INFO702 Forensic Investigation Report

Forensic Investigation of NARCOS-2019 Case Study

Investigators

Lead Forensics Analyst

Raine Roberts (21528080)

Forensics Analyst

Logan Webster (20499621)

Overview

Background

Australian intelligence alerted Customs to potential illegal activities involving two passengers, Jane Esteban and John Fredricksen, upon their arrival in Wellington, New Zealand from Brisbane. Customs officers searched their baggage and found both of their laptops as well as discovering one kilogram of methamphetamine hidden in Jane's suitcase.

During separate interrogations, John refused to answer questions, while Jane indicated she was instructed to deliver the suitcase to "Eastbourne library" or, if necessary, to 666 Rewera Avenue, Petone, as directed by John. A subsequent raid on the Petone address revealed drugs, firearms, and a desktop computer, suggesting further criminal involvement.

Objective

As a team of Customs forensic investigators, Raine Roberts and Logan Webster will examine the images and memory dumps from both suspects' laptops and the desktop computer to uncover their motives, goals, and objectives.

Persons of Interest

Primary Actors

During this investigation, three primary actors were uncovered, John Fredricksen, Jane Esteban and Steve Kowhai.

John Fredricksen

- Our investigation reveals that John Fredricksen (A.K.A Johnny Fredrick), is a middle-man distributor of narcotics currently operating in the Oceanic region for an Unnamed Supplier. He operates primarily from his front company, ‘High As a Kite LLC’ located 8515 Haven Wood Trail, Inala Brisbane. From this location John distributes narcotics to clients by shipping them inside cookware through DHL.
- John Fredricksen has recently sold 1kg of product to Steve Kowhai but must deliver it last minute, via plane. He has blackmailed a new client, Jane Esteban, with the threat of harming her children and is using her as a cover to sneak this product through customs via her luggage case.

(Additional Biographical and Selector data discovered during the investigation can be found in appendix, ‘1 - John Fredricksen.pdf’).

Jane Esteban

- Our investigations reveal that Jane Esteban, is an undercover agent for the Australian Federal Police. Jane is currently investigating the narcotics distributor, John Fredricksen. As her persona, Jane portrays herself as a plain-clothes civilian meth addict with two children, who is looking for small purchases of methamphetamine.
- Her undercover persona is blackmailed into going with John Fredricksen to Wellington, New Zealand at the threat of harm to these children.

(Additional Biographical and Selector data discovered during the investigation can be found in appendix, '2 - Jane Esteban.pdf').

Steve Kowhai

- Our investigations reveal that Steve Kowhai (A.K.A Crayfish1980), is a client of John Fredricksen and assumed affiliate of the notorious New Zealand gang 'Mongrel Mob'. We believe that when Steve receives the product from John, he then distributes it locally to his street level gang members who sell it on his behalf. Steve operates from his residence, 666 Rewera Avenue, Petone.
- Steve Kowhai has recently purchased 1kg of product from John Fredricksen, and needs it delivered quickly to a meeting point at Eastbourne Library or his residence.

(Additional Biographical and Selector data discovered during the investigation can be found in appendix, '3 - Steve Kowhai.pdf').

Secondary Actors

There was also a secondary actor, Jake Heke, another New Zealand client of John Fredricksen, of which enough information has been discovered to issue a warrant against.

Jake Heke

- Jake Heke is an Auckland based client of John Fredricksen. Not much is known about Jake, but sufficient information has been discovered to warrant a raid on his address by the Auckland Police, through the clients.odt list and the shipping label from DHL.
- Jake Heke operates from his address 5/34 Hapua Street Remuera, Auckland 1050 New Zealand.

(Additional Biographical and Selector data discovered during the investigation can be found in appendix, '4 - Jake Heke.pdf').

Note: All persons of interest have been compiled into appropriate appendices, which will be included alongside this document. References: ‘1 - John Fredricksen.pdf’, ‘2 - Jane Esteban.pdf’, ‘3 - Steve Kowhai.pdf’, ‘4 - Jake Heke.pdf’.

Devices of Interest

All exploitable information discovered on each device during the investigation compiled into appendices, this information includes account information, OS information, Time Zone information, IP addresses, physical addresses and information on devices that have been connected to each device.

NARCOS-1/SK-DESKTOP

- SK-DESKTOP is the desktop device belonging to Steve Kowhai. A comprehensive documentation of information can be found in appendix ‘1 - SK-DESKTOP'.

NARCOS-2/JFLAPTOP1

- JFLAPTOP1 is the laptop device belonging to John Fredricksen. A comprehensive documentation of information can be found in appendix ‘2 - JFLAPTOP1'.

NARCOS-3/JELAPTOP

- JELAPTOP is the laptop device belonging to Jane Esteban. A comprehensive documentation of information can be found in appendix ‘3 - JELAPTOP'.

Domains of Interest

All relevant domains of interest discovered in web and search history on each device during the investigation compiled into appendices.

NARCOS-1/SK-DESKTOP

- Domains searched indicate the person of interest **Steve Kowhai** has been searching for information on drugs, drug paraphernalia, where and how to sell drugs and plotting a drug supply route through Wellington City.
- Additional Information of **Steve Kowhai's** drug route can be found in the ‘Locations of Interest.pdf’ appendix.

A comprehensive documentation of information can be found in appendix ‘1 - SK-DESKTOP Domain List.pdf'.

NARCOS-2/JFLAPTOP1

- Domains searched indicate the person of interest **John Fredriksen** has been searching ways to hide narcotics while travelling to New Zealand, including hidden inside the body, and inside suitcases.

A comprehensive documentation of information can be found in appendix ‘1 - JFLAPTOP1 Domain List.pdf'.

NARCOS-3/JELAPTOP

- Domains searched indicate the person of interest **Jane Esteban** has been searching for tips on how to be a better undercover cop, such as reading guides and purchasing tools and clothes. She is also seen accessing the Australian Federal Police Force website as a user and downloading the Quasar RAT that she packaged into a ZIP Bomb.

A comprehensive documentation of information can be found in appendix ‘3 - JELAPTOP Domain List.pdf'.

Locations of Interest

All locations of interest discovered during the investigation, alongside screenshots discovered on each device.

Location List

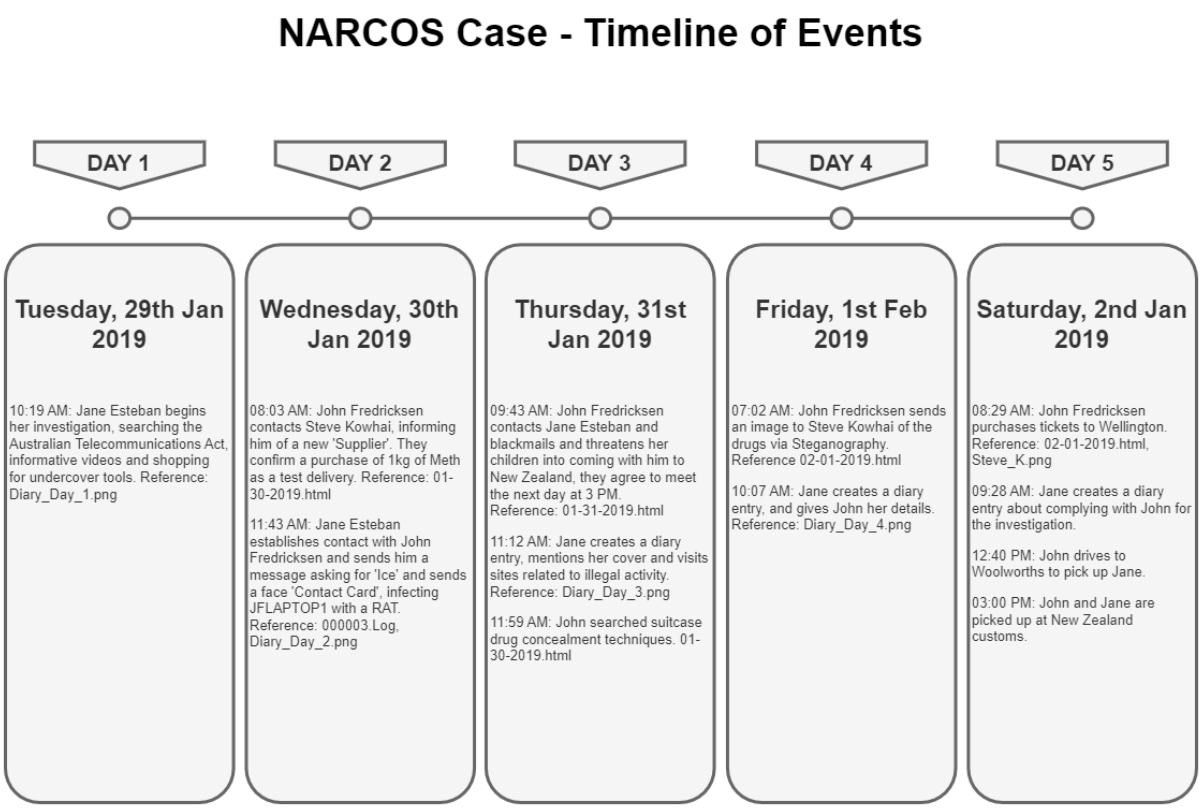
The below list is a comprehensive list of all locations discovered during the investigation, for more information please see appendix ‘Locations of Interest.pdf’ for images of each location, where they were found and a description of relevance to the case at large.

Location Number	Name of Location	Address	Country	ZIP Code
NAR-L-1	Eastbourne Library	38 Rimu Street, Eastbourne	New Zealand	Lower Hutt 5013
NAR-L-2	SK-House	666 Rewera Avenue, Petone	New Zealand	Lower Hutt 5012
NAR-L-3	High As a Kite LLC	8515 Haven Wood Trail, Inala Brisbane	Australia	Queensland 4077
NAR-L-4	Wellington International Airport	Stewart Duff Drive, Rongotai	New Zealand	Wellington 6022
NAR-L-5	Stokes Valley	Stokes Valley, Lower Hutt 5019	New Zealand	Stokes Valley, Lower Hutt 5019
NAR-L-6	Naenae	Naenae, Lower Hutt 5011	New Zealand	Naenae, Lower Hutt 5011
NAR-L-7	Wainuimata	Wainuiomata, Lower Hutt	New Zealand	Lower Hutt
NAR-L-8	JF-House	3 Pegasus St, Inala Brisbane	Australia	Inala, Queensland 4077, Australia
NAR-L-8	Woolworths	133 Oxley Station Rd	Australia	Oxley QLD 407, Australia
NAR-L-9	JH-House	5/34 Hapua Street Remuera	New Zealand	Auckland 1050 New Zealand

Evidence

All evidence has been compiled into appendix ‘Evidence List.pdf’, it contains all evidence discovered during the investigation including where and when it was found, and a description of the evidence.

Timeline



Prior Evidence

This list details evidence acquired prior to the investigation:

1. **1kg of Methamphetamine**
    a. **Discovered**: Lining of suitcase by Customs.
    b. **Description**: Methamphetamine found hidden in the suitcase lining during a Customs inspection prior to the main investigation.
2. **Additional Drugs and Firearms**
    a. **Discovered**: 666 Rewera Avenue, Petone.
    b. **Description**: Discovered during the raid on Steve Kowhai's residence, alongside a desktop computer with critical information.

Investigation Evidence

This section details all evidence collected from each suspect's devices during the investigation.

NARCOS-1 (SK-DESKTOP - Steve Kowhai)

1. **Evidence of Narcotics and Gang Affiliation**
    a. **Location**: SK-DESKTOP, Recycle Bin.
    b. **Description**: Files depicting narcotics, gang-related material, and affiliations with the Mongrel Mob gang.
2. **Steganographic File (BNE.png)**
    a. **Location**: SK-DESKTOP.
    b. **Description**: Image containing hidden evidence of narcotics, decrypted using steganography after extracting the password from a OneNote exploit.
3. **Discord Chat Logs (000007.log)**
    a. **Location**: Discord Cache.
    b. **Description**: Logs containing conversation between John Fredricksen and Steve Kowhai discussing new suppliers, shipment methods, and meeting arrangements.

NARCOS-2 (JOHNFLAPTOP1 - John Fredricksen)

1. **Clients List (clients.ods)**
    a. **Location**: Business folder.
    b. **Description**: List of narcotics clients, including Jane Esteban, Steve Kowhai, and Jake Heke, essential for confirming client distribution links.
2. **Flight Bookings (Steve_K.png)**
    a. **Location**: Business folder.
    b. **Description**: Screenshot of flight bookings for John and Jane, supporting the plan for Jane to transport methamphetamine.
3. **Encrypted Memo (Memo_Things.odt)**
    a. **Location**: Encrypted drive.
    b. **Description**: Document describing global drug smuggling tactics and indicating a supplier higher in the distribution network.
4. **Stock Image of Jane's "Children" (Janes_Kids.jpg)**
    a. **Location**: VMware folder.
    b. **Description**: Stock photo used to blackmail Jane. Reverse image search confirmed its use in Jane's undercover operation.

NARCOS-3 (JELAPTOP - Jane Esteban)

1. **Quasar RAT and Zip Bomb (Contact_Card.zip)**
    a. **Location**: Downloads.
    b. **Description**: Zip Bomb malware embedded with the Quasar RAT used to gain access to John's device, gathering critical evidence.
2. **Australian Federal Police Documentation**
    a. **Location**: Photos and Downloads.
    b. **Description**: Undercover survival guide and AFP paraphernalia, supporting Jane's role as an undercover agent.
3. **Diary Entries in OneNote**

    a. **Location**: OneNote Cache.
    b. **Description**: Diary logs detailing Jane's preparations and progress in her undercover operation.
4. **Discord Chat Logs (000003.log)**
    a. **Location**: Discord Cache.
    b. **Description**: Correspondence with John Fredricksen, revealing coerced participation and confirming undercover agent status.

Forensic Framework

The investigation into the NARCOS-2019 case followed the NIST (National Institute of Standards and Technology) Digital Forensics Framework, which provided a structured, four-phase approach: Collection, Examination, Analysis, and Reporting. (Salfati & Pease, June 2022)

Collection

Investigators preserved digital evidence from all devices associated with the suspects—SK-DESKTOP, JFLAPTOP1, and JELAPTOP—using write-blockers and documenting each device's chain of custody. Tools such as Autopsy and Volatility were employed to ensure integrity and capture critical data like memory dumps, deleted files, and chat logs.

Examination

In this phase, investigators extracted relevant data, such as encrypted files, hidden images, and cached logs, using techniques like steganography detection and cache exploitation. This process isolated evidence central to the case, including client lists and communications, without affecting non-relevant data.

Analysis

The analysis phase involved connecting suspects to criminal activities, revealing patterns in communications and searches, and mapping out narcotics distribution networks. The timeline of logs and interactions was thoroughly examined to construct a clear narrative of events and associations.

Reporting

Finally, a structured forensic report documented all findings and methods used, aligned with NIST standards to ensure clarity, precision, and legal readiness. This report provided a clear basis for judicial action under New Zealand law.

By applying the NIST Digital Forensics Framework, investigators maintained a rigorous, legally defensible approach, securing reliable evidence for prosecution in the NARCOS-2019 case.

Tools and Techniques

This section goes over tools and techniques used to collect evidence throughout the investigation.

Tools

Autopsy Version 4.21.0

- Autopsy is an open-source forensics tool kit the investigators used to investigate the NARCOS image files and extract evidence for the investigation.

Volatility Version 2.5

- Volatility is an open-source memory recovery tool. It was used in conjunction with Autopsy by the investigators to investigate the memory dump files to extract, read, and recover carved (previously deleted) files used for evidence in the investigation. (Volatility, 2024)

HxD Hex Editor Version 2.5.0.0

- HxD is an open-source Hex Editor program used by the investigators to investigate the Hex values of a file in conjunction with Autopsy. It was used to recover chat and keystroke logs during the investigation.

Obsidian Version 1.7.4

- Obsidian is an open-source knowledge base and note-taking tool used by investigators to compile data and evidence into case files. (Hoffman, Micah; Glynn, Griffin, 2024)

Techniques

Exploit for local cache on OneNote for Windows 10

- By following an exploit in OneNote discovered by Microsoft, the investigators were able to take the local package files from the various images OneNote caches and export them into a host device with OneNote for Windows 10, allowing access to private workbooks and more evidence. (Microsoft, 2019)

Strings Technique for Discord and Quasar Cache Logs

- By using the strings command on Discord local cache files and Quasar Profile Logs, the investigators were able to extract chat logs and keystroke logs from each device.

Unauthorized Account Access

- By extracting the email account username and password from the Quasar RAT logs, the investigators can access the email account of John Fredricksen.

OSINT Reverse Image Search

- By using the OSINT technique of Reverse Image search, the investigators were able to determine the validity of certain images discovered in the case, such as the image 'Janes_Kids.jpg'. Upon using this technique, the investigators determined that this image used to blackmail Jane was a stock photograph, and leant evidence to the fact that Jane Esteban is an undercover agent.
- https://www.wallpaperflare.com/two-children-sitting-beside-eachother-on-bench-kids-gator-fans-wallpaper-wgfni

Using AI to automatically clean dirty Discord and Quasar RAT Logs

- While collecting chat logs from Discord and Quasar, there was a multitude of dirty data in the form of additional characters or artifacts and repeating logs, by using artificial intelligence we can feed this dirty data and clean it automatically. In a true case, this would not be permissible by law as evidence due to the risk of 'AI Hallucinations', but it is an efficient way to perform this process automatically for key data while another agent performs true data cleansing manually.

Steganography via Image Steganography

- The people of interest used Steganography to hide evidence of packaged narcotics inside another image. By using steganography tools and techniques to identify the image and password that encrypted it, and then using the tool Image Steganography to decrypt the file and extract the hidden image.

Decryption via TrueCrypt

- The people of interest used TrueCrypt to create an encrypted drive and save it as a file. By extracting the program from the image in Autopsy and inspecting logs to find the decryption key the investigators mounted the file and extracted crucial evidence to the investigation.

Proposed Solution from Findings

Based on the evidence gathered throughout the forensic investigation, the following legal actions are recommended under New Zealand law (Ministry of Health, 1975):

1. **John Fredricksen**
    a. **Charges**: Under the **Misuse of Drugs Act 1975**, John Fredricksen may be charged with multiple offenses, including possession, importation, distribution, and

trafficking of Class A controlled drugs (methamphetamine). The evidence, including client lists, travel arrangements, and communications with associates, supports these charges.

   b. **Penalties**: If convicted, Fredricksen faces a maximum sentence of life imprisonment under **Section 6** of the **Misuse of Drugs Act 1975** for the importation and trafficking of Class A drugs.

2. **Steve Kowhai**
   a. **Charges**: Based on evidence of gang affiliations and drug distribution networks, Kowhai can be charged under both the **Misuse of Drugs Act 1975** for drug possession and trafficking.
   b. **Warrants**: A search warrant is recommended for additional properties and storage facilities linked to Kowhai, given his gang involvement and evidence of distribution networks.
   c. **Penalties**: If convicted, Kowhai faces potential life imprisonment under the **Misuse of Drugs Act 1975.**
3. **Jake Heke**
   a. **Warrants**: The investigation has yielded sufficient information to recommend a search warrant for Heke's Auckland residence to uncover further evidence of his involvement in narcotics distribution.
   b. **Potential Charges**: Based on the findings from any search, Heke may face charges under the **Misuse of Drugs Act 1975** for possession and distribution, particularly if further evidence is uncovered linking him to Fredricksen's trafficking network.
4. **Jane Esteban**
   a. **Status**: Although acting under duress, Jane's involvement as a forced courier raises legal complexities. As she is an undercover operative for the Australian Federal Police, her release to Australian authorities is advised upon confirmation of her status. New Zealand Police should verify her role with the AFP.
   b. **Handling**: Pending confirmation, her release to Australian jurisdiction will be coordinated under the **Mutual Assistance in Criminal Matters Act 1992**, allowing cross-border cooperation for her continued protection and support as an operative.

Conclusion

The forensic investigation into the **NARCOS-2019** case has successfully unearthed a complex drug trafficking operation spanning New Zealand and Australia, led by key players John Fredricksen and Steve Kowhai. Through meticulous digital forensics, Customs investigators Raine Roberts and Logan Webster have pieced together extensive evidence of narcotics distribution, gang involvement, and coerced participation of undercover agent Jane Esteban. The findings justify severe legal actions under New Zealand's stringent drug laws, ensuring that individuals involved face consequences proportionate to the gravity of their crimes.

This case underscores the critical role of cross-border intelligence and digital forensics in dismantling organized crime, reinforcing New Zealand's commitment to combating the narcotics trade and safeguarding public welfare. With the recommended warrants, charges, and cooperation with international agencies, the NARCOS-2019 case sets a precedent for transnational justice and collaborative law enforcement efforts.

Appendices

Appendix 1 - John Fredricksen.pdf
Additional biographical and selector data related to John Fredricksen, including personal identifiers and relevant information discovered during the investigation.

Appendix 2 - Jane Esteban.pdf
Additional biographical and selector data for Jane Esteban, containing details essential to her undercover role and investigation findings.

Appendix 3 - Steve Kowhai.pdf
Additional biographical and selector data on Steve Kowhai, highlighting affiliations and activities relevant to the investigation.

Appendix 4 - Jake Heke.pdf
Biographical and selector data concerning Jake Heke, including evidence leading to a warrant request.

Appendix 5 - SK-DESKTOP.pdf
Detailed information on the SK-DESKTOP device belonging to Steve Kowhai, including system configurations, network details, and connected device logs.

Appendix 6 – JFLAPTOP1.pdf
Information on the JFLAPTOP1 device, owned by John Fredricksen, covering system data, browsing history, and significant forensic findings.

Appendix 7 – JELAPTOP.pdf
Documentation of JELAPTOP, Jane Esteban’s laptop, with emphasis on its use in her undercover role and relevant forensic evidence.

Appendix 8 - SK-DESKTOP Domain List.pdf
Comprehensive list of domains accessed on SK-DESKTOP, detailing Steve Kowhai's online activities relevant to drug trafficking operations.

Appendix 9 - JFLAPTOP1 Domain List.pdf
Full record of domains accessed on JFLAPTOP1, illustrating John Fredricksen's search history related to concealing narcotics.

Appendix 10 - JELAPTOP Domain List.pdf
Detailed account of domains accessed on JELAPTOP, highlighting Jane Esteban's undercover search activities and interactions.

Appendix 11 - Locations of Interest.pdf
A catalog of significant locations related to the case, including screenshots, discovery points, and descriptions of relevance to the investigation.

Appendix 12 - Evidence List.pdf
Comprehensive list of all evidence collected throughout the investigation, including source devices, timestamps, and descriptions.

References

Hoffman, Micah; Glynn, Griffin. (2024). *Introduction to OSINT*. Retrieved from www.myosint.training: https://www.myosint.training/courses/introduction-to-osint?ref=f7428c

Microsoft. (2019, April 19). *Recovering Data from the OneNote Cache*. Retrieved from support.microsoft.com: https://support.microsoft.com/en-us/office/recovering-data-from-the-onenote-cache-df2a9500-630e-4f53-b88c-f1da124db89e

Ministry of Health. (1975, October 10). *Misuse of Drugs Act 1975*. Retrieved from www.legislation.govt.nz: https://www.legislation.govt.nz/act/public/1975/0116/latest/dlm436101.html

Salfati, E., & Pease, M. (June 2022). *Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT)*. US Department of Commerce.

Volatility. (2024). *The Volatility Framework*. Retrieved from volatilityfoundation.org: https://volatilityfoundation.org/the-volatility-framework/