Lab Report

Name:	Inor Wang
Title:	Static Disk Analysis w/ Autopsy
Case:	25-T109
Date:	11/14/2025

Table of Contents

Document Revision History

Name	Revision Date	Version	Description
Inor Wang	11/14/2025	0.1	Draft

Executive Summary

In this lab, the examiner used Autopsy, VeraCrypt, and supporting tools to perform static disk analysis of a Windows 10 Pro workstation used by the account **"AntiRenzik."** The focus was to document system configuration, identify installed and executed programs (especially VeraCrypt), review USB and web activity tied to ransom planning and a dog bite incident, reconstruct timelines for a ransom-related DOCX and a Google Takeout archive, analyze ransom images and EXIF GPS data, and decrypt a suspicious file flagged as potentially encrypted. The artifacts collectively show a single user researching ransom material, creating ransom notes and victim images, exporting and reviewing Gmail data, and hiding a manifesto and related content inside an encrypted VeraCrypt container.

Key findings

- **System Profile** – Hostname: DESKTOP-JEI7853; owner / username: AntiRenzik; operating system: Windows 10 Pro; processor architecture: AMD64.
- **Installed and Executed Programs –** Google Chrome version 78.0.3904.97 installed 2019-11-12 20:45:29 CST. ; VeraCrypt v1.24-Hotfix1 installed 2019-10-29 and flagged by Autopsy as an Encryption Program; recorded path /PROGRAM FILES/VERACRYPT. ; VeraCrypt executed five times with the following UTC timestamps: 2019-10-31 03:51:22, 2019-11-04 23:38:30, 2019-11-01 23:41:44, 2019-11-12 20:20:16, 2019-11-04 23:45:47.
- **USB device activity** – PNY device, model Product: 009F, ID AFA27H33YD35000553, connected 2019-11-04 18:31:33 CST; Alcor Micro Corp. Flash Drive, ID E432151F, connected 2019-11-05 16:14:07 CST.
- **Web bookmarks and history** – Only non-Google / non-social bookmark: "Ransom Note Generator" → http://www.ransomizer.com/ (domain ransomizer.com) created 2019-11-01 17:27:53 CDT. ; Chrome search "how to transport the victim over state lines" on 2019-11-05 16:18:43 CST; Chrome search "how to treat a dog bite" on 2019-11-12 14:11:08 CST, indicating the suspect was bitten by the victim shortly before that time.
- **Timeline for docx and zip files** – DOCX "In order to ensure that Renzik is treated properly.docx" located in the user's Downloads folder; source traced to the internet, specifically a Gmail attachment. ; Timeline correlation shows wordpad.exe execution

immediately adjacent to the DOCX access time; the examiner assesses the document was opened with WordPad. ; ZIP “takeout-20191112T181254Z-001” sourced from https://storage.cloud.google.com/dataliberation/20191112T indicating a Google Takeout export; after extraction, the suspect was reviewing exported Gmail mailbox contents, including raw email header TXT files.

- **Media and EXIF analysis** – Under Desktop\Pictures in the AntiRenzik profile, the first ransom note creation timestamp is 2019-11-01 17:14:47 CDT; the directory contains three ransom notes and four images of the victim. ; EXIF GPS data plus Google Maps place the victim at Baltimore/Washington International Airport (39°10'39.6"N 76°40'00.9"W); a building in New Orleans, Louisiana (29°57'01.0"N 90°03'59.0"W); and Lucy’s Retired Surfers Bar & Restaurant (29°56'47.0"N 90°04'03.0"W). ; Based on file timestamps, the visit to Lucy’s Retired Surfers Bar & Restaurant occurs first among these locations.
- **Encryption, container contents, and victim identity** – Autopsy’s Encryption Suspected results flagged IMPORTANT.jpg in the owner’s profile as possibly encrypted. ; Desktop text file VCPW.txt contains the password “argstrongpassword”, which the examiner used in VeraCrypt to mount IMPORTANT.jpg as a volume (A:). ; Root of the mounted container includes folder “Antirenzik@gmail.com” and text file “MANIFESTO” (MANIFESTO.txt); Windows PowerShell reported the MD5 hash of MANIFESTO.txt as 92D9a174A1269E1DA4262FFD259AE664. ; Reading MANIFESTO.txt confirms the victim (dog) is named Renzik.

From this lab’s artifacts alone, the examiner assesses that DESKTOP-JEI7853, controlled by “AntiRenzik,” was used to plan and document ransom activity against the dog Renzik, including ransom note generation, location tracking via photos, review of exported Gmail data, and storage of a manifesto and related material in an encrypted VeraCrypt container.

Synopsis

The client has provided a series of questions to guide a forensic examination of a suspect's computer system. These questions focus on first identifying the basic system details, such as the hostname, user account, operating system, and hardware architecture. The examiner is then asked to review installed and executed programs, USB device activity, and Chrome bookmarks to understand what software was present, what was run, and which external devices and websites may be involved. Additional questions center on web search history, timeline activity in the Downloads folder, and media files related to the victim, including ransom notes and photos. Finally, the examiner must identify and analyze an encryption program, determine whether any user files were encrypted, recover the decryption password, and review the decrypted contents. Together, these questions are designed to reconstruct the suspect's actions, trace how the victim was handled, and document evidence that supports or refutes the client's concerns.

Client Questions:

General Questions

1. What is the hostname of the system?
2. Who is the owner (also the username)?
3. What is the operating system?
4. What is the processor architecture?

Installed Programs

5. What version of Chrome is installed on the system?
6. When was Chrome installed?
7. According to installed programs, a program was installed on October 29, 2019, what is the name of the program?

Run Programs

8. In the last question, you were asked about a program that was installed on October 29, 2019. This program was ran 5 times, what are the date timestamps in UTC time?
9. What is the full path of the program that was ran?

USB Device Attached

10. Two USB devices were connected to the system before 11/12/2019. What is the device make, model, device ID, and date timestamp it was connected?

Web Bookmarks

11. There are four bookmarks setup in Google Chrome. Which one is not associated to Google or a social media platform?

12. What is this site?

Web History

13. According to web history, the suspect searched for how to transport the victim over state lines. When was this search conducted?

14. It appears that the suspect was injured by the victim… when?

Timeline Analysis

Explore the system owner's profile folder. Under their Downloads folder there appears to be two files of interest. A docx file (not the zone identifier) and a zip file. Right click on the docx file and click "View file in timeline...". Choose "File Created" and 1 hour before and after the date. Answer the following questions for the docx file.

15. What is the source of this document?

16. Was the file opened by the user? If so, what program was used to open it and how do you know?

Answer the following questions for the zip file.

17. What is the source of the zip file? (Hint: https://xxxx.google.com)

18. What was the suspect doing?

Media Analysis

Under the owner's profile, there is a directory with several images of the victim, to include the ransom note.

19. What is the creation date timestamp of the FIRST ransom note?

20. How many ransom notes are on this system?

21. How many images are there of the victim?

22. According to EXIF data, where was the victim taken to?

23. Which of these locations occurred first?

Other Interesting Findings

Now go back and run all ingest modules EXCEPT for Plaso. DO NOT RUN Plaso, otherwise you will be waiting for a long time!

24. According to Autopsy, there is a program that is used to encrypt files. What is the name of the program.

25. According to Autopsy, there is a file in the owner’s profile folder that maybe encrypted. What is the name of the file?

Using the program the suspect used to encrypt the file, decrypt it. You will need to find the password. Perhaps they saved it somewhere.

26. What is the password to decrypt the file?

27. What is the name of the folder in the root of this container?

28. What is the name of the text file in the root of this container?

29. What is the MD5 hash of the text file?

30. What is the name of the victim (dog)?

Scope of Work:

- Acquisition of disk captures, device1_laptop.e01.
- Analyzation of memory captures using Autopsy 4.22.1.
- Verification of evidentiary integrity using MD5, SHA1, and SHA256 cryptographic hashes.
- All tools were run against mounted, read-only images to preserve evidentiary integrity.

Evidence Analyzed

This section provides details of the digital evidence collected

Evidence ID	**E001**
Name	device1_laptop.e01
Type	EWF/Expert Witness/EnCase image file format
Size	3446.27 MB
MD5	DC176D653C5613E305E831525E874090
SHA1	87E09A16BECF8A5DB1D18804E29954309C87ABF6
SHA256	4F082EDFEEED1CE7F5050545435FA57A6ED59C3CCB72495CFA62771075BBD736

Tools Used

Workstation

Hostname	Operating System	Build	Physical / Virtual	Built
IS-4523-001-WINDOWS	Windows 11	2021	Virtual	09/06/2025

Software

Name	Version	Release	Purpose
Autopsy (Basis Technology)	4.22.1	Apr 2025	Autopsy was used as the primary forensic tool to perform static disk analysis of the acquired image, enabling the examiner to identify, correlate, and document relevant system, user, web, USB, and encryption artifacts.

Analysis Findings

Overview of Examination Procedures

The examiner conducted a structured static disk analysis using Autopsy on a forensic image of the suspect’s system. First, the examiner prepared the analysis environment by organizing separate Evidence and Cases directories, creating Autopsy case “25-0001”, and importing the NSRL and ClamAV hash sets before adding the EnCase/E01 disk image in read-only mode. Standard Autopsy ingest modules were then run, and key system details (hostname, user account, OS, and architecture) were documented using the Operating System Information artifact. Application installation and execution activity were reconstructed through the Installed Programs and Run Programs artifacts, while external device usage was reviewed via the USB Device Attached artifacts. The examiner then analyzed user internet activity using Web Bookmarks and Web History to identify searches, bookmarked ransom-related resources, and activity tied to the victim. File system events related to the ransom documents, the Google Takeout archive, and other relevant items were correlated in the Timeline view. For media, images of the victim and ransom notes were exported and their EXIF GPS data was parsed and checked with Google Maps (OSINT) to determine physical locations. Finally, Autopsy’s Encryption Programs and Encryption Suspected results were used to identify VeraCrypt and the suspicious IMPORTANT.jpg container, which was then decrypted with VeraCrypt using a password recovered from the desktop; the mounted volume contents were examined, and the MD5 hash of MANIFESTO.txt was computed in PowerShell to support integrity and identification of the ransom note and victim information. Additional targeted analysis was performed using:

- **Autopsy (Basis Technology)** — Used to analyze the disk image file

Throughout the process, all findings were documented and evidence files were correctly hashed.

Evidence Reviewed

device1_laptop.e01(E01): Device image file

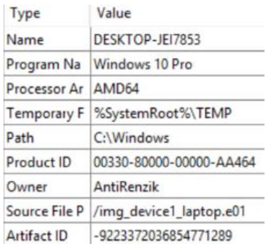
Key Findings

General Questions

1. What is the hostname of the system?

- **Analysis Performed:**
  - The examiner imported the NSRL hashset and ClamAV hashset into Autopsy, then created a new case named “25-0001”, and imported the disk image file into Autopsy.
  - The examiner then went to the “Operating System Information” data artifact within Autopsy which shows information about the operating system, as shown in Figure 1.
- **Answer:**
  The hostname of the system is **DESKTOP-JEI7853**, as shown in Figure 1.

- **Supporting Evidence:**



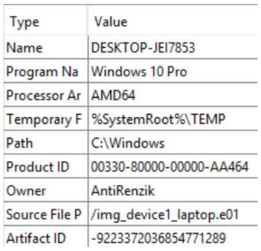
Type	Value
Name	DESKTOP-JEI7853
Program Na	Windows 10 Pro
Processor Ar	AMD64
Temporary F	%SystemRoot%\TEMP
Path	C:\Windows
Product ID	00330-80000-00000-AA464
Owner	AntiRenzik
Source File P	/img_device1_laptop.e01
Artifact ID	-9223372036854771289

Figure 1. The “Operating System Information” data artifact information

2. Who is the owner (also the username)?

- **Analysis Performed:**
  - The examiner then went to the “Operating System Information” data artifact within Autopsy which shows information about the operating system, as shown in Figure 2.
- **Answer:**
  The owner (also the username) of the system is **AntiRenzik**, as shown in Figure 2.

- **Supporting Evidence:**



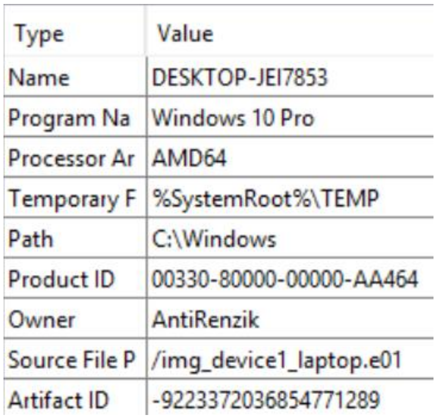
Type	Value
Name	DESKTOP-JEI7853
Program Na	Windows 10 Pro
Processor Ar	AMD64
Temporary F	%SystemRoot%\TEMP
Path	C:\Windows
Product ID	00330-80000-00000-AA464
Owner	AntiRenzik
Source File P	/img_device1_laptop.e01
Artifact ID	-9223372036854771289

Figure 2. The “Operating System Information” data artifact information

3. What is the operating system?

- **Analysis Performed:**
  - The examiner then went to the “Operating System Information” data artifact within Autopsy which shows information about the operating system, as shown in Figure 3.
- **Answer:**
  The operating system of the system is **Windows 10 Pro**, as shown in Figure 3.

- **Supporting Evidence:**



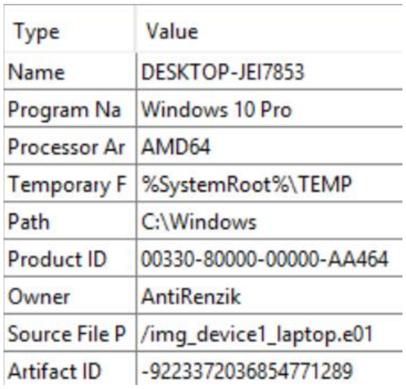
Type	Value
Name	DESKTOP-JEI7853
Program Na	Windows 10 Pro
Processor Ar	AMD64
Temporary F	%SystemRoot%\TEMP
Path	C:\Windows
Product ID	00330-80000-00000-AA464
Owner	AntiRenzik
Source File P	/img_device1_laptop.e01
Artifact ID	-9223372036854771289

Figure 3. The “Operating System Information” data artifact information

4. What is the processor architecture?

- **Analysis Performed:**
  - The examiner then went to the “Operating System Information” data artifact within Autopsy which shows information about the operating system, as shown in Figure 4.
- **Answer:**
  The processor architecture of the system is **AMD64**, as shown in Figure 4.

- **Supporting Evidence:**



Type	Value
Name	DESKTOP-JEI7853
Program Na	Windows 10 Pro
Processor Ar	AMD64
Temporary F	%SystemRoot%\TEMP
Path	C:\Windows
Product ID	00330-80000-00000-AA464
Owner	AntiRenzik
Source File P	/img_device1_laptop.e01
Artifact ID	-9223372036854771289

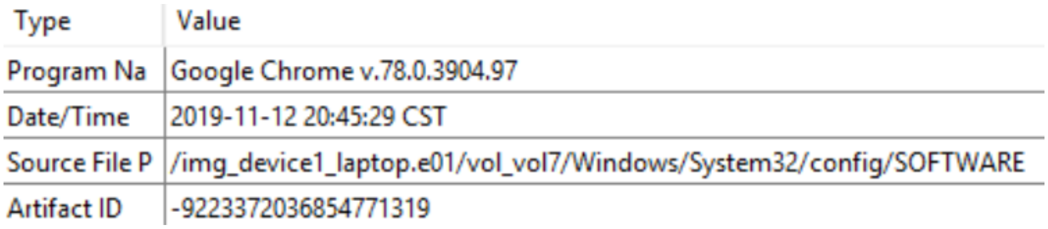
Figure 4. The “Operating System Information” data artifact information

Installed Programs

5. What version of Chrome is installed on the system?

- **Analysis Performed:**
  - The examiner then went to the “Installed Programs” data artifact and then Google Chrome within Autopsy which shows information about programs’ installation, as shown in Figure 5.
- **Answer:**
  The version of Chrome that is installed on the system is **v.78.0.3904.97**, as shown in Figure 5.

- **Supporting Evidence:**



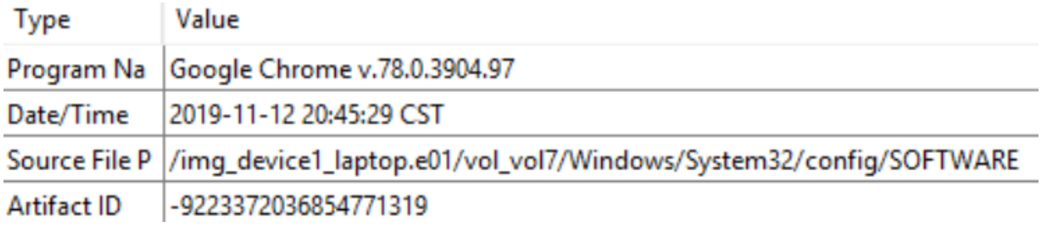
Type	Value
Program Na	Google Chrome v.78.0.3904.97
Date/Time	2019-11-12 20:45:29 CST
Source File P	/img_device1_laptop.e01/vol_vol7/Windows/System32/config/SOFTWARE
Artifact ID	-9223372036854771319

Figure 5. The data artifact of Google Chrome within the Installed Programs data artifact.

6. When was Chrome installed?

- **Analysis Performed:**
  - The examiner then went to the “Installed Programs” data artifact and then Google Chrome within Autopsy which shows information about programs’ installation, as shown in Figure 6.
- **Answer:**
  Chrome was installed on **2019-11-12 20:45:29 CST**, as shown in Figure 6.

- **Supporting Evidence:**



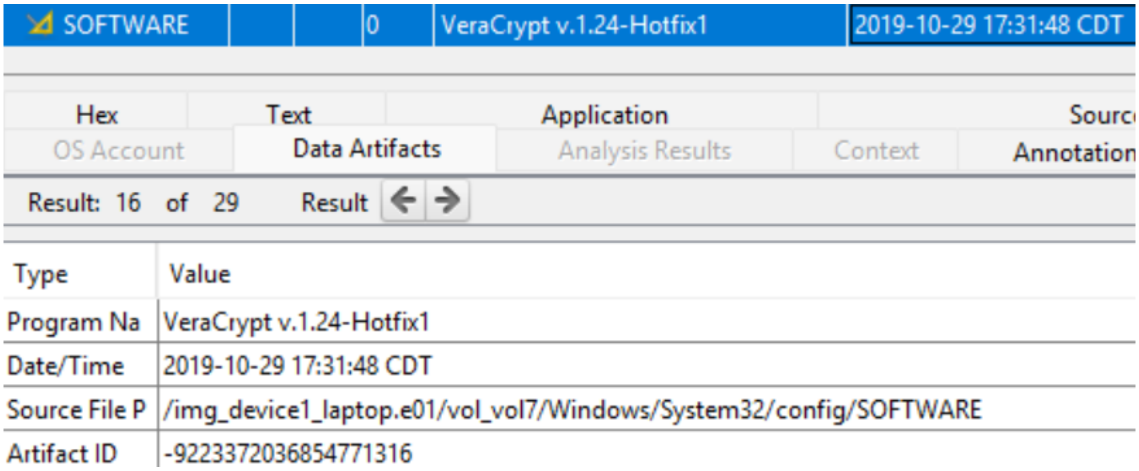
Type	Value
Program Na	Google Chrome v.78.0.3904.97
Date/Time	2019-11-12 20:45:29 CST
Source File P	/img_device1_laptop.e01/vol_vol7/Windows/System32/config/SOFTWARE
Artifact ID	-9223372036854771319

Figure 6. The data artifact of Google Chrome within the Installed Programs data artifact.

7. According to installed programs, a program was installed on October 29, 2019, what is the name of the program?

- **Analysis Performed:**
    - The examiner then went to the "Installed Programs" data artifact and then searched for a program that was installed on October 29, 2019, as shown in Figure 7.
- **Answer:**
  The **VeraCrypt v.1.24-Hotfix1** program was installed on October 29, 2019, as shown in Figure 7.

- **Supporting Evidence:**



SOFTWARE			0	VeraCrypt v.1.24-Hotfix1	2019-10-29 17:31:48 CDT

Result: 16 of 29 Result

Type	Value
Program Na	VeraCrypt v.1.24-Hotfix1
Date/Time	2019-10-29 17:31:48 CDT
Source File P	/img_device1_laptop.e01/vol_vol7/Windows/System32/config/SOFTWARE
Artifact ID	-9223372036854771316

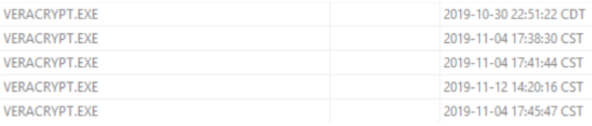
Figure 7. The data artifact of VeraCrypt within the Installed Programs data artifact.

Run Programs

8. In the last question, you were asked about a program that was installed on October 29, 2019. This program was ran 5 times, what are the date timestamps in UTC time?

- **Analysis Performed:**
  - The examiner then went to the “Run Programs” data artifact within Autopsy which shows information about programs that were ran on the system.
  - Then, the examiner found the program, VeraCrypt, that was ran 5 times, as shown in Figure 8.
- **Answer:**
  From top to bottom within Figure 8, the first date timestamp is **2019-10-31 03:51:22 UTC**. The second date timestamp is **2019-11-04 23:38:30 UTC**. The third date timestamp is **2019-11-01 23:41:44 UTC**. The fourth date timestamp is **2019-11-12 20:20:16 UTC**. The fifth date timestamp is **2019-11-04 23:45:47 UTC**.

- **Supporting Evidence:**



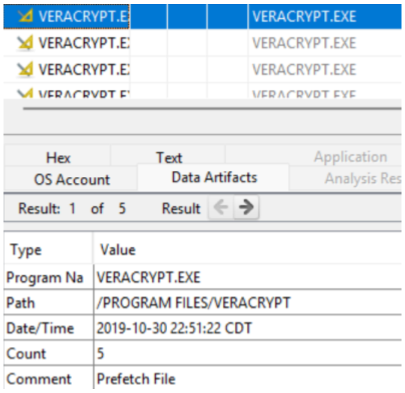
VERACRYPT.EXE		2019-10-30 22:51:22 CDT
VERACRYPT.EXE		2019-11-04 17:38:30 CST
VERACRYPT.EXE		2019-11-04 17:41:44 CST
VERACRYPT.EXE		2019-11-12 14:20:16 CST
VERACRYPT.EXE		2019-11-04 17:45:47 CST

Figure 8. Veracrypt bring ran 5 times shown in the Run Program data artifact

9. What is the full path of the program that was ran?

- **Analysis Performed:**
  - The examiner then went to the “Run Programs” data artifact within Autopsy which shows information about programs that were ran on the system.
  - Then, the examiner found the program, VeraCrypt, that was ran 5 times, as shown in Figure 9.
- **Answer:**
  The full path of VeraCrypt is **/PROGRAM FILES/VERACRYPT**, as shown in Figure 9.

- **Supporting Evidence:**



VERACRYPT.E			VERACRYPT.EXE
VERACRYPT.E:			VERACRYPT.EXE
VERACRYPT.E:			VERACRYPT.EXE
VERACRYPT.E'			VERACRYPT.EXE

Type	Value
Program Na	VERACRYPT.EXE
Path	/PROGRAM FILES/VERACRYPT
Date/Time	2019-10-30 22:51:22 CDT
Count	5
Comment	Prefetch File

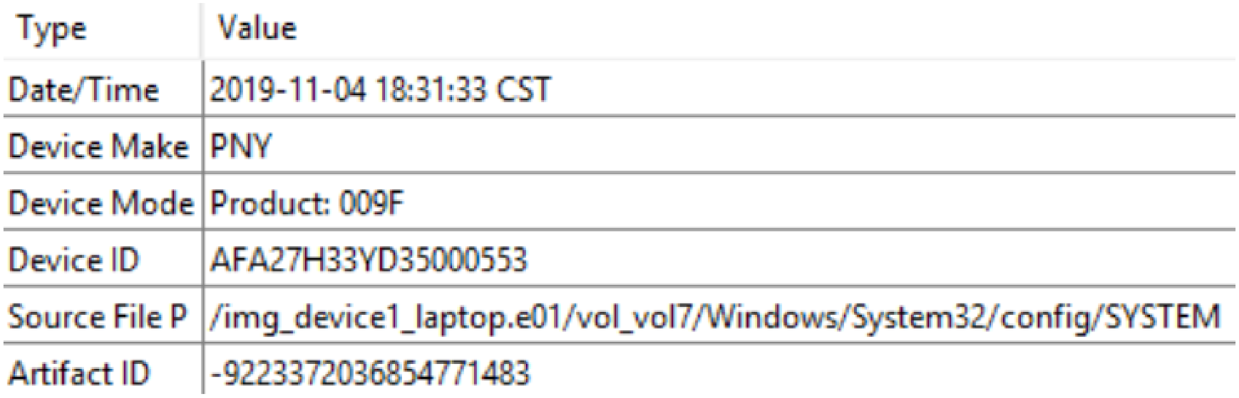
Figure 9. The data artifact information about VeraCrypt within Run Programs in Autopsy.

USB Device Attached

10. Two USB devices were connected to the system before 11/12/2019. What is the device make, model, device ID, and date timestamp it was connected?

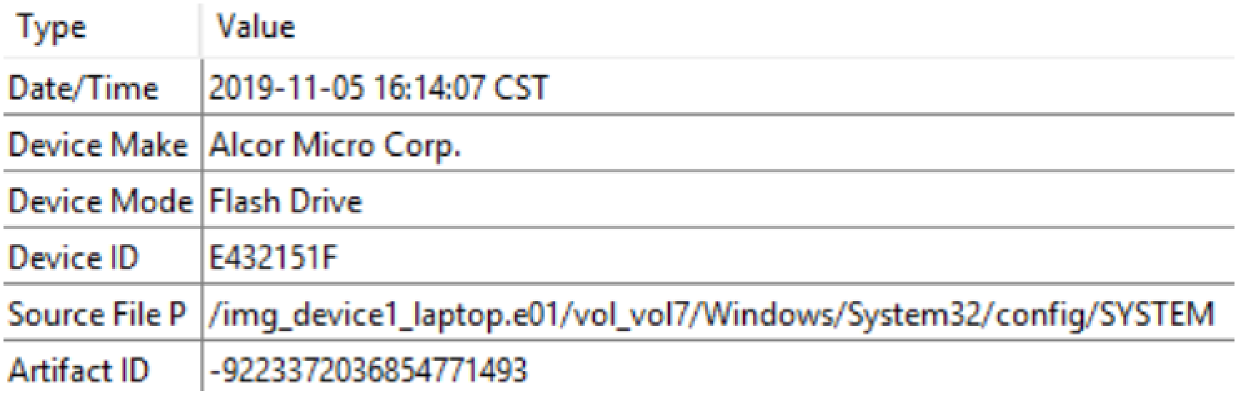
- **Analysis Performed:**
  - The examiner then went to the “USB Device Attached” data artifact within Autopsy which shows information about USB devices that were attached to the system.
  - Then, the examiner found two USB devices that were connected to the system before 11/12/2019, as shown in Figure 10 and 11.
- **Answer:**
  For the first USB device, the device make is **PNY**, the device model is **Product: 009F**, the device ID is **AFA27H33YD35000553**, and date timestamp is **2019-11-04 18:31:33 CST**, as shown in Figure 10. For the second USB device, the device make is **Alcor Micro Corp.**, the device model is **Flash Drive**, the device ID is **E432151F**, and date timestamp is **2019-11-05 16:14:07 CST**, as shown in Figure 11.

- **Supporting Evidence:**



Type	Value
Date/Time	2019-11-04 18:31:33 CST
Device Make	PNY
Device Mode	Product: 009F
Device ID	AFA27H33YD35000553
Source File P	/img_device1_laptop.e01/vol_vol7/Windows/System32/config/SYSTEM
Artifact ID	-9223372036854771483

Figure 10. Data artifact information of the PNY USB device make that was attached before 11/12/2019



Type	Value
Date/Time	2019-11-05 16:14:07 CST
Device Make	Alcor Micro Corp.
Device Mode	Flash Drive
Device ID	E432151F
Source File P	/img_device1_laptop.e01/vol_vol7/Windows/System32/config/SYSTEM
Artifact ID	-9223372036854771493

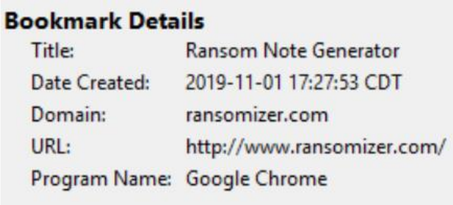
Figure 11. Data artifact information of the Alcor Micro Corp. USB device make that was attached before 11/12/2019

Web Bookmarks

11. There are four bookmarks setup in Google Chrome. Which one is not associated to Google or a social media platform?

- **Analysis Performed:**
    - The examiner then went to the “Web Bookmarks” data artifact and then searched for a bookmark that was setup in Google Chrome and not associated to Google or a social media platform, as shown in Figure 12.
- **Answer:**
  The bookmark that was not associated to Google or a social media platform was titled, “**Ransom Note Generator**”, and leads to the URL: **http://www.ransomizer.com/**, as shown in Figure 12.

- **Supporting Evidence:**



Bookmark Details

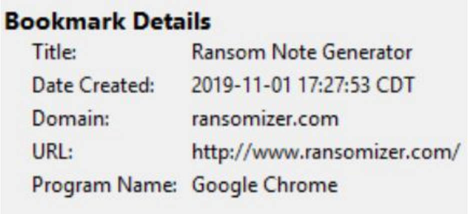
Title:	Ransom Note Generator
Date Created:	2019-11-01 17:27:53 CDT
Domain:	ransomizer.com
URL:	http://www.ransomizer.com/
Program Name:	Google Chrome

Figure 12. The bookmark that was setup in Google Chrome but not associated to Google or a social media platform.

12. What is this site?

- **Analysis Performed:**
    - The examiner then went to the “Web Bookmarks” data artifact and then searched for a bookmark that was not setup in Google Chrome, not associated to Google, and not associated to a social media platform, as shown in Figure 13.
- **Answer:**
  The site of the bookmark that was setup in Google Chrome but not associated with Google or a social media platform was **http://www.ransomizer.com/**, as shown in Figure 13. The domain was **ransomizer.com** and the bookmark was created on **2019-11-01 17:27:53 CDT**, as shown in Figure 13.

- **Supporting Evidence:**



Bookmark Details

Title:	Ransom Note Generator
Date Created:	2019-11-01 17:27:53 CDT
Domain:	ransomizer.com
URL:	http://www.ransomizer.com/
Program Name:	Google Chrome

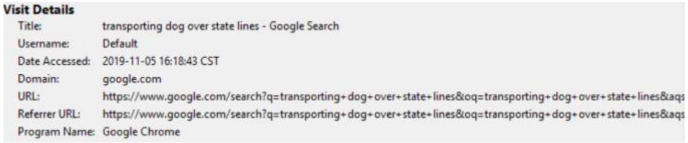
Figure 13. The bookmark that was setup in Google Chrome but not associated to Google or a social media platform.

Web History

13. According to web history, the suspect searched for how to transport the victim over state lines. When was this search conducted?

- **Analysis Performed:**
    - The examiner then went to the "Web History" data artifact and then searched for the data artifact of when the suspect searched for how to transport the victim over state lines, as shown in Figure 14.
- **Answer:**
  The date timestamp of the search whenever the suspect searched for how to transport the victim over state lines on Google Chrome is **2019-11-05 16:18:43 CST**, as shown in Figure 14.

- **Supporting Evidence:**



Visit Details

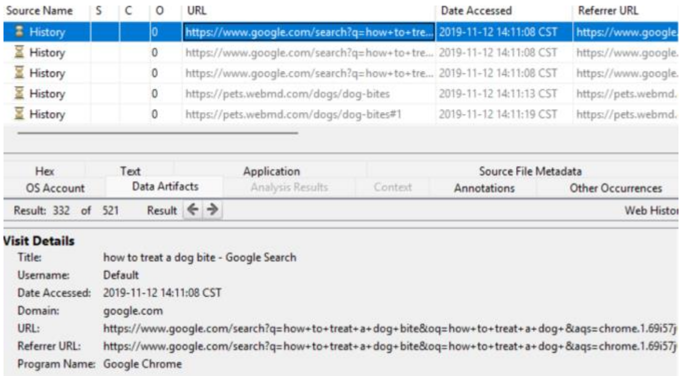
Title:	transporting dog over state lines - Google Search
Username:	Default
Date Accessed:	2019-11-05 16:18:43 CST
Domain:	google.com
URL:	https://www.google.com/search?q=transporting+dog+over+state+lines&oq=transporting+dog+over+state+lines&aqs
Referrer URL:	https://www.google.com/search?q=transporting+dog+over+state+lines&oq=transporting+dog+over+state+lines&aqs
Program Name:	Google Chrome

Figure 14. The data artifact information of the Google Search for how to transport the victim over state lines.

14. It appears that the suspect was injured by the victim… when?

- **Analysis Performed:**
    - The examiner then went to the "Web History" data artifact and then searched for the data artifact of when the suspect searched for how to treat a dog bite, as shown in Figure 15.
- **Answer:**
  The suspect got bit by the victim (dog) because the suspect searched in Google Chrome on how to treat a dog bite, as shown in Figure 15. The date timestamp of the first Google search is **2019-11-12 14:11:08 CST** which means the incident happened right before that date timestamp, as shown in Figure 15.

- **Supporting Evidence:**



Source Name	S	C	O	URL	Date Accessed	Referrer URL
History			0	https://www.google.com/search?q=how+to+tre...	2019-11-12 14:11:08 CST	https://www.google.
History			0	https://www.google.com/search?q=how+to+tre...	2019-11-12 14:11:08 CST	https://www.google.
History			0	https://www.google.com/search?q=how+to+tre...	2019-11-12 14:11:08 CST	https://www.google.
History			0	https://pets.webmd.com/dogs/dog-bites	2019-11-12 14:11:13 CST	https://pets.webmd.
History			0	https://pets.webmd.com/dogs/dog-bites#1	2019-11-12 14:11:19 CST	https://pets.webmd.

Visit Details

Title:	how to treat a dog bite - Google Search
Username:	Default
Date Accessed:	2019-11-12 14:11:08 CST
Domain:	google.com
URL:	https://www.google.com/search?q=how+to+treat+a+dog+bite&oq=how+to+treat+a+dog+&aqs=chrome.1.69i57j
Referrer URL:	https://www.google.com/search?q=how+to+treat+a+dog+bite&oq=how+to+treat+a+dog+&aqs=chrome.1.69i57j
Program Name:	Google Chrome

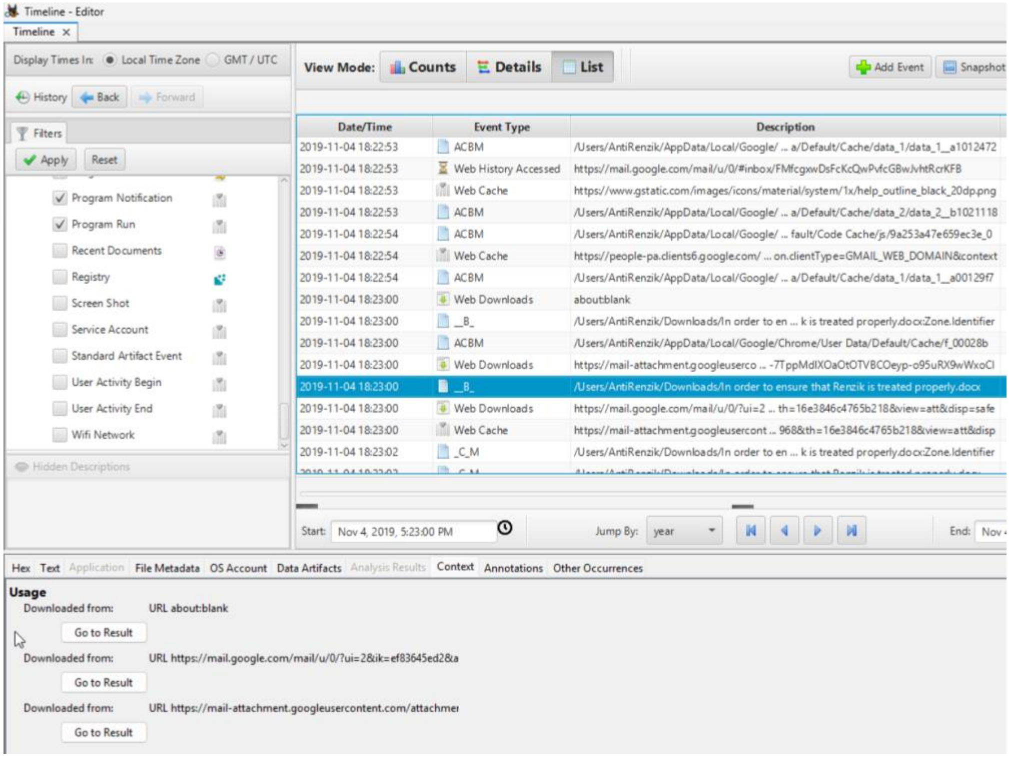
Figure 15. The data artifact information of the Google Search for how to treat a dog bite.

Timeline Analysis

15. What is the source of this document? (docx file)

- **Analysis Performed:**
  - The examiner went to the system owner's (AntiRenzik) profile folder, then proceeded to the Downloads directory, and then there was a docx file named, "In order to ensure that Renzik is treated properly.docx".
  - The examiner then right clicked on the docx file and clicked "View file in timeline…", then chose "File Created" and 1 hour before and after the date, which showed the Timeline tab as shown in Figure 16.
- **Answer:**
  The source of the docx file, "In order to ensure that Renzik is treated properly.docx", is the **internet more specifically, an attachment within Gmail** as shown in Figure 16.

- **Supporting Evidence:**



Display Times In: ● Local Time Zone ○ GMT / UTC

☑ Program Notification
☑ Program Run
☐ Recent Documents
☐ Registry
☐ Screen Shot
☐ Service Account
☐ Standard Artifact Event
☐ User Activity Begin
☐ User Activity End
☐ Wifi Network

Date/Time	Event Type	Description
2019-11-04 18:22:53	ACBM	/Users/AntiRenzik/AppData/Local/Google/ ... a/Default/Cache/data_1/data_1__a1012472
2019-11-04 18:22:53	Web History Accessed	https://mail.google.com/mail/u/0/#inbox/FMfcgxwDsFcKcQwPvfcGBwJvhtRcrKFB
2019-11-04 18:22:53	Web Cache	https://www.gstatic.com/images/icons/material/system/1x/help_outline_black_20dp.png
2019-11-04 18:22:53	ACBM	/Users/AntiRenzik/AppData/Local/Google/ ... a/Default/Cache/data_2/data_2__b1021118
2019-11-04 18:22:54	ACBM	/Users/AntiRenzik/AppData/Local/Google/ ... fault/Code Cache/js/9a253a47e659ec3e_0
2019-11-04 18:22:54	Web Cache	https://people-pa.clients6.google.com/ ... on.clientType=GMAIL_WEB_DOMAIN&context
2019-11-04 18:22:54	ACBM	/Users/AntiRenzik/AppData/Local/Google/ ... a/Default/Cache/data_1/data_1__a00129f7
2019-11-04 18:23:00	Web Downloads	about:blank
2019-11-04 18:23:00	__B_	/Users/AntiRenzik/Downloads/In order to en ... k is treated properly.docx:Zone.Identifier
2019-11-04 18:23:00	ACBM	/Users/AntiRenzik/AppData/Local/Google/Chrome/User Data/Default/Cache/f_00028b
2019-11-04 18:23:00	Web Downloads	https://mail-attachment.googleuserco ... -7TppMdlXOaOtOTVBCOeyp-o95uRX9wWxoCl
2019-11-04 18:23:00	__B_	/Users/AntiRenzik/Downloads/In order to ensure that Renzik is treated properly.docx
2019-11-04 18:23:00	Web Downloads	https://mail.google.com/mail/u/0/?ui=2 ... th=16e3846c4765b218&view=att&disp=safe
2019-11-04 18:23:00	Web Cache	https://mail-attachment.googleusercont ... 968&th=16e3846c4765b218&view=att&disp
2019-11-04 18:23:02	_C_M	/Users/AntiRenzik/Downloads/In order to en ... k is treated properly.docx:Zone.Identifier

Start: Nov 4, 2019, 5:23:00 PM Jump By: year End: Nov

Usage

Downloaded from: URL about:blank
Go to Result

Downloaded from: URL https://mail.google.com/mail/u/0/?ui=2&ik=ef83645ed2&a
Go to Result

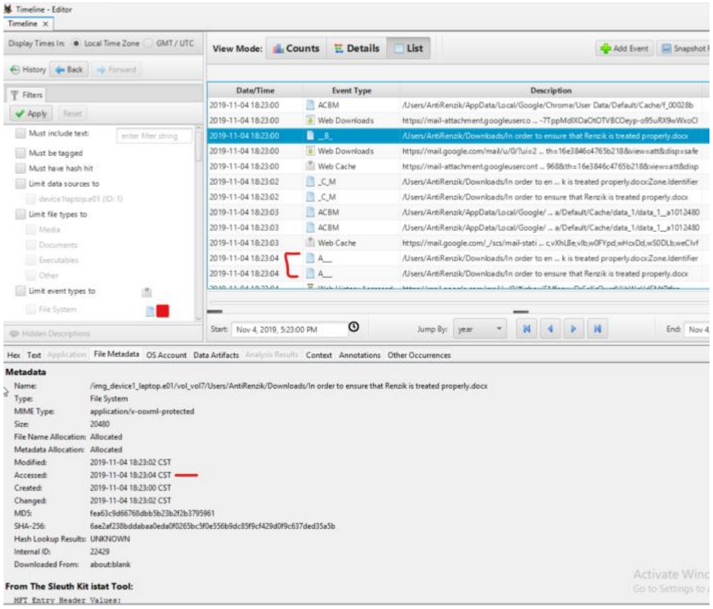
Downloaded from: URL https://mail-attachment.googleusercontent.com/attachmer
Go to Result

Figure 16. The source of the "In order to ensure that Renzik is treated properly.docx" docx file

16. Was the file opened by the user? If so, what program was used to open it and how do you know? (docx file)

- **Analysis Performed:**
  - The examiner is in the Timeline tab showing the docx file, as shown in Figure 17.
  - The examiner found that a program was ran right next to whenever the docx file was accessed, as shown in Figure 18.
- **Answer:**
  The docx file was accessed by the user and the wordpad.exe application, as shown in Figure 17 and 18. Wordpad.exe was ran extremely closely to when the docx file stated that it was accessed in the metadata therefore, the examiner believes the docx file was accessed via wordpad.exe.

- **Supporting Evidence:**



Date/Time	Event Type	Description
2019-11-04 18:23:00	ACBM	/Users/AntiRenzik/AppData/Local/Google/Chrome/User Data/Default/Cache/f_00028b
2019-11-04 18:23:00	Web Downloads	https://mail-attachment.googleuserco ... -7TppMdlXOaOtOTVBCOeyp-o95uRX9wWxoCl
2019-11-04 18:23:00	__B_	/Users/AntiRenzik/Downloads/In order to ensure that Renzik is treated properly.docx
2019-11-04 18:23:00	Web Downloads	https://mail.google.com/mail/u/0/?ui=2 ... th=16e3846c4765b218&view=att&disp=safe
2019-11-04 18:23:00	Web Cache	https://mail-attachment.googleusercont ... 968&th=16e3846c4765b218&view=att&disp
2019-11-04 18:23:02	_C_M	/Users/AntiRenzik/Downloads/In order to en ... k is treated properly.docx:Zone.Identifier
2019-11-04 18:23:02	_C_M	/Users/AntiRenzik/Downloads/In order to ensure that Renzik is treated properly.docx
2019-11-04 18:23:03	ACBM	/Users/AntiRenzik/AppData/Local/Google/ ... a/Default/Cache/data_1/data_1__a1012480
2019-11-04 18:23:03	ACBM	/Users/AntiRenzik/AppData/Local/Google/ ... a/Default/Cache/data_1/data_1__a1012480
2019-11-04 18:23:03	Web Cache	https://mail.google.com/_/scs/mail-stati ... c,vXhLBe,vlb,w0FYpd,wHcxDd,wS0DLb,weClvf
2019-11-04 18:23:04	A___	/Users/AntiRenzik/Downloads/In order to en ... k is treated properly.docx:Zone.Identifier
2019-11-04 18:23:04	A___	/Users/AntiRenzik/Downloads/In order to ensure that Renzik is treated properly.docx

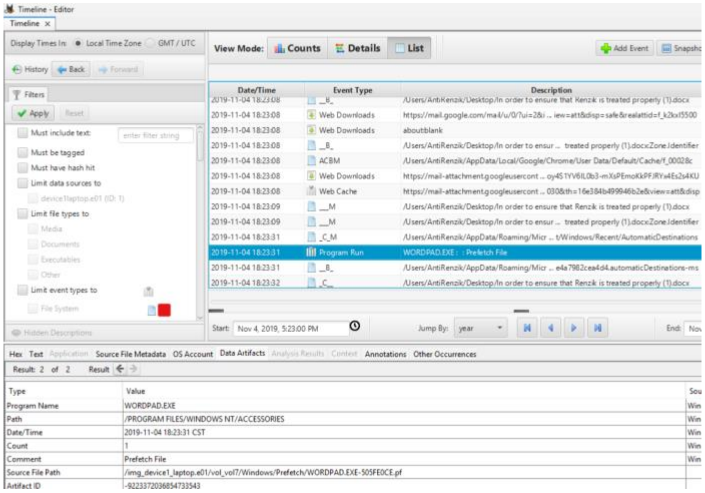
Metadata

Name:	/img_device1_laptop.e01/vol_vol7/Users/AntiRenzik/Downloads/In order to ensure that Renzik is treated properly.docx
Type:	File System
MIME Type:	application/x-ooxml-protected
Size:	20480
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2019-11-04 18:23:02 CST
Accessed:	2019-11-04 18:23:04 CST
Created:	2019-11-04 18:23:00 CST
Changed:	2019-11-04 18:23:02 CST
MD5:	fea63c9d66768dbb5b23b2f2b3795961
SHA-256:	6ae2af238bddabaa0eda0f0265bc5f0e556b9dc85f9cf429d0f9c637ded35a5b
Hash Lookup Results:	UNKNOWN
Internal ID:	22429
Downloaded From:	about:blank

From The Sleuth Kit istat Tool:

```
MFT Entry Header Values:
```

Figure 17. Timeline showing the docx file being accessed



Date/Time	Event Type	Description
2019-11-04 18:23:08	__B_	/Users/AntiRenzik/Desktop/In order to ensure that Renzik is treated properly (1).docx
2019-11-04 18:23:08	Web Downloads	https://mail.google.com/mail/u/0/?ui=2&i ... iew=att&disp=safe&realattid=f_k2kxl5500
2019-11-04 18:23:08	Web Downloads	aboutblank
2019-11-04 18:23:08	__B_	/Users/AntiRenzik/Desktop/In order to ensur ... treated properly (1).docx:Zone.Identifier
2019-11-04 18:23:08	ACBM	/Users/AntiRenzik/AppData/Local/Google/Chrome/User Data/Default/Cache/f_00028c
2019-11-04 18:23:08	Web Downloads	https://mail-attachment.googleusercont ... oy4S1YV6IL0b3-mXsPEmoKkPFJRYx4Es2s4KU
2019-11-04 18:23:08	Web Cache	https://mail-attachment.googleusercont ... 030&th=16e384b499946b2e&view=att&disp
2019-11-04 18:23:09	___M	/Users/AntiRenzik/Desktop/In order to ensure that Renzik is treated properly (1).docx
2019-11-04 18:23:09	___M	/Users/AntiRenzik/Desktop/In order to ensur ... treated properly (1).docx:Zone.Identifier
2019-11-04 18:23:31	_C_M	/Users/AntiRenzik/AppData/Roaming/Micr ... t/Windows/Recent/AutomaticDestinations
2019-11-04 18:23:31	Program Run	WORDPAD.EXE : : Prefetch File
2019-11-04 18:23:31	__B_	/Users/AntiRenzik/AppData/Roaming/Micr ... e4a7982cea4d4.automaticDestinations-ms
2019-11-04 18:23:32	_C__	/Users/AntiRenzik/Desktop/In order to ensure that Renzik is treated properly (1).docx

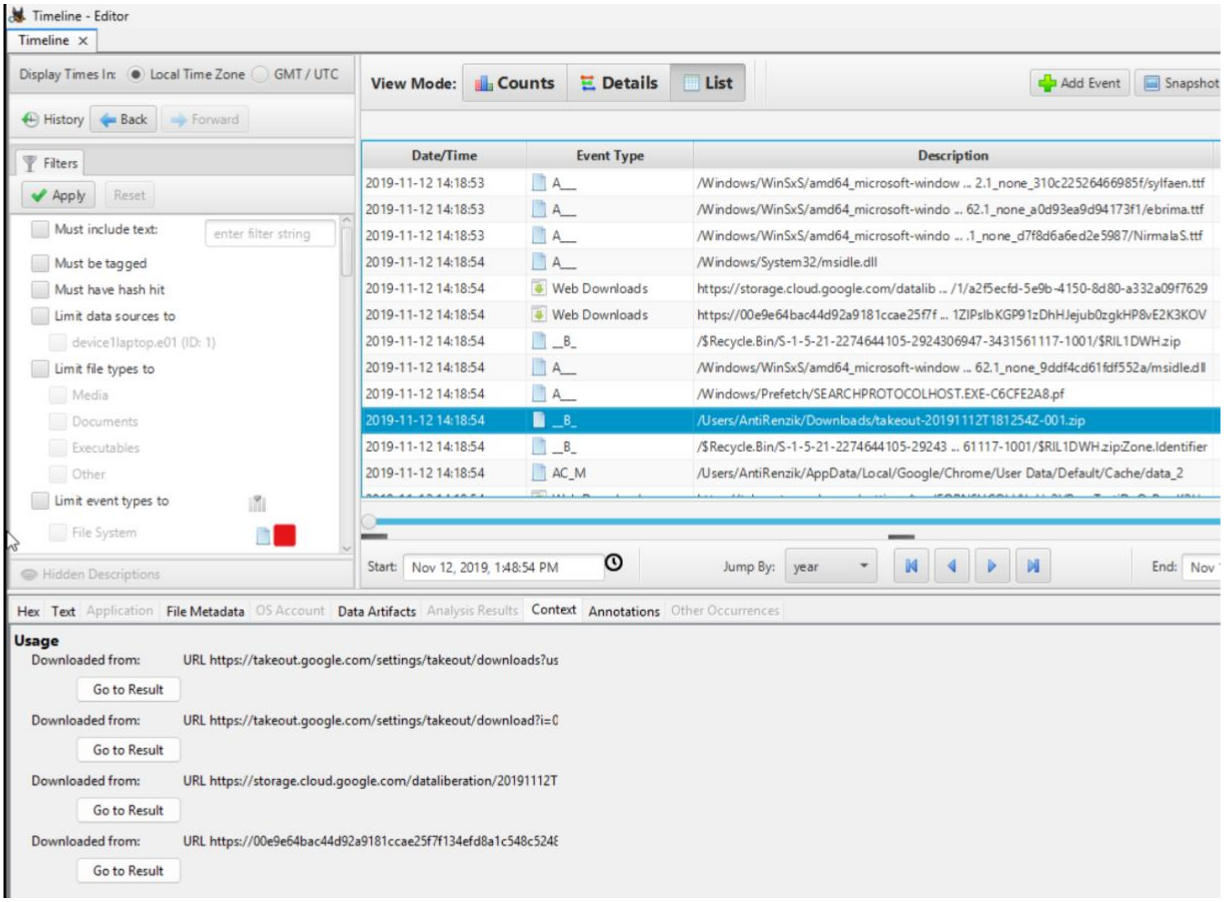
Type	Value	Sou
Program Name	WORDPAD.EXE	Win
Path	/PROGRAM FILES/WINDOWS NT/ACCESSORIES	Win
Date/Time	2019-11-04 18:23:31 CST	Win
Count	1	Win
Comment	Prefetch File	Win
Source File Path	/img_device1_laptop.e01/vol_vol7/Windows/Prefetch/WORDPAD.EXE-505FE0CE.pf	
Artifact ID	-9223372036854733543	

Figure 18. Timeline showing wordpad.exe

17. What is the source of the zip file? (Hint: https://xxxx.google.com)

- **Analysis Performed:**
  - The examiner went to the system owner's (AntiRenzik) profile folder, then proceeded to the Downloads directory, and then there was a docx file named, "In order to ensure that Renzik is treated properly.docx".
  - The examiner then right clicked on the docx file and clicked "View file in timeline…", then chose "File Created" and 1 hour before and after the date, which showed the Timeline tab as shown in Figure 19.
- **Answer:**
  The source of the zip file, "takeout-20191112T181254Z-001", was from **https://storage.cloud.google.com/dataliberation/20191112T**, as shown in Figure 19.

- **Supporting Evidence:**



Display Times In: ● Local Time Zone ○ GMT / UTC

□ Must include text:
□ Must be tagged
□ Must have hash hit
□ Limit data sources to
□ device1laptop.e01 (ID: 1)
□ Limit file types to
□ Media
□ Documents
□ Executables
□ Other
□ Limit event types to
□ File System

Date/Time	Event Type	Description
2019-11-12 14:18:53	A__	/Windows/WinSxS/amd64_microsoft-window ... 2.1_none_310c22526466985f/sylfaen.ttf
2019-11-12 14:18:53	A__	/Windows/WinSxS/amd64_microsoft-windo ... 62.1_none_a0d93ea9d94173f1/ebrima.ttf
2019-11-12 14:18:53	A__	/Windows/WinSxS/amd64_microsoft-windo ... .1_none_d7f8d6a6ed2e5987/NirmalaS.ttf
2019-11-12 14:18:54	A__	/Windows/System32/msidle.dll
2019-11-12 14:18:54	Web Downloads	https://storage.cloud.google.com/datalib ... /1/a2f5ecfd-5e9b-4150-8d80-a332a09f7629
2019-11-12 14:18:54	Web Downloads	https://00e9e64bac44d92a9181ccae25f7f ... 1ZIPslbKGP91zDhHJejub0zgkHP8vE2K3KOV
2019-11-12 14:18:54	_B_	/$Recycle.Bin/S-1-5-21-2274644105-2924306947-3431561117-1001/$RIL1DWH.zip
2019-11-12 14:18:54	A__	/Windows/WinSxS/amd64_microsoft-window ... 62.1_none_9ddf4cd61fdf552a/msidle.dll
2019-11-12 14:18:54	A__	/Windows/Prefetch/SEARCHPROTOCOLHOST.EXE-C6CFE2A8.pf
2019-11-12 14:18:54	_B_	/Users/AntiRenzik/Downloads/takeout-20191112T181254Z-001.zip
2019-11-12 14:18:54	_B_	/$Recycle.Bin/S-1-5-21-2274644105-29243 ... 61117-1001/$RIL1DWH.zip:Zone.Identifier
2019-11-12 14:18:54	AC_M	/Users/AntiRenzik/AppData/Local/Google/Chrome/User Data/Default/Cache/data_2

Start: Nov 12, 2019, 1:48:54 PM

Usage

Downloaded from: URL https://takeout.google.com/settings/takeout/downloads?us

Downloaded from: URL https://takeout.google.com/settings/takeout/download?i=0

Downloaded from: URL https://storage.cloud.google.com/dataliberation/20191112T

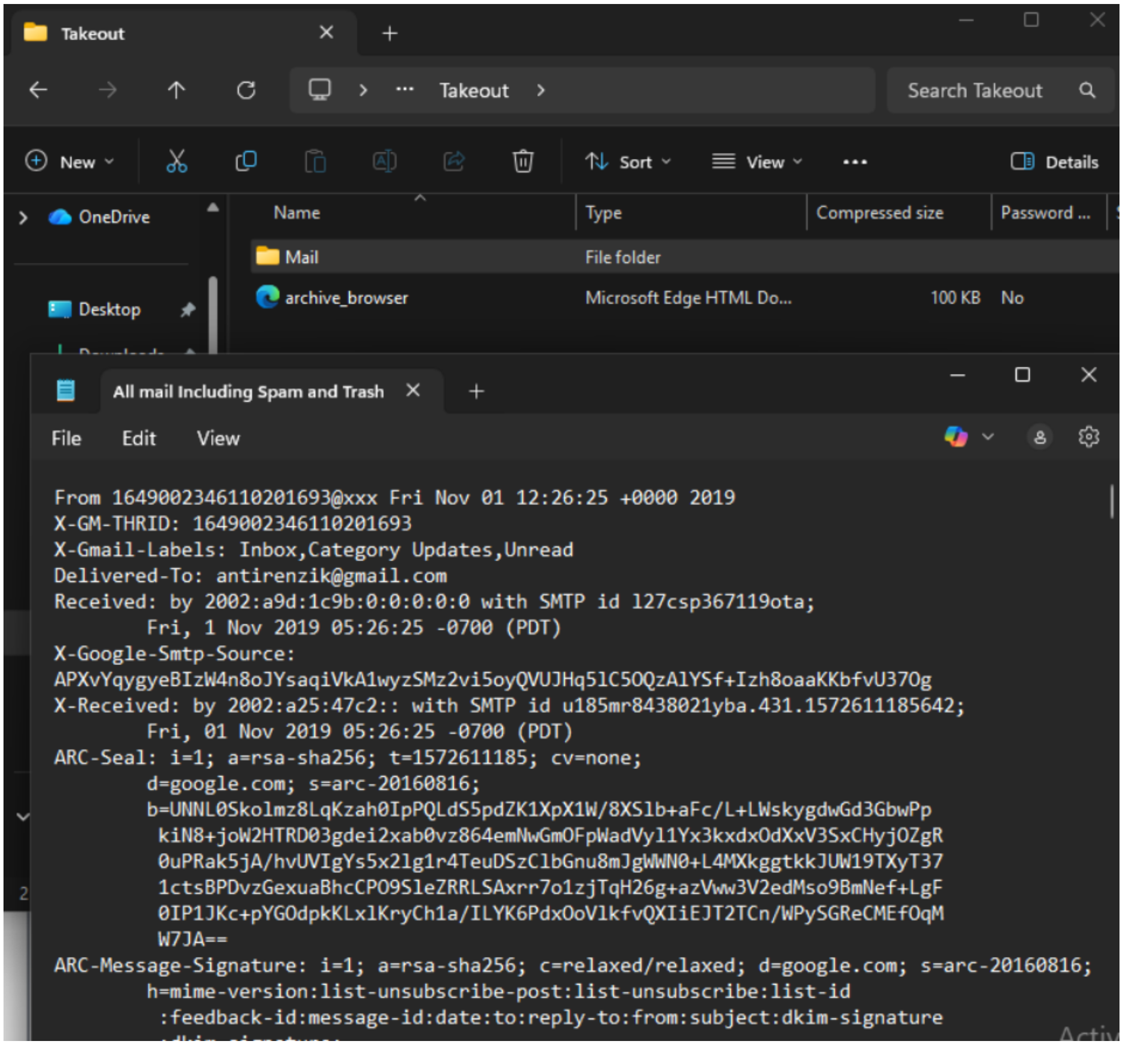
Downloaded from: URL https://00e9e64bac44d92a9181ccae25f7f134efd8a1c548c5248

Figure 19. The source of the "takeout-20191112T181254Z-001" zip file

18. What was the suspect doing? (zip file)

- **Analysis Performed:**
    - The examiner extracted the zip file onto the system and viewed the contents, as shown in Figure 20
- **Answer:**
  The suspect had downloaded a Google Takeout archive and was reviewing the exported Gmail mailbox contents, including raw email header data stored as TXT files, as shown in Figure 20.

- **Supporting Evidence:**



Name	Type	Compressed size	Password ...
Mail	File folder		
archive_browser	Microsoft Edge HTML Do...	100 KB	No

```
From 1649002346110201693@xxx Fri Nov 01 12:26:25 +0000 2019
X-GM-THRID: 1649002346110201693
X-Gmail-Labels: Inbox,Category Updates,Unread
Delivered-To: antirenzik@gmail.com
Received: by 2002:a9d:1c9b:0:0:0:0:0 with SMTP id 127csp367119ota;
        Fri, 1 Nov 2019 05:26:25 -0700 (PDT)
X-Google-Smtp-Source:
APXvYqygyeBIzW4n8oJYsaqiVkA1wyzSMz2vi5oyQVUJHq51C5OQzAlYSf+Izh8oaaKKbfvU37Og
X-Received: by 2002:a25:47c2:: with SMTP id u185mr8438021yba.431.1572611185642;
        Fri, 01 Nov 2019 05:26:25 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1572611185; cv=none;
        d=google.com; s=arc-20160816;
        b=UNNL0Skolmz8LqKzah0IpPQLdS5pdZK1XpX1W/8XSlb+aFc/L+LWskygdwGd3GbwPp
         kiN8+joW2HTRD03gdei2xab0vz864emNwGmOFpWadVyl1Yx3kxdxOdXxV3SxCHyjOZgR
         0uPRak5jA/hvUVIgYs5x2lg1r4TeuDSzClbGnu8mJgWWN0+L4MXkggtkkJUW19TXyT37
         1ctsBPDvzGexuaBhcCPO9SleZRRLSAxrr7o1zjTqH26g+azVww3V2edMso9BmNef+LgF
         0IP1JKc+pYGOdpkKLxlKryCh1a/ILYK6PdxOoVlkfvQXIiEJT2TCn/WPySGReCMEfOqM
         W7JA==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=mime-version:list-unsubscribe-post:list-unsubscribe:list-id
         :feedback-id:message-id:date:to:reply-to:from:subject:dkim-signature
```

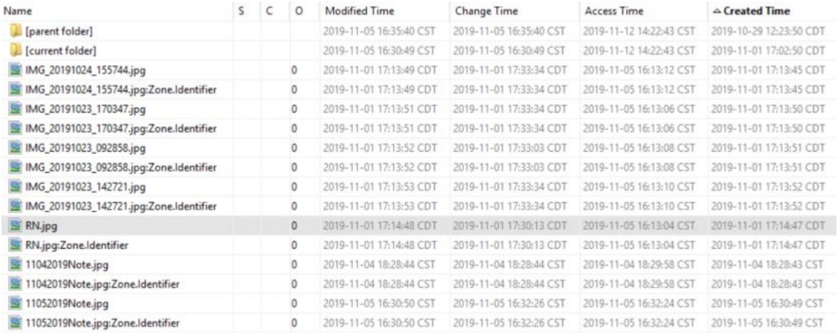
Figure 20. Opening the contents of the zip file

Media Analysis

19. What is the creation date timestamp of the FIRST ransom note?

- **Analysis Performed:**
  - The examiner went to the system owner's (AntiRenzik) profile folder, then proceeded to the Desktop directory, and then there was a directory called "Pictures" that contains several images of the victim and ransom notes, as shown in Figure 21.
- **Answer:**
  The creation date timestamp of the FIRST ransom note is **2019-11-01 17:14:47 CDT**, as shown in Figure 21.

- **Supporting Evidence:**



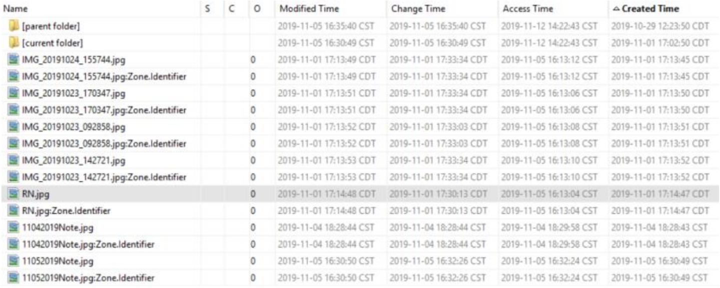
Name	S	C	O	Modified Time	Change Time	Access Time	▵ Created Time
[parent folder]				2019-11-05 16:35:40 CST	2019-11-05 16:35:40 CST	2019-11-12 14:22:43 CST	2019-10-29 12:23:50 CDT
[current folder]				2019-11-05 16:30:49 CST	2019-11-05 16:30:49 CST	2019-11-12 14:22:43 CST	2019-11-01 17:02:50 CDT
IMG_20191024_155744.jpg			0	2019-11-01 17:13:49 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:12 CST	2019-11-01 17:13:45 CDT
IMG_20191024_155744.jpg:Zone.Identifier			0	2019-11-01 17:13:49 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:12 CST	2019-11-01 17:13:45 CDT
IMG_20191023_170347.jpg			0	2019-11-01 17:13:51 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:06 CST	2019-11-01 17:13:50 CDT
IMG_20191023_170347.jpg:Zone.Identifier			0	2019-11-01 17:13:51 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:06 CST	2019-11-01 17:13:50 CDT
IMG_20191023_092858.jpg			0	2019-11-01 17:13:52 CDT	2019-11-01 17:33:03 CDT	2019-11-05 16:13:08 CST	2019-11-01 17:13:51 CDT
IMG_20191023_092858.jpg:Zone.Identifier			0	2019-11-01 17:13:52 CDT	2019-11-01 17:33:03 CDT	2019-11-05 16:13:08 CST	2019-11-01 17:13:51 CDT
IMG_20191023_142721.jpg			0	2019-11-01 17:13:53 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:10 CST	2019-11-01 17:13:52 CDT
IMG_20191023_142721.jpg:Zone.Identifier			0	2019-11-01 17:13:53 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:10 CST	2019-11-01 17:13:52 CDT
RN.jpg			0	2019-11-01 17:14:48 CDT	2019-11-01 17:30:13 CDT	2019-11-05 16:13:04 CST	2019-11-01 17:14:47 CDT
RN.jpg:Zone.Identifier			0	2019-11-01 17:14:48 CDT	2019-11-01 17:30:13 CDT	2019-11-05 16:13:04 CST	2019-11-01 17:14:47 CDT
11042019Note.jpg			0	2019-11-04 18:28:44 CST	2019-11-04 18:28:44 CST	2019-11-04 18:29:58 CST	2019-11-04 18:28:43 CST
11042019Note.jpg:Zone.Identifier			0	2019-11-04 18:28:44 CST	2019-11-04 18:28:44 CST	2019-11-04 18:29:58 CST	2019-11-04 18:28:43 CST
11052019Note.jpg			0	2019-11-05 16:30:50 CST	2019-11-05 16:32:26 CST	2019-11-05 16:32:24 CST	2019-11-05 16:30:49 CST
11052019Note.jpg:Zone.Identifier			0	2019-11-05 16:30:50 CST	2019-11-05 16:32:26 CST	2019-11-05 16:32:24 CST	2019-11-05 16:30:49 CST

Figure 21. Directory that includes several images of the victim and ransom notes. Highlighting the FIRST ransom note.

20. How many ransom notes are on this system?

- **Analysis Performed:**
  - The examiner went to the system owner's (AntiRenzik) profile folder, then proceeded to the Desktop directory, and then there was a directory called "Pictures" that contains several images of the victim and ransom notes, as shown in Figure 22.
- **Answer:**
  There are **three** ransom notes that are on the system, as shown in Figure 22.

- **Supporting Evidence:**



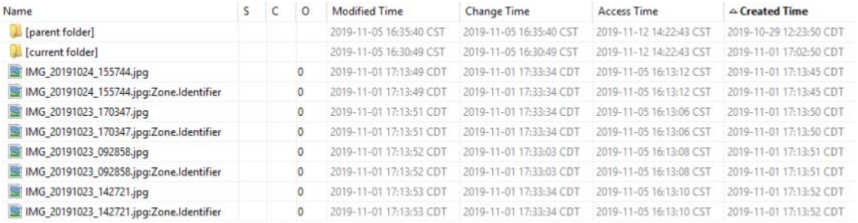
Name	S	C	O	Modified Time	Change Time	Access Time	▵ Created Time
[parent folder]				2019-11-05 16:35:40 CST	2019-11-05 16:35:40 CST	2019-11-12 14:22:43 CST	2019-10-29 12:23:50 CDT
[current folder]				2019-11-05 16:30:49 CST	2019-11-05 16:30:49 CST	2019-11-12 14:22:43 CST	2019-11-01 17:02:50 CDT
IMG_20191024_155744.jpg			0	2019-11-01 17:13:49 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:12 CST	2019-11-01 17:13:45 CDT
IMG_20191024_155744.jpg:Zone.Identifier			0	2019-11-01 17:13:49 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:12 CST	2019-11-01 17:13:45 CDT
IMG_20191023_170347.jpg			0	2019-11-01 17:13:51 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:06 CST	2019-11-01 17:13:50 CDT
IMG_20191023_170347.jpg:Zone.Identifier			0	2019-11-01 17:13:51 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:06 CST	2019-11-01 17:13:50 CDT
IMG_20191023_092858.jpg			0	2019-11-01 17:13:52 CDT	2019-11-01 17:33:03 CDT	2019-11-05 16:13:08 CST	2019-11-01 17:13:51 CDT
IMG_20191023_092858.jpg:Zone.Identifier			0	2019-11-01 17:13:52 CDT	2019-11-01 17:33:03 CDT	2019-11-05 16:13:08 CST	2019-11-01 17:13:51 CDT
IMG_20191023_142721.jpg			0	2019-11-01 17:13:53 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:10 CST	2019-11-01 17:13:52 CDT
IMG_20191023_142721.jpg:Zone.Identifier			0	2019-11-01 17:13:53 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:10 CST	2019-11-01 17:13:52 CDT
RN.jpg			0	2019-11-01 17:14:48 CDT	2019-11-01 17:30:13 CDT	2019-11-05 16:13:04 CST	2019-11-01 17:14:47 CDT
RN.jpg:Zone.Identifier			0	2019-11-01 17:14:48 CDT	2019-11-01 17:30:13 CDT	2019-11-05 16:13:04 CST	2019-11-01 17:14:47 CDT
11042019Note.jpg			0	2019-11-04 18:28:44 CST	2019-11-04 18:28:44 CST	2019-11-04 18:29:58 CST	2019-11-04 18:28:43 CST
11042019Note.jpg:Zone.Identifier			0	2019-11-04 18:28:44 CST	2019-11-04 18:28:44 CST	2019-11-04 18:29:58 CST	2019-11-04 18:28:43 CST
11052019Note.jpg			0	2019-11-05 16:30:50 CST	2019-11-05 16:32:26 CST	2019-11-05 16:32:24 CST	2019-11-05 16:30:49 CST
11052019Note.jpg:Zone.Identifier			0	2019-11-05 16:30:50 CST	2019-11-05 16:32:26 CST	2019-11-05 16:32:24 CST	2019-11-05 16:30:49 CST

Figure 22. Directory that includes several images of the victimand ransom notes.

21. How many images are there of the victim?

- **Analysis Performed:**
  - The examiner went to the system owner's (AntiRenzik) profile folder, then proceeded to the Desktop directory, and then there was a directory called "Pictures" that contains several images of the victim and ransom notes, as shown in Figure 23.
- **Answer:**
  There are **four** images of the victim, as shown in Figure 23.

- **Supporting Evidence:**



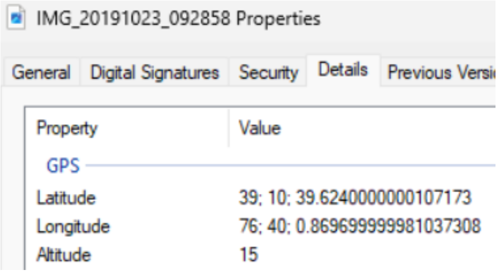
Name	S	C	O	Modified Time	Change Time	Access Time	▵ Created Time
[parent folder]				2019-11-05 16:35:40 CST	2019-11-05 16:35:40 CST	2019-11-12 14:22:43 CST	2019-10-29 12:23:50 CDT
[current folder]				2019-11-05 16:30:49 CST	2019-11-05 16:30:49 CST	2019-11-12 14:22:43 CST	2019-11-01 17:02:50 CDT
IMG_20191024_155744.jpg			0	2019-11-01 17:13:49 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:12 CST	2019-11-01 17:13:45 CDT
IMG_20191024_155744.jpg:Zone.Identifier			0	2019-11-01 17:13:49 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:12 CST	2019-11-01 17:13:45 CDT
IMG_20191023_170347.jpg			0	2019-11-01 17:13:51 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:06 CST	2019-11-01 17:13:50 CDT
IMG_20191023_170347.jpg:Zone.Identifier			0	2019-11-01 17:13:51 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:06 CST	2019-11-01 17:13:50 CDT
IMG_20191023_092858.jpg			0	2019-11-01 17:13:52 CDT	2019-11-01 17:33:03 CDT	2019-11-05 16:13:08 CST	2019-11-01 17:13:51 CDT
IMG_20191023_092858.jpg:Zone.Identifier			0	2019-11-01 17:13:52 CDT	2019-11-01 17:33:03 CDT	2019-11-05 16:13:08 CST	2019-11-01 17:13:51 CDT
IMG_20191023_142721.jpg			0	2019-11-01 17:13:53 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:10 CST	2019-11-01 17:13:52 CDT
IMG_20191023_142721.jpg:Zone.Identifier			0	2019-11-01 17:13:53 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:10 CST	2019-11-01 17:13:52 CDT

Figure 23. Directory that includes several images of the victim and ransom notes.

22. According to EXIF data, where was the victim taken to?

- **Analysis Performed:**
  - The examiner went to the system owner's (AntiRenzik) profile folder, then proceeded to the Desktop directory, and then there was a directory called "Pictures" that contains several images of the victim and ransom notes.
  - The examiner then proceeded to export all of the images of the victims to look at the EXIF data to see the GPS coordinates.
  - Then the examiner inputted the GPS coordinates of the images that made the GPS information available, into Google Maps (OSINT).
- **Answer:**
  The victim was taken to the **Baltimore/Washington International Airport (39°10'39.6"N 76°40'00.9"W)** as shown in the EXIF data and Google Maps search in Figure 24 and 25. The victim was taken to **a building in New Orleans, Louisiana (29°57'01.0"N 90°03'59.0"W)** as shown in the EXIF data and Google Maps search in Figure 26 and 27. The victim was taken to the **Lucy's Retired Surfers Bar & Restaurant (29°56'47.0"N 90°04'03.0"W)** as shown in the EXIF data and Google Maps search in Figure 28 and 29.

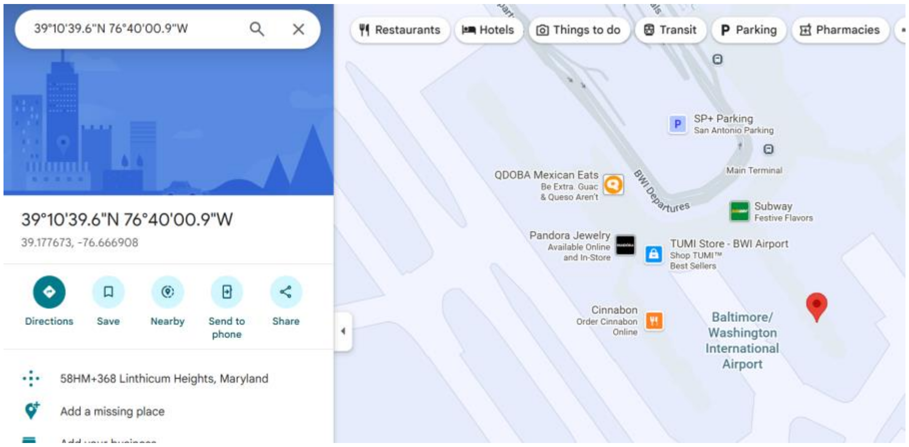
- **Supporting Evidence:**



IMG_20191023_092858 Properties

Property	Value
GPS	
Latitude	39; 10; 39.6240000000107173
Longitude	76; 40; 0.869699999981037308
Altitude	15

Figure 24. GPS coordinates of IMG_20191023_092858



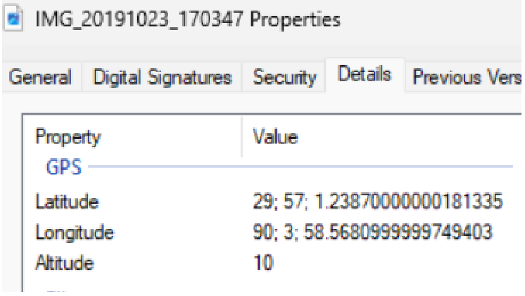
39°10'39.6"N 76°40'00.9"W

39°10'39.6"N 76°40'00.9"W
39.177673, -76.666908

58HM+368 Linthicum Heights, Maryland

Add a missing place

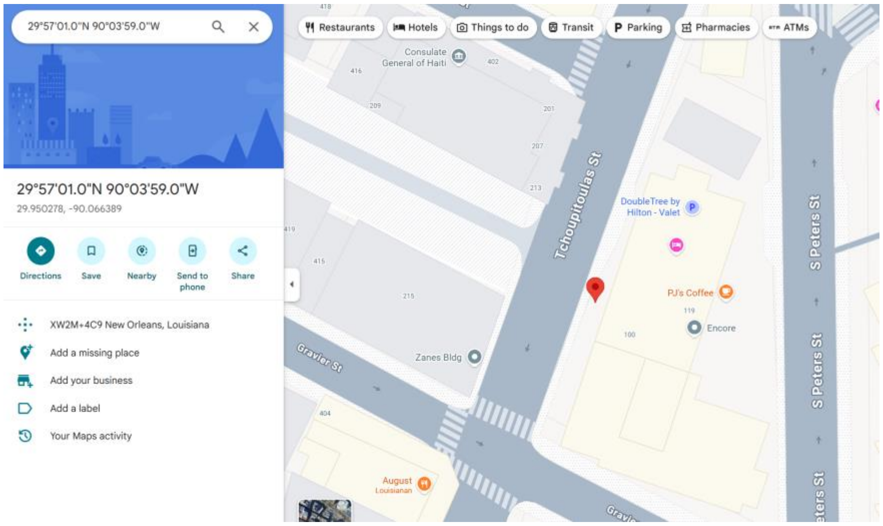
Figure 25. Google Maps search of the GPS coordinates from IMG_20191023_092858



IMG_20191023_170347 Properties

Property	Value
GPS	
Latitude	29; 57; 1.23870000000181335
Longitude	90; 3; 58.5680999999749403
Altitude	10

Figure 26. GPS coordinates of IMG_20191023_170347



29°57'01.0"N 90°03'59.0"W

29°57'01.0"N 90°03'59.0"W
29.950278, -90.066389

XW2M+4C9 New Orleans, Louisiana

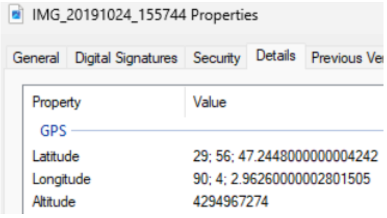
Add a missing place

Add your business

Add a label

Your Maps activity

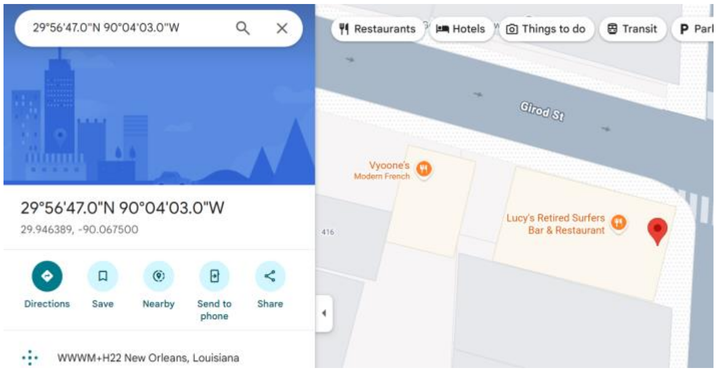
Figure 27. Google Maps search of the GPS coordinates from IMG_20191023_170347



IMG_20191024_155744 Properties

Property	Value
GPS	
Latitude	29; 56; 47.2448000000004242
Longitude	90; 4; 2.96260000002801505
Altitude	4294967274

Figure 28. GPS coordinates of IMG_20191024_155744



29°56'47.0"N 90°04'03.0"W

29°56'47.0"N 90°04'03.0"W
29.946389, -90.067500

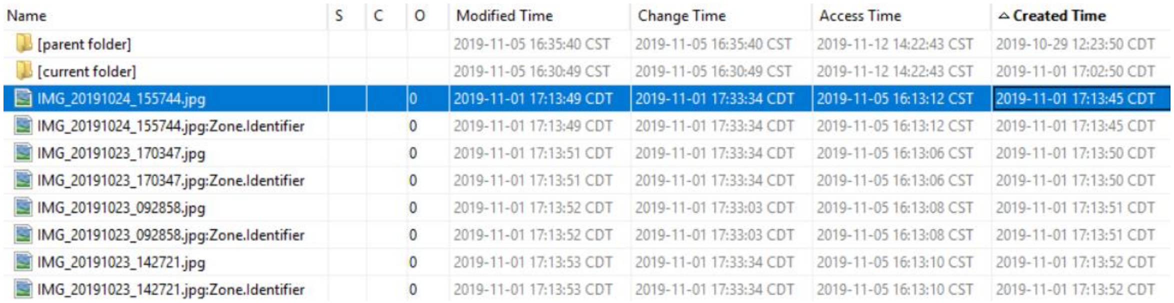
WWWM+H22 New Orleans, Louisiana

Figure 29. Google Maps search of the GPS coordinates from IMG_20191024_155744

23. Which of these locations occurred first?

- **Analysis Performed:**
  - The examiner went to the system owner's (AntiRenzik) profile folder, then proceeded to the Desktop directory, and then there was a directory called "Pictures" that contains several images of the victim and ransom notes, as shown in Figure 30.
  - The examiner highlighted the image that was created first, as shown in Figure 30.
- **Answer:**
  Whenever the victim was taken to the **Lucy's Retired Surfers Bar & Restaurant (29°56'47.0"N 90°04'03.0"W)** as shown in the EXIF data and Google Maps search in the previous question and Figure 29 and 30, **it was the first location** as shown in the date timestamps in Figure 30.

- **Supporting Evidence:**



Name	S	C	O	Modified Time	Change Time	Access Time	▵ Created Time
[parent folder]				2019-11-05 16:35:40 CST	2019-11-05 16:35:40 CST	2019-11-12 14:22:43 CST	2019-10-29 12:23:50 CDT
[current folder]				2019-11-05 16:30:49 CST	2019-11-05 16:30:49 CST	2019-11-12 14:22:43 CST	2019-11-01 17:02:50 CDT
IMG_20191024_155744.jpg			0	2019-11-01 17:13:49 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:12 CST	2019-11-01 17:13:45 CDT
IMG_20191024_155744.jpg:Zone.Identifier			0	2019-11-01 17:13:49 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:12 CST	2019-11-01 17:13:45 CDT
IMG_20191023_170347.jpg			0	2019-11-01 17:13:51 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:06 CST	2019-11-01 17:13:50 CDT
IMG_20191023_170347.jpg:Zone.Identifier			0	2019-11-01 17:13:51 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:06 CST	2019-11-01 17:13:50 CDT
IMG_20191023_092858.jpg			0	2019-11-01 17:13:52 CDT	2019-11-01 17:33:03 CDT	2019-11-05 16:13:08 CST	2019-11-01 17:13:51 CDT
IMG_20191023_092858.jpg:Zone.Identifier			0	2019-11-01 17:13:52 CDT	2019-11-01 17:33:03 CDT	2019-11-05 16:13:08 CST	2019-11-01 17:13:51 CDT
IMG_20191023_142721.jpg			0	2019-11-01 17:13:53 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:10 CST	2019-11-01 17:13:52 CDT
IMG_20191023_142721.jpg:Zone.Identifier			0	2019-11-01 17:13:53 CDT	2019-11-01 17:33:34 CDT	2019-11-05 16:13:10 CST	2019-11-01 17:13:52 CDT

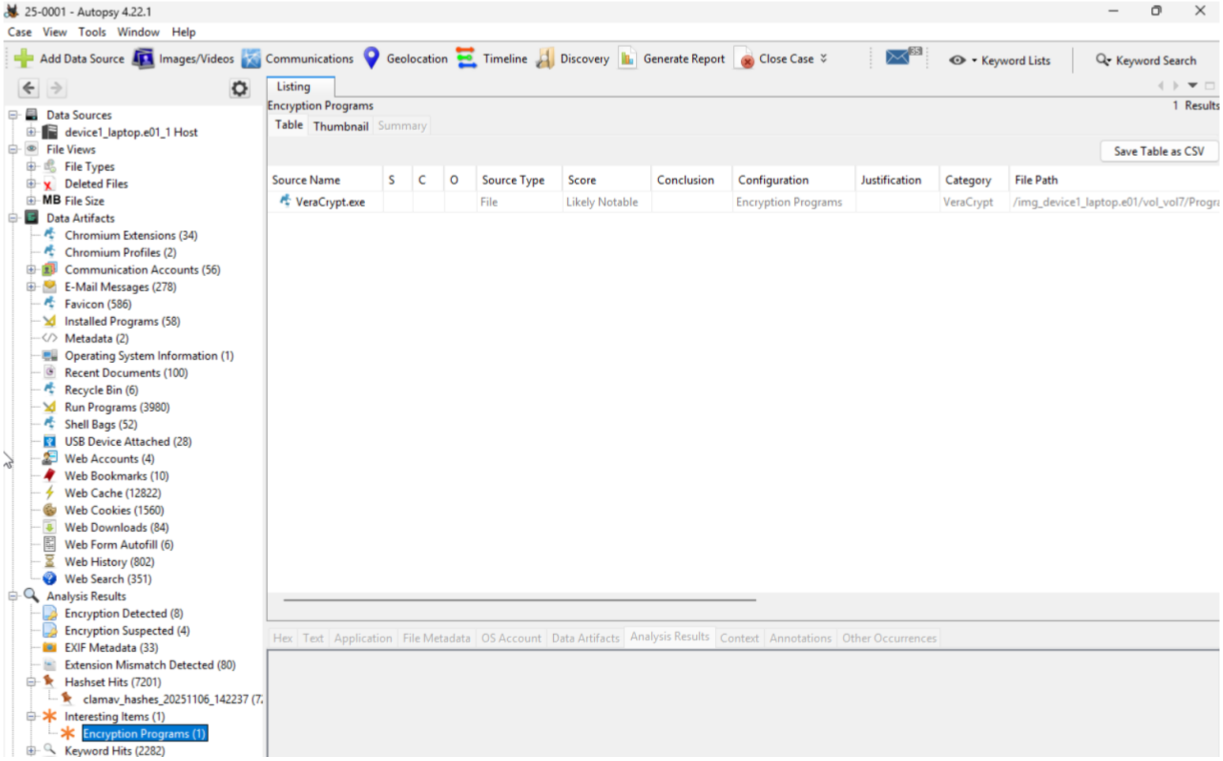
Figure 30. Directory that includes several images of the victim and ransom notes. Highlighting the image that occurred first.

Other Interesting Findings

24. According to Autopsy, there is a program that is used to encrypt files. What is the name of the program.

- **Analysis Performed:**
  - The examiner then ran all other ingest modules except for Plaso on the disk image within Autopsy.
  - The examiner then went to the Interesting Items section in Analysis Results that contains a section called, "Encryption Programs", as shown in Figure 31.
- **Answer:**
  According to Autopsy, there is a program that is used to encrypt files and the name of the file is **VeraCrypt**, as shown in Figure 31.

- **Supporting Evidence:**



Encryption Programs

1 Results

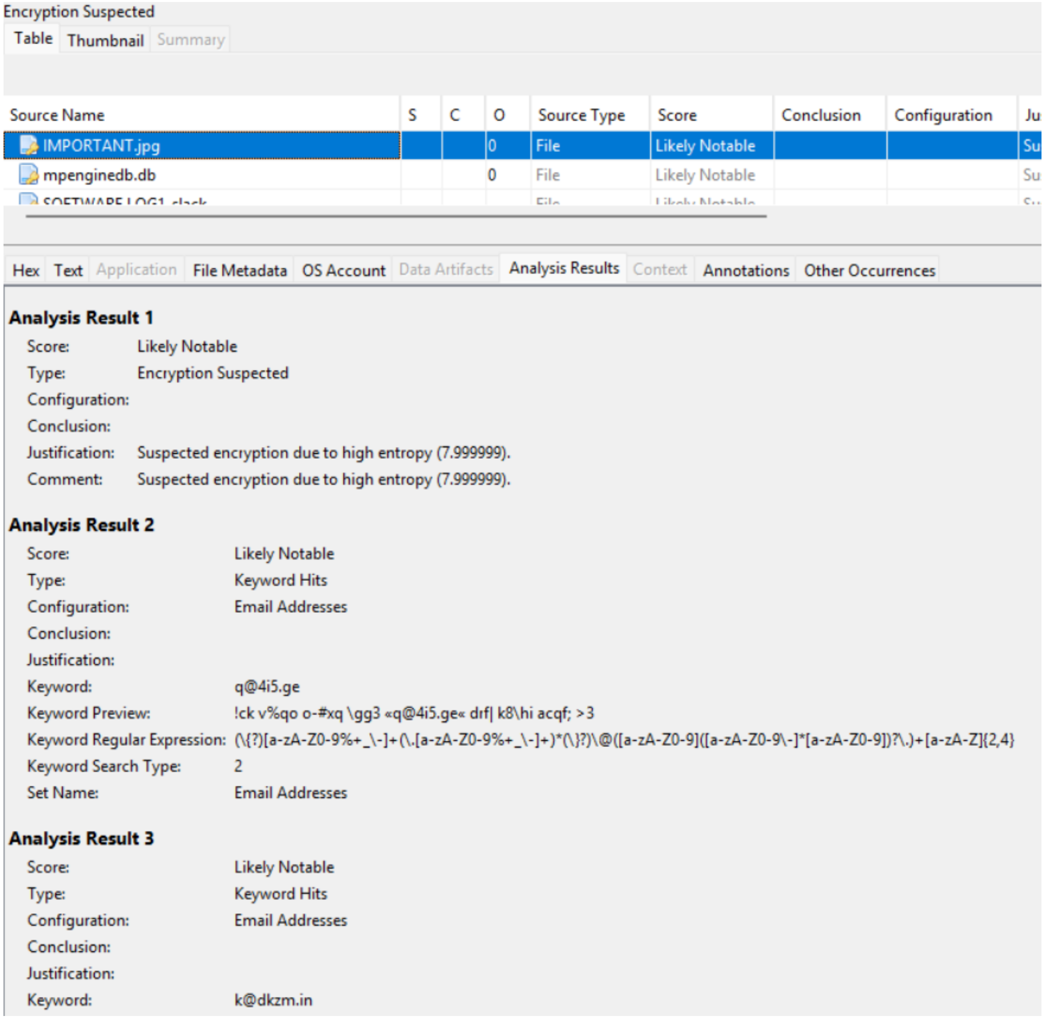
Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Justification	Category	File Path
VeraCrypt.exe				File	Likely Notable		Encryption Programs		VeraCrypt	/img_device1_laptop.e01/vol_vol7/Progr

Figure 31. The Encryption Programs analysis result in Autopsy

25. According to Autopsy, there is a file in the owner’s profile folder that maybe encrypted. What is the name of the file?

- **Analysis Performed:**
  - The examiner went to the Encryption Suspected section within Analysis Results to look for a file in the owner’s profile folder that is possibly encrypted, as shown in Figure 32.
- **Answer:**
  According to Autopsy, there is a file in the owner’s profile folder that is possibly encrypted, the name of the file is **IMPORTANT.jpg**, as shown in Figure 32.

- **Supporting Evidence:**



Source Name	S	C	O	Source Type	Score	Conclusion	Configuration	Ju
IMPORTANT.jpg			0	File	Likely Notable			Su
mpenginedb.db			0	File	Likely Notable			Su
SOFTWARE.LOG1-slack				File	Likely Notable			Su

Analysis Result 1

```
Score:          Likely Notable
Type:           Encryption Suspected
Configuration:
Conclusion:
Justification:  Suspected encryption due to high entropy (7.999999).
Comment:        Suspected encryption due to high entropy (7.999999).
```

Analysis Result 2

```
Score:                       Likely Notable
Type:                        Keyword Hits
Configuration:               Email Addresses
Conclusion:
Justification:
Keyword:                     q@4i5.ge
Keyword Preview:             !ck v%qo o-#xq \gg3 «q@4i5.ge« drf| k8\hi acqf; >3
Keyword Regular Expression:  (\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([a-zA-Z0-9]([a-zA-Z0-9\-]*[a-zA-Z0-9])?\.)+[a-zA-Z]{2,4}
Keyword Search Type:         2
Set Name:                    Email Addresses
```

Analysis Result 3

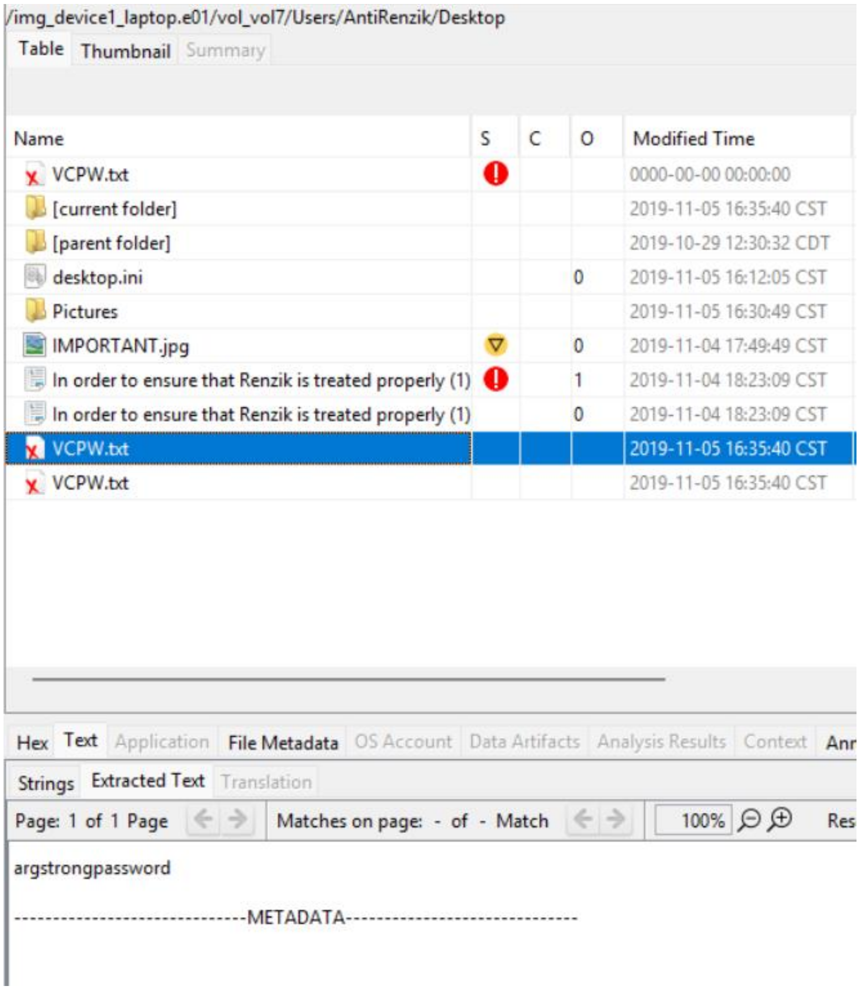
```
Score:                       Likely Notable
Type:                        Keyword Hits
Configuration:               Email Addresses
Conclusion:
Justification:
Keyword:                     k@dkzm.in
```

Figure 32. The Encryption Suspected analysis results section

26. What is the password to decrypt the file?

- **Analysis Performed:**
    - The examiner then went to the data source, specifically the Desktop folder within AntiRenzik's directory to look for the password to decrypt the file found previously, as shown in Figure 33.
- **Answer:**
  The password to decrypt the file is **argstrongpassword**, as shown in Figure 33.

- **Supporting Evidence:**



/img_device1_laptop.e01/vol_vol7/Users/AntiRenzik/Desktop

Name	S	C	O	Modified Time
VCPW.txt	!			0000-00-00 00:00:00
[current folder]				2019-11-05 16:35:40 CST
[parent folder]				2019-10-29 12:30:32 CDT
desktop.ini			0	2019-11-05 16:12:05 CST
Pictures				2019-11-05 16:30:49 CST
IMPORTANT.jpg	▽		0	2019-11-04 17:49:49 CST
In order to ensure that Renzik is treated properly (1)	!		1	2019-11-04 18:23:09 CST
In order to ensure that Renzik is treated properly (1)			0	2019-11-04 18:23:09 CST
VCPW.txt				2019-11-05 16:35:40 CST
VCPW.txt				2019-11-05 16:35:40 CST

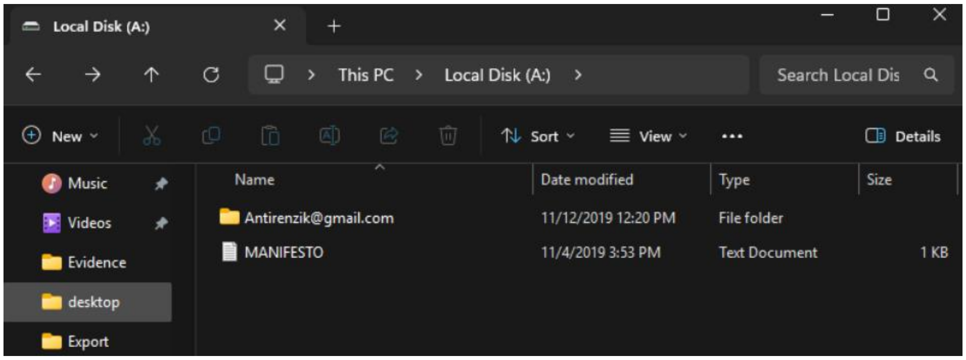
```
argstrongpassword

-----------------------------METADATA-----------------------------
```

Figure 33. The Text of VCPW.txt that contains the password to decrypt IMPORTANT.jpg

27. What is the name of the folder in the root of this container?

- **Analysis Performed:**
  - The examiner then went to the web to download VeraCrypt, a free open-source disk encryption software, to decrypt the file.
  - The examiner successfully mounted IMPORTANT.jpg to volume A: using the password found in the previous question, as shown in Figure 34.
- **Answer:**
  The name of the folder in the root of this container is **Antirenzik@gmail.com**, as shown in Figure 34.

- **Supporting Evidence:**



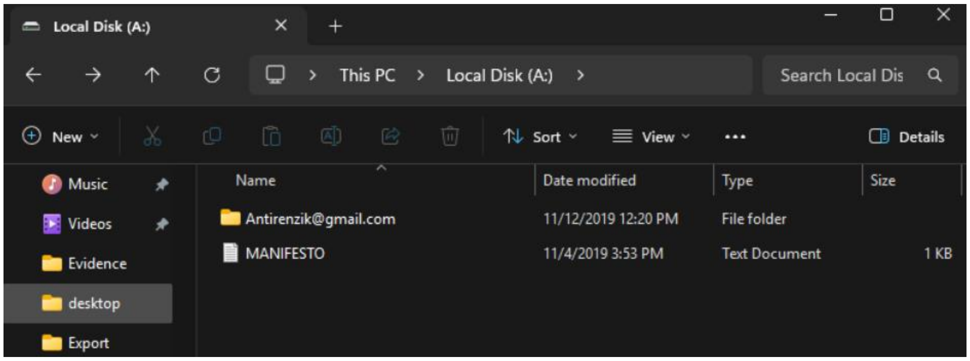
Name	Date modified	Type	Size
Antirenzik@gmail.com	11/12/2019 12:20 PM	File folder	
MANIFESTO	11/4/2019 3:53 PM	Text Document	1 KB

Figure 34. Showing the root directory of IMPORTANT.jpg after decryption

28. What is the name of the text file in the root of this container?

- **Analysis Performed:**
  - The examiner successfully mounted IMPORTANT.jpg to volume A: using the password found in question 26, as shown in Figure 35.
- **Answer:**
  The name of the text file in the root of this container is **MANIFESTO**, as shown in Figure 35.

- **Supporting Evidence:**



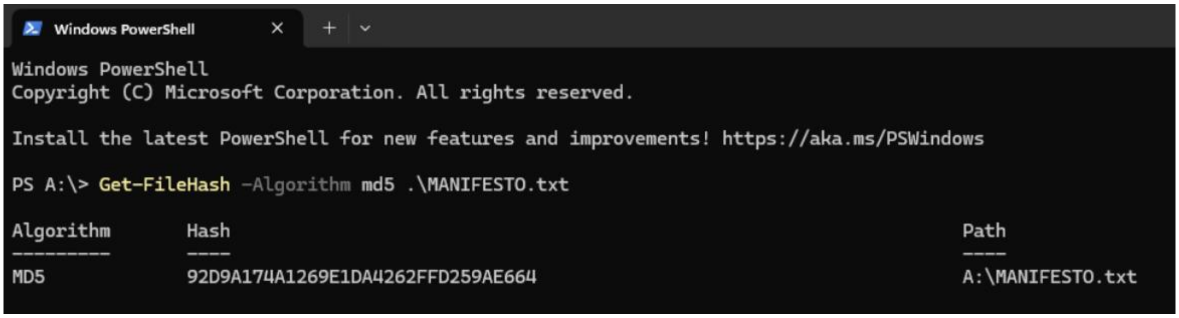
Name	Date modified	Type	Size
Antirenzik@gmail.com	11/12/2019 12:20 PM	File folder	
MANIFESTO	11/4/2019 3:53 PM	Text Document	1 KB

Figure 35. Showing the root directory of IMPORTANT.jpg after decryption

29. What is the MD5 hash of the text file?

- **Analysis Performed:**
  - The examiner opened a Windows Powershell terminal within the root of the container to get the MD5 hash of MANIFESTO.txt, as shown in Figure 36.
- **Answer:**
  The MD5 hash of the text file (MANIFESTO.txt) is **92D9a174A1269E1DA4262FFD259AE664**, as shown in Figure 36.

- **Supporting Evidence:**



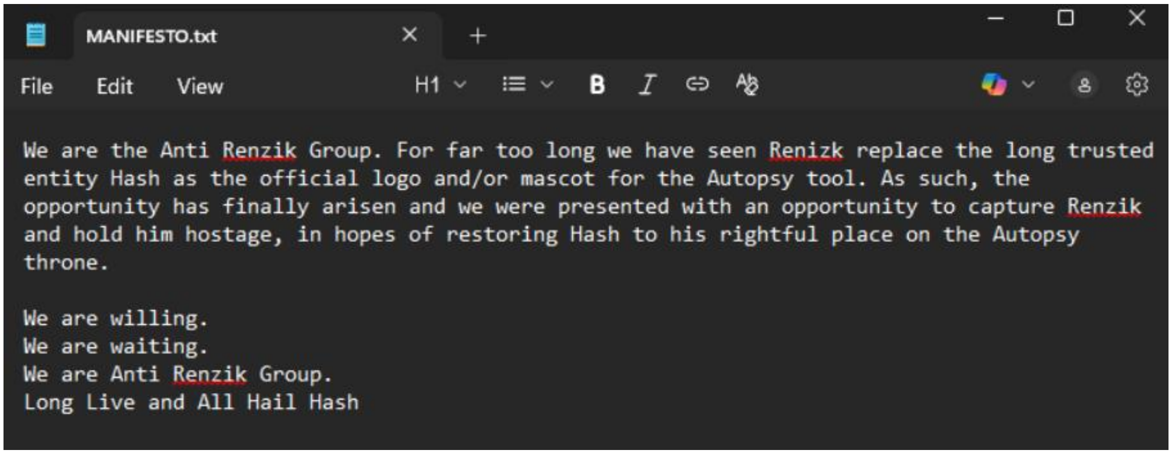
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS A:\> Get-FileHash -Algorithm md5 .\MANIFESTO.txt

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             92D9A174A1269E1DA4262FFD259AE664                                       A:\MANIFESTO.txt
```

Figure 36. Windows Powershell Terminal within the root of the container to get the MD5 hash of MANIFESTO.txt

30. What is the name of the victim (dog)?

- **Analysis Performed:**
  - The examiner then accessed MANIFESTO.txt via Notepad, as shown in Figure 37.
- **Answer:**
  The name of the victim (dog) is **Renzik**, as shown in Figure 37.

- **Supporting Evidence:**



We are the Anti Renzik Group. For far too long we have seen Renizk replace the long trusted entity Hash as the official logo and/or mascot for the Autopsy tool. As such, the opportunity has finally arisen and we were presented with an opportunity to capture Renzik and hold him hostage, in hopes of restoring Hash to his rightful place on the Autopsy throne.

We are willing.
We are waiting.
We are Anti Renzik Group.
Long Live and All Hail Hash

Figure 37. Examiner accessing MANIFESTO.txt via Notepad

Conclusion

The examiner, Inor Wang, enjoyed this lab. There is no critique from me. Thank you.

References

Carvey, H. A. (2014). Windows forensic analysis toolkit: Advanced analysis techniques for Windows 8 (Fourth edition). Syngress.

Johansen, G., & Safari, an O. M. C. (2020). Digital Forensics and Incident Response—Second Edition.

Ligh, M. H., Case, A., Levy, J., & Walters, A. (2014). The art of memory forensics: Detecting malware and threats in Windows, Linux, and Mac memory. Wiley.

Malware forensics field guide for Windows systems digital forensics field guides. (2012). Syngress.

Oettinger, W., & Safari, an O. M. C. (2020). Learn Computer Forensics.

Reddy, N. (2019). Practical cyber forensics: An incident-based approach to forensic investigations. APress. https://doi.org/10.1007/978-1-4842-4460-9.

VeraCrypt Project. (2025). *VeraCrypt*. https://veracrypt.io/en/Downloads.html.