

Vincent Cruz

Dr. Hicks

IS 4483-001

02 May 2023

Final Project

Support Requested

I was requested to analyze Terry Brown's seized hard drive and gmail inbox in order to find evidence that Special Agent Stabler's suspicions are correct and Terry Brown is in fact part of the drug operation. Topics of interest are whether or not a local HEB is being used as a pickup location, how Terry Brown and his distributor communicate, who he has sold to, as well as if file brick.jpeg is on his computer. These questions can be answered by looking for evidence in the files sorted by Autopsy, in areas like emails, images, and deleted files.

Discussion of Findings

1. Terry Brown communicates with his supplier by email, using Base64 encoding, between the hours of 16:54 and 18:01 CDT, shown in Exhibit A. The translated conversation is highlighted with Exhibit B.

Exhibit A

Source File	S	C	E-Mail From	E-Mail To	Subject	Date Received
📧 terrybrown.mbox			murphyboyssa@gmail.com;	terrybrownsa@gmail.com;	Re: Your Request	2020-06-27 18:01:02 CDT
📧 terrybrown.mbox			terrybrownsa@gmail.com;	murphyboyssa@gmail.com;	Re: Your Request	2020-06-27 17:54:15 CDT
📧 terrybrown.mbox			murphyboyssa@gmail.com;	terrybrownsa@gmail.com;	Re: Your Request	2020-06-27 17:42:38 CDT
📧 terrybrown.mbox			terrybrownsa@gmail.com;	murphyboyssa@gmail.com;	Re: Your Request	2020-06-27 17:15:14 CDT
📧 terrybrown.mbox			murphyboyssa@gmail.com;	TerryBrownSA@gmail.com;	Your Request	2020-06-27 16:54:05 CDT

Exhibit B

State when you are ready and your request

I'm ready and interested in your product (10 kilos).

Familiarize yourself with Quick Stego Stego program by cybernecence, then visit <https://tinyurl.com/y7k5naeh>
the dates make no sense - are you for real?!

Apologies - see updated link at <https://tinyurl.com/y7mr89qt>

2. It does appear Terry Brown has attempted/received product from the distributor. After following the links and using QuickCrypto to decode the hidden message in file Beach(1).jpeg, this message is found in Exhibit C. In Exhibit D, you can see a picture of the king arthur bag on Terry Brown's computer. Furthermore, in Exhibit E, you can see Brown's web search for the address given to him in the hidden message.

Exhibit C

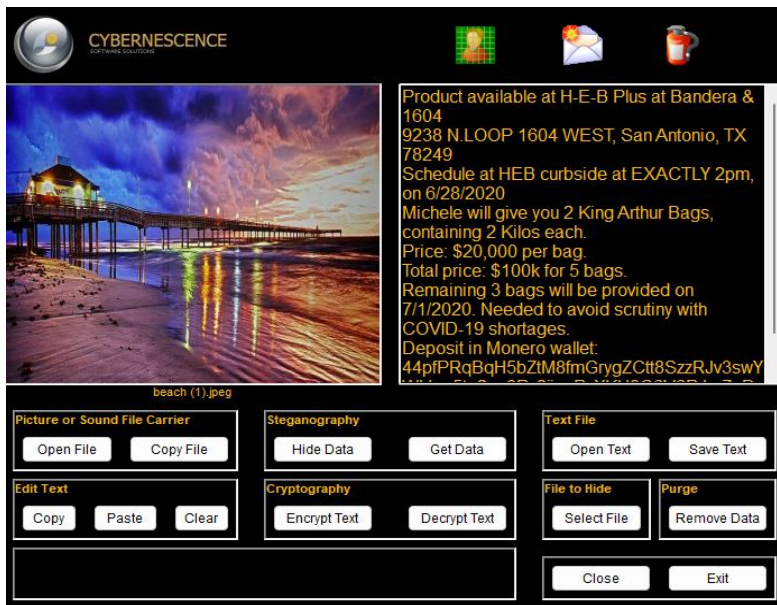


Exhibit D



Exhibit E

extracted Content

- EXIF Metadata (4)
- Encryption Suspected (2)
- Extension Mismatch Detected (16)
- Installed Programs (36)
- Metadata (83)
- Operating System Information (2)
- Operating System User Account (8)
- Recent Documents (5)
- Run Programs (807)
- Shell Bags (5)
- USB Device Attached (10)
- User Content Suspected (4)
- Web Bookmarks (6)
- Web Cookies (99)
- Web Downloads (12)
- Web History (57)
- Web Search (6)

Type	Value	Source(s)
Domain	www.google.com	Recent Activity
Text	Directions to H-E-B Plus at Bandera & 16049238 N LOOP 1604 WEST, San Antonio, TX 78249	Recent Activity
Program Name	Firefox	Recent Activity
Date Accessed	2020-06-27 18:06:08	Recent Activity
Source File Path	/img_Virtual Disk-flat.vmdk/vol3/Users/Terry Brown/AppData/Roaming/Mozilla/Firefox/Profiles/hj28uurh.default-release/places.sqlite	
Artifact ID	-9223372036854775625	

3. Upon adding the hash given by Agent Stabler to a new hashlist called brick, Autopsy found a file named "q" with a matching MD5 hash. Meaning though the file now has a different name, the data has not been changed. Evidence shown in Exhibit F and Exhibit G.

Exhibit F



Listing					
Brick					
Table Thumbnail					
Page: 1 of 1 Pages: < > Go to Page: <input type="text"/>					
Source File	S	C	MD5 Hash	Comment	File Path
 q			2402c544fbf6f2b054ec4d7f6de9560a		/img_Virtual Disk.vmdk/vol_vol3/Users/Terry Brown/Pictures/q

Exhibit G

4. It does appear Terry Brown had other clients. While looking through the folders on Brown's computer, I noticed a couple of text documents, one of which had "clients" in the file name, and a list of names, including Mike Sandoval AKA Agent Stabler. Shown in Exhibit H.

Exhibit H

The screenshot displays a file explorer on the left showing the directory structure of a virtual disk. The right pane shows the contents of the 'Documents' folder for user 'Terry Brown'. Below the file list, a search tool is open, displaying the contents of the file 'spurs.txt:clients.txt'.

File List:

Name	S	C	Modified Time	Change Time	Access Time
spurs.txt			2020-06-27 17:27:28 CDT	2020-06-27 17:27:28 CDT	2020-06-29 15:26:27 C
desktop.ini			2020-06-27 16:47:25 CDT	2020-06-27 16:47:25 CDT	2020-06-29 15:27:29 C
[parent folder]			2020-06-27 16:52:34 CDT	2020-06-27 16:52:34 CDT	2020-06-29 15:27:44 C
spurs.txt:clients.txt			2020-06-27 17:27:28 CDT	2020-06-27 17:27:28 CDT	2020-06-29 15:26:27 C
[current folder]			2020-06-27 17:25:59 CDT	2020-06-27 17:25:59 CDT	2020-06-29 15:27:03 C
My Music			2020-06-27 16:46:43 CDT	2020-06-27 16:46:43 CDT	2020-06-27 16:46:43 C

File Analysis Tool - Text View:

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset

Cierra Vega
Alden Cantrell
Kierra Gentry
Pierre Cox
Thomas Crane
Miranda Shaffer
Bradyn Kramer
Mike Sandoval

-----METADATA-----