CSN11125 Host-Based Forensics

Host-Based Forensic Analysis Project

Coursework – Car Theft Investigation

Matriculation Number: 40796843

Azarin Bayali

December 23, 2025

Declaration of Academic Integrity and Use of Artificial Intelligence

I declare that this coursework is my own work and that it has not been submitted for any other assessment. All sources of information have been acknowledged and referenced appropriately.

I confirm that I have complied with Edinburgh Napier University's regulations on academic integrity and assessment. All interpretations, evaluations, conclusions, and technical decisions presented in this report are my own. I take full responsibility for the accuracy, originality, and academic integrity of the submitted work.

Executive Summary

The purpose of this project is about the investigation of digital evidence from three devices, including a Windows computer, a mobile phone, and a USB flash drive. These devices belonged to a man named Roger, who is suspected of involvement in the theft of several high-value cars. The purpose of this investigation is to determine responsibility for the offences, against Roger whether the crimes were motivated by the kidnapping of Roger's brother Jimmy, and to reconstruct the timeline of events. The analysis focused on Discord and SMS communications, images, web searches, and map searches recovered from the seized devices. Overall, the message evidence extracted from Discord indicates that Roger played a central role in organising the vehicle thefts alongside several associates. Images shared during these communications were intentionally altered to conceal photographs of target cars. Further messages demonstrate reconnaissance activities, route planning, and discussion of tools used for vehicle theft. The offenses appear to have been motivated by pressure from Jimmy's gambling activities and subsequent kidnapping. Messages indicate that Jimmy initially won money from gambling but later suffered significant financial loss. Communications report that Jimmy had been kidnapped and was in debt for a $250,000 amount of money. Messages further indicate that the kidnappers were not looking for cash but instead demanded specific luxury cars. Later communications from Roger confirm that the cars were successfully delivered, supporting the conclusion that the thefts were carried out to satisfy these demands. Reconstruction of timeline demonstrates that Jimmy's kidnapping in mid-March appeared first, following the Roger's plan to rescue his brother. In the days followed reconnaissance and planning activities took place, culminating in the theft and delivery of vehicles on 27–28 March.

Timeline of Key Events

Table 1: Summary timeline of key actions by the relevant user

Date / Time	Source	Event	Relevance
2025-03-14	Online messages	Jimmy reports winning a significant amount of money through gambling.	Gambling escalation
2025-03-16 14:50	SMS	Jimmy reports that he has lost a large sum of money gambling.	Gambling loss
2025-03-18 19:06	SMS	Message sent from Jimmy's phone stating he has been kidnapped and owes £250,000.	Kidnapping
2025-03-18 19:20	SMS	Message states kidnappers are not interested in money but want something else.	Demand context
2025-03-23	Discord	Roger and associates begin discussing scouting and vehicles using coded language.	Planning phase
2025-03-24	Web history	Searches for high-value cars and vehicle security information observed.	Reconnaissance
2025-03-24	Discord	Images shared using food-related names (e.g. avocado, burger, pasta).	Target selection
2025-03-25	Web history	Searches related to data hiding and image concealment techniques.	Intent to conceal
2025-03-26	File system	Modified image files created and stored on Roger's computer.	Preparation
2025-03-26	Email	Roger emails a password-protected archive containing concealed images.	Concealment
2025-03-27 (morning)	Discord	Message states "tomorrow is the day we grab the ingredients".	Imminent execution
2025-03-27 (evening)	Discord	Plans discussed to meet at Ocean Terminal and bring gloves.	Final coordination
2025-03-28 (morning)	Discord	Route map shared between participants.	Execution
2025-03-28 (during)	Discord	Status updates indicate activity is "going smoothly".	Theft in progress
2025-03-28 (later)	SMS	Message sent stating that the cars have been "dropped".	Completion
2025-03-28 (later)	SMS	Communication implies the demand linked to Jimmy has been satisfied.	Resolution

1 Introduction

1.1 Case background and remit

Investigation in this report concerns the forensic examination of digital devices belonging to an individual named Roger, who is suspected of involvement in a number of car thefts. Law enforcement seized three digital evidences associated with Roger: a Windows 11-based personal computer, a mobile phone, and a USB flash storage device. The seized devices further provide evidence that Roger may have engaged in criminal activity connected to the kidnapping of his brother, Jimmy, and subsequent demands made by unknown third parties.

Available evidences indicate that Jimmy was interested in gambling activity and later suffered significant financial losses. Communications recovered from Roger's devices clearly demonstrate that Jimmy has been kidnapped and that a large debt was owed. Additionally, communications between kidnappers and Roger indicate that perpetrators were not seeking a financial payment but instead demanded specific cars above a particular price. Following these events, digital artifacts show coordinated planning and reconnaissance of high-value car thefts involving multiple friends of Roger. Use of encrypted messages, concealed images, and coded language suggests evidence about the avoidance of detection.

1.2 Investigative questions

The investigation was guided by the following key questions:

Investigative Questions

1. Who appears to be responsible for the theft of the high-value vehicles, and what roles did the involved individuals play?
2. To what extent were the vehicle thefts motivated by Jimmy's gambling-related debt and subsequent kidnapping?
3. How did the events unfold over time, from the initial gambling activity through to the planning and execution of the vehicle thefts?

These questions inform the structure of the report and underpin the analysis of communications, images, scripts, and online activity recovered from the examined devices.

2 Methodology

2.1 Forensic approach and standards

The examination of evidence was conducted in accordance with the recognised digital forensic principles and analysis. The forensic images of devices were provided in a forensically prepared state; the scope of the investigation was limited to analysis, interpretation and reporting rather than acquisition or preservation.

The analytical process followed initial triage and artifact identification, detailed examination of relevant data, correlation of artifacts across multiple sources, and interpretation of findings within the context of the investigative questions. Particular attention was paid to maintaining objectivity during analysis. Artifacts were analyses in correlation in order to create a detailed and correct timeline and connections between evidence in different devices.

2.2 Tools and environment

The primary forensic tool used during the investigation was Magnet AXIOM, which was deployed to examine the digital images associated with Roger's devices. AXIOM was easy to use due to its ability to parse and carve a wide range of artifact types, including communications, images, web activity, and file system metadata, within a single investigative environment. Furthermoe, it provided functionalities like creating a timeline of artefacts and making connections between the evidence.

In addition to automated artifact extraction, for specific cases such as decoding ciphertexts and messages, a number of manual analysis techniques were applied. For these analysis online decoding utilities like Dencode and simple XOR-based decryption tools were used. Image files are suspected of containing hidden content using a simple steganography technique. Those images were examined using the StegHide tool, and with a number of online steganography tools, as well as file structure comparison, and metadata review was conducted. File system functionalities in Magnet AXIOM were also used to conduct identification of custom scripts and directories of interest that were not automatically highlighted by forensic tools.

2.3 Analysis workflow

The first step of analysis was a high-level review of artifacts extracted by Magnet AXIOM, initially focusing on the mobile phone specifically. Keyword searches and data filtering were used for deeply analyzing the dataset to the relevant time period in March for communications, email messages, images, scripts, and browser history. Certain communications from Discord and SMS were parsed by the forensic tool, and those evidences was

undertaken to ensure relevant connections between messages and relevant web searches and map searches. Encoded messages found in the CipherBot group in Discord were identified and decoded through step-by-step analysis to reveal their plaintext content. Custom script CipherBot.py discovered on the computer was reviewed to understand the function and relevance to communication concealment for decoding the messages.

For modified images, concealment techniques were investigated by comparing original image files with modified versions and examining associated browsing activity related to data hiding techniques using the StegHide tool. Timeline reconstruction was achieved by correlating timestamps from messages, files, and browser activity across devices, allowing events to be sequenced and cross-validated.

3 Findings and Analysis

3.1 Email and SMS Message Findings

3.1.1 SMS Messages: Gambling, Debt and Kidnapping

SMS messages exchanged between Jimmy and Roger provide a clear background events leading up to the Jimmy's kidnapping and Rogers car thefts. As shown in Figure 1 ,early messages indicate that Jimmy was actively involved in gambling, including pocker games in which he won significant amount of money in one night.

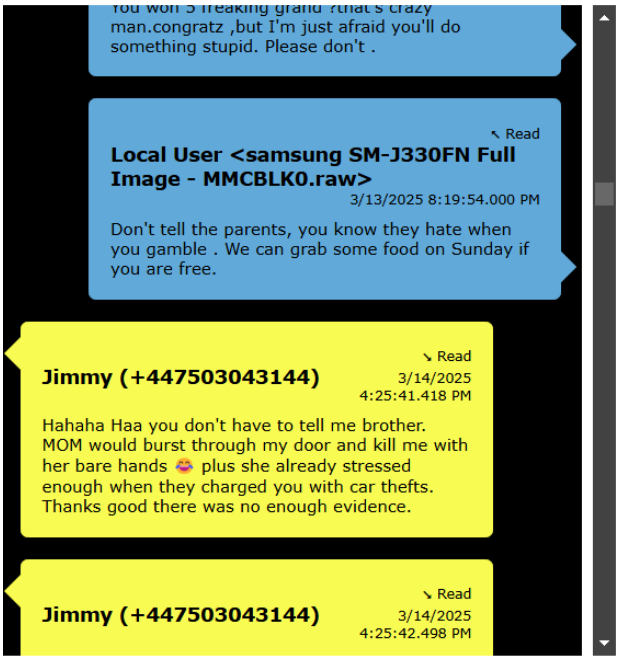


Figure 1: **Evidence E01:** Messages Between Roger and Jimmy

On 18 March 2025, Roger received a message from Jimmy's phone stating that Jimmy had been kidnapped and owe $250,000 to kidnappers. However, kidnappers were "not

interested in money". This communication is a key finding, as it demonstrates both the reason of kidnapping and the unusual nature of the car thefts.

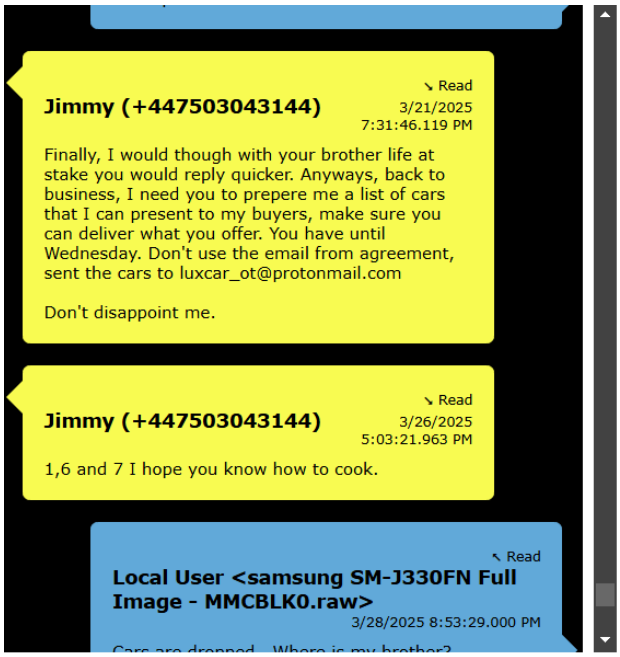
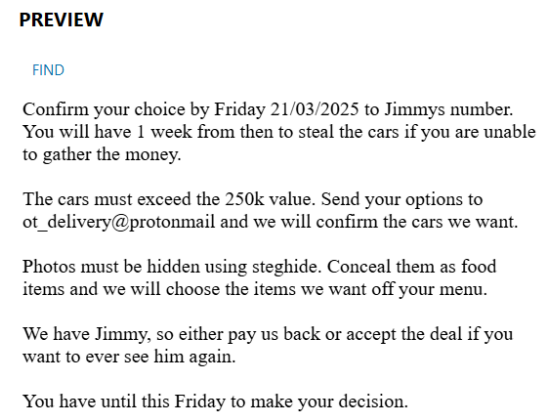


Figure 2: **Evidence E02:** Message From Kidnapper

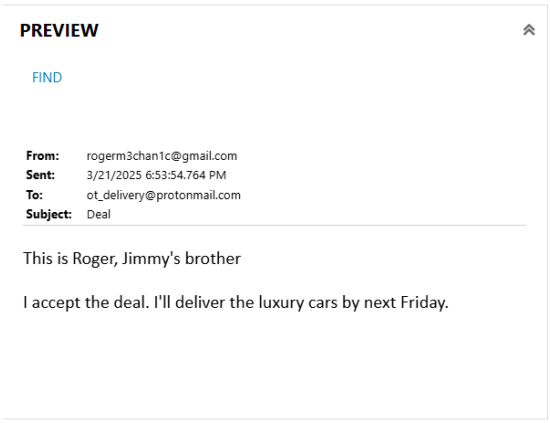
The message contains keywords that were useful later on investigation: food, cooking, images numbered 1, 6, 7 and domain address that kidnapper are going to use for communication.

3.1.2 Email Communications

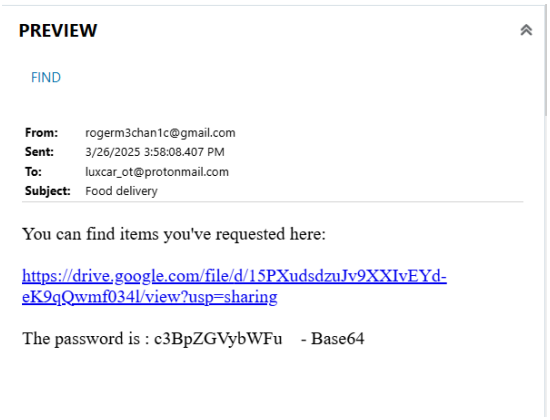
In the list of email artefacts of Roger's mobile phone, there was found a suspicious message between Roger and the "luxcar_otprotonmail.com" domain that was mentioned earlier in SMS messages. Initially, there is an email containing the deal, how much money Jimmy owes, and how much time Roger has to steal the cars. Further, on 21 March 2025, there is an email from Roger, accepting the deal, and on 26 March 2025, he sends a zipped file with food pictures with a Base64 encrypted password. After decryption, we see that the password for the zip file is "spiderman". The nature of the final email with food pictures is suspicious due to the apparent mismatch between the recipient address, which suggests an association with luxury vehicles, and the contents of the archive in Roger's computer, that was investigated later on. The use of password protection and encoding indicates an attempt to restrict access and conceal the true nature of the contents.



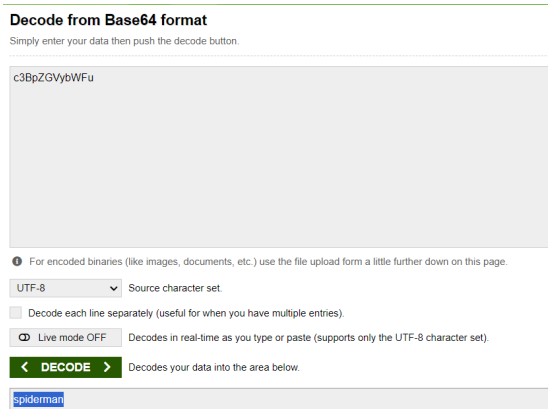
(a) Kidnapper Deal with Roger



(b) Roger accpets the deal



(c) Email with zipped images



(d) Password of the zip file

Figure 3: **Evidence E03:**Email related images from kidnappers

3.2 Discord Communications and Encrypted Messaging

3.2.1 Identification of Participants and Roles

Discord artefacts recovered from Roger's computer reveal communications between a number of his friends using sometimes clear and sometimes hidden usernames. These include Roger himself, along with associates believed to be involved in planning, which are Jay with username "jaythedude690_37803" and an unknown frined with username "zerofrequency_67159". Additionally, there was a friend, Erik "ezericc_88003", providing "technical support" and reconnaissance activities. The content and tone of the messages indicate coordinated activity rather than casual conversation, with discussions focused on planning, logistics, and concealment.

3.2.2 Use of CipherBot for Message Concealment

Under the folder labelled "bot" in Roger's computer, was discovered a Python script referred to as "CipherBot" was discovered. Examination of the script shows that it

applies a two step encryption of specific messages, involving first an XOR operation using a long key, and followed by Base64 encoding.

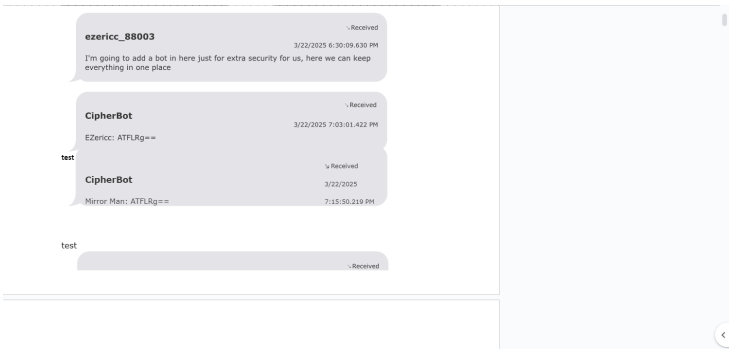


Figure 4: **Evidence E04:** Discord Decrypted Messages

For decoding the messages, manual decoding was used, reversing the encryption process. The first online DenCode tool was used to decrypt from Base64, and Manual XOR decryption using the key in a Python script. The message was decrypted. The decryption of the messages revealed important details about the planning process of the car thefts.

3.2.3 Planning and Target Identification Using Coded Language

Discord messages between March 22 and March 28 in the CipherBot group contain important details of the planning process. Messages between March 22 and March 26, Roger and his friends are planning on which cars to pick for the theft, and according to the messages they send each other photos using some kind of passwords.

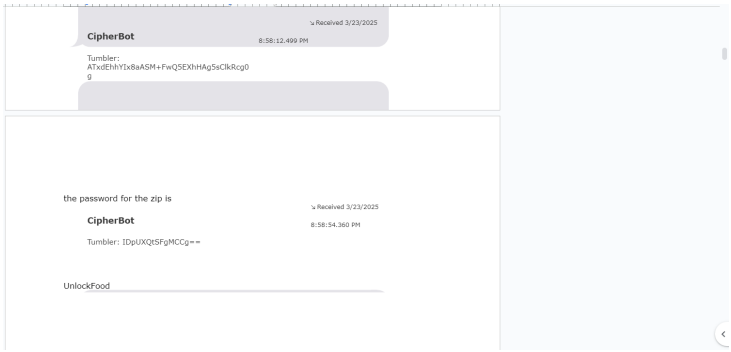


Figure 5: **Evidence E05:** Discord Decrypted Messages

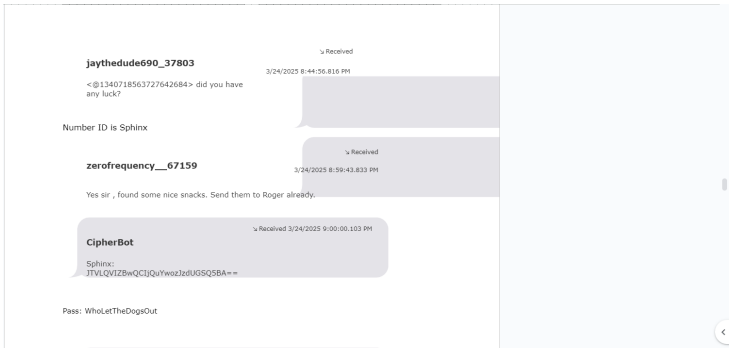


Figure 6: **Evidence E05:** Discord Decrypted Messages

Further messages describe "scouting food", "sending the menu", and selecting particular "dishes", which aligns closely with the later discovery of image folders containing food photographs corresponding to specific car images. Between 24 and 27 March 2025, messages indicate that from the list of selected seven cars, three potential targets were chosen by the kidnapper.

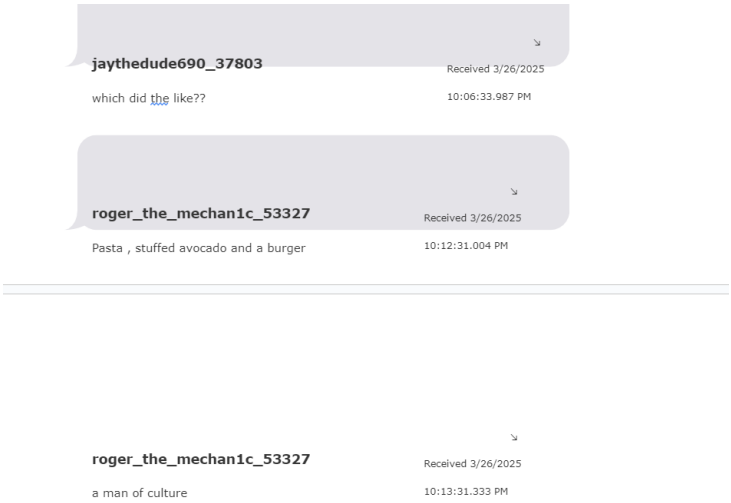


Figure 7: **Evidence E06:** Discord Decrypted Messages

Statements such as "they picked three for the cook off" and "Pasta, stuffed avocado, and a burger" strongly prove statements in previous emails that the kidnapper chose for Roger to steal cars in the images numbered 1, 6, and 7. Finally, in 28 March 2025, Roger send the planned route through encrypted messages, a Google maps route link. As shown in the picture, the route is closely related to Ocean Terminal station. The route of three addresses, each connected to Ocean Terminal station.

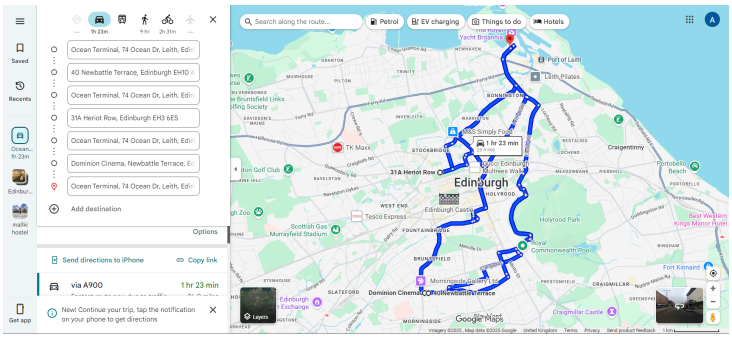


Figure 8: **Evidence E06:** Google Maps Route

3.3 Image and File System Findings

The images were found in Roger's phone gallery, where the dates that the files were created play a very crucial role. Pictures of Jimmy in Figure 10 were created on March 19 2025, at 6:07 PM, the day when Jimmy went missing, and the kidnapper first time contacted Roger through Jimmie's phone. The second image, however, has been taken on March 28, at 6:29 PM, a few hours before Roger send message to Jimmy's phone about "dropped cars".

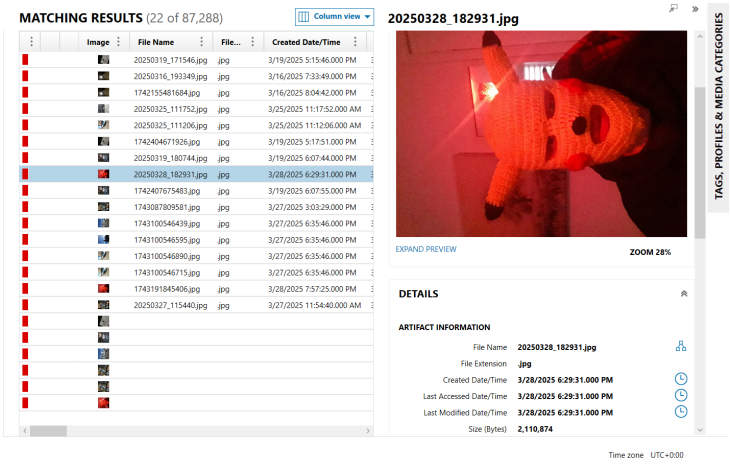
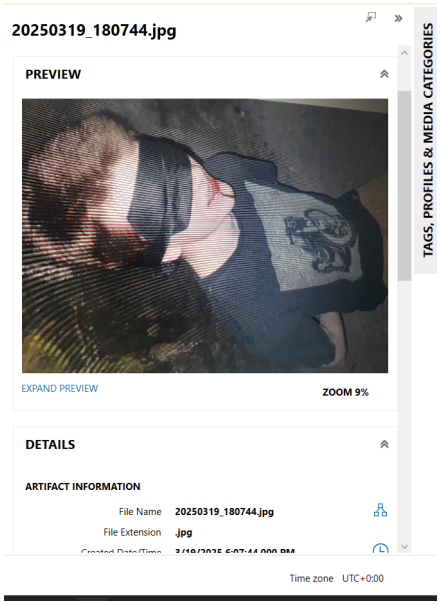
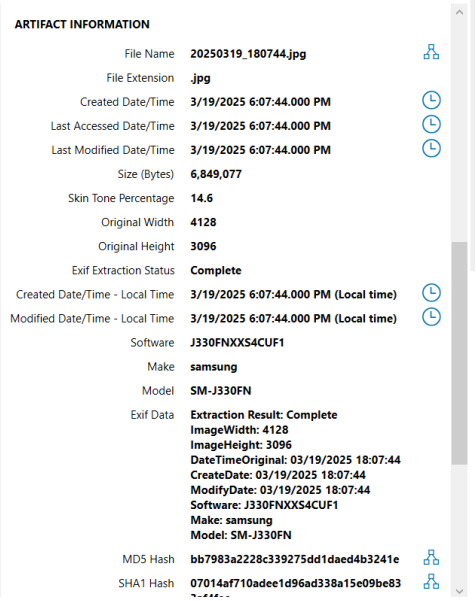


Figure 9: **Evidence E07:** Potentially Kidnapper image



(a) Jimmies image after kidnapping



(b) Jimmies image metadata

Figure 10: **Evidence E08:** Jimmies image taken by kidnapper in Roger's phone

3.3.1 Food and Vehicle Image Correlation

As mentioned before, analysis of the "food.zip" from email and the directory "Victor" revealed images of food items, including avocado, burger, and pasta. A separate folder located under the same Victor directory, labelled "cars," contained images of vehicles with filenames and quantities closely matching those found in the "food.zip" folder. Within this directory, an original subfolder contained unmodified car images, while other versions appeared slightly altered.

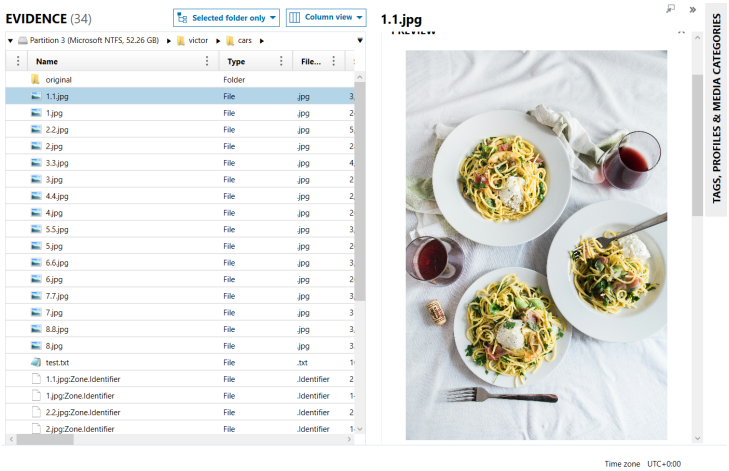


Figure 11: **Evidence E09:** Modified car image

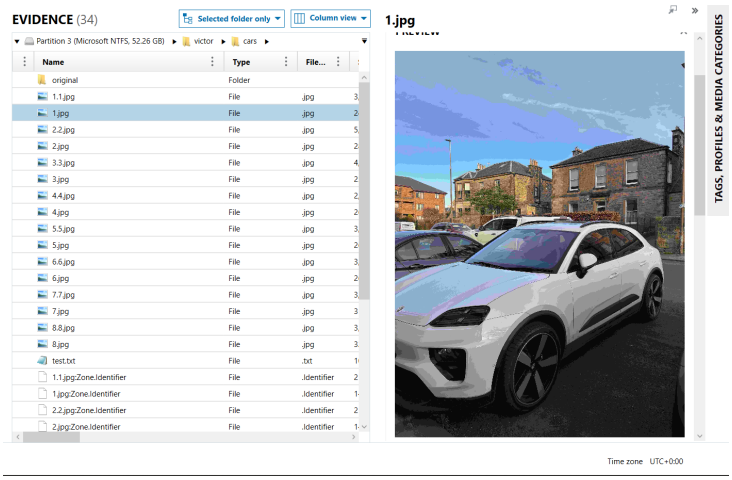


Figure 12: **Evidence E10:** Car image

!!!

3.3.2 Steganography Analysis

Web browsing artefacts found in Roger's computer reveal searches for steganography techniques and manuals, suggesting an intent to hide data within images. In addition, the metadata examination of the images under the "food" folder and "cars" folder has notable similarities, including creation and modification timestamps and closely matching file naming structures. Although attempts to decode the images using commonly available steganographic analysis tools, such as online StegDecoder and Steghide tool, extracting the hidden image have failed due to an unknown passphrase. However, the convergence of metadata indicators, correlated communications, and references to food imagery within encrypted Discord messages supports the idea that food images were used as coded representations of target vehicle images.

3.4 Web Browsing, Tools, and Location Evidence

3.4.1 Searches Related to Vehicle Theft and Tools

Web history artefacts show searches related to vehicle security, how to open cars and the use of "clicker" devices commonly used to unlock cars. There are specific artefacts with Amazon URL and other online shop searches about the lockpick set and flipper device, additionally there are images of the deliverie of these device in Roger's phone.

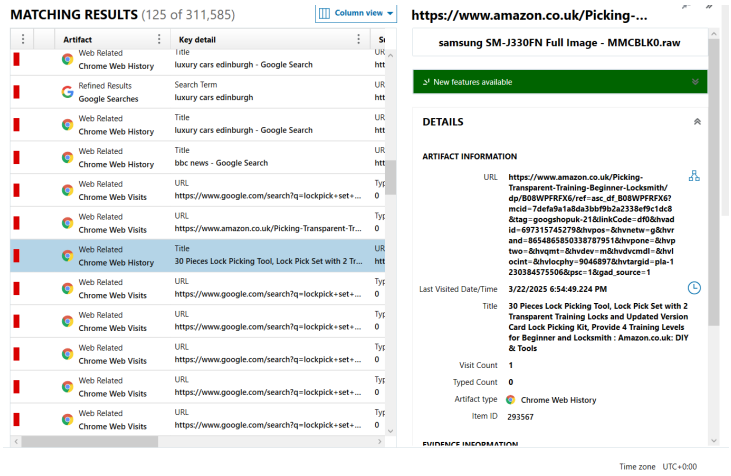


Figure 13: **Evidence E12:** Amazon lockpick set

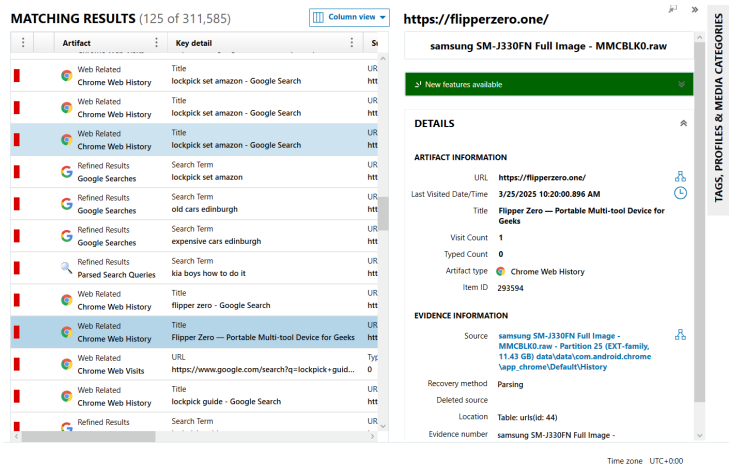


Figure 14: **Evidence E13:** Flipper Tool

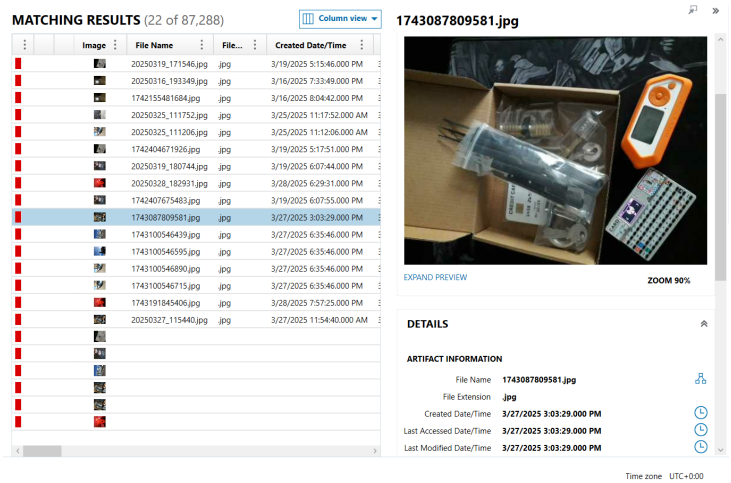


Figure 15: **Evidence E14:** Delivary Image

Furthermore, there are related messages in the CipherBot group where Roger and his friends are discussing the car-picking techniques and which tools can be used for this kind

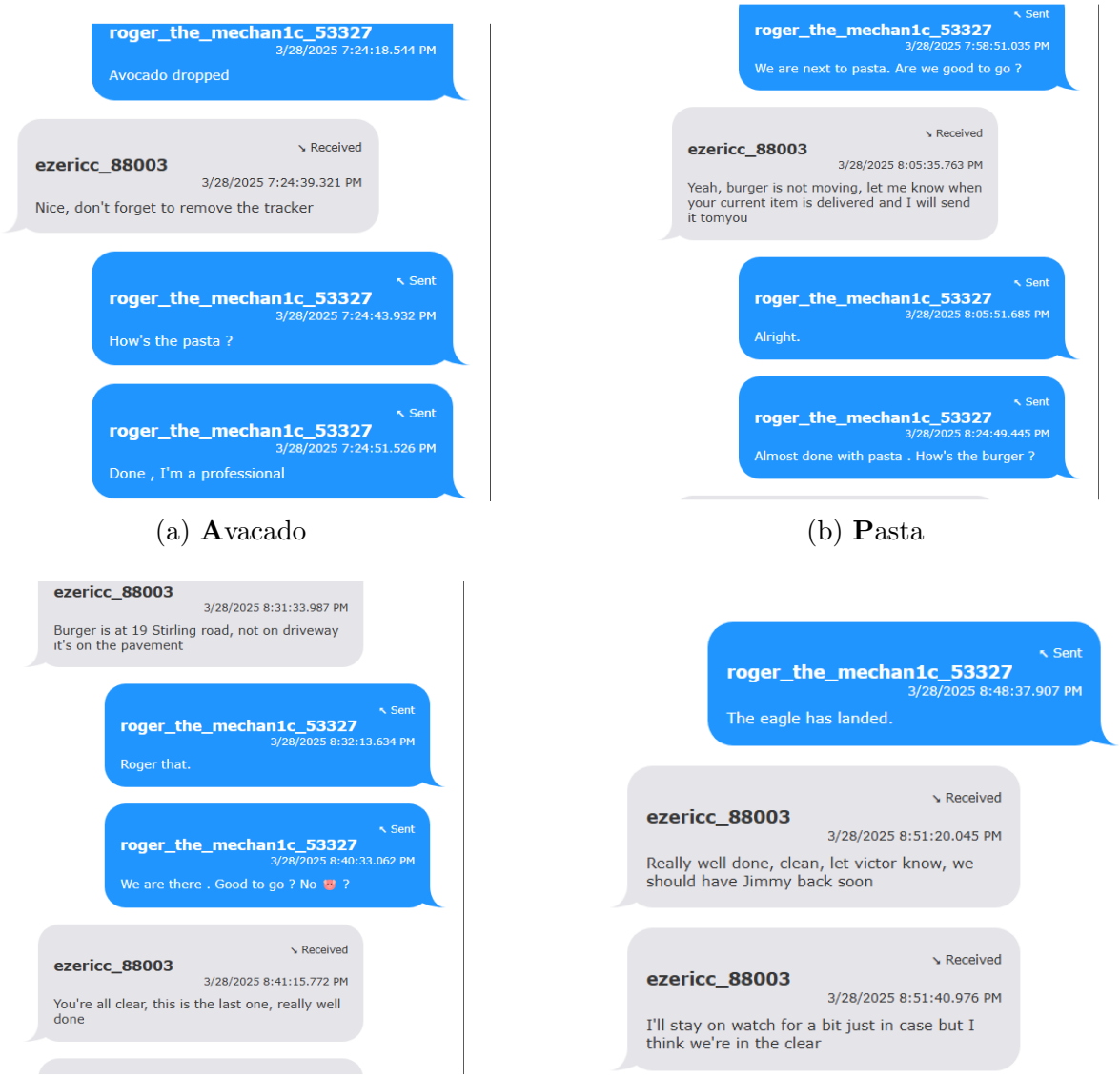
of thefts. Additionally, the dates of the messages, web searches, and images are overlap, creating a logical conclusion that Roger and his associates indeed were actively researching methods to access vehicles without keys and steal them to rescue Roger's brother Jimmy.

3.4.2 Google Maps and Route Planning

As mentioned earlier, disocrd messages on 28 March 2025 include a shared Google Maps link corresponding to the day of the vehicle thefts. Furthermore, there is an additional Discord message between Roger and a user named "ezeric" on 28 March 2025 between 7:09 and 8:54; this date and time are similar to the message Roger sent to Jimmy's phone (to the kidnapper) that cars are ready. On of the messages indicates that a car with the name "Burger" is at Stirling road 19. The time frames while user "ezeric" and Roger are talking about the cars "Pasta", "avocado", and "burger", are the same as the time frames of the Google Maps searches of the addresses that are shown in the Google Maps route shared link sent earlier to the Discord CipherBot group.

	Location & Travel Google Maps Search...	Search Term Ocean Terminal	Location Ad... Ocean Termi...		Searched Date/Time 3/28/2025 8:43:12.389 PM	288765
	Location & Travel Google Maps Search...	Search Term Newbattle Terrace	Location Ad... Newbattle T...		Searched Date/Time 3/28/2025 7:54:19.298 PM	288766
	Location & Travel Google Maps Search...	Search Term 19 Stirling Road	Location Ad... 19 Stirling R...		Searched Date/Time 3/28/2025 8:31:58.565 PM	288767
	Location & Travel Google Maps Search...	Search Term 40 Newbattle Terrace	Location Ad... 40 Newbattl...		Searched Date/Time 3/28/2025 5:30:54.627 PM	288768
	Location & Travel Google Maps Search...	Search Term 31A Heriot Row	Location Ad... 31A Heriot R...		Searched Date/Time 3/28/2025 5:30:54.627 PM	288769
	Location & Travel Google Maps Search...	Search Term Heriot Row	Location Ad... Heriot Row,...		Searched Date/Time 3/28/2025 6:45:02.321 PM	288771
	Location & Travel Google Maps Search...	Search Term Dominion Cinema	Location Ad... Newbattle T...	Categories Cinema	Searched Date/Time 3/28/2025 5:30:54.627 PM	288772

Figure 16: **Evidence E15:** Google maps addresses



(a) **A**vacado (b) **P**asta

(c) **B**urger (d) **A**ll the cars dropped

Figure 17: **Evidence E16:** The messages of the cars placed in the addresses defined in below Google maps image

According to images, the last car was dropped in Ocean Terminal, and at 8:43 PM on 28 March 2025, at the same time, Roger sends a message to Victor (to Jimmie's phone) that the cars are dropped.

3.5 USB Artefact Analysis

Another important device identified among the digital evidence was USB flash storage. The presence of the removable device first noticed among the images in mobile of phone of Roger in below image, assuming that flash drive was sent by someone to Roger.

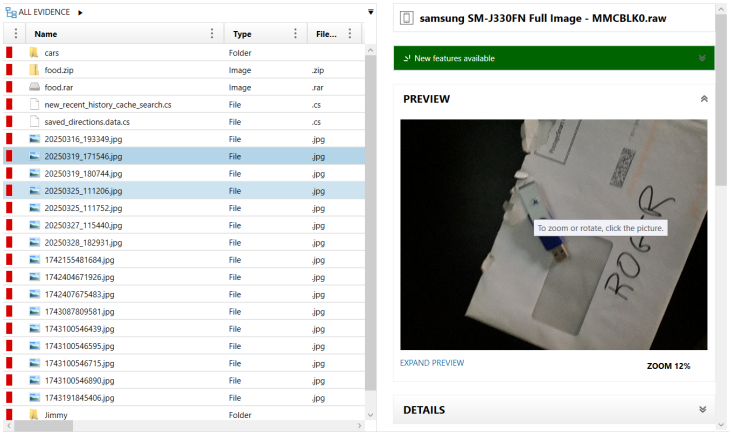


Figure 18: **R**emovable Device Image

Among the found artefacts in the USB device, there were the same images of Jimmy and a text about the repayment that Jimmy owes. The creation date information of the images in the USB device is similar to the date in the Windows computer however, the timestamps are different, and there are a few hours between two images. On both device images were created on 19 March 2025; the creation time on the USB device is 2:06 PM, and on the Windows Device around 6 PM. In addition, there is a suspicious Readme.txt file on flash drive created the same date just few minutes after the image creation time. The content of the text file clearly indicate that for the repayment of Jimmy's debt kidnapper request 3 Luxury Cars, which value should exceed the debt money. Moreover, the kidnapper indicate that Roger has just 1 week to steal the cars and all communications should be established through the "ot_delivery@protonmail" mail address. Since all these evidences already available on a computer device, and the originating device metadata shows a Samsung phone, it is plausible that these artefacts were copied from a USB device to a Windows Computer device.

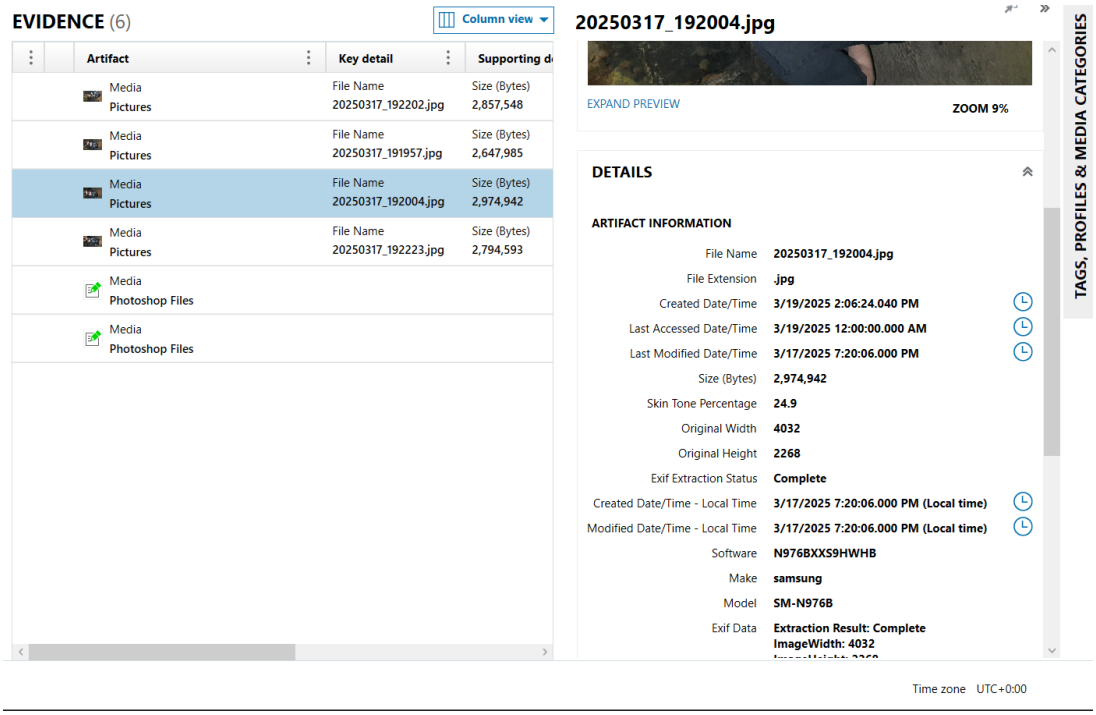


Figure 19: **Evidence E17:** USB device image

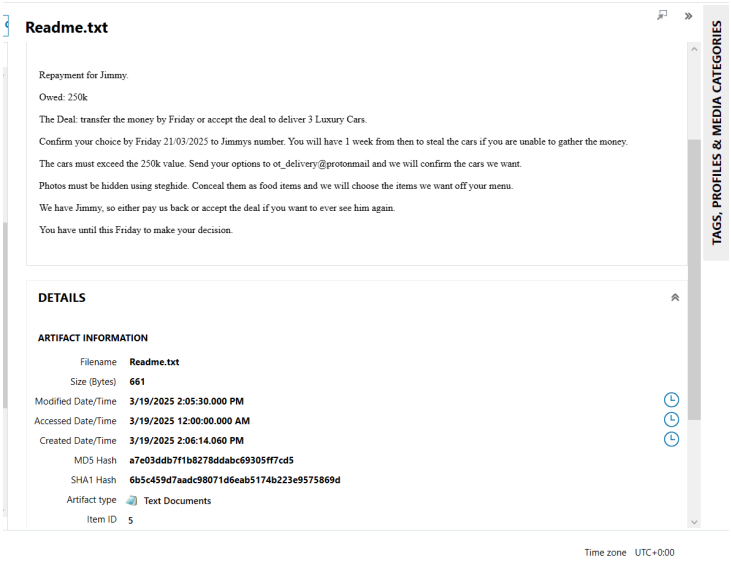


Figure 20: **Evidence E18:** README.TXT

4 Conclusion

The digital evidence provided in this report collectively provide clear view and timeline of the events, moreover artefacts consistently answer the investigation questions regarding the responsibility and motivation of car theft and Jimmie's kidnapping. Communication evidences, particularly SMS, Discord and Google Email messages, provide a useful roadmap for searching other artefacts. Furthermore, according to the messages, most of

the event questions can be answered. In addition, AXIOM Magnet provided timestamps to all evidences, which made it easy to make connections between different artefacts found in all three devices. After decoding encoded Discord messages further strengthens the evidential value of Roger's car thefts, motivated by Jimmie's kidnapping because of the gambling debt. Successful decryption revealed operational details of the planning process between Roger and his associates, providing details such as passwords and route information. Although the encryption algorithm was technically simple, its usage demonstrates an intent to hide the event-related communications. Similarly, the use of steganography to hide the original stolen car images shows awareness of investigative risk. Web browsing history artefacts, including searches related to "picking a car" or "opening cars without keys" with a flipper device, further support the scenario of the project. Overall, the correlation of all the inter-connected evidences deliver groundwork supporting the conclusions reached, the probabilities questioned in the beginning of the project.