Année 2020-2021 Semestre 1

RAPPORT DE PROJET

PROJET FORENSIQUE

« NARCOS »

Projet réalisé en Master 2 option Cybersécurité à l'ISEN TOULON par :

Kelly BOUTEMEUR

Antoine VIGGIANO

Théo SODA

Valentin MAGNAN

Projet encadré par :

Julien VIGNOLLES

Stanislas ARNOUD

Frédéric PAILLART

ISEN ALL IS DIGITAL! TOULON | yncréa

1 SOMMAIRE

2 PRESENTATION DU SCENARIO

En raison des renseignements fournis par le gouvernement australien, deux passagers, John Fredricksen et Jane Esteban, ont été interceptés par les douanes à leur arrivée à Wellington, en Nouvelle-Zélande, en provenance de Brisbane.

Le renseignement intérieur a déclaré que Jane Esteban et John Fredricksen pourraient être impliqués dans des activités illégales. Les suspects ont chacun été fouillés par un douanier.

Les ordinateurs portables Windows des deux individus ont été trouvés dans leurs bagages, et ont ainsi été récupérés pour être analysés.

Après une recherche plus poussée de la doublure de la valise, un kilogramme de méthamphétamine a été localisé.

Les deux suspects ont été emmenés dans des salles d'interrogatoire séparées où ils ont été interrogés.

Jane Esteban a déclaré qu'elle devait livrer la valise à la « bibliothèque d'Eastbourne », mais si tout le reste échouait, alors ils devaient la livrer au 666 Rewera Avenue, Petone.

Les douanes et la police ont par la suite fait une descente à cette adresse où de la drogue, des armes à feu et un ordinateur de bureau ont été trouvés dans la maison du suspect, Steve Kowhai.

En tant qu'enquêteur médico-légal des douanes, nous avons analysé les images et les vidages de mémoire des ordinateurs appartenant à Jane, John et Steve. Nous avons effectué une analyse forensique afin de mieux comprendre leurs motivations, leurs buts et leurs objectifs.

3 EXECUTIVE SUMMARY

Lors de nos recherches, notre équipe d'investigation des douanes a retrouvé des preuves incriminant 2 des 3 suspects de cette affaire.

Nous avons pu déduire que le 3ème suspect, Jane Esteban, n'est autre qu'un agent de la police australienne sous couverture. En effet, de nombreux éléments le montrent : son historique de navigation rempli de recherches tels que « comment agir comme une droguée » ou « comment être un agent sous couverture », ainsi que sa corbeille contenant le badge de la police australienne. De plus, son ordinateur contenait un dossier nommé Quasar, dans lequel était présent un sous-dossier John. Elle avait en effet infecté le PC de John avec le RAT Quasar (Remote Administration Tool) incluant un Keylogger, nous avons les logs de John sur 4 jours, du 30 janvier au 2 février 2019.

Steve et John ont quant à eux de nombreuses discussions (sur discord et par mail) concernant des commandes/livraisons de drogue(méthamphétamine), ils ont même utilisé des méthodes de stéganographie et de chiffrement pour cacher des éléments incriminants de leurs conversations.

4 DEMARCHE DE L'ANALYSE

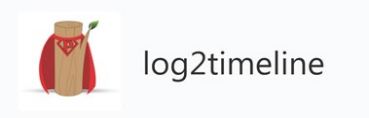
Pour mener à bien notre enquête, nous avons réalisé 3 dumps disques et 3 dumps mémoires des ordinateurs appartenant à Steve Kowhai, John Fredricksen et Jane Esteban, ils sont respectivement rangés dans les dossiers Narcos-1, Narcos-2 et Narcos-3.

Nous avons utilisé Sharepoint comme drive pour rassembler les éléments que l'on trouvait et Teams et Messenger pour communiquer entre nous.

4.1 ANALYSE DES DISQUES

Nous avons commencé par monter les images disques pour naviguer dans les disques et récupérer des preuves incriminant nos suspects.

Nous les avons également analysés avec Autopsy (historique de navigation, cache, cookies, fichiers supprimés…). Le temps d'analyse étant relativement long (~12h par image disque) et les résultats très volumineux, nous n'avons pas eu le temps d'y rechercher beaucoup de preuves.



Nous avons aussi récupéré des artefacts tels que les prefetchs (en utilisant log2timeline et psort.py pour les mettre en forme), les fichiers récents, et les hives des 3 disques.

Nous nous sommes également basés sur le poster Windows Forensique Analysis du SANS qui recense les emplacements de nombreux artefacts. (https://www.sans.org/security-resources/posters/windows-forensique-analysis/170/download)

4.2 ANALYSE MEMOIRE

Nous avons essayé les profils Volatility associés aux version Windows des PC mais ceux-ci ne correspondaient malheureusement pas, nous avons donc essayé également avec tous les profils de la dernière version de Volatility, sans succès.

5 RESULTATS DE L'ANALYSE

5.1 ARTEFACTS

Nous avons extrait des informations utiles de ces artefacts, tels que les fichiers récents, les versions des ordinateurs et leurs fuseaux horaires, les prefetchs.

On peut voir que certains fichiers récents de Jane ont un rapport avec la méthamphétamine, un paquet, des billets d'avion… Nous verrons par la suite à quoi ils correspondent.

Extension	Absolute Path	Opened On
gif	My Computer\Pictures\bomba-etkisi.gif	2019-01-29 03:06:25
jpg	My Computer\Documents\Misc\dropoff.jpg	2019-02-02 01:06:06
odt	My Computer\Documents\Misc\Memo Things.odt	2019-01-29 23:44:49
PNG	My Computer\Documents\Misc\flightbookings.PNG	2019-02-02 02:28:45
jpg	My Computer\Downloads\Misc\package.jpg	
jpg	My Computer\Pictures\eight_col_patches_crp.jpg	
jpg	My Computer\Pictures\price-meth-bust-4.jpg	
jpg	My Computer\Pictures\620x349.jpg	
jpg	My Computer\Documents\Misc\airport crystals.jpg	
jpg	My Computer\Documents\Misc\Method run.jpg	
jpg	My Computer\Pictures\33d49c521dd812b9421dff05dc47e5bb.jpg	
jpg	My Computer\Pictures\594bc6bd3f46ff331476280671d7745c.jpg	
jpg	My Computer\Pictures\7i2t6tk.jpg	
jpg	My Computer\Pictures\ee9a310ff1c7018bdbf1b201c5de5c63.jpg	
jpg	My Computer\Pictures\9648de1b909919145a4fe440cf89f576--gary-larson-cartoons-bad-day.jpg	
jpg	My Computer\Pictures\diving-crayfish-960x540.jpg	

FIGURE 1 : FICHIERS RECENTS DE JANE (OPEN/SAVE MRU)

regid.1991-06.com.microsoft_Windows-10-Pro.swidtag

```
<?xml version="1.0" encoding="utf-8"?>
<software_identification_tag xmlns="http://standards.iso.org/iso/19770/-2/2009/schema.xsd">
    <entitlement_required_indicator>true</entitlement_required_indicator>
    <product_title>Windows 10 Pro</product_title>
    <product_version>
        <name>10.0.17763.1</name>
        <numeric>
            <major>10</major>
            <minor>0</minor>
            <build>17763</build>
            <review>1</review>
        </numeric>
    </product_version>
    <software_creator>
        <name>Microsoft Corporation</name>
        <regid>regid.1991-06.com.microsoft</regid>
    </software_creator>
    <software_licensor>
        <name>Microsoft Corporation</name>
        <regid>regid.1991-06.com.microsoft</regid>
    </software_licensor>
    <software_id>
        <unique_id>Windows-10-Pro</unique_id>
        <tag_creator_regid>regid.1991-06.com.microsoft</tag_creator_regid>
    </software_id>
    <tag_creator>
        <name>Microsoft Corporation</name>
        <regid>regid.1991-06.com.microsoft</regid>
    </tag_creator>
</software_identification_tag>
```

FIGURE 2 : VERSION WINDOWS STEVE (VIA FICHIER REGID)

Value Name	Value Ty	Data
SystemRoot	RegSz	C:\Windows
BuildBranch	RegSz	rs4_release
BuildGUID	RegSz	ffffffff-ffff-ffff-ffff-ffffff
BuildLab	RegSz	17134.rs4_release.18041
BuildLabEx	RegSz	17134.1.amd64fre.rs4_re
CompositionEditionID	RegSz	Enterprise
CurrentBuild	RegSz	17134
CurrentBuildNumber	RegSz	17134
CurrentMajorVersionN	RegDword	10
CurrentMinorVersionN	RegDword	0
CurrentType	RegSz	Multiprocessor Free
CurrentVersion	RegSz	6.3
EditionID	RegSz	Professional
EditionSubManufacture	RegSz	
EditionSubstring	RegSz	
EditionSubVersion	RegSz	
InstallationType	RegSz	Client
InstallDate	RegDword	1548702766
ProductName	RegSz	Windows 10 Pro
ReleaseId	RegSz	1803
SoftwareType	RegSz	System
UBR	RegDword	523
PathName	RegSz	C:\Windows
ProductId	RegSz	00330-80000-00000-AA3
DigitalProductId	RegBinary	A4-00-00-00-03-00-00-00
DigitalProductId4	RegBinary	F8-04-00-00-04-00-00-00
RegisteredOwner	RegSz	JohnF
RegisteredOrganizatior	RegSz	
InstallTime	RegQword	131931763666846611

FIGURE 3 : VERSION WINDOWS JOHN (VIA REGKEY)

Value Name	Value Type	Data	Value Slack
Bias	RegDword	4294966576	
DaylightBias	RegDword	4294967236	
DaylightName	RegSz	@tzres.dll,-741	00-00-00-00
DaylightStart	RegBinary	00-00-09-00-05-00-02-00-00-00-00-00-00-00-00-00	50-46-5A-00
StandardBias	RegDword	0	
StandardName	RegSz	@tzres.dll,-742	00-00-00-00
StandardStart	RegBinary	00-00-04-00-01-00-03-00-00-00-00-00-00-00-00-00	B0-4F-5A-00
TimeZoneKeyName	RegSz	New Zealand Standard Time	
DynamicDaylightTimeDisabled	RegDword	0	
ActiveTimeBias	RegDword	4294966516	

FIGURE 4 : TIMEZONE STEVE (VIA REGKEY)

Nous pouvons maintenant créer un tableau récapitulatif des PC des suspects. Ceux-ci sont tous sous Windows 10 Pro avec des versions de build différentes. John et Jane ont leurs PC configurés avec le fuseau horaire UTC+10, correspondant à l'est de l'Australie. Celui de Steve est sur le fuseau UTC+12 correspondant à la Nouvelle-Zélande.

File	User	Timezone	OS	Version (major.minor.build.review)
Narcos-1	Steve	UTC+12	Windows 10 Pro	10.0.17763.1
Narcos-2	John	UTC+10	Windows 10 Pro	10.0.17134.1
Narcos-3	Jane	UTC+10	Windows 10 Pro	10.0.16299.?

FIGURE 5 : RECAPITULATIF

5.2 CORBEILLES

Nous avons inspecté les corbeilles des 3 suspects et y avons trouvé des preuves intéressantes.

5.2.1 STEVE

Sur le PC de Steve, nous avons découvert :

Une image de vêtement du Mongrel Mob Fatherland qui est un gang de Nouvelle-Zélande, très actif dans tout le pays et composé de plus de 1000 membres. Ils pratiquent toutes sortes d'activités illégales.

FIGURE 6 : IMAGE DU MONGREL MOB FATHERLAND

Cette image qui semble être le butin ou la réserve de Steve :

FIGURE 7 : IMAGE D'UN BUTIN DE CASH ET DE DROGUES

Et cette image de méthamphétamine que l'on a également retrouvée dans son cache web à l'url suivant :

https://inm-baobab-prod-eu-west-1.s3.amazonaws.com/public/inm/media/image/2016/05/27/40037258meth.jpg

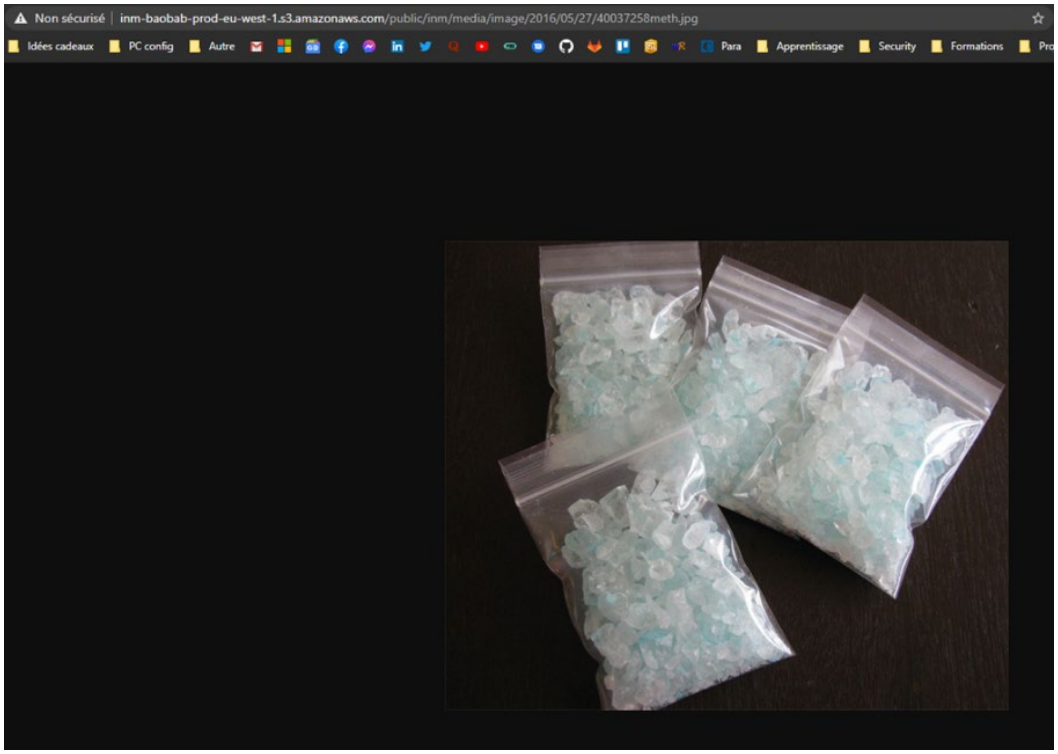


FIGURE 8 : IMAGE METH ON S3 BUCKET

Nous avons tenté de lister les fichiers du s3 bucket, mais celui-ci était correctement configuré (authentification nécessaire pour exécuter des opérations sur celui-ci).

```
C:\Users\valen>aws s3 ls s3://inm-baobab-prod-eu-west-1 --no-sign-request

An error occurred (AccessDenied) when calling the ListObjectsV2 operation: Access Denied
```

FIGURE 9 : TENTATIVE LS S3 BUCKET

En poursuivant nos recherches sur ce bucket, nous avons découvert qu'il appartenait à Pinterest.

N'ayant pas d'autorisations de la part de la plateforme, nous avons décidé de ne pas aller plus loin dans la recherche de faille de configuration du bucket.

5.2.2 JANE

Nous avons trouvé un badge de la police fédérale australienne dans la corbeille de Jane, ce qui pourrait prouver qu'elle est policière sous couverture.

FIGURE 10 : BADGE POLICE FEDERALE AUSTRALIENNE

5.2.3 JOHN

Pour finir, nous n'avons rien trouvé d'intéressant dans la corbeille de John.

5.3 QUASAR RAT

Dans les logs de quasar, nous avons trouvé d'autres informations intéressantes, dont notamment des conversations, des identifiants...

5.3.1 FICHIER CHIFFRE

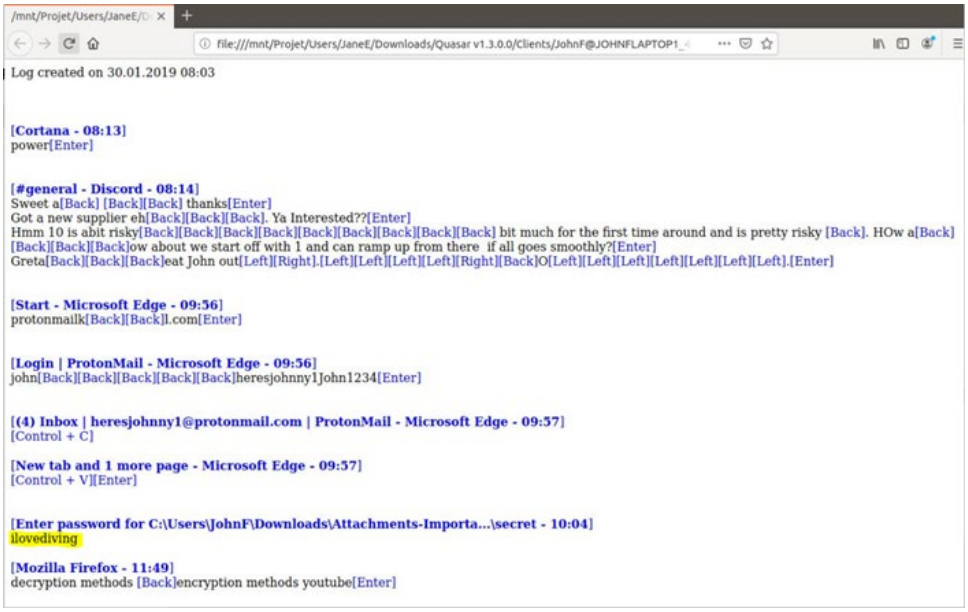


FIGURE 11 : QUASAR 30 JANVIER

Dans les logs du 30 janvier, plusieurs informations semblent intéressantes :

- Nous pouvons voir une partie d'une conversation Discord indiquant que nos suspects envisageaient de livrer 10kg de drogue, mais qu'afin d'éviter de prendre trop de risque, seulement 1kg de drogue sera livré. Il s'agit certainement du kilo de drogue retrouvé dans la valise de John. Nous verrons par la suite l'entièreté des conversations Discord.
- Un mot de passe ("ilovediving") utilisé pour le chiffrement du fichier secret qui a été retrouvé sur le PC de John.
- Les identifiants ProtonMail de John.

Ayant remarqué la présence du logiciel TrueCrypt sur le PC de John, nous l'avons réutilisé pour déchiffrer le fichier secret à l'aide du mot de passe « ilovediving » et avons obtenu le document Memo Things.odt ci-dessous :

Crystal Method

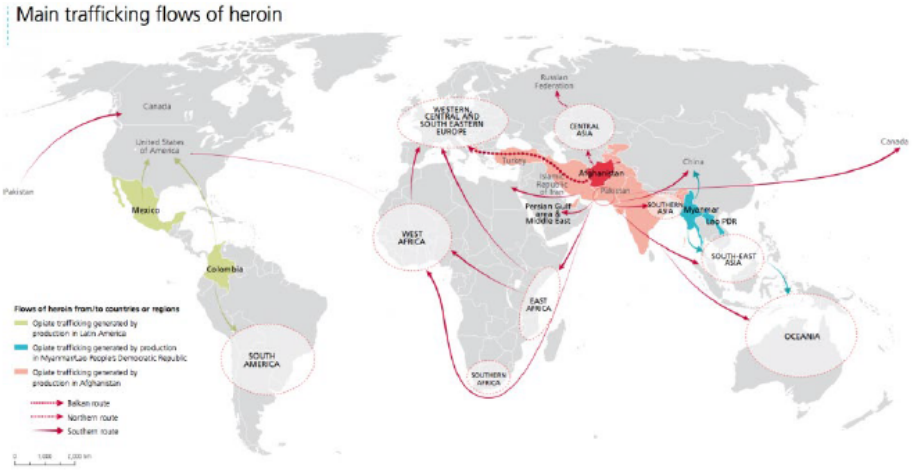
Destination – Wellington
Product – 1 kg crystal
Source – Brisbane (JF)

Wellington is part of the lower north island of New Zealand. It is accessable by road and sea. As tempting as the sea is, be aware that the coast of NZ may seem ideal, but everyone knows it's vulnerable as there have been several news reports about it.

The product is coming from Brisbane, Australia and as a result, will need to be delivered by sea or plane. Shipping the product would be ideal, the risk of detection is lower but would result in higher costs for a small amount of product. The product being delievered is only a test to check it's quality and will be the deciding factor in any decision to continue doing business with you. If the product is up to scratch, I will buy a larger supply next time. If we continue to do business it might be more practical to use shipping for future transactions.

This consignment will be delievered by plane, which will decrease travel time and lower the cost for all parties involved. Delievery by plane will bring along with it its own complications such as concealment, security screening/checks and drug dogs. I trust that you are aware of the risks and will take all necessary precautions.

Below is a map of drup flows from countires, could give us some info for later trades and where we can get more product from in the future.



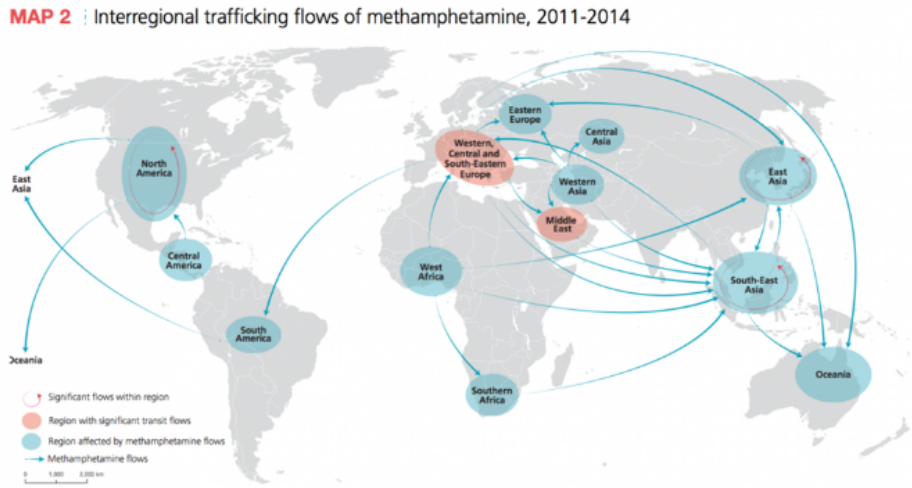


FIGURE 12 : MEMO THINGS.ODT

Ce document indique que :

- Le produit provient de Brisbane, en Australie et a comme destination la Nouvelle-Zélande. Il devra par conséquent être **livré par mer ou par avion**.
- **L'expédition par bateau du produit serait idéale car le risque de détection est moindre mais cela entraînerait des coûts plus élevés pour une petite quantité de produit**.
- Le produit livré n'est qu'un **test pour vérifier sa qualité**.
- **Si le produit est à la hauteur**, **une plus grande quantité serait achetée la prochaine fois.**
- **S'il y a d'autres commandes à l'avenir**, il serait plus pratique **d'utiliser les voies maritimes**. **L'envoi de test sera expédié par avion**, ce qui réduira le temps de trajet et les coûts pour les parties concernées.
- **La livraison par avion entraînera des complications telles que la dissimulation, les contrôles de sécurité et les chiens**. Il faudra ainsi prendre toutes les précautions nécessaires.

5.3.2 STEGANOGRAPHIE

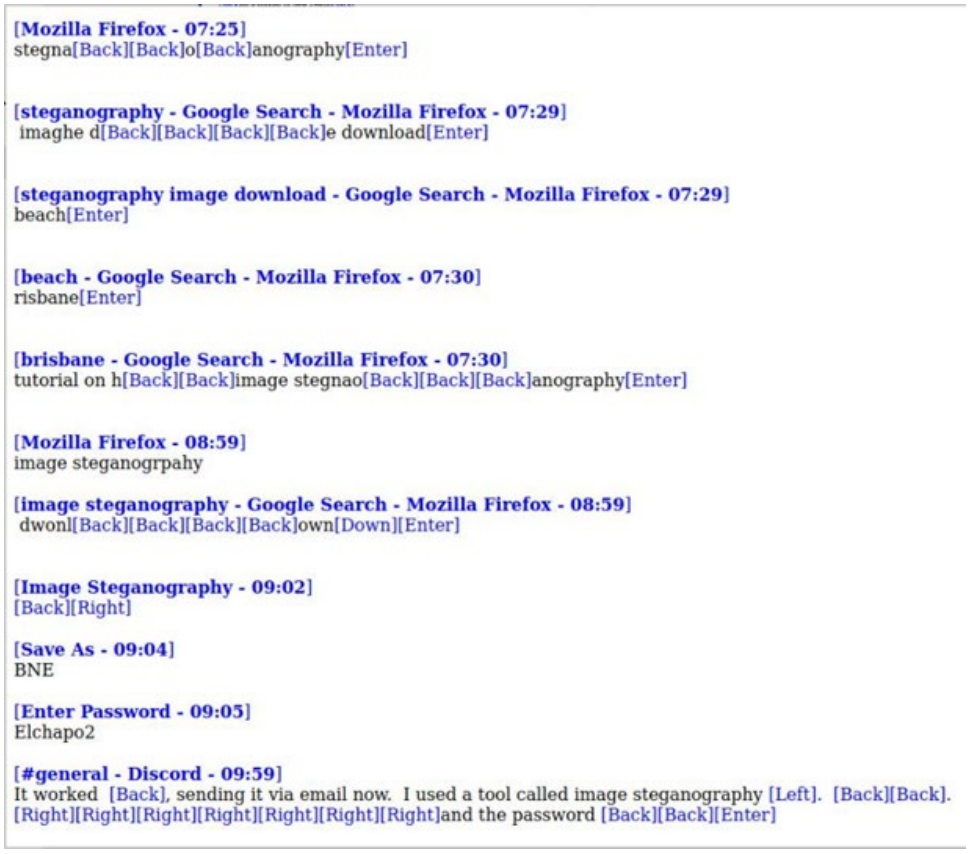


FIGURE 13 : QUASAR 1^{er} FEVRIER

Dans les logs du 1er février, nous avons remarqué qu'un fichier intitulé BNE était utilisé pour de la stéganographie et qu'il était lié au mot de passe « Elchapo2 ».

Nous en avons déduit que John avait utilisé un logiciel de stéganographie pour cacher une information dans cette image BNE et ainsi pouvoir l'envoyer à Steve en toute discrétion.

Le logiciel de stéganographie et l'image BNE étant toujours présents sur le PC de John, nous avons réutilisé le logiciel sur une VM Windows sans accès internet pour déchiffrer le fichier caché.

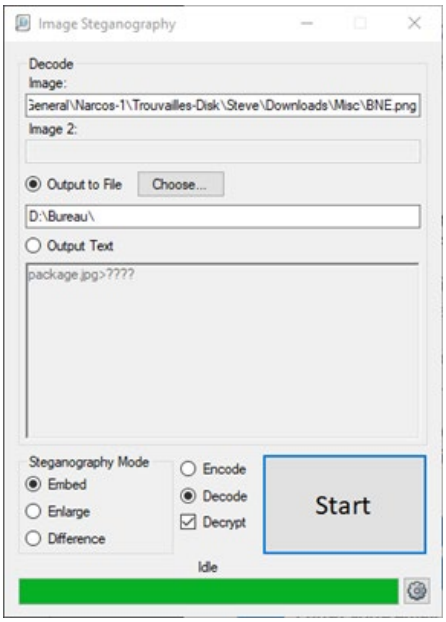


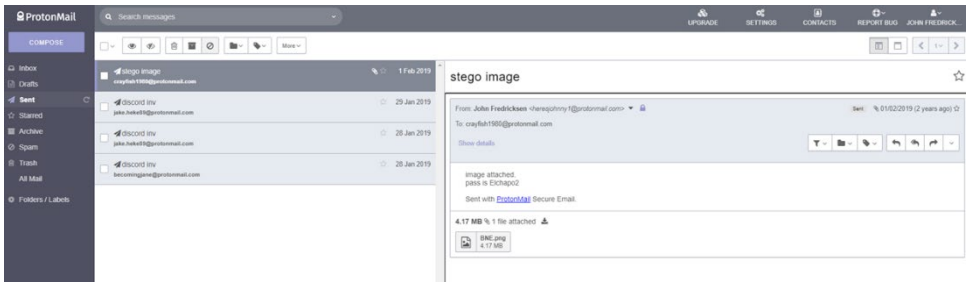
FIGURE 14 : LOGICIEL STEGANOGRAPHIE

FIGURE 15 : IMAGE BNE

Le fichier caché était une photo du sac de voyage avec la doublure ouverte pour y cacher la drogue.

FIGURE 16 : PACKAGE

Qui plus est, nous avons également retrouvé cette image BNE en pièce jointe d'un mail envoyé par John à Steve :



5.3.3 Identifiants Proton Mail & Discord

Comme remarqué dans les logs Quasar du 30 janvier, nous avons les identifiants Proton Mail de John.

Courriel : heresjohnny1@protonmail.com

Mot de passe : John1234

5.3.4 Configuration du RAT

Dans la corbeille de Jane (Fichier Default.xml), nous avons trouvé la configuration de Quasar pour le PC de John. On peut voir ci-dessous que :

- Le serveur de log a le port 4782 ouvert à l'adresse IP 202.2.12.13, probablement l'adresse publique du réseau auquel se connecte Jane.
- Le malware s'installe sous le nom d'updater Java
- Le Keylogger est activé
- Le répertoire de log de Quasar est caché sur le PC de Jane.

```
<settings>
  <Tag>John</Tag>
  <Hosts>202.2.12.13:4782;</Hosts>
  <Password>1234</Password>
  <Delay>3000</Delay>
  <Mutex>QSR_MUTEX_CxO1HuVkIgYkhY4NA9</Mutex>
  <InstallClient>True</InstallClient>
  <InstallName>updater</InstallName>
  <InstallPath>1</InstallPath>
  <InstallSub>Java</InstallSub>
  <HideFile>True</HideFile>
  <HideSubDirectory>True</HideSubDirectory>
  <AddStartup>True</AddStartup>
  <RegistryName>Java updater</RegistryName>
  <ChangeIcon>True</ChangeIcon>
  <IconPath>C:\Users\JaneE\Documents\contact_card.ico</IconPath>
  <ChangeAsmInfo>False</ChangeAsmInfo>
  <Keylogger>True</Keylogger>
  <LogDirectoryName>Logs</LogDirectoryName>
  <HideLogDirectory>True</HideLogDirectory>
  <ProductName>
  </ProductName>
  <Description>
  </Description>
  <CompanyName>
  </CompanyName>
  <Copyright>
  </Copyright>
  <Trademarks>
  </Trademarks>
  <OriginalFilename>
  </OriginalFilename>
  <ProductVersion>
  </ProductVersion>
  <FileVersion>
  </FileVersion>
</settings>
```

Figure 17 : Configuration Quasar

5.4 PROTON MAIL

Nous avons testé les identifiants de John sur le site de ProtonMail et il s'avérait que les identifiants fonctionnaient.

Nous avons pu trouver 2 éléments intéressants sur la boîte mail de John :

- Le lien d'un serveur Discord

FIGURE 18 : LIEN SERVEUR DISCORD

- Ainsi que le fichier "secret" précédemment envoyé en pièce jointe par Steve

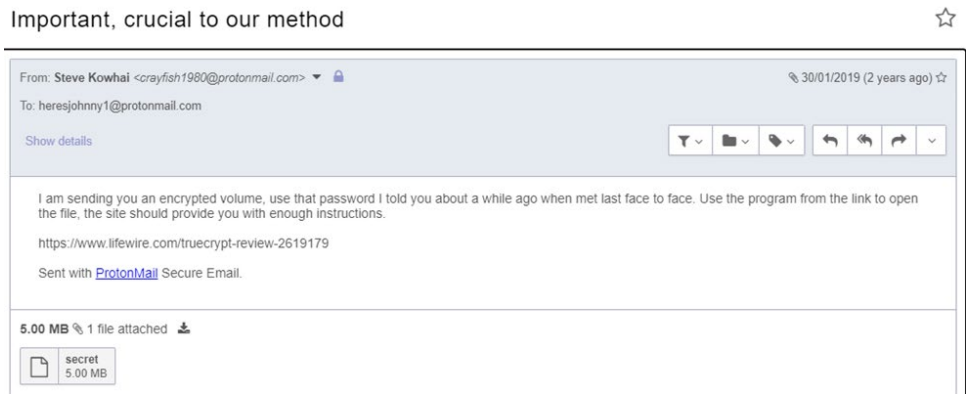


FIGURE 19 : FICHIER SECRET EN PJ

5.5 DISCORD

5.5.1 VIA LE CACHE

Nous avons retrouvé 2 types d'éléments dans le cache Discord des suspects : les Drafts (Brouillon des messages) et des images.

Pour extraire les messages nous avons écrit une regex :

{"\w+":{"\d+":{"\w+":\d+,"\w+":"[^"]+"}},"\w+":\d}


```
{"_state":{"539550615072800768":{"timestamp":1548802718174,"draft":"New supplier eh? Definitely Interested!  Can I get 10 keys of it delivered to Wellington"}},"_version":0}
{"_state":{"539550615072800768":{"timestamp":1548803049066,"draft":"Yeah yeah probably wiser, good one. In fact I have already put a document together in anticipation of chatting with you.  I'll send it through now. It contains some information regarding how I see this working out. Let me know what you think once you have read it. S O"}},"_version":0}
{"_state":{"539550615072800768":{"timestamp":1548969372835,"draft":"Good Thinking, I already know how. Heard of steganography?"}},"_version":0}
{"_state":{"539550615072800768":{"timestamp":1548969682114,"draft":"A way of hiding one image within another. There's a simple application called 'Image Steganography'."}},"_version":0}
{"_state":{"539550615072800768":{"timestamp":1548979899479,"draft":"Ya.. I just told you about the tool :face_palm:  Received it. Will check to see if it works and confirm soon. "}},"_version":0}
{"_state":{"539550615072800768":{"timestamp":1549074636655,"draft":"Good. Meet at the Eastbourne library and if we miss each other come to 666 Rewera Avenue, Petone."}},"_version":0}
```


FIGURE 20 : DRAFT DISCORD STEVE


```
{"_state":{"539556917140521030":{"timestamp":1548894459021,"draft":"Good, now that's what I wanted to hear. Here is the plan. You and I will be acting like a couple travelling on a holiday to New Zealand. This is what I want you to do: Look the part, act normal, and don't tell anyone about what we're doing. Understood?  "}},"_version":0}
{"_state":{"539556917140521030":{"timestamp":1548894646549,"draft":"Good. Talk tomorrow at 3PM or else"}},"_version":0}
{"_state":{"539556917140521030":{"timestamp":1548968561259,"draft":"ah bugger wrong person, disregard"}},"_version":0}
{"_state":{"539550615072800768":{"timestamp":1548968664658,"draft":"I  want to send an image an image of something to you but it needs to be done safely. Any ideas?"}},"_version":0}
{"_state":{"539550615072800768":{"timestamp":1548969435692,"draft":"No what's that?"}},"_version":0}
{"_state":{"539550615072800768":{"timestamp":1548969865411,"draft":"Okay, I'll have a look and see if I can get it to work and then send the image through "}},"_version":0}
{"_state":{"539550615072800768":{"timestamp":1548979265902,"draft":"It worked , sending it and the password via email now.  I used a tool called image steganography.. "}},"_version":0}
{"_state":{"539556917140521030":{"timestamp":1548986354248,"draft":"Right. What's your full name and date of birth? I need it for booking the flights ASAP."}},"_version":0}
{"_state":{"539556917140521030":{"timestamp":1549062103942,"draft":"Flights booked. I'll pick you up from the Woolworths (133 Oxley Station Rd, Oxley QLD 407, Australia) at ... Just bring yourself I'll cover everything else "}},"_version":0}
{"_state":{"539550615072800768":{"timestamp":1549072603960,"draft":"See you soon. John out"}},"_version":0}
```


FIGURE 21 : DRAFT DISCORD JOHN


```
{"_state":{"539556917140521030":{"timestamp":1548732544761,"draft":"Got any of that ice??"}},"_version":0}
{"_state":{"539556917140521030":{"timestamp":1548732661282,"draft":"Also I've got some friends that want to score too. Here's their contact card"}},"_version":0}
{"_state":{"539556917140521030":{"timestamp":1548892670459,"draft":"The  usual"}},"_version":0}
{"_state":{"539556917140521030":{"timestamp":1548893363366,"draft":"What is it..."}},"_version":0}
{"_state":{"539556917140521030":{"timestamp":1548893818636,"draft":"Umm I don't know, sounds pretty risky "}},"_version":0}
{"_state":{"539556917140521030":{"timestamp":1548893910236,"draft":"Err nah I'm not keen "}},"_version":0}
{"_state":{"539556917140521030":{"timestamp":1548894228331,"draft":"WHAT!  Please, I swear whatever you need I'll do it... I've put them through enough as it is. What do you want from me??"}},"_version":0}
{"_state":{"539556917140521030":{"timestamp":1548894506472,"draft":"Yes John got it "}},"_version":0}
{"_state":{"539556917140521030":{"timestamp":1549058223270,"draft":"My full name is Jane Esteban and my birthday is 13/07/1992"}},"_version":0}
{"_state":{"539556917140521030":{"timestamp":1549063700744,"draft":"I'll be there "}},"_version":0}
```


FIGURE 22 : DRAFT DISCORD JANE

Nous avons tenté de recréer les conversations à partir des drafts :

```
31/01/2019
JANE : Got any of that ice??
JANE : Also I've got some friends that want to score too. Here's their contact card
JOHN : Yo, what you after?
JANE : The  usual
JOHN : Also that contact card didn't open and I can't be bothered with new clients got bigger fish right now...
JOHN : Aight cool, umm actually I have a proposition for ya
JANE : What is it...
JOHN : I have a business dealing happening overseas and I need you to accompany me as cover. Everything will be paid for but you need to keep your trap shut
JANE : Umm I don't know, sounds pretty risky
JOHN : Yea I understand but ill make it worth your while
JANE : err nah I'm not keen
JOHN : I didn't want to do this but, you leave me no choice
JOHN : You don't wanna see them hurt do ya
JANE : WHAT!  Please, I swear whatever you need I'll do it... I've put them enough as it is. What do you want from me??
JOHN : Good, now that's what I wanted to hear. Here is the plan. You and I will be acting like a couple travelling on a holiday to New Zealand. This is what I want you to do: Look the part, act normal, and don't tell anyone about what we're doing. Understood?
JANE : Yes John got it
JOHN : Good. Talk tomorrow at 3PM or else
JANE : I'll be there
01/02/2019
JOHN : Right. What's your full name and date of birth? I need it for booking the flights ASAP.
JANE : My full name is Jane Esteban and my birthday is 13/07/1992
02/02/2019
JOHN : Flights booked. I'll pick you up from the Woolworths (133 Oxley Station Rd, Oxley QLD 407, Australia) at ... Just bring yourself I'll cover everything else
JOHN : See you soon. John out
```

FIGURE 23 : RECONSTITUTION CONVERSATION JANE / JOHN

```
30/01/2019
JOHN : Sweet thanks
JOHN : Got a new supplier. Ya interested??
STEVE : New supplier eh? Definitely Interested!  Can I get 10 keys of it delivered to Wellington
JOHN : Hmm 10 is a bit much for the first time around and is pretty risky. How about we start off with 1 and can ramp up from there  if all goes smoothly?
STEVE : Yeah yeah probably wiser, good one. In fact I have already put a document together in anticipation of chatting with you. I'll send it through now. It contains some information regarding how I see this working out. Let me know what you think once you have read it. S O
JOHN : Great. John Out.
01/02/2019
JOHN : ah bugger wrong person, disregard
JOHN : I  want to send an image an image of something to you but it needs to be done safely. Any ideas?
STEVE : Good Thinking, I already know how. Heard of steganography?
JOHN : No what's that?
STEVE : A way of hiding one image within another. There's a simple application called 'Image Steganography'.
JOHN : Okay, I'll have a look and see if I can get it to work and then send the image through
JOHN : It worked , sending it and the password via email now.  I used a tool called image steganography..
STEVE : Ya.. I just told you about the tool :face_palm:  Received it. Will check to see if it works and confirm soon.
STEVE : Good. Meet at the Eastbourne library and if we miss each other come to 666 Rewera Avenue, Petone.
```

FIGURE 24 : RECONSTITUTION CONVERSATION JOHN / STEVE

Dans le cache Discord du PC de Steve, nous avons également trouvé l'image d'un billet d'avion aller-retour Brisbane/Wellington pour 2 adultes avec les heures de départ et d'arrivée.

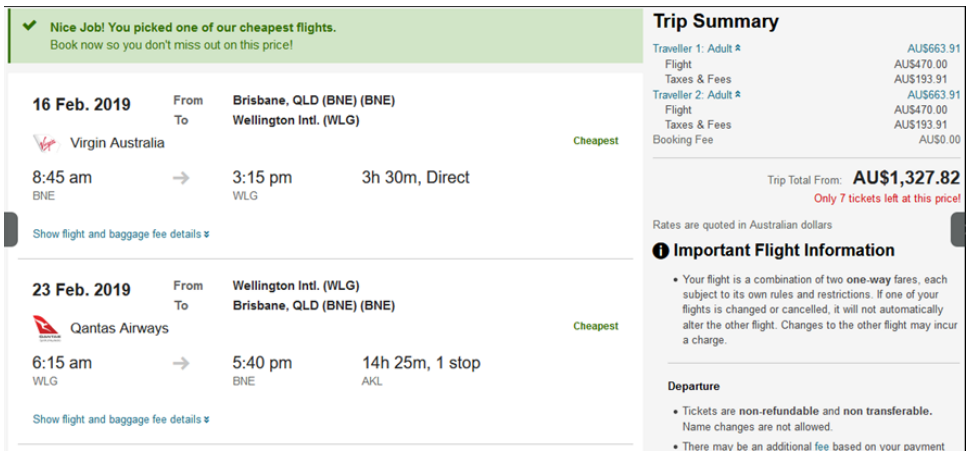


FIGURE 25 : BILLET BRISBANE-WELLINGTON

5.5.2 VIA L'APPLICATION

Nous avons tenté de nous connecter au serveur Discord envoyé par mail depuis notre compte, sans succès.

Nous avons donc pensé que John avait réutilisé ses identifiants ProtonMail pour d'autres services comme Discord, ce qui était le cas.

5.5.2.1 CONVERSATION JOHN / JAKE HEKE

Une discussion entre un certain Jake Heke et John Fredricksen concerne l'envoi d'une marchandise :

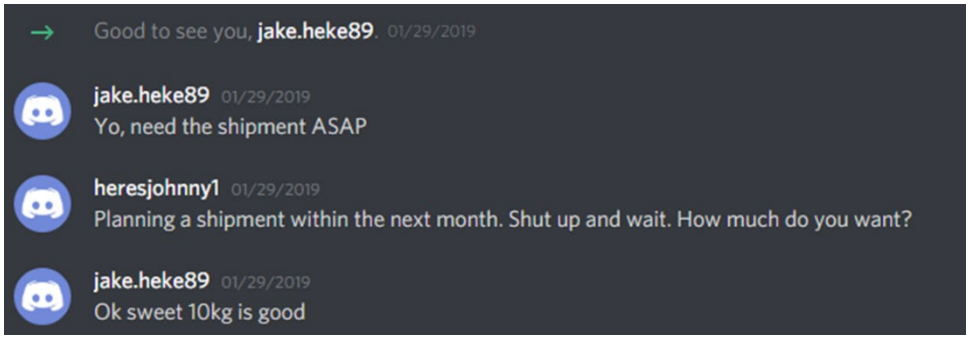


FIGURE 26 : CONVERSATION JOHN / JAKE HEKE

Cela confirme que John Fredricksen devait envoyer 10kg de drogue à Jake Heke.

5.5.2.2 CONVERSATION JOHN / JANE

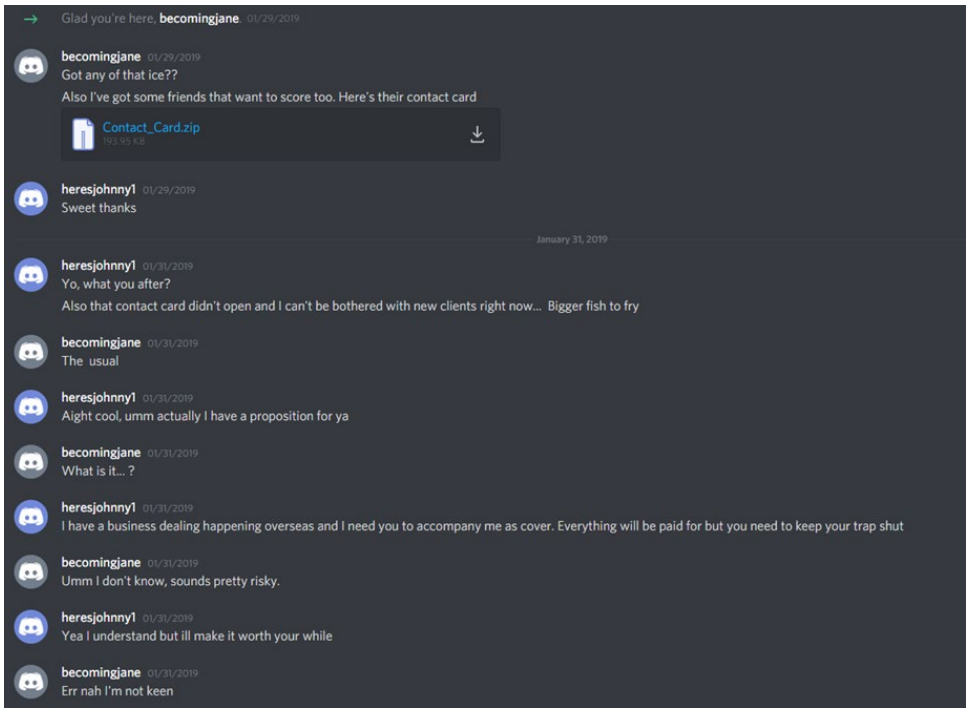


FIGURE 27 : CONVERSATION JOHN / JANE

Dans cette conversation, John indique qu'il a un gros client à l'étranger et qu'il a besoin de Jane pour l'accompagner en échange d'une rémunération. Jane refuse sa proposition mais n'acceptant pas cette décision, John menace de faire du mal à ses enfants :

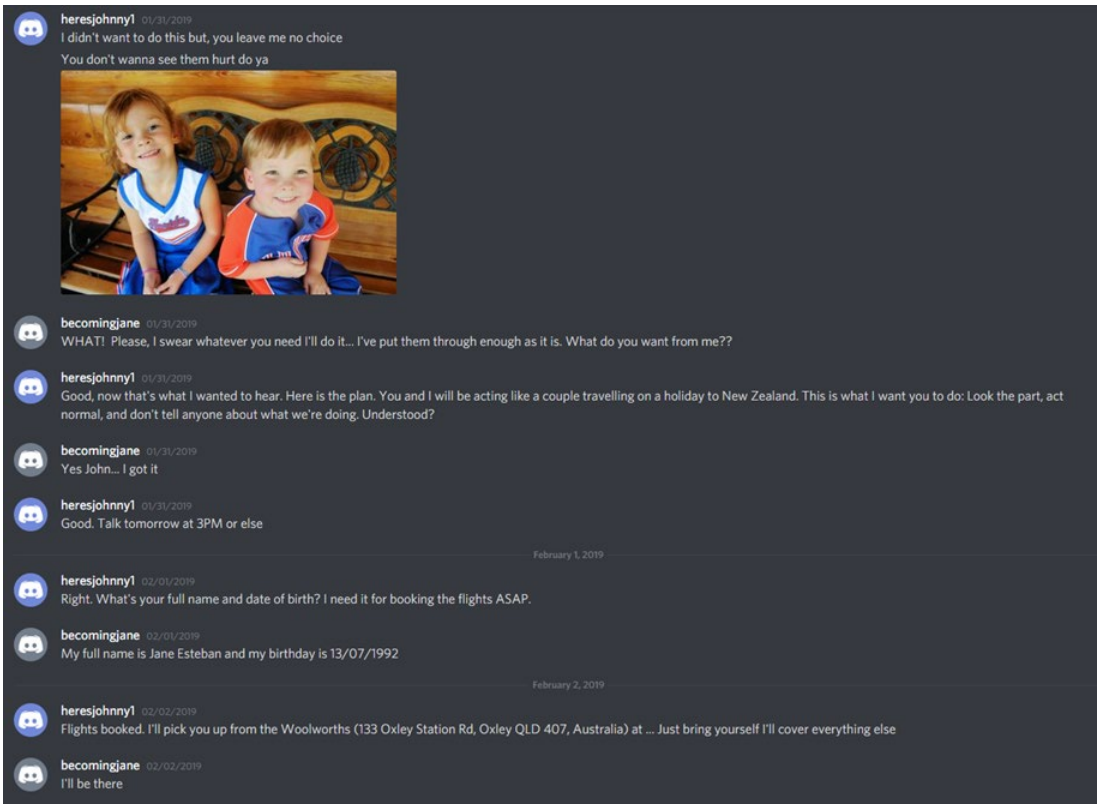


FIGURE 28 : CONVERSATION JOHN / JANE - MENACE

Jane a ainsi accepté le plan de John : se faire passer pour un couple voyageant en vacances en Nouvelle-Zélande.

Ensuite, Jane envoie son identité complète à John, à sa demande pour réserver les vols (nom de famille, date de naissance).

Pour finir, John lui a donné rendez-vous au 133 Oxley Station Rd, Oxley QLD 407 en Australie.

5.5.2.3 CONVERSATION JOHN / STEVE

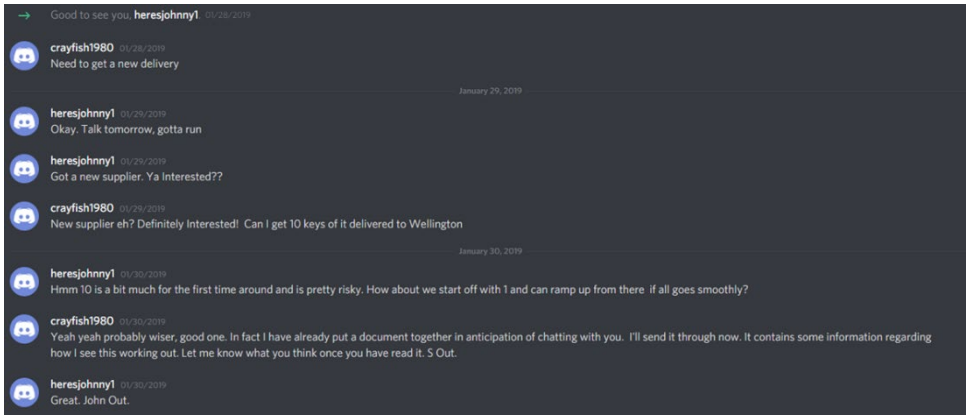


FIGURE 29 : CONVERSATION JOHN / STEVE

Dans cette conversation nous retrouvons les mêmes informations précédemment récupérées dans les logs de Quasar, à savoir, que nos suspects envisageaient de livrer 10kg de drogue, mais qu'afin d'éviter de prendre trop de risque, seulement 1kg de drogue sera livré. L'envoi d'un document explicatif a également été mentionné, il s'agit du document "secret" précédemment découvert.

Dans la suite de leurs échanges, on retrouve une fois de plus la preuve de l'utilisation de la stéganographie pour dissimuler des informations :

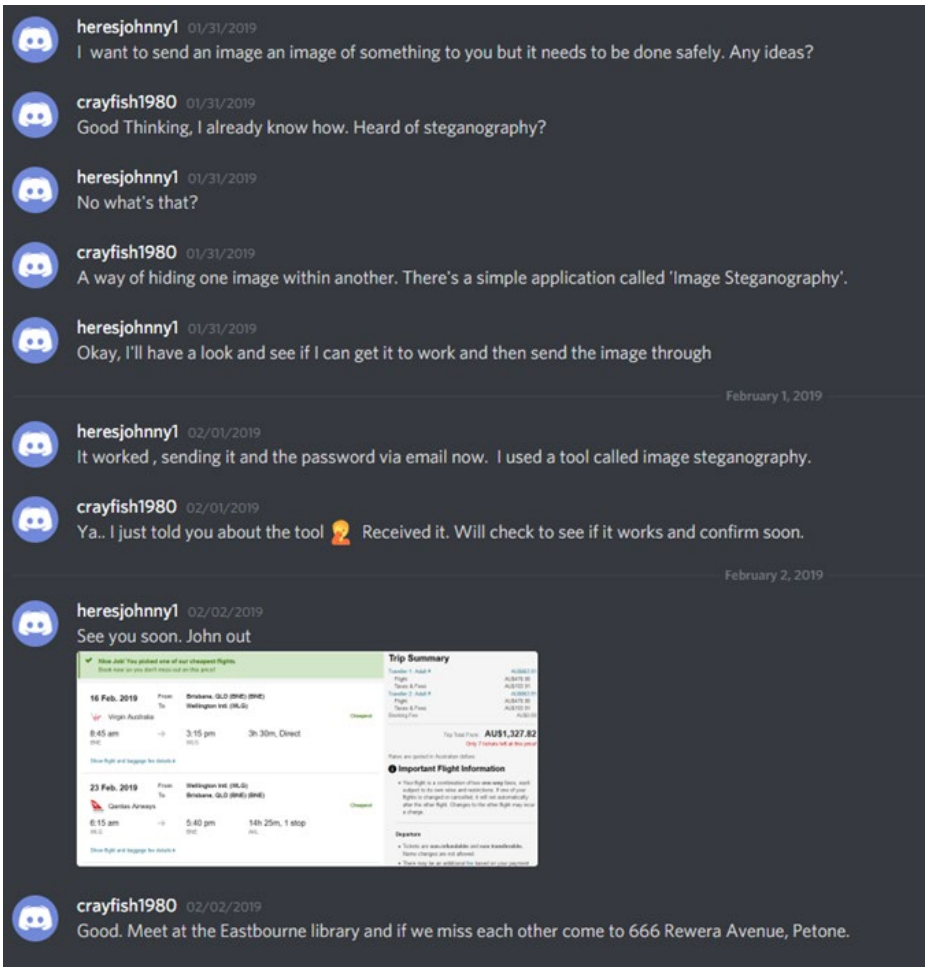


FIGURE 30 : CONVERSATION JOHN / STEVE

Steve dit à John qu'il a envoyé l'image avec une autre cachée à l'intérieur (BNE.png) et le mot de passe par mail.

Qui plus est, nous avons retrouvé l'image concernant les vols d'avions entre Brisbane et Wellington, c'est bien l'image que nous avons récupéré dans le cache de Discord de Steve.

Pour finir, Steve Kowhai a donné rendez-vous à John Fredricksen à la Bibliothèque d'Eastbourne. Il a également fourni une adresse secondaire en cas d'imprévu : 666 Rewera Avenue, Petone.

5.6 AUTRES ELEMENTS

5.6.1 TRAJETS

Nous avons découvert les images de différents trajets sur le PC de Steve Kowhai,:

- Le trajet de l'aéroport de Wellington à Eastbourne, pour que John et Jane puissent, comme prévu, rejoindre Steve à la bibliothèque.

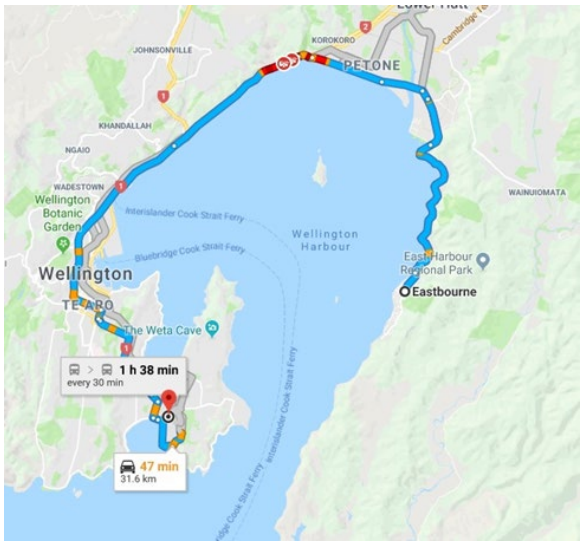


FIGURE 31 : TRAJET WELLINGTON / EASTBOURNE

- Le plan et les informations relatives à la bibliothèque d'Eastbourne, le lieu de rendez-vous avec Steve.

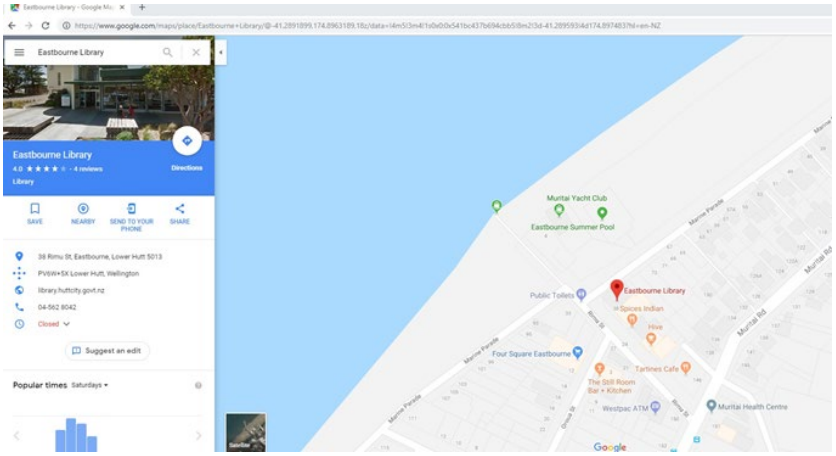


FIGURE 32 : PLAN BIBLIOTHEQUE EASTBOURNE

- Ainsi qu'une image « Method run.jpg », qui est le point de rendez-vous si quelque chose tourne mal.

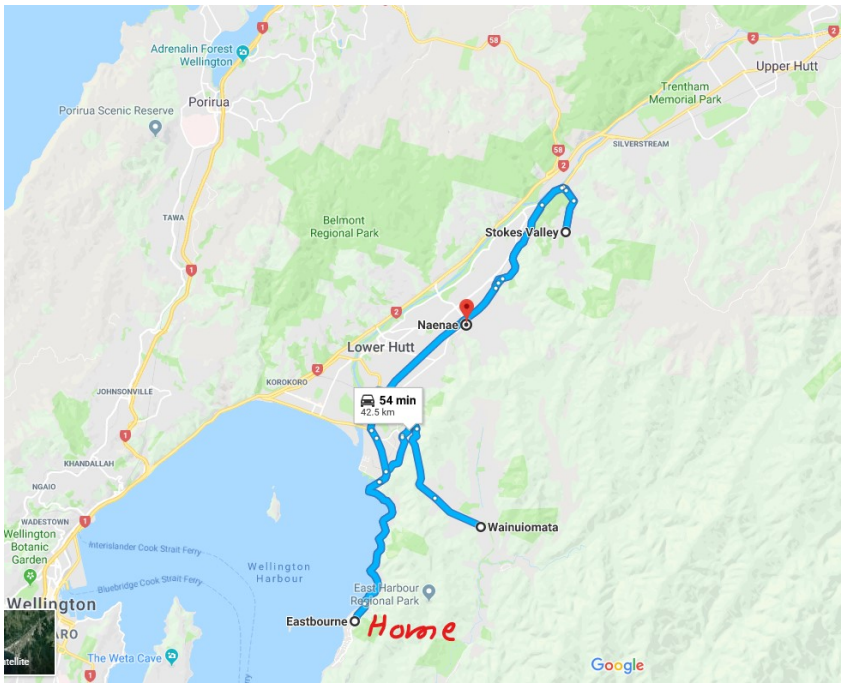


FIGURE 33 : METHOD RUN.JPG

5.6.2 HISTORIQUE NAVIGATEUR JOHN

Dans l'historique Firefox de John, nous avons relevé des comparateurs de vols et une agence de voyage en ligne appelée Travelgenio. Nous supposons que la réservation a été faite par l'intermédiaire de cette agence.

```
travelgenio.comlastTo1_Wellington%2C%20Wellington%2C%20New%20Zealand%20(WLG)nz.t
ravelgenio.com/^4
travelgenio.comlastFrom1_Brisbane%2C%20Brisbane%2C%20Australia%20(BNE)nz.travelg
enio.com/^4
```

FIGURE 34 : RESERVATION VOL HISTORIQUE FIREFOX DE JOHN

Nous avons également remarqué que John a utilisé Jivox et Bluekai, qui sont des services pour diffuser des annonces ou faire de la publicité ciblée. Nous émettons l'hypothèse d'une promotion en faveur de la drogue, c'est probablement aussi lié à l'image de méthamphétamine retrouvée sur le bucket s3 de Pinterest. Cette hypothèse reste cependant à confirmer.

5.6.3 FICHIER CLIENT

Une liste de clients a été retrouvée sur le disque de John :

File Edit View Insert Format Styles Sheet Data Tools Window Help

E14 | Monthly

This document is open in read-only mode.

	A	B	C	D	E	F
1	Name	Location	Product	Amount	Delivery	
2	Ricky Ross	Los Angeles	Mama Coca	20kg	Monthly	
3	Rhythmbox	New York, USA	Ferry Dust	15kg	Quarterly	
4	Chris Coke	Kingston Jamaica	Coke	20kg	Monthly	
5	Steve Kowhai	Wellington, New Zealand	Crank	15kg	Monthly	
6	Don Cholito	Puerto Rico	Snow	25kg	Quarterly	
7	Manuel Noriega	Panama	Smack	15kg	Monthly	
8	Joaquin Guzman	Guadalajara, Mexico	China White	15kg	Monthly	
9	Leroy Barnes	New York, USA	Load pack	15kg	Quarterly	
10	AL Capone	Sicilliy, Italy	Silly putty	25kg	Monthly	
11	Jane Esteban	Brisbane, Austraila	Uppers	1 gram	On demand	
12	Pablo Escobar	Colombia	White horse	15kg	Quarterly	
13	Franz Sanchez	Isthmus City	Mary Jane	20kg	Quarterly	
14	Jake Heke	Auckland	Tweak	10kg	Monthly	
15						
16						
17						
18						
19						
20						
21						
22						
23						

FIGURE 35 : FICHIER CLIENT

On peut ainsi relever l'identité de ses clients, leurs localisations, le type de substance commandé, la quantité ainsi que les fréquences de livraison.

Nous pouvons remarquer que Steve Kowhai fait partie de cette liste.

En poursuivant nos recherches, nous sommes tombés sur un bon de livraison à destination de Auckland en Nouvelle-Zélande pour un certain "Jake Heke". Jake Heke est présent dans la liste des clients de John.

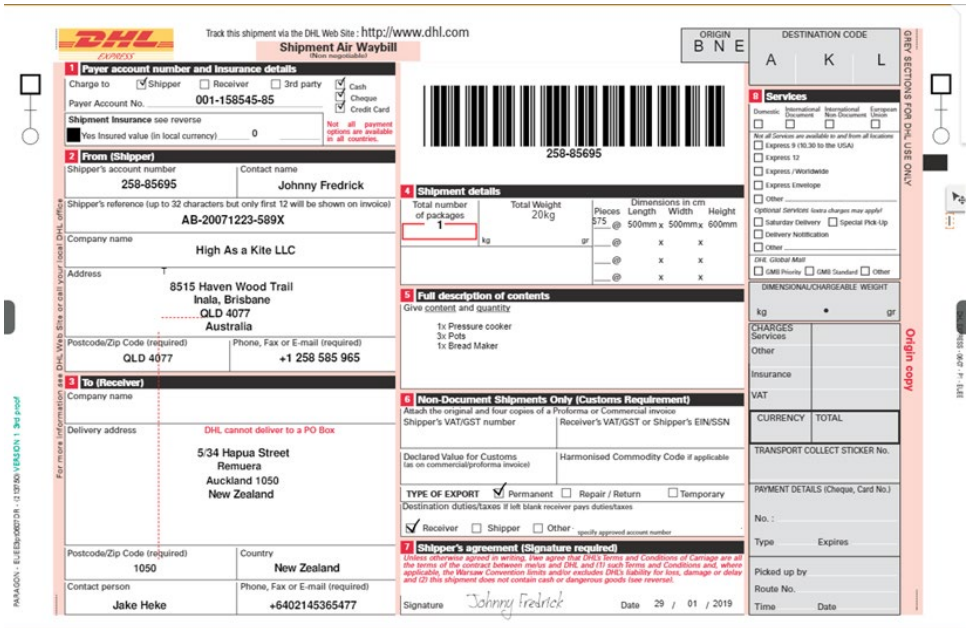


FIGURE 36 : BON DE LIVRAISON

D'après ce bon de livraison, il s'agit d'un colis de 20kg composé d'une machine à pain, de 3 pots et d'une cocotte-minute.

D’après les informations du document client de John, Jake Heke reçoit une livraison de 10kg de drogue chaque mois. Nous pensons que la drogue se trouve à l’intérieur de ce colis de 20kg mais que notre suspect la camoufle au travers d’autres éléments banals (Exemple : machine à pain).

6 RECOMMANDATIONS

6.1 POUR LES ENQUETEURS

Nous aurions dû chercher « à la main » dans le contenu des mémoires en utilisant des commandes de bases d'Unix tel que « strings » ou « grep ».

C'était une mauvaise idée de tenter de nous connecter au discord car des complices de John ou Steve pourraient très bien y avoir accès et remarquer l'activité anormale. Le cache des conversations Discord et des navigateurs combinés aux logs de Quasar auraient probablement pu suffire.

6.2 POUR JANE

Jane aurait dû effectuer ses recherches sous couverture en navigation privée pour que son ordinateur ne sauvegarde ni les recherches, ni les cookies, ni le cache.

Elle aurait pu utiliser un file shredder pour supprimer totalement les fichiers pouvant compromettre sa couverture comme par exemple le badge de la police qu'elle a jeté dans sa corbeille.

7 CONCLUSION

Grâce à notre investigation, nous avons trouvé suffisamment de preuves pour incriminer les suspects Steve et John.

Nous savons que Jane est une policière de la police fédérale australienne sous couverture, même s'il serait judicieux de vérifier auprès de ses supérieurs.

Nous connaissons maintenant :

- L'identité des clients de John, à moins qu'ils n'empruntent tous des fausses identités
- Ce que John et Steve avaient planifié et comment ils comptaient exécuter leur plan de livraison de drogue.

Nous avons donc une vision un peu plus large pour démanteler le réseau.