Federal Bureau of Investigation FBI Computer Analysis Response

th Court

Miami Division CART Miramar, Florida 33027

Team

2030 SW

145

REPORT OF EXAMINATION

To: SA Austin Winters
FBI Buffalo

Date: May 2,2020
Case ID: NS-19992-CC

Request No.: 54321

Request Date: March 26, 2020

Ref. No.: N/A

Title: YORKSHIRE BRED

Date item(s) received: May 21, 2018

Item(s) Submitted:

- **Q9923 shadowdrive1_evidence.E01 (1B1)**

Summary:

Case agent made several requests with respect to the submitted evidence. This section summarizes the results of the examination pursuant to those requests.

1. Was there any identifying information found about the suspect?

There was numerous personal information found about the suspect in the secretnote.txt file which included:

First Name: Samual
Last Name: Jamestown
Birthdate: April 1, 1984

Address: 192 Crestview RD, Vista, CA 93482 E-mail: sjamestown@bostontea.net

In addition to the personal information; there financial credit card information was also found with the card number, pin, secret number and credit limit of $23,094.

2. Was there any co-conspirators found in the fraud scheme?

After sorting through the Email in the sorted file section two emails were found that gave details the fraud scheme and possible co-conspirators.

a. In the cryptkeeper.eml file, there were details of trying to obtain access keys and attempting to retrieve the access code of an individual named Beth. The email also stated that Samual's code can be found in the e-mail. The email was from a possible co-conspirator code named Skeleton Key.

b. In the cryptkeeper2.eml file, it was confirmed that Beth's code was obtained and the second half of Samual's code could be obtained by solving a riddle given in the email. The email was sent by another possible co-conspirator with the code name Diablo.

3. Was there any evidence of any social media accounts?

By performing a keyword search on multiple social media platforms, browser cookies from Facebook, Twitter and LinkedIn were found. These social media accounts can be used to provide more information about the suspect like recent activities, more personal information like occupation, friends, family members and who the suspect has been interacting with.

4. Was any evidence of a sports car found?

A JPEG image of a 2011 Ford Camaro was found going through the images of the shadow copy. This Camaro was possibly purchased by the money gained from the credit card fraud.

5. Was there any evidence of the suspect being a project manager?

Going through the images, there was a projectmanager.crt file found. The file was actually an image of a t-shirt detailing what it's like being a project manager. This evidence can possible used to support the claim that the suspect is a project manager.

Details of Examination:

The following processes were performed:

A physical inventory of the submitted evidence was completed.

- A drive survey of the submitted images was conducted to find hardware information for the media.
- A forensic image of the submitted evidence was copied to forensically prepared media. The image was verified to match the original evidence.

A directory and file listing were created.

Performed a text search for data sought by the Case Agent. Provided a report of the results and extracted all files with positive and relevant hits of the text search.

Identified and extracted requested files for Case Agent review.

- A post-examination verification of the image was made, showing that the image was not altered during the examination.
- A CD containing the results of the examination (DEMM80521RK1) was produced.

Derivative Evidence/Copies:

DE9923 One (1) Compact Disk (CD) containing results of examination. Disposition of Items:

Derivative evidence DEE9923 and original specimens **Q9923** were returned to Evidence Control.

Examiner: Randy Van

SA/FE Randy Van

FBI Miami Division

Computer Analysis Response Team

NS-19992-CC
54321