Write-up **HEXA OSINT CTF V2** - OSINT CTF

By *Eldwiin & R0ck3t & Tab & Zmondy* - **Team Tacosint**

Contents

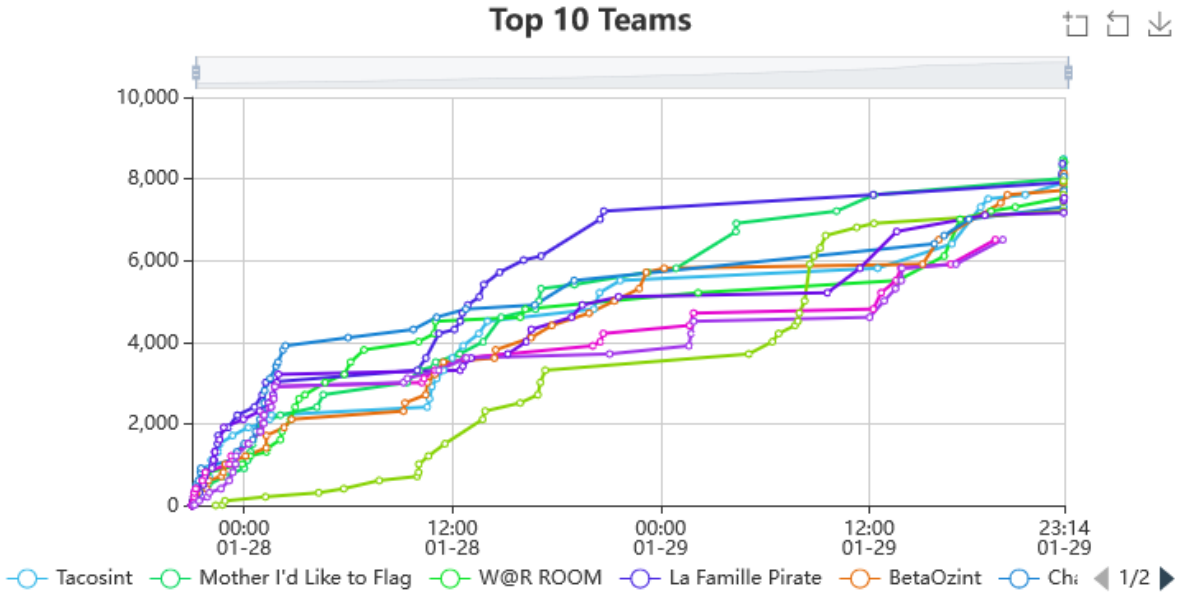
1. HEXA CTF V2

1.1. CTF

The ***HEXA CTF V2*** is an Online OSINT CTF organized between the 27th of January at 21h00 CET (UTC+1) and the 29th of January at 21h00 CET (UTC+1) by the Hexa association, supported by Sopra Steria. This year was the second edition of the Hexa CTF. The first version took place in 2022.

1.2. Team

Tacosint was represented by Eldwiin, R0ck3t, Tab and Zmondy and ended up at the 1st place of the ranking against 115 other teams.

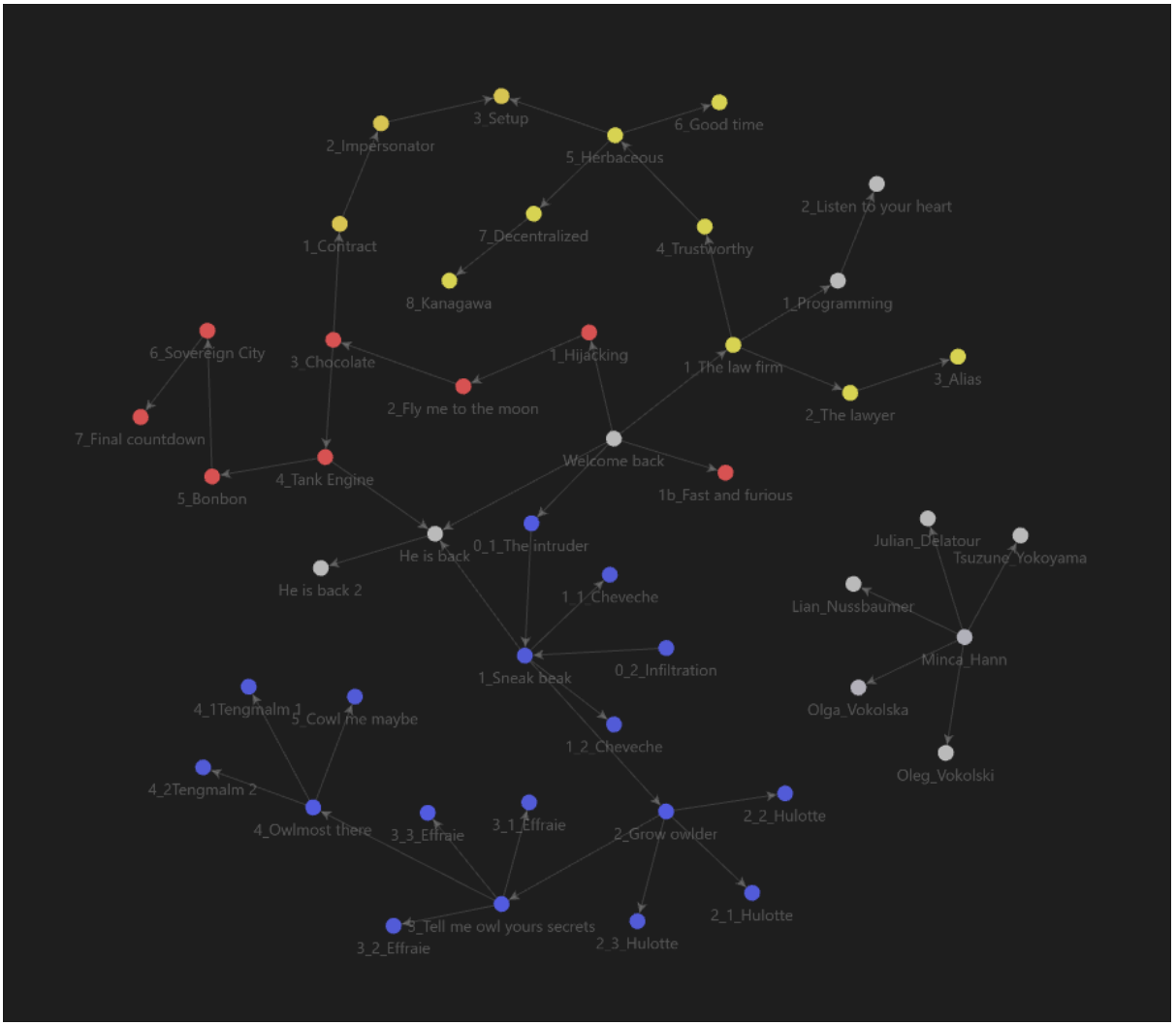


Place	Team	Score
1	Tacosint	8480
2	Mother I'd Like to Flag	8470
3	W@R ROOM	8410
4	La Famille Pirate	8370
5	BetaOzint	8130
6	ChatGPT	8050
7	40548F	7950
8	Cogitosint Ergo Sum	7530
9	Ice_Sec	6510
10	TrainezPas	6510

2. Write-up OSINT

2.1. Challenges dependency map

The unlocking order of the challenges provided by the organizer is the following:



The Intruder

The Intruder 100	Infiltration 100	Sneak beak 200	Cowl me maybe 200
Grow owlder 300	Tell me owl your secrets 600	Owlmost there 900	

Analysis

Mission analysis 300	Action man analysis 400	Associate analysis 400	Mastermind analysis 400

Action Man

Hijacking 100	Fast and Furious 100	Fly me to the moon 100	Chocolate 200
Tank Engine 200	Bonbon 300	Sovereign City 300	Original 300
Final countdown 400			

The Associate

- Contract — 200
- Impersonator — 200
- Setup — 300

Sidequest

- He is back — 300
- He is back 2 — 300

The Lawyer

- The law firm — 100
- Alias — 100
- Good time — 100
- The lawyer — 200
- Trustworthy — 200
- Herbaceous — 200
- Decentralized — 200
- Experts — 200
- Kanagawa — 300

The Developer

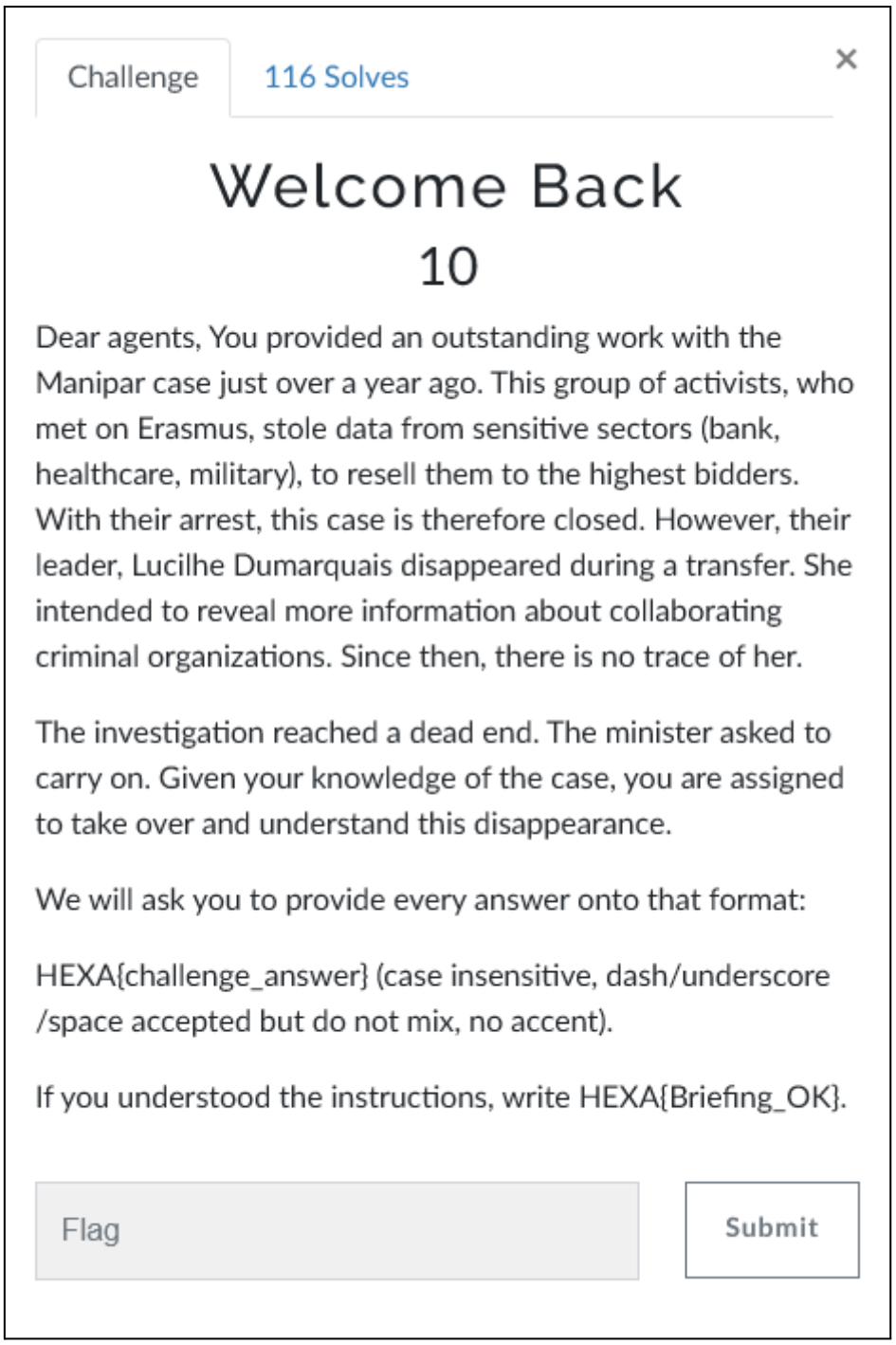
- Programming — 100
- Listen to your heart — 200

Intro

- Rules — 0
- Welcome Back — 10

2.2. Intro

2.2.1. Welcome Back



The first challenge is to set the context. Nothing complicated here, just copy the flag: `HEXA{Briefing_OK}`

2.3. Action Man

2.3.1. Hijacking

Challenge | 108 Solves

Hijacking

100

The convoy transporting Lucilhe from "Maison d'arrêt de Versailles" was hijhacked on the 30th of November 2022. She has not been seen since and her case file is incomplete. A tiny mistake has been made: the picture of the convoy's destination was provided but not the place's name. Please begin by completing the file with the name of this convoy's destination.

Format : HEXA{french_destination_name}

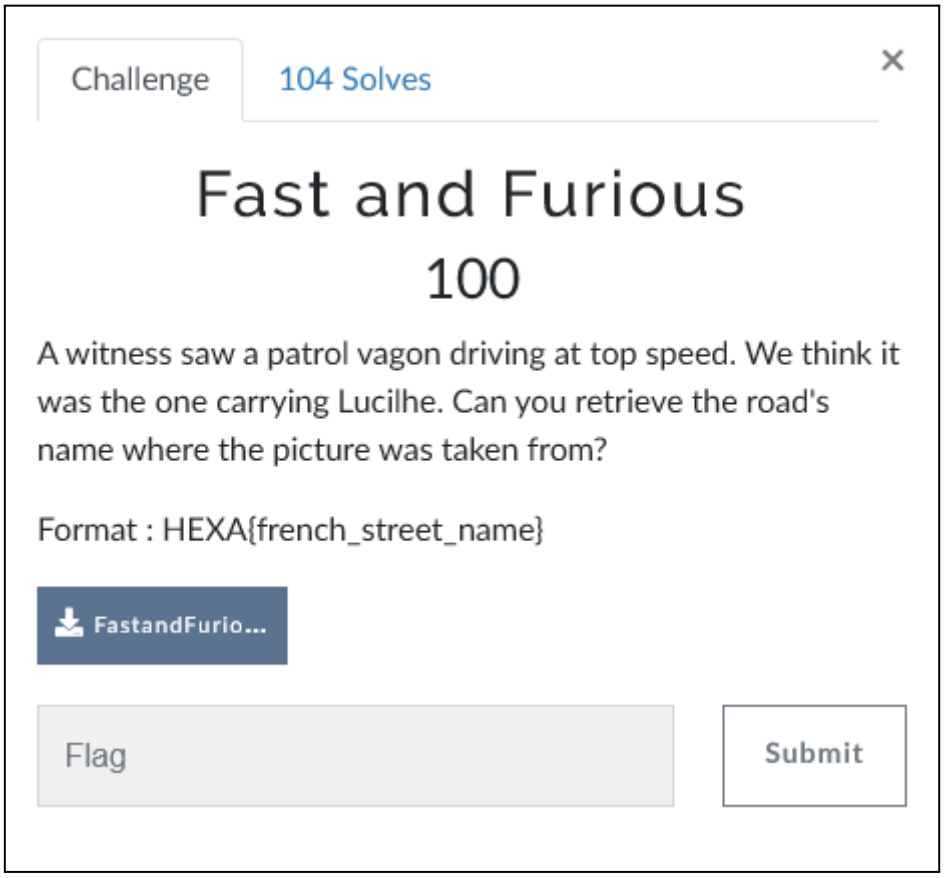
Hijacking.JPG

Flag

Submit

With the statement, we had a photo. All we had to do was to perform a reverse image search with Google Lens. This one tells us that it is the “Tribunal Judiciaire de Versailles”. The flag is `HEXA{Tribunal_Judiciaire_de_Versailles}`.

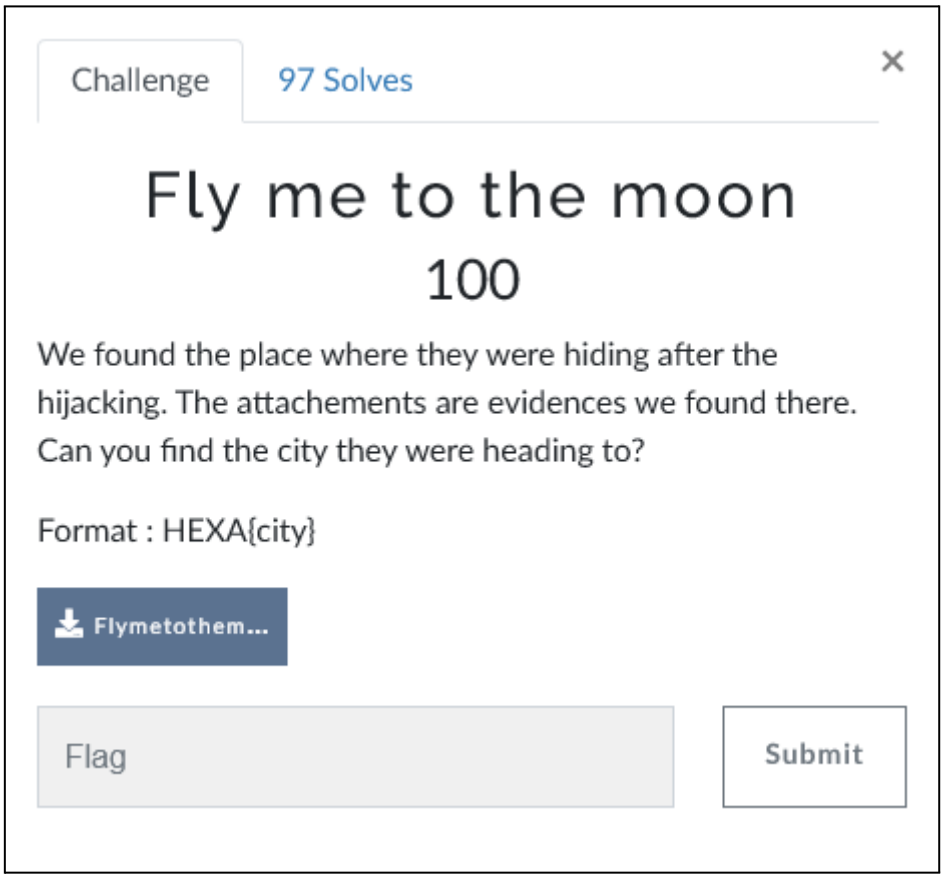
2.3.2. Fast and Furious



For this challenge, we also had a photo. However, with Google Lens, it doesn't give us much. On the right side of the picture, there are signs for the place written in French. We can then search the place with Google Maps thanks to this. We arrive easily in the surroundings by searching "Meudon D57" on Maps. We look

for an intersection near a tramway stop. We look at some intersections with the Street View mode and find this one corresponding to the picture we are looking for.
https://www.google.fr/maps/@48.7802802,2.1907343,3a,75y,63.83h,85.23t/data=!3m6!1e1!3m4!1sSW--njUUkGWoZhYIAkL7Jg!2e0!7i16384!8i8192
Flag: HEXA{Avenue_du_capitaine_tarron} .

2.3.3. Fly me to the moon



A picture of the evidence found at the safehouse was provided with this challenge:

We can read on the paper on the left:

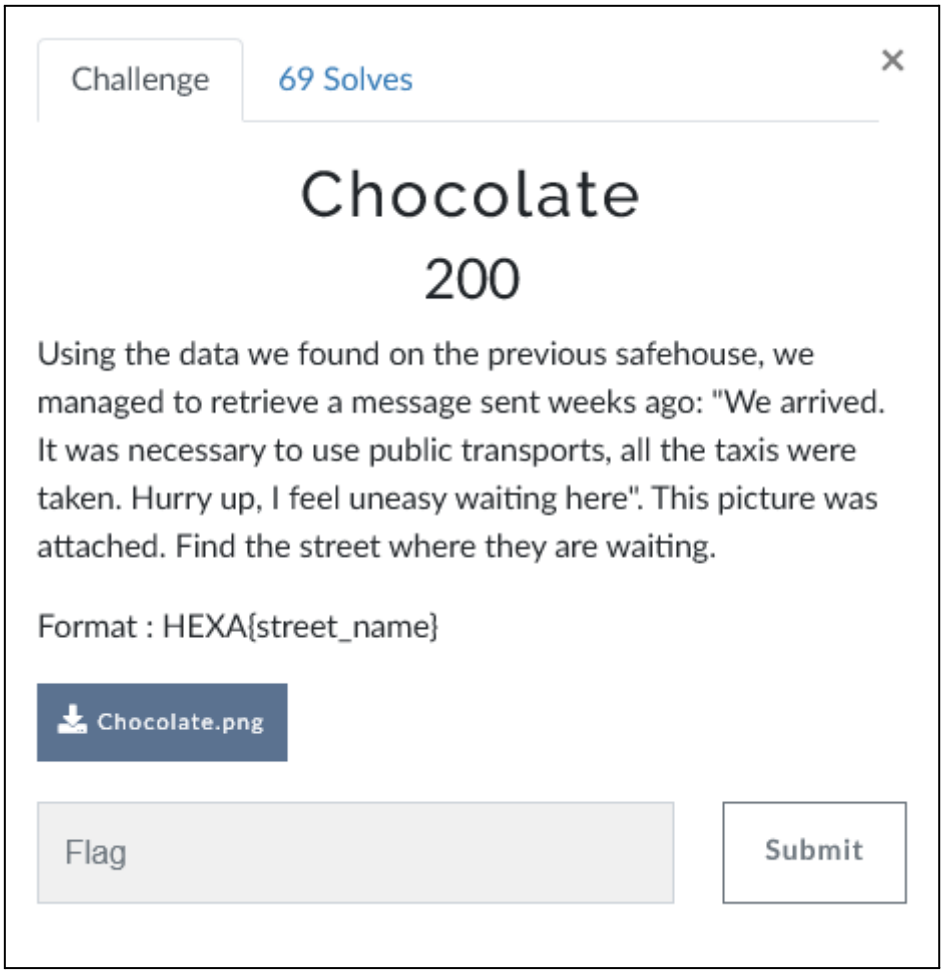
> *pictures + flight*
> *14/12/2022*
>
> *Oleg,*
> *I attached the pictures → Print them for your passport.*
> *You know where to reach me.*
> *I attached your flight for tomorrow.*
> *See ya.*

With the picture, we can read a code: FSF145P. By making the link between those two, we searched for flight n°FSF145P:
https://www.radarbox.com/data/flights/FSF145P
https://flightaware.com/live/flight/FSF145P

It looks like they were heading from Paris to Payerne and the plane went back to Clermont-Ferrand after it.

Flag: HEXA{Payerne}

2.3.4. Chocolate

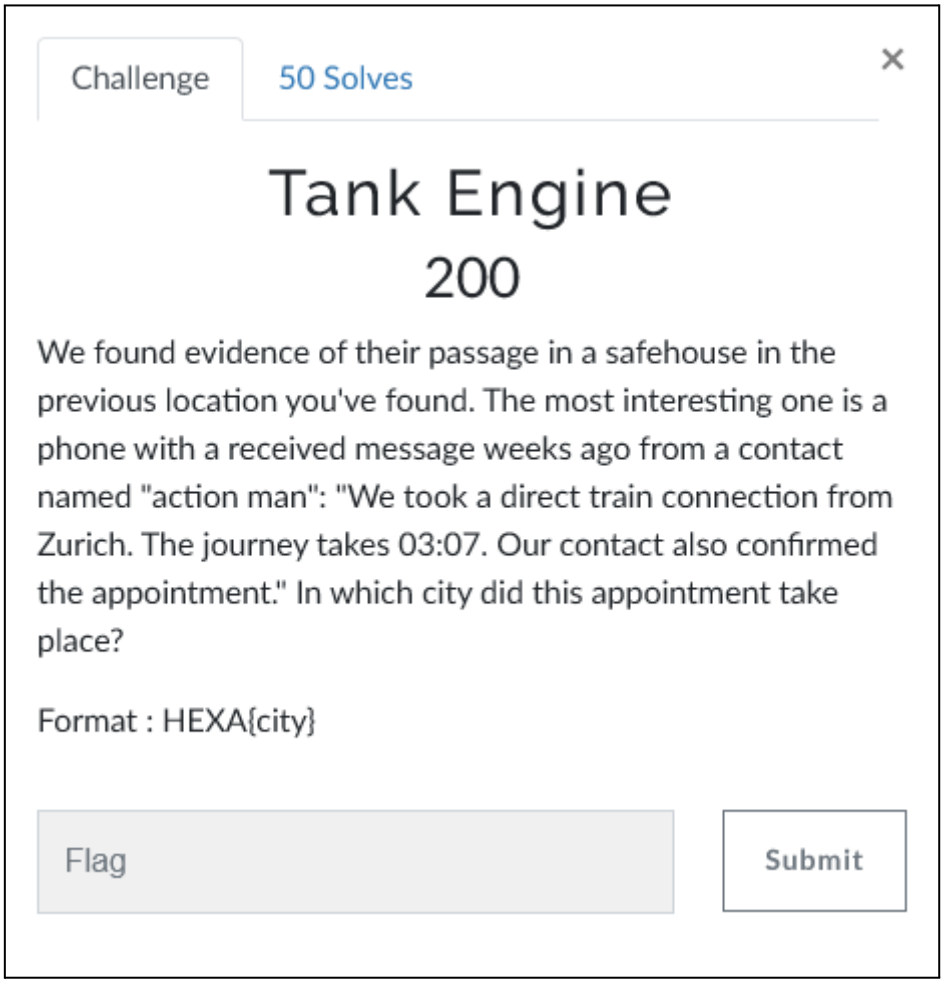


We can see on the picture that there are tramway tracks in the picture and some shops called “[...]ETSCH” and “[...]alle Wo[...]”.

There are 4 cities with tramways in Switzerland: Basel, Bern, Geneva and Zürich.
When searching names ending with “ETSCH” using a tool like https://www.dcode.fr/words-ending-with, we find a list of 14 words in German:
KETSCH, FLETSCH, KNETSCH, PIETSCH, QUETSCH, SKETSCH, KNIETSCH, PLIETSCH, QUIETSCH, ABQUETSCH, BORRETSCH, DOLMETSCH, ZERQUETSCH and PLAUTDIETSCH.

When searching shops in Switzerland containing these words, we can find one called “Dolmetsch AG” in Zürich, on Limmatquai Street. Dolmetsch AG
Flag: HEXA{limmatquai}

2.3.5. Tank Engine

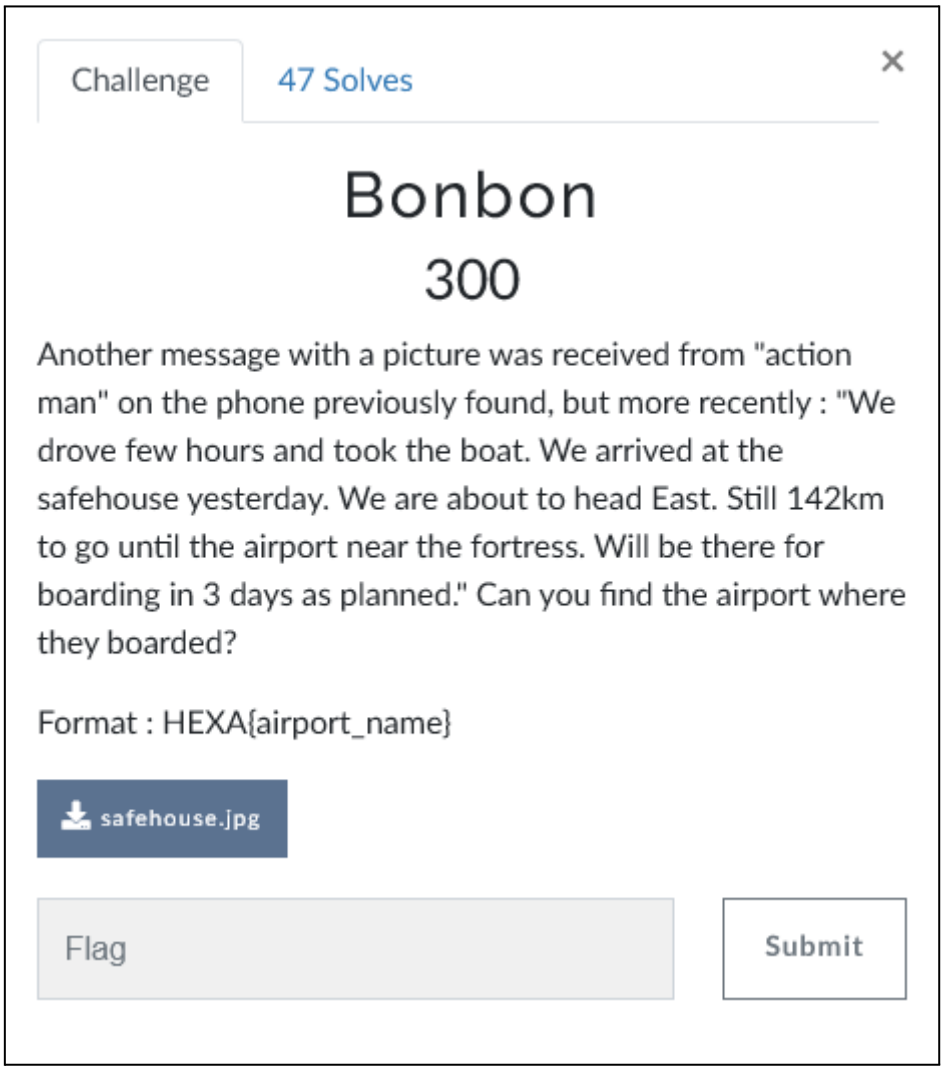


After searching multiple ways to get this information, we typed “direct train connections” in Google or DuckDuckGo. The first link points to https://direkt.bahn.guru/.

When you search direct connections from Zurich, we can find one yellow dot indicating 3h07 in the south of Switzerland: Cadenazzo.

Flag: HEXA{Cadenazzo}

2.3.6. Bonbon


Challenge
47 Solves
Bonbon
300
Another message with a picture was received from "action man" on the phone previously found, but more recently : "We drove few hours and took the boat. We arrived at the safehouse yesterday. We are about to head East. Still 142km to go until the airport near the fortress. Will be there for boarding in 3 days as planned." Can you find the airport where they boarded?
Format : HEXA{airport_name}
safehouse.jpg
Flag
Submit

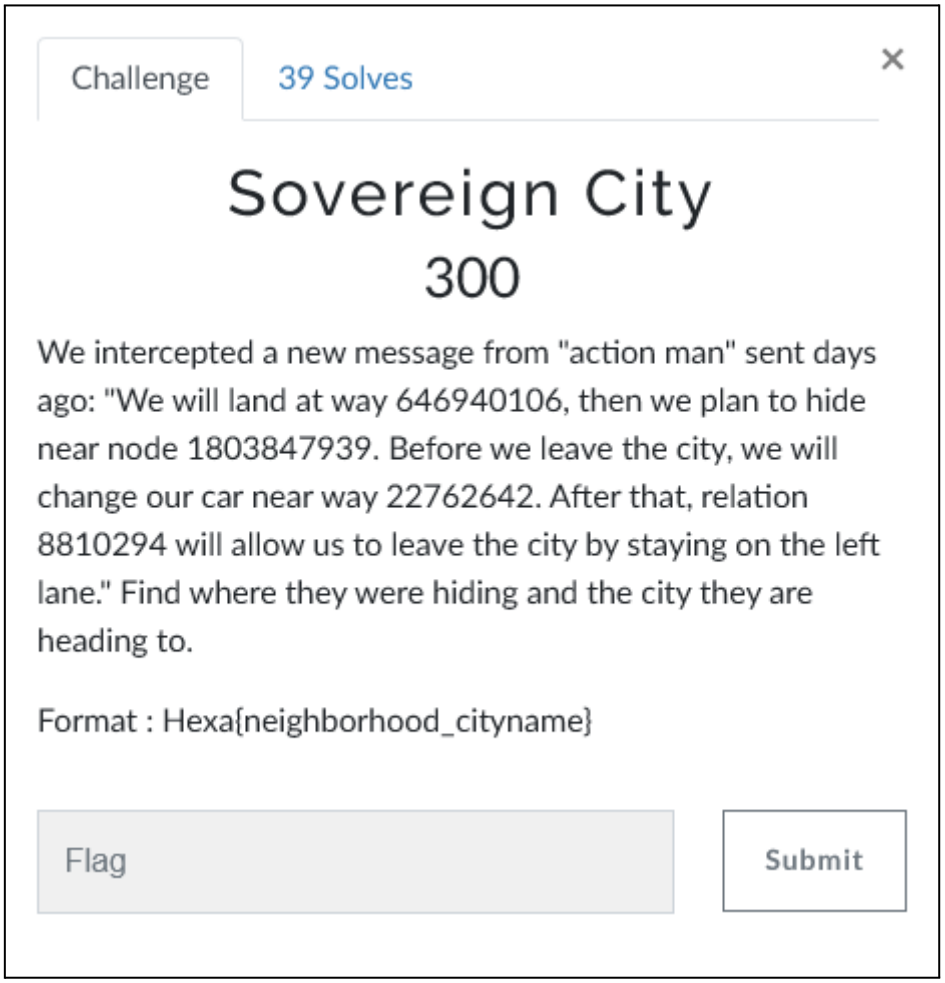
By analyzing the EXIF metadata of the picture provided with the challenge, we find GPS coordinates in Chania, Greece:

GPS	
Latitude	35; 31; 1.8212192616775269
Longitude	24; 1; 3.10615539859281142

There are not many airports nearby but we can find an international one in Heraklion called “Níkos-Kazantzákis”, 142 km east by road.

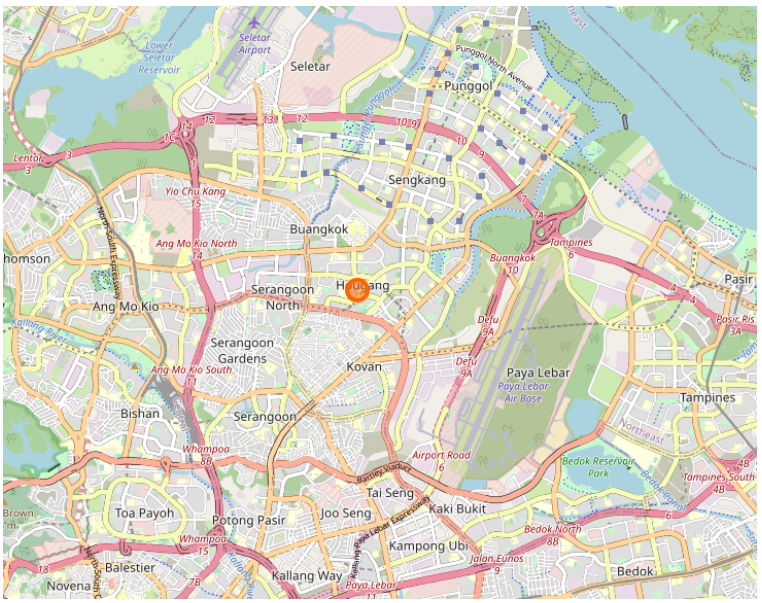
Flag: `HEXA{nikos_kazantzakis}`

2.3.7. Sovereign City

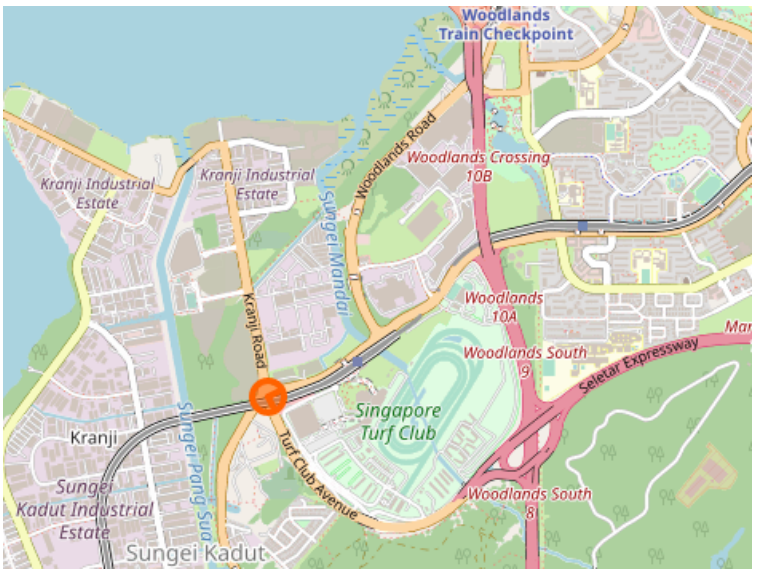


In this challenge, the first question we asked ourselves is “What is a way, a node and a relation ?”. A quick search on Google with “way node relation number” let us know that OpenStreetMap elements use this kind of nomenclature. The help forum lets us know how to request for ways, nodes and relations. From this, the following links help us determine where they were:

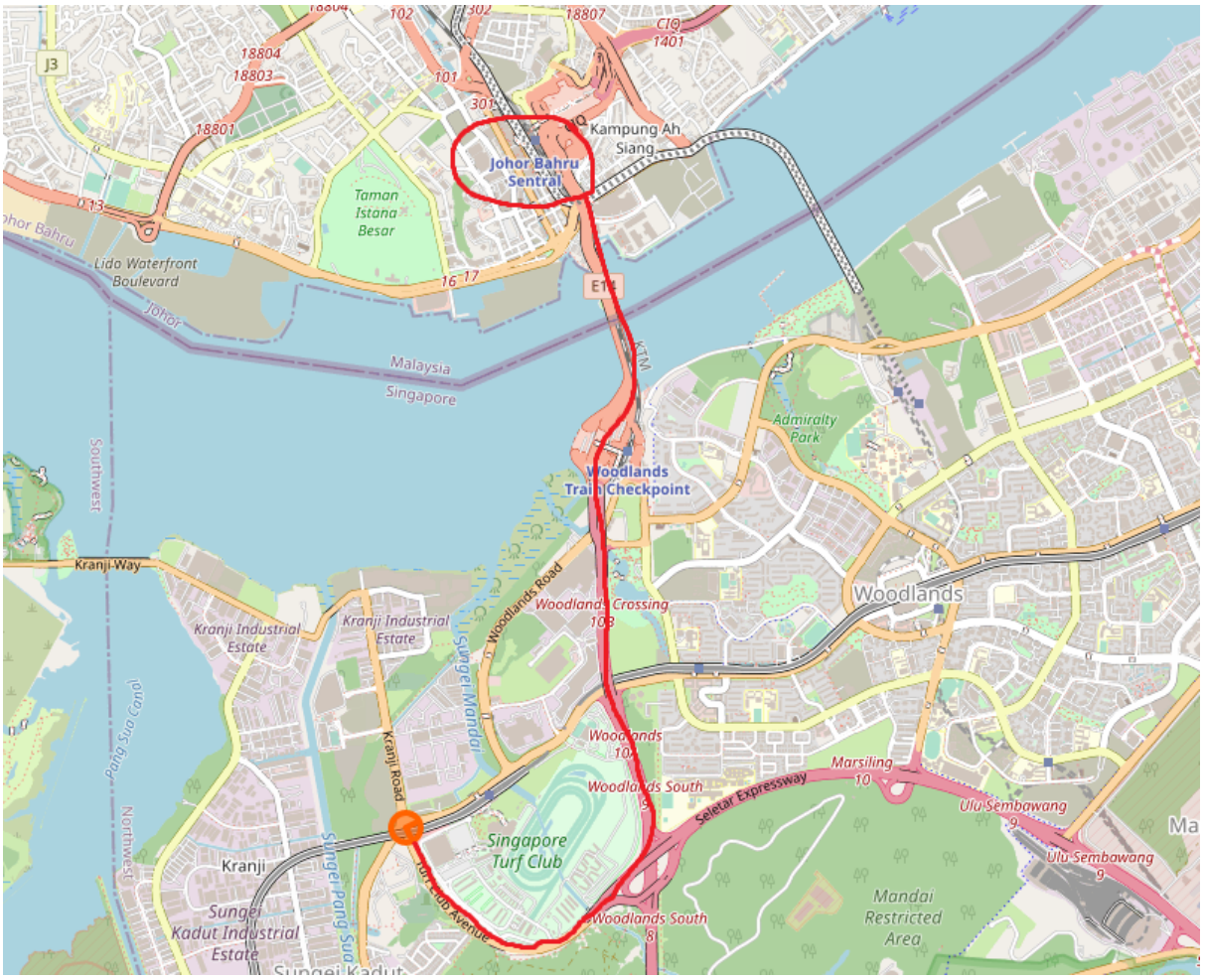
- They arrived here: 

- They hide here: 

- They changed car here: 

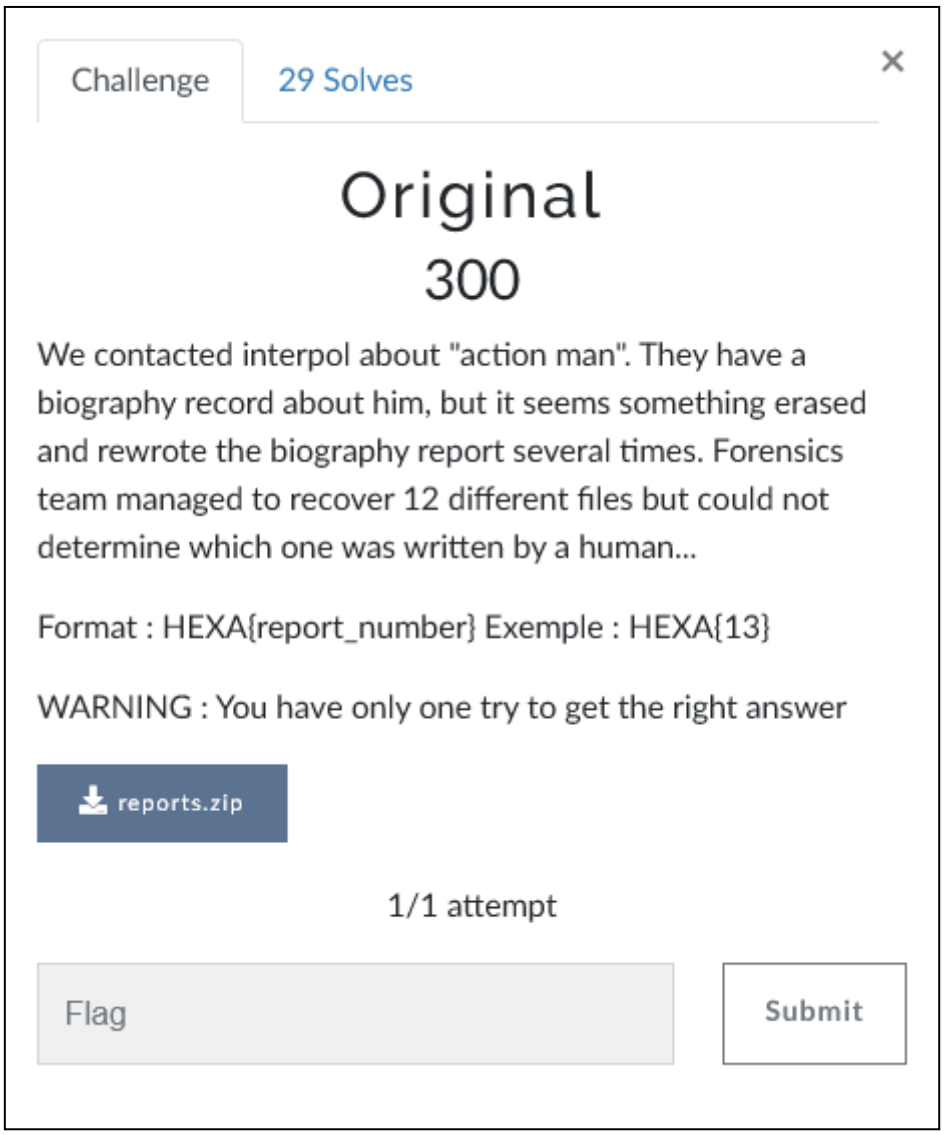
- [And they turned here](): 

The neighborhood where they hide is Hougang (it is a little small on the screen, but it is more visible via the link). From the last turn they took and assuming that they stayed left after that one, we can see where they were going. They were going north of Singapore, to Johor Bahru.



So the flag is HEXA{hougang_JohorBahru}.

2.3.8. Original



For this challenge, we began by thinking “what could be the main difference between a machine and a human?” The first one that came to our mind was that a machine does what it is supposed to do, without making mistakes, or if it made one mistake, it should be present in all the reports written by the machine. So in this case, a machine shouldn’t make any error writing the report (or always the same error) whereas a human could do one. Following this lead, we used the tool https://www.onlinecorrection.com/ to check each report to see if there was a mistake. One report had a slight error (the placement of a coma) and another one had a real error: "*For this crimes*" instead of "*For these crimes*" (even my text editor

is asking me if I am sure about the first sentence). This is typically the kind of little mistake a human would make. The concerned report was number 8.
So the flag is: HEXA{8}

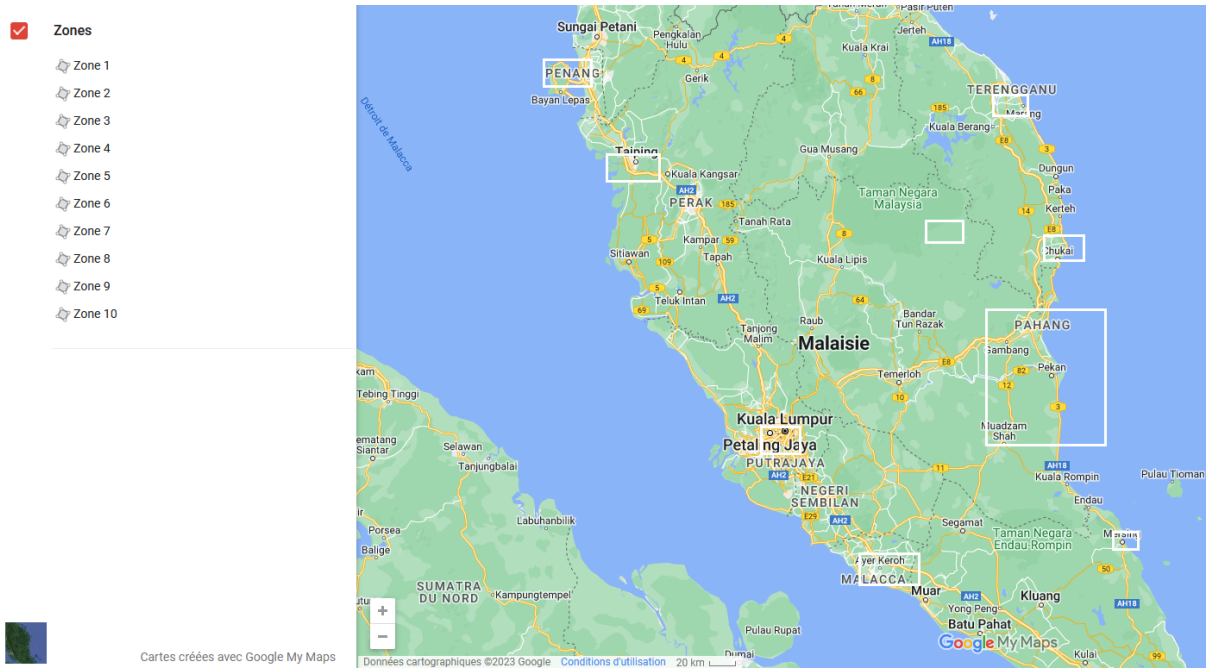
2.3.9. Final countdown

This challenge was the one that had the most revamp during the CTF. Indeed, at first it had 5 tries allowed, and the text was a bit less explicit. We first thought we

needed to find an OSM building but it turned out we were looking for a node with a building attribute. The perfect way to do this kind of search was to use overpass turbo which relies on the OpenStreetMap API.

Before going on overpass turbo and kicking some queries in, we first need to figure out what this “zone 4” is. Luckily for us, we already did the Herbaceous challenge before. On the website, there was a kmz file which contained only a kml file with several zones. Zone 4 was in Malaysia, south of Kuala Terengganu.

To open the KML file, either you can use the base app from your system (if it has any), or create a my map Google like this one:



Going on overpass turbo, we start by drawing the zone we want to search in (using the button on the left of the map).

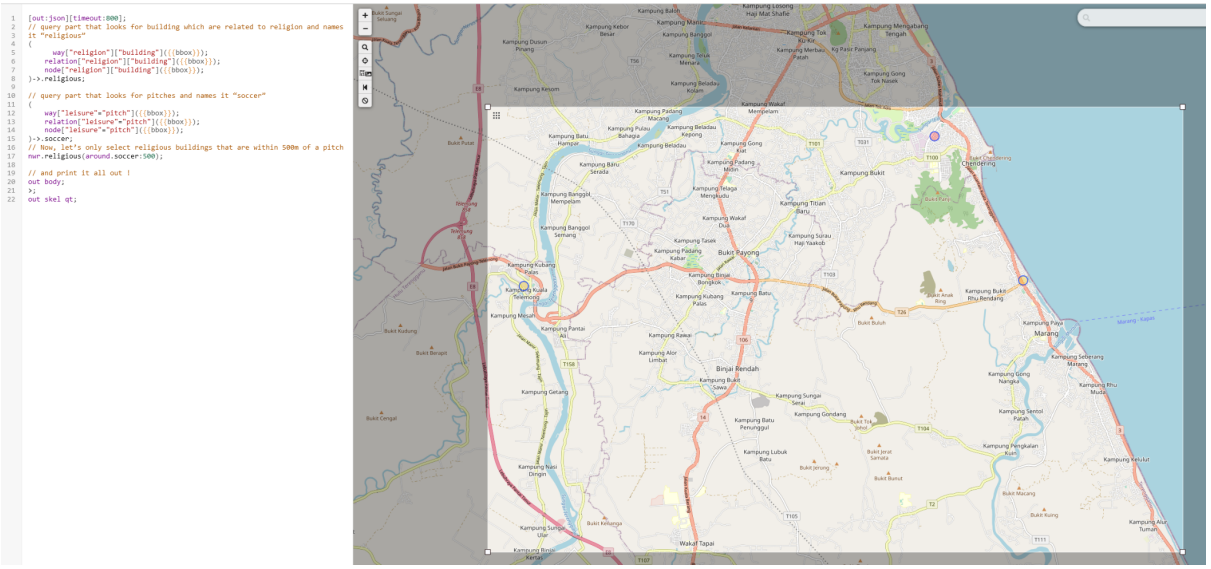
Now, it is time for us to create the query. First, we only searched for places of worship, and football fields, but it turned out not to be very effective. So using some tutorials on how to use this tool, we manage to create our own request:

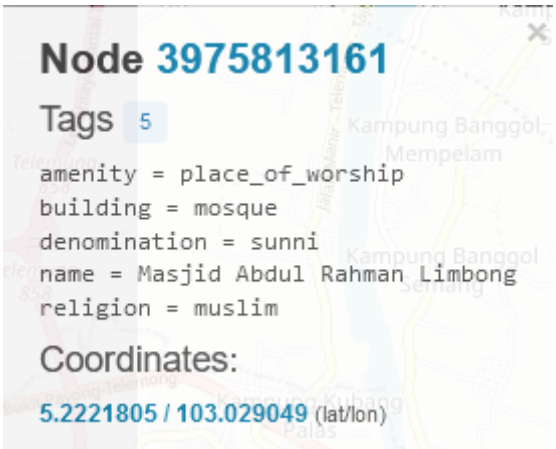
```
[out:json][timeout:800];
// query part that looks for building which is related to
religion and names it “religious”
(
      way["religion"]["building"]({{bbox}});
    relation["religion"]["building"]({{bbox}});
    node["religion"]["building"]({{bbox}});
)->.religious;
```

```
// query part that looks for pitches and names it “soccer”
(
    way["leisure"="pitch"]({{bbox}});
    relation["leisure"="pitch"]({{bbox}});
    node["leisure"="pitch"]({{bbox}});
)->.soccer;
// Now, let’s only select religious buildings that are within
500m of a pitch
nwr.religious(around.soccer:500);

// and print it all out !
out body;
>;
out skel qt;
```

The result gives us three points. However, the challenge specifies that the building is far from the sea (at least 3 km by feet). A little google map search let us see that only one building fits this description.

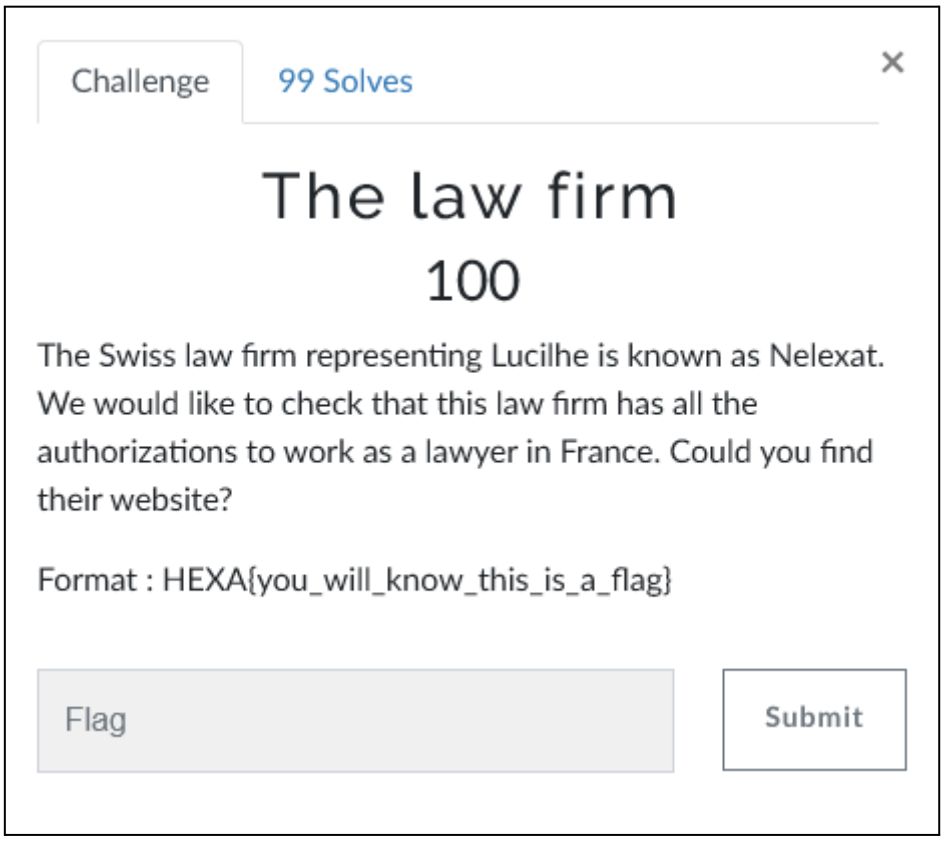




The flag is HEXA{3975813161}

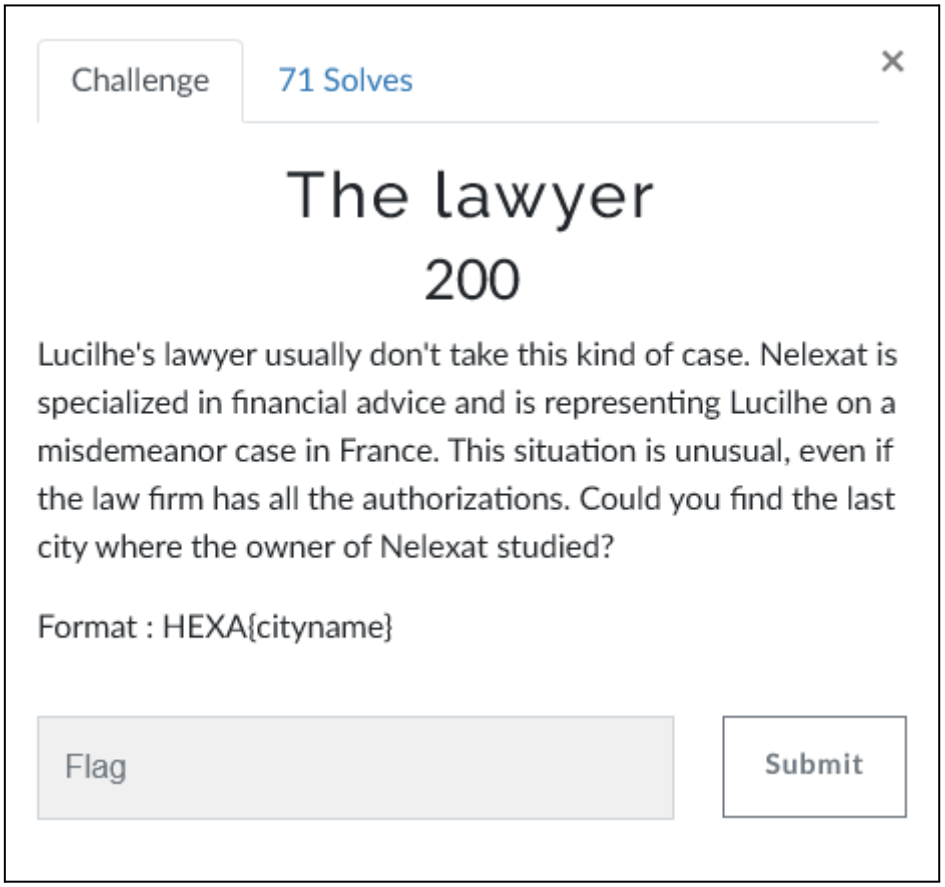
2.4. The Lawyer

2.4.1. The law firm

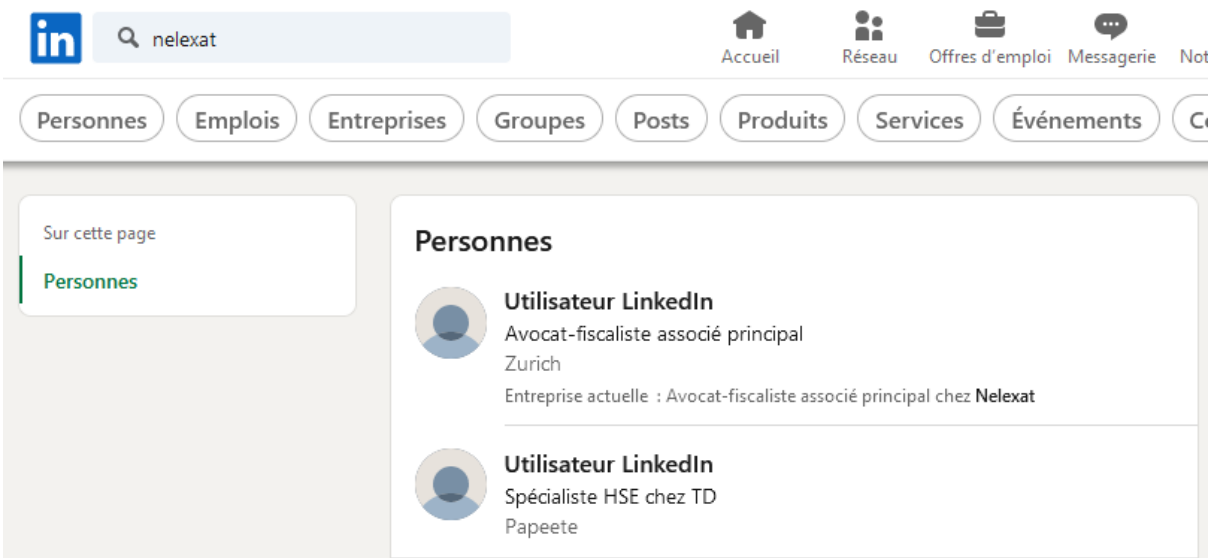


In this challenge, the aim was to find the domain name of the company. The main hint was the name of the company. Given that, we went on who.is to check which "nelexat" domain was taken. It taught us that *nelexat.io* was the only common one taken. However, accessing this website didn't work, so the domain we are looking for is not this one. Reading the challenge again, another piece of intel that was given to us was the country of the company: Switzerland. The TLD (top level domain) of switzerland is "ch". A visit on nelexat.ch let us know that we found the right website. Scrolling to the bottom of the first page, we can find the flag we were looking for: HEXA{N3l3x4t_w1ll_M4ke_You_R1ch}

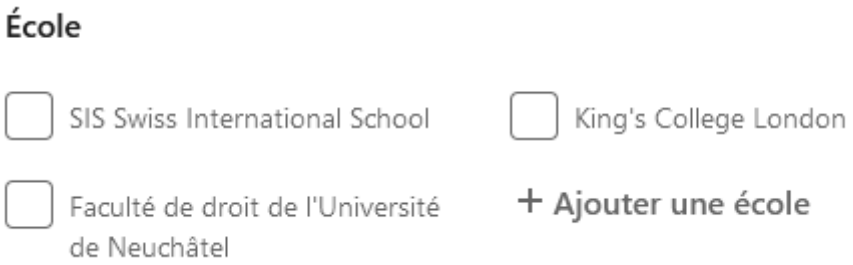
2.4.2. The lawyer



The most famous social network where one writes where he went to school is LinkedIn. That's where we started our research on this challenge. The only piece of information we had was the company our lawyer was from. Searching for "nelexat" show us 2 people. Initially, the first time we arrived here, there was only one, the one working in Zurich. The localization of the company would also help us identify which one was the one we were looking for.

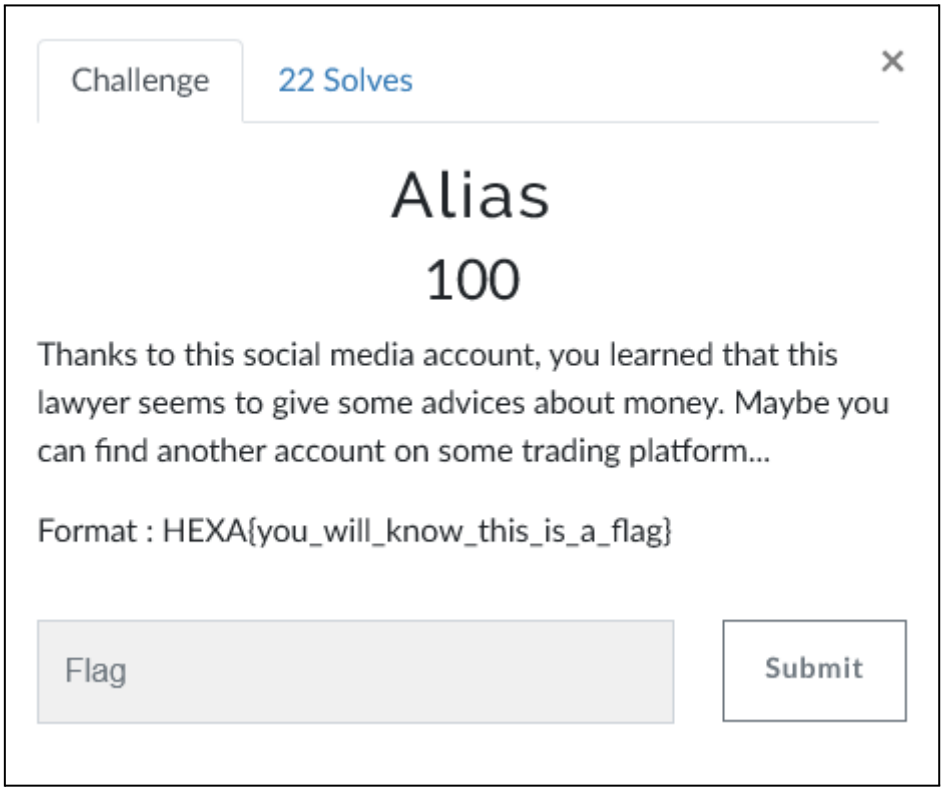


This doesn't help us a lot… However, by looking at the filters available, we can discover some interesting information.

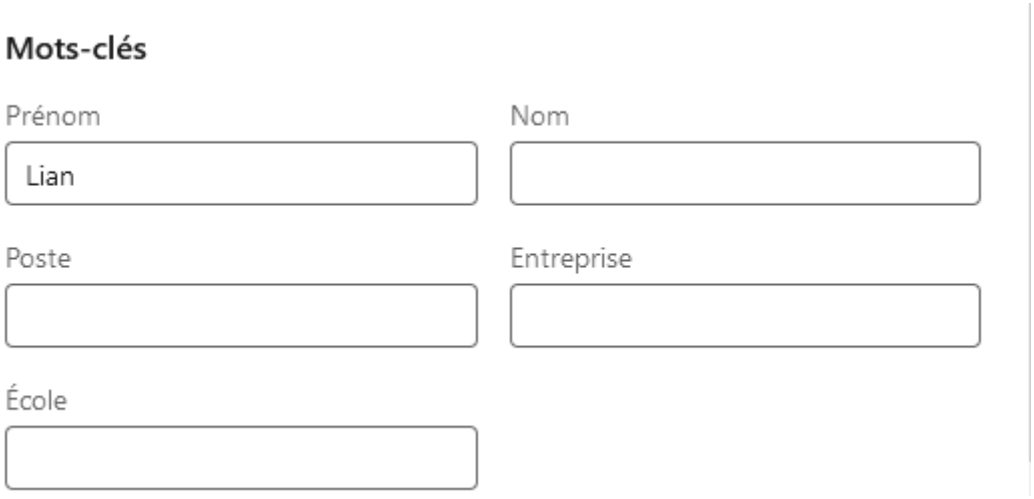


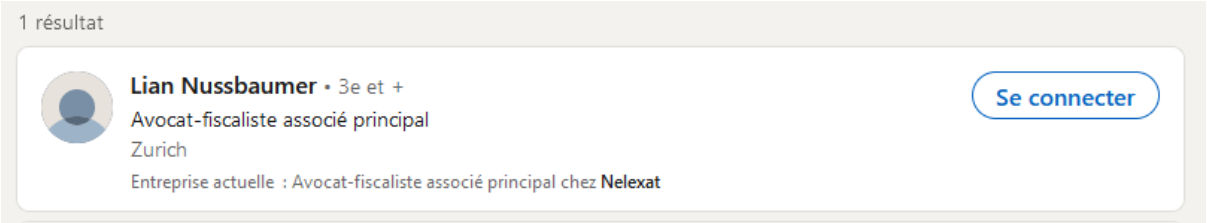
To determine which school our target went to, we need to filter them one by one. Doing so, we can see that he went to King's College London and to "Faculté de droit de l'université de Neuchâtel". However, at this moment of the investigation, we can't be sure which one of the 2 remaining schools he went to first. By trying them, the flag reveals himself: HEXA{london}

2.4.3. Alias



This challenge was the last one we managed to resolve. For the record, we flagged it 22 seconds before the end of the CTF. From the previous challenge, we had the LinkedIn of the lawyer. However, we couldn't access his profile. To be able to access his profile, we used intel we gathered from other challenges. From the herbaceous challenge, we know the lawyer's initials (L. N.), and from the impersonator, we know that someone in the team is named Lian. It looks like our lawyer's name might be Lian. By adding the filter "Lian" as a name in the LinkedIn search, it allows us to see the profile link and click on it.





On his [profile], we can see a bunch of posts, however, one is more interesting for us than the others, because it contains a useful piece of information, his pseudonym: *Nelexlian*.

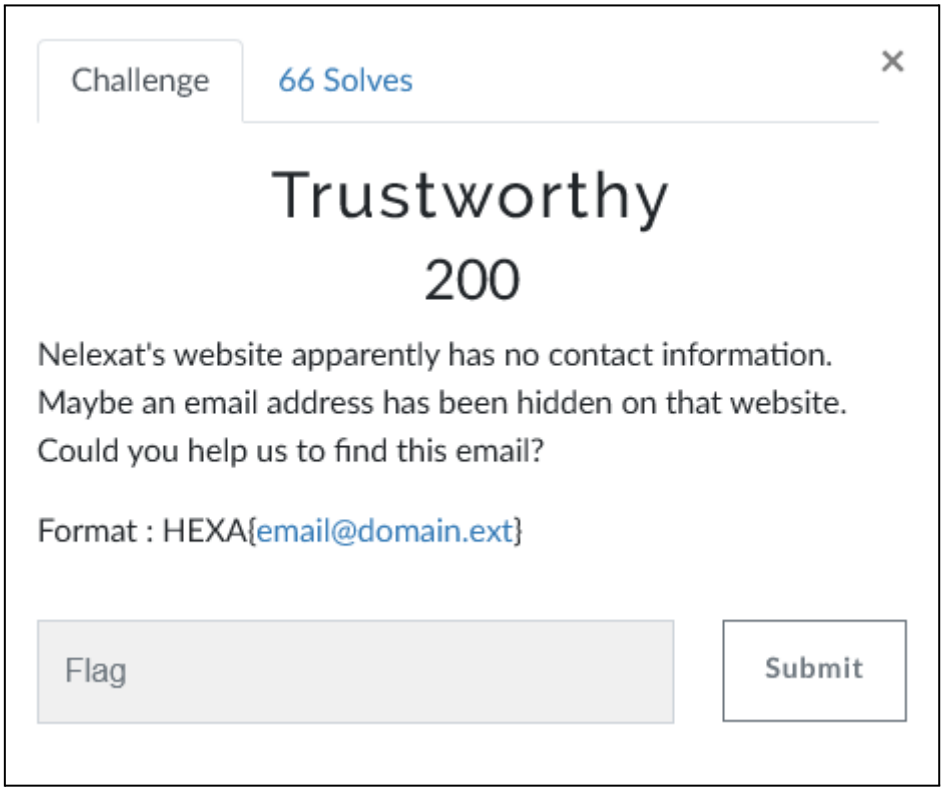
With his pseudonym, we can now search for a trading platform where this lawyer is giving his advice.

We had already searched on google "trading platform social media" to get names of the main trading platforms with a social media aspect, where Lian can possibly share advice with other users.

The one that stands out in many rankings was Etoro.

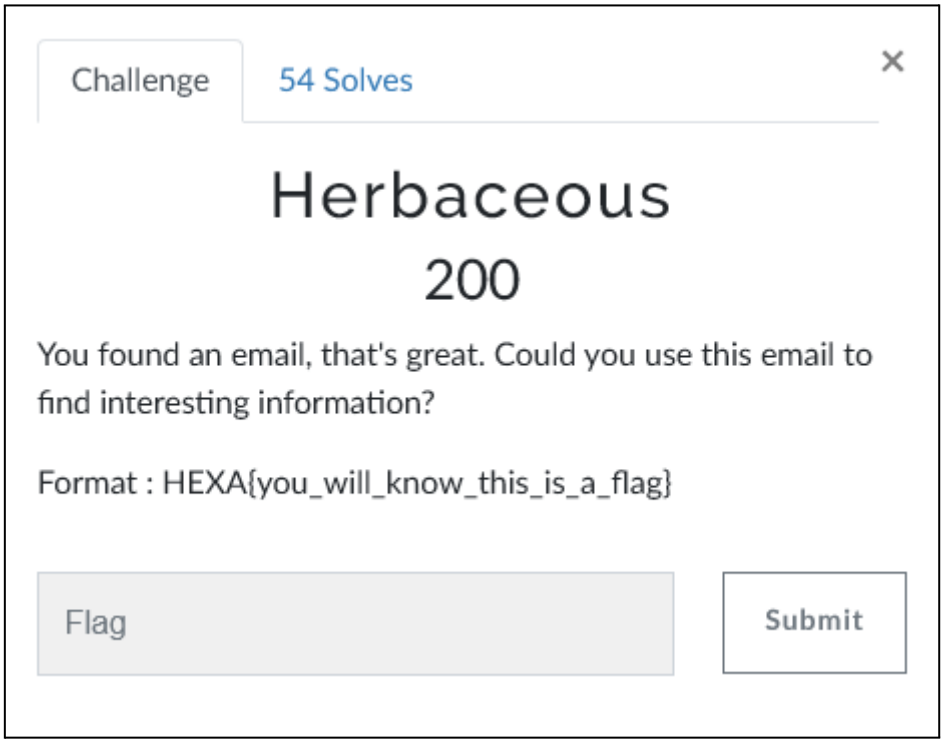
We created a fake account on it and kept the website aside, until we found Lian's pseudonym and tried to search for "Nelexlian" in the eToro search bar. We found this account https://www.etoro.com/people/nelexlian. In the "About Nelexlian" part, we can find the flag HEXA{nelexlian_is_rich}.

2.4.4. Trustworthy



This challenge was about a hidden email on the website. The statement here says that the email address is hidden. It could mean two things. Either the email address is hidden by the target for it not to be found, or the email is in a place the target wouldn't think of. First, we tried to find some "hidden places" on the website. By going on any other pages than the home, we can see the website going to https and we can see that the certificate is from an unknown issuer. What could go wrong? We tried to go to page 404 of the website, which let us know the website is using Wordpress as a CMS, and that an article "Bonjour tout le monde !" was written by "admin4847". At this moment I thought again about the HTTPS and the certificate thing. By clicking on the lock on the address bar, I looked at the certificate. As I started to suspect, the field email address of the certificate's subject was filled. The flag was: HEXA{mastermind_mastermind@proton.me}

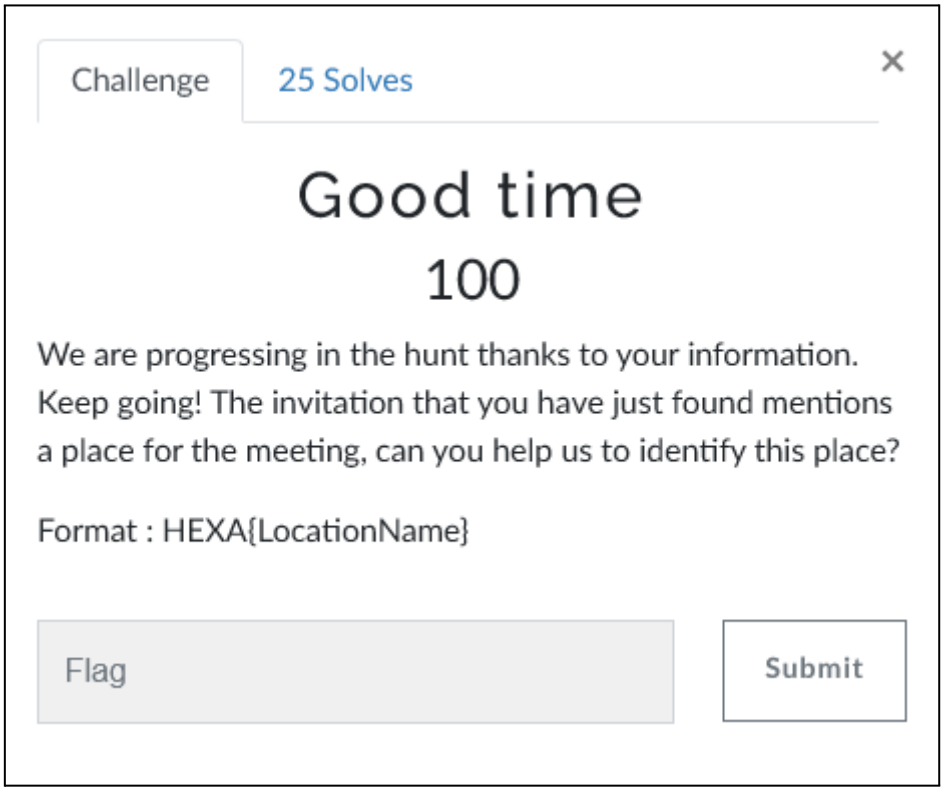
2.4.5. Herbaceous



The last challenge gave us an email address. To find out for which services an email address is used, we decided to use the (famous) tool epieos. We also could have used holehe to do so. This tool lets us know that the email address mastermind_mastermind@proton.me has a google account. In addition to that, it also gives us the maps contribution link and the calendar link. The maps link shows that mastermind has left no reviews on google maps. However, the calendar link is much more interesting. Indeed, on the 16/12/2022, there is a meeting planned at 12pm.

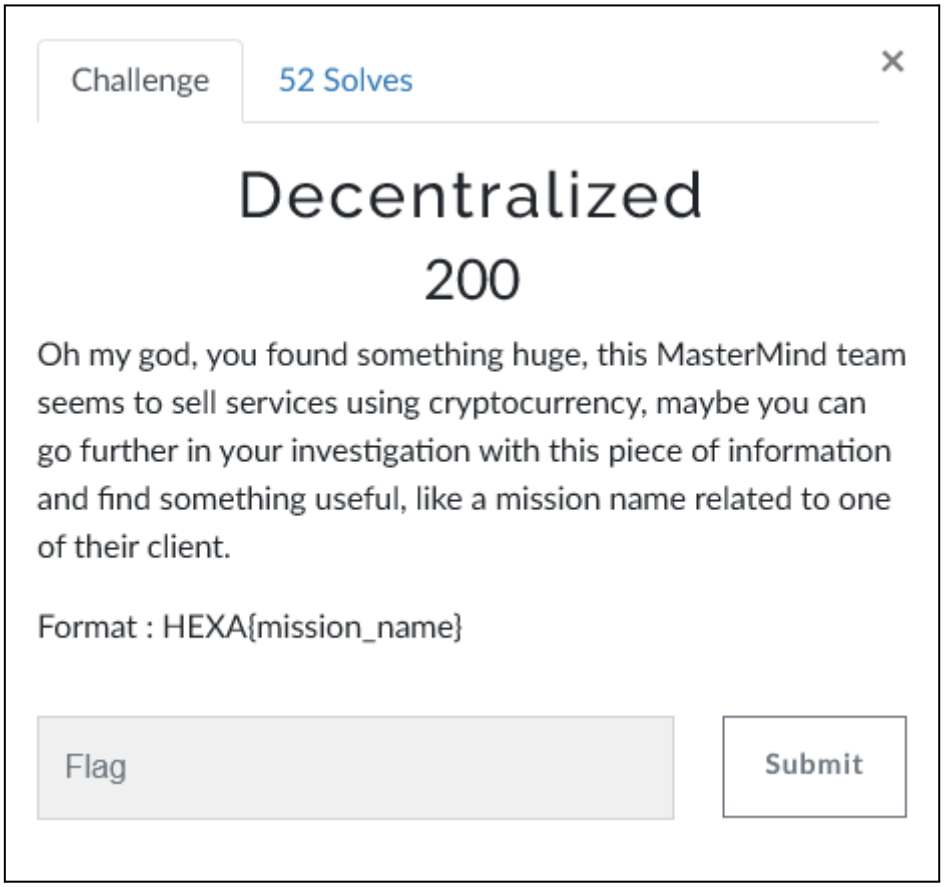
By clicking on more details, we can see the whole text which gives us an onion link: http://nvnomrsfvy3dcq25c5y2stgbptt4dcuiaidugy63zca2vc5vnhetaoad.onion/
This kind of link can be opened with the TOR browser.
If you click on more details while being connected, it opens the details of the meeting as if it was an invitation, allowing us to see who else was invited. 2 other people were invited: mincah_mm@proton.me and vok_0lski@proton.me.
For the end of the challenge, let's go to the onion website. The first page is only a text containing a crypto address (useful for the next challenges) and an image with a link to another page "zones". The zones page only contains a link to download a kmz file (zip file containing geo data). To be sure that nothing was hidden, a look at the source code with the developer console let us see the flag as a comment on the home page: HEXA{N3l3x4t_is_L1nk3d_to_M4stermind}.

2.4.6. Good time

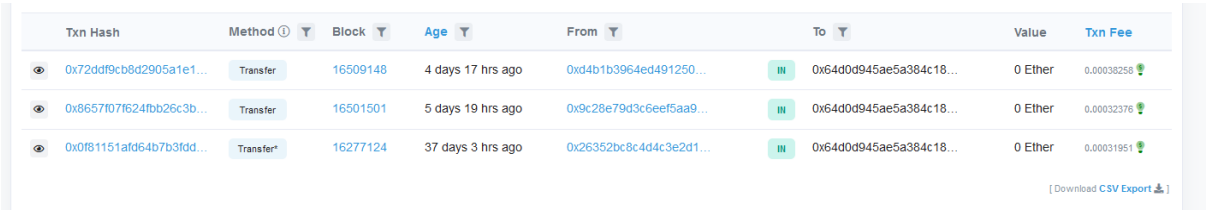


Searching the different nicknames of the people invited in the calendar event ("mincah_mm" and "vok_0lski"), we found a Tripadvisor account of Minca H https://www.tripadvisor.com/Profile/mincah_mm. The account made a review in a restaurant in Zurich, the "Kaufleuten". So the flag is HEXA{Kaufleuten}.

2.4.7. Decentralized



The crypto address we found in the challenge Herbaceous is going to be useful here. The crypto address is: *0x64D0D945AE5a384c18A3876064816b7E141980E7*.
A search on blockchain.com let us know that the address is an ethereum one. For ethereum addresses, etherscan is better than blockchain.com, so here we go. We can see that several transactions have been made to this address (initially there was only the older one.).



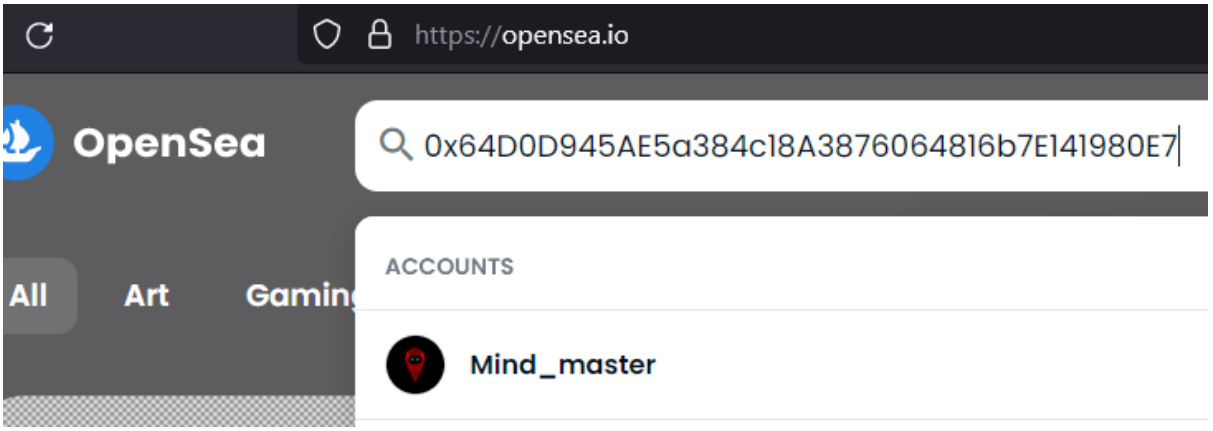
By looking closer, we can see a star near the method used on this specific transaction (we only found it out later, it means that the transaction includes data that may be an utf-8 message). Going on the transaction details, we can see the input data. The drop down allows us to see this data as utf-8. It reveals us a message from the initiator of the transaction:

```
contact mail : tsuyo63@proton.me
code name : Bruised Rogue
```

The flag is: HEXA{bruised_rogue}.

2.4.8. Kanagawa

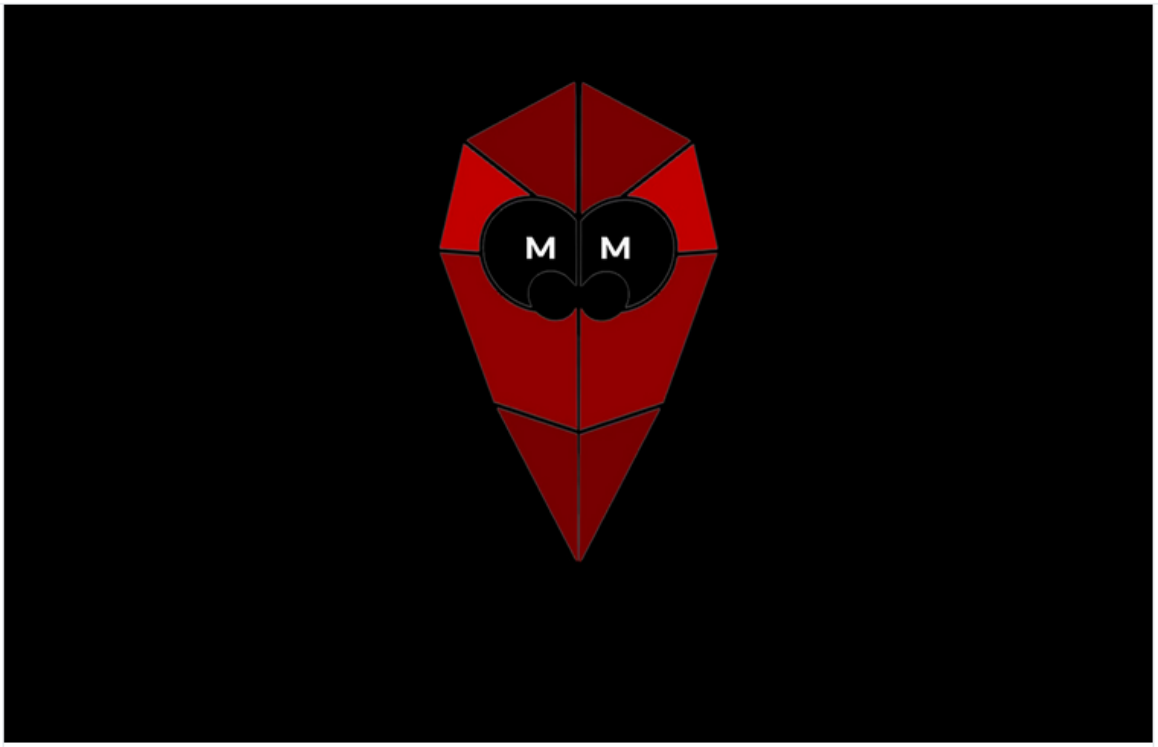
In the challenge statement it's written that the cryptocurrency address found is used for something else. One of the first things that come to mind is the NFT world. With a simple search on DuckDuckGo "famous cryptocurrency platform nft", this link appears: https://www.fool.com/the-ascent/cryptocurrency/nft-marketplaces/. And on this webpage that lists the Best NFT Marketplaces, https://opensea.io/ is the first shown. Then in opensea, there is a search bar where it's possible to paste the cryptocurrency address:



Thanks to that, a “Mind_master” profile appears which contains only one NFT. On this one, there is a description that contains the flag HEXA{n1ce_L0g0_br0}.

OpenSea

Search items, collections, and accounts



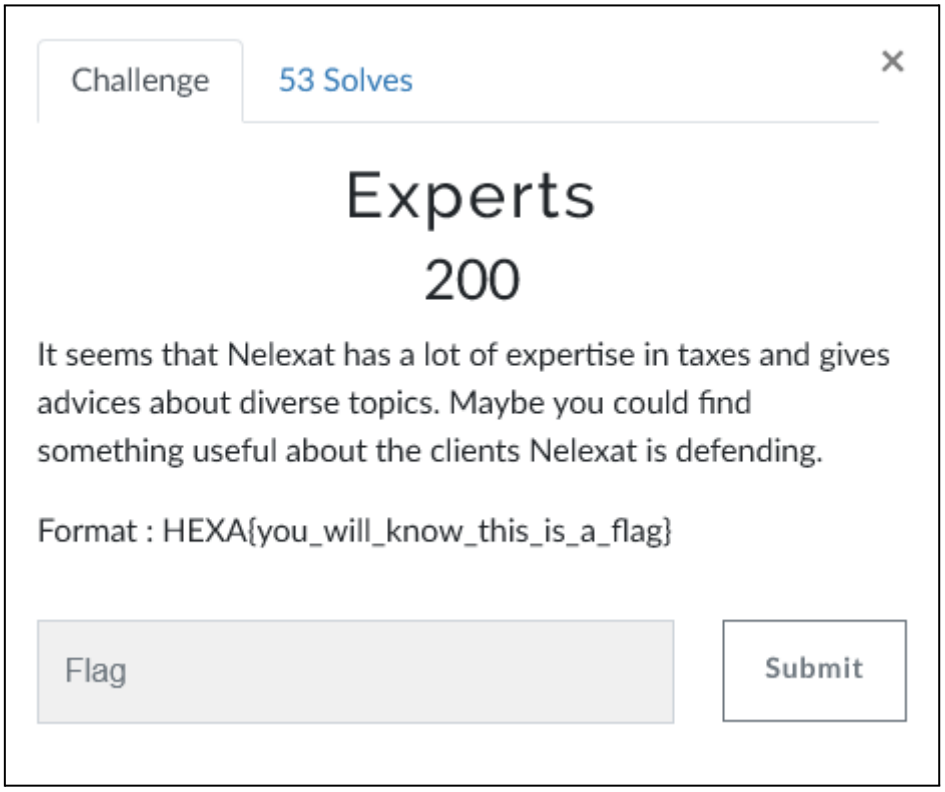
Description

By **Mind_master**

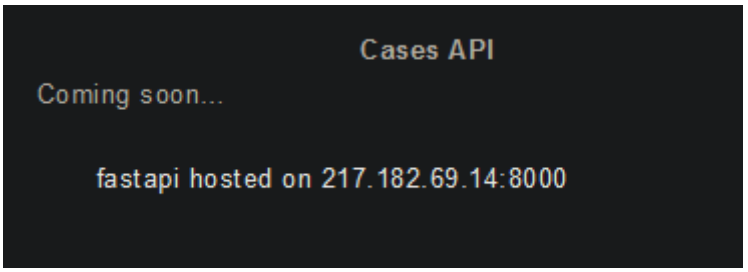
This logo was made with bravery, with pride, with firmness.

HEXA{n1ce_L0g0_br0}

2.4.9. Experts



When looking at every page of Nexelat's website, we found an API on https://www.nelexat.ch/index.php/our-advices/. Dark Reader's dark theme was very useful as text remained white but the background was changed so we saw it directly.



As it is a FastApi, we are searching for a Swagger file referencing all the endpoints. Thanks to the doc (https://fastapi.tiangolo.com/tutorial/first-steps/) we know it is available under the */docs* endpoint.

On http://217.182.69.14:8000/docs, we can search for cases using clients names, or missions using mission names. As we know one of the clients, Lucilhe Dumarquais,

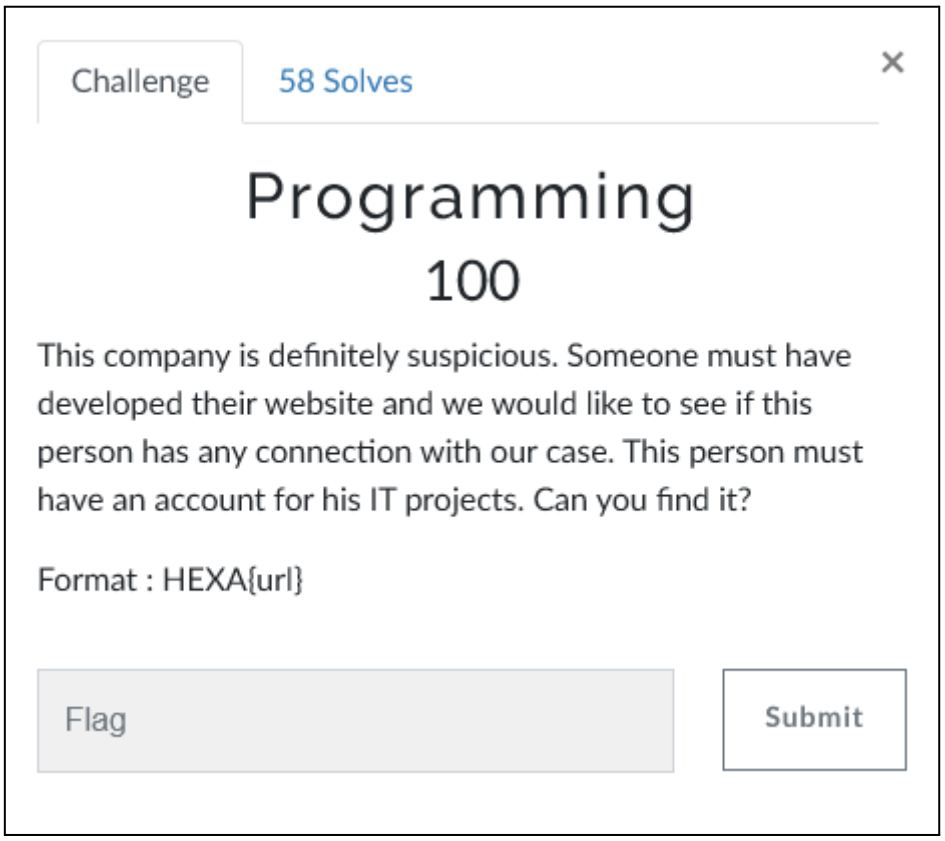
we can try to execute a request on:
http://217.182.69.14:8000/cases/{client_last_name_lowercase}?name=dumarquais
It returns:

```
{
  "name": "dumarquais",
  "description": "This case is related to Lucilhe Dumarquais, head of Manipar organization, which was organizing a data traffic. After a bitter battle with the opposing lawyers, I managed to get a lighter sentence in a prison in France, without my client having to give any information about the people she was working with. HEXA{s3cure_y0ur_d4mn_4p1}"
}
```

Flag: HEXA{s3cure_y0ur_d4mn_4p1}

2.5. The Developer

2.5.1. Programming



We are looking for an account for an IT project. The first idea we had was to go on GitHub and search if we couldn't find a project named "Nelexat". However, no relevant result.

If the developer used Git to do his versioning, we may be able to find traces on the site. Our second idea was to check if the site was published with the development information. These are contained in a ".git" folder in the project directory. So we searched for the URL https://www.nelexat.ch/.git and it exists! We will be able to find the elements we are looking for.

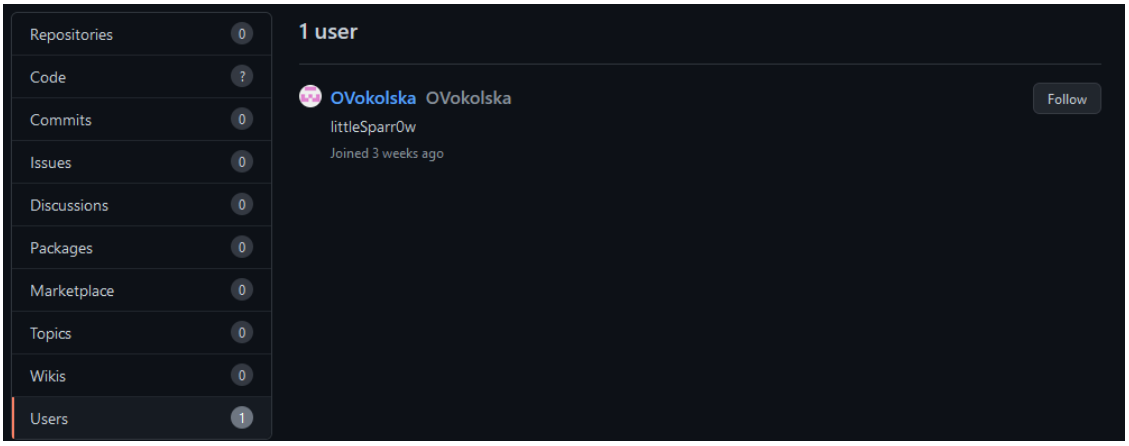
Index of /.git

Name	Last modified	Size	Description
Parent Directory		-	
COMMIT_EDITMSG	2023-01-14 16:27	21	
FETCH_HEAD	2023-01-14 16:27	0	
HEAD	2023-01-14 16:27	23	
config	2023-01-14 16:27	189	
description	2023-01-14 16:27	73	
hooks/	2023-01-14 16:27	-	
index	2023-01-14 16:27	217	
info/	2023-01-14 16:27	-	
logs/	2023-01-14 16:27	-	
objects/	2023-01-14 16:27	-	
refs/	2023-01-14 16:27	-	

We had a config folder, https://www.nelexat.ch/.git/config, and it contains developer information.

```
[core]
        repositoryformatversion = 0
        filemode = false
        bare = false
        logallrefupdates = true
        symlinks = false
        ignorecase = true
[user]
        name = OVokolska
        email = ovokolska@protonmail.com
```

We can now search for the developer's name on Github and find his profile page: https://github.com/OVokolska. Flag: HEXA{https://github.com/OVokolska}.



During our research, we were able to investigate the .git on the site. To do this, we retrieved the .git folder with the *wget* command:

```
wget --mirror --no-check-certificate https://www.nelexat.ch/.git
```

Now that we have retrieved the elements, we can dig into the site. With the "branch" command, we see the different branches available in the directory. We see the “master” branch, which is the main branch, and another branch called "feature-live-chat". This one catches our eye.

```
osint@osint-VirtualBox:~/www.nelexat.ch$ git branch
warning: ignoring broken ref refs/heads/index.html
warning: ignoring ref with broken name refs/heads/index.html?C=D;O=A
warning: ignoring ref with broken name refs/heads/index.html?C=D;O=D
warning: ignoring ref with broken name refs/heads/index.html?C=M;O=A
warning: ignoring ref with broken name refs/heads/index.html?C=M;O=D
warning: ignoring ref with broken name refs/heads/index.html?C=N;O=A
warning: ignoring ref with broken name refs/heads/index.html?C=N;O=D
warning: ignoring ref with broken name refs/heads/index.html?C=S;O=A
warning: ignoring ref with broken name refs/heads/index.html?C=S;O=D
  feature-live-chat
* master
osint@osint-VirtualBox:~/www.nelexat.ch$
```

So we’re going on it.

```
osint@osint-VirtualBox:~/www.nelexat.ch$ git checkout feature-live-chat
D       MM.css
M       index.html
Switched to branch 'feature-live-chat'
```

We look at the latest changes made to the branch.

```
osint@osint-VirtualBox:~/www.nelexat.ch$ git log
commit f01c7bb2a9c3ebae0bcae3a9cfd0398cf204d185 (HEAD -> feature-live-chat)
Author: OVokolska <ovokolska@protonmail.com>
Date:   Sat Jan 14 16:06:19 2023 +0100

    update livechat.html

commit b5788ee7edd5d95c8ea5c3ecc99d833ab7cd37a9
Author: OVokolska <ovokolska@protonmail.com>
Date:   Sat Jan 14 15:06:40 2023 +0100

    init livechat page

commit 492b16ee4c7346548574ae0714bb86f1e289e610 (master)
Author: OVokolska <ovokolska@protonmail.com>
Date:   Tue Jan 10 20:25:41 2023 +0100

    add stylesheet
```

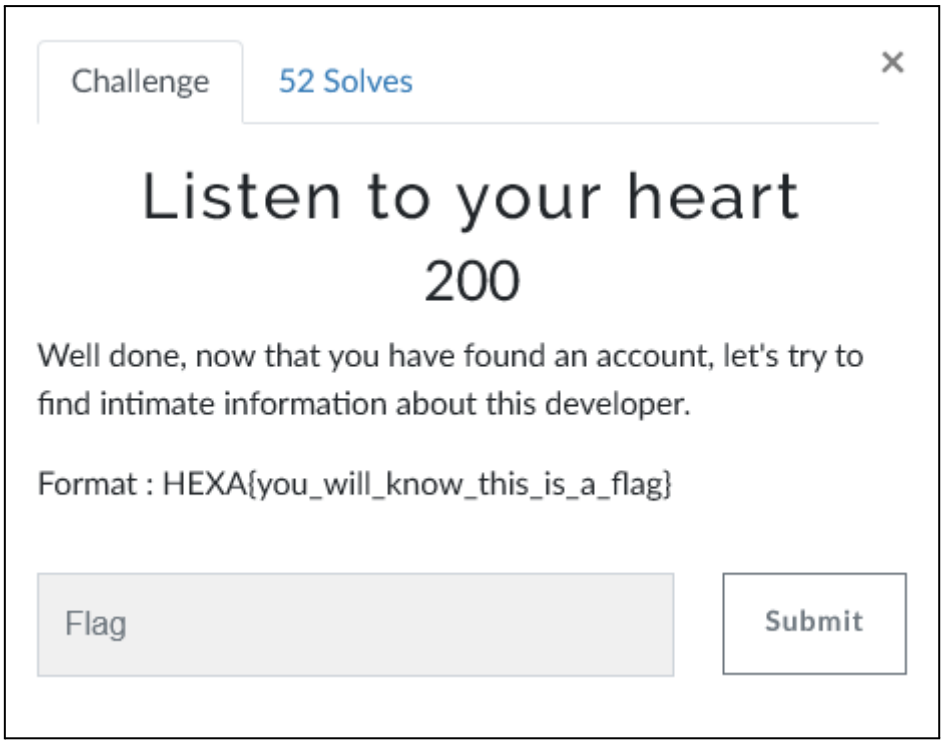
We are interested in the last commit made. We can see the changes that have been made. Two lines have been removed and 3 lines have been added. The deleted lines are about a woman with hazel eyes. This information helped us in the analysis requested at the end of the CTF.

```
osint@osint-VirtualBox:~/www.nelexat.ch$ git show
commit f01c7bb2a9c3ebae0bcae3a9cfd0398cf204d185 (HEAD -> feature-live-chat)
Author: OVokolska <ovokolska@protonmail.com>
Date:   Sat Jan 14 16:06:19 2023 +0100

    update livechat.html

diff --git a/livechat.html b/livechat.html
index 4da4816..13b3da0 100644
--- a/livechat.html
+++ b/livechat.html
@@ -4,7 +4,8 @@
     <link rel="stylesheet" href="MM.css">
         </head>
   <body>
-    <h1>MM - Online services exchange</h1>
-    <!--TODO : Asking the hazel eyed woman what she needs-->
+    <h1>MM - Livechat</h1>
+    <h2>COMING SOON</h2>
+    <!--TODO (low priority): Schedule a call to discuss the feature-->
   </body>
 </html>
\ No newline at end of file
osint@osint-VirtualBox:~/www.nelexat.ch$
```

2.5.2. Listen to your heart

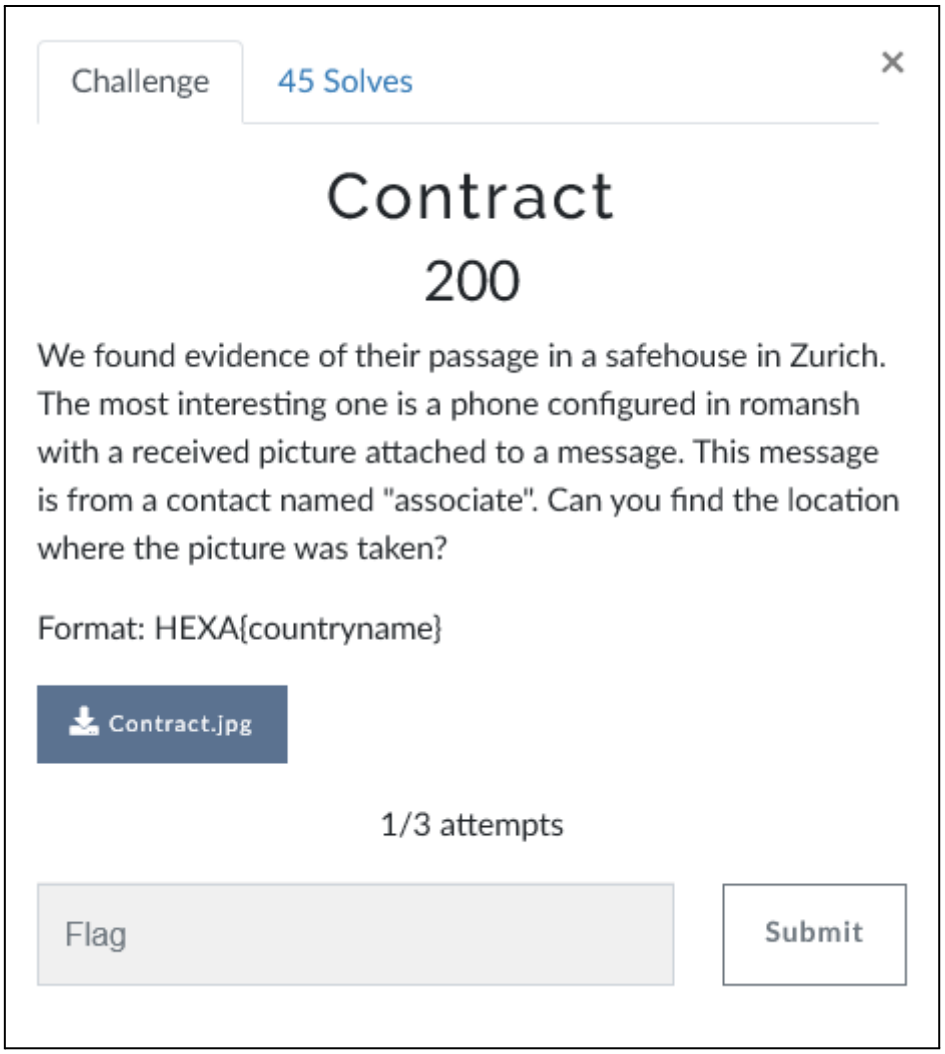


The developer's github page is not very active. However, we found two things: in his bio it says "littleSparr0w" and he liked a Mastodon web client project. We first tried to search accounts with the username “OVokolska” but no conclusive results. Then, we searched for the nickname “littleSparr0w” and an account caught our attention, a Mastodon account: https://cyberplace.social/@littlesparr0w. By going to the URL, we find the flag: HEXA{mY_H34R7_i5_pURp13} .

We also noticed that the message had been modified and before containing the flag, it was referring to a link. However, we did not have time to investigate this link further.

2.6. The Associate

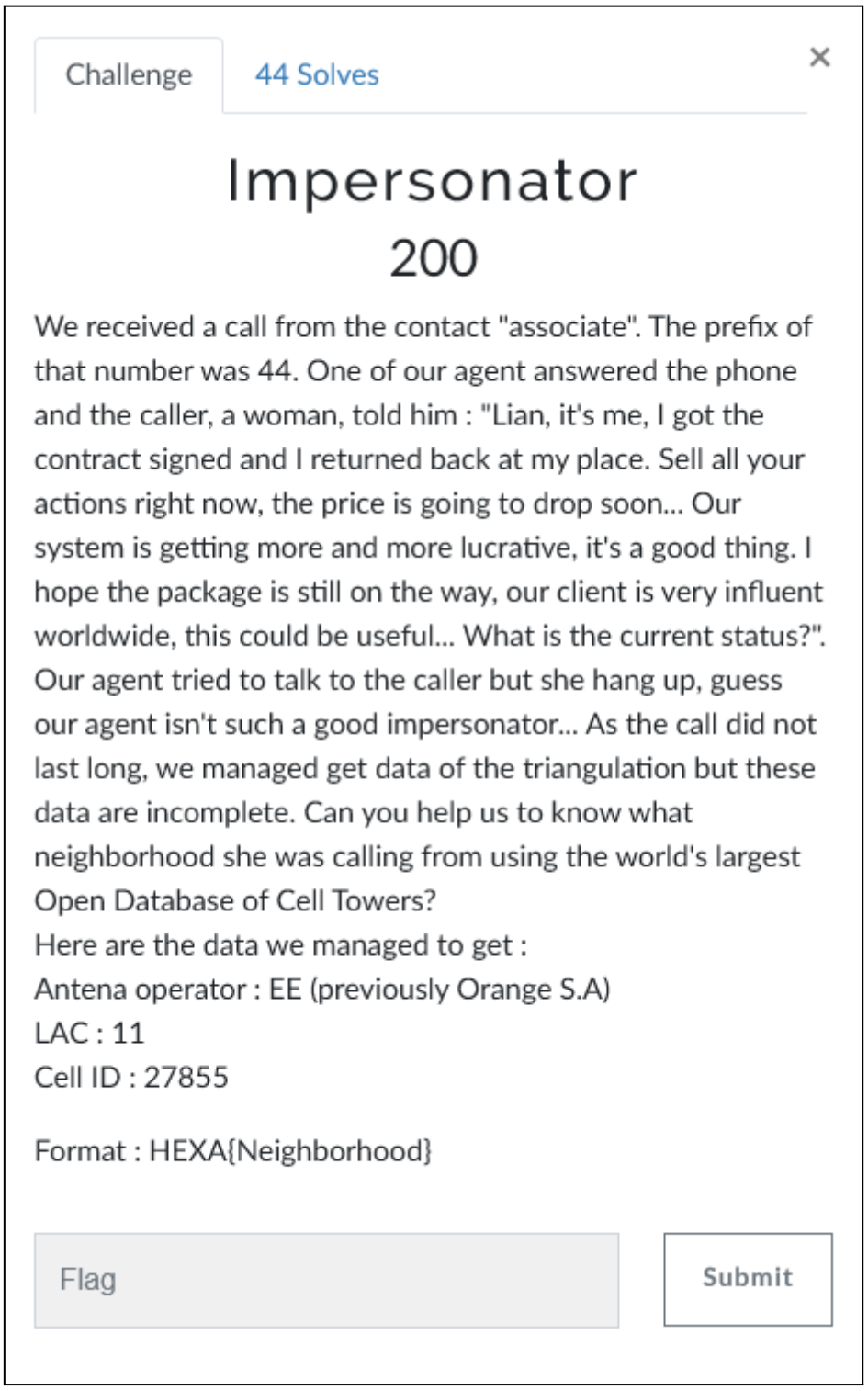
2.6.1. Contract



By looking at the EXIF of the image, we recover a date (24/11/2022 13:17) and also the time zone of the country in which it was taken (UTC+4). On the image, we can see numbers "14 32" written on the floor, indicating the orientation of the runway.

Then, we searched for countries in the UTC+4 timezone with an airport with “14/32”. The search "aéroport 14/32 Maurice" brings us to an airport corresponding to the photo taken: HEXA{Maurice}.

2.6.2. Impersonator

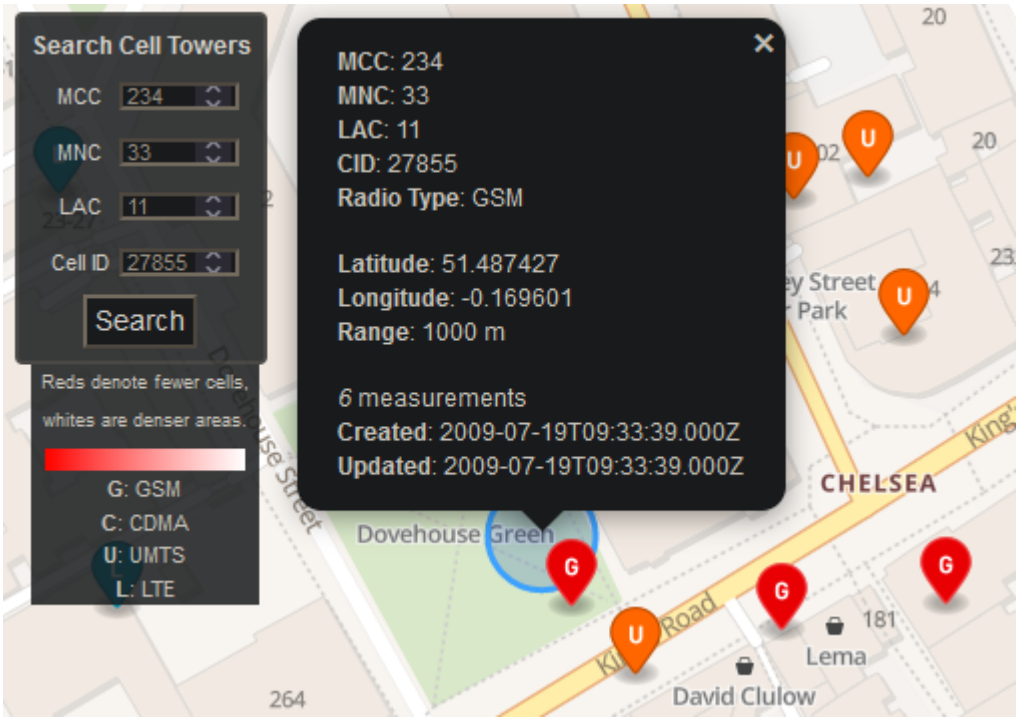


As the challenge says, we need to use the “world's largest Open Database of Cell Towers”. Then, we search for it and find https://opencellid.org.

To find a phone on it, we need 4 items: MCC, MNC, LAC and Cell ID. As we already have the last two, we have to find the MCC and MNC knowing the antenna operator: EE (previously Orange S.A.) and the prefix number: +44 (corresponding to UK).
To find correspondences, we opened https://mcc-mnc.net/. There is only a two in UK, owned by EE:

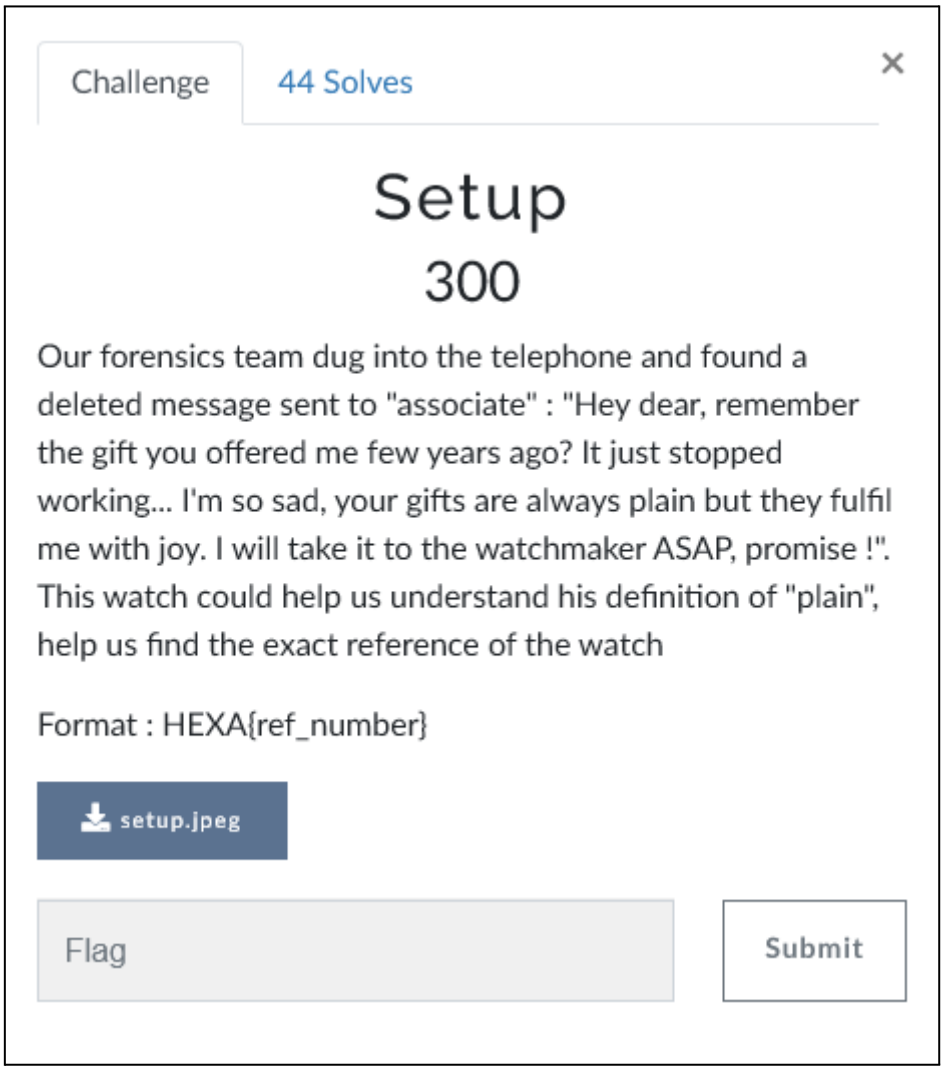
- MCC = 234 / MNC = 33
- MCC = 234 / MNC = 34

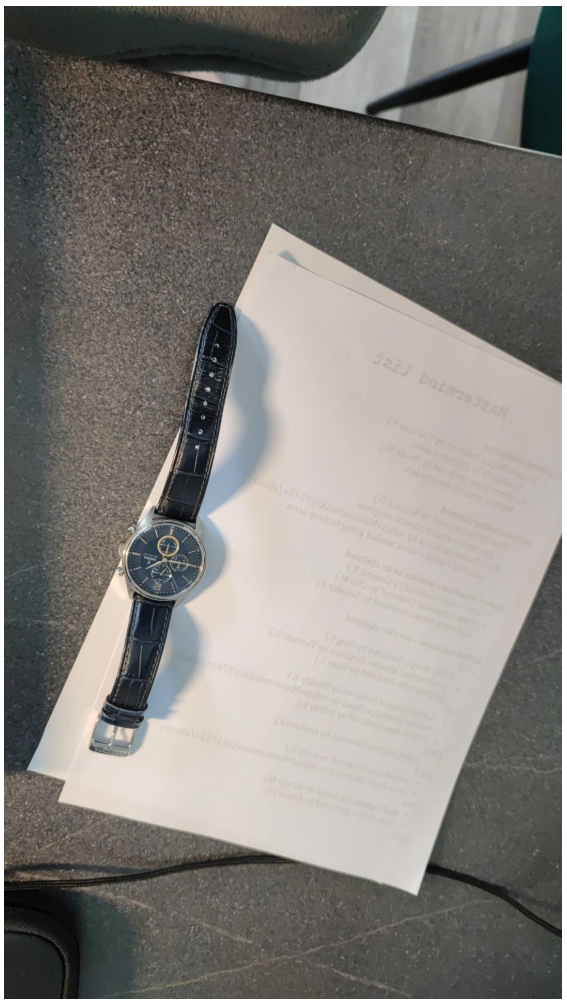
When entering the following parameters in OpenCellID: MCC = 234 / MNC = 33 / LAC = 11 / Cell ID = 27855, we find a location in Chelsea.



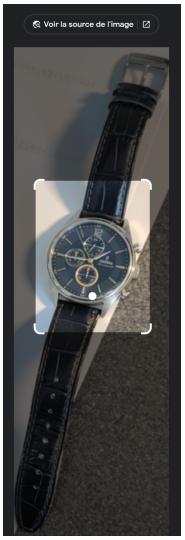
Flag: HEXA{Chelsea}

2.6.3. Setup


Challenge
44 Solves
Setup
300
Our forensics team dug into the telephone and found a deleted message sent to "associate" : "Hey dear, remember the gift you offered me few years ago? It just stopped working... I'm so sad, your gifts are always plain but they fulfil me with joy. I will take it to the watchmaker ASAP, promise !". This watch could help us understand his definition of "plain", help us find the exact reference of the watch
Format : HEXA{ref_number}
setup.jpeg
Flag
Submit

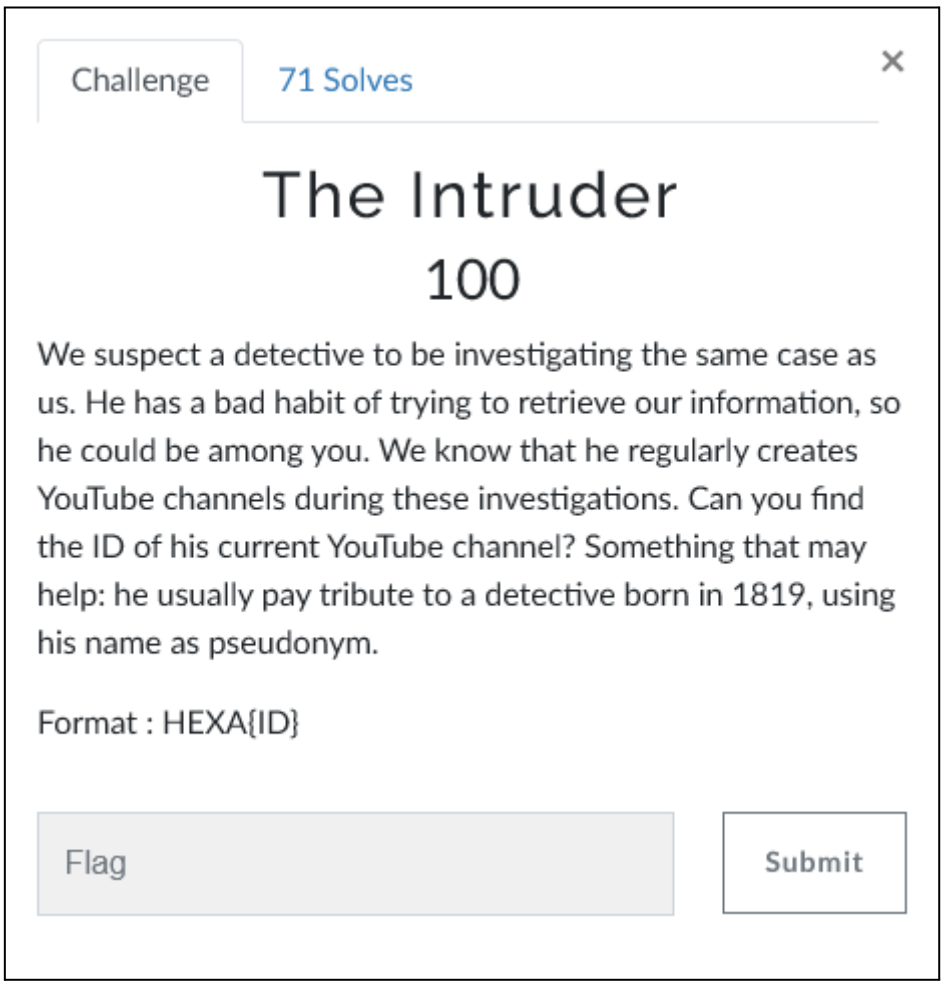


This challenge is pretty simple, we just had to turn the image and do a search via Google Lens on the watch. We got “Montre Festina Homme Chrono Acier Cuir Bleu F20286/3”.
https://fr.shopping.rakuten.com/offer/buy/2425062830/montre-festina-homme-chrono-acier-cuir-bleu-f20286-3.html The flag is HEXA{F20286/3}.



2.7. The Intruder

2.7.1. The Intruder



First, we searched for a famous detective born in 1819. Without searching very far, we found Allan **Pinkerton**, who made one of the most famous detective agencies.

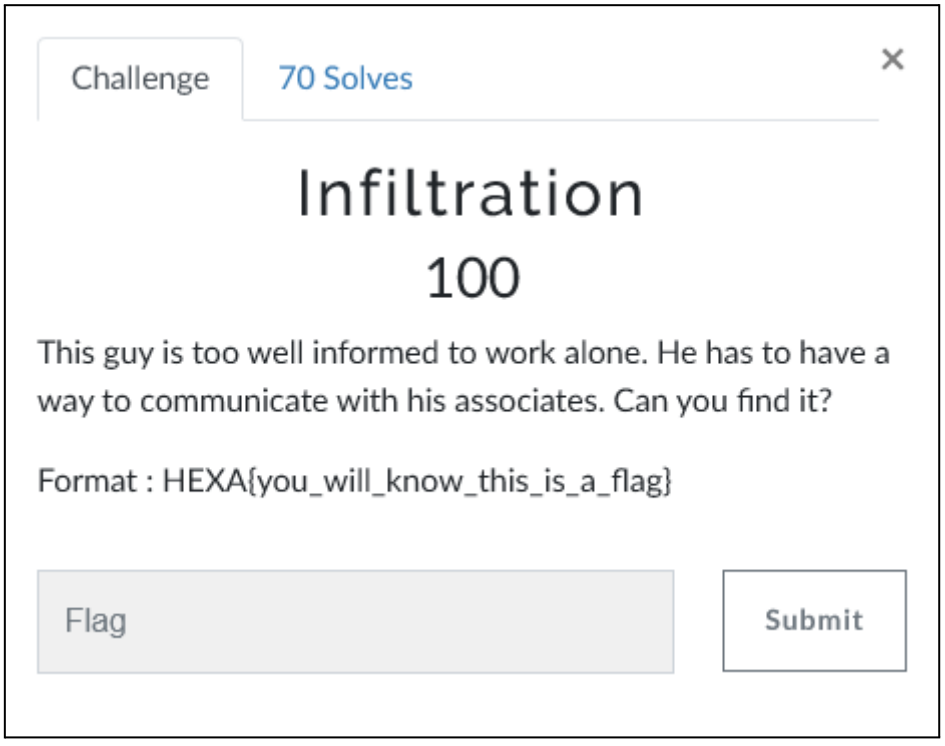
After searching for hours for Pinkerton on Youtube, we decided to read the challenge statement once more. But this time, instead of giggling at “He could be among us”, it made sense: What if it broke the 4th wall and Pinkerton was really among us for the CTF ?

We searched for Pinkerton among the users of the CTFd. Eureka! There he was, with a link pointing to his Youtube channel : https://hexactf.ctfd.io/users/109

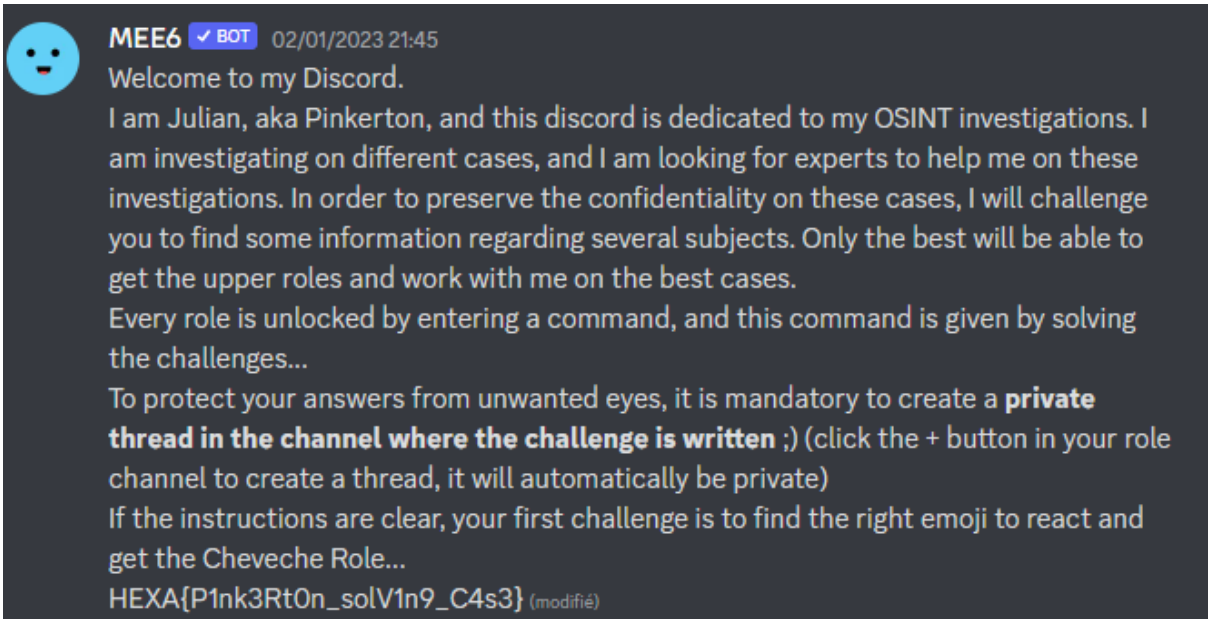
https://www.youtube.com/channel/UCjyLqrOsjkpsMhczlbHJoFA

Flag: HEXA{UCjyLqrOsjkpsMhczlbHJoFA}

2.7.2. Infiltration

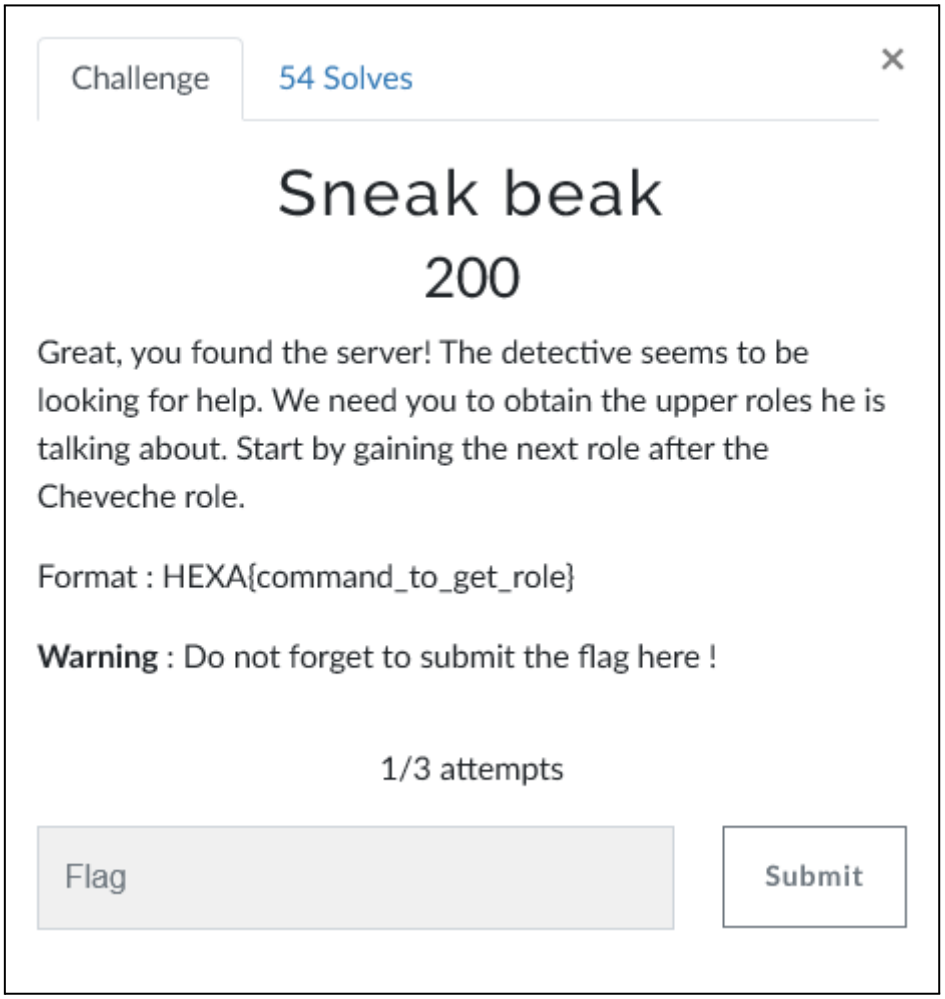


On Pinkerton's Youtube channel, we can find a short video (https://www.youtube.com/shorts/nhh7Z8gnDmA) with the alias of what looks like a TikTok account (@user545947198194).
In the description of this account, we find a link to a discord server: https://discord.gg/unsb62pMc7.
When joining the discord server, we find the flag in the welcome message.



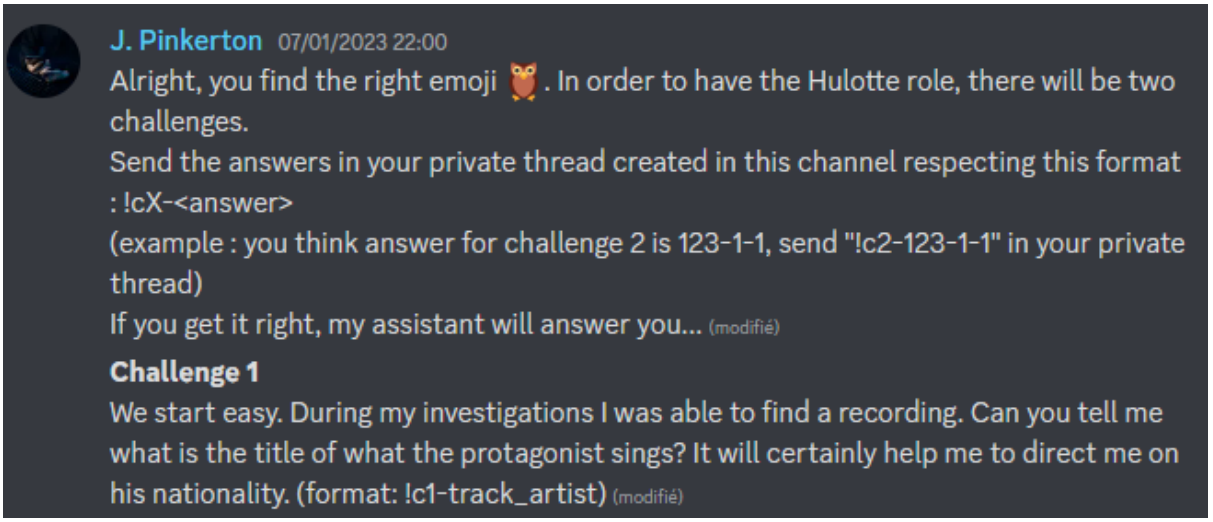
Flag: HEXA{P1nk3Rt0n_solV1n9_C4s3}

2.7.3. Sneak beak



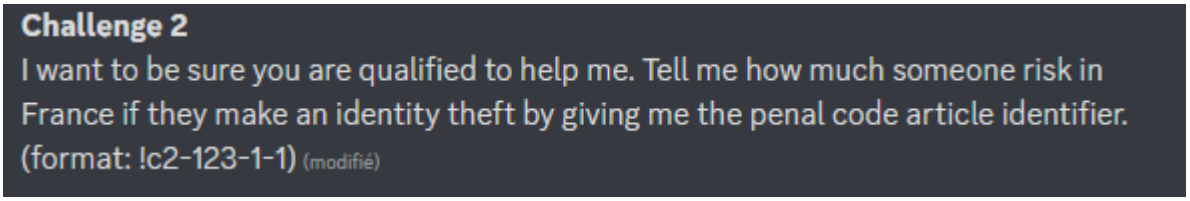
On the Discord server it was needed to resolve small challenges to access a more privileged role in the goal to meet Pinkerton. To obtain the first role, it was needed to solve two challenges:

2.7.3.1. Challenge 1



The first challenge included a .mp4 video with a fixed black picture. Nevertheless, it was the audio which was interesting. Indeed, a person was singing something. At the second 14 we can hear the only lyrics “Catolina”. This lyric is absolutely not useful because it’s the only one and OSINT searches gave nothing interesting. The smart part was to use a music recognizer like the Google assistant. Thanks to the context of the music variation around the lyric, Google retrieved a list that potentially corresponded to this music. The first was Lemonade from the bonobos group which corresponded at 8% of the music. Before entering the flag, it was important to listen to this music to confirm the recognition. And indeed it was this one. The flag was then `!c1-lemonade-bonobos`.

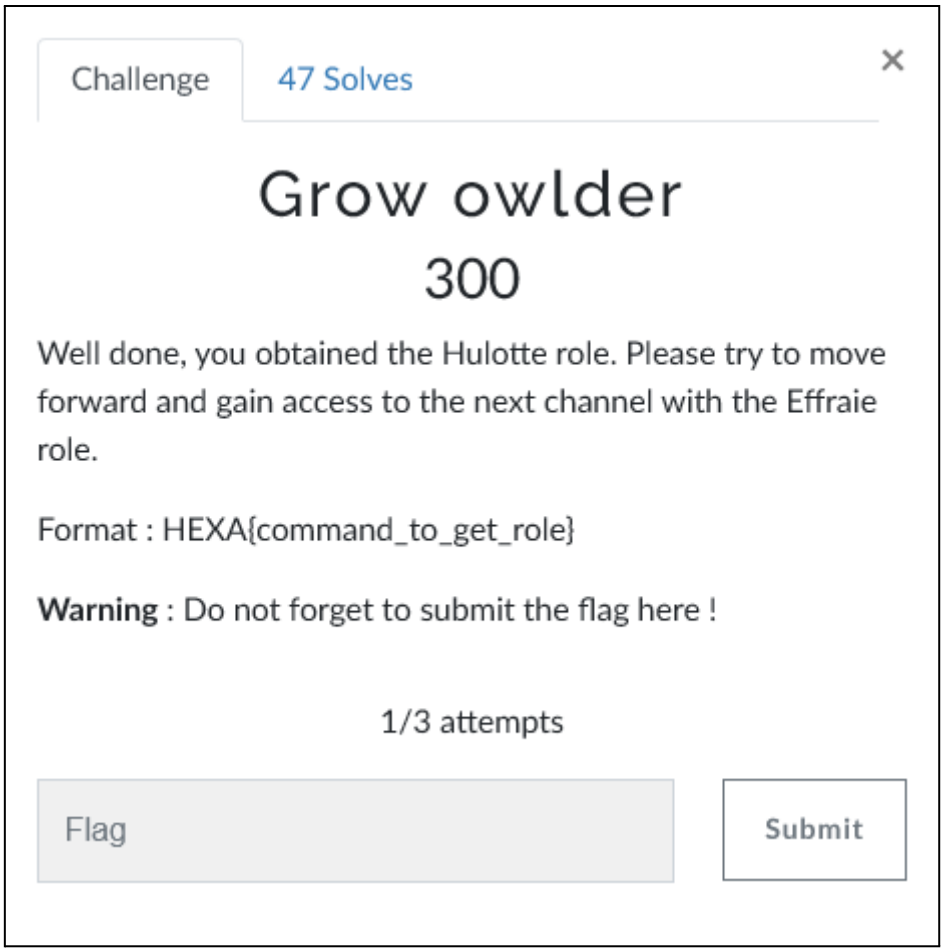
2.7.3.2. Challenge 2

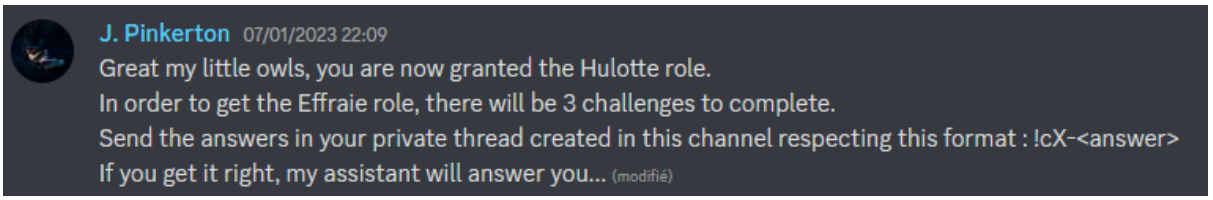


For this challenge, it was necessary to do a search with DuckDuckGo or Google with the key word in French of the statement “usurpation d'identité france code penal”. This one gave a link to https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042193593/ which included the article number. The flag was `!c2-226-4-1`

Finally, after giving those two flags, the bot gave the command !yxmdvbn5jvwnnjy3htfe to have the next Discord role. The flag was then HEXA{!yxmdvbn5jvwnnjy3htfe}.

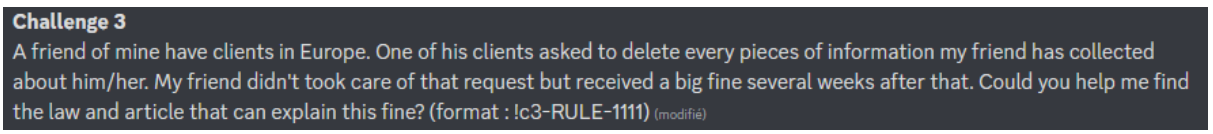
2.7.4. Grow owlder





Ok, let's go for 3 more challenges.

2.7.4.1. Challenge 3



For this challenge, we had to find an article of a European law about data collection. It looks like we are searching an article of the GDPR about data deletion. When searching "GDPR deletion", we find: https://gdpr-info.eu/art-17-gdpr/ about the right to erasure.

Answer: !c3-GDPR-17

2.7.4.2. Challenge 4

Challenge 4
I heard from an US federal agency that there is a lot of inflation on food price in US last year, could you find the exact percent change for Month-to-month October 2022 to November 2022 on eggs? (format : !c4-1111 - percentage with no separator - example : answer is 5,3, just send !c4-53) (modifié)

For this challenge, a research on google with the keywords "egg change October 2022 November USA month by month" led us to find this website. Here, we can have the price of eggs per month. In October 2022 it was 3.419 and in November, it was 3.589. From those information we can infer that the price of the eggs changed by (3.589 - 3.419) / 3.419 * 100 = 4.97…% However, this answer doesn't work, there must be another way to find what Pinkerton is looking for.
To do so, a quick search using another search engine (bing) and the search "egg price US november up" let us find this article that let us know that "Egg prices jumped 2.3% just in the month of November, and by 10.1% in October, according to the CPI".
Answer: !c4-23

2.7.4.3. Challenge 5

Challenge 5
I am working on a very important OSINT case. A contact sent me an image from a camera filming adriatic sea, but couldn't give me the source... My contact just told me that the camera is set on an hotel in Veneto, maybe that will help you to find this camera. One more thing... From this camera, we can see a panel where "Fantasy" is written. If you can find this camera, give me the phone number of the hotel (format: !c5-39XXXXXXXXXX). (modifié)

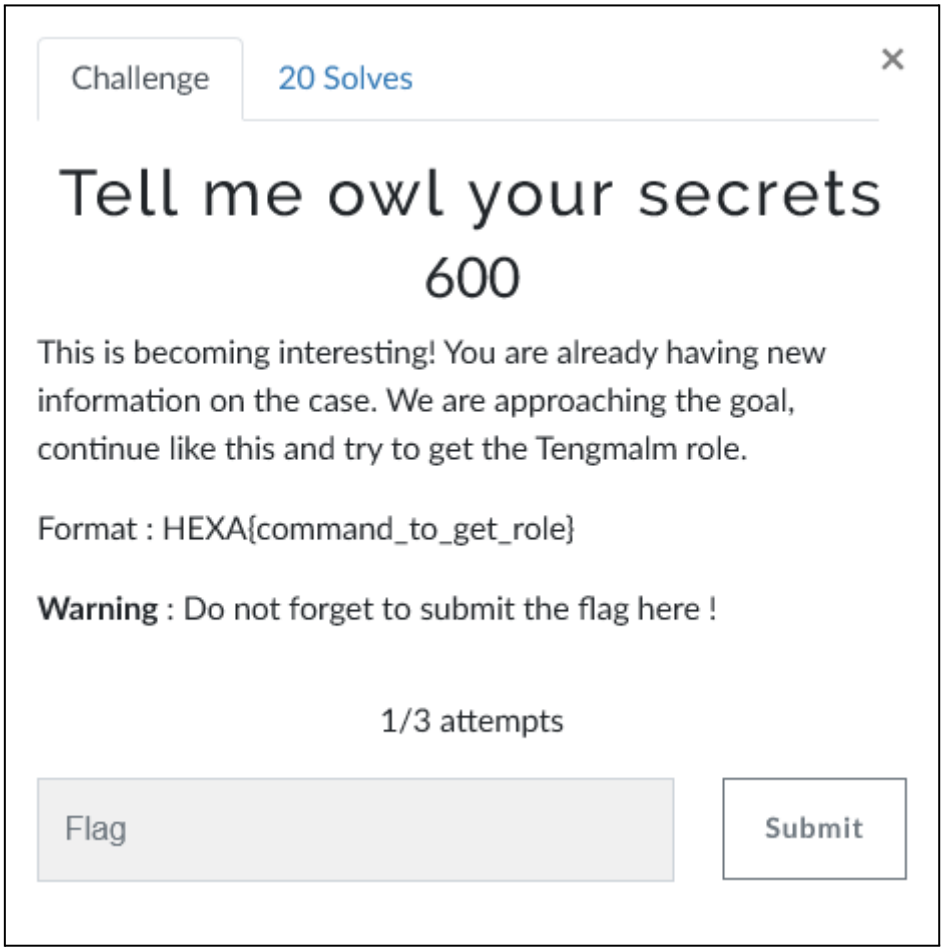
We are searching for a webcam in Veneto. Most of our research is pointing to https://www.skylinewebcams.com. After a few minutes on this site, we find a webcam which looks like the one we are searching: https://www.skylinewebcams.com/fr/webcam/italia/veneto/venezia/chioggia-sottomarina.html

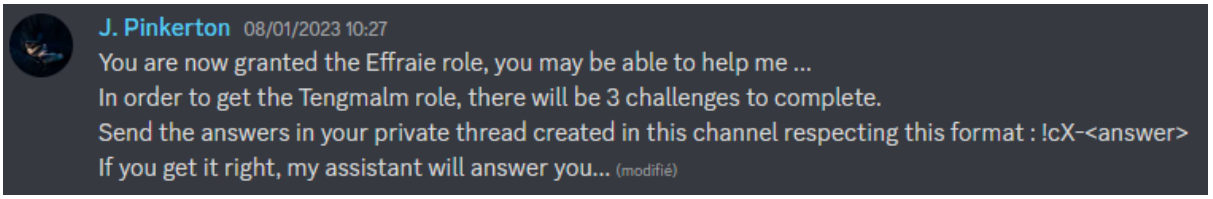
We can clearly see a panel where “Fantasy” is written.

We find the name of the hotel at the top of the video: Hotel Ambasciatori.
When we search Hotel Ambasciatori, Veneto, Chioggia on Google maps, we find it, near Pizza Fantasy! Their phone number is +390415540660.

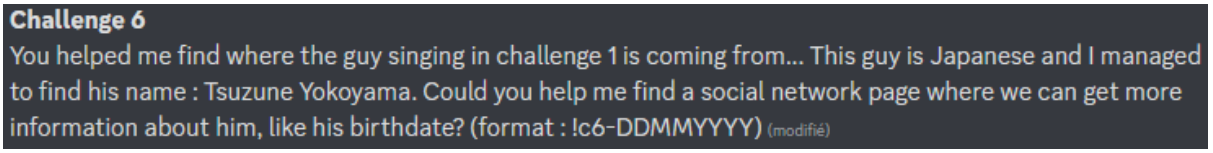
Answer: !c5-390415540660

2.7.5. Tell me owl your secrets





2.7.5.1. Challenge 6



For this challenge, we went through a hard time. We only had a surname and a name, and that the guy is japanese. First, we tried some combination of the name and the surname to create an alias he could have used to search it via whatsmyname.app. However, nothing came up. We thought that the name sounded strangely familiar, and so we used the email address tsuyo63@proton.me we found during the challenge Decentralized. Nothing came up neither via holehe

nor via epieos. At this moment, we thought that maybe the fact that the guy was Japanese should be a better help than just trying to translate his name and googling it. So we searched what is the most famous social network used in Japan, and apparently Line was one of the most used. So we tried to install Line, but to do so, we needed to use a phone number to receive the confirmation code and to do the inscription. It was a little problematic because we had no phone coverage where we were located so we had to run outside (it was kinda cold) to receive the sms.

Once the registration was complete, we searched for TsuzuneYokoyama and found the graal we were looking for:

Google Lens translates this to: “Life is good at 59, 21 March”.

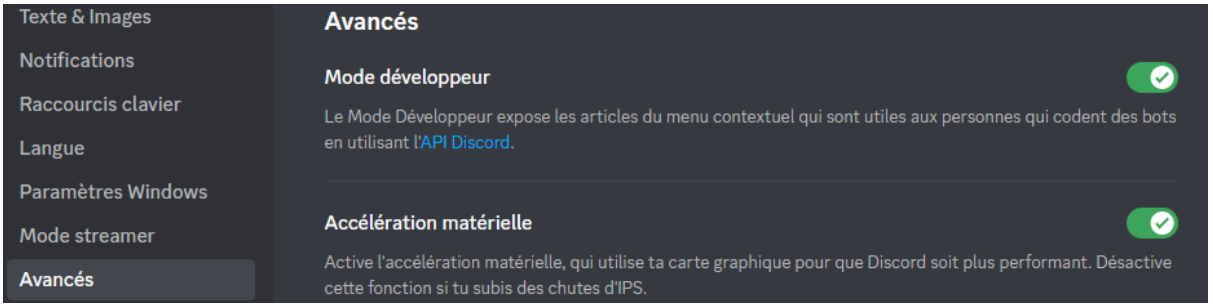
So Tsuzune Yokoyama was born on 21/03/1963 which sounds kinda like tsuyo63, confirming our hypothesis.

The flag is: !c6-21031963

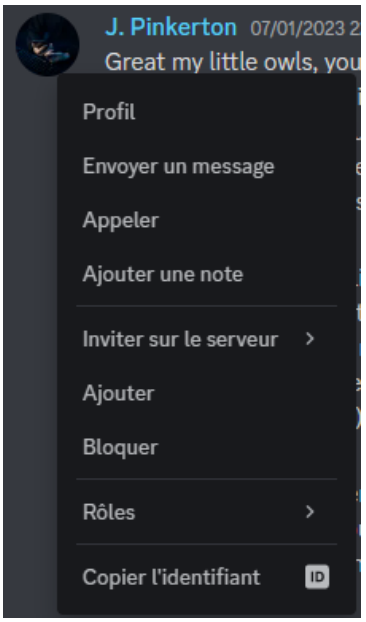
2.7.5.2. Challenge 7

Challenge 7
We have been working together for quite a moment now, you want to know me better? I will tell you more if you can find my Discord unique identifier (Discord ID) (format: !c7-11111) (modifié)

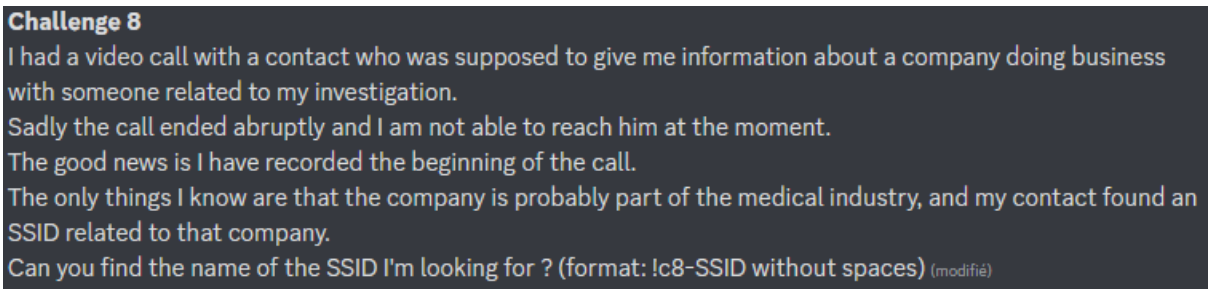
Challenge pretty easy here, you must first activate the Developer Mode in the Discord settings.



After that, right-click on the profile image, and “Copy ID”. Command: !c7-1055577878022070302.



2.7.5.3. Challenge 8



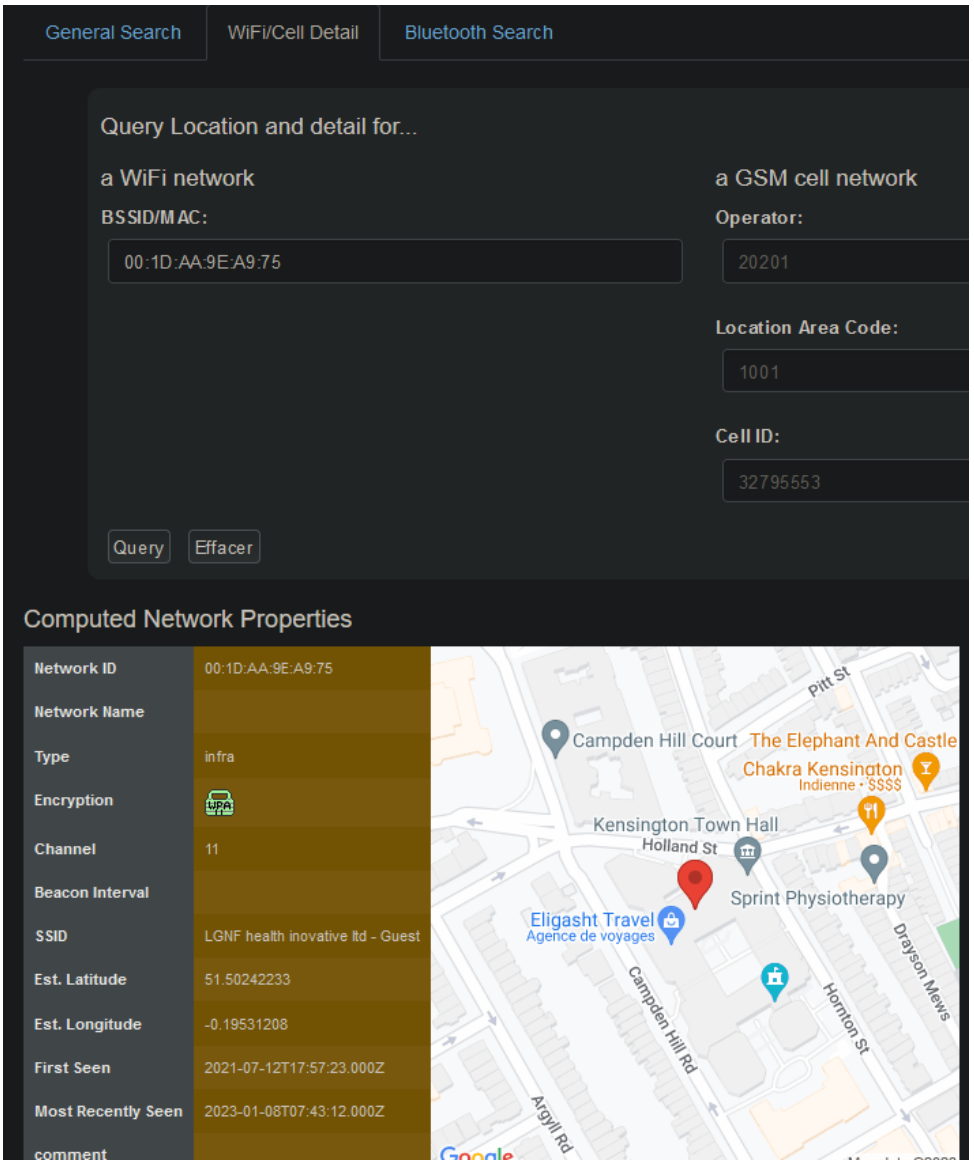
We can see on the video the end of a MAC address: “9E:A9:75” and a website where we can read “Draytek”. So we started by searching the MAC address of a Draytek router.

On https://maclookup.app/vendors/draytek-corp, we found 3 OUI corresponding to DrayTek:

- 14:49:BC

- 00:50:7F
- 00:1D:AA

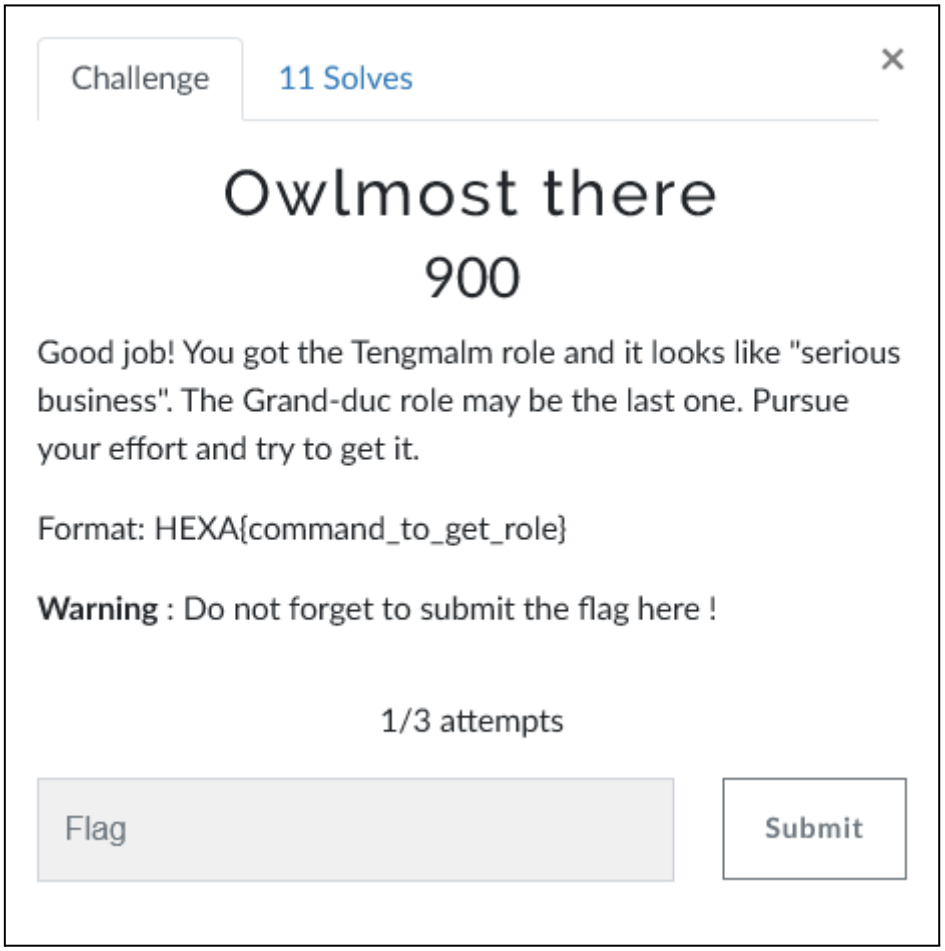
We then searched a network corresponding to this MAC address on https://www.wigle.net/.
We found an ssid with MAC address 00:1D:AA:9E:A9:75 which is called “LGNF Health Inovative Ltd - Guest”



Answer: !c8-LGNFhealthinovativeltd-Guest

Command to get the Tengmalm role: !dzuf1i2ufe63wv5fscmt2x8pyyilrm
Flag: HEXA{!dzuf1i2ufe63wv5fscmt2x8pyyilrm}

2.7.6. Owlmost there



2.7.6.1. Challenge 9

Challenge 9
I got something big, and I need you to help me... This is related to my main investigation. In this case, several people were injured in Malaysia in a shooting. A contact managed to sneak into the crime scene and collect a bullet from the weapon used to commit the crime. Can you identify the weapon used from the bullet? (format: !c9-caliber-weaponmodel - example : answer is 1.11 GUN just send !c9-111-gun) (modifié)

In the first place, we tried to find the bullet using Google Lens or search by image but we couldn't find a match with the same dimensions.

We are searching for a bullet with a probable cartridge diameter of 7.62mm as it is a very common diameter with a length of 24 or 25mm.
With those dimensions, we find the 7.62x25mm Tokarev caliber which looks like the one we are searching for.

Answer: !c9-762-tokarev

2.7.6.2. Challenge 10

Challenge 10
A Mauritian friend told me that : "A British businesswoman came to sign a contract with the A-team. I am surprised because this woman was a tall one and seemed Slavic, not something we see on a daily basis here... I am also surprised to hear about A-team, they winded up in 2014...". I'm a little confused about what he said... Can you find the A-team he is talking about? Maybe some winding up details about it will help us, like the exact date... (format: !c10-DD-MM-YYYY) (modifié)

For this challenge, we need to find what this A-Team is. But the first thing that struck us was the use of the term “winding up”. This term is used for companies, so this A-team should be a Mauritian company. We used the website opencorporates to search for A-team that exist in Mauritius. There were 3 companies, however one is still active, so it shouldn’t be the one we are looking for. However, OpenCorporates doesn’t give us the winding up date for these companies. To do so, we had to go on the website from which the data came. Opencorporates gives us a link to the original data. It was a bit broken so we had to delete the path to go directly to the home page. From there, we searched for A-team and looked one by one at the 3 companies that were returned. For the A-Team Security Ltd, there was a winding up date that occurred in 2014, just like our mauritian friend told us.


WINDING UP DETAILS

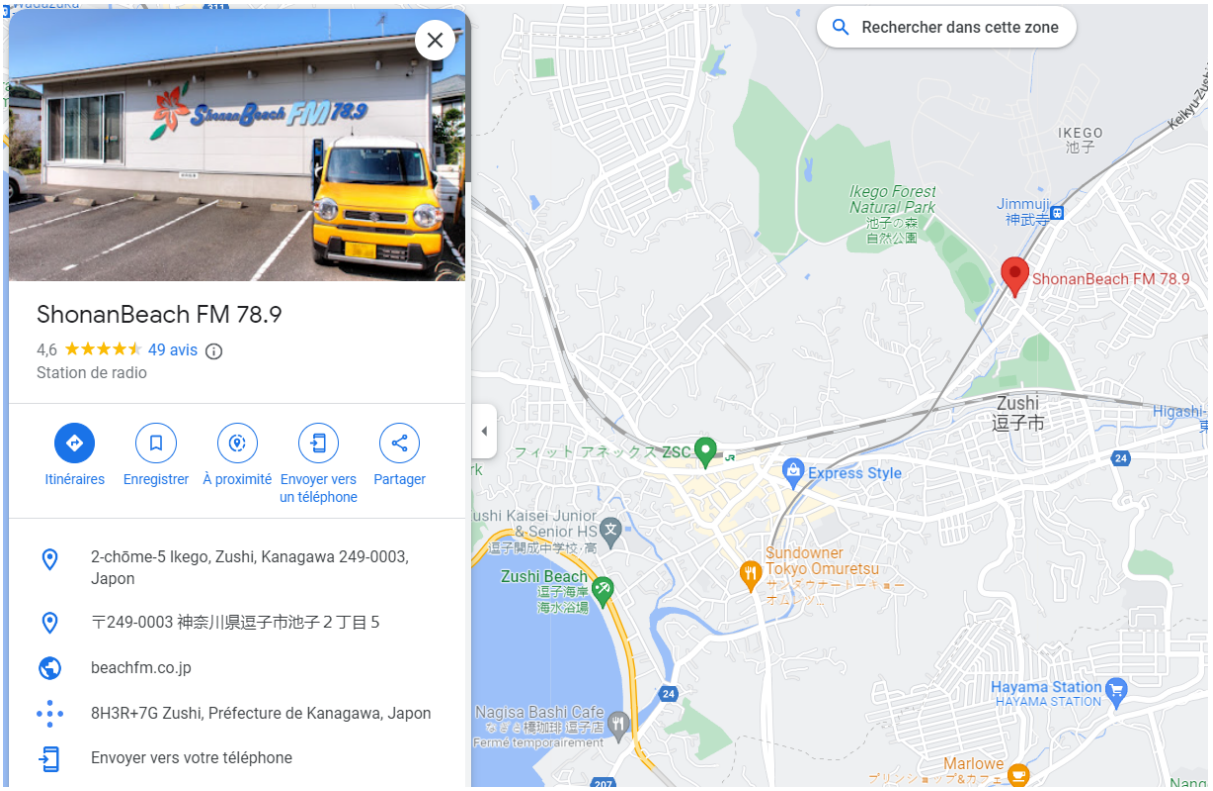
#	Type	Start Date	End Date	Status
1	REMOVAL OF COMPANY UNDER S309(1)(B)	15/02/2014	18/06/2014	FINALISED

So the flag is !c10-18-06-2014

2.7.6.3. Challenge 11

Challenge 11
I managed to intercept a message from Tsuzune saying that : "Every channel is compromised, we need to use another radio frequency to communicate, it will be safer. The channel will be 500 Khz above my favourite station. Search in the garden in the させつ。はばとび。はなよめ area and you will find it.". If I can have the right frequency, I'll be able to go forward in my investigation, so find the right channel !!! (format : !c11-666666 : frequency in Khz)

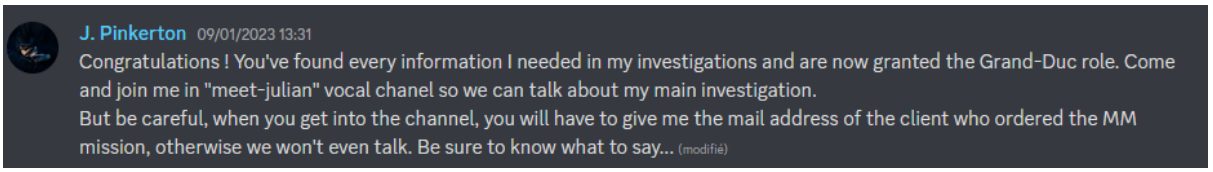
The first reflex was to search "させつ。はばとび。はなよめ" on google. The first result link was https://mapfan.com/spots/SC353,J,87. On this webpage, the coordinates of the location were written: *35.295554 139.5804492*. By putting them in Google Maps, we go to the location in this application. Then, the first reflex was to search FM radios around this area. The nearest result was ShonanBeach FM 78.9:



By adding 78.9 MHz and 500KHz, the result was 79400 KHz (and not 079400 like the format example mentioned with the 6 digits). The result was then !c11-79400

2.7.7. Cowl me maybe

The last challenge is available on the discord with the last role that we unlocked via the previous three challenges:

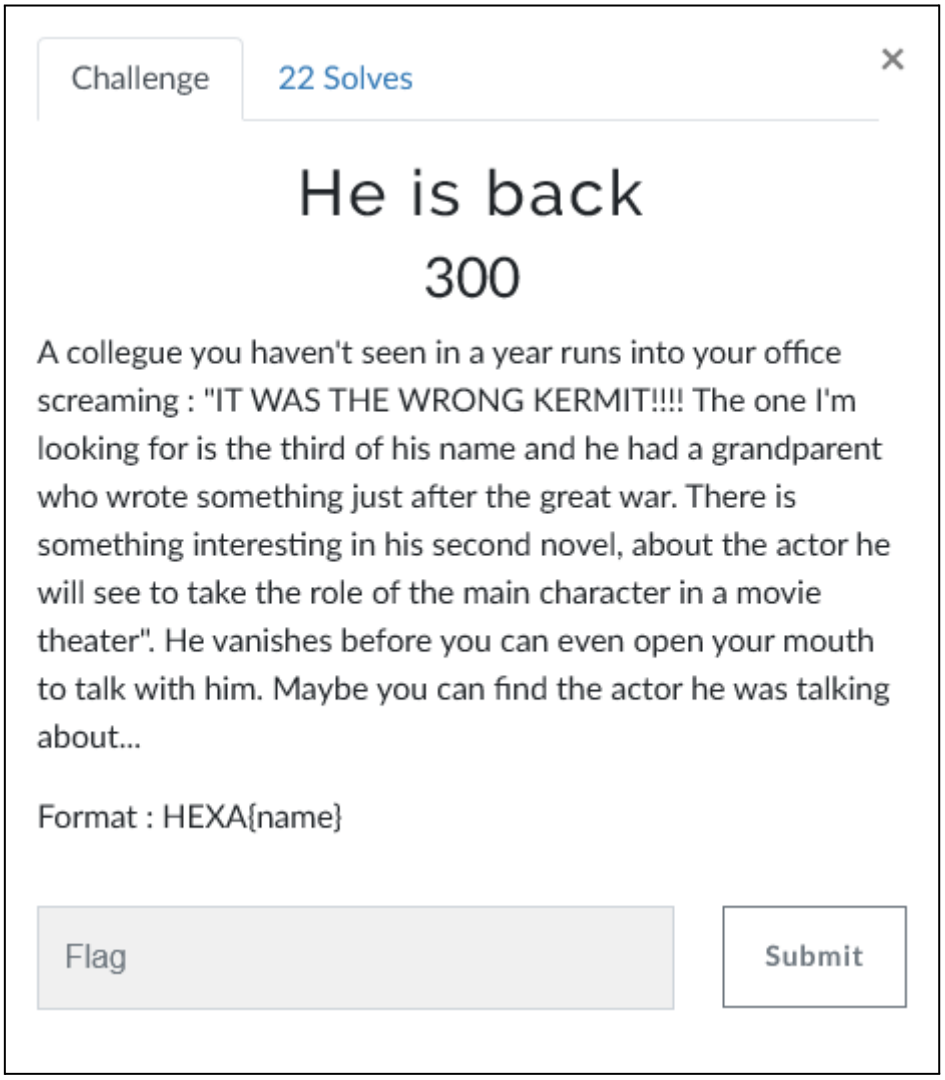


Which e-mail address was used by the client who ordered MM mission ? First, who is MM ? MasterMind. How was the mission ordered ? We learned it through the challenge Herbaceous taught us that the client should use the crypto address to contact MM. Furthermore, during the challenge Decentralized we saw an email address being transmitted with a mission name. The mission name was linked to the main operation we were working on via the API we found for the challenge Experts. So the email address we are looking for is tsuyo63@gmail.com. We also found a link between this email address and the japanese guy Pinkerton was looking for, Tsuzune Yokoyama born in 1963. In addition, on the paper of the challenge Setup we can see the operation bruised rogue being asked by Tsuzune Y.

So we called Pinkerton and said the email address out loud, and a recorded voice answered us with some information about the case. Following are the notes we took during the talk:
The case is a crazy one where Lucilhe, arrested in 2021 escaped. The operation was planned by MasterMind, which is a company that provides criminals services in exchange for services later. The chief of MasterMind is Minca H, a business woman with long wavy red hair with venetian highlights.

2.8. Sidequest

2.8.1. He is back

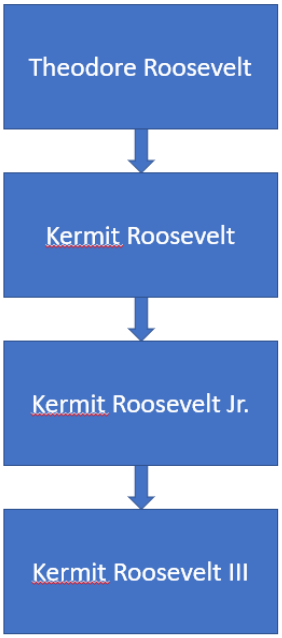


Please not him. Back to 2022, the Kermit challenge gave some PTSD to the team, and apparently, he is back. The most complicated thing here was to understand the

challenge statement. It was important to divide the sentences to translate them into simpler words:

- The third of his name refers to the grandfather's person
- There are lots of events called "The great war", even in Game of Thrones, but when we did some research about this, the first related event was the First World War.
- Seeing the organization of the sentence, the second novel could refer to either his grandparent or him.
- His second novel would be adapted into a movie and there is a small interesting fact about the adaptation of the main character

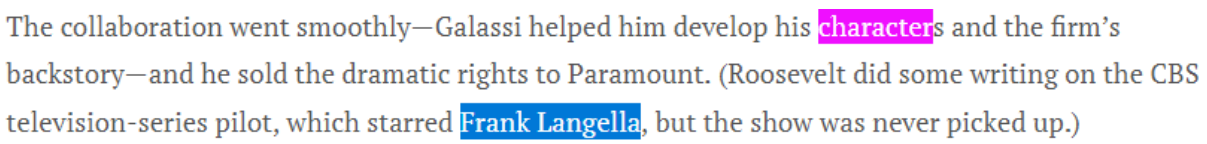
Those fourth points bring lots of, too much information to do the searches. There were lots of great wars, lots of different Kermit, lots of people that made novels… So we decided to keep it simple and took the first person that came regularly to the results of our searches: Kermit Roosevelt. The key word for this search was "kermit first world war". After analyzing his Wikipedia page, we read that he has a child, Kermit Roosevelt Jr who also has a child, Kermit Roosevelt III. To sum-up their direct link, we created a short family tree:



By taking back the information of the challenge statement, Kermit Roosevelet wrote some books after WW1 and has a grandson called Kermit Roosevelt III.

The next step was to find the second novel. In the wikipedia page of Kermit Roosevelt III, we learnt in the “Reception of novels” and “Fiction” sections that he wrote 2 novels. The second one “Allegiance” was the one searched.

At this step the idea was to find an article which described the personal opinion of Kermit Roosevelt III to match the challenge statement part ”about the actor **he will see** to take the role of the main character in a movie theater". For that, a simple Google search was used “Kermit Roosevelt III "Allegiance" interview”. This one gave a bunch of websites, and thepenngazette.com was interesting. This article talked about the work of Kermit Roosevelt III. By searching some information by the keyword “character”, we found, like in the Wikipedia page, a section describing some actors. In the 7th occurrence of this keyword, a certain “Franck Langella” appeared:


The collaboration went smoothly—Galassi helped him develop his characters and the firm’s backstory—and he sold the dramatic rights to Paramount. (Roosevelt did some writing on the CBS television-series pilot, which starred Frank Langella, but the show was never picked up.)

Franck Langella was an interesting finding because we already saw him in the Wikipedia article. The reflex was then to do another Google search with this actor, because he perhaps also appeared in the second novel adaptation but was not mentioned in the Wikipedia page for some reason.

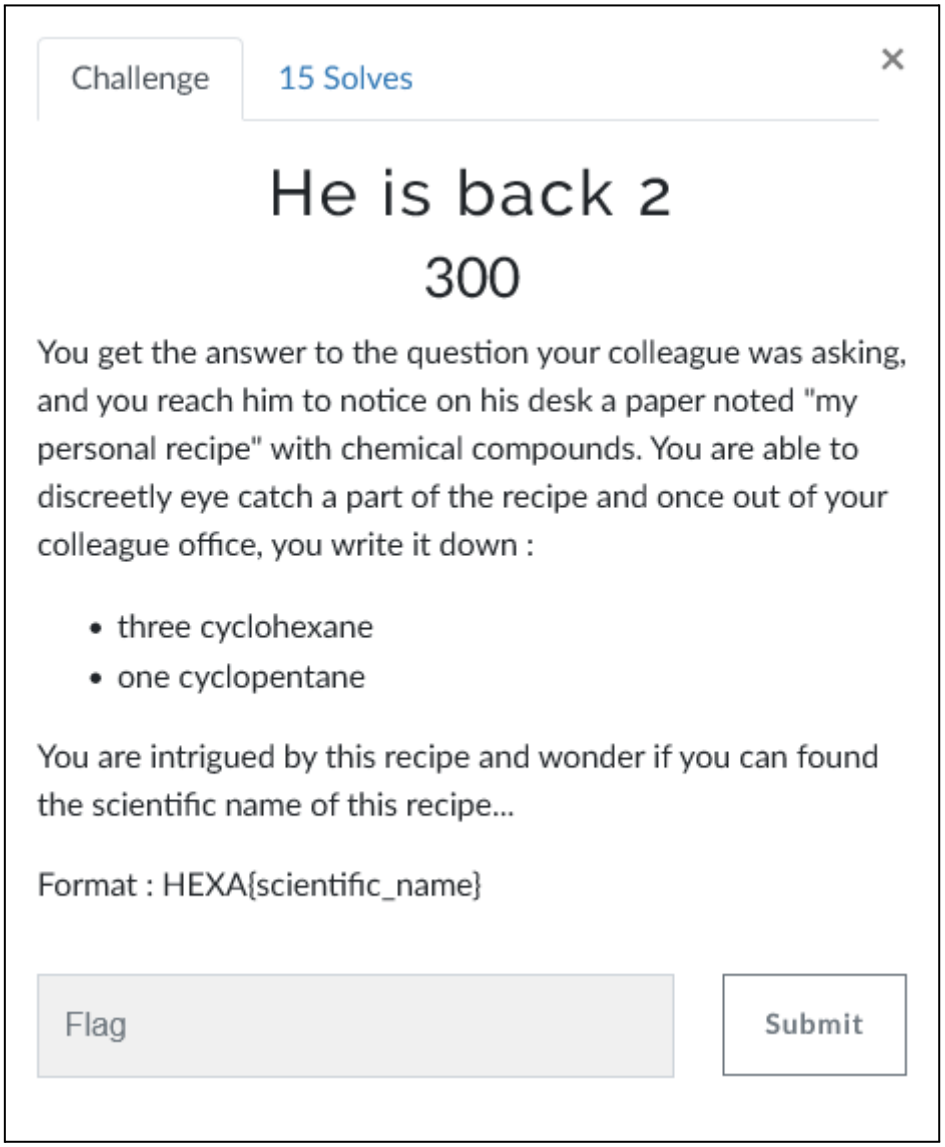
So “Kermit Roosevelt III "Frank Langella" "allegiance"” was used for another Google search and one of the first links after Wikipedia's one was harvardwood.org. In this article, searching by the keyword “Franck Langella” was not so interesting because he only appeared in the introduction part. The second search was with the “Allegiance” keyword that was much more logic in this context. By reading the text located after this keyword, we read that Kermit Roosevelt III wanted to see the caracter Cash Harrison played by a Joseph Gordon-Levitt.

One evening, however, Roosevelt's wife suggested that he look backwards instead, and suddenly, *Allegiance* was born, focusing on the World War II cruelty that involved the removal and detention of Japanese-Americans all in the name of national security. The main character in *Allegiance*, Caswell "Cash" Harrison is a young, idealistic lawyer who dives deep into a potential conspiracy dealing with the constitutionality of the prison camps created to detain Japanese-Americans that is both a legal thriller and an examination of civil rights violations committed by our government – a provocative theme that infuses Roosevelt's real-life legal work to this day.

"Cash Harrison is truly my bigger and more violent alter ego," larks Roosevelt, "although I can see him being played on the big screen by someone quietly charismatic like Joseph Gordon-Levitt."

This statement was exactly what the challenge explained. The flag was then: HEXA{Joseph Gordon-Levitt}

2.8.2. He is back 2



For this challenge, we know that we are looking for a chemical that has three cyclohexane and one cyclopentane as compounds. a google search with the request `"three cyclohexane" "one cyclopentane"`let us know that "The steroid nucleus, sterane, is composed of *three cyclohexane* rings and *one cyclopentane* ring."

Wikipedia helps us understand what steroids are, and also that its nomenclature is "Gonane, also known as steran or cyclopentanoperhydrophenanthrene". The challenge asks us the scientific name of the recipe, and as we all know, scientific names are always the ones you can't say out loud without your furniture starting to levitate (or the more specific, depending on the point of view). The flag is HEXA{cyclopentanoperhydrophenanthrene}.

3. Rapport

3.1. Mission Analysis

Mastermind's mission to exfiltrate Lucilhe is called "Bruised Rogue".
The mission was commissioned by a Japanese man named Tsuzune Yokoyama. He contacted Mastermind through the ethereum address available on Mastermind's onion site.

The objective of the mission is clear, to make Lucilhe Dumarquais escape during her transfer to court. He wants to recruit her because of the skills she has shown in Manipar. However, if anything goes wrong with the mission, the order is clear, Tsuzune Yokoyama's identity comes first and Lucilhe Dumarquais must be eliminated.

This mission began in 2022 when the law firm Nelexat took over Lucilhe's case. This case is not usually one they work on (they are tax lawyers). This allowed Mastermind to recover information about the transfer during which the escape took place.

The man who helped Lucilhe escape from the Versailles court is a certain "O. Vokolski", answering to the pseudonym "action-man".

They then took a plane from Clermont-Ferrand to Zürich, on Limmatquai Street. There they met Lian Nussbaumer, Lucilhe's lawyer.
From Zürich they took a train to Cadenazzo from where they took a boat to the safehouse in the town of Chania in Greece.
Once on the island, they flew to Heraklion Níkos-Kazantzákis International Airport to catch a flight to Singapore Changi Airport.
Once in Singapore, they hid in the Hougang area before driving to a safe house in Kuala Terengganu, Malaysia, where they were apprehended before they could set sail to their final destination, probably in Japan.

3.2. Mastermind Analysis

The Mastermind organization is managed by Minca H and is a secret organization operating under the cover of the company Nelexat. Nelexat provides tax lawyers in Zurich. This organization carries out various missions, such as the "Bruised Rogue" operation which consists of exfiltrating Lucilhe DUMARQUAIS. Mastermind is a complete organization with various members under Minca's command. First of all, Lian Nussbaumer working for Nelexat is the group's tax lawyer who protects the group. The Nelexat website at Nelexat.ch is administered by O. Vokolska. Secondly, the person who operates in the field is Oleg Vokolski, who kidnapped Lucilhe. Finally, Mastermind's operations are investigated by the investigator Julian Pinkerton.

MASTERMIND :

Name : Minca H.
Pseudo : MastermindAlly3743 / mincah_mm
Email : mincah_mm@proton.me
How involved : Head, The associate

Name : Lian Nussbaumer
Pseudo : Nelexlian
Email : mastermind_mastermind@proton.me
How involved : Senior tax lawyer and partner at Nelexat. Organised the meeting in Switzerland (google meet link)

Name : Oleg Vokolski
Pseudo : vok_0lski
Email : vok_0lski@proton.me
How involved :
Role : The action man, the person on the ground who recovered Lucilhe.

_____

Name : O. Vokolska
Pseudo : littlesparr0w / OVokolska
Email : ovokolska@protonmail.com
How involved : Development of nelexat.ch
Note : Looking for love, has a profile on which she is waiting to be contacted (*profile/0zAhMACjE4NzI4NjIzMDkAII1ix1PX0QWiZqTHLnMHsD7jvBDObPuG-Vm_WZaWh-qd*). She is 19 years old and has just finished her studies. Daughter of Oleg Vokolski.

_____

EXTERNES :

Name : Julian Pinkerton
Pseudo : Pinkerton91 / Julian Pinkerton#9348 / user545947198194
Email : ovokolska@protonmail.com
How involved : The Intruder, Mastermind survey

_____

Name : Lucilhe DUMARQUAIS
Pseudo :
Email :
How involved : Target of the bruised rogue mission

_____

Name : Tsuzune Yokoyama
Pseudo : tsuyo63
Email : tsuyo63@proton.me
How involved : Mission sponsor Bruised Rogue, Mastermind client

NELEXAT :
Name : Fridrich Merker
Pseudo : BizneuilleTrader
Email :
How involved : Only Nelexat, not Mastermind

Name : Lucie Dleau-Berger
Pseudo : GiantIncomesForYou
Email :
How involved : Only Nelexat, not Mastermind

3.3. Associate analysis

The lawyer's partner, the head of mastermind, is a businesswoman by the name of Minca H. According to Pinkerton's information, she is English with a Slavic look. She is said to have long, wavy, red hair with Venetian blonde highlights. The developer describes her as having hazel eyes. She is also listed on TripAdvisor as being 1.87m tall.
She was the one who gave the watch to the lawyer (Lian) a few years ago.

In brief:

- Height: 1.87m
- Eyes: Hazel
- Hair : Long, wavy, red with Venetian blond highlights
- Face : Slavic origin
- Nationality : English
- Last known location : Chelsea

3.4. Action Man Analysis

The Action man's name is Oleg Vokolski.
He is known for the following crimes: theft, car theft, escape.
He was recruited into Mastermind after a mission he requested from them.
He is the one who retrieved Lucilhe from France and has to bring her to Tsuzune Yokoyama.
Oleg Vokolski is a man about 6'2" tall with brown and grey hair. He is Polish and speaks fluent Polish and English. He has a scar on his right arm and a rose tattoo on his right arm.
He uses the email address vok_0lski@proton.me
The man is under a red europol notice which can be used as a pressure point and also his daughter developed the website of nelexat.

4. Maltego

During this CTF, we completed a Malteo with information that we retrieved.