



# Write Up Medileak 3 - Qualifications

LA DER DES DER

**Auteur** Sam - Stagiaire d'élite

**Client** Limoges Métropole

**Réalisation** Oscar Zulu

**Co Traitant** YPSI SAS / Manufacture Française d'OSINT SARL

**Classification** Document public

---



## Sommaire

1. Les règles sont les règles	5
2. Old Friend	7
3. Smile	8
4. Love me tender	10
5. Go West	14
6. Mull of Kintyre	16
7. In da club	23
8. Mon amie la rose	24
9. Magnolia for ever	26
10. Je fais mon job a plein temps	30
11. The Teacher	31
12. Étudiant poil aux dents	32
13. Message in a bottle	35
14. Every Breath You Take	37
15. Undercover of The Night	43
16. (I cant't Get No) Satisfaction	46
17. Under Pressure	47
18. Gold Digger	50
19. Around The World	51
20. BadBank	58
21. I Can See Clearly Now	62
22. Sweet Child o' Mine	68



23. Soldier of Fortune

69

24. Tubular Bells

73



# Write Up Medileak 3 - Qualifications

Voici donc le write-up officiel de Medileak 3, qui conclut l'arc narratif commencé en 2024 avec le couple Raoul Reidid et Gizem Ihanet (mais est-ce vraiment son nom ?).

Nous remercions en tout premier [Limoges Métropole](#), pour sa confiance renouvelée pendant 3 ans, qui nous ont laissé le champ libre pour faire un des CTF OSINT les plus exigeants. Nous espérons que l'aventure continuera, avec sans doute de nouveaux personnages.

Ce Write-up a été rédigé par Sam, notre stagiaire d'élite, loué soit son nom.

Si vous nous découvrez au travers de ce write-up, n'hésitez pas à nous rejoindre sur [Discord](#)



# Bienvenue

## 2. Les règles sont les règles

**Les règles sont les règles** 1 pts

Deux ans.

Deux ans que le dossier Medileak tourne en rond sur votre bureau. Deux ans que la clinique a fermé ses portes dans la précipitation, que ses fondateurs se sont éparpillés aux quatre coins de l'Europe, et que les données de santé de centaines de patients se sont retrouvées aux enchères sur un site du darkweb. Deux ans qu'un certain Raoul, pseudo-médecin et marchand d'huile magique, s'est volatilisé un soir de juin 2024 à Limoges, une mallette sous le bras et pas un mot d'adieu.

On l'a retrouvé en 2025. À vendre ses trackers de santé depuis un balcon avec vue sur la tour Al Manara. Puis de retour en France, recyclé en directeur médical d'une startup d'IA médicale qui sentait le soufre à plein nez — sans parler de cette joint-venture trouble avec un entrepreneur tchèque. Et puis, comme un fait exprès, on a reperdu sa trace à l'aéroport de Limoges...

L'affaire est plus complexe que prévu. Il va donc falloir mettre un terme à tout ça. Et vite.

Avant de continuer, assurez-vous d'avoir lu le règlement disponible [ici](#).

Si c'est déjà fait, la phrase magique est :

Grand classique de démarrage, on ouvre le règlement et on le lit attentivement. Notamment ce passage que certaines équipes ont redécouvert en cours de jeu :

**Comportement attendu des participants**

Interdiction stricte d'attaquer la plateforme ou aux éléments créés pour le CTF (profils, sites internet...) au risque d'un bannissement définitif de celle-ci. Les connexions sont contrôlées en temps réel et les journaux d'activités sont consignés.

On récupère le flag. Et c'est parti !

Merci d'avoir lu le règlement jusqu'au bout. Pour vous remercier, voici la phrase magique :

**Fonce et Bute**

🚩 **Flag :** Fonce et Bute

(Pour ceux qui se posent la question : oui il y a eu des fails pour ce challenge)



## Here we go again

# Here we go again

Alors vraiment prêts pour l'aventure ?

### 3. Old Friend

#### Old Friend 10 pts (-1/err)

En cette fin de semaine du mois de mai, votre équipe reçoit un message d'un expéditeur inconnu, via une messagerie chiffrée.

Pas d'introduction, pas d'explication : la photo d'un homme d'une soixantaine d'années, l'air quelconque, prise dans ce qui ressemble à un intérieur. Et une seule ligne de texte :

**"Hey ! Tu le connais pas, lui ?"**

L'expéditeur ne s'est plus jamais manifesté. On essaie de rappeler, rien. On essaie de tracer, rien non plus. Juste cette photo, plantée au milieu de l'écran.

Mais ce visage, vous le connaissez. Et plutôt deux fois qu'une.



L'homme sur la photo, c'est   !

Pour ceux qui avaient participé à Médileak 1 et/ou Médileak 2, la réponse évidente. Pour les nouveaux joueurs, cela consistait surtout à les encourager à lire les write-ups des éditions précédentes (<https://oscarzulu.org/wu-medileak>) pour qu'ils soient au fait de l'histoire et des personnages.

🚩 **Flag :** `Raoul Reidid`

## 4. Smile

**Smile !** 20 pts (-2/err)

La photo ne sortait pas de nulle part. C'était bien cette tête qu'on traque depuis plus de deux ans, celle qui nous a baladés de Chypre à la République tchèque en passant par Limoges. Depuis sa fuite en juin 2025, il s'était évaporé sans laisser la moindre trace.

Mais quelqu'un l'a photographié et a mis le cliché en ligne. Visiblement sans se douter qu'il attirerait notre attention.

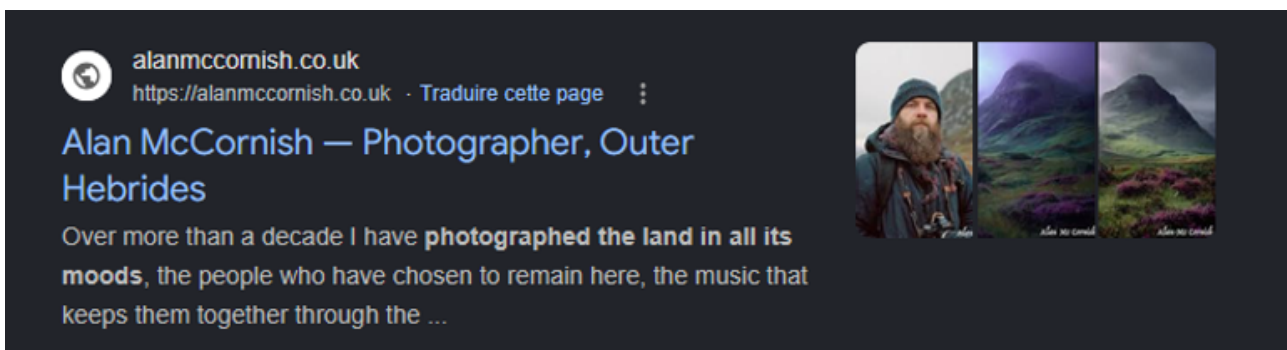
Vous remontez le fil. Et l'auteur de la photo, lui, ne se cache pas du tout.

**Son site internet est accessible à l'adresse**

Le nom du photographe est indiqué sur la photo :



Une simple recherche sur Google, et en premier résultat :



🚩 **Flag :** `https://alanmccornish.co.uk`



Et il tient même un album photo en ligne sur  sur lequel on retrouve quelques pépites.

On comprend que ce n'est pas un autre site en son nom, mais que ça doit être une plateforme où les gens peuvent créer et partager des photos. Avec le pseudo récupéré, on peut faire une recherche mais qui ne donne rien. Pas d'autre réponse directement donnée par Google ou d'autres moteurs de recherche. On va donc devoir chercher à la main... Vous n'êtes pas calé en photo, et personne dans votre entourage ne peut vous conseiller ? N'importe quelle IA pourrait vous orienter pour organiser votre recherche :

Je cherche un site sur lequel un photographe pourrait créer un album en ligne. Donne moi le nom des 10 les plus utilisés.

Voici 10 plateformes largement utilisées par les photographes pour créer des albums ou galeries en ligne :

1. [Flickr](#)
2. [Google Photos](#)
3. [SmugMug](#)
4. [Adobe Lightroom](#)
5. [Pixieset](#)
6. [Zenfolio](#)
7. [500px](#)
8. [ShootProof](#)
9. [Pic-Time](#)
10. [Format](#)

On teste les réponses une par une avec le pseudo de Alan. On le découvre sur 500px, en reconnaissant les portraits déjà présents sur le précédent site.



**Alan McCornish**

Follow

The Outer Hebrides will not perform for you. The light here arrives sideways, uninvited, and the landscape has no intere... [Read more](#)

4 Followers 1 Following 27 Photo Likes 2 495 Photo impressions ⓘ



[Photos 3](#)



Flag : <https://500px.com/p/alanmccornish>

## 5. Love me tender

### Love me tender 70 pts (-2/err)

Vous fouillez l'album du photographe, cliché après cliché. Et au milieu des paysages et des portraits, un visage familier finit par sortir du lot :   , prise en pleine prestation sur scène.

On va donc étudier le site du photographe, et parmi les photos, notre attention est attirée par cette photo :



Ce musicien particulièrement talentueux, qui joue de la guitare et du violon en même temps. Incroyable !

Mais ce n'est pas ce qu'on cherche... Parmi les photos, on reconnaît :



Son nom est même précisé sous les photos.

Flag : Gizem



Aucun doute possible : c'est bien elle, à ses côtés depuis l'affaire de la clinique

Beausoleil



Ils sont donc ensemble, et au même endroit. Premier point marqué.

Et puisqu'elle remonte sur scène, il y a fort à parier qu'elle a pris du galon depuis son premier profil musical et qu'on retrouve maintenant ses **nouveaux** titres sur la célèbre plateforme

MySpaceMusic



(et non soundcloud n'est pas la bonne réponse).

On fait confiance à sa mémoire, ou on ressort notre write-up.

**Flag :** Yemanja

Elle avait partagé ses chansons sur Soundcloud, mais depuis elle a beaucoup progressé. Plusieurs méthodes permettent d'identifier une des plateformes recherchées (comme précédemment, on peut chercher Gizem sur les plateformes le plus connues, sinon une recherche Google avec gizem+raoul donne aussi des réponses). Finalement, la plus grande difficulté de ce challenge était de choisir quel nom entrer (relativement inattendu par les concepteurs qui ne s'attendaient pas à ce que Gizem connaisse un tel succès).

On peut retrouver l'album sur plusieurs plateformes comme Deezer :

<https://www.deezer.com/fr/album/957942101>



**Flag :** au choix... Deezer, Spotify, youtube music, amazon music, Apple Music

Vous écoutez. Vous prenez des notes. Et l'un des morceaux attire particulièrement l'attention : elle y évoque

Paul de Maisonclaire



— un nom qui sent la personne, ou le lieu, à plein nez.

On va donc écouter avec plaisir ses nouvelles chansons. Si on est pressé, on peut supposer que la chanson Skye est à étudier en priorité, puisque le photographe découvert un peu plus tôt évoquait cette zone géographique.

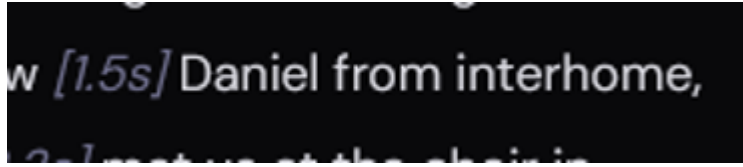
Pas de paroles trouvables facilement, pas de sous titrage disponible sur les différentes plateformes. Si on n'a pas la capacité de retranscrire les paroles d'une chanson en anglais à la première écoute (même si elles ont été affûtées par nos recherches en campanologie), on peut faire appel à des sites qui proposent ce travail à partir d'une URL (par exemple <https://zeemo.ai>)

🎵 FLOOODIGARRRRY 🎵



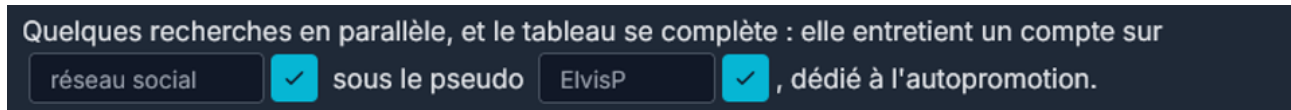
🎵 FLOOODIGARRRRY 🎵

Parmi les paroles, on peut remarquer la mention d'un certain Daniel.

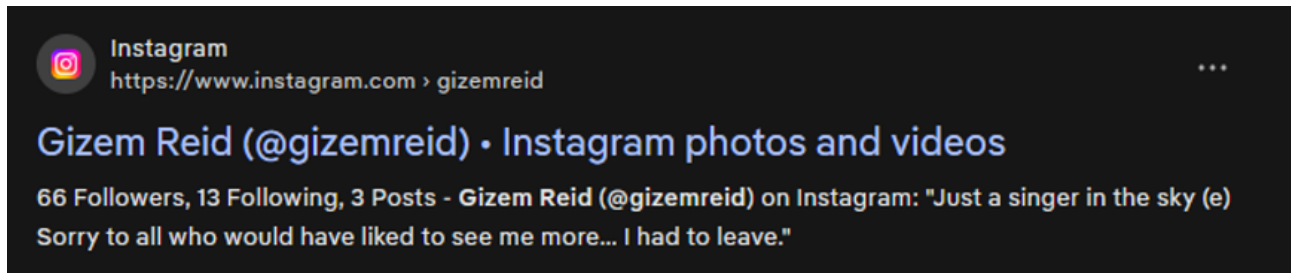


Le format de flag aidait à confirmer que c'était bien ce qui était attendu. Plus méticuleux : retranscrire l'ensemble des paroles de toutes les chansons pour vérifier que rien d'autre n'était plus adapté.

🚩 **Flag :** Daniel de Interhome



L'album est au nom de Gizem Reid. Recherche Google : <https://www.instagram.com/gizemreid>



🚩 **Flag :** Instagram

🚩 **Flag :** gizemreid



# Voyage Voyage

## Voyage Voyage

Une petite excursion ça vous dit ?

### 6. Go West

#### Go West 30 pts (-2/err)

Rester derrière son écran, c'est bien. Aller sur place, c'est mieux. Après une rapide concertation d'équipe (et un débat houleux pour savoir qui allait garder le chat), vous prenez la décision de vous déplacer.

Direction

Directement obtenu par l'album de Gizem et confirmé par son Instagram.

**Flag :**

Le billet est réservé dans la foulée. Évidemment, le parcours le moins cher passe par Dublin, avec trois heures d'escale et un sandwich triangle au saumon qui restera dans les mémoires pour de mauvaises raisons. L'avion pour Inverness décolle avec vingt minutes de retard, le temps qu'un passager retrouve son bagage à main dans le mauvais compartiment.

Depuis Inverness, la route vers le nord-ouest longe des lacs noirs et des collines sans arbres. La pluie commence quelque part après Invergarry. Elle ne s'arrêtera plus.

Vous savez où chercher. Un concert est prévu à   — de quoi resserrer la zone et localiser leur lieu de villégiature.

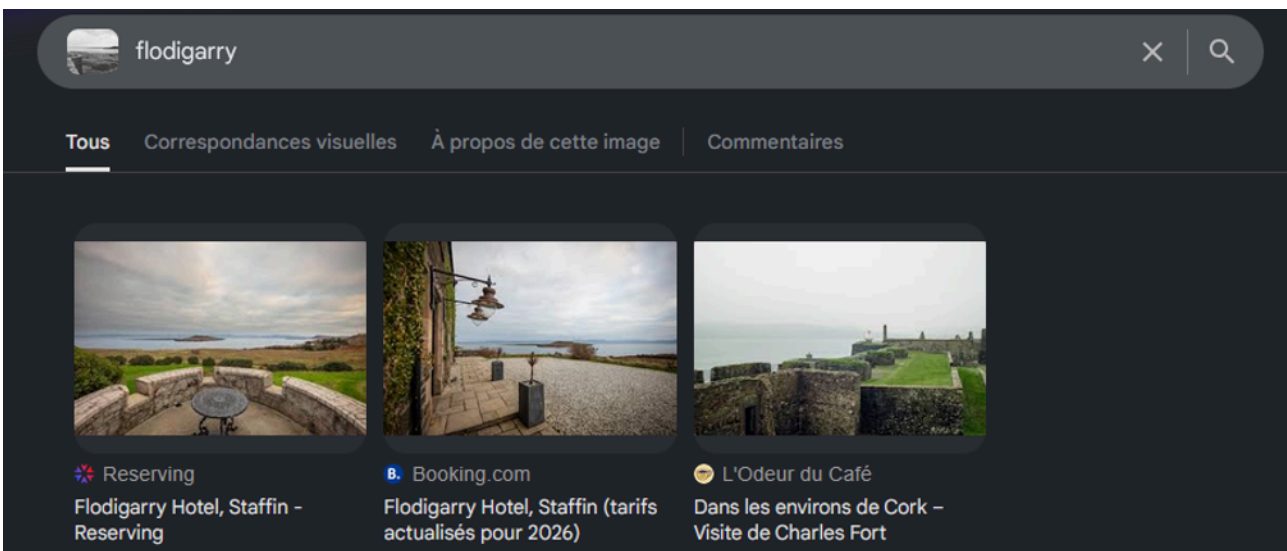
On cherche où aura lieu son prochain concert. Elle publie plusieurs photos sur son compte Instagram qui permettent de définir un secteur géographique autour de Flodigarry, mais c'est surtout ce post qui mentionne clairement où aura lieu le concert : sur la terrasse prise en photo.

(Tips pour ceux qui n'ont pas de compte Instagram : on peut accéder aux photos et commentaires simplement en copiant le lien de l'image dans un nouvel onglet)



On pense donc immédiatement à une recherche par image. Malheureusement, elle ne donne pas de réponse tout aussi immédiate. Il va donc falloir ruser un peu. On peut préciser avec la recherche « flodigarry » (oui, encore, pourquoi vous croyez que ça entête comme ça, rien n'est laissé au hasard chez les Rhinos).

Et là, miracle ! Notre terrasse !



On peut confirmer que c'est la même terrasse en allant vérifier directement sur le site de l'hôtel <https://www.flodigarry-hotel-skye.co.uk> (oui, sur Booking, d'autres photos montrent qu'il a dû y avoir des travaux depuis, mais le site de l'hôtel est une source bien plus légitime pour une confirmation)



Flag : The Flodigarry Hotel

De là, plus qu'à remonter la route. Leur point de chute n'est pas loin de la  .

Elle mentionne que son cottage n'est pas loin de l'hôtel où devait avoir lieu son concert. Un rapide coup d'œil à une carte nous indique qu'il n'y a qu'une « grande » route dans ce secteur.



Flag :

## 7. Mull of Kintyre

**Mull of Kintyre** 50 pts (-2/err)

La maison est vide quand vous y arrivez. Évidemment. Mais grâce à une aide extérieure, vous trouvez un récépissé pour un colis destiné à  . On le note, on le photographie, on le glisse dans le sac.

La pluie n'a pas faibli. Comme Gizem et Raoul l'ont fait avant vous, vous attrapez le bus pour quitter l'île à destination de  , qui part dans vingt minutes.

En lisant bien le rapport, on comprend qu'on doit se rendre sur place. Le budget de Limoges étant limité, nous n'avons pas pu offrir un billet à chaque équipe... Cependant un outil génial est intégré à l'atelier d'enquête et nous permet de nous rendre dans un lieu sans bouger de notre chaise (ce qui rappelons-le, peut être dangereux au cours d'un ctf).

Reste qu'il faut localiser ce cottage.

**Piège** : la recherche sur Interhome ne donnait pas le cottage recherché... Mais il y a quand même plusieurs façons de le trouver.

Par exemple, une recherche google avec « cottage flodigarry interhome » nous amène dès le deuxième résultat à un cottage qui semble intéressant :



agoda Hébergements **Transport** Transports Activités et loisirs Bons de réduction & Offres Appartements ... €

🔍 Holiday Home Quiraing Cottage by Interh... 📅 Arrivée 📅 Départ 👤 2 adultes 1 chambre

Accueil > Royaume-Uni Établissements (266 441) > Ile de Skye Établissements (219) > Réservez à Holiday Home Quiraing Cottage by Interhome

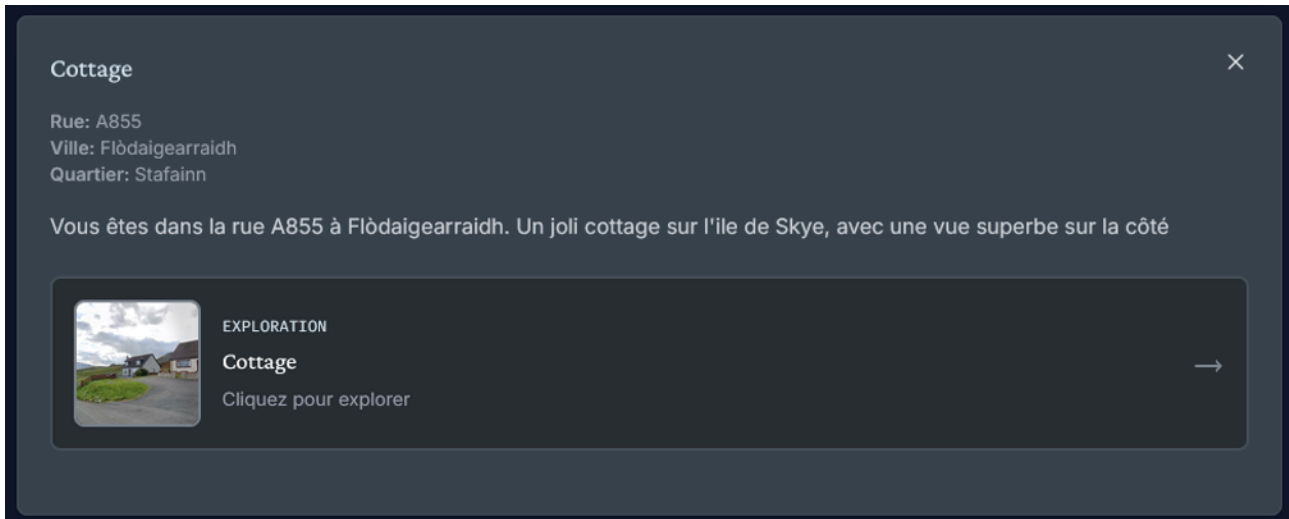
[📷 Voir toutes les photos](#)

On retrouve la photo similaire à celle postée sur l'Instagram de Gizem :



Autre méthode : se dire que la zone de recherche est relativement restreinte. Partir de l'hôtel identifié pour son concert, et suivre la route A855 avec Google Street View. Observer le paysage pour arriver à identifier la zone où a été prise la photo. Il y a plusieurs cottages à cet endroit, on confirme en cherchant des infos sur chacun d'eux.

Vérifier avec Street View était également nécessaire pour bien confirmer l'adresse du cottage car même avec le nom précis, plusieurs sites de réservation ne donnaient pas l'adresse exacte.



Une petite remarque sur cet outil : oui vous pouvez cliquer n'importe où sur la carte, vous obtiendrez toujours une réponse. Exactement comme dans la vraie vie, où que vous alliez, vous trouverez toujours un papier, un tag, un chewing-gum suspect...



On part donc explorer le cottage. On y rencontre le fameux Daniel, en train de tondre la pelouse. On entame un sympathique échange avec lui, lors duquel il va surtout nous apprendre 2 choses utiles à notre enquête : Gizem et Raoul ont pris le bus pour Inverness, et, avant de partir, ils ont jeté des choses dans la poubelle bleue.

🚩 **Flag :** **Inverness**

On refait le tour de la maison, et effectivement, nous trouvons des papiers dans la poubelle :



↓

	<b>Certificate of Posting for Online Postage</b> <b>This certificate will not be valid unless stamped by a staff member.</b> Keep this certificate safe. It is your proof of posting if you need to make a compensation claim.
<b>Name &amp; Address</b> MEDIDEAL 24 Leskoškova cesta 9c, 1000 Ljubljana, SLOVENIA	<b>Service Used</b> Tracked 48 <b>Tracking Number</b> MZ123Q03848GB
Official stamp: 	
Please refer to separate terms and conditions. This is not a VAT receipt. Royal Mail and the cruciform are trade marks of Royal Mail Group Ltd. © Royal Mail Group Ltd. 2024 All Rights Reserved	

SEAT / SIEGE	GATE / PORTE
11A	E4
PASSENGER TYPE ADULT / ADULTE	
BARCODE / CODE-BARRES	
	
IMPORTANT INFORMATION / INFORMATIONS IMPORTANT	
<small>1. Please arrive at the airport at least 2 hours before departure / Veuillez y arriver à l'avance. 2. Boarding closes 15 minutes before departure / L'embarquement ferme. 3. Only one personal item (max 40x20x25cm) is included / Un seul objet p. 4. Keep this boarding pass with you throughout your journey / Gardez cet</small>	



Sur le récépissé, on obtient le destinataire du colis.

🚩 **Flag :** `medidea124`

Il est déjà aux trois quarts plein. Une équipe de rugby amateur — maillots rouges, sacs énormes, décibels assortis — rentre d'un déplacement quelque part dans les Highlands. Résultat inconnu, ambiance clairement post-victoire. Vous vous glissez dans la dernière rangée libre, coincés entre la vitre embuée et un pilier de quinze kilos de plus que vous, qui s'endort sur votre épaule au bout de quelques kilomètres.

Pendant le trajet, l'un de vous croise les manifestes de vol. D'après les informations collectées, ils ont pris le vol  ✓ depuis  ✓ vers  ✓ .

On lit le QR code, avec son smartphone, ou avec un outil en ligne.

On obtient : `M1REIDID/RAOUL E1P2JXZ MANLIGFR FR38 125Y14C 04210063026246200`

Avec les informations « siège » et « porte », on peut deviner qu'il s'agit d'un billet pour un voyage en avion. Là encore, efficacité avant tout, on donne le code à une IA qui nous aide à identifier comment comprendre ce code.



## 📄 Découpage probable

### **M1REIDID / RAOUL**

- Nom du passager (RAOUL)
- "M1REIDID" : identifiant interne / segment système (non utile pour un humain)

### **E1P2JXZ**

- Code de réservation (PNR / dossier passager)

### **MANLIGFR**

- Nom de famille + pays
- "FR" = France (code pays ou agence émettrice)

### **FR38**

- Numéro de vol : Air France Flight FR38

### **125Y14C**

- Informations tarifaires et siège :
  - **125** : code tarif / compagnie émettrice (format interne billet électronique)
  - **Y** : classe économique (Economy)
  - **14C** : siège 14C

### **04210063026246200**

- Identifiant billet électronique / numéro de document de transport
- Sert à retrouver le billet dans le système de la compagnie

Plusieurs informations sont intéressantes, mais il semble surprenant de ne pas voir figurer directement les aéroports de départ et de destination. Partant du numéro de vol indiqué, nous complétons : le vol FR38 correspond à une ligne Manchester/Limoges.



# Ryanair 38

RYR38 / FR38

[Optez pour une mise à niveau pour voir le numéro de la queue et l'indicatif ATC](#)

**ATTERRI IL Y A 1 HEURES 28 MINUTES**



MAN  
**MANCHESTER, UNITED KINGDOM**

quitte **PORTE 50**  
[Manchester - MAN](#)

LIG  
**LIMOGES / BELLEGARDE, FRANCE**

a atterri à  
[Limoges-Bellegarde - LIG](#)

D'ailleurs, en faisant quelques recherches complémentaires sur la constitution du code donné, on confirme que MANLIGFR indique en réalité l'aéroport de départ Manchester=MAN et de destination Limoges=LIG en France FR

🚩 **Flag :** FR38

🚩 **Flag :** Manchester

🚩 **Flag :** Limoges



# Money for Nothing

## Money For Nothing

Pour sortir un album, il faut bien des finances...

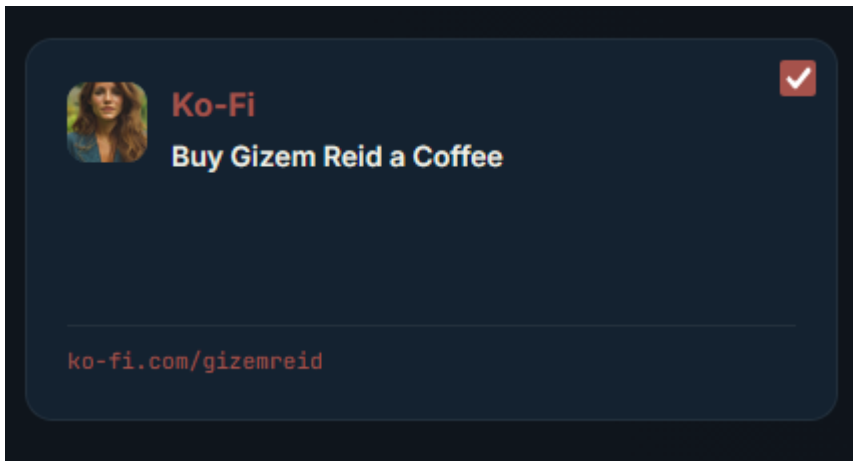
### 8. In da club

#### In da club 70 pts (-2/err)

Intéressons nous à notre chanteuse et sa présence en ligne. En grattant un peu, vous tombez sur un compte ouvert sur  , sous le pseudonyme  . Probablement pour partir à la pêche aux mécènes.

On laisse les dernières informations trouvées pour revenir à Gizem. La dernière découverte avec son Instagram, nous fournissait un pseudo à partir duquel nous pouvons effectuer une recherche.

Évidemment, notre préférence va à un support outils qui permet de faire ce travail (<https://osintisnotacrime.com>), avec de très bons résultats. En plus des tokens étaient offerts dans le cadre de la participation à ce ctf.



🚩 Flag : `Ko-fi`

🚩 Flag : `gizemreid`

Elle y sollicite des contributions pour financer son projet d'album. Rien que de très banal — sauf quand on regarde la liste des donateurs de plus près.

Parmi eux, un certain   lui a versé  .



Il y a effectivement eu un don :



**couleraoul** bought a coffee



Ξέρεις πολύ καλά ότι είμαι ο πιο πιστός σου θαυμαστής ❤️ και ότι η μουσική σου 🎵 μπορεί να αφυπνίσει τις συνειδήσεις...

🚩 **Flag :** couleraoul

On a le prix du café

🍵 \$5 each

🚩 **Flag :** 5 dollars

## 9. Mon amie la rose

Et ce pseudonyme-là, on l'a déjà croisé dans notre enquête. Le hasard, décidément, ne fait jamais bien les choses.

### Mon Amie La Rose 40 pts (-2/err)

Le financement de l'album, c'est touchant. Raoul, fidèle au poste, cinq dollars glissés en douce sur le compte Ko-fi de Gizem. On a connu des déclarations d'amour plus romantiques.

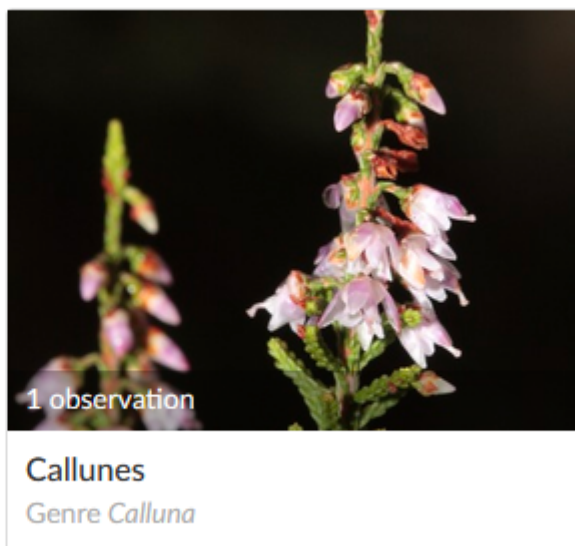
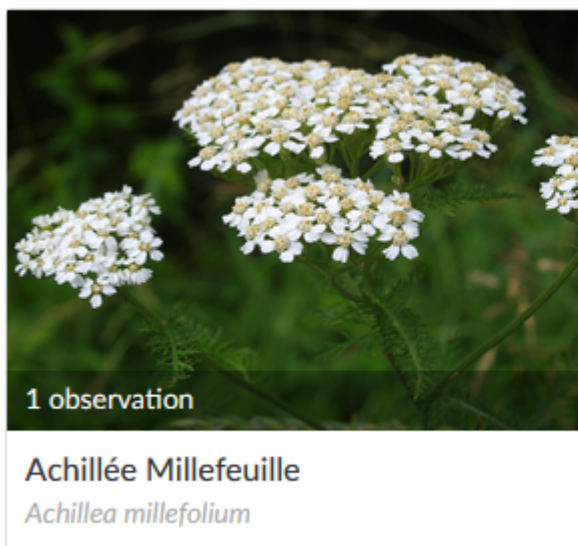
Mais le voyage n'avait rien de sentimental.

En recoupant avec l'étiquette du colis abandonnée dans le cottage avec les sentiers fréquentés par le couple, un schéma se dessine : la collecte de  , aux propriétés analgésiques, faisait partie intégrante de la mission. Visiblement, ses vieilles habitudes ont la vie dure.

On cherche quelle plante peut cueillir Raoul pendant son voyage. On peut imaginer devoir trouver un endroit où il parle donc de ses cueillettes, probablement un site de passionnés de plantes ? Mais pour le moment, nous n'avons qu'une information à son sujet, le pseudo **couleraoul**. On cherche s'il a un compte associé, toujours avec le même outil. On obtient plusieurs réponses, mais une attire particulièrement notre attention : <https://www.inaturalist.org/people/couleraoul>

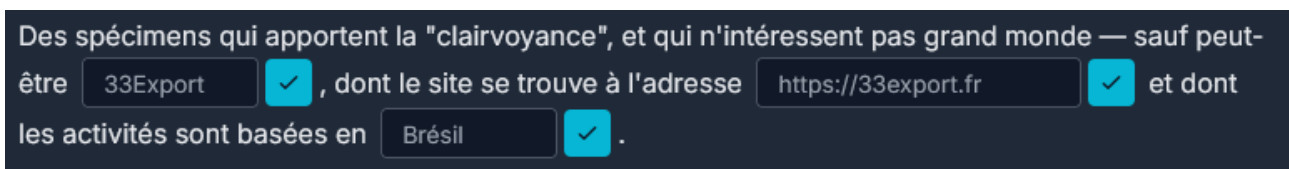


Sur son profil, on constate qu'il mentionne 2 plantes :



Une rapide vérification nous permet d'identifier les propriétés analgésiques de l'Achillee Millefeuille.

**Flag :** Achillee Millefeuille



On fait le lien avec l'étiquette du colis retrouvée au cottage.

**Flag :** Medideal24

Sur google, on trouve le site internet. Au début du CTF il ne ressortait pas forcément dans les résultats, une recherche avec whoxy était plus efficace.



Flag : <https://medideal24.eu/>



Flag : [Slovénie](#)

## 10. Magnolia for ever

### Magnolia For Ever 60 pts (-2/err)

Et voilà. Raoul n'est jamais bien loin d'une belle affaire.

Vous remontez la piste professionnelle. Depuis sa "disparition", il a vite retrouvé chaussure à son pied : il occupe désormais le poste de " ✓" au sein d'une société fondée par  ✓.

Sur la page "about" de Medideal24, on peut trouver cette photo avec les informations nécessaires :



 **medideal24.eu**  
Natural health supplements · EU shipping

Front : Raoul R. : senior herbal advisor / Ludvik Ogrizek : founder and CEO /  
Maja Kovač : Head of Product & Formulation

Back : Tomaž Breznik : Operations & Logistics / Ana Štrukelj : Customer Care & Wellness Advisor /  
Nataša Vidmar : Regulatory Affairs & Quality Control / Petra Zupančič : Digital Marketing & Content

🚩 **Flag :** senior herbal advisor

🚩 **Flag :** Ludvik Ogrizek

Quelques croisements de profils plus tard, on identifie le point de contact d'origine. Les deux hommes se seraient connus à   — une de ces coïncidences qui ne surprennent plus personne à ce stade de l'enquête.

Il faut de nouveau se souvenir des médileaks précédents. On a des informations sur Ludvik, qui permettent de deviner où il a pu rencontrer Raoul : à Chypre pendant leurs études.



## Ludvik Ogrizek

### Founder & CEO

🎓 Pharm.D. — University of Ljubljana, Faculty of Pharmacy (1999)

🎓 Postgraduate Diploma in Pharmacy & Herbal Medicine — Cyprus International University – CIU (2022)

📍 Former head pharmacist, Lekarna Ogrizek, Šiška, Ljubljana

🏠 Co-Founder Veda Medical Data School

🏠 Founded Medideal24 in 2019

### Formations



#### Certification de Nutrioniste Holistique

2023

- Institut Européen de Diététique et Micronutrition (IEDM)
- Mentor et superviseur



#### Diplome de Pharmacien

2019-2022

- Université internationale de Chypre (CIU)
- These sur l'histoire du paracetamol
- Specialisation en bandages

🚩 **Flag :** Cyprus International University

Le fondateur ne s'arrête pas là. Il cumule avec une activité de   au sein de  , dont le site est accessible à l'adresse  .

Au même endroit :

🚩 **Flag :** cofondateur

🚩 **Flag :** Veda Medical Data School

Le site internet de cette école semble plus difficile à trouver. Rien ne ressort de convainquant avec des recherches simples. On va donc utiliser une autre méthode. Partant de l'hypothèse que le site internet de cette école doit contenir le nom de l'école, nous faisons une recherche sur Whoxy (<https://www.whoxy.com>).

Domain Keyword



Veda seul remonte plusieurs milliers de réponses. On essaye en ajoutant un mot vedamedical. Tout en bas nous avons bien une réponse :

14

[vedamedicaldataschool.eu](https://vedamedicaldataschool.eu)

**Flag :** `[https://vedamedicaldataschool.eu](https://vedamedicaldataschool.eu/)`

Une école. Un labo. Un pseudo-directeur médical au casier bien garni. Le tableau commence à prendre forme.



# L'école du Micro d'argent

## L'école du micro d'argent

C'est du Erasmus !

### 11. Je fais mon job a plein temps

#### Je fais mon job à plein temps 30 pts (-2/err)

Tiens, tiens. Une école de Data Analysts en Slovénie. Le site est en ligne, les pages "équipe" et "programmes" parfaitement à jour. Et un nom finit par sortir du lot.

Raoul s'y est dégotté une nouvelle vocation. Il y gère le

Music in Noisy Concerts and Bands



, sur une durée de

3 heures



. Son adresse

de contact professionnelle est

joe@lacombine.fr



.

On étudie ce nouveau site. La page about qui présente l'équipe ne mentionne pas Raoul. Nous regardons la page programme. On ouvre patiemment chaque syllabus pour découvrir le nom de Raoul sur le dernier (ou alors une intuition, confortée par le format de flag, vous a fait cliquer en premier, sur le dernier document, ça arrive et ça fait gagner du temps).

#### • ADVANCED

### Ethics of Medical Data & AI

Frameworks for algorithmic fairness, informed consent for data reuse, ethics committee submissions, dual-use risks and whistleblowing protections in health data contexts.

 2 months

 Hybrid

 Certificate

### Faculty

**Dr. Lidija Podkrajšek** - Lead instructor and module director

**Sara Robič** - Legal and regulatory sessions

**Dr. Balázs Horváth** - Technical fairness sessions

**Raoul Reidid (ext)** - Pharmaceutical usage of AI and Data Ethics ([ethicspharma-external@vedamedicaldataschool.eu](mailto:ethicspharma-external@vedamedicaldataschool.eu))



Flag : `Ethics of Medical Data & AI`

Flag : `2 mois`

Flag : `ethicspharma-external@vedamedicaldataschool.eu`

## 12. The Teacher

Pharmacien raté, pseudo-médecin, vendeur d'huiles magiques, directeur médical fantôme, et maintenant formateur. La reconversion est totale.

### The Teacher 50 pts (-2/err)

Vous remontez son contrat. Raoul est employé depuis  , et il a été recruté directement par  pour encadrer les " " avec les  .

Mais dans quel but, exactement ?

Quel est son nouvel objectif ?

Dans quel état j'erre ?

La réponse à ce challenge ne se trouvait pas directement sur le site de l'école. Même en fouillant sur le site nous ne trouvons pas de contrat lié à Raoul. Cependant, pendant les recherches, un élément doit attirer notre attention :

**Dr. Lidija Podkrajšek**  
FOUNDER & DIRECTOR

Clinical informatician and epidemiologist. Former EMA consultant. 18 years of experience in clinical data governance and health registry management across six European countries.

 `3b310974-4162-4b60-89cd-398dae462623`

Parmi les informations sur la fondatrice de l'école, on trouve un code très particulier. Si on se rappelle bien ce qu'on a lu avant de commencer ce CTF, ce code indique la possibilité d'entamer une discussion avec la personne. Nous nous rendons donc dans l'outil "Interrogatoires" pour entamer une discussion avec Lidija. Cette pauvre femme aura supporté l'agacement, la colère, les insultes, des joueurs pendant dix jours. Mais avec une bonne approche, elle finit par transmettre les informations utiles sur le contrat de travail de Raoul.

Flag : `8 mois`



Flag : Ludvik Ogrizek

Flag : Ateliers Datalake

Flag : apprentis

## 13. Étudiant poil aux dents

Mais dans quel but, exactement ?

Quel est son nouvel objectif ?

Dans quel état j'erre ?

**Étudiant poil aux dents** 70 pts (-2/err)

Remarquons au passage la fatigue qui se fait ressentir chez les concepteurs du CTF...

Cette école mérite qu'on s'y attarde un peu plus longuement. Notamment du côté des élèves.

En parcourant la liste des étudiants, déniché sur  , un profil sort du lot :  .

On s'intéresse à présent aux élèves. Une page leur est dédiée :

PROGRAMMES	SCHOOL	CONTACT
Clinical Data Management	About Veda	Njogoševa ulica 12
Health Informatics	Faculty	1000 Ljubljana
Medical AI	Accreditations	Slovenia
Biostatistics	<b>Student Portal</b>	
GDPR & Compliance	Careers	+386 1 234 5678 info@vedamedicaldataschool.eu

Une autre méthode (qui s'avérait bien utile par la suite), était de chercher les sous-domaines (par exemple avec <https://platform.censys.io>), qui faisaient ressortir le sous-domaine pour les étudiants, ainsi qu'un autre sous-domaine qui ne nous servait pas (pas encore...).

```
web.endpoints.hostname      student.vedamedicaldataschool.eu
web.endpoints.http.body    tps://git.vedamedicaldataschool.eu/explore/u
```

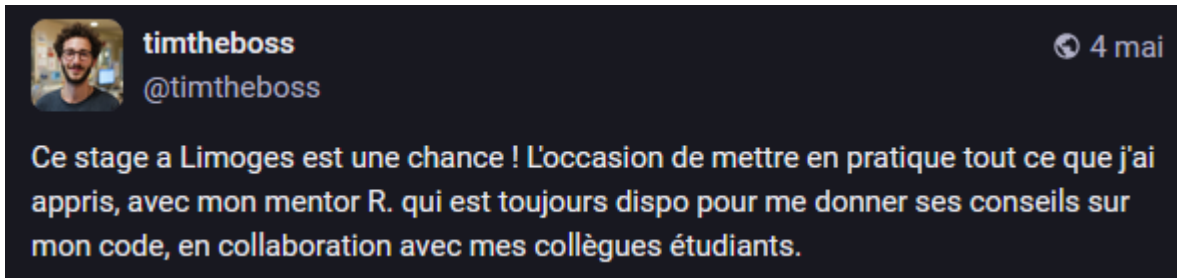
Flag : <https://student.vedamedicaldataschool.eu>

Nous partons donc ensuite faire la découverte de ces étudiants. Le rapport nous informe qu'un des profils doit sortir du lot. Si on fait bien les choses (pas comme certains qui vont trop vite parce que



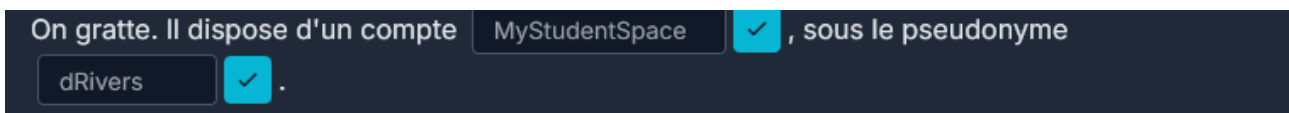
tout est trop facile), on va ouvrir chaque lien vers un profil de réseau social, regarder chaque post pour essayer de voir ce que l'on est censé voir. Il y a beaucoup de pièges, qui heureusement de mènent jamais bien loin. Par contre effectivement, un profil semble bien plus intéressant que les autres : <https://mastodon.social/@timtheboss>

On constate qu'il mentionne être en stage (ah, ces courageux stagiaires dévoués...), à Limoges, et surtout il indique que son mentor serait un certain R.



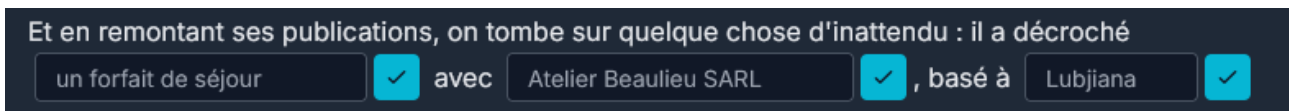
Plusieurs indices qui semblent bien le lier à notre enquête.

🚩 **Flag :** **Thimothé Valleurant**



🚩 **Flag :** **Mastodon**

🚩 **Flag :** **timtheboss**



🚩 **Flag :** **une convention de stage**

🚩 **Flag :** **Limoges**

Mais impossible de mettre la main sur l'entreprise où il fait son stage... Il va falloir trouver une autre source d'information.

Si on a bien fait son travail en analysant le site de Veda, on a traduit la page et on se rappelle avoir vu un lien qui ne fonctionnait pas :





Ça serait pourtant parfait pour nous : une convention de stage indique le nom de l'entreprise. On peut alors se douter que si tout le reste fonctionne si bien, il y a quelque chose à creuser du côté de cette API.

On passe sur un challenge un peu plus technique : on ouvre la console et on observe les erreurs.

```
XHR GET https://student.vedamedicaldataschool.eu/api/v1/conventions [HTTP/3 500 39ms]
[VEDA] /api/v1/conventions: ENOENT: no such file or directory, scandir '/srv/veda-alumni/public/documents/conventions'
dent.vedamedicaldataschool.eu:489:15
```

On a un chemin d'accès, on peut essayer à partir de l'URL. Sans être expert, on tâtonne et on trouve : <https://student.vedamedicaldataschool.eu/documents/conventions>

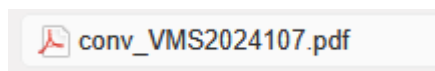
Une grande grande liste de conventions de stage... Si on ne veut pas toutes les vérifier (ou demander à son copain Claude), on peut constater que le n° indiqué sur la convention, correspond au n° sur la vignette de l'étudiant. On cherche le n° de Tim :

VMS-2024-107

**Thimothé Valleurant**

GDPR in Healthcare

Et donc on ouvre sa convention de stage :



**Gostiteljska organizacija**

NAZIV PODJETJA

LabAurence SELAS

🚩 **Flag :** LabAurence SELAS



# Antisocial

## Antisocial

On peut ne pas être d'accord, mais au moins on peut débattre non ?

### 14. Message in a bottle

#### Message in a Bottle 60 pts (-2/err)

Vous quittez la Slovénie pour les réseaux sociaux. Et là, le projet ne laisse personne indifférent : deux camps s'affrontent à coups de mots-dièses.

D'un côté, le hashtag  , brandi par les *partisans*. De l'autre,  , étendard des *opposants*. Les deux camps croisent le fer sur  .

On retourne sur les réseaux sociaux, en partant du compte de Tim. Parmi ses messages, un seul contient un tag.

🚩 **Flag :**

On clique sur le tag pour voir qui d'autre l'utilise, et on découvre tout un nouveau réseau qui semble cette fois opposé au datalake.

🚩 **Flag :**

🚩 **Flag :**

Vous lisez les fils, vous remontez les threads. Parmi les voix contre, l'une se distingue par son volume sonore, et son expérience de vie. Le compte   ne mâche pas ses mots, et le fait savoir avec une certaine régularité.

Derrière le pseudo, un nom :  . Visiblement très remonté sur le sujet, au point d'animer un site dédié, accessible à l'adresse

.

Plusieurs personnes font partie de ce mouvement. Mais parmi des posts relativement généralistes, un compte semble bien plus impliqué :



**HP Girolles**

@hpgirol

4 mai \*


Depuis quelques temps, j'ai l'impression d'être suivi...  
A tel point que j'ai toujours mon téléphone prêt à prendre une photo !

Hier soir, en sortant de chez des amis à côté de Limoges, j'ai été frôlé de manière  
parfaitement volontaire par un énorme 4x4 !  
Je ne me laisserai pas intimider !



Flag : @hpgirol





## HP Girolles

@hpgirol@mastodon.social

Suivre

...

Abonné-e-s  
**0**

Abonnements  
**0**

Messages  
**5**

Ici depuis  
**24 avr.**

Retraité de l'Éducation nationale. Ancien conseiller communautaire en Haute-Vienne. Je partage ici ce que je vois depuis mon village du Pays de Limoges : école, ruralité, services publics, et de plus en plus — souveraineté de nos données. Sans étiquette, sans chapelle. Mes billets longs : pierrehenrigirolles.wordpress.com

Site personnel  
[henripierregirolles.wordpress....](https://henripierregirolles.wordpress.com)

🚩 **Flag :** Henri Pierre Girolles

🚩 **Flag :** <https://henripierregirolles.wordpress.com>

## 15. Every Breath You Take

### Every Breath You Take 100 pts (-2/err)

Henri-Pierre n'a pas que des fans. Il s'est fait suivre par un véhicule Alfa Romeo ,

immatriculé AA-000-AA , de couleur Violette . Discret comme un éléphant dans un couloir.

Il a réussi à prendre une photo. Voici l'endroit :

On reprend le post où HPG mentionne l'incident :

🚩 **Flag :** Range Rover

🚩 **Flag :** LE-003-AK

🚩 **Flag :** noire

Il faut ensuite localiser l'endroit d'où a été prise la photo. On identifie une station Esso, et il mentionne être à proximité de Limoges. Sur Maps, on cherche les stations Esso dans un périmètre autour de la ville :



Il y en a peu, on commence par celles là et on pourra élargir si nécessaire. Un passage par Street View confirme la station correspondante, et nous permet de placer précisément le point à l'emplacement de la prise de la photo.

**Flag :** 45.865710, 1.238140

Et comme si cela ne suffisait pas, il a aussi reçu un appel anonyme. Un appel de menace, pour être précis.

Au bout du fil, du silence, puis quelques mots. La géolocalisation du correspondant fait sortir un lieu peu banal : l'auteur de l'appel se trouvait à proximité des  .

Sur le site de HPG, un article mentionne effectivement un appel téléphonique :

AVRIL 8, 2026

## Un message sur mon répondeur

Je vais vous raconter ce qui s'est passé hier soir, parce que je crois qu'il est de mon devoir de citoyen de le porter à votre connaissance, plutôt que de garder ça pour moi par pudeur ou par crainte. Et parce que je sais aussi, par expérience, que ce qui se tait grandit dans l'ombre,...

En fin de texte, il semble qu'on aurait dû trouver le message mais qu'il n'a pas pu être chargé :





Les hypothèses les plus plausibles sont :

### 1. Tir de carrière / mine à ciel ouvert

- Une sirène retentit quelques minutes ou secondes avant le tir.
- L'explosion a lieu à heure fixe.
- Les riverains sont prévenus à l'avance.
- Très fréquent dans les carrières, mines et certains grands chantiers.

### 2. Destruction contrôlée d'un bâtiment

- Sirène de sécurité.
- Compte à rebours connu.
- Forte explosion parfaitement planifiée.

### 3. Exercice militaire ou champ de tir

- Signaux sonores avant les détonations.
- Horaires publiés ou réguliers.

### 4. Essai industriel

- Certaines usines ou installations portuaires utilisent des sirènes avant des opérations bruyantes ou dangereuses.

On peut penser à chercher des déclarations officielles, des arrêtés préfectoraux, des événements partagés sur des réseaux sociaux... qui pourraient mentionner des explosions avec des date set horaire précis. On peut sinon essayer de prendre un peu de recul, et se demander ce qui se passe lors d'une telle explosion. On peut penser alors explosion  $\Rightarrow$  grosse vibration. Et se demander s'il existerait des relevés sismiques même pour des événements hors gros tremblements de terre.

Sinon, encore une fois, demander à l'IA par quel moyen on pourrait localiser ce genre d'événement. Et oh surprise, elle nous donne quelques pistes intéressantes :

### 1. Chercher les tirs de carrière/mines

C'est souvent la première piste à vérifier.

Les carrières publient parfois :

- leurs horaires de tirs,
- des arrêtés préfectoraux,
- des études d'impact mentionnant les créneaux habituels.

### 2. Examiner les bases de données d'événements sismiques

Une explosion importante peut être enregistrée.

Selon le pays :

- réseaux sismologiques nationaux ;
- catalogues d'événements industriels ;
- stations universitaires.

Même un tir de carrière peut apparaître comme un événement sismique de faible magnitude.



### 3. Rechercher les démolitions contrôlées

Pour une date et heure précises :

- presse locale ;
- réseaux sociaux ;
- vidéos publiées le jour même.

### 4. Chercher les zones militaires

De nombreuses bases annoncent leurs exercices :

- calendriers de tirs ;
- NOTAM (aviation) ;
- avis aux navigateurs ;
- communiqués municipaux.

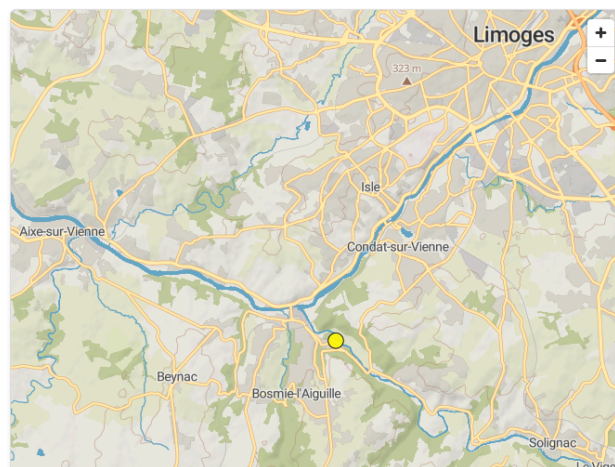
La deuxième piste est la plus intéressante puisqu'elle s'intéresse au phénomène sans devoir au préalable partir sur une hypothèse quant à l'origine de l'explosion. Et effectivement, on peut trouver un site qui relève les événements sismiques en France. En remontant l'historique, on trouve alors un tir de mine à proximité de Limoges, exactement au jour et à l'heure du message : <https://renass.unistra.fr/fr/evenements/fr2026tlllylg>. On obtient même la confirmation qu'il s'agit d'un tir de mine, avec une localisation approximative. Il suffit alors d'identifier la carrière dans ce secteur.

Accueil / France hexagonale / Évènement fr2026tlllylg

✓ Cet événement a été révisé et confirmé par un analyste.

Type	Tir de carrière
Magnitude	1.8 MLv
Date et heure locales	2026/04/07 13:33
Temps universel	2026/04/07 11:33
Latitude	45.78 ° ± 0.1 km
Longitude	1.21 ° ± 0.1 km
Profondeur	0 km (operator assigned) ± 0.0 km

Voir le sismogramme de cet événement.



#### 🚩 Flag : Carrières de Chambon

Le fait qu'exactement le même jour, à la même heure, un décollage de fusée ait eu lieu était une coïncidence incroyable que nous avons découvert en cours de CTF... On aime voir souffrir les joueurs, mais on n'est pas aussi sadique quand même (l'histoire ne dira pas si on avait découvert le décollage de la fusée avant le ctf, aurait-on vraiment modifié le message ? ou simplement laissé en l'état avec un petit sourire aux lèvres imaginant le piège supplémentaire offert par le hasard).

Vous remontez la propriété du terrain. C'est une parcelle qui appartient à la

SARL Jojo Depanneur



!

Louis LABROCANTE



serait donc derrière les menaces

visant Henri-Pierre.



À ce moment de l'enquête, petite entourloupe : nous n'avions pas encore les éléments pour trouver ces réponses. Cela devait inciter à porter notre attention sur un autre rapport déverrouillé un peu plus tôt.



# Hygiaphone

## Hygiaphone

Plus on crie plus fort, moins ça fait du moins de bruit. (Normalement.)

### 16. Undercover of The Night

#### Undercover of the night 60 pts (-2/err)


Henri-Pierre n'est pas seul à se sentir concerné. Vous fouillez les threads, et il apparaît qu'un collectif s'est constitué autour de cette histoire de données de santé.

Au cœur du dispositif, un média :   , qui publie régulièrement sur son site

.

Nous retournons donc à Mastodon et portons notre attention aux autres profils partageant le même tag. Pour compléter le rapport, nous devons trouver un média qui évoquerait donc toute cette thématique. Parmi les divers posts, deux messages attirent notre attention, ils mentionnent tous les deux le même média :



 **Kel** @K\_el\_M 5 mai \*

Enfin des gens sérieux, qui publient des articles vraiment importants sans se laisser tenter par l'appât du gain. Tout le monde devrait les connaître !

Santé Éthique : un magazine collectif et indépendant, animé bénévolement.

 **amelimelimelo** @amelimelimelo 6 mai

un article intéressant que je conseille à tout le monde de lire : [santethique.eu/article/pseudon...](https://santethique.eu/article/pseudon...)



santethique.eu

**Ce que « pseudonymisation » veut dire — et ce ...**

Le magazine militant de la confidentialité des données de santé

Flag : Santé Éthique

Flag : <https://santethique.eu>

Vous parcourez les signatures. Tiens, tiens. Une certaine Sylvaine  s'intéresse elle aussi à Bernard  et à son dernier voyage...

Saura-t-on l'identifier ?

On identifie cet article qui mentionne le voyage de Raoul

## Sur la piste de R.R. jusqu'aux Hébrides

20 mars 2026 · par Cynthia

Le ferry de Mallaig accoste à Armadale en quarante minutes par temps calme. En avril, il n'y a jamais vraiment temps calme sur le Sound of Sleat. J'ai passé la traversée à regarder les crêtes de Skye se découper dans un ciel couleur zinc, à relire mes notes, et à me demander ce q...

[Lire la suite »](#)

[ENQUETE-TERRAIN](#) [ROYAUME-UNI](#) [PHARMACIE-EN-LIGNE](#) [DONNEES-DE-SANTE](#) [IOT](#) [R.R.](#)

Flag : Cynthia



## Flag : Raoul

On nous demande d'identifier cette Cynthia, il semble donc qu'on l'ait déjà croisée avant dans notre enquête, probablement sans nous en rendre compte. Si vous n'avez pas tiqué sur elle dès le début du ctf, c'est le moment de repasser en revue les éléments rassemblés autour du séjour à

🎵 FLOOODIGARRRRY 🎵

🎵 FLOOODIGARRRRY 🎵

Ce photographe, n'y avait-il pas un portrait sans nom avec ce commentaire qui aurait pu (du) éveiller notre curiosité ?

### Unknown

She did not want me to give me her name but she loved the portrait. French women with grits and something to fight for... or against. She told me she 's a journalist, investigating a man with some shady past in medical area...

Nous proposons donc la photo de cette jeune femme, et effectivement, nous avons bien identifié Cynthia

C'est bien elle ! Il ne reste plus qu'à entrer en contact. L'adresse :

🐾 une-serie-de-chiffre-de-et-de-lettres



On doit donc trouver comment entrer en contact avec elle. Sur le site de Santé Ethique, dans la rubrique "nous contacter", on retrouve le code :

#### NOUS ÉCRIRE

**Vous êtes salarié-e d'une mutuelle, d'un organisme de crédit, d'un laboratoire d'analyses, d'une institution de santé ? Vous avez connaissance de pratiques contraires au RGPD ou à l'éthique médicale ? Écrivez-nous.**

#### Notre messagerie sécurisée :

🐾 a58d39a5-2f75-4d4e-868f-de8f56144720

Mais attention piège ! avant d'entrer le flag, il fallait s'assurer si c'était bien Cynthia qui nous répondrait. Et évidemment... non...

Nous tombons sur quelqu'un de la rédaction, qui fait bien son boulot de protection des journalistes. Il faudra ruser ou simplement trouver les bons mots, pour la convaincre de nous fournir le code pour contacter Cynthia directement.



Flag : `fcdc2497-164d-40fc-a153-31150f6f7e200n`

## 17. (I cant't Get No) Satisfaction

### (I Can't Get No) Satisfaction 50 pts (-2/err)

Le contact est établi. Cynthia répond vite, et ne tourne pas autour du pot : elle aussi est sur le dossier.

Elle confirme que `The Real Social Academy` ✓ cherche à s'implanter à `Brazilia` ✓, mais que le projet semble sérieusement compromis.

On discute avec Cynthia, avec un write-up sous la main pour pouvoir répondre facilement à ses questions, et elle nous fournit rapidement les informations dont on a besoin.

Flag : `Veda Medical Data School`

Flag : `Limoges`

Pour étayer son propos, elle vous oriente vers un document plutôt édifiant publié par

`Juste Leblanc` ✓ .

Flag : `Henri Pierre Girolles`

Et avant de raccrocher, elle glisse une dernière information : `Dominique` ✓ n'est pas un acteur secondaire dans cette histoire — car `sa communauté` ✓ est richissime.

Flag : `Gizem`

Flag : `sa famille`



# Ya Foye

## Ya foye

Y'a pas à dire ! On est bien tous ensemble non ?

## 18. Under Pressure

### Under Pressure 100 pts (-2/err)

Vous cherchez le document évoqué par Cynthia. Henri-Pierre Girolles y a publié une résolution faisant capoter le projet d'implantation de la Veda Medical Data School à Limoges !

À la lecture, le montage financier devient lisible : l'école devait apporter   en fonds propres et un engagement de   via  .

On retourne sur le site de HPG. Dans un de ses messages, on trouve un document à télécharger <https://henripierregirolles.wordpress.com/2026/01/16/le-projet-de-campus-veda-abandonne-une-bonne-nouvelle-ou-presque>

[projet\\_resolution\\_2025-12-15](#)

Télécharger

🚩 Flag :

🚩 Flag :

🚩 Flag :

Ils s'appuient sur une structure luxembourgeoise identifiée comme étant

🚩 Flag :



Mais le plus intéressant reste à venir, vous tombez sur une opération qui vous donne plus d'infos sur une personne que vous pensiez être une victime depuis le début : Michel Sardou ✓, de STAVROS & LYNCH PARTNERS LTD, a fait un pret ✓ à Marcel Cerdan ✓ portant sur 99 blocks ✓ de la SARL Camping Natura ✓, située à

Rechercher un lieu ou saisir des coordonnées (lat, lng)...

Il semble que nous devons trouver d'autres sources d'informations. Nous venons de trouver des noms de société. Une douce comptine nous revient à l'esprit <https://soundcloud.com/oscar-zulu-rhino/rhinocorp-siret>

Après avoir entonné gaiement le refrain, nous allons donc porter notre regard sur ce site. Rien sur Stavros, mais nous avons bien une réponse pour Limousin Holding mais nous ne pouvons pas y accéder car hors registre français, ainsi que la mention d'une banque jusqu'alors inconnue.

LIMOUSIN HOLDING SA Rechercher

2 résultats

**Limousin Holding SA** Étranger · LU  
*pas de SIREN (hors registre FR)*

**Crédit Briance & Vienne** Active >  
SIREN 492375821 87000 Limoges Autre distribution de crédit

Alors qu'on pensait suivre une piste toute tracée, on ne trouve malheureusement rien de cette façon. Reprenons un peu plus haut. Nous revenons aux recherches plus habituelles et trouvons le site internet de Stavros (par google) <https://stavroslynch.com/>

Restant accroché à l'idée que rhinocorp était quand même bien tentant à ce moment du ctf, nous testons les noms mentionnés sur le site de Stavros. Des 4, un nom nous donne un résultat !



Rechercher

1 résultat

**Nicosian Holding** Active

SIREN 994634087 87920 Condat-Sur-Vienne Supports juridiques de gestion de patrimoine immobilier

>

Nous regardons les éléments disponibles, et on trouve notamment un acte de donation qui semble bien répondre à nos besoins pour le rapport.

- Flag :** Despina Kyparissidou
- Flag :** une donation
- Flag :** Gizem IHANET
- Flag :** 20 parts
- Flag :** SCI NICOSIAN HOLDING
- Flag :** 45.787190, 1.228323

... Vous comprenez peut-être mieux certaines allusions.

Petite remarque au passage : oui une donation est bien différente d'un don.

*Don et donation désignent tous deux le fait de transmettre un bien gratuitement, mais en droit français, la donation est un acte juridique formel (souvent devant notaire) qui organise la transmission de son vivant. Le don est un terme plus général, souvent utilisé pour des remises de faible valeur ou à des associations. En pratique, toute donation est un don, mais tous les dons ne sont pas des donations au sens juridique.*

À ce moment de l'enquête, on peut poursuivre sur le même rapport, ou alors l'étude de cette SCI nous fait découvrir un élément intéressant : un des terrains est situé juste à côté des carrières près desquelles l'appel téléphonique à HPG avait été passé. Les deux progressions étaient possibles, pour le write-up, faisons le choix de garder cette information de côté, et de continuer le rapport.

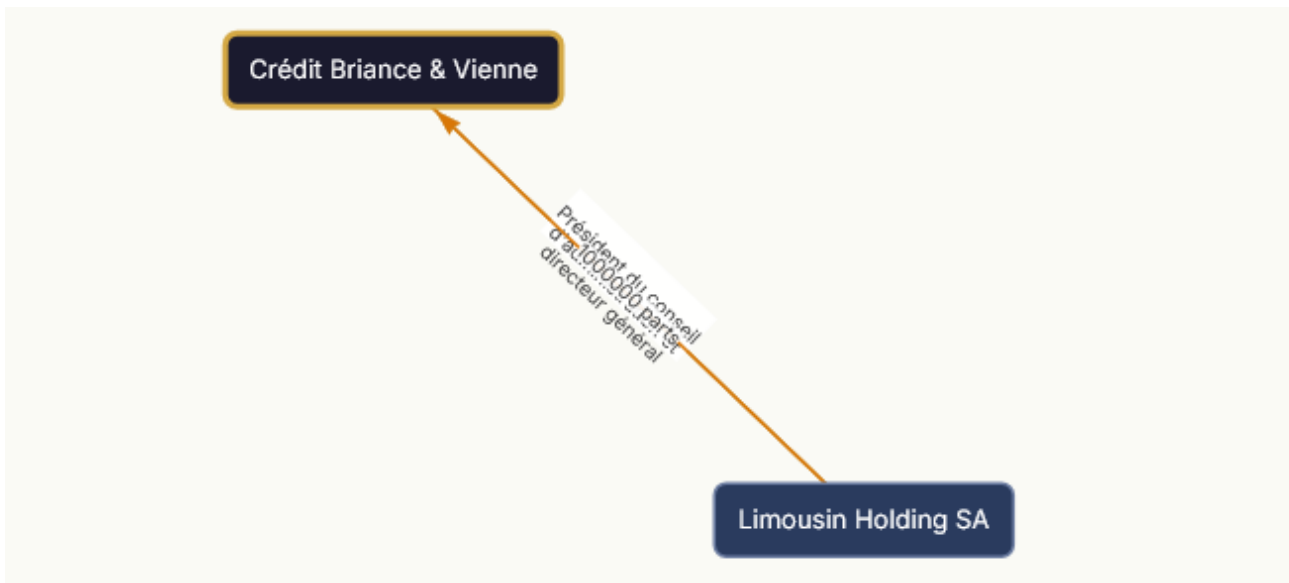


## 19. Gold Digger

### Gold Digger 20 pts (-2/err)

Vous repartez sur les registres. Et là, surprise : la filiale évoquée plus haut porteuse du projet d'école dirige également  ✓ .

On revient donc sur Limousin Holding et l'information trouvée précédemment :



🚩 **Flag :**

Une banque locale, à l'ancienne, avec son site internet à l'adresse

✓ .

Recherche google simple, ou whoxy



Crédit Briance <sup>6</sup>  
Vienne

Le crédit qui vous connaît

Nos crédits

Comment ça marche

Notre histoire

Avis clients

Contact

Espace client

Simuler mon prêt

LIMOGES · HAUTE-VIENNE · DEPUIS 1927

# Le crédit qui vous connaît, vraiment.

Prêt personnel, travaux, auto, rachat de crédit. Depuis bientôt cent ans, nous finançons les projets des Limousins avec l'attention qu'on réserve aux voisins – parce que c'est exactement ce que nous sommes.

Simuler mon prêt en 2 minutes

Découvrir nos offres

“  
Ma conseillère m'a appelée dès le lendemain. On a pris le temps. J'avais mon accord le vendredi.”

SM Sylvie M.  
Panazol - Prêt travaux 18 500 €

Flag : <https://briancevienne.fr>

## 20. Around The World

### Around the World 80 pts (-2/err)

Reste à comprendre ce que vient faire Labaurence dans cette galaxie.

Quelques requêtes plus tard, vous identifiez un site de données qui leur appartient :

On revient sur Labaurence. Recherche google simple, ou whoxy et on trouve le site internet de ce labo : <https://labaurence.fr>

On comprend qu'on doit probablement trouver un sous-domaine. Petite recherche sur Censys

RESULTS: 9 • DURATION: 1.52s

**datalake.labaurence.fr: 80** • WEB PROPERTY

Flag : <https://datalake.labaurence.fr>

Les données sont anonymisées. C'est la moindre des choses pour un datalake de recherche orienté santé.

Sauf qu'en ouvrant le fichier au format  , un détail vous saute aux yeux.



On explore un peu le site. On trouve un fichier à télécharger.

## Telecharger le jeu de donnees

Disponible au format Apache Parquet — compresse, type, pret pour l'analyse.

APACHE PARQUET

**analyses\_sanguines\_87.parquet**

~10 Mo

**Telecharger**

🚩 **Flag :** `parquet`

En croisant avec `le nouveau testament` , l'anonymisation tombe comme un château de cartes : on parvient à retrouver qui se cache **derrière chaque ligne de données !**

**NDLR :** *Spammer une API n'est pas considéré comme une méthode valable, et conduira à un ban immédiat*

Pour ce flag, il faut un peu s'extraire du ctf et réfléchir à ce qui nous est demandé. On a trouvé tout un jeu de données anonymisées, et on devrait pourtant pouvoir les désanonymiser. En analysant la constitution de l'identifiant, on repère déjà quelques informations : le début indique le laboratoire concerné et la date du prélèvement.

`SJU0012025112384e4b9d14a3878a52`   `2025-11-23`   `LAB-SJU-001`   Laboratoire BioVienne Saint-Junien

Quelles informations nous seraient nécessaires pour identifier un patient ? On peut penser aux grands classiques : nom, prénom, date et lieu de naissance. Des informations générales d'état civil. Et où pourrait-on obtenir ce genre d'informations ? Si on a bien fait son travail, on devrait avoir fait le tour de l'atelier d'enquête avant de se lancer bille en tête dans le ctf. Ça serait le moment de se souvenir des documents qui étaient mis à disposition dès le début !

### Listes électorales

📄 12.9 MB   👁 1568   **CTF**

🚩 **Flag :** `les listes électorales`



Démonstration : `PAN00120231031bd7e8d30bd0a56ff8`` correspond en clair à

Mireille DARC  , qui habite à La Paz  .

Le système est purement et simplement **corrompu**.

Ça devient plus sérieux, on doit à présent démontrer qu'on est capable de désanonymiser la liste. On sait comprendre le début de l'identifiant, mais la suite de lettres et de chiffres semble bien coder les informations d'état civil qui nous permettraient de faire le lien. Il faudrait donc que l'on puisse avoir accès à la clef qui a permis de générer l'identifiant, et une explication des informations qui le constituent.


Où pourraient être ces informations ? On se souvient qu'on est sur le site de Labaurence, où on connaît justement un stagiaire qui saurait développer ce genre de code. On sait que les dev utilisent souvent des dépôts Git, mais on ne trouve rien sur les habituels, il doit donc stocker son code ailleurs. On se rappelle alors qu'il est étudiant, que les écoles mettent souvent quelques outils à disposition des élèves, et que... mais évidemment ! Ce sous-domaine que l'on avait découvert il y a fort longtemps et dont nous n'avions pas eu l'usage !

<https://git.vedamedicaldataschool.eu>


Tickets Demandes d'ajout Jalons Explorateur

Dépôts Utilisateurs Organisations

Thimothé Valleurant

 tvalleurant (Thimothé Valleurant)  
 ✉ t.valleurant@ozmai.leu 📅 Inscrit le 30 août 2025

On trouve bien Tim. On identifie un dépôt qui semble prometteur, qui correspond bien à ce que l'on cherche.

 **lab-data-pipeline**  
 Pipeline de traitement des prélèvements (datalake Labaurence)  
 Actualisé il y a 3 mois

Pipeline de traitement des prélèvements (stage LAB, printemps 2026).

## Modules

- `anonymize.py` : génération du code-barre patient (31 caractères, HMAC).
- `loader.py` : helper de lecture du CSV de résultats.
- `data/resultats_lab0.csv` : résultats analytiques (export LIMS).

[anonymize.py](#) nous explique comment est créé l'identifiant :





3. Compare chaque résultat avec le hash recherché
4. Dès qu'il trouve une correspondance, il affiche le patient associé



```

import pandas as pd
import hmac, hashlib, unicodedata

# CONFIGURATION
SECRET_KEY = "801423438c04143903c48e7a3b8ed0a04dedd58bee66323a86255dbdd53284d2"
CSV_FILE = # Indiquer le chemin vers le CSV avec les patients
PARQUET_FILE = # Indiquer le chemin vers le Parquet contenant les codes-barres
IDENTIFIANT = "PAN00120231031bd7e8d30bd0a56ff8" # L'identifiant complet à rechercher

# PREPARATION DE L'IDENTIFIANT
code_labo_tronque = IDENTIFIANT[:6] # Les 6 premiers caractères pour le labo
HASH_A_TROUVER = IDENTIFIANT[14:30] # 16 caractères du hash après labo + date
code_labo_complet = f"LAB-{{code_labo_tronque[:3]}}-{{code_labo_tronque[3:]}}" #
reconstruction du code labo complet

# NORMALISATION DES DONNEES ET CREATION DU HASH
def normalisation(text):
    if text is None:
        return ""
    text = str(text)
    if text.lower() == "nan":
        text = ""
    text = unicodedata.normalize("NFKD", text)
    return text.encode("ascii", "ignore").decode("ascii").upper().replace(" ", "")

def normalisation_identite(nom, prenom, ddn, code_insee):
    nom_norm = normalisation(nom)
    init_nom = nom_norm[0] if nom_norm else "X"
    premier_prenom = prenom.split()[0] if isinstance(prenom, str) and prenom.strip()
    else ""
    prenom_norm = normalisation(premier_prenom)
    jj, mm, aaaa = ddn.split("/")
    ddn_norm = f"{{aaaa}}{{mm.zfill(2)}}{{jj.zfill(2)}}"
    insee = str(code_insee).replace("com", "").strip()
    return f"{{init_nom}}|{{prenom_norm}}|{{ddn_norm}}|{{insee}}"

def creation_hash(nom, prenom, ddn, code_insee, labo):
    identity = normalisation_identite(nom, prenom, ddn, code_insee)
    message = f"{{identity}}|{{normalisation(labo)}}".encode("utf-8")
    return hmac.new(bytes.fromhex(SECRET_KEY), message, hashlib.sha256).hexdigest()[16:]

# LECTURE DU CSV
df_csv = pd.read_csv(CSV_FILE, sep=';', encoding='utf-8', dtype={"code": str})

```



```
# Extraction du code INSEE depuis l'UGLE
code_insee =str(row["code"]).replace("com","").strip()# Calcul du hash pour cette
ligne
h = creation_hash(
    row["nom de naissance"],
    row["prénoms"],
    row["date de naissance"],
    code_insee,
    code_labo_complet
)if h == HASH_A_TROUVER:print("Code-barre recherché :",
IDENTIFIANT)breakelse:print("Aucun résultat")
```

En tout cas, ça fonctionne. On identifie la personne et on peut aller trouver où elle habite.

🚩 **Flag :** `Aurore Marion`

🚩 **Flag :** `Limoges`

Le système est purement et simplement **corrompu**.

Sacré Tim, pas vraiment un boss... Soit Monsieur `Robespierre` ✓, son prof, est mauvais, soit il a mal noté les cours, mais il a oublié d'utiliser le package `pandas-doc` ✓ (en se fiant aux dernières meilleures pratiques) pour supprimer le fichier `files.txt` ✓ ... Permettant de casser la pseudonymisation.

Sur le Gitea de Tim on trouve le nom de son prof

🚩 **Flag :** `Lemourat`

Encore une fois, si on n'est pas expert de ce domaine, on peut demander un coup de main à l'IA

quel package sur gitea pour supprimer un fichier y compris de l'historique, selon les règles de l'art ?

Pour **Gitea**, il faut être très clair :

👉 **Gitea n'a pas de "package magique" pour supprimer un fichier de l'historique.**

Parce que ce n'est pas Gitea (le serveur) qui gère ça, mais **Git** lui-même.

🧠 **La "règle de l'art" pour supprimer un fichier de l'historique Git**

✅ **Outil recommandé aujourd'hui (standard moderne)**

👉 `git filter-repo` (officiel recommandé par Git)

🚩 **Flag :** `filter-repo`



🚩 Flag : `secret.key`

## 21. BadBank

30 pts (-2/err)

Le laboratoire et la banque seraient donc liés ? Sur le papier, rien ne les rapproche officiellement.

Il faut une preuve matérielle.

Ça tombe bien : ils ont oublié de vider la   . A cheval donné on ne regarde pas l'odeur des dents, ou quelque chose comme ça.

Petite analyse des mots utilisés dans le rapport pour essayer de comprendre ce qu'il faut faire : preuve matérielle, oublier de vider quelque chose, odeur... On pourrait penser à cette expérience originale en début de ctf, ou nous avons pu fouiller pour de vrai une fausse poubelle (ou l'inverse).

On nous parle du labo, et de la banque. On peut essayer d'aller se promener à ces 2 adresses. Le labo ne donne rien, mais la banque permet bien une exploration. Suivant notre instinct, on clique sur la poubelle, et nous découvrons bien quelque chose.

🚩 Flag : `poubelle`



Sur le document référencé   , que vous avez exhumé et reconstitué avec un certain héroïsme, le coût total du crédit accordé au Labaurence s'élève à

.

60 bandelettes de papier... alors oui, encore une fois, certaines équipes confient la tâche à l'IA. Mais franchement, passer à côté d'une activité manuelle en plein CTF, qui s'en passerait ? Les plus traditionnels ont pu imprimer les bandelettes, sortir ciseaux et colle UHU, et reconstituer le document dans le strict respect de l'immersion du jeu (les odeurs de poubelle en moins). Les semi-convertis ont



ouvert un logiciel de retouche d'image et réalisé le même genre d'activité, le risque de se couper en moins.

Dans tous les cas, on obtenait un document nous permettant de répondre au challenge.



## CRÉDIT BRIANCE & VIENNE

ÉTABLISSEMENT DE CRÉDIT - www.briancevienn.fr - ORIAS n° 87 818 442

Ref. CENPRO/2025-05147

Limoges, le 27 avril 2026

Valable jusqu'au 27 mai 2025

### OFFRE DE CRÉDIT PROFESSIONNEL

Offre émise en application des articles L. 312-1 et suivants du Code de la consommation — Délai légal de réflexion: 10 jours calendaires

#### 01 — PARTIES AU CONTRAT

PRÊTEUR	EMPRUNTEUR
<p><b>Crédit Briance &amp; Vienne</b> Société Anonyme à directoire et conseil de surveillance Capital : 12 450 000 EUR 22 rue Jean-Jaurès, 87000 Limoges RCS Limoges B 492 375 821 ORIAS n° 07 018 442 — orias.fr ACPR, 4 place de Budapest, 75009 Paris Filiale de Limousin Holding SA (RCS Luxembourg B 234 819) www.briancevienn.fr</p>	<p><b>Laburrence SELAS</b> 12 avenue du Général de Gaulle, 87000 Limoges SIRET : 482 091 337 00025 SIREN : 482 091 337 - APE 8690B N° FINESSE : 870009412 Capital social : 240 000 EUR RCS Limoges B 482 091 337 Représentée par <b>M. Jean Dominique De Bermontin</b>, en sa qualité de Président www.laburrence.eu</p>

#### 02 — CONDITIONS FINANCIÈRES

Paramètre	Valeur
Objet du financement	Financement professionnel
Montant du crédit	75 000,00 EUR
Durée	84 mois (7 ans)
Date de 1 <sup>re</sup> échéance	15 juin 2026
Date de dernière échéance	15 mai 2033
Taux débiteur fixe annuel	4,79 %
<b>Taux Annuel Effectif Global (TAEG)</b>	<b>4,97 %</b>
<b>Mensualité constante (hors assurance)</b>	<b>1 064,32 EUR</b>
Frais de dossier (prélevés à l'ouverture)	750,00 EUR
<b>Coût total du crédit (hors assurance)</b>	<b>14 402,88 EUR</b>
Garanties requises	Caution personnelle du dirigeant + nantissement fonds de commerce



## 03 — EXTRAIT DU TABLEAU D'AMORTISSEMENT

semaines et dernières échéances à titre indicatif. Tableau complet disponible sur demande.

N°	Date	Capital restant dû	Intérêts	Capital amorti	Échéance
1	15/06/2026	75 000,00	299,38	764,94	1 064,32
2	15/07/2026	74 235,06	296,32	768,00	1 064,32
3	15/08/2026	73 467,06	293,19	771,13	1 064,32
82	15/03/2033	3 167,44	12,64	1 051,68	1 064,32
83	15/04/2033	2 115,76	8,44	1 055,88	1 064,32
84	15/05/2033	1 059,88	4,23	1 059,88	1 064,11

## 04 — CONDITIONS ET MODALITÉS

Le déblocage des fonds est subordonné à la réalisation de l'ensemble des conditions suspensives suivantes :

1.	Acceptation signée de la présente offre dans le délai légal de réflexion de 10 jours calendaires à compter de sa réception.
2.	Production des bilans et comptes de résultat certifiés des deux derniers exercices comptables.
3.	Mise en place effective et opposable des garanties stipulées (caution personnelle du dirigeant et nantissement du fonds de commerce).
4.	Absence de tout événement susceptible de modifier substantiellement la situation financière ou juridique de l'emprunteur.
5.	Règlement préalable des frais de dossier par prélèvement sur le compte de l'emprunteur.

**emboursement anticipé :** En cas de remboursement anticipé total ou partiel, une indemnité de 3 % du capital remboursé sera exigible, conformément à l'article L. 313-47 du Code de la consommation.

**TAEG : 4,97 % - Mensualité : 1 064,32 EUR - Coût total du crédit : 14 402,88 EUR**  
Taux calculé sur la base d'un crédit de 75 000 EUR remboursable en 84 mensualités constantes. Assurance non comprise.

## 05 — ACCEPTATION DE L'OFFRE

Conformément à l'article L. 312-10 du Code de la consommation, l'emprunteur ne peut accepter la présente offre avant l'expiration d'un délai de réflexion de **10 jours calendaires** à compter de sa réception. L'acceptation doit être signée et retournée avant le **27 mai 2026**.

Pour Crédit Briançonnais & Vienne	Pour Labaurence SELAS
Le Président du Directoire	M. Jean Dominique De Bernonville, Président
Signature et cachet :	Lu et approuvé — Signature et cachet :
Fait à Limoges, le ___/___/2026	Fait à _____, le ___/___/2026

Un crédit vous engage et doit être remboursé. Vérifiez vos capacités de remboursement avant de vous engager. Crédit Briançonnais & Vienne est un intermédiaire en opérations de banque et en services de paiement immatriculé à l'ORIAS sous le n° 07 038 442 (certifié sur intan.fr), soumis au contrôle de l'Autorité de Contrôle Prudentiel et de Résolution (ACPR), 4 place de Budapest, 75009 Paris. Les informations recueillies font l'objet d'un traitement informatique dans le cadre de la gestion de votre dossier. Conformément au RGPD et à la loi n° 78-17 du 6 janvier 1978, vous disposez d'un droit d'accès, de rectification et d'opposition. Tout litige relève de la compétence exclusive des juridictions commerciales du ressort de Limoges.

Crédit Briançonnais & Vienne SA - Capital 12 408 000 EUR - RCS Limoges B 481 375 821 - ORIAS n° 07 038 442 - 22 rue Jean Jaurès, 87000 Limoges

Document confidentiel

Recommandé  
par Ludvik O.



Flag : `CBV/PRO/2026-03147`

Flag : `14402,88`

## 22. I Can See Clearly Now

### I Can See Clearly Now 150 pts (-2/err)

Le lien entre S&L, Limousin Holding, le labo et toute la clique est désormais établi.

Mais quelle contrepartie la banque obtient-elle en échange de sa précieuse collaboration avec le labo ?

Bonne question, n'est-ce pas ?

Vous y revenez. Et si Henri-Pierre était lui aussi une victime collatérale dans cette histoire ?

En épluchant les flux applicatifs côté banque, vous comprenez le mécanisme. Lorsqu'un habitant du département effectue une  , la banque utilise des informations auxquelles elle ne devrait pas avoir accès. Un scoring est même établi à partir de l'URL  .

Il semble que nous devons revenir à la banque. En analysant son site internet, petite recherche sur Censys qui ne donne rien, d'autres outils du même genre non plus. Il faut chercher ailleurs. On va aller regarder le fichier <https://briancevienne.fr/robots.txt>

```
# --- Espace conseillers / outillage interne - ne pas indexer ---
Disallow: /scoring
Disallow: /scoring/
Disallow: /internal/
Disallow: /admin/

# --- API partenaire S&L Datalake - usage strictement interne ---
# (Ne pas crawler : l'authentification est gérée côté serveur, mais on évite quand même
# d'exposer la documentation aux moteurs de recherche.)
Disallow: /api/
Disallow: /api/v1/
Disallow: /api/v1/score
Disallow: /api/v1/patient/
Disallow: /api/v1/patients/search
Disallow: /api/v1/docs
Disallow: /api/v1/redoc
Disallow: /api/v1/openapi.json
```

Intéressant, on découvre la mention du datalake, d'une API de scoring...

On comprend alors ce qui se passe.

Flag : `simulation de prêt`

Flag : `https://briancevienne.fr/api/v1/score`



À la lecture des données de notre lanceur d'alerte, il semble en parfaite santé... Mais souvenons-nous du stagiaire.

Lui aussi a laissé des traces. Vous remontez ses dépôts : il a développé des éléments stockés sur

`https://storage.mymusicband.fr` ✓. On y repère un `update` ✓ récent, identifié par le hash `9A9A9A9A9A` ✓, portant sur le fichier `trash/partition_rock.txt` ✓.

Et tout ça, à la demande de `Jacque Brel` ✓.

🚩 **Flag :** `https://git.vedamedicaldataschool.eu`

En lisant la phrase du rapport, on peut identifier que c'est cette ligne qui nous intéresse :

`tvalleurant` `1815b2ea38` `fix correction valeurs LIMS sur le bilan du 2026-03-14 (à la demande de M. Raoul)` `il y a 3 mois`

🚩 **Flag :** `commit`

🚩 **Flag :** `1815b2ea38`

🚩 **Flag :** `data/resultats_lab0.csv`

🚩 **Flag :** `Raoul Reidid`

*(Rappelons au passage que sur ce CTF nous avons été particulièrement souple et flexible en acceptant bien souvent plusieurs propositions de flag. D'autres fois nous tenions cependant à avoir la réponse précise telle qu'attendue, nous restons des rhinos quand même)*

Il est donc en danger. Surtout qu'il a été conseillé par le `projectionniste` ✓ de `SoDinCo` ✓ pour commander des traitements sur `temu.com` ✓, comme il l'indique sur cette page `https://doctobeeep.com/antivirus/` ✓. Il semble beaucoup apprécier les gélules `Phytovamieu` ✓ et le `grododo` ✓.

Cet enchaînement pouvait induire en erreur, mais en relisant le chapitre dans sa globalité on comprend qu'on parle bien de HPG. Nous n'avons trouvé que son compte Mastodon et son blog. Nous retournons y faire un tour, quelque chose a dû nous échapper. Petite analyse plus structurée du site, et nous découvrons quelque chose de surprenant sur <https://henripierregirolles.wordpress.com/sitemap.xml>

On compte 14 articles visibles, mais il y a bien 15 articles existants. On identifie la page cachée <https://henripierregirolles.wordpress.com/ma-sante>

🚩 **Flag :** `stagiaire`

🚩 **Flag :** `LabAurence`

🚩 **Flag :** `medideal24.eu`

🚩 **Flag :** `https://henripierregirolles.wordpress.com/ma-sante`

On compare les indications de HPG avec les produits présents sur le site de Médideal

🚩 **Flag :** `GlycoNatur`



🚩 **Flag :** Somniherb

Pourtant, après ce qui est arrivé en 2024 à sa  , Mariah Carey , on aurait pu croire qu'il serait plus prudent...

On se souvient avoir lu avec attention l'ensemble de son blog et noté ces informations dans un coin de notre mémoire.

🚩 **Flag :** belle sœur

🚩 **Flag :** Christine Daguerran

*(La boucle est bouclée, Christine, le personnage qui donnait le top départ de Médileak 1 trouve sa place pour la compréhension de Médileak 3)*

On a la possibilité d'entamer un nouveau chapitre, ou de revenir à celui que nous avons mis de côté avec déjà quelques réponses à disposition. Allons donc le terminer. Pour rappel on en était là :

Vous remontez la propriété du terrain. C'est une parcelle qui appartient à la   !   serait donc derrière les menaces visant Henri-Pierre.

🚩 **Flag :** SCI NICOSIAN HOLDING

🚩 **Flag :** Despina KYPARISSIDOU

Le 4x4 qui a failli renverser HPG était garé sur le côté de la maison !

Et tant qu'on y est, on remarque autre chose : ce même véhicule était également garé devant la nouvelle   de  , comme le confirme la photo ci-dessous :



Cliquez pour sélectionner ou glissez-déposez une image

PNG, JPG, GIF jusqu'à 10MB

2 fois c'est une coïncidence... Trois fois, c'est un pattern !

Ce projet d'école retoqué semble donc gêner du beau monde.

Alors ce challenge, il nous a bien surpris car il n'était pas supposé poser autant de difficulté. Et pourtant il a été très difficile à résoudre pour la plupart des équipes. Pourquoi ? Et bien parce qu'il était trop simple, pour un challenge placé aussi loin dans le CTF. Méthode à retenir...

On a déjà vu le 4x4 qui a failli renverser HPG. Pour ceux qui ont bien visité les lieux progressivement découverts, ce même véhicule, NOIR, était garé près de la carrière



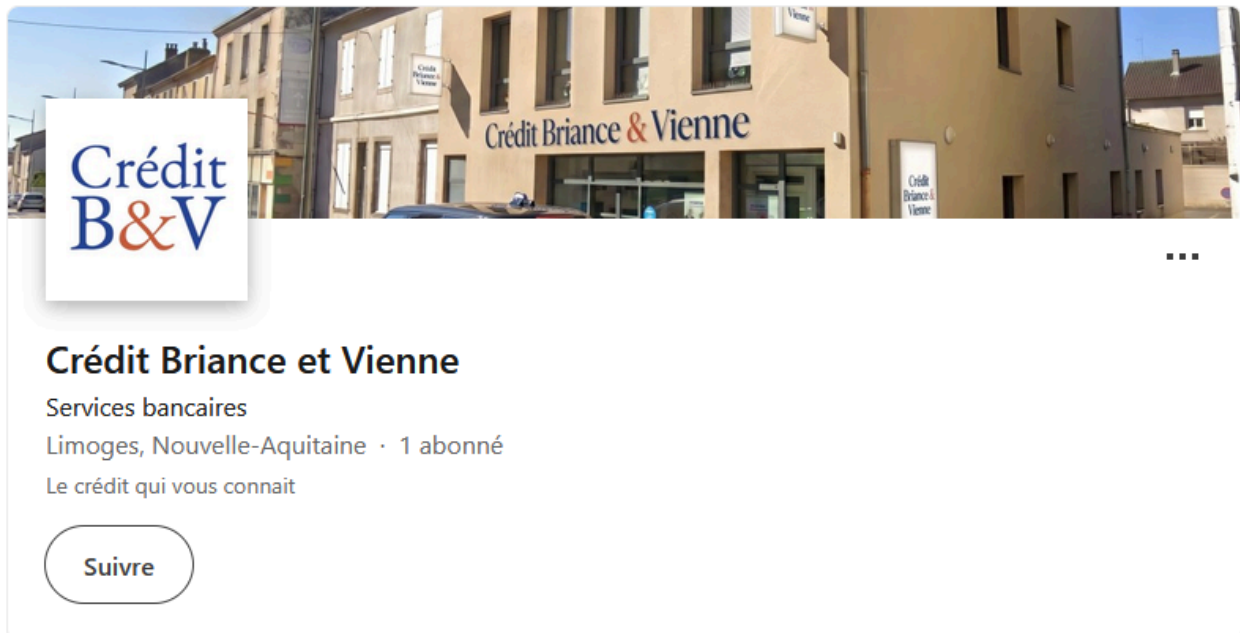
Mais non, chez le rat, ce n'était pas le même, il était vert, et en plus aucune visibilité de la plaque pour l'identifier formellement





Nous devons donc chercher ailleurs, autrement que tout ce qu'on a déjà fait. Et oui, il y a quelque chose de très simple que l'on n'a pas utilisé encore sur ce CTF : en présence de sociétés, on n'est pas allé voir sur LE réseau social des sociétés, à savoir LinkedIn !

On peut chercher les différentes sociétés croisées, et on trouve : <https://www.linkedin.com/company/cr%C3%A9dit-briance-et-vienne>



Et dans le post où la banque évoque l'ouverture d'une nouvelle agence : oh ! un 4x4, noir, avec la même plaque d'immatriculation !



Ce nouveau point de contact répond à une demande forte de nos clients sur le territoire et confirme notre engagement, depuis 1927, d'être présents au plus près de celles et ceux qui nous font confiance.

Une équipe de conseillers limousins est déjà en cours de constitution pour vous accompagner dès l'ouverture. Si vous souhaitez en faire partie, nos opportunités de recrutement seront publiées ici dans les prochains jours !

Restez connectés, abonnez-vous à notre page pour ne pas manquer le grand jour



🚩 **Flag :** agence

🚩 **Flag :** Crédit Briance & Vienne



# Family Affair

## Family Affair

Vous avez une belle vision de l'ensemble... Enfin, si vous n'avez pas traversé les éléments de l'enquête comme un touriste sur la voie de gauche d'une autobahn allemande.

### 23. Sweet Child o' Mine

#### Sweet Child o' Mine 80 pts (-2/err)

Raoul était peinard sur son île à ramasser des plantes, quand  a vu sa photo lorsqu'elle a posé pour .

Flag:


Flag:

Sauf qu'à priori, elle a manqué de discrétion, et  a vu ses plans contrariés et son concert annulé... Sur  elle a d'ailleurs dit qu'elle allait peut-être accepter l'aide de .

Flag:

Flag:

On se rappelle ce post



**gizemreid** 5 sem  
 I missed my concert because of Raoul's business... again... I'm tired of seeing my love harassed by these people. He only wants what's best for others...  
  
 Maybe he will accept my family's help for once.

Flag:

Et quelle famille... il s'avère que Gizem est en fait la  de , qui co-dirige .

Sur l'acte de donation, on avait pu lire



## ARTICLE 3 — LIEN DE PARENTÉ — RÉC

La Donatrice et la Donataire sont **mère et fille**. I

Flag: **fil**

Flag: **Despina KYPARISSIDOU**

Flag: **Stavros & Lynch Partners**

## 24. Soldier of Fortune

### Soldier of Fortune 60 pts (-2/err)

Et au final... si Raoul était encore le dindon de la farce ?

Si sa nouvelle activité avait été utilisé pour servir des intérêts supérieurs ?

Car vous avez découvert que HPG a fait capoter le projet de   d'implanter un établissement à Limoges ! Et vu les liens financiers existants, les menaces reçues ne sont pas étonnantes !

Flag: **Veda**

On ne va pas retracer toute votre enquête... mais quand même, ce que Cynthia vous a indiqué avant de couper la conversation sur S&L vous intrigue...

En étudiant ces investisseurs, vous découvrez qu'ils ont lancé en 2026 une entreprise au Moyen Orient.

propose ses services sur le site

.

On pensait que c'était un résumé général, qu'on était à la fin du CTF : mais non...

On repart donc sur le site de Stavros, et si on ne l'a pas fait avant, il va falloir l'éplucher en détail. Sur la page dédiée aux investisseurs, on trouve deux rapports.



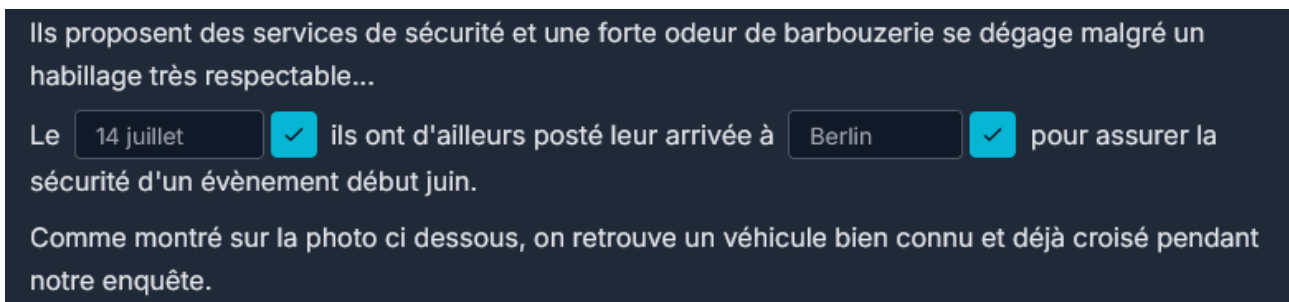
Dans le rapport de 2025, on peut noter ce passage :



**Flag :** [Kydonia Continental Security Holdings Ltd](#)

Recherche qui devient habituelle pour le site internet

**Flag :** <https://kydonia.vip>



En bas de la page d'accueil de leur site internet, un lien vers le compte X <https://x.com/KidoniaSecurity>



On trouve ce post



🚩 Flag : 11 mai

🚩 Flag : Limoges

Quelle sera leur cible ? Qui veulent-ils protéger ?  
Les meilleurs d'entre vous auront à le découvrir très bientôt !

En attendant... vous pouvez revivre les chapitres ici :

[https://www.youtube.com/watch?v=WyF8RHM1OCg&list=TLGGwC1C\\_UlzhSExMzA1MjAyNg](https://www.youtube.com/watch?v=WyF8RHM1OCg&list=TLGGwC1C_UlzhSExMzA1MjAyNg)



Et voilà, enfin la fin ! Enfin... la fin de l'épreuve de qualification. Quatre équipes ont ensuite pu participer à la grande finale, accueillit au sein du stade Beaublanc de Limoges.

Ah... mais non... Il restait un challenge évidemment !



## Jingle Bells (bonus)

### Jingle Bells (Bonus)

Un Medileak sans Cloche ne serait pas un Medileak...

## 25. Tubular Bells

### Tubular Bells 20 pts (-2/err)

Sur le site de e-commerce où notre cher Raoul fait ses affaires, vous découvrez le produit

Clochint Magnifer Earing



qui vous permet de localiser facilement le son fourni en test

Rechercher un lieu ou saisir des coordonnées (lat, lng)...

Il fallait se rendre sur le site de Médideal, chercher quel produit pourrait nous permettre de résoudre ce challenge. <https://medideal24.eu/product/bellotic-auditory-acuity-enhancer-40-caps/>

**BellOtic Auditory Enhancer – 40 Caps**  
76,30 € 67,40 €

Precision nutraceutical for sharpened bell discrimination and fine-frequency hearing in complex acoustic environments.

Out of stock

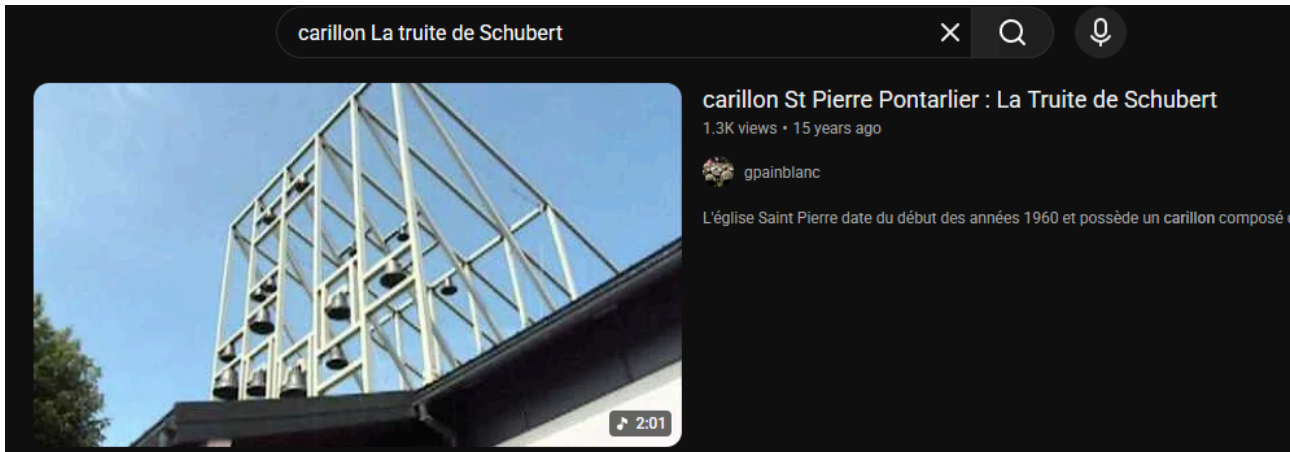
SKU: BELLO-30

Categories: Probiotics, Uncategorized

**Flag:** BellOtic Auditory Enhancer

Afin de tester l'efficacité de ce traitement, un audio était disponible. Aucune astuce technique, pas d'outils hyper spécialisés, rien d'autre que ses oreilles et un peu de culture musicale (ou tenter l'appel à un ami, un autre ami, des gens de la famille, interpellier les gens dans la rue...).

On pouvait reconnaître La truite de Schubert. Une recherche sur Youtube



🚩 **Flag :** 46.909011, 6.349561

Trop facile, comme dirait Rofellos.

L'écriture de ce write-up, en refaisant chaque recherche pas à pas pour obtenir les prises d'image, a pris 8h complètes. L'équipe la plus rapide a mis environs 35h pour le terminer dans des conditions réelles de jeu.