

PSP0201

Week 4

Writeup

Group Name: Undecided

Members

ID	Name	Role
1211101390	Aslamia Najwa Binti Ahmad Khadri	Leader
1211100431	Mohammad Omar Torofder	Member
1211103388	Vishnu Karmegam	Member
1211103092	Farryn Aisha binti Muhd Firdaus	Member

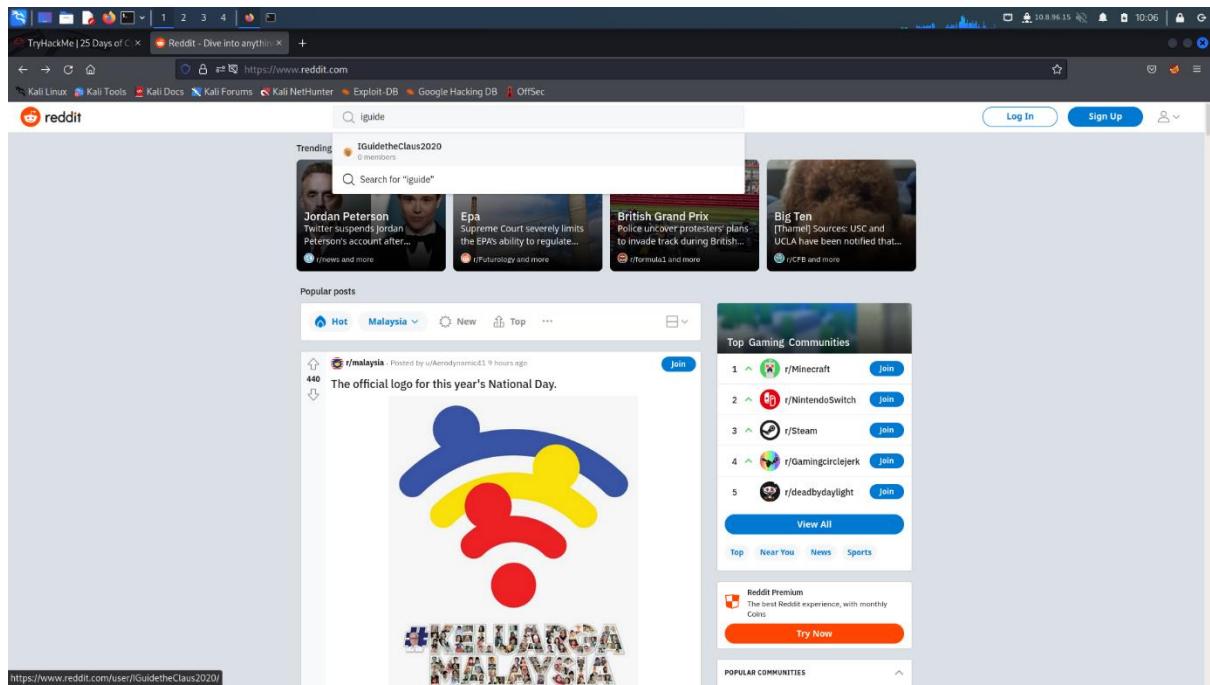
Day 14: OSINT – Where's Rudolph?

Tools used: Firefox

Solution/walkthrough:

Question 1

To find the URL that will take us directly to Rudolph's Reddit comment history, we first went to Reddit website.



We searched Rudolph's username in Reddit with the username provided in the tryhackme room.

The screenshot shows a web browser window with multiple tabs open. The active tab is a Reddit profile page for the user [u/IGuidetheClaus2020](#). The profile picture is a cartoon reindeer head. The user has 36 karma and a 'Cake day' on November 23, 2020. They have received a 'One-Year Club' trophy. The sidebar includes links for Help, About, Reddit Coins, Reddit Premium, Careers, Press, Advertise, Blog, Terms, Content Policy, Privacy Policy, and Mod Policy. At the bottom, it says 'Reddit Inc © 2022. All rights reserved.'

Once we found Rudolph's Reddit account, we navigate to the comments. By doing so, we obtained the URL that will directly lead us to Rudolph's Reddit comment history.

The screenshot shows the same Reddit profile page for [u/IGuidetheClaus2020](#), but now the 'Comments' tab is selected. The comments section is populated with posts from the user, including one where they mention being born in Chicago. The interface is identical to the previous screenshot, with the sidebar and footer visible.

Question 2

Browsing through Rudolph's comment history in Reddit, we found a comment mentioning that Rudolph was born in Chicago.

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. chicago.suntimes.com/2020/3... r/books Posted by u/specza

IGuideTheClaus2020 5 points · 2 years ago
Fun fact: I was actually born in Chicago and my creator's name was Robert!

Reply Share

Question 3

Robert was mentioned in Rudolph's comment earlier. We went to go google and searched for Robert's last name which was May.

Google search results for "rudolph creator robert". The results page includes a snippet from Wikipedia about Robert L. May, a photo of him, and sections for "People also ask" and "Books".

People also ask :

- Who invented Rudolph?
- When did Robert May create Rudolph?
- Where was Robert L. May born?
- Where did the idea of Rudolph come from?

Books

View 2+ more

Rudolph the red-nosed reindeer (1939) Rudolph Shines Again (1964) Rudolph's second Christmas (1964) Rudolph to the Rescue (1964)

Question 4

After observing other comments left by Rudolph in Reddit, we discover that he loves Twitter.

IGuideTheClaus2020 commented on Looooool redd.it/zv70q... r/Twitter Posted by u/FriegusTheBoss

IGuideTheClaus2020 1 point · 2 years ago
Ouch. Some days I love Twitter. Some days, it's just...lol.

Reply Share

For confirmation, we also search for his username in name check-up website where it mentioned that the username is available in Twitter. Hence, Rudolph might have a Twitter account.

Find Available Username

IGuidetheClaus2020

Need name suggestion? or +100 Search Results

Share Tweet

Start Now!

Click on domains after search for purchase options and whois info

.com	.net	.org	.co	.biz	.io	.at	.us	.me
Available	Taken	Available						
.co.uk	.eu	.info	.xyz	.live	.pro	.am	.tv	.shop
Available								
.life	.ch	.today	.in	.club	.cc	.tech	.site	.online
Available								
.store	.space	.website	.vip	.host	.press	.digital	.guru	.de
Available								
.ltd	.tk	.nl	.ca	.tw	.fr	.ws	.work	.tools
Available								

Kodo Kado 百万小说创作大赏 总奖额 TWD 500 万

Question 5

We searched for his Twitter account and found his username 'IGuideClaus2020'.

IGuideClaus2020

23 Tweets

IGuideClaus2020
@IGuideClaus2020

Seeking the truth. Really.

Business inquiries: rudolphthered@hotmail.com

North Pole Joined November 2020

5 Following 172 Followers

Not followed by anyone you're following

Tweets Tweets & replies Media Likes

IGuideClaus2020 Retweeted Tesla Nov 8, 2020

20k Superchargers and counting

You might like

Ashutosh mishra @ashutoshmishra78 Follow

Jon | Dark (he/him) @darkstar7471 Follow

harry @harrytxtt Follow

Show more

Trends

#GemilangkanLagi

Cheer on our national shutters at the PETRONAS Malaysian Open 2022

Promoted by PETRONAS

1 - Trending worldwide

金スマ

61K Trends

Question 6

Scrolling through Rudolph's tweet, we found a lot of tweets mentioning Bachelorette. Upon searching Bachelorette, we realize that it is a TV show, and it appears to be Rudolph's favourite TV show.

A screenshot of a Twitter profile for the user @GuideTheClaus2020. The tweet content is: "Love me some Bachelorette. But Ed? C'mon!". The timestamp is 10:11 AM - Nov 25, 2020. The sidebar on the right displays the "Relevant people" section, which includes the user's profile picture and bio: "Seeking the truth. Really. Business inquiries: rudolphthered@hotmail.com". Below that is the "Trends" section, which lists "#GemilangKanLagi" as a promoted trend.

Question 7

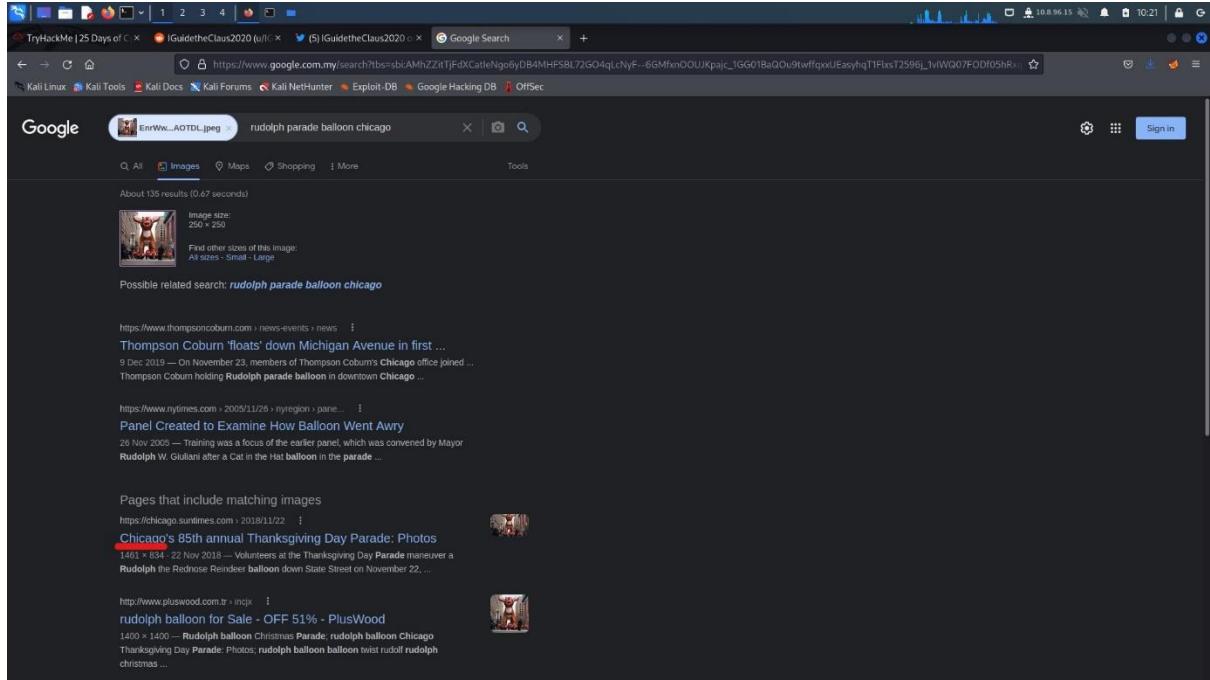
One of Rudolph's tweets on 25 November 2020 showed pictures of a parade. We decided to save the photos.

A screenshot of a Twitter profile for the user @GuideTheClaus2020. The tweet content is: "Day and night. It got a little cold, so I put a scarf on. Hehe". The timestamp is 9:57 AM - Nov 25, 2020. The sidebar on the right displays the "Relevant people" section, which includes the user's profile picture and bio: "Seeking the truth. Really. Business inquiries: rudolphthered@hotmail.com". Below that is the "Trends" section, which lists three trending topics: "#GemilangKanLagi", "#StrangerThings4", and "#時をかける少女".

We went to Google to search by image that we saved earlier.

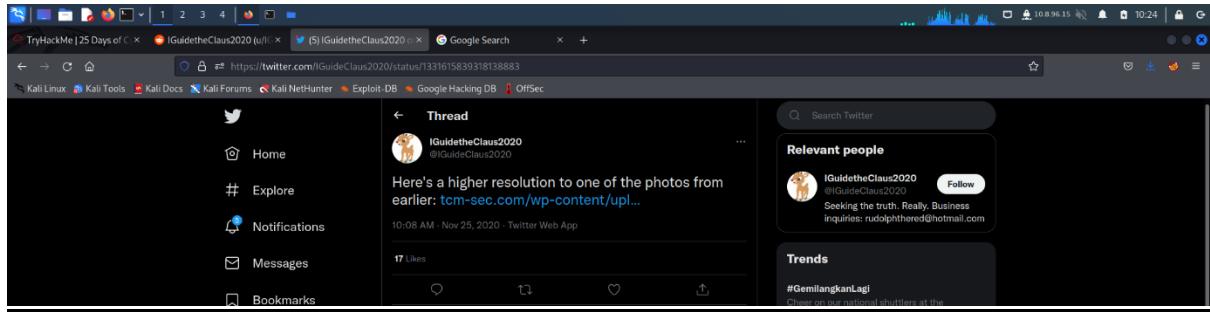
A screenshot of a Google Images search interface. At the top, there is a search bar with the placeholder text "Search by image". Below the search bar are two input fields: "Paste image URL" and "Upload an image". To the right of these fields is a "Sign in" button. On the far right, there is a "Sign in to Google" box with the text "Save your passwords securely with your Google Account" and two buttons: "No thanks" and "Sign in".

After searching by image of the parade, we found articles mentioning that the parade took place in Chicago.

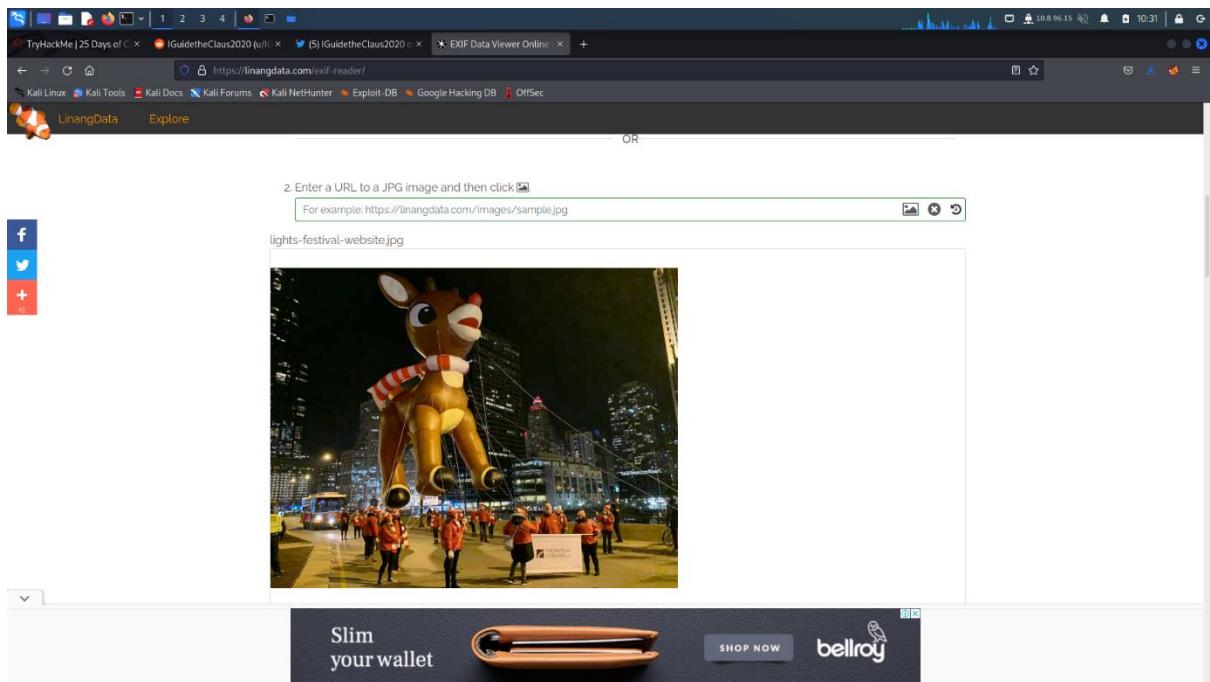


Question 8

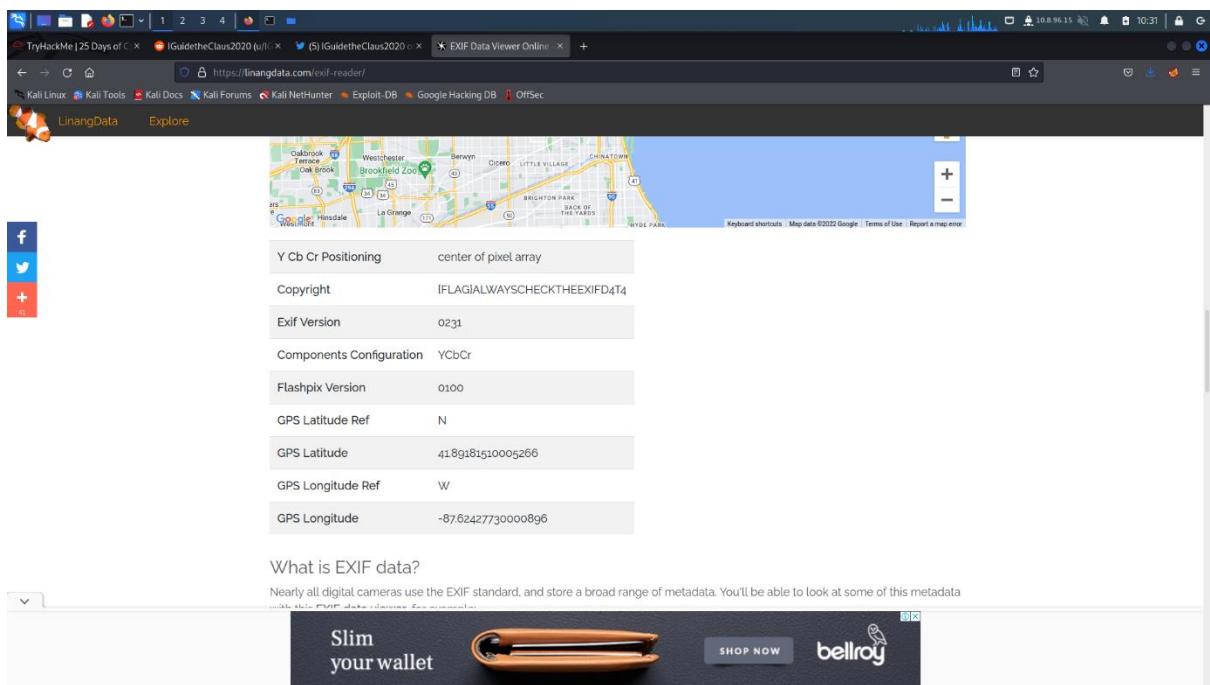
Another Rudolph's tweet on 25 November 2020 gave us a link to a higher resolution to one of the photos earlier. We saved the high-resolution photo.



We went to a website that will show us the metadata of the photo to gain information of the location.



The GPS Latitude and GPS Longitude value gave us the specific location of the parade.



Question 9

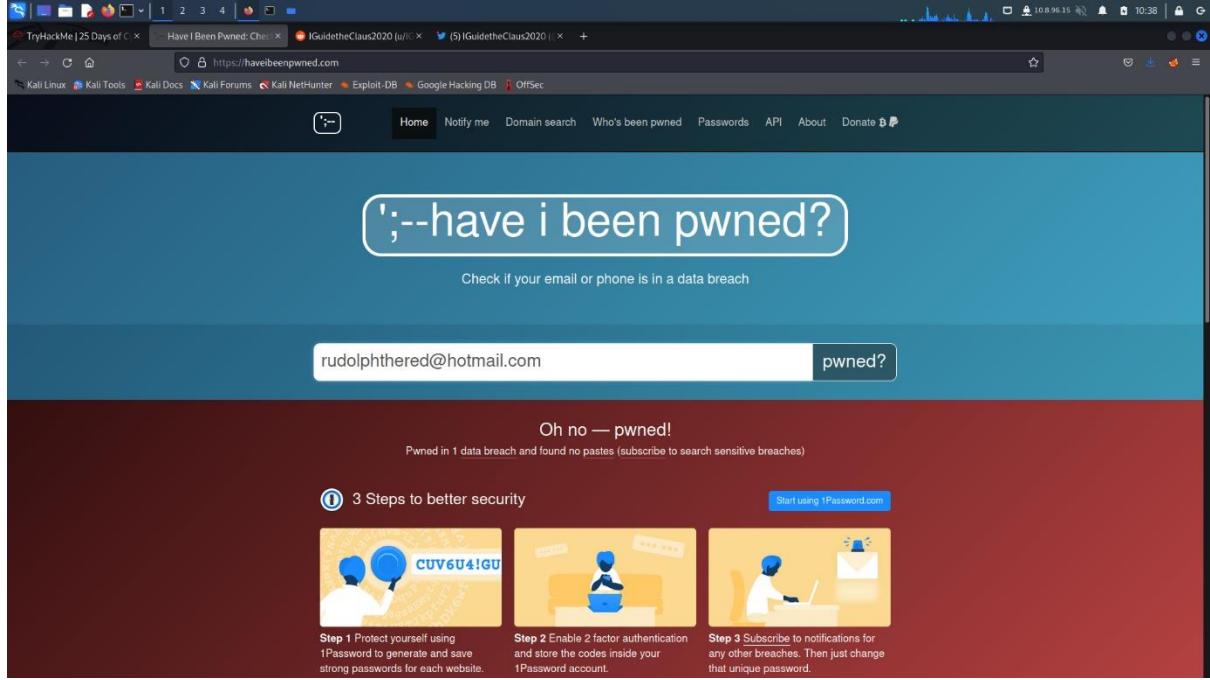
The website we use to scan the metadata has also showed us the flag which was under the copyright.

Copyright

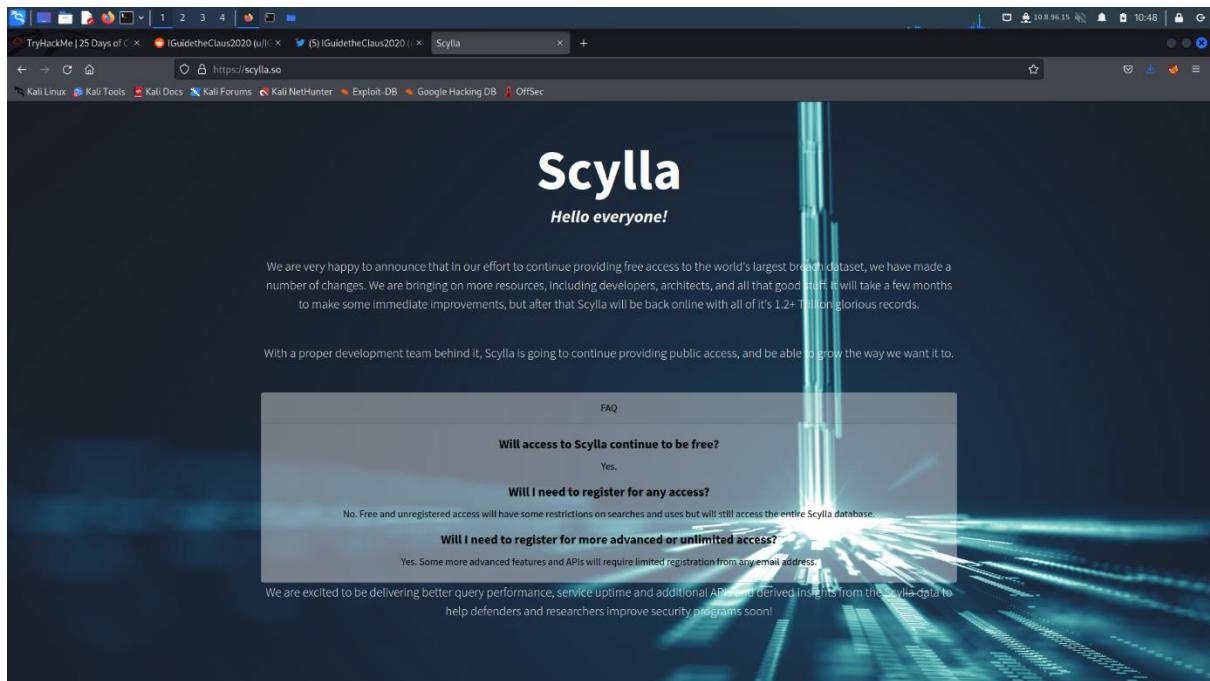
[FLAG]ALWAYSCHECKTHEEXIFD4T4

Question 10

We went to haveibeenpwned.com website to scan whether Rudolph's email has been pawn or not and the result said that Rudolph has been pawned.



Next, to find out what's the password to Rudolph's email, we went to scylla.so website but unfortunately, it is currently unavailable.



We searched for other alternatives, but we could not find any, so we resort to our last option which is obtaining the password from other people's walkthrough. Here, we finally retrieve the password 'spygame'.

HYPERION GRAY

*Search is in beta, please report bugs to the scylla github repo Please note the API is rate limited to 2 searches per second.

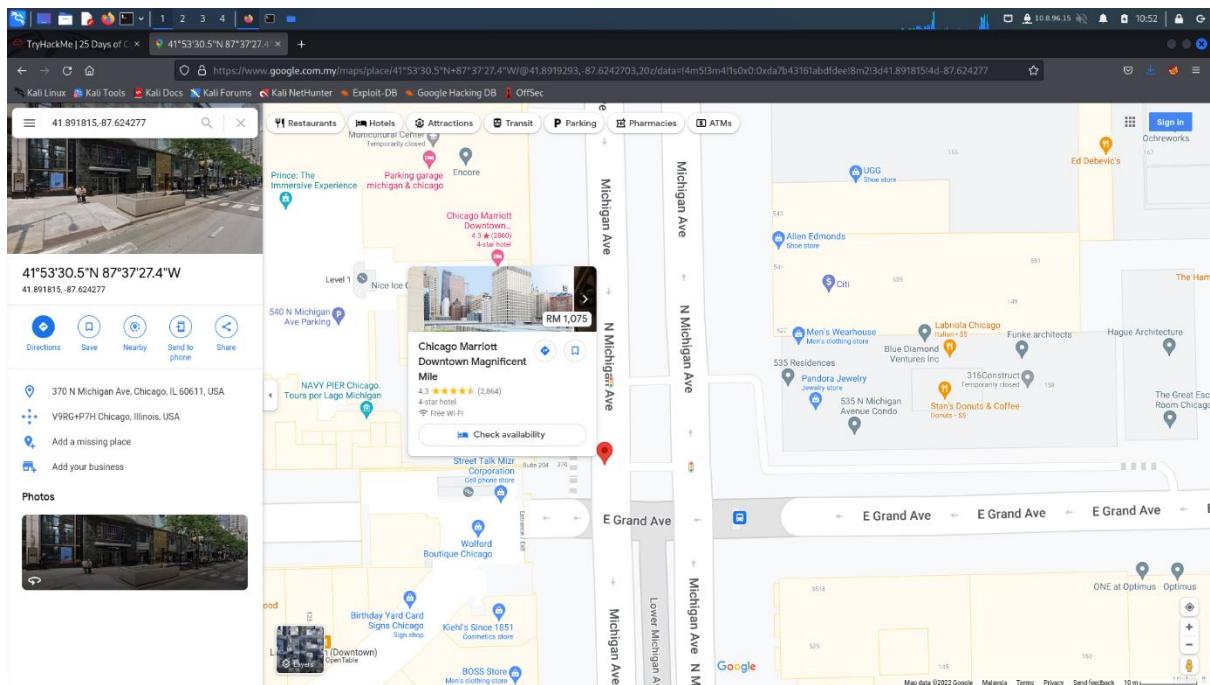
Please enter a search term...
udolphthered@hotmail.com

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

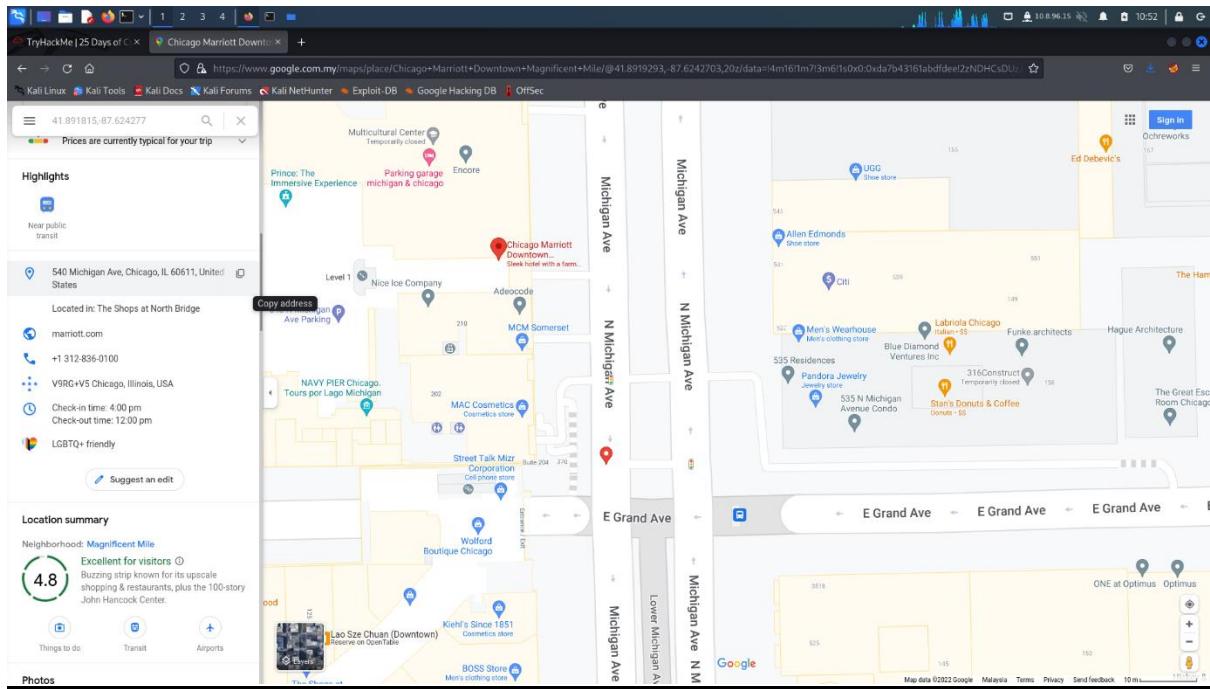
1-1 of 1 < >

Question 11

We searched for the street number of the hotel address with the latitude and longitude that we secure earlier in Google Map.



Near the coordinate location, we found a hotel close by. We clicked the hotel to gain more information and found the street number.



Thought Process/Methodology:

After receiving Rudolph's username, we immediately browsed to Reddit and searched for his username. Once we found it, we opened his account page and navigate to the comments. By doing so, we obtained the URL that will directly lead us to Rudolph's comment history. After that, we decided to look around his comment history and stumbled across a comment of his mentioning that he was born in Chicago. The comment also mentioned that Robert was his creator. We went to Google to further investigate his creator and found Robert's last name which was May. We proceeded to observe other comments left by Rudolph. There was a comment that noted his love for Twitter. For confirmation that Rudolph uses Twitter, we went to a website that will check whether his username exist in certain platform or not and Rudolph's username is available in Twitter. We searched for his username in Twitter and found his account. Scrolling through Rudolph's tweet, we found a lot of tweets mentioning Bachelorette. After careful research, we concluded that Bachelorette is a TV show that appeared to be Rudolph's favourite. We then continued exploring his tweet. On one of his tweets on 25 November 2020, we discover pictures of a parade. We saved the pictures to search by image in Google. Once we do so, we found articles pointing out that the parade happens in Chicago. Afterward, we found a tweet by Rudolph that gave us a link that led us to a higher resolution photo of the parade. To find more information regarding the photo, we investigated a website that showed us the metadata of the photo. On the website, we obtained the coordinate of the parade and the flag. Next, we checked whether Rudolph's email has been pawned or not and discover that it has indeed been pawned. We went to Scylla website to find Rudolph's email password but our dismay, the website is currently unavailable. We looked for other alternatives but could not find any. Alas, we resorted to our last option which is obtaining the password from other people's walkthrough. There, we finally retrieve Rudolph's password 'spygame'.

Finally, we searched for the street number of the hotel address with the latitude and longitude that we secure earlier in Google Map. We found a hotel close by. We look for more information on the hotel and found the street number.