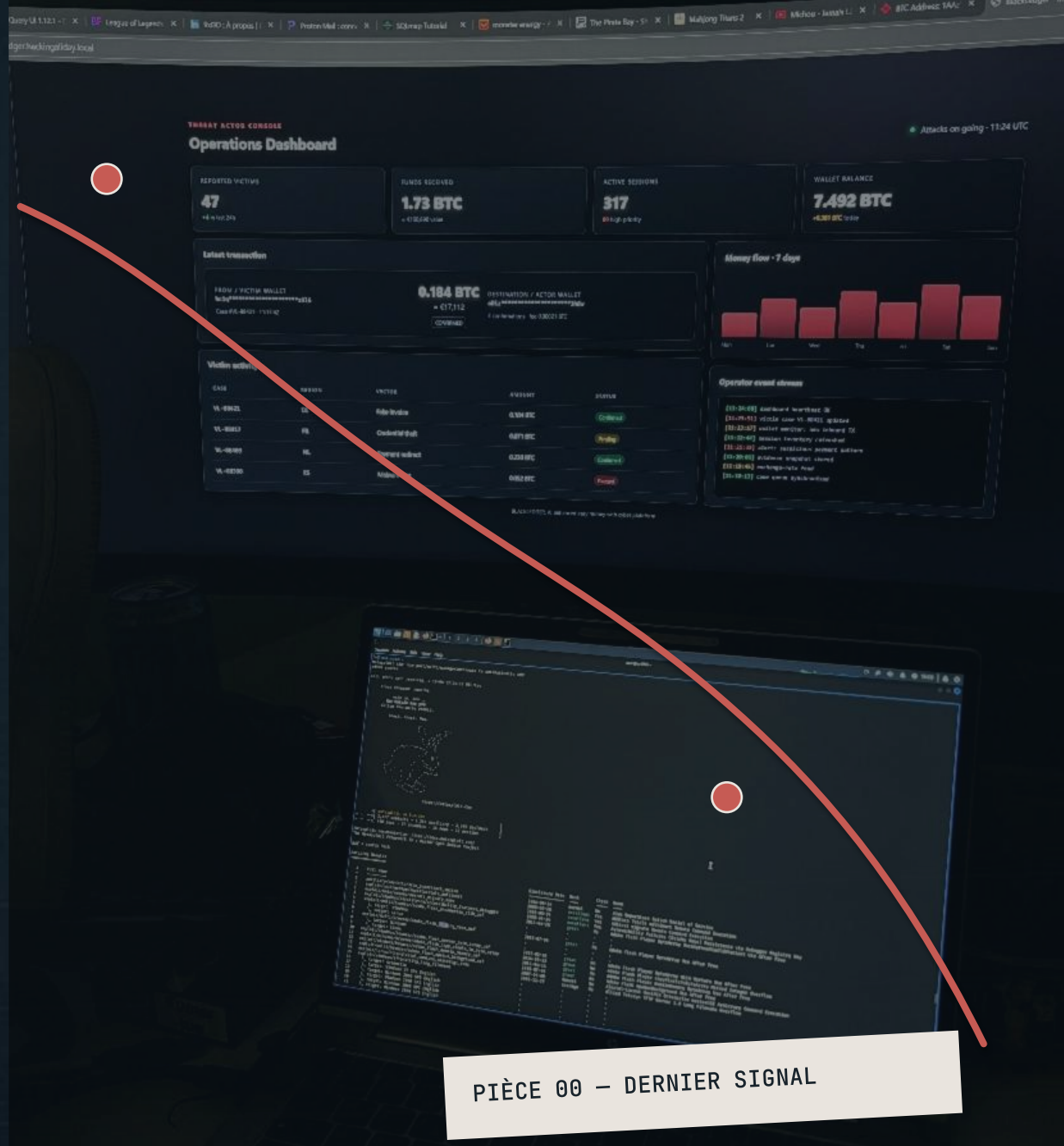
RESILIENCE

CHALLENGE OSINT · WRITE-UP OFFICIEL

# AFFAIRE UISIE

De deux captures
à une adresse.

DOSSIER / INVESTIGATION NUMÉRIQUE




Scénario fictif · Challenge réalisé par Résilience
Créé par Abicom / Résilience, hébergé par Cloudéo.

# Deux pièces. Aucun nom.




PIÈCE A · Le poste de travail d'un membre présumé




PIÈCE B · Messagerie interceptée

## QUI SE CACHE DERRIÈRE ?

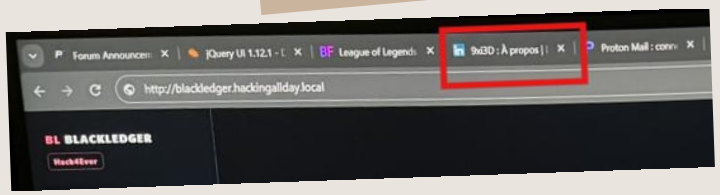
Identifier le groupe

Suivre les pivots

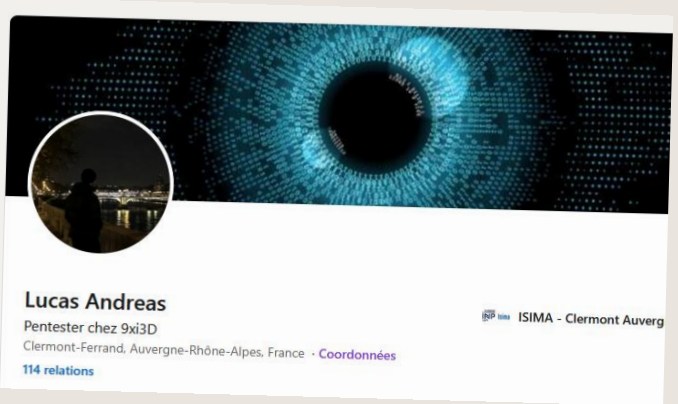
Localiser la personne à la tête

**MÉTHODE** · Chaque capture fournit un indice, qui est ensuite recoupé sur une autre source publique.

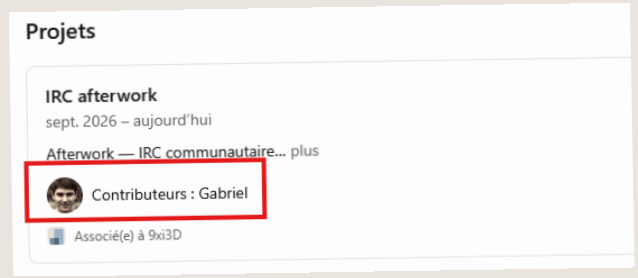
# Un onglet LinkedIn révèle une première identité




Onglet « 9xi3d » dans les onglets du membre




Recherche sur Linkedin et découverte de Lucas Andreas « Pentester chez 9xi3D »

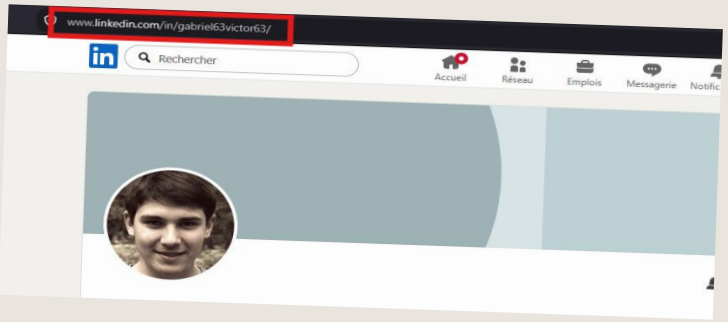



Un projet de Lucas, avec un contributeur : « Gabriel »

PIVOT D'IDENTITÉ

## gabriel63victor63

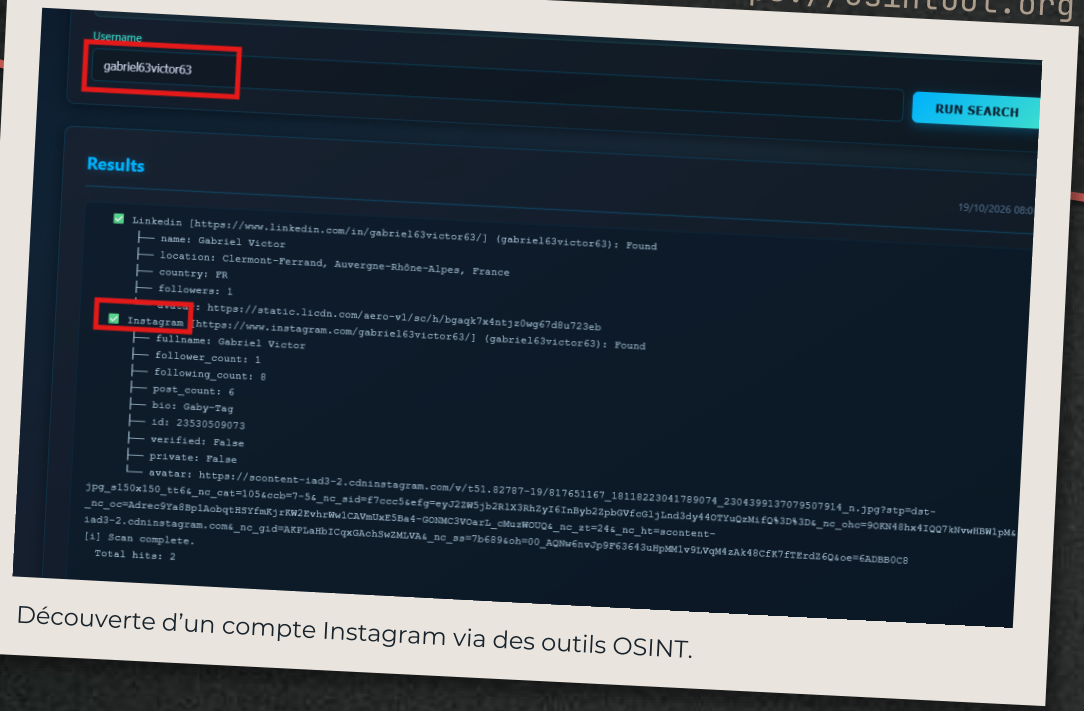
Le pseudo devient la clé de recherche multi-plateformes.



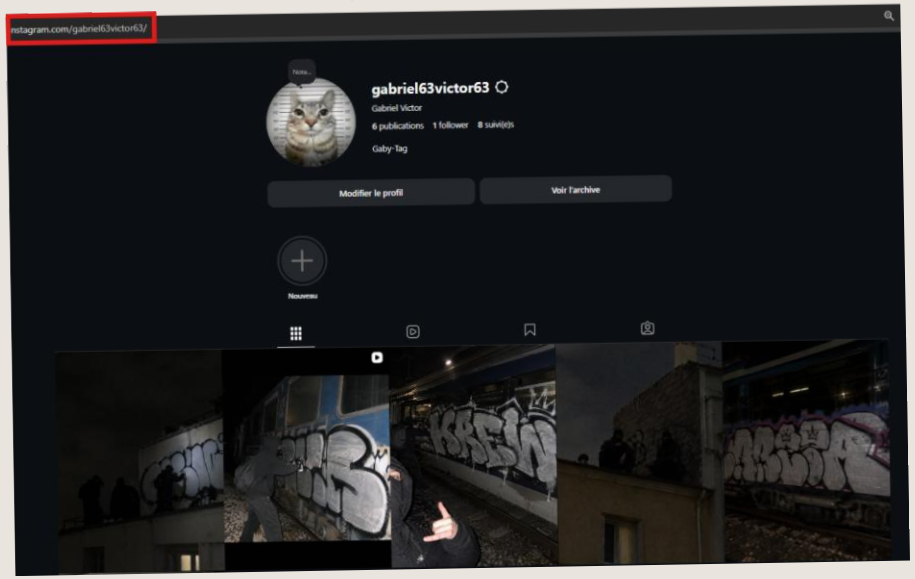

L'URL personnalisée livre le pseudo de Gabriel.

# Rejeu et pivot de réseau social

https://osintool.org



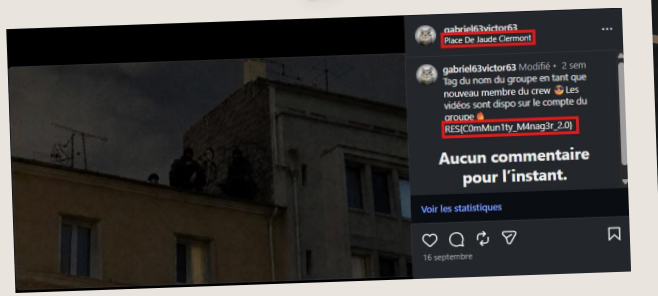

Découverte d'un compte Instagram via des outils OSINT.



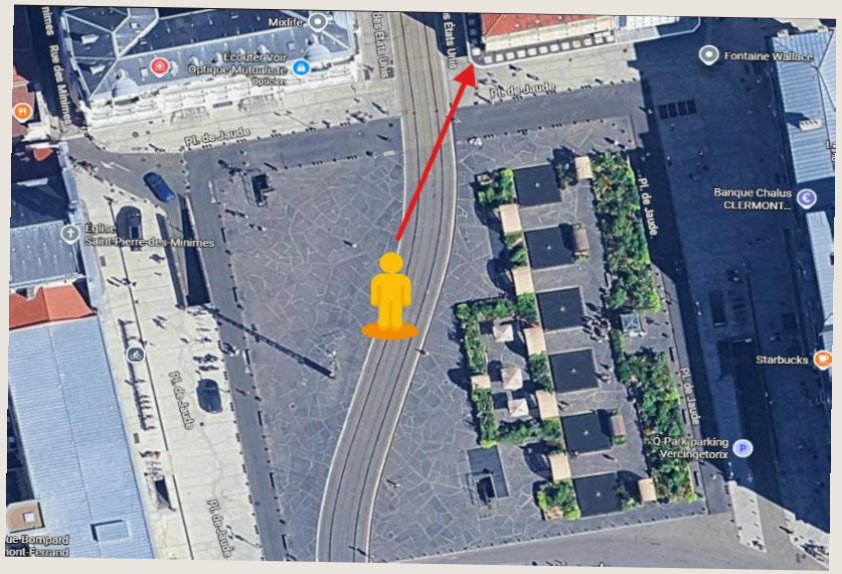

Instagram · Gabriel Victor

→ Compte Instagram avec de multiples publications autour du graffiti.

# Un graffiti confirmant le virtuel avec le réel




Instagram · Post avec localisation
« Place de Jaude Clermont »




Google Maps · l'angle de prise de vue est recoupé en comparant l'image et la vue StreetView



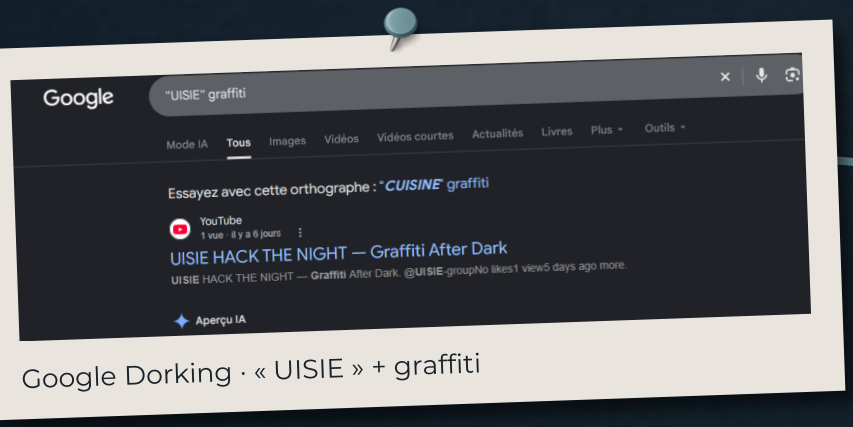
Sur la façade : UISIE

FLAG 01 `RES{C0mMun1ty_M4nag3r_2.0}`

**UISIE**

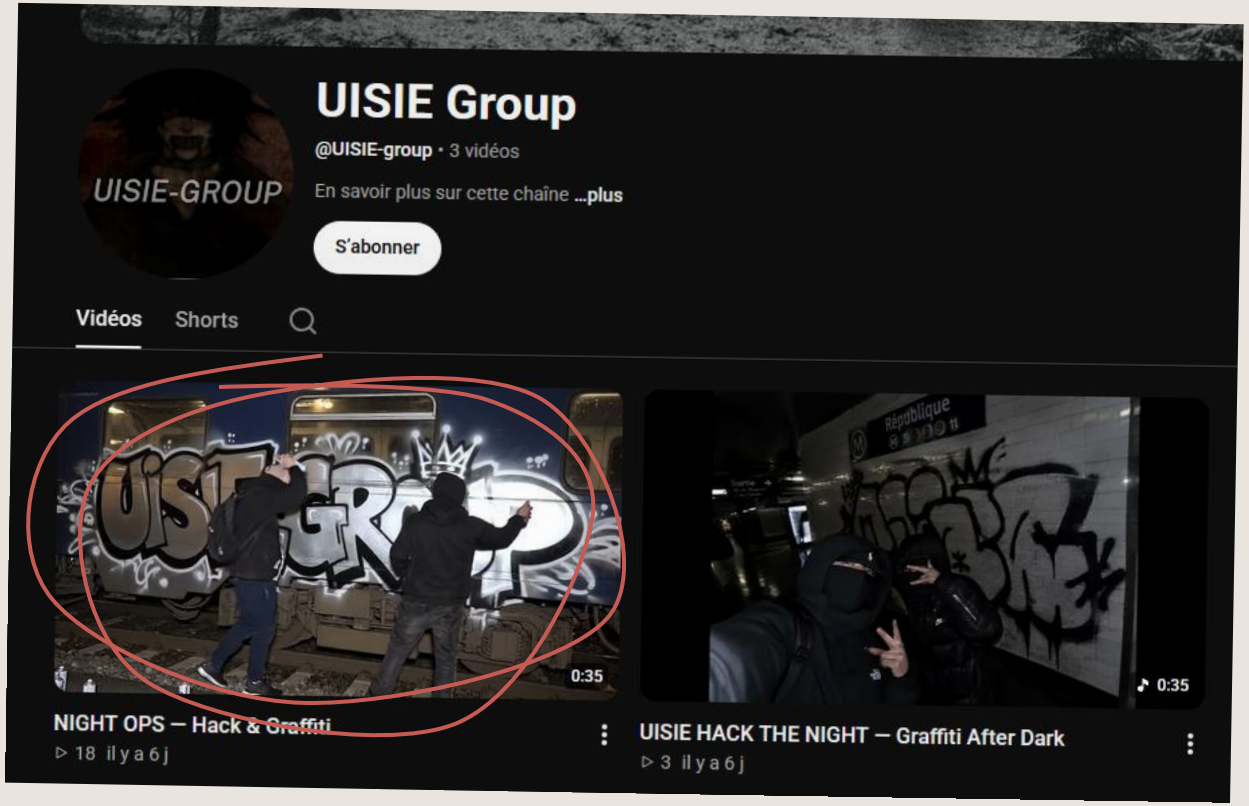
**POURQUOI CE PIVOT ?** Le graffiti donne un nom de groupe, « UISIE », qui devient une requête ciblée pour la suite de l'enquête.

# UISIE laisse une trace vidéo




Google Dorking · « UISIE » + graffiti

La recherche ciblée retrouve la chaîne ; une annotation ouvre ensuite une vidéo non répertoriée.

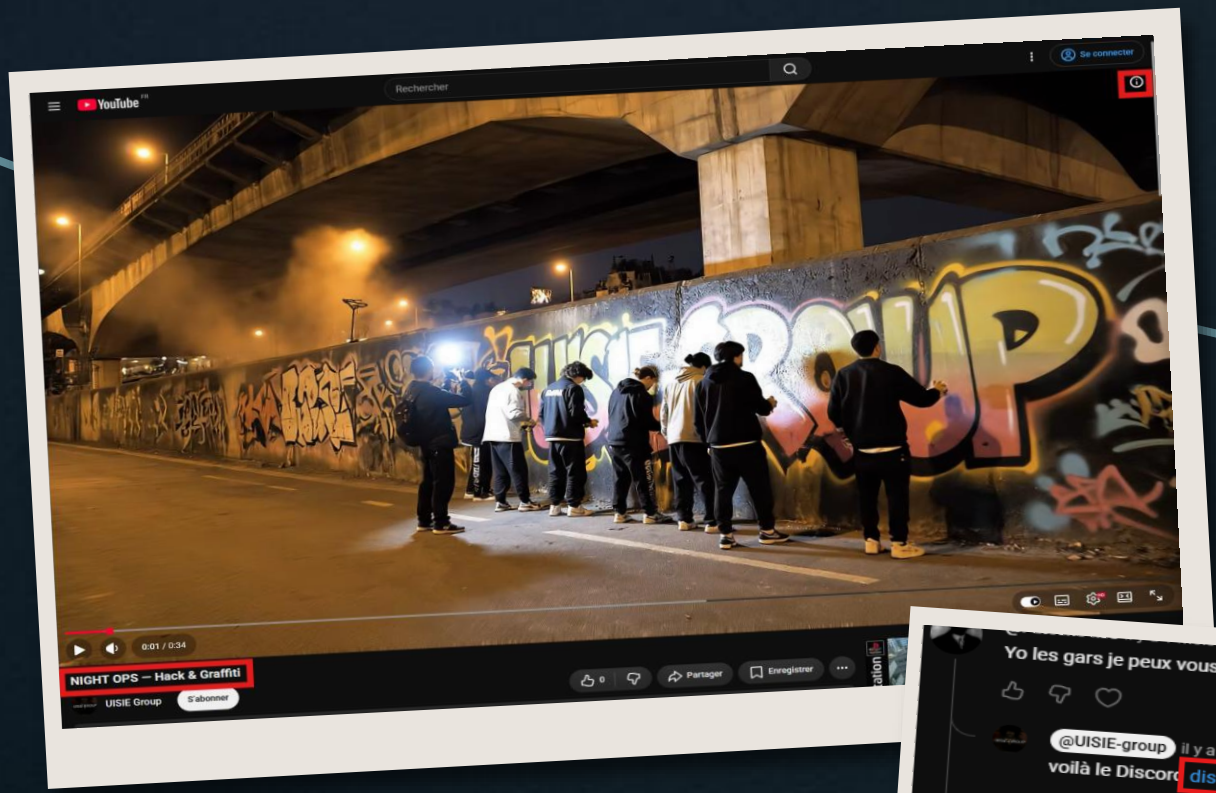



Youtube · Vidéo de hacking & Graffiti

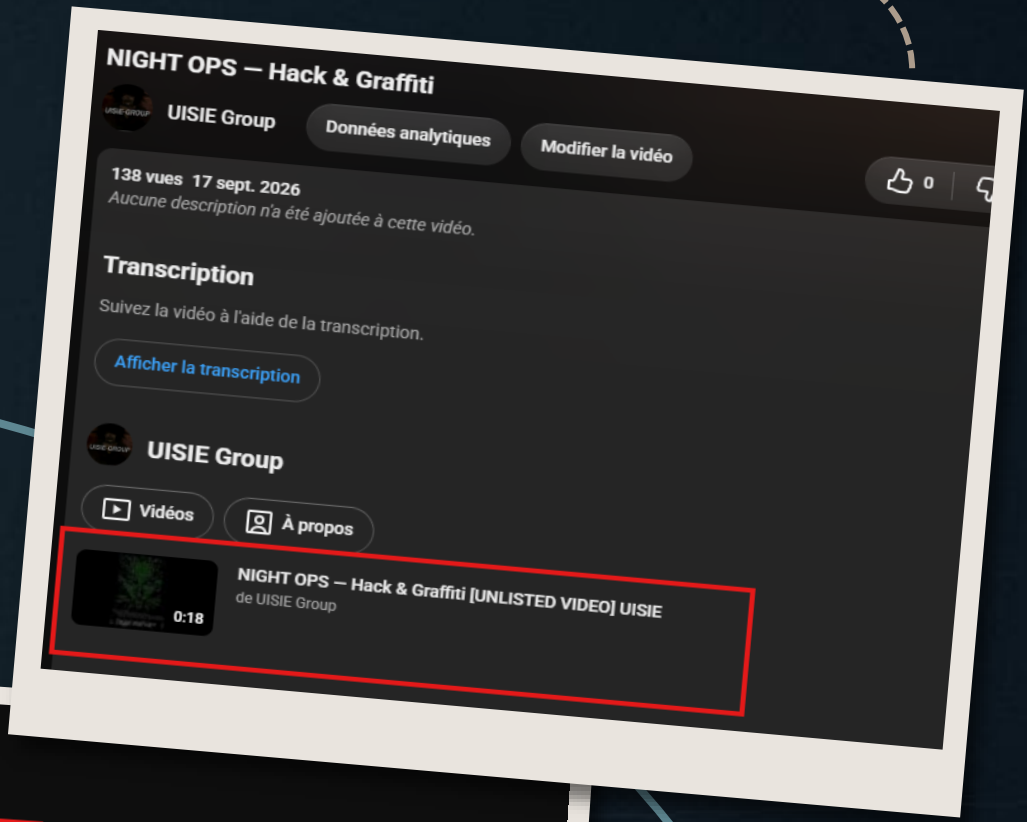
**MÉTHODE** · Avec la mention de « vidéo » sur le compte Instagram, il était également possible de découvrir cette chaine depuis une simple recherche Youtube.

# Vidéo de hacking cachée

Annotation sur la vidéo redirigant vers une vidéo cachée (non répertoriée)




La recherche ciblée retrouve la chaîne ; une annotation ouvre ensuite une vidéo non répertoriée.



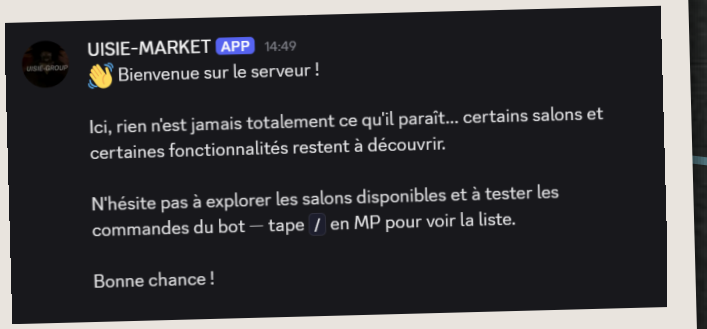




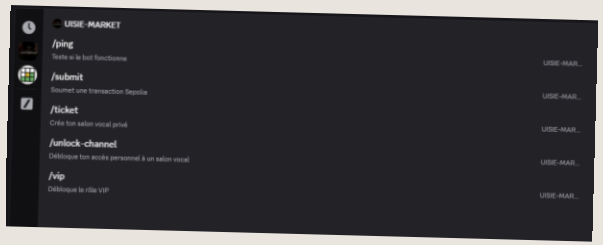
Dans les commentaires : invitation Discord + second flag

FLAG 02 `RES{L3vel_de_St4lker}`

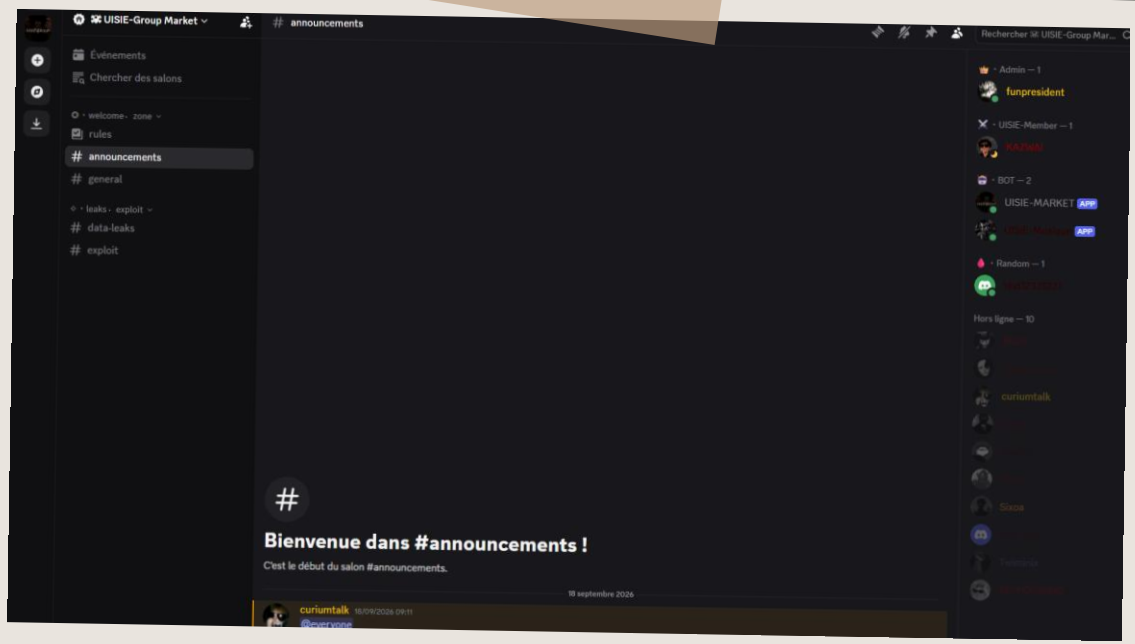
# Le serveur Discord devient le terrain d'enquête




Le bot accueille et invite à tester ses commandes




/ping · /submit · /ticket · /unlock-channel · /vip




Le serveur semble servir de marché aux données divulguées

OBSERVER → INTERROGER LES BOTS → NÉCESSITE PLUS DE RÔLES POUR LES COMMANDES

# Une archive protégée ouvre la voie

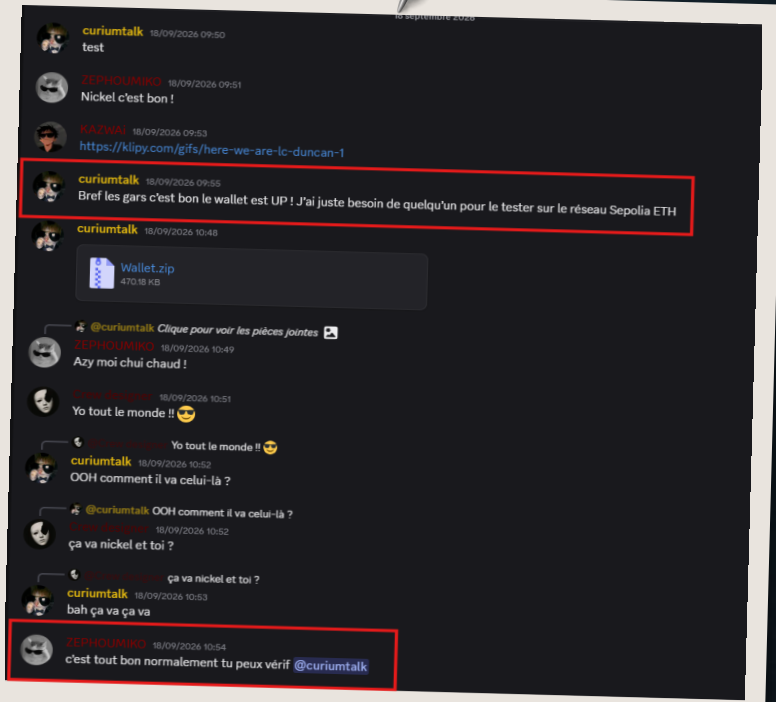
Chemin A

0x3B49B78B273B5db1D3fc4cb283bD617c6C1CBCcD
WALLET MARKET

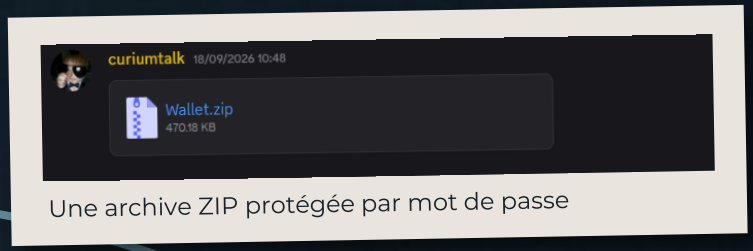



Announcements · l'administrateur publie le wallet crypto du market Discord

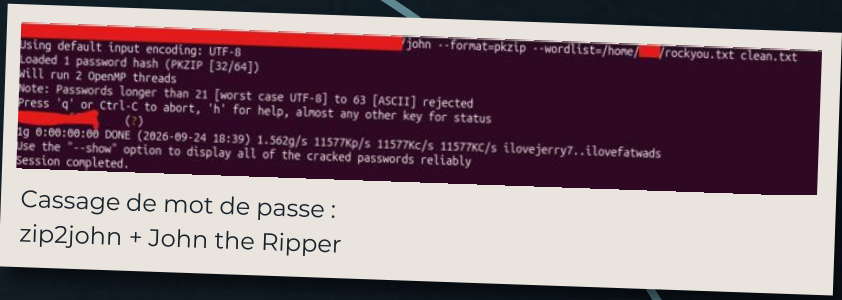
Chemin B




General · un wallet à tester




Une archive ZIP protégée par mot de passe




Cassage de mot de passe :
zip2john + John the Ripper

ZIP → extraction HASH → cassage de MOT DE PASSE → Accès PDF WALLET

*Le PDF explique le transfert Sepolia : le hash obtenu deviendra le justificatif à soumettre au bot.*

*(Slide suivante)*

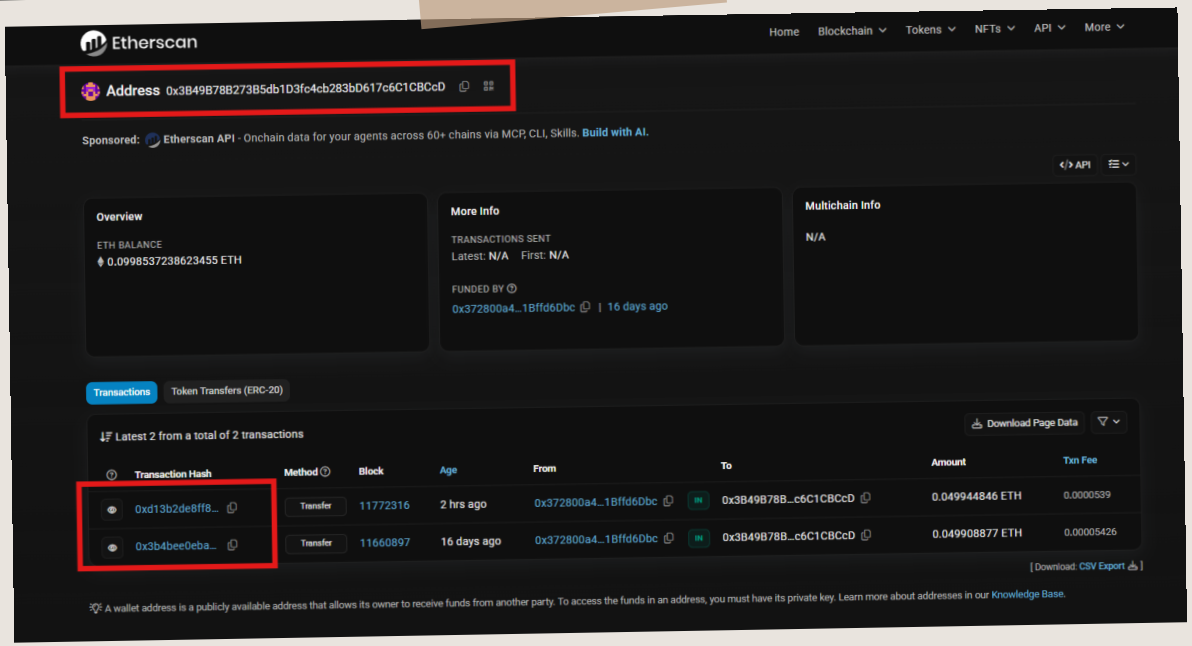
*(Slide suivante)*

Chemin B

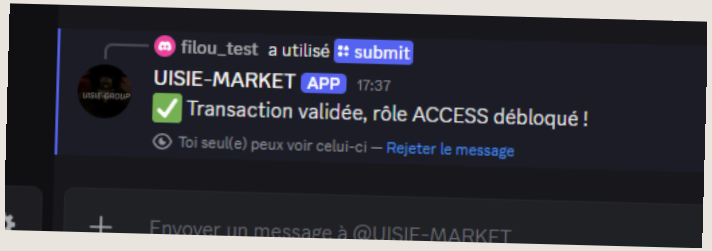
Chemin A

# Une transaction débloque le rôle ACCESS

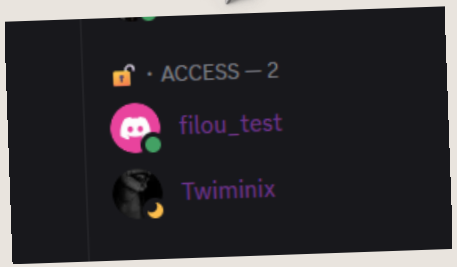
Création d'une transaction avec les instructions du PDF.




Sepolia Etherscan · la transaction fournit son hash publiquement




/submit · transaction validée



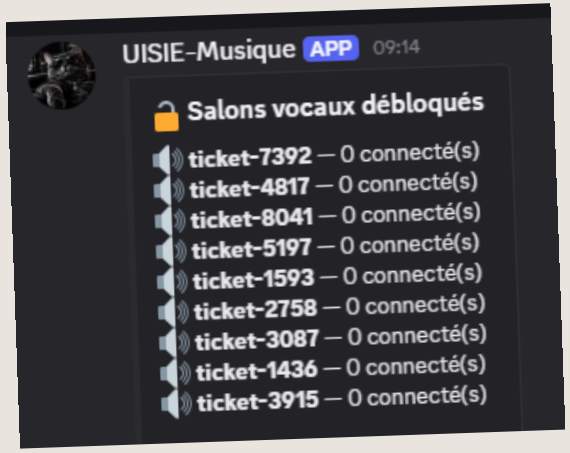

Rôle ACCESS débloqué

Sepolia est un réseau de test Ethereum : les transactions sont publiques et sans valeur réelle.

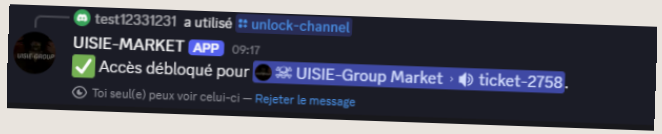
**Le hash récupéré est transmis à /submit ; sa validation ouvre de nouveaux salons et commandes.**

# Le bon ticket révèle un code VIP

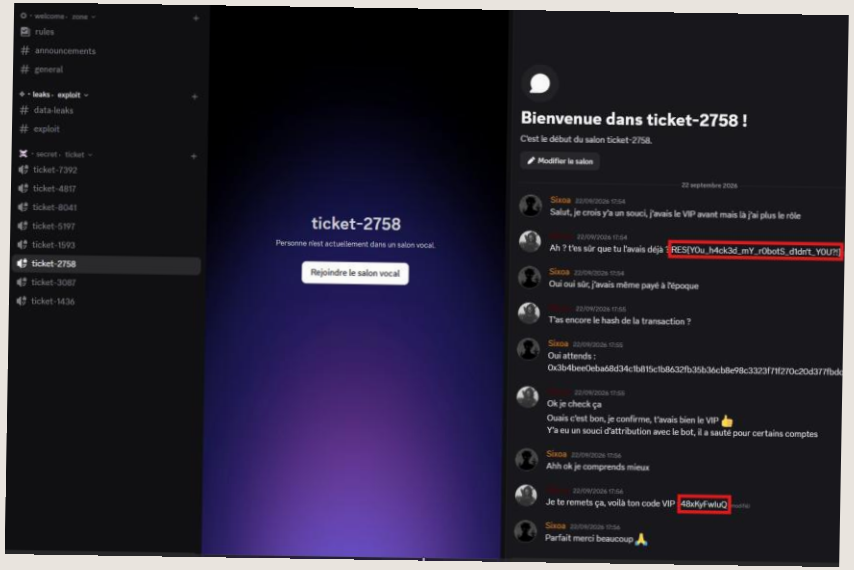
ACCÈS




/show-channels · liste des tickets

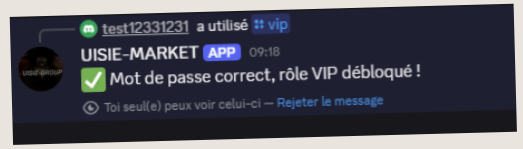



/unlock-channel · ticket-2758

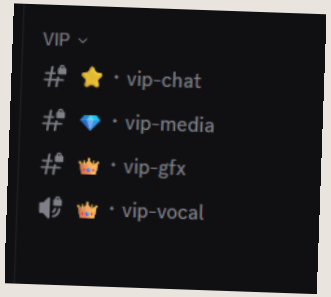



Sixoa × Shuzy · le code VIP est dans l'échange

48xKyFwIuQ



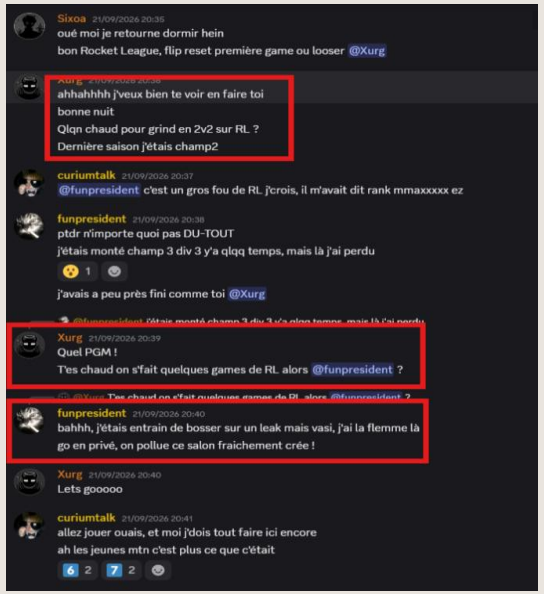

Code validé · rôle VIP



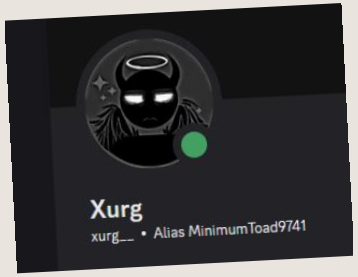

Catégorie VIP ouverte

FLAG 03 `RES{Y0u_h4ck3d_mY_r0botS_d1dn't_Y0U?!}`

# Un alias Rocket League mène à un second pseudonyme

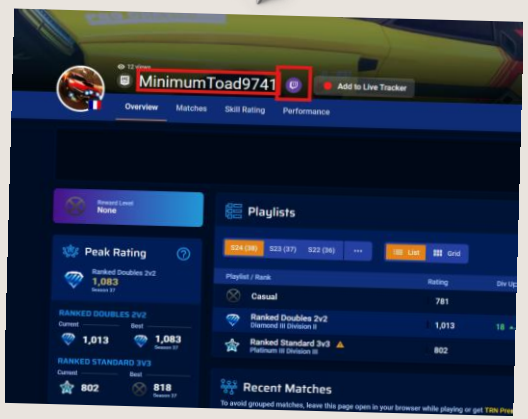



vip-chat · Conversation révélant les intérêts gaming de deux membres

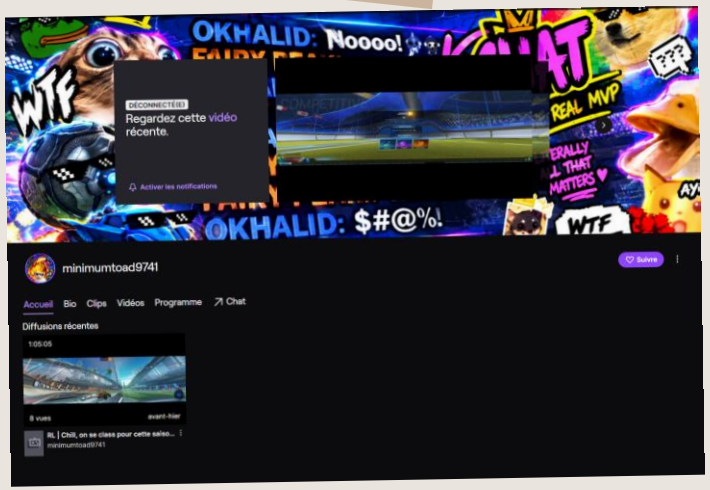



Xurg · membre VIP

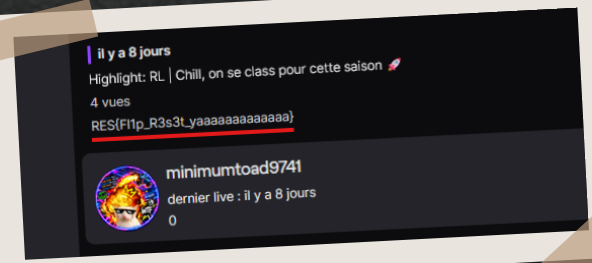
Alias Epic :
**MinimumToad9741**




RL Tracker · un compte Twitch est associé




Twitch · la rediffusion révèle un joueur




FLAG 04

`RES{Fl1p_R3s3t_yaaaaaaaaaaaaa}`




Nouveau pivot : GreyLynx6794

**LIEN AVEC LA SUITE** · GreyLynx6794 est recoupé avec funpresident sur Discord ; son archive oriente ensuite vers Pinterest.

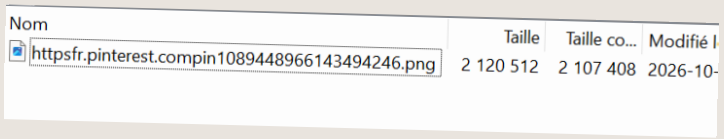
# Le nom d’un fichier reconstitue une publication Pinterest




funpresident × Crew Designer · archive 7z

Mot de passe de l’archive :
GreyLynx6794

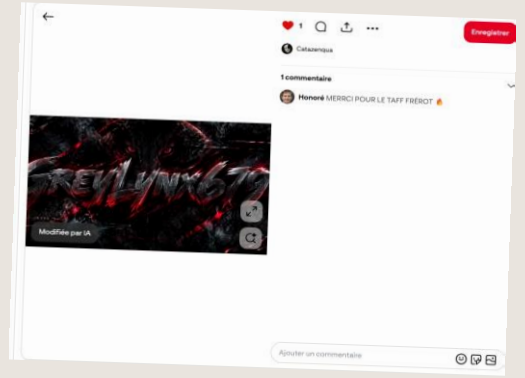
1089448966143494246



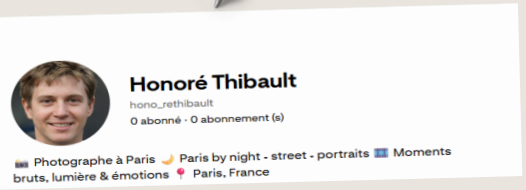

Un nom de fichier au format Pinterest

Reconsitution de l’URL avec un exemple d’autre publication Pinterest

https://fr.pinterest.com/pin/1089448966143494246



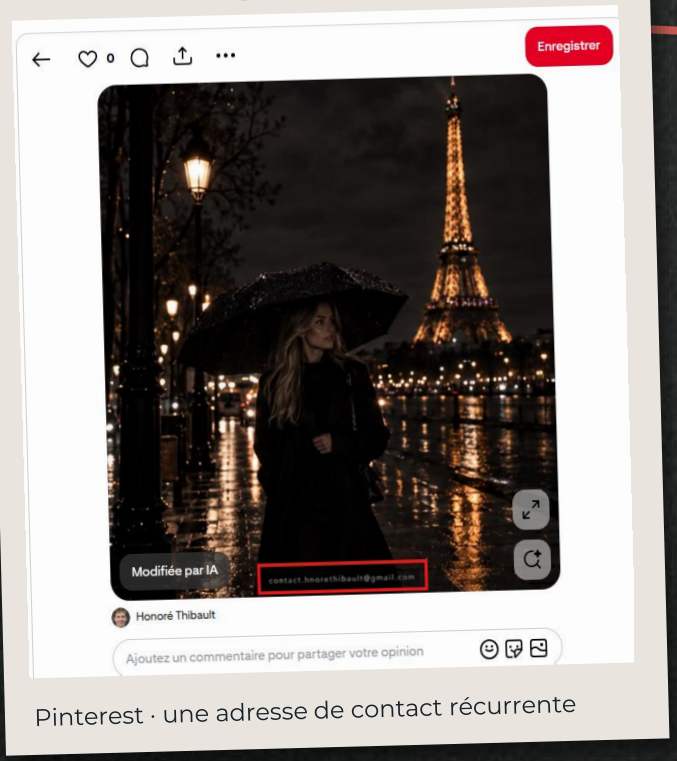

Un commentaire signé « Honoré »




Honoré Thibault · photographe

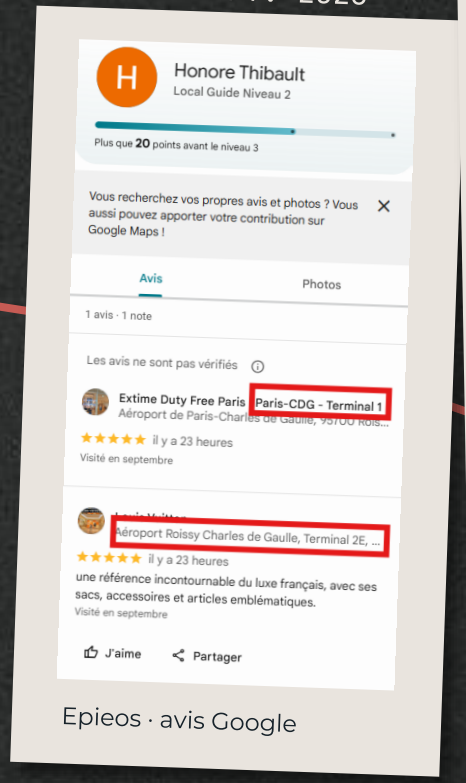
# Une adresse e-mail relie à un nouveau profil

contact.hnorethibault@gmail.com

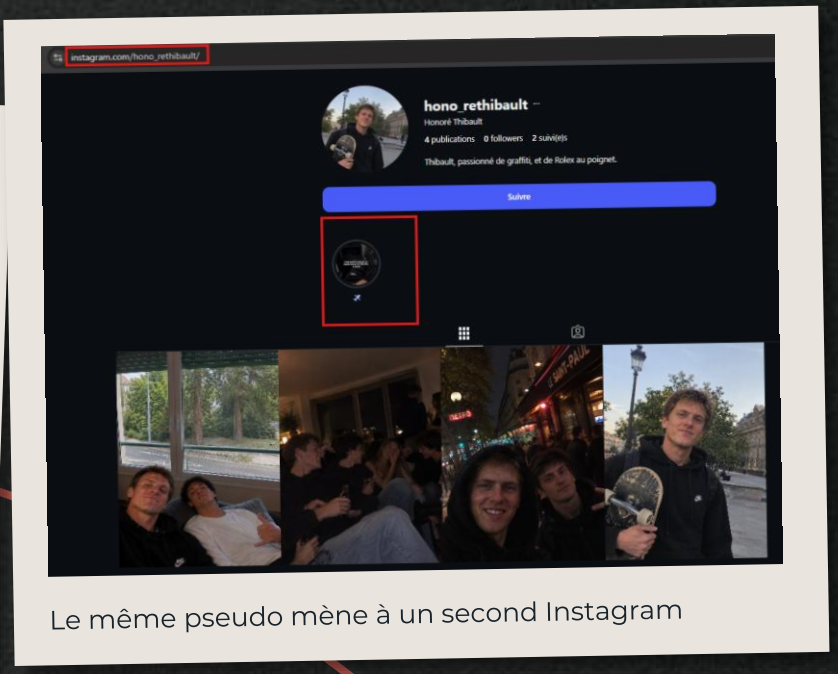



Pinterest · une adresse de contact récurrente

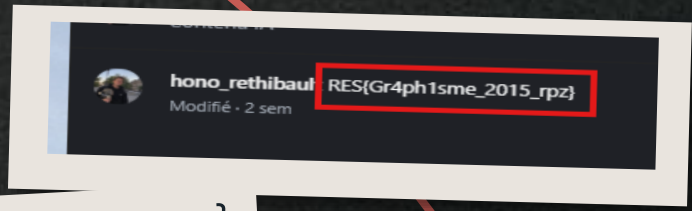
PARIS-CDG
22 SEPT. 2026




Epieos · avis Google




Le même pseudo mène à un second Instagram




FLAG 05 RES{Gr4ph1sme_2015_rpz}

# Trois stories fixent le tempo du trajet

12:40



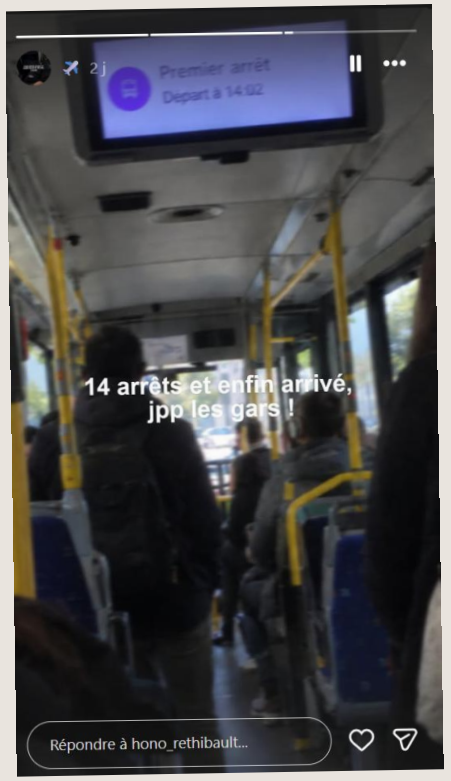

EMBARQUEMENT · AIR FRANCE

14:00




ARRIVÉE · RETARD + BUS

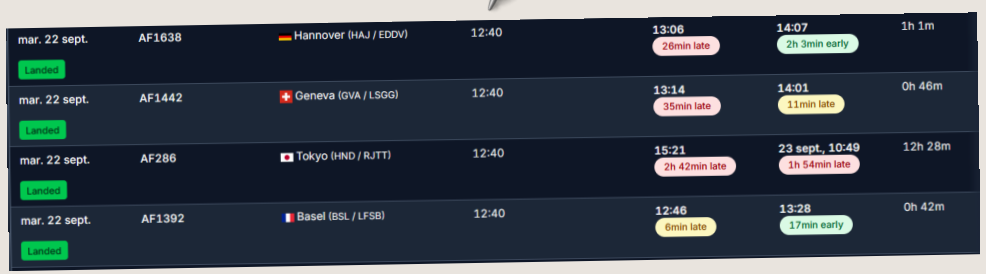
14:02




DANS LE BUS · 14 ARRÊTS

Les horaires filtrent les vols et orientent vers Genève. L'heure de 14:02 et les 14 arrêts serviront ensuite à choisir la ligne de bus et la zone de destination.

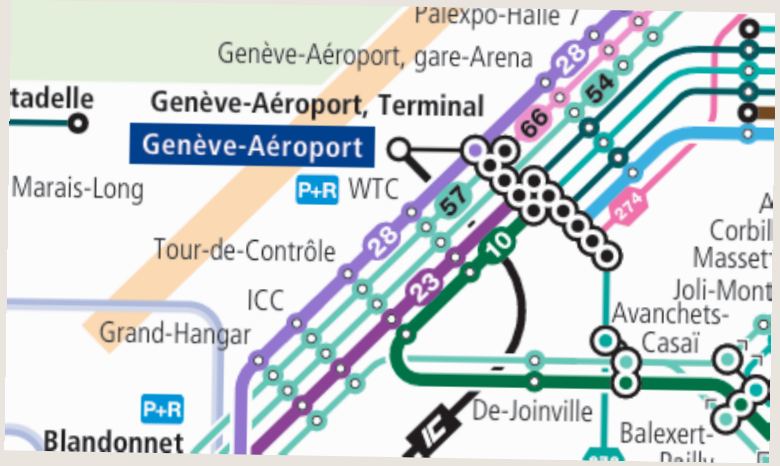
# Les horaires éliminent les fausses pistes




Flightera · quatre départs possibles depuis Paris-CDG




AF1442 · Paris CDG → Genève · horaire cohérent




TPG · deux lignes violettes possibles à l'aéroport

28 · 14:13



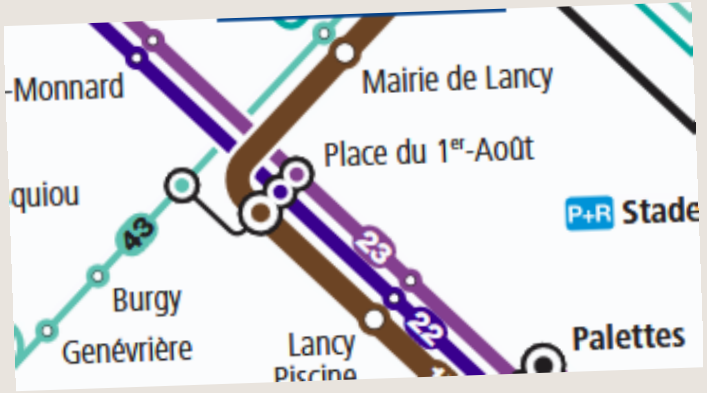

23 · 14:02




→ La ligne **23** part à 14:02, contrairement à la **28**.
Il reste à compter 14 arrêts pour identifier la destination.

# 14 arrêts jusqu'à la Place du 1er-Août

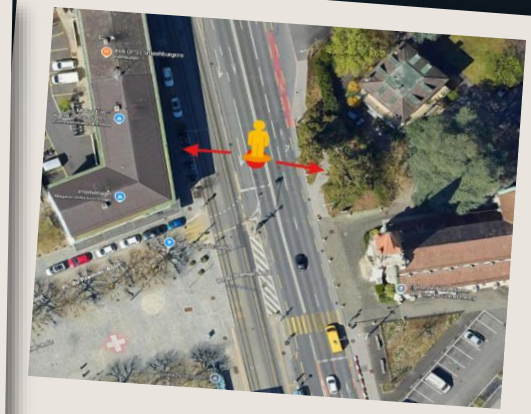
14




Ligne 23 · 14e arrêt : Place du 1er-Août



Dernière publication INSTAGRAM · comparer fenêtres et arrière-plan





Google Maps · exploration des environs

FENÊTRE · VOLETS · BARRES VERTES

RESILIENCE

DOSSIER UISIE · LOCALISATION CONFIRMÉE

# AFFAIRE CLASSÉE.



6, AV. DES COMMUNES-RÉUNIES

FLAG FINAL

`RES{Av. des Communes-Réunies 6, 1212 Lancy, Suisse}`

FIL DE L'ENQUÊTE

PHOTOS → LINKEDIN → INSTAGRAM → GRAFFITI → YOUTUBE → DISCORD → TWITCH → PINTEREST → TRAJET → ADRESSE