ICT378 TJD 2025

Cyber Forensics and Incident Response

Final Assignment

Date: 31/3/25

Submitted by: Bhargav Raj Dutta

Student ID: 34834517

Table of Contents

Executive Summary of the Report

This report includes a detailed analysis of a digital forensic investigation that was conducted on the evidence that were acquired at the Airport which were related to a drug smuggling case and the case has two suspects at first who are John Fredricksen and Jane Esteban. This investigation was started when the suspects were intercepted by New Zealand customs, and they came from Brisbane. When their bags were inspected by the officials, they found 1 kg of methamphetamine drug that was hidden in Jane's luggage. After discovery of narcotic substance both threat actors were detained and interviewed more on this. From Jane officials got to know that the drugs package was planned to be delivered to either Eastbourne Library or to 666 Rewera Avenue, Petone. When police made a raid at Petone they found more drugs, firearms and a desktop PC. The forensic and memory images of the suspects laptops and desktops were submitted for investigation to find more about the drug trafficking case and with more investing police found a third suspect by the name of Steve Kowhai.

A forensic approach was done from start so that the chain of custody is maintained, and no one can alter the chain of custody that started by safely acquiring data from the seized devices. Also, the hash values are also calculated for the files before and after the investigation so that we can make sure that no hashes have been altered. FTK imager was used to make image files of the files that are in dump form or in other format and to make copy of the same file while the original content remains unaltered. Each of the image files are analyzed via Autopsy and Magnet axiom that showed a lot of hidden information such as images, pdf docx, web history etc. and a lot of hidden information. This methodology was applied to gather as much information as possible. By following this we can conduct fair investigation and present the chain of evidence in court.

The evidence that was collected were preserved as well. The hash values of the images were calculated before and after the investigation to check the principle of data integrity. The memory dumps were recovered from a live system to capture live activities of the system. The chain of custody is also maintained, and copies of the images are used to analyze and gather information. Forensic tools such as Autopsy, FTK imager, magnet axiom, OS forensics were used to perform the investigation.

This forensic investigation provided us a detailed information of the suspects, their personal details such as files they have, app they used, systems they used, how they used to communicate, also their mode of communication

Some of the Key Findings were

- **Chats of John and Steve using Discord and talking about drugs**
- **An image that has hidden information about drugs information**
- **Email history, download history and web search of the suspects**
- **Jane identity as an undercover cop**
- **Images of drugs and money**
- **Google search about Drugs and how to smuggle it**
- **Files of the suspects as well that was recovered from Jane and Steve**
- **Flight Tickets**
- **Antivirus used**
- **Several images that can be used against them**
- **Encrypted Files**

Methodology

The methodology that I followed is that 1st I calculated the hash values of all the files before the investigation and, I checked the hash value after I finished the investigation once the hash value is still the same and they are not altered as well so the principle of integrity is maintained. For example, the hash value for Narcos 1 was **996182c381ec9e7025f40519107615e4** before the investigation and after the investigation the value was the exact same and nothing was altered

To start with the investigation the windows operating system was used and the tools that were used are Autopsy. A VM environment was created to perform the steps where I set up a window 11 VM with a shared folder with the host machine. Now to start with the investigation I downloaded all the files online and each of them were 8,9 GB in size and moreover that files that I downloaded I started the process of investigation one by one. 1st I selected the Steve image file that was recovered from the Narcos 1 file. I used autopsy tool for this part where I clicked on create a new case, named the case as Steve image file and then I browsed the file that I just unzipped. Now once I selected the file autopsy then start analyzing its contents once Autopsy analyzed the contents of the file, I could see all the information of Steve such as images, documents, web search and a lot. I followed the same procedure for all the other files as well and collected as much evidence as I could and, I have attached the images accordingly so that they can be used by investigators later if it goes to court. So, for Narcos 2, 3 I did the same process of extracting it and checking all the contents of each file one by one. To save important files and data I simply extracted the data to my work folder.

The detailed steps that were followed are

- I checked the MD5 hash value of the images for image integrity
- Then also I Identified all the file systems and the partitions that are on the file
- Moreover, I tried to recover all the files that are deleted as well to find important evidence.
- Then once this is done then I tried to identify different user profiles
- After that Checked the devices that they used and matched if the id of those devices if they are the admin of the device
- Checked all the web history and time stamps of their activities online

- I also Found out that they used discord and proton mail to communicate
- then I analyzed their Web activity and got their browser history, checked their cookies and cache and gathered important evidence against them
- Then I moved on to Document Analysis where I found some pdf documents, some word files, I also extracted the meta data and moreover I got a lot of important docx here
- Then I analyzed the images from all the suspects and found our images related to drugs, flight ticket bookings and much more that were important for the investigation
- Then after analyzing as much meta data as I can I documented the same process as well.
- I saved the list of evidence by saving them in my work folder

So, these were the steps that I followed for the forensic investigation. There was a lot of information from each of these files so some of the best practices that I followed are I used keywords to find evidence related to the case and I used keywords such as drugs, meth, etc. that help me to gather a lot of information. The reason for using Autopsy over magnet axiom is that 1st of all it is open source as we know that Magnet axiom is a proprietary software and is used in real forensics investigation but in case of autopsy its compatible with even Linux and I used it on my windows Laptop. When I used autopsy, it didnt take much time to load the files and I had gathered as much evidence as I can. While axiom is a strong software that can be used particularly for finding information about the emails and chats that were done between the suspects. So, these were some differences between the two tools. By following the methodology above I was able to make this report and gather sufficient evidence against all the three suspects.

1) Identify relevant user account profiles and computer names associated with the suspect's computers

Suspect 1: Steve Kowhai

So, when Steve data was being analyzed his computer details are found such as user id, device id, OS id, processor type etc. The devices are named as SK -Desktop and it was a windows 10 pc.

image 1.1

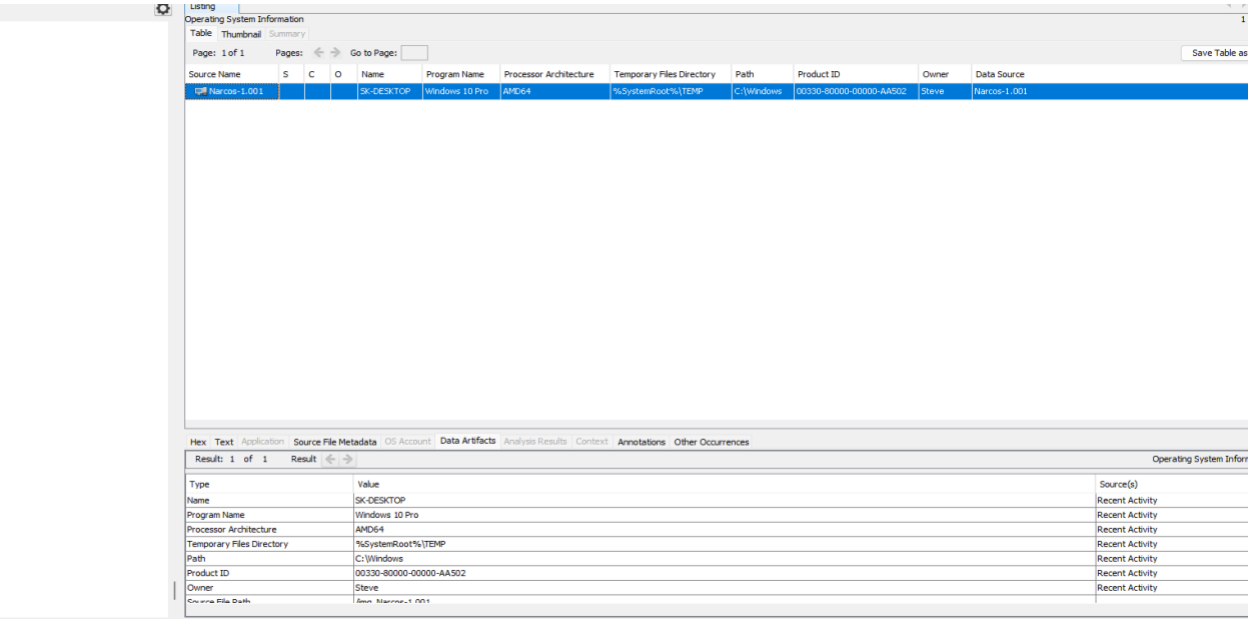


Figure 1.1

This image 1.1 shows us that the computer system that was found by police at the location mentioned by Jane had a desktop and it belongs to Steve Kowhai. It is named as SK-DESKTOP. It is a windows 10 PC with AMD 64 processor and the owner is Steve here.

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-80-956008885-3418522649-1831038044-185329			0		Narcos-1.001_1 Host	Local	NT SERVICE	
S-1-5-18				SYSTEM	Narcos-1.001_1 Host	Local	NT AUTHORITY	
S-1-5-19				LOCAL SERVICE	Narcos-1.001_1 Host	Local	NT AUTHORITY	
S-1-5-80-3028837079-3186095147-955107200-370196			0		Narcos-1.001_1 Host	Local	NT SERVICE	
S-1-5-20				NETWORK SERVICE	Narcos-1.001_1 Host	Local	NT AUTHORITY	
S-1-5-21-1474204758-2504895174-1356074821-1001			0	Steve	Narcos-1.001_1 Host	Domain		2019-01-28 23:35:06 GST
S-1-5-21-1474204758-2504895174-1356074821-1000			0		Narcos-1.001_1 Host	Domain		
S-1-5-80-2620923248-4247863784-3378508180-26591			0		Narcos-1.001_1 Host	Local	NT SERVICE	
S-1-5-21-397955417-626881126-188441444-4882392			0		Narcos-1.001_1 Host	Domain		
S-1-5-21-1474204758-2504895174-1356074821-500			0	Administrator	Narcos-1.001_1 Host	Domain		2019-01-28 23:15:38 GST
S-1-5-21-1474204758-2504895174-1356074821-501			0	Guest	Narcos-1.001_1 Host	Domain		2019-01-28 23:15:38 GST
S-1-5-21-1474204758-2504895174-1356074821-503			0	DefaultAccount	Narcos-1.001_1 Host	Domain		2019-01-28 23:15:38 GST
S-1-5-21-1474204758-2504895174-1356074821-504			0	WDAGUtilityAccount	Narcos-1.001_1 Host	Domain		2019-01-28 23:15:38 GST

Figure 1.2

Image 1.2

Now in the image 1.2 we can see that device id S-1-5-21 the number is matching with the admin id as the number is same with the id number of Steve so from this, we get to know that this computer was used by Steve.

As per the images above we can see that Steve used the PC and he has named it as SK Desktop.

Suspect 2: John

When John's memory image was examined using autopsy then his information about the devices, he used to be revealed such as Operating system, system id, which devices has admin access

image 1.3 John's Laptop id details could be seen such as it was a laptop with amd 64 and Windows 10 pro OS. It is named as JohnFLaptop

Image 1.3

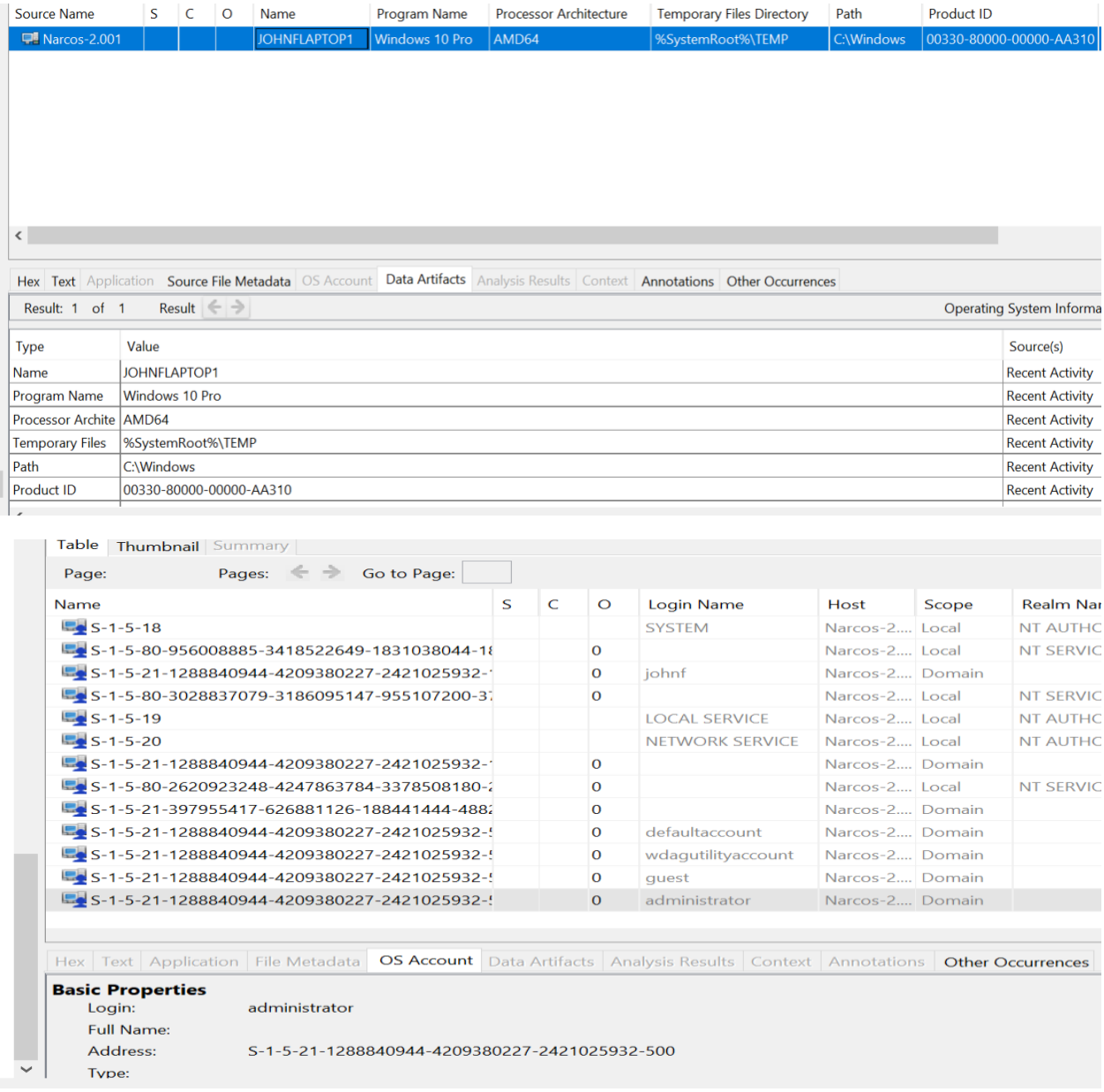


Image 1.4 This image shows us the device id that john used, and the computer used by john has the admin access as well, so it means that john was the admin of the devices.

Suspect: Jane

When Jane image files were analyzed then we got to know that the devices Jane used, what was the operating system, the device id and way more.

Image 1.5

From image 1.5 we can see that Jane has the same device id as admin, moreover its scope is domain, and this proves that jane has the admin access of the device.

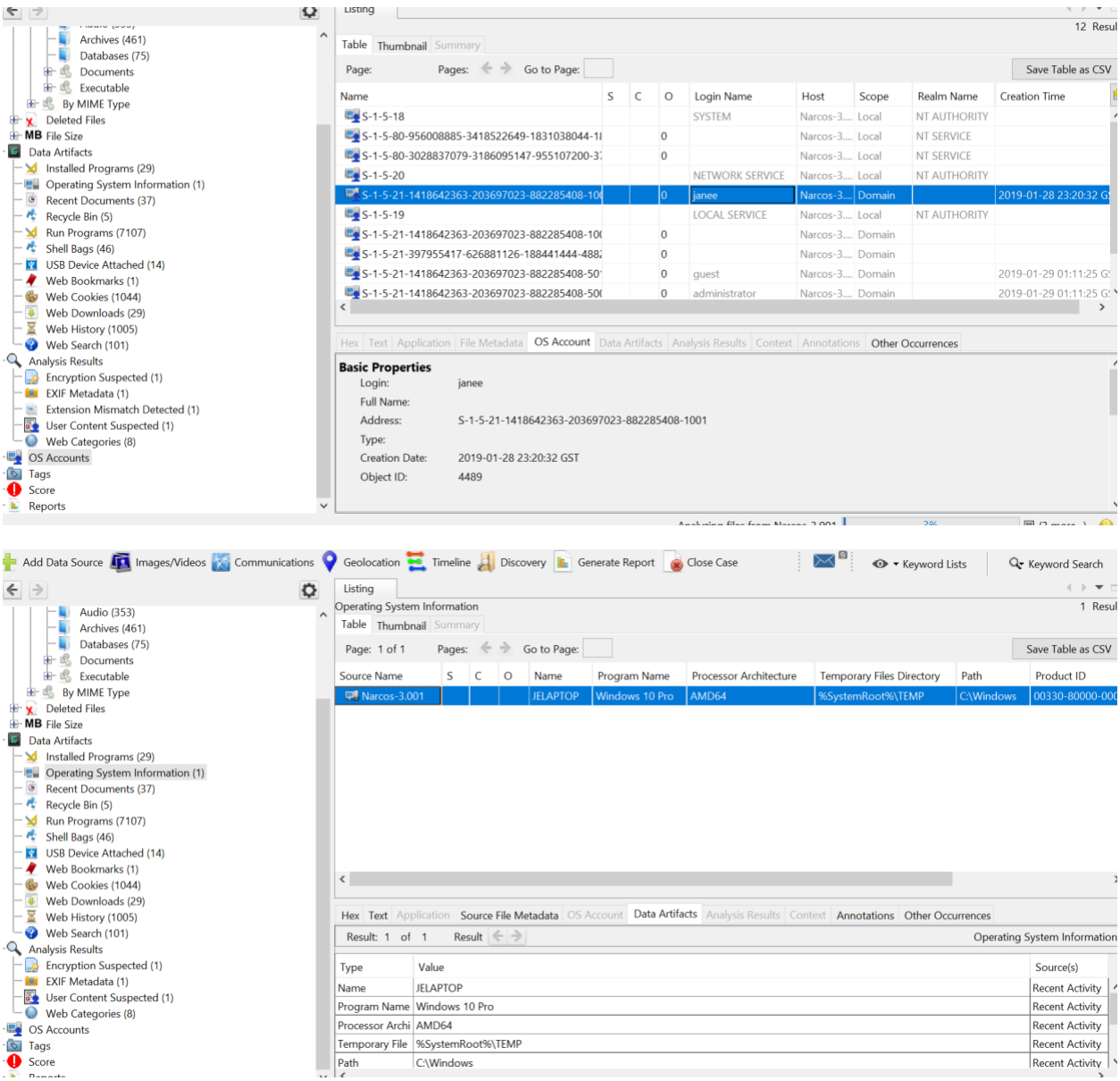


Image 1.6

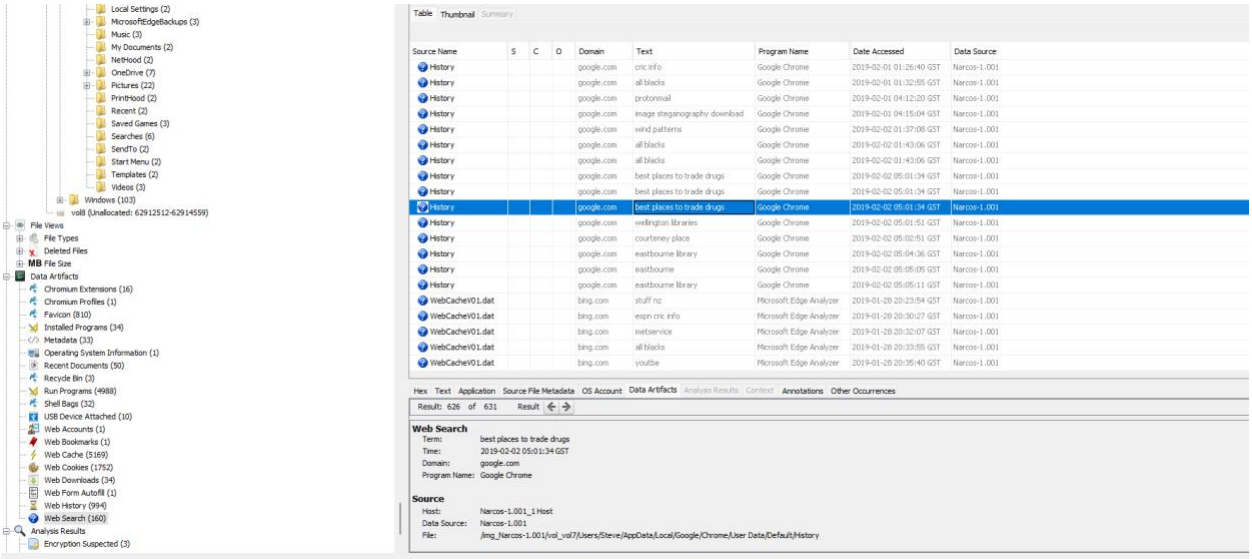
This image 1.6 shows the name of Jane computer as JELAPTOP and the OS is windows 10 pro, the processor is amd64.

2) Identify the roles of each suspect

Suspect: Steve Kowhai

These images below show the web searches of Steve where he searched about the best places to trade drugs, how to do money laundering and how to cut drugs. We can say he is a suspect as he also researched about how to use steganography tools, also his searches about drugs crystal meth. It looks like Steve role was to find information about the drugs and other activities that are related to it.

Image 2.1 This image shows the web search of Steve kowhai where he searched about places to trade drugs and his user agent was google chrome



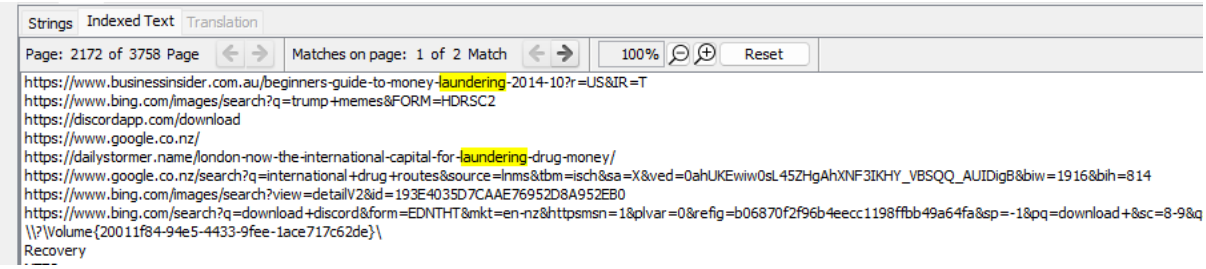


Image 2.2 This image shows Steve's search history on how to do money laundering

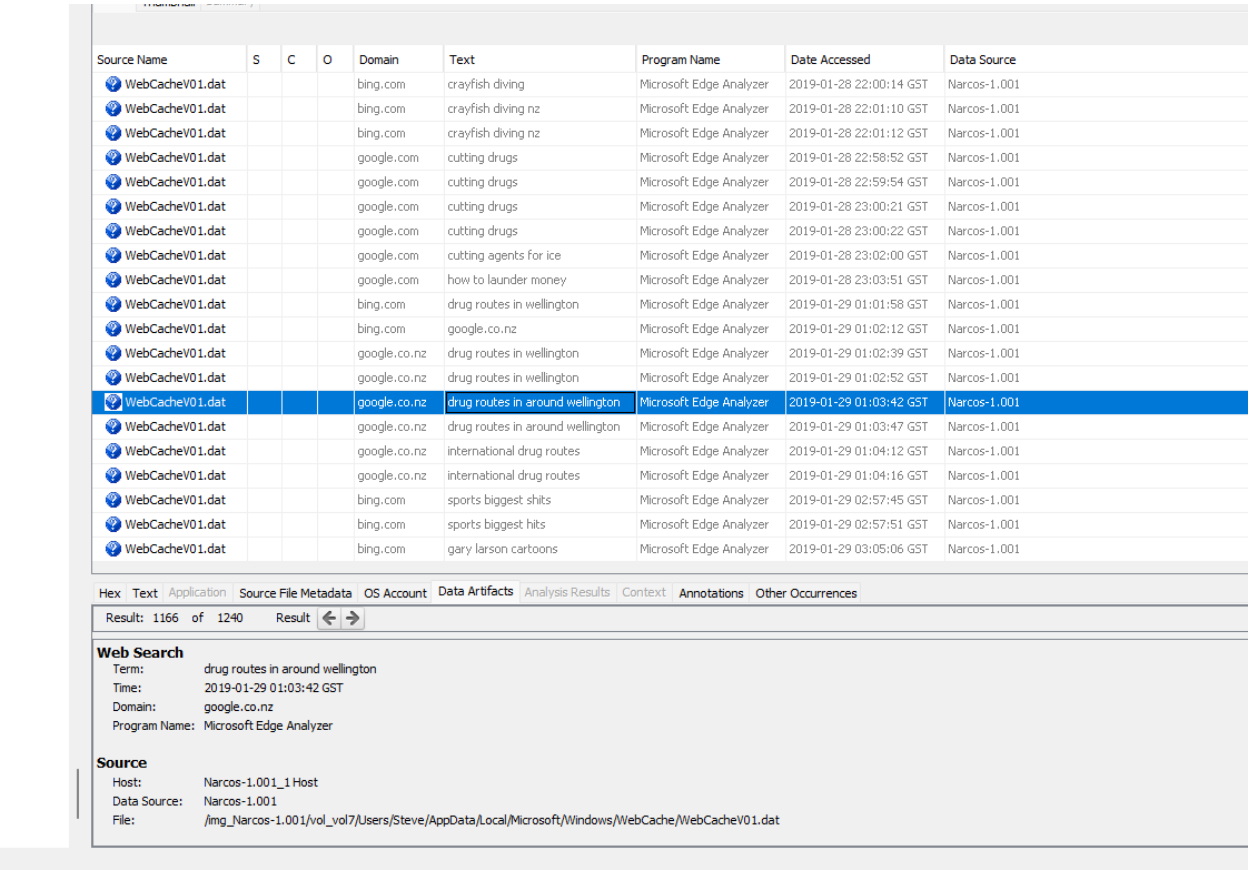


Image 2.3 it shows his searches for crayfish diving in New Zealand, how to cut drugs, also he searches about the international drug routes as well.

Image 2.4 Steve searches for image steganography tool which is simply used to hide information inside an image.

History	google.com	image steganograph	Google Chrome	2019-02-01 04:15:04	Narcos-1.001
History	google.com	wind patterns	Google Chrome	2019-02-02 01:37:08	Narcos-1.001
History	google.com	all blacks	Google Chrome	2019-02-02 01:43:06	Narcos-1.001

Image 2.5 This image shows his searches about crystal meth and drugs paraphernalia

23	History	google.com	crystal meth	Google Chrome	2019-01-31 06:56:24	Narcos-1.001
24	History	google.com	crystal meth	Google Chrome	2019-01-31 06:56:24	Narcos-1.001
25	History	google.com	crystal meth	Google Chrome	2019-01-31 06:56:30	Narcos-1.001
26	History	google.com	crystal meth	Google Chrome	2019-01-31 06:56:33	Narcos-1.001
27	History	google.com	drug paraphernalia	Google Chrome	2019-01-31 06:57:16	Narcos-1.001
28	History	google.com	drug paraphernalia	Google Chrome	2019-01-31 06:57:21	Narcos-1.001
29	History	google.com	drug paraphernalia	Google Chrome	2019-01-31 06:57:21	Narcos-1.001
30	History	google.com	drug paraphernalia	Google Chrome	2019-01-31 06:57:21	Narcos-1.001

Suspect: John F

These images below show us about the google searches, evidence that john is also a suspect in this drug case. As in image 2.6 we can see that john is searching for content like how to cut drugs, how to do money laundering etc. that makes him a suspect in this investigation. These were some of the findings that made him a suspect. Also, he searched about how much drugs he can carry in his body.

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
WebCacheV01.dat				bing.com	drug memes	Microsoft Edge Analyzer	2019-01-28 21:53:45 GST	Narcos-2.001
WebCacheV01.dat				bing.com	drug memes	Microsoft Edge Analyzer	2019-01-28 21:54:18 GST	Narcos-2.001
WebCacheV01.dat				bing.com	drug meme walpaper	Microsoft Edge Analyzer	2019-01-28 21:56:12 GST	Narcos-2.001
WebCacheV01.dat				bing.com	how to cut drugs	Microsoft Edge Analyzer	2019-01-28 23:01:55 GST	Narcos-2.001
WebCacheV01.dat				bing.com	how to cut drugs	Microsoft Edge Analyzer	2019-01-28 23:02:18 GST	Narcos-2.001
WebCacheV01.dat				bing.com	youtube	Microsoft Edge Analyzer	2019-01-28 23:02:33 GST	Narcos-2.001
WebCacheV01.dat				youtube.com	how to cut drugs	Microsoft Edge Analyzer	2019-01-28 23:03:06 GST	Narcos-2.001
WebCacheV01.dat				youtube.com	cutting drugs	Microsoft Edge Analyzer	2019-01-28 23:04:24 GST	Narcos-2.001
WebCacheV01.dat				bing.com	how to launder money	Microsoft Edge Analyzer	2019-01-28 23:07:36 GST	Narcos-2.001
WebCacheV01.dat				bing.com	brisbane lions AFL	Microsoft Edge Analyzer	2019-01-28 23:10:41 GST	Narcos-2.001
WebCacheV01.dat				bing.com	brisbane lions afl	Microsoft Edge Analyzer	2019-01-28 23:11:01 GST	Narcos-2.001
WebCacheV01.dat				bing.com	drugs subreddit	Microsoft Edge Analyzer	2019-01-28 23:13:20 GST	Narcos-2.001
WebCacheV01.dat				bing.com	drugs subreddit	Microsoft Edge Analyzer	2019-01-28 23:17:29 GST	Narcos-2.001
WebCacheV01.dat				bing.com	protonmail	Microsoft Edge Analyzer	2019-01-29 02:10:47 GST	Narcos-2.001
WebCacheV01.dat				bing.com	dhl	Microsoft Edge Analyzer	2019-01-29 03:43:19 GST	Narcos-2.001

Image 2.6 This image above shows us the content searched by john such as cutting drugs, drugs related memes etc.

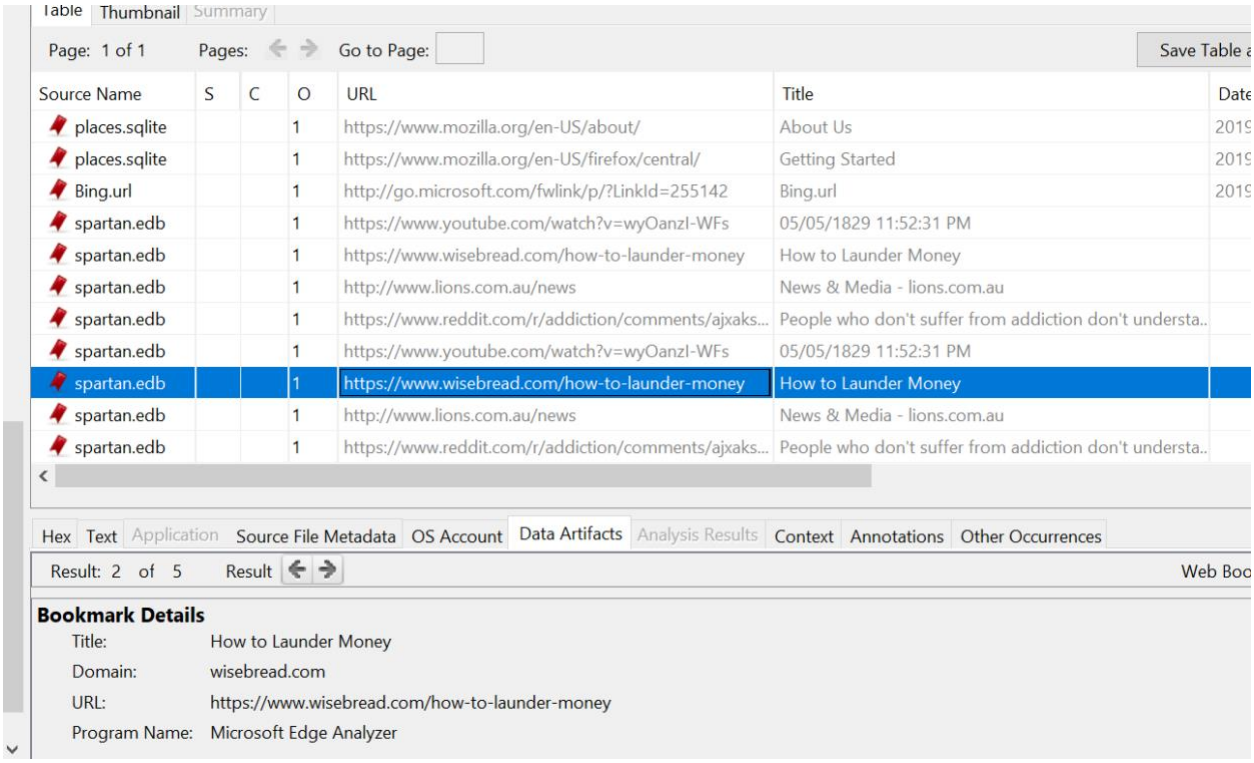


Image 2.7 It shows us the searches that was bookmarked by John on how to do money laundering.

Image 2.8

Details

Name:	cd[Meta]
Date Accessed:	2019-01-31 06:10:28 GST
Date Created:	2019-01-31 06:10:28 GST
Value:	{"title":"FYI: How Much Cocaine Can You Fit In Your, Ahem, Body? | Popular Science"}

Other

Count:	1

John has searched about how much drugs can be fit in the body as well.

Suspect 3: Jane

From images below we got to know that Jane is an undercover cop for the Australian Federal police as we can get know to know the information from her web history where she searched about how to act as a desperate for drug dealing so that the drug dealers don't suspect her as an undercover Cop.

Image 2.9 This image was recovered from Jane files which shows that she was working for the Australian Federal Police.

Image 3.0 This image shows us that jane searched about passing drugs, about methamphetamine and how to act like a drug dealer

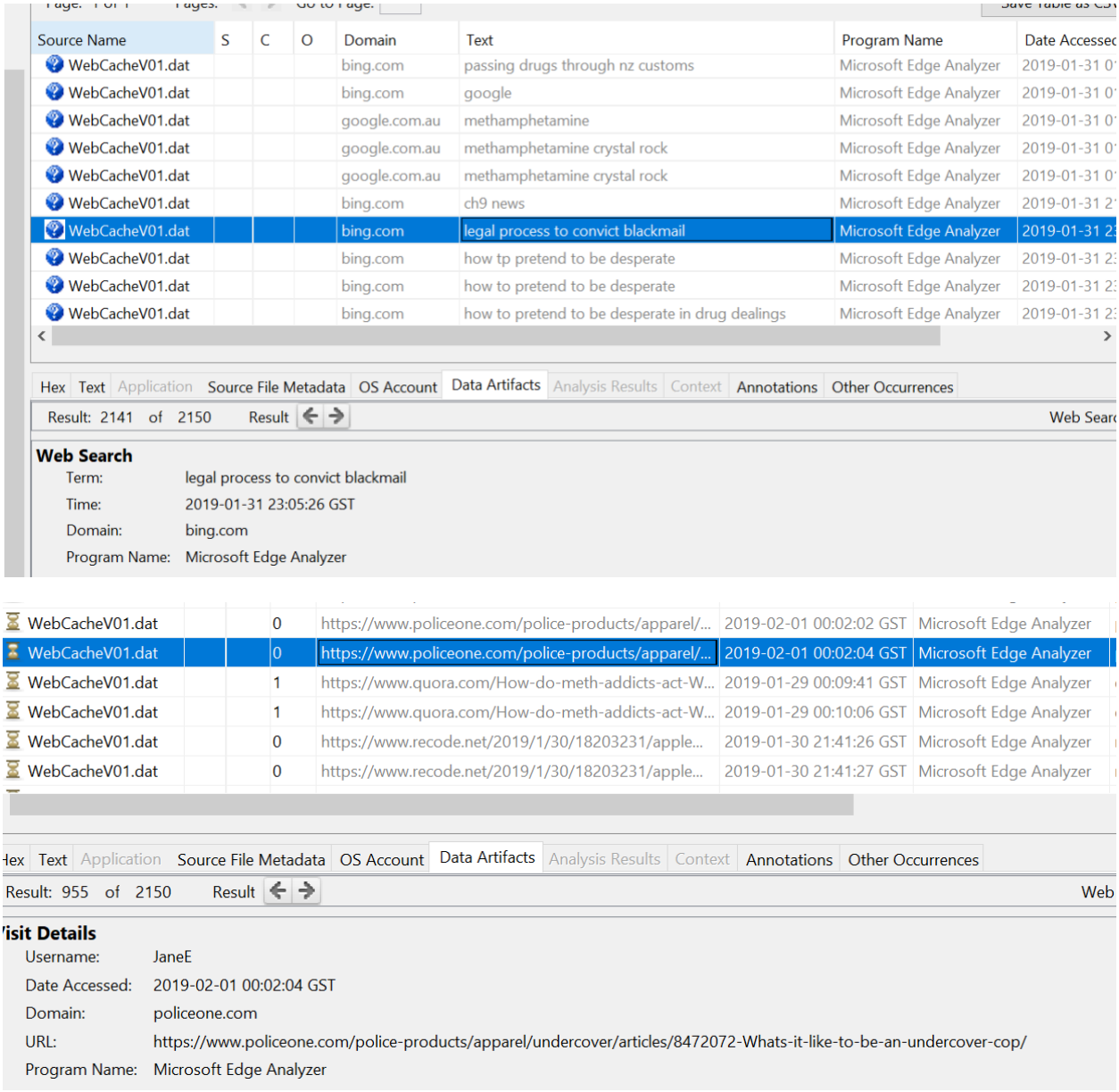


Image 3.1 shows that she searched about how does it feel to be an undercover cop and, we can see other searches about drugs as well.

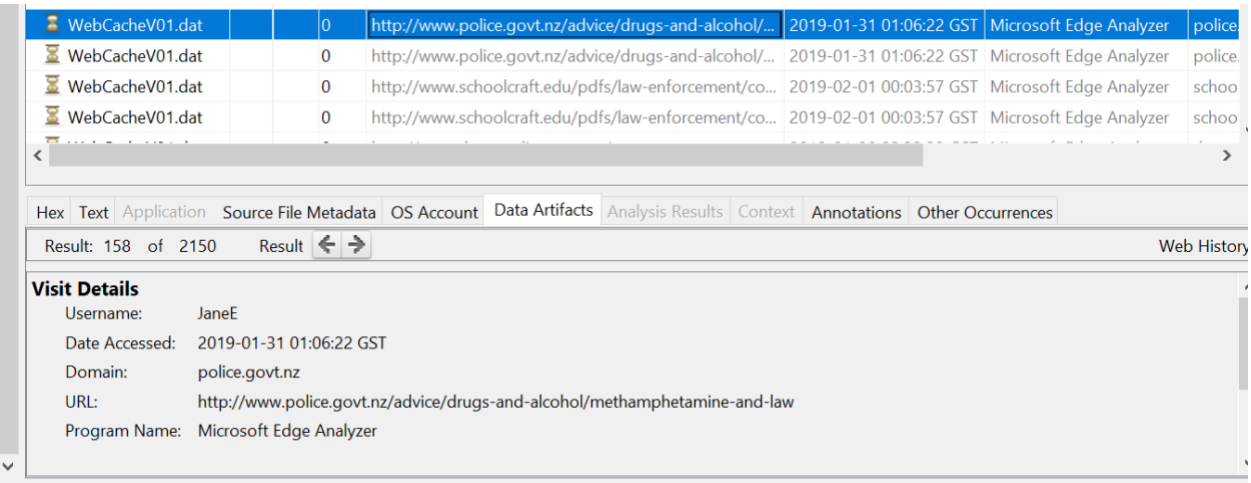
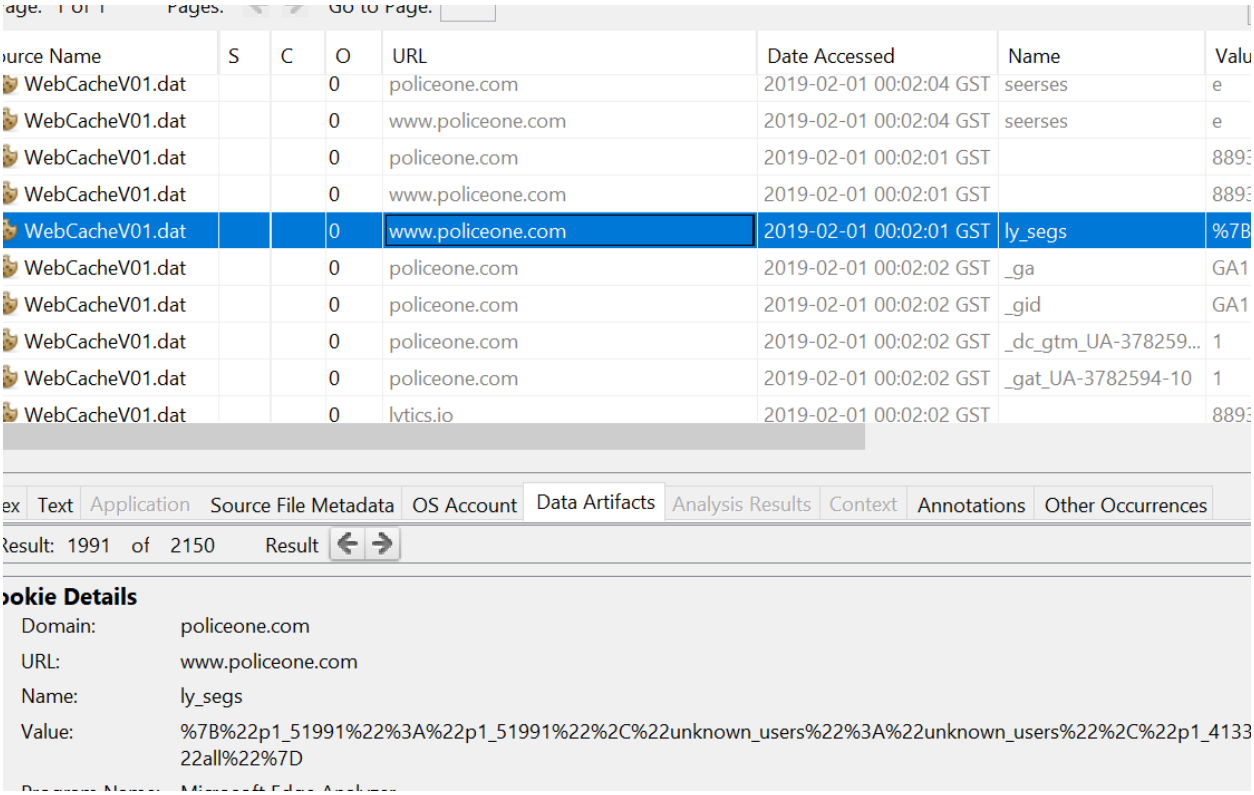


Image 3.2 This image shows us that she visited NZ police website to know about the drugs and rules and regulations

Image 3.3 These cookies session of accessing police sites confirms she was working for Australian police being undercover.



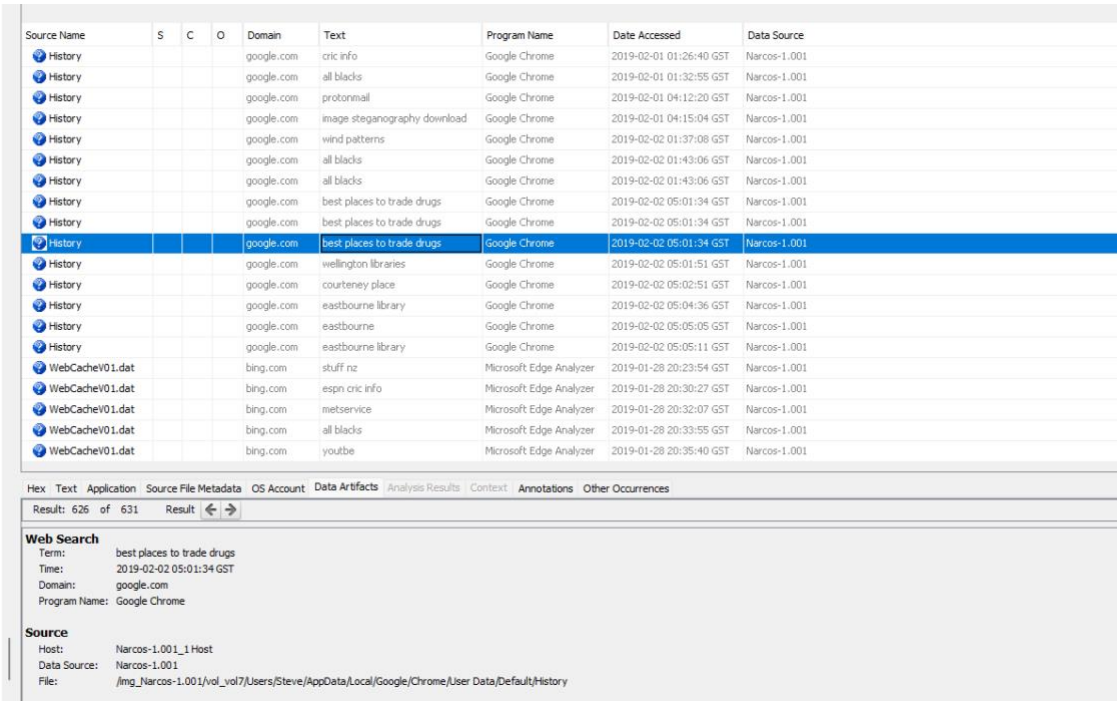
3) Identify relevant web activity on each suspect's computer

Now let’s analyze the web activity of every suspect

Steve’s web activity

Steve searched a lot of data about drugs, how to trade, how to do money laundering, also we can see him downloading image steganography tool to hide information. I have attached some snaps below with evidence of his searches.

Image 3.4 This image shows us the web search history of Steve.



Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
History				google.com	cric info	Google Chrome	2019-02-01 01:26:40 GST	Narcos-1.001
History				google.com	all blacks	Google Chrome	2019-02-01 01:32:55 GST	Narcos-1.001
History				google.com	protonmail	Google Chrome	2019-02-01 04:12:20 GST	Narcos-1.001
History				google.com	image steganography download	Google Chrome	2019-02-01 04:15:04 GST	Narcos-1.001
History				google.com	wind patterns	Google Chrome	2019-02-02 01:37:08 GST	Narcos-1.001
History				google.com	all blacks	Google Chrome	2019-02-02 01:43:06 GST	Narcos-1.001
History				google.com	all blacks	Google Chrome	2019-02-02 01:43:06 GST	Narcos-1.001
History				google.com	best places to trade drugs	Google Chrome	2019-02-02 05:01:34 GST	Narcos-1.001
History				google.com	best places to trade drugs	Google Chrome	2019-02-02 05:01:34 GST	Narcos-1.001
History				google.com	best places to trade drugs	Google Chrome	2019-02-02 05:01:34 GST	Narcos-1.001
History				google.com	wellington libraries	Google Chrome	2019-02-02 05:01:51 GST	Narcos-1.001
History				google.com	courteney place	Google Chrome	2019-02-02 05:02:51 GST	Narcos-1.001
History				google.com	eastbourne library	Google Chrome	2019-02-02 05:04:36 GST	Narcos-1.001
History				google.com	eastbourne	Google Chrome	2019-02-02 05:05:05 GST	Narcos-1.001
History				google.com	eastbourne library	Google Chrome	2019-02-02 05:05:11 GST	Narcos-1.001
WebCacheV01.dat				bing.com	stuff nz	Microsoft Edge Analyzer	2019-01-28 20:23:54 GST	Narcos-1.001
WebCacheV01.dat				bing.com	espn cric info	Microsoft Edge Analyzer	2019-01-28 20:30:27 GST	Narcos-1.001
WebCacheV01.dat				bing.com	metservice	Microsoft Edge Analyzer	2019-01-28 20:32:07 GST	Narcos-1.001
WebCacheV01.dat				bing.com	all blacks	Microsoft Edge Analyzer	2019-01-28 20:33:55 GST	Narcos-1.001
WebCacheV01.dat				bing.com	youtbe	Microsoft Edge Analyzer	2019-01-28 20:35:40 GST	Narcos-1.001

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 626 of 631 Result

Web Search

Term: best places to trade drugs
Time: 2019-02-02 05:01:34 GST
Domain: google.com
Program Name: Google Chrome

Source

Host: Narcos-1.001_1 Host
Data Source: Narcos-1.001
File: /img_Narcos-1.001/vol_vol7/Users/Steve/AppData/Local/Google/Chrome/User Data/Default/History

WebCacheV01.dat	google.co.nz	drug routes in wellin	Microsoft Edge Anal	2019-01-29 01:02:52	Narcos-1.001	
WebCacheV01.dat	google.co.nz	drug routes in aroun	Microsoft Edge Anal	2019-01-29 01:03:55	Narcos-1.001	
WebCacheV01.dat	google.co.nz	drug routes in aroun	Microsoft Edge Anal	2019-01-29 01:03:44	Narcos-1.001	
WebCacheV01.dat	google.co.nz	drug routes in aroun	Microsoft Edge Anal	2019-01-29 01:03:47	Narcos-1.001	
WebCacheV01.dat	google.co.nz	international drug ro	Microsoft Edge Anal	2019-01-29 01:11:15	Narcos-1.001	
WebCacheV01.dat	google.co.nz	international drug ro	Microsoft Edge Anal	2019-01-29 01:09:37	Narcos-1.001	
WebCacheV01.dat	bing.com	sports biggest shits	Microsoft Edge Anal	2019-01-29 02:57:45	Narcos-1.001	
WebCacheV01.dat	bing.com	sports biggest hits	Microsoft Edge Anal	2019-01-29 02:57:51	Narcos-1.001	
WebCacheV01.dat	bing.com	gary larson cartoons	Microsoft Edge Anal	2019-01-29 03:05:06	Narcos-1.001	
WebCacheV01.dat	bing.com	gary larson cartoons	Microsoft Edge Anal	2019-01-29 03:05:18	Narcos-1.001	
WebCacheV01.dat	bing.com	gary larson cartoons	Microsoft Edge Anal	2019-01-29 03:05:11	Narcos-1.001	
WebCacheV01.dat	bing.com	Favorite Gary Larson	Microsoft Edge Anal	2019-01-29 03:05:34	Narcos-1.001	
WebCacheV01.dat	bing.com	gary larson cartoons	Microsoft Edge Anal	2019-01-29 03:08:54	Narcos-1.001	
WebCacheV01.dat	bing.com	gary larson cartoons	Microsoft Edge Anal	2019-01-29 03:09:09	Narcos-1.001	
WebCacheV01.dat	youtube.com	rugby union best hits	Microsoft Edge Anal	2019-01-29 03:09:35	Narcos-1.001	
WebCacheV01.dat	bing.com	gary larson cartoons	Microsoft Edge Anal	2019-01-29 03:13:06	Narcos-1.001	
WebCacheV01.dat	youtube.com	rugby union thugs	Microsoft Edge Anal	2019-01-29 03:13:26	Narcos-1.001	
WebCacheV01.dat	youtube.com	rugby union dirty pla	Microsoft Edge Anal	2019-01-29 03:13:41	Narcos-1.001	
WebCacheV01.dat	bing.com	taxis wellington	Microsoft Edge Anal	2019-01-29 04:27:46	Narcos-1.001	
WebCacheV01.dat	bing.com	drink deals wellingto	Microsoft Edge Anal	2019-01-29 04:28:17	Narcos-1.001	
WebCacheV01.dat	bing.com	drink deals courtene	Microsoft Edge Anal	2019-01-29 04:28:26	Narcos-1.001	
WebCacheV01.dat	bing.com	poquito bar	Microsoft Edge Anal	2019-01-29 04:29:03	Narcos-1.001	
WebCacheV01.dat	bing.com	install chrome	Microsoft Edge Anal	2019-01-29 21:04:44	Narcos-1.001	

Image 3.5 It has all the web searches of Steve regarding drugs

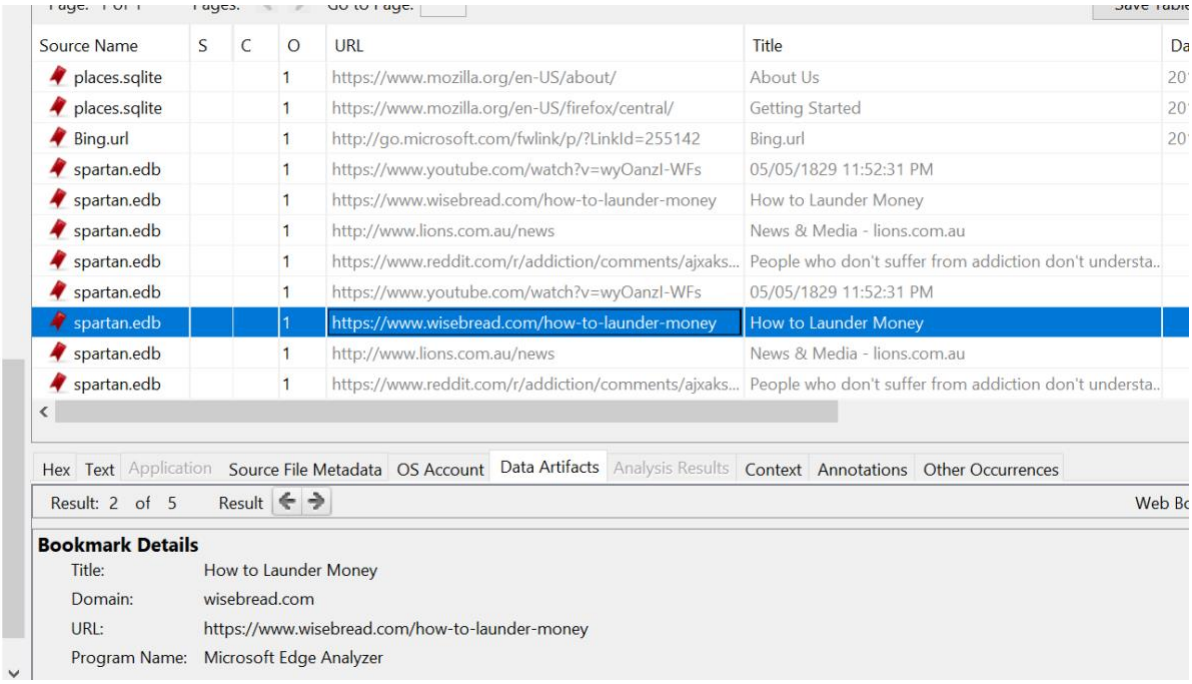
Image 3.6 It shows us his activity of searches related to drugs

23	History	google.com	crystal meth	Google Chrome	2019-01-31 06:56:24	Narcos-1.001
24	History	google.com	crystal meth	Google Chrome	2019-01-31 06:56:24	Narcos-1.001
25	History	google.com	crystal meth	Google Chrome	2019-01-31 06:56:30	Narcos-1.001
26	History	google.com	crystal meth	Google Chrome	2019-01-31 06:56:33	Narcos-1.001
27	History	google.com	drug paraphernalia	Google Chrome	2019-01-31 06:57:16	Narcos-1.001
28	History	google.com	drug paraphernalia	Google Chrome	2019-01-31 06:57:21	Narcos-1.001
29	History	google.com	drug paraphernalia	Google Chrome	2019-01-31 06:57:21	Narcos-1.001
30	History	google.com	drug paraphernalia	Google Chrome	2019-01-31 06:57:21	Narcos-1.001

John’s Web activity:

Web activity of John is very similar to Steve, he also searched about drugs, how to do money laundering, information about drugs etc.

Image 3.7 This image shows us his web history such as how to do money laundering.



Source Name	S	C	O	URL	Title	Da
places.sqlite			1	https://www.mozilla.org/en-US/about/	About Us	20
places.sqlite			1	https://www.mozilla.org/en-US/firefox/central/	Getting Started	20
Bing.url			1	http://go.microsoft.com/fwlink/p/?LinkId=255142	Bing.url	20
spartan.edb			1	https://www.youtube.com/watch?v=wyOanzI-WFs	05/05/1829 11:52:31 PM	
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/ajxaks...	People who don't suffer from addiction don't understa..	
spartan.edb			1	https://www.youtube.com/watch?v=wyOanzI-WFs	05/05/1829 11:52:31 PM	
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/ajxaks...	People who don't suffer from addiction don't understa..	

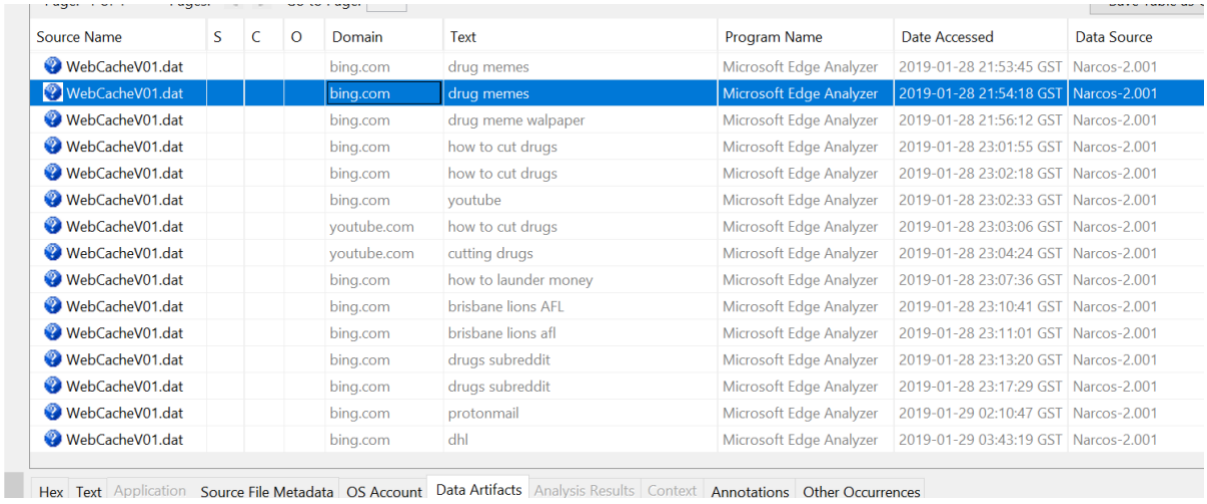
Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 2 of 5 Result

Bookmark Details

Title: How to Launder Money
Domain: wisebread.com
URL: https://www.wisebread.com/how-to-launder-money
Program Name: Microsoft Edge Analyzer

Image 3.8 It shows his web activities of searching for drugs.



Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
WebCacheV01.dat				bing.com	drug memes	Microsoft Edge Analyzer	2019-01-28 21:53:45 GST	Narcos-2.001
WebCacheV01.dat				bing.com	drug memes	Microsoft Edge Analyzer	2019-01-28 21:54:18 GST	Narcos-2.001
WebCacheV01.dat				bing.com	drug meme walpaper	Microsoft Edge Analyzer	2019-01-28 21:56:12 GST	Narcos-2.001
WebCacheV01.dat				bing.com	how to cut drugs	Microsoft Edge Analyzer	2019-01-28 23:01:55 GST	Narcos-2.001
WebCacheV01.dat				bing.com	how to cut drugs	Microsoft Edge Analyzer	2019-01-28 23:02:18 GST	Narcos-2.001
WebCacheV01.dat				bing.com	youtube	Microsoft Edge Analyzer	2019-01-28 23:02:33 GST	Narcos-2.001
WebCacheV01.dat				youtube.com	how to cut drugs	Microsoft Edge Analyzer	2019-01-28 23:03:06 GST	Narcos-2.001
WebCacheV01.dat				youtube.com	cutting drugs	Microsoft Edge Analyzer	2019-01-28 23:04:24 GST	Narcos-2.001
WebCacheV01.dat				bing.com	how to launder money	Microsoft Edge Analyzer	2019-01-28 23:07:36 GST	Narcos-2.001
WebCacheV01.dat				bing.com	brisbane lions AFL	Microsoft Edge Analyzer	2019-01-28 23:10:41 GST	Narcos-2.001
WebCacheV01.dat				bing.com	brisbane lions afl	Microsoft Edge Analyzer	2019-01-28 23:11:01 GST	Narcos-2.001
WebCacheV01.dat				bing.com	drugs subreddit	Microsoft Edge Analyzer	2019-01-28 23:13:20 GST	Narcos-2.001
WebCacheV01.dat				bing.com	drugs subreddit	Microsoft Edge Analyzer	2019-01-28 23:17:29 GST	Narcos-2.001
WebCacheV01.dat				bing.com	protonmail	Microsoft Edge Analyzer	2019-01-29 02:10:47 GST	Narcos-2.001
WebCacheV01.dat				bing.com	dhl	Microsoft Edge Analyzer	2019-01-29 03:43:19 GST	Narcos-2.001

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

ion (1)

Web activity of Jane shows that she searched about how to act that she is involved with the dealer, but she is not as we know that she is working for the Australia Federal Police.

Image 3.9 This image shows the web activity of Jane

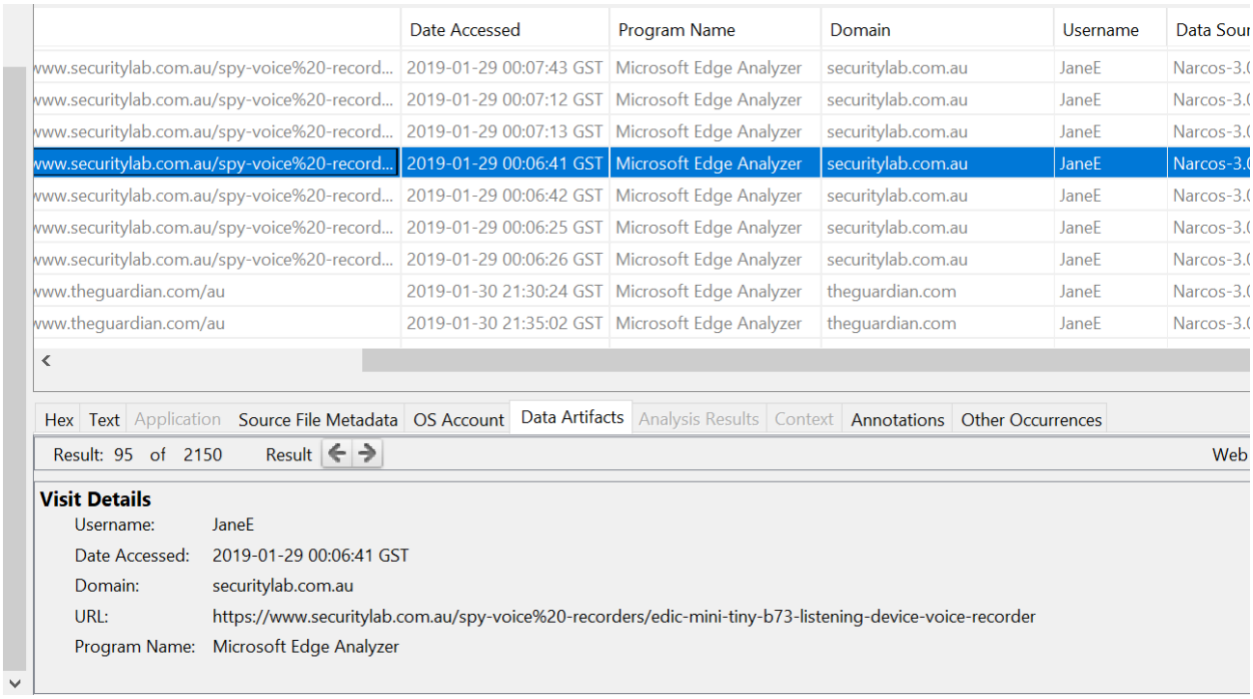


Image 4.0

This image shows that Jane searched about how to blackmail

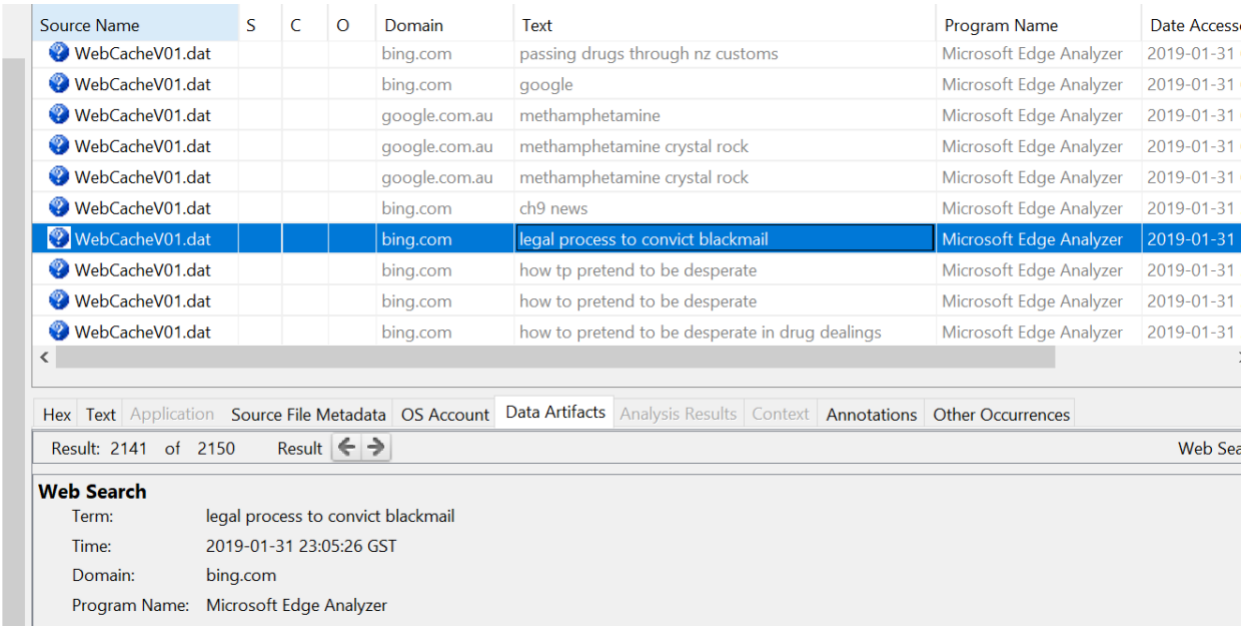


image 4.0

Finding 4) Identify images that help to build a profile of the three suspects' behavior.

For Steve Kowhai I found a lot of images that can be used as evidence such as picture of drugs, the google map route that they would have taken after

Image 4.1 This image shows us the cash and the drugs that were found from steve’s folder

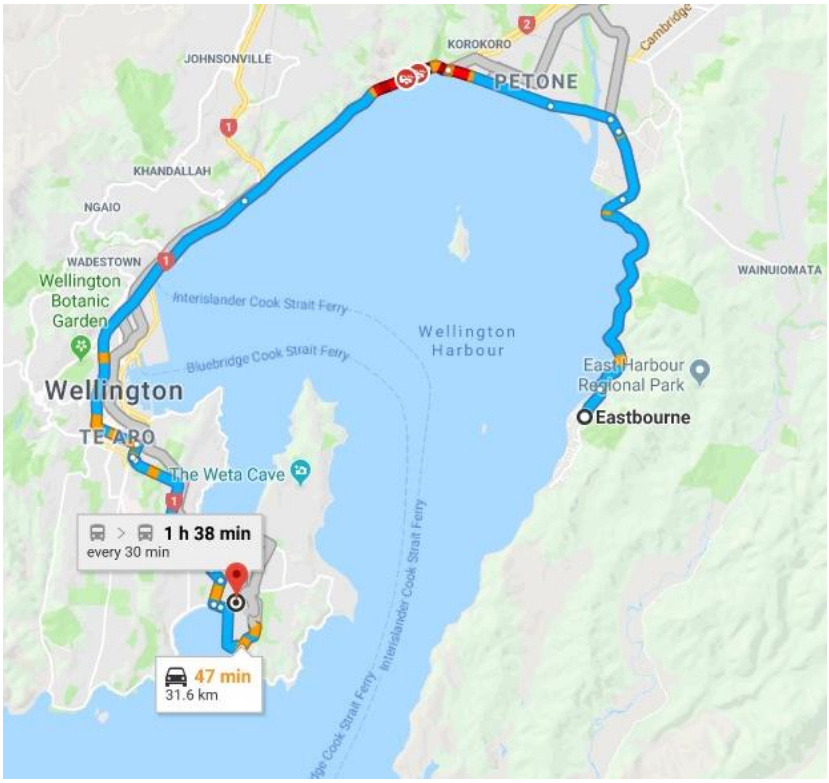


Image 4.2 This was the place where the drug was supposed to be delivered as mentioned by the suspects at the airport

Image 4.3 It's the another location where the drugs was to be taken .

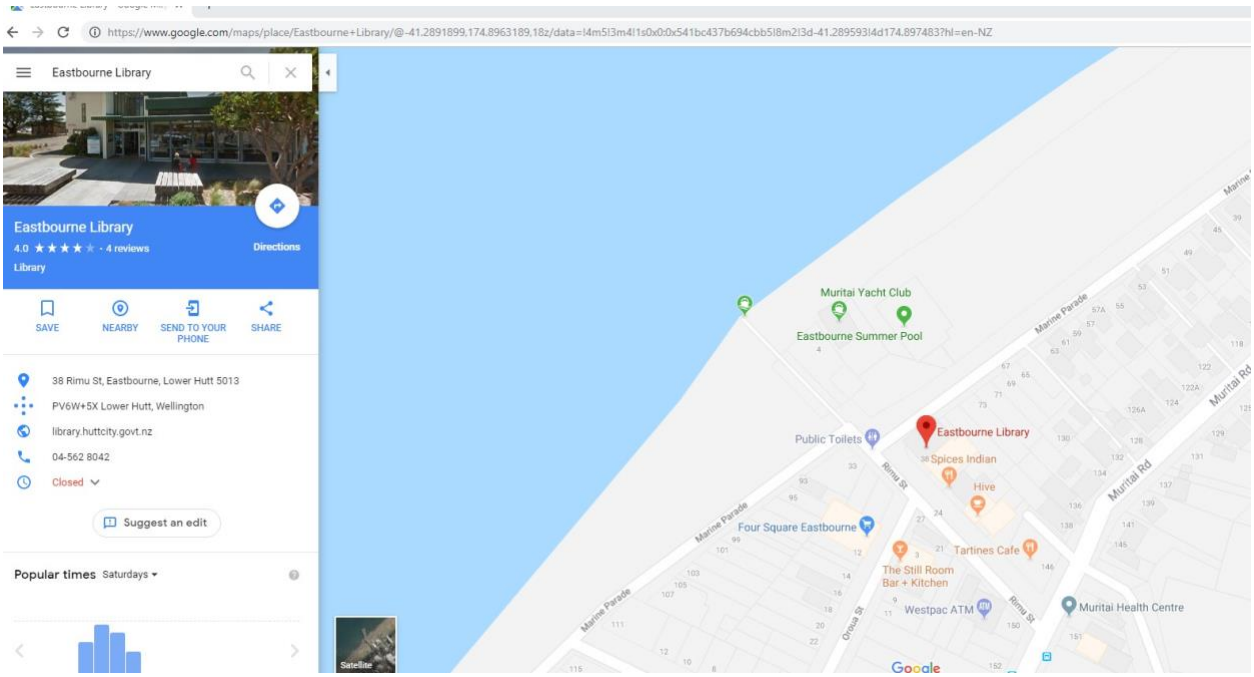


Image 4.4 Images of drugs in packets and solidified form

Image 4.5 This image shows that Eastbourne is marked as the home of Steve

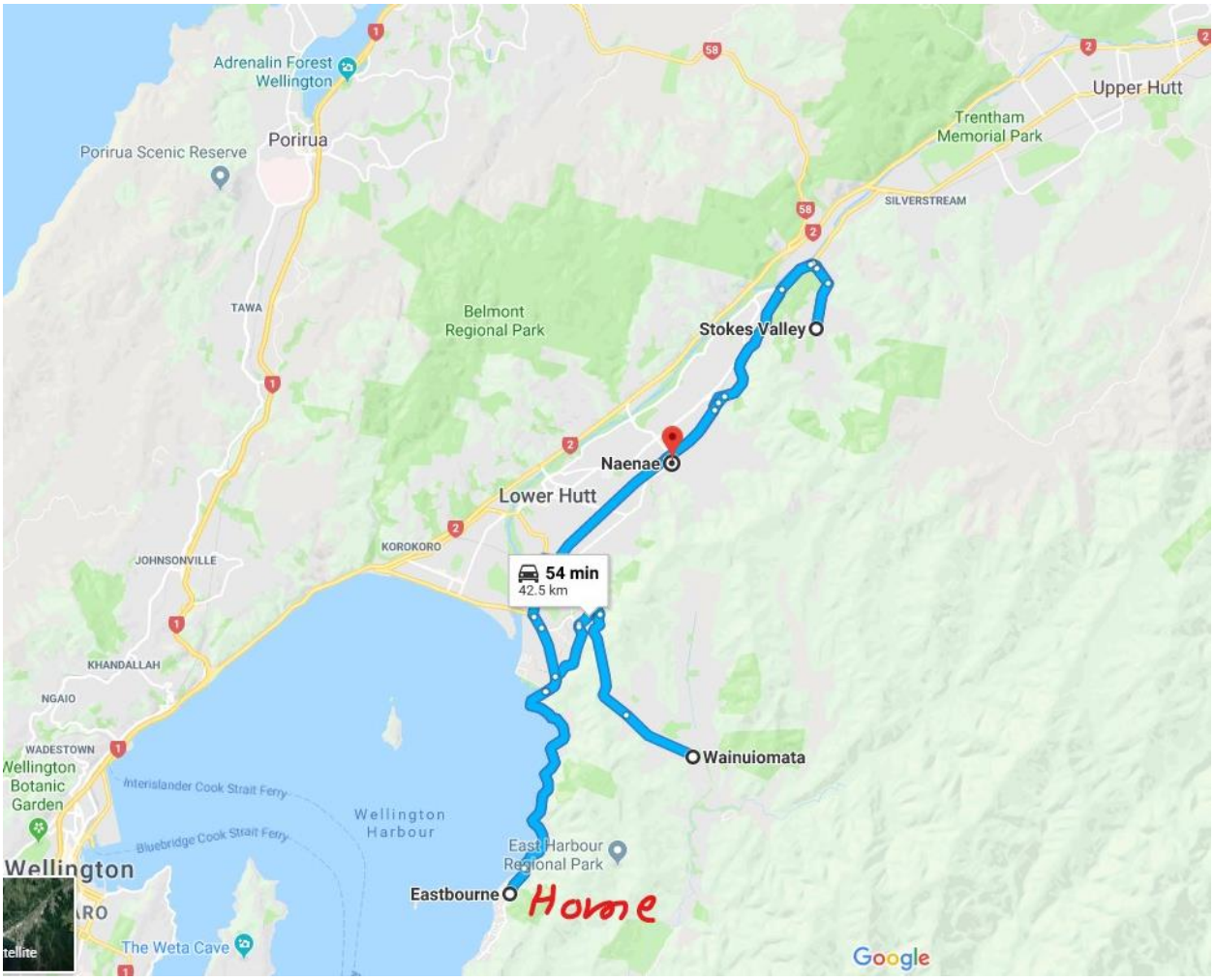
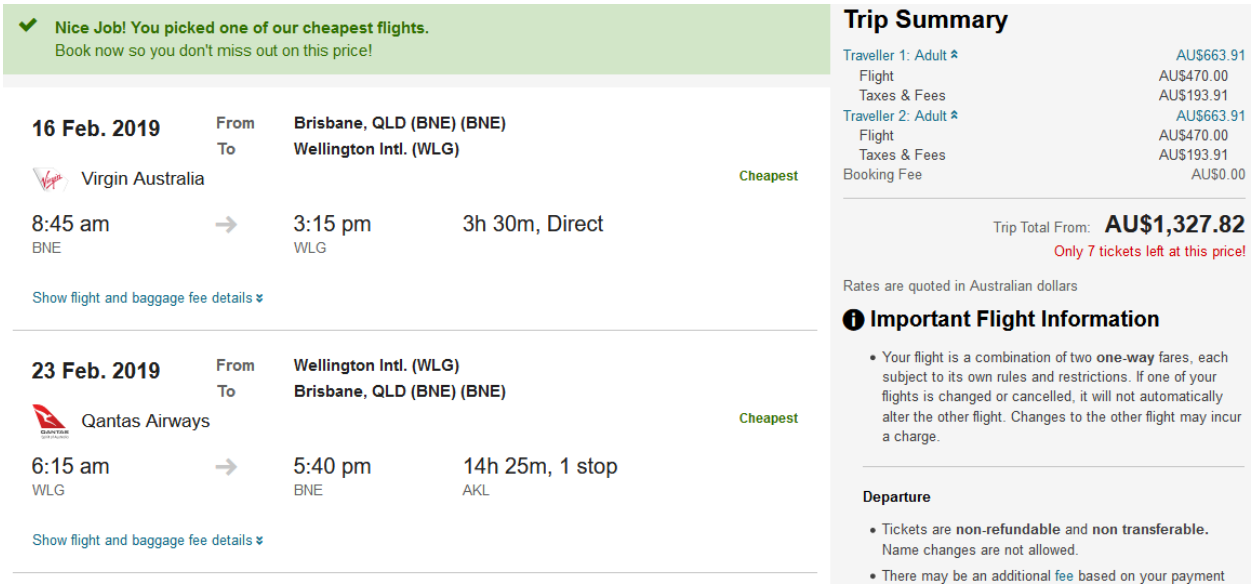


Image 4.5.1 This image shows the flight booking made from Brisbane to Wellington



For John I found the following images

Image 4.6 This mail was used by john to do conversation we can see that from his web activity as well

Image 4.7 John also used discord as we can see the same from the web history.

Image 4.8 This is the image of drugs hidden under packets

Image 4.9 John also tried to book last minute flight as well to Wellington from Brisbane

Image 5.0 This image is the one which has some packages that were recovered from john's folder

Image 5.1 Image of money

For jane I found the following:

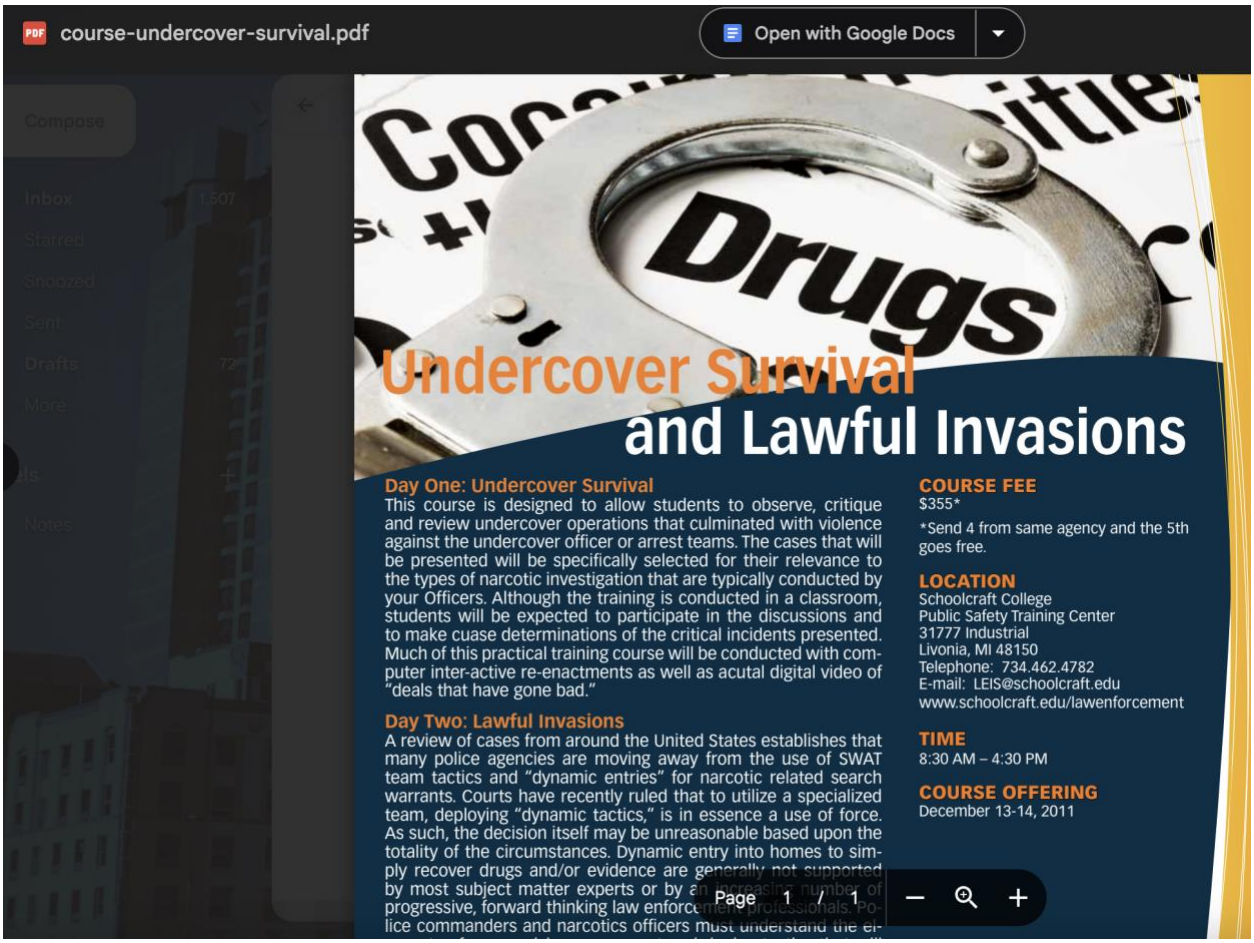
Image 5.2 This is the photo of drugs in crystal form

Image 5.3 another image of drugs

Image 5.4 Image of a handcuff and drugs in the background

Image 5.5 Inage of more crystals of drugs

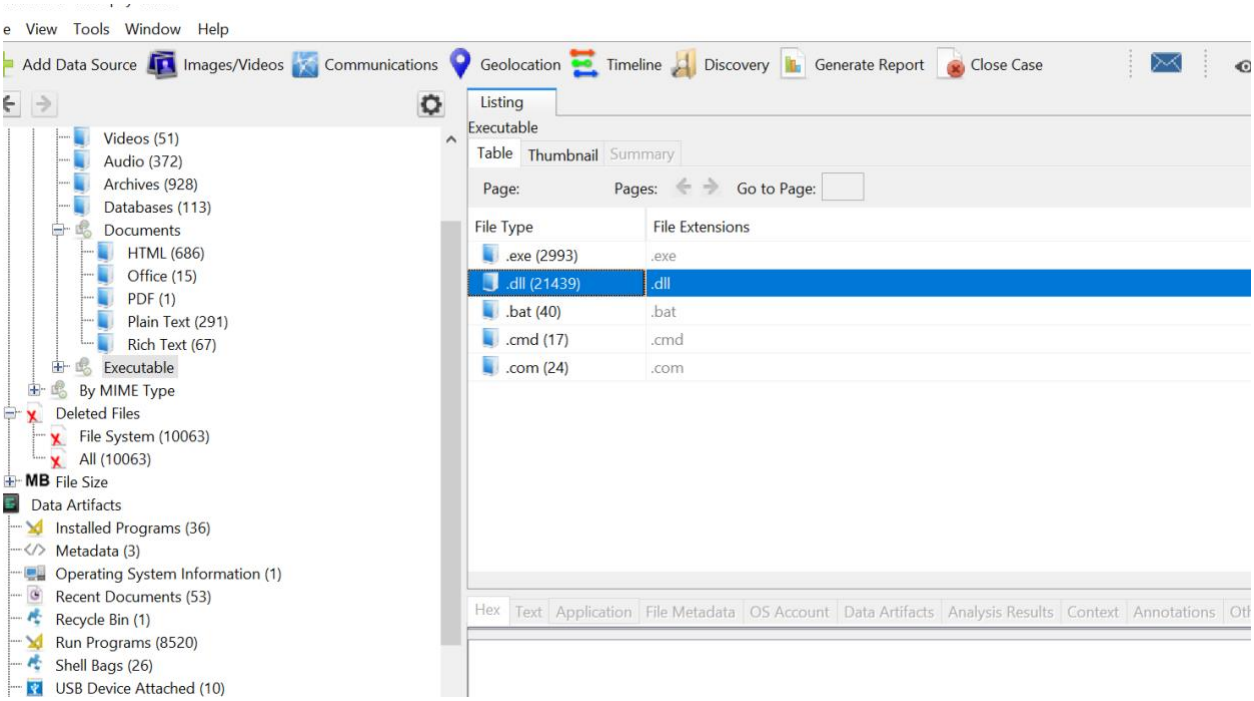
Image 5.6 A pdf file that shows undercover cop survival



5) Identify binary files that could help the investigation.

From john's folder some binary files are found that can be helpful in the investigation

Image 5.7 It has list of binary files.



6) Identify the means and the content of communications between all the suspects.

Image 5.8

This shows us that Steve accessed proton mail to communicate

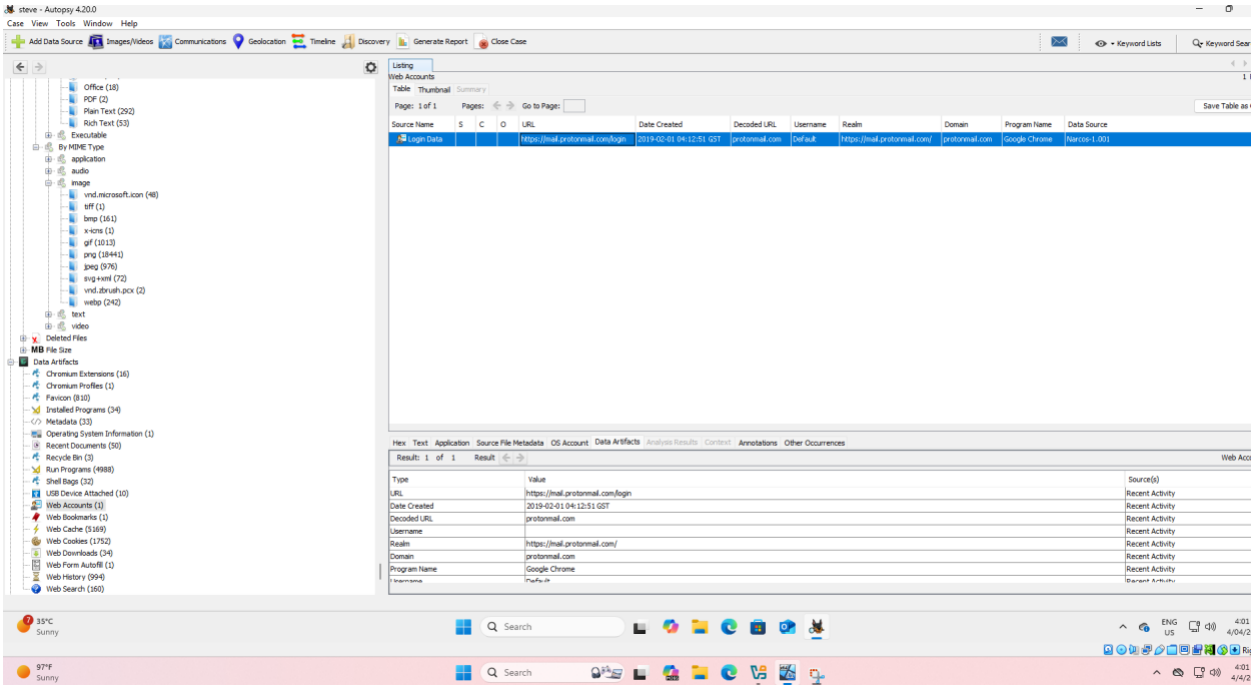


Image 5.9

WebCacheV01.dat	bing.com	download open offic	Microsoft Edge Anal	2019-01-28 20:42:24	Narcos-1.001
WebCacheV01.dat	bing.com	download discord	Microsoft Edge Anal	2019-01-28 20:55:46	Narcos-1.001
WebCacheV01.dat	bing.com	protnmail	Microsoft Edge Anal	2019-01-28 21:02:11	Narcos-1.001

This shows that Steve has downloaded discord and used proton mail.

John

Image 6.0 It shows john used discord

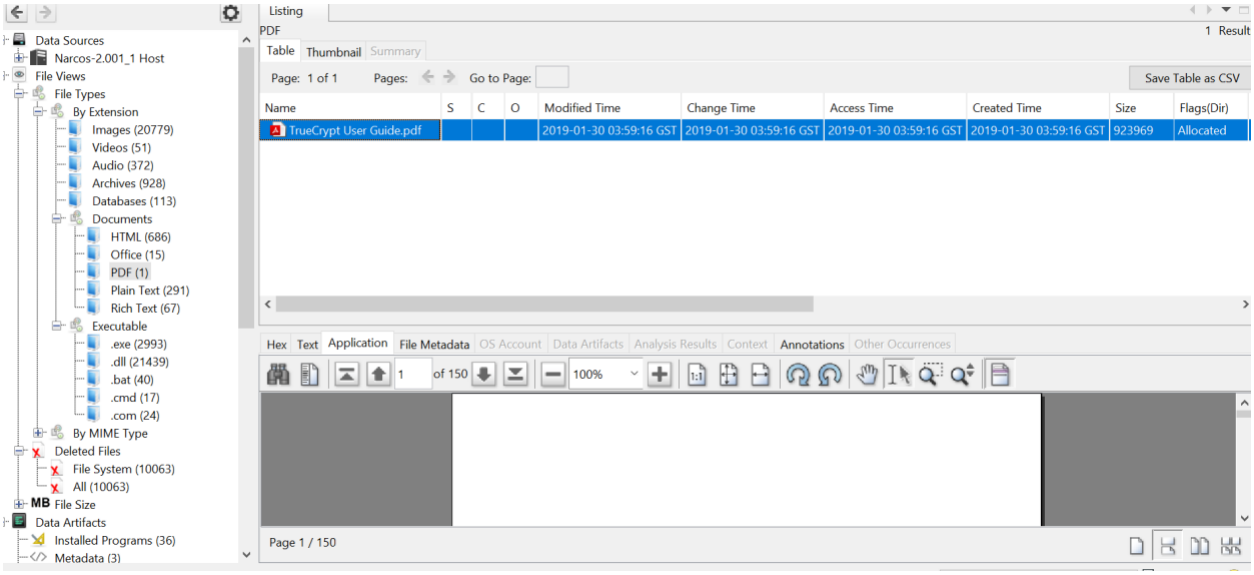
SRUDB.dat	\users\johnf\appdata\local\discord\app-0.0.304\disco...	JohnF	2019-01-31 02:57:00 GST	System Resource Usa
SRUDB.dat	\users\johnf\appdata\local\discord\update.exe	JohnF	2019-01-31 02:57:00 GST	System Resource Usa
SRUDB.dat	\users\johnf\appdata\roaming\java\updater.exe	JohnF	2019-01-31 02:57:00 GST	System Resource Usa

Image 6.1 He downloaded images of discord

Image 6.2 He used mail

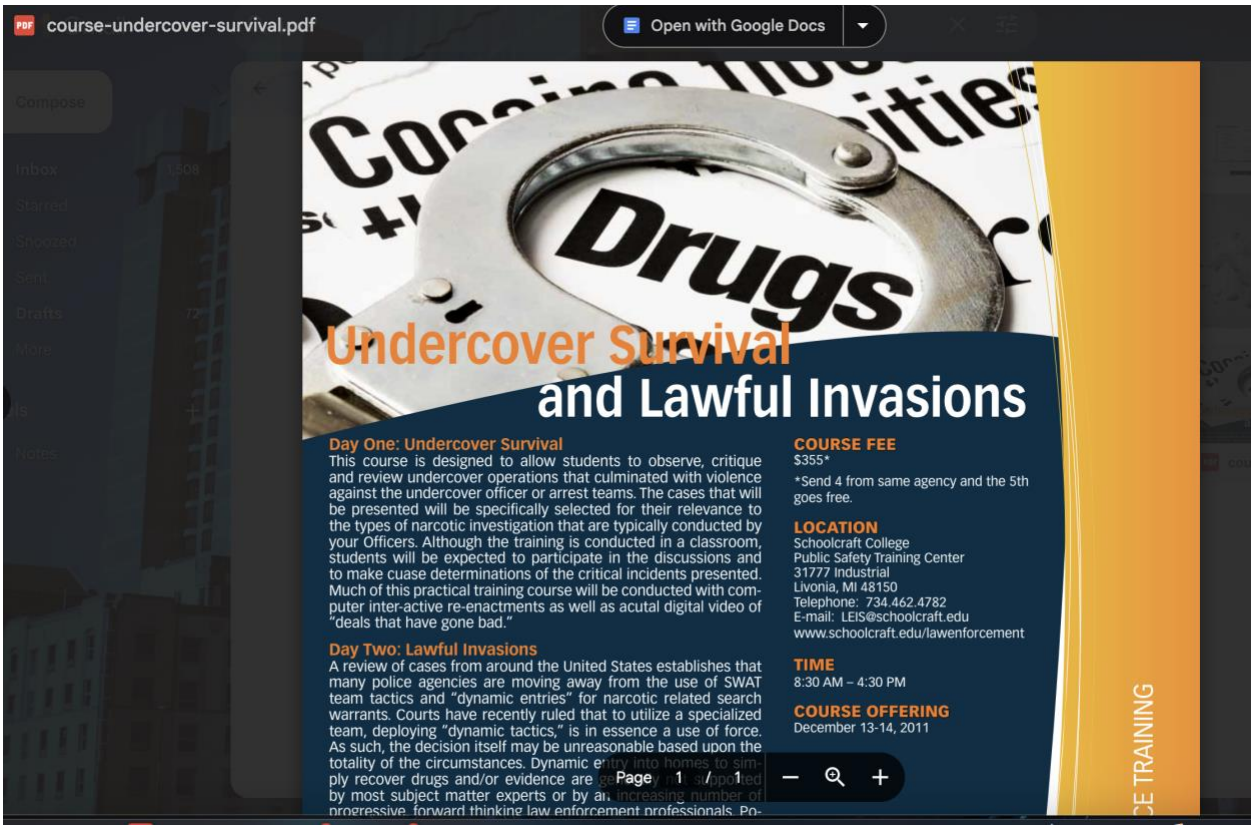
7) Identify any documents that could help the investigation.

Image 6.3 pdf of john that was used to decrypt



Jane pdf

Image 6.4 This pdf has tips to survive as an undercover



8) Identify encryption methods used by the suspects and determine two methods that can circumvent the encryption

image 6.5 This image shows that encryption is being guessed due to high entropy as it was found on Jane's system. This file is stored in the form of a database

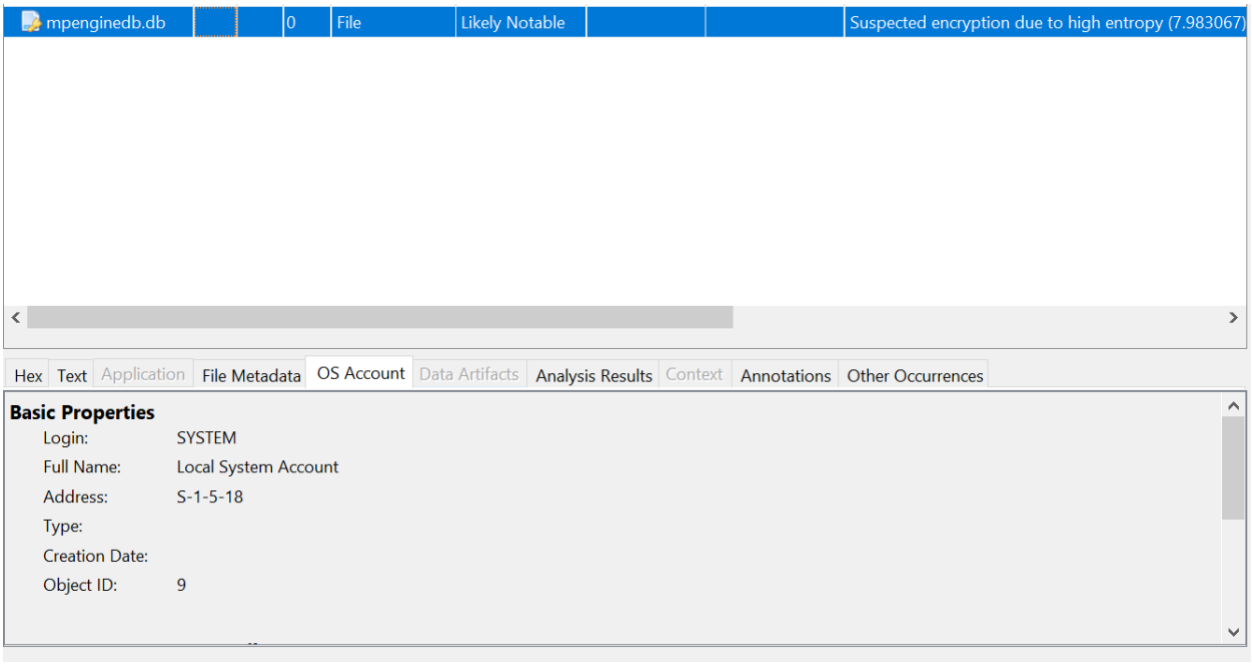


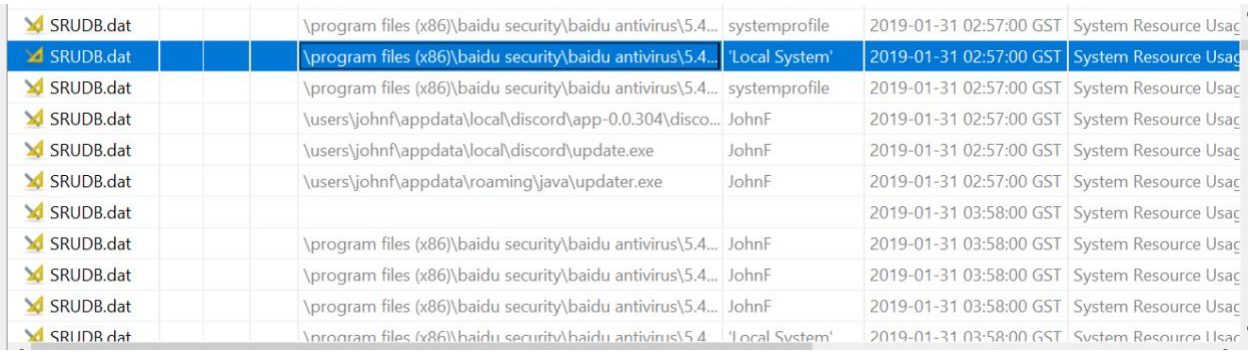
Image 6.6 This shows that Steve used TrueCrypt to encrypt message and then used cc cleaner as per his web history.

History	google.com	truecrypt
History	google.com	truecrypt
History	google.com	protonmail
History	google.com	ccleaner

9) Identify the vulnerability that allowed the malware to function

I didn't find any Vulnerability, but I found that the suspect John used Baidu Antivirus

Image 6.7



SRUDB.dat	\program files (x86)\baidu security\baidu antivirus\5.4...	systemprofile	2019-01-31 02:57:00 GST	System Resource Usag
SRUDB.dat	\program files (x86)\baidu security\baidu antivirus\5.4...	'Local System'	2019-01-31 02:57:00 GST	System Resource Usag
SRUDB.dat	\program files (x86)\baidu security\baidu antivirus\5.4...	systemprofile	2019-01-31 02:57:00 GST	System Resource Usag
SRUDB.dat	\users\johnf\appdata\local\discord\app-0.0.304\disco...	JohnF	2019-01-31 02:57:00 GST	System Resource Usag
SRUDB.dat	\users\johnf\appdata\local\discord\update.exe	JohnF	2019-01-31 02:57:00 GST	System Resource Usag
SRUDB.dat	\users\johnf\appdata\roaming\java\updater.exe	JohnF	2019-01-31 02:57:00 GST	System Resource Usag
SRUDB.dat			2019-01-31 03:58:00 GST	System Resource Usag
SRUDB.dat	\program files (x86)\baidu security\baidu antivirus\5.4...	JohnF	2019-01-31 03:58:00 GST	System Resource Usag
SRUDB.dat	\program files (x86)\baidu security\baidu antivirus\5.4...	JohnF	2019-01-31 03:58:00 GST	System Resource Usag
SRUDB.dat	\program files (x86)\baidu security\baidu antivirus\5.4...	JohnF	2019-01-31 03:58:00 GST	System Resource Usag
SRUDB.dat	\program files (x86)\baidu security\baidu antivirus\5.4	'Local System'	2019-01-31 03:58:00 GST	System Resource Usag

10) Identify whether changes have occurred to these artefacts across the different Win 10 builds.

There are no changes to the files /images as the hash value is same as before investigation and after the investigation and the principle of integrity is maintained.

Conclusion

In conclusion we got sufficient evidence for illegal drug activity after analyzing all the files of the suspects we found a lot of evidence that they were dealing with drug trafficking as mentioned I have attached images of drugs that were found from the images which were recovered from the suspects and can play a significant role if this document will be presented in the court. As the chain of custody is maintained from the very 1st step to the last step. Also, we found web searches regarding how to cut drugs, how to do money laundering, searches for drug laws of New Zealand and, I found a lot of evidence where the suspects were searching about meth, how to use it and a lot and lots of data.

The evidence that I provided is reliable as it proves that the suspects were doing drug trafficking which is not good for the society as drugs consumption can be injurious to health and its supply should be stopped accordingly. My evidence is useful as it has solid proofs against the threat actors that they did drug trafficking and, I found a lot of information that can be used against them in the court, and it will help police to investigate more based on my findings

The person Steve is the drug supplier , I found images of drugs from his files and he is main for supplying the drugs , as I could find some maps where drugs was to be taken and it’s the same place that Jane mentioned where the drugs was to be taken so basically there were two places where drug was about to be taken .So Steve was not innocent . Same for John I found a lot of drugs related memes, drugs images, web searches for drug trafficking, money laundering as it is confirmed that its him as the system id matches and the system, he was using so he was the admin.

Jane was innocent as she was an undercover cop working for the Australian Federal Police and I found several evidence against her that she is a cop. Hence in conclusion this report did a detailed investigation of finding evidence in drug trafficking.

Appendix

Persons of Interests are

1) Steve kowhai – Drug dealer who was mastermind in this investigation.

2) John F.- John teams up with Steve and does this drug trafficking act

3) Jane E – Jane was an undercover cop who worked as she was with the drug dealers and was a part of the case

Evidence listing

Found users devices and their role with it

Found images regarding Narcos

Found Web activity of suspects

Got a list of evidence

Software and tools used in the investigation

Autopsy

VMware

FTK imager

Magnet Axiom