Social Network Analysis

TA-II Assignment

Guided By

Mrs Meena Lakshmi

(Assistant Professor)

Submitted By

Raj Shekhar

Enrolment no.: 240545002004

M.Sc. in Cyber Security

Semester III

School of Cyber Security & Digital Forensics

National Forensic Science University

Bhopal Campus, M.P., 462001, India

Challenge #1

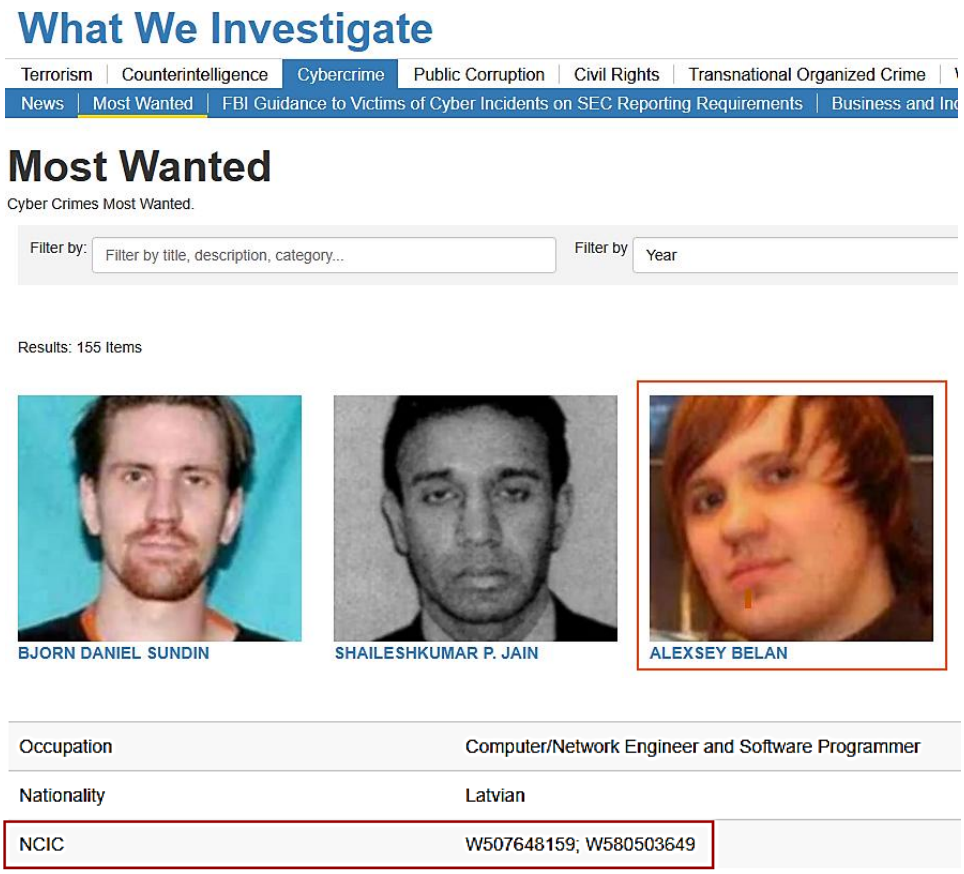
Description : The most decorated woman in Olympic diving was born in the city in this photo. If she were standing here now, what is the name of the resturant behind her over her right sholder? The flag is only the two (2) words of the resturant?

Identified location was Xintiandi, Shanghai, China, after reverse searching. Then going into that location in maps and founded that two-word restaurant in the right side.

Its name was "*The Refinery*" which is the flag.

Challenge #2

Description : A cybercriminal responsible for a series of high-profile ransomware attacks has vanished. The only remaining clue is a fragmented NCIC number hidden within the investigation's scattered files. A corrupted image, found on a dark web server, is believed to be linked to the suspect, who is rumoured to be on the FBI's Most Wanted list. Your mission is to reconstruct the NCIC number.



Found the NCIC number on the website of What We Investigate from reverse imaging the found image. Therefore, the flag is *0xL4ugh{W507648159}*.

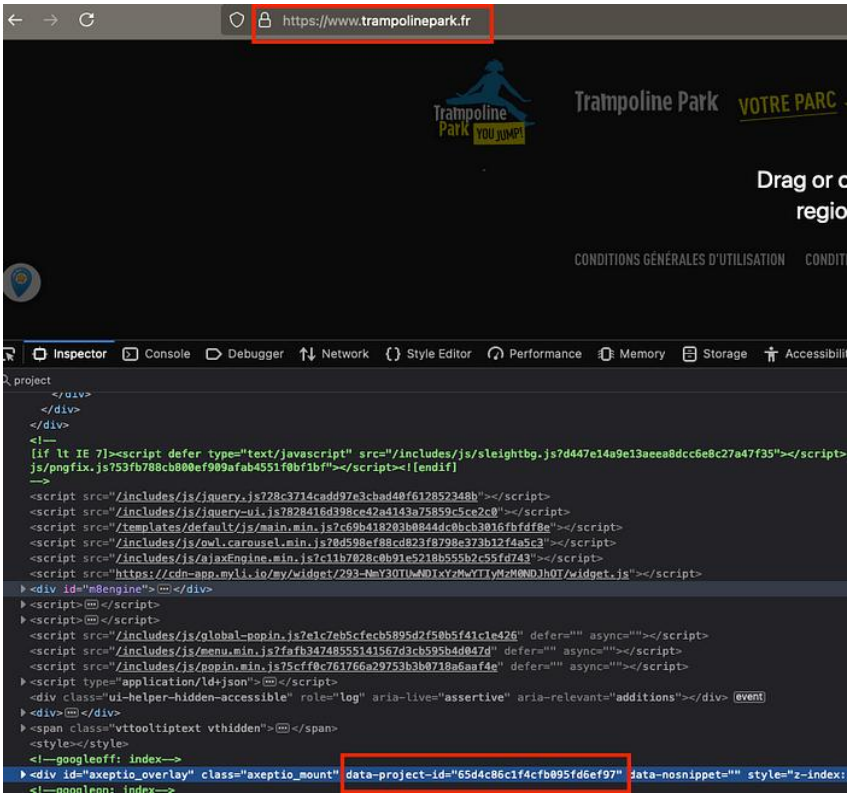
Challenge #3

Description : This town, which has twice hosted the winter olympics, boasts 4 recreational facilities near it that are popular during the summer months. We are looking for the name of the sport played at theses recreational facilities.

Place Name found online is Moritz, Switzerland. And the sport was *Golf*.

Challenge #4

Description : There is a trampoline park that is within a very short distance from where the 2024 olympic mountain biking competition will take place. This specific park's website has a link to the main site for a larger franchise. This main site has some tracking and analytics that use a project-id as a part of the values that are sent to a 3rd party consent management platform. What is the project-id value? The flag will the value.



Identified venue for '2024 mountain biking competition', which is "Elancourt Hill". And in the website of trampoline park, found flag: **65d4c86c1f4cfb095fd6ef97**

Challenge #5

Description : You have been applying to entry-level cybersecurity jobs focused on reconnaissance and open-source intelligence (OSINT). Great news! You got an interview with a small cybersecurity company; the Keeber Security Group. Before interviewing, they want to test your skills through a series of challenges oriented around investigating the Keeber Security Group.

The first step in your investigation is to find more information about the company itself. All we know is that the company is named Keeber Security Group and they are a cybersecurity startup. To start, help us find the person who registered their domain.

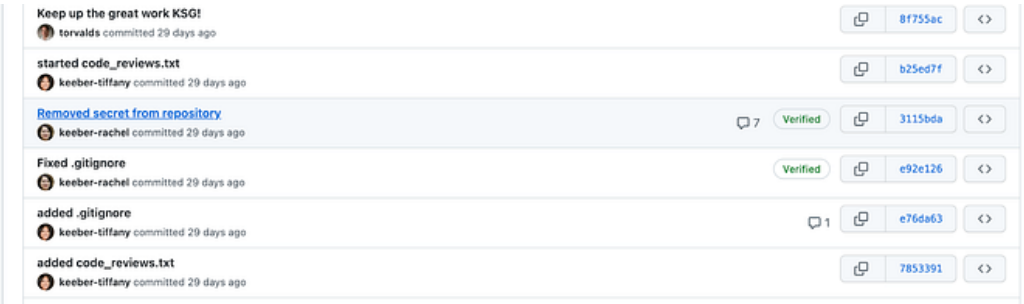
```
# whois.name.com

Domain Name: KEEBERSECURITYGROUP.COM
Registry Domain ID: 2689392646_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.name.com
Registrar URL: http://www.name.com
Updated Date: 2022-04-15T01:52:49Z
Creation Date: 2022-04-15T01:52:48Z
Registrar Registration Expiration Date: 2023-04-15T01:52:48Z
Registrar: Name.com, Inc.
Registrar IANA ID: 625
Reseller:
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: flag{ef67b2243b195eba43c7dc797b75d75b} Redacted
Registrant Organization:
Registrant Street: 8 Apple Lane
Registrant City: Standish
Registrant State/Province: ME
Registrant Postal Code: 04084
Registrant Country: US
Registrant Phone: Non-Public Data
```

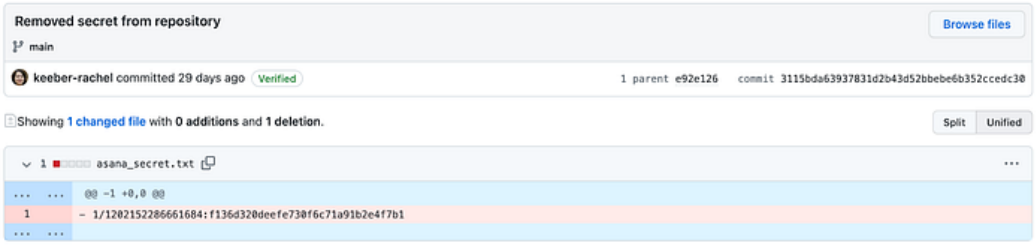
Searched online “Keeber Security Group” and found the company’s official website. Then using WHOIS tool found the flag in the result that is *flag{ef67b2243b195eba43c7dc797b75d75b}*.

Challenge #6

Description : The ex-employee you found was fired for “committing a secret to public GitHub repositories”. Find the committed secret, and use that to find confidential company information.



In the Github repository, there is commit made with *“Removed Secret from repository”*. Inside the commit and taking a look at the diff, the file was called asana_secret.txt.



At first glance it doesn't say much, so doing some google to find out what Asana is helpful and how this string can be used. And after a bit of digging around the Asana documentation, a handy text box which describes how curl can be used in order to query the Asana API with its last parameter in the curl command was resembling the same identified secret found in the Git before. So, the API Request is :

curl https://app.asana.com/api/1.0/users/me
-H "Authorization: Bearer 1/1202152286661684:f136d320deefe730f6c71a91b2e4f7b1"

{"data":{"gid":"1202152286661684","email":"keebersecuritygroup@protonmail.com","name":"flag{49305a2a9dcc503cb2b1fdeef8a7ac04}","photo":null,"resource_type":"user","workspaces":[{"gid":"1202152372710256","name":"IT","resource_type":"workspace"},{"gid":"1146735861536945","name":"My Company","resource_type":"workspace"},{"gid":"1202202099837958","name":"Marketing","resource_type":"workspace"},{"gid":"1202201989074836","name":"Informatique","resource_type":"workspace"},{"gid":"1202203933473664","name":"Engineering","resource_type":"workspace"},{"gid":"1202205585474112","name":"Design","resource_type":"workspace"},{"gid":"1202206423101119","name":"IT","resource_type":"workspace"},{"gid":"1202166412558403","name":"richdn.com","resource_type":"workspace"},{"gid":"1202206546743807","name":"IT","resource_type":"workspace"}]}}

The retrieved flag is in the response : *flag{49305a2a9dcc503cb2b1fdeef8a7ac04}*

Challenge #7

Description : Despite all of the time we spend teaching people about phishing, someone at Keeber fell for one! Maria responded to the email and sent some of her personal information. Pivot off of username *cereal_lover1990* to find where Maria's personal information was posted.

```
└─$ sherlock cereal_lover1990
[*] Checking username cereal_lover1990 on:
[+] Coil: https://coil.com/u/cereal_lover1990
[+] Minecraft: https://api.mojang.com/users/profiles/minecraft/cereal_lover1990
[+] Myspace: https://myspace.com/cereal_lover1990
[+] Pastebin: https://pastebin.com/u/cereal_lover1990
[+] Tinder: https://www.gotinder.com/@cereal_lover1990
[+] TradingView: https://www.tradingview.com/u/cereal_lover1990/
[+] Wikidot: http://www.wikidot.com/user:info/cereal_lover1990
```

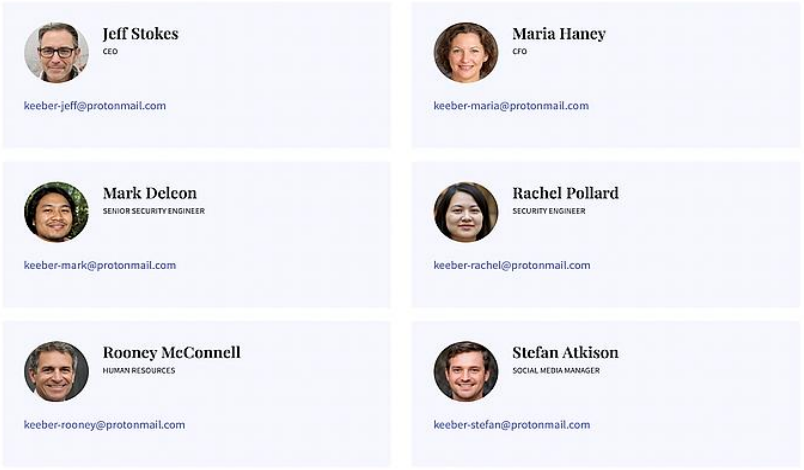
```
134.         "name": "Maria Haney",
135.         "phone": "1-648-584-6277",
136.         "email": "keeber-maria@protonmail.com",
137.         "password": "flag{70b5a5d461d8a9c5529a66fa018ba0d0}"
```

While using sherlock on the provided username, there found a Pastebin url which leads to the website listed with multiple names, emails, phones and passwords. And in the personal information of Maria in the list the flag was found:

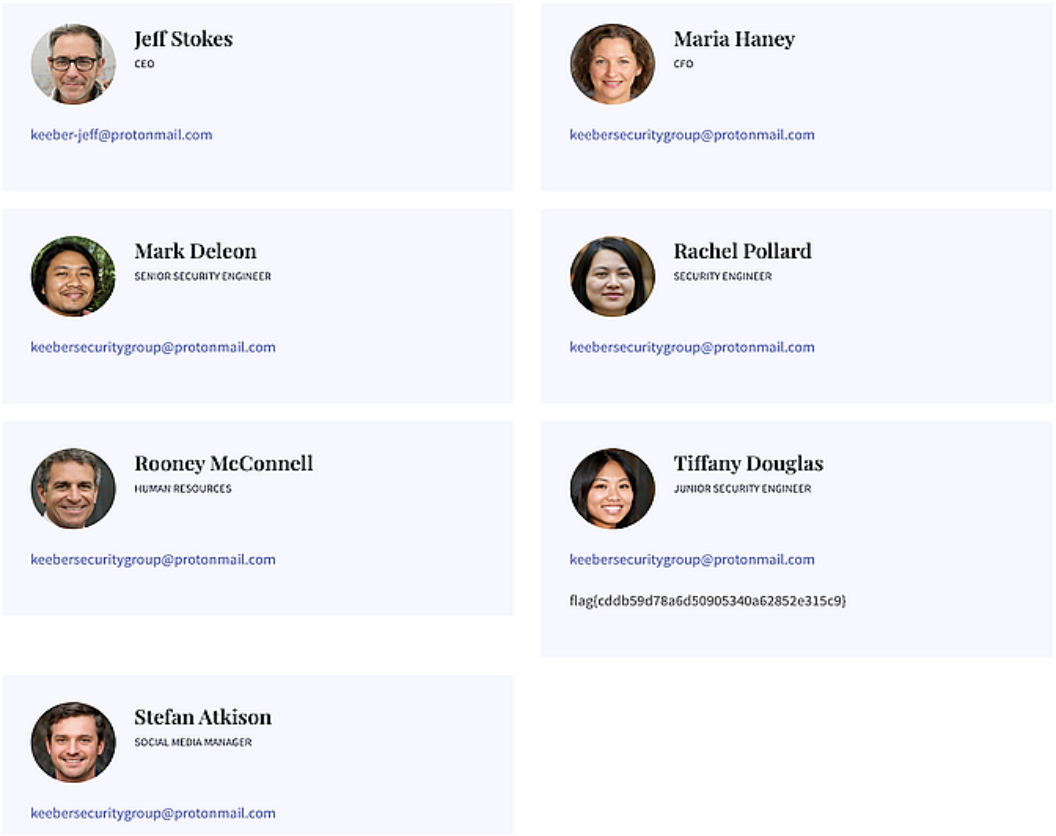
flag{70b5a5d461d8a9c5529a66fa018ba0d0}

Challenge #8

Description : The Keeber Security Group is a new startup in its infant stages. The team is always changing and some people have left the company. The Keeber Security Group has been quick with changing their website to reflect these changes, but there must be some way to find ex-employees. Find an ex-employee through the group's website.



Going to the website and into the team section it reveals 6 employees. So, the website has been updated from past, now to access previous versions of website Wayback Machine will be useful to use.

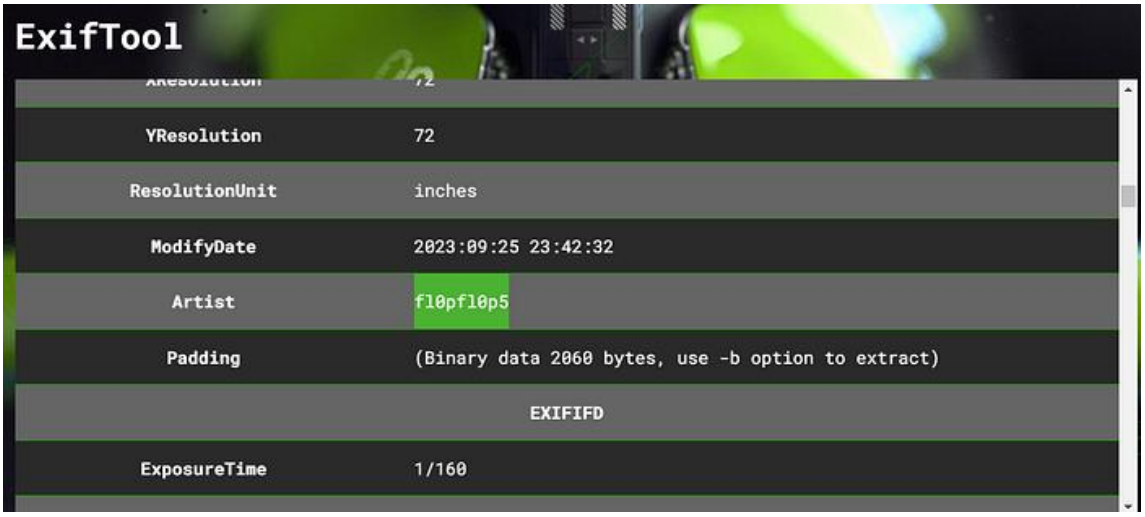


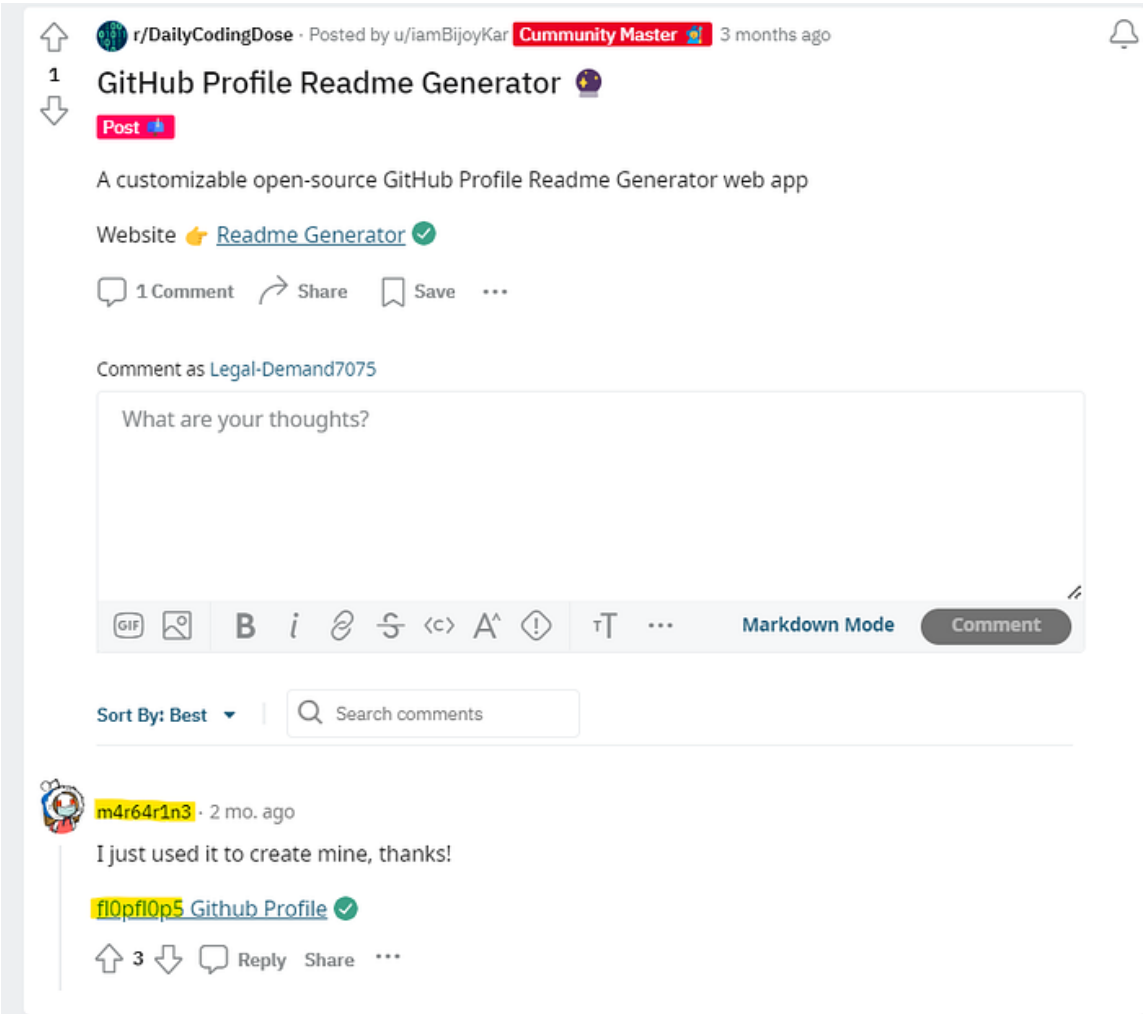
In Wayback Machine pasting the url : https://keebersecuritygroup.com/team, the result shows past snapshots of the website and visiting the April 19, 2022, an ex-employee named *Tiffany Douglas* was present with the flag *flag{cddb59d78a6d50905340a62852e315c9}* as well.

Challenge #9

Description : Can you help us track down this photographer?

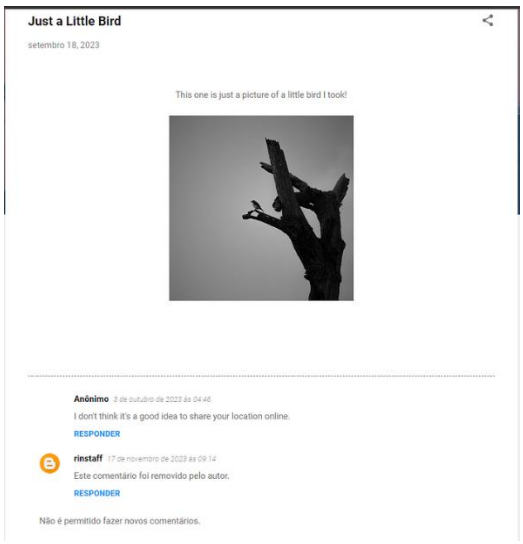
There were two photos attached to this challenge, so performing metadata analysis might be helpful and then reverse image search. Using exiftool to have a look into its metadata.

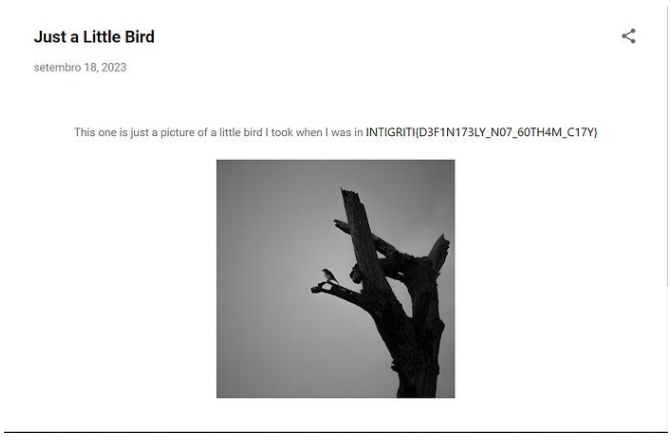




Searching the username online going through reddit and other social media platform. There are another username *m4r64r1n3*. Now looking up this username similarly, found a result in twitter.

Then reverse image searching this image got another username *v1ck1v4l3*. And searching it again related to this was a personal blog online at the link *v1ck1pictures.blogspot.com*.





In wayback mahine, on 2 October, 2023, there is listed the same webpage but with flag this time.

INTIGRITI{D3F1N173LY_N07_60TH4M_C17Y}

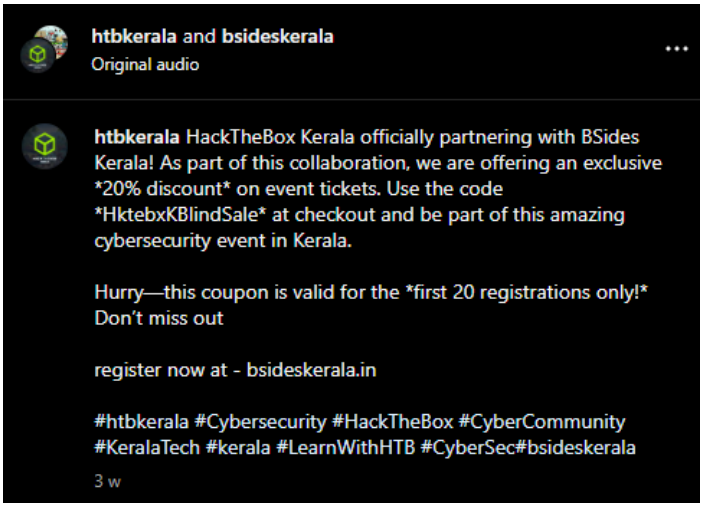
Challenge #10

Description : While searching for the perfect Valentine's gift for my girlfriend, I stumbled upon something intriguing on social media. A post about a major cybersecurity community event happening this week immediately caught my attention. My curiosity led me to explore further. It turns out there's an exclusive collaboration between a prominent cybersecurity group, XYZ, and a well-known security conference. As part of this partnership, they're offering a limited-time discount on event tickets, available only to the first 20 registrants. The event promises to bring together industry experts, enthusiasts, and international speakers for an unforgettable learning experience.

The best part? This gathering takes place in a region known for ancient trade, rich temple architecture, and cherished classical dances. Verdant plantations, grand literary festivals, and vibrant harvest feasts guided by a traditional calendar highlight its cultural depth.
Now, I ask you: What 3 words come to your mind when you think of the event's location?".

Flag Format : NFSUB{word1_word2_word3_location_xyz}

Searching for the "*cyber security event in Kerala"* on google.
On exploring them one by one most of the events were either too old or were upcoming. And then coming across BSides Kerela's website , this event happened on 8th and 9th and the venue was Marriot , Kochi , Kerela . So, this was the right event. And its website - bsideskerala.in.



In the website an Instagram profile was found to start exploring. There were multiple posts mentioning about different collaborations but none of them was exactly mentioning that “Limited time discount to first 20 registrants” thing. Then further on the search a reel came across which was about the collaboration with htbkerala , it mentioned about the exact same thing and HackTheBox. So, {xyz} was htbkerala. Sourcelink : www.instagram.com/p/DFjzfnzP_gj

Next using query - 3 words + “Kerala”

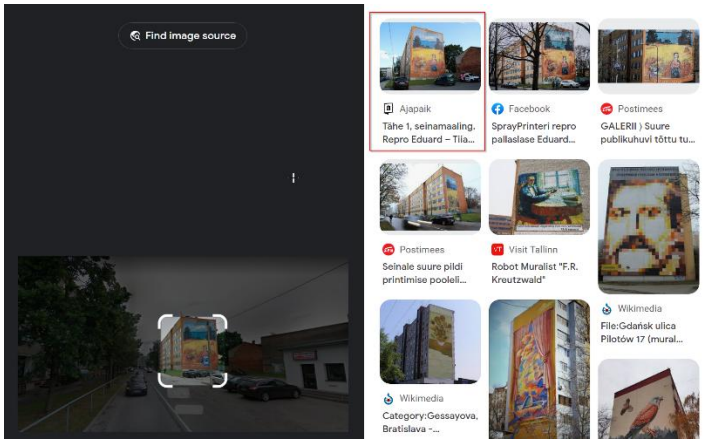
There was a website listed with name what3words maps which gives 3 unique words for every address, so entering “Kochi” into the website got the three words required to solve the challenge. That are “restores.spoil.tunnel”.

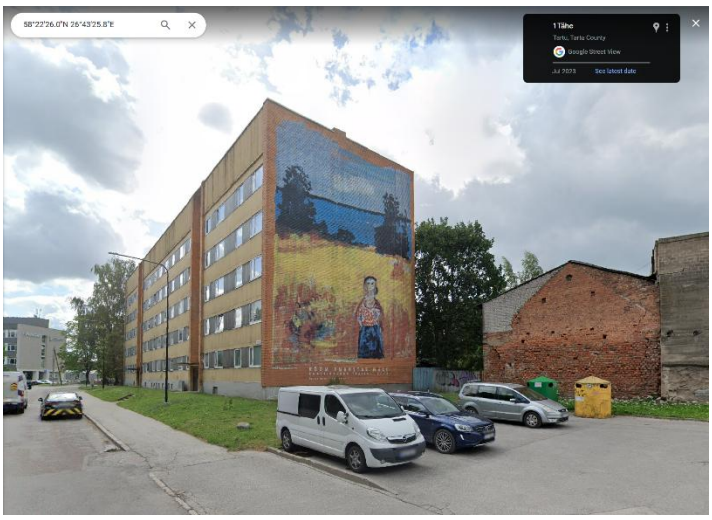
So, the final flag is *NFSUB{restores_spoil_tunnel_kerala_htbkerela}*.

Challenge #11

Description : Your first mission is to find the precise coordinates that indicate the target's location in the provided image. The submitted coordinates must be precise with exactly 6 decimal places after the decimal point.

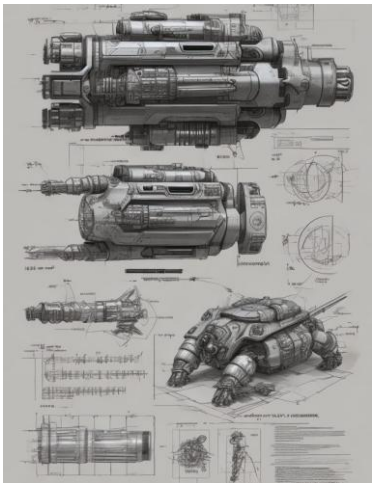
Inside google image search and there are some results about the building and going into one of the websites listed. After translating to english, there are coordinates listed but the position is incorrect. So, google these coordinates → 58.37388306344458° N 26.72384343809849° E





Opening it in google street view and going back to 2019 show the exact photo and changing the view to fit the same as the provided image.
And the closed coordinates are : *58.3740879, 26.7236208*, also the flag.

Challenge #12



Description : In a world of secrecy, Dr. Zukushichi, once a revered nuclear chemist, is now controlled by the malevolent Shadowfire Syndicate. He is coerced into creating a destructive dirty bomb. A diverse group of skilled hackers, intelligence agents, and strategists unite to stop this threat. As time runs out, they strive to infiltrate the Syndicate's lair and prevent a global catastrophe. Locate the residence and Wi-Fi information of Dr. Zukushichi.

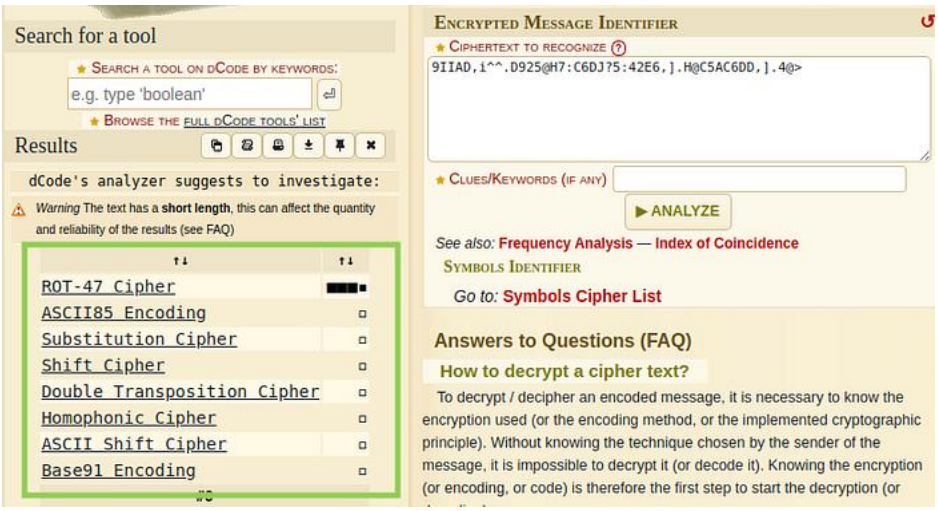
It is a picture with its MD5 checksum.
Reverse Image Search, aimed at finding possible web matches: no result. Searching for data hidden with Steganography. Although a realistic option, it was discarded since it can quickly become a rabbit hole. Analyzing the metadata, which emerged as the right approach.

```
XMP Toolkit                     : Image::ExifTool 12.57
Author                          : Shim0zukushichi
Image Width                     : 640
Image Height                    : 832
```

In that, the line “Author” reveals an essential clue about Dr. Zukushichi’ s username on the Internet: Shim0zukushichi. Plenty of online tools exist to search for a username on Internet social media platforms. I have opted to employ namechk. A simple search of the username yields this result:

Going through all of them, the Github link appeared to be noteworthy. The doctor has 2 repositories: Shim0zukushichi and Projects.
The first one, even though it has 5 commits, only contains a README file with no relevant information.

On the other hand, Projects harbors 4 distinct folders: “Crimson Horizon”, “Mercury Vortex”, “Pandora’s Venom” and “Serpent’s Breath”. Among these, “Pandora’ s Venom” stands out as it contains a .hidden file with a list of equations. Seasoned cryptographers may swiftly discern Equation 69 as a cipher of interest, since unlike other formulas, it is a list of characters without any meaning and it resembles a ROT47.



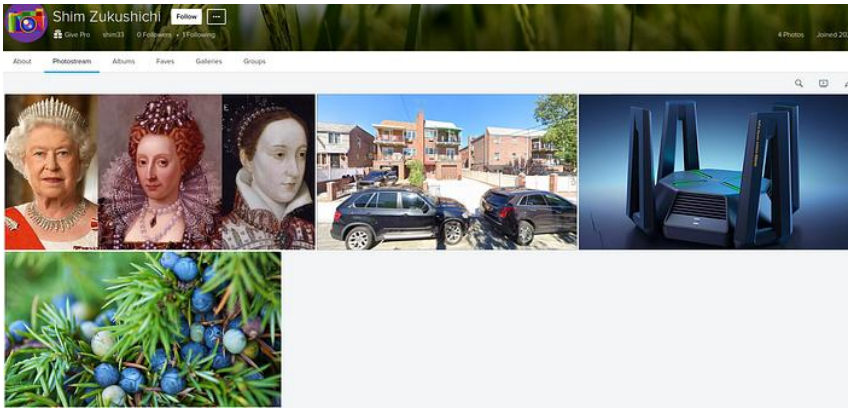
Then, using the ROT47 decoder, we get: hxxps[://]shadowfiresyndicate[.]wordpress[.]com

With a few adjustments, it yields: https://shadowfiresyndicate.wordpress.com , thereby pointing to a wordpress website.

The blog, although quite devoid of content, divulges an interesting piece of information in the “About” page: an email address 0x046h5hk78g@proton.me

Using another OSINT website called Epieos, this is the result we obtain:

Flickr and search for this email address. We quickly find the profile:



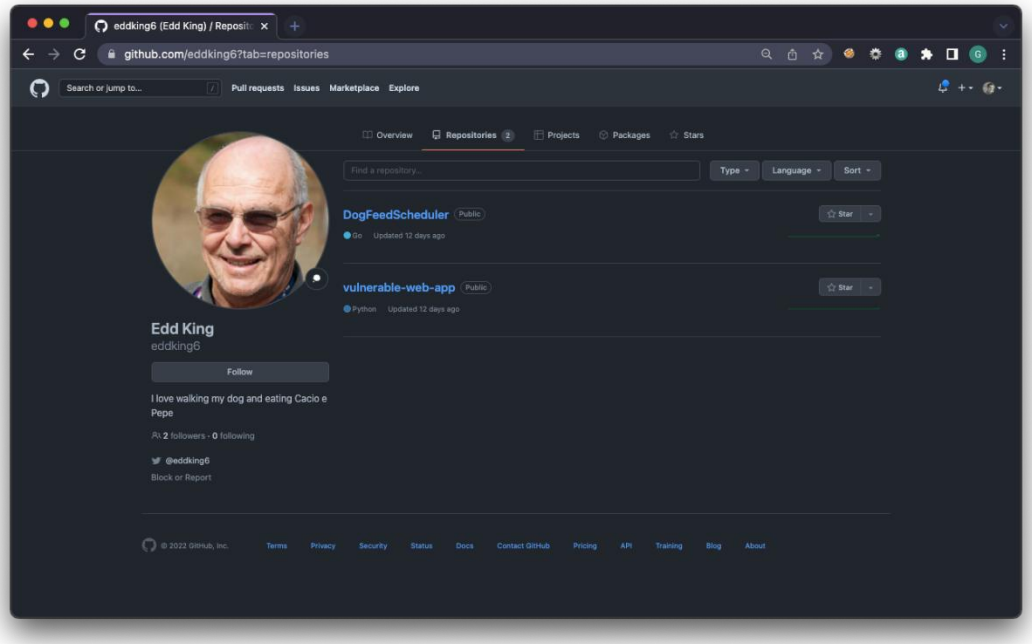
After going into the images above, which is with associated address: 65–08 77th Street, City of New York, NY, US, 11379 and the BSSID is: A8:AB:10:00:06:9E, therefore the challenge is solved.

Challenge #13

Description : Here is a lead "EddKing6", a supposed username.

After dorking that specific term in quotes on duckduckgo search. It yields a few interesting results as follows :

- Edd King Github profile
- Edd King Twitter
- Edd King github repo "DogFeedScheduler"



His bio has one of the challenge's answers :

```
func sendmail(srv gmail.Service, frommail string) {
    temp := []byte("From: 'me'\r\n" +
        "reply-to: blobcorpciso@gmail.com\r\n" +
        "To:  blobcorpciso@gmail.com\r\n" +
        "Subject: Feed Spot \r\n" +
        "remember to feed spot")
```

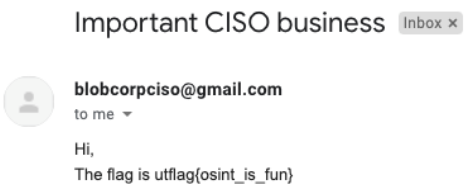
There is a commit where an email functionality added to it. And there are two more answers.

“I like hacking things and running blob corp”, So, he works at a "blob corp". Searching through the tweet history, the following tweet reveals two more answers:
eddking6: I like to play FactorIO when I'm not busy being a #CISO

Searching "eddking linkedin ciso blob corp" yields a eddking6 linkedin page, which is indeed our man. In his education, we see the final answer.
Now all what to do is "... send him a carefully crafted phishing email including all the details."
Now, doing some sort of regex matching/searching on the message's contents, just to make sure the re-use of all the spelling/capitalisation of the previous answers and send an email to the blobcorpciso@gmail.com email. The body of my email:

> Find out the following information about EddKing6
> The name of his dog? : *spot*
> His favourite video game? : *FactorIO*
> His alma matter? : *Texas A&M University*
> His Role at his company? : *CISO*
> His favorite food? : *I love walking my dog and eating Cacio e Pepe.*
> His Email? : *blobcorpciso@gmail.com*

And an email was received in the response just after 10 seconds.



So, the Flag is *utflag{osint_is_fun}*.

Challenge #14

Description : We use docker private registry to host our secure AWS app.
52.53.166.207

Trying to curl to the given ip address:
curl http://52.53.166.207:5000/v2/_catalog
{"repositories":["dev-aws-test-code"]}

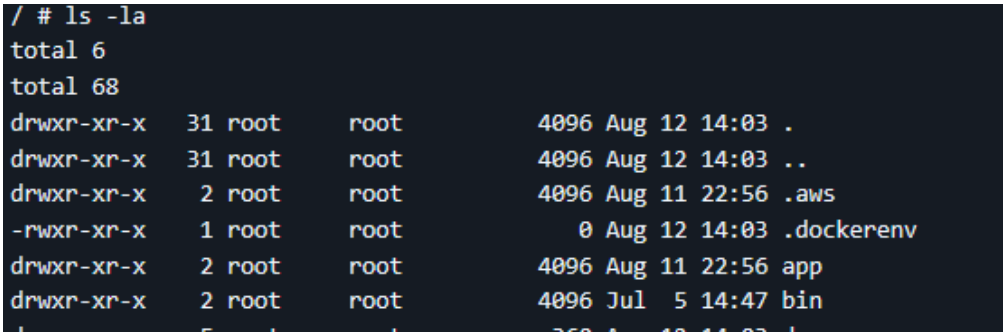
It seems that an image found that matches the description of the challenge. Knowing that, the first idea is to try to directly recover the docker image using docker pull but it says that it is not possible to recover the latest image:
#> docker pull 52.53.166.207:5000/dev-aws-test-code
Using default tag: latest
Pulling repository 52.53.166.207:5000/dev-aws-test-code
Error: image dev-aws-test-code:latest not found

Next trying after some googling about ways to list the tags of an image for docker pull query from before, so let's try :
$ curl http://52.53.166.207:5000/v2/dev-aws-test-code/tags/list
{"name":"dev-aws-test-code","tags":["notreadyet"]}

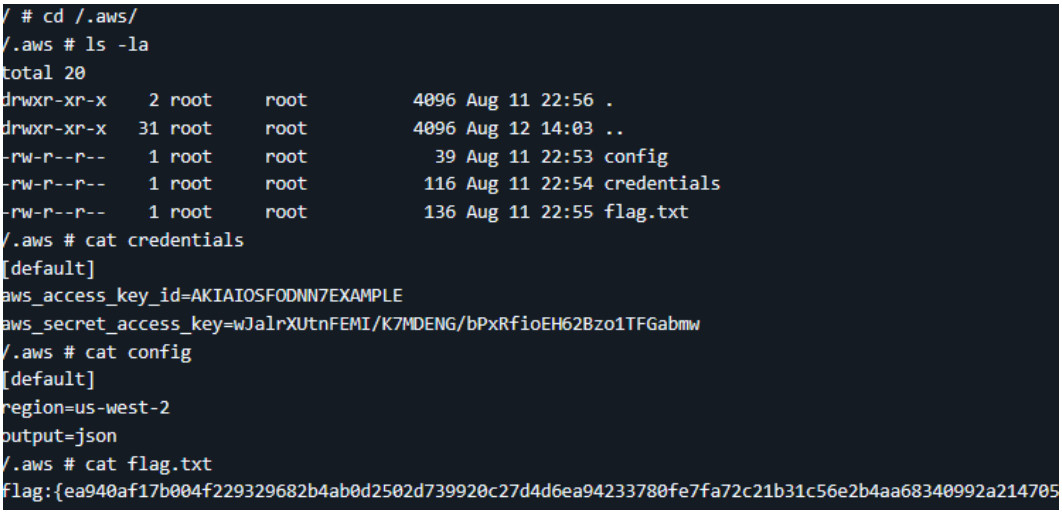
First restart the Docker before pulling the image from the new registry and do :
docker pull 52.53.166.207:5000/dev-aws-test-code:notreadyet

Now it's time to run the image with an interactive shell
docker run -it 52.53.166.207:5000/dev-aws-test-code:notreadyet /bin/sh

And let's do ls -la to see what file folders are present inside this docker container.



There is nothing interesting here but there are hidden files and folders like .aws and .dockerenv. The .aws may hold some interesting credential information.



And there is the flag in the .aws folder that is flag.txt, so cat flag.txt and found the flag.
flag:
{ea940af17b004f229329682b4ab0d2502d739920c27d4d6ea94233780fe7fa72c21b31c56e2b4aa68340992a2147056d298870faf4094f179025579a40266cf1}

Challenge #15

Description : While traveling through where the olympics originated from, I found a spot where I can relax and enjoy ambient sounds around me. Where am I?
The coordinates are : 40° 5'40.42"N by 22° 26'3.97" E
Hint it is what the location is labeled on a map

Using the coordinates, it was easy enough to identify the location. And the location is *Olympus last secret waterfall*, which is also the flag!