***Final Project***

***Fraud Case***

**Name Manderas Kidane**

**ID Number: N01496615**

**Computer Forensic**

**Course # :cis4366**

**Date 12/9/2022**

List of Appendices

[Synopsis/Summary 3](#_Toc121507425)

[Objective 3](#_Toc121507426)

[Evidence Analyzed 4](#_Toc121507427)

[Laptop & hard drive information 4](#_Toc121507428)

[Computer Name 6](#_Toc121507429)

[Windows version: 6](#_Toc121507430)

[Registered owner 7](#_Toc121507431)

[Registered organization 7](#_Toc121507432)

[Digital forensic hash Both a hash and verification hash for the digital forensic image 8](#_Toc121507433)

[Email address used by suspect 9](#_Toc121507434)

[Name of person(s) to whom Frauder may have communicated 10](#_Toc121507435)

[Information on USB devices attached 11](#_Toc121507436)

[Evidence/Relevant Findings 13](#_Toc121507437)

[Supporting Details 14](#_Toc121507438)

[Conclusion 20](#_Toc121507439)

[Attachments 21](#_Toc121507440)

# Synopsis/Summary

Detective Sherlock Holmes #2544 of the Economic Crimes Unit is looking into a credit card fraud case involving Chris Frauder in 11-19-21. A search warrant was served at Frauder's residence at 123 Acme Street by Detective Holmes. One laptop was located after the search. On November 19–21, I received both the laptop and a copy of the search warrant. The case number allocated to the case is 21-111919, and I imaged the laptop as soon as I received it on 11-19-21.and start finding evidence related to credit card fraud using autopsy software.

# Objective

In this report, the investigation's findings are summarized using photos created using data from a laptop that was seized during the search on the fraudster's home. and to gather evidence that supports the materials used in user laptops, considers some of the problems raised, and searches for relevant evidence.

# Evidence Analyzed

## Laptop & hard drive information

* **Make: Dell**
* **Model:**
* **S/N: FQZ2C2**
* **Installed OS: Windows 10 Pro**

****

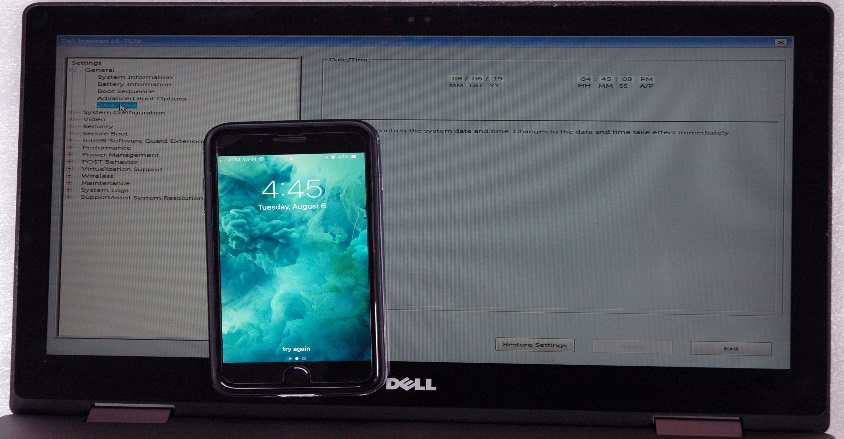
**Bottom picture of computer**

****

**Top picture of computer**



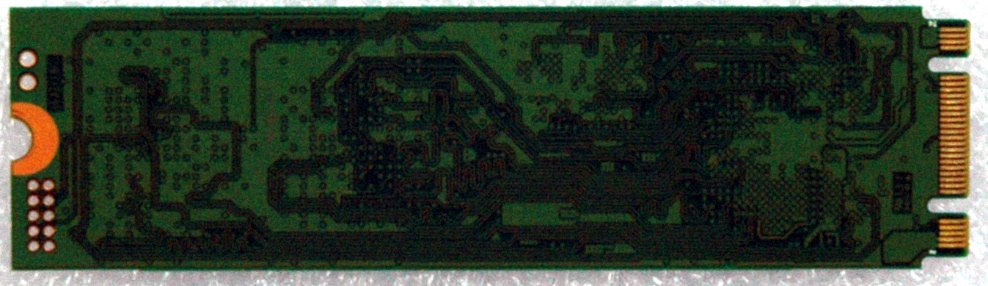
**Picture of make, model and serial number of computer**

****

***BIOS/UEFI time settings with cell phone displaying current date and time.***

**Drive Information (SSD)**

* **S/N: FS69N5324111009K21**
* **Size:512GB**

****

**Bottom Picture of picture of SSD drive**

****

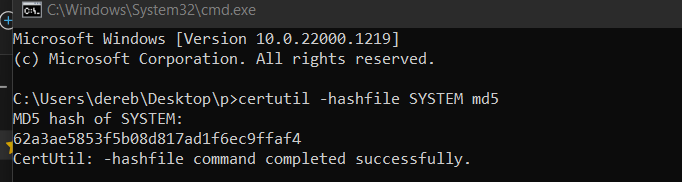
**Top Picture of picture of SSD drive**

## Computer Name

* **Computer Name: Skim-machine**

|  |
| --- |
| **File Metadata**: /img\_Fraud.E01/Windows/System32/config/SYSTEM/controlset/control/ComputerName    *Screenshots 1: pictures showing the computer name used by user.* |

**MD5 hashes for system registry files:**

****

### Windows version:

* **Windows version: Windows 10 Pro**

**Installed date: 2019-03-18 23:05:39EDT**

**File metadata:** img\_Fraud.E01/Windows/System32/config/SOFTWARE/ **Windows version**

### Registered owner

* **Registered owner: C, C Frauder**

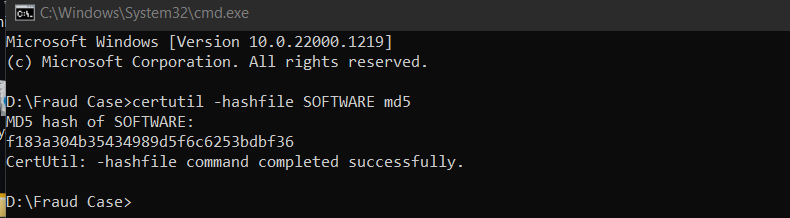
**File metadata:** img\_Fraud.E01/Windows/System32/config/SOFTWARE/ **Registered owner**

### Registered organization

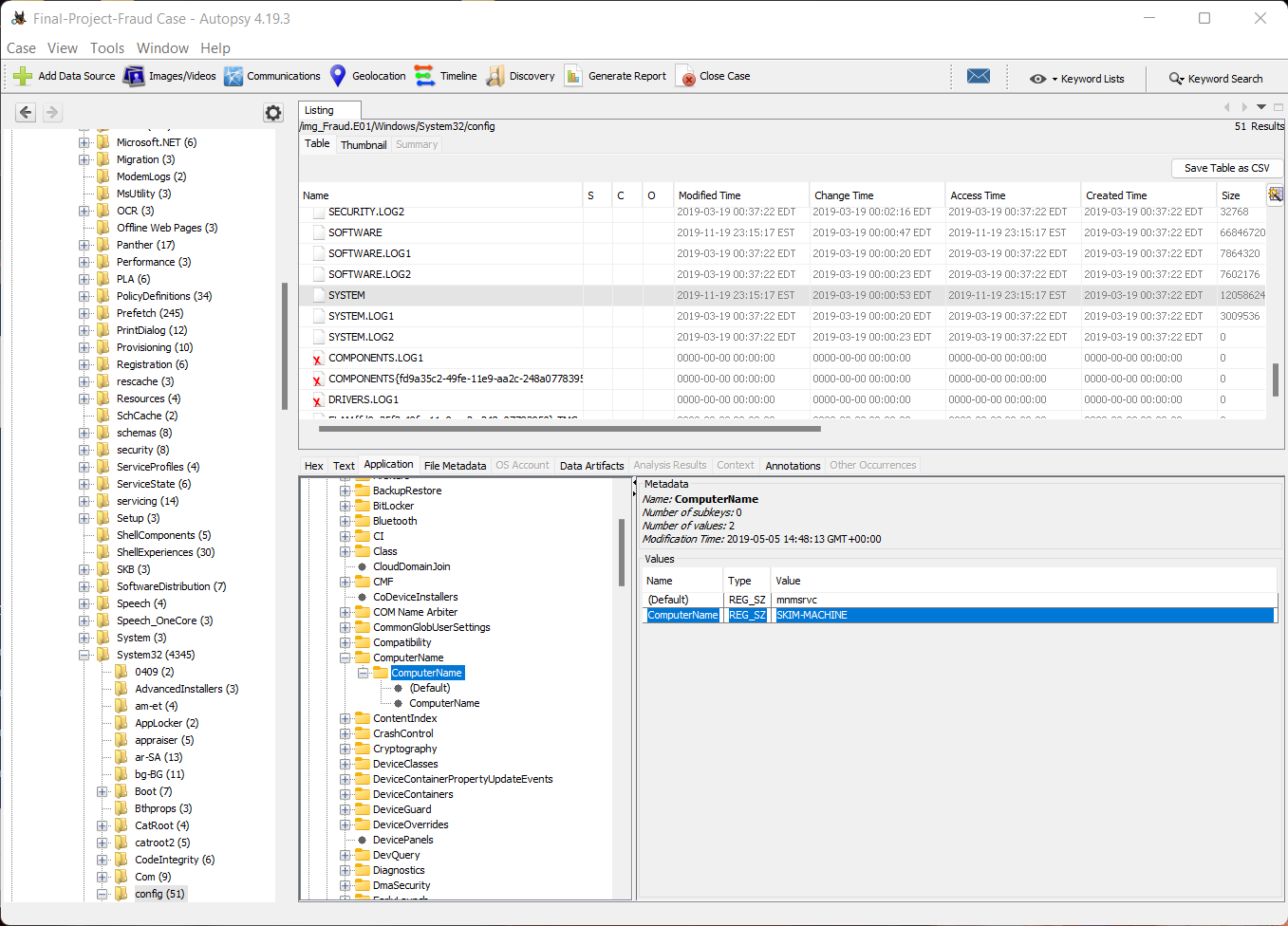
* **Registered organization: Five-star Operation**

**File metadata:** img\_Fraud.E01/Windows/System32/config/SOFTWARE/ **Registered organization:**

**MD5 hashes for SOFTWARE registry file for the whole information:**

****

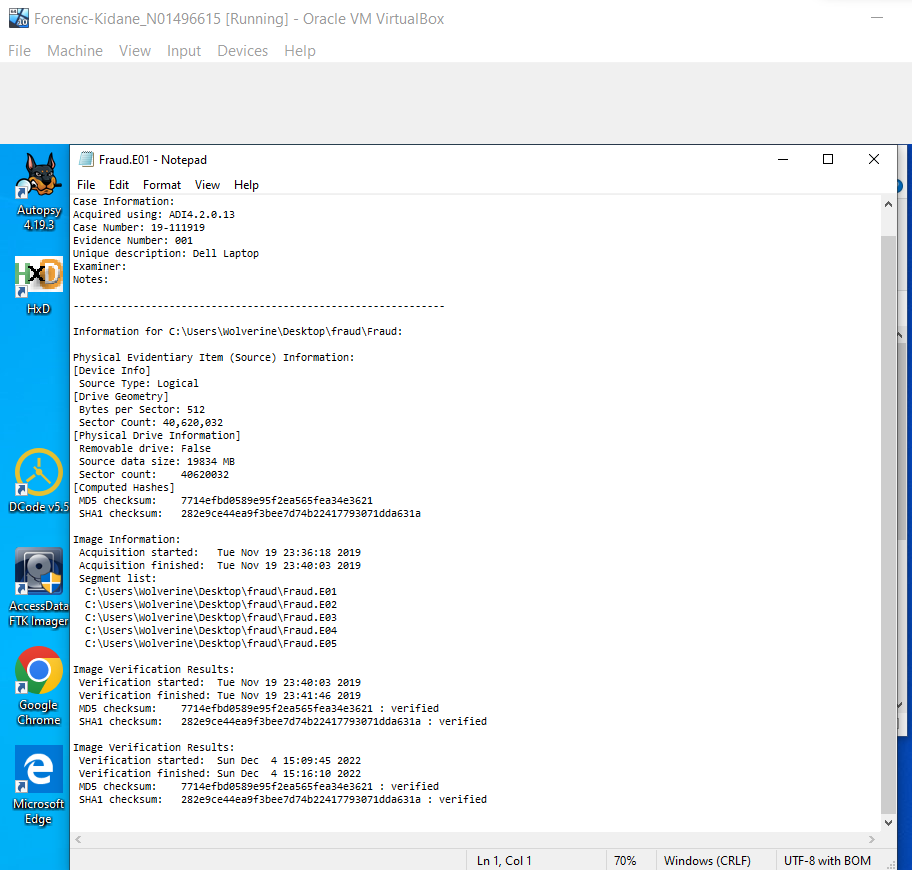
**File metadata:** img\_Fraud.E01/Windows/System32/config/SOFTWARE

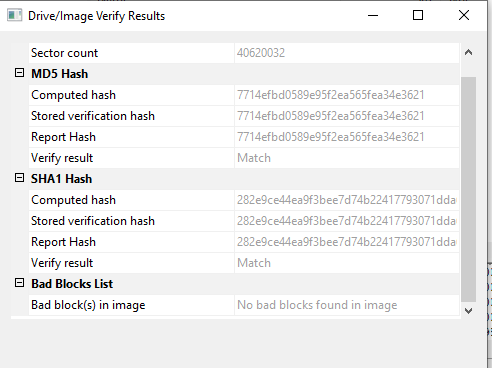
****

*Screenshots 2: pictures showing the windows version, owner and registered organization.*

### Digital forensic hash Both a hash and verification hash for the digital forensic image

* **Digital forensic hash for Both a hash and verification hash for the digital forensic image**

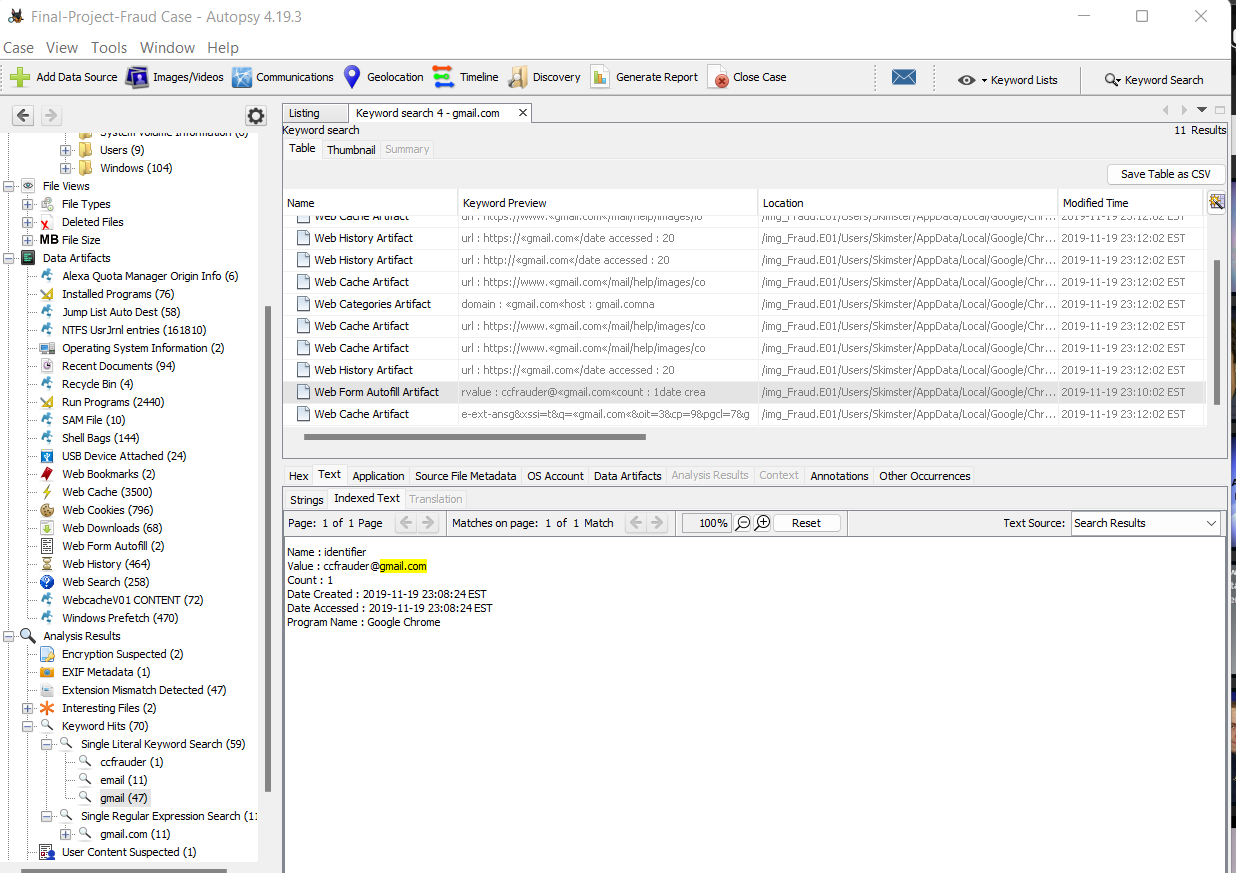


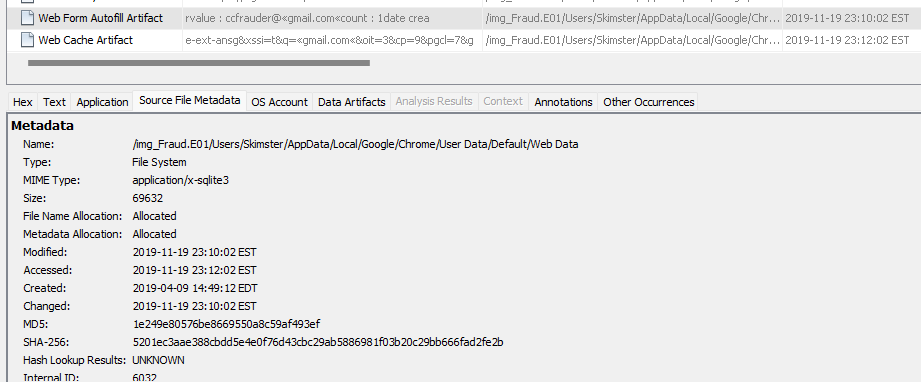


*Screenshots 3&4: pictures showing digital forensic hash for Both a hash and verification hash for the digital forensic image using Ftk Imager.*

### Email address used by suspect

* **Email address used by suspect:** [**ccfrauder@gmail.com**](mailto:ccfrauder@gmail.com)

****

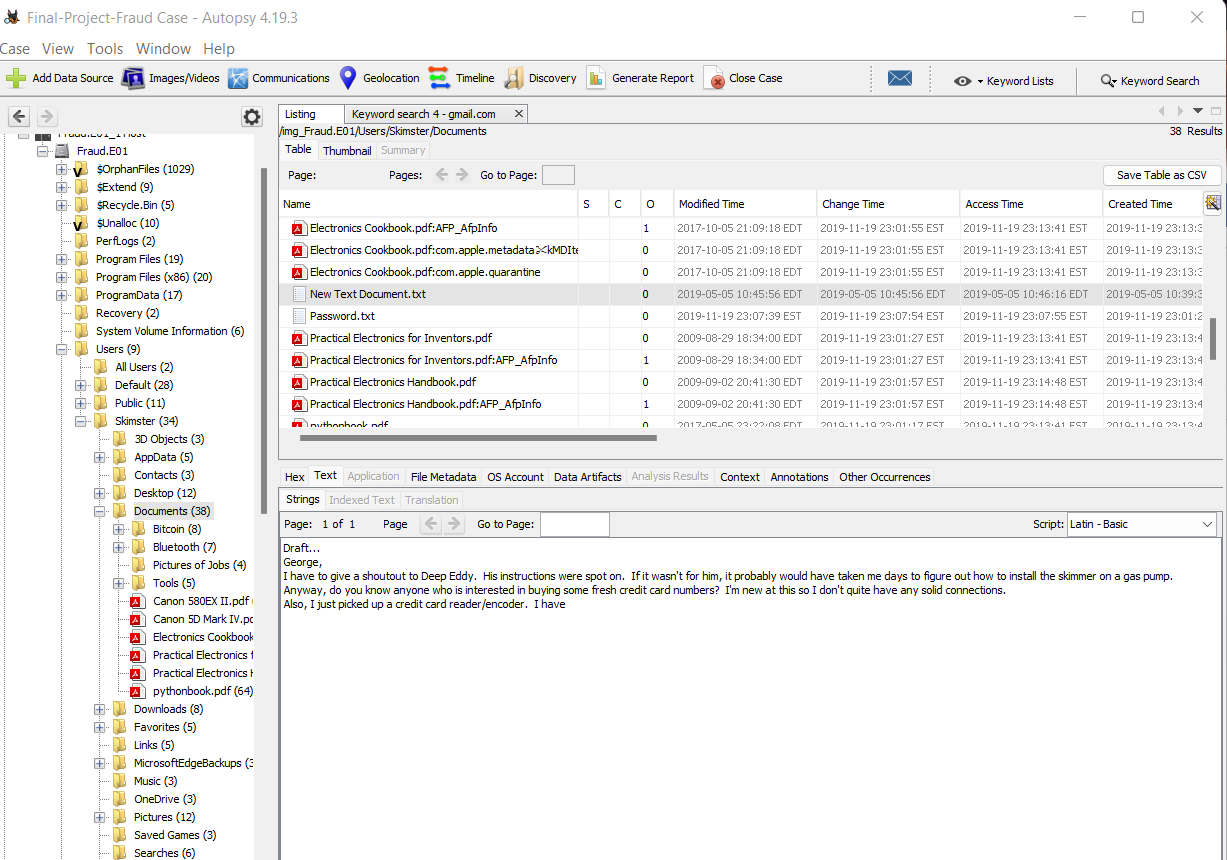
****

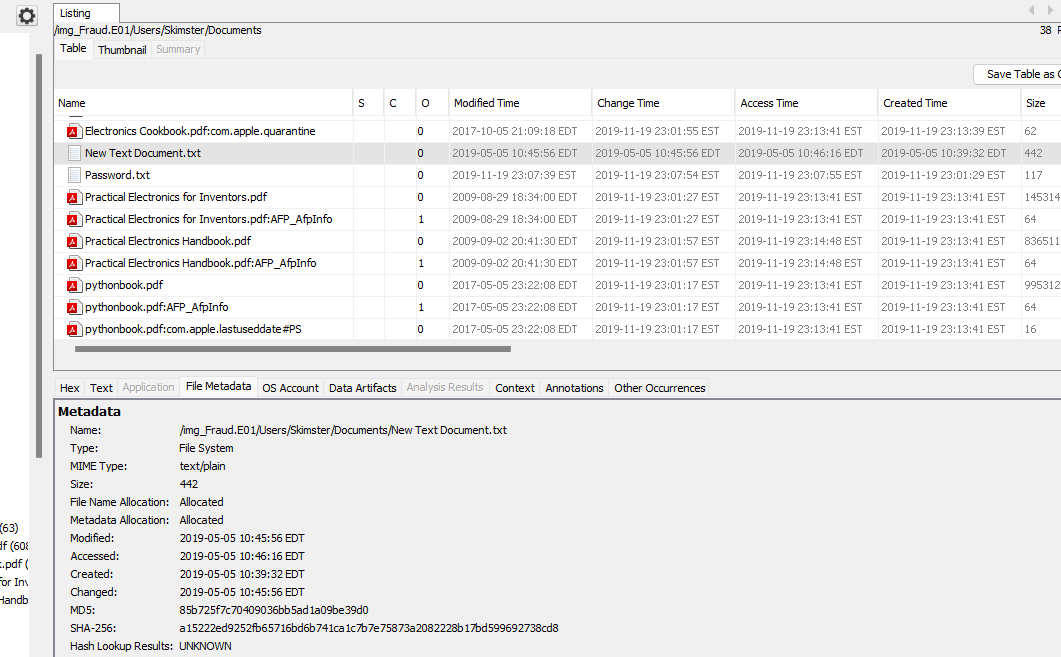
*Screenshots 5: pictures showing Email address used by suspect and source file metadata that include both hash.*

### Name of person(s) to whom Frauder may have communicated

* **Name of person(s) to whom Frauder may have communicated.**

According to a text document found on the suspect's computer, the suspect was in contact with **George**.

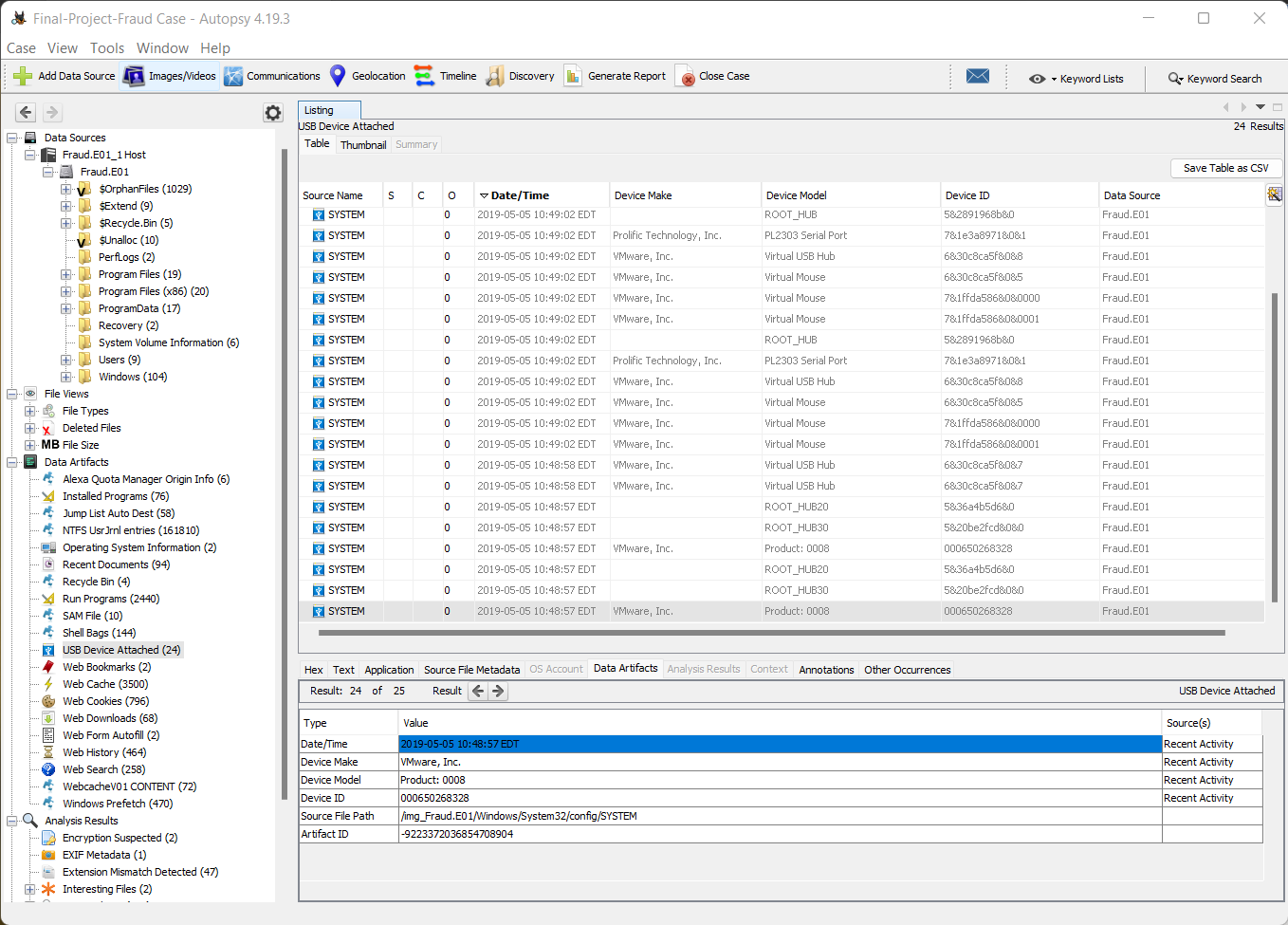


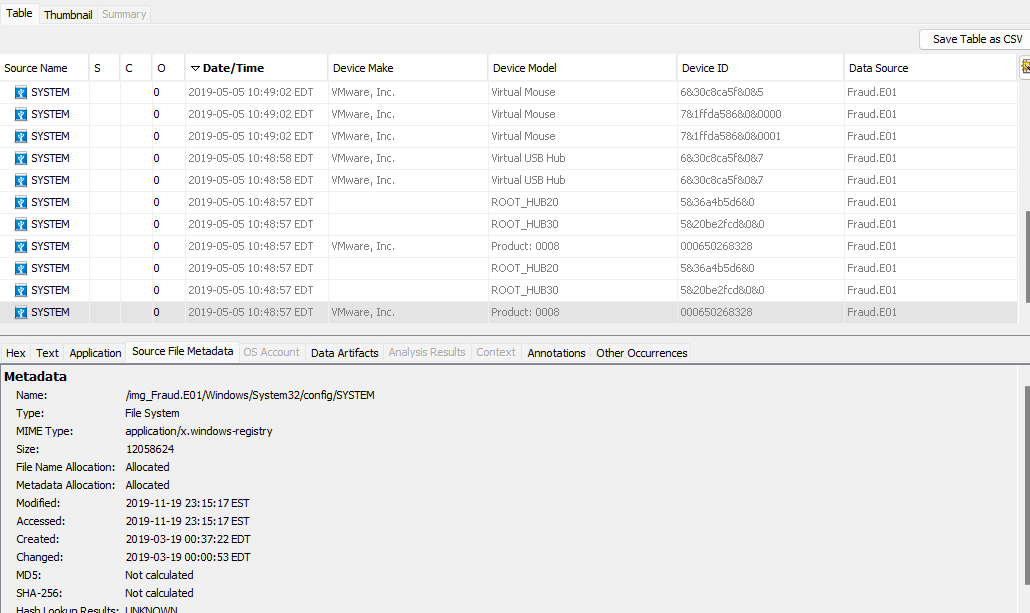


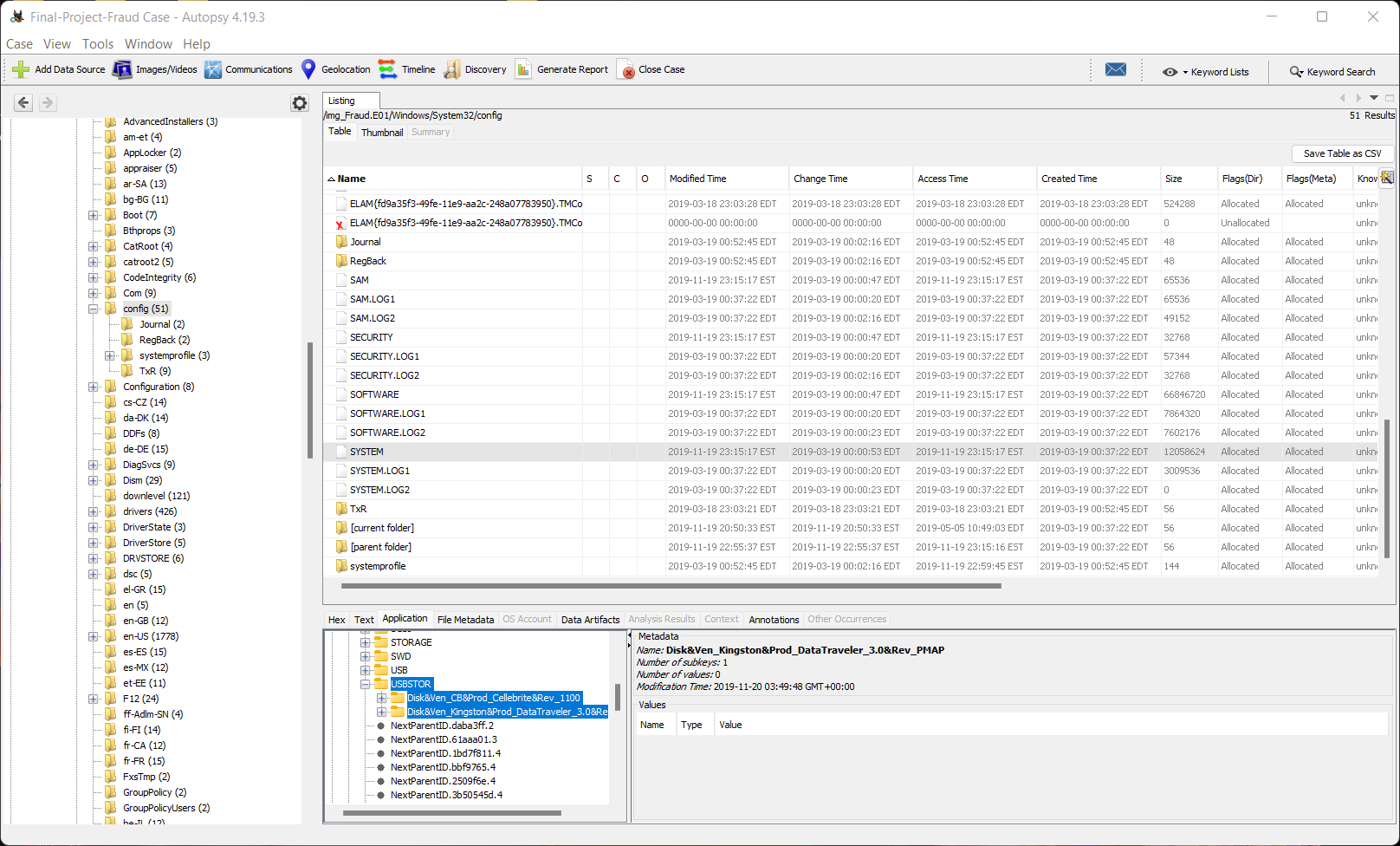
*Screenshots 6:* *pictures showing the source metadata for the document, the name of the person who communicated with the suspect, and the content of the communications.*

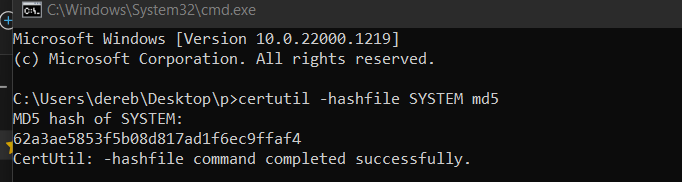
### Information on USB devices attached

On 2019-05-05, a USB device with the manufacturer "VMware, Inc." was attached, and on 2019-11-19, two USB devices with the manufacturer "A-DATA Technology co, ltd." were attached. Kingston Technology was also included. The last connected USB device is VMware, inc model and highlighted below.







****

*Screenshots 7: pictures showing Information on USB devices attached and metadata for attached USB Device in system file.*

# 

# Evidence/Relevant Findings

1 In the recycle bin, two files were discovered. One is a text file named c2.txt that was found on a user's desktop and contains the credit card information of twenty different persons. and also, one software program called Missiri were found in the recycle bin. full-screen image displaying the files and their metadata found in click too see *Fig*ure 1 .

2 For the search term "Tor," several online histories were found in Google Chrome's history, and one program was discovered on Skimster's desktop. On 2019-11-19, user Skimster conducted those searches on the same day. for additional evidence, see (Figure 2)shows an image of the file's metadata.

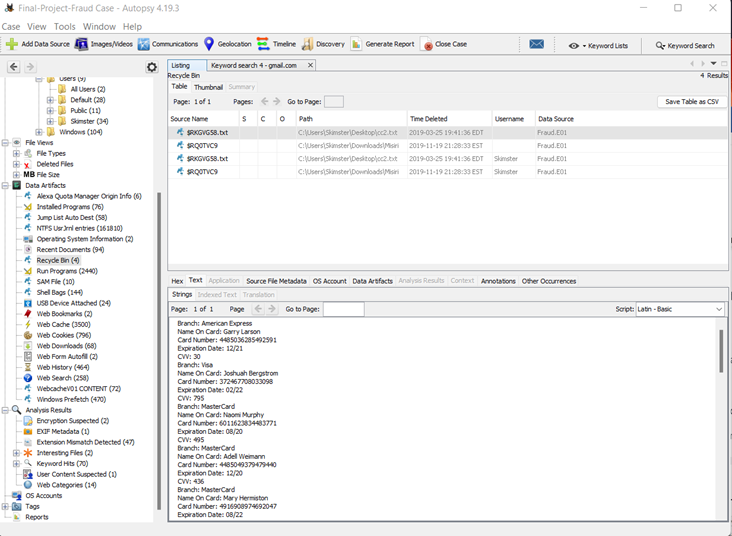
3 Two images were found in a folder called "pictures of Jobs in user documents," and they included an image of a reader with an SD card attached and an image of a guy using his card at a gas pump. also, for visual proof Image of the file and its metadata may be found in *Figure 3.*

4 One folder were found on Desktop named “msr605” containing two folders named” Mac software” and “windows software” containing a setup .and “read me.txt” document containing step-by-step how to install the software and how to read data from swiped card. for full detail text file and its metadata shown on *Figure 4.*

5 New document.txt" file created on 2019-05-05 were found in user Skimster documents containing a text communication with George. Asking that how to install skimmer on gas pump and mentioning that he picked the credit card reader/encoder. See the full communication on *Figure 5.*

6 On 2019-05-05, a USB device with the manufacturer "VMware, Inc." was attached, and on 2019-11-19, two USB devices with the manufacturer "A-DATA Technology co, ltd." were attached. Kingston Technology was also included. The last connected USB device is VMware, inc model and see highlighted on (*Figure 6).*

# Supporting Details



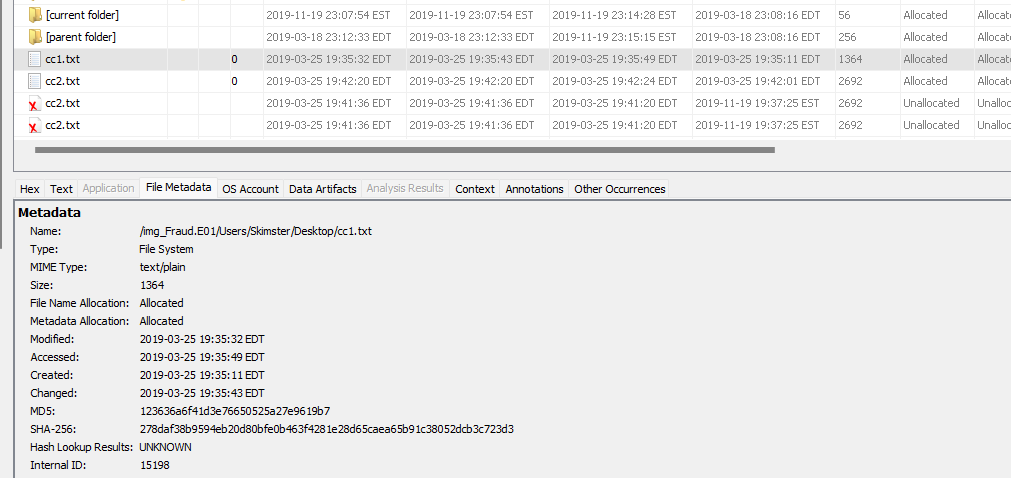
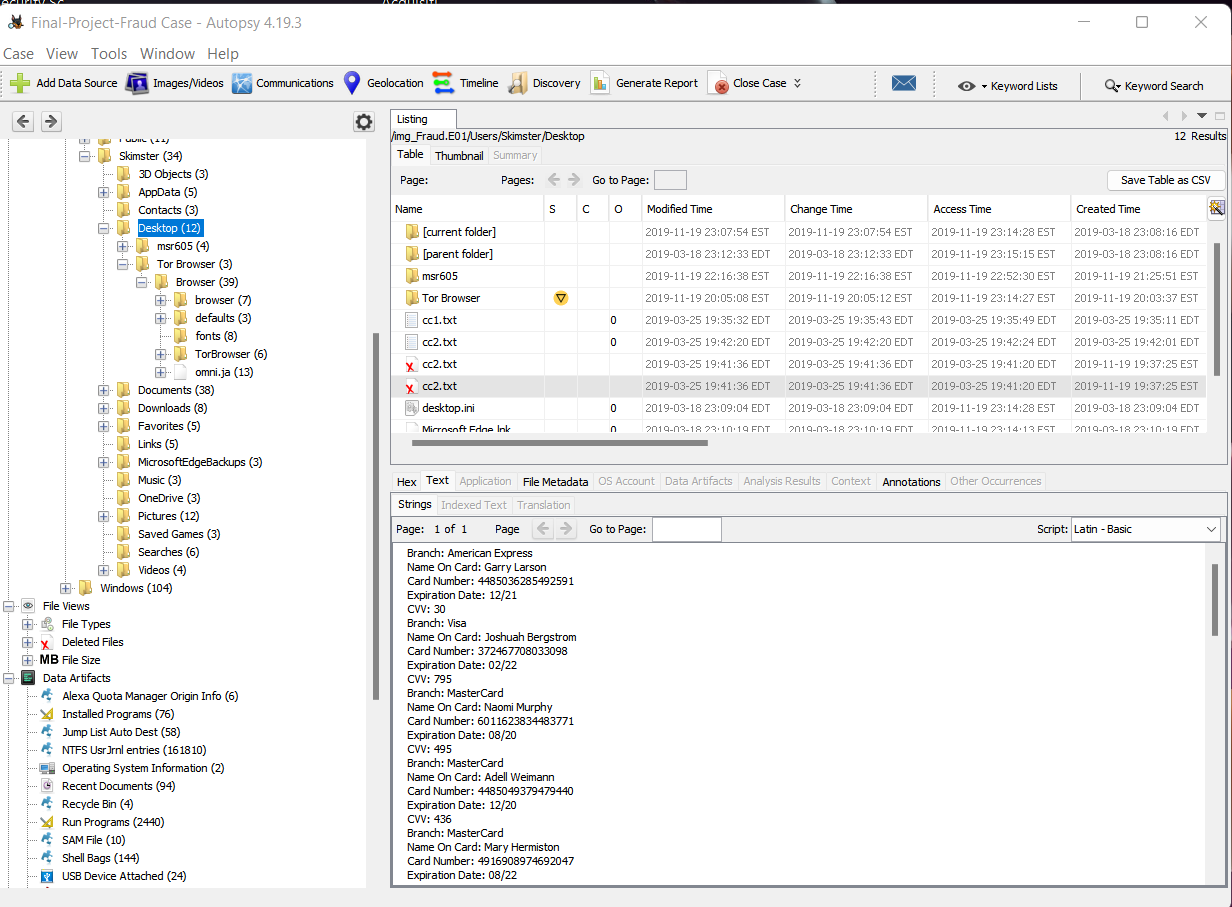
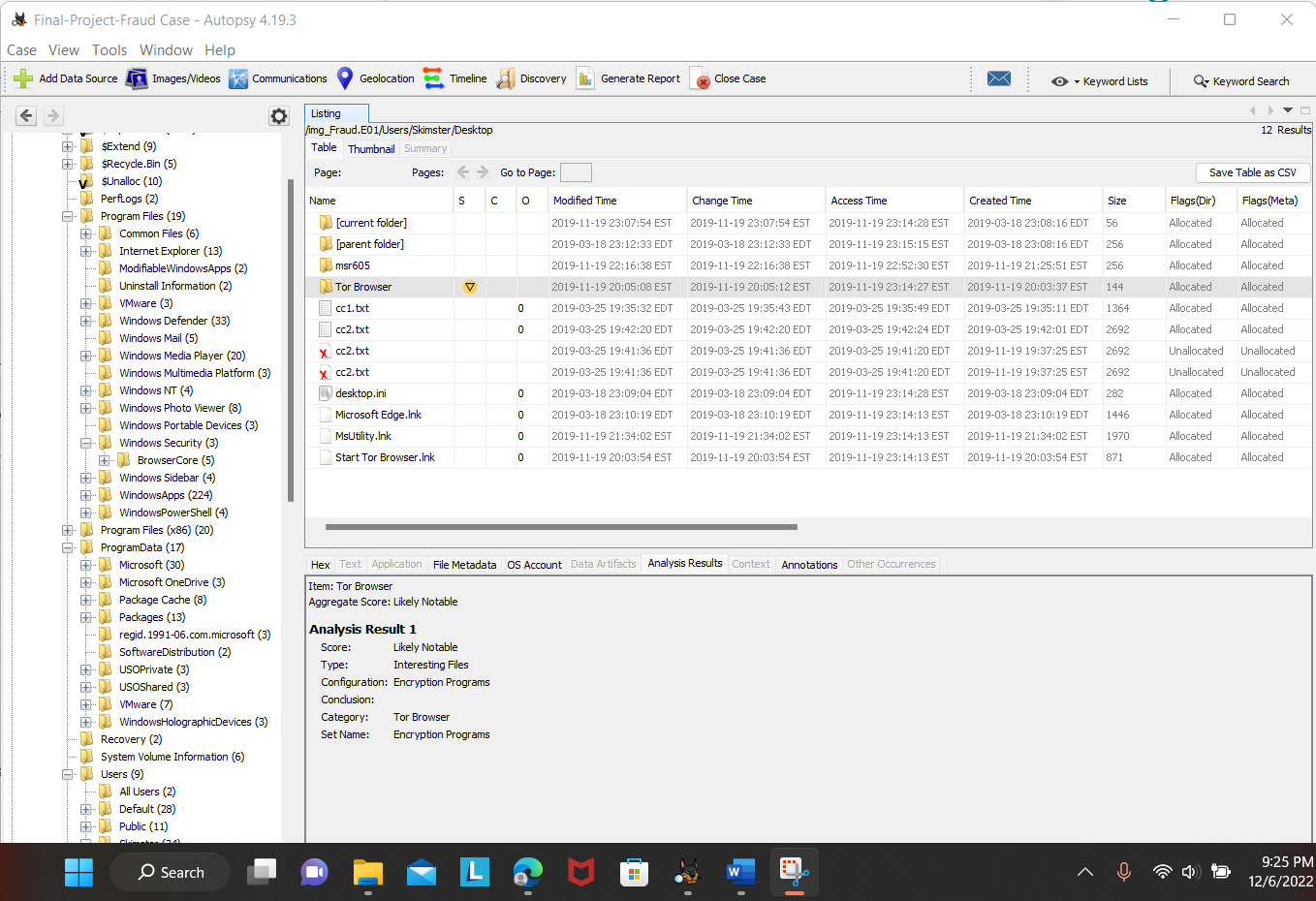
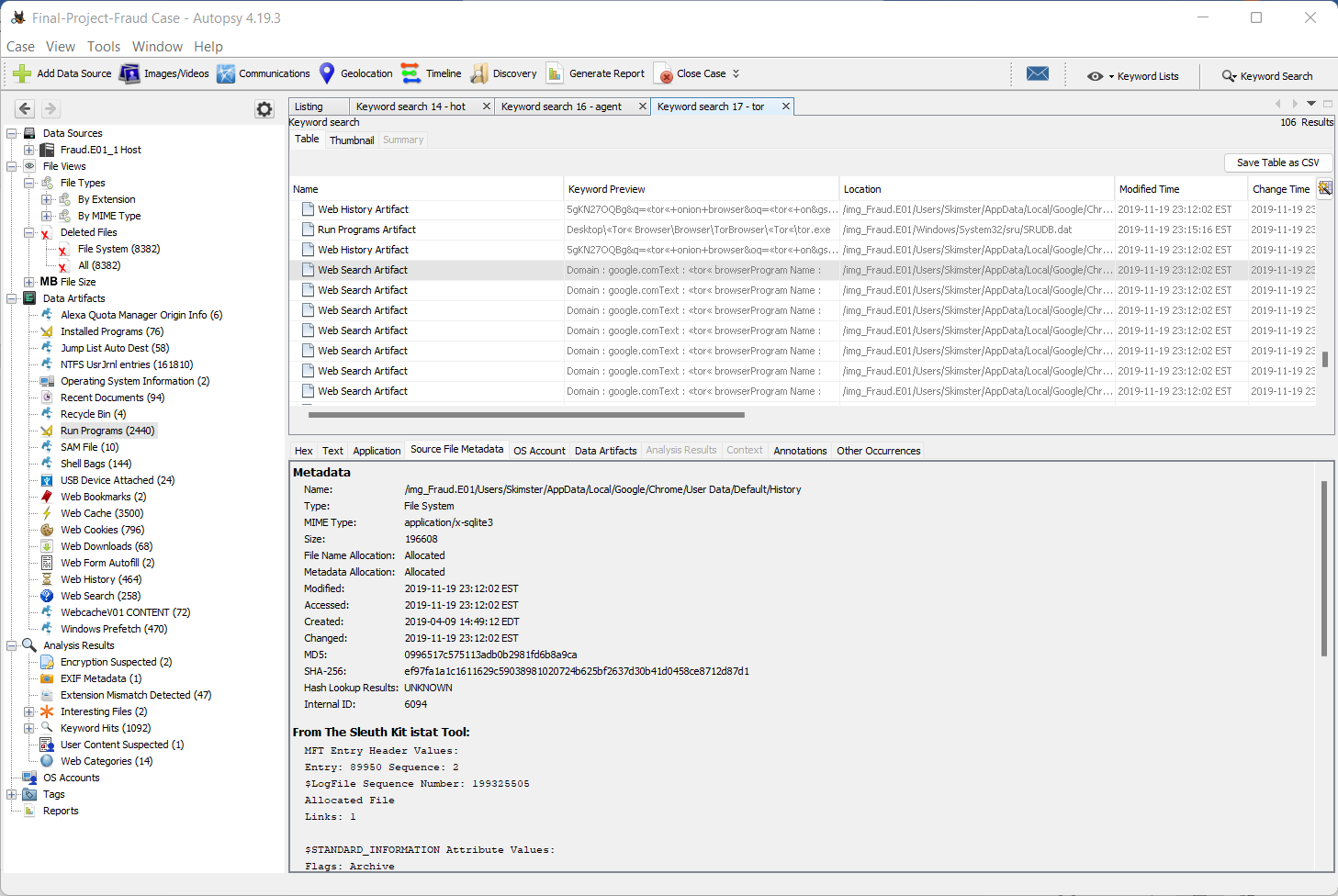


Figure 1 a screenshot of the same text file, which contained up to twenty people's credit card information, being discovered in two different locations—one in the recycle bin and the other on the user's desktop. Additionally, "misiri," a deleted software configuration, hashes and records metadata about every file found.



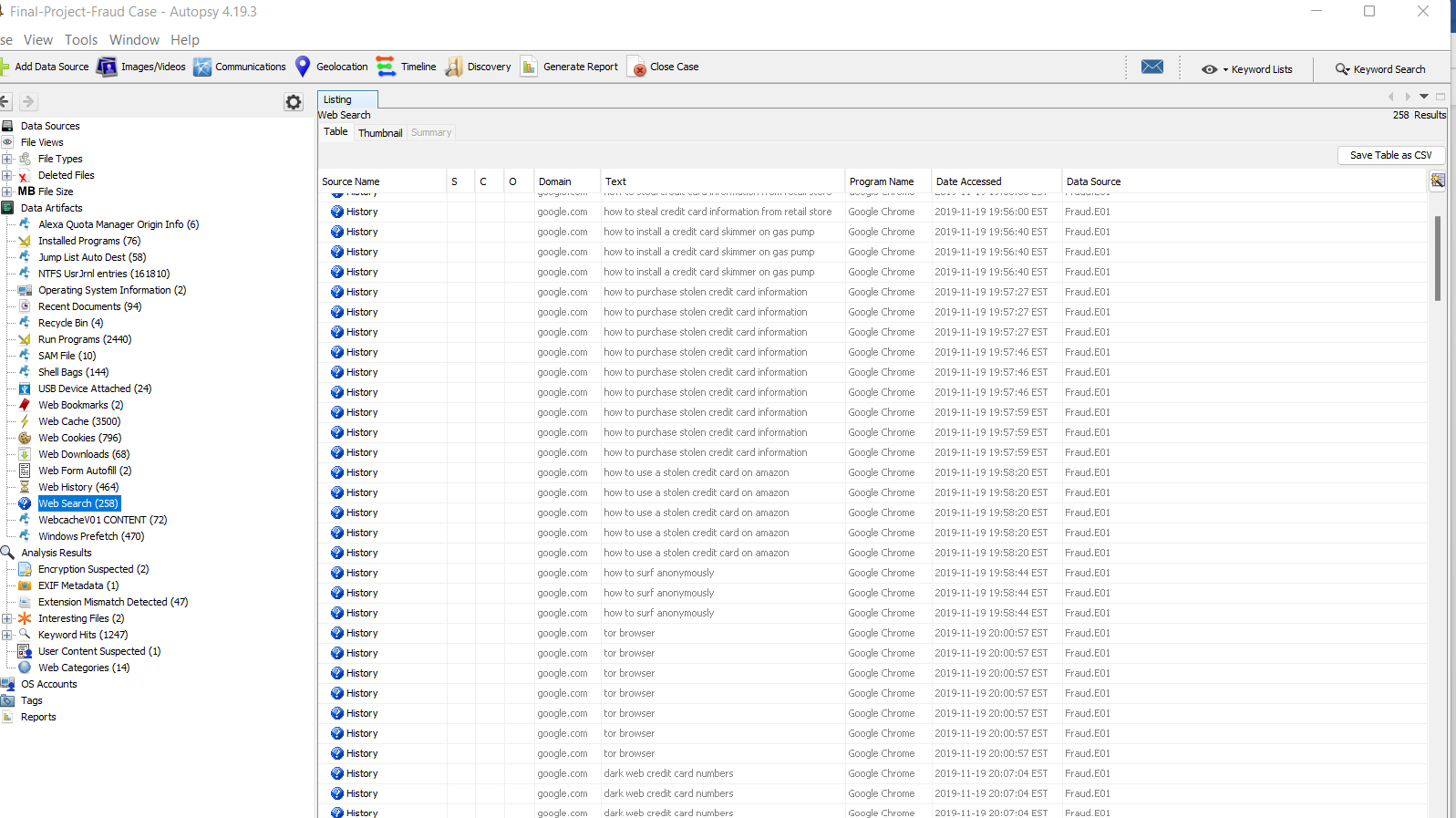
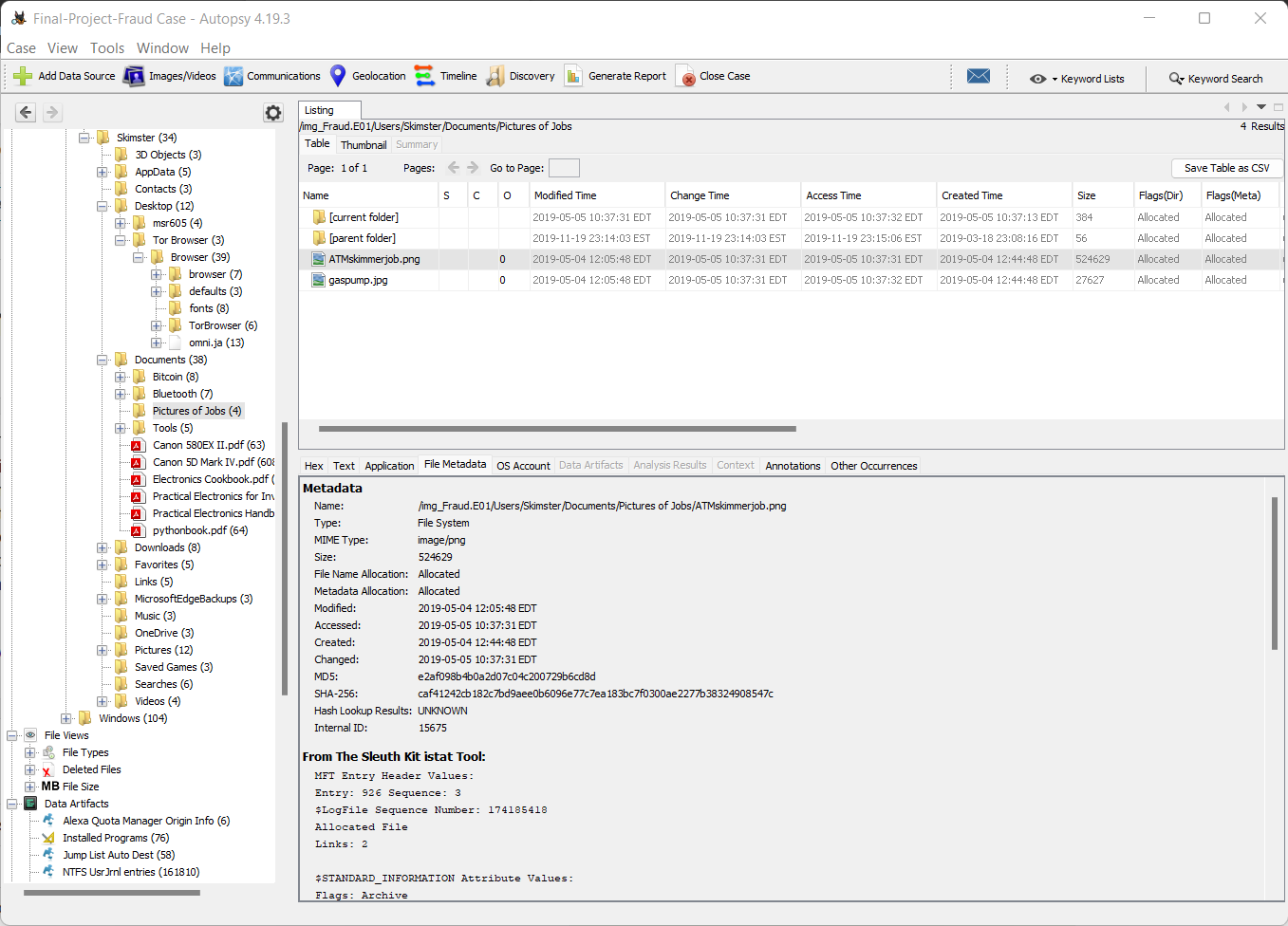
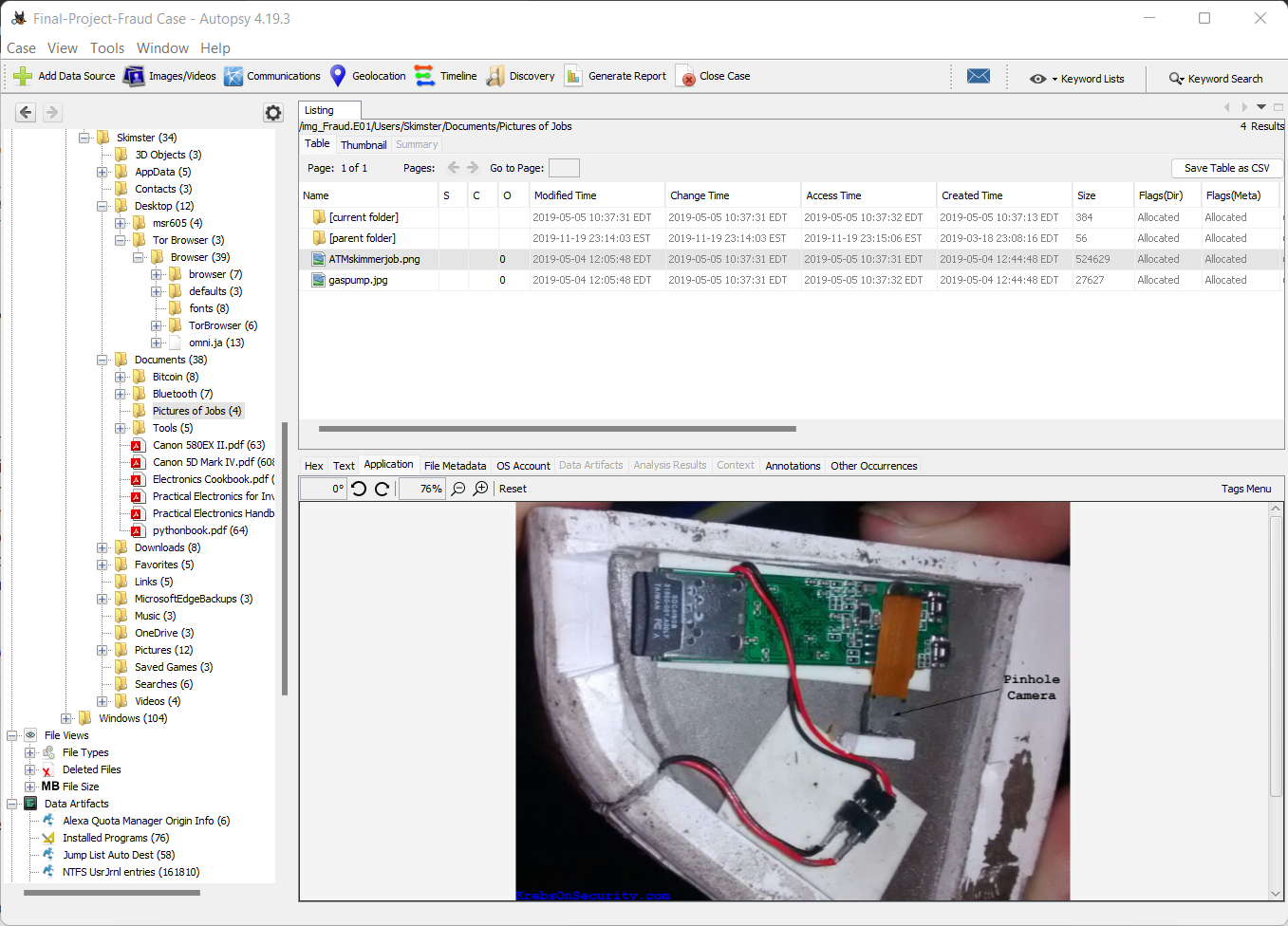


Figure 2 internet history for tor browser, hash and metadata of the file



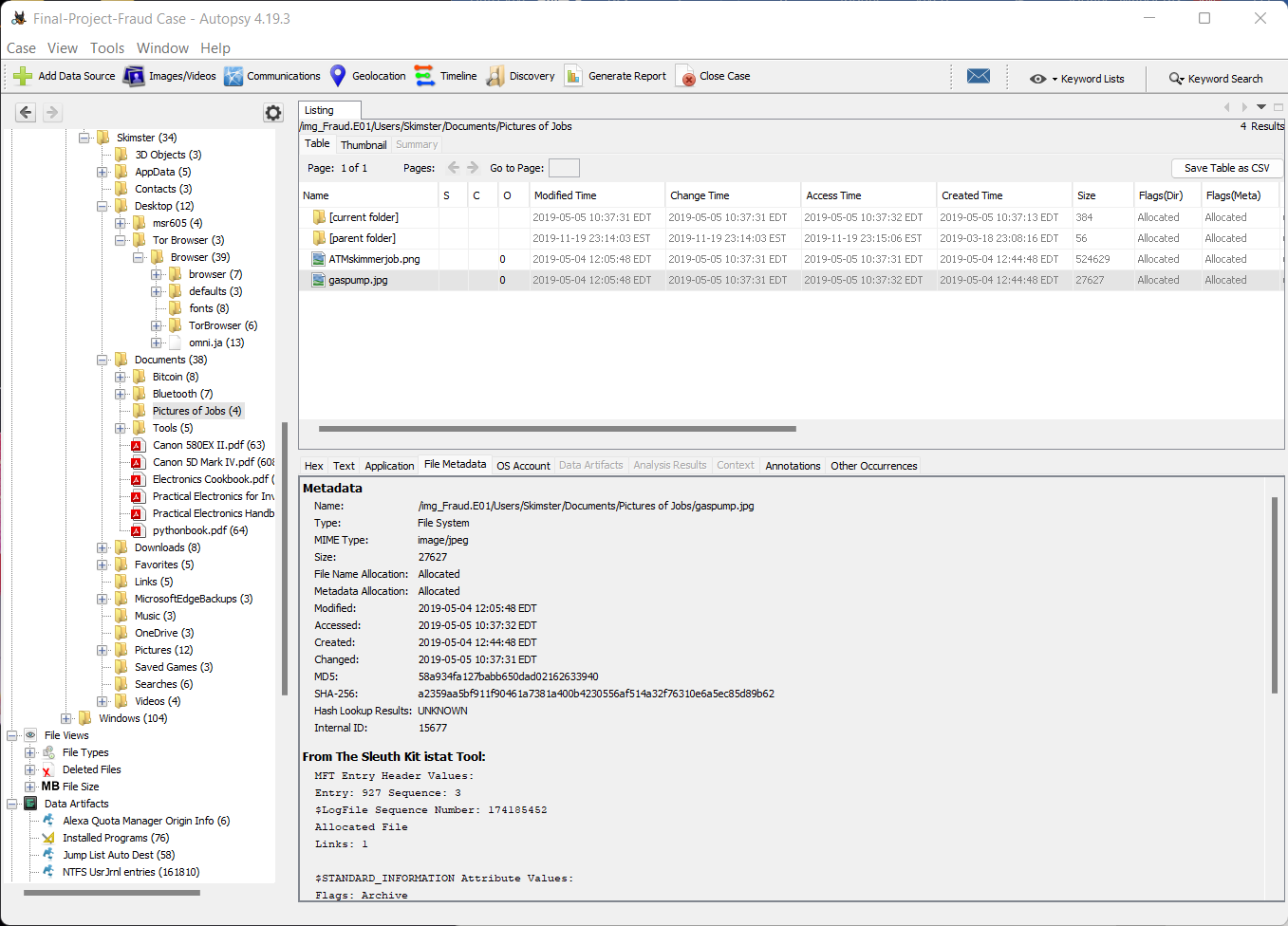
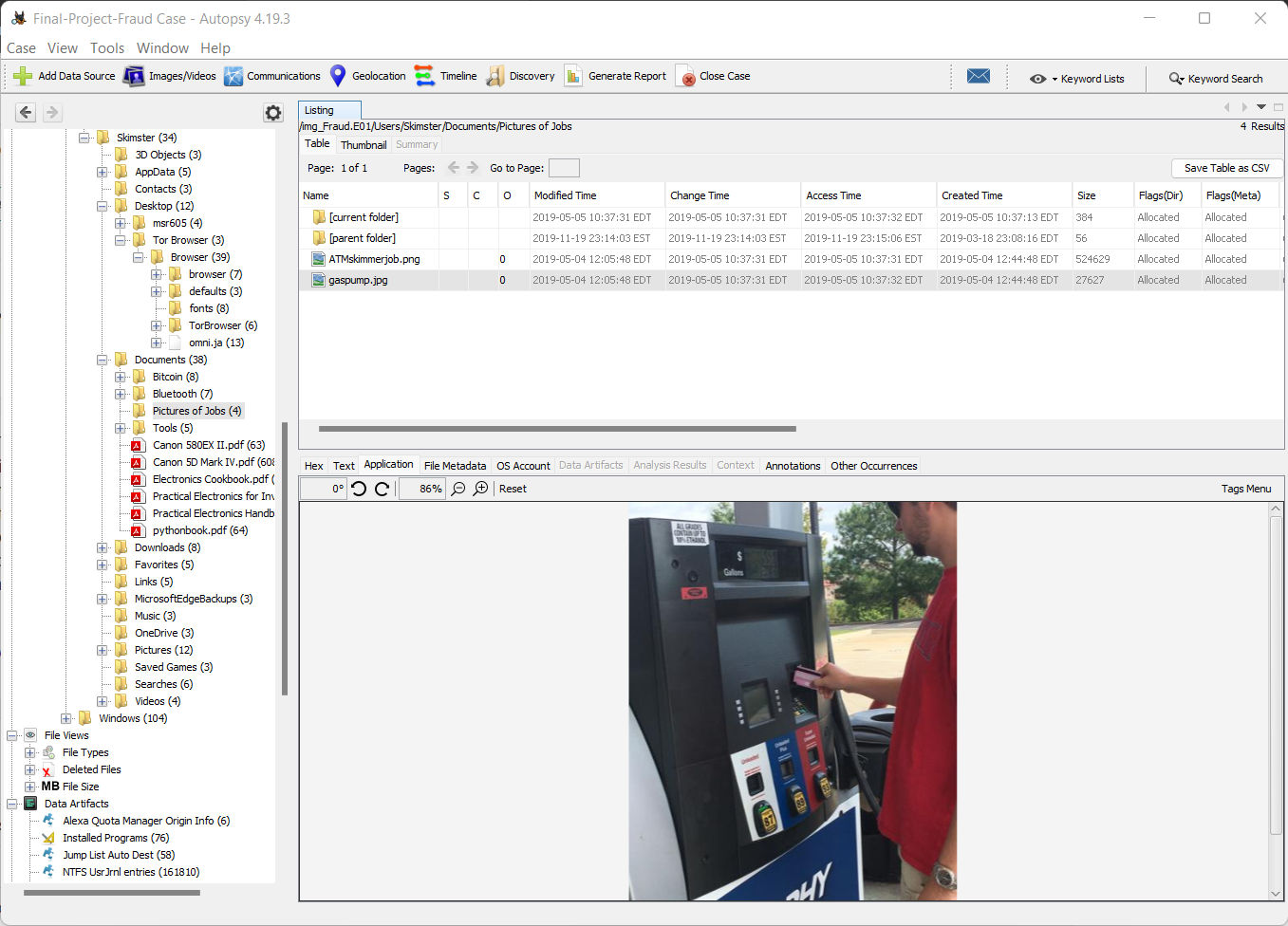
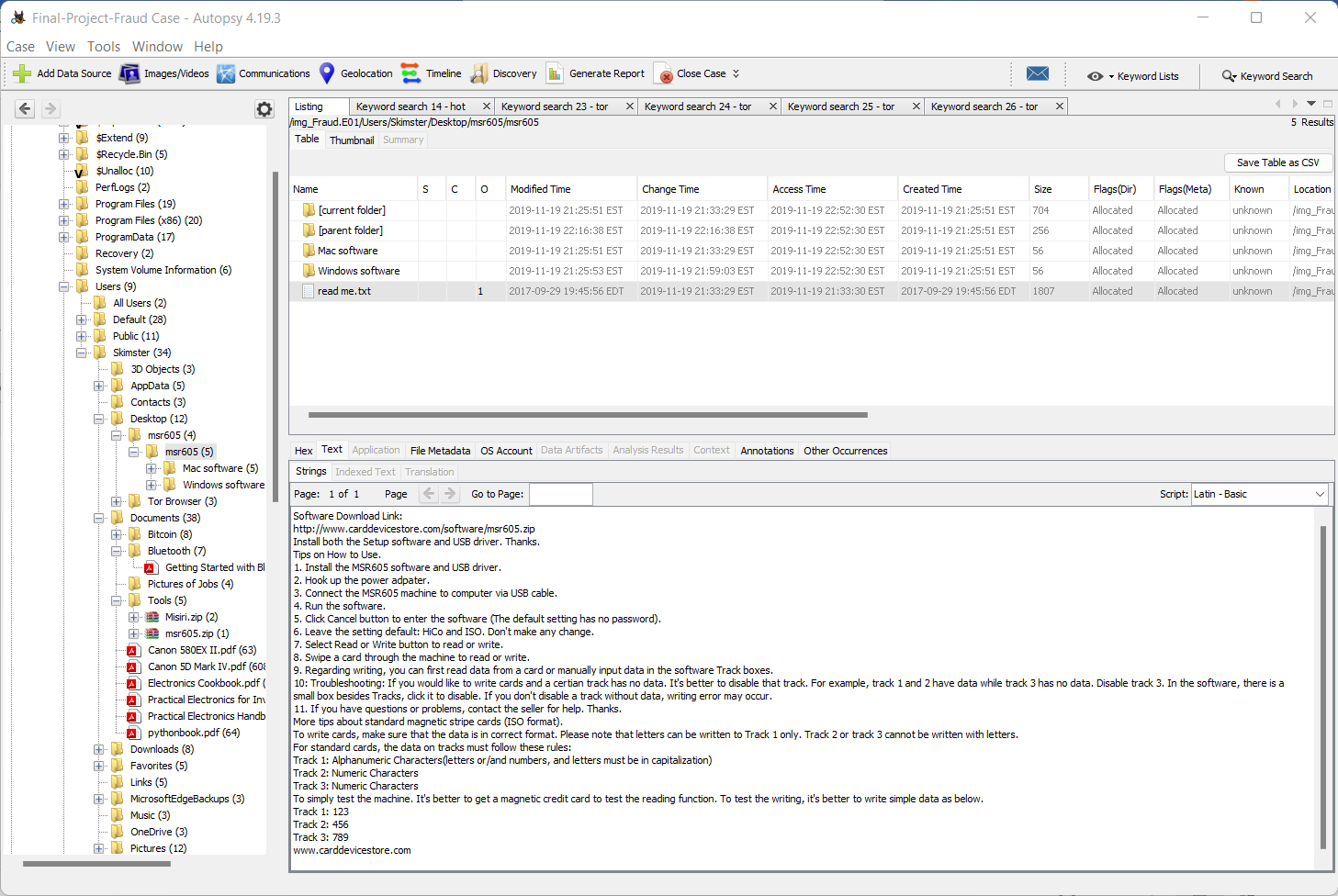


Figure 3 *picture showing card reader and person who is sliding credit card, hash and metadata for each file.*



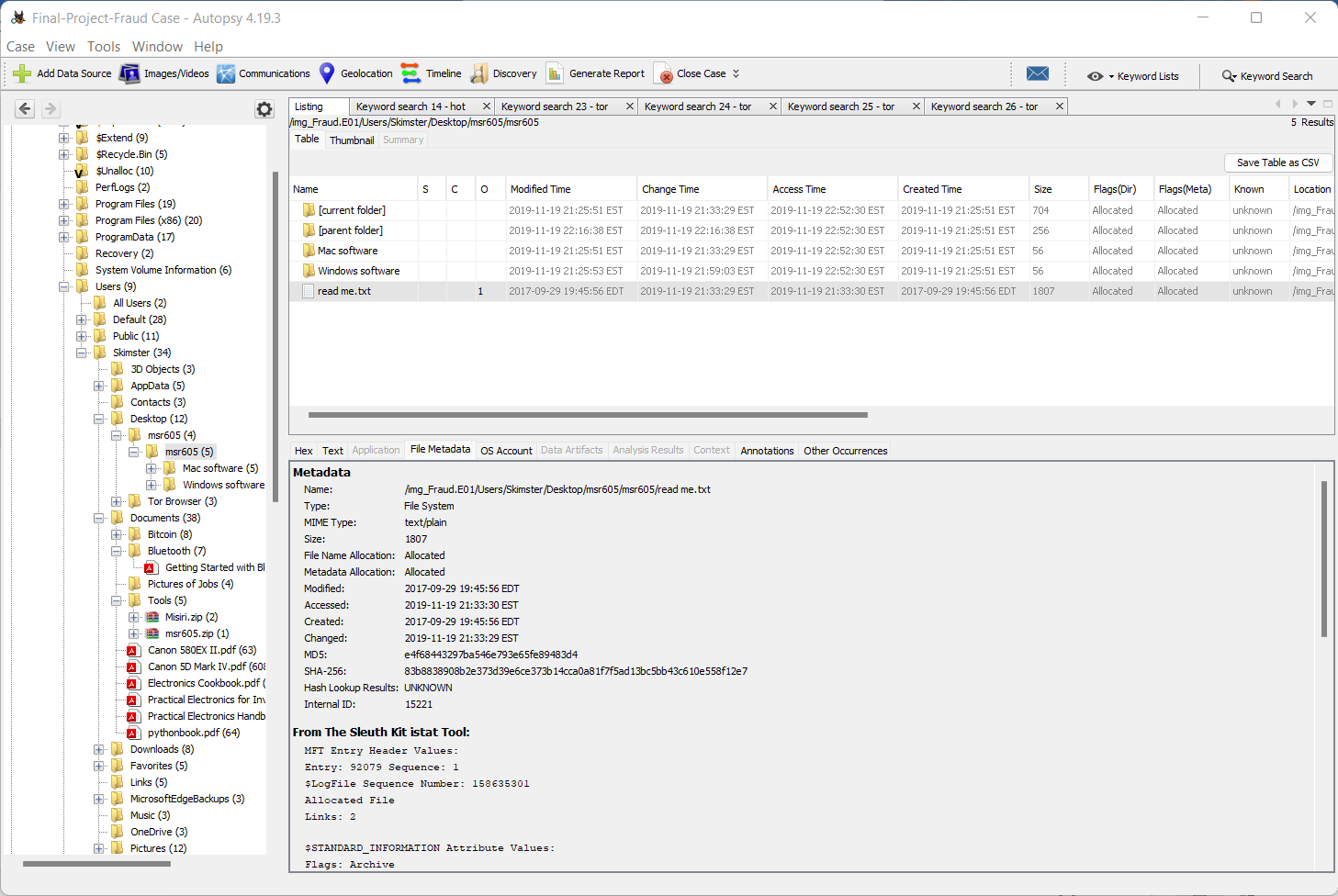
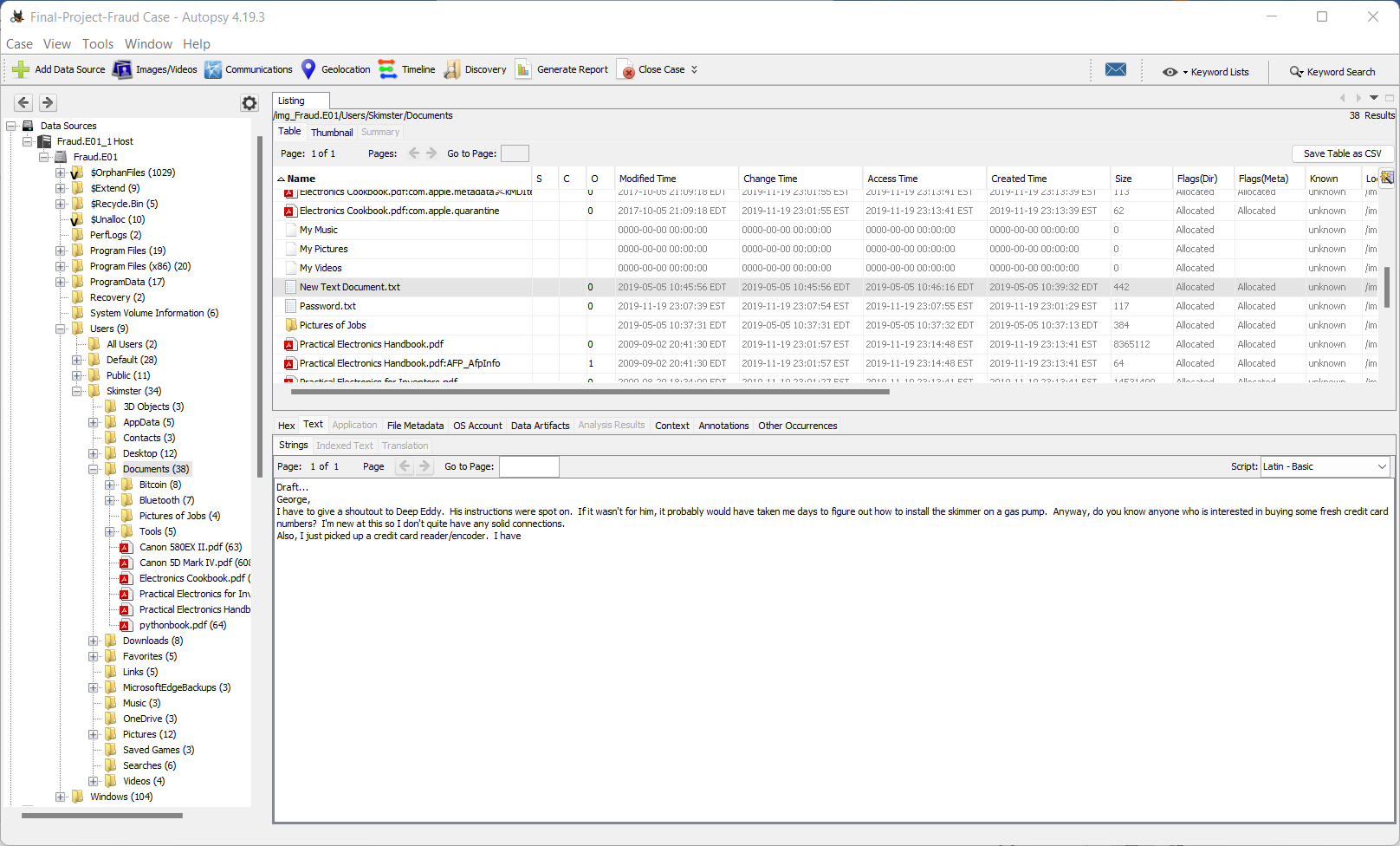


Figure 4 picture showing the software” msr605” that suspect used and content of “read me.txt” file including hash of the file and its meta data.



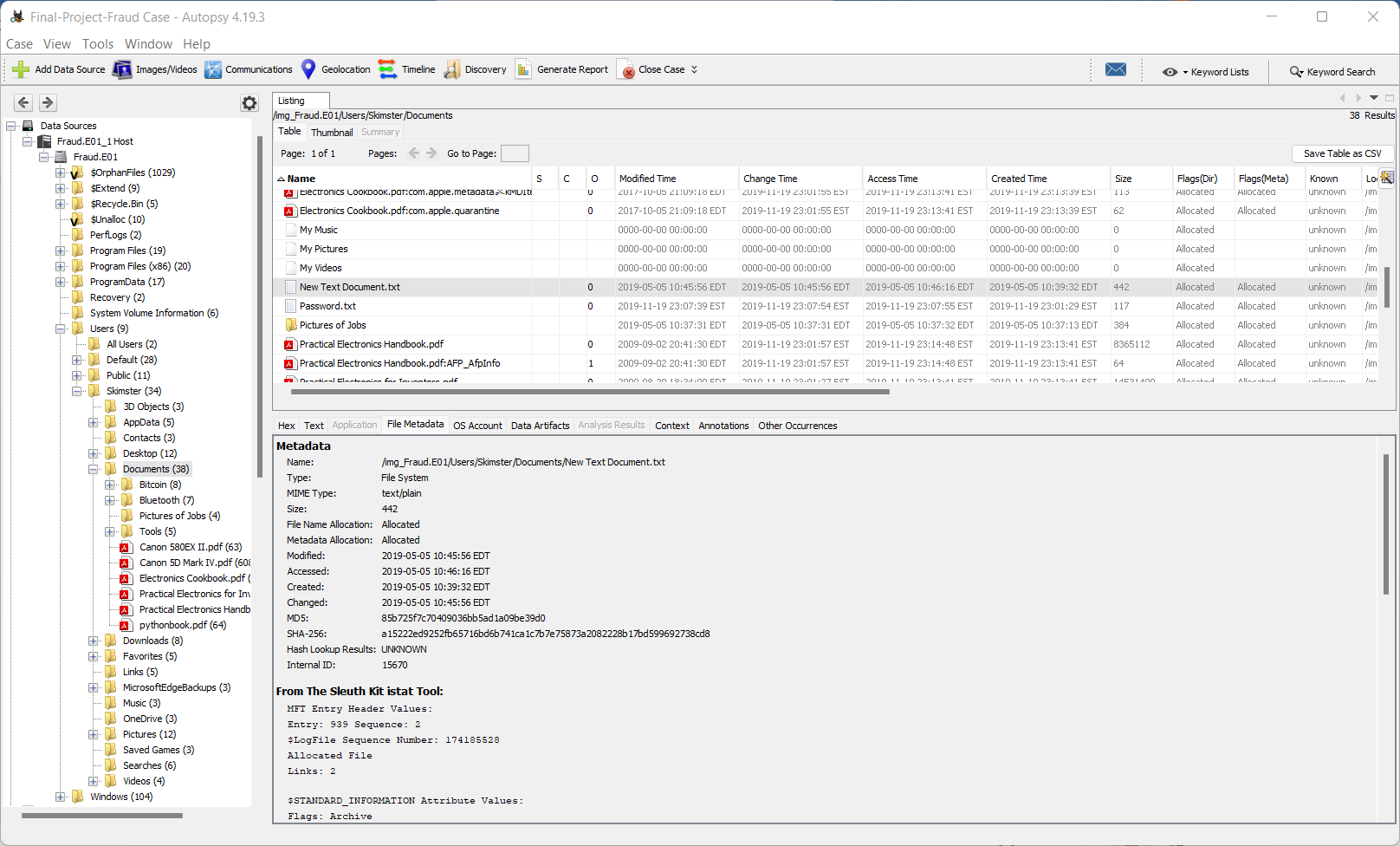
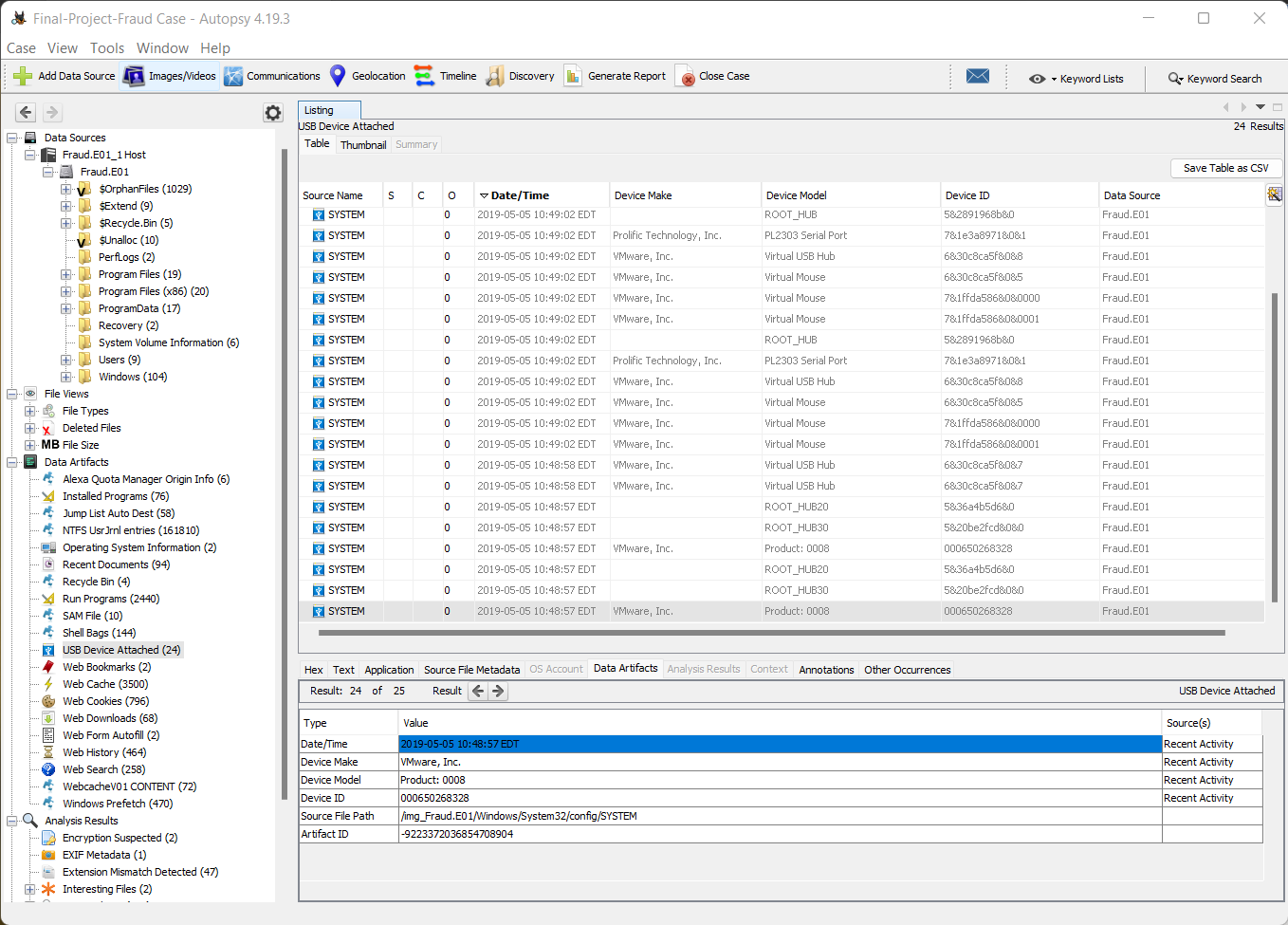
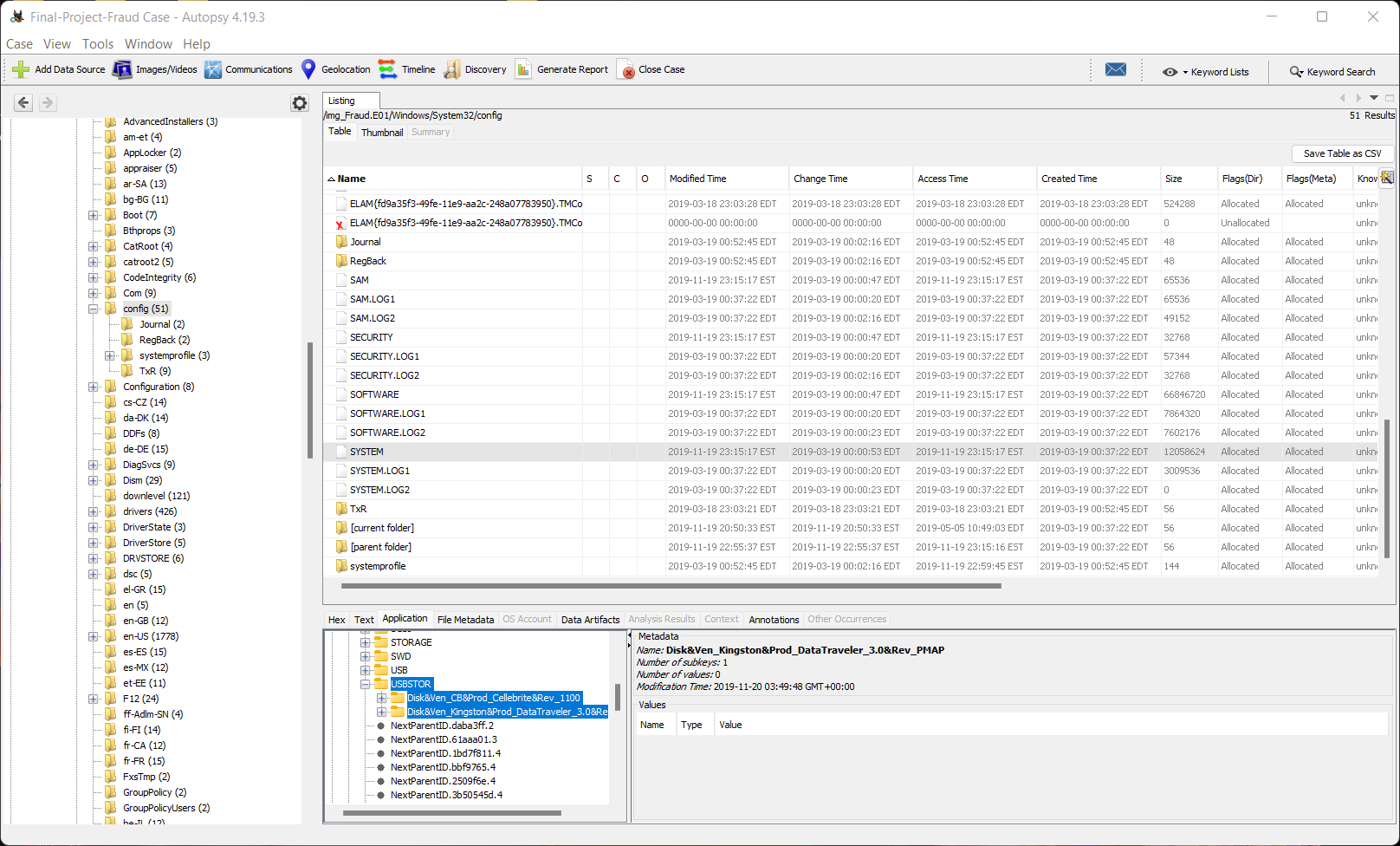
**

Figure 5 picture showing the text file called “New document.txt” that shows the person(George)that suspect comunicated with and the body of comunication.





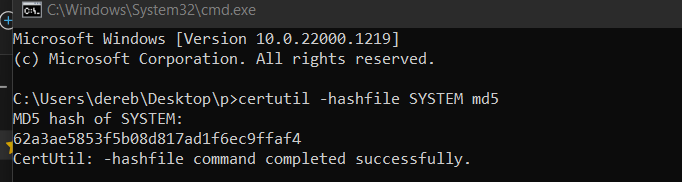
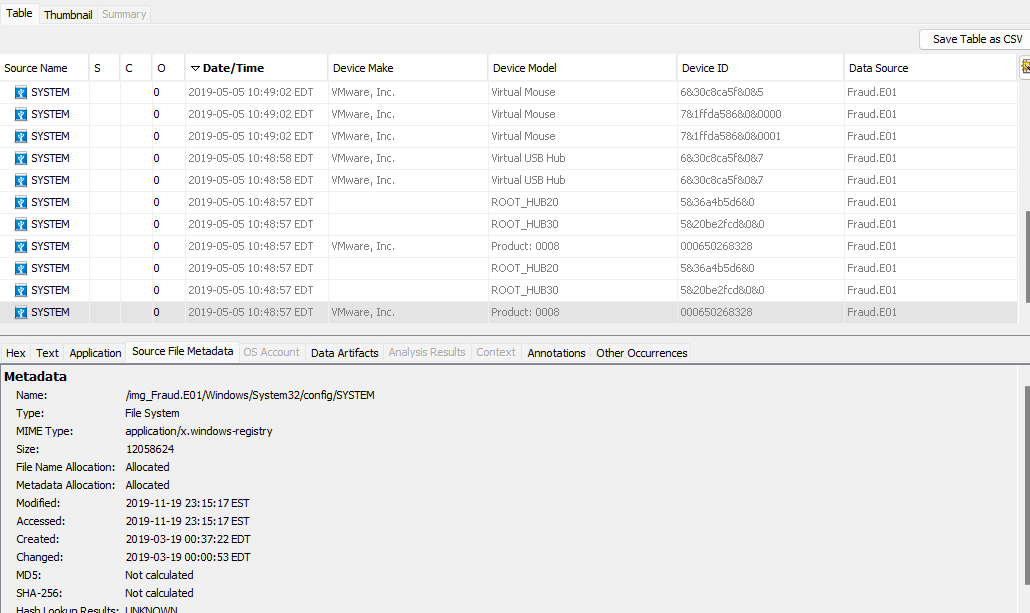
****

Figure 6 pictures showing Information on USB devices attached and metadata for attached USB Device in system file.

# Conclusion

According to information on a laptop found in the home of suspect Chris Frauder, it is called Skim-machine, and its registered owner also goes by the name cc Frauder and uses the email address "ccfrauder@gmail.com". I was able to confirm that the laptop relates to Chris Frauder, and while looking for additional information about the case, I discovered that Frauder used his computer to run some suspicious software and keep a record of the websites he visited. Examples include the search terms "how to steal credit card from retail store," "how to install credit card skimmer on gas pump," and other search terms on the Tor browser (*see Figure 2*).

The identical information is contained in a text file named "read me.txt" *(see Figure 4*) that can be located on the desktop in a folder called "msr60" that also contains the program setup for Windows and Mac. The text document describes how to install the setup, use the software to read from swiped cards, and other things. The fraudster also communicated with a person named George, asking for instructions on how to use the skimmer (*see Figure 5).* This prompted an investigation into a more serious case. While looking for an image file, I also found two crucial images in a document containing pictures of jobs. Image titled "ATM $skimmer and gas pump" (*Figure 3 for image*). The first image shows a card reader (skimmer machine) with an SD attached to it. The second image shows a person using a card reader at a gas pump.

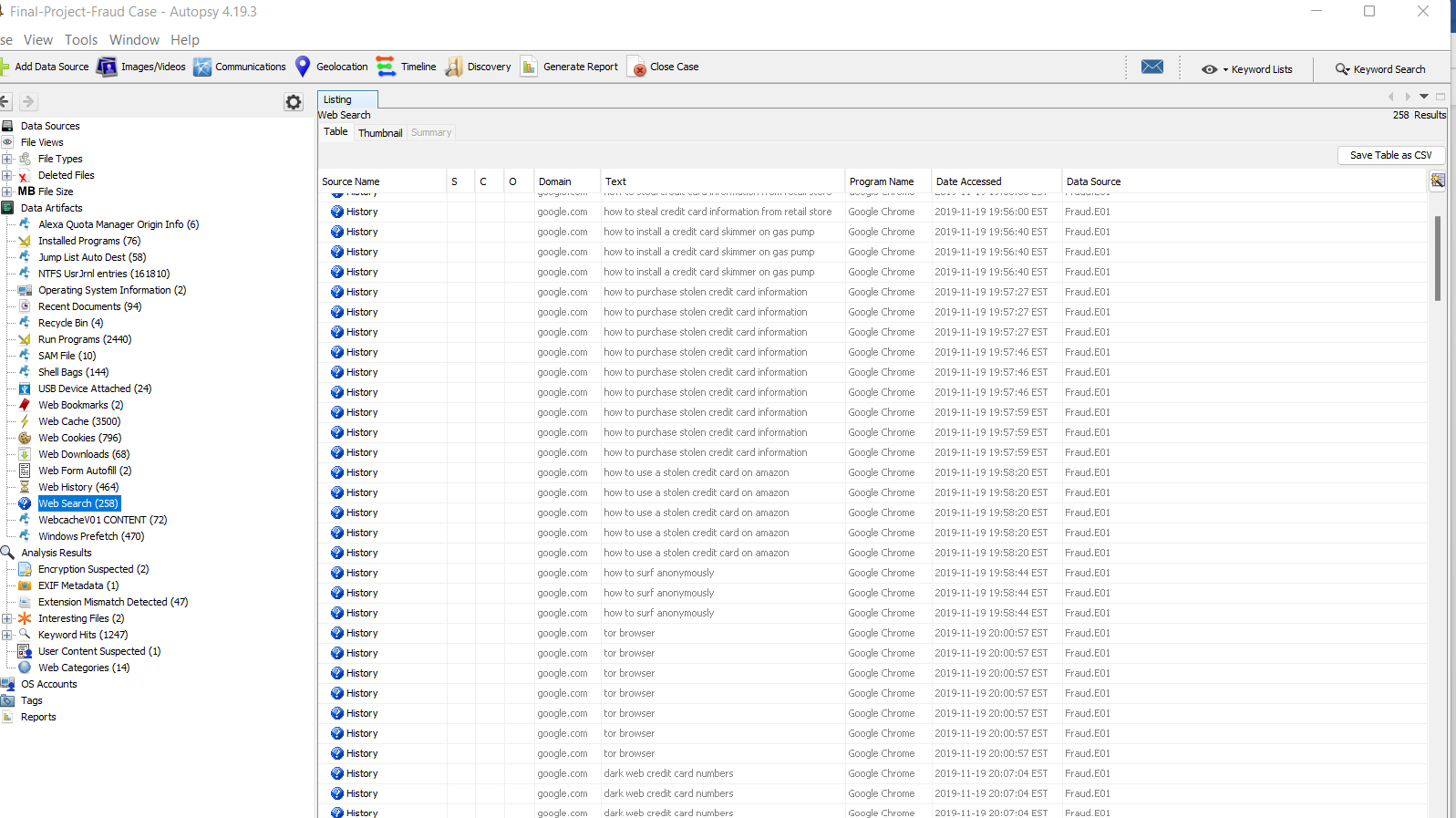
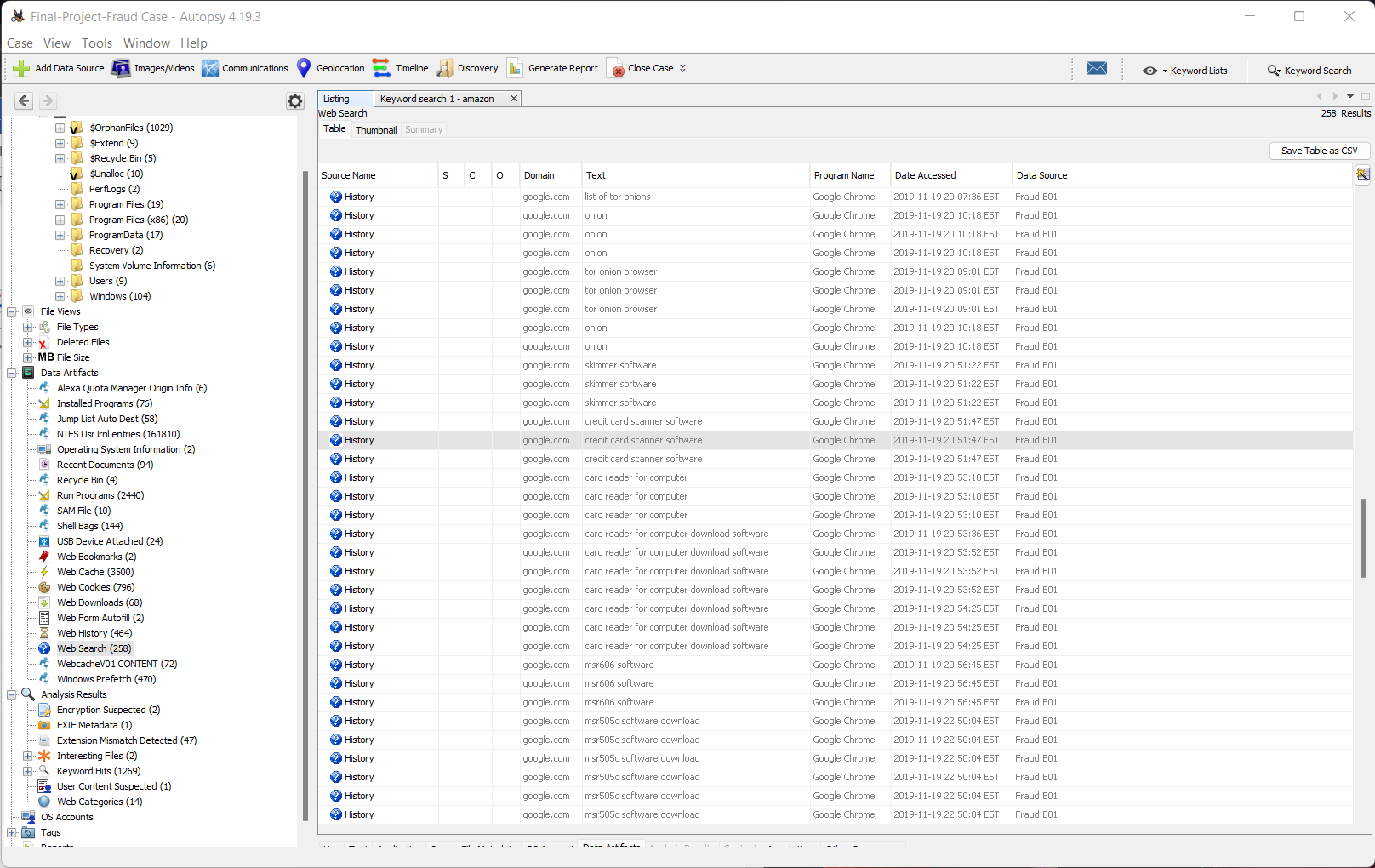
On user desktop the there was a text file called “cc2.txt” (see Figure 1) which contains twenty peoples whole credit card information. Same text file was found in recycling bin which was deleted by skimister.

In my opinion from those evidence, I think a suspect Chris frauder had been using credit card skimmer tools and machine, then used it on gas pump credit card machine and hooked his reader. And collect up to twenty peoples credit card information.

Date 12/8/9/2022

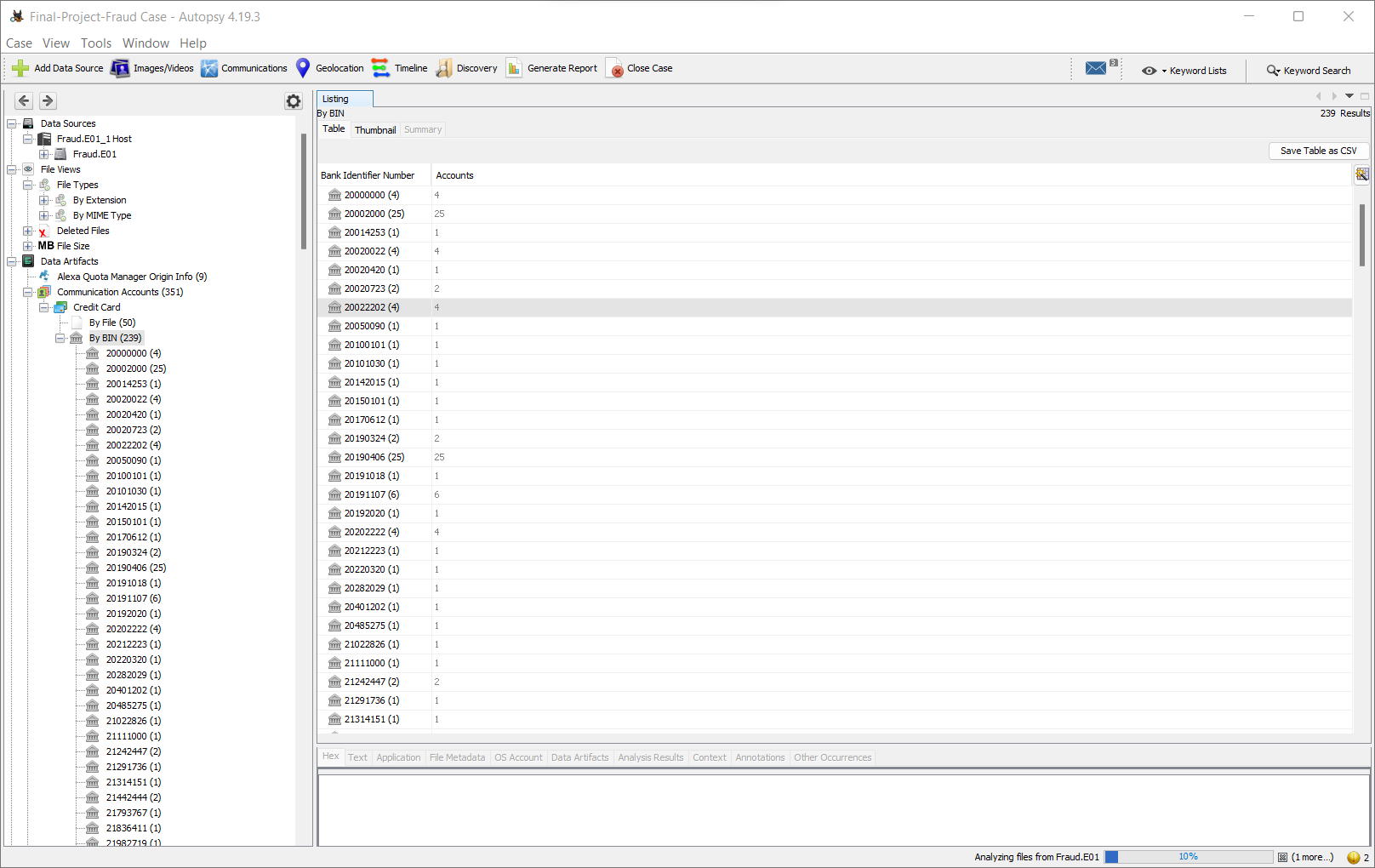
Manderas Kidane

# Attachments

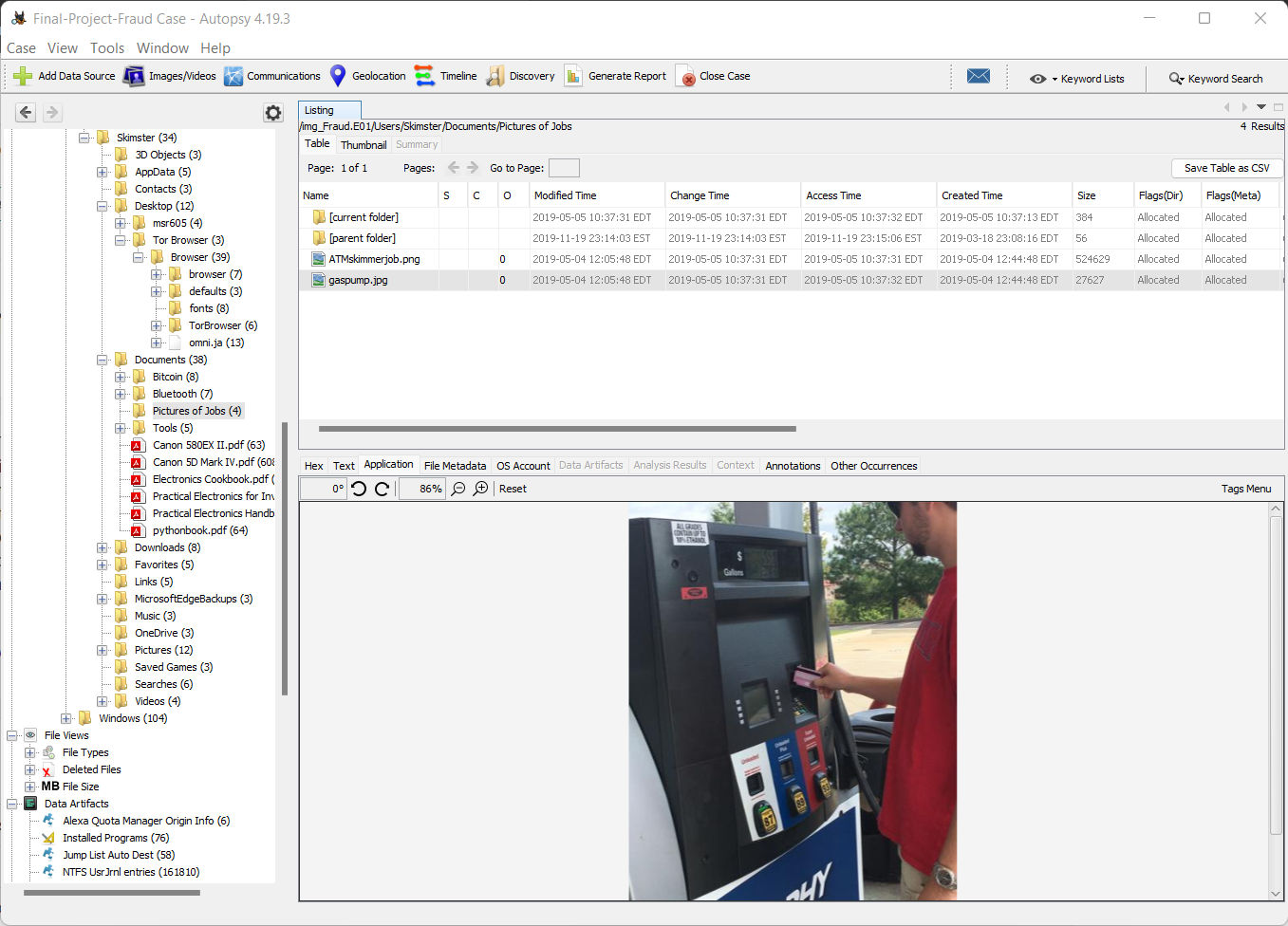


*Internet web history that suspects searched and visited on 2019-11-19.*

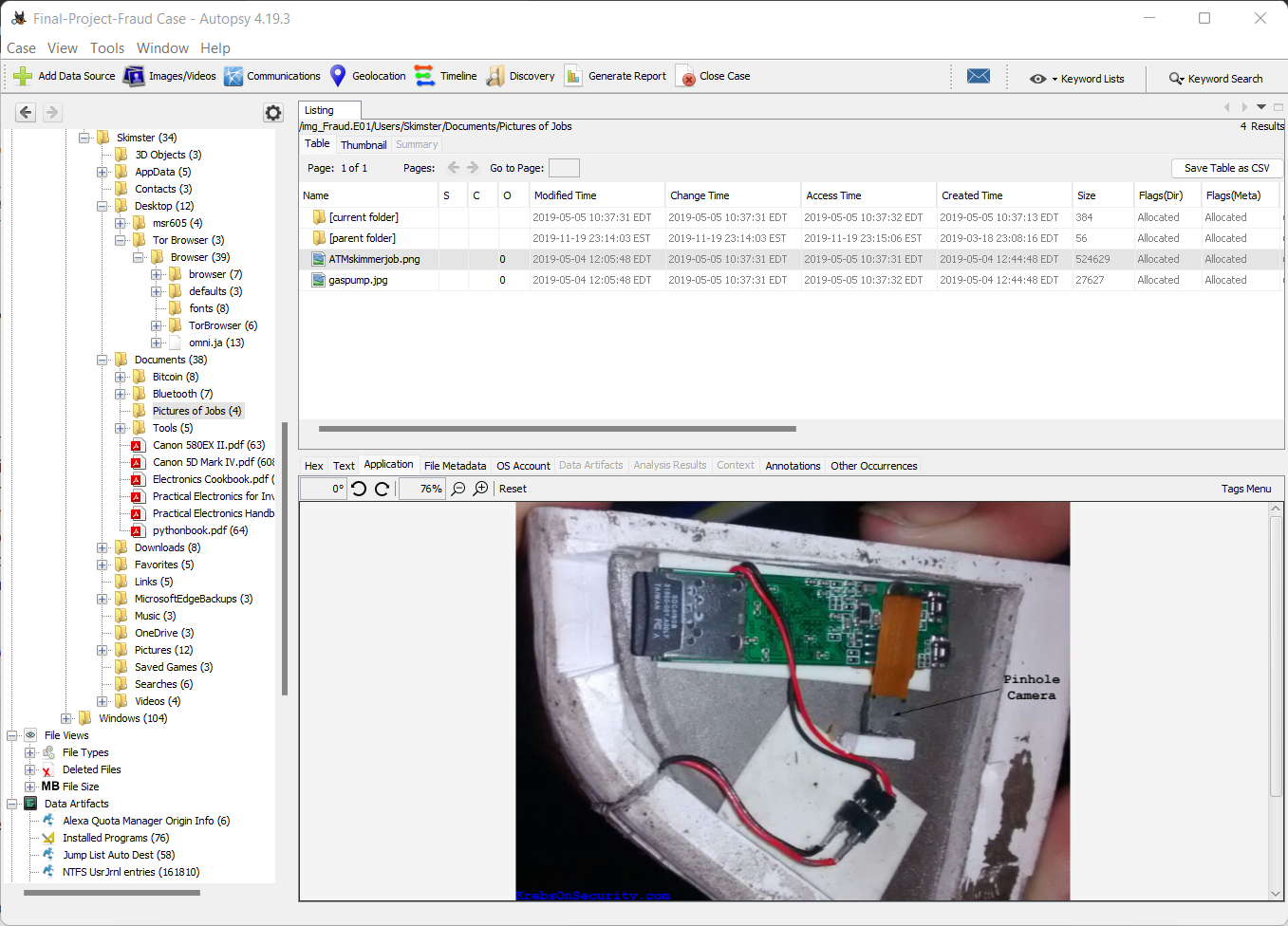
**Exhibits:**

****

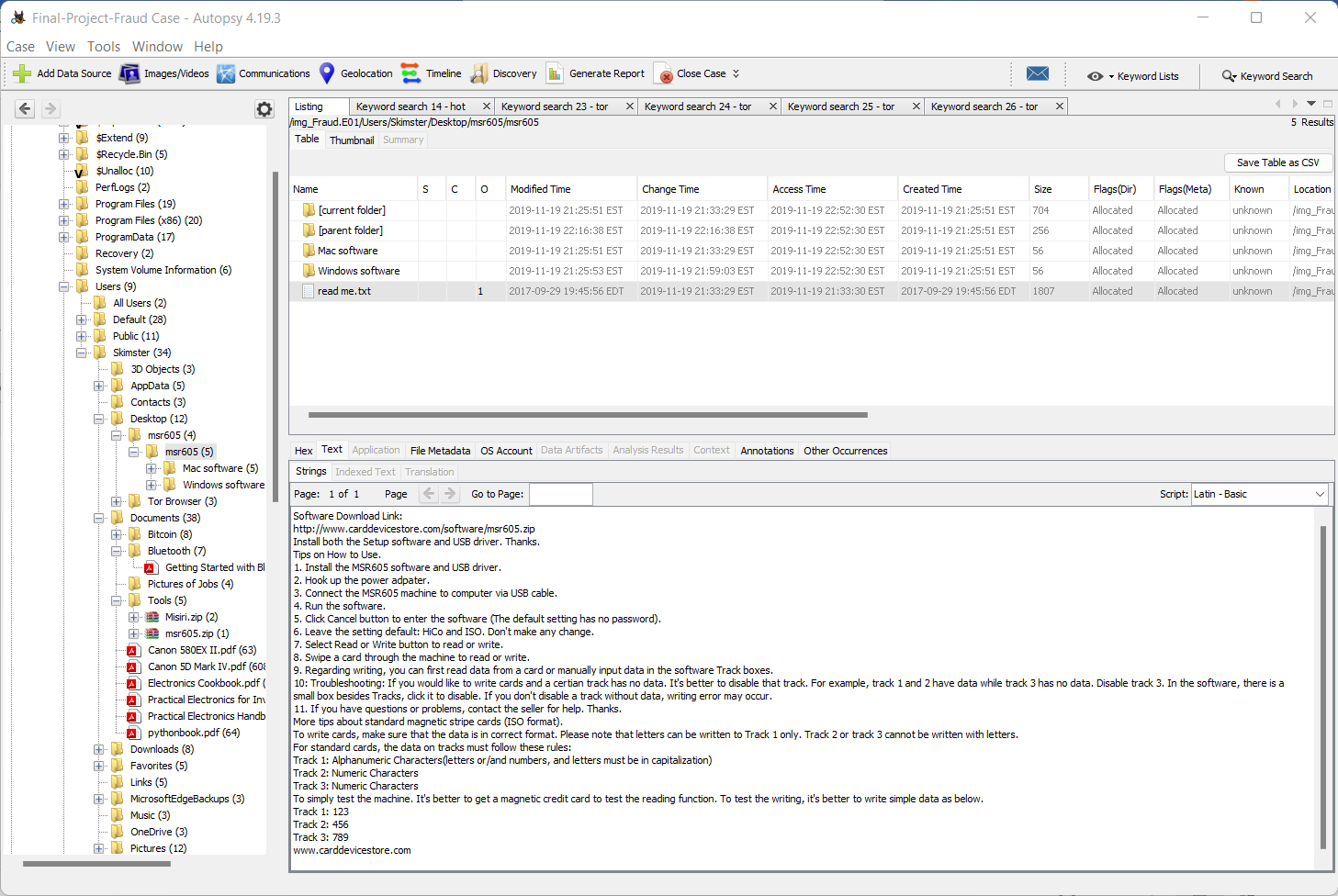
*List of credit cards with bank identification number.*

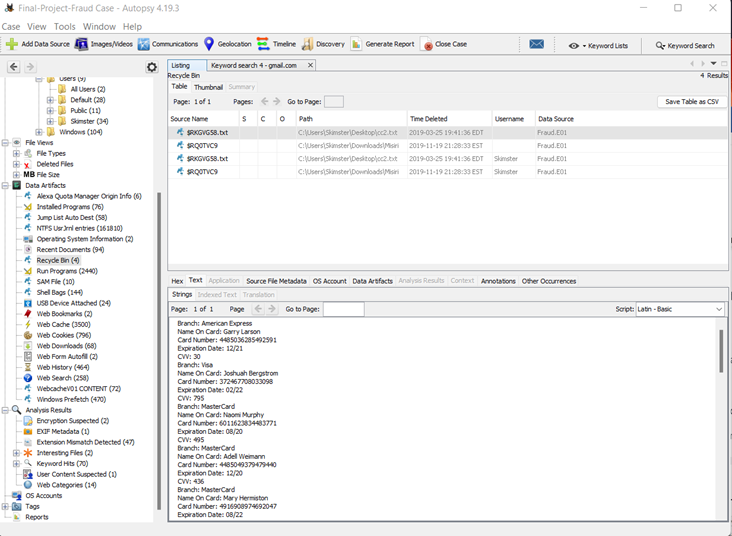


**Exhibits:**



**Exhibits:**





**Exhibits:**

