New Zealand Customs Service
Drug Investigations Unit
Computer Forensics Laboratory
1 Hinemoa Street, The Customhouse
Pipitea, Wellington 6011
(0800) 428 786

MEMO TO FILE

FORENSIC EXAMINER PROCESSING NOTES:	**Thomas D. Green (300536064)**
FORENSIC CASE NUMBER:	**ECL-DRUG-2025-0063**
REQUESTER:	SCO. Alan Thompson (SCO-4587) NZCS Drug Investigations Unit (+64 4 901 4500)
OFFENCE:	Importation of Class A Drug (Methamphetamine)
CASE NUMBER:	NZ-ECL-2025-0342
RECEIVED:	May 10, 2025
OPENED:	May 16, 2025
COMPLETED:	May 25, 2025
FORENSIC HOURS:	25 hours
OS EXAMINED:	Microsoft® Windows 10 Pro
FILE SYSTEM:	NTFS (New Technology File System)
DATA ANALYSED:	30720 mb
EVIDENCE DESCRIPTION, ITEM 1:	EV-001 (One Custom-Built Desktop Computer)
Storage Device:	32 GB Internal Drive
Serial Number:	N/A (Custom Build)
Passcode/Pin:	No passcode or credentials provided
Process Architecture:	AMD64
Artifact ID:	-9223372036854775446
Device ID:	b9bc9ee7-97bb-4e26-8f93-73b50305764e
Product ID:	00330-80000-00000-AA502

Action Taken:

May 16, 2025

1300 Hours

The ECS Computer Workstation was booted into a Virtual Machine running Windows 11. Received and reviewed the Narcos-1.zip file from Digital Forensic Examiner Ian Welch.

Also reviewed the associated Digital Evidence Request to understand the scope of the case. The objective is to examine the desktop computer for digital evidence related to the primary offence, importation of ‘Class A’ drug (Methamphetamine), determine the nature of the relationship between John Fredrickson and the un-identified suspect, and find indicators of future intent or criminal activity.

1400 Hours

Verified the integrity of the Narcos-1.zip file by comparing it’s MD5 and SHA1 hashes against those provided. Hash validation was performed using Windows PowerShell with the certutil command as follows:

- certutil -hashfile “C:\Users\cyber\Downloads\Narcos-1.zip” MD5
- certutil -hashfile “C:\Users\cyber\Downloads\Narcos-1.zip” SHA1

The calculated hashes were:

- MD5: 7F3D290BB7706637B0BFF613190284BD
- SHA1: 1E7F6ACC658D83FB6DF9E4BC9EFA436EBA1EF3C6

Both hash values matched the hashes provided with the .zip file, confirming that the evidence was not tampered with and remained forensically sound.

1450 Hours

Extracted the Narcos-1.zip archive to a new disk partition (E: drive) using File Explorer’s built-in extraction tool. Noted that Digital Forensic Examiner Ian Welch used FTK Imager 4.2.0.13 on 8 May 2025 at 14:15, (FTK Imager output Narcos-1.001.txt output stating that it was performed 17 Feb 2019 at 17:34:16 finishing at 17:41:53) to acquire the drive image and memory dump.

The image consists of segmented files (Narcos-1.001 through Narcos-1.021), indicating a split image set generated during acquisition. FTK Imager also recorded and verified the MD5 and SHA1 hash values at both the start and end of the imaging process.

- MD5: c63a3d19e9c9495b573f45be544e50f9
- SHA1: 4d8e5041f47e0b0fc0eacc85d300661946537418

These hash values will be used to verify the integrity of the extracted image (Narcos-1.001) during further forensic examination.

1500 Hours

Began setting up an Autopsy case using Autopsy 4.21.0 for forensic analysis of the evidence image. Created a new case titled "Narcos 2025", selecting the Single-User case type, as I will be the sole examiner conducting the investigation. In the Optional Information section, I entered:

- Case Number: NZ-DRUG-2025-0063
- Examiner Name: Thomas Green
- Business Phone: +64 4 901 4501
- Email Address: t.green@customs.govt.nz
- Organisation: New Zealand Customs Service, Drug Investigation Unit

Finalised the case setup by clicking Finish, successfully creating the Autopsy case environment for subsequent forensic tasks.

1550 Hours

Added primary evidence image Narcos-1.001 as the data source within the "Narcos 2025" Autopsy case. Set the time zone to (GMT +12:00) Pacific/Auckland to match the local time of acquisitioned device. Left the hashes values blank, as hash computation will be handled during the ingest module process.

Before running Autopsy analysis on the entire case, I selected a set of relevant ingest modules to do on startup including:

- Recent Activity
- Hash Lookup
- File Type Identification
- Extension Mismatch Detector
- Embedded File Extractor
- Picture Analyzer
- Email Parser
- Encryption Detection
- Interesting Files Identifier
- Central Repository
- PhotoRec Carver
- Data Source Integrity.

Did not perform keyword search in initial ingest module run as I wanted to gather facts and findings first for it to be more effective when run. Finalised the data source addition by clicking Finish, initiating ingest processing for forensic analysis.

May 18, 2025

1500 Hours

Observed ingest modules finishing and began logical analysis of the data contained in the Autopsy case.

1510 Hours

I first verified the integrity of the loaded image by comparing its computed hashes within Autopsy against those recorded in the original FTK Imager report. Within Narcos-1.001 File Metadata section of the image on Autopsy, we can identify:

- MD5: c63a3d19e9c9495b573f45be544e50f9
- SHA1: 4d8e5041f47e0b0fc0eacc85d300661946537418
- SHA256: 5e2e3e8f05edba603c9b22f8d91514d7b4fb1df66d575354070dc9bc9a9a59cb

The MD5 and SHA1 hashes exactly match those recorded by FTK Imager at the time of acquisition, confirming that the Autopsy mounted image retained forensic integrity, and the segmented image files remain unaltered since acquisition.

1530 Hours

Commenced analysis by implementing tags to categorize and link observed artifacts to relevant investigation areas. The following initial tags that were created to annotate artifacts were:

- #communication -> Communications-related data, e.g. emails, messaging platforms.
- #contributing_documentation -> Document files, accessed images, web pages, etc. that help build the case.
- #drugs -> Artifacts indicative of drug-related content or behavior.
- #images -> Specific images related and confirmed being related to the case.
- #john_connection -> Chats, messages, docs relating to John.
- #location -> Images, web data, documents relating to location's.
- #login/passwords -> Discovered credentials, login artifacts, or saved password data.
- #obfuscation -> Evidence of data hiding, encrypted files, steganography.

- #timeline -> Timeline of user activity, e.g. files access, downloads, messages.
- #user_identity -> user-specific artifacts (user folders, registry info, account details)

This allows structured tracking of observed data and will support development of a narrative and timeline as analysis progresses.

1600 Hours

I then went and identified OS details in the Data Artifacts section:

- Name: SK-DESKTOP
- Program Name: Windows 10 Pro
- Processor Architecture: AMD64
- Product ID: 00330-80000-00000-AA502
- Owner: Steve

After analysing this, I went and looked at the image's Data Sources Summary, to confirm further understanding of the user's device:

- Size: 32 GB
- Files: 240229
- Artifacts: 207505
- Geolocation: Upper Hutt, Wellington; New Zealand

1620 Hours

I then went and confirmed the image's file system design. Confirmed in vol4 (Basic data partition) in file $Boot (/$boot) that the file system is NTFS (New Technology File System) (#user_identity).

May 21, 2025

1100 Hours

Decided to perform intial analysing of the Data Artifacts section in Autopsy, to gain understanding on the Artifacts provided, which would contribute to a more coherent Keyword Search.

1130 Hours

Conducted initial review of the Chromium Extensions artifact category. Lists browser extensions that were either pre-installed or actively used by the user within a

Chromium-based browser, like Google Chrome or Microsoft Edge. Notable findings include:

- Name: Docs
    - Description: Create and edit documents
    - Version: 0.10
    - Source File Path: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/Secure Preferences
- Chrome PDF Viewer
    - Version: 1
    - Source File Path: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/Secure Preferences
- Google Drive
    - Description: Create, share and keep all your stuff in one place.
    - Version: 14.2
    - Source File Path: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/Secure Preferences
- Google Hangouts
    - Version: 1.3.12
    - Source File Path: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/Secure Preferences
- CryptoTokenExtension
    - Description: CryptoToken Component Extension
    - Version: 0.9.74
    - Source File Path: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/Secure Preferences
- Gmail
    - Description: Fast, searchable email with less spam
    - Version: 8.1
    - Source File Path: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/Secure Preferences

1180 Hours

Performed initial review of the Chromium Profiles artifact category. Only a single profile-related artifact was present:

- Source Name: Local State (#login/passwords).
    - Path: Default
    - Name: Person 1

  - Program Name: Google Chrome
  - Source File Path: /Users/Steve/AppData/Local/Google/Chrome/User Data/Local State

This is the default name assigned by Chromium-based browsers when a user has not signed into a Google account. This profile is a temporary local profile used to store browsing data such as bookmarks, browsing history, and extension configurations without linking to a Google Account.

1200 Hours

Conducted an initial review of the Favicon artifact category, which stores records of websites visited by the user based on stored favicon data. Date Accessed times cannot be determined in these Favicon outputs. There is however Date Modified dates associated with each entry. Notable findings included:

- http://www.wcl.govt.nz/about/branches (#location)
  - URL:
    - http://www.wcl.govt.nz/about/branches/brooklyn, AND
    - http://www.wcl.govt.nz/about/branches/ruthgotlieb
  - Date Modified: 2019-02-02 14:01:56.
  - Identified user accessing the branches page, specifically viewing the Brooklyn and Ruth Gotlieb libraries.
- https://qz.com (#drugs)
  - URL: https://qz.com/481037/dark-web/
  - Date Modified: 2019-02-02 13:57:19
  - User visited an article discussing the dark web and becoming a drug lord.
- https://sourceforge.net (#obfuscation)
  - URL: https://sourceforge.net/projects/image-steg/files/latest/download
  - Date Modified: 2019-02-01 13:15:10
  - User downloaded an image steganography tool.
- https://www.drugfreeworld.org (#drugs)
  - URL: https://www.drugfreeworld.org/drugfacts/crystalmeth.html.
  - Date Modified: 2019-01-31 15:55:03
  - User viewed educational material discussing crystal meth.
- https://www.google.com/maps (#location)
  - URL: Multiple URLs indicating different locations around the wellington region e.g. /dir//Eastbourne,+Lower+Hutt+5013.
  - Date Modified: 2019-01-31 10:17:26

    - User viewed coordinates and locations within the Wellington region. Will follow up on locations in further analysis.
- https://earth.nullschool.net (#location)
    - URL: Multiple URLs focusing on: /#current/wind/surface/level/orthographic=[coordinate].
    - Date Modified: 2019-01-30 10:23:15
    - User used site to visualize global wind patterns; user viewed coordinates including ones in New Zealand.
- https://mail.protonmail.com (#communication)
    - URL: Multiple URLs, two including https://mail.protonmail.com/login AND https://mail.protonmail.com/login/unlock, and two identifying different resources in /inbox/.
    - Date Modified: 2019-01-30 12:34:21
    - User frequently visited secure proton email service. Showed artifacts suggesting user signed in, accessed their inbox, and unlocked content.
- https://www.cleaner.com (#obfuscation)
    - URL: https://www.cleaner.com/ccleaner/download/standard
    - Date Modified: 2019-01-30 12:40:39
    - User downloaded a privacy and system cleaning tool.
- https://www.lifewire.com (#obfuscation)
    - URL: https://www.lifewire.com/truecrypt-review-2619179
    - Date Modified: 2019-01-30 12:26:57
    - User accessed reviews of TrueCrypt which is a disk encryption software.
- www.softpedia.com (#obfuscation)
    - URL: https://www.softpedia.com/dyn-postdownload.php/9196da93f480ba08f95035b293f60971/5c50ef6a/44cf/4/2
    - Date Modified: 2019-01-30 12:27:15
    - User accessed an online webpage to download TrueCrypt.

1280 Hours

Conducted an initial review of the Installed Programs artifact category, which records software installations on the system. Notable findings were:

- Microsoft Visual C++ 2008 Redistributable x86 v.9.0.30729.6161
    - Date/Time: 2019-01-28 19:37:36
    - Source File Path: Windows/System32/config/SOFTWARE
- Microsoft Visual C++ 2008 Redistributable x64 v.9.0.30729.6161

  - Date/Time: 2019-01-28 19:37:36
  - Source File Path: Windows/System32/config/SOFTWARE
  - User downloaded both 32 and 64-bit versions of Microsoft Visual C++ indicating that he is going to be running programs needing C++ libraries. Indicates that he is running 64-bit system as needed both x64 and x86 versions.
- VMware Tools v.10.2.0.7259539 (#obfuscation)
  - Date/Time: 2019-01-28 19:38:25
  - Source File Path: Windows/System32/config/SOFTWARE
  - Downloaded VMware tools indicating the user using a VM.
- OpenOffice v.4.16.9790
  - Date/Time: 2019-01-28 19:38:25
  - Source File Path: Windows/System32/config/SOFTWARE
  - Free alternative for Microsoft office, that can be used to write/edit documents.
- TrueCrypt v.7.1a (#obfuscation)
  - Date/Time: 2019-01-29 23:28:24
  - Source File Path: Windows/System32/config/SOFTWARE
  - Installed TrueCrypt software that performs full-disk encryption on entire disk.
- CCleaner v.5.52 (#obfuscation)
  - Date/Time: 2019-01-29 23:41
  - Windows/System32/config/SOFTWARE
  - Installed CCleaner software that performs file removal.

1320 Hours

Conducted an initial review of the Recent Documents artifact category. This section primarily consists of .lnk shortcut files, which provide metadata about recently accessed files, including file paths, timestamps, and associated applications. Notable findings include:

- https—cdn.discordapp.com-attachments-539550615072800768-541074665892741121-Steve_K.PNG.lnk (#communication)
  - Date Accessed: 2019-02-02 15:28:16
  - Can observe the link contains the filename Steve_K.PNG.
- Encrypted or Obfuscated filenames
  - Multiple .lnk files
  - e.g. ee9a310ff1c7018bdbf1b201c5de5c63.lnk

 - Files all point to .jpg files with hash-like, encrypted or non-descriptive filenames
- Screen sketch documents (#contributing_documentation)
  - e.g. ms-screensketch—edit-source=screenclip&isTemporary=true&sharedAccessToken=9aF99417-0207-4143-95C9-7DB74B203685&viewId=-132139.lnk
  - Date/Time(s): 2019-01-31 10:25:05, 2019-01-31 10:20:52, 2019-02-02 14:05:42
  - User has created (3) screen-sketch documents using Snip & Sketch or Snipping Tool application to open and annotate screenshots or images.
- airport crystals.lnk (#drugs)
  - Path: C:\Users\Steve\Documents\Misc\airport crystals.jpg
  - Date Accessed: 2019-01-31 10:25:18
  - Source File Path: Users/Steve/AppData/Roaming/Microsoft/Windows/Recent/airport crystals.lnk
- price-meth-bust-4.lnk (#drugs)
  - Path: C:\Users\Steve\Pictures\price-meth-bust-4.jpg
  - Date Accessed: 2019-01-31 15:58:22
  - Source File Path: Users/Steve/AppData/Roaming/Microsoft/Windows//Recent/price-meth-bust-4.lnk
- eight_col_patches_crp.lnk (#drugs)
  - Path: C:\Users\Steve\Pictures\eight_col_patches_crp.jpg
  - Date Accessed: 2019-01-31 15:59:38
  - Source File Path: Users/Steve/AppData/Roaming/Microsoft/Windows/Recent/eight_col_patches_crp.lnk
- dropoff.lnk (#contributing_documentation)
  - Path: C:\Users\Steve\Documents\Misc\dropoff.jpg
  - Date Accessed: 2019-02-02 14:06:05
  - Source File Path: Users/Steve/AppData/Roaming/Microsoft/Windows/Recent/dropoff.lnk
- flightbookings.lnk (#contributing_documentation)
  - Path: C:\Users\Steve\Documents\Misc\flightbookings.PNG
  - Date Accessed: 2019-02-02 15:25:44

  - Source File Path: Users/Steve/AppData/Roaming/Microsoft/Windows/Recent/flightbookings.lnk
- Method run.lnk (#contributing_documentation)
  - Path: C:\Users\Steve\Documents\Misc\Method run.jpg
  - Date Accessed: 2019-01-31 10:21:24
  - Source File Path: Users/Steve/AppData/Roaming/Microsoft/Windows/Recent/Method run.lnk
- package.lnk (#contributing_documentation)
  - Path: C\Users\Steve\Downloads\Misc\package.jpg
  - Data Accessed: 2019-02-01 15:49:18
  - Source File Path: Users/Steve/AppData/Roaming/Microsoft/Windows/Recent/package.lnk

Will follow up on each of these links to images to determine what they show.

1480 Hours

Conducted an initial review of the Recycle Bin artifact category. This section consists of artifacts that are currently sitting in the recycle bin on the users computer. Notable findings include:

- $R5WIK39.jpg (#contributing_documentation)
  - Path: C:\Users\Steve\Pictures\eight_col_patches_crp.jpg
  - Time Deleted: 2019-02-01 15:48:41
  - Source File Path: $Recycle.Bin/S-1-5-21-1474204758-2504895174-1356074821-1001/$R5WIK39.jpg
  - Shows a picture of two Mongrel Mob jackets.
- $RA3IE5E (#drugs)
  - Path: C:\Users\Steve\Pictures\price-meth-bust-4.jpg
  - Time Deleted: 2019-02-01 15:48:41
  - Source File Path: $Recycle.Bin/S-1-5-21-1474204758-25048951740135697482101-1001/$RA3IE5E.jpg
  - Shows a picture of meth and other drugs, with $5,391 in cash.
- $RIIK1AS.jpg (#drugs)
  - Path: C:\users\Steve\Pictures\620x349.jpg
  - Time Deleted: 2019-02-01 15:48:41
  - Source File Path: $Recycle.Bin/S-1-5-21-147204758-2504895174-1356074821-1001/$RIIK1AS.jpg

- Shows a picture of four bags of methamphetamine.

1500 Hours

Conducted an initial review of the Run Programs artifact category. This section contains information on when programs were last run, which is useful for determining user activity. Arranged the output by last runtime to get understanding of user process. Notable findings were:

- CCLEANER.EXE-E5FE256A.pf (#obfuscation)
  - Program Name: CCLEANER.EXE
  - Path: /PROGRAM FILES/CCLEANER
  - Date/Time: 2019-01-31 15:28:52
  - Program run 1 times on 2019-01-31 at 15:28:52 and 3 times on 2019-02-01 between 15:41:17 and 15:56:13.
- CCLEANER64.EXE-1137D9AC.pf (#obfuscation)
  - Program Name: CCLEANER64.EXE
  - Path: /PROGRAM FILES/CCLEANER
  - Program was run 3 times on 2019-01-31 at 09:41:16 and 15:28:52, and 4 times on 2019-02-01 between 09:41:16 and 15:56:09.
- CCSETUP552.EXE-C1C2B3F0.pf (#obfuscation)
  - Program Name: CCSETUP552.EXE
  - Path: /USERS/STEVE/DOWNLOADS
  - Date/Time: 2019-01-30 12:41:04
- DISCORD.EXE-794770(A9/AA/AB/B1).pf (#communication)
  - Program Name: DISCORD.EXE
  - Path:/USERS/STEVE/APPDATA/LOCAL/DISCORD/APP-0.0.304
  - was run 32 times between 2019-01-29 and 2019-02-02
- TRUECRYPT.EXE-9A3632C4.pf (#obfuscation)
  - Program Name: TRUECRYPT.EXE
  - Path: /PROGRAM FILES/TRUECRYPT
  - Date/Time: 2019-01-30 12:31:25
- TRUECRYPT FORMAT.EXE-9F933A19.pf (#obfuscation)
  - Program Name: TRUECRYPT FORMAT.EXE
  - Path: /PROGRAM FILES/TRUECRYPT
  - Date/Time: 2019-01-30 12:31:29
- TRUECRYPT SETUP 7.1A.EXE-CE6985BB.pf
  - Program Name: TRUECRYPT SETUP 7.1A.EXE
  - Path: /USERS/STEVE/DOWNLOADS

  - Date/Time: 2019-01-30 12:28:17
- VMTOOLSD.EXE-52E2146D.pf (#obfuscation)
  - Program Name: VMTOOLSD.EXE
  - Path: /PROGRAM FILES/VMWARE/VMWARE TOOLS
  - Was run 2 times on 2019-01-29 at 08:38:26 and 08:40:58. Was run 1 time on 2019-01-30 at 10:02:23. Was run 2 times on 2019-02-02 at 13:39:27 and 15:38:16.

1550 Hours

Conducted an initial review of USB Device Attached artifact category. This section contains information on connected devices attached to the users device. Notable findings were:

- Source Name: System (#obfuscation)
  - Device Make: VMware, Inc.
  - Device Model: Virtual USB Hub.
  - Device ID: 6&30c8ca5f&0&7 and 6&30c8ca5f&0&8
  - Source File Path: Windows/System32/config/SYSTEM
  - Two devices of the same device model but different IDs. These were both connected/attached on 2019-02-02 at 15:37:25.
- Source Name: System (#obfuscation)
  - Device Make: VMware, Inc.
  - Device Model: Virtual Mouse.
  - Device ID: 6&30c8ca5f&0&5, 7&1ffda586&0&0000 and 7&1ffda586&0&0001
  - Three devices of the same device model but different IDs. These were connected/attached on 2019-02-02 at 15:37:25.
- Source Name: System (#user_identity)
  - Device Make: Western Digital Technologies, Inc.
  - Device Model: Elements Portable (WDBUZG).
  - Device ID: 57584D3145373444574D314E
  - This was connected/attached on 2019-02-01 at 15:41:46.
- Source Name: System (#user_identity)
  - Device Make: Seagate RSS LLC
  - Device Model: Backup Plus Slim Portable Drive 1 TB
  - Device ID: 57584D3145373444574D314E
  - This was connected/attached on 2019-02-01 15:41:46

1600 Hours

Conducted an initial review of Web Accounts artifact category. This section contains information of known web accounts on the computer. There was only one item listed in this section:

- Source Name: Login Data (#communication)
  - URL https://mail.protonmail.com/login
  - Date Created: 2019-02-01 13:12:51
  - Decoded URL: protonmail.com
  - Program Name: Google Chrome
  - Username: Default
  - Source File Path: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/Login Data
  - Can see there is no username associated with the address or anything else identifiable.

<u>May 21, 2025</u>

1050 Hours

Conducted an initial review of Web Cache artifact category. This section provides me with web cache data for websites and applications the user has visited. Notable findings were:

- Source: data_1 (#communication)
  - URL: https://cdn.discordapp.com/attachments/539550615072800768/541074665892741121/Steve_K.PNG
  - Domain: discordapp.com
  - Data created: 2019-02-02 15:28:16.
  - Source Path: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000bf6
  - On further analysis of this data artifact we can see this is it is a 'guploader-uploadid' with the content-type: image/png. We are also provided the path to the output.
  - Path: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000bf6

1100 Hours

Conducted an initial review of Web Downloads artifact category. This section provided me with a list of downloaded artifacts from websites the user had done. Notable findings were:

- Method run.jpg:Zone.Identifier (#contributing_documentation)
  - Created: 2019-01-31 16:04:13
  - Modified: 2019-01-31 10:22:24
  - Accessed: 2019-01-31 16:04:13
  - Path: Users/Steve/Documents/Misc/Method run.jpg
- airport crystals.jpg:Zone.Identifier (#contributing_documentation)
  - Created: 2019-01-31 10:25:18
  - Modified: 2019-01-31 10:25:18
  - Accessed: 16:04:13
  - Path: Users/Steve/Documents/Misc/airport crystals.jpg
- dropoff.jpg:Zone.Identifier (#contributing_documentation)
  - Created: 2019-02-02 14:06:05
  - Modified: 2019-02-02 14:06:06
  - Accessed: 2019-02-02 15:31:06
- BNE.png:Zone.Identifier (#contributing_documentation)
  - Created: 2019-02-01 13:13:19
  - Modified: 2019-02-01 13:13:20
  - Accessed: 2019-02-02 15:31:06
  - Path: Users/Steve/Downloads/Misc/BNE.png
- History (#communication)
  - Created: 2019-01-30 10:05:55
  - Modified: 2019-02-02 15:28:48
  - Accessed: 2019-02-02 15:28:48
  - Domain: protonmail.com
  - URL: blob:https://mail.protonmail.com/f7f4f3a9-ba89-4f46-b2a8-c58bb8f99d4f
  - Date Accessed: 2019-02-01 13:13:19
  - Path: C:\Users\Steve\Downloads\BNE.png (no longer exists)
- History (#contributing_documentation, #communciation)
  - Created: 2019-01-30 10:05:55
  - Modified: 2019-02-02 15:28:48
  - Accessed: 2019-02-02 15:28:48
  - Domain: discordapp.com

  - URL: https://cdn.discordapp.com/attachments/539550615072800768/541074665892741121/Steve_K.PNG
  - Date Accessed: 2019-02-02 15:28:26
  - Path: C:\Users\Steve\Documents\Misc\flightbookings.PNG
- History (#obfuscation)
  - Created: 2019-01-30 10:05:55
  - Modified: 2019-02-02 15:28:48
  - Accessed: 2019-02-02 15:28:48
  - Domain: softpedia-secure-download.com
  - URL: https://softpedia-secure-download.com/dl/f260b98f6df9dab1ec044f710a9af031/5c50e160/100017615/software/security/encrypt/TrueCrypt%20Setup%207.1a.exe
  - Date Accessed: 2019-01-30 12:27:43
  - Path: C:\Users\Steve\Downloads\TrueCrypt Setup 7.1a.exe
- History (#obfuscation)
  - Created: 2019-01-30 10:05:55
  - Modified: 2019-02-02 15:28:48
  - Accessed: 2019-02-02 15:28:48
  - Domain: ccleaner.com
  - URL: https://download/ccleaner.com/ccsetup552.exe
  - Date Accessed: 2019-01-30 12:40:51
  - Path: C:\Users\Steve\Downloads\ccsetup552.exe
- History (#obfuscation)
  - Created: 2019-01-30 10:05:55
  - Modified: 2019-02-02 15:28:48
  - Accessed: 2019-02-02 15:28:48
  - Domain: sourceforge.net
  - URL: https:/versaweb.dl.sourceforge.net/project/image-steg-Image%20Steganography%Steganography%201.5.2%20Setup.exe
  - Date Accessed: 2019-02-01 13:16:32
  - Path: C:\Users\Steve\Downloads\Image Steganography 1.5.2 Setup.exe

1150 Hours

Conducted an initial review of Web Form Autofill artifact category. This section provided me with only one autofill output:

- Source Name: Web Data (#login/passwords)

  - Name: username
  - Value: crayfish1980
  - Date Created: 2019-01-30 12:34:33
  - Date Accessed: 2019-02-01 13:22:00
  - Source File: Users/Steve/AppData/Local/Google/Chrome/User Data/Default

1200 Hours

Conducted an Initial review of Web History artifact category. This section provided me with a list of web cache .dat files and History files. Notable findings were:

- History (#location)
  - Username: Steve
  - Domain: Google AND google.com
  - Program Name: Microsoft Edge Analyzer and Google Chrome
  - Can see user using google.com/maps, searching for places around Wellington. Analysing the URL address's we can see these places include:
    - Stoke Valley, Cannons Creek, Porirua, Lower Hutt, Upper Hutt, Eastbourne, Eastbourne Library, Wainuiomata, Wellington International Airport, Rongotai, drug routes in around wellington, international drug routes, new zealand drug foundation. Relevant coordinates are associated with the history URLs.
  - Web history for this ranges from 2019-01-31 – 2019-02-02. Further investigation will be performed later.
- History (#drugs)
  - Title: What is Methamphetamine? What is Crystal Meth? How is Meth Used?
  - Date Accessed: 2019-01-31 15:55:01
  - Domain: drugfreeworld.org
  - URL: https://www.drugfreeworld.org/drugfacts/crystalmeth.html
  - Program Name: Google Chrome
  - Source File: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/History
- History (#location)
  - Title: About the library
  - Username: Default
  - Date Accessed: 2019-02-02 14:02:25
  - Domain: wcl.govt.nz
  - URL: http://www.wcl.govt.nz/about/branches/brooklyn
  - Program Name: Google Chrome

  - Source File: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/History
- History (#location)
  - Title: Ruth Gotlieb (Kilbirnie) Library
  - Username: Default
  - Date Accessed: 2019-02-02 14:02:35
  - Domain: wcl.govt.nz
  - URL: http://www.wcl.govt.nz/about/branches/ruthgotlieb
  - Program Name: Google Chrome
  - Source File: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/History
- WebCache.dat (#drugs)
  - Username: Steve
  - Date Accessed: 2019-01-28 22:59:05
  - Domain: Wikipedia.org
  - URL: https://en.wikipedia.org/wiki/Cutting_agent
  - Program Name: Microsoft Edge Analyzer
  - Source File: Users/Steve/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat
- WebCacheV01.dat (#drug)
  - Username: Steve
  - Date Accessed: 2019-01-28 23:00:40
  - URL: https://sunrisehouse.com/cause-effect/cutting-agents-drug-manufacturing/
  - Program Name: Microsoft Edge Analyzer
  - Source File: Users/Steve/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat
- WebCacheV01.dat (#drugs)
  - Username: Steve
  - Date Accessed: 2019-01-28 23:02:07
  - URL: https://www.therecoveryvillage.com/meth-addiction/dangers-meth-cutting-agents/
  - Source File: Users/Steve/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat

- WebCacheV01.dat (#drugs)
  - Username: Steve
  - Date Accessed: 2019-01-28 23:02:10
  - Domain: vice.com
  - URL: https://www.vice.com/en_nz/article/59d8wd/four-dealers-describe-the-worst-chemicals-they-use-to-cut-drugs
  - Program Name: Microsoft Edge Analyzer
  - Source File: Users/Steve/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat
- WebCacheV01.dat (#drugs)
  - Username: Steve
  - Date Accessed: 2019-01-28 23:03:57
  - Domain: businessinsider.com.au
  - URL: https://www.businessinsider.com/au/beginners-guide-to-money-laundering-2014-10?r=US&IR=T
  - Program Name: Microsoft Edge Analyzer
  - Source File: Users/Steve/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat
- WebCacheV01.dat (#drugs)
  - Username: Steve
  - Date Accessed: 2019-01-28 23:03:57
  - Domain: oceanbreezerecovery.org
  - URL: https://oceanbreezerecovery.org/blog/drug-cutting/
  - Program Name: Microsoft Edge Analyzer
  - Source File: Users/Steve/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat

1230 Hours

Conducted an initial review of Web Search artifact category. This section provided me with a list of Web Cache .dat files and History files. Notable findings were:

- Source Name: History (#obfuscation)
  - Term: truecrypt
  - Time: 2019-01-30 12:26:30
  - Domain: google.com

  - Program Name: Google Chrome
  - Source File: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/History
- Source Name: History (#communication)
  - Term: protonmail
  - Time: 2019-01-30 12:34:09
  - Domain: google.com
  - Program Name: Google Chrome
  - Source File: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/History
- Source Name: History (#obfuscation)
  - Term: ccleaner
  - Time: 2019-01-30 12:40:35
  - Domain: google.com
  - Program Name: Google Chrome
  - Source File: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/History
- Source Name: History (#drugs)
  - Term: drug paraphernalia
  - Time: 2019-01-31 15:57:16
  - Domain: google.com
  - Program Name: Google Chrome
- Source Name: History (#drugs)
  - Term: drug paraphernalia meth
  - Time: 2019-01-31 15:57:50
  - Domain: google.com
  - Program Name: Google Chrome
- Source Name: History (#drugs)
  - Term: gangs nz drugs
  - Time: 2019-01-31 15:59:17
  - Domain: google.com
  - Program Name: Google Chrome
  - Source File: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/History
- Source Name: History (#obfuscation)
  - Term: image steganography download
  - Time: 2019-02-01 13:15:04

  - Domain: google.com
  - Program Name: Google Chrome
  - Source File: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/History
- Source Name: History (#drugs)
  - Term: best places to trade drugs
  - Time: 2019-02-02 14:01:34
  - Domain: google.com
  - Program Name: Google Chrome
  - Source File: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/History
- Source Name: History (#location)
  - Term: wellington libraries
  - Time: 2019-02-02 14:01:51
  - Domain: google.com
  - Program Name: Google Chrome
  - Source File: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/History
- Source Name: History (#location)
  - Term: courtney place
  - Time: 2019-02-02 14:01:51
  - Domain: google.com
  - Program Name: Google Chrome
  - Source File: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/History
- Source Name: History (#location)
  - Term: eastbourne library
  - Time: 2019-02-02 14:04:36
  - Domain: google.com
  - Program Name: Google Chrome
  - Source File: Users/Steve/AppData/Local/Google/Chrome/User Data/Default/History
- Source Name: WebCacheV01.dat (#location)
  - Term: international drug routes
  - Time: 2019-01-29 01:04:12
  - Domain: google.co.nz
  - Program Name: Microsoft Edge Analyzer

- Source File: Users/Steve/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat

1300 Hours

Planned next approach to analysing the user's disk image. Started creating a keyword list to go through off of notable findings from initial analysis as well as interpretation. Added list of common street/slang terms for methamphetamine to the keyword list from the American Addiction Center; Meth Slang Terms page (https://americanaddictioncenters.org/blog/meth-slang-terms). Started running the Keyword Search ingest module against the keyword list created.

<u>May 22, 2025</u>

1300 Hours

Keyword Search ingest module finished running and has identified keywords specified in the keyword lists. Note that the Autopsy keyword search run was buffering, resulting in high usage of memory the Virtual machine had been allocated. This resulted in running keyword searches multiple times and also stopping the keyword search early. Results include:

- steve (Substring Match) –> 24153 Total Matches
- kowhai (Substring Match) –> 46 Total Matches
- john (Substring Match) –> 1062 Total Matches
- crayfish (Substring Match) –> 97 Total Matches
- crayfish1980 (Substring Match) –> 97 Total Matches
- @protonmail (Substring Match) –> 71 Total Matches
- discord (Substring Match) –> 2818 Total Matches
- truecrypt (Substring Match) –> 687 Total Matches
- steganography (Substring Match) –> 221 Total Matches
- crystal (Substring Match) –> 712 Total Matches
- meth (Substring Match) –> 73491 Total Matches
- powder (Substring Match) –> 365 Total Matches
- drugs (Substring Match) –> 364 Total Matches
- dropoff (Substring Match) –> 74 Total Matches
- eastbourne (Substring Match) –> 272 Total Matches
- wainui (Substring Match) –> 185 Total Matches
- naenae (Substring Match) –> 124 Total Matches

- stokes valley (Substring Match) –> 18 Total Matches
- upper hutt (Substring Match) –> 11 Total Matches
- lower hutt (Substring Match) –> 88 Total Matches
- wellington (Substring Match) –> 945 Total Matches
- username (Substring Match) –> 20321 Total Matches
- password (Substring Match) –> 34527 Total Matches
- jane (Substring Match) –> 656 Total Matches
- esteban (Substring Match) –> 7 Total Matches
- money (Substring Match) –> 2618 Total Matches
- cash (Substring Match) –> 1562 Total Matches
- coin (Substring Match) –> 11057 Total Matches
- dollar (Substring Match) –> 1252 Total Matches
- speed (Exact Match) –> 1501 Total Matches
- crank (Exact Match) –> 17 Total Matches
- ice (Exact Match) –> 856 Total Matches
- chalk (Exact Match) –> 35 Total Matches
- wash (Exact Match) –> 60 Total Matches
- trash (Exact Match) –> 99 Total Matches
- dunk (Exact Match) –> 26 Total Matches
- gak (Exact Match) –> 294 Total Matches
- pookie (Exact Match) –> 0 Total Matches
- christina (Exact Match) –> 5 Total Matches
- doze (Exact Match) –> 46 Total Matches
- white cross (Exact Match) –> 4 Total Matches
- cotton candy (Exact Match) –> 4 Total Matches
- rocket fuel (Exact Match) –> 6 Total Matches
- scooby snax (Exact Match) –> 0 Total Matches

1400 Hours

From early analysis, I had identified information that I wanted to go back and grab and cover. I constructed a plan which was:

- Identify and tag executables and file data; CCleaner, Image Steganography, TrueCrypt, VMToolsd.
- Identify and tag relevant images; Steve_K.PNG, Method run.jpg, airport crystals.jpg, dropoff.jpg, flightbookings.png.
- Identify and structure location google searches.

- Identify and read discord communications.
- Look over keyword search hits for more useful information.
- Establish timeline.

1500 Hours

Went and identified CCleaner executable files to add them to evidence tags. Identified in the /Program Files/CCleaner, the executables for CCleaner 32-bit and 64-bit executables.

- CCleaner.exe (#obfuscation)
  - Created: 2019-01-10 23:01:44
  - Modified: 2019-01-10 23:01:44
  - Accessed: 2019-02-02 15:38:42
  - Source File Path: Program Files/CCleaner/CCleaner.exe
- CCleaner64.exe (#obfuscation)
  - Created: 2019-01-10 23:01:44
  - Modified: 2019-01-10 23:01:44
  - Accessed: 2019-02-02 15:38:16
  - Source File Path: Program Files/CCleaner/CCleaner.exe

Can identify here that these two files are being accessed in the same period from when CCleaner was executed (2019-02-02) as per analysis in the Run Programs artifact category, however the created dates don't match with the download times identified when analysing the Web Downloads artifact category.

1530 Hours

Identified the ccsetup552.exe in /Users/Steve/Downloads/ that was downloaded from https://download/ccleaner.com/ccsetup552.exe.

- ccsetup552.exe (#obfuscation)
  - Created: 2019-01-30 12:40:51
  - Modified: 2019-01-30 12:41:07
  - Accessed: 2019-02-02 03:23:30

Confirms to us that he downloaded CCleaner on this date and is using the executables files located in Program Files. This confirms analysis earlier in run programs data artifacts when the program was run on 2019-01-30 at 12:41:04.

1540 Hours

In the Users/Steve/Downloads/ folder we can also identify both startups for other obfuscation methods identified in earlier analysis:

- Image Steganography 1.5.2 Setup.exe (#obfuscation)
  - Created: 2019-02-01 13:16:32
  - Modified: 2019-02-01 13:16:34
  - Accessed: 2019-02-02 03:23:31
- TrueCrypt Setup 7.1a.exe (#obfuscation)
  - Created: 2019-01-30 12:27.43
  - Modified: 2019-01-30 12:27.51
  - Accessed: 2019-02-02 03:23:32

1600 Hours

First went to obtain the executables linked to the TrueCrypt Setup 7.1a.exe. Located the TrueCrypt.exe in ProgramFiles/TrueCrypt. As well as other TrueCrypt executables and files.

- TrueCrypt.exe (#obfuscation)
  - Created: 2019-01-30 12:28:24
  - Modified: 2019-01-30 12:28:24
  - Accessed: 2019-02-02 15:39:16
- TrueCrypt Format.exe (#obfuscation)
  - Created: 2019-01-30 12:28:24
  - Modified: 2019-01-30 12:28:24
  - Accessed: 2019-02-02 03:23:32
- TrueCrypt Setup.exe (#obfuscation)
  - Created: 2019-01-30 12:28:24
  - Modified: 2019-01-30 12:27:51
  - Accessed: 2019-02-02 03:23:32

This confirms the files being created from running TrueCrypt Setup 7.1a.exe on 2019-01-30 at 12:28:17. Tagged the corresponding executables.

1640 Hours

Identified a configuration file for TrueCrypt:

- Configuration.xml (#obfuscation)
  - Created: 2019-01-30 12:31:46
  - Modified: 2019-01-30 13:34:14

  - Accessed: 2019-01-30 13:34:14
  - Source File: Users/Steve/AppData/Roaming/TrueCrypt/Configuration.xml

Has configuration settings chosen by the user for TrueCrypt. Can identify which settings are on and off given a config key, as indicated by:

- >0</config> = off
- >1</config> = on

Can identify configurations:

- <config key=“CachePasswords”>0</config>
- <config key=“SaveVolumeHistory”>0</config>
- <config key=“WipePasswordCacheOnExit”>0</config>
- <config key= “WipeCacheOnAutoDismount”>1</config>

1680 Hours

Could not identify the Image Steganography.exe tool created from Image Steganography 1.5.2 Setup.exe. Have labeled this one from earlier and will be added to extracted findings.

1700 Hours

Identified earlier when doing initial review in Run Programs artifact category, that VMTOOLSD.EXE was run multiple times over 2019-01-29 to 2019-02-02, indicating that the user was actively using a VM. Have tagged down the following executable:

- vmtoolsd.exe (#obfuscation)
  - Changed: 2019-01-29 08:38:03
  - Accessed: 2019-02-02 15:38:19

<u>May 23, 2025</u>

1400 Hours

Analysed results for @protonmail keyword search hits. Investigated the settings.dat.LOG2 file, which also got results for kowhai and crayfish1980.

- Name: Users/Steve/AppData/Local/Packages/Microsoft.Office.OneNote_8wekyb3d8bbwe/Settings/settings.dat.LOG2 (#communication and #login/passwords)
- Accessed/Modified/Created: 2019-01-30 10:08:43

Upon analysis of the file, we can identify the OneNotePrimaryAccountCID and ConnectedAccountCID of the users Microsoft account: 2418c0082017486a. Can also see the Email address associated with the Microsoft account is crayfish1980@protonmail.com. Can also see the first and last name of the user, "Steve" and "Kowhai" respectively.

1420 Hours

Analysed results for @crayfish1980 keyword search hits. Investigated the skypexSkypeId.data file.

- skypexSkypeId.data (#communication and #login/passwords
    - Users/Steve/AppData/Local/Packages/Microsoft.SkypeApp_kzf8qxf38z9g5c/LocalState/AsyncStorage/skypexSkypeId.data
    - Created/Modified: 2019-02-01 13:23:51
    - Accessed: 2019-02-02 15:39:18

1430 Hours

Analysed results for dropoff keyword search hits. Analysed the dropoff.jpg image.

- Users/Steve/Documents/Misc/dropoff.jpg (#images, #location)
- Created: 2019-02-02 14:06:05
- Modified: 2019-02-02 14:06:06
- Accessed: 15:31:06

Confirmed image shows a snapshot google maps screenshot of Eastbourne library. Can clarify it as a screenshot from earlier analysis in recent documents from output "ms-screensketch--…" being performed at 2019-02-02 14:05:42.

1440 Hours

Analysed the users Google Chrome cache directory:

- Users/Steve/AppData/Local/Google/Chrome/User Data/Default/Cache/

to identify any other useful information user may have snapshotted or related to the case. Found multiple cached images from webpages the user had visited, related to his search history on methamphetamine and the dark web, identified earlier from looking at the Web History data artifacts section (#drugs).

Identified images of eastbourne library:

- f_000033 (#location and #images)
  - Created Time: 2019-01-30 10:06:42
- f_00007b (#location and #images)
  - Created Time: 2019-01-30 10:07:25

Identified images of other libraries and places in hutt valley region that were part of user's google searches:

- f_000bde (#location)
  - Created Time: 2019-02-02 14:04:40
  - Image of Moera Library, Lower Hutt.
- f_000bdd
  - Created Time: 2019-02-02 14:04:40
  - Image of Stokes Valley Community Hutt.
- f_000bdc
  - Created Time: 2019-02-02 14:04:40
  - Image of Naenae Community Library.
- f_000bdb
  - Created Time: 2019-02-02 14:04:40
  - Images of Walter Nash Centre, Taita, Lower Hutt.

Also identified a cached image of a return plane ticket, going from Brisbane, QLD (BNE) to Wellington International Airport. (WLG) at 8.45am departure and 3.15 arrival times on the 16th February, 2019. Has a return trip on the 23rd February. There are two cached files that have the same image:

- f_00006a (#images)
  - Created Time: 2019-02-02 15:16:58
- f_000bf6 (#images)
  - Created Time: 2019-02-02 15:28:18

1460 Hours

Identified more Google Chrome cached images. Notable findings were:

- f_000347 (#location)
  - Created Time: 2019-01-31 10:05:56
  - Shows a circled building/warehouse.
- f_000348 (#location)
  - Created Time: 2019-01-31 10:05:56
  - Shows a circled building/warehouse.

- f_00061e (#location)
  - Created Time: 2019-02-01 10:13:32
  - Shows a circled area of un-built property.

Also identified more libraries and buildings that the user was searching for. Can identify cached images showing the Walter Nash center, Naenae community library, Stokes Valley community hub, Moera library, Wellington city library.

1480 Hours

Went and identified the user's documents folder:

- User/Steve/Documents

Can identify a deleted file "secret". File is recovered from unallocated space. Does not contain any data or was corrupted. (#related_documentation).

1500 Hours

Went and identified the users documents folder:

- User/Steve/Documents/Misc

to locate the .jpg's and .png's identified in earlier analysis. Notable items include:

- Method run.jpg (#images and #location)
  - Created: 2019-01-31 10:21:24
  - Modified: 2019-01-31 10:22:24
  - Accessed: 2019-01-31 16:04:13
  - Shows a google maps snapshot, pinned at locations; Eastbourne, Stokes Valley, and Wainuiomata. Also has a annotation on the image stating "Home" next to the Eastbourne marker.
- airport crystals.jpg (#images and #location)
  - Created: 2019-01-31 10:25:18
  - Modified: 2019-01-31 10:25:18
  - Accessed: 2019-01-31 16:04:13
  - Shows a google maps snapshot, pinned at locations; Airport and Eastbourne.
- flightbookings.PNG (#images)
  - Created: 2019-02-02 15:28:44
  - Modified: 2019-02-02 15:28:45
  - Accessed: 2019: 2019-02-02 15:31:06

<u>May 24, 2025</u>

1400 Hours

After identifying the dropoff point was Eastbourne from dropoff.jpg, I analysed results from Eastbourne keyboard search hits. Analysed the 000006.log file (#communication and #john_connection).

- Name: Users/Steve/AppData/Roaming/Discord/Local Storage/leveldb/000006.log
- Created: 2019-01-29 16:43:06
- Accessed: 2019-02-02 15:38:47

Analysis results identify keyword preview of conversation performed in discord. This includes:

- :"good.meet at the Eastbourne library"}}
- of it delivered to wellington""}}
- know how, heard of steganography?"}}

1500 Hours

Identified that steganography has been used on some image acquired. Identified steganography executable being downloaded in Web Downloads earlier. Scaled the web downloads category in date accessed to identify ordering of files accessed. Can see that a downloaded png, BNE.png, from https://mail.protonmail.com on 2019-02-01 at 13:13:19, and a steganography tool had been downloaded from https://downloads.sourceforge.net 3 minutes later. Can also confirm that the steganography tool has been run as per:

- Image Steganography.exe.log
  - Created/Modified: 2019-02-01 13:19:15
  - Source: Users/Steve/AppData/Local/Microsoft/CLR_v4.0/UsageLogs/Image Steganography.exe.log

1510 Hours

Downloaded steganography tool from web history link identified from earlier:

- https://downloads.sourceforge.net/project/image-steg/Image%20Steganography%201.5.2%20Setup.exe?r=https%3A%2F%2Fsourceforge.net%2Fprojects%Fimage-steg%2F&ts=1548980184&use_mirror=versaweb

1520 Hours

Located BNE.png in C:\Users\Steve\Downloads.

- BNE.png (#obfuscation and #images)
  - Created: 2019-02-01 13:13:19
  - Modified: 2019-02-01 13:13:20
  - Accessed: 2019-02-02 15:31:06

Extracted the image to my C: drive, to perform decoding/decryption on. On first attempt extracting the image using Image Steganography 1.5.2 message popped up stating that a password was needed to decode BNE.png.

1700 Hours

Through analysing results from kowhai keyword search hits, I identified a 00000006.bin file:

- Name: Users/Steve/AppData/Local/Packages/Microsoft.Office.OneNote_8wekyb3d8bbwe/LocalState/AppData/Local/OneNote/16.0/cache/0000006.bin. (#login/passwords)
- Created: 2019-02-01 13:24:48.
- Modified: 2019-02-01 13:26:04.

Can observe in the extracted text of the file:

- C:\Users\Steve\Downloads\Misc\BNE
- Pass equals Elchapo2

1720 Hours

Re-ran the image steganography program to decode BNE.png. Decoded the file using the password Elchapo2. Extracted a file named package.jpg. File contents show a suitcase, with the bottom lifted up to hide contents, and 3 wrapped contents to the left of it.

1780

Extracted list of earth.nullschool.net and google maps web searches and took screenshots of each web search from list and added each screenshot to a designated directory.

May 25, 2025

1100 Hours

Decided to look into Discord conversation using ChromeCacheView v1.77. Obtained this online and extracted the executable program. Then went and acquired the cache folder of Discord from Users/Steve/AppData/Roaming/Discord/Cache. I extracted this folder to my C: drive and then opened it in ChromeCacheView.

1130 Hours

While observing content in ChromeCacheView, I identified the filetype:

- URL: https://media.discordapp.net/attachments/539550615072800768/541074665892741121/Steve_K.PNG?width=960&height=446.
  - Created Time: 02/02/2019 03:16:58
  - Last Accessed: 02/02/2019 03:27:23
  - Cache Name: f_00006a

The image contains the plaintext, we identified earlier when observing the Google Chrome cache folder, indicating that this file was grabbed when observing discord. Also matches the flightbookings.PNG seen earlier when viewing the users documents folder (User/Steve/Documents/Misc).

1140 Hours

Identified a file in ChromeCacheView called 50.json, containing the URL:

- https://discordapp.com/api/v6/channels/539550615072800768/messages?limit=50

I extracted this file to analyse in Notepad. Can identify messages between user ‘crayfish1980’ and ‘heresjohnny1’. Can identify messages between them including:

- “…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”.
- “Hmm 10 is a bit much for the first time around and is pretty risky. How about we start off with 1 and can ramp up from there if all goes smoothly?”.

1200 Hours

Started working on the timeline, through #timeline tag. Built on 'File Tags' and 'Result Tags' to then produce my final findings. Tags listed below are arranged in modified time. File Tags include:

- f_000033 (#images, #location)
- f_00007b (#images, #location)
- CCleaner (#obfuscation)
- ms-screensketch--edit-source=screenclip&isTemporary=true&sharedAccessToken=D3901329-3635-43B4-9431-361FED7CEE1C&viewId=-66587.lnk (#contributing_documentation)
- Method_run.jpg (#images, #location)
- ms-screensketch--edit-source=screenclip&isTemporary=true&sharedAccessToken=9AF99417-0207-4143-95C9-7DB74B203685&viewId=-132139.lnk (#contributing_documentation)
- airport crystals.jpg (#images, timeline)
- BNE.png (#obfuscation, #images)
- Image Steganography.exe.log (#obfuscation)
- 00000006.bin (#login/passwords)
- 620x349.jpg (#drugs, #images)
- price-meth-bust-4.jpg (#drugs, #images)
- eight_col_patches_crp.jpg (#images, #contributing_documentation)
- package.lnk (#contributing_documentation)
- f_000bde (#location)
- f_000bdd (#location)
- f_000bdc (#location)
- f_000bdb (#location)
- ms-screensketch--edit-source=screenclip&isTemporary=true&sharedAccessToken=FC4FC88E-C59A-4E62-81D2-3904BD1B796C&viewId=-197825.lnk (#contributing_documentation)
- dropoff.jpg (#images, #location)
- f_0006a (#images)
- f_000bf6 (#images)
- flightbookings.PNG (#images)
- 000006.log (#communication, #john_connection)

Result Tags include files that back up user behavior:

- Results from Web Downloads
- Results from Web History

- Results from Favicon
- Results from Run Programs

1400 Hours

I finished my forensic analysis. Generated a case report of all data using Autopsy's Generate Report module.

Findings

Relevant user account profile and computer name associated with the desktop:

The following system and user profile information was extracted from the image "Narcos-1.001" during forensic analysis in Autopsy:

- Computer Name: SK-DESKTOP
- Operating System: Microsoft Windows 10 Pro
- Processor Architecture: AMD64
- Product ID: 00330-80000-00000-AA502
- Registered Owner: Steve
- Device Storage Size: 32 GB
- Total Files: 240,229
- Total Artifacts Extracted: 207,505
- File System Type: NTFS (New Technology File System)
- Geolocation (Inferred from User Activity): Upper Hutt, Wellington, New Zealand

This information was identified through the Data Source Summary, File Metadata, and Data Artifacts views in Autopsy. Establishes the primary user, Steve, computer name associated with the desktop, SK-DESKTOP, under investigation.

Relevant web activity:

Identified web activity from 28th January 2019 to 2nd February 2019. We can see the user, Steve, conducting a variety of web searches and downloads. Identified these through analysis of Data Artifacts sections; Web History, Web Downloads, Web Search. Have tagged the relevant information to their corresponding areas throughout analysis. Web activity can also be accessed in the binary files, Web Data and WebCacheV01.dat, also. Relevant web activity includes:

- Web History:
  - https://mail.protonmail.com/...
  - https://www.ccleaner.com/...
  - https://www.google.com/maps/...

  - https://www.google.com/maps/dir/...
  - https://www.drugfreeworld.org/drugfacts/crystalmeth.html
  - https://www.sourceforge.net/projects/image-steg/
  - https://qz.com/481037/dark-web/
  - https://www.wcl.govt.nz/...
  - https://library.huttcity.govt.nz/...
  - https://cdn.discordapp.com/attachments/
  - https://en.wikipedia.org/wiki/Cutting_agent
  - https://www.therecoveryvillage.com/meth-addiction/dangers-meth-cutting-agents/
  - https://oceanbreezerecovery.org/blog/drug-cutting/
  - https://en.wikipedia.org/wiki/Money_laundering
- Web Searches:
  - “best places to trade drugs”
  - “crystal meth”
  - “cutting agents for ice”
  - “cutting drugs”
  - “drug paraphernalia”
  - “drug paraphernalia meth”
  - “drug routes in around wellington”
  - “drug routes in wellington”
  - “eastbourne library”
  - “gangs nz drugs”
  - “how to launder money”
  - “image steganography download”
  - “international drug routes”
  - “protonmail”
  - “truecrypt”
  - “wellington libraries”
- Web Downloads:
  - Method run.jpg:Zone.Identifier
  - airport crystals.jpg:Zone.Identifier
  - dropoff.jpg:Zone.Identifier
  - History: flightbookings.PNG
  - History: BNE.png
  - History: Image Steganography 1.5.2 Setup.exe
  - History: TrueCrypt Setup 7.1a.exe
  - History: ccsetup552.exe
  - History: 40037258meth.jpg (Noted as 620x349.jpg in report)

  - History: eight_col_patches_crp.jpg
  - History: price-meth-bust-4.jpg

Images that help to build a profile of the user's behavior:
Method run.jpg is an image of a snapshot from Google Maps, showing a route with locations like Eastbourne, Wainuiomata, Naenae, and Stokes Valley. Can also see in the image, an annotation "Home" written in next to Eastbourne. Image *airport crystals.jpg* is a snapshot from Google Maps, showing a route from Wellington Airport with a destination of Eastbourne. *BNE.png* is an image showing a city skyline, when extracted using the Steganography tool the user used, using the password "Elchapo2", the image *package.jpg* is extracted, showing a suitcase with a hidden compartment at the bottom, and three wrapped packages next to it. Image *620x349.jpg* is a downloaded image from the internet, showing four bags of meth. Image *price-meth-bust-4.jpg* is an image that contains a selection of narcotics and $5391.00 in cash. Image *dropoff.jpg* is a snapshot from Google Maps, showing the location of Eastbourne library. Images *f_000033* and *f_00007b* are images obtained from Google Chrome cache, showing Eastbourne library. Images *f_00006a*, *f_000bf6* and *flightbookings.PNG* are all the same image containing the return flight tickets going from Brisbane to Wellington. Images; *f_000bde*, *f_000bdd*, *f_000bdc* and *f_000bdb* are all images of libraries and community centers alone the route seen in Method run.jpg, showing locations in Lower Hutt, Stokes Valley, Naenae, and Taita.

Binary files that could help the investigation:
Have identified multiple binaries that would be useful for the investigation. In terms of obfuscation, the user was using CCleaner which can be used to remove unwanted files, registries and caches. Have located the following CCleaner related binaries; *CCleaner.exe*, *CCleaner64.exe* and *ccsetup552.exe*.

Have identified relevant TrueCrypt binaries that can be used to perform full disk encryption. Have located the following TrueCrypt binaries; *TrueCrypt Setup 7.1a.exe*, *TrueCrypt Setup.exe*, *TrueCrypt.exe* and *TrueCrypt Format.exe*.

Identified *vmtoolsd.exe* which was used by the user on multiple occasions between 2019-01-29 and 2019-02-02.

Have identified Image Steganography binaries that can be used to extract data/images out of files, as used with BNE.png which was discussed earlier. Have located the following Image Steganography binary; *Image Steganography 1.5.2 Setup*.

Have identified a file named *00000006.bin*, which contains the password, “Elchapo2” to extract used using the steganography tool to extract package.png from BNE.png.

Have identified files, *Web Data* and *WebCacheV01.dat*, which contain Chrome and Microsoft web autofill data, history, searches.

Means and the content of communications between the two suspects:
Communication identified between the Steve and John Fredricksen, was from Discord. Two files were recovered that showed communication between users crayfish1980 and heresjohnny1. Initially found *000006.log* which contains messages discussing Steganography, Eastbourne and 666 Rewera Drive, which are all locations of importance. Using ChromeCacheView, identified a *50.json* file which contains communications from 28 January 2019 to 02 February 2019. Discord seems like the only way the two suspects communicated at this time.

NOTE (Not part of forensic examiner report): Would like to say that Discord was a popular tool for dealing drugs and other illegal activity around the 2019 period, due to Discord’s encryption policies and processes around that time. This led it to be under a lot of scrutiny by countries like the US and UK, leading to its headquarters’ being now based out of the US to abide by laws, regulations and security policies – essentially for communications to be more easily decrypted during criminal investigations. Discord is now under a lot of pressure around its new encryption policies, which are very insecure.

Any documents that could help the investigation:
Identified two documents that could provide further analysis of other web related actively, both relating to the user’s Microsoft accounts. Extracted *settings.dat.LOG2* located in

- Users/Steve/AppData/Local/Packages/Microsoft.Office.OneNote_8wekyb3d8bbwe/Settings/

which provides us with the user’s information including; crayfish1980@protonmail.com and Steve Kowhai. Typically, Microsoft usernames are associated with a user’s email address, which would indicate that Steve signed up to Microsoft using his protonmail account. Also identified the user’s skype ID from *skypexSkypeId.data* from

- Users/Steve/AppData/Local/Packages/Microsoft.SkypeApp_kzf8qxf38z9g5c/LocalState/AsyncStorage/

showing the ID: “live:crayfish1980”. Analysis into these two accounts, would possibly provide further information on possible potential buyers or communications with John Fredrickson and Jane Esteban.

Any attempts to delete relevant evidence:
Identified three images that had been attempted to be deleted, through analysis of Data Artifacts: Recycle Bin. Images *$R5WIK39.jpg*, *$RA3IE5E.jpg* and *$RIIK1AS.jpg*, which are; *eight_col_parches_crp.jpg*, *price-meth-bust-4.jpg* and *620x349.jpg*. All three files are downloaded from the internet, and the pictures contain of two mongrel mob jackets, narcotics and drug money, and four bags of meth, respectively, and provides further relevance to the case. Also identified a file called *secret* that was recovered from unallocated space but had no data in file metadata or it had been corrupted.

The user also used *CCleaner* which was run three times on 2019-01-31 and four times on 2019-02-01. This program can perform deletion of registries, files, and caches. Could not identify log files associated with the programs use or what files were deleted when run. This also falls under the classification of an obfuscation method as I cannot identify deleted contents.

Obfuscation or encryption methods that the suspect used:
Identified that the user used *TrueCrypt 7.1a*, which was installed on 2019-01-30 at 12:27:43 and actively used between 2019-01-30 to 2019-02-02 15:39.16. There was no evidence of volumes that TrueCrypt encrypted or recovered during analysis, which is a main limitation of this forensic analysis. Identified a *Configurations.xml* document which contains the configurations run by TrueCrypt as per its last modification on 2019-01-30 13:34:14. Configurations include (as per 0=off, 1=on):

- <config key=“CachePasswords”>0</config>
- <config key=“SaveVolumeHistory”>0</config>
- <config key=“WipePasswordCacheOnExit”>0</config>
- <config key= “WipeCacheOnAutoDismount”>1</config>

indicating that the user does not want any history of their cache's on memory.

Identified that the user was using *Image Steganography 1.5.2*, which was installed on 2019-02-02 at 03:23:31 and used on 2019-02-01 13:19:15 as per the Image Steganography.exe.log. This was used to extract package.png from image BNE.png, downloaded from protonmail.

Also identified from early analysis, that the user was using a virtual machine, as per running vmtoolsd.exe two times on 2019-01-29, one time on 2019-01-30 and two times on 2019-02-02. Cannot identify what the user was using the VM for, leading to unknown user activity.

Tools Used

- Autopsy 4.21.0
- ChromeCacheView 2.52
- Image Steganography 1.5.2

Glossary

- **OS (Operating System):** The software that manages hardware and software resources on a computer.
- **.exe (Executable File):** A Windows program file that can be run by the operating system. Often targeted in malware investigations due to its ability to perform operations on execution.
- **.png (Portable Network Graphics):** An image file format that supports lossless compression. Commonly used for screenshots, website graphics, and digital media.
- **.jpg / .jpeg (Joint Photographic Experts Group):** A compressed image format used widely for photographs and web graphics. May contain metadata useful for forensic analysis (e.g., EXIF).
- **.log (Log File):** A plain text file that records events, operations, or errors created by software or the system. Useful for timeline reconstruction.
- **.dat (Data File):** A generic file extension for binary or structured data used by specific applications. Requires context-specific interpretation.
- **.data:** Typically used by programs to store serialized or binary data. Not a standard format and often needs manual or programmatic parsing.
- **.lnk (Shortcut File):** Windows shortcut files that point to other files or programs. Contain metadata about file paths, usage timestamps, and access history.
- **.url (Internet Shortcut File):** A file used by Windows to store a web address. Typically found in user directories or browser favorites and useful for web activity analysis.
- **.bin (Binary File):** A generic binary file that can represent compiled code, firmware, or disk images. May require hex or byte-level inspection for meaning.
- **Autopsy:** A digital forensics platform used for analyzing disk images and extracting evidence, artifacts, and metadata. It provides modules for keyword searching, timeline analysis, file recovery, and more.
- **NTFS (New Technology File System):** A proprietary file system developed by Microsoft for Windows. It supports large volumes, file-level security, compression, encryption, and journaling.
- **Artifact:** A piece of data that provides evidence of user activity or system operation. Examples include web history, recent documents, registry entries, or cache files.
- **Disk Image:** An exact byte-for-byte copy of a digital storage medium, such as a hard drive. In this case, the .001 file format refers to a segmented raw disk image.
- **Processor Architecture (AMD64):** A 64-bit architecture developed by AMD, also known as x86-64. It determines how the system processes instructions and memory.

- **Product ID:** A Windows licensing identifier showing which version of Windows was installed. Used to confirm authenticity and OS configuration.
- **Registered Owner:** The user account name assigned during OS installation. Often reveals the primary user of the device.
- **Web Cache:** Temporary files stored by a web browser to improve performance. Can include HTML, images, scripts, and even embedded content.
- **Geolocation Metadata:** Information that indicates the approximate physical location of the user, often inferred from browser activity, IP addresses, or metadata in files.
- **Binary File:** A file containing non-text data, often executables or compiled code. Can be analyzed for potential malware or hidden functionality.
- **Obfuscation:** The deliberate concealment of information within code or files to make it difficult to understand or detect. Often used by malware to avoid detection.
- **Encryption:** The transformation of data into a coded format to prevent unauthorized access. Forensics tools may detect encryption methods to assess potential concealment.
- **Ingest Module:** An Autopsy component that processes files for indexing and artifact extraction during analysis.
- **Virtual Machine:** A software-based emulation of a physical computer that runs an operating system and applications in an isolated environment.

Examiner Name	Thomas Green
Examiner Signature	
Data	2025-01-25