

lordsudo.xyz

Irisctf osint challenge

5–7 minutes



Challenge 1:Czech Where?

Description

Iris visited this cool shop a while back, but forgot where it was! What street is it on?

This is the image of the shop.



Hint

FYI: flag is all lowercase and _ for spaces. Please remove all accent marks if there are any. Wrap your answer in irisctf{ }.

Solution

The first thing that comes to mind is to check the image metadata for any probable location information, though in most cases it is usually stripped off the image.

IMAGE METADATA LOCATION FULL METADATA

UPLOAD ANOTHER IMAGE

Image metadata

Name	czechwhere.png
File size	317 KB (334922 bytes)
File type	PNG
MIME type	image/png
Image size	645 x 314 (0.20 megapixel)

Metadata takes 185 Bytes (0.1%) of this image and may include sensitive info. To protect your privacy, download this image without metadata by clicking the button below.

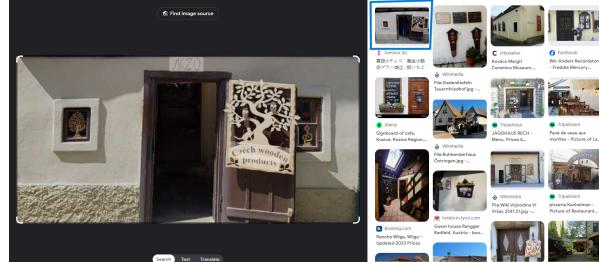
REMOVE METADATA

Location

This photo doesn't include location data.
We can't find where it was taken.

Just as we thought, the location data has been stripped from the image.

We can now do a reverse search with the image and we see an article with the same image. The article points to Golden Lane, Prague castle.



December 21, 2019, 22:30 czech 2019

☀️ Summer trip ☆ Czech Golden Lane @ Prague Castle ⓘ

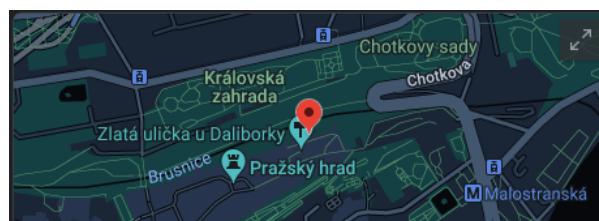
Next was Koganejōji.

Traditional houses line the narrow lanes inside Prague Castle.

Most of the places are souvenir shops, and even though they are included in the ticket, you can't enter unless you pay.

I wonder if they don't let you in for free in the sense that you can see old houses.

A further google search with the shop name leads us right to the address.



Czech Wooden Products

[Directions](#)

[Save](#)

Address: Zlatá ulička u Daliborky, 119 00 Praha 1-Hradčany, Czechia

This gives us the flag: `irisctf{zlatá_úlicka_u_daliborky}`

Challenge 2: Away on Vacation

Description

Iris and her assistant are away on vacation. She left an audio message explaining how to get in touch with her assistant. See what you can learn about the assistant.

The Audio file was provided and its transcript too

Transcript

Hello, you've reached Iris Stein, head of the HR department! I'm currently away on vacation, please contact my assistant Michel. You can reach out to him at michelangelocorning0490@gmail.com. Have a good day and take care.

Solution

Out of Curiosity I sent an email to Michel and got the following response.

Dear,
Thank you for the email. I'm currently away on vacation to celebrate New Years! If you would like a quicker response, feel free to reach out to my social media. I mostly talk about birds on it.
Have a great start to the year, and take care!

We can use epieos.com and find out what data we can get from there and this gives us the full name of the google account in question.

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

Query: michelangelo corning0490@gmail.com

Photo: [View profile picture](#) [Sign up](#)

Name: Michelangelo Corning

ID: 10529103895063888014

Last Update: [View update](#) [Sign up](#)

Services:

- Google Maps:** <https://www.google.com/maps/contrib/10529103895063888014>
- Google Calendar:** <https://calendar.google.com/calendar/u/0/embed?src=michelangelo.corning049...>
- Google Plus Archive:** [https://web.archive.org/web/*/plus.google.com/10529103895063888014*](https://web.archive.org/web/*/plus.google.com/10529103895063888014)

A google search with the name shows us two social media accounts i.e LinkedIn and Instagram

michelangelo corning
Assistant at Stein Station
Los Angeles Metropolitan Area · [Contact Info](#)
2 followers

[Join to view profile](#) [Message](#)

michelangelo_corning [Follow](#)

7 posts · 9 followers · 2 following

Michael here! I love watching wood carving and bird-watching videos in my free time.

[POSTS](#) [TAGGED](#)

We can confirm that the instagram account belongs to him since its all about birds and that's what he hinted towards in his email. Scrolling through the posts we come across a very interesting one that gives us the flag.

michelangelo.corning • [Follow](#)

michelangelo.corning Eyes in The Sky

There are a lot of conspiracy theories about birds being drones for the government. But what's the difference with social media?

Our data is monitored, collected, and utilized for what people believe is the 'bigger picture' of the holy algorithm. Curated feeds and targeted ads are merely the curtain it is the invisible hand that draws back the curtain to expose what's on stage.

<https://public.433fitting.ducks>

This gives us the flag: `irisctf{pub1c_4cc0unt5_4r3_51tt1ng_duck5}`.

Challenge 3: Personal Breach

Description

Security questions can be solved by reconnaissance. The weakest link in security could be the people around you.

This challenge provides us with a link to a web page where we are required to provide some information.

Iris Stein's Info

Please include the spaces.

How old is Iris?

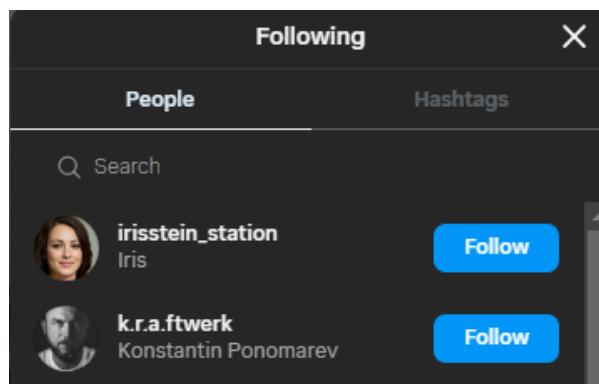
What hospital was Iris born in?

What company does Iris work for?

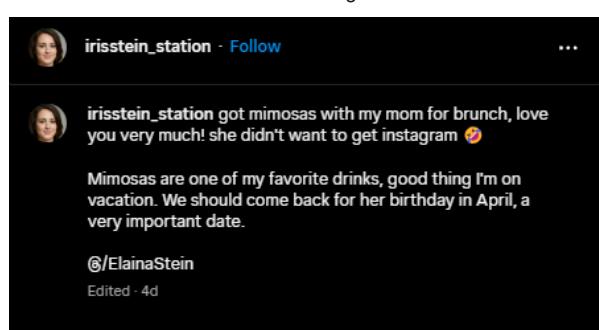
Submit

Solution

Going back to Michel's page, we can check his following which leads us to Iris' Instagram handle.



Perusing through her feed there isn't much of help apart from a single post where she mentions her mum and also tags a handle.



Searching for that username on Instagram bore no fruits, so i decided to shift my focus to the most obvious platform used by the "Elders" - Facebook.

Searching through facebook gave various accounts but finding the exact one was really easy.



 **Elaina Stein** [Add friend](#) [Message](#)

Posts About Friends Photos Videos Check-ins More ...

Scrolling down through her profile we hit basically a gold mine.

Life events

[See all](#)



A day to remember and share. Iris's day!

April 27, 1996



Sweet Birthday Babyy :)

April 8, 1965

We have a hit on Iris' Birthdate which gives us her age - 27yrs

In the comments of the birthday post, we basically hit another gold mine as we can now find the hospital she was born in.

A day to remember and share. Iris's day!
April 27, 1996

 1  1

[Like](#) [Comment](#) [Share](#)

 **Elaina Stein**
I still remember Iris coming into the world. It all happened so fast on a cold day, one minute I was stuck in traffic and the next I was rushed to the closest hospital. Her dad had to rush over from work to help with the delivery. Everything is a blur ... [See more](#)



 Like Reply 2d

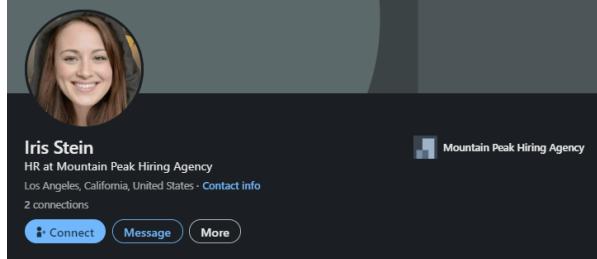
A reverse search of the image gives us the hospital or alternatively we could search by the leading statement from the mum's comment "best maternity hospital in Manhattan" This search gives us results from Yelp which leads us to the answer.

All "maternity hospitals" results in New York, New York

 **1. Lenox Hill Hospital**
2.9 (305 reviews)
Hospitals Upper East Side Open all day
This review is for the labor and delivery and the **maternity ward**. We had a baby here on September... [more](#)

Now for the final answer, we can do a search on LinkedIn for Iris And we get a hit. Information from the previous question tells us that she works in the HR department and thus we can verify that it indeed is her profile and get her company.

[Redacted]



Iris Stein
HR at Mountain Peak Hiring Agency
Los Angeles, California, United States · [Contact info](#)
2 connections
[Connect](#) [Message](#) [More](#)

Using all the details found we can now enter the answers on the web page to get our flag.



Iris Stein's Info
Please include the spaces.

How old is Iris? ✓
 What hospital was Iris born in? ✓
 What company does Iris work for? ✓

[Submit](#)

irisctf{s0cial_m3dia_is_an_inf3cti0n}

This gives us the flag: `irisctf{s0cial_m3dia_is_an_inf3cti0n}`

Challenge 4: A Harsh Reality of Passwords

Description

Recently, Iris's company had a breach. Her password's hash has been exposed. This challenge is focused on understanding Iris as a person.

Hash:

\$2b\$04\$DkQOnBXHNLw2cnsmSEdM0uyN3NHLUb9l5IIUF3akpLwoy7dlhgyEC

The flag format is `irisctf{plaintextPassword}`

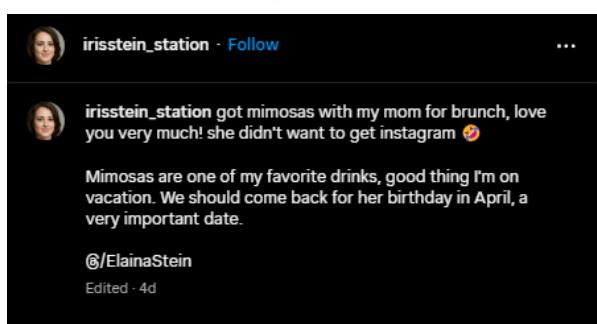
Hint

Focus on Iris and what she finds important! There are three words (not letters, but words), and a certain amount of numbers following it. There's no leet words, proper capitalization nothing like (ExAmPLE), no special characters as well like -, ! etc. If you find a specific date, do not include the month's name into your word list. Just use the numbers!!

Solution

We start with a hash and need to decrypt it for which we shall require a wordlist. This needs us to gather key information to include in the wordlist.

Scouring through her Instagram, she mentioned her Mum's birthday being an important date and we can get this from the mum's facebook. This should be our numbers - as per the hint.



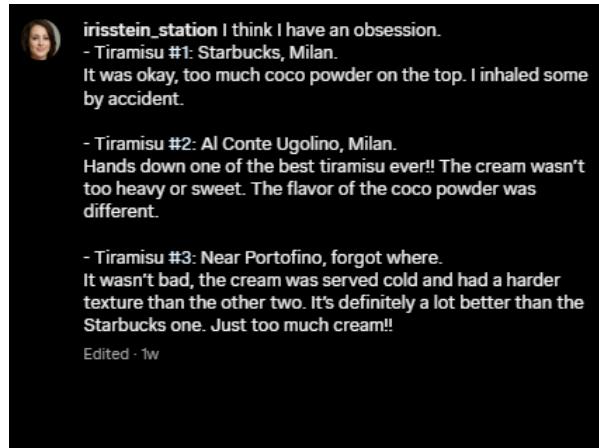
irisstein_station · Follow

irisstein_station got mimosas with my mom for brunch, love you very much! she didn't want to get instagram 😊

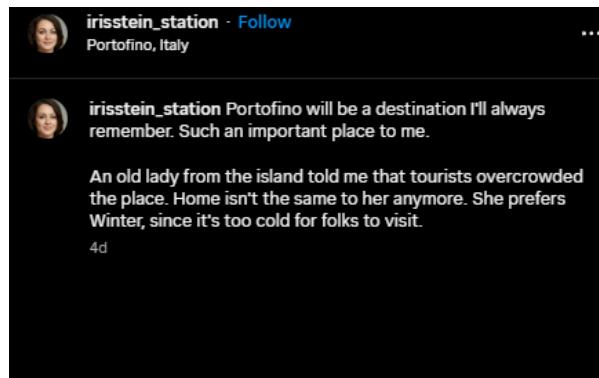
Mimosas are one of my favorite drinks, good thing I'm on vacation. We should come back for her birthday in April, a very important date.

@ElainaStein
Edited · 4d

She also mentioned having 'mimosas', and we can add that too. As we keep scrolling she mentions she has an obsession with 'Tiramisu' and we can take note of this too.



In another post, she mentions how 'Portofino' will always be a destination to remember.



Going through all the posts and various things that may be important we can gather enough information to create a wordlist.

We can generate the wordlist using a python script

```
from itertools import permutations

def generate_combinations(words, num_str):
    word_combinations = permutations(words, 3)
    all_word_combinations = [''.join(combo) for combo in word_combinations]

    num_combinations = permutations(num_str, len(num_str))
    all_num_combinations = [''.join(combo) for combo in num_combinations]

    combined_results = [word_combo + num_combo for word_combo in all_word_combinations for num_combo in all_num_combinations]
    return combined_results

def write_to_file(results, filename):
    with open(filename, 'w') as file:
        for result in results:
            file.write(result + '\n')

def main():
    words = ["Iris", "Stein", "Elaine", "Tiramisu", "Portofino", "Mimosas", "Italy"]
    date_numbers = "08041965"

    all_combinations = generate_combinations(words, date_numbers)
    write_to_file(all_combinations, 'iriswordlist.txt')

if __name__ == "__main__":
    main()
```

We now have a wordlist file that we can run against the hash. The hash is input in a text file and run against hashcat

```
hashcat -m 3200 hash.txt iriswordlist.txt
```

```
$ hashcat -m 3200 hash.txt iriswordlist.txt --show
$2b$04$DkQ0nBXHNLw2cnsmSEdM0uyN3NHLUb9ISIIUF3akpLwoy7dlhgycPortofinoItalyTiramisu0481965
```

This gives us the matching password PortofinoItalyTiramisu0481965

The flag: iriscf{PortofinoItalyTiramisu0481965}

Nos vemos en mi próximo artículo...

