# Digital Forensics Report

Prepared for: Felix Pichard

Created by : Anastasia Cotorobai
Yanis Alim

Master 2 - MSIP9

28/10/2020

SCIENCES SORBONNE UNIVERSITÉ

AFORP FORMATION CENTRE DE FORMATION INDUSTRIEL ET TECHNOLOGIQUE

# Summary

# 1. Introduction

The purpose of this report is to provide corroborative evidence of the motivation, opportunity and intent leading to the theft of the dog Renzik. The facts presented within this report are those presented within this report are those within the preparer's own area of expertise and knowledge and do not extend to matters and knowledge outside such expertise.

## 1.1. Summary of case and tasking

In the period between October and November 2020, a case was open for the theft of the dog Renzik.

Our purpose is to find all the necessary evidence that can help us to establish the truth.

We are especially searching for digital artefacts that can lead us to the suspect(s) identity and dog location.

## 1.2. Statement of compliance

We understand our duty as an expert witness to provide independent assistance by way of objective unbiased opinion in relation to matters within my expertise. We will inform all parties if our opinion changes.

# 2. Forensic Examination

All examinations, measurements, tests and experiments related to the Digital image of the accused's computer were performed by the expert and we have summarised our findings on which the expert relies.

## 2.1. Tools

The forensic tools employed in the performance if this investigation were as follows :

- **FTK Imager :**

  FTK Imager is an imaging and data preview tool by AccessData which allows an examiner not only to create forensic images in different formats, including RAW, SMART, E01, and AFF, but also to preview data sources in a forensically sound manner.

  It was used by Felix Pichard to safely create a copy of the suspect's computer and sdcard.

- **Autopsy :**

  Open source Digital Forensics Software which provides investigators with the tools to conduct complex investigations with accuracy and efficiency. It allows completely non-invasive computer forensic investigations while allowing examiners to easily manage large volumes of computer evidence and view computer drive contents including files, operating system artefacts, file system artefacts, and deleted files or file fragments located in file slack or unallocated space.

To the experts knowledge, there is no software above that possesses any material issues whose severity would invalidate the findings thereof.

## 2.2. Chain of Custody

**_LENOVO_PC**

**Consultant: (Name/ID#):** Yanis Alim ID_NO_31337 , Anastasia Cotorobai ID_NO_1337

**Client:** University of Pierre & Marie-Curie

**Auditee:** Lenovo PC used by AntiRenzik

**Date/Time of Custody:** 11:00 am, 28 October 2020

**Location of Seizure**: 48 Boulevard des Batignolles, 75017 Paris

| **Description of Evidence** | | |
|---|---|---|
| **Item #** | **Quantity** | **Description of Item (Model, Serial #, Marks, Scratches)** |
| 1 | 1 | Lenovo Thinkpad HDD Model ATA ST500DM002-1BD14 |
| | | Serial No: W3T9K3YD |
| | | Size 500GB |

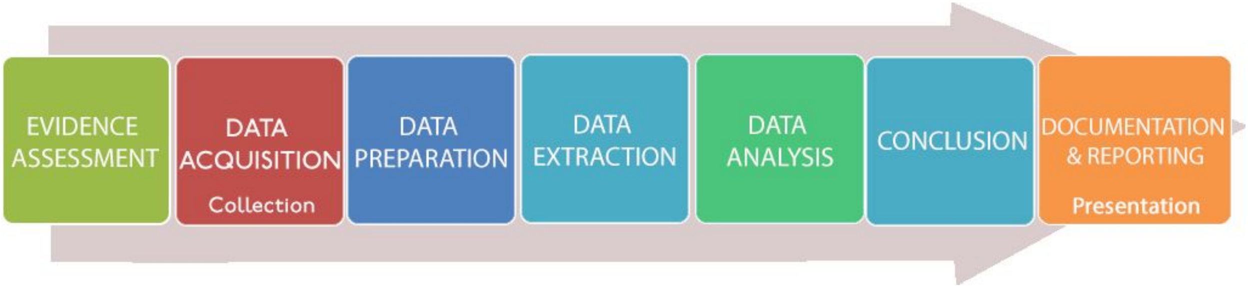
| **Chain of Custody** | | | | |
|---|---|---|---|---|
| **Item #** | **Date/Time** | **Released by** | **Received by** | **Comments** |
| 1 | 04:00 pm 26/10/2020 | Felix Pichard | Felix Pichard | Pc had been accessed prior to imaging in order to create a safe copy.<br>Impact on integrity of data will be assessed through metadata tag analysis<br>Impact of integrity on deleted artifacts to be assessed during recovery process<br>Location: PC was not moved, it was turned on at the time of arrival. Imaging of the PC was done through FTK Imager without shutting down the PC.<br>Further alterations to the system were therefore avoided by preventing the shutdown. |
| 1 | 02:00 pm 27/10/2020 | Anastasia Cotorobai | Felix Pichard | Image: **device1_laptop.e01**<br>Size: **42 949 672 960 bytes** |

| | | | | |
|---|---|---|---|---|
| | | | | 0 bad sectors found<br>MD5 :<br>**dc176d653c5613e305e831525e874090**<br>SHA1:<br>**87e09a16becf8a5db1d18804e29954309c87abf6** |
| 1 | 02:00 pm<br>27/10/2020 | Yanis Alimi | Felix Pichard | Image: **device2_mediacrd.e01**<br>Size: **9170 908  bytes**<br>0 bad sectors found<br>MD5 :<br>**c8343d3976eec2985e7580a2b6321591**<br>SHA1:<br>**826bdc5346f77c62251927e598fe066fe460ce24** |

## 2.3. Policy & Procedure Development

As the primary aim of any digital forensics investigation is to allow others to follow the same procedures and steps and still end with the same result and conclusions, considerable effort must be spent on developing policies and standard operating procedures (SOP) in how to deal with each step and phase of the investigation.

Our procedure is divided into 7 dependents steps :



## 2.4. Evidence Assessment

All sources of possible digital evidence should be thoroughly assessed with respect to the scope of the case. This will help establish the size of the investigation and determine the next steps.

In our case, the “computer” and the “media card” weren’t moved from their place and the digital forensic team came into place to do the assessment.

## 2.5. Data Acquisition

Digital evidence is fragile and can be easily altered, damaged, or destroyed by improper handling or examination. Even the act of opening files can alter timestamp information destroying information on when the file was last accessed. So special precautions are needed to preserve this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion..

When the forensics team arrived into the scene, they found the computer of the suspect turned on.

Felix Pichard did his best to not lose any valuable data and he did a copy of the computer with the media card without shutting down the computer, he used FTK Imager to create an Encase Image (E01) file of the computer and the media card .

The E01 file keeps backup of various types of acquired digital evidence that includes disk imaging, storing of logical files, etc

## 2.6. Evidence Examination

The same general forensic principles apply when examining digital evidence as they do to any other crime scene. However, different types of cases and media may require different methods of examination.

It is important to distinguish between :

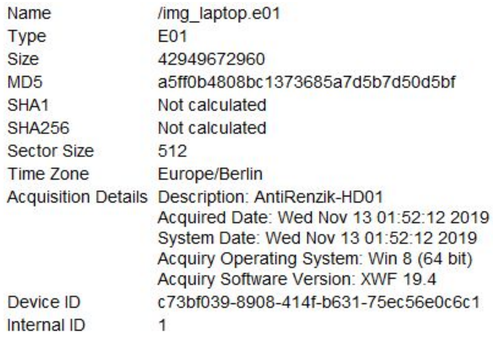
- **Extraction** refers to the recovery of data from whatever media the data is stored on.
- **Analysis** refers to the interpretation of the recovered data and placement of it in a logical and useful format, answering such questions as how did it get there, where did it come from, and what does it mean?

## Step 1: Preparation

Prepare working directory/directories on separate media to which evidentiary files and data can be recovered and/or extracted. These should be checked to make sure they are **'forensically clean'** so that investigators can be sure any evidence belongs to the case being investigated, rather than leftover from other cases.

We got the Encase Image File for the computer and media card from Felix Pichard at 10:00pm, 26/10/2020 and we did 2 copies for them for backup :

```
$ cp device1_laptop.e01 device1_laptop.e01_copy1
$ cp device1_laptop.e01 device1_laptop.e01_copy2
$ cp device2_mediacard.e01 device2_mediacard.e01_copy1
$ cp device2_mediacard.e01 device2_mediacard.e01_copy2
```



| | |
|---|---|
| Name | /img_laptop.e01 |
| Type | E01 |
| Size | 42949672960 |
| MD5 | a5ff0b4808bc1373685a7d5b7d50d5bf |
| SHA1 | Not calculated |
| SHA256 | Not calculated |
| Sector Size | 512 |
| Time Zone | Europe/Berlin |
| Acquisition Details | Description: AntiRenzik-HD01<br>Acquired Date: Wed Nov 13 01:52:12 2019<br>System Date: Wed Nov 13 01:52:12 2019<br>Acquiry Operating System: Win 8 (64 bit)<br>Acquiry Software Version: XWF 19.4 |
| Device ID | c73bf039-8908-414f-b631-75ec56e0c6c1 |
| Internal ID | 1 |

## Step 2: Extraction

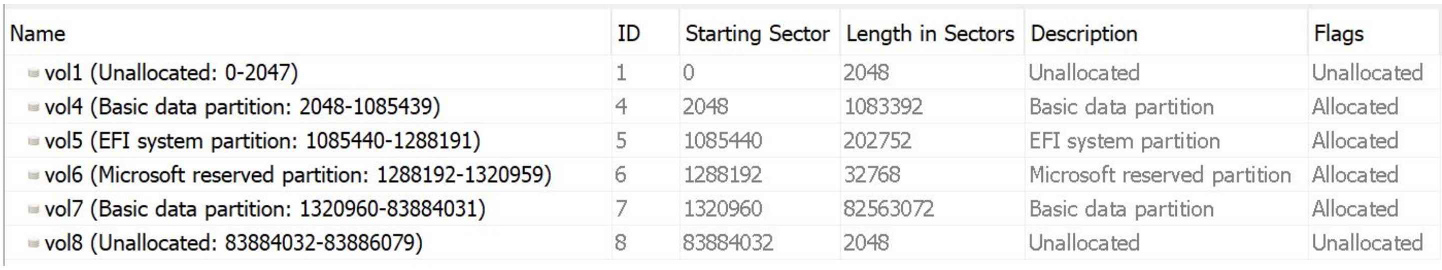
This is the actual process of extracting the data from digital devices. There are two different types of extraction, physical and logical.:

- **Physical extraction** phase: identifies and recovers data across the entire physical drive without regard to the file system. Essentially, any image is made and then subjected to the following methods: keyword searching, file carving, and extraction of the partition table and unused space on the physical drive.

  We can find the type of the partition system using *mmstat* as following:

```
tsurugi@lab:~$ mmstat device1_laptop.e01
gpt
```

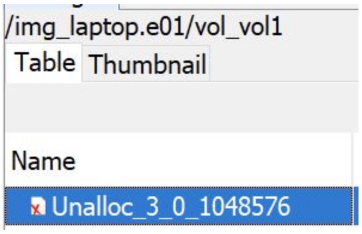
Using Autopsy, we could see:  that we have 6 partitions ( 4 allocated , 2 unallocated )



| Name | ID | Starting Sector | Length in Sectors | Description | Flags |
|---|---|---|---|---|---|
| vol1 (Unallocated: 0-2047) | 1 | 0 | 2048 | Unallocated | Unallocated |
| vol4 (Basic data partition: 2048-1085439) | 4 | 2048 | 1083392 | Basic data partition | Allocated |
| vol5 (EFI system partition: 1085440-1288191) | 5 | 1085440 | 202752 | EFI system partition | Allocated |
| vol6 (Microsoft reserved partition: 1288192-1320959) | 6 | 1288192 | 32768 | Microsoft reserved partition | Allocated |
| vol7 (Basic data partition: 1320960-83884031) | 7 | 1320960 | 82563072 | Basic data partition | Allocated |
| vol8 (Unallocated: 83884032-83886079) | 8 | 83884032 | 2048 | Unallocated | Unallocated |

The first partition (vol1) has an unallocated space with the name of  **"Unalloc_3_0_1048576"** :

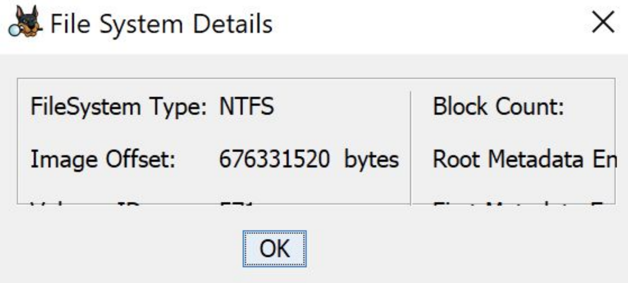
- Unalloc : means unallocated space
- 3 : the parent
- 0 : the start offset
- 1048576 : is the end offset



/img_laptop.e01/vol_vol1

Unalloc_3_0_1048576

The file system type of vol7 is the default file system of the Windows NT family: NTFS



File System Details

FileSystem Type: NTFS

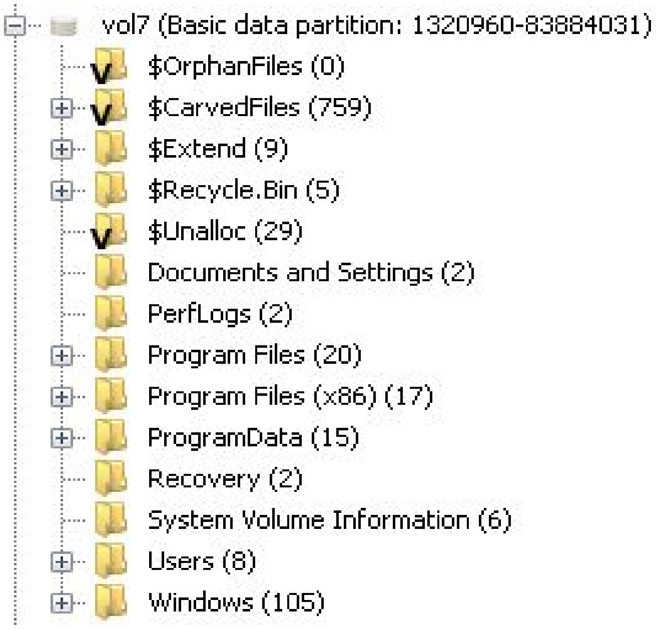
Image Offset: 676331520 bytes

Block Count:

Root Metadata En

- **Logical extraction** phase: identifies and recovers files and data based on the installed operating system(s), file system(s), and/or application(s). This will involve an examination of active files, recovering deleted files, looking at file slack (i.e unusual space between files) and unallocated file space: May contain remnants of deleted files not found during the recovery process.

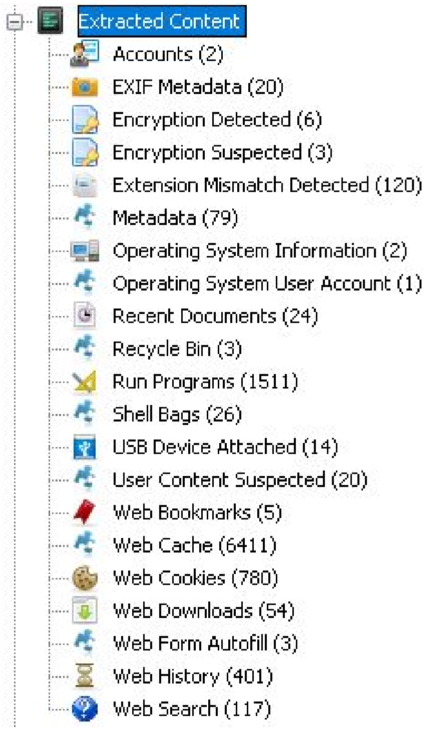
  Using autopsy data ingest module, we can view the file system information to reveal characteristics such as directory structure, file attributes, file names, date and time stamps, file size, and file location.



```
vol7 (Basic data partition: 1320960-83884031)
    $OrphanFiles (0)
    $CarvedFiles (759)
    $Extend (9)
    $Recycle.Bin (5)
    $Unalloc (29)
    Documents and Settings (2)
    PerfLogs (2)
    Program Files (20)
    Program Files (x86) (17)
    ProgramData (15)
    Recovery (2)
    System Volume Information (6)
    Users (8)
    Windows (105)
```

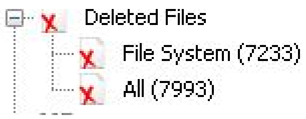
**Extraction of files pertinent to the examination :**

Methods to accomplish this may be based on file name and extension, file header, file content, and location on the drive :



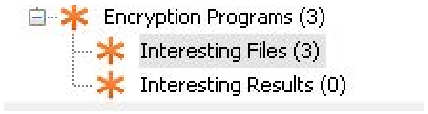
Extracted Content
- Accounts (2)
- EXIF Metadata (20)
- Encryption Detected (6)
- Encryption Suspected (3)
- Extension Mismatch Detected (120)
- Metadata (79)
- Operating System Information (2)
- Operating System User Account (1)
- Recent Documents (24)
- Recycle Bin (3)
- Run Programs (1511)
- Shell Bags (26)
- USB Device Attached (14)
- User Content Suspected (20)
- Web Bookmarks (5)
- Web Cache (6411)
- Web Cookies (780)
- Web Downloads (54)
- Web Form Autofill (3)
- Web History (401)
- Web Search (117)

Recovery of deleted files :

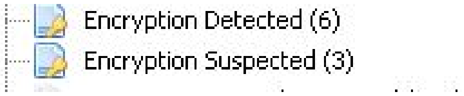


Deleted Files
- File System (7233)
- All (7993)

Extraction of password-protected, encrypted, and compressed data :



Encryption Programs (3)
- Interesting Files (3)
- Interesting Results (0)



- Encryption Detected (6)
- Encryption Suspected (3)

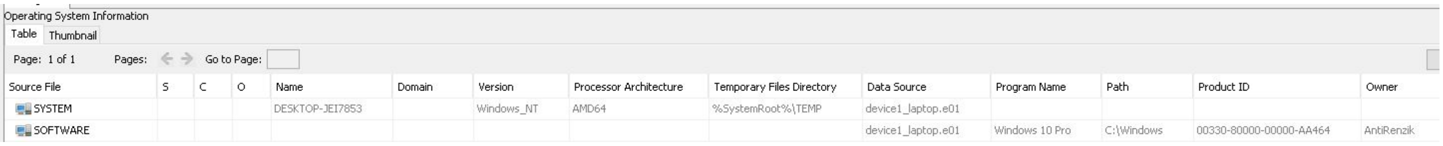
## Step 3: Analysis

Analysis is the process of interpreting the extracted data to determine their significance to the case. Various analytical methods exist, examples of which include:

- ### Applications and files

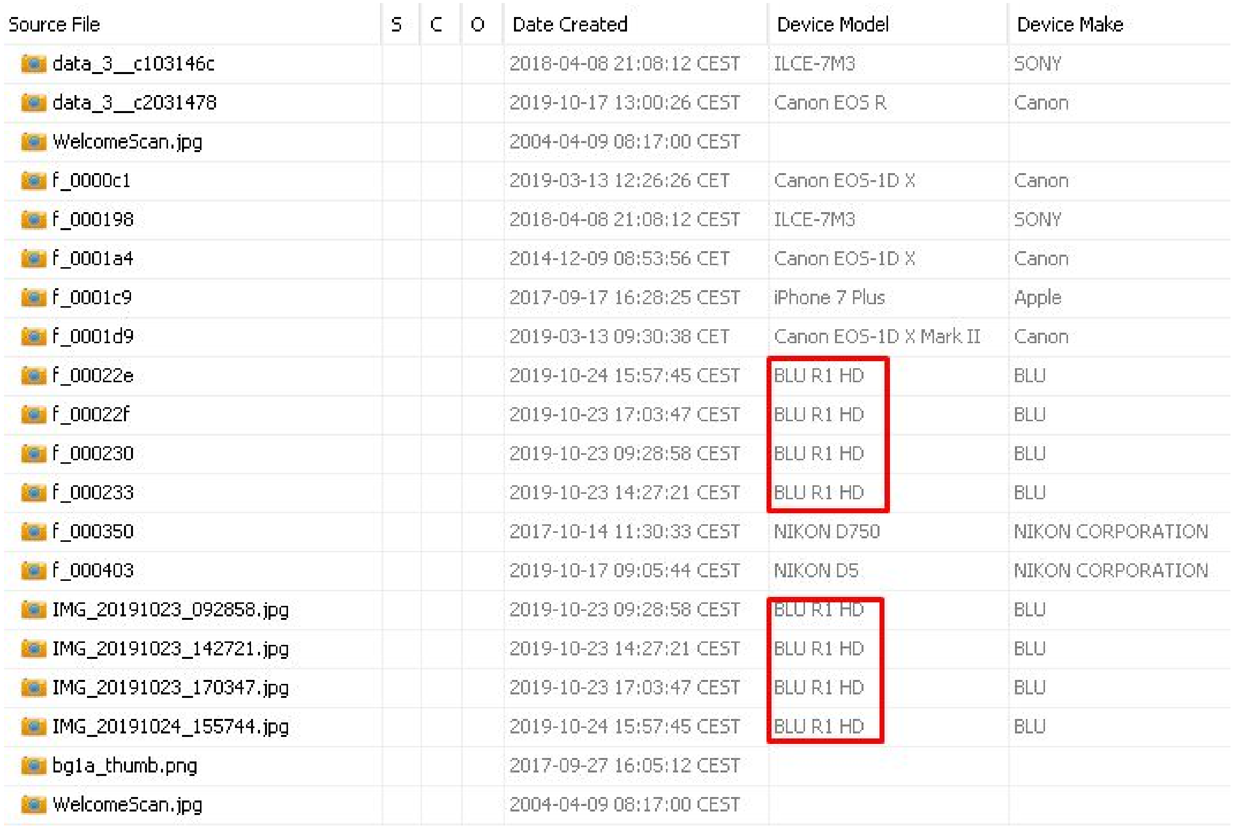
Many programs used or created by the owner can provide insight into the capability both of the system and the knowledge of the user. Results of this analysis may indicate additional steps that need to be taken in the extraction and analysis processes. In our case:

Operating system information :



| Source File | S | C | O | Name | Domain | Version | Processor Architecture | Temporary Files Directory | Data Source | Program Name | Path | Product ID | Owner |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SYSTEM | | | | DESKTOP-JEI7853 | | Windows_NT | AMD64 | %SystemRoot%\TEMP | device1_laptop.e01 | | | | |
| SOFTWARE | | | | | | | | | device1_laptop.e01 | Windows 10 Pro | C:\Windows | 00330-80000-00000-AA464 | AntiRenzik |

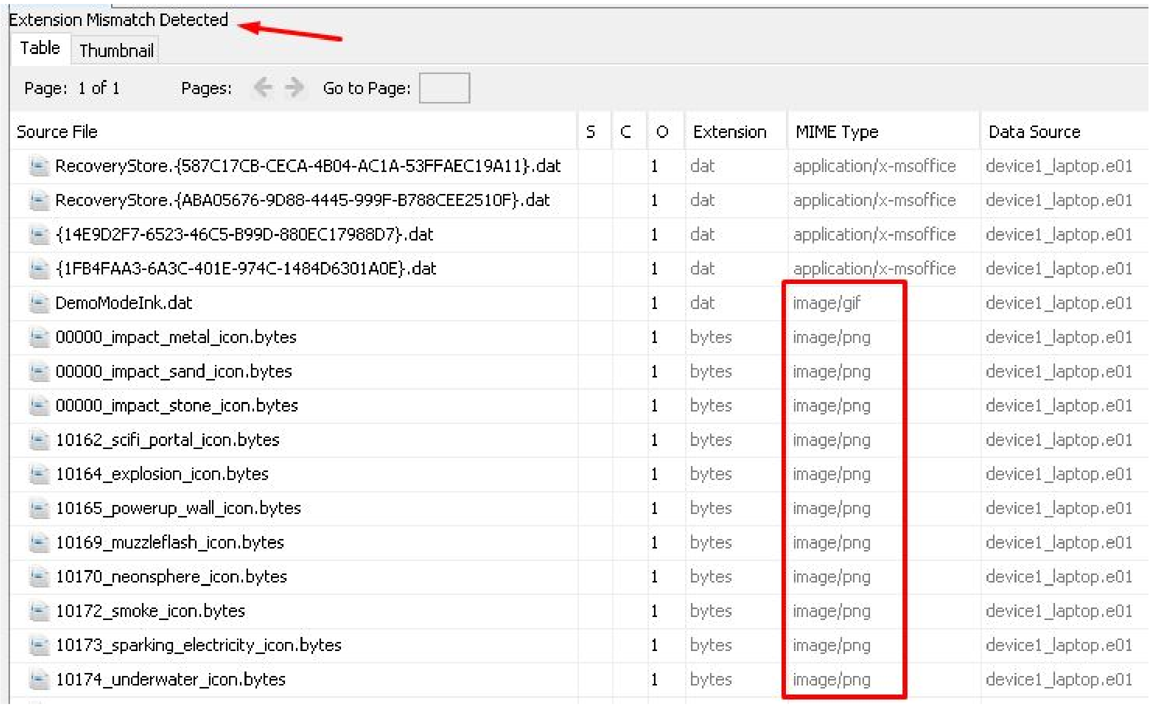
Using the exif metadata, we can determine the Device Model, Device Make, GPS Coordinates and etc... :



| Source File | S | C | O | Date Created | Device Model | Device Make |
|---|---|---|---|---|---|---|
| data_3__c103146c | | | | 2018-04-08 21:08:12 CEST | ILCE-7M3 | SONY |
| data_3__c2031478 | | | | 2019-10-17 13:00:26 CEST | Canon EOS R | Canon |
| WelcomeScan.jpg | | | | 2004-04-09 08:17:00 CEST | | |
| f_0000c1 | | | | 2019-03-13 12:26:26 CET | Canon EOS-1D X | Canon |
| f_000198 | | | | 2018-04-08 21:08:12 CEST | ILCE-7M3 | SONY |
| f_0001a4 | | | | 2014-12-09 08:53:56 CET | Canon EOS-1D X | Canon |
| f_0001c9 | | | | 2017-09-17 16:28:25 CEST | iPhone 7 Plus | Apple |
| f_0001d9 | | | | 2019-03-13 09:30:38 CET | Canon EOS-1D X Mark II | Canon |
| f_00022e | | | | 2019-10-24 15:57:45 CEST | BLU R1 HD | BLU |
| f_00022f | | | | 2019-10-23 17:03:47 CEST | BLU R1 HD | BLU |
| f_000230 | | | | 2019-10-23 09:28:58 CEST | BLU R1 HD | BLU |
| f_000233 | | | | 2019-10-23 14:27:21 CEST | BLU R1 HD | BLU |
| f_000350 | | | | 2017-10-14 11:30:33 CEST | NIKON D750 | NIKON CORPORATION |
| f_000403 | | | | 2019-10-17 09:05:44 CEST | NIKON D5 | NIKON CORPORATION |
| IMG_20191023_092858.jpg | | | | 2019-10-23 09:28:58 CEST | BLU R1 HD | BLU |
| IMG_20191023_142721.jpg | | | | 2019-10-23 14:27:21 CEST | BLU R1 HD | BLU |
| IMG_20191023_170347.jpg | | | | 2019-10-23 17:03:47 CEST | BLU R1 HD | BLU |
| IMG_20191024_155744.jpg | | | | 2019-10-24 15:57:45 CEST | BLU R1 HD | BLU |
| bg1a_thumb.png | | | | 2017-09-27 16:05:12 CEST | | |
| WelcomeScan.jpg | | | | 2004-04-09 08:17:00 CEST | | |

We can conclude that there are 8 pictures taken by a BLU R1 HD Device Model.

Also, there is a way to determine if there are mismatch extensions :

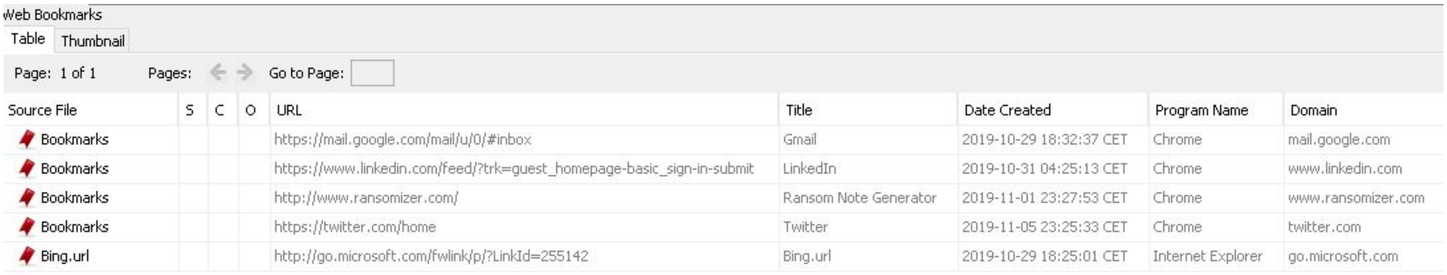

Extension Mismatch Detected

| Source File | S | C | O | Extension | MIME Type | Data Source |
|---|---|---|---|---|---|---|
| RecoveryStore.{587C17CB-CECA-4B04-AC1A-53FFAEC19A11}.dat | | | 1 | dat | application/x-msoffice | device1_laptop.e01 |
| RecoveryStore.{ABA05676-9D88-4445-999F-B788CEE2510F}.dat | | | 1 | dat | application/x-msoffice | device1_laptop.e01 |
| {14E9D2F7-6523-46C5-B99D-880EC17988D7}.dat | | | 1 | dat | application/x-msoffice | device1_laptop.e01 |
| {1FB4FAA3-6A3C-401E-974C-1484D6301A0E}.dat | | | 1 | dat | application/x-msoffice | device1_laptop.e01 |
| DemoModeInk.dat | | | 1 | dat | image/gif | device1_laptop.e01 |
| 00000_impact_metal_icon.bytes | | | 1 | bytes | image/png | device1_laptop.e01 |
| 00000_impact_sand_icon.bytes | | | 1 | bytes | image/png | device1_laptop.e01 |
| 00000_impact_stone_icon.bytes | | | 1 | bytes | image/png | device1_laptop.e01 |
| 10162_scifi_portal_icon.bytes | | | 1 | bytes | image/png | device1_laptop.e01 |
| 10164_explosion_icon.bytes | | | 1 | bytes | image/png | device1_laptop.e01 |
| 10165_powerup_wall_icon.bytes | | | 1 | bytes | image/png | device1_laptop.e01 |
| 10169_muzzleflash_icon.bytes | | | 1 | bytes | image/png | device1_laptop.e01 |
| 10170_neonsphere_icon.bytes | | | 1 | bytes | image/png | device1_laptop.e01 |
| 10172_smoke_icon.bytes | | | 1 | bytes | image/png | device1_laptop.e01 |
| 10173_sparking_electricity_icon.bytes | | | 1 | bytes | image/png | device1_laptop.e01 |
| 10174_underwater_icon.bytes | | | 1 | bytes | image/png | device1_laptop.e01 |

The file type that has the most mismatch extension is image/png.

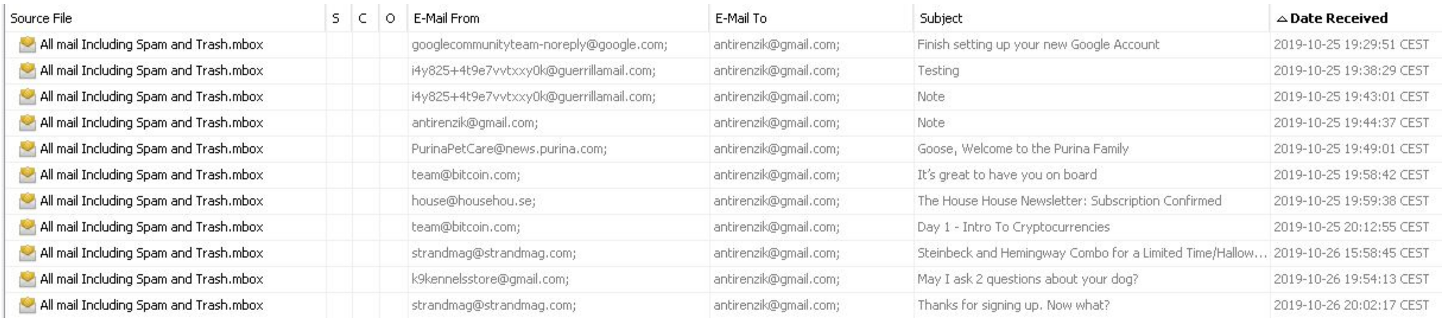
We can view relations between files, for example, correlating Internet history to cache files and email files to email attachments.

In our case, the bookmark contains 5 entries :


Web Bookmarks

| Source File | S | C | O | URL | Title | Date Created | Program Name | Domain |
|---|---|---|---|---|---|---|---|---|
| Bookmarks | | | | https://mail.google.com/mail/u/0/#inbox | Gmail | 2019-10-29 18:32:37 CET | Chrome | mail.google.com |
| Bookmarks | | | | https://www.linkedin.com/feed/?trk=guest_homepage-basic_sign-in-submit | LinkedIn | 2019-10-31 04:25:13 CET | Chrome | www.linkedin.com |
| Bookmarks | | | | http://www.ransomizer.com/ | Ransom Note Generator | 2019-11-01 23:27:53 CET | Chrome | www.ransomizer.com |
| Bookmarks | | | | https://twitter.com/home | Twitter | 2019-11-05 23:25:33 CET | Chrome | twitter.com |
| Bing.url | | | | http://go.microsoft.com/fwlink/p/?LinkId=255142 | Bing.url | 2019-10-29 18:25:01 CET | Internet Explorer | go.microsoft.com |

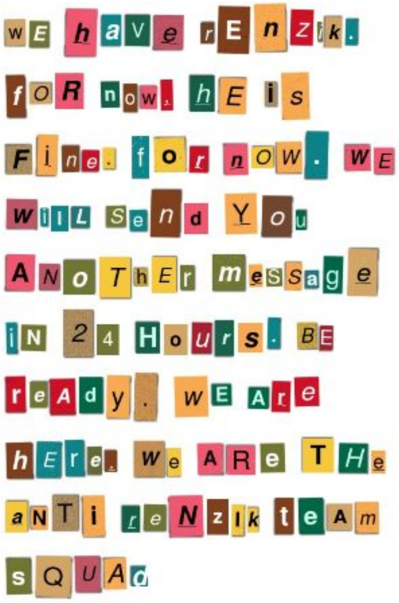
We can extract all stored mails :



| Source File | S | C | O | E-Mail From | E-Mail To | Subject | ▵ Date Received |
|---|---|---|---|---|---|---|---|
| All mail Including Spam and Trash.mbox | | | | googlecommunityteam-noreply@google.com; | antirenzik@gmail.com; | Finish setting up your new Google Account | 2019-10-25 19:29:51 CEST |
| All mail Including Spam and Trash.mbox | | | | i4y825+4t9e7vvtxxy0k@guerrillamail.com; | antirenzik@gmail.com; | Testing | 2019-10-25 19:38:29 CEST |
| All mail Including Spam and Trash.mbox | | | | i4y825+4t9e7vvtxxy0k@guerrillamail.com; | antirenzik@gmail.com; | Note | 2019-10-25 19:43:01 CEST |
| All mail Including Spam and Trash.mbox | | | | antirenzik@gmail.com; | antirenzik@gmail.com; | Note | 2019-10-25 19:44:37 CEST |
| All mail Including Spam and Trash.mbox | | | | PurinaPetCare@news.purina.com; | antirenzik@gmail.com; | Goose, Welcome to the Purina Family | 2019-10-25 19:49:01 CEST |
| All mail Including Spam and Trash.mbox | | | | team@bitcoin.com; | antirenzik@gmail.com; | It's great to have you on board | 2019-10-25 19:58:42 CEST |
| All mail Including Spam and Trash.mbox | | | | house@househou.se; | antirenzik@gmail.com; | The House House Newsletter: Subscription Confirmed | 2019-10-25 19:59:38 CEST |
| All mail Including Spam and Trash.mbox | | | | team@bitcoin.com; | antirenzik@gmail.com; | Day 1 - Intro To Cryptocurrencies | 2019-10-25 20:12:55 CEST |
| All mail Including Spam and Trash.mbox | | | | strandmag@strandmag.com; | antirenzik@gmail.com; | Steinbeck and Hemingway Combo for a Limited Time/Hallow... | 2019-10-26 15:58:45 CEST |
| All mail Including Spam and Trash.mbox | | | | k9kennelsstore@gmail.com; | antirenzik@gmail.com; | May I ask 2 questions about your dog? | 2019-10-26 19:54:13 CEST |
| All mail Including Spam and Trash.mbox | | | | strandmag@strandmag.com; | antirenzik@gmail.com; | Thanks for signing up. Now what? | 2019-10-26 20:02:17 CEST |

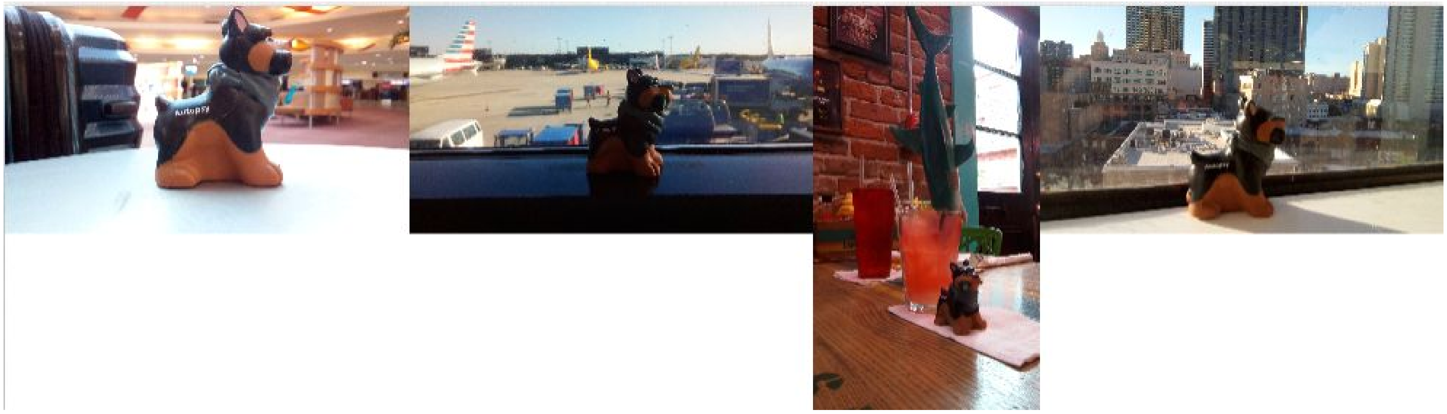
Ordering mails by the timeline, we can conclude a lot of things :

- **2019-10-25 19:43:01 CEST:** AntiRenzik is working with another person : i4y825+4t9e7vvtxxy0k@guerrillamail.com
- **2019-10-25 19:44:37 CEST:** AntiRenzik makes a note to be sent later :



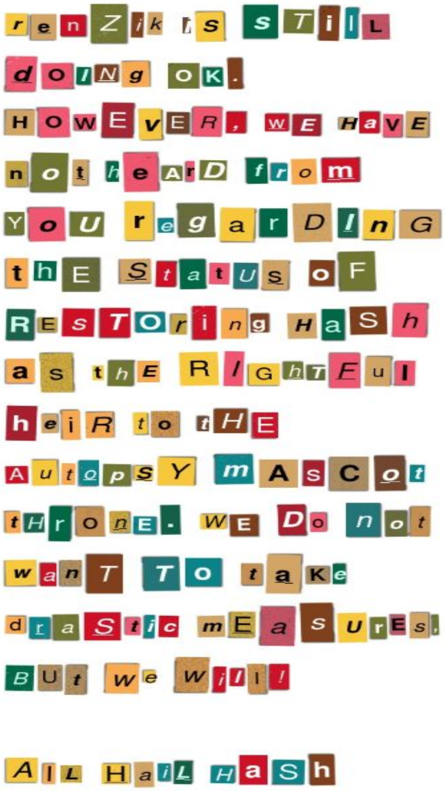
WE have rEnzik.
fOR now. hE is
Fine. for now. WE
will Send You
AnoTher message
iN 24 Hours. BE
ready. wE Are
here. We ARE THe
anTi reNzik teAm
SQUAd

- **2019-10-25 19:49:01 CEST:** AntiRenzik is interested in dogs and how to take care of them
- **2019-10-25 19:58:21 CEST:** AntiRenzik opens a bitcoin wallet
- **2019-11-01 21:12:46 CEST:** peacockleprechaun@gmail.com sent 4 pictures of Renzik containing GPS Coordinates of Renzik within the exif metadata that leads to :



  - ***401-423 Girod St, New Orleans, LA 70130, USA***
  - ***Central Business District, New Orleans, Louisiana 70130, USA***
  - ***7050 Friendship Rd, Baltimore, MD 21240, USA***
- **2019-11-01 21:24:57:** The new person says that they had stolen Renzik from Basis and no one seems to know, maybe it's time to step up? We also notice that they prefer Hash as a dog than Renzik
- **2019-11-01 23:30:33 CEST:** AntiRenzik sends the prepared note to Mr Carrier briancarrrier@basistech.com

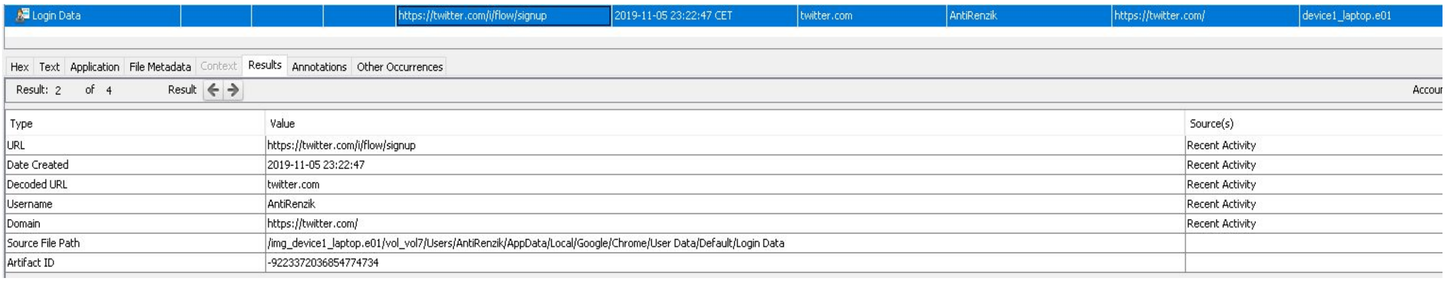
- **2019-11-01 23:33:11 CEST:** AntiRenzik sends again the note because the last one wasn't delivered due to a mail error and uses a new mail this time info@basistech.com and a new message :



renZik is still
doing ok.
However, we have
not heard from
you regarding
the status of
restoring hash
as the rightful
heir to the
autopsy mascot
throne. we do not
want to take
drastic measures,
but we will!

All Hail hash

- **2019-11-04 18:10:30 CEST:** AntiRenzik asks Peacockleprechaun about status updates
- **2019-11-04 18:16:31 CEST:** Peacockleprechaun send a password protected doc to AntiRenzik with the name of ***"In order to ensure that Renzik is treated properly.docx"*** Then says that the password is the mascot which isn't Renzik
- **2019-11-04 22:33:30 CEST:** Peacockleprechaun sends a note to AntiRenzik : "*The password to open the file IMPORTANT is* ***argstrongpassword****. Because we only use the strong passwords"*
- **2019-11-05 20:20:18 CEST:** AntiRenzik creates a twitter account with the name AntiRenzik

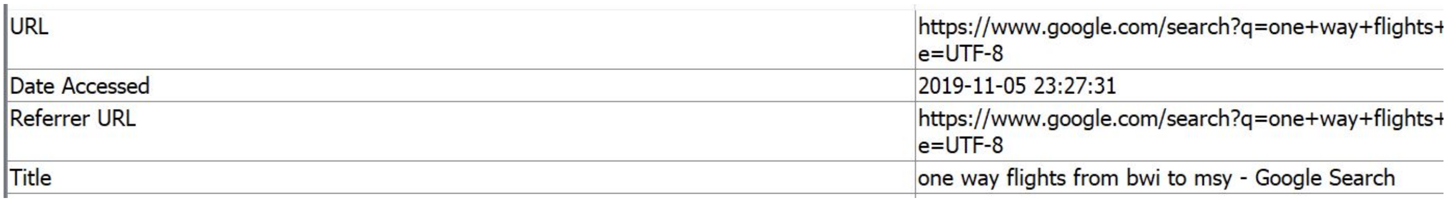


| Login Data | | | | https://twitter.com/i/flow/signup | 2019-11-05 23:22:47 CET | twitter.com | AntiRenzik | https://twitter.com/ | device1_laptop.e01 |
|---|---|---|---|---|---|---|---|---|---|

| Type | Value | Source(s) |
|---|---|---|
| URL | https://twitter.com/i/flow/signup | Recent Activity |
| Date Created | 2019-11-05 23:22:47 | Recent Activity |
| Decoded URL | twitter.com | Recent Activity |
| Username | AntiRenzik | Recent Activity |
| Domain | https://twitter.com/ | Recent Activity |
| Source File Path | /img_device1_laptop.e01/vol_vol7/Users/AntiRenzik/AppData/Local/Google/Chrome/User Data/Default/Login Data | |
| Artifact ID | -9223372036854774734 | |

- **2019-11-05 23:16:54 CEST:** AntiRenzik tells peacockleprechaun that he will fly down to New Orleans

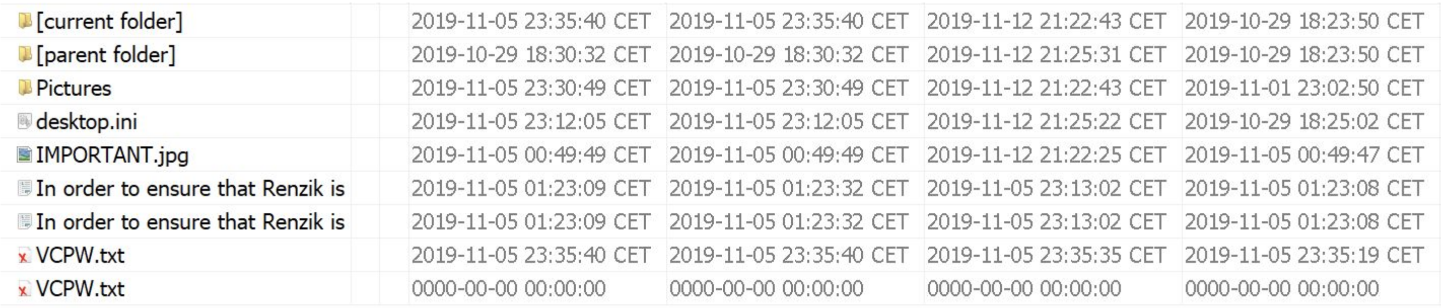
We also noticed in the history of his searches :



| | |
|---|---|
| URL | https://www.google.com/search?q=one+way+flights+<br>e=UTF-8 |
| Date Accessed | 2019-11-05 23:27:31 |
| Referrer URL | https://www.google.com/search?q=one+way+flights+<br>e=UTF-8 |
| Title | one way flights from bwi to msy - Google Search |

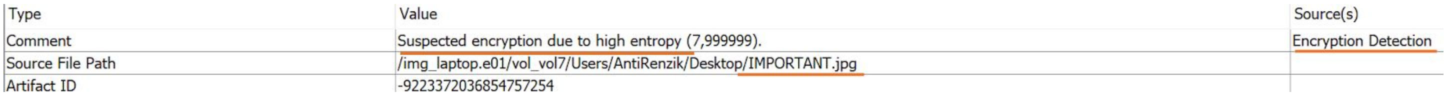
- **2019-11-07 19:33:20 CEST:** AntiRenzik receives an email from LinkedIn where he used his real name : ***"Goose Honkerson"*** specifying that he's ***"Top Goose at Anti Renzik Group"***
- **2019-11-12 04:41:59 CEST:** Peaacockleprechaun asks AntiRenzik for a meetup
- **2019-11-12 12:03:32 CEST:** AntiRenzik suggests a place and time : ***Jackson Square, 701 Decatur St, New Orleans, LA 70116 at 4pm***

## Encrypted files

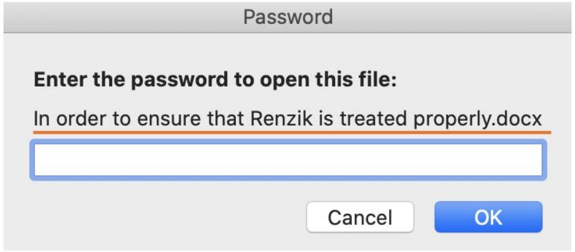


| | | | | |
|---|---|---|---|---|
| [current folder] | 2019-11-05 23:35:40 CET | 2019-11-05 23:35:40 CET | 2019-11-12 21:22:43 CET | 2019-10-29 18:23:50 CET |
| [parent folder] | 2019-10-29 18:30:32 CET | 2019-10-29 18:30:32 CET | 2019-11-12 21:25:31 CET | 2019-10-29 18:23:50 CET |
| Pictures | 2019-11-05 23:30:49 CET | 2019-11-05 23:30:49 CET | 2019-11-12 21:22:43 CET | 2019-11-01 23:02:50 CET |
| desktop.ini | 2019-11-05 23:12:05 CET | 2019-11-05 23:12:05 CET | 2019-11-12 21:25:22 CET | 2019-10-29 18:25:02 CET |
| IMPORTANT.jpg | 2019-11-05 00:49:49 CET | 2019-11-05 00:49:49 CET | 2019-11-12 21:22:25 CET | 2019-11-05 00:49:47 CET |
| In order to ensure that Renzik is | 2019-11-05 01:23:09 CET | 2019-11-05 01:23:32 CET | 2019-11-05 23:13:02 CET | 2019-11-05 01:23:08 CET |
| In order to ensure that Renzik is | 2019-11-05 01:23:09 CET | 2019-11-05 01:23:32 CET | 2019-11-05 23:13:02 CET | 2019-11-05 01:23:08 CET |
| VCPW.txt | 2019-11-05 23:35:40 CET | 2019-11-05 23:35:40 CET | 2019-11-05 23:35:35 CET | 2019-11-05 23:35:19 CET |
| VCPW.txt | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 |

In the Desktop folder of AntiRenzik user we found a password protected document "***In order to ensure that Renzik is treated properly.docx***" and the IMPORTANT.jpg which is an encrypted image.



| Type | Value | Source(s) |
|---|---|---|
| Comment | Suspected encryption due to high entropy (7,999999). | Encryption Detection |
| Source File Path | /img_laptop.e01/vol_vol7/Users/AntiRenzik/Desktop/IMPORTANT.jpg | |
| Artifact ID | -9223372036854757254 | |

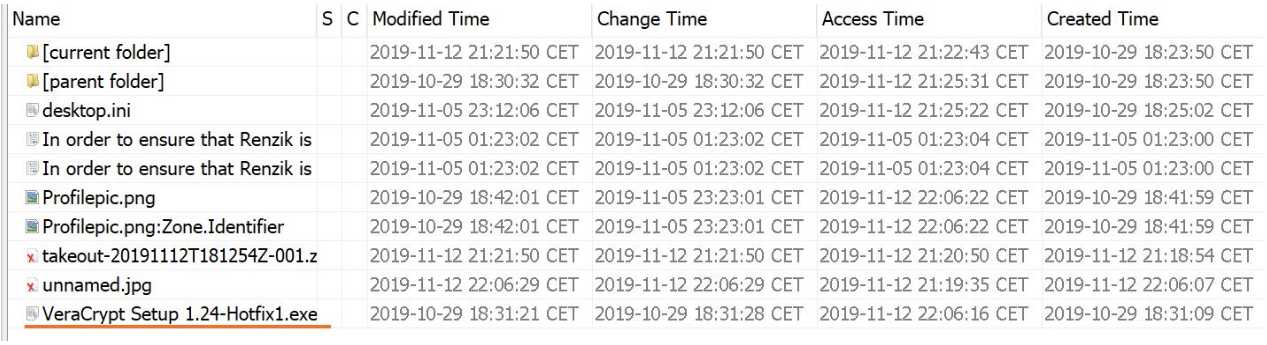


Password

**Enter the password to open this file:**

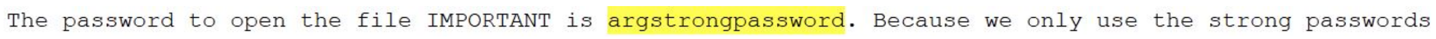
In order to ensure that Renzik is treated properly.docx

We were quite sure that the IMPORTANT.jpg is a VeraCrypt -ed image, thanks to the VeraCrypt Setup executable we've found in the Downloads folder of the same user - AntiRenzik and the VCPW.txt in Desktop folder which stands for VeraCryptPassWord.



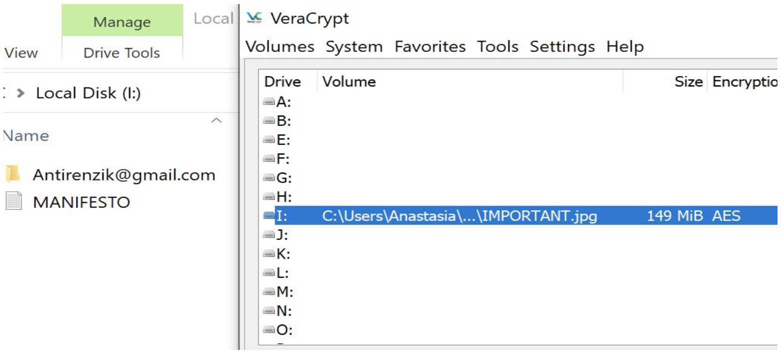
| Name | S | C | Modified Time | Change Time | Access Time | Created Time |
|---|---|---|---|---|---|---|
| [current folder] | | | 2019-11-12 21:21:50 CET | 2019-11-12 21:21:50 CET | 2019-11-12 21:22:43 CET | 2019-10-29 18:23:50 CET |
| [parent folder] | | | 2019-10-29 18:30:32 CET | 2019-10-29 18:30:32 CET | 2019-11-12 21:25:31 CET | 2019-10-29 18:23:50 CET |
| desktop.ini | | | 2019-11-05 23:12:06 CET | 2019-11-05 23:12:06 CET | 2019-11-12 21:25:22 CET | 2019-10-29 18:25:02 CET |
| In order to ensure that Renzik is | | | 2019-11-05 01:23:02 CET | 2019-11-05 01:23:02 CET | 2019-11-05 01:23:04 CET | 2019-11-05 01:23:00 CET |
| In order to ensure that Renzik is | | | 2019-11-05 01:23:02 CET | 2019-11-05 01:23:02 CET | 2019-11-05 01:23:04 CET | 2019-11-05 01:23:00 CET |
| Profilepic.png | | | 2019-10-29 18:42:01 CET | 2019-11-05 23:23:01 CET | 2019-11-12 22:06:22 CET | 2019-10-29 18:41:59 CET |
| Profilepic.png:Zone.Identifier | | | 2019-10-29 18:42:01 CET | 2019-11-05 23:23:01 CET | 2019-11-12 22:06:22 CET | 2019-10-29 18:41:59 CET |
| takeout-20191112T181254Z-001.z | | | 2019-11-12 21:21:50 CET | 2019-11-12 21:21:50 CET | 2019-11-12 21:20:50 CET | 2019-11-12 21:18:54 CET |
| unnamed.jpg | | | 2019-11-12 22:06:29 CET | 2019-11-12 22:06:29 CET | 2019-11-12 21:19:35 CET | 2019-11-12 22:06:07 CET |
| VeraCrypt Setup 1.24-Hotfix1.exe | | | 2019-10-29 18:31:21 CET | 2019-10-29 18:31:28 CET | 2019-11-12 22:06:16 CET | 2019-10-29 18:31:09 CET |

Another occurrence of "argstrongpassword" was found in ChromeCacheExtractor.



```
The password to open the file IMPORTANT is argstrongpassword. Because we only use the strong passwords
```

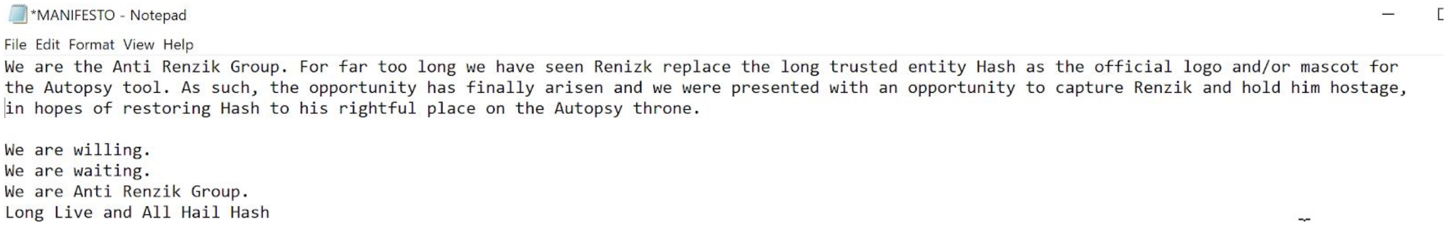
We extracted IMPORTANT.jpg and tried to decrypt the content using VeraCrypt App.



Antirenzik@gmail.com
MANIFESTO

| Drive | Volume | Size | Encryptio |
|---|---|---|---|
| A: | | | |
| B: | | | |
| E: | | | |
| F: | | | |
| G: | | | |
| H: | | | |
| I: | C:\Users\Anastasia\...\IMPORTANT.jpg | 149 MiB | AES |
| J: | | | |
| K: | | | |
| L: | | | |
| M: | | | |
| N: | | | |
| O: | | | |

The IMPORTANT.jpg reveals new mails and a MANIFESTO.

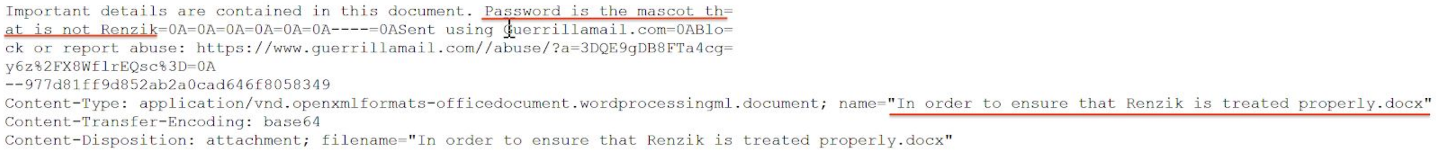


```
We are the Anti Renzik Group. For far too long we have seen Renizk replace the long trusted entity Hash as the official logo and/or mascot for
the Autopsy tool. As such, the opportunity has finally arisen and we were presented with an opportunity to capture Renzik and hold him hostage,
in hopes of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

The Manifesto clearly disclose the Anti Renzik Group intentions which are to restore the Hash mascot replaced by Renzik.

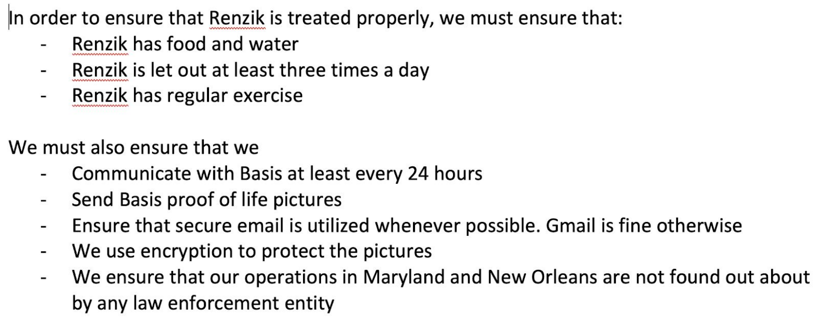
Going through AntiRenzik mails we found an interesting mail which reveals the password to unlock "In order to ensure that Renzik is treated properly.docx" document.



```
Important details are contained in this document. Password is the mascot th=
at is not Renzik=0A=0A=0A=0A=0A=0A-----=0ASent using Guerrillamail.com=0ABlo=
ck or report abuse: https://www.guerrillamail.com//abuse/?a=3DQE9gDB8FTa4cg=
y6z%2FX8WflrEQsc%3D=0A
--977d81ff9d852ab2a0cad646f8058349
Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document; name="In order to ensure that Renzik is treated properly.docx"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="In order to ensure that Renzik is treated properly.docx"
```

The password is the mascot that is not Renzik and the mascot that is not Renzik is obviously Hash.

The content of the unlocked docx file with “Hash” password is the following:



In order to ensure that Renzik is treated properly, we must ensure that:

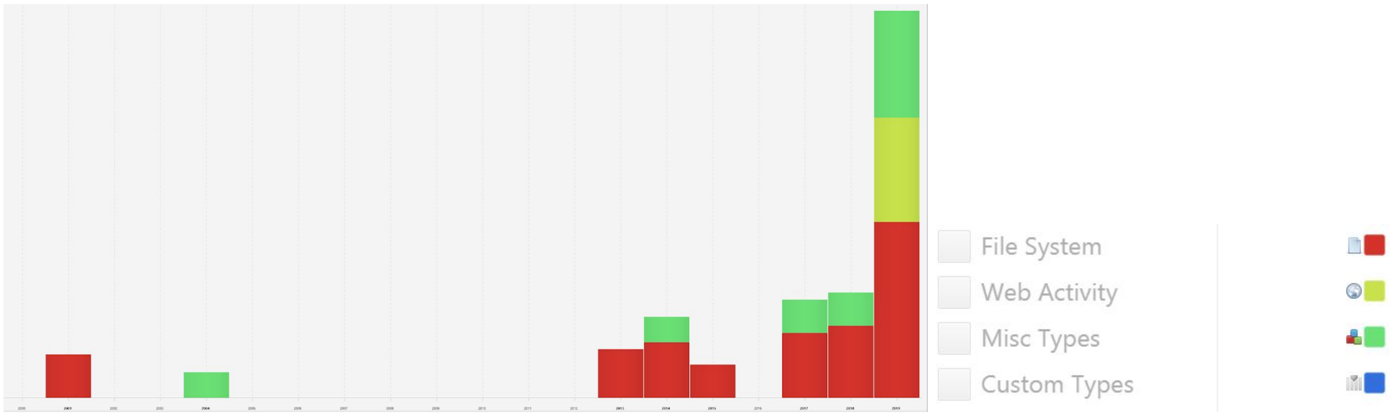
- Renzik has food and water
- Renzik is let out at least three times a day
- Renzik has regular exercise

We must also ensure that we

- Communicate with Basis at least every 24 hours
- Send Basis proof of life pictures
- Ensure that secure email is utilized whenever possible. Gmail is fine otherwise
- We use encryption to protect the pictures
- We ensure that our operations in Maryland and New Orleans are not found out about by any law enforcement entity

- ## Timeframe

Timeframe analysis is useful in determining a sequence of events on digital systems which can be used as a part of associating usage of the computer to an individual(s) at the time the events occurred.

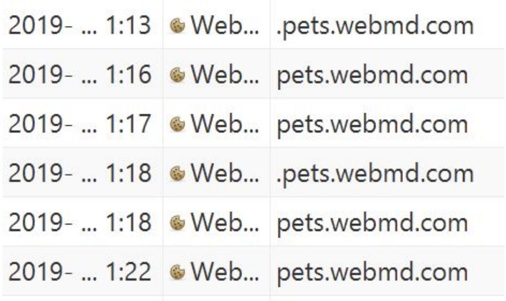


We can see from the Autopsy Activity Timeline that the activity is not homogenous, with a majority of events occurring  in 2017, 2018 and 2019.

We’ll take a closer look at the web activity : browsing history, cookies, searches.
By now we know that only web activity was made in 2019.

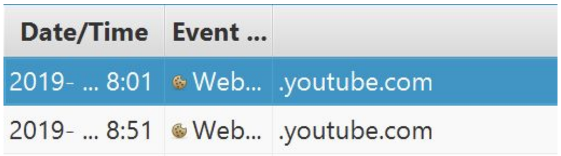
### *Cookies*

Using the Autopsy timeline activity list, we filtered web cookies and discovered some pets related websites.

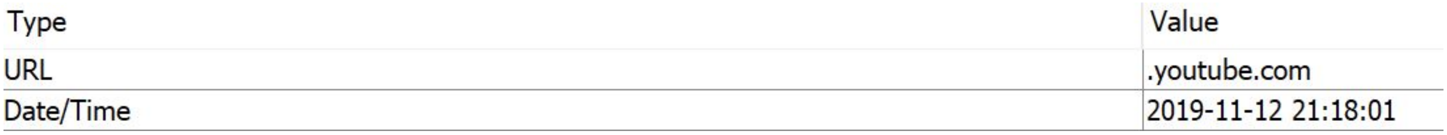


| | | |
|---|---|---|
| 2019- ... 1:13 | Web... | .pets.webmd.com |
| 2019- ... 1:16 | Web... | pets.webmd.com |
| 2019- ... 1:17 | Web... | pets.webmd.com |
| 2019- ... 1:18 | Web... | .pets.webmd.com |
| 2019- ... 1:18 | Web... | pets.webmd.com |
| 2019- ... 1:22 | Web... | pets.webmd.com |

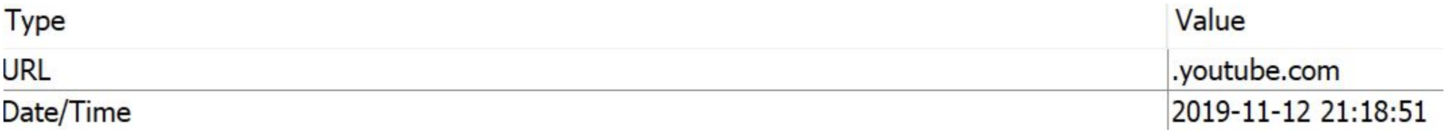
By filtering youtube cookies we've seen that all of them are made on 12 November 2019.



| Date/Time | Event ... | |
|---|---|---|
| 2019- ... 8:01 | Web... | .youtube.com |
| 2019- ... 8:51 | Web... | .youtube.com |



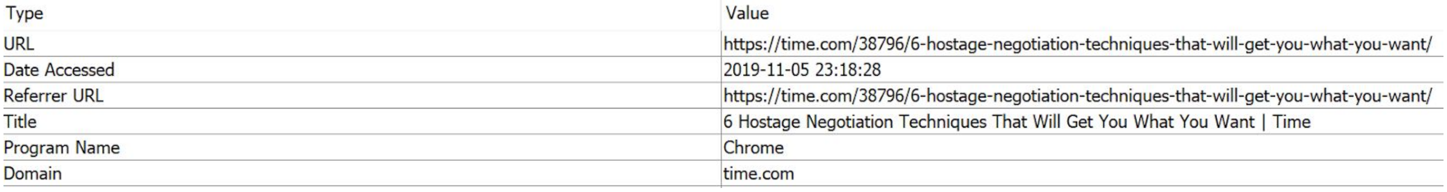
| Type | Value |
|---|---|
| URL | .youtube.com |
| Date/Time | 2019-11-12 21:18:01 |



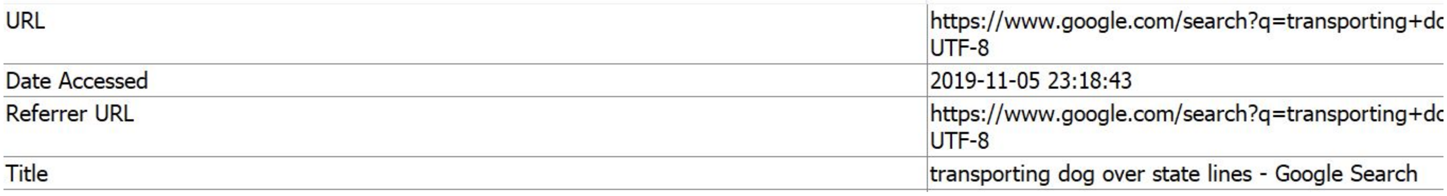
| Type | Value |
|---|---|
| URL | .youtube.com |
| Date/Time | 2019-11-12 21:18:51 |

## *Web History*

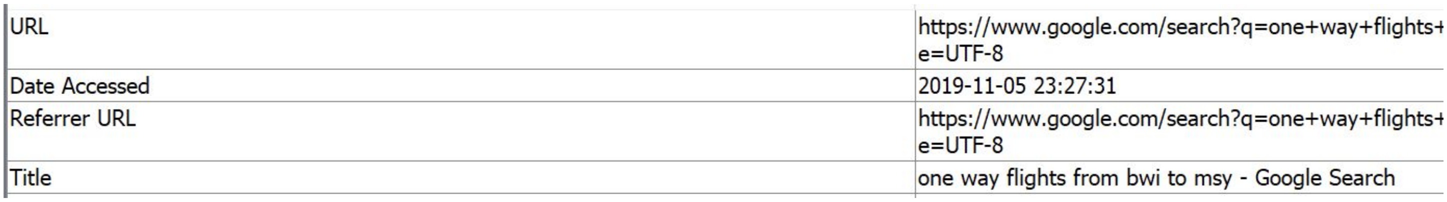
From the Web history list we can conclude that the dog was stolen somewhere before or between 5 Nov and 21 Nov.
We found evidence proving that the 5 Nov the defendant was preparing for dog hostage negotiation and dog transportation.



| Type | Value |
|---|---|
| URL | https://time.com/38796/6-hostage-negotiation-techniques-that-will-get-you-what-you-want/ |
| Date Accessed | 2019-11-05 23:18:28 |
| Referrer URL | https://time.com/38796/6-hostage-negotiation-techniques-that-will-get-you-what-you-want/ |
| Title | 6 Hostage Negotiation Techniques That Will Get You What You Want \| Time |
| Program Name | Chrome |
| Domain | time.com |

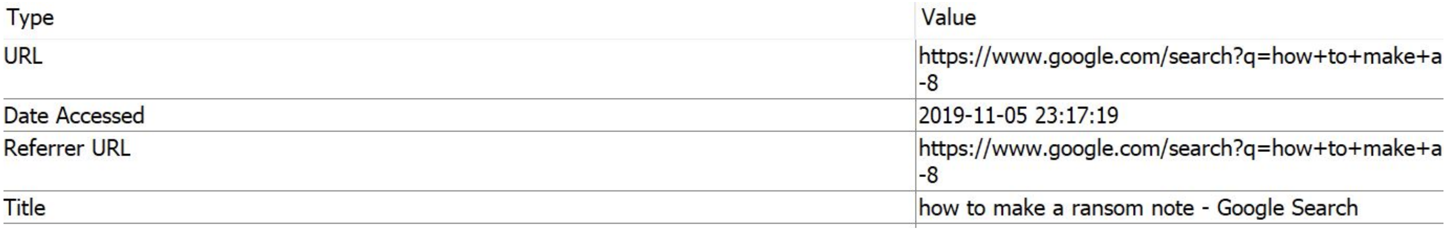


| | |
|---|---|
| URL | https://www.google.com/search?q=transporting+dc<br>UTF-8 |
| Date Accessed | 2019-11-05 23:18:43 |
| Referrer URL | https://www.google.com/search?q=transporting+dc<br>UTF-8 |
| Title | transporting dog over state lines - Google Search |



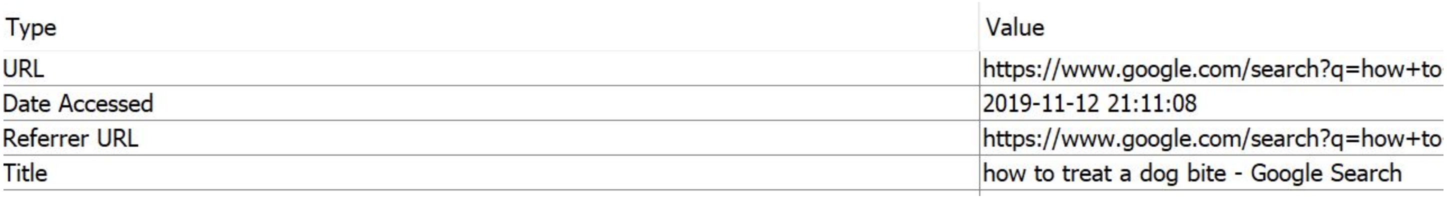
| | |
|---|---|
| URL | https://www.google.com/search?q=one+way+flights+<br>e=UTF-8 |
| Date Accessed | 2019-11-05 23:27:31 |
| Referrer URL | https://www.google.com/search?q=one+way+flights+<br>e=UTF-8 |
| Title | one way flights from bwi to msy - Google Search |

The same day (5 Nov), the defendant was also preparing a ransomware note:



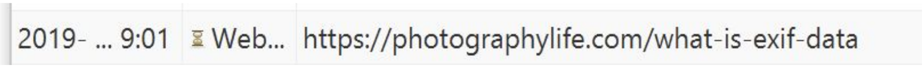
| Type | Value |
|---|---|
| URL | https://www.google.com/search?q=how+to+make+a<br>-8 |
| Date Accessed | 2019-11-05 23:17:19 |
| Referrer URL | https://www.google.com/search?q=how+to+make+a<br>-8 |
| Title | how to make a ransom note - Google Search |

Then we found a web search entitled “How to treat a dog bite” on 12 Nov 2019, as the dog was already stolen.



| Type | Value |
|---|---|
| URL | https://www.google.com/search?q=how+to |
| Date Accessed | 2019-11-12 21:11:08 |
| Referrer URL | https://www.google.com/search?q=how+to |
| Title | how to treat a dog bite - Google Search |

We’ve also supposed that he was trying to escape the forensic experts.

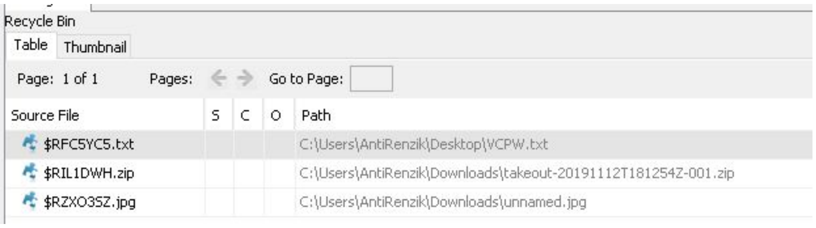


2019- ... 9:01 ⧗ Web... https://photographylife.com/what-is-exif-data

## Data hiding

Data can be concealed on a computer system. Data hiding analysis can be useful in detecting and recovering such data and may indicate knowledge, ownership, or intent.

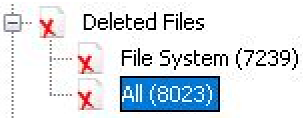
In our case we can recover some files from the recycle bin :



Recycle Bin

| Source File | S | C | O | Path |
|---|---|---|---|---|
| $RFC5YC5.txt | | | | C:\Users\AntiRenzik\Desktop\VCPW.txt |
| $RIL1DWH.zip | | | | C:\Users\AntiRenzik\Downloads\takeout-20191112T181254Z-001.zip |
| $RZXO3SZ.jpg | | | | C:\Users\AntiRenzik\Downloads\unnamed.jpg |

Or even recover those who are deleted from the recycle bin :



- **Ownership and possession**

In most cases it is essential to identify the individual(s) who created, modified, or accessed a file. It is also important to establish ownership as this can help to link a person to his data and to events linked with this same data.

In our case we only have AntiRenzik as user, so no need to dig deeper on this part

# 3. Conclusion

All the evidence was obtained from the review of the system artefacts, emails artefacts and deleted files.

During the course of the artefacts extractions, the experts identified encrypted files on the machine. These files were as a matter of course in the investigation, decrypted by the experts and it was subsequently discovered that they were planning to remove the Renzik mascot as a logo for Autopsy.

The expert therefore concluded that in the course of his employment, the suspect has used his computer to manage the whole operation remotely. These findings are resumed as below :

AntiRenzik were in touch with Peacockleprechaun  peacockleprechaun@gmail.com who used sometimes a private mail i4y825+4t9e7vvtxxy0k@guerrillamail.com. They were both trying to send multiple notes to the Basis group, but they had no reply from them. The dog was well treated ( but sometimes he was bleeding ) by Peacockleprechaun who was in New Orleans meanwhile AntiRenzik was in Baltimore, USA (BWI), trying to push pressure on Basis to change the official mascot of Autopsy from Renzik to Hash.

After a while, AntiRenzik created a Twitter and LinkedIn account and he used his real name which is “Goose Honkerson”. Goose decided to fly to New Orleans so that he could check the dog and he gave an appointment to his friend Peacockleprechaun .

They are going to meet the ***12 November at  Jackson Square, 701 Decatur St, New Orleans, LA 70116 at 4pm***.

In the opinion of the experts, Goose Honkerson and his friend Peacockleprechaun were involved and complicit, respectively in the theft of the Renzik from the period of 25 october to the 12th of November 2019.

Date : October 28, 2020

Signature:

Y.Alim

Signature:

A.Cotorobai