Version 1.0

October 19, 2022

A picture containing text

Description automatically generated

Presented by: Tyson, Andrew, Kathryn

ITS 2555 Module 7: College of Southern Maryland

|  |  |
| --- | --- |
| **Investigator:** | **Gale Pomper** |

|  |
| --- |
| Badge #3377 |
| (Professor at College of Southern Maryland) |

|  |  |
| --- | --- |
| **DIGITAL FORENSICS EXAMINERS (Tech):** | **Tyson, Kathryn, Andrew** |

|  |
| --- |
| Digital Forensic Tech #1003373 |
| Cyber security students at CSM |
| Maryland |

|  |  |
| --- | --- |
| **SUBJECT:** | **Digital Forensics Examination Report** |

|  |  |
| --- | --- |
| Accused 1: | John Fredrickson |
| Offense: | Drug Possession |
| Accused 2: | Jane Esteban |
| Offense: | Drug Possession |
| Accused 3: | Steve Kowhai |
| Offense: | Drug Possession and Trafficking |
| Date of Request: | September 9 2022 |
| Date of Conclusion: | October 17, 2022 |
| Report Publish Date: | October 18, 2022 |

**Disclaimer:** The chosen case scenario is for learning purposes only and any association to an actual case and litigation is purely coincidental. Evidence presented in the case scenario is fictitious and are not intended to reflect actual evidence. Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement, recommendation, or favoring by the U.S., State, or local governments, and the information and statements shall not be used for the purposes of advertising

Table of Contents

1 DIGITAL FORENSICS REPORT............................................................................................................1

* 1. CASE INFORMATION...........................................................................................................1
  2. PARTIES INVOLVED.............................................................................................................1

2.2 SUMMARY...........................................................................................................................2

3.1 EVIDENCE SUBMITTED........................................................................................................3

3.2 SOFTWARE UTILIZED...........................................................................................................3

4.1 HASH OF ORIGINAL EVIDENCE............................................................................................4

2 FORENSIC EXAMINATION OF EVIDENCE..........................................................................................5

5.1 FORENSIC IMAGES EXAMINED............................................................................................5

5.1.1 DESCRIPTION......................................................................................................................5

5.1.2 VIRUS AND MALWARE........................................................................................................5

3 FORENSIC EXAMINATION OF FILES................................................................................................10

10.1 TIMELINE...........................................................................................................................10

14.2 CONTACTS.........................................................................................................................14

4 ARTIFACTS......................................................................................................................................15

15.1 DOCUMENTS ARTIFACTS...................................................................................................15

18.1 EMAIL AND BROWSER ARTIFACTS....................................................................................18

23.1 URLs..................................................................................................................................23

24.1 IMAGES ARTIFACTS...........................................................................................................24

5 OTHER............................................................................................................................................28

28.1 PASSWORD LIST................................................................................................................28

6 DISPOSITION..................................................................................................................................29

29.1 EVIDENCE DISPOTITION....................................................................................................29

29.2 FORENSIC EMANINER’S CONCLUSION..............................................................................29

7 ATTACHMENTS..............................................................................................................................30

30.1 APPROVAL SIGNATURES...................................................................................................30

31.1 EVIDENCE INTAKE FORM..................................................................................................31

33.1 CHAIN OF CUSTODY FORM...............................................................................................33

34.1 FINAL DISPOSAL AUTHORITY............................................................................................34

8 APPENDIX.......................................................................................................................................36

36.1 DOCUMENTS ARTIFACTS...................................................................................................36

42.1 EMAIL AND BROWSER ARTIFACTS....................................................................................42

58.1 IMAGE ARTIFACTS.............................................................................................................58

Digital Evidence Forensic Report

|  |  |
| --- | --- |
|  | 22950 Hollywood Rd.  Leonardtown, MD 20650-4700 |

# Case Information:

|  |  |  |  |
| --- | --- | --- | --- |
| Agency Case # | DF2555 | Originating Agency Case #: | DF2555 |
| Distribution: | IT  Internal Audit  Emp. Relations  X Other ; District Attorney of Maryland | | |
| Date/Time Report Completed: | 2022-10-17 | Date/Time Incident Occurred: | 2019-02-16 20:13:47 UTC |
| Type of Report: | Criminal | | |

# Parties Involved:

|  |  |  |  |
| --- | --- | --- | --- |
| Involved | Witness | Complainant | Mentioned |
| Name | Last: Fredricksen | First: John | Title: Mr. |
| Mailing Address: | 8515 Haven Wood Trail Inala, Brisbane QLD 4077 Austrailia | Email: | heresjohnny1@protonmail.com |
| Cell Phone: | TBD | Work Phone: | +1 (258) 585-965 |

|  |  |  |  |
| --- | --- | --- | --- |
| Involved | Witness | Complainant | Mentioned |
| Name | Last: Estaban | First: Jane | Title: Ms. |
| Mailing Address: | Brisbane, Austrailia | Email: | becomingjane@protonmail.com |
| Cell Phone: | TBD | Work Phone: | TBD |

|  |  |  |  |
| --- | --- | --- | --- |
| Involved | Witness | Complainant | Mentioned |
| Name | Last: Kowhai | First: Steve | Title: Mr. |
| Mailing Address: | Wellington, New Zealand | Email: | crayfish1980@protonmail.com |
| Cell Phone: | TBD | Work Phone: | TBD |

|  |  |  |  |
| --- | --- | --- | --- |
| Involved | Witness | Complainant | Mentioned |
| Name | Last: Heke | First: Jake | Title: Mr. |
| Mailing Address: | 5/34 Hapua Street Remuera, Auckland 1050 New Zealand | Email: | TBD |
| Cell Phone: | +640 (214) 536-5477 | Work Phone: | TBD |

# Summary:

On the 16th of February 2019, At the Wellington Airport, two suspects known as John Fredricksen and Jane Estaban were placed under arrest under the suspicion of smuggling drugs. While placing the suspects under arrest the officers collected digital items such as phones and laptops for a basic digital analysis. However, a more thorough investigation began after discovering Methamphetamine on John Fredricksen's person. After all the evidence was collected, the officers began to copy each piece of digital evidence to collect the drive image and the memory dump of the devices. These copies were sent to the digital forensic analysis team for further investigation.

Once we received each suspect's drive images and memory dumps, we began our legal investigation by examining the digital evidence. Through our investigation, we have discovered the user’s names and system information. After documenting the system information of each drive image and memory dump, we then utilized the fully licensed software listed below, under “Software Utilized”. Using the listed applications, we were successfully able to track down and locate several artifacts that fit within our three categories listed as Documents, Email & Browser, and Images. These are the three main categories of digital evidence that we collected. All Items of evidence are documented by date/time, a file paths, and MD5 hashes. A few of the items of evidence had to be decrypted using our software. We also listed the most visited websites and the passwords we uncovered from the suspects image drives.

At the end of our report, we have attached an Evidence Intake form, a Chain of Custody Tracking form, and a Final Disposal Authority Form. These forms include all the case information. To conclude the evidence report, we have included an appendix of all the artifacts that were found and included full-sized images for a better look and understanding of the listed evidence.

Evidence Submitted:

|  |  |
| --- | --- |
| Item # | Item Name |
| 1 | Narcos-1.001-021 (Hard Drive) (Computer) |
| 2 | Narcos-Mem-1.001-003 (Memory Image) (Computer) |
| 3 | Narcos-2. 001-021 (Hard Drive) (Laptop) |
| 4 | Narcos-Mem-2. 001-003 (Memory Image) (Laptop) |
| 5 | Narcos-3. 001-021 (Hard Drive) (Laptop) |
| 6 | Narcos-Mem-3. 001-003 (Memory Image) (Laptop) |

Software Utilized

All software utilized in this examination is fully licensed and registered to [Agency Name] or its agents. All software and forensic hardware have been validated pursuant to UMUC policies and procedures.

|  |  |  |  |
| --- | --- | --- | --- |
| List Software | | | |
| FTK Imager | VMware | PDF Crack |  |
| Autopsy | MD5 Checker | Bulk Extractor |  |
| Windows 10 Pro | Kali Linux | VirtualBox |  |

# Hash of Original Evidence

The original media was connected to a forensic hardware write blocker (asset tag #) and the write blocker connected to a forensic computer (asset tag #). Prior to doing anything with the original media, the media was hashed to obtain a baseline hash value. This allows the hash value of the original media to later be compared to the hash value of the forensic image created of the original media. By comparing the hash values of the original media and that of the forensic image, the forensic image can be authenticated as an exact duplicate copy of the original evidence.

The forensic imaging software utilized in this process creates an imaging report, detailing the hash value(s) of the newly created forensic image. The hash value(s) of the forensic image was compared to the original hash value obtained prior to imaging the device.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Item # | Hash Value | Matched Original | Did Not Match Original | Screenshot of Verified Hash | Explanation of non-match |
| 1  image1.001 | MD5: C63a3d19e9c9495b573f45be544e50f9  SHA1: 4d8e5041f47e0b0fc0eacc85d300661946537418  Other: | Yes |  | Table  Description automatically generated |  |
| 2  Mem1.001 | MD5: 9ca08c17b4a359d61f6f8f7bb6328c1c  SHA1: 191a10f54e04ad05d9d6a430e01ef6203406accb  Other: | Yes |  |  |  |
| 3  Image2.001 | MD5: 6265dbaa16a354daddba311334484660  SHA1: 576d20ffc835d98724e472c1714eaecff37f13d  Other: | Yes |  |  |  |
| 4  Mem2.001 | MD5: 0f7e7be4d2844457e2111eaffa1e77ec  SHA1: 3d6f1ff3e3d61b42837a7ebf0ffe058433c628  Other: | Yes |  |  |  |
| 5  Image3.001 | MD5: b66ca567bec6b0a195b99c57dfa0919f  SHA1: 57c9a704b09fbb50118da57f62546824e062a73a  Other: | Yes |  | Graphical user interface, text, application  Description automatically generated |  |
| 6  Mem3.001 | MD5: 8e8a3a91eb89fe6c3cd10231f13141fe  SHA1: 90b3d8ba9e96373c96ee9460193c1b585eadb009  Other: | Yes |  | Graphical user interface, text, application  Description automatically generated |  |

Forensic Examination of Evidence

**Item #1**

Steve Kohwai

**Description**: Steve’s Image information

|  |  |
| --- | --- |
| Image Evidence | Evidence Technical Details |
|  | System Make/Model: VMware pro-16 |
| Operating System: Windows 10 pro |
| Device Name: SK-Desktop |
| Memory: |
| Storage: 31.21 GB |
| Product Name: Windows 10 pro |
| Registered Owner: Steve |
| Install Date: 2019-01-28 14:15:39 |
| Last Shutdown: 2019-02-01 21:28:22 |
| Time Zone: EST |
| IP address (if applicable): |
| MAC address (if applicable): |
| Additional Users (if applicable): Administrator, Guest, DefaultUser, systemprofile, LocalService, NetworkService, WDAGUtilityAccount |

# Forensic Imaging

After obtaining the hash value(s) of the original media, a forensic image was created. The forensic image was placed on a: Virtual Machine

|  |  |
| --- | --- |
|  | Government/Company Owned, Forensically Wiped Hard Drive |
|  | Government/Company Owned, Forensically Wiped Storage Area Network (SAN) |
|  | Other: |

# Virus and Malware

The original media was scanned for malware. Prior to the scan, all malware definitions were updated. The results were: Malware

|  |  |
| --- | --- |
|  | No malware detected |
|  | Malware detected. If checked, provide an explanation: Narcos Mem-1, Malware |

**Item #2**

Steve Kohwai

**Description**: Steve’s Memory information

|  |  |
| --- | --- |
| Memory Evidence | Evidence Details |
|  | System Make/Model: VMware pro 16 |
| Operating System: Windows 10 pro |
| Device Name: SK-Desktop |
| Memory: |
| Storage: 4.29 GB |
| Processor: AMD64 |
| Device ID: 505f6c36-2d21-4251-aa87-1554fdec5b55 |
| Product ID: 00330-80000-00000-AA502 |
| IP Address: |
| MAC Address: |
| Main User Account: |
| Additional Users: |

# Forensic Imaging

After obtaining the hash value(s) of the original media, a forensic image was created. The forensic image was placed on a:

|  |  |
| --- | --- |
|  | Government/Company Owned, Forensically Wiped Hard Drive |
|  | Government/Company Owned, Forensically Wiped Storage Area Network (SAN) |
|  | Other: |

# Virus and Malware

The original media was scanned for malware. Prior to the scan, all malware definitions were updated. The results were:

|  |  |
| --- | --- |
|  | No malware detected |
|  | |  |  | | --- | --- | |  | Malware detected. If checked, provide an explanation: Narcos Mem-1, Malware | |

**Item #3 Narcos 2.001-021**

**John Fredricksen**

**Description:** John’s Image Drive Details

|  |  |
| --- | --- |
| Image Evidence | Evidence Technical Details |
|  | System Make/Model: VMWare 16.0 |
| Operating System: Windows 10 Pro |
| Device Name: JOHNLAPTOP1 |
| Memory: 4 GB |
| Storage: 32.21 GB |
| Product Name: Windows 10 Pro |
| Registered Owner: JohnF |
| Install Date: 2019-01-28 18:12:46 UTC |
| Last Shutdown: 019-02-02 04:07:38 UTC |
| Time Zone: UTC |
| IP address (if applicable): TBD |
| MAC address (if applicable): TBD |
| Additional Users (if applicable): Guest, Administrator, WDAGUtilityAccount |

# Forensic Imaging

After obtaining the hash value(s) of the original media, a forensic image was created. The forensic image was placed on a:

|  |  |
| --- | --- |
|  | Government/Company Owned, Forensically Wiped Hard Drive |
|  | Government/Company Owned, Forensically Wiped Storage Area Network (SAN) |
|  | Other: |

# Virus and Malware

The original media was scanned for malware. Prior to the scan, all malware definitions were updated. The results were:

|  |  |
| --- | --- |
|  | No malware detected |
|  | Malware detected. If checked, provide an explanation: Quasar file. |

**Item #4** Narcos-Mem-2. 001-003

**John Fredricksen**

**Description:** John’s Memory File Details

|  |  |
| --- | --- |
| Image Evidence | Evidence Details |
|  | System Make/Model: VMWare 16.0 |
| Operating System: Windows 10 Pro |
| Device Name: JOHNFLAPTOP1 |
| Memory: 4 GB |
| Storage: 32 GB |
| Processor: AMD64 |
| Device ID: TBD |
| Product ID: 00330-80000-00000-AA310 |
| IP Address: TBD |
| MAC Address: TBD |
| Main User Account: JohnF |
| Additional Users (if applicable): Guest, Administrator, WDAGUtilityAccount |

# Forensic Imaging

After obtaining the hash value(s) of the original media, a forensic image was created. The forensic image was placed on a:

|  |  |
| --- | --- |
|  | Government/Company Owned, Forensically Wiped Hard Drive |
|  | Government/Company Owned, Forensically Wiped Storage Area Network (SAN) |
|  | Other: |

# Virus and Malware

The original media was scanned for malware. Prior to the scan, all malware definitions were updated. The results were:

|  |  |
| --- | --- |
|  | No malware detected |
|  | Malware detected. If checked, provide an explanation: Quasar file. |

**Item #5 Narcos 3.001-21**

**Jane Estaban**

**Description:** Jane’s Image File details

|  |  |
| --- | --- |
| Image Evidence | Evidence Technical Details |
|  | System Make/Model: VMware 16.0 |
| Operating System: Windows 10 Pro |
| Device Name: JELAPTOP |
| Memory: |
| Storage: 32 GB |
| Product Name: Windows 10 Pro |
| Registered Owner: JaneE |
| Install Date: 2019-01-28 14:20:32 |
| Last Shutdown: 2019-02-01 22:09:36 |
| Time Zone: UTC |
| IP address (if applicable): |
| MAC address (if applicable): |
| Additional Users (if applicable): |

# Forensic Imaging

After obtaining the hash value(s) of the original media, a forensic image was created. The forensic image was placed on a:

|  |  |
| --- | --- |
|  | Government/Company Owned, Forensically Wiped Hard Drive |
|  | Government/Company Owned, Forensically Wiped Storage Area Network (SAN) |
|  | Other: |

# Virus and Malware

The original media was scanned for malware. Prior to the scan, all malware definitions were updated. The results were:

|  |  |
| --- | --- |
|  | No malware detected |
|  | Malware detected. If checked, provide an explanation: Contact Card.zip file |

**Item #6 Narcos-Mem-3. 001-3**

**Jane Estaban**

**Description:** Jane’s Memory File details

|  |  |
| --- | --- |
| Image Evidence | Evidence Details |
|  | System Make/Model: VMware 16.0 |
| Operating System: Windows 10 Pro |
| Device Name: JELAPTOP |
| Memory: |
| Storage: 32 GB |
| Processor: AMD64 |
| Device ID: 8fb04a30-5719-4016-9a84-1b43133f48c9 |
| Product ID: 00330-80000-00000-AA263 |
| IP Address: |
| MAC Address: |
| Main User Account: JaneE |
| Additional Users: |

# Forensic Imaging

After obtaining the hash value(s) of the original media, a forensic image was created. The forensic image was placed on a:

|  |  |
| --- | --- |
|  | Government/Company Owned, Forensically Wiped Hard Drive |
|  | Government/Company Owned, Forensically Wiped Storage Area Network (SAN) |
|  | Other: |

# Virus and Malware

The original media was scanned for malware. Prior to the scan, all malware definitions were updated. The results were:

|  |  |
| --- | --- |
|  | No malware detected |
|  | Malware detected. If checked, provide an explanation: Contact Card.zip File |

Forensic Examination of Files

***Timeline***

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Time | Details | Persons involved |
| 2019-01-23 | 0:18:28 UTC | Image artifact #4  A shipping label was found on John Fredricksen's computer showing John shipping something under the company name “High As a Kite LLC” to As a Kite LLC” to someone named Jake Heke in New Zealand. This contains both the suspects' numbers and addresses. The contents include a Pressure Cooker, a Bread Maker, and 3 Pots. This was found in the suspect's Documents>Business folder in Autopsy. (db804b47095901e20d6666b1e9a56003) | John Fredricksen and Jake Heke |
| 2019-01-23 | 01:29:41 UTC | Image artifact #6  An Image was found on John F’s laptop and the image name is “Janes Kids”. This is a picture of Janes kids. This was found in the suspect's Documents>Business folder in Autopsy. | John Fredricksen and Jane Estaban |
| 2019-01-28 | 14:35:24 EST | Email and Browser artifact #13  Steve Kowhai searches drug routes in wellington using google. This URL search was found using Autopsy. (d69b6ea8e6a1c05c57c4b0523bb37ac0) | Steve Kowhai |
| 2019-01-28 | 14:35:24 EST | Email and Browser artifact #14  Steve Kowhai searches cutting drugs using google. This URL search was found using Autopsy. (d69b6ea8e6a1c05c57c4b0523bb37ac0) | Steve Kowhai |
| 2019-01-28 | 17:47:33 EST | Image artifact #7  This image was found on Jane E’s laptop, located within the pictures folder. It is an image of an Australian police badge. (e13f7de15d62717449376d6a54ce3d5e) | Jane Estaban |
| 2019-01-28 | 19:09:54 UTC | Email and Browser artifact #1  John Fredericksen searches up a steganography tutorial on YouTube to learn how to hide messages within images. This URL search was found in Autopsy. (50a698fff857f00065e7b6b0ceee2188) | John Fredricksen |
| 2019-01-28 | 19:09:54 UTC | Email and Browser artifact #8  John Fredericksen visited a website that sells bags and packs for concealment. This URL search was found in Autopsy. | John Fredricksen |
| 2019-01-28 | 19:28:09 UTC | Doc artifact #1  This document is John’s Client list and it contains 13 individuals that are being supplied with illegal substances, each substance is under an undercover name such as Tweak, Snow, and Mary Jane. This document was found in John F’s Business folder using Autopsy. (db804b47095901e20d6666b1e9a56003) | John Fredricksen, Ricky Ross, Frank Lucas, Chris Coke, Steve Kowhai, Don Cholito, Manuel Noriega, Joaquin Guzman, Leroy Barnes, AL Capone, Jane Estaban, Pablo Esocbar, Franz Sanchez, and Jake Heke |
| 2019-01-29 | 06:01:55 UTC | Email and Browser artifact #3  John Fredericksen searches up how to cut drugs in Bing, Microsoft Edge. This URL search was found in Autopsy. (8a812dea96f1879c7746895bff0fb5dd) | John Fredricksen |
| 2019-01-29 | 06:10:30 UTC | Email and Browser artifact #6  John Fredericksen researched how to launder money. He searched for this using Bing on Microsoft Edge. This URL search was found in Autopsy. (8a812dea96f1879c7746895bff0fb5dd) | John Fredricksen |
| 2019-01-29 | 10:49:20 UTC | Email and Browser artifact #4  John Fredericksen searches “shipping companies for packaging au” for his company to distribute illegal substances using Microsoft Edge in Australia. This URL search was found in Autopsy.  (8a812dea96f1879c7746895bff0fb5dd) | John Fredricksen |
| 2019-01-29 | 10:52:03 UTC | Email and Browser artifact #5  John Fredericksen researched a Harvey Norman pressure cooker. Based on recent discoveries such as the shipping label located on John F’s laptop, the shipping label shows that a pressure cooker was one of the items that were shipped to Jake Heke. He searched for this using Bing on Microsoft Edge. This URL search was found in Autopsy. (8a812dea96f1879c7746895bff0fb5dd) | John Fredricksen |
| 2019-01-29 | 14:12:32 UTC | Doc artifact #7  A Document was found on John's Laptop under the encrypted secret file. True Crack was used to decrypt the file “secret” using the password “ilovediving”. (db804b47095901e20d6666b1e9a56003) | John Fredricksen |
| 2019-01-29 | 16:05:55 EST | Email and Browser artifact #11  Steve Kowhai searches security encryption download links in softpedia. This URL search was found using Autopsy. (f3f979c6dee9fbb7cbdf5818aaa4b723) | Steve Kowhai |
| 2019-01-29 | 16:05:55 EST | Email and Browser artifact #12  Steve Kowhai searches the best places to trade drugs using google. This URL search was found in Autopsy. (f3f979c6dee9fbb7cbdf5818aaa4b723) | Steve Kowhai |
| 2019-01-29 | 16:05:55 EST | Email and Browser artifact #15  Steve Kowhai searches Image Steganography Download using Source Forge. This URL search was found in Autopsy. (f3f979c6dee9fbb7cbdf5818aaa4b723) | Steve Kowhai |
| 2019-01-30 | 08:03 EST | Doc artifact #3  This log found on Jane E’s laptop begins with a discord conversation/log between Jane and John. Then it shows John starting a web browser and then logging into ProtonMail. The last thing it shows is the password for one of John’s files. This was found using Autopsy and going to the downloads folder. (fd3a044bee4d5af72faba9630867d4fd) | Jane Estaban and John Fredricksen |
| 2019-01-30 | 16:20:50 EST | Image artifact #8  Image of GPS route taken to deliver drugs in New Zealand. This Image search was found in Autopsy. (62a67a4a7b775932906d588b8a5b46fc) | Steve K |
| 2019-01-30 | 16:25:05 EST | Image artifact #9  Image of GPS route taken to the New Zealand Airport. This Image search was found in Autopsy. (d2ac41c5c252dc7632d7297e626fc27d) | Steve K |
| 2019-01-30 | 21:48:40 EST | Image artifact #3  Image of lots of cash and bags of various drugs. This Image search was found in Autopsy. (480DA4FF5734C6D20787AF08FC9DA46E) | Steve K |
| 2019-01-30 | 21:48:41 EST | Image artifact #2  Image of gang-affiliated biker vests. This Image search was found in Autopsy. (EA016DB23A40F61C10CE802692DF7C0C) | Steve K |
| 2019-01-30 | 21:57:04 EST | Image artifact #1  Image of bags of meth. This Image search was found in Autopsy. (60398A8EC59753CE5AADB99A566844D7) | Steve K |
| 2019-01-31 | 01:01:39 UTC | Email and Browser artifact #7  John Fredericksen visited a website that shows details on how to conceal drugs on a person. This URL search was found in Autopsy. | John Fredricksen |
| 2019-01-31 | 01:12:25 UTC | Email and Browser artifact #2  John Fredericksen searches up suitcase concealments for drugs to try to conceal his drugs through the airport. This URL search was found in Autopsy. (50a698fff857f00065e7b6b0ceee2188) | John Fredricksen |
| 2019-01-31 | 06:37 EST | Doc artifact #4  This log found on Jane E’s laptop starts with a discord conversation between Jane and John. It also contains google searches for drug detector dogs, body packing, suitcase concealments, and flights to New Zealand. This was found using Autopsy and searching through the downloads folder. (948b4c559b944d6c0f2e1da8e285d835) | Jane Estaban and John Fredricksen |
| 2019-01-31 | 19:04:19 EST | Doc artifact #2  This pdf document found on Jane E’s computer contains information about a course called Undercover Survival and Lawful Invasions. It shows how much the course is, who instructs it, and what is talked about at the course. This was found using Autopsy in JaneE’s Documents folder. (Fa714f0aad66bf3953d061adf2457f86) | Jane Estaban |
| 2019-01-31 | 22:58:46 | Image artifact #10  An Image was found on John F’s laptop in the VMware files and the image name is package.jpg. This is a picture of a drug concealment bag; we have reason to believe he was trying to sneak this into the airport. This was found using autopsy. | John Fredricksen |
| 2019-02-01 | 07:02 EST | Doc artifact #5  This log starts off with a discord conversation. Then it shows how Firefox was used to look up steganography and how to use it. Then it goes back to discord and tells what password was for the image. This was found using Autopsy in the downloads folder of Jane E’s laptop. (f51aa5754e54915e93d329a3eefdc042) | Jane Estaban |
| 2019-02-01 | 21:43:20 UTC | Image artifact #5  Flight Tickets that John F purchased were found on John Fredricksen's computer. This shows that John bought plane tickets to Wellington, and plane tickets back to Brisbane Australia where he came from. This means that he spent a week in Wellington. The File is named Steve K. This was found in the suspect's Documents>Business folder in Autopsy. (d1b21a1cddcb3494d637f2424cc5f0f1) | John Fredricksen |
| 2019-02-02 | 01:47:02 UTC | Email and Browser artifact #9  John Fredericksen searched the address 3 Pegasus St Inala QLD 4077 Australia 26 times on Google Maps. This URL search was found in Autopsy. | John Fredricksen |
| 2019-02-02 | 01:47:52 UTC | Email and Browser artifact #10  John Fredericksen researches and reads an article about how much cocaine can fit in a human body. This URL search was found in Autopsy. | John Fredricksen |
| 2019-02-02 | 08:04 EST | Doc artifact #6  This log found on Jane E’s laptop starts with a google search of flights from Brisbane to Wellington and then shows a conversation on discord. This was found using Autopsy and looking through the downloads folder. (7edea768c94997ed685bf7bc51cc325a) | Jane Estaban |
| 2019-02-16 | 20:13:47 UTC | Jane and John apprehended at the Wellington Airport in New Zealand. | John Fredricksen and Jane Esteban |

The timeline above shows the events that occurred from 2019-01-23 to 2019-02-16 between John Fredricksen, Jane Esteban, Steve Kowhai, Jake Heke, and others involved.

***Contacts***

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Phone number(s) | Email address | Physical Address |
| John Fredericksen | +1 (258) 585-965 | heresjohnny1@protonmail.com | 8515 Haven Wood Trail Inala, Brisbane QLD 4077 Austrailia |
| Jane Estaban | TBD | becomingjane@protonmail.com | TBD |
| Steve Kowhai | TBD | crayfish1980@protonmail.com | TBD |
| Jake Heke | +640 (214) 536-5477 | TBD | 5/34 Hapua Street Remuera, Auckland 1050 New Zealand |
| Steve Discord/ Elinor Pearson | +1 (923) 548-3751 | Elinorpearson@flexigen.com | 600 Bayview Avenue, Draper, Montana, 3088 United States |
| Steve Discord/ Carey Savage | +1 (897) 574-3014 | careysavage@veraq.com | 485 Willow Street, Henrietta, California, 7234 Unites States |
| Steve Discord/ Irwin Davidson | +1 (883) 527-2041 | irwindavidson@danja.com | 439 Cook Street, Chapin, Kentucky, 7398 United States |

John Frederickson’s contact information and address were found in autopsy. Jake Heke is John’s client, and his contact information were found in autopsy. Elinor Pearson, Carey Savage, and Irwin Davidson are clients of Steve, and their contact information were found in autopsy.

***Documents***

Artifact #1: John F Client List for Drug Distribution Company (High As a Kite LLC)

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: db804b47095901e20d6666b1e9a56003 |
| Path location: Users/JohnF/Documents/Business/clients.ods |
| File Name: clients.ods |
| Date/Time: 2019-01-28 19:28:09 UTC |
| Creator: John F |
| Last modified: 2019-01-29 03:02:47 UTC |
| Last accessed: 2019-01-29 23:04:14 UTC |

This document is John’s Client list and it contains 13 individuals that are being supplied with illegal substances, each substance is under an undercover name such as Tweak, Snow, and Mary Jane. This document was found in John F’s Business folder using Autopsy.

Artifact #2: Jane E’s Undercover Survival Course information

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: fa714f0aad66bf3953d061adf2457f86 |
| Path location: /img\_Narcos-3.001/vol\_vol7/Users/JaneE/Documents/course-undercover-survival.pdf |
| File Name: course-undercover-survival.pdf |
| Date/Time: 2019-01-31 19:04:19 EST |
| Creator: JaneE |
| Last modified: 2019-01-31 19:04:19 EST |
| Last accessed: 2019-01-31 19:04:19 EST |

This pdf document found on Jane E’s computer contains information about a course called Undercover Survival and Lawful Invasions. It shows how much the course is, who instructs it, and what is talked about at the course. This was found using Autopsy in JaneE’s Documents folder.

Artifact #3: Jane E’s first log

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: fd3a044bee4d5af72faba9630867d4fd |
| Path location: /img\_Narcos-3.001/vol\_vol7/Users/JaneE/Downloads/Qusar v1.3.0.0/Clients/JohnF@JOHNFLAPTOP\_4DD90B0/Logs/01-30-2019.html |
| File Name: 01-30-2019.html |
| Date/Time: 30.01.2019 08:03 |
| Creator: JaneE |
| Last modified: 2019-02-01 21:52:34 EST |
| Last accessed: 2019-02-01 21:52:34 EST |

This log found on Jane E’s laptop begins with a discord conversation/log between Jane and John. Then it shows John starting a web browser and then logging into ProtonMail. The last thing it shows is the password for one of John’s files. This was found using Autopsy and going to the downloads folder.

Artifact #4: Jane E’s second log

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: 948b4c559b944d6c0f2e1da8e285d835 |
| Path location: /img\_Narcos-3.001/vol\_vol7/Users/JaneE/Downloads/Qusar v1.3.0.0/Clients/JohnF@JOHNFLAPTOP\_4DD90B0/Logs/01-31-2019.html |
| File Name: 01-31-2019.html |
| Date/Time: 31.01.2019 06:37 |
| Creator: JaneE |
| Last modified: 2019-02-01 21:52:34 EST |
| Last accessed: 2019-02-01 21:52:34 EST |

This log found on Jane E’s laptop starts with a discord conversation between Jane and John. It also contains google searches for drug detector dogs, body packing, suitcase concealments, and flights to New Zealand. This was found using Autopsy and searching through the downloads folder.

Artifact #5: Jane E’s third log

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: f51aa5754e54915e93d329a3eefdc042 |
| Path location: /img\_Narcos-3.001/vol\_vol7/Users/JaneE/Downloads/Qusar v1.3.0.0/Clients/JohnF@JOHNFLAPTOP\_4DD90B0/Logs/02-01-2019.html |
| File Name: 02-01-2019.html |
| Date/Time: 01.02.2019 07:02 |
| Creator: JaneE |
| Last modified: 2019-02-01 21:52:34 EST |
| Last accessed: 2019-02-01 21:52:34 EST |

This logs starts off with a discord conversation. Then it shows how Firefox was used to look up steganography and how to use it. Then it goes back to discord and tells what password was for the image. This was found using Autopsy in the downloads folder of Jane E’s laptop.

Artifact #6: Jane E’s fourth log

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: 7edea768c94997ed685bf7bc51cc325a |
| Path location: /img\_Narcos-3.001/vol\_vol7/Users/JaneE/Downloads/Qusar v1.3.0.0/Clients/JohnF@JOHNFLAPTOP\_4DD90B0/Logs/02-02-2019.html |
| File Name: 02-02-2019.html |
| Date/Time: 02.02.2019 08:04 |
| Creator: JaneE |
| Last modified: 2019-02-01 21:52:34 EST |
| Last accessed: 2019-02-01 21:52:34 EST |

This log found on Jane E’s laptop starts with a google search of flights from Brisbane to Wellington and then shows a conversation on discord. This was found using Autopsy and looking through the downloads folder.

Artifact #7: JohnF Crystal Method

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: db804b47095901e20d6666b1e9a56003 |
| Path location: C:/Users/JohnF/Downloads/Attachments-Important, crucial to our method/secret |
| File Name: Memo Things.odt |
| Date/Time: 2019-01-29 14:12:32 UTC |
| Creator: JohnF |
| Last modified: 2019-01-29 |
| Last accessed: 2019-01-30 |

A Document was found on John's Laptop under the encrypted secret file. True Crack was used to decrypt the file “secret” using the password “ilovediving”.

***Email and Browser***

Artifact #1: John F YouTube Search Steganography Tutorial (URL Search)

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: 50a698fff857f00065e7b6b0ceee2188 |
| Path location: Users/JohnF/AppData/Roaming/Mozilla/Firefox/Profiles/fj248tbu.default/places.sqlite |
| Date/Time: 2019-01-28 19:09:54 UTC |
| Sender: N/A |
| Recipient: N/A |

John Fredericksen searches up a steganography tutorial on YouTube to learn how to hide messages within images. This URL search was found in Autopsy.

Artifact #2: John F Researches “suitcase concealments for drugs” (URL Search)

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: 50a698fff857f00065e7b6b0ceee2188 |
| Path location: Users/JohnF/AppData/Roaming/Mozilla/Firefox/Profiles/fj248tbu.default/places.sqlite |
| Date/Time: 2019-01-31 01:12:25 UTC |
| Sender: N/A |
| Recipient: N/A |

John Fredericksen searches up suitcase concealments for drugs to try to conceal his drugs through the airport. This URL search was found in Autopsy.

Artifact #3: John F Researches “how to cut drugs” (URL Search)

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: 8a812dea96f1879c7746895bff0fb5dd |
| Path location: Users/JohnF/AppData/Local/Microsoft/Windows/WebCache/ WebCacheV01.dat |
| Date/Time: 2019-01-29 06:01:55 UTC |
| Sender: N/A |
| Recipient: N/A |

John Fredericksen searches up how to cut drugs in Bing, Microsoft Edge. This URL search was found in Autopsy.

Artifact #4: John F Researches “shipping companies for packaging au” (URL Search)

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: 8a812dea96f1879c7746895bff0fb5dd |
| Path location: Users/JohnF/AppData/Local/Microsoft/Windows/WebCache/ WebCacheV01.dat |
| Date/Time: 2019-01-29 10:49:20 UTC |
| Sender: N/A |
| Recipient: N/A |

John Fredericksen searches “shipping companies for packaging au” for his company to distribute illegal substances using Microsoft Edge in Australia. This URL search was found in Autopsy.

Artifact #5: John F Researches “harvey norman pressure cooker au” (URL Search)

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: 8a812dea96f1879c7746895bff0fb5dd |
| Path location: Users/JohnF/AppData/Local/Microsoft/Windows/WebCache/ WebCacheV01.dat |
| Date/Time: 2019-01-29 10:52:03 UTC |
| Sender: N/A |
| Recipient: N/A |

John Fredericksen researched a Harvey Norman pressure cooker. Based on recent discoveries such as the shipping label located on John F’s laptop, the shipping label shows that a pressure cooker was one of the items that were shipped to Jake Heke. He searched for this using Bing on Microsoft Edge. This URL search was found in Autopsy.

Artifact #6: John F Researches “how to launder money” (URL Search)

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: 8a812dea96f1879c7746895bff0fb5dd |
| Path location: Users/JohnF/AppData/Local/Microsoft/Windows/WebCache/ WebCacheV01.dat |
| Date/Time: 2019-01-29 06:10:30 UTC |
| Sender: N/A |
| Recipient: N/A |

John Fredericksen researched how to launder money. He searched for this using Bing on Microsoft Edge. This URL search was found in Autopsy.

Artifact #7: John F Visits a website titled “Body Packing – The Internal Concealment of Illicit Drugs” (Web History)

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: |
| Path location: Users/JohnF/AppData/Roaming/Mozilla/Firefox/Profiles/fj248tbu.default/places.sqlite |
| Date/Time: 2019-01-31 01:01:39 UTC |
| Sender: N/A |
| Recipient: N/A |

John Fredericksen visited a website that shows details on how to conceal drugs on a person. This URL search was found in Autopsy.

Artifact #8: John F Visits a website titled “Concealment Packs and Bags | CCW Bags” (Web History)

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: |
| Path location: Users/JohnF/AppData/Roaming/Mozilla/Firefox/Profiles/fj248tbu.default/places.sqlite |
| Date/Time: 2019-01-28 19:09:54 UTC |
| Sender: N/A |
| Recipient: N/A |

John Fredericksen visited a website that sells bags and packs for concealment. This URL search was found in Autopsy.

Artifact #9: John F Visits Google Maps Address “3 Pegasus St Inala QLD 4077 Australia” 26 Times (Web History)

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: |
| Path location: Users/JohnF/AppData/Roaming/Mozilla/Firefox/Profiles/fj248tbu.default/places.sqlite |
| Date/Time: 2019-02-02 01:47:02 UTC |
| Sender: N/A |
| Recipient: N/A |

John Fredericksen searched the address 3 Pegasus St Inala QLD 4077 Australia 26 times on Google Maps. This URL search was found in Autopsy.

Artifact #10: John F Visits a website titled “How Much Cocaine Can You Fit In Your, Ahem, Body” (Web History)

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: |
| Path location: Users/JohnF/AppData/Roaming/Mozilla/Firefox/Profiles/fj248tbu.default/places.sqlite |
| Date/Time: 2019-02-02 01:47:52 UTC |
| Sender: N/A |
| Recipient: N/A |

John Fredericksen researches and reads an article about how much cocaine can fit in a human body. This URL search was found in Autopsy.

Artifact #11: Steve K Visits a website titled “Security – Encrypting Downloads” (Web History)

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
| Graphical user interface, text, application, email  Description automatically generated | Hash Value: f3f979c6dee9fbb7cbdf5818aaa4b723 |
| Path location: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/History |
| Date/Time: 2019-01-29 16:05:55 EST |
| Sender: N/A |
| Recipient: N/A |

Steve Kowhai researched how to encrypt downloaded data in file explorer. This URL search was found in Autopsy.

Artifact #12: Steve K Visits a website titled “best places to trade drugs” (Web History)

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
| Text  Description automatically generated with medium confidence | Hash Value: f3f979c6dee9fbb7cbdf5818aaa4b723 |
| Path location: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/History |
| Date/Time: 2019-01-29 16:05:55 EST |
| Sender: N/A |
| Recipient: N/A |

Steve Kowhai researches the best place to trade drugs. This URL search was found in Autopsy.

Artifact #13: Steve K Visits a website titled “drug routes in wellington” (Web History)

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
| A picture containing graphical user interface  Description automatically generated | Hash Value: d69b6ea8e6a1c05c57c4b0523bb37ac0 |
| Path location: Users/Steve/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat |
| Date/Time: 2019-01-28 14:35:34 EST |
| Sender: N/A |
| Recipient: N/A |

Steve Kowhai researches drug routes in Wellington. This URL search was found in Autopsy.

Artifact #14: Steve K Visits a website titled “cutting drugs” (Web History)

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
| A picture containing text  Description automatically generated | Hash Value: d69b6ea8e6a1c05c57c4b0523bb37ac0 |
| Path location: Users/Steve/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat |
| Date/Time: 2019-01-28 14:35:34 EST |
| Sender: N/A |
| Recipient: N/A |

Steve Kowhai researched how to cut drugs. This URL search was found in Autopsy.

Artifact #15: Steve K Visits a website titled “Image Steganography Download” (Web History)

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
| Text, letter  Description automatically generated | Hash Value: f3f979c6dee9fbb7cbdf5818aaa4b723 |
| Path location: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/History |
| Date/Time: 2019-01-29 16:05:55 EST |
| Sender: N/A |
| Recipient: N/A |

Steve Kowhai researches a steganography download link. This URL search was found in Autopsy.

|  |  |  |
| --- | --- | --- |
| URL | Number of times accessed | Date/Time accessed |
| <https://www.youtube.com/watch?v=iUNUjqSXWj0>  (Steganography Tutorial – Hide Messages In Images - Youtube) | 8 | 2019-01-31 13:31:04 PST |
| Google.com (suitcase concealments for drugs) | 6 | 2019-01-30 18:12:25 PST |
| Bing.com (how to cut drugs) | 5 | 2019-01-28 23:01:55 PST |
| Bing.com (shipping companies for packaging au) | 3 | 2019-01-29 03:49:20 PST |
| Bing.com (Harvey Norman pressure cooker au) | 4 | 2019-01-29 03:52:03 PST |
| <https://www.softpedia.com/get/Security/Encrypting/?utm_source=spd&utm_campaign=postdl_redr> | 3 | 2019-02-01 21:28:48 EST |
| Google.com (best places to trade drugs) | 17 | 2019-02-01 21:28:48 EST |
| Google.no.nz (drug routes in wellington) | 33 | 2019-02-01 21:39:26 EST |
| Google.com (cutting drugs) | 47 | 2019-02-01 21:39:26 EST |
| <https://sourceforge.net/projects/image-steg/> | 7 | 2019-02-01 21:28:48 EST |

This is a list of the URLs the suspects have searched and clicked on, showing the number of times accessed.

***Images***

Artifact #1: Steve K Meth

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
| A picture containing paper, wrapped, plastic  Description automatically generated | Hash Value: 60398A8EC59753CE5AADB99A566844D7 |
| Path Location: Users/Steve/Pictures/620x349.jpg |
| File Name: 620x349.jpg |
| Date/Time: 2019-01-30 21:57:04 EST |
| Creator: Steve K |
| Last modified:  2019-01-31 21:48:41 EST |
| Last accessed:  2019-01-30 22:04:13 EST |
|  | Image of: Meth |

Image found in Steve K.’s users/pictures directory shows multiple bags of meth.

Artifact #2: Steve K Biker vests

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
| A picture containing text  Description automatically generated | Hash Value: EA016DB23A40F61C10CE802692DF7C0C |
| Path Location:  Users/Steve/Pictures/620x349.jpg |
| File Name: eight\_col\_patches\_crp.jpg |
| Date/Time:  2019-01-30 21:59:38 EST |
| Creator: Steve K |
| Last modified: 2019-01-31 21:48:41 EST |
| Last accessed:  2019-01-31 21:42:46 EST |
|  | Image of: Biker Apparel |

Image found in Steve K.’s users/pictures directory shows multiple vests, gang affiliated.

Artifact #3: Steve K Drugs and Money

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
| A picture containing text, indoor, wooden  Description automatically generated | Hash Value: 480DA4FF5734C6D20787AF08FC9DA46E |
| Path Location:  Users/Steve/Pictures/price-meth-bust-4.jpg |
| File Name:  price-meth-bust-4.jpg |
| Date/Time: 2019-01-30 21:58:22 EST |
| Creator: Steve K |
| Last modified:  2019-01-31 21:48:41 EST |
| Last accessed:  2019-01-30 22:04:13 EST |
|  | Image of: Cash, Drugs |

Image found in Steve K.’s users/pictures directory shows many bags containing illegal substances and approximately $5,391.00 in cash.

Artifact #4: JohnF Shipping Label

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: 4fdf3dd6bac6ba99f6eafcedd9a64efa |
| Path location: Users/JohnF/Documents/Business/shipping.PNG |
| File Name: shipping.PNG |
| Date/Time: 2019-01-23 0:18:28 UTC |
| Creator: John F |
| Last modified: 2019-01-23 0:18:28 UTC |
| Last accessed: 2019-01-29 2:58:47 UTC |
|  | Image of: Shipping Label |

A shipping label was found on John Fredricksen's computer showing John shipping something under the company name “High As a Kite LLC” to Jake Heke in New Zealand. This contains both the suspects' numbers and addresses. The contents include a Pressure Cooker, a Bread Maker, and 3 Pots. This was found in the suspect's Documents>Business folder in Autopsy.

Artifact #5: JohnF Flight Tickets

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: d1b21a1cddcb3494d637f2424cc5f0f1 |
| Path location: Users/JohnF/Documents/Business/Steve K.PNG |
| File Name: Steve K.PNG |
| Date/Time: 2019-02-01 21:43:20 UTC |
| Creator: John F |
| Last modified: 2019-02-01 21:43:21 UTC |
| Last accessed: 2019-02-02 0:57:27 UTC |
|  | Image of: Flight Tickets to Wellington |

Flight Tickets that John F purchased were found on John Fredricksen's computer. This shows that John bought plane tickets to Wellington, and plane tickets back to Brisbane Australia where he came from. This means that he spent a week in Wellington. The File is named Steve K. This was found in the suspect's Documents>Business folder in Autopsy.

Artifact #6: JohnF has a photo of Janes Kids on his Laptop

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: |
| Path location: |
| File Name: Janes Kids.jpg |
| Date/Time: 2019-01-23 01:29:41 UTC |
| Creator: John F |
| Last modified: 2019-01-23 01:29:42 UTC |
| Last accessed: 2019-01-30 23:21:55 UTC |
|  | Image of: Janes Kids |

An Image was found on John F’s laptop and the image name is “Janes Kids”. This is a picture of Janes kids. This was found in the suspect's Documents>Business folder in Autopsy.

Artifact #7: Jane E has an image of a police badge

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: e13f7de15d62717449376d6a54ce3d5e |
| Path location: /img\_Narcos-3.001/vol\_vol7/Users/JaneE/Pictures/background.jpg |
| File Name: background.jpg |
| Date/Time: 2019-01-28 17:47:33 EST |
| Creator: JaneE |
| Last modified: 2019-01-28 17:47:33 EST |
| Last accessed: 2019-01-28 17:47:33 EST |
|  | Image of: A police badge |

This image was found on Jane E’s laptop, located within the pictures folder. It is an image of an Australian police badge.

Artifact #8: Steve K image of map of New Zealand, drug routes

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
| Graphical user interface  Description automatically generated with medium confidence | Hash Value: 62a67a4a7b775932906d588b8a5b46fc |
| Path location: /Users/Steve/AppData/Local/Packages/Microsoft.ScreenSketch\_8wekyb3d8bbwe/TempState/ |
| File Name: (35628D63-554D-4654-BA8F-DEF067313F361).png |
| Date/Time: 2019-01-30 16:20:52 EST |
| Creator: Steve K |
| Last modified: 2019-01-30 16:20:50 EST |
| Last accessed: 2019-01-30 16:20:50 EST |
|  | Image of: Drug routes |

This is an image found in Steve’s image files, located in local app data. The image is a GPS route taken when delivering drugs.

Artifact #9: Steve K image of New Zealand

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
| Graphical user interface, application, website  Description automatically generated | Hash Value: d2ac41c5c252dc7632d7297e626fc27d |
| Path location: Users/Steve/AppData/Local/Packages/Microsoft.ScreenSketch\_8wekyb3d8bbwe/TempState/ |
| File Name: (D0ECD46B-96DB-49E0-8187-555D488B1B40).png |
| Date/Time: 2019-01-30 16:25:04 EST |
| Creator: Steve K |
| Last modified: 2019-01-30 16:25:05 EST |
| Last accessed: 2019-01-30 16:25:06 EST |
|  | Image of: GPS route to airport |

This is an image found in Steve’s image files, located in local app data. The image is a GPS route from Steve’s house to the Airport.

Artifact #10: John F image of a packaged concealment bag

|  |  |
| --- | --- |
| Image of artifact | Artifact Details |
|  | Hash Value: |
| Path location: /Users/JohnF/AppData/Local/Temp/vmware-JohnF/VMwareDnD/770cd05f/package.jpg |
| File Name: package.jpg |
| Date/Time: 2019-01-31 22:58:46 |
| Creator: John F |

An Image was found on John F’s laptop in the VMware files and the image name is package.jpg. This is a picture of a drug concealment bag; we have reason to believe he was trying to sneak this into the airport. This was found using autopsy.

***Other***

Password List

|  |  |  |
| --- | --- | --- |
| Password | Where located | Associated File |
| ilovediving | /img\_Narcos-3.001/vol\_vol7/Users/JaneE/Downloads/Qusar v1.3.0.0/Clients/JohnF@JOHNFLAPTOP\_4DD90B0/Logs/01-30-2019.html | C:\Users\JohnF\Downloads\Attachments-Importa...\secret |
| Steve1234 | /img\_Narcos-3.001/vol\_vol7/Users/JaneE/Downloads/Qusar v1.3.0.0/Clients/JohnF@JOHNFLAPTOP\_4DD90B0/Logs/02-01-2019.html | Protonmail.com |
| John1234 | /img\_Narcos-3.001/vol\_vol7/Users/JaneE/Downloads/Qusar v1.3.0.0/Clients/JohnF@JOHNFLAPTOP\_4DD90B0/Logs/01-30-2019.html | Protonmail.com |

This is a list of the passwords that were found during our forensic investigation.

Disposition

# Evidence Disposition

On 09/06/2022 SA Gale Pomper of CSM Cyber Crime Division requested analysis of John Fredricksen, Jane Esteban, and Steve Kowhai’s (Unknown) laptops, desktop, drives, and memory. Specifically looking for information that may lead to John Fredricksen, Jane Esteban, and Steve Kowhai’s criminal activities. The Cyber Action Team (CAT) was provided with a chain of custody form from SA Pomper. A forensic copy of the original evidence was completed following the policies and procedures of CSM. The original evidence is locked in a secure evidence collection room within the Cyber Crime Division location and properly documented. Any data presented here was obtained from the forensic copy of the original evidence.

Forensic Examiner’s Conclusion

While conducting our investigation we used forensic tools and techniques to locate the user’s names and system information of each suspect’s drive images and memory dumps. Using the forensic tools, we were also able to locate multiple artifacts that were placed into a category according to the type of evidence it was (jpg, email, etc.). All the artifacts were carefully documented, and each artifact has a description stating what the image is of. Our investigation also led us to finding passwords used on the suspect’s devices and what websites they frequented most.

As we began and continued the investigation, we found that on each suspect’s device there were certain pieces of evidence that could lead to an arrest. On John Fredricksen’s laptop there was a client list that contained individuals that were being supplied with illegal substances (Document - Artifact #1). Also found was searches for concealing drugs (Email and Browser - Artifact #2) and for cutting drugs (Email and Browser - Artifact #3). He also looks up methods on how to launder money (Email and Browser - Artifact #6). Another artifact we found on his laptop was an image of Jane Esteban’s kids (Images - Artifact #6), and a concealment bag (Images - Artifact #10). On Steve Kowhai’s (Unknown) desktop we found images of methamphetamine (Images - Artifact #1) and an image of multiple types of illegal substances and money (Images - Artifact #2). Also, we found two separate routes that were used for drug trafficking in New Zealand (Images - Artifact #8 and Artifact #9). On Jane Esteban’s laptop we found a police badge (Images - Artifact #7) and logs that she has taken regarding the case (Documents - Artifact #3, Artifact #4, Artifact #5, and Artifact #6).

After reviewing all the artifacts, we found on the three individuals’ laptop or desktop we concluded that Jane Esteban was an undercover cop, who pretended to be an addict, and came into contact with John Fredricksen. He sold drugs to Jane and then later asked her if she could help him to traffic drugs into New Zealand and when she refused, he threatened Jane with a photo of her kids, saying that he was going to harm them if she did not follow through with what he was asking. This was stated in one of the logs that Jane had made. Another conclusion that we came to is that Steve Kowhai was a client of John’s and was planning on helping him traffic drugs across New Zealand.

**Attachments**

Chain of Custody

Evidence Intake Form

**Approvals**

|  |  |
| --- | --- |
| Tyson, Kathryn, Andrew | Gale Pomper |
| Report Author(s) Digital Signature | Report Approver Digital Signature |

Evidence Intake Form

|  |  |  |
| --- | --- | --- |
| **Case Information** | | **Case-Ref#: DF2555** |
| **Is this the first request for this case?** First  Follow-up prior request | | |
| **Request Date:** 02/16/2019 | | |
| **Request Type:** Examination  Create an Image  Onsite | | |
| **Submitting Person:** Gale Pomper  **Investigator:** Tyson Blackwell, Kathryn Crider, Andrew Singleton | | **Priority:**  Low  Normal  High |
| **Seizure Location:** Wellington, New Zealand (Airport) | **Date of Search and Seizure:** 02/16/2019 | **Date Needed:** 02/20/2019 |
| **Type of Seizure:**  Warrant  Consent  Other  Explain: | | |

|  |
| --- |
| **Details of evidence item(s) (description):** |
| 1. John’s Drive Image. Windows 10 Laptop. No damage found. 2. Jane’s Drive Image. Windows 10 Laptop. No damage found. 3. Steve’s Drive Image. Windows 10 Desktop. No damage found. 4. John’s Memory Image. Windows 10 Laptop. No damage found. 5. Jane’s Memory Image. Windows 10 Laptop. No damage found. 6. Steve’s Memory Image. Windows 10 Desktop. No damage found. |
| **Service Type Request (description):** |
| 1. Two passengers named John Fredricksen and Jane Esteban were intercepted at the airport in Wellington, New Zealand. In John’s baggage there was a laptop and in Jane’s baggage there was a small windows laptop. After Jane was interrogated customs was able to obtain search warrant to the address that Jane gave to them. Once they raided the place they found a desktop belonging to Steve (Unknown). This request is to examine the devices: 2. To discover the three suspect’s motives 3. Relationship between John and Steve (Unknown) 4. Any other evidence needed for the case |
|  |

|  |  |
| --- | --- |
| Submitting Person: Gale Pomper | Lab Personnel: Tyson Blackwell, Kathryn Crider, Andrew Singleton |
| Signature: Gale Pomper | **Signature:** Tyson Blackwell, Kathryn Crider, Andrew Singleton |

**CSM Digital Forensics Department**  
 **EVIDENCE CHAIN OF CUSTODY TRACKING FORM**

Case Number: \_\_\_DF2555\_\_\_\_\_\_\_ Offense: \_\_\_\_Drug Trafficking\_\_\_\_\_

Submitting Officer: (Name/ID#) \_\_\_\_Gale Pomper\_\_\_\_\_\_\_\_\_

Victim: \_\_\_Wellington, New Zealand\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Suspect: \_\_John Fredericksen, Steve Kowhai, Jane Estaban\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date/Time Seized: \_\_\_2/16/2019\_\_\_\_\_\_\_\_\_\_\_Location of Seizure: \_\_Wellington Airport\_\_\_

|  |  |  |
| --- | --- | --- |
| **Description of Evidence** | | |
| **Item #** | **Quantity** | **Description of Item** (Model, Serial #, Condition, Marks, Scratches) |
| 1 | 1 | Steve’s Drive Image, Desktop |
| 2 | 1 | Steve’s Memory Image, Desktop |
| 3 | 1 | John’s Drive Image, Windows 10 Laptop |
| 4 | 1 | John’s Memory Image, Windows 10 Laptop |
| 5 | 1 | Jane’s Drive Image, Windows 10 Laptop |
| 6 | 1 | Jane’s Memory Image, Windows 10 Laptop |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Chain of Custody** | | | | |
| **Item #** | **Date/Time** | **Released by** (Signature & ID#) | **Received by** (Signature & ID#) | **Comments/Location** |
| 1 | 2/16/2019 8:00 pm | Tyson Blackwell | Gale Pomper | Image of Steve’s OS returned to supervising officer |
| 2 | 2/16/2019 8:00 pm | Tyson Blackwell | Gale Pomper | Image of Steve’s OS returned to supervising officer |
| 3 | 2/16/2019 8:00 pm | Andrew Singleton | Gale Pomper | Image of John’s OS returned to supervising officer |
| 4 | 2/16/2019 8:00 pm | Andrew Singleton | Gale Pomper | Image of John’s OS returned to supervising officer |
| 5 | 2/16/2019 8:00 pm | Kathryn Cryder | Gale Pomper | Image of Jane’s OS returned to supervising officer |
| 6 | 2/16/2019 8:00 pm | Kathryn Cryder | Gale Pomper | Image of Jane’s OS returned to supervising officer |

APD\_Form\_#PE003\_v.1 (12/2012) Page 1 of 2 pages (See back)

|  |  |
| --- | --- |
| **Final Disposal Authority** |  |
| **Authorization for Disposal**  **Item(s) #: \_\_\_5 and 6\_\_\_\_\_\_\_ on this document pertaining to (suspect): \_\_\_\_\_Jane Esteban\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)** X Return to Owner ☐ Auction/Destroy/Divert  Name & ID# of Authorizing Officer: \_\_\_\_\_Gale Pomper\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature: \_\_\_\_\_Gale Pomper\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date: \_\_\_\_2022-10-17\_\_\_\_\_\_\_\_\_\_\_ |  |
| **Witness to Destruction of Evidence**  Item(s) #: \_\_\_\_\_\_\_\_\_\_ on this document were destroyed by Evidence Custodian \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ID#:\_\_\_\_\_\_  in my presence on (date) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.  Name & ID# of Witness to destruction: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| **Release to Lawful Owner**  Item(s) #: \_\_\_\_\_\_\_\_\_\_ on this document was/were released by Evidence Custodian \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ID#:\_\_\_\_\_\_\_\_\_ to  Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ City: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_State: \_\_\_\_\_\_\_ Zip Code: \_\_\_\_\_\_\_\_\_\_  Telephone Number: (\_\_\_\_\_) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Under penalty of law, I certify that I am the lawful owner of the above item(s).  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   Copy of Government-issued photo identification is attached. ☐ Yes ☐ No |  |
| **This Evidence Chain-of-Custody form is to be retained as a permanent record by the Anywhere Police Department.** |  |
|  |  |

APD\_Form\_#PE003\_v.1 (12/2012) Page 2 of 2 pages (See front)

Appendix A: Artifacts Images.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Image Name | Artifact Reference | | Artifact Path | |
| John F Client List for Drug Distribution Company (High As a Kite LLC) | Documents- Artifact #1 | | /img\_Narcos-2.001/vol\_7/Users/JohnF/Documents/Business/clients.ods | |
| A picture containing text  Description automatically generatedText  Description automatically generatedText  Description automatically generated | | | | |
|  | | | | |
| Jane E’s Undercover Survival Course information | Documents- Artifact #2 | | /img\_Narcos-3.001/vol\_vol7/Users/JaneE/Documents/course-undercover-survival.pdf | |
|  | | | | |
|  | | | | |
| Jane E’s first log | Documents- Artifact #3 | | /img\_Narcos-3.001/vol\_vol7/Users/JaneE/Downloads/Qusar v1.3.0.0/Clients/JohnF@JOHNFLAPTOP\_4DD90B0/Logs/01-30-2019.html | |
|  | | | | |
|  | | | | |
| Jane E’s second log | Documents- Artifact #4 | | /img\_Narcos-3.001/vol\_vol7/Users/JaneE/Downloads/Qusar v1.3.0.0/Clients/JohnF@JOHNFLAPTOP\_4DD90B0/Logs/01-31-2019.html | |
|  | | | | |
|  | | | | |
| Jane E’s third log | Documents- Artifact #5 | | /img\_Narcos-3.001/vol\_vol7/Users/JaneE/Downloads/Qusar v1.3.0.0/Clients/JohnF@JOHNFLAPTOP\_4DD90B0/Logs/02-01-2019.html | |
|  | | | | |
|  | | | | |
| Jane E’s fourth log | Documents- Artifact #6 | | /img\_Narcos-3.001/vol\_vol7/Users/JaneE/Downloads/Qusar v1.3.0.0/Clients/JohnF@JOHNFLAPTOP\_4DD90B0/Logs/02-02-2019.html | |
|  | | | | |
|  | | | | |
| John F Crystal Method | Documents-Artifact #7: | | C:/Users/JohnF/Downloads/Attachments-Important, crucial to our method/secret | |
|  | | | | |
| John F YouTube Search Steganography Tutorial (URL Search | Email and Browser – Artifact #1 | | /img\_Narcos-2.001/vol\_7/Users/JohnF/AppData/Roaming/Mozilla/Firefox/Profiles/fj248tbu.default/places.sqlite | |
|  | | | | |
|  | | | | |
| John F Searches “suitcase concealments for drugs” | Email and Browser – Artifact #2 | | /img\_Narcos-2.001/vol\_7/Users/JohnF/AppData/Roaming/Mozilla/Firefox/Profiles/fj248tbu.default/places.sqlite | |
|  | | | | |
|  | | | | |
| John F searches “how to cut drugs” | Email and Browser – Artifact #3 | | /img\_Narcos-2.001/vol\_7/Users/JohnF/AppData/Local/Microsoft/Windows/WebCache/ WebCacheV01.dat | |
|  | | | | |
|  | | | | |
| John F searches “shipping companies for packaging au” | Email and Browser – Artifact #4 | | /img\_Narcos-2.001/vol\_7/Users/JohnF/AppData/Local/Microsoft/Windows/WebCache/ WebCacheV01.dat | |
|  | | | | |
|  | | | | |
| John F searches “harvey norman pressure cooker au” | Email and Browser – Artifact #5 | | /img\_Narcos-2.001/vol\_7/Users/JohnF/AppData/Local/Microsoft/Windows/WebCache/ WebCacheV01.dat | |
|  | | | | |
|  | | | | |
| John F searches “how to launder money” | Email and Browser – Artifact #6 | | /img\_Narcos-2.001/vol\_7/Users/JohnF/AppData/Local/Microsoft/Windows/WebCache/ WebCacheV01.dat | |
|  | | | | |
|  | | | | |
| John F Visits a website titled “Body Packing – The Internal Concealment of Illicit Drugs” | Email and Browser – Artifact #7 | | /img\_Narcos-2.001/vol\_7/Users/JohnF/AppData/Roaming/Mozilla/Firefox/Profiles/fj248tbu.default/places.sqlite | |
|  | | | | |
|  | | | | |
| John F Visits a website titled “Concealment Packs and Bags | CCW Bags” | Email and Browser – Artifact #8 | | /img\_Narcos-2.001/vol\_7/Users/JohnF/AppData/Roaming/Mozilla/Firefox/Profiles/fj248tbu.default/places.sqlite | |
|  | | | | |
|  | | | | |
| John F Visits Google Maps Address “3 Pegasus St Inala QLD 4077 Australia” 26 Times | Email and Browser – Artifact #9 | | /img\_Narcos-2.001/vol\_7/Users/JohnF/AppData/Roaming/Mozilla/Firefox/Profiles/fj248tbu.default/places.sqlite | |
|  | | | | |
|  | | | | |
| John F Visits a website titled “How Much Cocaine Can You Fit In Your, Ahem, Body” | Email and Browser – Artifact #10 | | /img\_Narcos-2.001/vol\_7/Users/JohnF/AppData/Roaming/Mozilla/Firefox/Profiles/fj248tbu.default/places.sqlite | |
|  | | | | |
|  | | | | |
| Steve K Visits a website titled “Security – Encrypting Downloads” | Email and Browser – Artifact #11 | | /img\_Narcos-1.001/vol\_vol7/Users/Steve/AppData/Local/Google/Chrome/User Data/Default/History | |
| Graphical user interface, text, application, email  Description automatically generated | | | | |
|  | | | | |
| Steve K visits a site called “Best places to trade drugs” | | Email and Browser – Artifact #12 | | /img\_Narcos-1.001/vol\_vol7/Users/Steve/AppData/Local/Google/Chrome/User Data/Default/History |
| Text  Description automatically generated with medium confidence | | | | |
|  | | | | |
| Steve K visits a site called “drug routes in wellington” | | Email and Browser – Artifact #13 | | /img\_Narcos-1.001/vol\_vol7/Users/Steve/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat |
| A picture containing graphical user interface  Description automatically generated | | | | |
|  | | | | |
| Steve K visits a site called “cutting drugs” | | Email and Browser – Artifact #14 | | /img\_Narcos-1.001/vol\_vol7/Users/Steve/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat |
| A picture containing text  Description automatically generated | | | | |
|  | | | | |
| Steve K visits a site called “Image Steganography Download” | | Email and Browser – Artifact #15 | | /img\_Narcos-1.001/vol\_vol7/Users/Steve/AppData/Local/Google/Chrome/User Data/Default/History |
| Text, letter  Description automatically generated | | | | |
|  | | | | |
| Steve K Meth | Images – Artifact #1 | | /img\_Narcos-1.001/vol\_vol7/Users/Steve/Pictures/620x349.jpg | |
| A picture containing paper, wrapped, plastic  Description automatically generated | | | | |
|  | | | | |
| Steve K Biker Vests | Images – Artifact #2 | | /img\_Narcos-1.001/vol\_vol7/Users/Steve/Pictures/620x349.jpg /eight\_col\_patches\_crp.jpg | |
| A picture containing text  Description automatically generated | | | | |
|  | | | | |
| Steve K Drugs and Money | Images – Artifact #3 | | /img\_Narcos-1.001/vol\_vol7/Users/Steve/Pictures/price-meth-bust-4.jpg | |
| A picture containing text, indoor, wooden  Description automatically generated | | | | |
|  | | | | |
| John F Shipping Label | Images – Artifact #4 | | /img\_Narcos-2.001/vol\_7/Users/JohnF/Documents/Business/shipping.PNG | |
|  | | | | |
|  | | | | |
| John F Flight Ticket | Images – Artifact #5 | | /img\_Narcos-2.001/vol\_7/Users/JohnF/Documents/Business/Steve K.PNG | |
|  | | | | |
|  | | | | |
| John F photo of Jane’s Kids | Images – Artifact #6 | | /img\_Narcos-2.001/vol\_7/Users/JohnF/AppData/Local/Temp/vmware-JohnF/VMwareDnD/a7dfe109/Janes Kids.jpg | |
|  | | | | |
|  | | | | |
| Jane E Police badge image | Images – Artifact #7 | | /img\_Narcos-3.001/vol\_vol7/Users/JaneE/Pictures/background.jpg | |
|  | | | | |
| Steve K GPS route of drug routes | Images – Artifact #8 | | /img\_Narcos-1.001/vol\_vol7/Users/Steve/AppData/Local/Packages/Microsoft.ScreenSketch\_8wekyb3d8bbwe/TempState/(35628D63-554D-4654-BA8F-DEF067313F361).png | |
| Graphical user interface  Description automatically generated with medium confidence | | | | |
| Steve K GPS route to Airport | Images – Artifact #9 | | /img\_Narcos-1.001/vol\_vol7/Users/Steve/AppData/Local/Packages/Microsoft.ScreenSketch\_8wekyb3d8bbwe/TempState/(D0ECD46B-96DB-49E0-8187-555D488B1B40).png | |
| Graphical user interface, application, website  Description automatically generated | | | | |
| |  |  |  | | --- | --- | --- | | John F packaged concealment bag | Images – Artifact #10 | /img\_Narcos-1.001/vol\_vol7/Users/JohnF/AppData/Local/Temp/vmware-JohnF/VMwareDnD/770cd05f/package.jpg | | | | | |