Calvin Hsieh

February 7, 2022

CIS 60 Final Case Study Spring 2021: An Analysis

Forensic Image file:	Suspect_s Device.dvi
Case Reference:	CS 60 Digital Forensics - 4/30/21 final case study 2021
	Note: The linked document above includes a link to the image file.
(Alternate Case Ref:	Merritt College CS 60 Digital Forensics 2021 Final Case Study Description)
Tools used:	Autopsy 4.18.0 in Windows 10 Home
Was the tool relevant?	Yes. Autopsy was comprehensive and useful.
Any issues with the case?	No serious issues found with the case.

How can it be improved?

- Include more potentially incriminating documents to make the case more interesting. Below are some suggestions.
    - Receipts of the purchase of credit card dumps.
    - Receipts and delivery addresses of the ebay purchase of credit card reader.
    - Leave evidence in the recycle bin.
    - Encrypted files with evidence, but include the password in an email or in the metadata of files.

Comments on the preparation of case image for Autopsy 4.18 (in Windows 10 Home)

- The following VirtualBox command (for Windows 10 Home installation) was used to convert the disk image from the .dvi format to the .img raw format:

C:\Program Files\Oracle\VirtualBox> .\VBoxManage.exe clonemedium 'Suspect_s Device.vdi' 'Suspect_s Device.img' --format raw

- When creating a new case within Autopsy for this case image, I chose the following options:
    - Select: “Disk image or VM file”
    - When selecting the options for “Configure Ingest Modules”, every option was checked except for “Plaso”.

Summary of the major evidence found

- Some email addresses
- Telegram contact
- downloaded programs
- Credit card dumps url
- credit card equipment purchasing sites were visited.
- Credit Card Magnetic Stripe Reader equipment seems to have been purchase
- Credit card dumps seem to have been purchased, but there were no receipts, only a file name suggesting there was a purchase.
- CommonThief MSR might have been used.
- Autopsy was installed.
- Some .jpg files of emails and of the tutanota email interface. But they may also look like advertisements or demo of the web Tutanota's web interface
- Some .jpg files of credit card reader. They look like advertisements for card reader manufacturers.

The Suspect's account was used to research and perhaps used to purchase credit card dumps and a credit card reader. The account was also used to research secure email services.

Assuming I have found all of the important evidence, I do not think I found anything too incriminating, and I do not think I found any additional leads other than some email addresses and a Telegram contact.

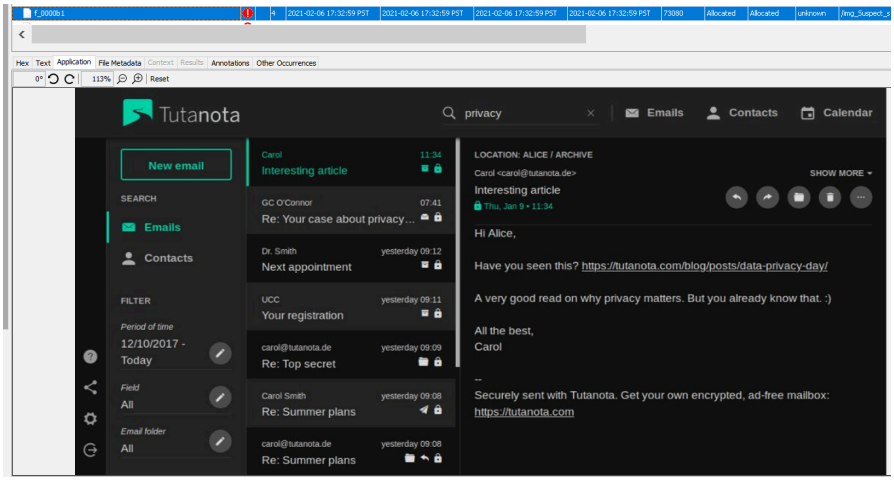
Selected Autopsy Analysis Results

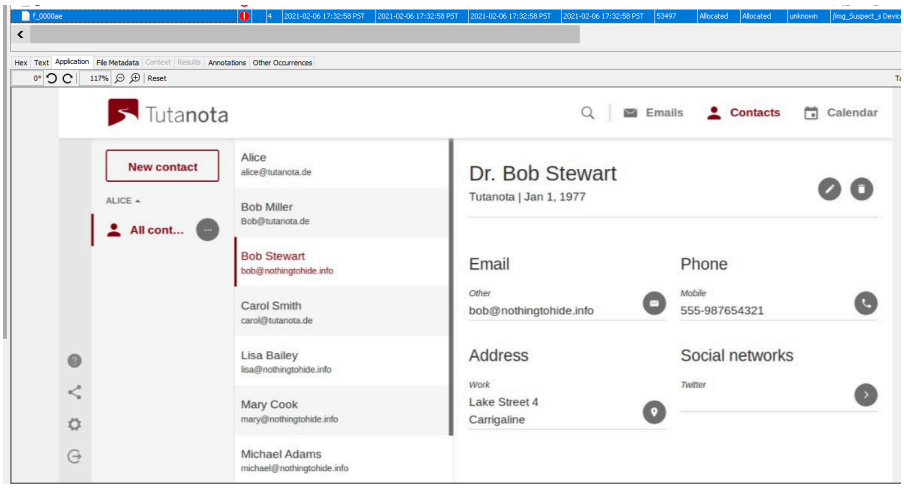
- Search term: "credit card"
    - Found a document that is an Ad for a Credit Card Reader
    - /img_Suspect_s Device.img/vol_vol3/Users/Suspect/AppData/Local/Microsoft/Edge/User Data/Default/Cache/f_0000d7/f_0000d7/0

- CPU: AMD64
- OS: Windows 10 Home, Date: 2020-11-23
- Owner: Suspect
- User accounts:
    - Administrator
    - Suspect
- Data source: Only Vol 3 seems interesting.
- Software installed:
    - Autopsy
- Users:
    - Suspect
        - Desktop
            - URL shortcut: goldentrack.cc for credit card dumps.
        - Documents:
            - PDF Ad for goldentrack credit card dumps
            - GoldentrackDumpPurchaseConfirmationScreenshot.pdf. The file name suggests it is a receipt, but the content looks like it is an Ad for credit card dumps.
        - Downloads:
            - CommonThief_MSR_Source.zip
            - ZipSetup.exe
            - Autopsy-4.17.0-64bit.msi
            - Scalpel-0.5.4.tar.gz
            - Tutanota-desktop-win.exe
                - Note: Tutanota is an encrypted email service.

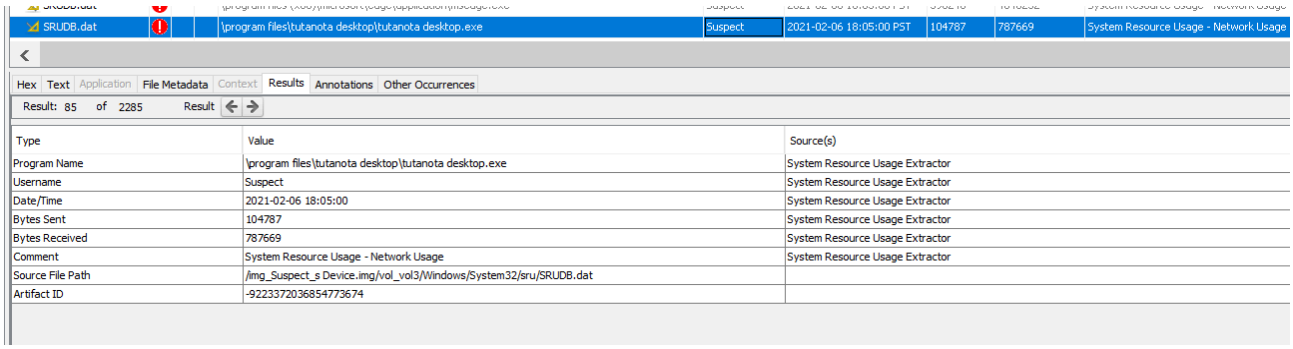
        - Thunderbird setup 78.5.1.exe
        - Email with link to encrypted content on the web
            - https://mail.tutanota.com/#mail/MNpRuDx----2FbMdkmVdN5LSp3yh8b8TNw
    - Email addresses found
        - suspect1@tutanota.com
        - admin@illegalcarddumps.com
    - Telegram: @dumps777
    - metadata names found
        - suspect1@tutanota.com
        - harlan: Owner of the file regripper.pdf: “Windows Forensic Analysis”
    - Recent Documents
        - Scalpel
        - Goldentrack links
        - CommonThief_MSR

    - Web search
        - express zip file compression
        - scalpel download windows
        - download autopsy free
        - goldendum.cc
        - ebay signup
        - tutanota desktop
        - free email no phone
        - ctemplar
        - download thunderbird
        - msr605 magnetic stripe card reader writer encoder
        - but mag strip encoder
        - common thief msr
        - download mag stripe reader
    - Web history
        - Tor project
        - Telegram: Contact @dumps777
        - blockchain-dns.info
        - NCH Software
    - Images (.jpg)
        - Photos of credit card readers
            - These photos look like they are advertisements for card reader sellers.

- 
- Photos of Tutanota email server interface
  - They look like advertisements of Tutanota or example screenshots of Tutanota's interface.
- 

- 

- Executed programs
  - Suspect ran the Tutanota Desktop application for secure email.



SRUDB.dat | \program files\tutanota desktop\tutanota desktop.exe | Suspect | 2021-02-06 18:05:00 PST | 104787 | 787669 | System Resource Usage - Network Usage

Hex | Text | Application | File Metadata | Context | Results | Annotations | Other Occurrences

Result: 85 of 2285 Result

Type	Value	Source(s)
Program Name	\program files\tutanota desktop\tutanota desktop.exe	System Resource Usage Extractor
Username	Suspect	System Resource Usage Extractor
Date/Time	2021-02-06 18:05:00	System Resource Usage Extractor
Bytes Sent	104787	System Resource Usage Extractor
Bytes Received	787669	System Resource Usage Extractor
Comment	System Resource Usage - Network Usage	System Resource Usage Extractor
Source File Path	/img_Suspect_s Device.img/vol_vol3/Windows/System32/sru/SRUDB.dat	
Artifact ID	-9223372036854773674	