
# Rapport Investigation
# Anti-Renzik Group

28.10.2020

—

## Groupe

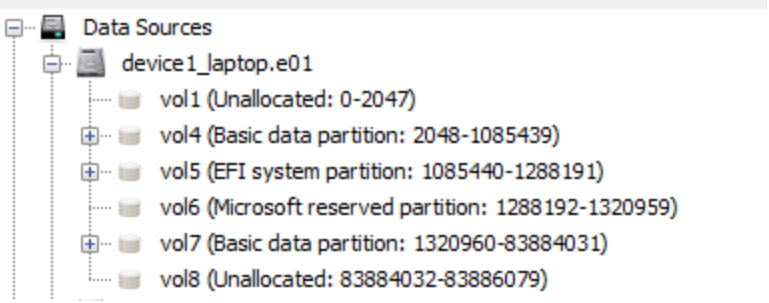
Redouane Taoussi

Matthieu Christophe

Dhia Layadi

# 1 - Questions

## 1. Combien de partitions sont présentes sur le disque du laptop ?



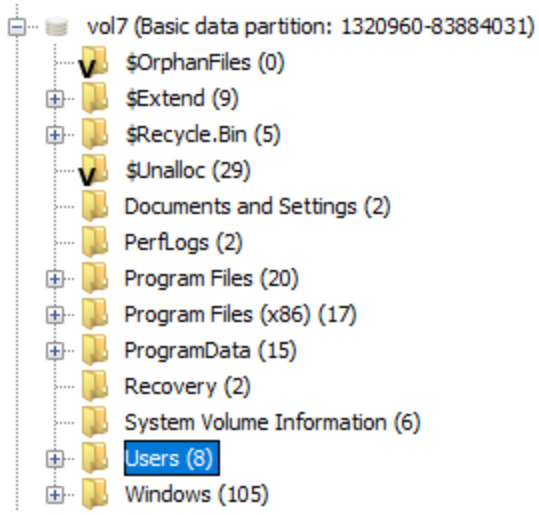

Il y'en a 6 partions sur le disque laptop.

## 2. Quel est le nom de l'espace non-alloué dans vol1 ?

On distingue dans vol1 environ 2048 secteurs non alloué, on peut donc penser à la partition MBR (BIOS) qui réserve cet espace.

## 3. Quel est le système de fichiers dans le Vol7 ?

Nous constatons que la partition vol7 contient le système d'exploitation "Windows" où l'on trouve la plupart des données personnels du criminel. C'est un "Filesystem Windows" (C:)



4. ## En regardant les métadonnées EXIF, combien de photographies ont-été prises avec un BLU R1 HD ?

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| f_00022e | | 2 | 2019-10-24 15:57:45 CEST | BLU R1 HD | BLU | device1_laptop.e01 | 1573798 | /img_device1_laptop.e01/vol_ |
| f_00022f | | 2 | 2019-10-23 17:03:47 CEST | BLU R1 HD | BLU | device1_laptop.e01 | 2099201 | /img_device1_laptop.e01/vol_ |
| f_000230 | | 2 | 2019-10-23 09:28:58 CEST | BLU R1 HD | BLU | device1_laptop.e01 | 1732489 | /img_device1_laptop.e01/vol_ |
| f_000233 | | 2 | 2019-10-23 14:27:21 CEST | BLU R1 HD | BLU | device1_laptop.e01 | 1355987 | /img_device1_laptop.e01/vol_ |
| IMG_20191023_092858.jpg | | 2 | 2019-10-23 09:28:58 CEST | BLU R1 HD | BLU | device1_laptop.e01 | 1732489 | /img_device1_laptop.e01/vol_ |
| IMG_20191023_142721.jpg | | 2 | 2019-10-23 14:27:21 CEST | BLU R1 HD | BLU | device1_laptop.e01 | 1355987 | /img_device1_laptop.e01/vol_ |
| IMG_20191023_170347.jpg | | 2 | 2019-10-23 17:03:47 CEST | BLU R1 HD | BLU | device1_laptop.e01 | 2099201 | /img_device1_laptop.e01/vol_ |
| IMG_20191024_155744.jpg | | 2 | 2019-10-24 15:57:45 CEST | BLU R1 HD | BLU | device1_laptop.e01 | 1573798 | /img_device1_laptop.e01/vol_ |
| IMG_20191023_092858.jpg | | 2 | 2019-10-23 09:28:58 CEST | BLU R1 HD | BLU | device1_laptop.e01 | 1732521 | /img_device1_laptop.e01/vol_ |
| IMG_20191023_142721.jpg | | 2 | 2019-10-23 14:27:21 CEST | BLU R1 HD | BLU | device1_laptop.e01 | 1356019 | /img_device1_laptop.e01/vol_ |
| IMG_20191023_092858.jpg | | 2 | 2019-10-23 09:28:58 CEST | BLU R1 HD | BLU | device1_laptop.e01 | 1732521 | /img_device1_laptop.e01/vol_ |
| IMG_20191023_170347.jpg | | 2 | 2019-10-23 17:03:47 CEST | BLU R1 HD | BLU | device1_laptop.e01 | 2099233 | /img_device1_laptop.e01/vol_ |
| IMG_20191024_155744.jpg | | 2 | 2019-10-24 15:57:45 CEST | BLU R1 HD | BLU | device1_laptop.e01 | 1573830 | /img_device1_laptop.e01/vol_ |
| IMG_20191023_170347.jpg | | 2 | 2019-10-23 17:03:47 CEST | BLU R1 HD | BLU | device1_laptop.e01 | 2099233 | /img_device1_laptop.e01/vol_ |
| IMG_20191023_142721.jpg | | 2 | 2019-10-23 14:27:21 CEST | BLU R1 HD | BLU | device1_laptop.e01 | 1356019 | /img_device1_laptop.e01/vol_ |

Il y'a 15 photographires prise en BLU R1  HD

5. ## Quel type de fichier a un grand taux d'extensions inattendues (extension mismatch) ?

Parmi les 114 fichiers (extension mismatch) 

, plus de la moitié sont d'extension ".bytes".

6. ## Combien de "Web Bookmarks" sont listés ?

Il y en a 5

| Source File | S | C | O | URL |
|---|---|---|---|---|
| Bookmarks | | | 1 | https://mail.google.com/mail/u/0/#inbox |
| Bookmarks | | | 1 | https://www.linkedin.com/feed/?trk=guest_homepage-basic_sign-in-submit |
| Bookmarks | | | 1 | http://www.ransomizer.com/ |
| Bookmarks | | | 1 | https://twitter.com/home |
| Bing.url | | | 1 | http://go.microsoft.com/fwlink/p/?LinkId=255142 |

7. ## De quels mois et année proviennent les cookies associés avec le nom de domaine "youtube.com" ?

| | | | | | |
|---|---|---|---|---|---|
| Cookies | | | 1 | .youtube.com | 2019-11-12 21:18:51 CE |

Année: 2019

Mois : Novembre

8. Dans les "Web History", quel jour est associé la recherche Google "how to treat a dog bite" ?

| Type | Value |
|---|---|
| Domain | www.google.com |
| Text | how to treat a dog bite |
| Program Name | Chrome |
| Date Accessed | 2019-11-12 21:11:08 |
| Source File Path | /img_device1_laptop.e01/vol_vol7/Users/AntiRenzik/AppData/Local/Google/Chrome/User Data/Default/History |
| Artifact ID | -9223372036854761517 |

12 novembre 2019

9. Dans le Web History, quel jour est associé avec la recherche "how to make a ransom note" ?

| Type | Value | Source(s) |
|---|---|---|
| URL | https://www.google.com/search?q=how+to+make+a+ransom+note&oq=how+to+make+a+ransom+note&aqs=chrome..69i57j0l5.4005j1j7&sourceid=chrome&ie=UTF-8 | Recent Activity |
| Date Accessed | 2019-11-05 23:17:19 | Recent Activity |
| Referrer URL | https://www.google.com/search?q=how+to+make+a+ransom+note&oq=how+to+make+a+ransom+note&aqs=chrome..69i57j0l5.4005j1j7&sourceid=chrome&ie=UTF-8 | Recent Activity |
| Title | how to make a ransom note - Google Search | Recent Activity |
| Program Name | Chrome | Recent Activity |
| Domain | www.google.com | Recent Activity |
| Source File Path | /img_device1_laptop.e01/vol_vol7/Users/AntiRenzik/AppData/Local/Google/Chrome/User Data/Default/History | |
| Artifact ID | -9223372036854775635 | |

2019-11-05 23:17:19

10. Dans "Accounts", quel est le nom de compte associé avec le compte Twitter ?

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

AntiRenzik

# 2 - Investigation

## Résumé

L'objectif de ce rapport est de fournir des procédures d'examen, des conclusions et des recommandations provenant de fictifs témoins des événements de cyberintimidation ayant conduit au kidnaping de la mascotte de Autopsy .

Ces informations permettent de présenter l'étape de l'enquête. Le rapport comprend les normes, les principes, les méthodes et les questions juridiques de la police scientifique numérique qui peuvent avoir un impact sur la décision du tribunal. Le rapport est impartial et vise à aider le tribunal à rendre un jugement sur les fait à l'encontre de AntiRenzik.

Ce rapport se concentre sur les preuves numériques recueillies auprès du suspects. Par conséquent, le rapport omet les preuves recueillies sur le téléphone et l'ordinateur portable de celui-ci.

## Objectifs

1. Analyser le disque de l'ordinateur.
2. Apporter des informations afin d'aider le tribunal à rendre les faits.
3. Trouver l'emplacement de l'otage

## Analyse des preuves informatiques (Artefactes)

La section suivante  est l'endroit où sont présentées toutes les preuves recueillies et leurs interprétations. Elle fournit des informations détaillées concernant l'attribution des numéros d'étiquette des preuves, la description des preuves et les numéros de série des supports si elle existe .

### Caractéristiques

Ci-dessous les hash des deux disques partagés:
**SHA256 hash of device1_laptop.e01:**
4f082edfeeed1ce7f5050545435fa57a6ed59c3ccb72495cfa62771075bbd736

**SHA256 hash of device2_mediacard.e01:**
7235027f18e5d2439ffa607dff8bbaaaf743bddd28ce9f701001abf8a5a18fed

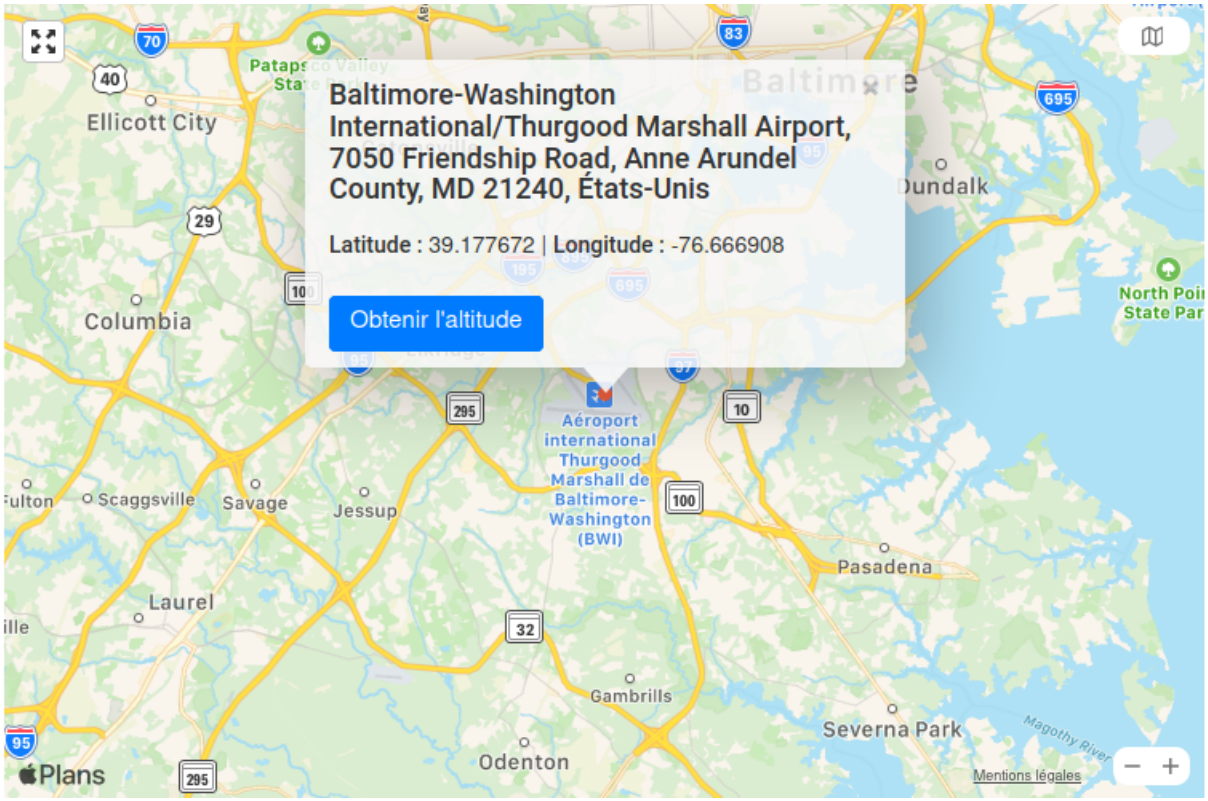
## Fichiers audiovisuel (Image/video)

Grâce à l'outil Autopsy, nous avons réussi à trouver les différentes images et vidéos présentes dans le disque "device1_laptop.e01".

Durant notre investigation, nous avons trouvé plusieurs images du chien pris en otage. Ces images ont été prises par un téléphone "BLUR HD1", l'entête de ces images contient des informations intéressantes comme la géolocalisation:

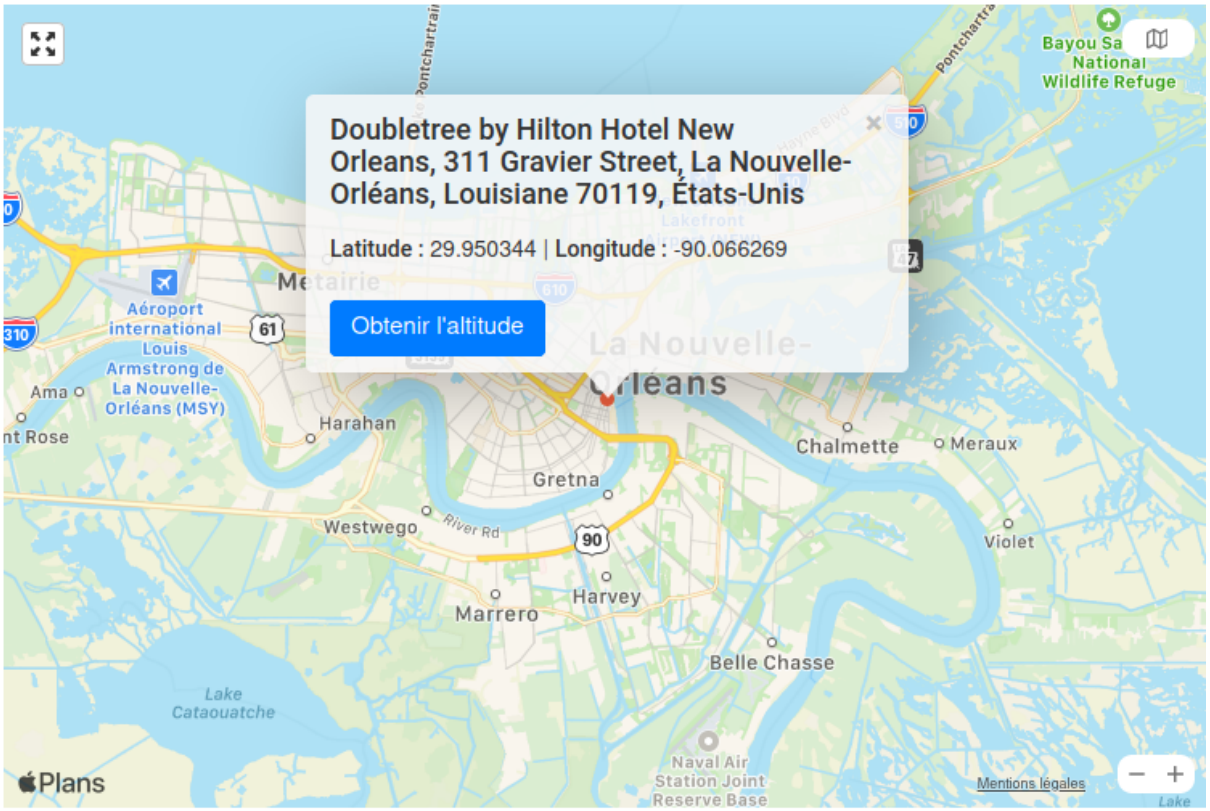

Information sur la position:

| | |
|---|---|
| GPS Latitude | 39 deg 10' 39.62" N |
| GPS Longitude | 76 deg 40' 0.87" W |
| GPS Position | 39 deg 10' 39.62" N, 76 deg 40' 0.87" W |

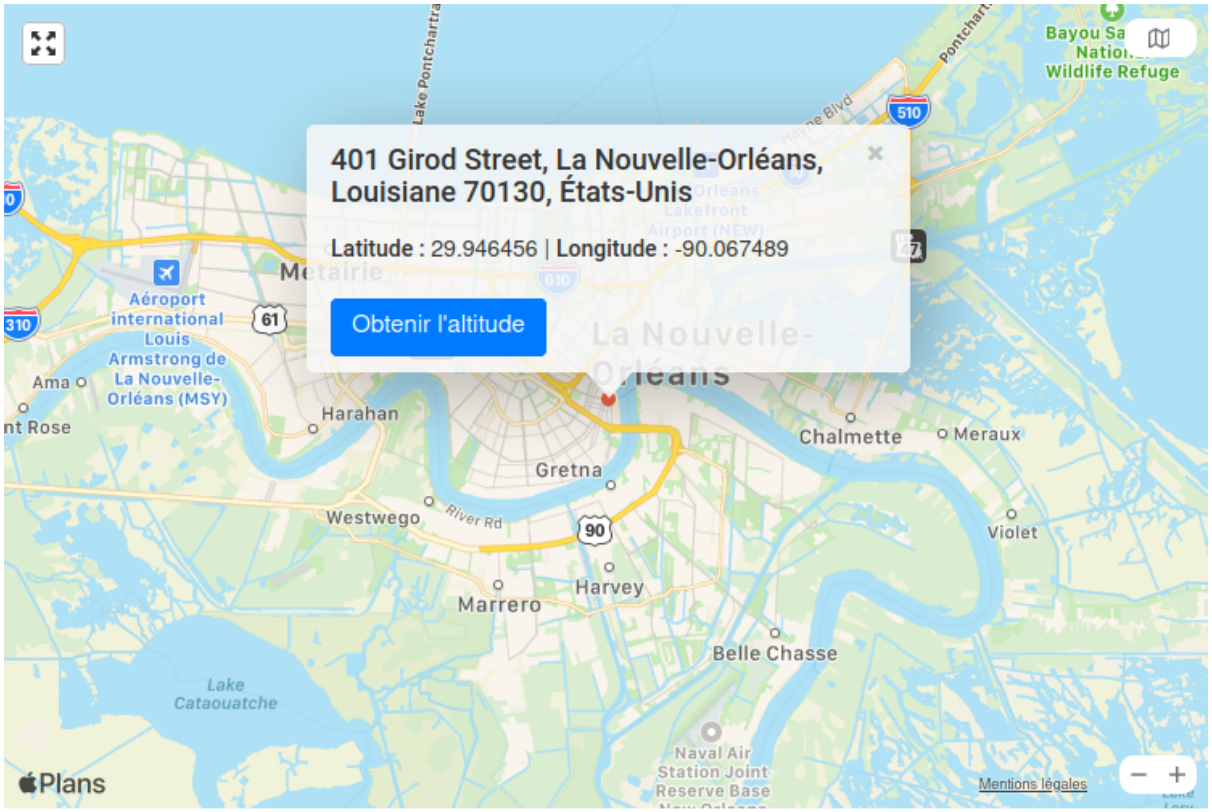

Baltimore-Washington International/Thurgood Marshall Airport, 7050 Friendship Road, Anne Arundel County, MD 21240, États-Unis
Latitude : 39.177672 | Longitude : -76.666908
Obtenir l'altitude
Ellicott City
Columbia
Scaggsville
Savage
Jessup
Laurel
Aéroport international Thurgood Marshall de Baltimore-Washington (BWI)
Pasadena
Gambrills
Severna Park
Odenton
Plans
Mentions légales


Autopsy

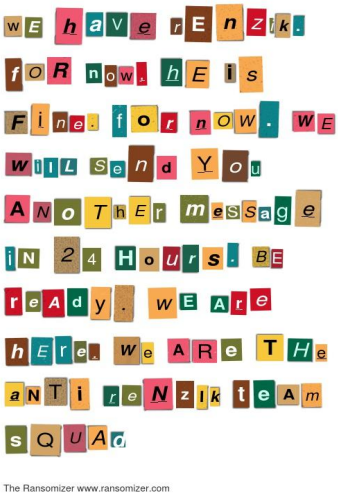
| | |
|---|---|
| GPS Latitude | 29 deg 57' 1.24" N |
| GPS Longitude | 90 deg 3' 58.57" W |
| GPS Position | 29 deg 57' 1.24" N, 90 deg 3' 58.57" W |

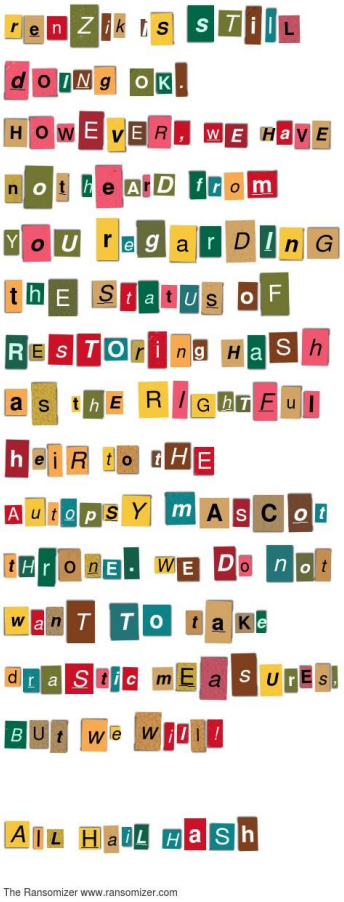


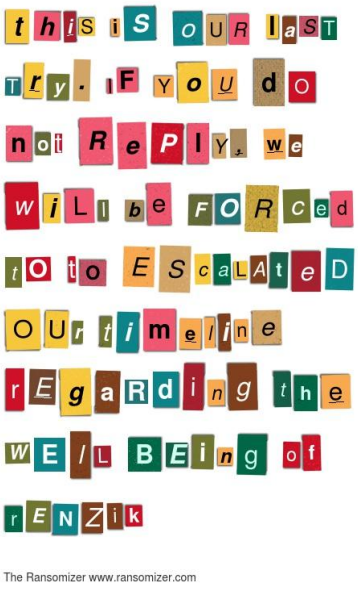
| | |
|---|---|
| GPS Latitude | 29 deg 56' 47.24" N |
| GPS Longitude | 90 deg 4' 2.96" W |
| GPS Position | 29 deg 56' 47.24" N, 90 deg 4' 2.96" W |




Nous avons également trouvé des lettres de rançons menaçant la vie du chien:






En continuant l'investigation des images du disque, nous avons remarqué la présence d'un tutoriel expliquant comment utiliser l'outil VeraCrypt. Cet outil permet chiffrer une partition. Nous avons donc décidé de trouver un fichier chiffré. Toujours grâce à l'outil Autopsy, nous avons identifié le fichier chiffré "IMPORTANT.jpg" et le mot de passe qui se trouvait dans un fichier supprimé "VCPW.txt".
La partition chiffrée contenait un fichier texte contenant le message suivant:

"*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*"

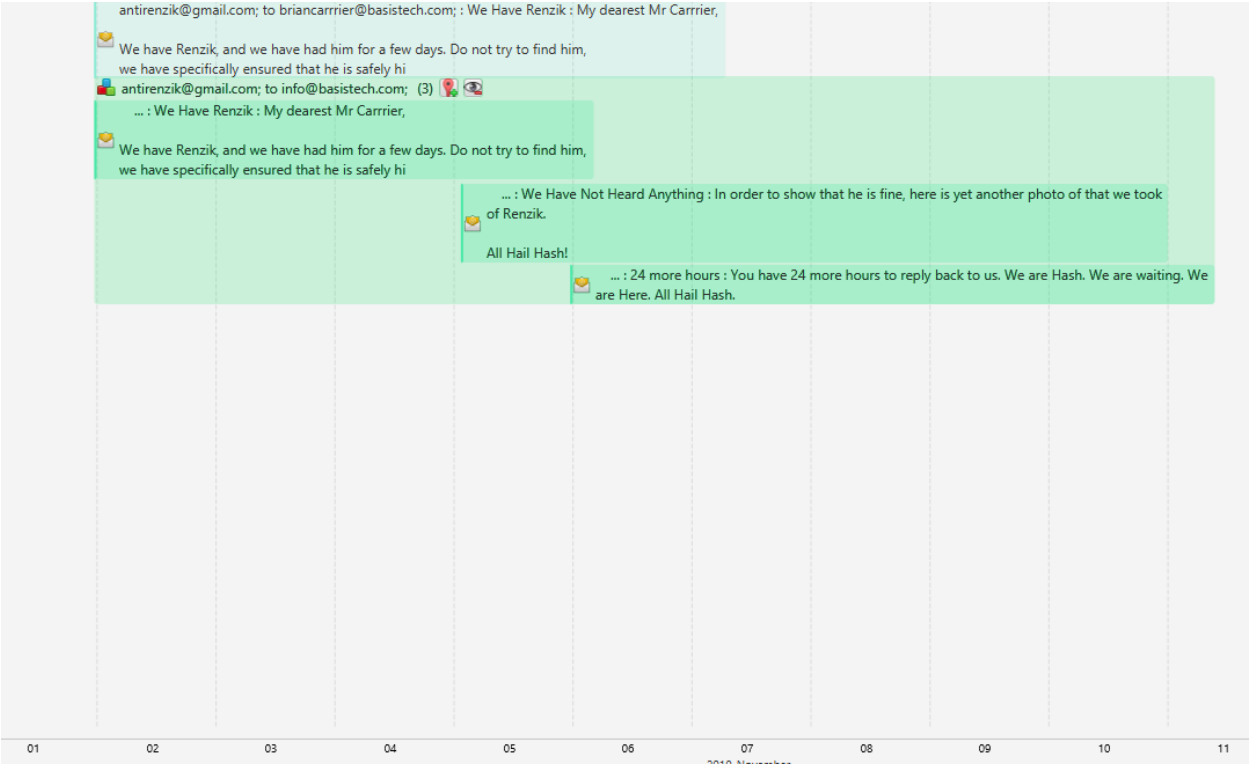
## Communication

Nous avons trouvé des traces de communication entre l'accusé et un éventuel complice, les mail des suspects sont peacockleprechaun@gmail.com et antirenzik@gmail.com.

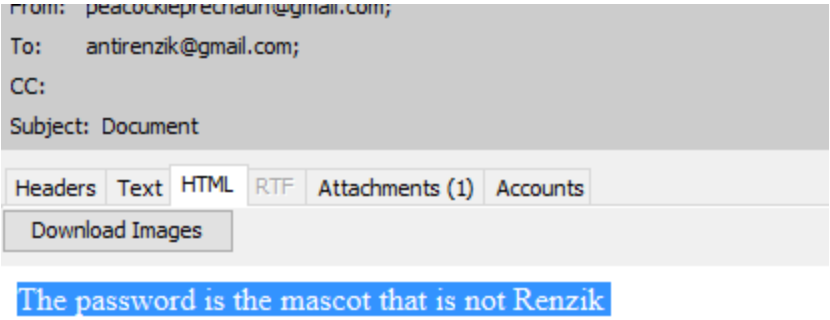
Ils ont échangé 13 emails pendant la période du premier novembre 2019 au 12 novembre 2019

| Date/Time | Event Type | |
|---|---|---|
| 2019-11-01 21:12:46 | Email | peacockleprechaun@gmail.com; to antirenzik@gmail.com; : Photos : Just sending on the photos that you requested. I wish you knew where your microSD card was! |
| 2019-11-01 21:24:57 | Email | peacockleprechaun@gmail.com; to antirenzik@gmail.com; : ARG questions : So, we've had Renzik for a few days and no one from Basis seems to know. I sent you a ransom note example from a private address last week, perhaps it |
| 2019-11-01 23:27:26 | Email | antirenzik@gmail.com; to peacockleprechaun@gmail.com; : Re: ARG questions : Agreed. I will send the first letter today.<br><br>All Hail Hash<br><br>On Fri, Nov 1, 2019 at 1:25 PM Peacock Leprechaun <<br>peacockleprechaun@gmail.com> wrote:<br><br>> |
| 2019-11-01 23:32:01 | Email | antirenzik@gmail.com; to peacockleprechaun@gmail.com; : Re: ARG questions : Idiot! You told me that his name was spelled Carrrier, but the email bounced and said the message could not be delivered. Guess we will just use the q |
| 2019-11-01 23:35:10 | Email | antirenzik@gmail.com; to peacockleprechaun@gmail.com; : Re: ARG questions : Also, what the heck is the "Anti Renzik Team Squad"? We are the Anti Renzik Group. I will make the ransom notes from now on. You are just going to con |
| 2019-11-04 18:10:30 | Email | antirenzik@gmail.com; to peacockleprechaun@gmail.com; : Status updates? : Its been a few days, how is Renizk doing? You are supposed to be checking in every day with an update. I know it was the weekend and I am sure you wer |
| 2019-11-04 22:23:08 | Email | peacockleprechaun@gmail.com; to antirenzik@gmail.com; : Document : The password is the mascot that is not Renzik |
| 2019-11-04 22:23:59 | Email | peacockleprechaun@gmail.com; to antirenzik@gmail.com; : Re: Status updates? : Renzik is doing ok so far. He seems to be annoyed every time I go down to visit. He growls at me a lot too. I think we are okay for another ransom not |
| 2019-11-05 23:16:54 | Email | antirenzik@gmail.com; to peacockleprechaun@gmail.com; : Still nothing : Still nothing heard from Basis. However, with the problems that you are continuing to have with Renzik, I think it is best to fly down to New Orleans |
| 2019-11-12 13:40:59 | Email | peacockleprechaun@gmail.com; to antirenzik@gmail.com; : Meetup? : It's been a few days since you said you were going to be down here, but I've not heard anything. Did you make it down yet? If so, what's the plan boss |
| 2019-11-12 19:09:36 | Email | peacockleprechaun@gmail.com; to antirenzik@gmail.com; : Re: Meetup? : That works for me. Although I have some news, this morning after giving him food, Renzik bit me. The bleeding has mostly stopped. Do you know what kin |
| 2019-11-12 21:12:23 | Email | antirenzik@gmail.com; to peacockleprechaun@gmail.com; : Re: Meetup? : For the bite: https://pets.webmd.com/dogs/dog-bites#1<br><br>For the dog type, I am not sure. Google didnt show any results for it either, so I really can |
| 2019-11-12 22:04:19 | Email | antirenzik@gmail.com; to peacockleprechaun@gmail.com; : Re: Meetup? : Yes, I arrived, although a few days later than I had initially planned. I assume that everything is going well with Renzik still. Haven't seen |

Ces échanges mentionnent des photos du chien kidnappé, des lieux de rendez-vous, des lettres envoyés.
Nous retrouvons aussi les mails échangés de rançons au groupe Basis tech.
Nous notons deux mails intéressants.
briancarrrier@basistech.com , info@basistech.com




Parmi ces mails échangés, nous avons constaté la présence d'un message qui nous a intrigué.




Le fichier attaché avec ce message "In order to ensure that Renzik is treated properly" pouvait aussi nous aider à avoir plus d'informations. Cette autre mascot "Hash" était mentionné dans un des messages de revendication du groupe AntiRenzik, que nous avons trouvé dans un fichier chiffré .

Le contenu de ce fichier attaché est le suivant:

*"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*"

## Artefact Web

Toujours grâce à l'outil Autopsy, nous avons récupéré l'historique web du criminel. Parmi ses recherches, les suivantes nous ont intriguées:

- "History","www.google.com","why is my ransom note not being answered","Chrome","2019-11-05 23:17:59 CET","device1_laptop.e01"

- "History","www.google.com","hostage negotiation tactics","Chrome","2019-11-05 23:18:25 CET","device1_laptop.e01"

- "History","www.google.com","new orleans parks french quarter","Chrome","2019-11-12 22:03:33 CET","device1_laptop.e01"

- "History","www.google.com","how to make a ransom note","Chrome","2019-11-05 23:17:19 CET","device1_laptop.e01"

- "History","www.google.com","cafe dumonde new orleans","Chrome","2019-10-31 04:43:55 CET","device1_laptop.e01"

- "History","www.google.com","transporting dog over state lines","Chrome","2019-11-05 23:18:43 CET","device1_laptop.e01"

Nous avons aussi pu récupérer un site web utilisé pour la création de doc, celui-ci contient un utilisateur dans l'URL avec l'autorisation auprès du webadmin. Il est donc possible de récupérer les fichier de celui-ci

https://www.offidocs.com/filemanager02.php?username=344421
https://www.offidocs.com/filemanager02.php?username=344421
https://www.offidocs.com/filemanager02.php?username=344421
https://www.offidocs.com/filemanager02.php?username=344421#elf_l1_Lw
https://www.offidocs.com/filemanager02.php?username=344421#elf_l1_Lw
https://www.offidocs.com/osessionx02/#/?username=guest13&password=server0113
https://www.offidocs.com/osessionx02/#/?username=guest13&password=server0113
https://www.offidocs.com/osessionx02/#/client/REVGQVVMVABjAGRlZmF1bHQ=?username=guest13&password=server0113
https://www.offidocs.com/osessionx02/#/client/REVGQVVMVABjAGRlZmF1bHQ=?username=guest13&password=server0113

## Recommendations

Compte tenu des informations trouvées  après analyse des disques. Nous pouvons affirmer que ce matériel a été utilisé dans le cadre de l'enlèvement de Renzik.

Le jury devrait considérer comme suspects principaux les membres du groupe AntiRenzik Team squad, les artefactes et échanges retrouvés sur l'ordinateur indiquent un complice à l'enlèvement du chien Renzik.