



# CTF IN THE WRONG PLACE AT THE RIGHT TIME

[RESUME](#)

AIDE

Ben Ammar Nourdine, Dubourgeois  
Camille, Hugues Rejaud

# SOMMAIRE

<b>Introduction.....</b>	<b>3</b>
Organisateurs et contexte.....	3
Scénario.....	3
Justification.....	4
<b>Réalisation.....</b>	<b>4</b>
Sensibilisation.....	4
Introduction aux bases de l'OSINT.....	4
Infrastructure (schéma du projet).....	5
Ressources.....	5
Techniques et outils.....	5
<b>Organisation du CTFd.....</b>	<b>6</b>
Les Problèmes Rencontrés.....	6
La création et l'intégration du QR code.....	7
L'intelligence Artificielle et les Sock-Puppets.....	7
La création des clés chiffrées.....	7
Compte Telegram.....	8
Gestion des groupes sur la partie physique.....	8
Mauvaise compréhension.....	8
Évaluation de la difficulté.....	8
Les Améliorations Possible.....	8
Retour des participants.....	9
Résolution du CTF.....	9
Conclusion.....	19
Remerciements.....	19
<b>Annexe.....</b>	<b>20</b>
Les organisateurs.....	20
Cadre légal.....	20
Qu'est-ce que n'est pas l'OSINT.....	21
Domaines d'application.....	21
Les Sous-Famille d'OSINT.....	22
Les cours sur les différents types d'OSINT présentés:.....	23
GEOINT.....	23
Challenge Cours GEOINT.....	24
Résolution du Challenge.....	25
IMINT.....	27
Challenge Cours IMINT.....	31
Résolution du Challenge.....	31

# Introduction

## Organisateurs et contexte

Dans le cadre des YDAYS au sein du Laboratoire SSI,

Camille Dubourgeois, Nourdine Ben Ammar, Hugues Rejaud ont décidé de créer un CTF portant sur l'OSINT pour notre projet fil rouge.

Nous avons choisi de mettre en avant l'OSINT dans notre CTF pour plusieurs raisons fondamentales. Tout d'abord, nous croyons fermement en la nécessité de sensibiliser les individus à l'importance de cette discipline dans le contexte de la sécurité informatique moderne.

L'OSINT offre un aperçu unique sur la manière dont les informations accessibles publiquement peuvent être exploitées pour évaluer les vulnérabilités potentielles d'un système ou aider à la recherche de personnes. En mettant en place un CTF centré sur l'OSINT, nous visons à éduquer les participants sur les méthodes et les outils disponibles pour recueillir, analyser et exploiter ces données de manière éthique et responsable.

Le projet nous a permis de découvrir aussi la création de CTF, être capable de créer des challenges intéressants pour les participants, et vérifier que les raccourcis n'existent pas pour résoudre les challenges. Nous avons appris sur la gestion et l'organisation d'un événement physique, pouvoir aider les gens et bien sur surveiller que tout se passe bien.

## Scénario

### *In the Wrong place at the Right time*

« Julia Spanghero, une jeune femme de 18 ans, a été enlevée de manière alarmante dans la région parisienne, plus précisément à Versailles, en France. Son enlèvement s'est produit le 1 mars 2024 vers X heures alors qu'elle partait faire un jogging. Julia Spanghero, décrite comme une étudiante brillante et pleine de vie, n'a donné aucun signe précurseur indiquant une volonté de disparaître volontairement.

Les témoins ont rapporté avoir vu une camionnette blanche s'arrêter brusquement près de Julia, avant qu'elle ne soit forcée d'y entrer.

Il est fortement soupçonné qu'une organisation criminelle puisse être derrière cet enlèvement. Des motifs précis ou des demandes de rançon n'ont pas encore été communiqués, plongeant la famille de Julia dans l'angoisse et l'incertitude.

Nous vous invitons à nous aider à retrouver Julia au plus vite. »

## Justification

Il à été naturel d'associer l'OSINT à l'enlèvement de personnes. Autant ces compétences peuvent desservir mais dans certains contextes ils sont utilisés à but de contribution citoyenne tout comme les actions menées par « Trace Labs » ou Bellingcat ». Nous pensons que montrer une des faces cachées d'internet peut être intéressantes et que tout peut se trouver sur le net si nous cherchons correctement.

Cela peut raviver le débat de l'anonymisation sur le web en partant du principe que certaines sources sont complètement publiques et ouvertes (sauf prédisposition prise par les utilisateurs dans certain cas particulier). Parfois des personnes disparaissent contre leur gré, ce qui arrive malheureusement plus souvent que l'on ne croit, à travers cet exercice vous êtes comme dans la peau d'un enquêteur qui retrace les événements avec les outils et informations à sa disposition afin de tenter de retrouver la/les personne(s).

Il peut être vraiment exaltant d'effectuer ses recherches et frustrant et parfois choquant. En effet parfois les recherches peuvent conduire dans des lieux plutôt sombres du net...

Néanmoins, il arrive de manière récurrente que les recherches n'aboutissent pas ou ont un dénouement malheureux et parfois positif.

## Réalisation

### Sensibilisation

Afin de débuter le projet nous avons décidé de commencer par des bases et faire des rappels concernant le cadre légal. Nous avons jugé essentiel d'informer nos participants sur les enjeux éthiques et juridiques liés à la collecte et à l'utilisation des informations publiques en ligne. De plus, un des objectifs du projet est de pouvoir sensibiliser les publics d'entreprises.

De plus sur chaque site ou applications utilisés on y retrouve une mention légal qui précise que tout cela est fictif et que nous sommes dans le cadre d'un exercice d'OSINT

Ces informations se trouvent dans le document qui se trouve en annexe. (CF. annexe)

### Introduction aux bases de l'OSINT

Pour notre projet, nous avons élaboré des documents détaillés expliquant les concepts fondamentaux de l'IMINT (renseignement d'imagerie), du SOCMINT (renseignement des médias sociaux) et du GEOINT (renseignement géospatial).

Ces documents ont été conçus pour fournir aux participants une compréhension approfondie de chaque domaine, y compris leurs méthodes, leurs outils et leurs applications dans le contexte de l'OSINT.

Nous avons jugé intéressant de fournir à nos participants les connaissances nécessaires pour aborder les épreuves du CTF avec confiance et compétences

De plus, une fois avoir lu et compris le cours, les participants pourront réaliser des challenges d'introduction mettant en pratique ce qu'ils auront appris.

## Infrastructure (schéma du projet)

En termes d'infrastructure , nous avons eu besoin de mettre en place un site web hébergé sur TOR via nginx dans une Virtual Machine (VM Ubuntu) ainsi que d'hébergé sur un VPS (Virtual Private Server) notre CTFd .

Concernant le site Web, il a été utilisé , du HTML + CSS + un proxy nginx ainsi que le service TOR.

## Ressources

Pour créer le CTF nous avons dû réfléchir sur une trame particulière afin que tous nos challenges aient un sens entre eux, une sorte de fil rouge. De plus, il a fallu étudier comment mettre en place les différents faux-compte, sur quelle plateforme etc.

Pour les réseaux et les différentes identités nous avons utilisé :

1. · ProtonMail
2. · Mastodons
3. · Instagram
4. · Strava
5. · Discord
6. · TOR/nginx
7. - Medium

Et pour l'hébergement du CTF :

- CTFD

## Techniques et outils

Dans la réalisation de notre CTF nous avons dû utiliser certains outils .

- **Aperisolv** : La plateforme de prédilection pour analyser les données, *Aperisolv* a fourni les outils nécessaires pour démêler les fils de l'information.
- **CyberChef** :Nous à permis d'encoder la plupart des informations que nous voulions dissimuler .Ici nous avons utiliser :
  - Base64
  - Base85
  - Hex

- **Génération de QR Code via Python** : Grâce à Python, nous avons pu créer via la librairie “qr” notre qrcode en y intégrant nos informations
- **Crocheter des Coffres-forts** : Dans un défi de compétences, nous avons mis les compétences des participants à travers l'épreuve en crochant des coffres-forts cela à permis pour certain d'améliorer leur dextérité dans cette discipline et pour d'autres une initiations ..
- **Acrobat première** : Afin de réaliser la vidéo d'introduction nous avons dû user de cet outil vraiment performant, qui nous a permis de manipuler à notre guise l'audio et de re-découper le son en fond correspond au thème des personnes disparues dans la réalité
- **Ai human generator** : Nous à permis de générer par IA tous les avatars du CTF comme par exemple “Julia”.
- **Ai NSFW** : Afin de rendre plus crédible la disparition de Julia dans le contexte d'une organisation criminelle nous avons dû modifier Julia . Ainsi nous avons pu la montrer dans une posture plus inquiétante ,démontrant l'importance de la retrouver..
- **Whatsmyname** : Est un outil vraiment puissant permettant de rechercher un pseudos ou un nom sur la plupart des réseaux sociaux
- **Holehe**: Tool en cli permettant une autre recherche sur les “username”
- **Exiftools** : Le même principe qu'aperisovl, il nous révèle les métadonnées contenu dans les images (coordonnée gps,auteur etc) sans la partie stéganographie.
- **Namint** : Outils permettant de rechercher une personne par son prénom et son nom sur une majorité de plateformes en formant différente combinaison entre son nom et prénom .
- **fcrackzip ou JhonTheRipper** : Outil permettant de cracker par bruteforce ou wordlist le mot de passe d'un fichier zip .
- **zip** : Outil permettant de créer une archive chiffrée.
- **Google lens** : Outil permettant de faire de la recherche d'image inversée.

# Organisation du CTFd

## Les Problèmes Rencontrés

Durant la conception du CTF nous nous sommes heurtés à plusieurs difficultés. La première étant la cohérence entre les différents challenges, en effet il fallait impérativement que les différentes résolutions respectent une logique et amène aux défis suivants . Pour entrer dans les détails nous joignons dans l'annexe la résolution du CTF et un schéma logique basé sur l'outil Osint Tracker (cf.annexe) .De plus certains aspect technique ont dû être abandonnées tel que la création d'un groupe "criminel" via Telegramm, pour la raison simple de ne pas acheter un numéro de téléphone supplémentaire et aussi la prise en compte de la difficulté que les concurrent aurait pu rencontrer .

## La création et l'intégration du QR code

Sur les aspects techniques, l'intégration et la génération du QR code ne fut pas sans difficultés . Le problème étant l'impossibilité de modifier directement via google maps une image en y intégrant notre QR Code menant au logo de l'organisation . Pour outrepasser cette action nous avons dû réfléchir à créer des "story" sur instagram et coller notre QRcode sur notre image noyée dans les différentes story .

La génération du Qr Code n'a pas étaient sans reste, il fallait qu'il soit ni trop grand ,ni trop petit afin de pouvoir être incrusté dans l'image . Le problème étant que les participants ont eu des difficultés à scanner celui-ci dû à sa résolution amoindrie du à l'incrustation sur l'image .En outre , la génération de celui-ci étaient légèrement complexe; les outils en ligne étant peu fiable, nous avons dû passer par un script python utilisant la librairie "qrcode" afin de le créer . (cf.annexe)

## L'intelligence Artificielle et les Sock-Puppets

Néanmoins, les difficultés techniques ne résidaient pas en totalité sur ce genre d'actions . La création des faux comptes (Sock-Puppet) ne fut pas trivial . Nous avons dû générer des photos par Intelligence Artificiel (cf.annexe).Le problème étant que les IA vraiment efficaces étant payante ,il a fallu s'adapter et utiliser les outils gratuits .Un des soucis était de re-générer une image à partir d'une personne générer par IA afin d'en obtenir une autre positions par exemple .

Nous ne détaillerons pas la partie concernant la photo de "Julia" NSFW .

Que se soit sur "mastodon" , "strava" , "instagram" .....

## La création des clés chiffrées

Lors de la mise en place du CTF avec les étudiants, possiblement par un problème de mise en place, les clés usb n'étaient plus chiffrées, les étudiant avaient donc accès à un éléments dont ils n'auraient pas dû avoir accès. Il a donc fallu refaire le chiffrement avant que d'autres étudiants parviennent à l'épreuve. Même si le chiffrement n'était pas compliqué à mettre en place, il a été un élément stressant car cette partie du challenge nécessitait un minimum de connaissances/compétences pour être réalisé.

## Compte Télégram

Dans un premier temps le groupe de malfaiteurs devaient se trouver sur l'application Telegram au lieu de discord. Malheureusement ce principe n'a pas vu le jour car il fallait un faux numéro de téléphone type burner et nous ne voulions pas investir la dedans. Il fallait aussi être sûr que chaque participant accepte d'avoir un compte Télégram donc mettre son numéro de téléphone.

## Gestion des groupes sur la partie physique

Par manque d'anticipation de notre part, même si au final celui-ci a été plutôt bien géré, la partie physique ne pouvant être réalisé par tout le monde en même temps, il a fallu pendant le CTF instaurer une règle pour que tout le monde puisse s'essayer aux challenges sans handicaper les autres participants. Il a donc été décidé que pour la partie crochetage, les groupes avaient 5 minutes pour essayer d'obtenir la clé usb si un autre groupe attendait pour résoudre ce challenge. Pour les coffres, la même règle est appliquée, 5 minutes par groupe dans le cas où un autre groupe attendait. Sur le dernier challenge qui était assez complexe et par usure du matériel qui modifiait le challenge au fur et à mesure, il été décidé que le challenge était remis en l'état ou il avait été laissé pour chaque groupe.

## Mauvaise compréhension

Certains groupes ont énormément avancé dans le challenge, sans pour autant valider les étapes dans le CTFd. La mauvaise compréhension se faisait car notre premier challenge et notre dernier challenge demandaient tous deux des coordonnées. Certains sont donc arrivés sur le premier challenge avec les coordonnées du dernier challenge sans comprendre pourquoi cela ne fonctionnait pas. Nous n'avons pour le coup pas compris si c'était dû à une mauvaise explication du challenge de notre part ou bien un raté de la part des étudiants.

## Évaluation de la difficulté

Au début du CTF nous avons eu des doutes sur la difficulté de notre CTF, étant notre premier exercice en la matière nous avions peur d'un ctf fini en 15 minutes. Finalement la plupart des participants ont joué le jeu et notre CTF a tenu plus de la demie journée qui était le temps minimum. La difficulté du CTF était faite pour que tout le monde puisse participer en commençant par des étapes simples et en se complexifiant. Nous nous sommes rendus compte au fur et à mesure de la résolution des challenges que certains challenge comportait des coquilles et ont dû faire l'objet de changements minimes pendant le CTF.

## Les Améliorations Possible

En proposition d'amélioration pour la suite, nous avons pensé à une deuxième partie sur l'enquête de cette organisation. Cela permet de faire un CTF sur une durée plus longue et élargir les aspects de l'OSINT en trouvant des nouveaux challenges avec des tools et techniques différentes. Il faudrait grâce aux différents retours des participants améliorer notre vue logique des challenge, effectuer une phase de test plus important avec plus de testeurs.

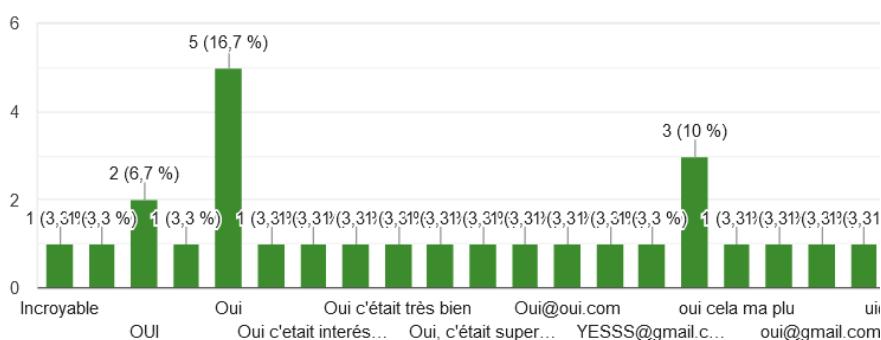
## Retour des participants

Une fois que tous les participants avaient fini le CTF, nous avons demandé au directeur de Labo de faire suivre un lien à tous les participants pour avoir un retour sur notre travail. Nous avons tous les trois été très agréablement surpris de ne voir aucun retour négatif, seulement quelques propositions ou corrections à apporter.

Quelques statistiques :

Cela vous as t'il plu ?

30 réponses



Il était important d'avoir également les retours négatifs afin de mieux se préparer si potentiellement il y a une partie 2 .

Ce qui ne vous a pas plu ? Et pourquoi ?

30 réponses

certaines réponse pas précisé si attendu en anglais ou fr ou russe, un petit manque de rigueur sur le format des flags mais c'était ok franchement

J'ai certes très bien mangé, mais j'ai encore faim !

tout est bien

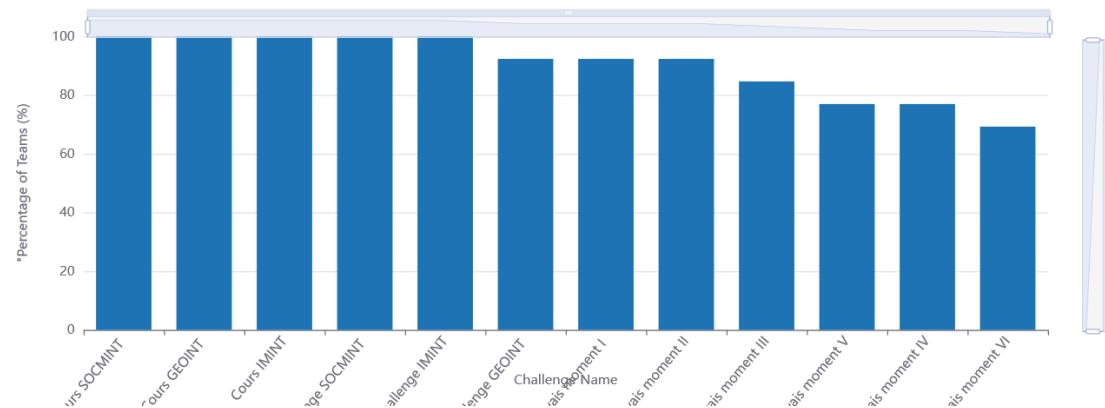
Un peu désorienté sur le challenge "Au mauvais endroit au mauvais moment", nous avons sauté l'étape du camion, et nous avons rentré les coordonnées trouvées sur le site Tor.

le dernier coffre a ouvrir car je n'ai pas trouvé la chose très concrète

J'aurais apprécié que ça soit plus long, parce que c était trop court :)

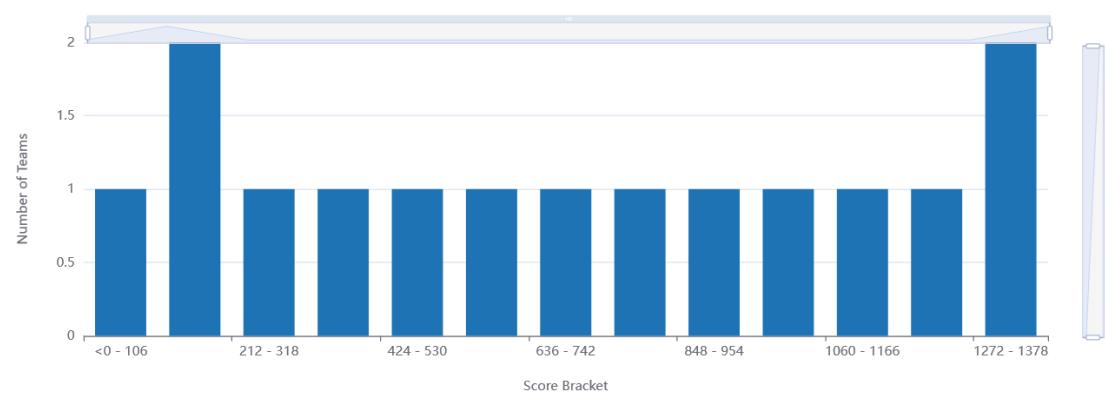
mm quelque détails manquant notamment sur le format des challenges mais pas bloquant en soit

Solve Percentages per Challenge



Néanmoins, il n'y avait pas un écart massif entre les équipes et ce malgré un niveaux hétérogène au sein du CTF comme en témoigne ce document iconographique :

Score Distribution



Cependant nous remarquons également que certaines équipes ont tout simplement jeté l'éponge ou ne se sont pas investies à 100 % dans ce qui leur était proposé .

En conclusion, nous pouvons affirmer avec certitude que notre objectif a été atteint, et que celui-ci à vraiment intéressé le public en majorité. Les différentes remontées nous permettront d'améliorer notre prochain CTF d'osint.

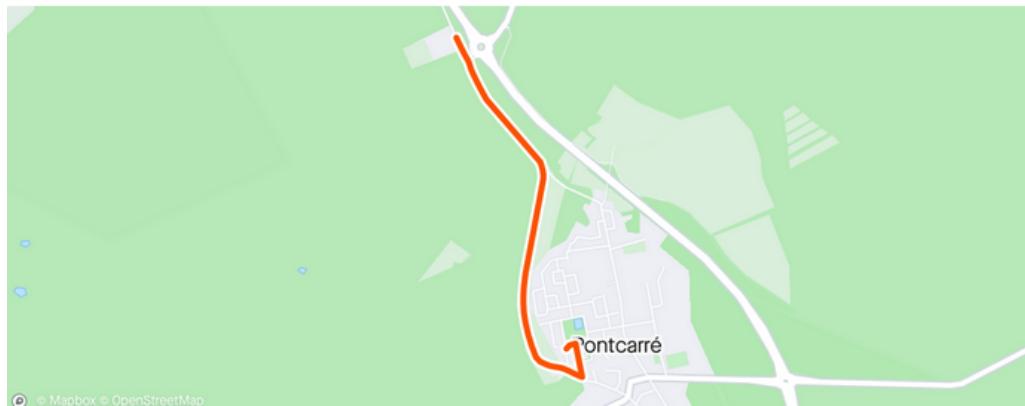
## Résolution du CTF

Dans un premier temps il fallait trouver via les informations données par le 1 challenge sur quelle réseau/plateforme c'était inscrite Julia :

The screenshot shows a Strava user profile for 'Julia Spanghero'. On the left, there's a summary section with 0 subscribers and 0 followers, and 1 activity. The latest activity is 'Course chez papa et maman' from February 14, 2024. Below that is a 'Your training journal' section. To the right, the detailed activity page for 'Course chez papa et maman' is shown. It includes a description: 'Merci à mes parents de pouvoir m'évader de la région parisienne ! Grosse course on reprend demain le même parcours'. The activity details are: Distance 22,64 km, Average pace 11:59 /km, Time 4h 31min, and 11 performances. A congratulatory message says 'Félicitations, vous venez d'établir votre PR sur semi-marathon !'. Below this is a map of the route, which starts in Pontcarré and goes into the 'Forêt régionale de Ferrières'.

Après quelque recherche nous trouvons un compte strava avec différent parcours, il y en a un qui est terminé et un autre non, pour le flag il nous faut l'endroit où Julia à disparue :





Après une recherche sur google maps on trouve **FLAG N°1** : 48.808\_2.695

Dans sa description elle nous donne l'informations qu'elle possédait un autre compte intitulé "@ju\_fraiche" :

Hello !  
Amoureuse de la course, j'adore me challenger !  
Je participe régulièrement à des marathons et à la  
marche pour le cancer .  
Je fais partie d'un club sur Paris , qui a pour activité  
principal la préparation physique !

À bientôt sur les parcours !

PS : vous pouvez me suivre sur instagram (@ju\_fraiche)  
pour voir tout mes parcours

En cherchant un peu sur le net on peut déduire que ce pseudos et sois sur twitter ou sur instagram au vue du "@"

En utilisant cette outil : <https://inflact.com/tools/profile-analyzer/>

Nous nous apercevons que c'est bien Julia !

ju\_suis\_tf  ju\_fraiche

**Ju\_suis\_fraiche**

Spain

Passion Running  Yoga et détente  "Tourne toi vers le soleil et l'ombre sera derrière toi"

9 excellent ?

On en allant sur instagram nous pouvons observer plusieurs stories :



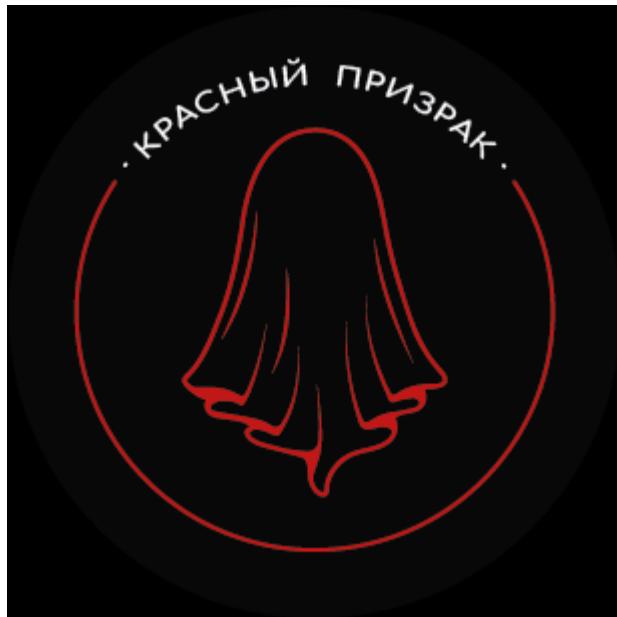
Plusieurs villes apparaissent avec probablement les parcours de jogging de Julia , concentrons nous sur Pontcarré" à priori elle a 2 parcours la bas et un qui ne s'est pas terminé correctement . En inspectant les stories une à une il y a un nouvel indice :



Bingo un QR code sauvage apparaît , et si on essayait de le décoder ?



En décodant celui-ci nous retrouvons un logo un peu particulier héberger sur :  
<https://notjustwork.fr/img-rg.jpg>



Ici au premier abord cela semble être un logo particulier, avec le nom d'un groupe peut être celui ayant enlever Julia, essayons de traduire l'écriture :

<b>fantome noir et rouge</b>	<b>×</b>	<b>черно-красный призрак</b> cherno-krasnyy prizrak
----------------------------------	----------	--

En regardant un peu les mots on voit une similitude sur le logo et "призрак", celui-ci veut dire rouge en russe . Essayons de modifier un peu la recherche

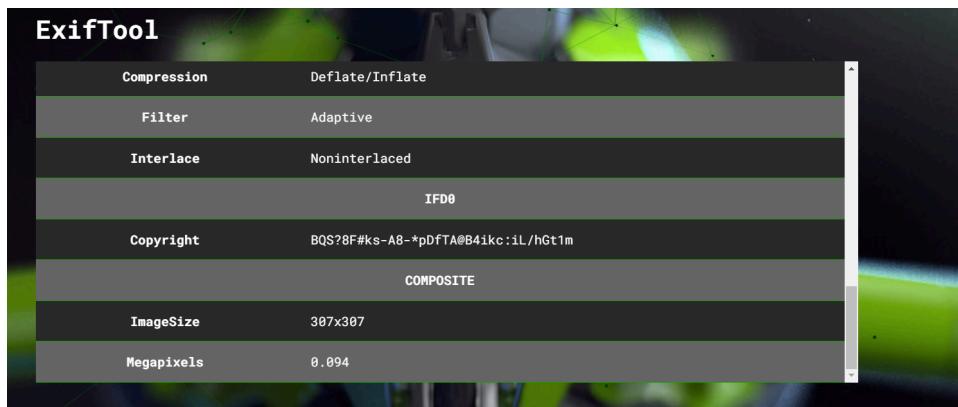
<b>fantome et rouge</b>	<b>×</b>	<b>призрак и красный</b>
-------------------------	----------	--------------------------

Nous sommes tout prêt seul un caractères est en trop voulant dire "et"

<b>fantome rouge</b>	<b>×</b>	<b>красный призрак</b>
----------------------	----------	------------------------

Donc notre organisation s'appelle Fantôme Rouge ou Red Ghost .

Regardons l'image d'un peu plus près elle doit surement cacher d'autres informations ,en utilisant aperisolve nous pouvons remarquer qu'il y a d'autre infos cacher dans les métadatas :



Les Copyright semblent assez étrange ...

Dans le doute on essaye de décoder avec notre tool favori "Cyberchef" et celui-ci nous annonce:

The screenshot shows the CyberChef interface with the following details:

- Input: BQS?8F#ks-A8-\*pDfTA@B4ikc:iL/hGt1m
- Alphabet: ! - u
- Decoding mode: Base85
- Output: https://discord.gg/DPpjyGV

Du base 85 décoder nous amène sur un discord.

Pour le flag il nous faut le nom de l'organisation et le fameux lien discord

**FLAG N°2 :** red-ghost\_https://discord.gg/Wwg44ARsNn

Bien entendu nous allons devoir suivre cette piste :

The screenshot shows a Discord channel named #welcome. A message from a user named "Кинг конг" (King Kong) on March 20, 2024, at 14:26, contains the following text:

C'est le début du salon #welcome.  
Modifier le salon

20 mars 2024

Кинг конг 20/03/2024 14:26  
Всех приветствуем, посетители и покупатели разрешены, но вы можете присоединиться к нам с определенной ролью, которую можно запросить, нажав на соответствующий emoji. Да здравствует Россия-матушка! (modified)

On se balade un peu sur le discord de l'organisation et nous voyons que certains channel nous bloquent, peut-être pas le bon rôle ?

On commence à inspecter les conversations ...

Шалашаска 14/02/2024 10:39

Какие варианты ты можешь найти на рынке темных сетей? Хочешь купить что-то особенное? На нашем сайте "Теневой Рынок" ты найдешь широкий ассортимент наркотиков высочайшего качества. Мы предлагаем анонимные транзакции и гарантированную конфиденциальность. Наши продавцы тщательно проверены и обеспечивают быструю и надежную доставку. Не упусти шанс воспользоваться нашими услугами и сделать свою жизнь немного ярче.

1

Наши бутоны обладают неповторимым ароматом и потрясающим вкусом, который оставит вас в восторге. Мы гарантируем высокое качество и чистоту каждого продукта, так что вы можете наслаждаться своим выбором без каких-либо сомнений. Не упустите возможность испытать истинное удовольствие с нашим качественным каннабисом



Наши цены на каннабис доступны в диапазоне от 1 до 5 биткоинов. Мы принимаем

À priori on est bien sur le marketplace de l'organisation, il y a de la drogue des filles et pas de mal clients, mais toujours rien concernant l'obtention du rôle , les traduction des texte ne nous rapporte rien . Par contre un salon attire notre attentions : Le Welcome

Кинг конг 20/03/2024 14:26

Всех приветствуем, посетители и покупатели разрешены, но вы можете присоединиться к нам с определенной ролью, которую можно запросить, нажав на соответствующий emoji. Да здравствует Россия-матушка! (modifié)

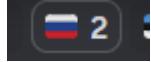
🇷🇺 1 🇺🇦 1 🇮🇩 1 🇵🇾 1 🇩🇪 1 🇷🇺 1 🇲🇽 1 🇸🇮 1 🇰🇷 1 🇹🇷 1 🇭🇷 1

🇷🇸 1

En traduisant le russe nous obtenons :

“Tous sont les bienvenus, les visiteurs et clients sont autorisés, mais vous pouvez nous rejoindre avec un rôle spécifique, qui peut être demandé en cliquant sur l'emoji approprié. Vive la Mère Russie !”

Bingo, maintenant à nous de choisir. En partant du principe que l'organisation est Russe :



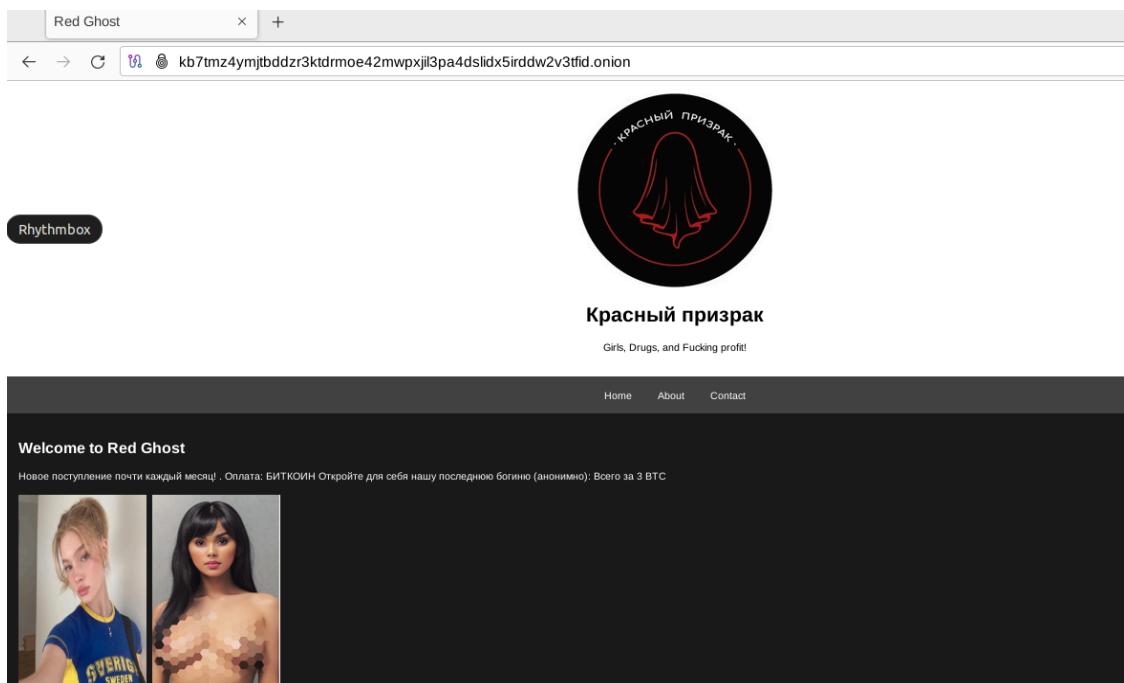
Celui-ci nous confère donc le rôle soldat... Allons explorer les salons privés !

Dans le salon plan nous récupérons une informations qui semblent être un hexdump au premier coup d'oeil (et oui nous sachons) :

```
00000000 32 30 20 37 30 20 36 66 20 33 32 20 37 38 20 33 |20 70 6f 32 78 3|
00000010 36 20 36 65 20 36 64 20 36 62 20 36 62 20 37 34 |6 6e 6d 6b 6b 74|
00000020 20 36 36 20 36 34 20 37 31 20 37 33 20 37 32 20 |66 64 71 73 72 |
00000030 37 39 20 37 38 20 36 66 20 36 33 20 37 31 20 36 |79 78 6f 63 71 6|
00000040 31 20 36 66 20 33 36 20 33 37 20 36 39 20 37 34 |16f 36 37 69 74|
00000050 20 36 62 20 37 39 20 37 39 20 36 39 20 37 39 20 |6b 79 79 69 79 |
00000060 36 34 20 36 63 20 36 35 20 36 66 20 36 35 20 37 |64 6c 65 6f 65 7|
00000070 35 20 37 61 20 33 33 20 36 37 20 37 32 20 33 37 |5 7a 33 67 72 37|
00000080 20 37 30 20 36 39 20 33 32 20 36 66 20 33 36 20 |70 69 32 6f 36 |
00000090 37 37 20 36 38 20 37 32 20 36 32 20 37 61 20 36 |77 68 72 62 7a 6|
000000a0 63 20 36 33 20 36 31 20 36 34 20 32 65 20 36 66 |c 63 61 64 2e 6f|
000000b0 20 36 65 20 36 39 20 36 66 20 36 65 | 6e 69 6f 6e| (modifié)
```

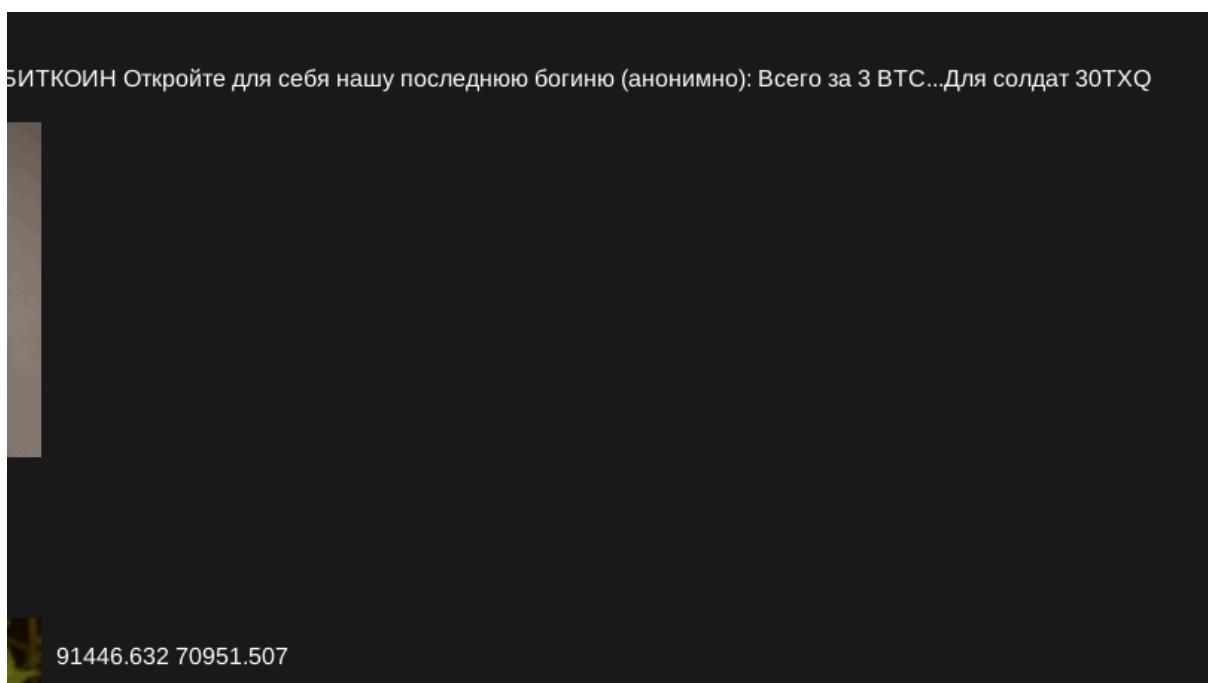
Encore une fois notre tool préférer Cyberchef :

po2x6nmkktfdqsryxocqao67itkyyiydleoetzgr7pi2o6whrbzcad.onion



Voilà Julia et d'autres filles !!!!

En inspectant le site web sur le darknet on peut voir ceci qui n'a rien à faire là on dirait :



Cela ressemble à des coordonnées MGRS, le flag nous demande des coordonnées au format 'standard (google map quoi)', il suffit de taper dans google "30TXQ coordonnées"

<https://coordinates-converter.com/fr/decimal/51.000000,10.000000?karte=OpenStreetMap&zoom=8>

En récupérant les vraies coordonnées, le challenge physique commence et vous pouvez répondre au FLAG N°3 en entrant le site en .onion ainsi que le nom du bâtiment et des protections de celui-ci !

**FLAG N°3 :** po2x6nmkktfdqsryxcqao67itkyyiydleoetzgr7pi2o6whrbzcad.onion\_bordeaux-ynov-campus\_nfc

La première partie du challenge physique était du crocheting, une boîte à clé fermé avec un cadenas contenant une clé usb :



Une fois la boîte ouverte, il faut mettre la clé usb sur un poste et récupérer une archive chiffrée.

Pour déchiffrer l'archive, une brute force s'impose avec comme outils JhonTheRipper ou frackzip et comme wordlist, une bonne vieille Rockyou.txt.

Une ligne de commande pouvant être utilisée :

```
fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt archive.zip
```

Et on trouve que le mot de passe était : *peanutbutter*

Une fois l'archive déchiffrée, on obtient un document qui n'est autre que la documentation qui va servir à ouvrir le premier coffre. Il fallait donc trouver la partie de la documentation qui explique comment passer outre le code de base et se rendre au coffre pour passer au challenge suivant :

#### **Creating the Override Code**

1. Input: # - #; [SUPER] will appear on the display. Do not pause between # - # entries.

2. Input: Override Code; the safe will unlock.

The default Override Code is: 6 5 3 5 8 9

Il fallait taper sur le coffre :

## puis attendre de voir le mot SUPER s'afficher sur l'écran et pour finir taper 653589 (merci **TT**).



**FLAG N°4 : ##653589**

Voilà l'avant dernière partie terminée, plus qu'un dernier coffre à ouvrir.

Pour ouvrir ce dernier coffre, il fallait commencer par faire une petite recherche de documentation sur ce dernier. Rien de plus simple que d'utiliser notre cher ami google lens :



On tombe alors sur la page d'un vendeur comme Leroy Merlin :

<https://www.leroymerlin.fr/produits/quincaillerie/cadenas-coffre-fort-et-securite-des-biens/coffre-fort/coffre-fort-a-code/coffre-fort-sft-15enp-h-15-x-l-20-x-p-15-cm-73321451.html>

Et dans les documentations, on retrouve celle qui nous intéresse :

<https://media.adeo.com/marketplace/LMFR/19309143/3427692.pdf>

Une fois la lecture de ce dernier faite, pinces et cintres étaient à disposition des challengers pour réussir à enlever la petite trappe qui cachait le bouton de réinitialisation du coffre. Et le tour est joué, Julia est saine et sauve. En échange de votre acte héroïque, elle vous donne le dernier flag et PAF, vous avez terminé ce CTF 😊. **FLAG N°5 : 1\_M\_@L1VE**

## Conclusion

La mise en place de ce CTF d'OSINT a été une expérience enrichissante pour notre équipe. Non seulement cela nous a permis de développer nos compétences personnelles en OSINT, mais cela nous a également appris à mieux gérer la collaboration, la planification et la communication. Ce projet nous a motivés à poursuivre notre apprentissage et notre exploration en OSINT.

Nous voudrions mettre en place une seconde partie à ce CTF qui serait plus complexe et plus fourni. Elle aurait pour but de démanteler l'association de malfaiteurs RedGhost. Cela se fera peut-être l'année prochaine.

## Remerciements

Un grand merci aux personnes qui nous ont aidés de près ou de loin à la conception de ce CTF :

Sacha, Bryan, Pierre-lin, Julie, Adrien 😊

## Annexe

Road Map Challenge In the Wrong place at the Right time :

Disponible en fichier PDF dans le dossier rendu.

## Les organisateurs

Membres :

- Ben Ammar Nourdine : Master 1 Cybersécurité
  - Team Lies\_O "CTF OSCAR ZULU"
  - OZINT.eu = Ezpert/Team=Ynov Street/
  - 404 CTF
  - Stranger Case(en solo)
- Camille Dubourgeois : Master 2 Cybersécurité
  - OZINT.eu = Ezpert Team=Ynov\_Street
  - EC2
- Hugues Rejaud : Master 2 Cybersécurité
  - OZINT.eu = Ezpert Team=Ynov\_Street
  - EC2

## Cadre légal

Le cadre légal de l'OSINT, ou "Open Source Intelligence", varie d'un pays à l'autre en fonction des lois sur la confidentialité, la protection des données et la réglementation en matière de cybersécurité. Dans de nombreux pays, la collecte d'informations à partir de sources publiques en ligne est généralement légale, car ces données sont accessibles au public. Cependant, il existe des limites importantes à respecter.

Il est essentiel de se conformer aux lois locales et nationales sur la vie privée, en évitant d'accéder à des informations protégées par des droits d'auteur ou en utilisant des méthodes intrusives telles que le piratage informatique. De plus, la divulgation publique des informations collectées peut également être soumise à des réglementations spécifiques.

## Qu'est-ce que n'est pas l'OSINT

Pour clarifier ce que n'est pas l'OSINT, voici quelques points à considérer :

1. Ce n'est pas du piratage : L'OSINT repose sur la collecte légale d'informations à partir de sources publiques. Il ne doit pas impliquer de techniques de piratage, d'intrusion dans des systèmes informatiques ou d'accès illégal à des données privées.
2. Ce n'est pas de l'espionnage illégal : L'OSINT n'implique pas d'activités d'espionnage clandestines ou de collecte d'informations sensibles sans autorisation. Il se limite aux données accessibles au public.
3. Ce n'est pas de la désinformation : L'OSINT vise à recueillir des informations objectives et factuelles. Il ne devrait pas être utilisé pour propager de fausses informations ou des rumeurs.
4. Ce n'est pas une activité illégale : L'OSINT est généralement conforme aux lois sur la protection de la vie privée et la réglementation en matière de données, tant que l'on respecte les limites légales et éthiques.
5. Ce n'est pas une technique de collecte d'informations secrètes : L'OSINT se concentre sur la collecte d'informations ouvertes au public, ce qui le distingue des activités de renseignement classique qui visent à recueillir des informations secrètes.

## Domaines d'application

Voici quelques-uns des principaux domaines d'application de l'OSINT :

**Sécurité nationale et renseignement** : Les agences gouvernementales utilisent l'OSINT pour surveiller les menaces potentielles, suivre des groupes terroristes, et recueillir des informations sur les activités internationales.

**Application de la loi** : Les forces de l'ordre utilisent l'OSINT pour enquêter sur des affaires criminelles, identifier des suspects, surveiller les médias sociaux, et recueillir des preuves en ligne.

**Gestion des crises** : L'OSINT est précieux pour anticiper et répondre à des catastrophes naturelles, des incidents de sécurité, ou des crises de santé publique en surveillant les médias sociaux et d'autres sources d'information en temps réel.

**Veille concurrentielle** : Les entreprises utilisent l'OSINT pour collecter des informations sur leurs concurrents, les tendances du marché, et les commentaires des clients, ce qui les aide à prendre des décisions stratégiques.

**Gestion des risques** : Les entreprises et les organisations évaluent les risques potentiels en utilisant l'OSINT pour surveiller les menaces en ligne, les cyberattaques, les activités criminelles et les mouvements sociaux.

**Journalisme d'investigation** : Les journalistes utilisent l'OSINT pour découvrir des informations pertinentes, valider des histoires, et creuser plus profondément dans des sujets d'intérêt public.

**Recherche en sciences sociales** : Les chercheurs utilisent l'OSINT pour étudier les tendances sociales, analyser des données démographiques, et explorer des questions liées à la société, à la politique et à la culture.

**Intelligence économique** : Les organisations utilisent l'OSINT pour surveiller l'environnement des affaires, détecter des opportunités ou des menaces potentielles, et protéger leurs intérêts.

**Gestion de la réputation en ligne** : Les individus, les entreprises et les personnalités publiques utilisent l'OSINT pour surveiller leur image en ligne, gérer les retours d'informations, et répondre aux commentaires négatifs.

**Analyses de marché** : Les professionnels du marketing utilisent l'OSINT pour recueillir des données sur les comportements des consommateurs, les préférences, et les tendances afin d'adapter leurs stratégies commerciales.

## Les Sous-Famille d'OSINT

**Le SOCMINT** : renseignement à partir des réseaux sociaux

**l'IMINT** : renseignement à partir d'images

**Le SIGINT** : renseignement à partir de signaux électroniques

**l'HUMINT** : renseignement à partir de sources humaines

**Le GEOINT** : renseignement à partir d'imagerie géospatiale

**Le MASINT** : renseignement à partir de mesures

Mention spéciale pour la recherche cadastrale qui ne finit pas par "INT". Néanmoins cela reste de l'OSINT

## Les cours sur les différents types d'OSINT présentés:

### GEOINT

#### Définition du GEOINT :

Le GEOINT est l'acronyme de Geospatial Intelligence, une discipline qui intègre des données géographiques avec des renseignements pour créer une compréhension holistique d'une situation.

#### Composants du GEOINT :

**Imagerie géospatiale** : Utilisation de photographies aériennes, d'images satellites, et d'autres sources visuelles pour obtenir des informations sur la géographie.

**Données géospatiales** : Cartes, données topographiques, données de terrain, etc.

**Analyse géospatiale** : Processus d'interprétation des données géospatiales pour obtenir des renseignements utiles.

**Systèmes d'information géographique (SIG)** : Outils informatiques pour stocker, analyser et visualiser des données géospatiales.

#### Imagerie géospatiale :

##### 1. Sources d'imagerie :

Satellites : Offrent une vue globale et une capacité de surveillance continue.

Drones : Utiles pour des zones spécifiques et des missions ciblées.

Avions : Utilisés pour des missions spéciales et des régions inaccessibles par satellite.

##### 2. Interprétation d'images :

Identification d'objets, d'installations, de mouvements, etc. Utilisation de la photo-interprétation pour extraire des renseignements.

**3. Objectif du GEOINT** : Fournir des informations critiques pour soutenir la prise de décision dans des domaines tels que la sécurité nationale, la défense, la gestion des catastrophes, etc.

#### Données géospatiales :

**1. Cartographie et SIG** : Utilisation de cartes pour visualiser des données géospatiales. Les SIG permettent de combiner, analyser et visualiser des données pour en tirer des renseignements.

**2. Données topographiques** : Informations sur la forme de la terre, l'élévation, les cours d'eau, etc.

#### Analyse géospatiale :

- 1. Analyse du terrain** : Étude des caractéristiques physiques de la terre pour comprendre leur impact sur les opérations.
- 2. Analyse des déplacements et des tendances** : Suivi des mouvements de troupes, de véhicules, de populations, etc.

#### Applications du GEOINT :

- 1. Sécurité nationale et défense** : Surveillance des activités militaires adverses. Identification de sites stratégiques.
- 2. Gestion des catastrophes** : Évaluation des dommages après des événements tels que des ouragans, des tremblements de terre, etc. Planification des opérations de secours.
- 3. Analyse du renseignement** : Soutien aux opérations de renseignement en intégrant des données géospatiales dans l'analyse traditionnelle.

**Conclusion** : Le GEOINT est une discipline en constante évolution, tirant parti des technologies modernes pour fournir des renseignements cruciaux. En intégrant les aspects géographiques aux analyses traditionnelles, le GEOINT offre une perspective plus complète pour soutenir la prise de décision dans divers domaines.

### Challenge Cours GEOINT

Le 13/06/2023 un des plus gros braquages de l'histoire du casino de gujan à eu lieu ! Effectivement un jeune étudiant gujanais gagne 2 Millions d'euros.

Juste après sa victoire, il décide de prendre sa voiture et d'aller s'acheter un Jet privé à l'aérodrome le plus proche.

Pouvez-vous me dire combien de voitures de couleur claires étaient présentes sur le parking du casino ce jour-là ?

Quel est le nom de l'aérodrome ? ainsi que la distance qui sépare notre jeune millionnaire de son futur Jet (kilomètre près).

### Résolution du Challenge

Après une recherche google pour trouver un site pour remonter dans le temps sur les images satellites, on tombe sur le site <https://livingatlas.arcgis.com/wayback/> qui retrace tout l'historique des images satellites. Il suffit maintenant d'entrer l'adresse du casino de Gujan-Mestras et de

remonter à la date voulu donc le 13/06/2023. On tombe sur le parking du casino avec un total de 13 voitures claires.



Pour la deuxième partie du challenge il suffit de localiser l'aérodrome le plus proche du Casino de Gujan et de faire un itinéraire jusqu'à celui-ci :

aérodrome

Arcachon – La Teste-de-Buch Airport  
4.7 ★★★★★ (170) ⓘ  
Airport · Aérodrome Arcachon

Aero Club of Arcachon  
4.7 ★★★★★ (216) ⓘ  
Aeroclub · Av. de l'Aérodrome  
Open · Closes 12:30PM · Reopens  
1:30 PM · 05 56 54 72 88

ULM Evasion  
4.9 ★★★★★ (176) ⓘ  
Aeroclub · Aérodrome de  
Open · Closes 12:30PM · Reopens  
4:30 PM · 06 78 40 32 43

AÉRODROME ARCACHON VILLEMARIE  
33260 LA TESTE DE BUCH  
5.0 ★★★★★ (1) ⓘ  
Airport

ULM IZI-FLY Arcachon  
4.9 ★★★★★ (98) ⓘ  
Aeroclub · Av. de l'Aérodrome  
Closes soon · 12 PM · Reopens  
2PM · 06 88 73 98 71

Arcachon

AÉRODROME ARCACHON VILLEMARIE 33260 LA TESTE DE BUCH

5.0 ★★★★★ (1) ⓘ  
Airport

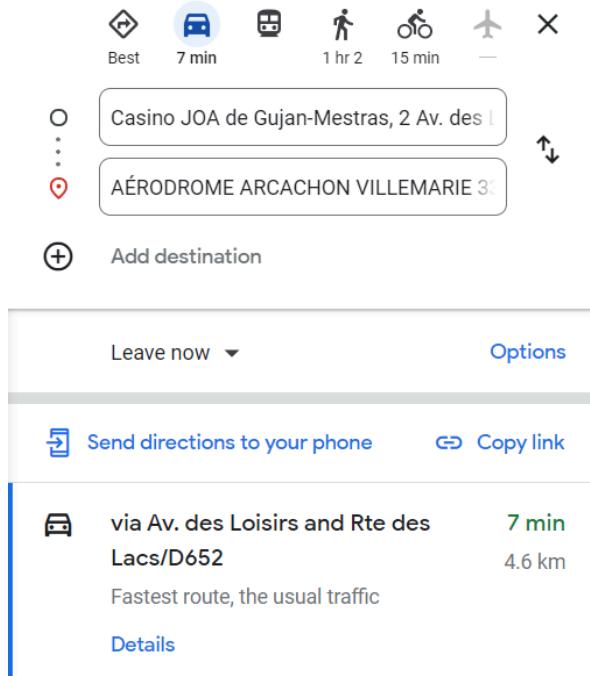
Overview    Reviews    About

Directions    Save    Send to phone    Share

33260 La Teste-de-Buch

HVXP+2H La Teste-de-Buch

On trouve le nom de l'aérodrome "villemarie"



On sait maintenant qu'il y a 4,6 km en voiture pour faire du Casino Gujan à l'aérodrome, on arrondit à 4 pour le Flag.

Flag : 13\_villemarie\_4\_geoint

## IMINT

L'intelligence par imagerie (Imagery Intelligence ou IMINT) est un type de collecte de renseignements qui se concentre sur l'acquisition d'images d'activités humaines ou d'objets depuis l'espace dans le but de les identifier et de les analyser. L'IMINT peut être utilisé à diverses fins, y compris l'armée, l'application de la loi et la collecte de renseignements.

Il existe plusieurs méthodes de collecte d'IMINT, notamment les satellites, les drones, les avions et les plates-formes au sol telles que les caméras et les jumelles. Les images collectées peuvent être utilisées pour générer des cartes, détecter des cibles et suivre des mouvements. IMINT peut également être utilisé pour recueillir des informations sur les intentions ou les capacités d'un adversaire.

Bien qu'IMINT soit un outil puissant, il a certaines limites. Premièrement, la qualité des images collectées dépend de la plateforme utilisée et des conditions météorologiques au moment de la collecte. Deuxièmement, les analystes doivent être formés pour interpréter correctement les images. La résolution d'image peut être un défi, en particulier lorsque vous essayez d'identifier de petites cibles à de grandes distances.

## Exemple concret :

### Les métas données :

Les métadonnées sont des données qui décrivent d'autres données. Elles fournissent des informations contextuelles sur les données principales, telles que leur origine, leur format, leur taille, leur structure, leur propriétaire, leur date de création, etc.

Par exemple, si une photo numérique est considérée comme une donnée principale, ses métadonnées pourraient inclure des informations telles que la date et l'heure de la prise de vue, le modèle de l'appareil photo utilisé, les paramètres de l'appareil photo tels que l'ouverture et la vitesse d'obturation, les coordonnées GPS de l'endroit où la photo a été prise, etc.

Les métadonnées sont essentielles pour organiser, rechercher et comprendre les données principales. Elles sont largement utilisées dans les systèmes d'information, les bases de données, les bibliothèques numériques, les systèmes de gestion de contenu, etc.

Résumé des informations que l'on cherche en général dans les métas données :

- Les données géographiques (GPS, lieu, ...)
- Le modèle d'appareil photo
- Les données techniques de l'image (taille, format, résolution.)
- Les paramètres de configuration de l'appareil (objectif utilisé, focale, ouverture, ...)
- Le crédit photo (titre, auteur, ...)
- Les données temporelles (date et heure)

Les images sont l'un des points d'entrée et de pivot les plus courants dans les recherches OSINT. Il est fréquemment utile d'être capable d'identifier où une photo a été prise, ou ce qui est représenté dessus.

Outils utiles : jimpl, exiftool, Aperi'solv

### La recherche d'image inversée :

Une recherche d'image inversée vous permet de prendre une image et de trouver l'endroit où elle a été publiée à l'origine, d'autres pages qui ont publié la même image, différentes tailles de la même image et des images similaires. En quelques cliques vous pourrez donc retrouver dans quel pays se trouve le bâtiment que vous trouvez incroyable ou encore à quel pays appartient le drapeau que vous avez en face de vous.

Avec Google Lens :

Prenons l'image suivante :



Vous cherchez à avoir plus d'informations sur ce bâtiment ? Rendez-vous sur google :



Et copier ensuite votre image ici :



Rechercher une image avec Google Lens

X



Faites glisser une image ici ou  
[importe un fichier](#)

OU

Coller le lien de l'image

Rechercher

Et vous obtenez le résultat suivant :

The screenshot shows the Google Lens interface. On the left, there is a large image of the Burj Khalifa at night. Below it are three buttons: "Rechercher", "Texte", and "Traduction". To the right, the search results for "Burj Khalifa" are displayed. At the top, there is a card for the building itself, showing a rating of 4.7 stars and the text "Lieu remarquable". Below this are several other images of the tower and its surroundings. Further down, there are links to purchase posters from eBay and Mob.org, along with a link to Printler. At the bottom, there is a poll asking if the results were useful, with "Oui" and "Non" options.

Vous savez maintenant qu'il s'agit du Burj Khalifa MAIS votre soif de savoir veux plus d'informations.  
Vous pouvez donc cliquer ici :

[Voir la source de l'image](#)

Et vous pourrez retrouver toutes les références où la photo a été utilisée :

Le floutage SafeSearch est activé



Cinq méga-chantiers qui vont changer la planète - Edition du soir Ouest-France - 04/09/2018

4 sept. 2018 · 360x630



Les plus hauts bâtiments 10 du monde

30 juin 2023 · 700x1225



La tour la plus haute du monde - Records du monde

7 janv. 2019 · 170x297



Les plus hauts immeubles du monde | Ultimes : rare, étrange, extrême...

2 oct. 2015 · 450x788



Des gratte-ciels de plus en plus hauts : la démesure des constructions humaines

14 janv. 2024 · 274x480

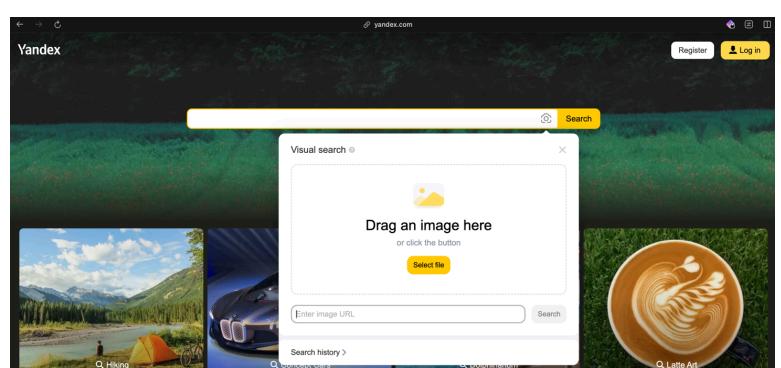
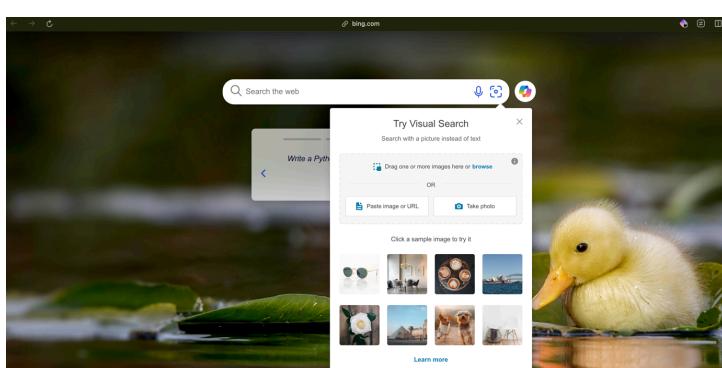


Burj Khalifa Skyscraper Dubai UAE Photo Poster Art Print - PICK SIZE | eBay

229x400



La recherche d'image inversée est en général la première étape de l'IMINT, mais attention, si Google ne vous donne pas de résultat cela ne veut pas dire qu'il n'y en a pas mais seulement qu'il n'en existe pas sur google. Pour maximiser vos chances de trouver des informations, il est conseillé de faire des recherches supplémentaires en utilisant d'autres moteurs de recherches comme Yandex ou Bing.



## Challenge Cours IMINT

D'après une source sûre, un nouveau groupe de hacker nommé Kheops doit se donner rendez-vous en soirée la semaine prochaine. La seule information que vous avez, est ce gif intercepté par votre source. Il vous demande de l'aide grâce à vos talents d'OSINT pour retrouver le lieu du rendez-vous.

Vous donnerez le nom du lieu ainsi que son adresse et le type principale d'OSINT utilisé

Voici un extrait du gif du challenge, le gif du challenge se trouve dans les ressources en annexe.

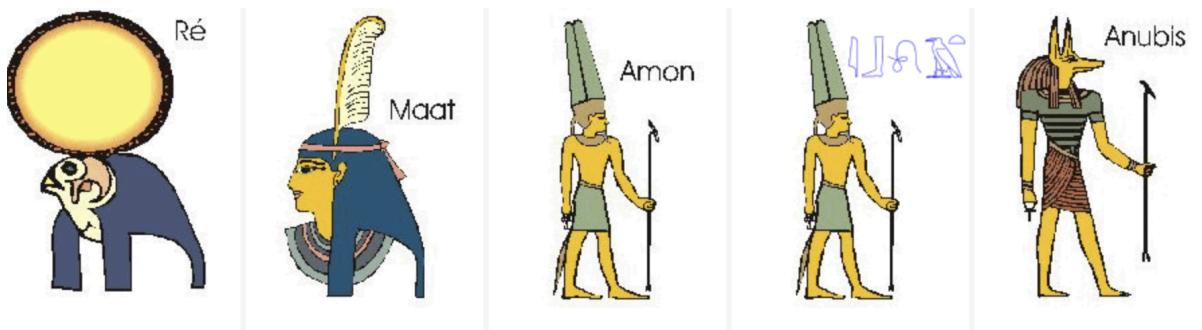


## Résolution du Challenge

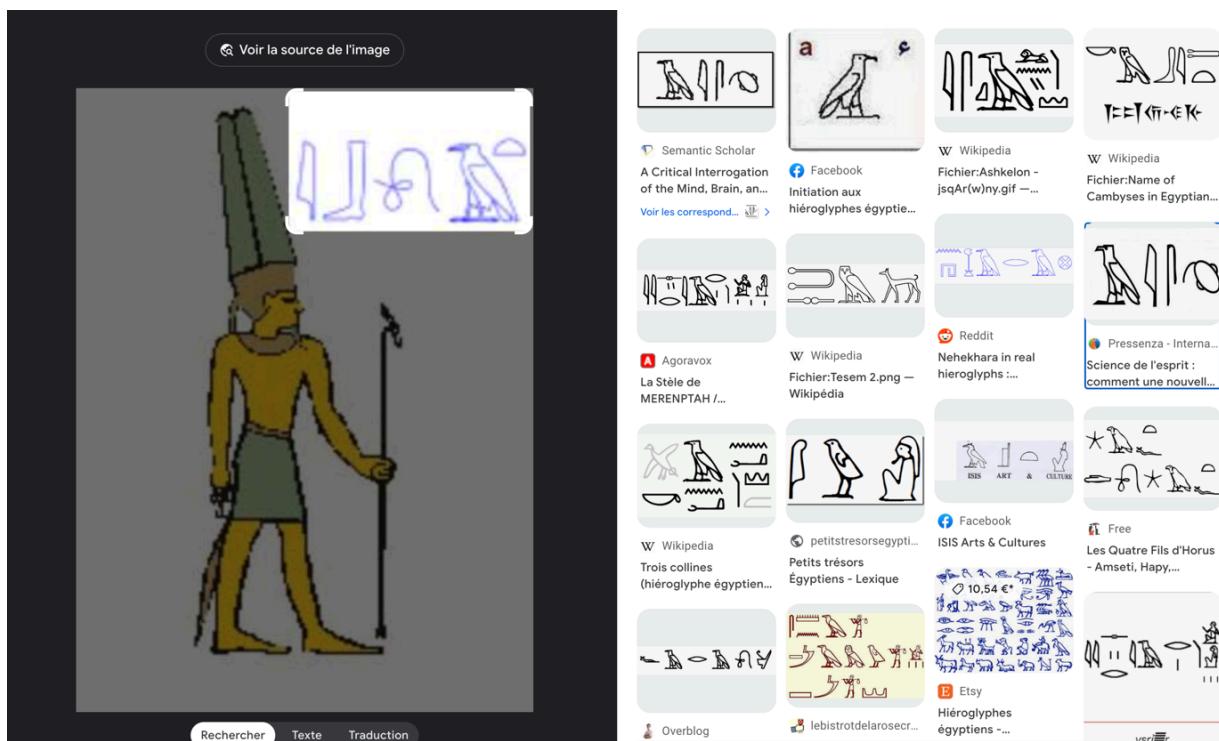
### Résolution – Partie 1 :

La première chose à remarquer sur le gif est que des écritures différentes des noms des dieux égyptiens apparaissent très rapidement. Il faut alors essayer de décomposer le gif avec un outil trouvé sur un internet.

Nous obtenons donc :



Nos doutes sont bien fondés, une image à l'air d'avoir des hiéroglyphes à la place du nom du dieu. Faisons une petite recherche d'image inversée pour confirmer cela.



Prenons le premier lien :



Figure 1. The ancient Egyptian hieroglyph for brain as shown in the Edwin Smith papyrus. Source: <https://commons.wikimedia.org/wiki/File:Hieroglyphic-brain.jpg>

Nous avons plus ou moins la confirmation qu'il s'agit bien de ça, maintenant, il faut tester !

Il faut maintenant trouver un site pour déchiffrer ce texte, après une recherche rapide, nous trouvons celui-ci :

[http://www.apprendre-en-maternelles.com/Exercices/decode\\_hieroglyphes.php](http://www.apprendre-en-maternelles.com/Exercices/decode_hieroglyphes.php)

Nous trouvons donc le texte suivant : iboat

Qu'est-ce que Iboat ?

Faisons une recherche sur google.

**IBOAT**  
https://www.iboat.eu :

#### IBOAT: Welcome On Board

Concerts, Clubs, Cantine sur les flots, ...

#### L'Agenda

Concerts, clubs, marchés, ateliers jeune public, ... Découvrez tous ...

#### Agenda

Concerts, clubs, markets, children's and teens' workshops, etc ...

#### Infos Pratiques

BASSIN A FLOT N°1. COURS HENRI BRUNET 33300 ...

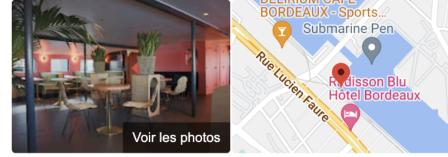
#### La Plage de l'iBoat

Pour les affamés. Dès midi, nos cuisines se mettent en route ...

#### Le Bateau

IBOAT, OPERATEUR CULTUREL INDEPENDANT DEPUIS 2011 ...

[Autres résultats sur iboat.eu »](#)



#### IBOAT

3,8 ★★★★☆ 2423 avis ⓘ

€€ · Bar

[Site Web](#)

[Itinéraire](#)

[Enregistrer](#)

Poissons et fruits de mer dans un restaurant insolite au décor élégant situé dans un ferry, avec salle de concert et discothèque.

**Services disponibles:** Propose d'excellents cocktails · Propose des concerts · Dispose d'un cabaret

**Adresse :** Bassin à Flot n°, 1 Cr Henri Brunet, 33300 Bordeaux

Il s'agit d'un restaurant, parfait pour un lieu de rendez-vous.

La première partie de flag est trouvé, il s'agit de **iboat**

#### Résolution – Partie 2 :

Il ne nous manque plus qu'à trouver l'adresse.

**Adresse :** Bassin à Flot n°, 1 Cr Henri Brunet, 33300 Bordeaux

Nous avons donc notre deuxième partie de flag **1-cr-henri-brunet**

#### Résolution – Partie 3 :

La partie la plus simple, ce challenge répondait au cours sur l'IMINT, il fallait donc mettre en troisième partie de flag **imint**

Flag : iboat\_1-cr-henri-brunet\_imint

## SOCMINT

Le Social Media Intelligence (Socmint) est une pratique de collecte, d'analyse et d'utilisation de données issues des médias sociaux pour obtenir des insights, comprendre les tendances, les comportements, les opinions et même détecter des menaces potentielles. Cette méthode a des applications variées dans différents domaines tels que la sécurité, le renseignement, le marketing, la gestion de crise, et bien plus encore.

## Collecte de données

La première étape du Socmint consiste à collecter des données à partir des plateformes de médias sociaux telles que Twitter, Facebook, Instagram, LinkedIn, Reddit, etc. Cette collecte peut être effectuée à l'aide d'outils spécifiques, de crawlers web ou d'APIs offertes par ces plateformes. Les données collectées incluent les messages, les publications, les commentaires, les images, les vidéos, les profils utilisateurs, etc.

## Analyse des données

Une fois les données collectées, elles sont analysées pour extraire des informations pertinentes. Cela implique l'utilisation de techniques telles que l'analyse de sentiment pour comprendre les opinions générales, l'analyse de réseau pour identifier les relations entre les utilisateurs et les tendances, l'extraction de motifs pour repérer des comportements spécifiques, et d'autres méthodes d'analyse statistique et qualitative.

## Utilisation des insights

Les informations et les insights obtenus à partir de l'analyse des données sont utilisés dans divers domaines. Dans la sécurité et le renseignement, le Socmint peut être utilisé pour détecter des menaces émergentes, surveiller les activités suspectes, ou identifier des réseaux criminels. Dans le marketing, il peut aider à comprendre les besoins des consommateurs, évaluer les campagnes et mesurer la réception des produits ou services. En gestion de crise, il permet de surveiller l'évolution des opinions et de réagir rapidement à des problèmes émergents.

## Outils et technologies

Le Socmint utilise une variété d'outils et de technologies pour collecter, analyser et visualiser les données des médias sociaux. Ces outils peuvent inclure des plateformes d'analyse sociale, des logiciels de surveillance en temps réel, des tableaux de bord de veille stratégique, des applications d'analyse de sentiments et bien plus encore. Ces technologies évoluent constamment pour s'adapter aux changements des plateformes de médias sociaux et pour offrir des fonctionnalités plus avancées.

## Défis et considérations éthiques

Le Socmint soulève également des défis éthiques tels que la protection de la vie privée, la manipulation des données, la véracité des informations et l'utilisation responsable des données collectées. Il est crucial de respecter les règlements et les lois en vigueur concernant la collecte et l'utilisation des données des utilisateurs.

## Challenge Socmint

“Vous avez été mandaté par le bureau d'enquête national afin de retrouver le profil d'une personne ayant divulgué des informations importantes et confidentielles sur l'entreprise FoxHound Business.

Vous n'êtes pas seul, et avons pour vous rassembler un minimum d'éléments pour vous aider dans votre recherche d'OSINT :

Son prénom et nom : Raina Lussier. “

Retrouvez l'ID de transaction et donnez-nous le nom de la personne qu'elle mentionne sur un de ces posts. Cette personne peut être liée. Donnez-nous également le nom de l'article quelle a publié sur le net .

Tips: Il faudra parfois créer des comptes pour avoir certaines réponses !

Format du flag: 0x\_jeanne\_famillesoint

## Résolution du Challenge

On commence par rechercher le nom complet sur google et on finit par trouver un des articles sur Medium.

<https://medium.com/@raina.lussier.pro/la-mode-au-coeur-des-chooses-c8b6927ca568>

En utilisant “whatsmyname” on remarque également un compte twitter :

Raina Lussier @RaiLussier · 3h  
La mode est plus qu'une passion c'est un mode de vie !

medium.com  
La Mode au coeur des choses  
La mode transcende bien plus que des vêtements et des tendances éphémères. Elle est un langage ...

En inspectant les différents articles on s'aperçoit d'une URL suspecte :



<https://www.buymeacoffee.com/aHR0cHMIM0EIMkYIMkZtYXN0b2RvbUYRXNvY2IhbCUyRmhvbWU=>

Cela ne ressemble pas à un lien standard et celui-ci semble encoder, on utilise “cyberchef” afin de savoir si nous sommes proche de la vérité

En décodant le lien, nous obtenons une informations importante , un lien vers un compte mastodons:

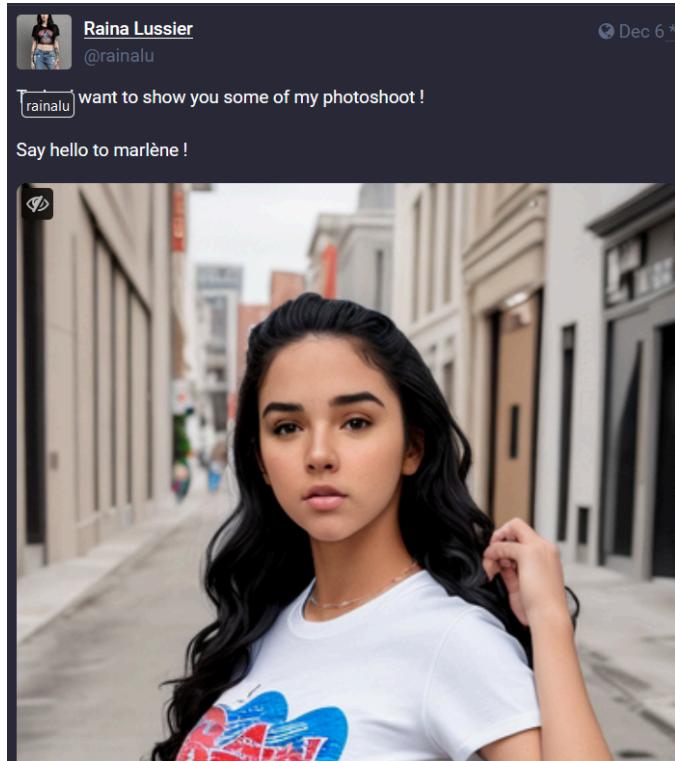
<https://mastodon.social/home>

En effectuant quelque recherche de profil en utilisant le nom données on trouve le compte :

A dark grey rectangular card representing a Mastodon profile. In the top left corner is a small square thumbnail image of a woman with long dark hair, wearing a black t-shirt with a red graphic and blue jeans. To the right of the thumbnail, the name "Raina Lussier" is displayed in white bold text. Below the name, the handle "@rainalu" is shown in white, followed by a blue button-like icon containing the text "mastodon.social".

On nous demande

“Retrouvez l'ID de transaction et donnez-nous le nom de la personne qu'elle mentionne sur un de ces posts. Cette personne peut être liée. Donnez-nous également le nom de l'article quelle a publié sur le net . ”



Sur le 1er post nous récupérons le nom de la jeune fille !

I can't stand this company anymore, between the corruption and the things left unsaid... I would never have thought that of them!

Fortunately I have what it takes to blackmail them

Here is the link to a cryptocurrency transaction that proves corruption within this company!

0x1fc35B79FB11Ea7D4532dA128DfA9Db573C51b09

Sur le second post l'ID de transaction !

L'entreprise FoxHound Business nous remercie pour nos services !

Flag Final : **0x1fc35B79FB11Ea7D4532dA128DfA9Db573C51b09\_marlene\_socmint**

**Happy Osint !**