

Narcos 2019

Digital Forensics Report

Prepared by:

Niccolo Arboleda

Table of Contents

1 Introduction.....	2
1.1 Scenario.....	2
2 Forensics Examination.....	2
2.1 Tools.....	3
2.2 Evidence Classes.....	3
2.2.1 Evidence Class 1 - Narcos-1.001.....	3
2.2.2 Evidence Class 2 - Narcos-2.001.....	6
2.2.3 Evidence Class 3 - Narcos-3.001.....	6
2.2.4 Combined Evidence.....	6
3 Summary and Conclusions.....	7

Disclaimer:

The characters and the scenario in this report are fictional. This paper is only intended for research purposes and as a personal project.

1. Introduction

This report provides corroborative evidence of the connection between Jane Esteban, John Fredericksen, and Steve K. There is also evidence pointing to why they were going to meet up in Wellington and their plans.

1.1 Scenario

Due to intelligence provided by the Australian government, two passengers were intercepted by Customs upon arriving at Wellington, New Zealand from Brisbane. The Intel provided stated that Jane Esteban and John Fredricksen may be involved in illegal activity.

The suspects were searched by a customs officer. John Fredricksen's baggage consisted of clothing, toiletries and a Windows laptop. Jane Esteban's baggage also consisted of clothing, toiletries and a small windows laptop.

Upon further search of the lining of John Fredricksen's suitcase, one kilogram of Methamphetamine was located. Both suspects were taken into separate interview rooms where they were interrogated. John Fredricksen refused to answer any questions.

Jane Esteban stated all she knew and that she had to deliver the suitcase to the *Eastbourne library* but if all else failed then they were to deliver it to 666 Rewera Avenue, Petone as told by John Fredricksen.

Customs and police subsequently raided that address. There was nobody present at the address. Customs did, however, find drugs, guns and a desktop computer in the living room of the suspect's house.

You are a Customs forensics investigator. Customs officers have delivered a forensic image and memory dump of the suspect's desktop computer to you. Your task is to determine the relationship between John Fredrickson and the suspect, their future intentions and any other supporting evidence that pertains to the case.

Source: *2019 Narcos – Digital Corpora*. (n.d.).

<https://digitalcorpora.org/corpora/scenarios/2019-narcos/>

2. Forensic Examination

The examination uses the image files found in the two laptops at the airport and the desktop at 666 Rewera Avenue.

2.1 Tools

The forensic tool used in this investigation is Autopsy 4.21.0. It is an open-source forensics software that collects data artifacts from computer hard drives.

2.2 Evidence Classes

Evidence Class	Description	Type
1	The image extracted from the desktop at 666 Rewera Avenue (Narcos-1.001)	Windows image file
2	The image extracted from John Fredricksen's laptop (Narcos-2.001)	Windows image file
3	The image extracted from Jane Esteban's laptop (Narcos-3.001)	Windows image file

2.2.1 Evidence Class 1 - Desktop Image

Exhibit A



A deleted file in the desktop image named price-meth-bust-4.jpg shows a picture of money and narcotics on a table.

Exhibit B



A deleted file named 620x349.jpg shows a crystalized substance in small plastic bags.

Exhibit C

Type	Value
Name	SK-DESKTOP
Program Name	Windows 10 Pro
Processor Architecture	AMD64
Temporary Files Directory	%SystemRoot%\TEMP
Path	C:\Windows
Product ID	00330-80000-00000-AA502
Owner	Steve
Source File Path	/img_Narcos-1.001
Artifact ID	-9223372036854775642

Operating System information revealed the name of the desktop owner. Steve K.

Exhibit D

History			google.com	crystal meth	Google Chrome	2019-01-30 21:56:24 EST	Narcos-1.001
History			google.com	crystal meth	Google Chrome	2019-01-30 21:56:24 EST	Narcos-1.001
History			google.com	crystal meth	Google Chrome	2019-01-30 21:56:30 EST	Narcos-1.001
History			google.com	crystal meth	Google Chrome	2019-01-30 21:56:33 EST	Narcos-1.001
History			google.com	drug paraphernalia	Google Chrome	2019-01-30 21:57:16 EST	Narcos-1.001
History			google.com	drug paraphernalia	Google Chrome	2019-01-30 21:57:21 EST	Narcos-1.001
History			google.com	drug paraphernalia	Google Chrome	2019-01-30 21:57:21 EST	Narcos-1.001
History			google.com	drug paraphernalia	Google Chrome	2019-01-30 21:57:21 EST	Narcos-1.001
History			google.com	drug paraphernalia	Google Chrome	2019-01-30 21:57:26 EST	Narcos-1.001
History			google.com	drug paraphernalia	Google Chrome	2019-01-30 21:57:30 EST	Narcos-1.001
History			google.com	drug paraphernalia	Google Chrome	2019-01-30 21:57:37 EST	Narcos-1.001
History			google.com	drug paraphernalia meth	Google Chrome	2019-01-30 21:57:50 EST	Narcos-1.001
History			google.com	drug paraphernalia meth	Google Chrome	2019-01-30 21:57:50 EST	Narcos-1.001
History			google.com	drug paraphernalia meth	Google Chrome	2019-01-30 21:57:50 EST	Narcos-1.001
History			google.com	drug paraphernalia meth	Google Chrome	2019-01-30 21:58:03 EST	Narcos-1.001
History			google.com	gangs nz drugs	Google Chrome	2019-01-30 21:59:17 EST	Narcos-1.001
History			google.com	gangs nz drugs	Google Chrome	2019-01-30 21:59:32 EST	Narcos-1.001
History			google.com	gangs nz drugs	Google Chrome	2019-01-30 21:59:32 EST	Narcos-1.001
History			google.com	gangs nz drugs	Google Chrome	2019-01-30 21:59:32 EST	Narcos-1.001
History			google.com	stuff nz	Google Chrome	2019-01-31 16:11:34 EST	Narcos-1.001
History			google.com	metservice	Google Chrome	2019-01-31 16:25:55 EST	Narcos-1.001
History			google.com	cric info	Google Chrome	2019-01-31 16:26:40 EST	Narcos-1.001
History			google.com	all blacks	Google Chrome	2019-01-31 16:32:55 EST	Narcos-1.001
History			google.com	protonmail	Google Chrome	2019-01-31 19:12:20 EST	Narcos-1.001
History			google.com	image steganography download	Google Chrome	2019-01-31 19:15:04 EST	Narcos-1.001
History			google.com	wind patterns	Google Chrome	2019-02-01 16:37:08 EST	Narcos-1.001
History			google.com	all blacks	Google Chrome	2019-02-01 16:43:06 EST	Narcos-1.001
History			google.com	all blacks	Google Chrome	2019-02-01 16:43:06 EST	Narcos-1.001
History			google.com	best places to trade drugs	Google Chrome	2019-02-01 20:01:34 EST	Narcos-1.001
History			google.com	best places to trade drugs	Google Chrome	2019-02-01 20:01:34 EST	Narcos-1.001
History			google.com	best places to trade drugs	Google Chrome	2019-02-01 20:01:34 EST	Narcos-1.001
History			google.com	wellington libraries	Google Chrome	2019-02-01 20:01:51 EST	Narcos-1.001
History			google.com	courteney place	Google Chrome	2019-02-01 20:02:51 EST	Narcos-1.001
History			google.com	eastbourne library	Google Chrome	2019-02-01 20:04:36 EST	Narcos-1.001
History			google.com	eastbourne	Google Chrome	2019-02-01 20:05:05 EST	Narcos-1.001
History			google.com	eastbourne library	Google Chrome	2019-02-01 20:05:11 EST	Narcos-1.001

The desktop image has traces of search history looking at the rendezvous point or Eastbourne on google maps and searches for meth and drug paraphernalia. There are also searches for drug routes in Wellington and which gangs are affiliated with them in the area.

Note: Steganography was also searched, which may mean other pictures have embedded messages.

2.2.2 Evidence Class 2 - Laptop image of Jason Fredericksen

Exhibit E

spartan.edb		1	https://www.wisebread.com/how-to-launder-money	How to Launder Money
spartan.edb		1	http://www.lions.com.au/news	News & Media - lions.com.au
spartan.edb		1	https://www.reddit.com/r/addiction/comments/ajxak...	People who don't suffer from ad
spartan.edb		1	https://www.youtube.com/watch?v=wyOanzl-WFs	1829-05-05 11:52:31 PM
spartan.edb		1	https://www.wisebread.com/how-to-launder-money	How to Launder Money

Web bookmarks revealed the suspect was looking at information on how to launder money.

Exhibit F

Steve K.Ink			C:\Users\JohnF\Documents\Business\Steve K.PNG	2019-02-01 17:43:21 EST	Narcos-2.001
-------------	--	--	---	-------------------------	--------------

The suspect has files connecting him to Steve K.

2.2.3 Evidence Class 3 - Laptop image of Jane Esteban

Exhibit G

SYSTEM	1	2019-01-30 22:04:08 EST	Seagate RSS LLC	Backup Plus Slim Portable Drive 1 TB	MSFT30NA9LP8HF	Narcos-1.001
SYSTEM	1	2019-01-28 23:15:55 EST	Seagate RSS LLC	Backup Plus Slim Portable Drive 1 TB	MSFT30NA9LP8HF	Narcos-3.001

According to USB device information, Jane Esteban passed a portable drive to Steven K between January 28 and 30. The device ID of the drive is identical on both images.

2.2.4 Combined Evidence from All Classes

Exhibit H

SYSTEM	1	2019-02-01 22:02:28 EST	Western Digital Technologies, Inc.	Elements Portable (WDBUZG)	57584D3145373444574D314E	Narcos-3.001
SYSTEM	1	2019-02-01 21:56:41 EST	Western Digital Technologies, Inc.	Elements Portable (WDBUZG)	57584D3145373444574D314E	Narcos-2.001
SYSTEM	1	2019-01-31 21:41:46 EST	Western Digital Technologies, Inc.	Elements Portable (WDBUZG)	57584D3145373444574D314E	Narcos-1.001













USB device information revealed that a portable drive was shared between the suspects between the dates of January 31 and February 1. The device ID of the drive is identical on all images.

Exhibit I

</> Skype_Call_Dialing.m4a				2015-06-16 09:59:25 EDT	2015-06-16 09:59:25 EDT	Narcos-2.001
</> Skype_Call_Ended.m4a				2015-06-16 09:59:25 EDT	2015-06-16 09:59:25 EDT	Narcos-2.001
</> Skype_Call_Dialing.m4a				2015-06-16 09:59:25 EDT	2015-06-16 09:59:25 EDT	Narcos-1.001
</> Skype_Call_Ended.m4a				2015-06-16 09:59:25 EDT	2015-06-16 09:59:25 EDT	Narcos-1.001
</> Skype_Call_Dialing.m4a				2015-06-16 09:59:25 EDT	2015-06-16 09:59:25 EDT	Narcos-3.001
</> Skype_Call_Ended.m4a				2015-06-16 09:59:25 EDT	2015-06-16 09:59:25 EDT	Narcos-3.001

Process data from the drives show that all the suspects were in contact with each other through Skype going back to 2015. The time stamps from the Skype calls are identical to the second.

Exhibit J

List Name	Files with Hits
 666 Rewera Avenue (2)	2
 Eastbourne (34)	34
 Jane (3670)	3670
 Jane Esteban (4)	4
 John (515)	515
 New Zealand (1092)	1092
 Petone (63)	63
 Wellington (1262)	1262
 drugs (684)	684
 library (56619)	56619
 meth (53255)	53255
 methamphetamine (134)	134

A keyword search using the information extracted from the suspects suggests that they have collaborated with each other.

3. Summary and Conclusions

The evidence shows that the suspects were in collaboration with one another in the handling and selling of illegal narcotics from at least 2015 to 2019.

The evidence also suggests that they were planning to start a business in Wellington to launder the money they were making from selling drugs and expand their infrastructure using local trade routes.

Sources:

File Images and Scenarios are from Digital Corpora.

2019 Narcos – Digital Corpora. (n.d.). <https://digitalcorpora.org/corpora/scenarios/2019-narcos/>