

Jérémie SCHEMITH

Ayoub BOUASRIA

Simon VILLECHENAUD

Valentine GILLES

**Atelier 1 :**

**MOBILE FORENSICS**



8INF968 – Atelier pratique cybersécurité I

# Table des matières

[**Table des matières 2**](#_n7efmlo5o77a)

[**Introduction 4**](#_bidzcua4uwdo)

[**I. Matériel utilisé 5**](#_ecv4vdiohg4a)

[1. Le Smartphone 5](#_gicblaq1ro5v)

[2. Les logiciels 5](#_tw9qpt3j8tr3)

[a. AVDManager 5](#_g7swjzuso8vh)

[b. FTK Imager 6](#_r9j4lo4tvnlc)

[c. Autopsy 6](#_t05p6rvr24fp)

[d. exiftool 6](#_41ayjpk9dql0)

[**II. Création d’une image disque d’un smartphone 7**](#_fon1zr9okld1)

[1. Le Rootage du Smartphone 7](#_g3auqe78g8e5)

[2. Impact sur l'Intégrité des Données 7](#_56ebdvnrdxtz)

[**III. Création d’une image disque d’un smartphone virtuel (AVD Manager) 8**](#_as3dwecdmoon)

[1. La création d’un smartphone virtuel 8](#_fw3nkt9zqo8x)

[2. Rooter l’AVD 8](#_9jkarwjimlif)

[3. Créer une image de l’AVD 8](#_vrlscp3sa2g3)

[4. Mise en place du CTF Forensique 11](#_te0ojofnbih0)

[Envoyer un SMS à l’AVD 11](#_o2b0vekpodek)

[Appeler l’AVD 12](#_cnpw0ihwokoh)

[Modifier les métadonnées d’une image 12](#_tyx0ii9pbycb)

[Problèmes rencontrés 12](#_z52zmi4yhmrc)

[**IV. Exploitation des données de notre image 13**](#_y9rryd5ycxul)

[1. Scénario : Braquage d’un bijoux 13](#_92iw0guxhn20)

[2. Création d’une copie des données 13](#_w2x5fle29syc)

[3. Utilisation d’Autopsy Forensic 13](#_1nc4i2z0zw92)

[a. Création d’un Case 13](#_6s4wpu3chk9o)

[b. Web History 14](#_c3c4iy5sfs90)

[c. Geolocalisation 15](#_yulp3dqi946h)

[d. Contacts 15](#_96x3xmtmvfhx)

[e. Messages / Call logs 15](#_yyiy789ulflm)

[f. Images 16](#_3exqm8kpmp27)

[g. Deleted Image/Link 17](#_qmjblfkri1uf)

[h. Image Metadata 17](#_3stx5ixtwv2s)

[**Conclusion 18**](#_btsh38lq19u0)

[**Pistes d’amélioration 18**](#_jjygohso2wec)

[I. Contexte 19](#_4vhd18fdwtvy)

[**II. Initialisation de l’enquête 19**](#_hmcrxko7vuzo)

[**III. Analyse des communications 21**](#_2imphwuxok96)

[1. Numéro de téléphone et pseudonyme 21](#_3cqf94l6zbmo)

[2. Contacts 21](#_l609ghnx60te)

[3. Messagerie 22](#_7keemr9nv2u)

[4. Localisation 23](#_tux674umejet)

[**IV. Utilisation de l’outil de recherche 24**](#_413c366moq9u)

[1. Adresse e-mail 24](#_fxfw3m7ndl9w)

[2. D’autres recherches 25](#_vvtwzvt97zi1)

[**V. Réseaux Sociaux & Applications 25**](#_tuk64gc7kg2o)

[1. Reddit 26](#_3pr46q49os27)

[2. Twitter/X 26](#_wa0fjo18842n)

[3. Telegram 28](#_2e5mm06udbwz)

[4. Google Camera 29](#_hjl4dnhyui82)

[5. AllTrails 30](#_crbnfg43g3rg)

[**VI. Historique de navigation Web 32**](#_qa6piqghx741)

[**VII. Conclusion 32**](#_8klhpoqw5rdc)

# Introduction

Lors de cette analyse Forensique, nous avions l’opportunité de créer l’image du contenu d’un smartphone et de l’analyser. Nous avons donc créé un scénario d’enquête à résoudre. Dans la suite de ce rapport, nous allons traiter de la création de preuves et de l’image virtuelle, puis de l’analyse de cette dernière.

# 

Partie 1 : Création et analyse d’une image Android

# Matériel utilisé

## Le Smartphone



Google Pixel 5 sous Android

*Des problèmes d’utilisation du smartphone nous mèneront finalement à utiliser un smartphone virtuel.*

## Les logiciels

Afin de créer et analyser notre image de smartphone, nous avons dû utiliser différents logiciels.

### AVDManager

[avdmanager](https://developer.android.com/studio/command-line/avdmanager?hl=fr) est un outil de ligne de commande qui permet de créer et de gérer des appareils virtuels Android à partir de la ligne de commande. Un appareil virtuel Android (ou AVD) permet de définir les caractéristiques d'un téléphone Android, d'une montre Wear OS ou d'un appareil Android TV que l’on souhaite simuler dans Android Emulator.

### FTK Imager

[FTK imager](https://www.exterro.com/ftk-imager) est un outil d'acquisition d'images gratuit sous Windows. Il est possible de faire une image d'un disque dur, d'une clef usb, de la mémoire d'un Iphone ou d'un samsung galaxy, voir aussi de chaque disque dur composant un RAID avant d'en récupérer les données.

### Autopsy

Autopsy est un logiciel permettant d’investiguer sur les données d’un ordinateur ou d’un téléphone à partir de fichiers ou d’une image disque. L'extraction d'informations et de données à partir d'appareils mobiles peut inclure les éléments suivants :

* Appels téléphoniques
* Messages de chat
* Images
* Vidéos
* Artefacts stockés cachés
* Les métadonnées GPS et de géolocalisation stockées sur des appareils mobiles.

### exiftool

ExifTool est une bibliothèque Perl indépendante de la plate-forme ainsi qu'une application en ligne de commande pour lire, écrire et éditer des méta-informations dans une grande variété de fichiers. ExifTool prend en charge de nombreux formats de métadonnées différents.

# Création d’une image disque d’un smartphone

## Le Rootage du Smartphone

Le bootloader est une interface de démarrage qui contrôle le chargement du système d'exploitation et des composants essentiels du smartphone. Pour obtenir un accès root, il est généralement nécessaire de déverrouiller le bootloader. Nous avons pour cela utilisé l’outil fastboot du Android SDK Toolkit pour notre smartphone Google Pixel 5.

Voici les étapes générales pour ce processus :

* Installation du Android SDK Toolkit : Le SDK Android est installé, et le terminal est configuré pour reconnaître les commandes Fastboot et ADB.
* Activation du mode développeur : Sur le Google Pixel 5, le mode développeur est activé en tapotant plusieurs fois sur le numéro de build dans les paramètres du téléphone.
* Activation du débogage USB et désactivation du verrouillage OEM (Original Equipment Manufacturer) : Dans les options pour les développeurs, le débogage USB est activé et l’OEM désactivé.
* Connexion du téléphone au PC : Le smartphone est connecté au PC via un câble USB.
* Exécution de la commande Fastboot : La commande Fastboot est utilisée pour déverrouiller le bootloader, ce qui implique la suppression de toutes les données du téléphone, compromettant ainsi l'intégrité des données.

## Impact sur l'Intégrité des Données

Le déverrouillage du bootloader supprime toutes les données du smartphone, ce qui compromet l'intégrité des données stockées. Cette action est essentielle pour obtenir un accès root, mais elle doit être exécutée avec précaution, car elle peut entraîner une perte irréversible de données.

Afin de régler ce problème, nous avons finalement décidé d’utiliser un téléphone virtuel.

# 

# Création d’une image disque d’un smartphone virtuel (AVD Manager)

## La création d’un smartphone virtuel

Voici les étapes à suivre :

* **Ouvrir AVD Manager** : Lancer Android Studio et accédez à "AVD Manager" depuis la barre d'outils ou le menu "Tools".
* **Créer un Nouveau Périphérique Virtuel** : Cliquez sur "Create Virtual Device" et suivez les étapes pour choisir un périphérique virtuel, sélectionner un système d'exploitation et configurer les paramètres.
* **Lancer le Périphérique Virtuel** : Une fois créé, sélectionnez le périphérique virtuel dans la liste et cliquez sur "Launch" pour démarrer le téléphone virtuel.

Nous avons utilisé un Pixel 6 Pro avec Android 8.1 API 27, qui ne pose pas de problème à rooter.

## Rooter l’AVD

Afin de simuler un environnement Android avec des privilèges root sur un téléphone virtuel, nous avons utilisé un script spécifique nommé rootAVD, disponible sur GitHub à l'adresse<https://github.com/newbit1/rootAVD>. Ce script a été choisi pour son efficacité et sa fiabilité dans le processus de rootage des périphériques virtuels Android créés avec Android Virtual Device (AVD) Manager de Android Studio.

Pour lister les versions d’Android qu’il était possible de router nous avons utilisé la commande :



Grâce à cette commande nous avons vu qu’il était possible de rooter nôtre AVD.

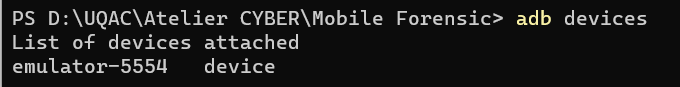
Commande pour rooter l’AVD :



Le terminal nous renvoie le message “Success” , il est maintenant possible d'exécuter la commande “su” sur le smartphone en mode shell. L’utilitaire Magisk a été installé sur le téléphone pour le rooter.

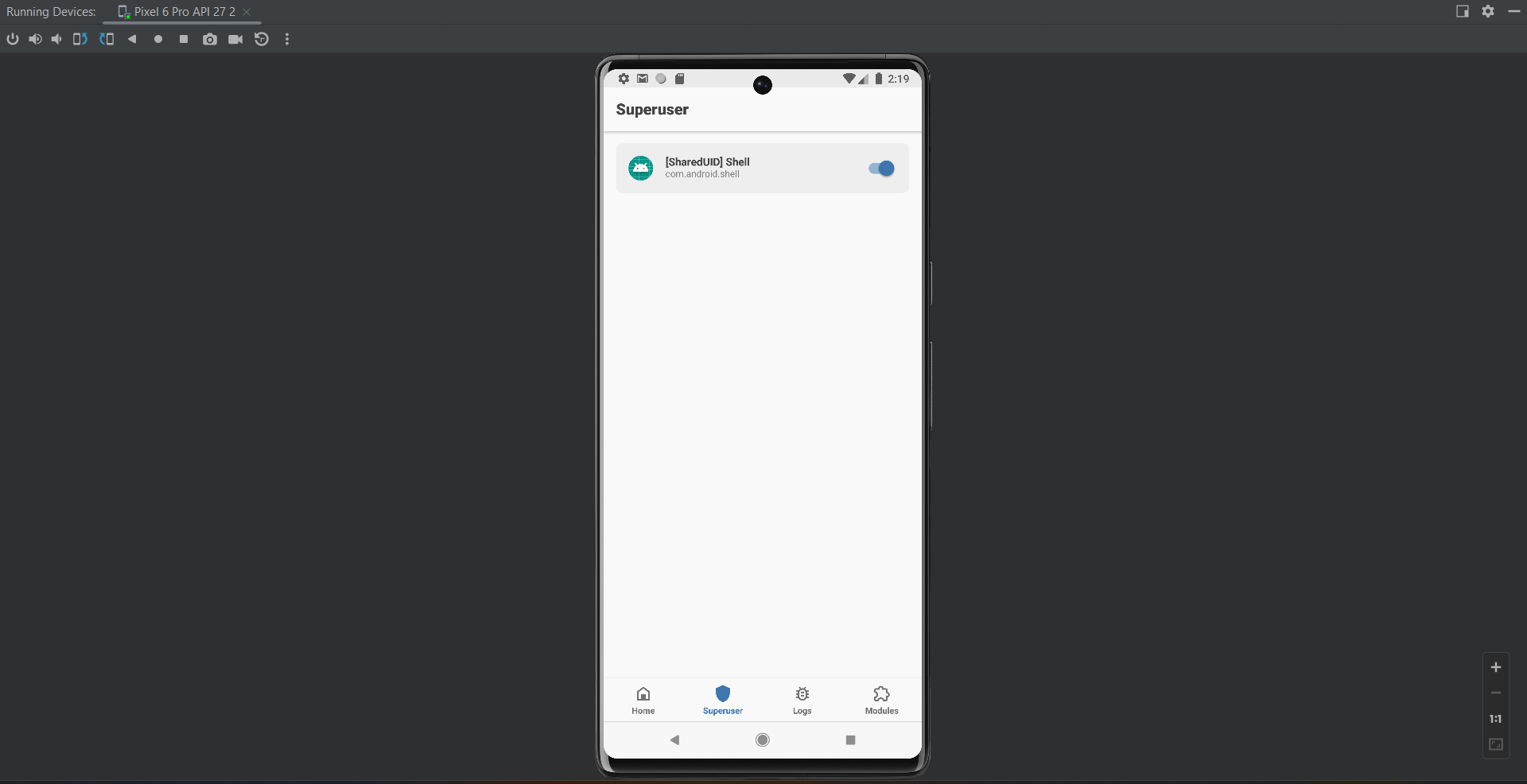
## Créer une image de l’AVD

Premièrement nous allons vérifier si notre AVD est bien reconnu par ADB.



D’après la commande “adb devices” notre émulateur est bien fonctionnel sur le port 5554.

Nous avons maintenant la possibilité d’ouvrir un shell et d’élever nos droits à ceux du superutilisateur. Au préalable il va falloir cocher une option supplémentaire dans l’utilitaire Magisk afin de ne pas bloquer la commande “su” :



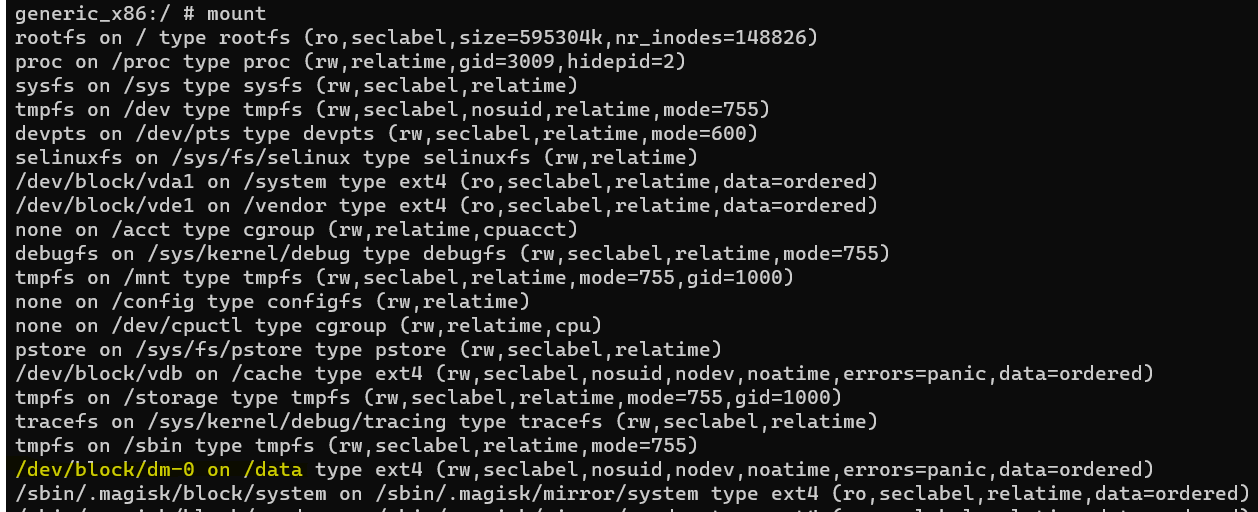
Après cela nous allons pouvoir ouvrir un shell avec les privilèges superutilisateur :



Il nous est maintenant possible de lire ce qui est dans la partition /data, cette partition est la partition dont nous cherchons à créer une image puisqu’elle continent les données exploitables par Autopsy.



A l’aide de la commande mount nous allons repérer sur quel point de montage est monté la partition /data :



On note l’information “/dev/block/dm-0” qui va nous être utile pour créer notre image.

L’AVD par défaut est dans un réseau NAT/PAT , donc un réseau isolé. Nous allons devoir utiliser du Port Forwarding pour transférer des fichiers de notre smartphone virtuel à notre machine physique.



Pour transférer les fichiers nous allons utiliser l’utilitaire NetCat qui n’est pas présent de base sur l’AVD , nous allons donc installer BusyBox qui regroupe une variété de commande Linux utilisable dans un téléphone Android

En ayant télécharger au prélable l’APK BusyBox sur notre machine physique Windows :



Une fois l’utilitaire BusyBox installé, nous allons utiliser la commande dd qui va nous servir à créer une image puis nous allons transmettre cette image via NetCat :

Android :



Windows :



Une fois les données transférées, elles sont exploitables sur Autopsy.

Il existait une autre façon plus simple de récupérer les données sur /data , en utilisant la commande adb pull :



## Mise en place du CTF Forensique

Nous devons maintenant ajouter des preuves dans le télephone. Voici quelques éléments techniques qui nous ont permis de créer l’enquête.

### Envoyer un SMS à l’AVD

Au préalable , il faut activer l’utilisation de Telnet sur Windows. On va maintenant se connecter avec Telnet au smartphone et nous allons pouvoir utiliser des commandes de base notamment envoyer des messages.

Connexion à l’AVD :



Authentification :



Liste de commandes :



Envoyer un SMS :



### Appeler l’AVD

Nous allons utiliser ADB pour appeler l’AVD.

Appeler l’AVD :



### Modifier les métadonnées d’une image

A l’aide de l’utilitaire Exiftool , il est facile de modifier les métadonnées d’une image pour cacher des informations.

Par exemple modifier le champs Description :



### Problèmes rencontrés

L’utilisation tardive du smartphone virtuel suite aux problèmes rencontrés avec le téléphone physique ne nous a pas permis d’exploiter complètement les possibilités qu’offrait AVD Manager pour insérer des données dans le téléphone, et par conséquent l’image de notre téléphone comportait beaucoup moins d’informations qu’une image de téléphone trouvée sur le net. En plus de cela, il était beaucoup moins facile de manipuler le smartphone virtuel. Par exemple, il n’était pas possible de prendre des photos ou d’activer le GPS.

Lors de la création d’une image disque, nous avons cherché à mettre des preuves en lien avec la localisation du téléphone virtuel (géolocalisation). Lorsque nous avons utilisé Autopsy Forensic nous ne sommes pas parvenu à obtenir la position gps du téléphone, même lors d’une recherche avancée dans les fichiers de l’image, nous ne pouvions l’obtenir que dans les méta données des photos prisent directement avec l’appareil photo. Nous avons installé un vpn (bitmask) pour tenter de changer la localisation, mais cela n’a pas abouti.

# 

# Exploitation des données de notre image

## Scénario : Braquage d’un bijoux

L'histoire commence avec l'apparition d'un diamant rare et précieux dans une galerie d'art renommée. Les rumeurs sur sa valeur inestimable se propagent rapidement, attirant l'attention d'un gang de voleurs de bijoux chevronnés.

On soupçonne un groupe de braqueurs de vouloir le dérober. Un des suspects est arrêté et nous avons récupéré son téléphone.

## Création d’une copie des données

Tout d’abord il faut récupérer les données du téléphone sans les compromettre.

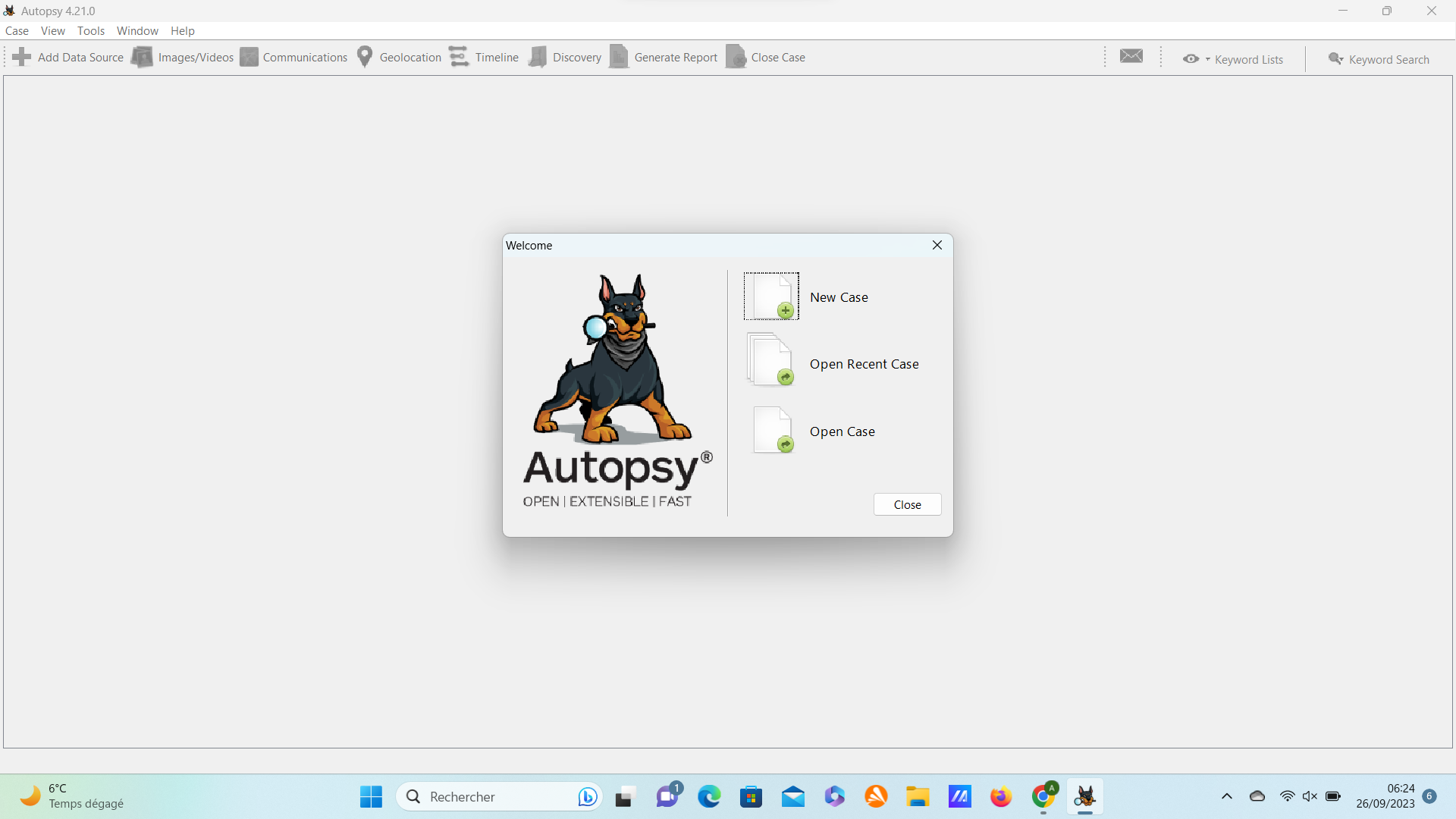
Nous faisons donc une copie des données extraites du téléphone pour ne pas altérer les preuves, et pouvoir se protéger juridiquement.

Une fois ce travail réalisé nous pouvons analyser les données via *Autopsy Forensic.*

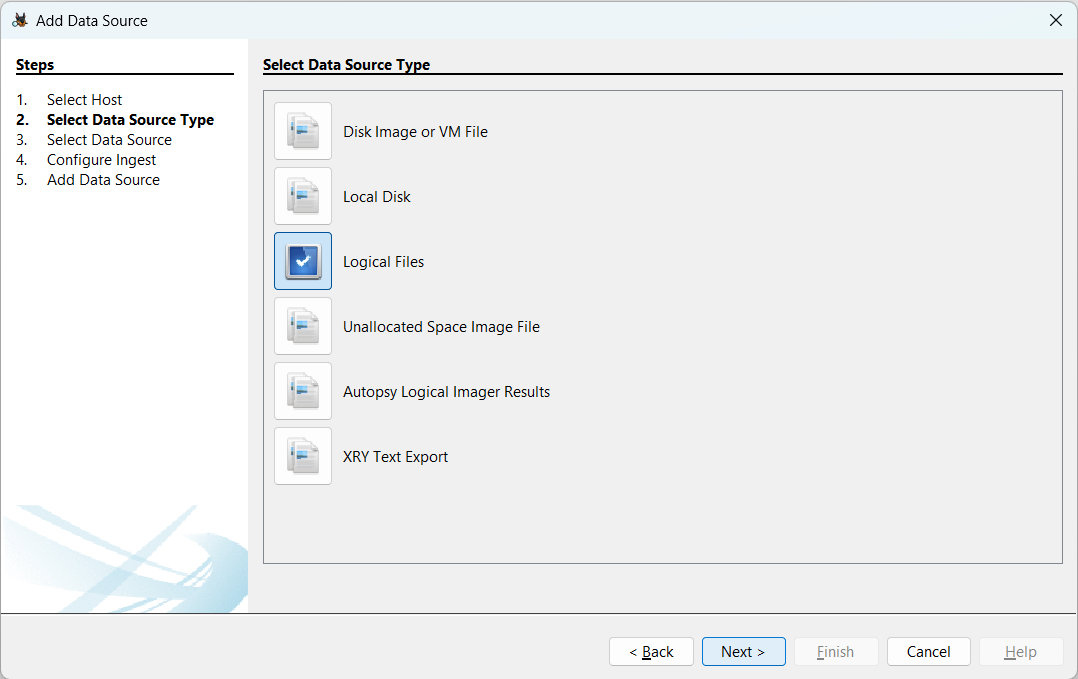
## Utilisation d’Autopsy Forensic

Nous avons pris le choix d’utiliser Autopsy Forensic, car c’est un logiciel libre de droit, sa facilité de prise en main, son utilisation multiplateforme

### Création d’un Case



Les données récupérées ici sont extraits dans un dossier /data. On choisit donc l’option “Logical Files”.



### Web History

Nous nous sommes tout d’abord penchés sur l’historique Web de notre suspect.

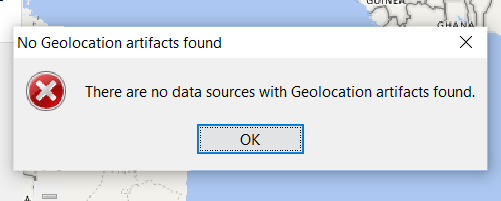


Les informations qui en ressortent sont les suivantes : notre suspect a cherché 3 fois le terme “diamant”, une fois la suite de mots “voler diamant” et une fois “braquage”. Cela confirme que l’homme que nous avons arrêté avait bien un comportement suspect. Mais cela ne suffit pas pour confirmer notre piste.

Les coordonnées GPS de la deuxième recherche ne donnent aucune piste, puisqu’elles semblent correspondre à l'emplacement du siège de Google.

### Geolocalisation

Notre suspect ne semble pas avoir activé sa géolocalisation. Nous ne pouvons donc pas tracer son trajet des derniers jours.

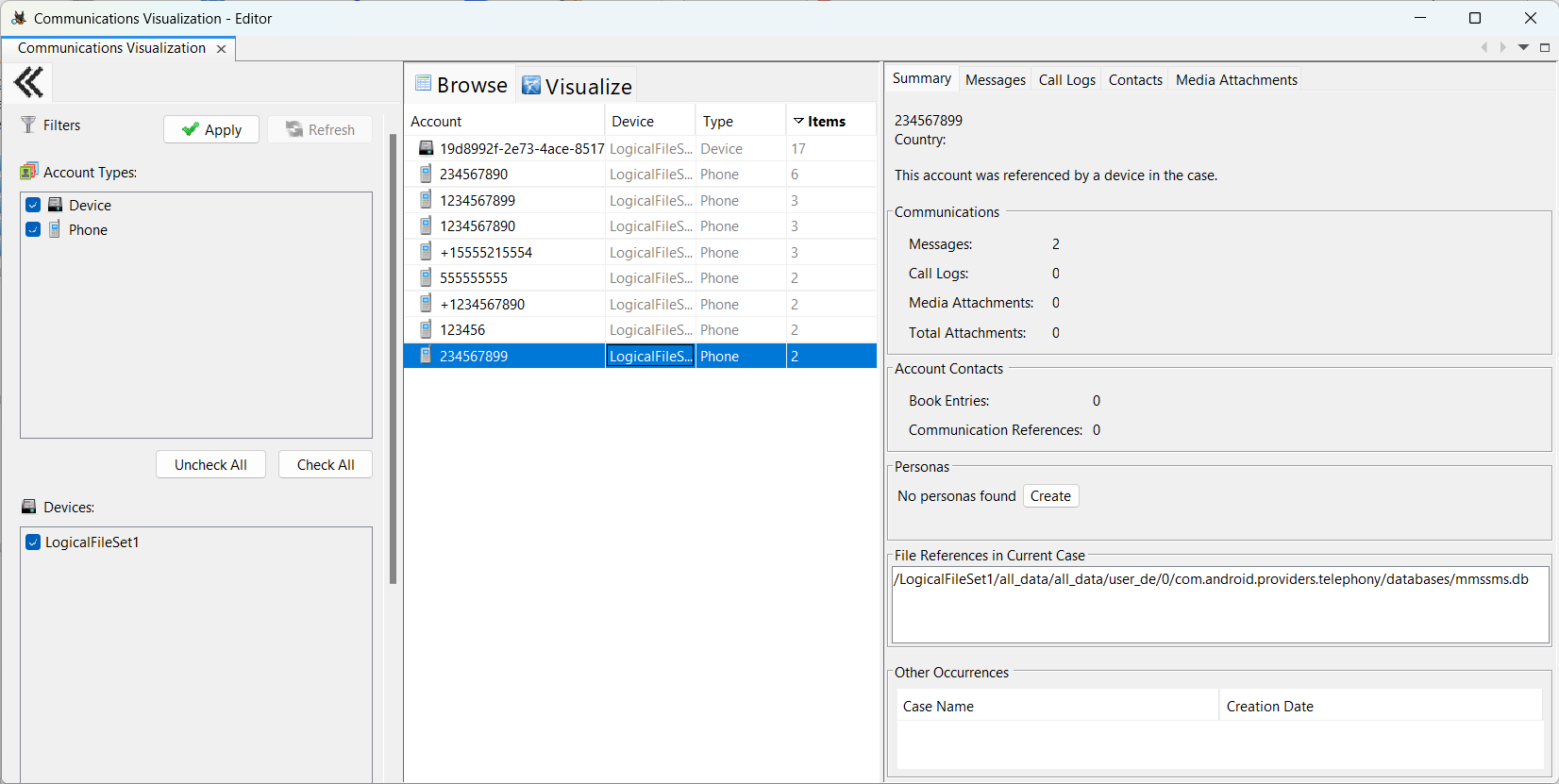


### Contacts

Notre suspect n’a que 3 contacts. Il semblerait qu’il utilise des noms de code pour les reconnaître. Est-ce un jeu entre amis ou bien un moyen de cacher leur identité ?

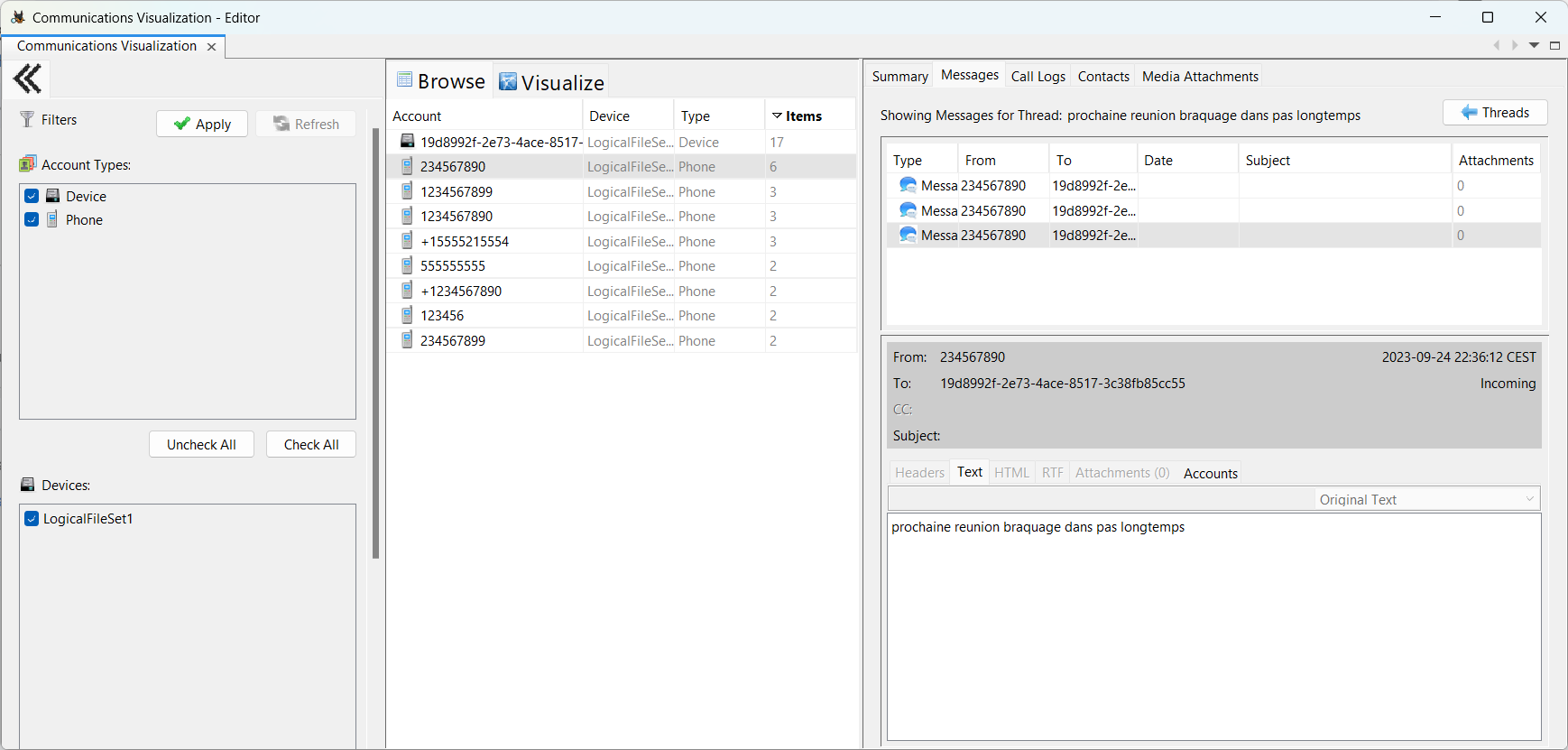


### Messages / Call logs



En analysant les messages de notre suspect, nous avons trouvé plusieurs communications avec différents numéros.

On notera des communications avec 8 numéros différents. Une communication avec le numéro +234567890 a attiré notre attention.



Nous remarquons plusieurs appels avec ce numéro, mais aussi trois messages mentionnant une réunion pour un braquage à venir.



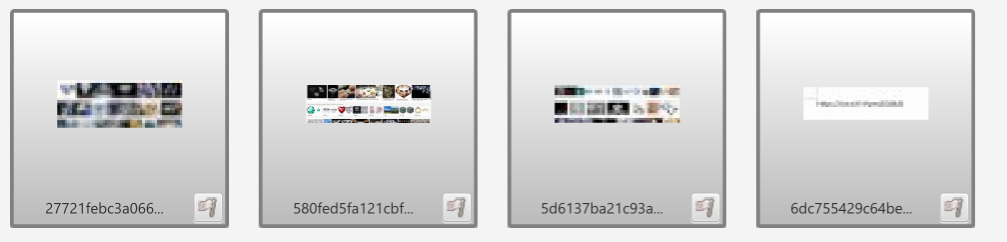
La réponse de notre suspect a attiré notre attention. Il semblerait que nous devrions jeter un œil a des medata. Cela nous servira sûrement pour la suite.



### Images

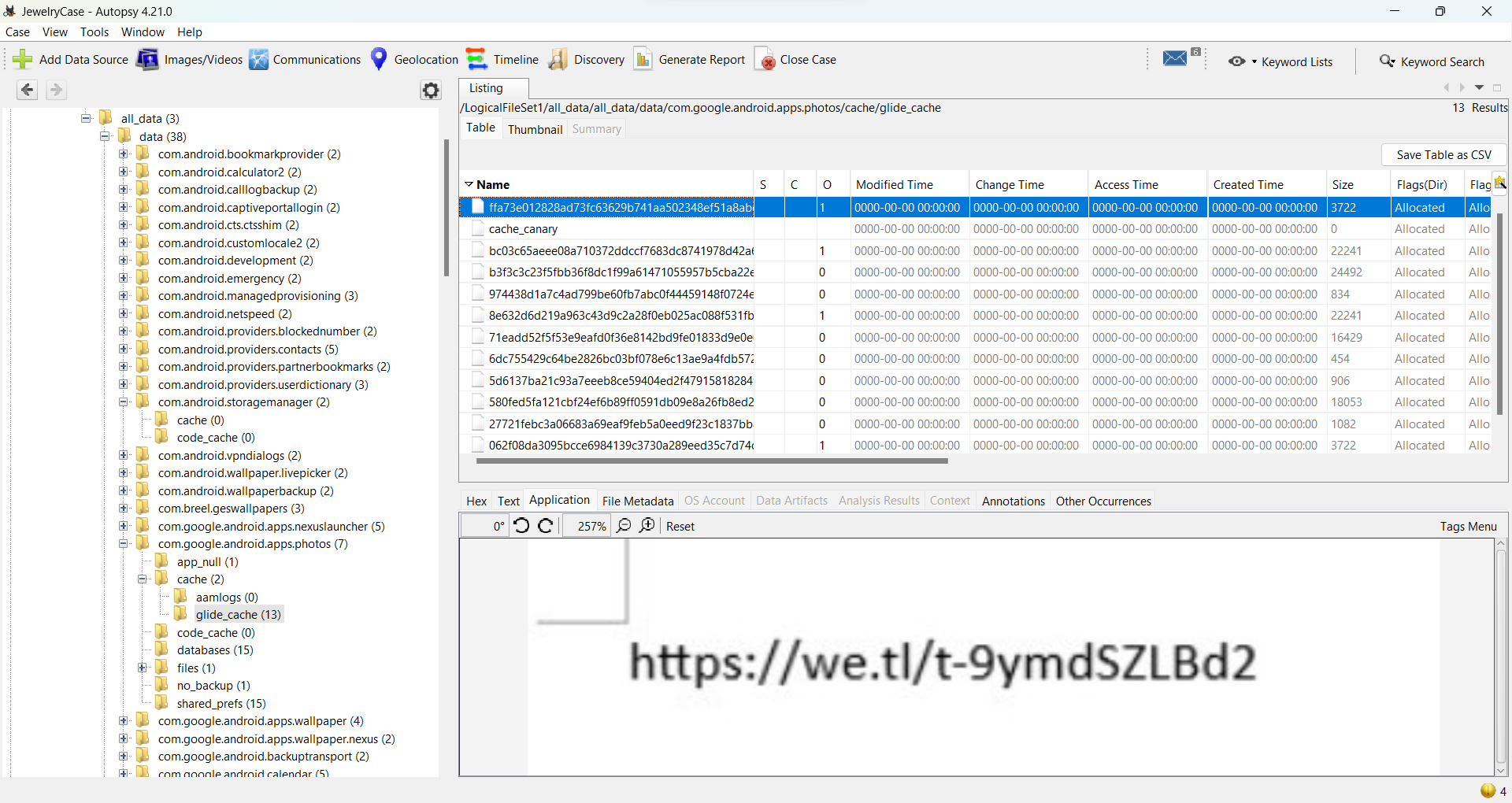
Nous avons trouvés 4 images présente dans le téléphone

Les trois premières images représentent des bijoux, et la quatrième image est un URL pris en photo. Malheureusement la qualité est dégradée. L’image a peut être été supprimée.



### Deleted Image/Link

En cherchant dans les images stockées dans le cache, nous avons trouvé un lien redirigeant vers un fichier WeTransfer.



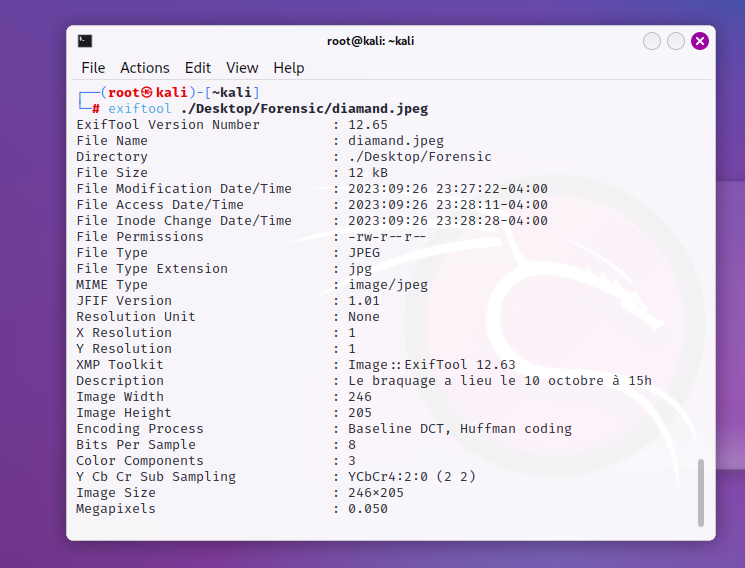
En téléchargeant le fichier, on tombe alors sur une image de bijoux. Nous allons donc l’étudier.



### Image Metadata

Suite au message précédemment reçu, évoquant l’importance des metadata dans notre affaire, nous avons décidé d’observer des métadonnées de cette photo.

A l’aide de l’outil **exiftool** nous pouvons analyser les métadonnées présentes dans la photo :



Un message secret y est caché indiquant la date et l’heure du braquage le **10 Octobre à 15h** .

## Conclusion

Nous avons donc des preuves que notre suspect prévoyait de voler un diamant, mais nous ne possédons pas d’information sur le lieu. Il nous sera donc nécessaire d’obtenir ses aveux. La suite de notre enquête consistera à déterminer qui sont ses complices, grâce à ses aveux, ou en remontant la piste du numéro que nous avons pu obtenir, ainsi que les deux autres contacts enregistrés.

## Pistes d’amélioration

Étant donné que nous avons investi beaucoup de temps dans nos efforts pour récupérer une image à partir du téléphone physique, nous n'avons pas pu implémenter dans le smartphone virtuel les diverses preuves auxquelles nous avions pensé, telles que :

* Utilisation de l’adresse mail (mail envoyés, cookies de connexion)
* Messagerie chiffrée (Signal, Télégram)
* Utilisation de Tor
* Événements google Agenda
* Notes vocales ou textuelles
* Compte d’application (Instagram, BeReal, Snapchat, Twitter, Messenger/Facebook)
* Application de services (Uber, Ubereats, Skip, DoorDash, Vinted)

Partie 2 : Exploitation des données d’une image téléchargée

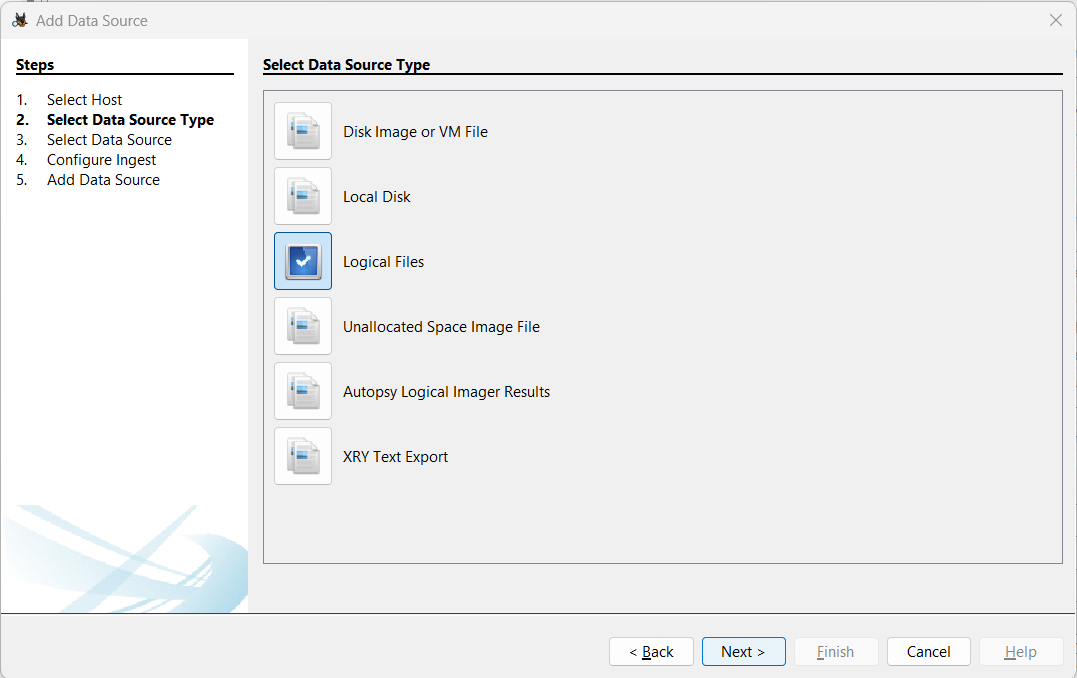
# Contexte

Nous avons à notre disposition une image de smartphone sous Android 12 téléchargée [ici](https://digitalcorpora.org/corpora/cell-phones/).

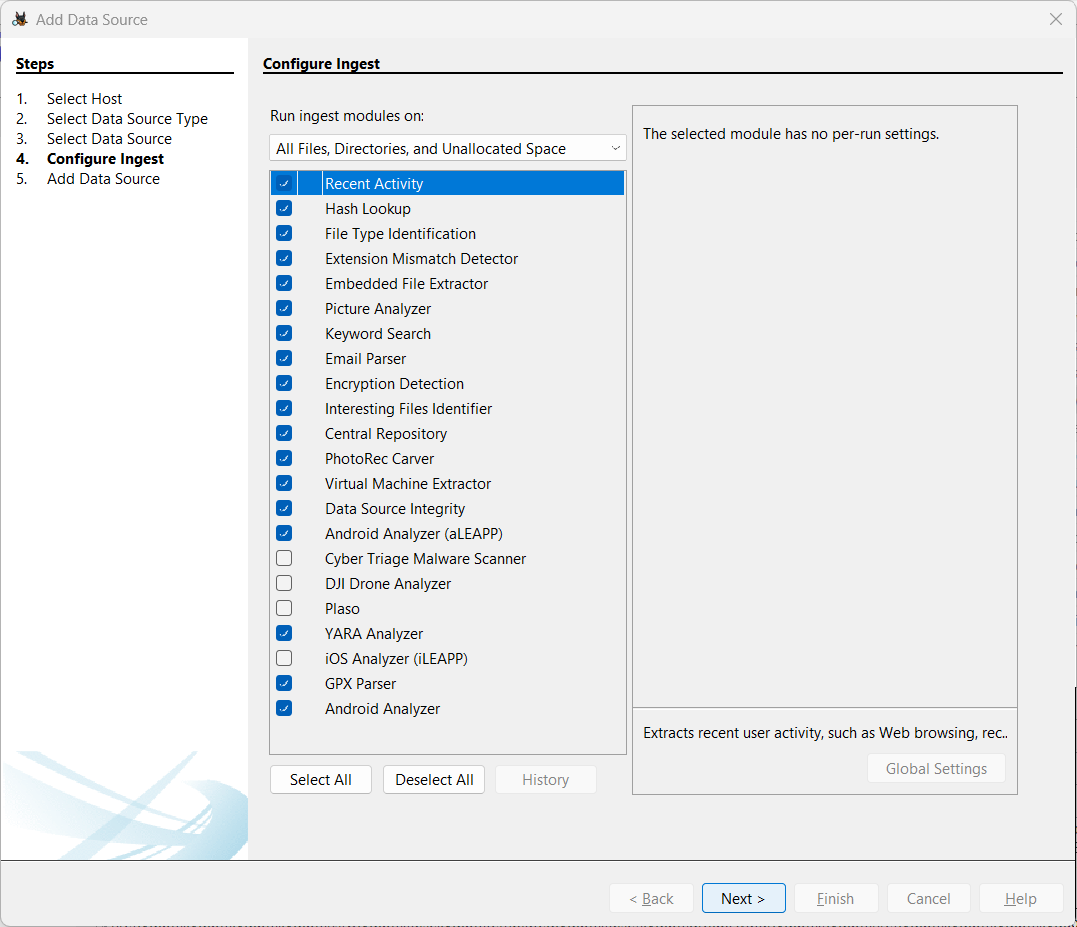
Nous allons tenter d’extraire le plus d’informations possible de ce téléphone afin de pouvoir dresser un profil de son utilisateur.

# Initialisation de l’enquête

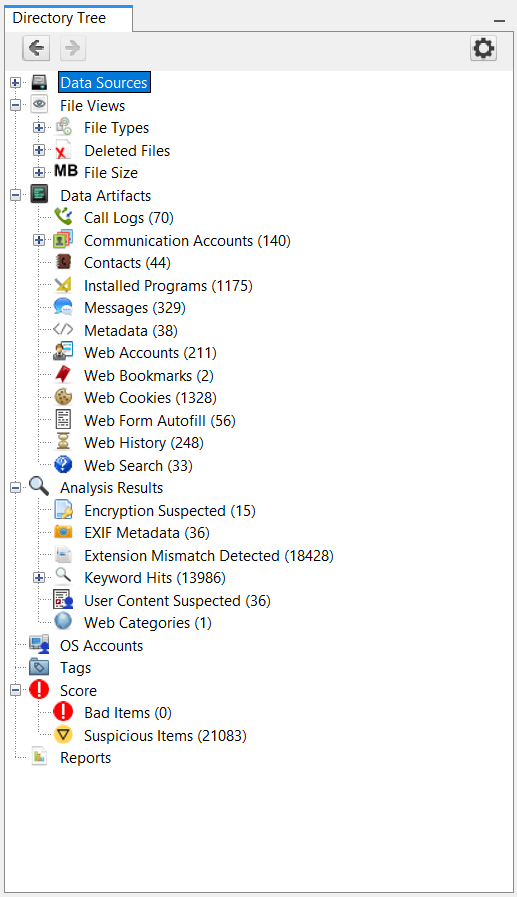
Tout d’abord, étant donné qu’on a accès au dossier data, on va les importer dans Autopsy via l’option Logical Files.



Au niveau des modules Ingest, pour mener l’analyse, on a choisi de laisser les paramètres par défaut tout en enlevant les modules “IOS Analyzer” et “DJI Drone Analyzer” étant donné qu’on est sûr qu’ils seront inutile vu que les données analysées appartiennent à un Google Pixel 3 sous Android 12.



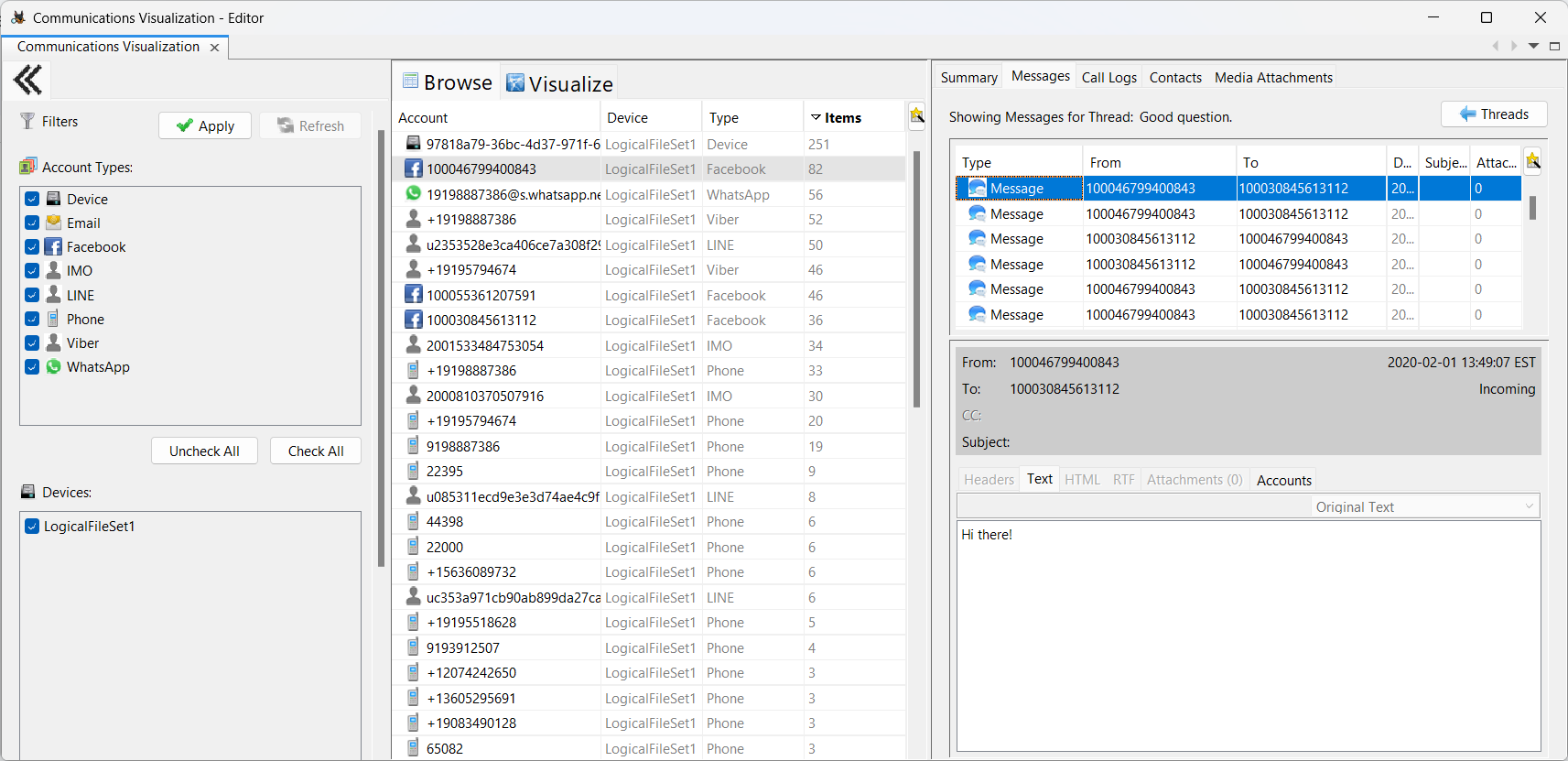
Une fois que chaque module ait terminé son analyse, nous obtenons via le Directory Tree, à l’ensemble des résultats :



# Analyse des communications

## Numéro de téléphone et pseudonyme

Pour commencer l’analyse des informations, on utilise l’outil de visualisation des communications intégré à Autopsy :

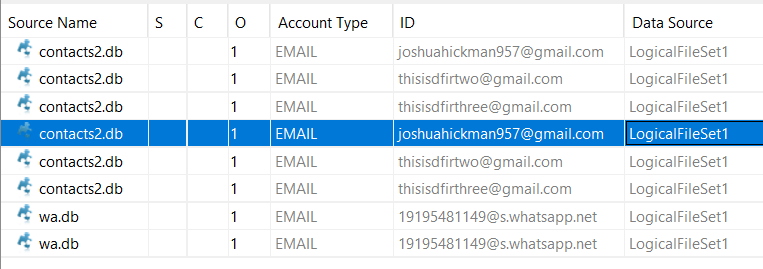


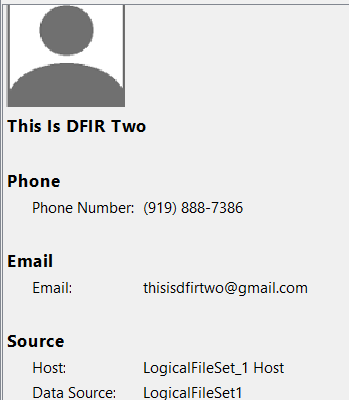
Grâce à cet outil on comprend plusieurs informations :

Le pseudonyme du propriétaire du téléphone est **“This is DFIR”** et il utilise le numéro de téléphone **+1 919 579 4674**. Via une recherche sur internet, on sait que l’indicatif 919 du numéro de téléphone correspond à la **ville Raleigh en Caroline du Nord aux Etats-Unis** d’Amérique. Peut-être que d’autres informations plus tard viendront confirmer ou infirmer cette supposition.

## Contacts

L’utilisateur a dans ses contacts 3 adresses e-mail différentes. On remarque que le nom de **Joshua Hickman** se trouve dans l’une de ces adresses.





Etant donné que le pseudonyme de notre utilisateur est This Is DFIR, on peut supposer que This Is DFIR Two et Three sont aussi des comptes à lui. Il faudra aussi s’intéresser au contact Josh Hickman.

## Messagerie

Grâce aux SMS qu’il reçoit, on remarque qu’il utilise beaucoup d'applications de messagerie différentes. Il échange en grande quantité avec “**This Is DFIR Two**”. On peut supposer que ce compte lui sert à faire des tests.

A chaque fois ces deux comptes s'envoient quelques messages sans intérêts particuliers, essayent d’en supprimer un, puis s’envoie une ou deux images, et s'appellent en audio uniquement puis enfin s'appellent en vidéo si l’application le permet. Les appels sont toujours très courts et durent entre 90 et 120 secondes.

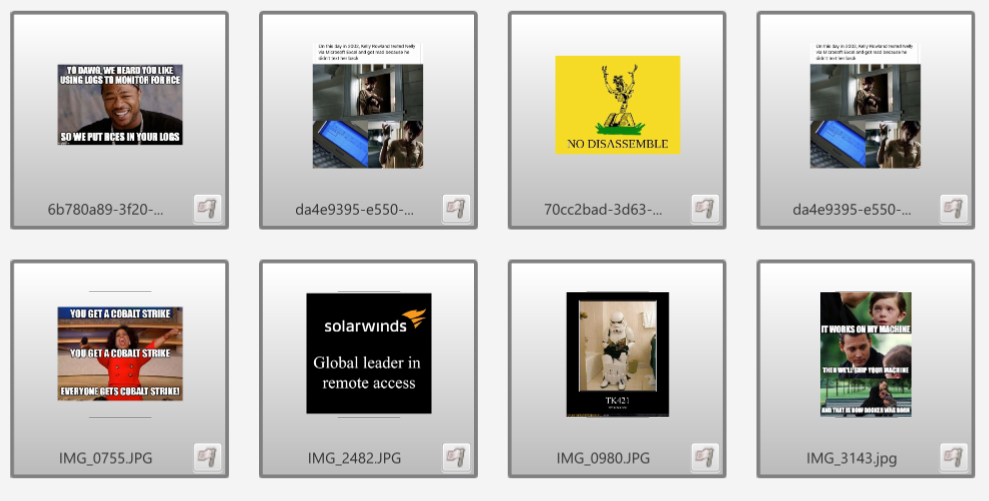
Les applications avec lesquels il va communiquer avec “This Is DFIR Two” sont :

* Facebook Messenger,
* WhatsApp,
* Viber,
* Line,
* IMO.

Ils ont également échangé par messages classiques (SMS) mais aucune information pertinente n’a été détectée outre le fait qu’ils ont essayé de spam rapidement une dizaine de messages avec le contenu.

Le numéro utilisé par “This Is DFIR Two” est **+1 919 888 7386**. On remarque qu’il s’agit de la même zone géographique que l’autre numéro de téléphone (Raleigh, Caroline du Nord, Etats-Unis).

Dans les photos échangées via les différentes applications de messagerie, on retrouve des memes en grande quantité. On peut supposer que notre utilisateur apprécie échanger des memes, puisqu’il en a enregistré plus d’une cinquantaine sur son téléphone.

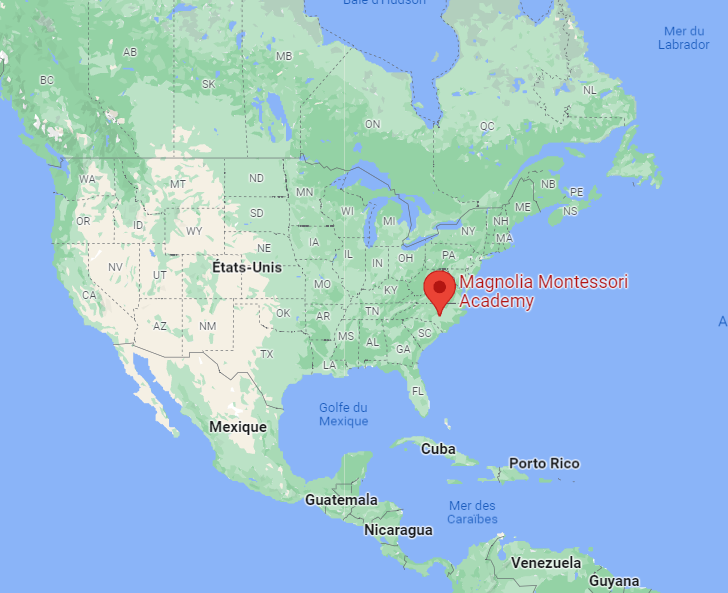


## Localisation

Grâce à Viber, nous savons qu’ils ont échangé des zones google map sous forme de lien vers une image. Vu qu’elles sont hébergées sur les serveurs de google, on a pu les récupérer :



En retrouvant les zones avec google maps, on se rend compte qu’elle corresponde avec les informations précédemment récoltées concernant la ville de **Raleigh en Caroline du Nor**d, ce qui appuis sur nos soupçons concernant sa localisation :



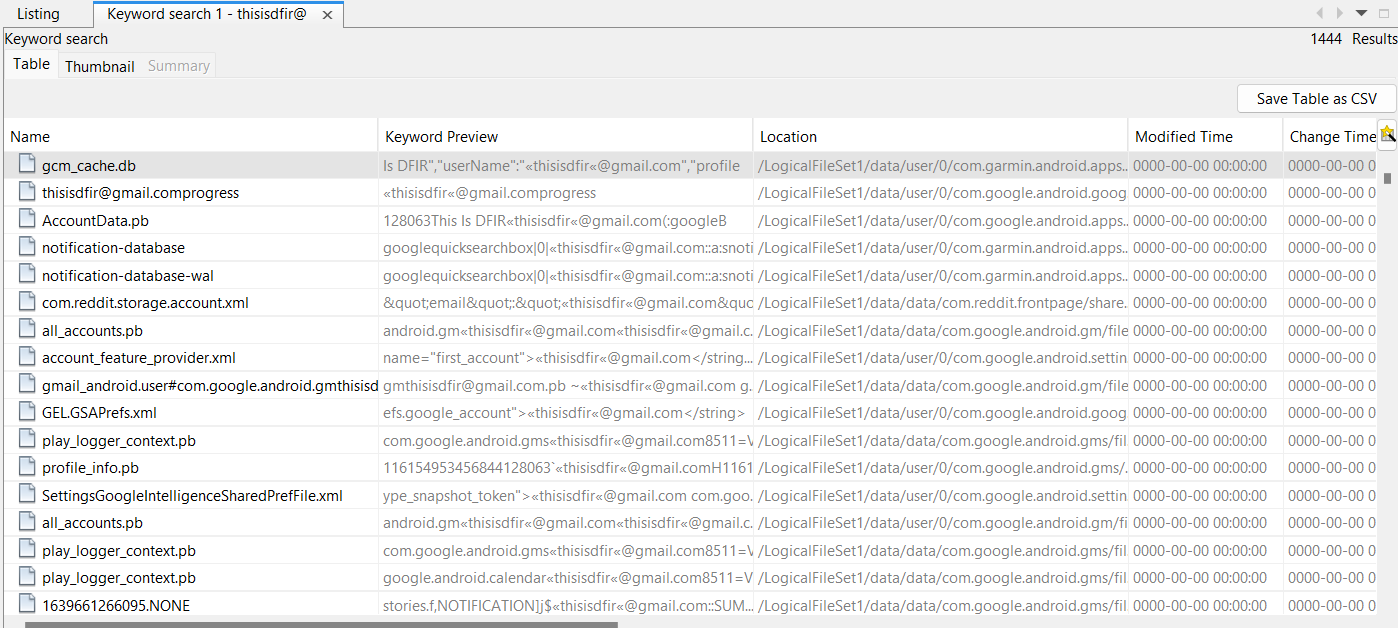
Par ailleurs, lorsqu’il crée son compte Line, il reçoit un message de vérification de connexion dans lequel on trouve son adresse IP : **64.98.122.70**.



# Utilisation de l’outil de recherche

## Adresse e-mail

Étant donné la structure des adresses e-mail trouvées dans ses contacts, la première recherche que l’on a effectuée est celle du mot-clé “thisisdfir@” afin de trouver un e-mail lui appartenant. Cette recherche a produit un nombre de 1444 résultats et nous avons ainsi pu instantanément trouver que son email le plus utilisé est “[**thisisdfir@gmail.com**](mailto:thisisdfir@gmail.com)”.



## D’autres recherches

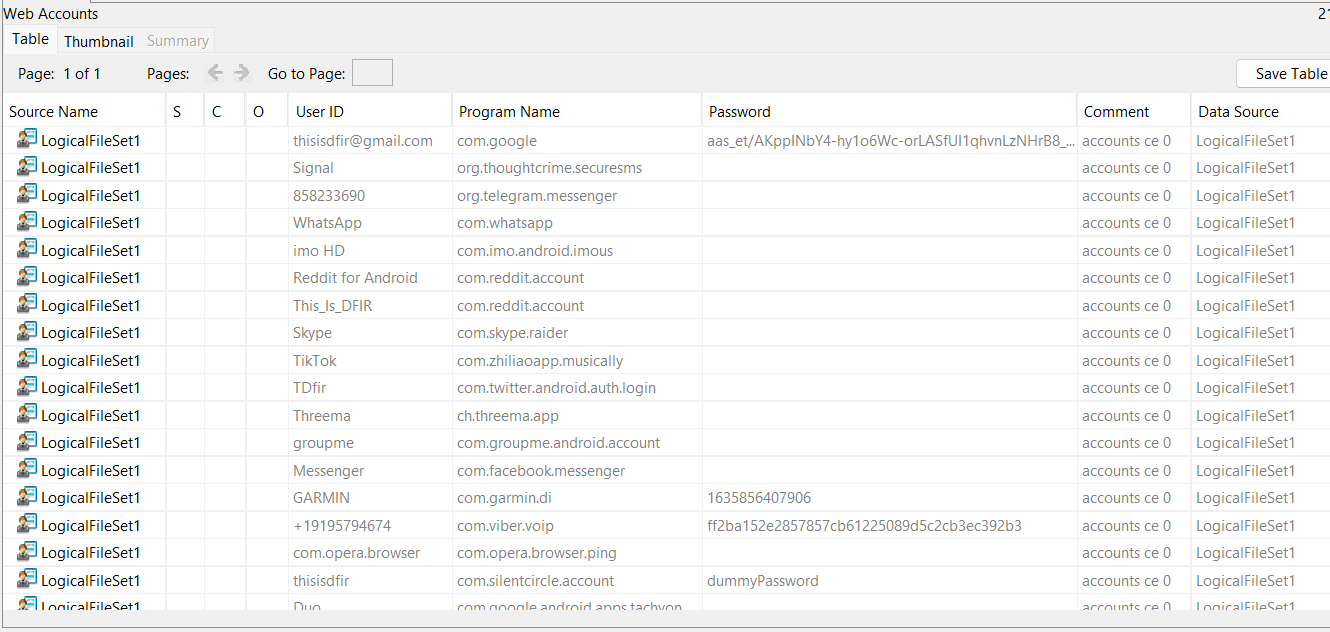
La deuxième recherche que l’on a réalisé concernait celle de l’IP précédemment trouvé (64.98.122.70), on se disait qu’il y allait peut-être y avoir des logs de requêtes ARP afin de pouvoir obtenir l’adresse MAC du téléphone mais les résultats sont trop nombreux et inexploitables.

La troisième idée que l’on a eu venait du fait que la plupart des applications ne sauvegardent pas les images directement dans le téléphone mais sur des serveurs distants. Ainsi, en cherchant la chaîne de caractères “s3.amazonaws.com”. Entre les urls non complètes, celles auxquelles on a pas accès et les nombreux fichiers de configurations json et javascript, on a seulement pu trouver une image de profil par défaut qui ne nous donne pas d’informations.



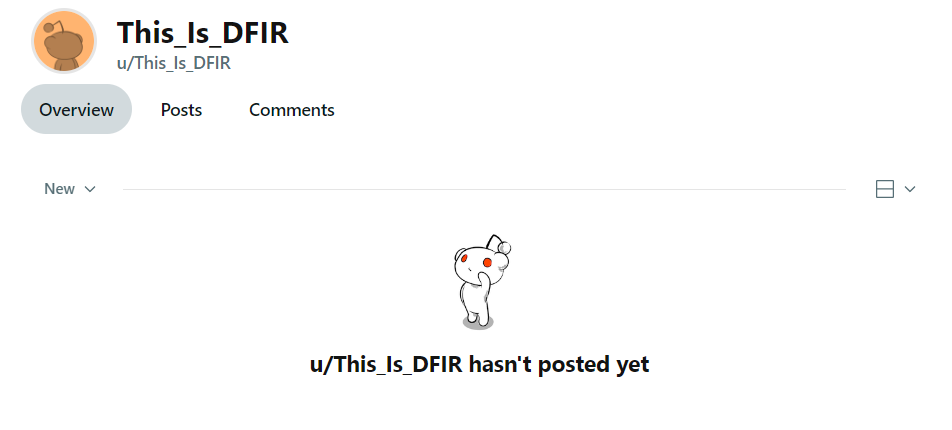
# Réseaux Sociaux & Applications

Avec l’aide de la partie “Web Accounts” dans “Data Artifacts”, on trouve facilement une liste des applications sur lesquelles l’utilisateur a un compte. Dans cette liste, il y a de nombreux comptes que l'on n'avait pas encore trouvés lors des précédentes étapes de recherche.



On note Signal, Reddit, Skype, TikTok, Threema, Telegram et Twitter. Par la suite, on essaiera d’obtenir plus d’informations concernant ces différents comptes.

## Reddit

Dans le cas de Reddit, son username semble être This\_Is\_DFIR. Cependant, il n’a jamais rien posté avec son compte.

## Twitter/X

Concernant Twitter/X, son pseudo est @TDfir. Voilà à quoi ressemble son compte :

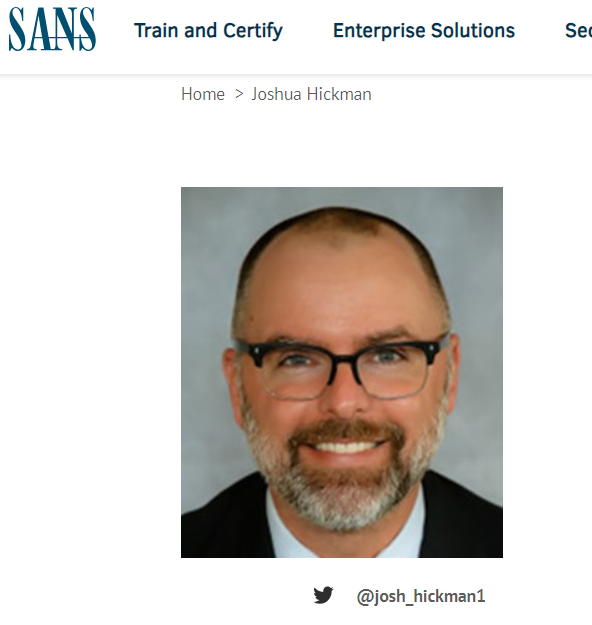
|  | |
| --- | --- |
|  |  |

Par rapport à ses abonnements, il y en a 2 que l’on peut directement ignorer puisque Tim Cook et Chrissy Teigen sont des personnalités publiques donc cela ne nous intéresse pas beaucoup. Par contre ses 3 autres abonnements recoupent les informations qu’on a déjà récupérées. Les 2 comptes nommés “ThisIsDFIRTwo” semblent bien être ses autres comptes. **Josh Hickman** est le même nom que l’on avait trouvé en analysant les communications. Il est possible que ce soit la même personne, mais il nous faut une preuve.

Parmi les personnes qui se sont abonnés à ce compte, on retrouve ses deux autres comptes ainsi que Josh Hickman et un autre compte. Cependant, étant donné que n’importe qui peut s’abonner à ce compte, ce n’est probablement pas une information intéressante.

Sur le compte de Josh Hickman, on découvre que sa localisation est en Caroline du Nord, c’est-à-dire la même zone géographique que ce qu’on avait trouvé lors de l’analyse des messages.

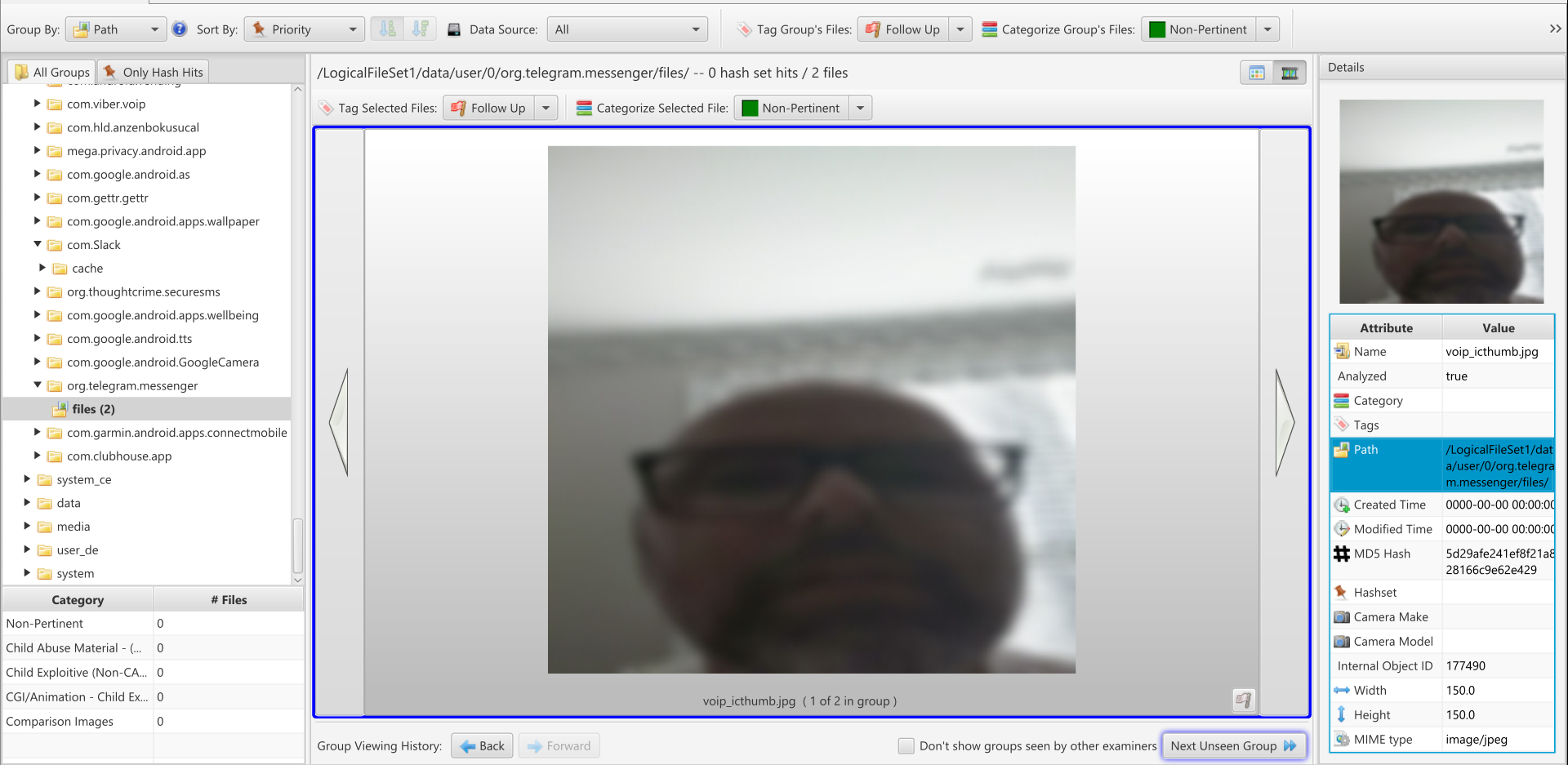
Par ailleurs, Josh indique sur son compte le lien vers son blog : <https://thebinaryhick.blog>. Sur ce dernier, on apprend que son nom complet est **Joshua Hickman** et qu’il pratique le Digital Forensic. En cherchant un peu sur internet, on trouve sur le site du SANS Institute une photo de Joshua Hickman, ainsi qu’une description. On apprend donc que Joshua est “Subject Matter Expert” chez Cellebrite. On remarque que le compte twitter indiqué correspond bien à celui qu’on a analysé un peu plus tôt.





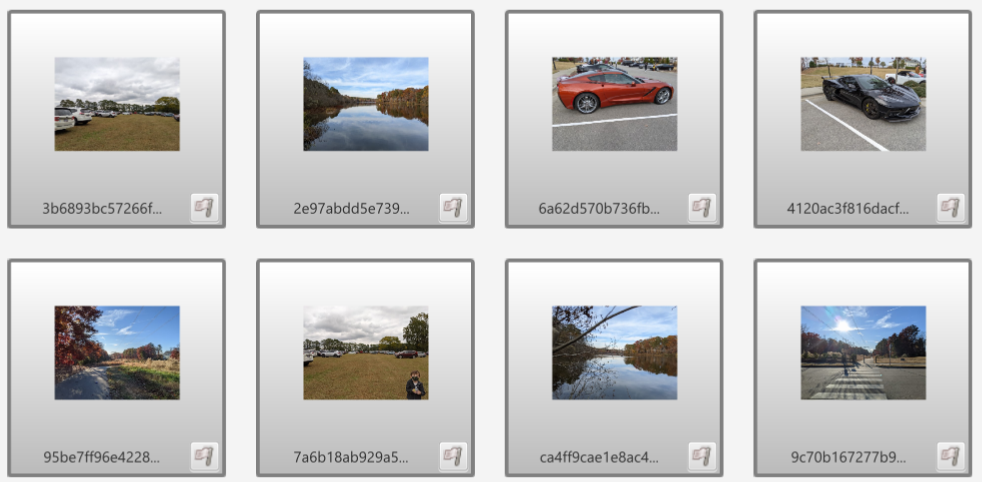
## Telegram

Dans le cas de Telegram, on a son numéro d’identification de compte : “858233690”. Mais on ne peut pas trouver d’autres informations à partir de là. Par contre, dans les fichiers du téléphones, on a trouvé cette image qui semble être une photo de profil. Peut-être s’agit-il de lui ?



## Google Camera

On trouve également plusieurs photos intéressantes dans les fichiers de Google Camera.



Et notamment, celle-ci :



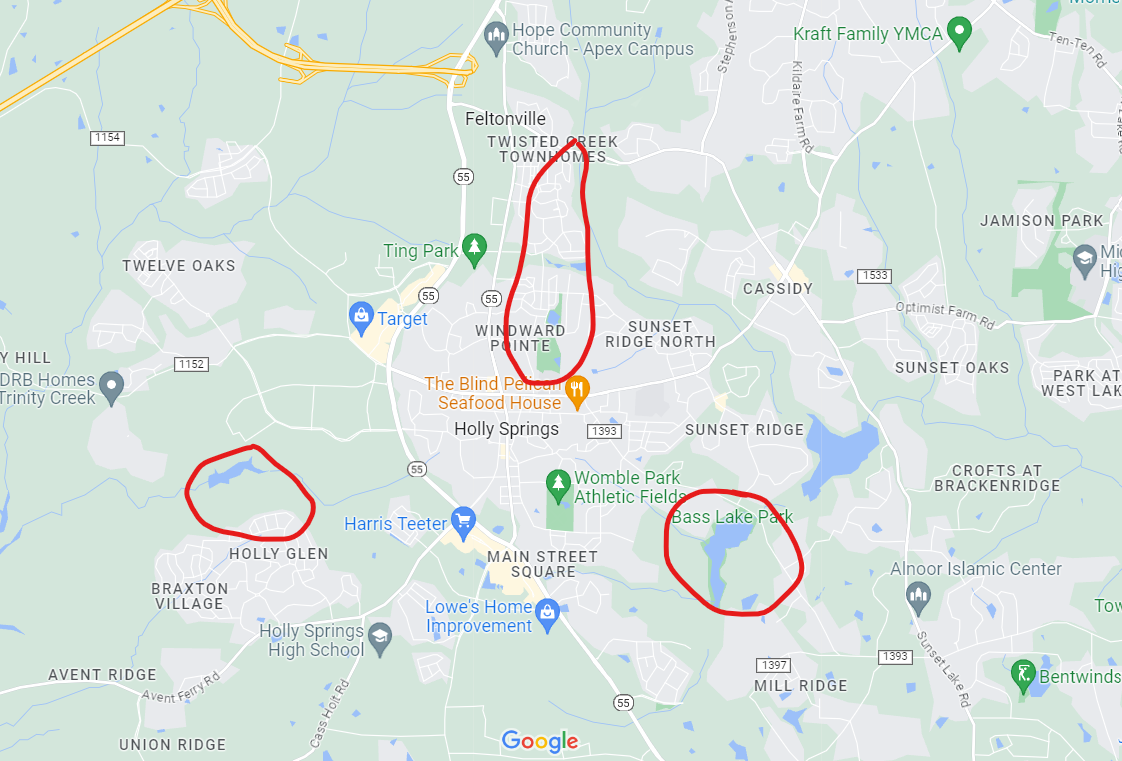
En comparant les 2 photos trouvées dans les fichiers et celle de Joshua Hickman du site de SANS Institute, on peut conclure qu’elles décrivent toutes la même personne et que **Joshua Hickman et ThisIsDFIR sont en réalité la même et unique personne**.

## AllTrails

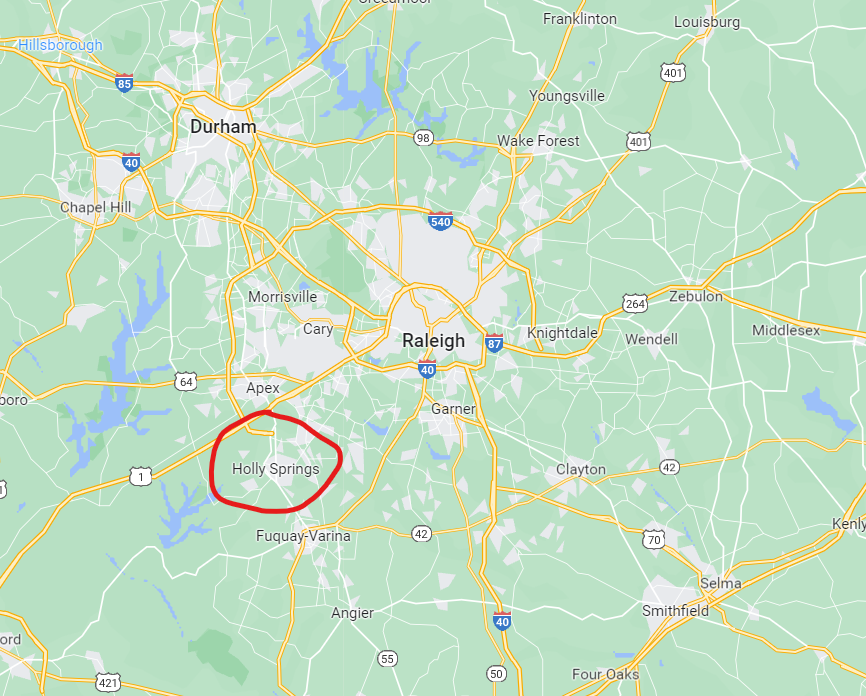
Une autre application intéressante est AllTrails. Il s’agit d’une application dédiée au fitness et aux voyages utilisée dans le cadre d'activités de loisirs en plein air. Ainsi, elle traque les déplacements réalisés lorsque l’utilisateur cours ou marche. Grâce à l’explorateur d’Extension Mismatch Detected dans les résultats d’analyse, on peut facilement récupérer les images en cache des applications afin de les afficher. Ainsi, on a trouvé des parcours que Joshua a réalisé lors de ses activités physiques :

|  |  |  |
| --- | --- | --- |

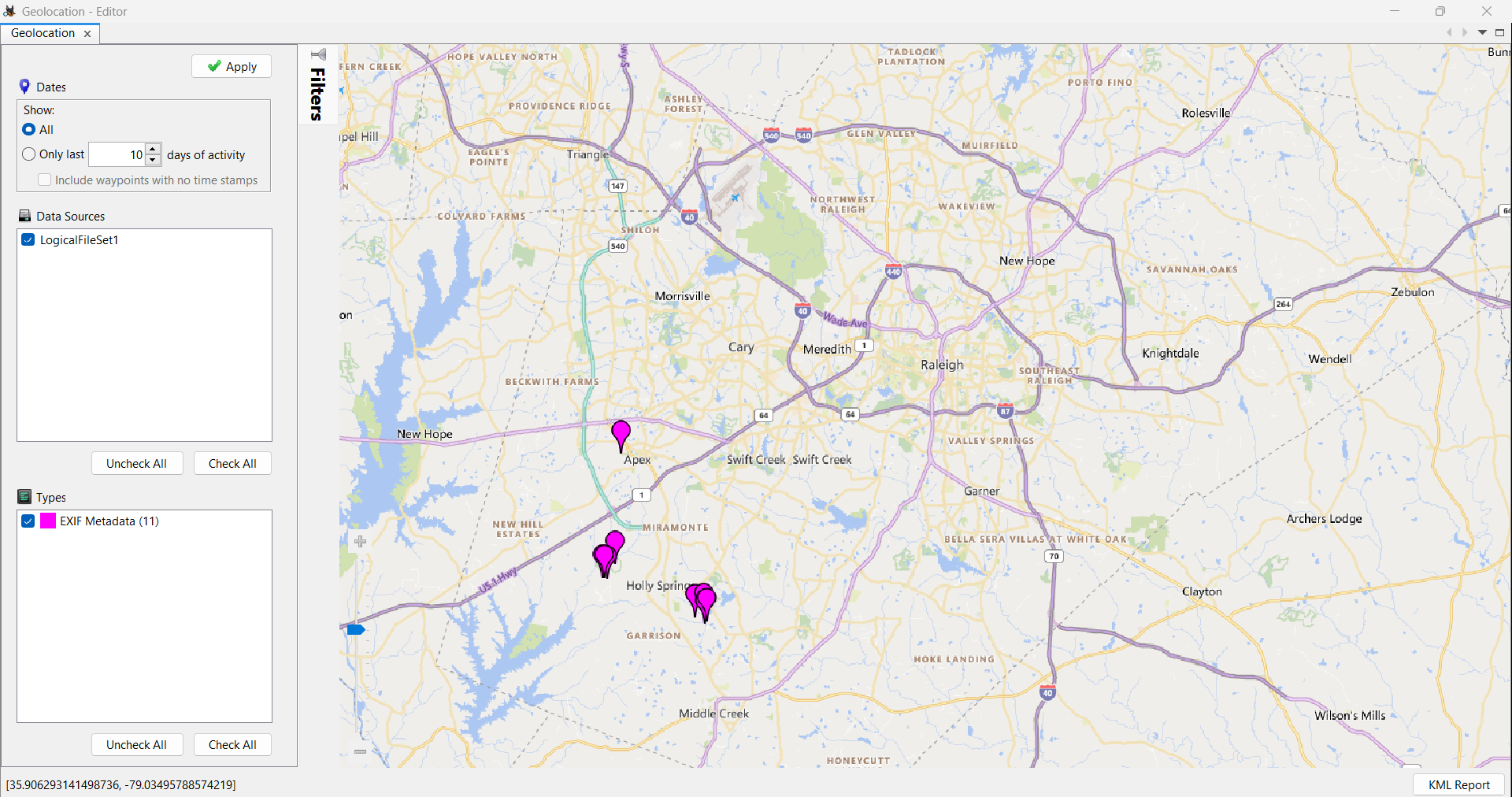
On a recherché ces zones autour de la ville qu’on a précédemment trouvé (Raleigh en Caroline du Nord). Voici la zone qui correspond sur laquelle on a indiqué le lieu de ces 3 trails :



Ainsi, on peut supposer que vu qu’il court dans cette zone, il devrait habiter quelque part par là (image montrant la proximité avec Raleigh) :



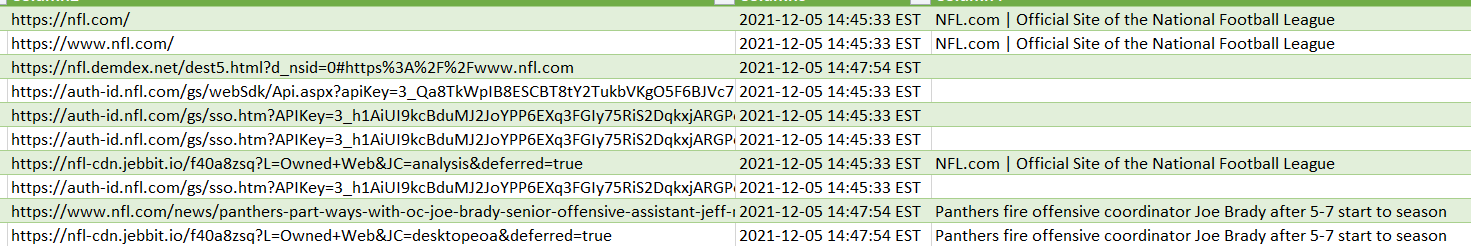
En utilisant l’outil de Géolocalisation intégré à Autopsy on trouve des points autour de cette ville également :



On note que ces points dépendent uniquement de méta données de différentes images. Ainsi, on peut recouper ces informations avec les précédentes informations de localisation et donc confirmer que Joshua habite à Holly Spring.

# Historique de navigation Web

L’analyse de ses données Web ne nous donne pas beaucoup plus d’informations que ce que nous avons déjà. Cependant, nous avons pu trouver une recherche récurrente.

En effet, en analysant son historique de navigation, on remarque que sur 574 résultats de navigation, 98 concerne le site de la NFL. On peut donc supposer que Joshua est **fan de football américain**.

Un lien vers une conversation Mega se trouve aussi dans l’historique :

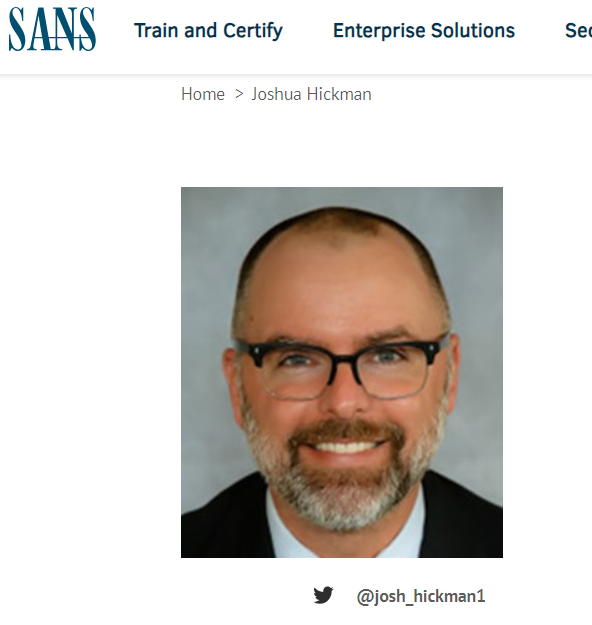
<https://mega.nz/chat/shZBQSrS#Fecr48QPYXZhNaxGkG74EA>

En cliquant dessus, on tombe sur une conversation entre ThisIs DFIR et ThisIs DFIRTwo, mais elle ne donne pas d'informations exploitables.

### 

# Conclusion

Avec les informations que nous avons pu obtenir, voici le portrait que nous pouvons faire de notre utilisateur :



**Prénom :** Joshua

**Nom :** Hickman

**Pseudos :** ThisIs DFIR, ThisIs DFIRTwo, ThisIs DFIRThree

**Lieu de vie :** Holly Springs, Caroline du Nord, Etats-Unis

**Numéros de téléphone :** +1 919 579 4674/+1 919 888 7386/+1 919 391 2507

**Adresse mail :** [thisisdfir@gmail.com](mailto:thisisdfir@gmail.com), [thisisdfirtwo@gmail.com](mailto:thisisdfir@gmail.com), [thisisdfirthree@gmail.com](mailto:thisisdfir@gmail.com), [joshuahickman957@gmail.com](mailto:joshuahickman957@gmail.com)

**Adresse IP :** 64.98.122.70

**Job :** Subject Matter Expert chez Cellebrite

**Hobbies :** Trailing, Football Américain, partager des memes