# **Evidence List**

# **Evidence:**

# **Prior Evidence:**

Evidence Discovered prior to the investigation:

- 1kg of Methamphetamine
  - Discovered: Lining of suitcase by Customs.
  - Description: This methamphetamine was discovered in the lining of the suitcase by customs prior to the investigation.
- Additional Drugs and Guns discovered during raid
  - Discovered: 666 Rewera Avenue, Petone.
  - Description: Discovered during the the raid of the residence of Steve Kowhai, along side his PC.

# **NARCOS-1** Evidence:

Evidence discovered during the investigation of NARCOS-1, **SK-DESKTOP** belonging to **Steve Kowhai** 

- Evidence of narcotics
  - Discovered: SK-DESKTOP, Recycle Bin
  - Description: These files depicting narcotics and drug busts were discovered in the recycle bin of SK-DESKTOP.





- Evidence of gang affiliation
  - Discovered: SK-DESKTOP, Recycle Bin
  - Description: This file depicting possible gang affiliation with known New Zealand gang, Mongrel Mob, was discovered in the Recycle Bin of SK-DESKTOP.



- Evidence of narcotics and drug paraphernalia
  - Discovered: SK-DESKTOP, Memory Dump
  - Description: These files depicting narcotics and drug paraphernalia were discovered inside the memory dump of SK-DESKTOP.









# • 1kg Methamphetamine

- Discovered: SK-DESKTOP, BNE.png
- Description: This evidence is hidden inside BNE.png, and must be extracted using Steganography. The password was discovered using an exploit to gain access to Steve Kowhais OneNote:

# Stego

Friday, 1 February 2019 1:24 PM

The location = C:\Users\Steve\Downloads\Misc \BNE Pass equals Elchapo2

Success



- 000007.log
  - Discovered: SK-DESKTOP, Discord Cache
  - Description: A log found on Steve's desktop that aligns with a log found in Jane's Remote Access tool, a conversation between John and Steve dated 01.02.2019 07:02AM
- To John Fredricksen

# **New Supplier Conversation**

 "New supplier eh? Definitely Interested! Can I get 10 keys of it delivered to Wellington."

## **Document Preparation**

 "Yeah yeah probably wiser, good one. In fact, I have already put a document together in anticipation of chatting with you. I'll send it through now. It contains some information regarding how I see this working out. Let me know what you think once you have read it."

# **Steganography Discussion**

- "Good Thinking, I already know how. Heard of steganography?"
- "A way of hiding one image within another. There's a simple application called 'Image Steganography'."

# **Tool Acknowledgment**

 "Ya.. I just told you about the tool :face\_palm: Received it. Will check to see if it works and confirm soon."

### **Meeting Arrangement**

 "Good. Meet at the Eastbourne library and if we miss each other come to 666 Rewera Avenue, Petone."

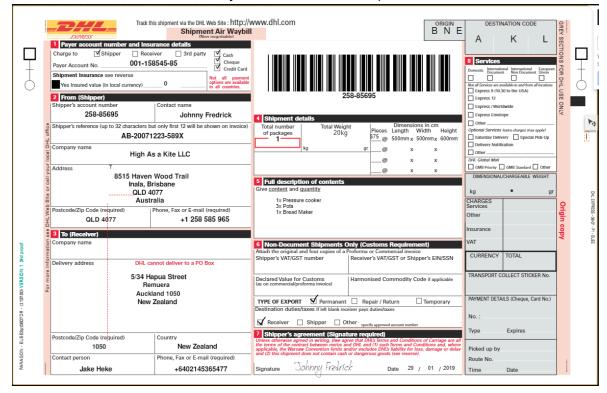
# **NARCOS-2 Evidence:**

Evidence discovered during the investigation of NARCOS-2, **JOHNFLAPTOP1** belonging to **John Fredricksen**.

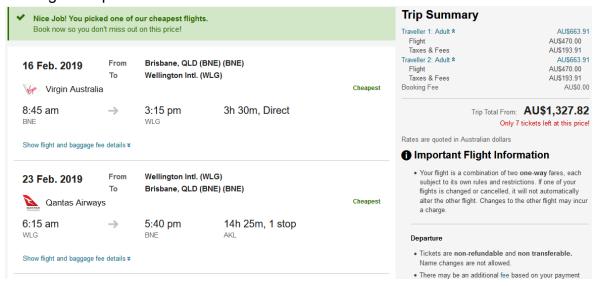
- Clients.ods
  - Discovered: JOHNFLAPTOP1, Business
  - Description: This file depicts past and future clients for narcotics delivery, including Persons of Interest, Jane Esteban, Steve Kowhai and Jake Heke.

Clients.ods
-------------

- Shipping.png
  - Discovered: JOHNFLAPTOP1, Business
  - Description: This file depicts a past shipment of narcotics to Person of Interest,
     Jake Heke, and can be used by the NZ Police to request a search warrant.



- Steve\_K.png
  - Discovered: JOHNFLAPTOP1, Business
  - Description: A screen shot of flight bookings for two adults from Brisbane Airport to Wellington Airport.



- Contact\_Card.zip
  - Discovered: JOHNFLAPTOP1, Downloads
  - Description: This package appears to be a ZIP Bomb. Once unpacked,
     Contact\_Card.zip works in the background to stealth install a Remote Access Tool named Quasar. This RAT is linked to JELAPTOP, and Jane Esteban uses it to gain evidence against John Fredricksen.
- Secret.file and Memo Things.odt

- Discovered: JOHNFLAPTOP1, Attachments
- Description: This file is an encrypted drive, once mounted using the program
   TrueCrypt and using the password to unlock it, a file named Memo\_Things.odt can
   be found. This file describes the methods taken to smuggle drugs across the world,
   and hints towards another supplier above John Fredricksen, who is mentioned in
   John's initial communication with Steve Kowhai.

Memo Things.odt

# Janes\_Kids.jpg

- Discovered: JOHNFLAPTOP1, VMWare
- Description: This file depicts Jane Estebans fake children, and is being used to blackmail Jane Esteban. Reverse image search reveals this image to be a stock image: <u>HD wallpaper: two children sitting beside eachother on bench, kids, gator</u> <u>fans | Wallpaper Flare</u>



### 000013.Log

- Discovered: JOHNFLAPTOP1, Discord Cache
- Description: A discord cache pulled from John Fredricksen's laptop. It shows correspondence between John and Jane which aligns with the RAT Logs, and also messages between John and Steve which align with the Discord Logs from Steve.

#### To Jane Esteban

#### Travel Plan

"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?"

#### Talk Confirmation

"Good. Talk tomorrow at 3PM or else."

### Information Request

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

# Flight Confirmation

 "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."

#### Farewell

"See you soon. John out."

### To Steve Kowhai

#### Correction

"Ah bugger, wrong person, disregard."

# Image Transfer

"I want to send an image of something to you, but it needs to be done safely. Any ideas?"

# Tool Inquiry

"No, what's that?"

# Follow-up on Image Transfer

 "Okay, I'll have a look and see if I can get it to work and then send the image through."

### Image Transfer Confirmation

 "It worked, sending it and the password via email now. I used a tool called image steganography."

# **NARCOS-3 Evidence:**

Evidence discovered during the investigation of NARCOS-2, **JELAPTOP** belonging to **Jane Esteban**.

## Evidence of narcotics

- Discovered: JELAPTOP, Memory Dump
- Description: These images were discovered in the memory dump of JELAPTOP, and depict various narcotics with watermarks from prominent drug enforcement agencies.













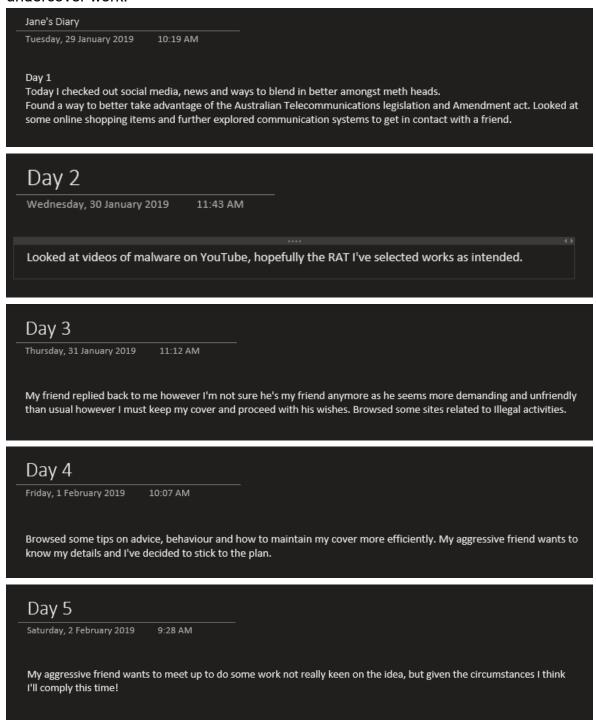




- Quasar v1.3.0.0, Contact\_Card.zip, Logs
  - Discovered: JELAPTOP, Downloads
  - Description: The Remote Access Tool and Zip Bomb Malware used to infect JFLAPTOP1, inside these folders we can see the logs obtained by the Remote Access Tool.
    - 01-30-2019 CLEANED.txt
    - 1 01-31-2019 CLEANED.txt

02-01-2019 CLEANED.txt
02-02-2019 CLEANED.txt

- OneNote Diary
  - Discovered: JELAPTOP, Microsoft.Office.OneNote 8wekyb3d8bbwe
  - Description: By performing an exploit against Microsoft OneNote for Windows 10, this diary was discovered on the laptop of Jane Esteban, depicting her plan for undercover work.



- Australian Federal Police paraphernalia
  - Discovered: JELAPTOP, Photos + Downloads
  - Description: Various evidence discovered that reinforces Jane Esteban being an undercover agent, including an under cover survival course guide pdf, and AFB

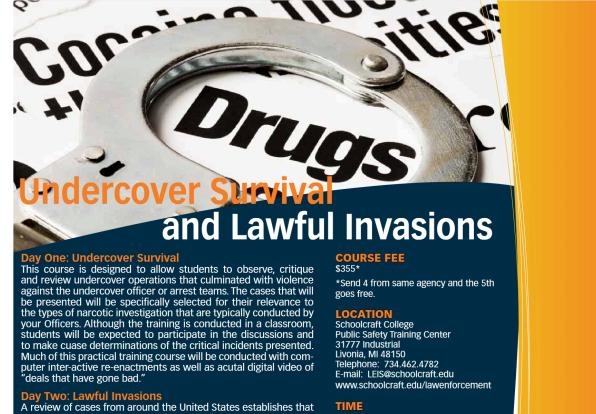
images.



456355880







many police agencies are moving away from the use of SWAT team tactics and "dynamic entries" for narcotic related search warrants. Courts have recently ruled that to utilize a specialized team, deploying "dynamic tactics," is in essence a use of force. As such, the decision itself may be unreasonable based upon the totality of the circumstances. Dynamic entry into homes to sim-

**TIME** 8:30 AM – 4:30 PM

COURSE OFFERING December 13-14, 2011

## 000003.Log

- Discovered: JELAPTOP, Discord Cache
- Description: Discord cache showing chat logs sent to John Fredricksen, these align with the chat logs found on Johns device and the RAT logs.
- To John Fredricksen
- Request
  - "Got any of that ice??"

# Additional Info

"Also I've got some friends that want to score too. Here's their contact card."

### Caution

"Umm I don't know, sounds pretty risky."

#### Refusal

"Err nah, I'm not keen."

# Pleading

"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??"

#### Confirmation

"Yes John, got it."

#### Identification

"My full name is Jane Esteban, and my birthday is 13/07/1992."

### Commitment

• "I'll be there."