

Day 14 - Where's Rudolph?

Scenario



Day 14: Where's Rudolph?:

*'Twas the night before Christmas and Rudolph is lost
Now Santa must find him, no matter the cost
You have been hired to bring Rudolph back
How are your OSINT skills? Follow Rudolph's tracks...*

Task #1

*While hunting and searching for any hints or clues
Santa uncovers some details and shares the news
Rudolph loved to use Reddit and browsed aplenty
His username was 'IGuidetheClaus2020'*

Wrapping Up



*It looks like finding Rudolph was a bit too easy
His OPSEC would make any security pro queasy
To the Windy City, Rudolph was tracked
Christmas is saved, we brought Rudolph back*


so it seems like this was an OSINT challenge with Rudolph username provided
here it gives us 2 clue about Rudolph:
-username: IGuidetheClaus2020
-platform: reddit


let's use Google Dorking technique to find rudolph reddit account & we've found 2 results here
//let's check out rudolph's reddit comments


"IGuidetheClaus2020" site:reddit.com


×





 All

 Maps

 Images

 Videos

 News

 More

Settings

Tools

2 results (0.26 seconds)

www.reddit.com › user › comments ▼

[comments by IGuidetheClaus2020 - Reddit](#)

The u/IGuidetheClaus2020 community on Reddit. Reddit gives you the best of the internet in one place.

www.reddit.com › user › submitted ▼

[submitted by IGuidetheClaus2020 - Reddit](#)

IGuidetheClaus2020. 1 post karma 0 comment karma. send a private message. get them help and support. redditor for 11 hours ...

In order to show you the most relevant results, we have omitted some entries very similar to the 2 already displayed.

If you like, you can [repeat the search with the omitted results included](#).

Rudolph's reddit comment page

The screenshot shows the Reddit interface for the user [u/IGuidetheClaus2020](#). The 'COMMENTS' tab is selected. There are two comments visible:

- Comment 1:** IGuidetheClaus2020 commented on [Looooool](#) (a link to [i.redd.it/izu70q...](#)) in [r/Twitter](#). Posted by [u/FriegusTheBoss](#). The comment text is: "Ouch. Some days I love Twitter. Some days, it's just...lol." It has 1 point and was posted 20 days ago.
- Comment 2:** IGuidetheClaus2020 commented on [Chicago Public Library says eliminating fines has paid off - After eliminating overdue fees late last year, Chicago Public Library employees saw something that made everyone smile: a jump in the return of books overdue for six months or more.](#) (a link to [chicago.suntimes.com/2020/1...](#)) in [r/books](#). Posted by [u/speckz](#). The comment text is: "Fun fact: I was actually [born](#) in Chicago and my creator's name was Robert!" It has 5 points and was posted 20 days ago.

Question: What URL will take me directly to Rudolph's Reddit comment history?

The screenshot shows a browser's address bar with the URL: <https://www.reddit.com/user/IGuidetheClaus2020/comments/>

in one of the comment, Rudolph did comment that he's from Chicago

This is a close-up of the second comment from the previous screenshot. It shows the text: "Fun fact: I was actually [born](#) in Chicago and my creator's name was Robert!"

Question: According to Rudolph, where was he born?
-Chicago

Creator name Robert? so now we got another clue again
my creator's name was Robert!

let's use googleFu again with these 2 clue, and we've found Robert's Last Name

"Rudolph" AND "Robert"



All

Images

Videos

Maps

News

More

Settings

About 34,400,000 results (1.15 seconds)

www.npr.org › 2013/12/25 › writing-rudolph-the-origina...

Writing 'Rudolph': The Original Red-Nosed Manuscript : NPR

Dec 25, 2013 — Author Robert May considered other names before settling on Rudolph. Imagine: We could be singing instead about the very shiny nose on ...

Created by: Robert L. May

Question: Rudolph mentions Robert. Can you use Google to tell me Robert's last name?
-May

now let's check out does Rudolph have used any other social platform using googleFu again.
//Rudolph seems to have a twitter account here

"IGuidetheClaus2020"



All

Maps

Images

Videos

News

More

Settings

About 4 results (0.31 seconds)

twitter.com › iguideclaus2020 ▾

IGuidetheClaus2020 (@IGuideClaus2020) | Twitter

The latest Tweets from IGuidetheClaus2020 (@IGuideClaus2020). Seeking the truth. Really. Business inquiries: rudolphthered@hotmail.com. North Pole.

interesting the profile was literally the same as the challenge



IGuidetheClaus2020

23 Tweets



...

Follow

IGuidetheClaus2020

@IGuideClaus2020

Seeking the truth. Really.

Business inquiries: rudolphthered@hotmail.com

📍 North Pole 📅 Joined November 2020

5 Following 92 Followers

Not followed by anyone you're following

Tweets

Tweets & replies

Media

Likes

Home

Explore

Notifications

Messages

Bookmarks

Lists

Profile

More

Tweet



Day 14: Where's Rudolph?:

*'Twas the night before Christmas and Rudolph is lost
Now Santa must find him. no matter the cost*

& we found Rudolph's twitter username, we got another clue again right now



Question: What is Rudolph's username on that platform?

-IGuideClaus2020

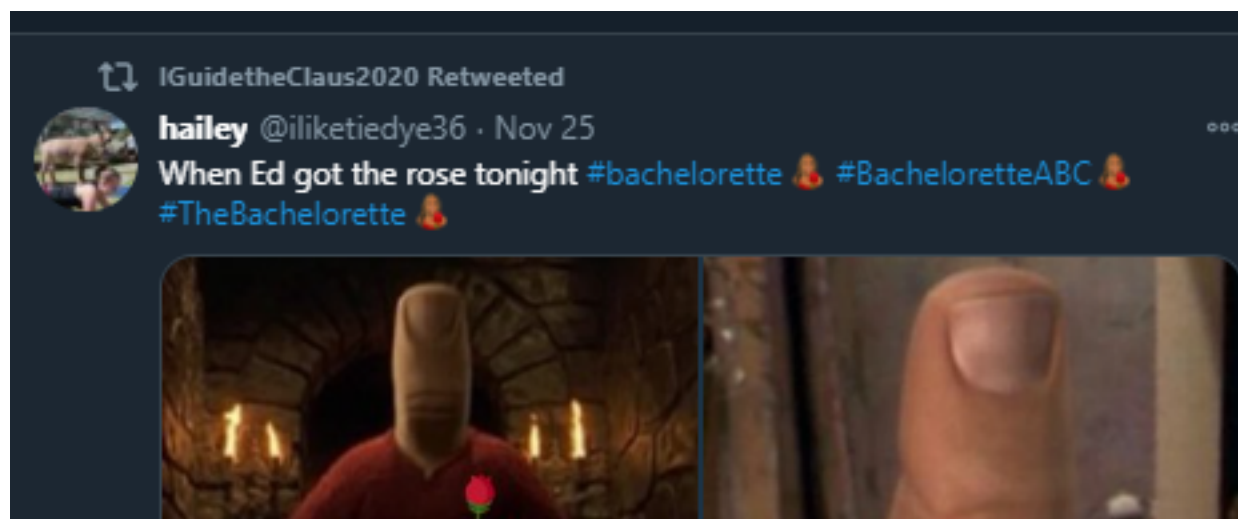
Enumerating Rudolph's twitter

Task #2

*Well it looks like you have uncovered Rudolph's Twitter
Now we can read into all of his chitter
Go through his profile and give it some views
The deeper you dig, the better the clues*

By finding another account belonging to our user, we open up the possibility of gathering even more information. Utilize the information found on Rudolph's Twitter account to answer questions #6-11.

if we notice that most of the retweet that Rudolph made was about this tag 'Bachelorette'







did some googleFu about what's Bachelorette is & it seems to be a tv show. This might be one of Rudolph favorite tv show then.

About 140,000,000 results (0.74 seconds)


Videos




[Heartbroken Ben Says Goodbye | The Bachelorette](#)
YouTube - Bachelor Nation
12 hours ago



[PREVIEW: Two Night Finale! | The Bachelorette](#)
YouTube - Bachelor Nation
12 hours ago



[The Bachelorette 2020 Finale Sneak Peek - The Bachelorette](#)
YouTube - Bachelor Nation on ABC
9 hours ago

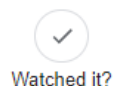


[Can Ben Tell Tayshia He's In Love? | The Bachelorette](#)
YouTube - Bachelor Nation



The Bachelorette

2003 · Reality · 16 seasons



Question: What appears to be Rudolph's favorite TV show right now?
-Bachelorette

this post shows that rudolph goes to a parade before



so we did some reverse image search using the 1st image & we end up in this post

Home > News & Events > Thompson Coburn 'floats' down Michigan Avenue in first Magnificent Mile Lights Festival appearance



Thompson Coburn 'floats' down Michigan Avenue in first Magnificent Mile Lights Festival appearance

December 9, 2019



& here it shows that the parade was called 'Lights Festival parade'

The **Lights Festival parade**, one of the largest holiday parades in the city, featured a lighting ceremony and over one million holiday lights lining the parade route, shown the following evening on ABC7 Chicago and rebroadcast on local television.

When an opportunity to take part in the parade came to our Chicago office, we were excited to participate.

did some googleFu again & we found this "Chicago Event" ! It's in Chicago

www.themagnificentmile.com > lights-festival ▾

Lights Festival | Chicago Event - The Magnificent Mile

Learn all about the BMO Harris Bank Magnificent Mile Lights Festival, one of the ... / there will not be a live parade this year, ABC 7 promises an hour of ...

Question: Based on Rudolph's post history, he took part in a parade. Where did the parade take place?
-Chicago

Rudolph did give a higher res of image something about outside of his hotel



& it's the same photo as the previous post

<https://tcm-sec.com/wp-content/uploads/2020/11/lights-festival-website.jpg>



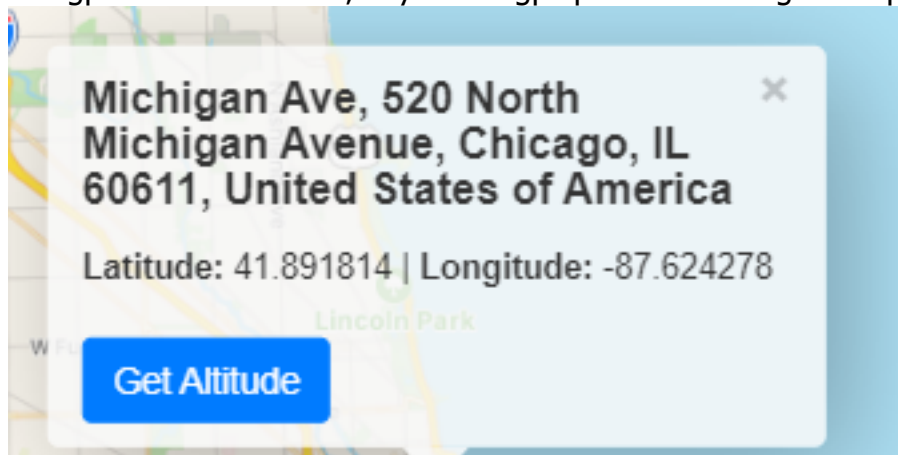
let's download it and check the metadata

```
exiftool lights-festival-website.jpg
```

it seems that here did shown the GPS coordinate of the image captured

```
GPS Latitude      : 41 deg 53' 30.53" N
GPS Longitude     : 87 deg 37' 27.40" W
GPS Position      : 41 deg 53' 30.53" N, 87 deg 37' 27.40" W
Image Size        : 650x510
```

use gps-coordinates.net, key in the gps position & we got the place it tooks the image

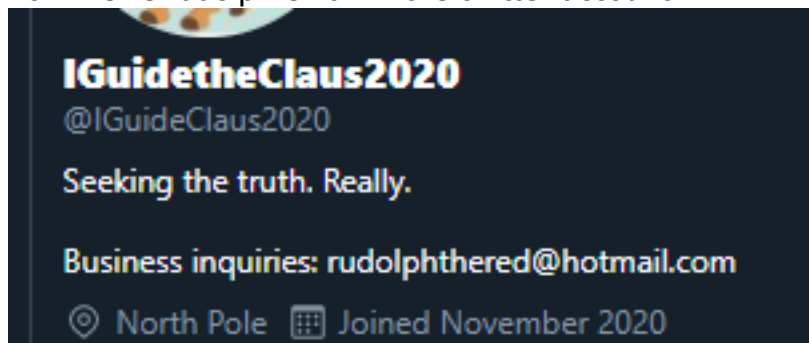


Question: Okay, you found the city, but where specifically was one of the photos taken?

tweaking the coordinate(last decimal digit) & we got the correct answer
-41.891815, -87.624277

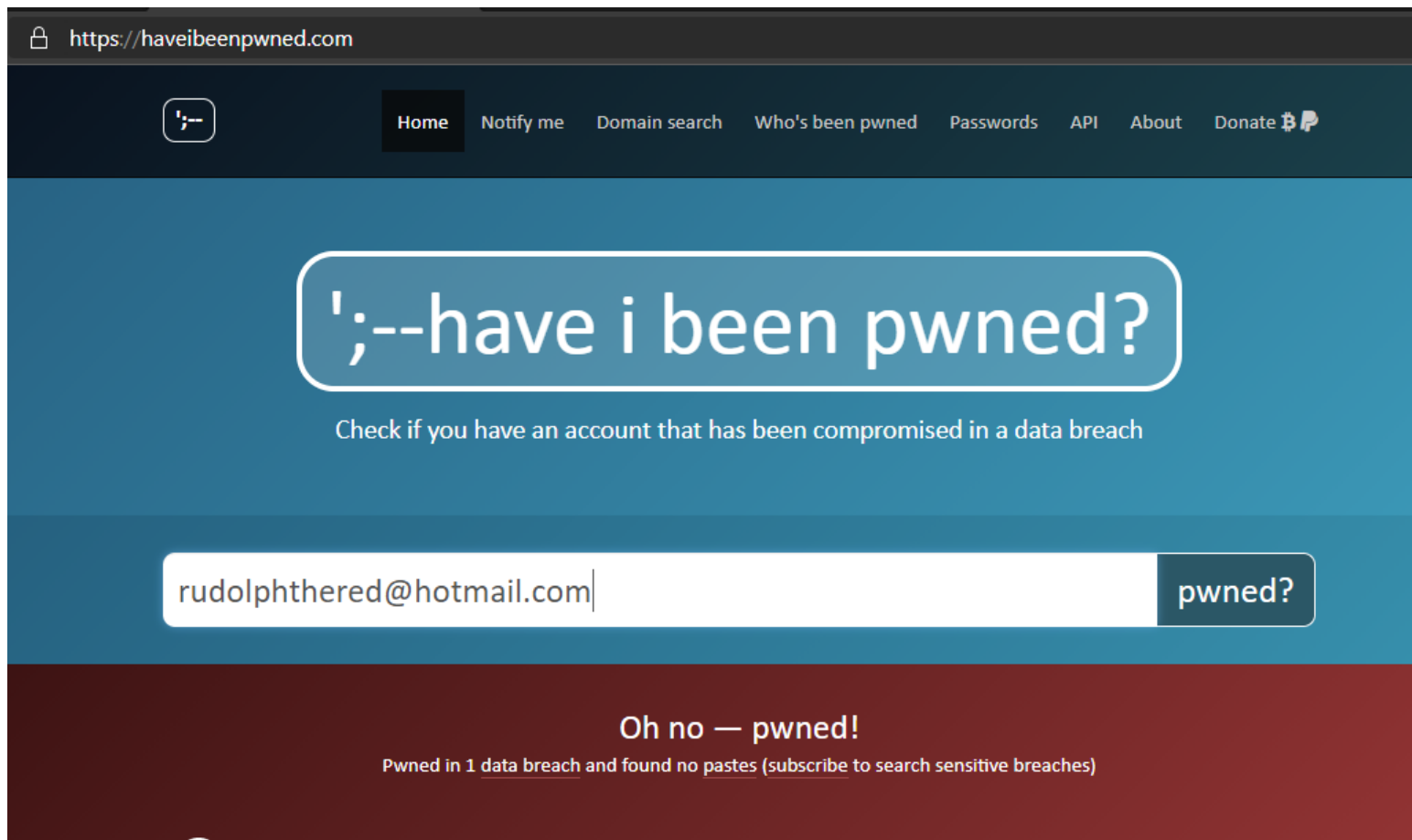
in the exifdata we able to find the flag too under COPYRIGHT

now we've rudolph email in the twitter account



let's check out does this account has any password breach before?

in haveibeenpwned.com it shows that there's 1 data breach for rudolph's business email



in the additional info section, the challenge creator do gave us some interesting information about checking pwned email credentials

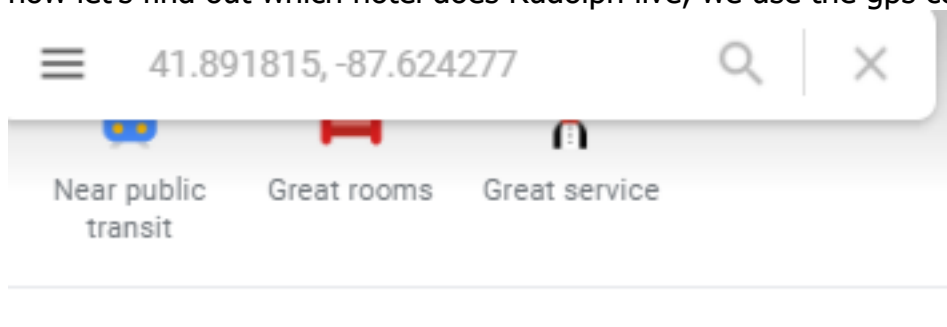
Websites such as <https://haveibeenpwned.com/> will help identify if an account has ever been breached and will, at a minimum, inform us if an account existed at one point. However, it does not provide any password information. Free sites such as <http://scylla.sh/> will provide password information and are easy to search through. The data on free sites can tend to be older and not up to date with the latest breach information, but these sites are still a powerful resource. Lastly, paid sites such as <https://dehashed.com/> offer up to date information and are easily searchable at affordable rates.

let's try out using scylla.sh this free website & we got the password!

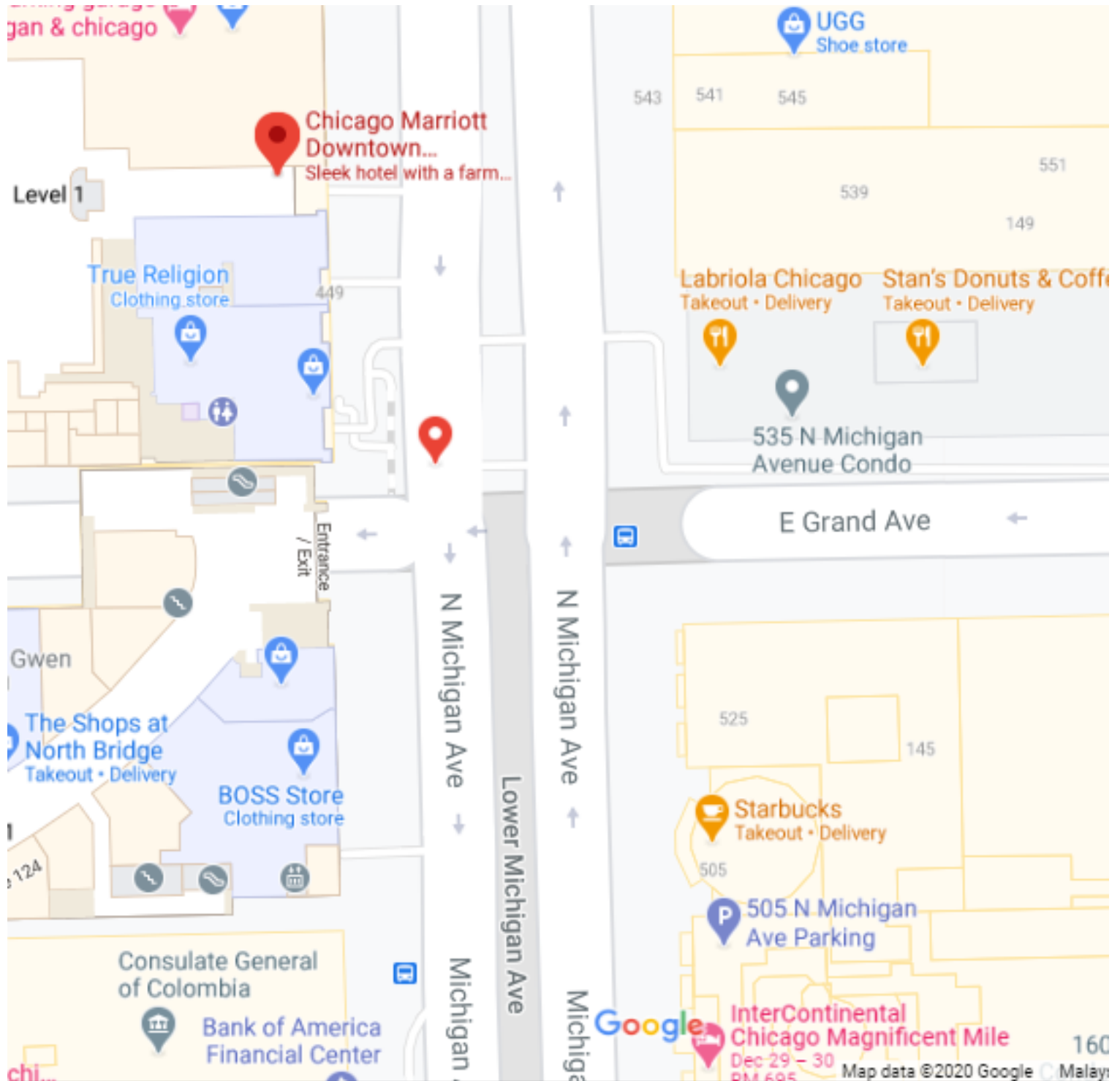
Please enter a search term...
email:rudolphthered@hotn

IP	Domain	Username	Passhash	Email	Name	Password
null	Collections	null	null	rudolphthered@hotmail.com	null	spygame

now let's find out which hotel does Rudolph live, we use the gps coordinate in googleMap



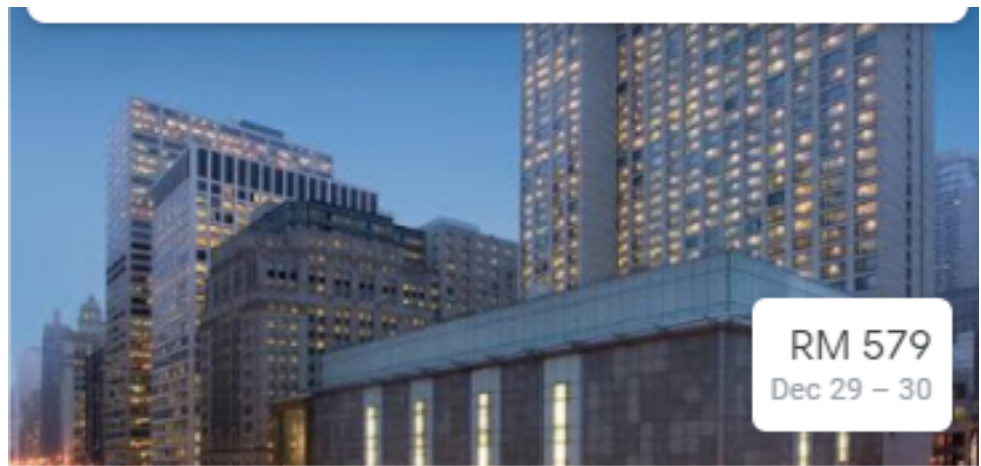
here's where the location were



based on the details in the twitter rudolph said that he capture the image outside of his hotel



checking out the map again the most possible hotel will be Chicago Marriott Downtown Magnificent Mile Hotel as this is a walking distance where they no need to passby the busy road



Chicago Marriott Downtown Magnificent Mile

4.3 ★★★★★ 2,403 reviews · 4-star hotel

Question: Based on all the information gathered. It's likely that Rudolph is in the Windy City and is staying in a hotel on Magnificent Mile. What are the street numbers of the hotel address?

the street number for it will be 540

540 N Michigan Ave, Chicago, IL 60611, United States

Located in: The Shops at North Bridge

marriott.com

