Forensic Investigation

CASE: ECL-DRUG-2025-0063

Forensic Examiner: Thomas Green

Digital Forensics Team Alpha

New Zealand Customs Service, Drug Investigations Unit

Contents

1. Introduction
2. Forensic Methodology
3. User Abbtribution
4. Relationship with John
5. Drug Ring
6. Customers
7. Timeline
8. Anti-Forensics
9. Limitations and Recommendations

1. Introduction

Case Information

Suspects: John Fredrickson and Jane Esteban

Primary Offense: Importation of Class A Controlled Drug (Methamphetamine)

Evidence: Item #: EV-001

Deliver package to Eastbourne Library OR 666 Rewera Avenue

Examination Tasks

1. Identify the owner/primary user of the desktop computer.
2. Determine the relationship between John Fredricksen and desktop owner.
3. Analyze communications to identify other members or drug trafficking network and roles.
4. Identify any potential customers of the drug trafficking network.
5. Establish timeline of drug importation and future plans based on evidence.
6. Evaluate whether there was effort to hide electronic evidence.

2. **Forensic Methodology**

Chain of Custody

Pre-Acquisition of image.

Acquisition of image.

Laws and Guidelines.

Validation Methods used.

Technical Specifications

OS Version

Other Relevant Information

Forensic Tools Used

Autopsy 4.21.0

ChromeCacheViewer 2.52

Image Steganography 1.52

3.1. **User Attribution**

Device Information

Registered Owner

User Profile Directory

Account Headings

Consistent Email/Username Usage

Steve’s name appears in protonmail access

Online alias is crayfish1980. Appears in:

- skype
- protonmail
- discord

3.2 **User Attribution**

Steve’s Role in Operation

Web History.

- “Dark web marketplaces”
- “How to launder money”
- “How to cut ice”
- “International Drug routes”
- “Drug routes around Wellington”

Responsible for dealing and planning trafficking routes for moving the product around Wellington Region.

Focused on broader distribution network

4.1 **Relationship with John**

John’s Role

Executed the physical smuggling of meth.
Maintained contact with Steve via Discord.

Steve provided instructions to John.

Account Headings

Discord Username → heresjohnny1

4.2 **Relationship with John**

Discord Communications

crayfish1980: New Supplier eh? Definietely Interested! Can I get 10 keys...
heresjohnny1: ...10 is a bit much for first time around...start with 1 and ramp up from there.

Confirms that John runs the smuggling operations, and Steve is the distributor.

crayfish1980: Good. Meet at the Eastbourne library and if we miss each other come to 666 Rewera Avenue, Petone.

5.1 **Drug Ring**

Network

No identified Drug Ring apart from known members of operation:

- Steve Kowhai
- John Fredricksen
- Jane Esteban

Steve is the operation’s key leader, provides instructions.
John Fredricksen executes the smuggling of drugs.

Limitations on analysis for Jane Esteban, cannot identify her role in Steve’s drug network/ring.

5.2 **Drug Ring**

Capabilities

Steve has search history researching meth:

- cutting drugs/cutting agents for ice
- how to launder money

as well as websites visited:

- https://qz.com/481037/dark-web/
- https://www.businessinsider.com/au/beginners-guide-to-money-laundering

This tells us that their operation is fairly new based on how basic these terms are in comparison to an established and experienced drug ring.

5.3 **Drug Ring**

Expanding Network

Possibly looking at spots in Wellington to sell drugs to other suppliers as per Google Searches:

- “best places to trade drugs”
- “gangs nz drugs”

Google searches also contain:

- “drug routes in around wellington”
- “drug routes in wellington”
- “international drug routes”

6.1 **Customers**

Identifiable Customers

From analysing Steve’s web history, it is clear that there is no potential buyers lined up.

- “best places to trade drugs”
- “drug routes in around wellington”
- “drug routes in wellington”
- “international drug routes”

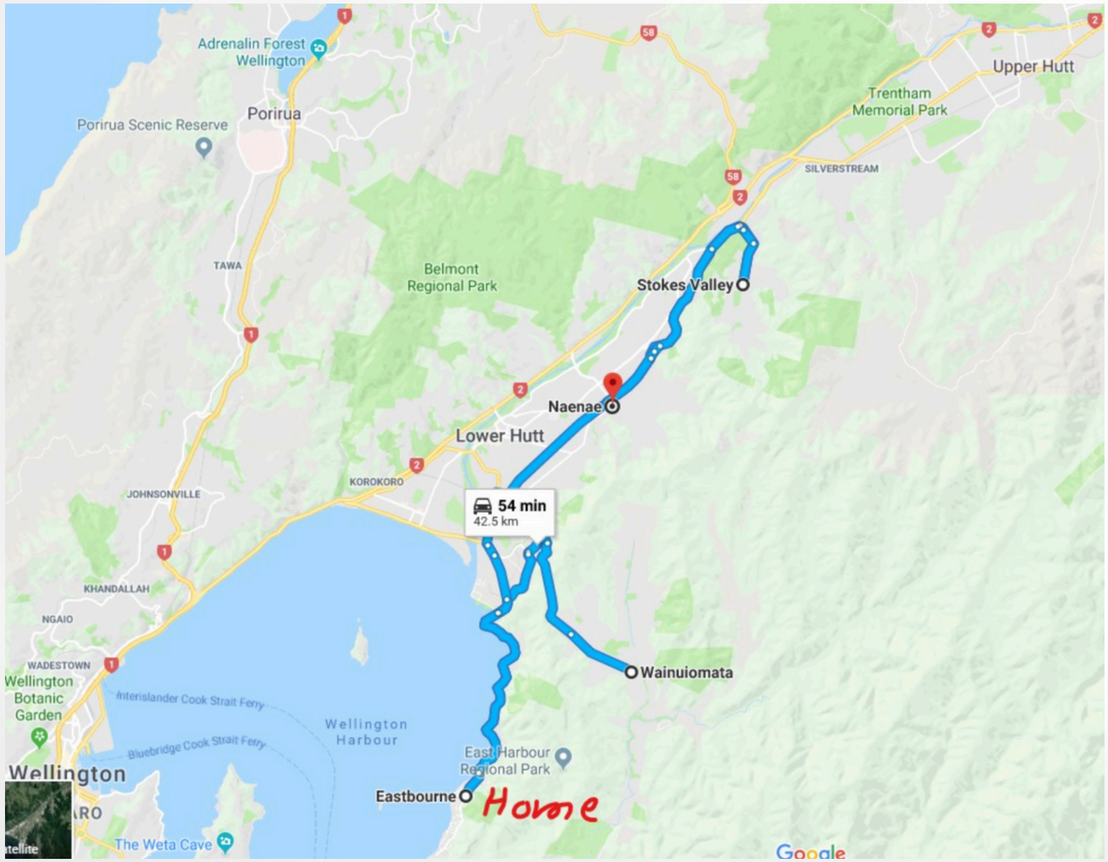
No other communications via Discord or other social platforms was identified with potential customers.

Clear that Steve is either going to trade or sell.

6.2 **Customers**

Potential Locations

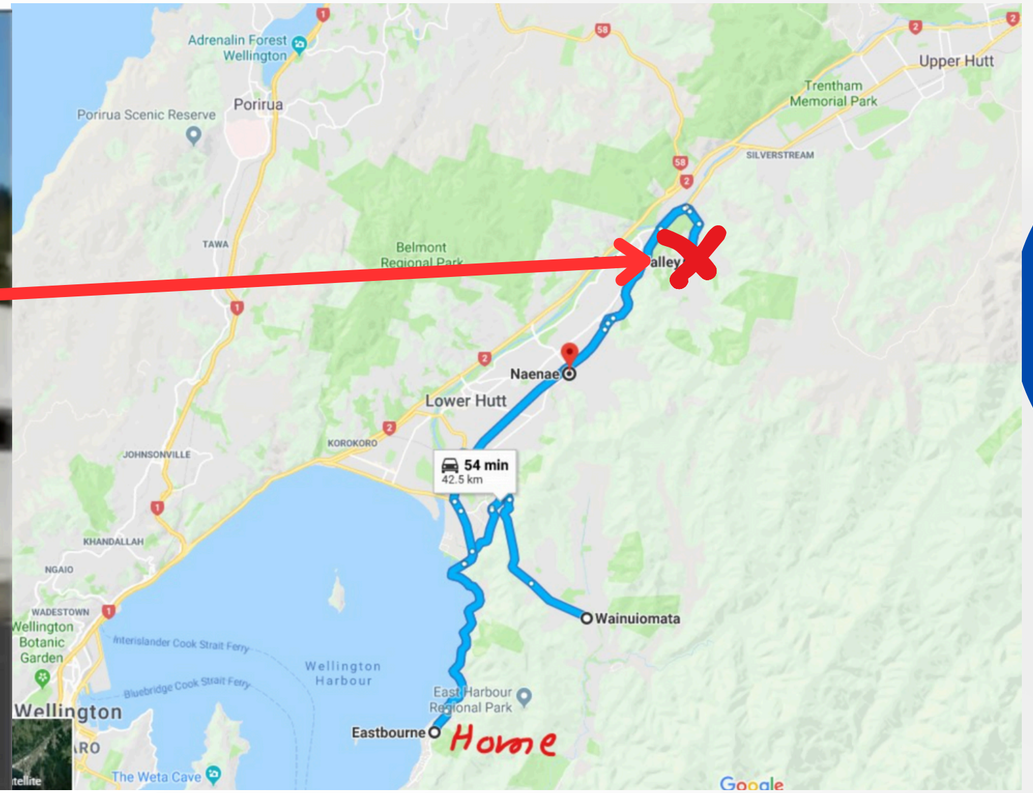
Identified that Steve has done research on potential places for distribution that is part of his route as per Method run.jpg



Here we can see four identifiable hotspots for which Steve has identified selling the product.

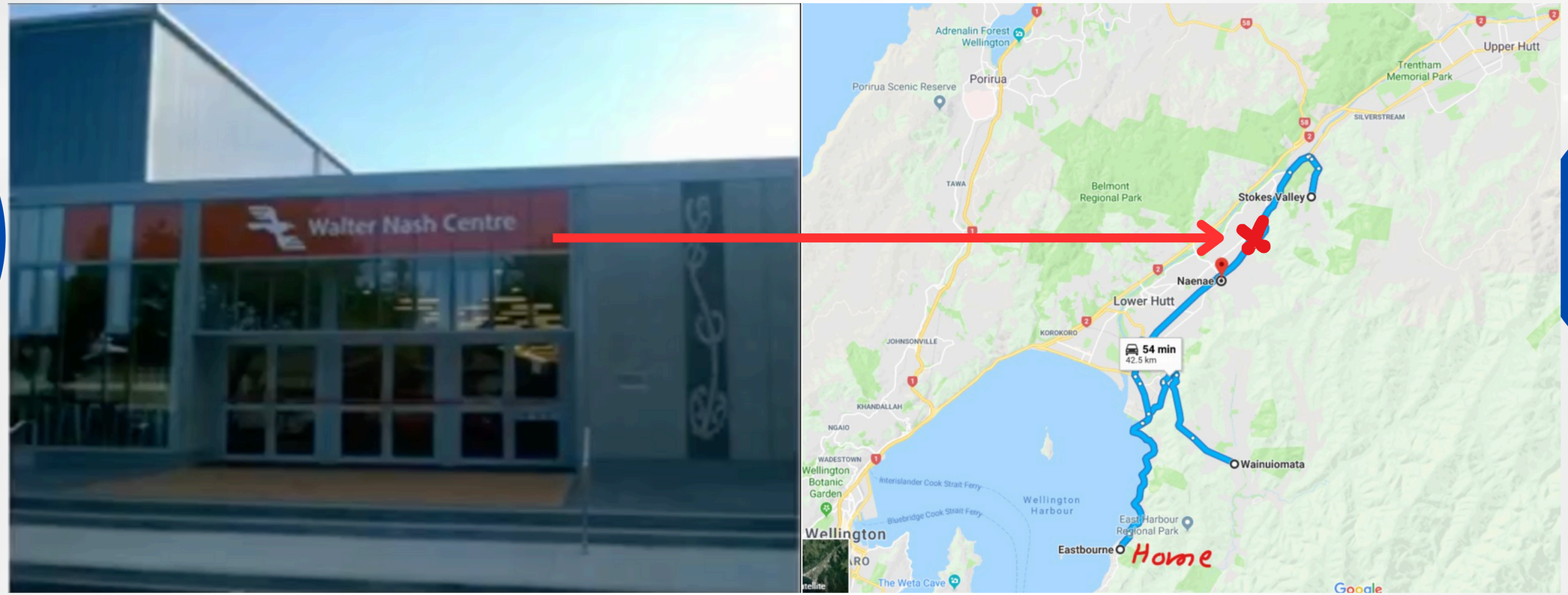
6.3 **Customers**

Potential Location One



6.4 **Customers**

Potential Location Two



6.5 **Customers**

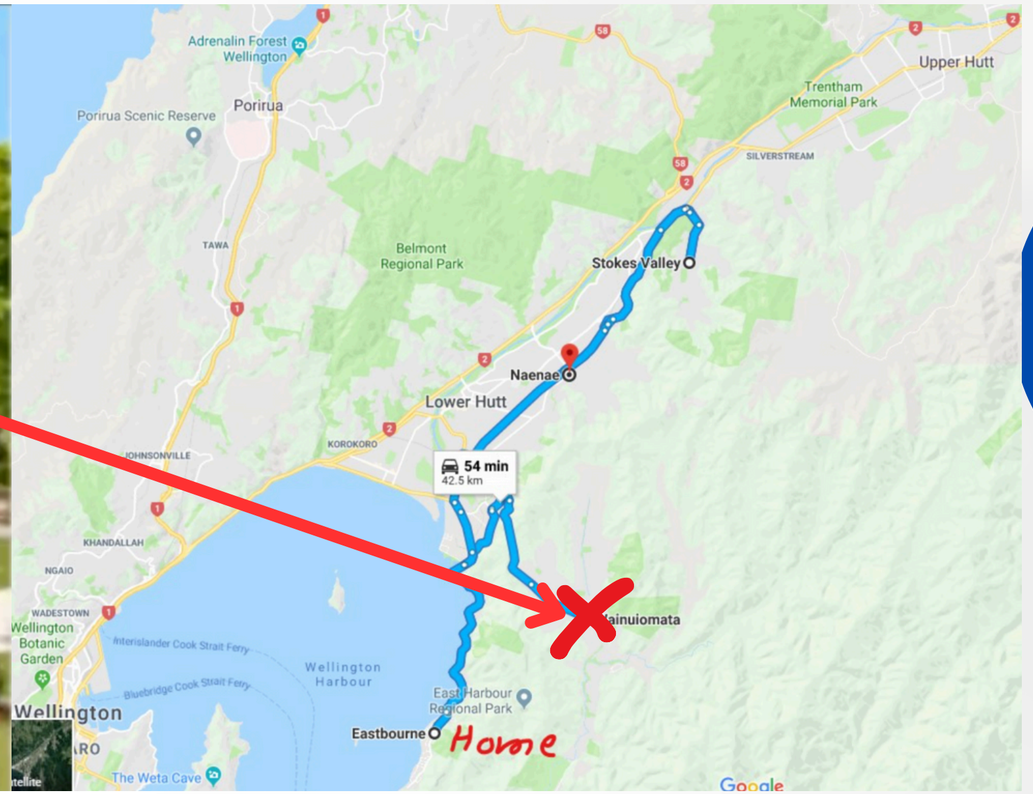
Potential Location Three

6.5 **Customers**

Potential Location Four

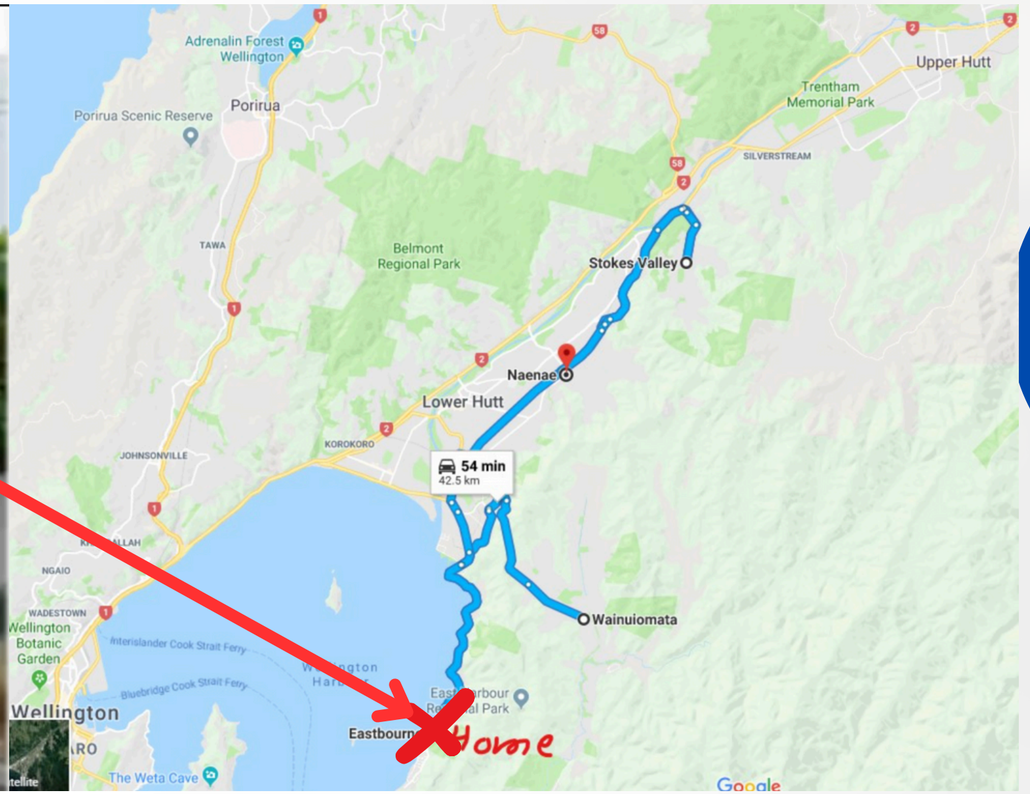
6.6 **Customers**

Potential Location Five



6.7 **Customers**

Potential Location Six



Also the location provided from Steve to John for dropoff.

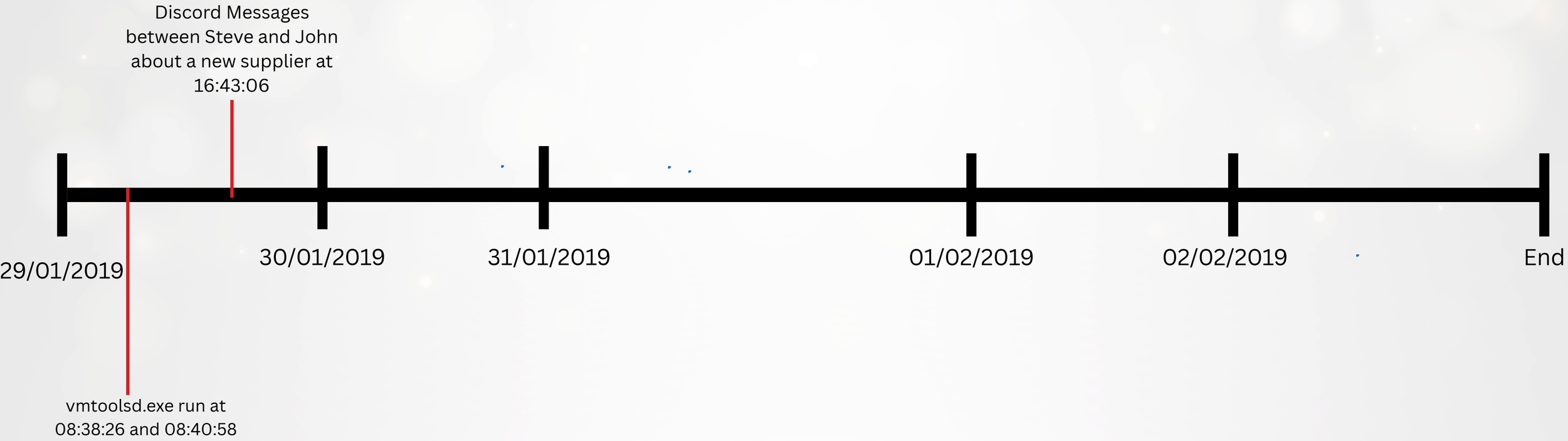
7.1 **Timeline**

Result Tags

File Tags

7.2 **Timeline**

29/01/2019

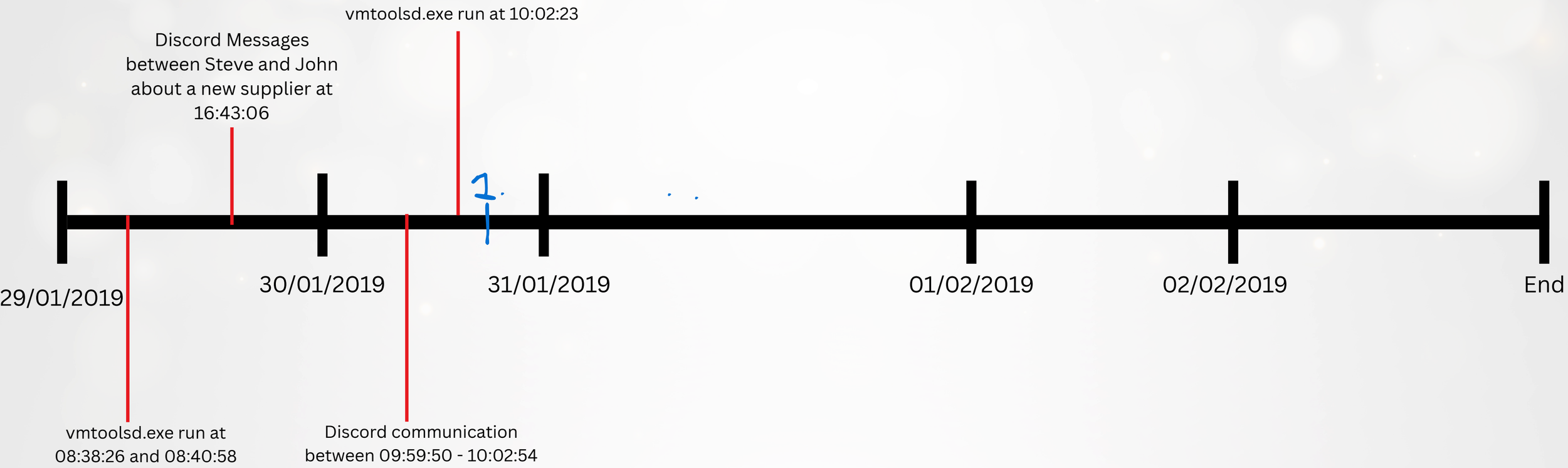


Result Tags

File Tags

7.3 **Timeline**

30/01/2019



Result Tags

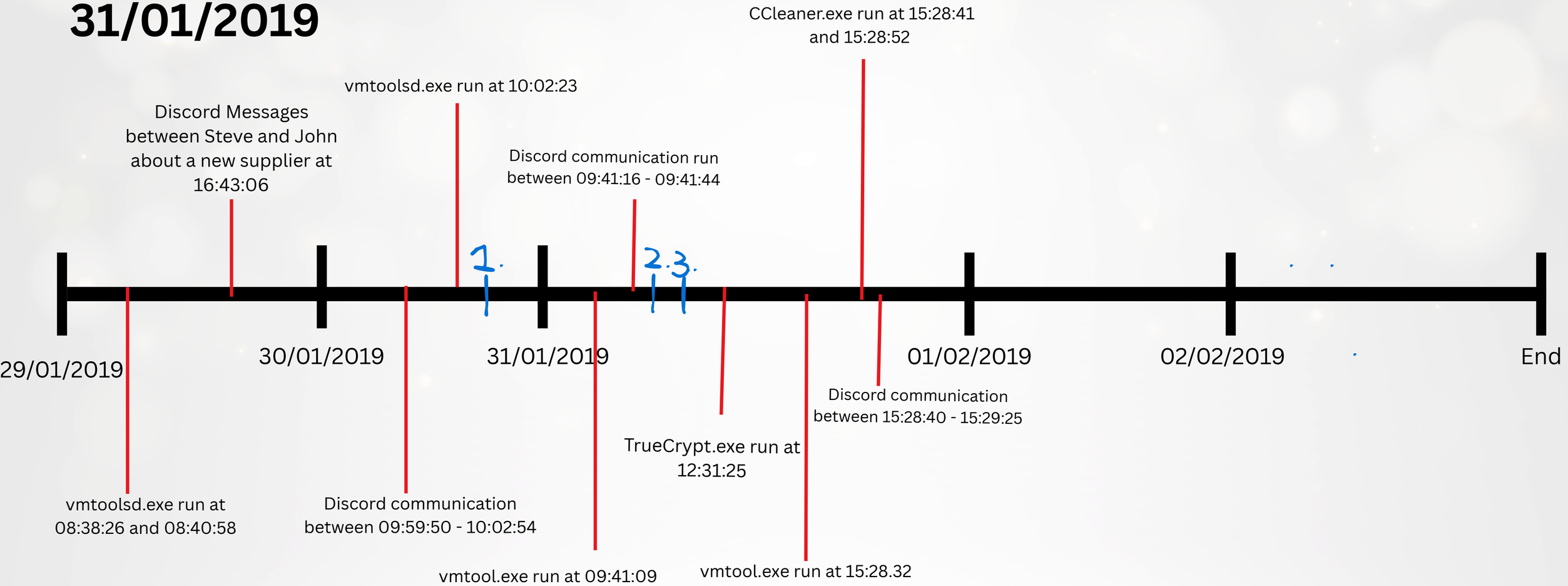
File Tags

7.4 Timeline

File Tag One

7.5 **Timeline**

31/01/2019

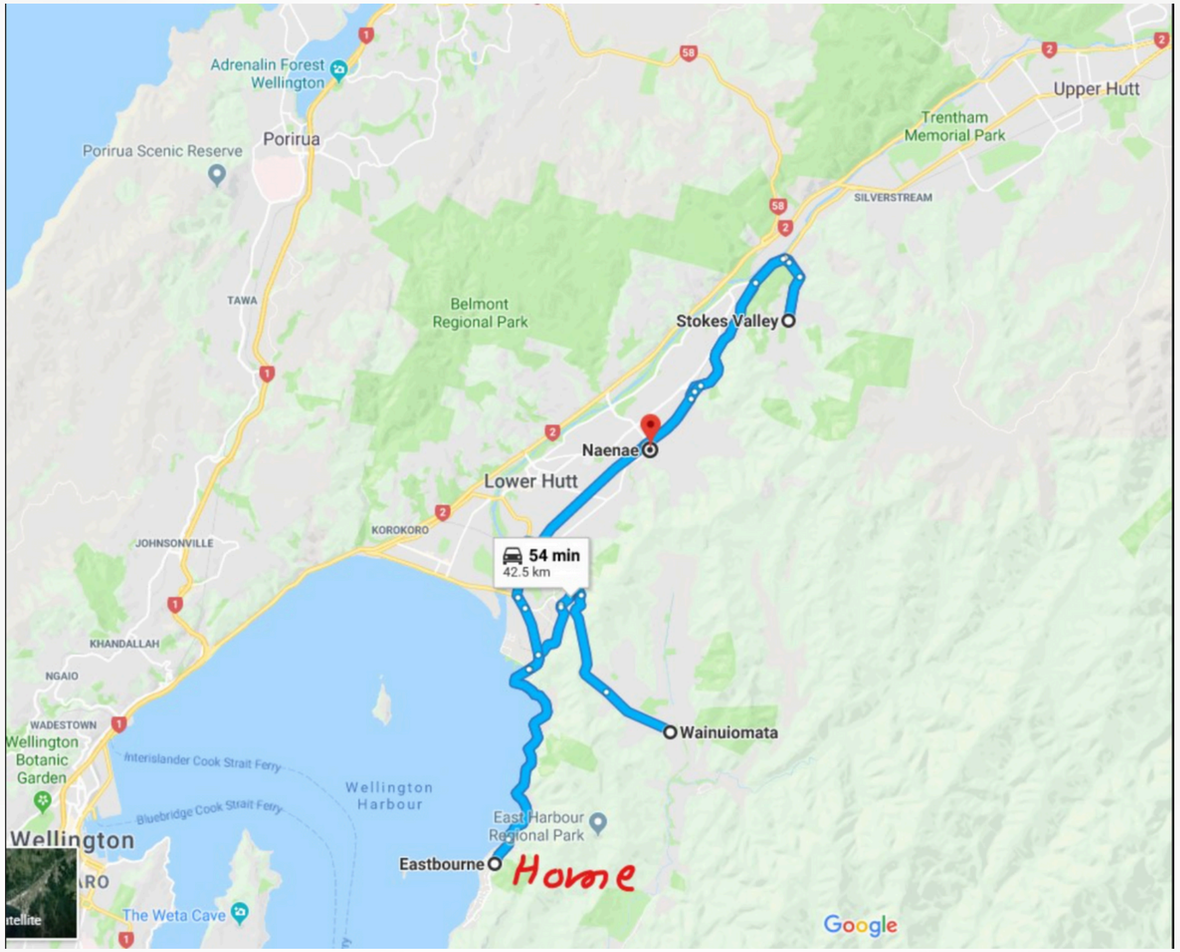


Result Tags

File Tags

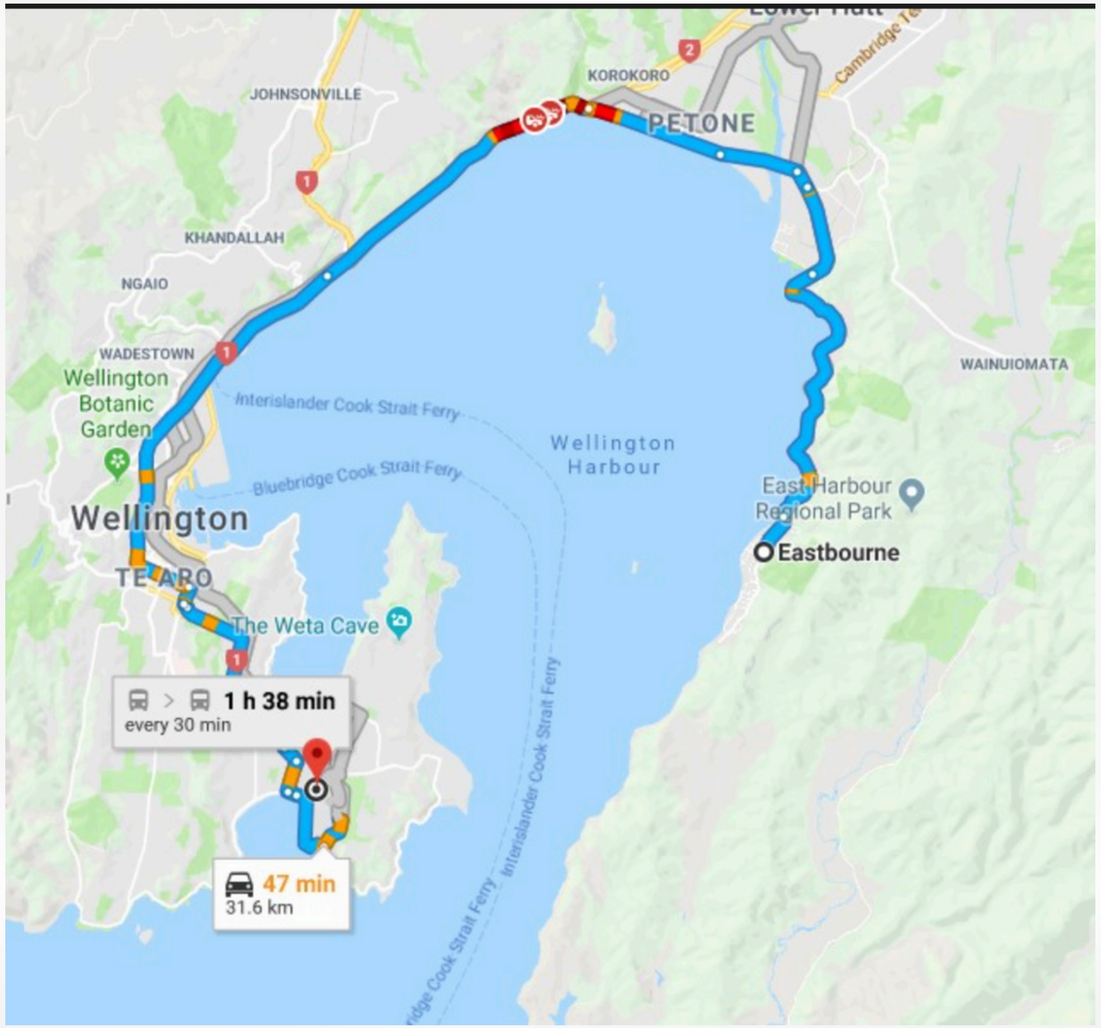
7.6 Timeline

File Tag Two



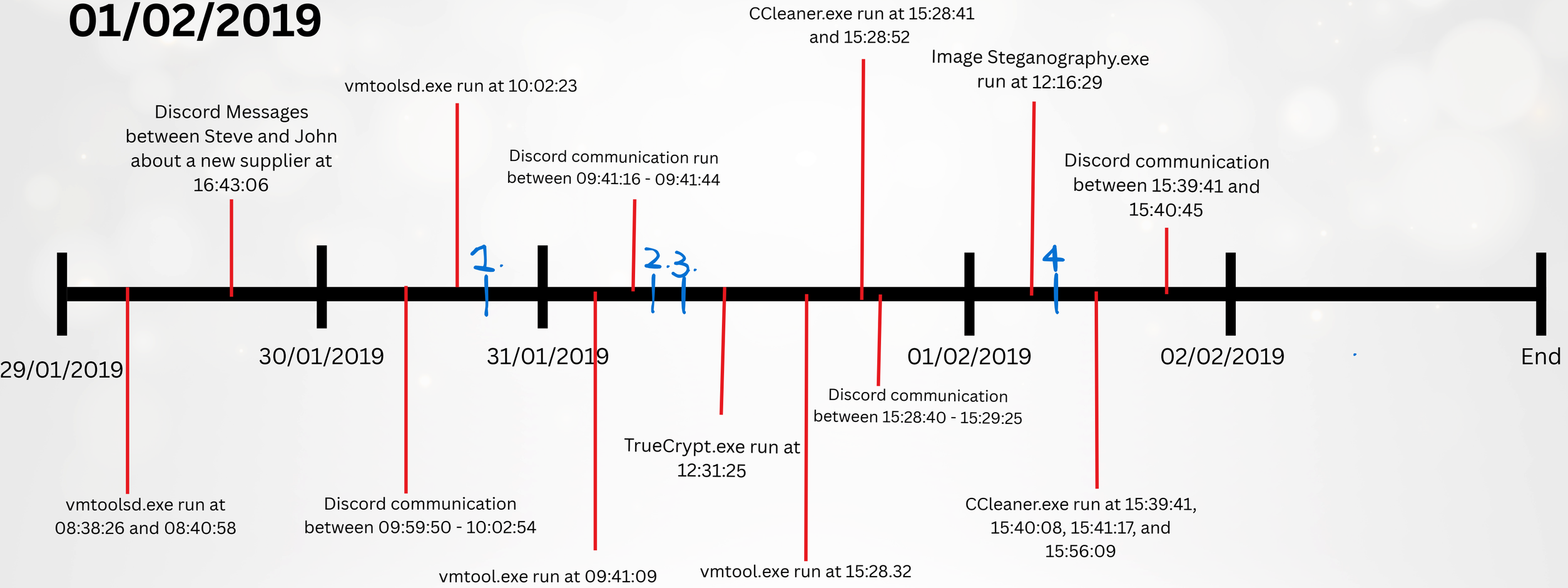
7.7 Timeline

File Tag Three



7.8 **Timeline**

01/02/2019



Result Tags

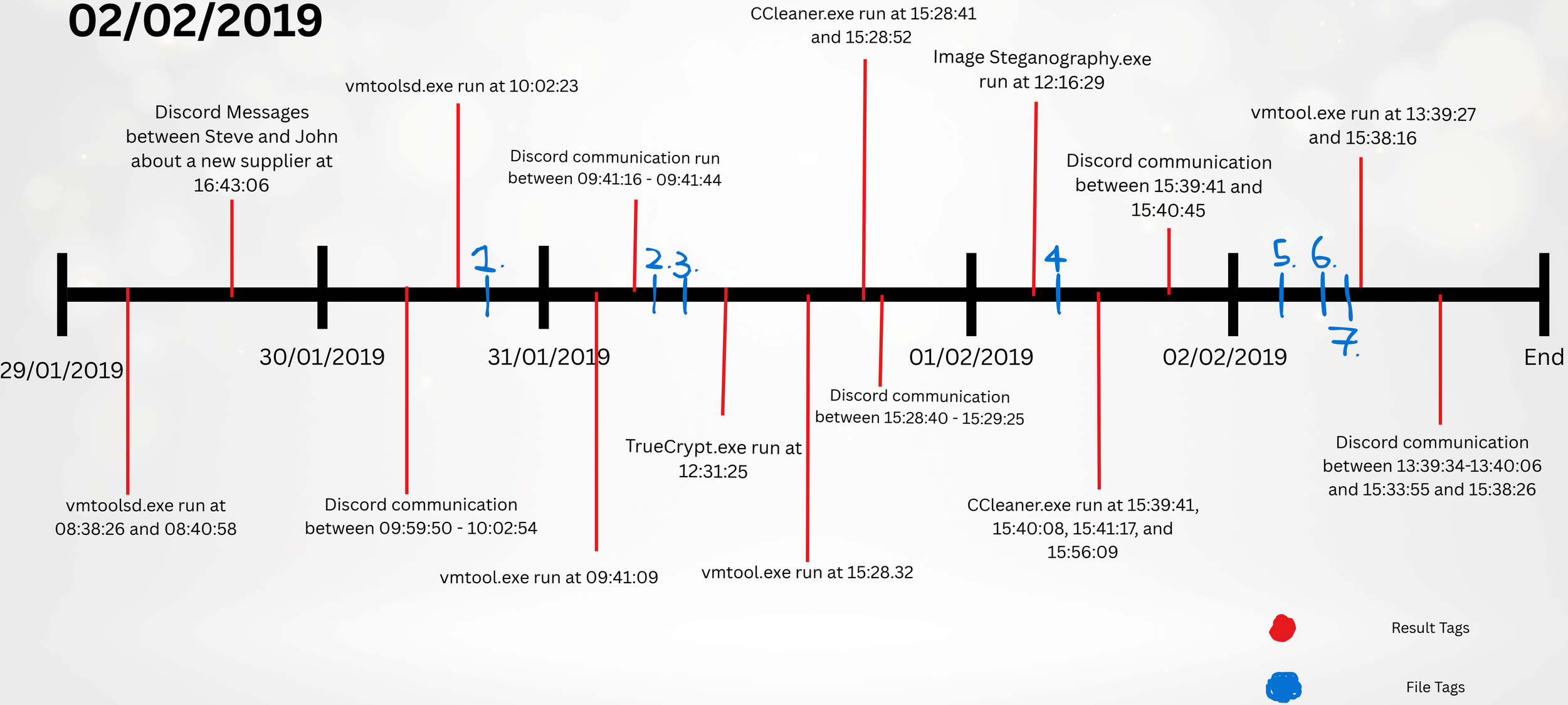
File Tags

7.9 Timeline

File Tag Four

7.10 **Timeline**

02/02/2019

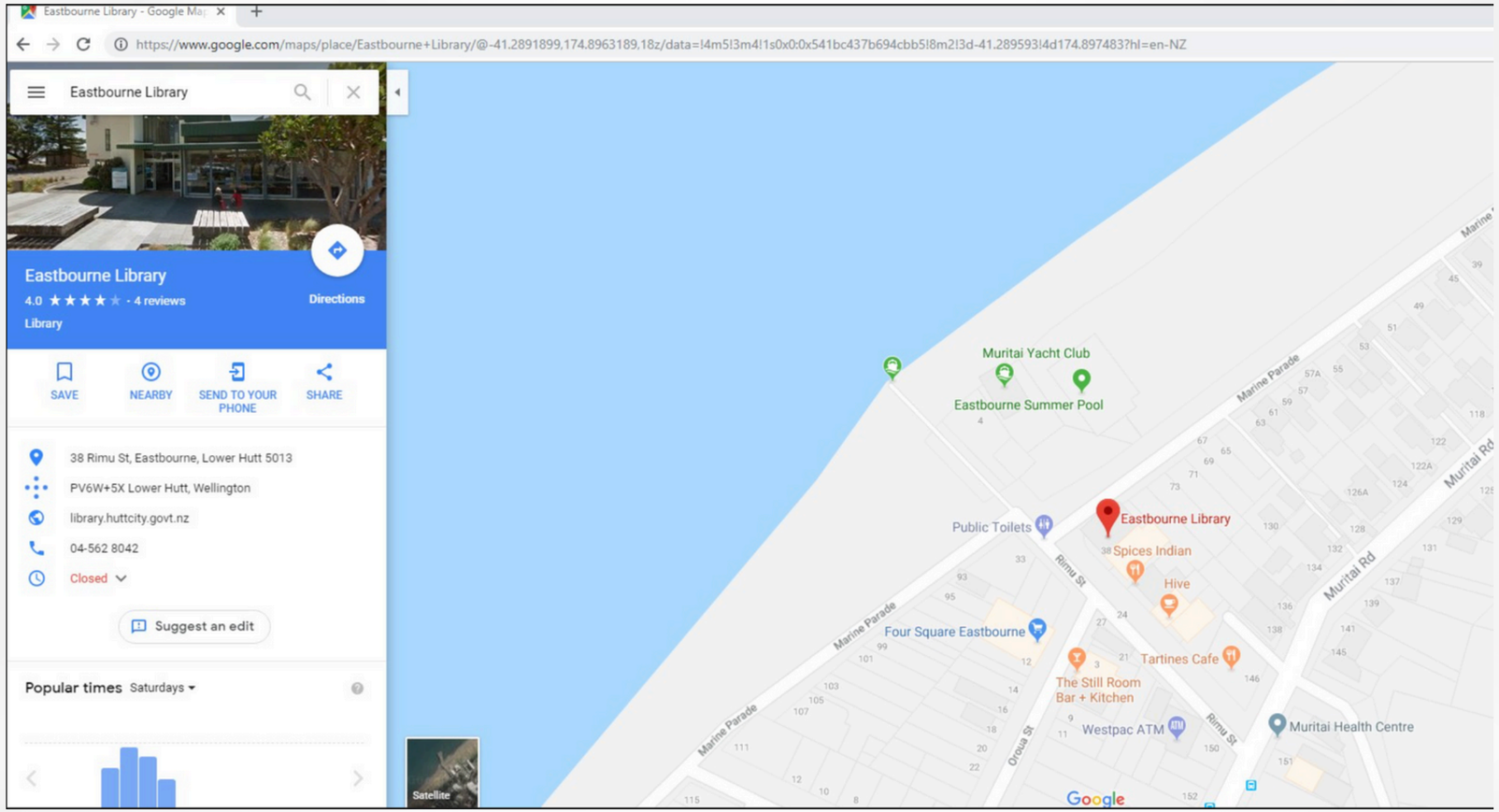


7.11 **Timeline**

File Tag Five

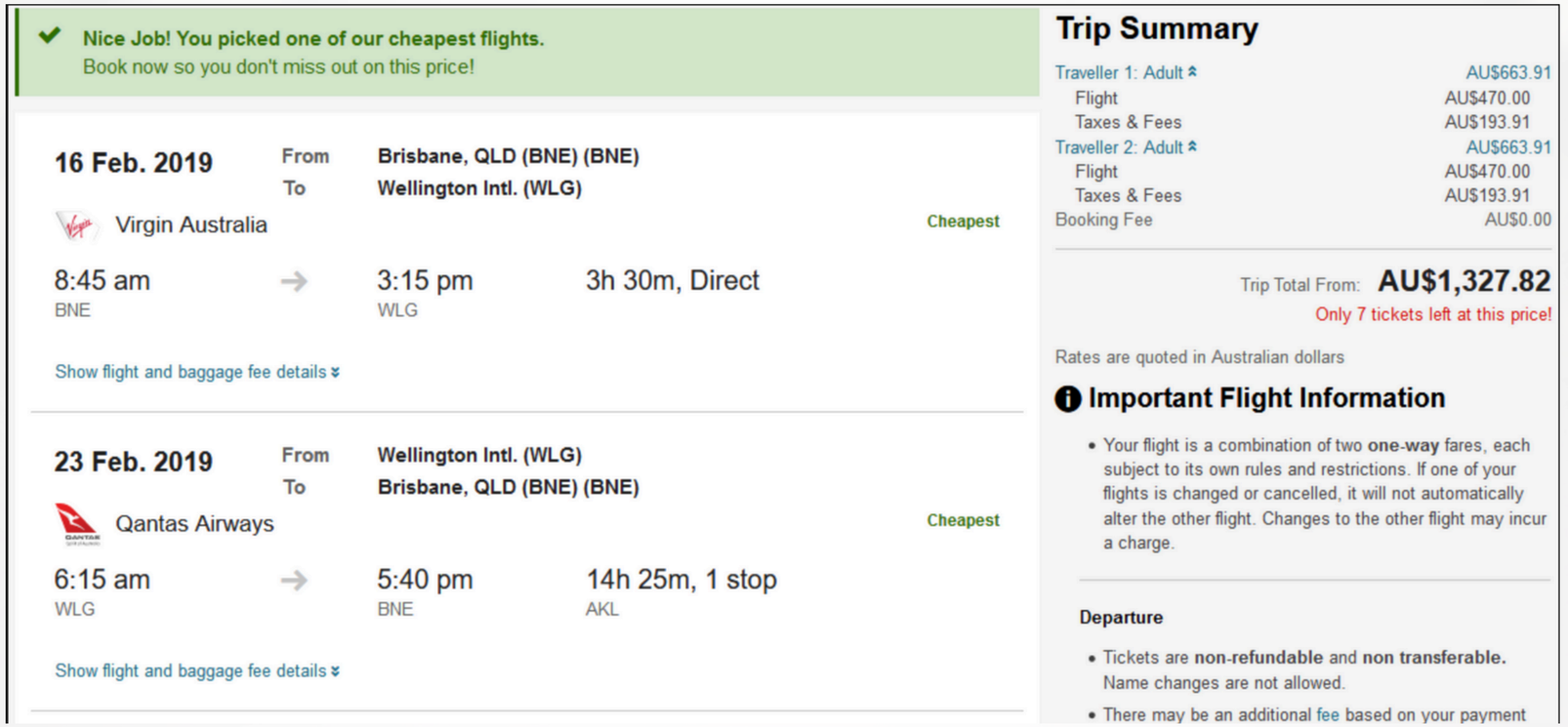
7.12 Timeline

File Tag Six



7.13 **Timeline**

File Tag Seven



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

16 Feb. 2019
From **Brisbane, QLD (BNE) (BNE)**
To **Wellington Intl. (WLG)**

Virgin Australia — Cheapest

8:45 am BNE → 3:15 pm WLG — 3h 30m, Direct

Show flight and baggage fee details

23 Feb. 2019
From **Wellington Intl. (WLG)**
To **Brisbane, QLD (BNE) (BNE)**

Qantas Airways — Cheapest

6:15 am WLG → 5:40 pm BNE — 14h 25m, 1 stop AKL

Show flight and baggage fee details

Trip Summary

Traveller 1: Adult	AU$663.91
Flight	AU$470.00
Taxes & Fees	AU$193.91
Traveller 2: Adult	AU$663.91
Flight	AU$470.00
Taxes & Fees	AU$193.91
Booking Fee	AU$0.00

Trip Total From: **AU$1,327.82**
Only 7 tickets left at this price!

Rates are quoted in Australian dollars

Important Flight Information

- Your flight is a combination of two **one-way** fares, each subject to its own rules and restrictions. If one of your flights is changed or cancelled, it will not automatically alter the other flight. Changes to the other flight may incur a charge.

Departure

- Tickets are **non-refundable** and **non transferable.** Name changes are not allowed.
- There may be an additional fee based on your payment

7.14 **Timeline**

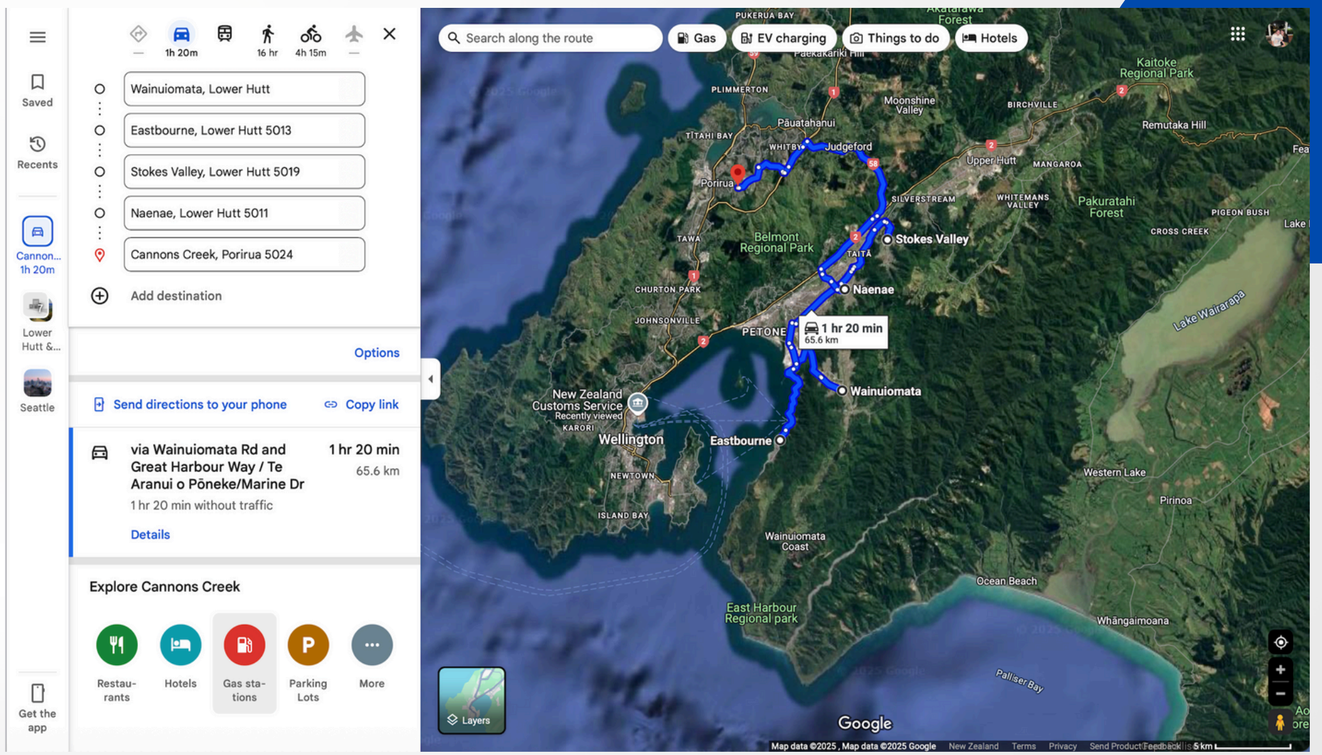
Future Plans

Identified earlier that Steve was searching for:

- “international drug routes
- “drug routes in around wellington”

indicating that the current Method run.jpg does not reflect their main area of operation.

Identified from analysis of google maps web searches, that Steve was also looking at areas in Porirua, specifically Cannons Creek. This could be a future expansion he may make.



8.1 **Anti-Forensics**

CCleaner

CCleaner.exe and CCleaner64.exe located in Program Files/CCleaner

Program run multiple times:

- 3x on 2019-01-31
- 4x on 2019-02-01

Cleans browser history, registry entries, and temporary files.

No log files found.

8.2 **Anti-Forensics**

TrueCrypt

Identified TrueCrypt.exe in Program Files/TrueCrypt

Executed multiple times between 2019-01-30 and 2019-02-02

Configurations.xml for TrueCrypt contained settings:

- CachePasswords = off
- SaveVolumeHistory = off
- WipePasswordCacheOnExit = off
- WipeCacheOnAutoDismount = on

No encrypted volumes found.

8.3 **Anti-Forensics**

Image Steganography

Used Image Steganography Tool downloaded from SourceForge.

Discussion of Steganography in Discord conversation’s between Steve and John.

Identified BNE.png file downloaded from ProtonMail. Required password, “Elchapo2”, to decrypt using Steganography tool used.

Revealed package.png, containing suitcase with a hidden compartment and three wrapped packages to the right of the case.

8.4 **Anti-Forensics**

Virtual Machine

Identified presence and repeated use of VMware Tools suggesting virtual environment for concealment of user actions.

Located program vmtoolsd.exe in Program Files/VMware/VMware Tools.

Ran multiple times between 2019-01-20 and 2019-02-02

9.1 **Limitations and Recommendations**

Multiple obfuscation and anti-forensics measures were employed and actively used on the desktop including:

- TrueCrypt
- CCleaner
- Virtual Machine

This resulted in not identifying further user behavior (logfiles, registry, caches) possibly limiting the scope of the cases analysis.

9.2 **Limitations and Recommendations**

Analysis of web accounts. Identified that the user, used the default user when logging into Chrome, but identified that the user had:

- Microsoft account
- Proton mail account
- Discord account

Further and deeper analysis into these three and possibly identifying earlier chats between Steve and John could be extracted at a later time.

9.3 **Limitations and Recommendations**

Virtual Machine issues when running Autopsy case. Due to the lack of memory and limited volume segmentation in my virtual environment.

This caused some Autopsy modules to be slow or ineffective leading to gaps in analysis.

End of Witness Testimony