

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.

Track this shipment via the DHL Web Site : <http://www.dhl.com>

Shipment Air Waybill
(Non negotiable)

ORIGIN **B N E** DESTINATION CODE **A K L**

1 Payer account number and insurance details
 Charge to ☒ Shipper ☐ Receiver ☐ 3rd party ☒ Cash ☒ Cheque ☒ Credit Card
 Payer Account No. **001-158545-85**
 Shipment Insurance see reverse
☒ Yes Insured value (in local currency) **0** Not all payment options are available in all countries.

2 From (Shipper)
 Shipper's account number **258-85695** Contact name **Johnny Fredrick**
 Shipper's reference (up to 32 characters but only first 12 will be shown on invoice) **AB-20071223-589X**
 Company name **High As a Kite LLC**
 Address **8515 Haven Wood Trail
Inala, Brisbane
QLD 4077
Australia**
 Postcode/Zip Code (required) **QLD 4077** Phone, Fax or E-mail (required) **+1 258 585 965**

3 To (Receiver)
 Company name
 Delivery address **DHL cannot deliver to a PO Box
5/34 Hapua Street
Remuera
Auckland 1050
New Zealand**
 Postcode/Zip Code (required) **1050** Country **New Zealand**
 Contact person **Jake Heke** Phone, Fax or E-mail (required) **+6402145365477**

4 Shipment details
 Total number of packages **1** Total Weight **20kg**
 Dimensions in cm
 Pieces **575** Length **500mm** Width **500mm** Height **600mm**
 kg gr

5 Full description of contents
 Give content and quantity
 1x Pressure cooker
 3x Pots
 1x Bread Maker

6 Non-Document Shipments Only (Customs Requirement)
 Attach the original and four copies of a Proforma or Commercial invoice
 Shipper's VAT/GST number Receiver's VAT/GST or Shipper's EIN/SSN
 Declared Value for Customs (as on commercial/proforma invoice) Harmonised Commodity Code if applicable
 TYPE OF EXPORT ☒ Permanent ☐ Repair / Return ☐ Temporary
 Destination duties/taxes if left blank receiver pays duties/taxes
☒ Receiver ☐ Shipper ☐ Other specify approved account number

7 Shipper's agreement (Signature required)
 Unless otherwise agreed in writing, I/we agree that DHL's Terms and Conditions of Carriage are all the terms of the contract between me/us and DHL, and (1) such Terms and Conditions and, where applicable, the Warsaw Convention limits and/or excludes DHL's liability for loss, damage or delay and (2) this shipment does not contain cash or dangerous goods (see reverse).
 Signature **Johnny Fredrick** Date **29 / 01 / 2019**

Services
☐ Domestic ☐ International Document ☐ International Non Document ☐ European Direct
☐ Express 12 ☐ Express / Worldwide ☐ Express Envelope
☐ Other
 Optional Services (extra charges may apply)
☐ Saturday Delivery ☐ Special Pick-Up
☐ Delivery Notification
☐ Other
☐ DHL Global Mail ☐ CMB Priority ☐ CMB Standard ☐ Other

DIMENSIONAL/CHARGEABLE WEIGHT
 kg * gr
 CHARGES
 Services
 Other
 Insurance
 VAT
 CURRENCY TOTAL
 TRANSPORT COLLECT STICKER No.
 PAYMENT DETAILS (Cheque, Card No.)
 No. :
 Type Expires
 Picked up by
 Route No.
 Time Date

PARAGON - EUEB30070R - (3/27/00) VERSION 1 3rd proof

- Steve_K.png

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

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

Date	From	To	Airline	Class	Time	Duration
16 Feb. 2019	Brisbane, QLD (BNE) (BNE)	Wellington Intl. (WLG)	Virgin Australia	Cheapest	8:45 am	3h 30m, Direct
23 Feb. 2019	Wellington Intl. (WLG)	Brisbane, QLD (BNE) (BNE)	Qantas Airways	Cheapest	6:15 am	14h 25m, 1 stop

Show flight and baggage fee details

Trip Summary

Traveller	Flight	Taxes & Fees	Booking Fee
Traveller 1: Adult *	AUS\$663.91	AUS\$470.00	AUS\$193.91
Traveller 2: Adult *	AUS\$663.91	AUS\$470.00	AUS\$193.91
Trip Total From:	AUS\$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

- 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: [HD wallpaper: two children sitting beside eachother on bench, kids, gator fans | Wallpaper Flare](#)



- 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

📄 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.

Jane's Diary

Tuesday, 29 January 2019 10:19 AM

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

Wednesday, 30 January 2019 11:43 AM

Looked at videos of malware on YouTube, hopefully the RAT I've selected works as intended.

Day 3

Thursday, 31 January 2019 11:12 AM

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

Friday, 1 February 2019 10:07 AM

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

Saturday, 2 February 2019 9:28 AM


My aggressive friend wants to meet up to do some work not really keen on the idea, but given the circumstances I think I'll comply this time!

- 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.





Undercover Survival and Lawful Invasions

Day One: Undercover Survival
 This course is designed to allow students to observe, critique and review undercover operations that culminated with violence against the undercover officer or arrest teams. The cases that will be presented will be specifically selected for their relevance to the types of narcotic investigation that are typically conducted by your Officers. Although the training is conducted in a classroom, students will be expected to participate in the discussions and to make cause determinations of the critical incidents presented. Much of this practical training course will be conducted with computer inter-active re-enactments as well as actual digital video of "deals that have gone bad."

Day Two: Lawful Invasions
 A review of cases from around the United States establishes that 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-

COURSE FEE
 \$355*
 *Send 4 from same agency and the 5th goes free.

LOCATION
 Schoolcraft College
 Public Safety Training Center
 31777 Industrial
 Livonia, MI 48150
 Telephone: 734.462.4782
 E-mail: LEIS@schoolcraft.edu
 www.schoolcraft.edu/lawenforcement

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."

