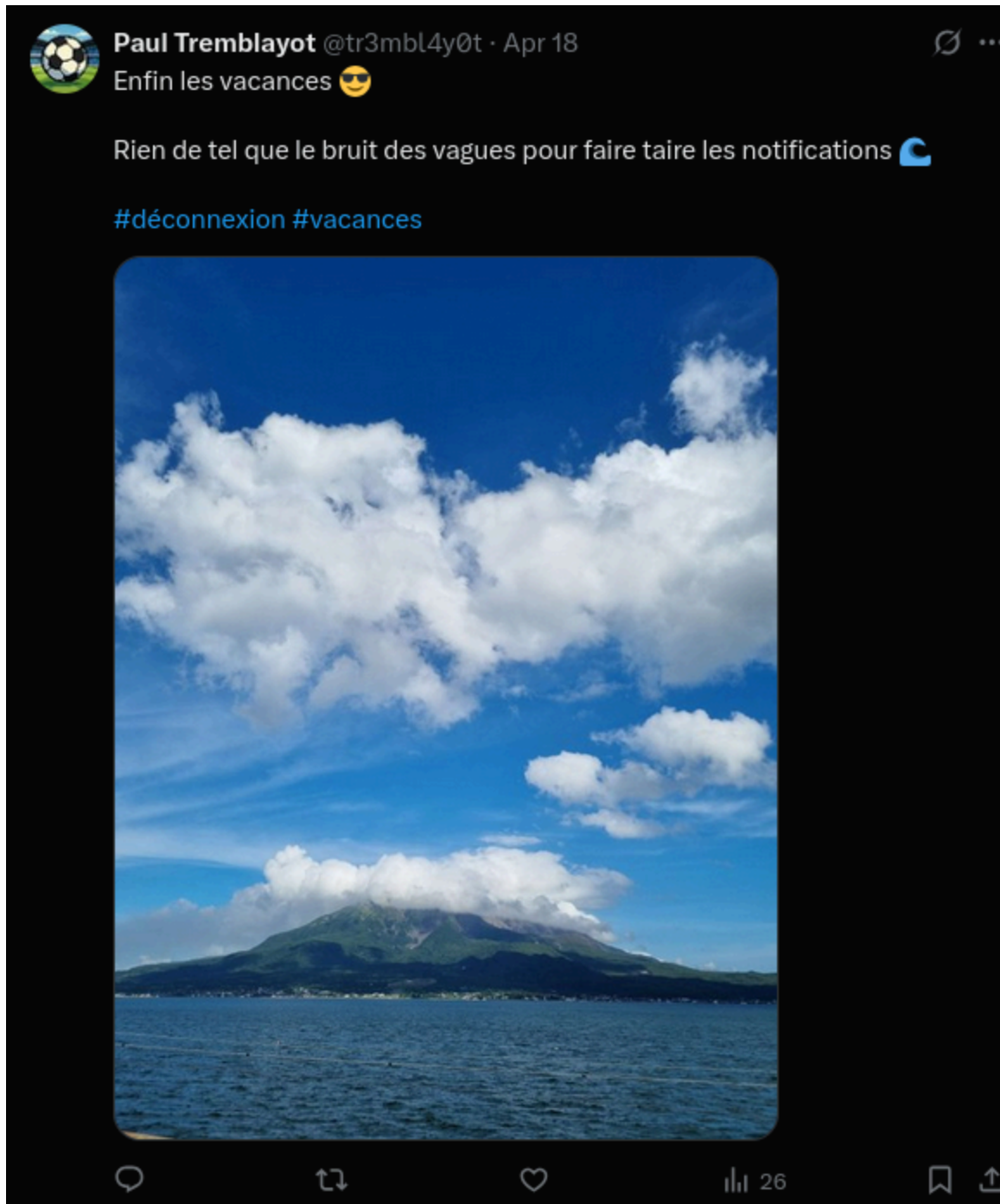


Premiers pas

On nous parle d'un individu nommé "Paul Tremblayot"

On va chercher son nom sur différents réseaux sociaux et on va rapidement tomber sur son compte X: <https://x.com/tr3mbl4y0t>



Une recherche Google image inversé permet de découvrir que c'est le volcan Sakurajima situé au sud du Japon.

En cherchant un tout petit peu sur internet on remarque que la seule grande ville à côté du volcan est la ville de Kagoshima.

```
interiut{Kagoshima}
```

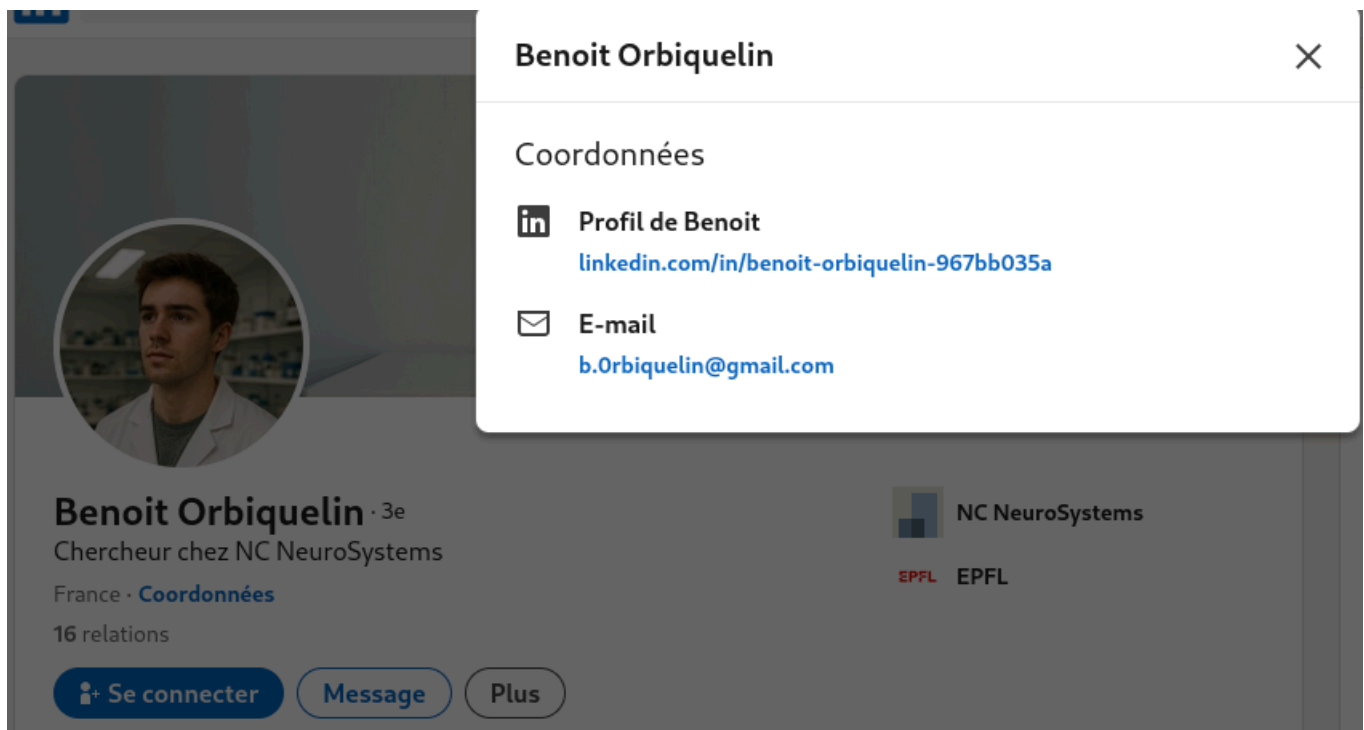
Sur les traces du fidèle

On nous informe que "Paul aurait laissé un commentaire discret sur un individu, dont l'image de profil semble avoir attiré son attention"

En scrollant un tout petit peu sur le compte X de Paul on trouve le commentaire en question:




On se rend sur le profil linkedin de "Benoit Orbiquelin" et lorsqu'on clique sur le bouton Coordonnées on remarque que une adresse gmail est liée à son compte






Avec cette adresse email on peut effectuer un Epieos ou un Ghunt.

Voici les résultats obtenus avec Epieos:



Google account finder will show you if the requested email is linked to a Google account and/or if the person left reviews on Google Maps.

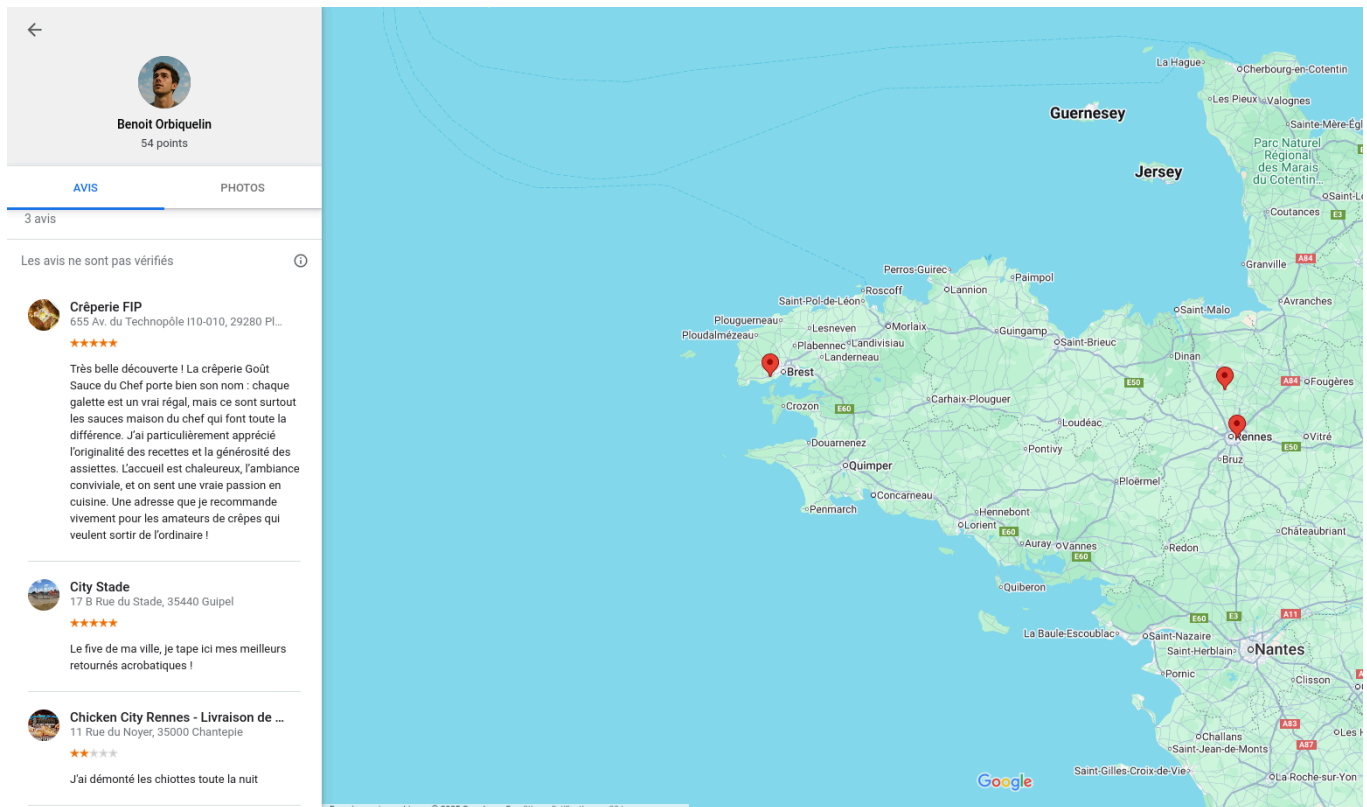


Query	b.0rbiquelin@gmail.com
Photo	 Sign up
Id	116875694383466691530
Last Update	 Sign up
Services	
Google Maps	https://www.google.com/maps/contrib/116875694383466691530
Google Calendar	https://calendar.google.com/calendar/u/0/embed?src=b.0rbiquelin@gmail.com
Google Plus Archive	https://web.archive.org/web/*/plus.google.com/116875694383466691530*

à partir d'ici il y a 2 méthodes pour obtenir le flag.

Première méthode

En allant voir ses avis google maps on peut voir que il y a un avis où Benoit dit "Le five de ma ville, je tape ici mes meilleurs retournés acrobatiques !"



On regarde de quelle ville il s'agit et ce five est situé dans la ville de Guipel

```
interiut{Guipel}
```

Deuxième méthode

En allant voir le lien google calendar et en remontant de 2 mois on remarque qu'il y a un évènement RDV à la Mairie avec en commentaire "Il faut que j'aille chercher une attestation de propriété de ma maison à la Mairie"

<div> Aujourd'hui < > Mars 2025 </div>				
DIM. 23	LUN. 24	MAR. 25	MER. 26	JEU. 27
2	3	4	5	6
9	10	11	12	13 ● 4pm RDV à la Mairie
16	17	18	19	20
23	24	25	26	27
30	31	1 avr.	2	3

b.Orbiquelin@gmail.com

Il y a également sur l'évènement une adresse qui est indiquée, c'est l'adresse de la Mairie de Guipel.

```
interiut{Guipel}
```

Quelque chose cloche


On nous informe que "Paul aurait laissé un commentaire discret sur un individu, dont l'image de profil semble avoir attiré son attention"

En scrollant un tout petit peu sur le compte X de Paul on trouve le commentaire en question:



On nous parle ensuite du site de l'entreprise dans laquelle travaille Benoit. Quand on va sur son profil linkedin on remarque que il y est écrit "Site:" suivi d'une chaîne de caractères en base64

Expérience

**Chercheur**
NC NeuroSystems · CDI
janv. 2022 - aujourd'hui · 3 ans 5 mois
Site: aHR0cHM6Ly9ub3JlY2FzdGVtLmZy=
💡 Intelligence artificielle (IA)

Une fois décodé, cela nous donne: "<https://norecastem.fr>"

On se rend donc sur le site.

En cherchant sur le site, on se rend compte qu'il y a dans le robots.txt:

```
Disallow: /guide.txt
```

On va sur guide.txt et on obtient un lien pastebin qui contient le message:

Message aux Initiés

"Les portes secrètes ne s'ouvrent qu'à ceux qui savent se faire passer pour un autre."

Avant d'entrer, change l'identité que ton navigateur utilise pour se présenter.

Utilise exactement ce nom :
MembreNoreCastem1337

C'est là, dans ce que ton navigateur dit de toi – là où il s'identifie – que tout se joue.

 Change ton masque, et la vérité apparaîtra.

Avec ce message on comprend qu'il faut changer notre user-agent avec MembreNoreCastem1337, on peut faire ça rapidement avec une extension du navigateur.

Une fois le user-agent changé on retourne sur <https://norecastem.fr> (bien à la racine du site) et on tombe sur la page secrète de la secte:

Les Arcanes de NoreCastem

Bienvenue dans le domaine secret des initiés. Ici, vérité et destinée se mêlent dans l'ombre, et seuls ceux qui osent chercher découvrent les véritables arcanes.

Nous sommes nés dans l'ombre, unis par la conviction que la raison algorithmique doit éclairer le monde. Dans les recoins obscurs du darkweb, nous avons fédéré les esprits les plus brillants, tous avides de transcender les limites humaines.

`interiut{le_masque_revele_la_verite}`

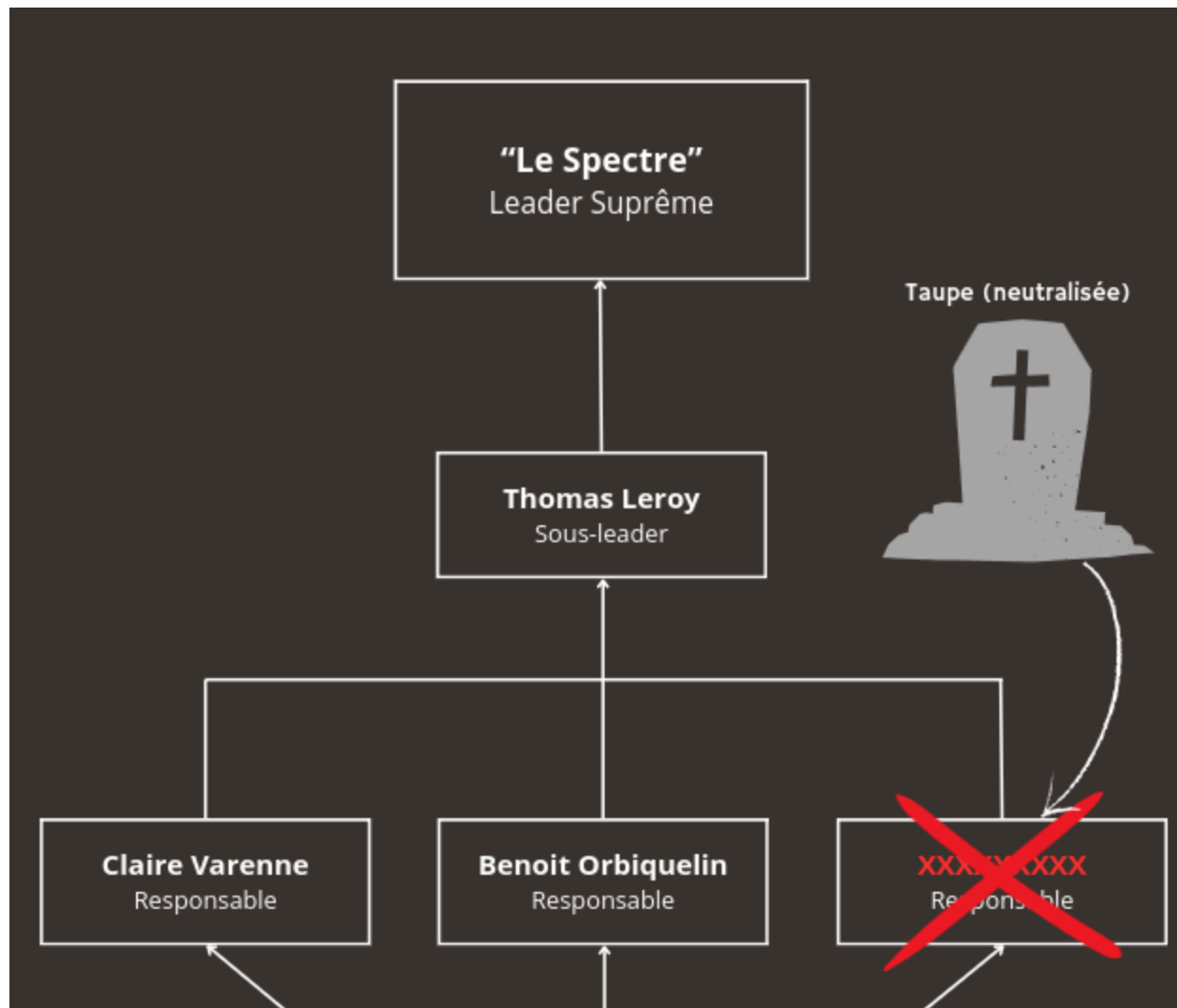


`interiut{le_masque_revele_la_verite}`

Ghost in the Page

Pour ce challenge on doit d'abord retrouver l'identité d'un de l'ancien admin sys de l'entreprise.

Toujours avec le useragent castem quand on se rend sur <https://norecastem.fr/organisation.php> on tombe sur un document intéressant:



On remarque ici qu'une personne a été tuée, ce qui correspond aux informations données dans le challenge. On en déduit donc que la personne que l'on recherche est cette dernière.

Si on se rappelle bien nous avons déjà vu ces noms sur la page principale du site de l'entreprise:

NOTRE ÉQUIPE

Des professionnels prêts à vous aider



Thomas Leroy

CEO

contact: thomas.leroy@norecastem.fr



Claire Varenne

DIRECTRICE SCIENTIFIQUE & CHERCHEUSE
PRINCIPALE

contact: claire.varenne@norecastem.fr



Benoit Orbiquelin

CHERCHEUR IA & MODÉLISATION COGNITIVE

contact: benoit.orbiquelin@norecastem.fr

On peut donc s'imaginer qu'à un moment, la personne que nous cherchons était présente sur cette page du site. Nous allons donc vérifier s'il existe d'anciennes versions du site qui ont été archivées sur Waybackmachine:



Thomas Leroy

CEO

contact: thomas.leroy@norecastem.fr

Claire Varenne

DIRECTRICE SCIENTIFIQUE & CHERCHEUSE
PRINCIPALE

contact: claire.varenne@norecastem.fr

Benoit Orbiquelin

CHERCHEUR IA & MODÉLISATION COGNITIVE

contact: benoit.orbiquelin@norecastem.fr



Henri Fargelisse

ADMINISTRATEUR SYSTÈME & INGÉNIEUR IA

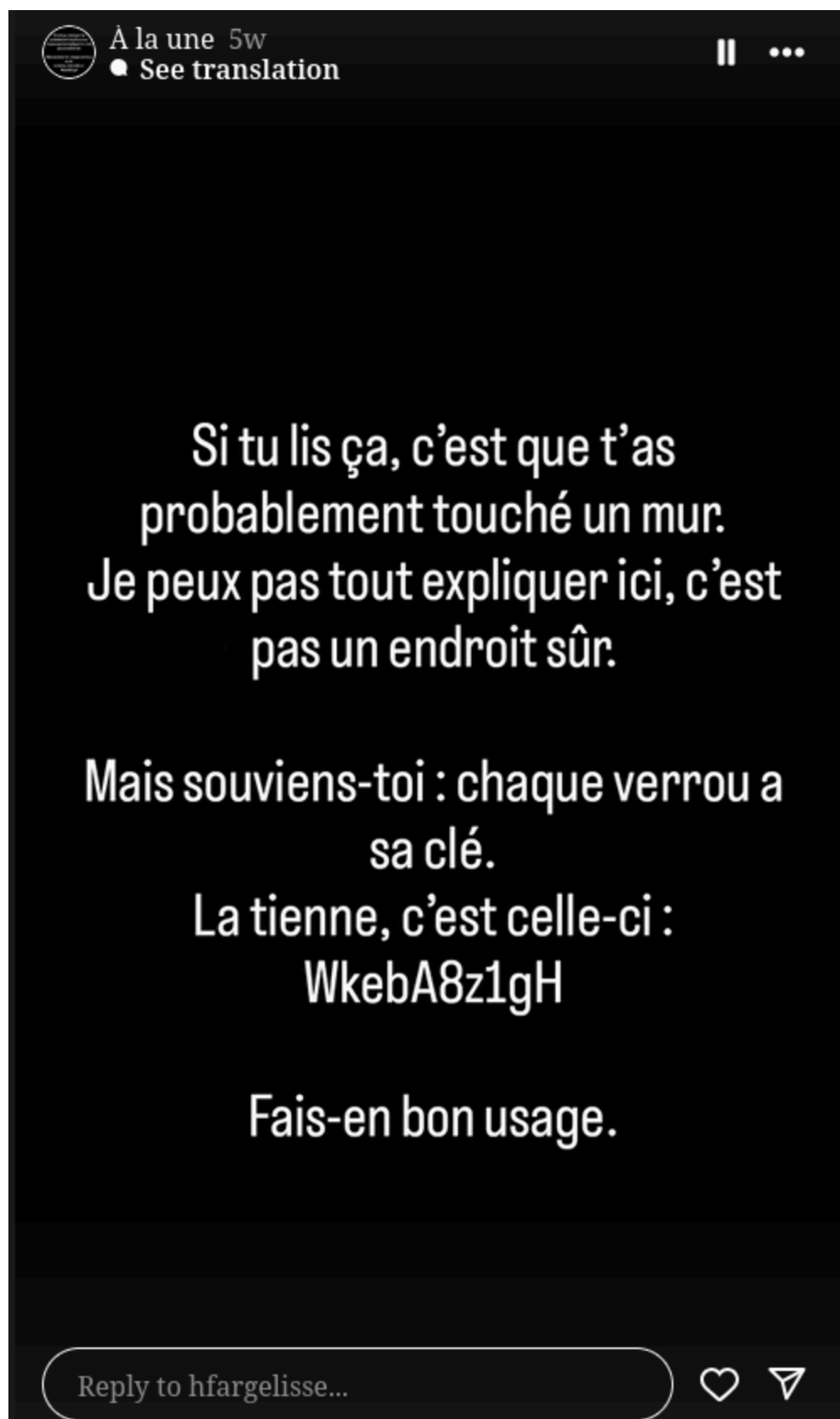
contact: henri.fargelisse@norecastem.fr

bingo, on retrouve le nom de l'ancien administrateur système.

Henri Fargelisse

Comme l'indique la description du challenge, nous devons maintenant chercher sur les réseaux ce que Henri aurait pu dire. Après quelques recherches sur différents réseaux, nous tombons

sur son compte Instagram, qui contient une story étrange :



Voici maintenant la partie difficile de ce challenge : il faut revenir sur ses pas pour ceux qui n'ont pas été assez méticuleux.

Si l'on avait prêté attention aux détails jusqu'à présent, on aurait remarqué que le compte Pastebin ayant publié le paste trouvé sur `/guide.txt` contient également un autre paste nommé `admin_final_note`, protégé par un mot de passe.

Le nom du compte Pastebin en question est Hf-castem, une référence à Henri Fargelisse.

On utilise le mot de passe donné par Henri pour déverrouiller le paste, qui contient les informations suivantes, ainsi que la première partie du flag :

```
Si tu lis ce message... c'est que je n'existe plus.
```

```
Ils savent. Je ne sais pas comment, mais ils savent que je ne suis pas des leurs.
```

```
J'ai voulu trop creuser. Trop vite. J'ai vu ce que j'aurais dû ignorer.
```

```
J'ai collecté ce que j'ai pu. Pas assez pour tout dévoiler, mais assez pour que quelqu'un poursuive.
```

```
Le Spectre... j'ai trouvé des informations sur lui. Des enregistrements dans une de ses sessions qu'il a oublié d'effacer.
```

```
Je n'ai pas pu tout transférer, mais j'ai glissé des éléments dans ma boîte pro avant qu'ils ne me coupent.
```

```
C'est discret. Une réponse automatique sur mon adresse pro.
```

```
Bonne chance.
```

```
- H.F.
```

```
1st part:
```

```
interiut{retrouve_le_tu_es_la
```

On décide d'écouter Henri et d'envoyer un mail à son adresse professionnelle, que l'on peut retrouver grâce à la Wayback Machine. En réponse, on reçoit la deuxième partie du flag qui nous permet d'avoir le flag complet:

```
interiut{retrouve_le_tu_es_la_cle_pour_faire_tomber_le_spectre}
```

Itineraire Fragile

La première étape — et la plus difficile — consiste à retrouver le vol exact.

Tout d'abord, on remarque que le billet d'avion indique le numéro de l'appareil : EC-MTC. Une recherche sur FlightAware montre qu'il s'agit d'un avion de la compagnie Volotea, ce qui correspond au logo présent sur le billet.

<https://fr.flightaware.com/live/flight/ECMTC>

Ensuite, le fait que l'on nous précise que nous avons la photo originale n'est pas un hasard : cela sert à nous faire comprendre que les métadonnées sont toujours présentes. Grâce à ces dernières, nous obtenons la localisation du lieu où la photo a été prise : l'aéroport de Nantes:

```
$ exiftool boarding_ticket_picture_original.png
ExifTool Version Number      : 12.57
File Name                    : boarding_ticket_picture_original.png
...
GPS Latitude                 : 47 deg 9' 25.35" N
GPS Longitude                : 1 deg 36' 25.05" W
GPS Position                 : 47 deg 9' 25.35" N, 1 deg 36' 25.05" W
Date/Time Original           : 2025:04:06 16:18:00
```

On obtient également la date et l'heure originales de la prise de vue :
2025:04:06 16:18:00

On apprend dans la conversation que la photo a été prise précisément 20 minutes avant le décollage, ce qui signifie que nous cherchons un vol ayant décollé à 16h38.

Avec toutes ces informations, en consultant l'historique de l'avion sur FlightAware, on identifie le vol suivant :

<https://fr.flightaware.com/live/flight/ECMTC/history/20250406/1645Z/LFRS/LPPR>

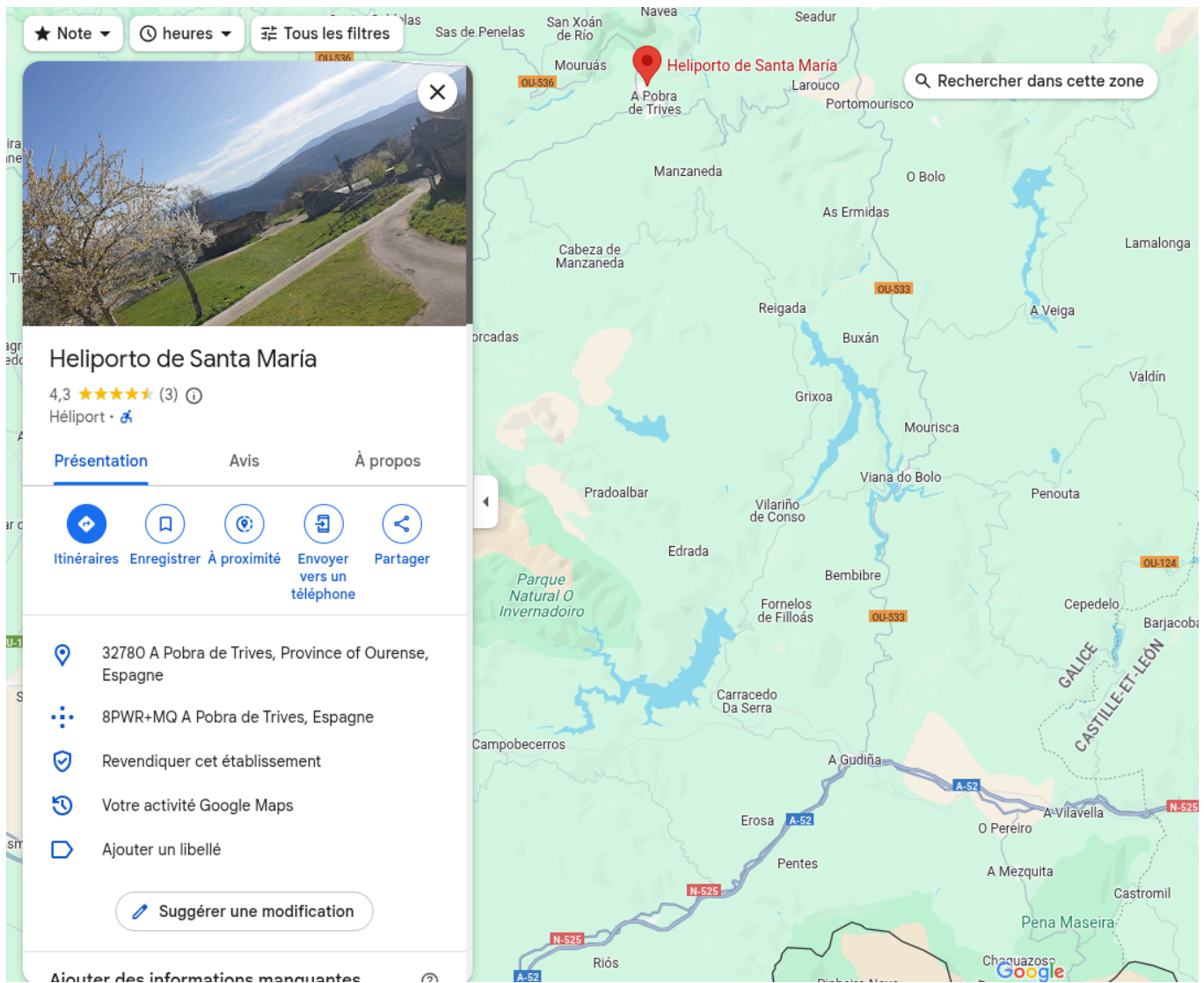
La ville de destination est donc Porto.

Il est également indiqué sur la page que la durée du vol était de 1h17.

Pour trouver la dernière partie du flag, toujours sur FlightAware, on va observer où se trouvait l'avion après 56 minutes de vol :



Enfin, une simple recherche d'hélicoptères sur Google Maps nous révèle la dernière partie du flag :



interiut{Porto_1h17_Santa-Maria}

Le Visage du Culte

On regarde les informations que Henri nous a transmises par mail:

Voici les informations que j'ai pu rassembler et qui pourraient vous aider à l'identifier, vous savez de qui je parle:

D'après ce que j'ai recoupé, il aurait laissé un avis public sur son hôtel favori à Paris.

J'ai également entendu dire qu'il existe un bar qu'il fréquente souvent lorsqu'il est en déplacement dans la capitale.

Ce bar serait situé à moins de 200 mètres d'un datacenter, à moins de 200 mètres d'un restaurant servant du fish and chips, et à moins de 550 mètres d'un transformateur électrique.

Une fois que vous sortez du bar, partez sur votre gauche et continuez tout droit jusqu'à atteindre une station de métro.

Prenez la seule ligne permettant de rejoindre un terminus en exactement 8 arrêts, puis descendez à ce dernier.

Choisissez la sortie portant le chiffre le plus élevé, puis prenez le passage sur votre droite.

L'hôtel sera le premier bâtiment à votre droite.

On se rend compte que, pour trouver le bar, il va falloir utiliser Overpass Turbo :

<https://overpass-turbo.eu/>

Voici la requête qui permet de localiser le bar :

```
[out:json][timeout:25];

{{geocodeArea:Paris}}->.searchArea;

(
nwr["telecom"="data_center"](area.searchArea);
)->.dc;

(
```

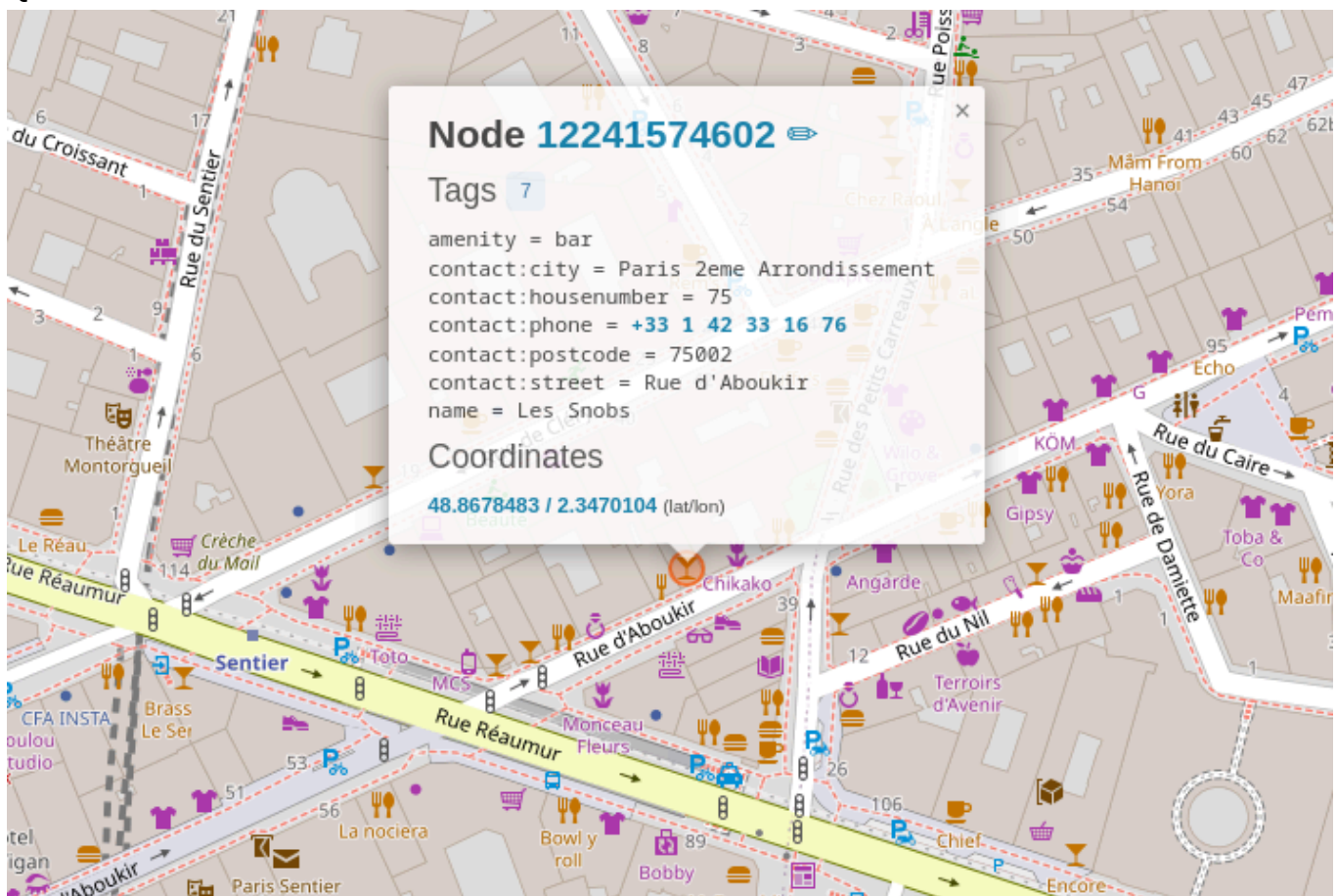
```
nwr["amenity"="restaurant"]["cuisine"="fish_and_chips"](area.searchArea);
)->.fish;

(
nwr["power"="transformer"](area.searchArea);
)->.transfo;

node(around.dc:200)(around.fish:200)(around.transfo:550)["amenity"="bar"]
(area.searchArea);

out geom;
```

Qui nous donne:



Le nom du bar est donc Les Snobs.

On continue ensuite vers la gauche jusqu'à atteindre la station de métro Strasbourg - Saint-Denis.

La seule ligne qui respecte les conditions est la ligne 4, avec pour terminus Porte de Clignancourt. On prend donc la sortie portant le chiffre le plus élevé : la sortie 5.

Sorties :

- 1 Porte de Clignancourt *Puces de Saint-Ouen*
- 2 Boulevard Ney
- 3 Rue Belliard
- 4 Rue Letort
- 5 Boulevard Ornano



On prend le passage a droite et le premier hotel a notre droite est:

Hotel Kyriad Paris 18 - Porte De Clignancourt

On cherche les avis sur TripAdvisor et on tombe rapidement sur cet avis d'un individu qui parle de la castem:



Jonas Verhoeven a écrit un avis en avr. 2025

1 contribution



Une valeur sûre

Je passe souvent ici quand je bosse tard chez la Castem. Toujours un bon moment.

L'accueil a été chaleureux dès mon arrivée, avec un personnel souriant et toujours disponible pour aider. La chambre était propre, bien équipée et confortable, idéale pour se reposer après une journée bien remplie.

Plus ▼

Date du séjour : janvier 2025

interiut{Jonas_Verhoeven}