NEW ZEALAND
CUSTOMS SERVICE
TE MANA ĀRAI O AOTEAROA

# OPERATION NARCOS

## DIGITAL FORENSIC EXAMINATION OF STEVE KOWHAI

Version 1.0

Shishir Saxena
Hope Posesione

22/11/2024

ISC

# Contents

Introduction
Scope
Timeline
Findings
Artefacts
Conclusion

# Introduction

- Overview of forensic examination scope and purpose
- Key investigation focus area, User activity, including OS, partition details, email forensic, web searches, recycle bin, unallocated space analysis, registry evaluation, and RAM artifacts
- Importance of Timestamps and maintaining a Chain of Custody

# Scope

**Evidence Acquisition for Steve Kowhai's Computer**

Images were acquired from Steve's drive and memory using a software write blocker to prevent modification

**Chain of Custody Maintenance**

Ensure the chain of custody was preserved in the required format

To uphold evidence reliability during audits

**Data integrity Verification**

Digital hash values verified at the scene

confirmed evidence remained intact and unaltered throughout the analysis

| Chain of Custody History | | | | | |
|---|---|---|---|---|---|
| **ase Name: Operation Narcos** | | | | | |
| **ate/Time Acquired: 14/10/2024 12.00 pm** | | | | | |
| **nvestigators: Shishir Saxena (SS) and Hope Posesione (HP)** | | | | | |
| **rtifacts:** Disk Image Narcos-1.00-021 \| Narcos_Mem-1.001 -003 | | | | | |
| **ocation of seizure:** 666 Rewera Avenue, Petone Wellington | | | | | |
| **N** | **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 |

"Whoa! Mr. Lewis! We don't know what that thing is or where it came from, but after what happened to the dog last week, we advise people not to touch it."

# Timeline and Findings

- Timeline Analysis - Investigated User Recent activity revealing significant timestamps and user action. Opened documents and travel plans (e.g. flight details) indicated coordination with John in Brisbane
- Registry View and OS Analysis - Identified user login credential (Steve Kowhai) and computer name (SK-Desktop). Recent file timestamp linked to smuggling operation evidence.
- Communication Log Examination – Uncovered communication involving Discord and Prontonmail. Found emails, chat logs, and files pointing to drug trafficking activities.
- Web searches and downloads
- Unallocated and Recovered Files - Recovered deleted files from the Recycle

| Drug paraphernalia | 2019-01-31 15:57:30 NZDT |
|---|---|
| Crystal meth | 2019-01-31 15:56:24 NZDT |
| Gangs NZ drugs | 2019-01-31 15:59:32 NZDT |
| Best places to trade drugs | 2019-02-02 14:01:34 NZDT |
| Cutting drugs | 2019-01-28 22:58:52 NZDT |
| Cutting agents for ice | 2019-01-28 23:02:00 NZDT |
| How to launder money | 2019 -01- 28 23:03:51NZDT |
| Drug routes in Wellington | 2019-01-29 01:01:58 NZDT |
| International drugs routes | 2019-01-29 01:04:16 NZDT |

"I've got it, too, Omar … a strange feeling like we've just been going in circles."

# 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)

Listing

Web Downloads 34 Resu

Table Thumbnail Summary

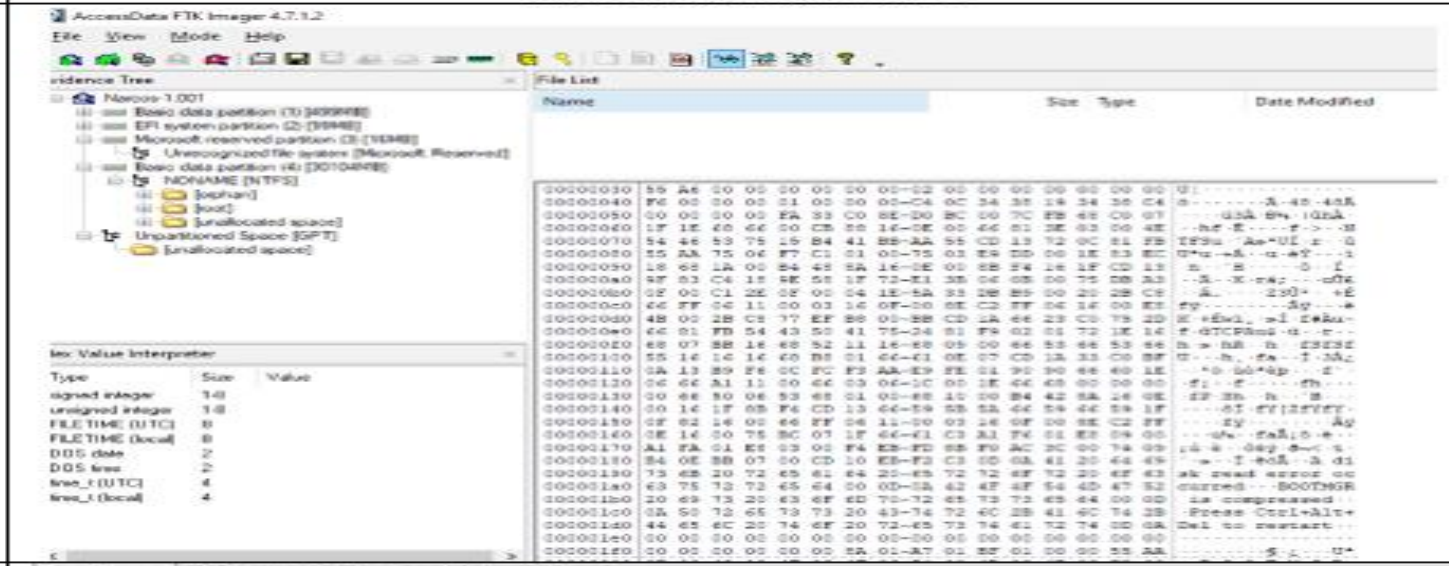
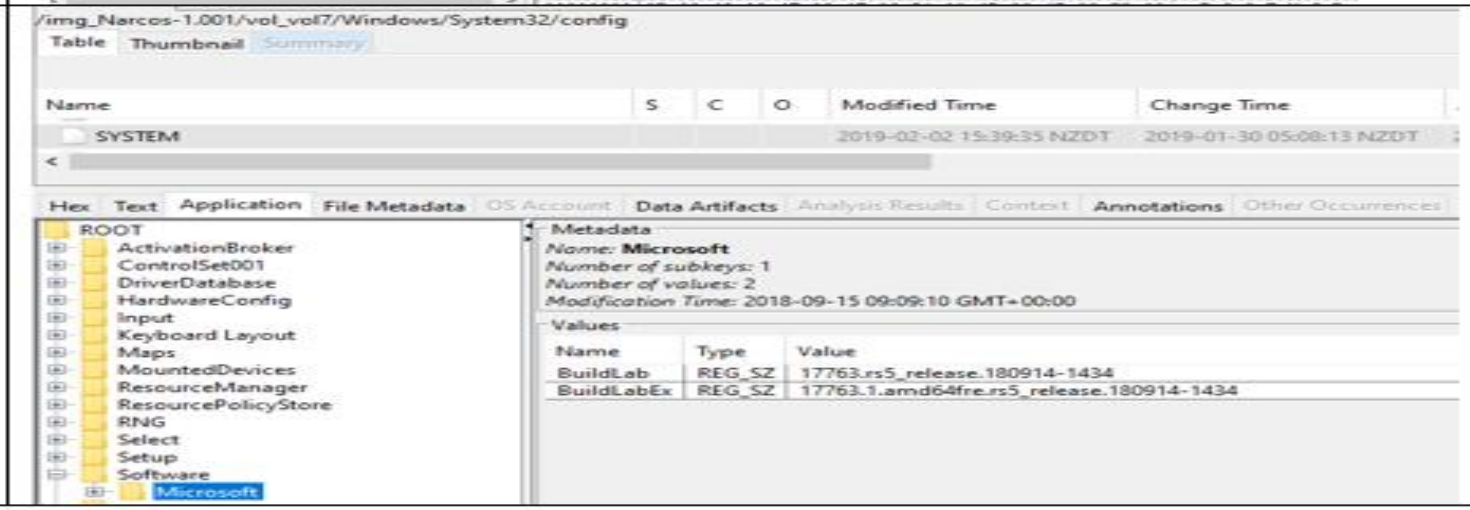
Save Table as CSV

| Source Name | S | C | ... | Path | URL | Date Accessed | Domain |
|---|---|---|---|---|---|---|---|
| History | | 2 | | C:\Users\Steve\Downloads\TrueCrypt Setup 7.1a.exe | https://softpedia-s... | 2019-01-30 12:27:43 NZDT | softpedia-s |
| History | | 3 | | C:\Users\Steve\Downloads\ccsetup552.exe | https://download.c... | 2019-01-30 12:40:51 NZDT | ccleaner.co |
| History | | 3 | | C:\Users\Steve\Pictures\620x349.jpg | https://image.iol.co.. | 2019-01-31 15:56:56 NZDT | iol.co.za |
| History | | 4 | | C:\Users\Steve\Pictures\price-meth-bust-4.jpg | https://localtvkstu.f... | 2019-01-31 15:58:15 NZDT | wordpress.c |
| History | | 3 | | C:\Users\Steve\Pictures\eight_col_patches_crp.jpg | https://www.radion.. | 2019-01-31 15:59:35 NZDT | radionz.co.n |
| History | | 3 | | C:\Users\Steve\Downloads\BNE.png | blob:https://mail.pr.. | 2019-02-01 13:13:19 NZDT | protonmail |
| History | | 4 | | C:\Users\Steve\Downloads\Image Steganography 1.5.2 Setup.exe | https://downloads.... | 2019-02-01 13:16:32 NZDT | sourceforg |
| History | | 4 | | C:\Users\Steve\Downloads\Image Steganography 1.5.2 Setup.exe | https://versaweb.dl... | 2019-02-01 13:16:32 NZDT | sourceforg |
| History | | 3 | | C:\Users\Steve\Documents\Misc\flightbookings.PNG | https://cdn.discord... | 2019-02-02 15:28:26 NZDT | discordapp |
| airport crystals.jpg:Zone.Id | | | | /Users/Steve/Documents/Misc/airport crystals.jpg | | | |
| dropoff.jpg:Zone.Identifie | | | | /Users/Steve/Documents/Misc/dropoff.jpg | | | |
| Method run.jpg:Zone.Iden | | | | /Users/Steve/Documents/Misc/Method run.jpg | | | |
| BNE.png:Zone.Identifier | | | | /Users/Steve/Downloads/Misc/BNE.png | about:internet | | |
| edb00003.log:Zone.Identi | | | | /Users/Steve/MicrosoftEdgeBackups/backups/MicrosoftEdgeBackup20190201/DatastoreBackup/edb | | | |
| schema.txt:Zone.Identifier | | | | /Users/Steve/MicrosoftEdgeBackups/backups/MicrosoftEdgeBackup20190201/DatastoreBackup/sch | | | |
| spartan.edb:Zone.Identifie | | | | /Users/Steve/MicrosoftEdgeBackups/backups/MicrosoftEdgeBackup20190201/DatastoreBackup/spa | | | |
| spartan.pat:Zone.Identifie | | | | /Users/Steve/MicrosoftEdgeBackups/backups/MicrosoftEdgeBackup20190201/DatastoreBackup/spa | | | |
| MicrosoftEdgeCookiesBac | | | | /Users/Steve/MicrosoftEdgeBackups/backups/MicrosoftEdgeBackup20190201/MicrosoftEdgeCookie | | | |
| MicrosoftEdgeSettingsBac | | | | /Users/Steve/MicrosoftEdgeBackups/backups/MicrosoftEdgeBackup20190201/MicrosoftEdgeSetting | | | |
| Backup.dat:Zone.Identifier | | | | /Users/Steve/MicrosoftEdgeBackups/backups/MicrosoftEdgeBackup20190201/Protected - It is a viol | | | |
| 33d49c521dd812b9421df | | | | /Users/Steve/Pictures/33d49c521dd812b9421dff05dc47e5bb.jpg | | | |
| 594bc6bd3f46ff33147628 | | | | /Users/Steve/Pictures/594bc6bd3f46ff331476280671d7745c.jpg | | | |
| 7i2t6tk.jpg:Zone.Identifier | | | | /Users/Steve/Pictures/7i2t6tk.jpg | | | |
| 9648de1b909919145a4fe | | | | /Users/Steve/Pictures/9648de1b909919145a4fe440cf89f576--gary-larson-cartoons-bad-day.jpg | | | |

# 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 |

# 7 APPENDIX FOR ARTEFACTS

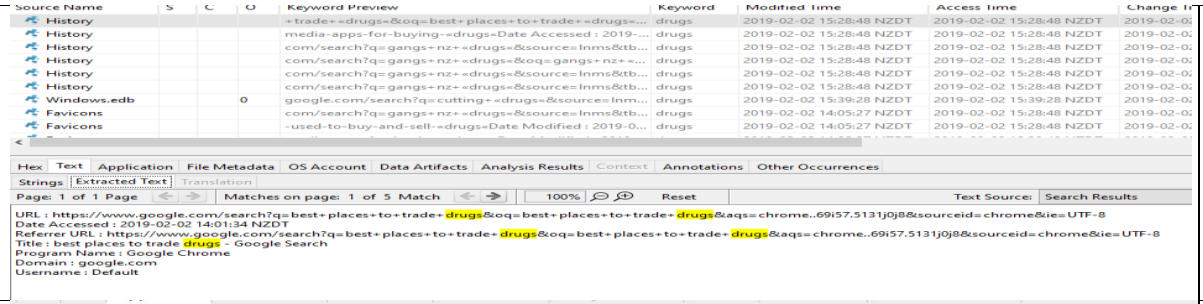
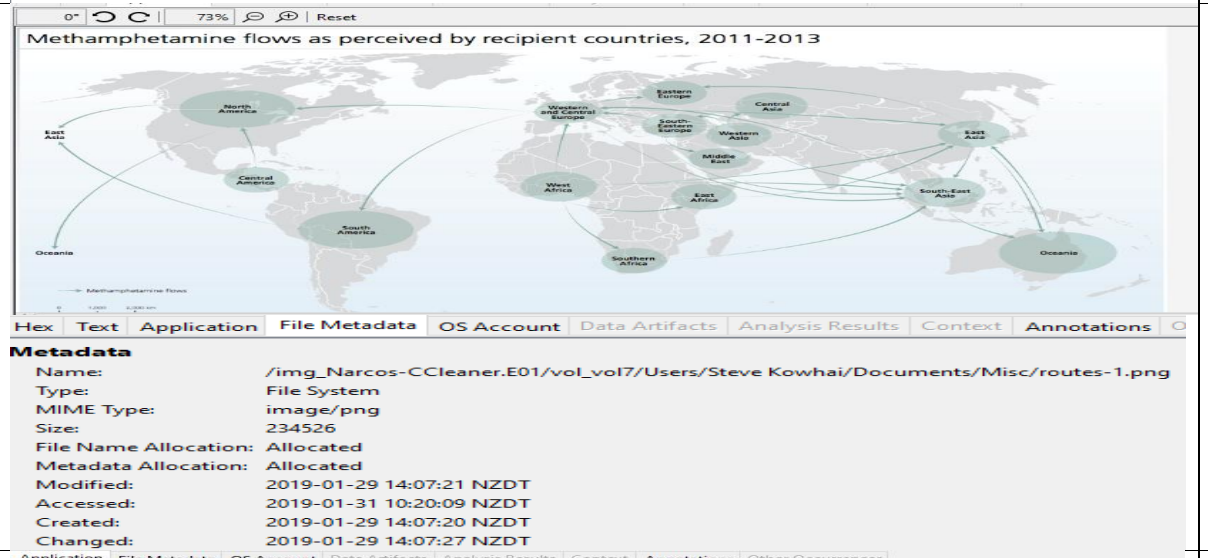
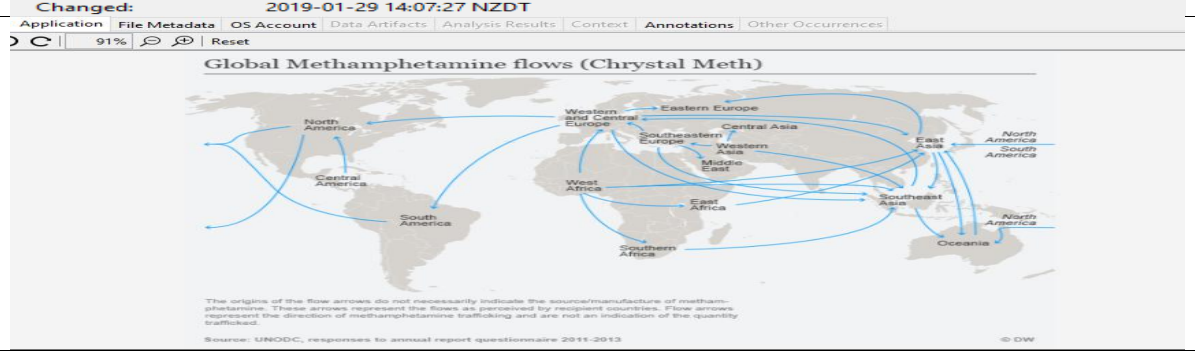
| Exhibit No. | Item | Image Evidence | Date and Time Obtained |
|---|---|---|---|
| | | Disk and User Information | |
| S001 | Partition system from FTK Imager |  | 14/10/24, 10:36 pm |
| S002 | Computer System Information |  | 18/10/24 8:33 pm |

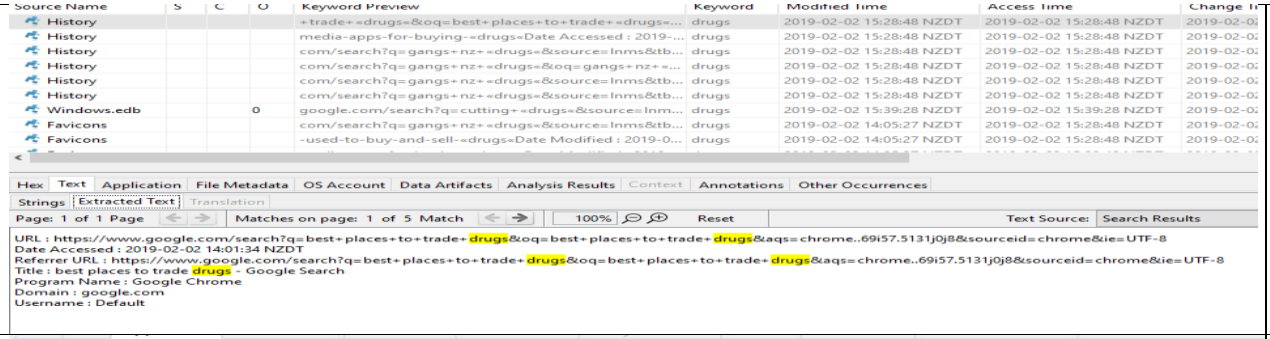
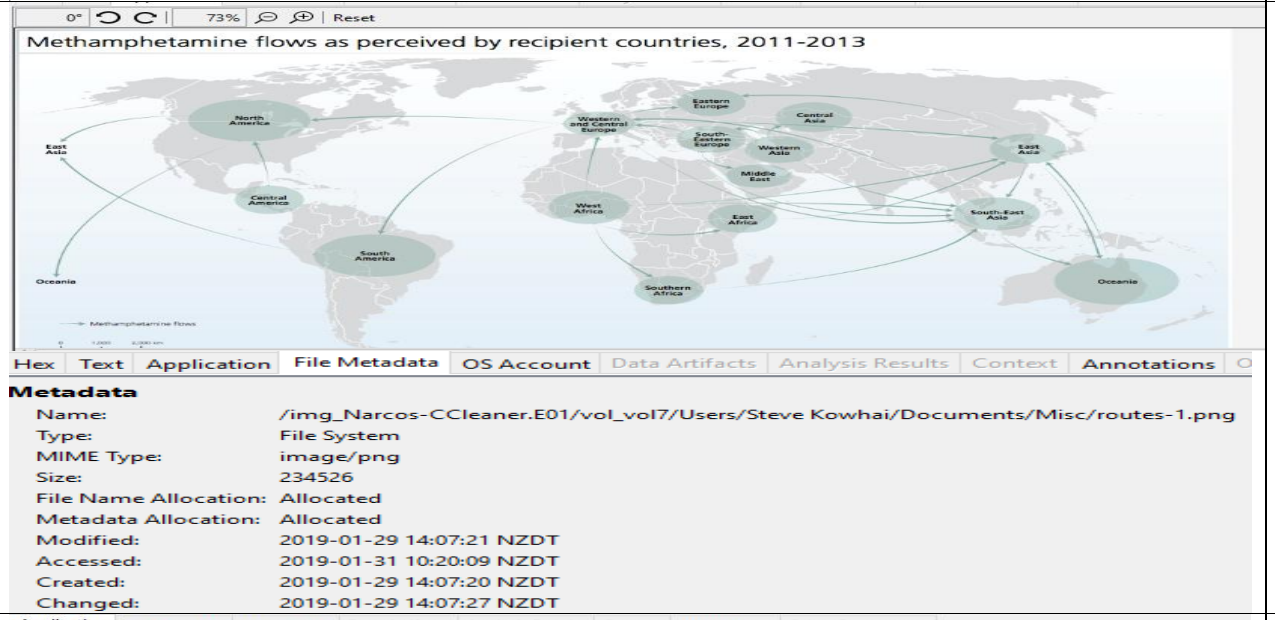
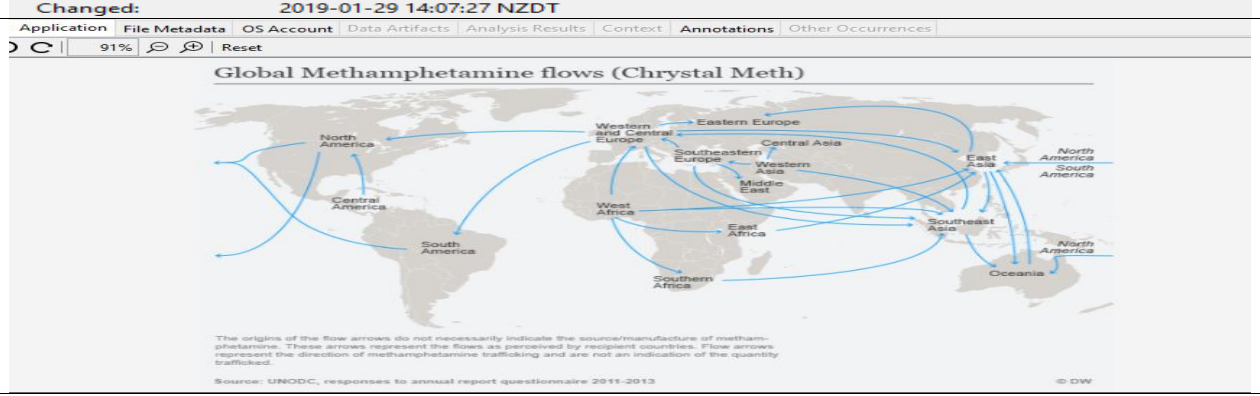
| | | | |
|---|---|---|---|
| S003 | Computer Name | /img_Narcos-1.001/vol_vol7/Windows/System32/config<br>Table Thumbnail Summary<br>Name S C O Modified Time Change Time<br>SOFTWARE 2019-02-02 15:39:35 NZDT 2019-01-30 05:08:09 NZDT<br>SOFTWARE.LOG1 2018-09-15 18:09:26 NZST 2019-01-30 05:07:39 NZDT<br>SOFTWARE.LOG2 2018-09-15 18:09:26 NZST 2019-01-30 05:07:36 NZDT<br>SYSTEM 2019-02-02 15:39:35 NZDT 2019-01-30 05:08:13 NZDT<br>SYSTEM.LOG1 2018-09-15 18:09:26 NZST 2019-01-30 05:07:38 NZDT<br>Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrenc<br>CMF<br>CoDeviceInstallers<br>COM Name Arbiter<br>CommonGlobUserSettings<br>Compatibility<br>ComputerName<br>ComputerName<br>ContentIndex<br>CrashControl<br>Cryptography<br>DeviceClasses<br>DeviceContainerPropertyUpdateEvents<br>DeviceContainers<br>Metadata<br>Name: **ComputerName**<br>Number of subkeys: 0<br>Number of values: 2<br>Modification Time: 2019-01-29 21:00:56 GMT+00:00<br>Values<br>Name Type Value<br>(Default) REG_SZ mnmsrvc<br>ComputerName REG_SZ SK-DESKTOP | 18/10/24 8:47 pm |
| S004 | Time zone of Computer | /img_Narcos-1.001/vol_vol7/Windows/System32/config<br>Table Thumbnail Summary<br>Name S C O Modified Time Change Time Access Time<br>SYSTEM 2019-02-02 15:39:35 NZDT 2019-01-30 05:08:13 NZDT 2019-02-02 15:39:35 NZDT<br>SYSTEM.LOG1 2018-09-15 18:09:26 NZST 2019-01-30 05:07:38 NZDT 2018-09-15 18:09:26 NZST<br>SYSTEM.LOG2 2018-09-15 18:09:26 NZST 2019-01-30 05:07:35 NZDT 2018-09-15 18:09:26 NZST<br>Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences<br>ServiceGroupOrder<br>ServiceProvider<br>Session Manager<br>SNMP<br>SQMServiceList<br>Srp<br>SrpExtensionConfig<br>StillImage<br>Storage<br>StorageManagement<br>StorPort<br>StSec<br>SystemResources<br>TabletPC<br>Terminal Server<br>TimeZoneInformation<br>Ubpm<br>UnitedVideo<br>USB<br>Metadata<br>Name: **TimeZoneInformation**<br>Number of subkeys: 0<br>Number of values: 10<br>Modification Time: 2019-01-28 20:09:06 GMT+00:00<br>Values<br>Name Type Value<br>Bias REG_DWORD 0xfffffd30 (4294966576)<br>DaylightBias REG_DWORD 0xfffffffc4 (4294967236)<br>DaylightName REG_SZ @tzres.dll,-741<br>DaylightStart REG_BIN 00 00 09 00 05 00 02 00 00 00 00 00 00 00 00 0<br>StandardBias REG_DWORD 0x00000000 (0)<br>StandardName REG_SZ @tzres.dll,-742<br>StandardStart REG_BIN 00 00 04 00 01 00 03 00 00 00 00 00 00 00 00 0<br>TimeZoneKeyName REG_SZ New Zealand Standard Time<br>DynamicDaylightTimeDisabled REG_DWORD 0x00000000 (0)<br>ActiveTimeBias REG_DWORD 0xfffffcf4 (4294966516) | 18/10/24 9:17 pm |
| S005 | Various users on the computer and Steve's Information | /img_Narcos-1.001/vol_vol7/Windows/System32/config<br>Table Thumbnail Summary<br>Save Table a<br>Name S C O Modified Time Change Time Access Time Created<br>SECURITY.LOG2 2018-09-15 18:09:26 NZST 2019-01-30 05:07:46 NZDT 2018-09-15 18:09:26 NZST 2018-09-<br>SOFTWARE 2019-02-02 15:39:35 NZDT 2019-01-30 05:08:09 NZDT 2019-02-02 15:39:35 NZDT 2018-09-<br>Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences<br>Perflib<br>PerHwIdStorage<br>Ports<br>Prefetcher<br>Print<br>ProfileList<br>S-1-5-18<br>S-1-5-19<br>S-1-5-20<br>S-1-5-21-1474204758-2504895<br>Default<br>ProfilesDirectory<br>ProgramData<br>Public<br>ProfileNotification<br>related.desc<br>RemoteRegistry<br>Schedule<br>SecEdit<br>Sensor<br>setup<br>SoftwareProtectionPlatform<br>Metadata<br>Name: **S-1-5-21-1474204758-2504895174-1356074821-1001**<br>Number of subkeys: 0<br>Number of values: 14<br>Modification Time: 2019-02-02 02:39:26 GMT+00:00<br>Values<br>Name Type Value<br>ProfileImagePath REG_EXPAND_SZ C:\Users\Steve<br>Flags REG_DWORD 0x00000000 (0)<br>FullProfile REG_DWORD 0x00000001 (1)<br>State REG_DWORD 0x00000000 (0)<br>Sid REG_BIN 01 05 00 00 00 00 00 05 15 00 00 00 56 94 DE 57..<br>LocalProfileLoadTimeLow REG_DWORD 0x4eef817a (1324319098)<br>LocalProfileLoadTimeHigh REG_DWORD 0x01d4baa0 (30718624)<br>ProfileAttemptedProfileDownloadTimeLow REG_DWORD 0x00000000 (0)<br>ProfileAttemptedProfileDownloadTimeHigh REG_DWORD 0x00000000 (0)<br>ProfileLoadTimeLow REG_DWORD 0x00000000 (0)<br>ProfileLoadTimeHigh REG_DWORD 0x00000000 (0)<br>LocalProfileUnloadTimeLow REG_DWORD 0x83bc257b (2210145659)<br>LocalProfileUnloadTimeHigh REG_DWORD 0x01d4baa0 (30718624)<br>RunLogonScriptSync REG_DWORD 0x00000000 (0) | 18/10/24 9:48 pm |
| S006 | Internet activity by Steve | | 18/10/24 10:36 pm |

| | | | |
|---|---|---|---|
| S006 | Internet activity by Steve | /img_Narcos-1.001/vol_vol7/Users/Default<br>Table Thumbnail Summary<br>Name S C O Modified Time Change Time Access Time<br>NTUSER.DAT 2019-01-29 08:16:49 NZDT 2019-01-30 05:08:08 NZDT 2019-01-29 0<br>NTUSER.DAT.LOG1 2018-09-15 18:09:26 NZST 2019-01-30 05:07:45 NZDT 2018-09-15 1<br>NTUSER.DAT.LOG2 2018-09-15 18:09:26 NZST 2019-01-30 05:07:45 NZDT 2018-09-15 1<br>Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences<br>ROOT<br>AppEvents<br>Console<br>Control Panel<br>Environment<br>EUDC<br>Keyboard Layout<br>Network<br>Software<br>Google<br>Chrome<br>NativeMessagingHosts<br>com.microsoft.browsercore<br>Metadata<br>Name: com.microsoft.browsercore<br>Number of subkeys: 0<br>Number of values: 1<br>Modification Time: 2019-01-29 16:08:06 GMT+00:00<br>Values<br>Name Type Value<br>(Default) REG_SZ C:\Program Files\Windows Security\BrowserCore... | 18/10/24 10:36 pm |
| S007 | Internet Settings | /img_Narcos-1.001/vol_vol7/Users/Default<br>Table Thumbnail Summary<br>Name S C O Modified Time Change Time Access Time<br>NTUSER.DAT 2019-01-29 08:16:49 NZDT 2019-01-30 05:08:08 NZDT 2019-01-29 08:35:07 NZD<br>NTUSER.DAT.LOG1 2018-09-15 18:09:26 NZST 2019-01-30 05:07:45 NZDT 2018-09-15 18:09:26 NZS<br>NTUSER.DAT.LOG2 2018-09-15 18:09:26 NZST 2019-01-30 05:07:45 NZDT 2018-09-15 18:09:26 NZS<br>Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences<br>Holographic<br>ime<br>Internet Settings<br>5.0<br>Cache<br>Cache<br>Persistent<br>Connections<br>Http Filters<br>RPA<br>P3P<br>Passport<br>DisableCachingOfSSLPages<br>IE5_UA_Backup_Flag<br>PrivacyAdvanced<br>SecureProtocols<br>User Agent<br>Metadata<br>Name: Internet Settings<br>Number of subkeys: 6<br>Number of values: 6<br>Modification Time: 2018-09-15 07:35:59 GMT+00:00<br>Values<br>Name Type Value<br>DisableCachingOfSSLPages REG_DWORD 0x00000000 (0)<br>IE5_UA_Backup_Flag REG_SZ 5.0<br>PrivacyAdvanced REG_DWORD 0x00000001 (1)<br>SecureProtocols REG_DWORD 0x00000a80 (2688)<br>User Agent REG_SZ Mozilla/5.0 (compatible; MSIE 9.0; Win32)<br>CertificateRevocation REG_DWORD 0x00000001 (1) | 18/10/24 11:02 pm |

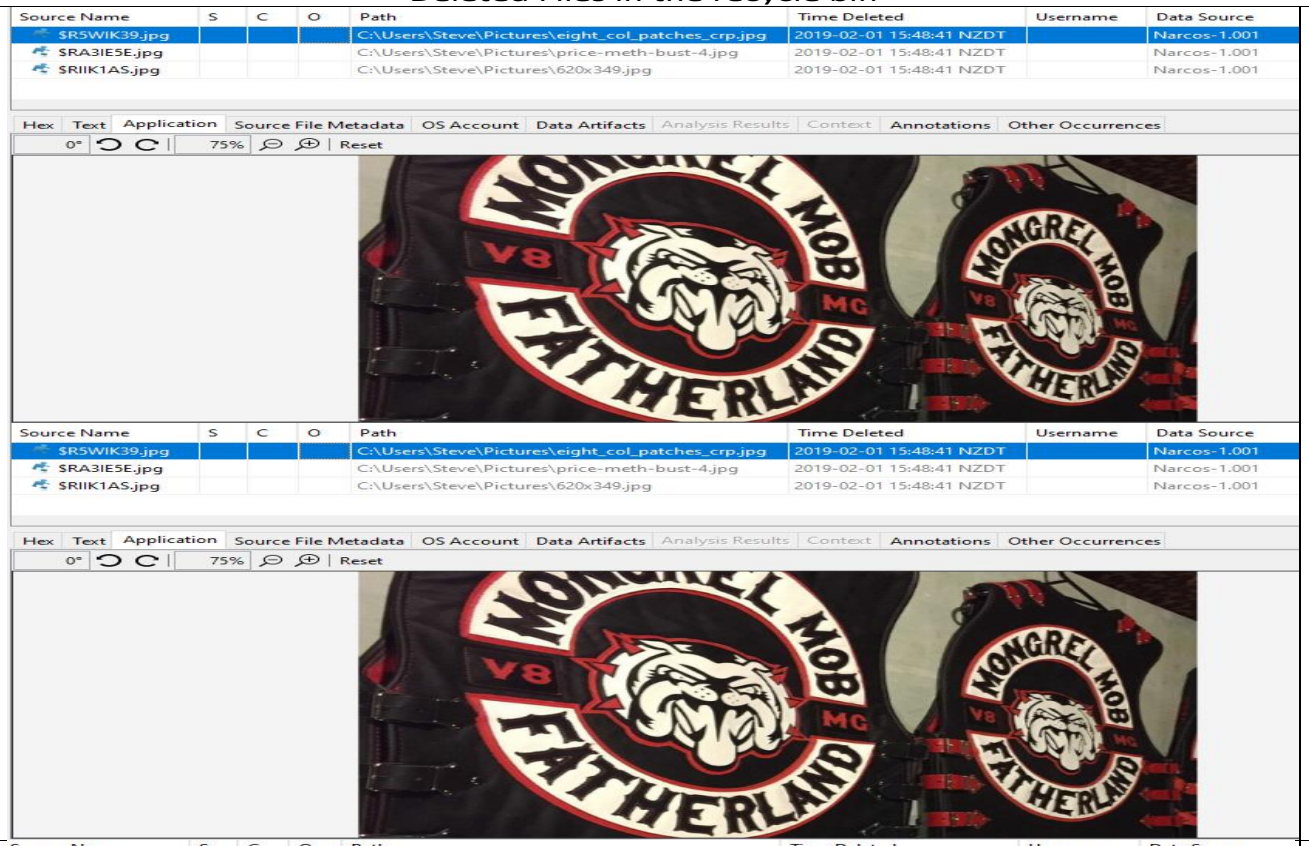
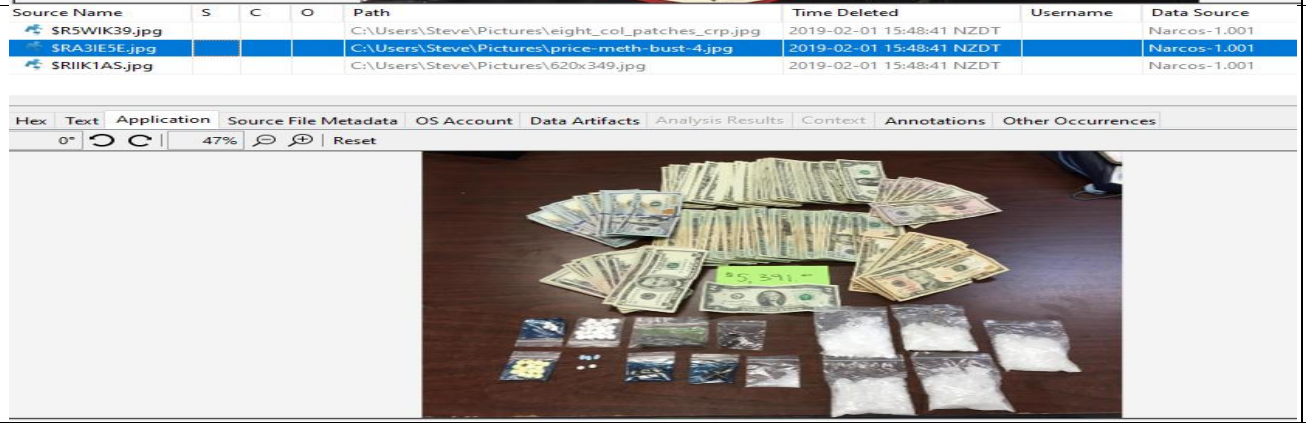
Searches performed and Sites Visited by Steve

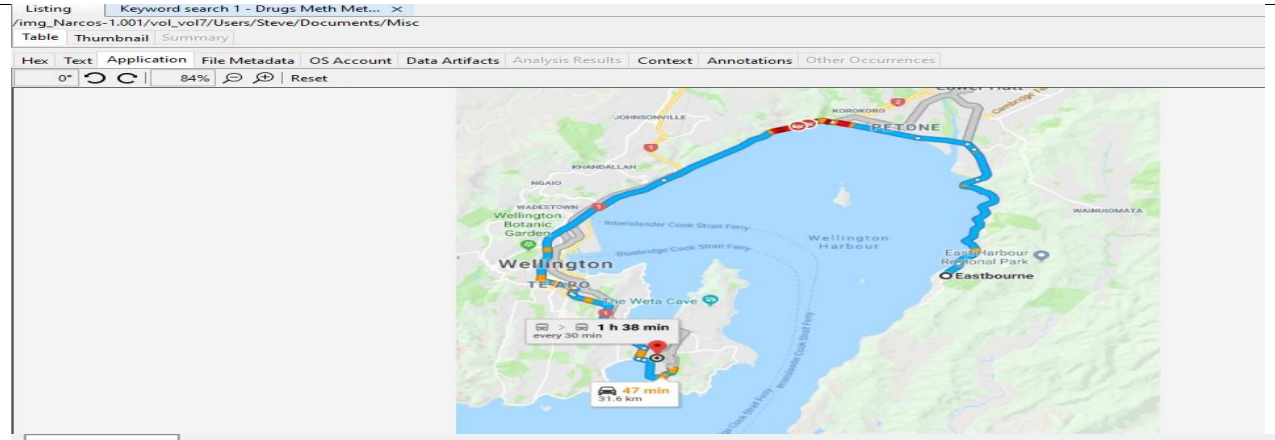
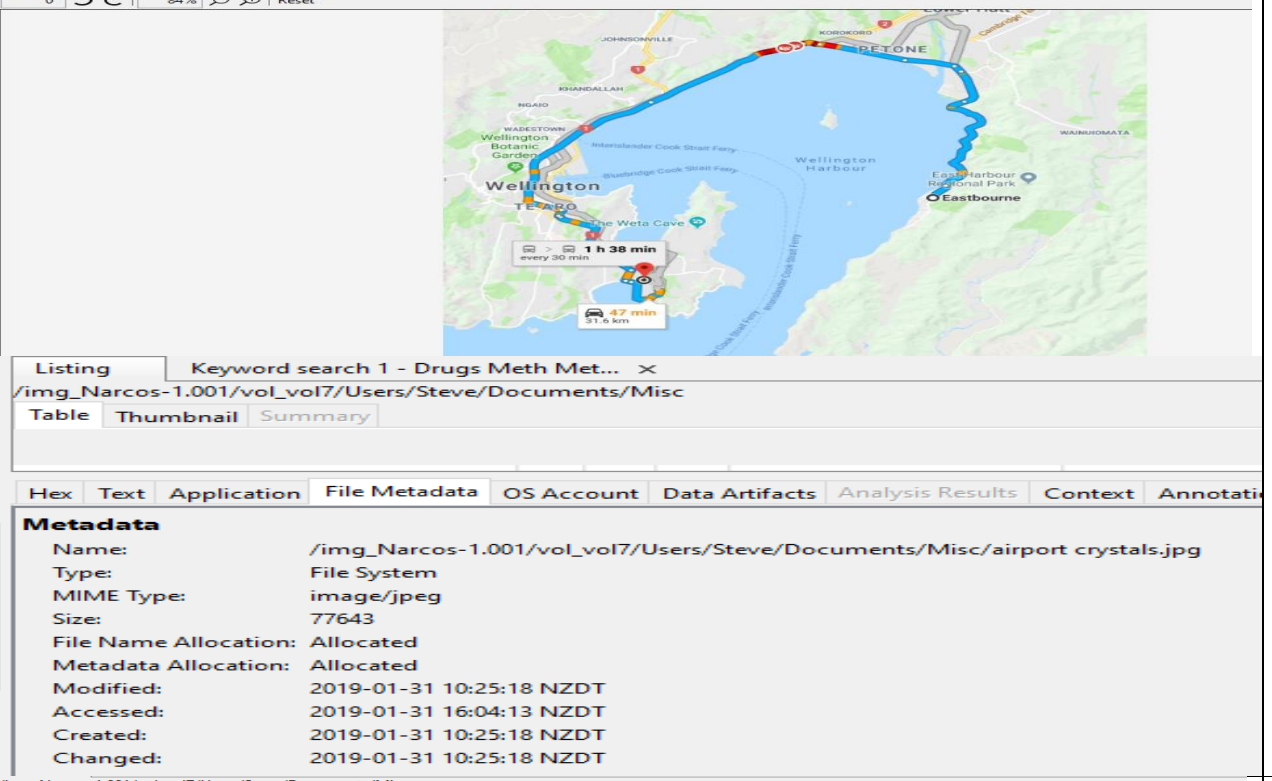
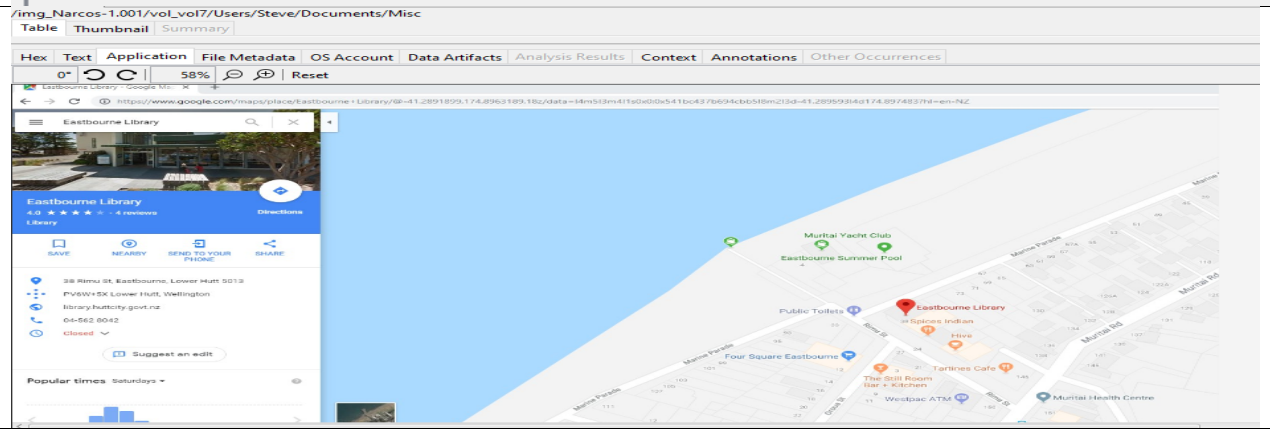
| | | | |
|---|---|---|---|
| S008 | Search For methamphetamine, Crystal meth | Strings Extracted Text Translation<br>Page: 1 of 1 Page Matches on page: 1 of 1 Match 100%<br>URL : https://www.drugfreeworld.org/drugfacts/crystalmeth.html<br>Date Accessed : 2019-01-31 15:55:01 NZDT<br>Referrer URL : https://www.drugfreeworld.org/drugfacts/crystalmeth.html<br>Title : What is Methamphetamine? What is Crystal Meth? How is Meth Used? - Drug-Free World<br>Program Name : Google Chrome<br>Domain : drugfreeworld.org<br>Username : Default<br>History C:\Users\Steve\Pictures\price-«meth»-bust-4.jpgPath ... meth 2019-02-02 15:28:48 NZDT 2019-02-02 15:28:48 NZDT<br>$RA3IE5E.jpg C:\Users\Steve\Pictures\price-«meth»-bust-4.jpgTime... meth 2019-01-31 15:58:22 NZDT 2019-01-31 16:04:13 NZDT<br>History com/search?q=crystal+«meth»&oq=crystal+«meth»... meth 2019-02-02 15:28:48 NZDT 2019-02-02 15:28:48 NZDT<br>History What is Crystal «Meth»? How is «Meth» Used? - Drug-... meth 2019-02-02 15:28:48 NZDT 2019-02-02 15:28:48 NZDT<br>Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences<br>Strings Extracted Text Translation<br>Page: 1 of 1 Page Matches on page: 1 of 2 Match 100% Reset Text Source: Search Results<br>Path : C:\Users\Steve\Pictures\price-meth-bust-4.jpg<br>Path ID : 598057<br>URL : https://localtvkstu.files.wordpress.com/2015/04/price-meth-bust-4.jpg?quality=85&strip=all<br>Date Accessed : 2019-01-31 15:58:15 NZDT<br>Domain : wordpress.com<br>Username : Default<br>Program Name : Google Chrome | 17/10/24 8:30 pm |

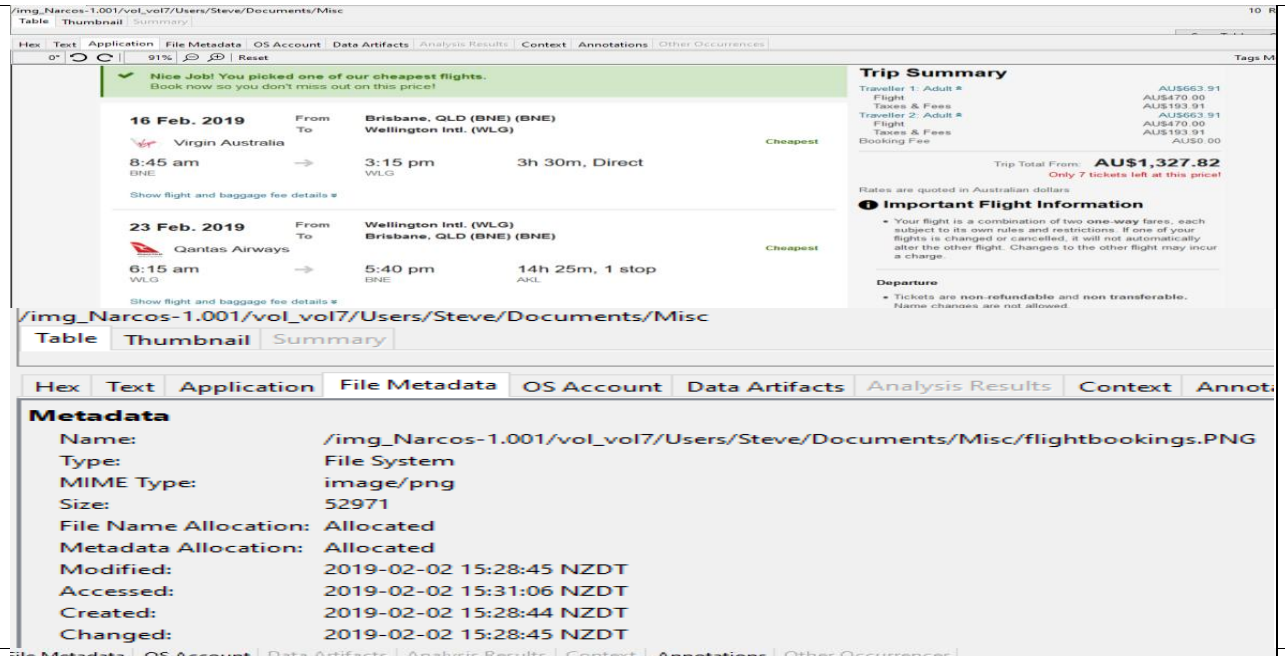
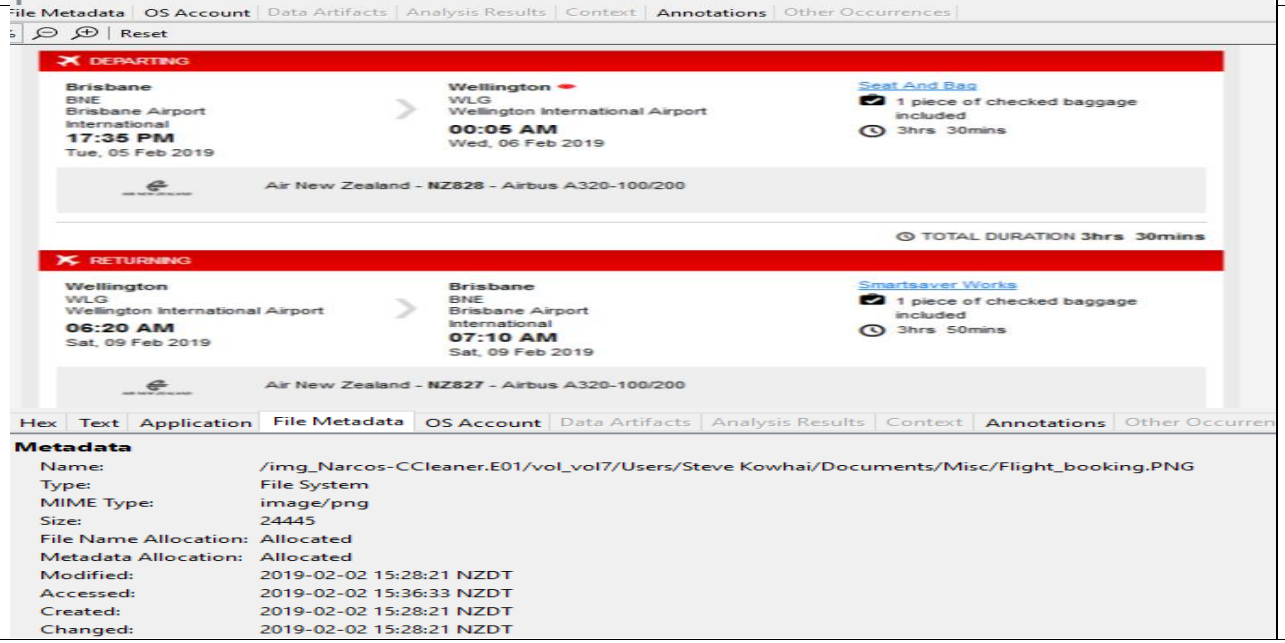
| | | | |
|---|---|---|---|
| S009 | Search for the Drug trade. |  | 17/10/24 8:38 pm |
| S010 | Methamphetamine flows as perceived by recipient countries. |  | 17/10/24 8:55 pm |
| S011 | Global meth flows |  | 17/10/24 8:58 pm |

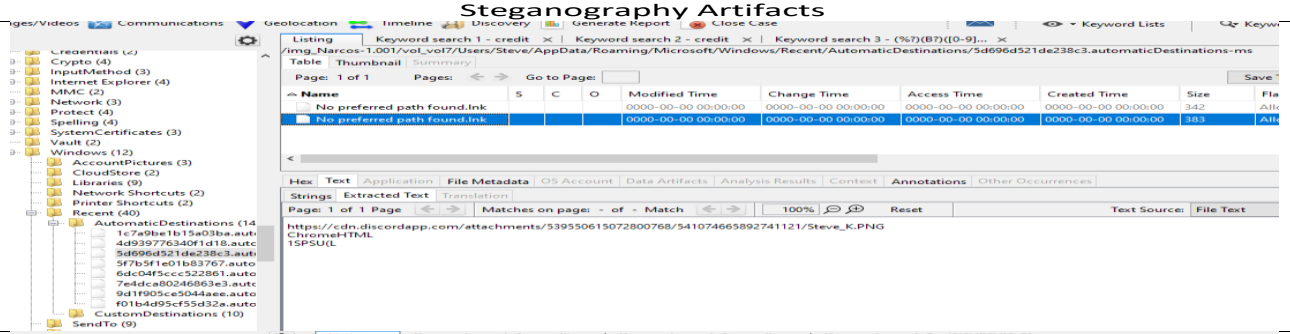
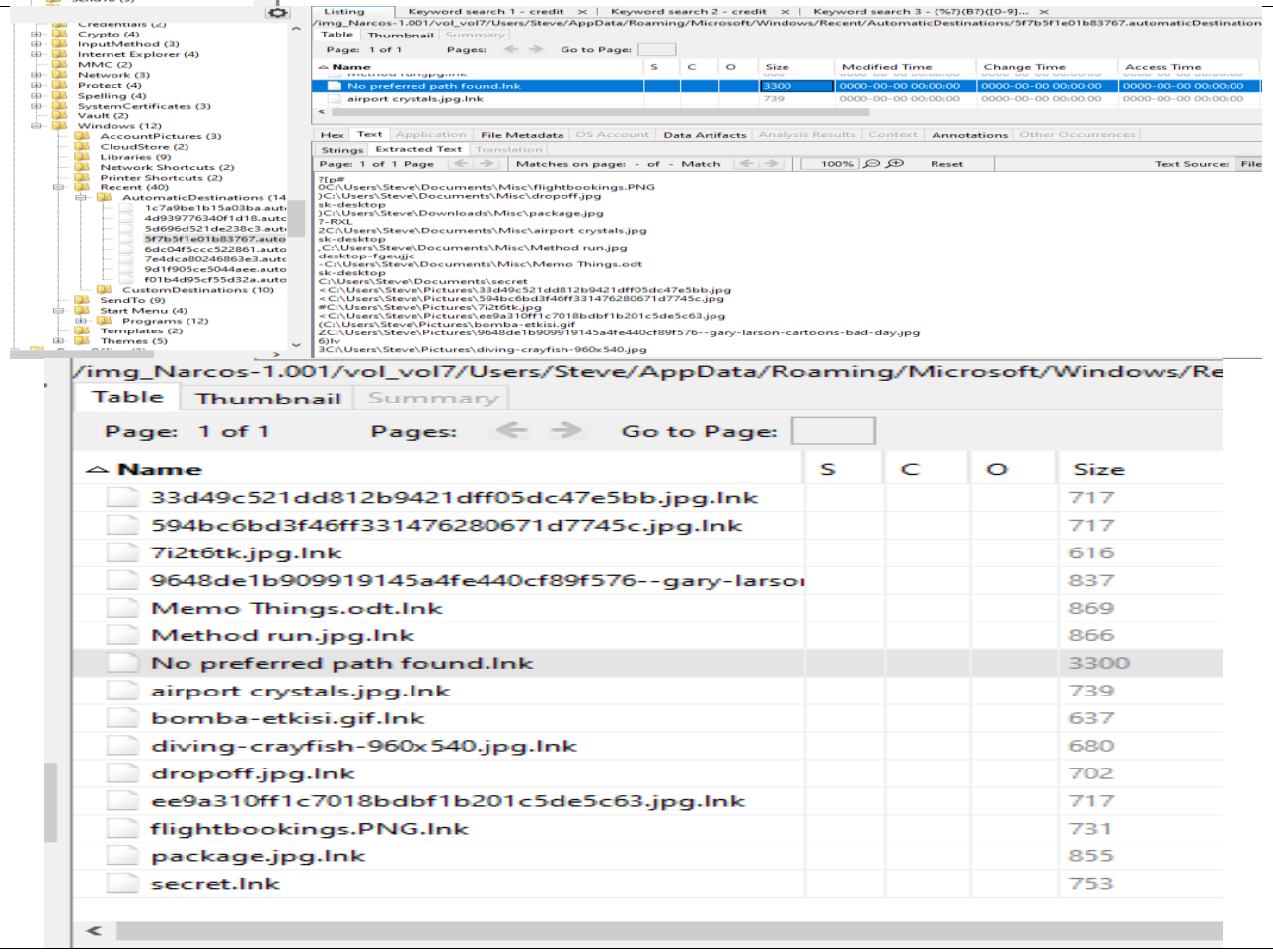
| | | | |
|---|---|---|---|
| S009 | Search for the Drug trade. |  | 17/10/24 8:38 pm |
| S010 | Methamphetamine flows as perceived by recipient countries. |  | 17/10/24 8:55 pm |
| S011 | Global meth flows |  | 17/10/24 8:58 pm |

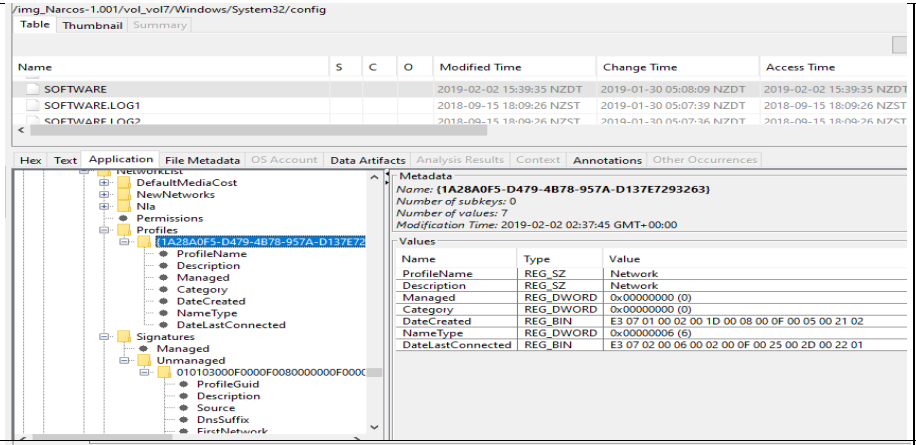
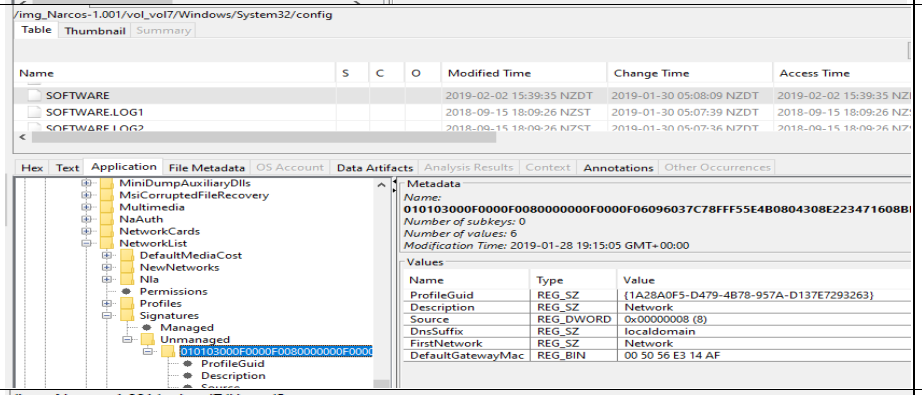
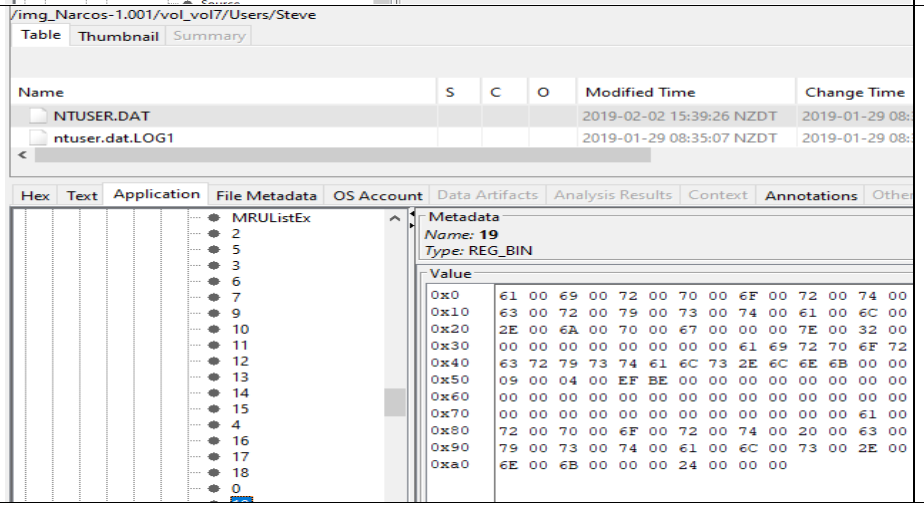
Deleted Files in the recycle bin

| | | | |
|---|---|---|---|
| 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 |

| | | | |
|---|---|---|---|
| S023 | Route for Eastbourne Library from Wellington Airport |   | 17/10/24 10:46 pm |
| S024 | Drop off point |  | 17/10/24 10:51 pm |

| | | | |
|---|---|---|---|
| S026 | Flight bookings – site |  | 17/10/24 11:09 pm |
| S027 | Flight bookings – confirmation |  | 17/10/24 11:10 pm |

| | | Steganography Artifacts | |
|---|---|---|---|
| S051 | Attachment to Discord |  | 26/10/24 6:10 pm |
| S052 | Files Hidden |  | 26/10/24 7:23 pm |

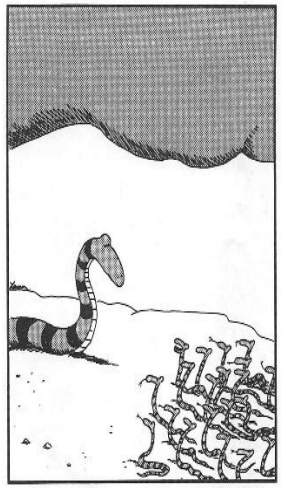
| | | | |
|---|---|---|---|
| S033 | Profile for IP |  | 20/10/24<br>4:18 pm |
| S034 | Past IP |  | 20/10/24<br>4:32 pm |
| S035 | REG |  | 20/10/24<br>10:09 pm |

/img_Narcos-1.001/vol_vol7/Users/Steve/AppData/Roaming/Microsoft/Windows/Re

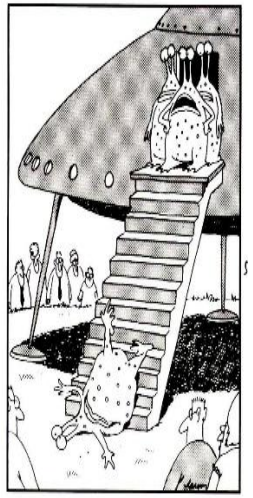
Table | Thumbnail | Summary

Page: 1 of 1 Pages: Go to Page:

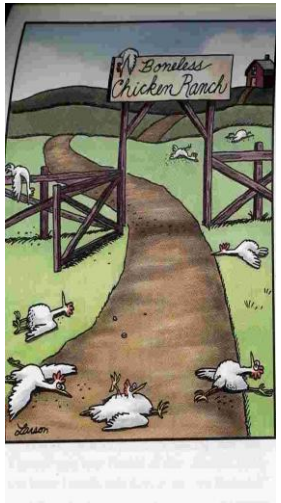
| Name | S | C | O | Size |
|---|---|---|---|---|
| 33d49c521dd812b9421dff05dc47e5bb.jpg.lnk | | | | 717 |
| 594bc6bd3f46ff331476280671d7745c.jpg.lnk | | | | 717 |
| 7i2t6tk.jpg.lnk | | | | 616 |
| 9648de1b909919145a4fe440cf89f576--gary-larso | | | | 837 |
| Memo Things.odt.lnk | | | | 869 |
| Method run.jpg.lnk | | | | 866 |
| No preferred path found.lnk | | | | 3300 |
| airport crystals.jpg.lnk | | | | 739 |
| bomba-etkisi.gif.lnk | | | | 637 |
| diving-crayfish-960x540.jpg.lnk | | | | 680 |
| dropoff.jpg.lnk | | | | 702 |
| ee9a310ff1c7018bdbf1b201c5de5c63.jpg.lnk | | | | 717 |
| flightbookings.PNG.lnk | | | | 731 |
| package.jpg.lnk | | | | 855 |
| secret.lnk | | | | 753 |

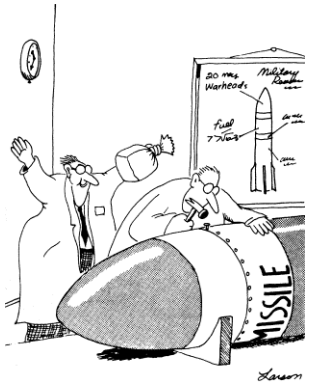


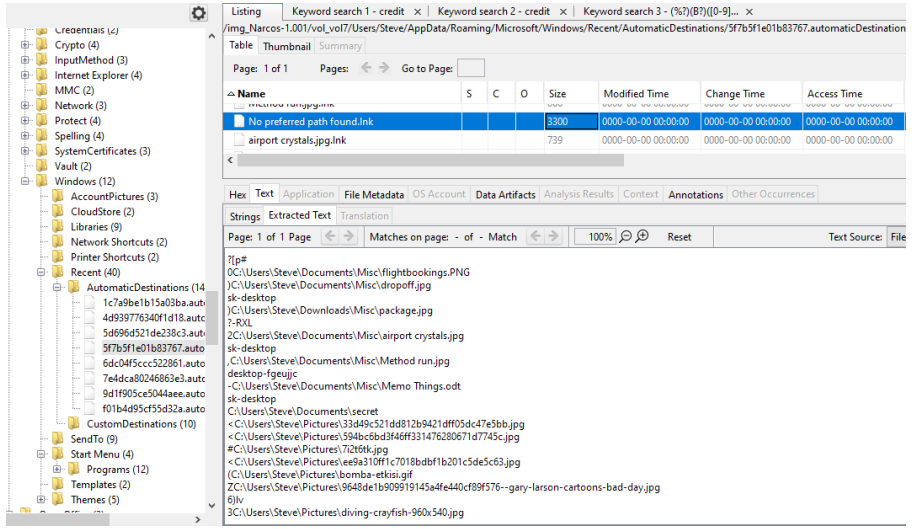
"No, really, Mom—who do you like best?"

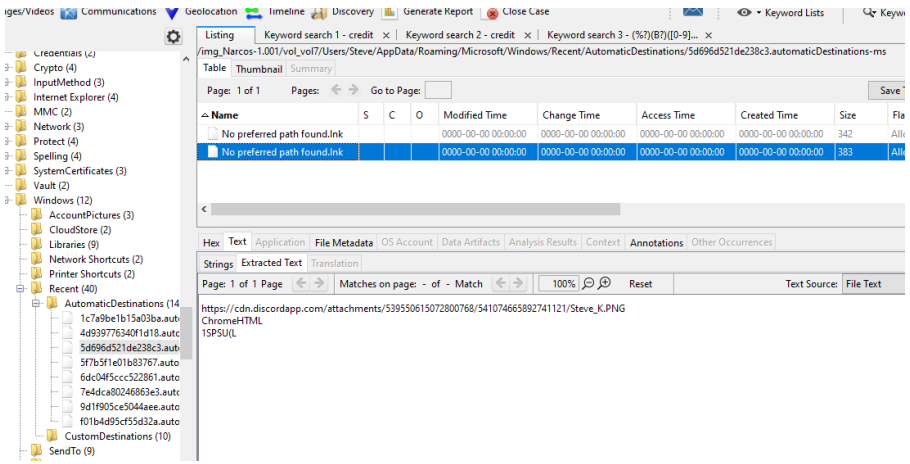


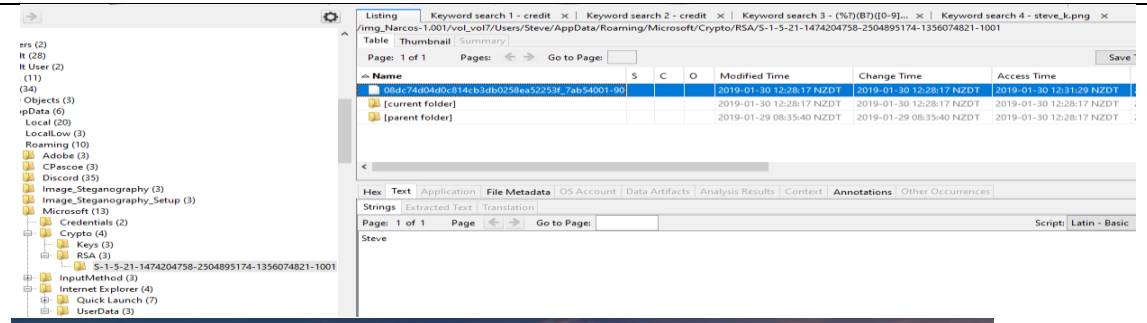
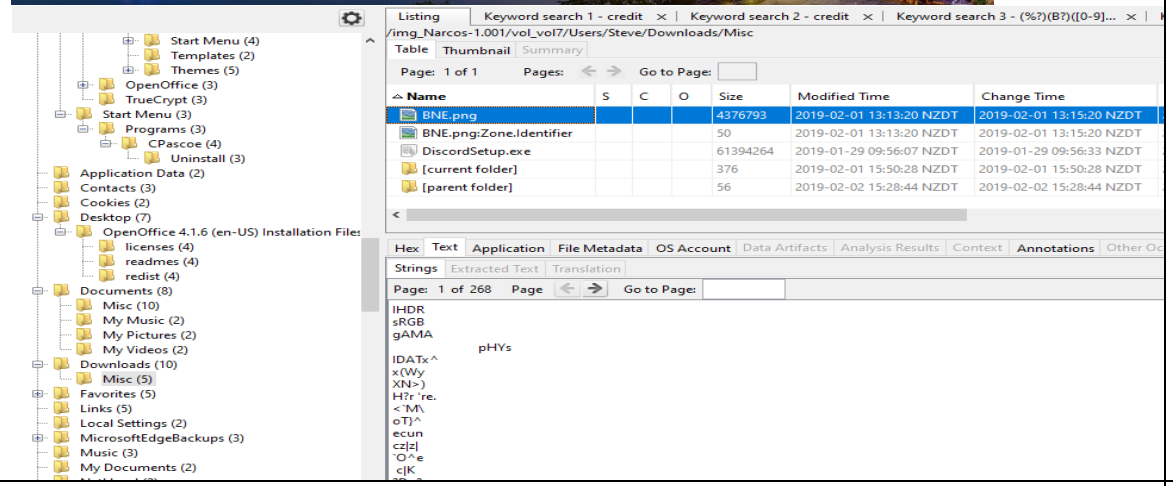
"Wonderful! Just wonderful! ... So much for instilling them with a sense of awe."

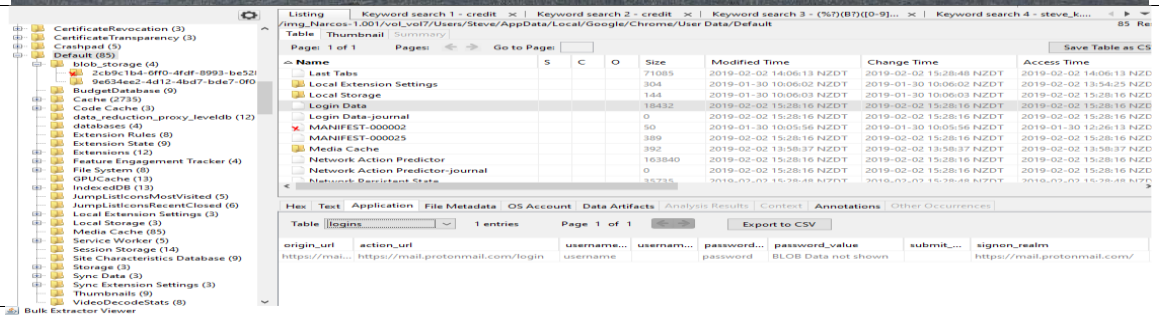
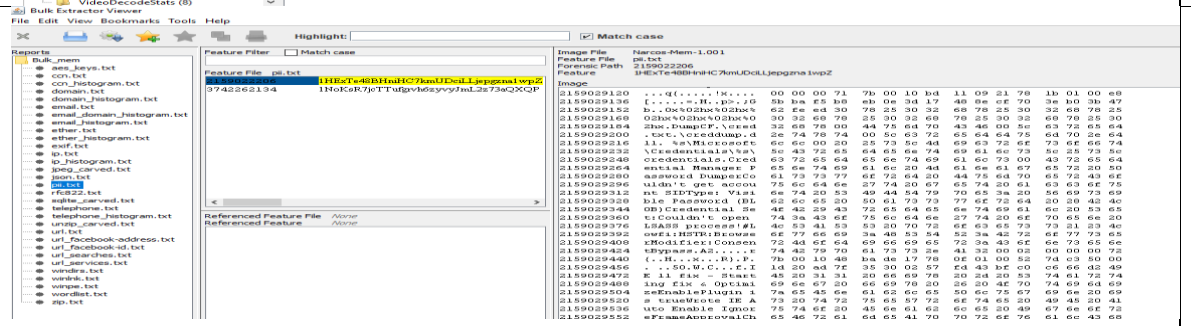


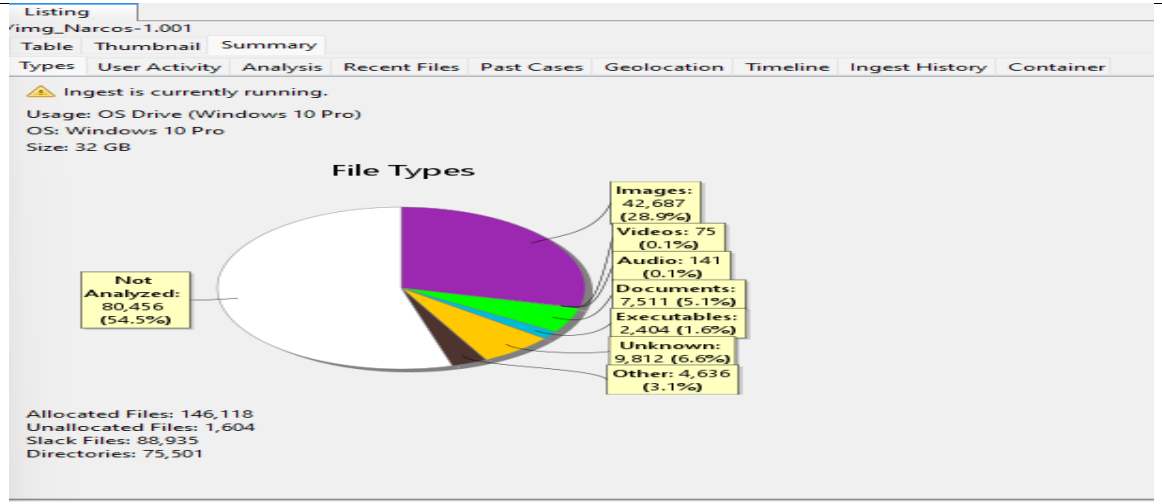



| | | | |
|---|---|---|---|
| S053 | RSA key name |  <br> <br>  | 26/10/24<br>9:28 pm |
| | | Based on password ‘Elchapo2’ conveyed by the other team we could decipher the image of BNE.png and we got the image of package.jpg using image steganography. | |

| | | | |
|---|---|---|---|
| S054 | Image Stenography Result – package.jpg | | 02/11/24 12:24pm |
| S055 | Login, Jumplist and Thumbnail |  | 02/11/24 1:53 pm |
| S056 | Password from Bulk extractor (pii.txt) |  | 02/11/24 2:58 pm |
| S057 | Truecrypt | TrueCrypt User Guide.pdf | 26/10/24 8:26 pm |

| | | | |
|---|---|---|---|
| S061 | File Type Analysed of OS extract from Autopsy |  | 18/11/24 10:45AM |
| | | This confirm OS Drive (Window PRO) size 32 GB | |
| S062 | Recent Domain | Recent Domains<br>Domain \| Visits \| Last Accessed<br>youtube.com \| 29 \| 2019/01/30 10:15:05<br>protonmail.com \| 25 \| 2019/02/01 15:40:19<br>allblacks.com \| 24 \| 2019/02/02 10:47:49<br>metservice.com \| 24 \| 2019/02/02 10:36:55 | 18/11/24 12.25pm |
| S063 | Recent Device File | Recent Devices Attached<br>Device Id \| Last Accessed \| Make and Model<br>MSFT30NA9LP8HF \| 2019/01/31 16:04:08 \| Seagate RSS LLC - Backup Plus Slim Portable...<br>57584D3145373444574D314E \| 2019/02/01 15:41:46 \| Western Digital Technologies, Inc. - Element...<br>7&1ffda586&0&0001 \| 2019/02/02 15:37:25 \| VMware, Inc. - Virtual Mouse<br>6&30c8ca5f&0&5 \| 2019/02/02 15:37:25 \| VMware, Inc. - Virtual Mouse | 18/11/24 12.29pm |
| SO64 | Recent Open Documents | Recently Opened Documents<br>Path \| Date<br>C:\Users\Steve\Documents\Misc\flightbo... \| 2019/02/02 15:28:44<br>No preferred path found \| 2019/02/02 15:28:16<br>C:\Users\Steve\Documents\Misc\dropoff.j... \| 2019/02/02 14:06:05<br>C:\Users\Steve\Downloads\Misc\package.j... \| 2019/02/01 15:49:18<br>C:\ProgramData\Microsoft\Windows\Start... \| 2019/01/31 16:08:50<br>C:\Users\Steve\Pictures\eight_col_patches... \| 2019/01/31 15:59:38<br>C:\Users\Steve\Pictures\price-meth-bust-... \| 2019/01/31 15:58:22<br>C:\Users\Steve\Pictures\620x349.jpg \| 2019/01/31 15:57:04<br>C:\Users\Steve\Documents\Misc\airport cr... \| 2019/01/31 10:25:18 | 20/11/24 12.30pm |

# 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.