**Graphical user interface

Description automatically generated with medium confidence**

|  |
| --- |
| Photo displaying partial image of two pie charts on a canvas-textured page |
| OPERATION NARCOS  DIGITAL FORENSIC EXAMINATION OF STEVE KOWHAI  Version 2.0 |
| |  |  |  | | --- | --- | --- | | Shishir Saxena Hope Posesione | 22/11/2024 | ISCG 7404 | |

# EXECUTIVE SUMMARY

This forensic investigation is related to Operation Narcos, as it began with two passengers intercepted and searched by a Wellington Customs Officer, following intelligence provided by the Australian Government. The suspects, who were found in possession of methamphetamine and other illegal materials, are believed to be involved in a more extensive drug distribution network.

Forensic analysis was required in this case as digital devices, including two laptops and a desktop computer, were seized from the suspect's residence, which may hold evidence of illicit activities.

Various digital forensic tools like FTK imager, Autopsy, Bulk extractor, software write blocker, etc., along with the best practices, were employed to maintain the sanctity of the evidence acquired.

The artifacts collected are summarized in the report.

Table of Contents

[EXECUTIVE SUMMARY 1](#_Toc183188785)

[1. INTRODUCTION 4](#_Toc183188786)

[2. ENGAGEMENT AND SCOPE 4](#_Toc183188787)

[2.1 Interrogation and Search 4](#_Toc183188788)

[2.2 Suspect Involvement 4](#_Toc183188789)

[2.3 Our Role 4](#_Toc183188790)

[3. Scope of Investigation 5](#_Toc183188791)

[3.1 Evidence Acquisition 5](#_Toc183188792)

[3.2 Data Integrity 5](#_Toc183188793)

[4. FINDINGS AND DISCUSSIONS 6](#_Toc183188794)

[4.1. Timeline - Steve Kowhai 6](#_Toc183188795)

[4.2 Registry Analysis and OS and Partition Information 6](#_Toc183188796)

[4.3 Examination of Communication Logs ( dates from 28/01/2019 to 01/02/2019) 6](#_Toc183188797)

[4.4 Examination of unallocated files and recovered files: 7](#_Toc183188798)

[4.5 Detailed Chain of Custody 8](#_Toc183188799)

[4.6 Findings 9](#_Toc183188800)

[5. DIGITAL EXAMINATION 10](#_Toc183188801)

[5.1 Forensic Procedures and Tools 10](#_Toc183188802)

[5.2 FTK Imager 10](#_Toc183188803)

[5.3 Registry Viewer 10](#_Toc183188804)

[5.4 Bulk Explorer 10](#_Toc183188805)

[5.5 Image Steganography Tool 10](#_Toc183188806)

[5.6 Autopsy Tool 10](#_Toc183188807)

[5.7. Detailed examination of user Steve Kowhai’s desktop and tools used 11](#_Toc183188808)

[5.7.1 Desktop details from Registry Explorer and Autopsy. Partition from FTK Imager 11](#_Toc183188809)

[5.7.2 Web activity from Autopsy 11](#_Toc183188810)

[5.7.3 Images Downloaded from Autopsy 12](#_Toc183188811)

[5.7.4 Email/chat activity from Autopsy and Bulk Extractor 12](#_Toc183188812)

[5.7.5 Encrypted conversation from Bulk Extractor 12](#_Toc183188813)

[5.7.6 Deleted files recovered: earlier stored in the pictures folder of Steve 12](#_Toc183188814)

[5.7.7 Steganographic Activity 12](#_Toc183188815)

[6. CONCLUSION 13](#_Toc183188816)

[7 APPENDIX FOR ARTEFACTS 14](#_Toc183188817)

# ****1. INTRODUCTION****

This report focuses on the forensic examination of Steve Kowhai’s uncovering communications, documents, and other digital artifacts that provide insight into the suspect's motives and involvement in the drug trafficking operation.

The investigation includes multiple areas of digital forensics, such as examining OS and partition details, email forensics, unallocated space and recovered files, relevant files and folders, registry analysis, and live memory forensics using Bulk Extractor for RAM artifacts.

Moreover, this analysis report will detail the investigative procedures taken and the evidence uncovered, emphasizing timestamps, dates, and maintaining the chain of custody to ensure the integrity and reliability of the findings.

# 2. ENGAGEMENT AND SCOPE

## 2.1 Interrogation and Search

Following the statement provided by Jane Esteban during the interrogation, she was aware of the hidden drug John Fredricksen had instructed her to deliver the suitcase to the “Eastbourne Library.” If any issues arose, she was told to take it to 666 Rewera Avenue, Petone in Wellington.

However, when authorities arrived at the specified address, they found drugs, firearms, and a desktop computer in the living room, but no one was present during the search.

## 2.2 Suspect Involvement

To gain insight into the case, the following sections will detail the forensic evidence of Steve Kowhai, covering both forensic images and Live RAM acquisitions that can shed light on his involvement in events related to the case.

## 2.3 Our Role

Through a detailed analysis of digital artifacts, our role as Forensic Investigator aims to build a thorough understanding of Steve’s potential involvement, such as downloading sensitive files and revealing critical information to a compelling case.

# 3. Scope of Investigation

## 3.1 Evidence Acquisition

a. Acquisition of images for Steve Kowhai’s computer:

* We acquired the images for Steve’s drive and memory with a software write blocker (as we must copy from the remote location). This was done to ensure that we do not add or modify the mages inadvertently and that the sanctity of the suspect’s file remains intact.
* We re-ensured this with the hash analysis by stating that both files have identical hashes before and after copying.
* We stored this copied image as original on our computer and made a copy with the same hash for further analysis.

b. We maintained a ‘chain of custody’ of images in the required format throughout our analysis. This was to ensure the reliability and sanctity being preserved for further audit. (see section 4.6 of this report).

## 3.2 Data Integrity

The digital hash value of the evidence collected at the scene was verified to ensure no modifications have occurred, and this is considered to have remained intact and unaltered.

* *Refers to Appendix SO58, SO59, SO60.*

# 4. FINDINGS AND DISCUSSIONS

## 4.1. Timeline - Steve Kowhai

The investigation involves acquiring forensic images of a Desktop found during searches by law enforcement. Specifically, more details are provided in section 5.7 of this report. The analysis utilizes forensic tools to examine the image files exclusively focusing on the user activity timelines for relevant evidence such as:

## 4.2 Registry Analysis, OS, and Partition Information

* User login: Steve
* Computer Name: SK-Desktop (*initials for Steven Kowhai*)

The artifacts and property owner of the found desktop are believed to be known as Steve Kowhai.

In recent open documents, referring to Appendix S030, S061, S062, S063 for timestamps, we found records of:

a) Recent Pictures and Document files (dates 31/01/2019 and 02/02/2019 refer to Appendix S064)

We know Steve has brought a return ticket to meet John in Brisbane.

Images provide plans of the whereabouts of Janes's package destination.

* C:/Users/Steve/Documents/Misc/flightbooking (refer to Appendix S026)
* C:/Users/Steve/Documents/Misc/dropoff.jpg, package.jpg, airport crystal.jpg, method run.jpg (refer to Appendix S064 for timestamps)

b) Recent Downloads (dates 31/01/2019 and 02/02/2019 refer Appendix S065)

* C:/Users/Steve/Downloads/BNE.jpg:
* C:/Users/Steve/Downloads/ccsetup.com
* TrueCrypt C:/Users/Steve/Downloads/TruCryprt7.Setup.exe

The time of events indicates that Steve Kowhai may be actively attempting to conceal evidence of illegal activities. The download of images with hidden steganographic data, cleaning tools, and the acquisition of encryption software suggest that he is trying to cover up his involvement in criminal activities, possibly related to illicit drug operations.

## 4.3 Examination of Communication Logs (dates from 28/01/2019 to 01/02/2019)

Analyzing email communication to uncover details related to the Drug trafficking operation. This included email accounts, attachments, messages, and more.

* Discord setup.exe and Protonmail were downloaded and installed (refer to appendix S068)
* Email records found (email sent/received, keywords, proton email account, phone number)
* Discord chatroom examining logs record of a conversation between Steve and John extracted from Autopsy (refer to findings section 4.6) discussing the smuggling operation.
* Also, a file ‘Secret’ was discovered received by [crayfish1980@protonmail.com](mailto:crayfish1980@protonmail.com) from an email sent by [heresjohnny1@protonmail.com](mailto:heresjohnny1@protonmail.com)
* John sent BNE.png image via discord attachment.

## 4.4 Examination of unallocated files and recovered files:

1. Recycle Bin (refer S020, S021, S022 and S064 for timestamps)

During the forensic examination, several documents were found that had been recently accessed by the suspect, including files related to illicit drug operations. They contained timestamps that are critical for establishing a timeline of events. As referenced in Appendix S064, these documents were opened shortly before specific deleted files were retrieved from the Recycle Bin.

## 4.5 Detailed Chain of Custody

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Chain of Custody History**  **Case Name: Operation Narcos**  **Date/Time Acquired: 14/10/2024 12.00 pm**  **Investigators: Shishir Saxena (SS) and Hope Posesione (HP)**  **Artifacts:** Disk Image Narcos-1.00-021 | Narcos\_Mem-1.001-003  **Location of seizure:** 666 Rewera Avenue, Petone Wellington | | | | | |
| **SN** | **Time** | **Date** | **Description** | **Investigator** | **Purpose** |
| **1** | 12.00 PM | 14/10/2024 | Operation Narcos (Steve) case was allocated | S.S and H. P | To acquire digital extraction assignment for court report |
| **2** | 12:36 PM | 14/10/2024 | Digital extraction was initiated, and disk images were copied | S. S | Preparing evidence for analysis |
| **3** | 10:20 PM | 14/10/2024 | A copy of the image file was loaded into FTK Imager. | H. P | Ensuring evidence integrity and security |
| **4** | 10:00 AM | 15/10/2024 | Disk Image loaded into the Autopsy Tool | S. S | Collect preliminary evidence |
| **5** | 10:00 AM | 16/10/2024 | Live RAM extracted using Bulk Extractor | S. S | Extracting evidence |
| **6** | 12:00 PM | 17/10/2024 | Image file loaded in Registry Explorer | S. S | Viewing Registry Explorer |
| **7** | 2:00 PM | 17/10/2024 | Web Search, history, keywords search analyzed findings | S. S and H. P | Analysed information related to the case. |
| **8** | 8.:00AM | 18/10/2024 | OS and Partitioned analyzed findings | H. P | Analysed user access and activity history |
| **9** | 12:00 PM | 18/10/2024 | Web Downloads analysed findings | H. P | Review download files evidence |
| **10** | 4:00 PM | 18/10/2024 | Unallocated files, recycle bin files analyzed. | S. S | Analyzed images and deleted files |
| **11** | 12:00 PM | 26/10/2024 | Email findings analyzed | S. S | Analysed email messages |
| **12** | 9:00 PM | 26/10/2024 | Image Steganography Captured | S. S | Revealed hidden messages |
| **13** | 10:00 AM | 31/10/2024 | Discord Chat analysed | H. P | Analysed Discord conversation |
| **14** | 4:00 PM | 21/11/2024 | Summary Report Compile Findings | H. P | Report Summary Audit |
| **15** | 1:00 PM | 22/11/2024 | Summary Report QA | S.S | Finalizing Report Summary |

## 4.6 Findings

* Desktop computer SK-Desktop has a user Steve Kowhai who was searching for the Scope of selling drugs (refer S012) and Global meth flow and countries shared in the world (refer S010 and S011)
* User Crayfish1980 on domain protonmail belongs to user Steve (refer to S045 and S046)
* An encrypted email conversation between Crayfish1980 and heresjohnny1 (refer S050) suggests that they were in talk about methamphetamine.
* User Steve obtained an encrypted file BNE.png image from John's protonmail, which contained meth packets in a suitcase
* He also shared Flight bookings from Brisbane to Wellington and back (refer to S026 for site and S027 for confirmed booking)
* They were due to meet at Eastbourne Library and an alternate place, 666 Rewera Avenue, if they missed each other. (as shown below in the transcript)
* Discord Chat Interception

|  |  |  |  |
| --- | --- | --- | --- |
| **John** | **Timestamp** | **Steve** | **Timestamp** |
| "New supplier, eh? Definitely Interested! Can I get 10 keys of it delivered to Wellington" | 2019-01-28  02.38.38.174  NZDT | “Yeah, yeah probably wiser, good one. In fact, I have already put a document together in anticipation of chatting with you. I'll send it through now. It contains some information regarding how I see this working out. Let me know what you think once you have read it S.O"} | 2019-01-30 12:04:09 NZDT |
| “Good Thinking, I already know how. Heard of steganography?" | 2019-01-30 02:56:12.835 NDZT | "A way of hiding one image within another. There's a simple application called 'Image Steganography'." | 2019-01-30 02:56:12.35NZDT |
| “Ya. I just told you about the tool: face\_palm: Received it. Will check to see if it works and confirm soon. " | 2019-02-01 13:11:39 NZDT | "Good. Meet at the Eastbourne library and if we miss each other come to 666 Rewera Avenue, Petone." | 2019-01-31 02:10:36.655NZDT |

# 5. DIGITAL EXAMINATION

## 5.1 Forensic Procedures and Tools

We used the following Forensic procedures and best practices:

* Utilized a software write blocker – to ensure evidence is protected without tampering or damages.
* Utilized HashCalc - To verify MD5 hashes.
* Maintained an auditable Chain of Custody to record historical procedures, including timestamps and screenshots of evidence.
* Preserving original evidence and working on the copy.
* Maintaining records of day, date, and time of all acquired files and artifacts from the suspect’s images. *Please refer to the Appendix to view the collected evidence.*
* Analysing the artifacts without any preconceived bias or favour.
* Preparing a report based only on the facts of the case.

Tools used in our examination as we started:

## 5.2 FTK Imager

FTK Imager tool creates forensic images for data preservation and verifies evidence's authenticity in legal proceedings.

## 5.3 Registry Explorer

An essential digital forensics tool to analyse the Windows Registry, it provides system preferences, application settings, user profiles, and other important system information.

## 5.4 Bulk Extractor

Our team primarily used the Bulk Extractor tool to extract data from Live RAM Memory, specifically to collect digital evidence such as phone numbers, IP addresses, and email addresses.

## 5.5 Image Steganography Tool

We used this software to extract secrets within image files to reveal messages during our investigation.

## 5.6 Autopsy tool

The autopsy tool platform analyses digital evidence by examining disk images, files, and folders and creating timelines. It is also used to recover and analyse deleted data.

## 5.7 Detailed examination of user Steve Kowhai’s desktop and tools used

## 5.7.1 Desktop details from Registry Explorer, Autopsy, and Partition from FTK Imager

* Name of the desktop: SK-DESKTOP, dated 29/01/2019 (refer to S003)
* Hardware: 17763.1.AMD64FRE.RS5 release 180914-1434 loaded on 15/09/2018 (refer to S002)
* Software: Microsoft Windows 10 (refer to S003)
* Time: NZ standard time (refer to S004)
* Partition scheme: MBR with four partitions, NTFS (refer to S001)
* Devices ever plugged onto the desktop: refer to S030

## 5.7.2 User data/activity from Autopsy and Registry Explorer. Personal details from Bulk extractor

* User Steve: information under 1001 group (refer S005) under path C:\users\Steve
* Last logon: 02/02/2019 02:39:26 GMT
* Internet activity from registry: refer to S006
* Internet setting from registry: Mozilla 5.0 (refer to S007)
* Start-up information from registry: refer to S028
* Past and present IP profile: refer to S034 and S033
* TCP / IP setting from the registry: refer to S032
* Devices mounted by Steve from the registry: refer to S031
* Autoform and login details for Protonmail from Autopsy: username crayfish1980 (refer to S018 and S019)
* Recent documents accessed by Steve from the registry (refer to S029)
* Password from bulk extractor (refer to S056)
* Credit cards and telephone no. used (refer S047 and S048)

## 5.7.3 Web Activity from Autopsy

* Keyword searches: refer S016
* URL searches from Bulk extractor (refer to S049)
* Searches online done by user Steve (31/01/2019 15:55:01 NZDT):

1. What is Methamphetamine? What is crystal meth? How is meth used? (refer to Appendix S008)
2. Best places to trade drugs (refer to S009)
3. Scope of selling drugs (refer to S012)
4. Search for gangs in New Zealand (refer to S013)
5. Search for encrypted email, i.e., protonmail (refer to S017)

## 5.7.4 Images Downloaded from Autopsy

* Global meth flow and countries share in world (refer S010 and S011)
* Downloads of software TrueCrypt and Protonmail, Discord, image Steganography version 1.5.2 (refer S015)
* Encrypted file BNE.png image from John from protonmail
* Flight bookings from Brisbane to Wellington and back (refer S026 for the site and S027 for confirmed booking) and refer S039 for registry entries
* Route for Eastbourne Library from the airport (refer to S023)
* Methods to run from Home marked by user Steve (S025)

## 5.7.5 Email/chat activity from Autopsy and Bulk Extractor

* Discord chat between the two channels (refer to S044)
* History of discord chat activity Steve asking: *“Good. Meet at the Eastbourne Library, and if we miss each other, then come to 666 Rewera Avenue, Peton” (refer to* S043)
* Registry activity to Discord handoff (refer to S041)
* Flight details shared on Discord (refer to S042)
* Attachment Steve\_k.png to Discord (refer S051)

## 5.7.6 Encrypted conversation from Bulk extractor

* User Crayfish1980 on domain proton mail belongs to Steve (refer to S045 and S046)
* Encrypted email conversation between Crayfish1980 and heresjohnny1 (refer S050)
* Jumplist login details for protonmail (refer to S055)

## 5.7.7 Deleted files recovered: earlier stored in the pictures folder of Steve

* Eight\_col\_patches (refer S020 and S037 for registry data)
* Crystal meth bust (refer S021 and S036 for registry data)
* Crystal meth packets (refer S022 and S038 for registry data)

## 5.7.8 Steganographic activity

* Hidden file link of 3300kb with 16 files found (refer to S052)
* RSA keyname found against user Steve. The file named BNE.png 4376kb is found in the download folder. (refer S053) Password Elchapo2 was deciphered by another team. With the image Steganography tool, the hidden file was discovered (refer to S054)

# 6. CONCLUSION

The user with login, Steve, was logged on to a desktop named SK-desktop, and he searched about the drug trade, the price of methamphetamine, and the gangs of New Zealand. Besides, he downloaded pictures of meth busts, meth packets, and the logo for the ‘Mongrel Mob’ with the intention of trading drugs. He was in contact with another user named heresjohnny1 on Discord and Protonmail for delivery of the drugs. They finalized to start with 1gm of meth and take further if it goes through and shared flight details on Discord. They were due to meet at ‘Eastbourne Library’ and another place if they miss. He also had a plan ready to escape, as found in one of the photos.

User Steve had downloaded the Protonmail and image steganography for safe and encrypted messaging. He also downloaded a picture that had a hidden photo of a suitcase with meth in packets sent by John.

This can safely be concluded with the above facts that user Steve used the computer SK-Desktop to search and finalize the trade of meth with John and delivery to be done at Eastbourne library.

# 7 APPENDIX FOR ARTEFACTS

|  |  |  |  |
| --- | --- | --- | --- |
| Exhibit No. | Item | Image Evidence | Date and Time Obtained |
|  |  | Disk and User Information |  |
| S001 | Partition system from FTK Imager |  | 14/10/24, 10:36 pm |
| S002 | Computer System Information |  | 18/10/24 8:33 pm |
| S003 | Computer Name |  | 18/10/24 8:47 pm |
| S004 | Time zone of Computer |  | 18/10/24 9:17 pm |
| S005 | Various users on the computer and Steve's Information |  | 18/10/24 9:48 pm |
| S006 | Internet activity by Steve |  | 18/10/24 10:36 pm |
| S007 | Internet Settings |  | 18/10/24 11:02 pm |
|  |  | Searches performed and Sites Visited by Steve |  |
| S008 | Search For methamphetamine, Crystal meth |  | 17/10/24 8:30 pm |
| S009 | Search for the Drug trade. |  | 17/10/24 8:38 pm |
| S010 | Methamphetamine flows as perceived by recipient countries. |  | 17/10/24 8:55 pm |
| S011 | Global meth flows |  | 17/10/24 8:58 pm |
| S009 | Search for the Drug trade. |  | 17/10/24 8:38 pm |
| S010 | Methamphetamine flows as perceived by recipient countries. |  | 17/10/24 8:55 pm |
| S011 | Global meth flows |  | 17/10/24 8:58 pm |
| S009 | Search for the Drug trade. |  | 17/10/24 8:38 pm |
| S016 | Keyword searches | A screenshot of a computer  Description automatically generated | 17/10/24 9:54 pm |
| S017 | Search for encrypted email Protonmail and steganography. |  | 17/10/24 10:06 pm |
| S018 | Auto-fill web form |  | 17/10/24 10:14 pm |
| S019 | Login for email |  | 17/10/24 10:19 pm |
|  |  | Deleted Files in the recycle bin |  |
| S020 | Recycle Bin – Mongrel Mob Patches |  | 17/10/24 10:32 pm |
| S021 | Recycle Bin – Crystal Meth and Money obtained from Meth Bust |  | 17/10/24 10:33 pm |
| S022 | Recycle Bin – Crystal Meth Packets |  | 17/10/24 10:34 pm |
| S023 | Route for Eastbourne Library from Wellington Airport |  | 17/10/24 10:46 pm |
| S024 | Drop off point |  | 17/10/24 10:51 pm |
| S025 | Method to Run |  | 17/10/24 10:53 pm |
| S026 | Flight bookings – site |  | 17/10/24 11:09 pm |
| S027 | Flight bookings – confirmation |  | 17/10/24 11:10 pm |
| S028 | Startup information |  | 20/10/24 3:15 pm |
| S029 | Recent Documents accessed by Steve |  | 20/10/24 3:26 pm |
| S030 | Devices on computer |  | 20/10/24 3:38 pm |
| S031 | Mounted devices by Steve |  | 20/10/24 3:44 pm |
| S032 | TCP/ IP Setting |  | 20/10/24 3:56 pm |
| S033 | Profile for IP |  | 20/10/24 4:18 pm |
| S034 | Past IP |  | 20/10/24 4:32 pm |
| S035 | REG |  | 20/10/24 10:09 pm |
| S036 | REG related to S021, recycle bin meth bust image |  | 20/10/24 10:23 pm |
| S037 | REG related to S020, recycle bin gang patch image |  | 20/10/24 10:27 pm |
| S038 | REG related to S022, recycle bin crystal meth bags image |  | 20/10/24 10:33 pm |
| S039 | REG related to S026, flight bookings site image |  | 20/10/24 10:41 pm |
| S040 | REG related to secret |  | 20/10/24 10:49 pm |
| S041 | REG related to discord handoff |  | 20/10/24 10:56 pm |
|  |  | Data from Discord |  |
| S042 | Flight details are shared in Discord. |  | 20/10/24 11:08 pm |
| S043 | History of Chat |  | 20/10/24 11:18 pm |
| S044 | Discord chat |  | 31/10/24 10:02 am |
| S045 | Protonmail | A screenshot of a computer  Description automatically generated | 26/10/24 12:43 pm |
|  |  | Email: crayfish1980@prptonmail.com belongs to Steve Kowahi |  |
| S046 | Email domain |  | 26/10/24 12:52 pm |
| S047 | Credit cards Numbers | A screenshot of a computer  Description automatically generated | 26/10/24 1:08 pm |
| S048 | Telephones | A screenshot of a computer  Description automatically generated | 26/10/24 1:27 pm |
| S049 | URL searches | A screenshot of a computer  Description automatically generated | 26/10/24 1:49 pm |
| S050 | Wordlist | A screenshot of a computer  Description automatically generated | 02/11/24 4:03 pm |
|  |  | Steganography Artifacts |  |
| S051 | Attachment to Discord | A screenshot of a computer  Description automatically generated | 26/10/24 6:10 pm |
| S052 | Files Hidden | A screenshot of a computer  Description automatically generated  A cartoon of several viking men on a boat  Description automatically generatedA cartoon of a person pointing at a monster  Description automatically generatedCartoon of chickens running on a dirt road  Description automatically generated  A cartoon of frogs on stairs  Description automatically generatedA cartoon of two men in a room  Description automatically generated  A crab in the water  Description automatically generatedA cartoon of a snake and many small worms  Description automatically generated | 26/10/24 7:23 pm |
| S053 | RSA key name | A bridge over water with a city in the background  Description automatically generatedA screenshot of a computer  Description automatically generatedA screenshot of a computer  Description automatically generated | 26/10/24  9:28 pm |
|  |  | Based on password ‘Elchapo2’ conveyed by the other team we could decipher the image of BNE.png and we got the image of package.jpg using image steganography. |  |
| S054 | Image Stenography Result – package.jpg |  | 02/11/24 12:24pm |
| S055 | Login, Jumplist and Thumbnail | A screenshot of a computer  Description automatically generated | 02/11/24 1:53 pm |
| S056 | Password from Bulk extractor (pii.txt) |  | 02/11/24 2:58 pm |
| S057 | Truecrypt |  | 26/10/24 8:26 pm |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| S058 | Allocated Drive Images | |  |  |  | | --- | --- | --- | | **Drive Images** | | | | **Actor** | **File Name** | **MD5 Hash** | | Steve Kowhai | Narcos-1.001-021 | c63a3d19e9c9495b573f45be544e50f9 | | Jane Estaban | Narcos-3.001-021 | b66ca567bec6b0a195b99c57dfa0919f | | John Fredricksen | Narcos-2.001-021 | 6265dbaa16a354daddba311334484660 | | **Memory images** | | | | **Actor** | **File Name** | **MD5 Hash** | | Steve Kowhai | Narcos-Mem-1.001-003 | 9ca08c17b4a359d61f6f8f7bb6328c1c | | Jane Estaban | Narcos-Mem-3.001-003 | 8e8a3a91eb89fe6c3cd10231f13141fe | | John Fredricksen | Narcos-Mem-2.001-003 | 0f7e7be4d2844457e2111eaffa1e77ec | | 14/10/24 12:24pm |
|  |  | Hash numbers above matched the below number, verifies they are unaltered copies |  |
| S059 | Drive Image extracted by  FKT Imager | A screenshot of a computer  Description automatically generated | 14/10/24  12.25pm |
| S060 | Live R |  | 14/10/24  12.29pm |

|  |  |  |  |
| --- | --- | --- | --- |
| S061 | File Type Analysed of OS extract from  Autopsy | A screenshot of a computer  Description automatically generated | 18/11/24  10:45AM |
|  |  | This confirm OS Drive (Window PRO) size 32 GB |  |
| S062 | Recent Domain | A screenshot of a computer  Description automatically generated | 18/11/24  12.25pm |
| S063 | Recent Device File | A screenshot of a computer  Description automatically generated | 18/11/24  12.29pm |
| SO64 | Recent Open Documents | A screenshot of a computer  Description automatically generated | 20/11/24  12.30pm |
| S065 | Recent Downloads | A screenshot of a computer  Description automatically generated | 18/10/24  12:40pm |
| S066 | Partitions  Related to S001 | A screenshot of a computer  Description automatically generated | 19/10/24  10:00 am |
| S067 | Autopsy extraction of  Steves Computer |  | 21/11/2024  12:pm |
| S068 | Discord conversation timestamp | |  |  |  |  |  | | --- | --- | --- | --- | --- | | Name | Modified Time | Change Time | Access Time | Created Time | | BNE.png | 2019-02-01 13:13:20 NZDT | 2019-02-01 13:15:20 NZDT | 2019-02-02 15:31:06 NZDT | 2019-02-01 13:13:19 NZDT | | DiscordSetup.exe | 2019-01-29 09:56:07 NZDT | 2019-01-29 09:56:33 NZDT | 2019-02-02 15:31:06 NZDT | 2019-01-29 09:56:03 NZDT | | **Discord Chatroom Conversation between John and Steve** | | | | | | 31/10/2024  8:00 am |