 3. 4 Evidence Recovered from John Fredrickson's drive

Artefacts	**Location**	**MD5-Hash**	**Timestamp**
1540752698-brisbane.jpg	**C:\Users\JohnF\Pictures\1540752698-brisbane.jpg**	e261bd112aff55ce35ef043c282a650f	31/01/2019 21:30:17
BNE.png	**C:\Users\JohnF\Pictures\BNE.png**	dffa98bdd7371d1806adb09db27ba283	31/01/2019 23:05:17
package.jpg	**C:\Users\JohnF\Pictures\package.jpg**	8ba9265a1563ff871a471c552bab0b67	31/01/2019 23:05:17
secret	**C:\Users\JohnF\Downloads\Attachments-Important, crucial to our method\secret**	6c1b3daeda50ba945a76e1bf95ae9012	30/01/2019 00:00:49

Memo Things.odt	**C:\Users\JohnF\Downloads\Attachments-Important, crucial to our method\Memo Things.odt**	18302ce1440a264fdd66ba51e1dc9ac2	30/01/2019 00:00:49
Steve K.PNG	**C:\Users\JohnF\Documents\Business\Steve K.PNG**	d1b21a1cddcb3494d637f2424cc5f0f1	01/02/2019 01:18:28
shipping.PNG	**C:\Users\JohnF\Documents\Business\shipping.PNG**	4fdf3dd6bac6ba99f6eafcedd9a64efa	23/01/2019 01:18:28
clients.ods	**C:\Users\JohnF\Documents\Business\clients.ods**	db804b47095901e20d6666b1e9a56003	29/01/2019 04:02:47
Contact Card.zip	**C:\Users\JohnF\Downloads\Contact Card.zip**	409b88b2b275353f2ca05983cef1abf5	29:01:2019 22:01:31
drugmeme 1.jfif	**C:\Users\JohnF\Documents\Memes\drugmeme 1.jfif**	e31c66987f4edcae0bdc3e8b18aaa6ed	28/01/2019 20:11:43
Janes Kids.jpg	**C:\Users\JohnF\AppData\Local\Temp\vmware-johnF\VMwareDnD\a7dfe109\Janes Kids.jpg**	15d63e81576565e09efe2aa43eab9084	31/01/2019 02:29:42

Jane Esteban, who appears to be an undercover Australian police officer from the evidence found in her drive, however, the evidence also proved that Jane Esteban got addicted to drugs and finds it hard to quit doing hard-drugs. Jane Esteban is an accomplice of John Fredricksion, she regularly demands hard-drug product "**Uppers"** amounting to 1 gram from John Fredrickson who is a supplier.

Series of hard-drug images were found on Jane Esteban's drive describing various kinds of drugs, their impacts on the body system, and possible ways to quit doing drugs. Jane Esteban agreed a deal with John Fredrickson to both act like a couples going on a holiday in New Zealand with John with the main intention of delivering a hard-drug product to Steve Kowhai and it was agreed between John Fredrickson and Jane Esteban to smuggled the drug product through Jane Esteban's suitcase.

Jane Esteban had recorded all the browser activities and keystroke of John Fredrickson computer which revealed the conversion between Jane and John, and also the transaction

conversation between John F and Steve Kowhai. Some of the evidence recovered from Jane Esteban's drive includes:

- The contact card **Contact Card.zip** that is being used as a business card by John Fredrickson and Jane Esteban.
- A folder named **Clients "C:\Users\JaneE\Downloads\Quasar v1.3.0.0\Clients\JohnF@JOHNFLAPTOP1_4DD90B0\Logs"** that contains the logs of the conversations between Jane Esteban and John Fredrickson, and also between John Fredrickson and Steve Kowhai.
- A remote connection software **Quasar.exe** that was used by Jane Esteban to connect with John Fredrickson computer remotely to capture John's keystrokes and saved all the record on her (Jane Esteban) drive.
- Hard-drug images related to **Crystal** (the product meant to be delivered to Steve Kowhai) describing various kinds of drugs, their impacts on the body system, and possible ways to quit doing drugs.

Jane Esteban's Operating System Information

Variable	**Value**
Kernel Base	0xe12e7c09d000
DTB	0x1ab000
Is64Bit	True
IsPAE	False
layer_name	0 WindowsIntel32e
memory_layer	1 FileLayer
KdVersionBlock	0xe12e7c3eb5a0
Major/Minor	15.16299
MachineType	34404
KeNumberProcessors	4
SystemTime	2019-02-02 02:53:45+00:00
NtSystemRoot	C:\Windows

NtProductType NtProductType	NtProductWinNt NtProductWinNt
NtMajorVersion NtMajorVersion	10 10
NtMinorVersion NtMinorVersion	0 0
PE MajorOperatingSystemVersion PE MajorOperatingSystemVersion	10 10
PE MinorOperatingSystemVersion PE MinorOperatingSystemVersion	0 0
PE Machine PE Machine	34404 34404
PE TimeDateStamp PE TimeDateStamp	Fri Sep 29 01:53:04 2017 Fri Sep 29 01:53:04 2017

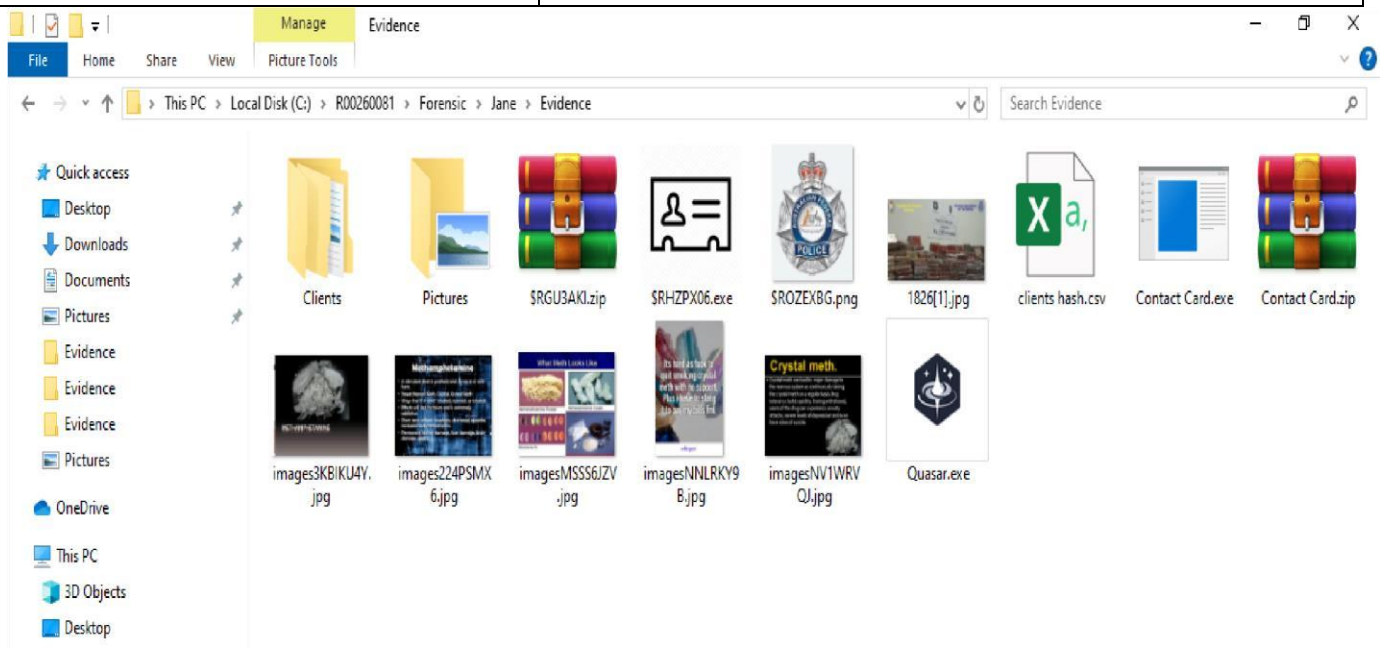


Fig 3.5 Evidence Recovered from Jane Esteban's drive

Artefacts	**Location**	**MD5-Hash**	**Timestamp**
Contact Card.zip	**C:\Users\JaneE\Downloads\ Contact Card.zip**	409b88b2b275353f2ca0598 3cef1abf5	29/01/2019 03:32:31

Quasar v1.3.0.0.exe	**C:\Users\JaneE\Downloads\Quasar v1.3.0.0\Clients\Quasar.exe**	5d56758eb0cf106dba55475e9bf9b479	29/01/2019 22:01:31
01-30-2019.html	**C:\Users\JaneE\Downloads\Quasar v1.3.0.0\Clients\JohnF@JOHNFLAPTOP1_4DD90B0\Logs\01-30-2019.html**	fd3a044bee4d5af72faba9630867d4fd	02/02/2019 02:52:34
01-31-2019.html	**C:\Users\JaneE\Downloads\Quasar v1.3.0.0\Clients\JohnF@JOHNFLAPTOP1_4DD90B0\Logs\01-31-2019.html**	948b4c559b944d6c0f2e1da8e285d835	02/02/2019 02:52:34
02-01-2019.html	**C:\Users\JaneE\Downloads\Quasar v1.3.0.0\Clients\JohnF@JOHNFLAPTOP1_4DD90B0\Logs\02-01-2019.html**	f51aa5754e54915e93d329a3eefdc042	02/02/2019 02:52:34
02-02-2019.html	**C:\Users\JaneE\Downloads\Quasar v1.3.0.0\Clients\JohnF@JOHNFLAPTOP1_4DD90B0\Logs\02-02-2019.html**	7edea768c94997ed685bf7bc51cc325a	02/02/2019 02:52:34

Combined Artefacts:

Artefact	Locations	MD5-Hash	Timestamp
BNE.png	**C:\Users\JohnF\Pictures\BNE.pn g**	dffa98bdd7371d1806adb09db27ba283	31/01/2019 23:05:17
	C:\Users\Steve\Downloads\Misc\BNE.png		01/02/2019 00:13:25

1540752698-brisbane.jpg	**C:\Users\JohnF\Pictures\1540752698-brisbane.jpg**	e261bd112aff55ce35ef043c282a650f	31/01/2019 21:30:17
package.jpg	**C:\Users\JohnF\Pictures\package.jpg**	8ba9265a1563ff871a471c552bab0b67	31/01/2019 23:05:17
shipping.PNG	**C:\Users\JohnF\Documents\Business**	4fdf3dd6bac6ba99f6eafcedd9a64efa	23/01/2019 01:18:28
dropoff.jpg	**C:\Users\Steve\Documents\Misc\dropoff.jpg**	7feb763bebe42c3a3464c9ee3bb1d3e8	02/02/2019 01:06:06
airport Crystals.jpg	**C:\Users\Steve\Documents\Misc\airport Crystal.jpg**	f938f92d9dbaeda2e92246deeebe830a	30/01/2019 21:25:18
Method run.jpg	**C:\Users\Steve\Documents\Misc\Method run.jpg**	69b225bc0ef5a0c003f1e2a6646aaf92	30/01/2019 21:22:24

flightbookings.PNG	**C:\Users\Steve\Documents\Misc\flightbooking.PNG**	d1b21a1cddcb3494d637f2424cc5f0f1	02/02/2019 02:28:45

	C:\Users\JohnF\Documents\Business\Steve K.PNG		01/02/2019 01:18:28
$RA3IE5E.jpg	**C:\Recycle.Bin\S-1-5-21-1474204758-2504895174-1356074821-1001\RA3IE5E.jpg**	480da4ff5734c6d20787af08fc9da46e	31/01/2019 02:58:22
$RIIK1AS.jpg	**C:\Recycle.Bin\S-1-5-21-1474204758-2504895174-1356074821-1001\$RIIK1AS.jpg**	60398a8ec59753ce5aadb99a566844d7	31/01/2019 02:56:06

secret	**C:\Users\JohnF\Downloads\Attachments-Important, crucial to our method\secret**	6c1b3daeda50ba945a76e1bf95ae9012	30/01/2019 00:00:49
Memo Things.odt	**C:\Users\JohnF\Downloads\Attachments-Important, crucial to our method\Memo Things.odt**	18302ce1440a264fdd66ba51e1dc9ac2	30/01/2019 00:00:49
clients.ods	**C:\Users\JohnF\Documents\Business\clients.ods**	db804b47095901e20d6666b1e9a56003	29/01/2019 04:02:47
Contact Card.zip	**C:\Users\JohnF\Downloads\Contact Card.zip**	409b88b2b275353f2ca05983cef1abf5	29:01:2019 22:01:31
	C:\Users\JaneE\Downloads\Contact Card.zip		29/01/2019 03:32:31
drugmeme 1.jfif	**C:\Users\JohnF\Documents\Memes\drugmeme 1.jfif**	e31c66987f4edcae0bdc3e8b18aaa6ed	28/01/2019 20:11:43
Quasar.exe	**C:\Users\JaneE\Downloads\Quasar v1.3.0.0\Clients\Quasar.exe**	5d56758eb0cf106dba55475e9bf9b479	29/01/2019 22:01:31
01-30-2019.html	**C:\Users\JaneE\Downloads\Quasar v1.3.0.0\Clients\JohnF@JOHNFLAPTOP1_4DD90B0\Logs\01-30-2019.html**	fd3a044bee4d5af72faba9630867d4fd	02/02/2019 02:52:34
01-31-2019.html	**C:\Users\JaneE\Downloads\Quasar v1.3.0.0\Clients\JohnF@JOHNFLAPTOP1_4DD90B0\Logs\01-31-2019.html**	948b4c559b944d6c0f2e1da8e285d835	02/02/2019 02:52:34

02-01-2019.html	**C:\Users\JaneE\Downloads\Quas ar v1.3.0.0\Clients\JohnF@JOHNFL APTOP1_4DD90B0\Logs\02-01-2 019.html**	f51aa5754e54915e93d3 29a3eefdc042	02/02/2019 02:52:34
02-02-2019.html	**C:\Users\JaneE\Downloads\Quas ar v1.3.0.0\Clients\JohnF@JOHNFL APTOP1_4DD90B0\Logs\02-02-2 019.html**	7edea768c94997ed685b f7bc51cc325a	02/02/2019 02:52:34

Chapter Four

Relationship Between The Three Suspects (Steve Kowhai, John Fredrickson, and Jane Esteban)

John Fredrickson:

- The primary drug supplier.

- He coordinated transactions and shipments of illicit substances to Steve Kowhai.
- He used encryption and steganography tools to hide transaction details between him and Steve Kowhai.
- He dealt directly with Steve Kowhai who is one of his primary clients, and worked closely with Jane Esteban, who acted as his accomplice.
- John Fredrickson also has pictures of Jane Esteban's kids **Janes Kids.jpg** which also proved their cordial relationship.

Steve Kowhai:

- A drug buyer and recipient of illicit substances.
- He communicated with John Fredrickson to arrange transactions and sent John a secret file that contained travel routes and future intentions.
- He received concealed drug-related images (**BNE.png**) and flight plans via email and Discord from John Fredrickson. Jane Esteban:
- Played a dual role as an accomplice and a cover for John Fredrickson, she's one of John Fredrickson's clients.
- She pretended to be John's spouse during travel to facilitate the smuggling operation.
- She provided logistical support, including acting as a courier for concealed drugs.

The three suspects formed a network, John Fredrickson (supplier) coordinated deals, Jane Esteban (accomplice) provided cover for smuggling activities while Steve Kowhai is the buyer who funded and expected to receive the products.

Conclusion

The forensic investigation revealed a well organised transnational drug trafficking network involving three suspects: John Fredrickson, Steve Kowhai, and Jane Esteban. Based on the analysis of digital evidence from their devices, the following conclusions can be drawn:

1. John Fredrickson:

- **Role:**

  Central figure and supplier of illicit drugs.

- **Activities:**

  He coordinated drug shipments using encrypted files and steganography to conceal transaction details.

  He maintained a client list that included buyers such as Steve Kowhai and others.

  He also organised logistics, including flight and delivery plans.

- **Evidence:**

  Encrypted files detailing drug deals and future plans.
  Images with hidden content related to drug products. Client lists and delivery records.

2. Steve Kowhai:

- **Role:**

  Client and recipient of the drugs.

- **Activities:**

  He purchased drugs from John Fredrickson and received encrypted files and communications related to shipments.

  He had maps and flight plans indicating delivery routes to his location in Wellington, New Zealand.

- **Evidence:**

  Encrypted images containing drug delivery details.

  Maps and travel itineraries matching John Fredrickson's travel plans.

  Pictures of drugs and cash indicating involvement in illicit activities.

3. Jane Esteban:

- **Role:**

  Accomplice and logistical support.

- **Activities:**

  Acted as a cover by posing as John Fredrickson's spouse to facilitate drug smuggling.

  She used remote desktop tools to monitor John Fredrickson's activities. She provided support in concealed drug packages.

- **Evidence:**

  Communication logs with both John Fredrickson and Steve Kowhai. Remote connection software and browser logs capturing incriminating activities. Drug-related images and evidence of logistical planning.

Summary

The evidence establishes that John Fredrickson orchestrated the drug trafficking operation with Steve Kowhai as the buyer and Jane Esteban as an accomplice. The suspects used advanced encryption techniques, steganography, and sophisticated planning to facilitate the transport of illicit substances. Their collective activities were intercepted before the drugs could be delivered, and the findings will support their prosecution for drug trafficking and related crimes.

The recovered evidence, including encrypted files, steganography images, flight tickets, and conversation logs, provides irrefutable proof of their collective involvement in international drug trafficking operations.

References

1. U.S. Department of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement, Special Report, NCJ 199408, Washington, D.C., Apr. 2004. Accessed: Oct 30, 2024. [Online]. Available: http://www.ojp.usdoj.gov/nij