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

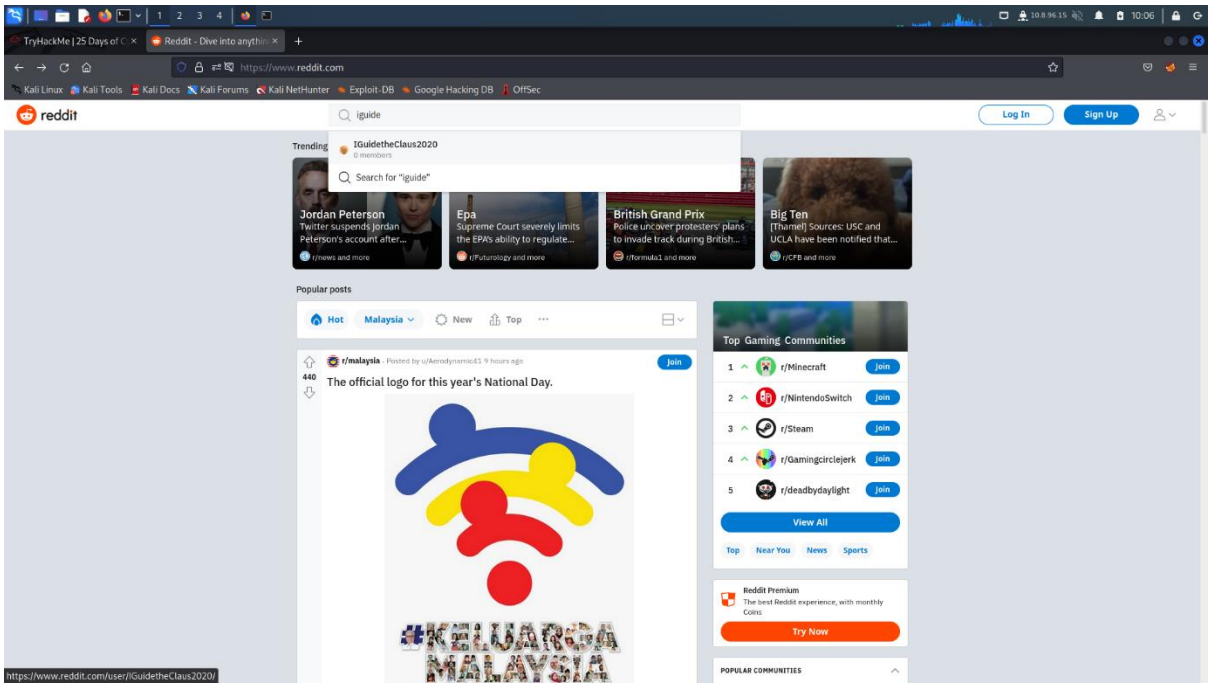
Day 14: OSINT – Where's Rudolph?

Tools used: Firefox

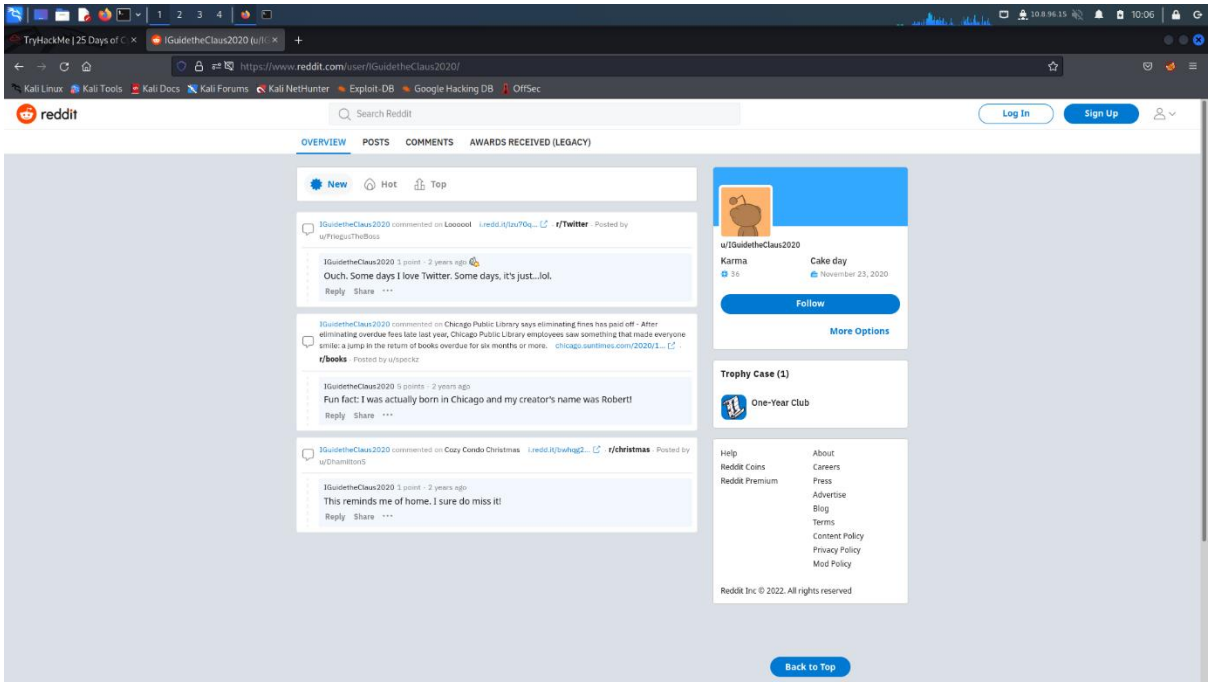
Solution/walkthrough:

Question 1

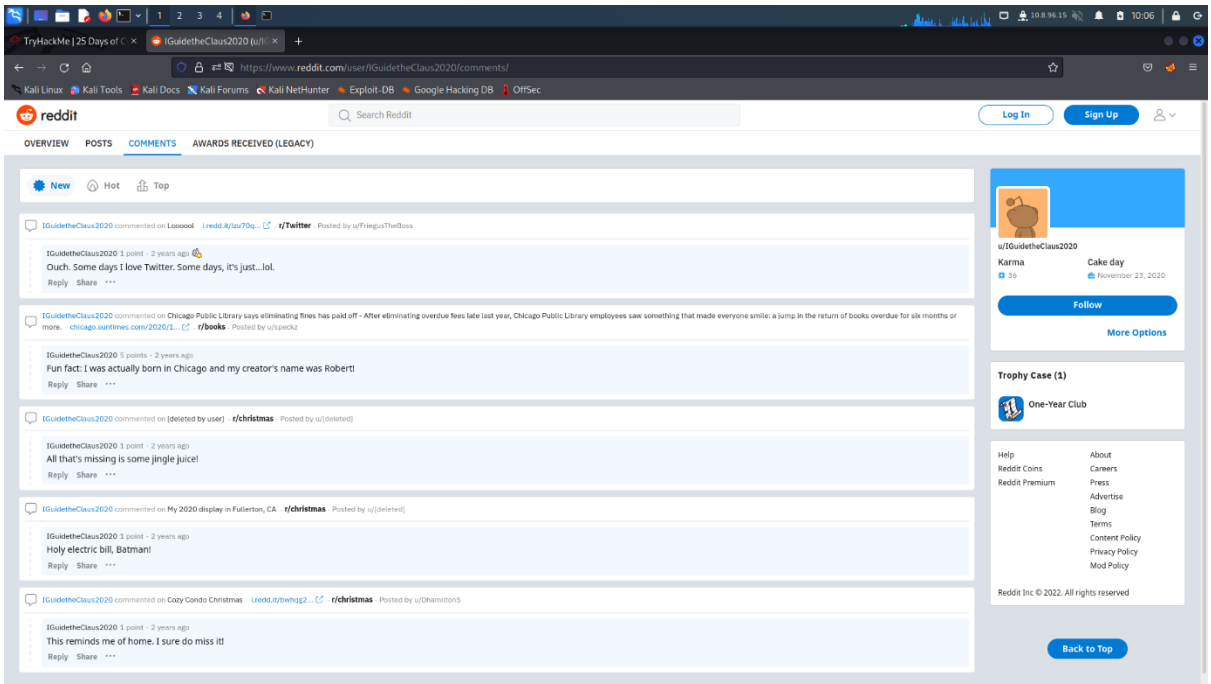
To find the URL that will take us directly to Rudolph's Reddit comment history, we first went to Reddit website.



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

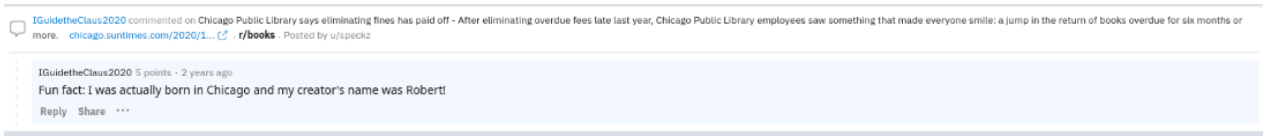


Once we found Rudolph's Reddit account, we navigate to the comments. By doing so, we obtained the URL that will directly lead us to Rudolph's Reddit comment history.



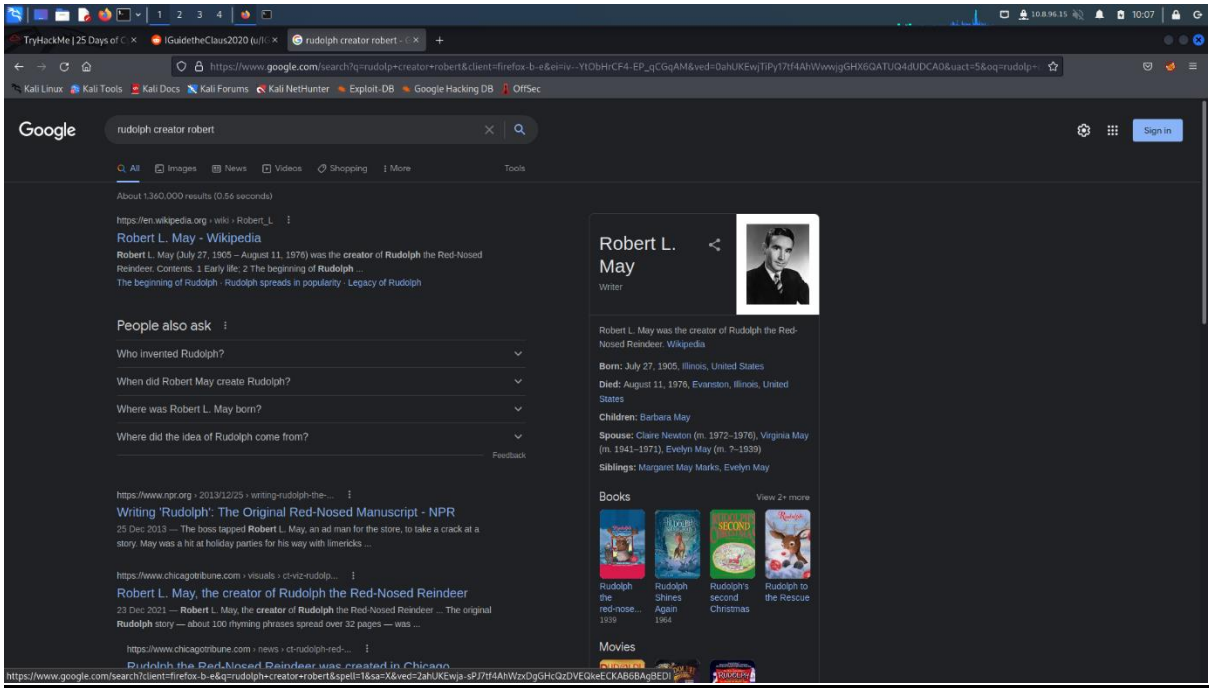
Question 2

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



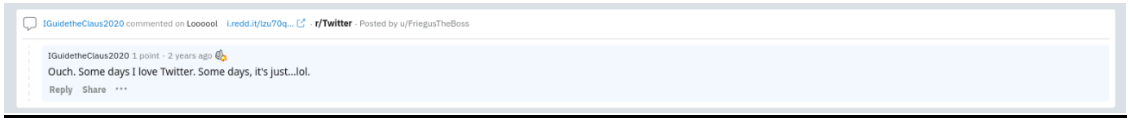
Question 3

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

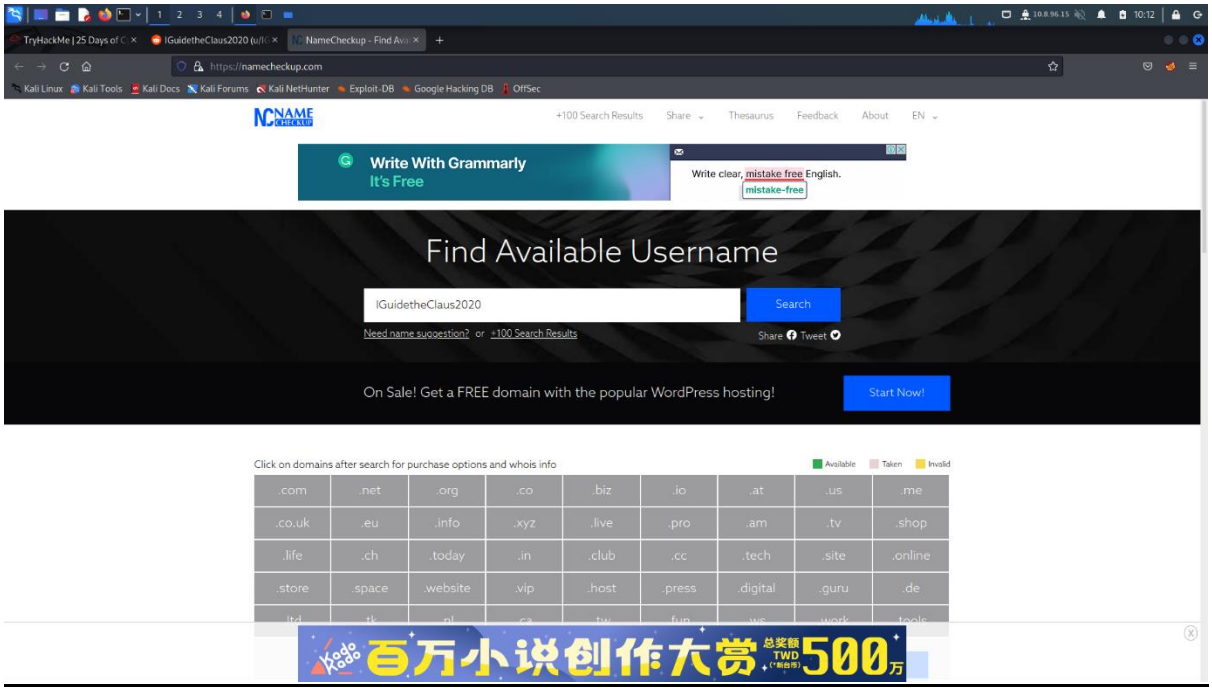


Question 4

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

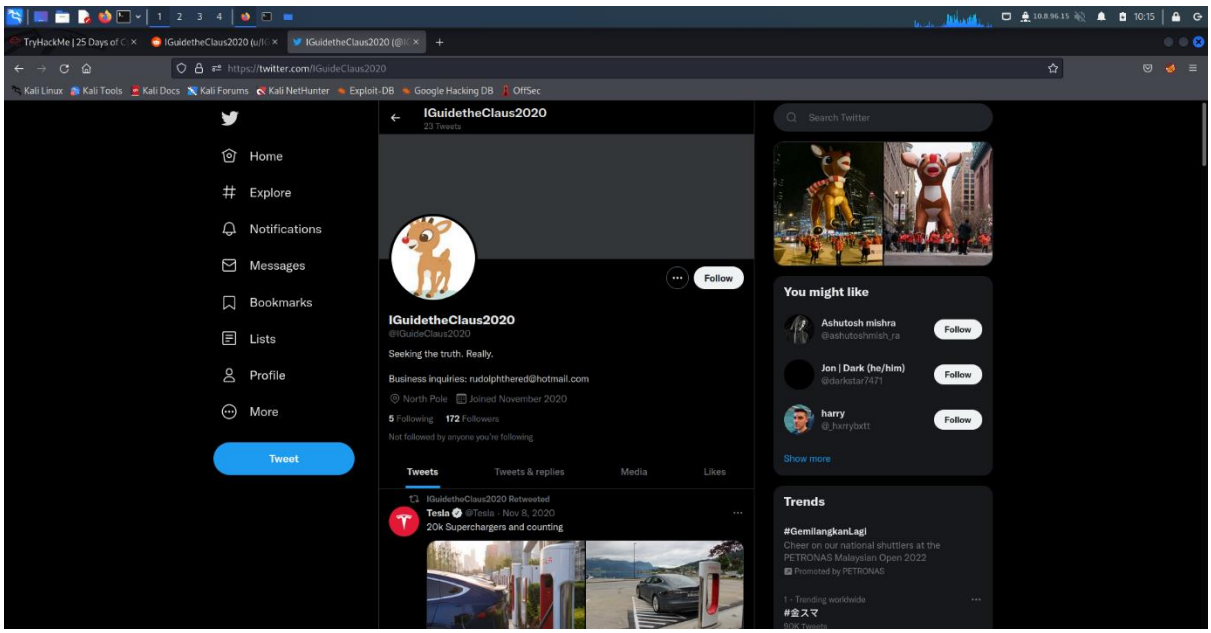


For confirmation, we also search for his username in name check-up website where it mentioned that the username is available in Twitter. Hence, Rudolph might have a Twitter account.



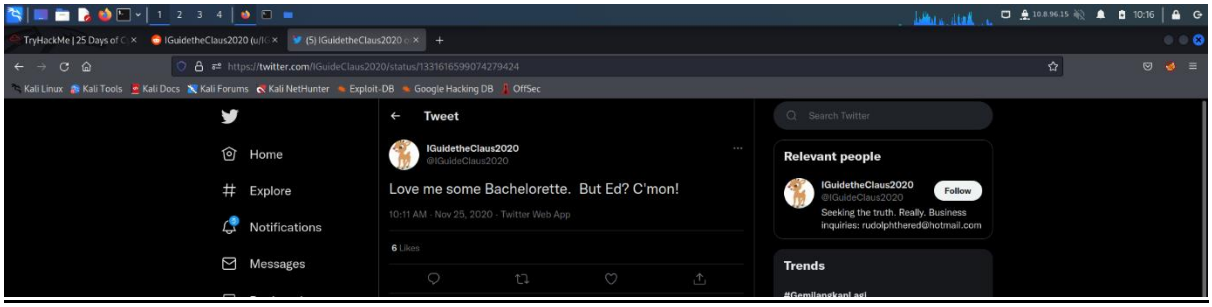
Question 5

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



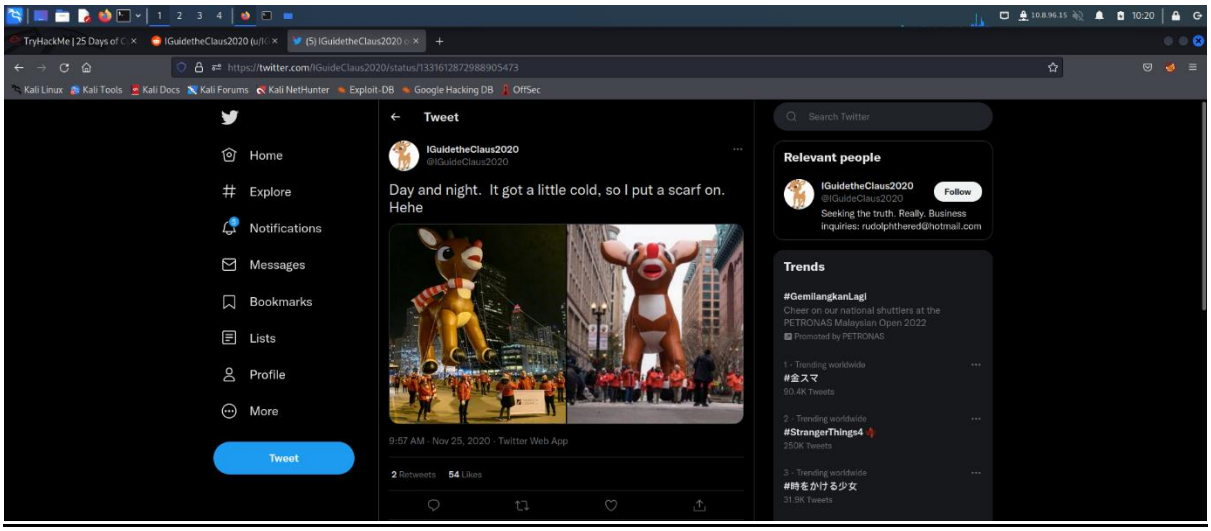
Question 6

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.

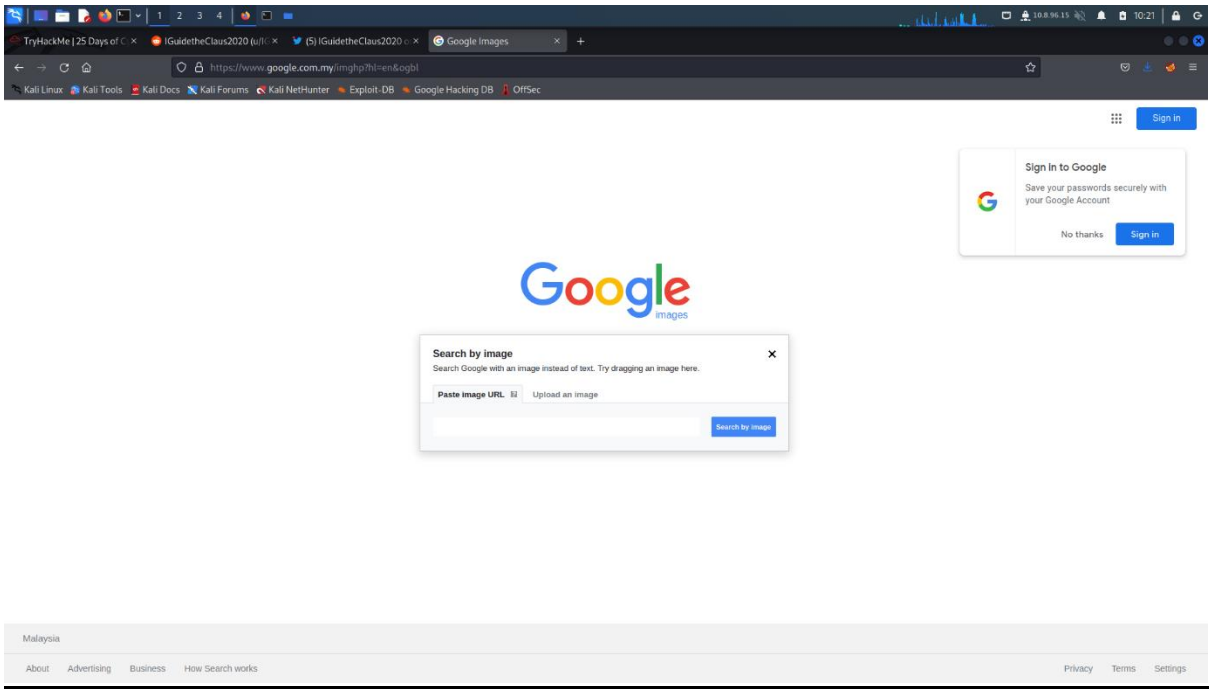


Question 7

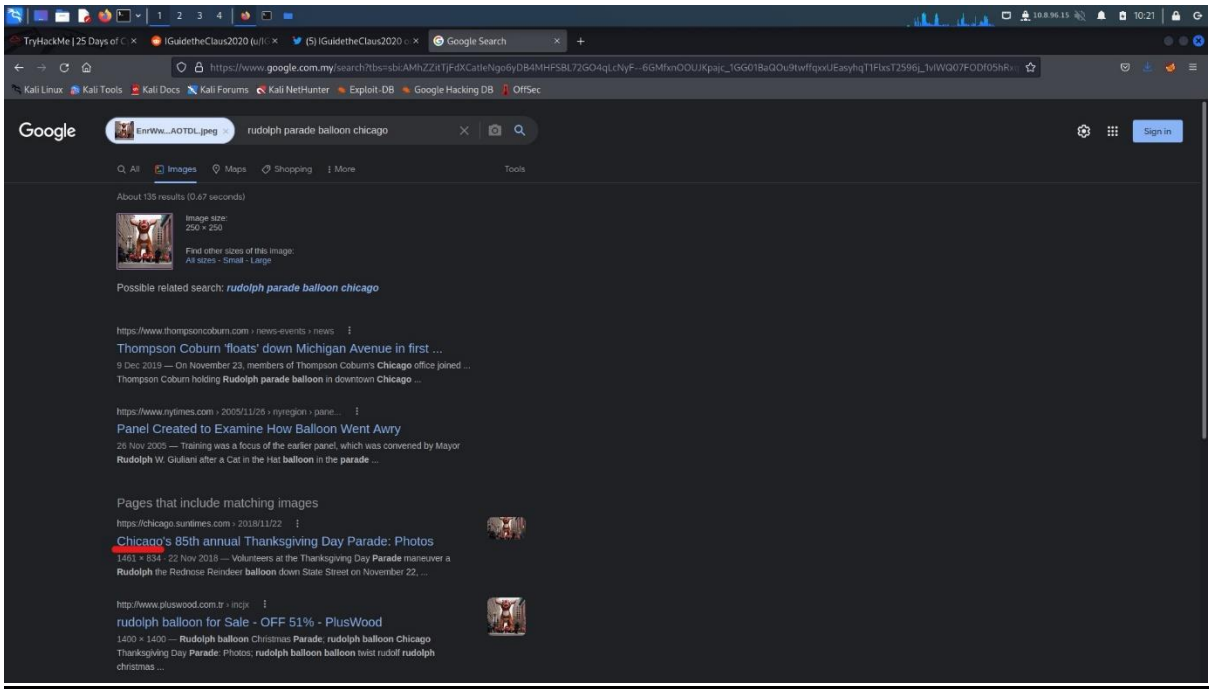
One of Rudolph's tweets on 25 November 2020 showed pictures of a parade. We decided to save the photos.



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

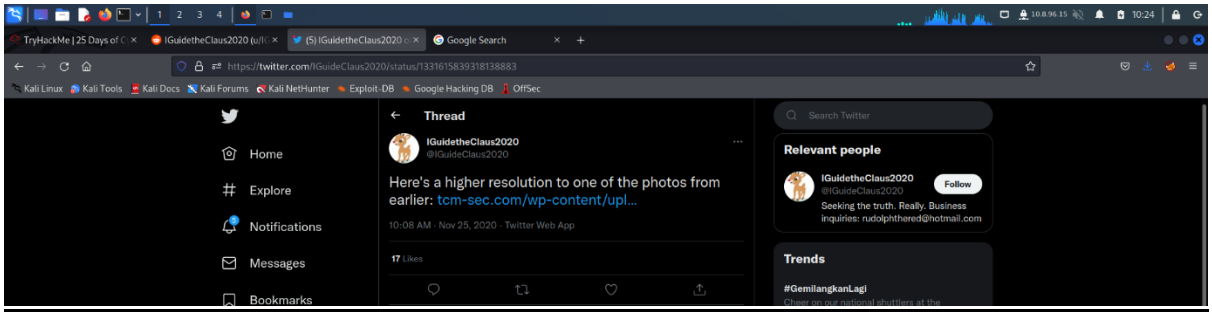


After searching by image of the parade, we found articles mentioning that the parade took place in Chicago.

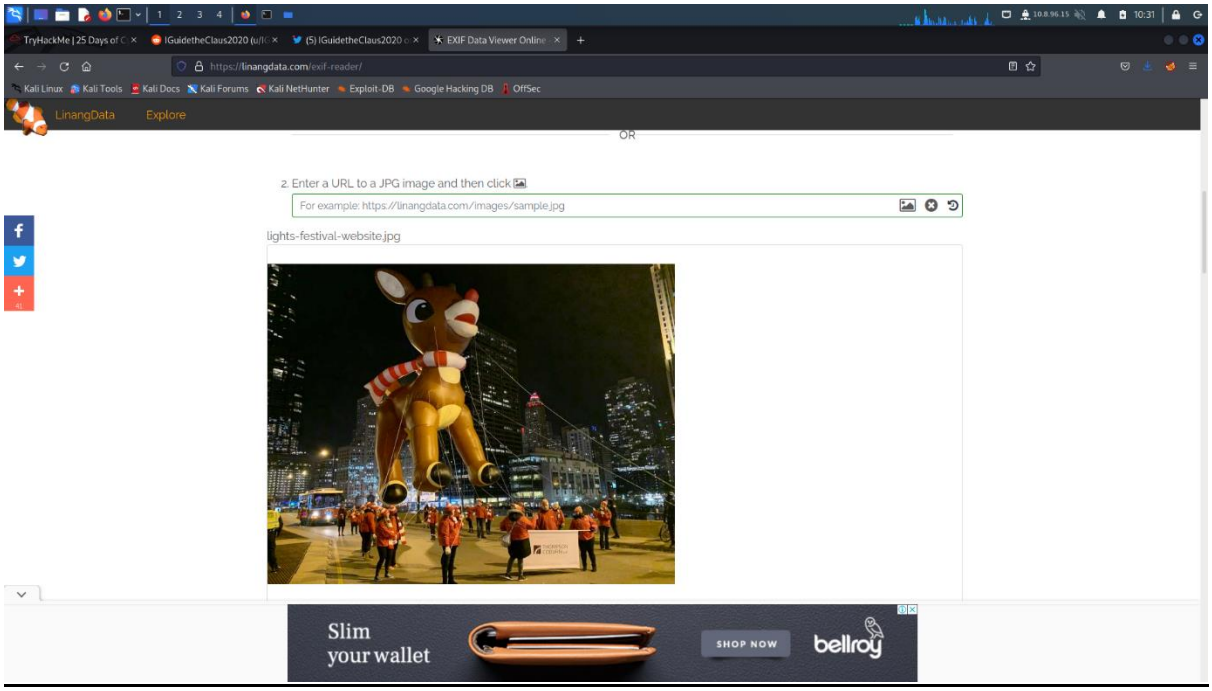


Question 8

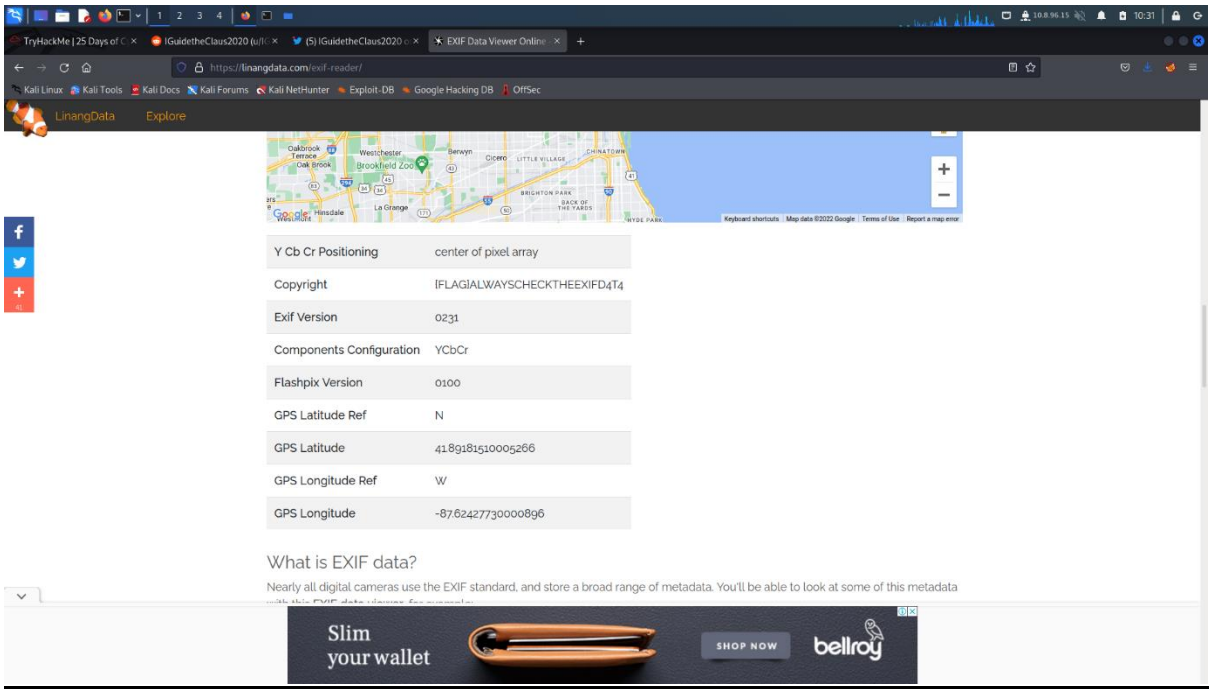
Another Rudolph's tweet on 25 November 2020 gave us a link to a higher resolution to one of the photos earlier. We saved the high-resolution photo.



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.

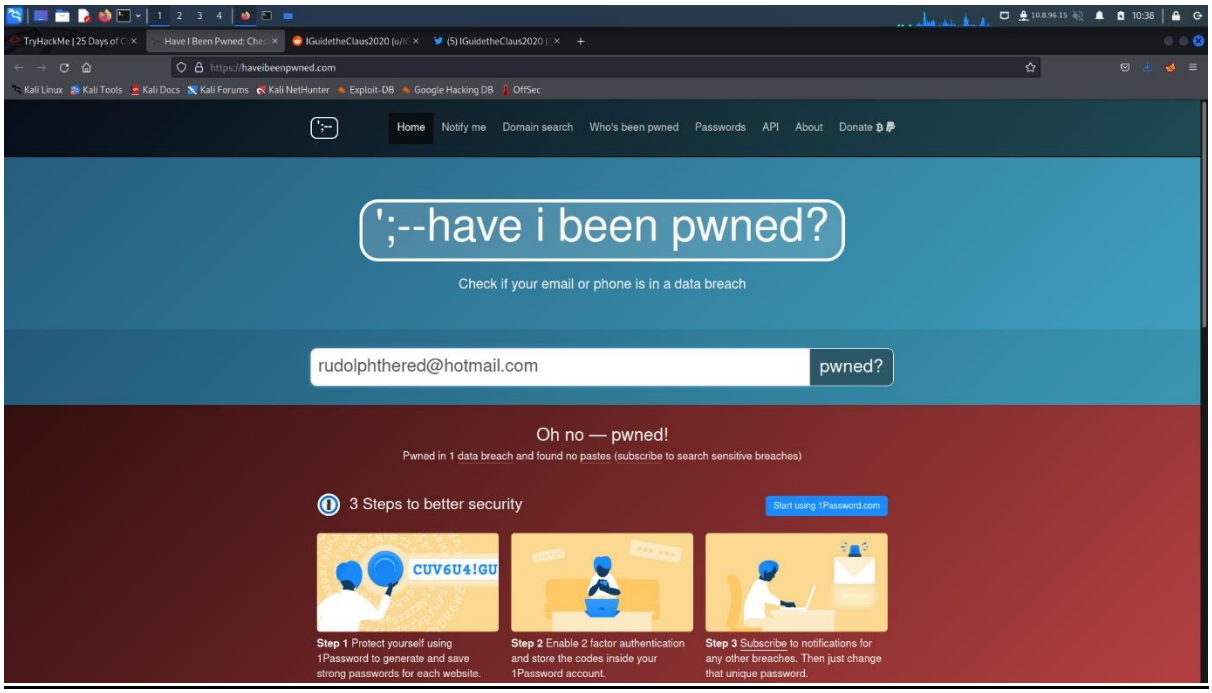


Question 9

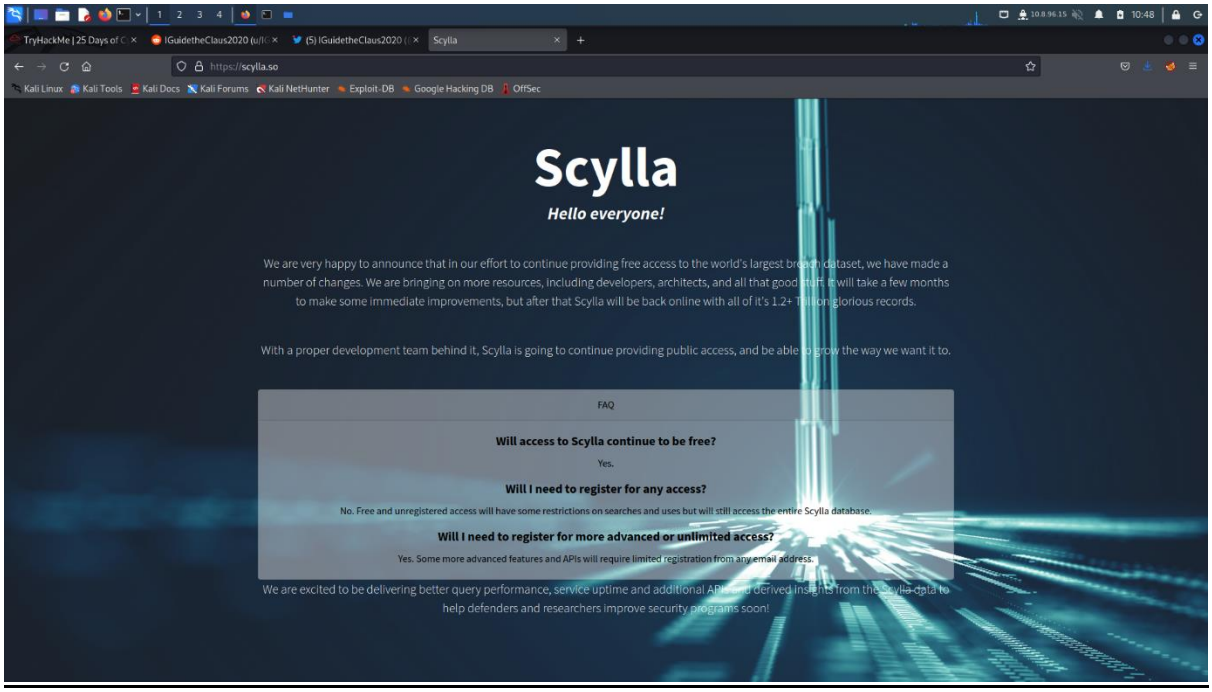
The website we use to scan the metadata has also showed us the flag which was under the copyright.

Question 10

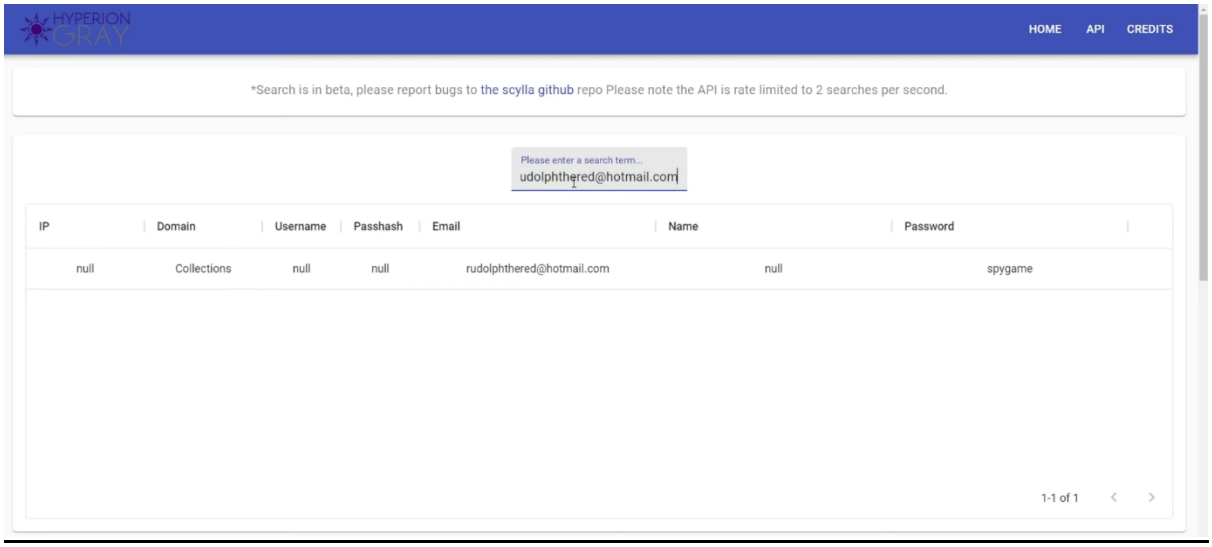
We went to haveibeenpwned.com website to scan whether Rudolph's email has been pawn or not and the result said that Rudolph has been pawned.



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

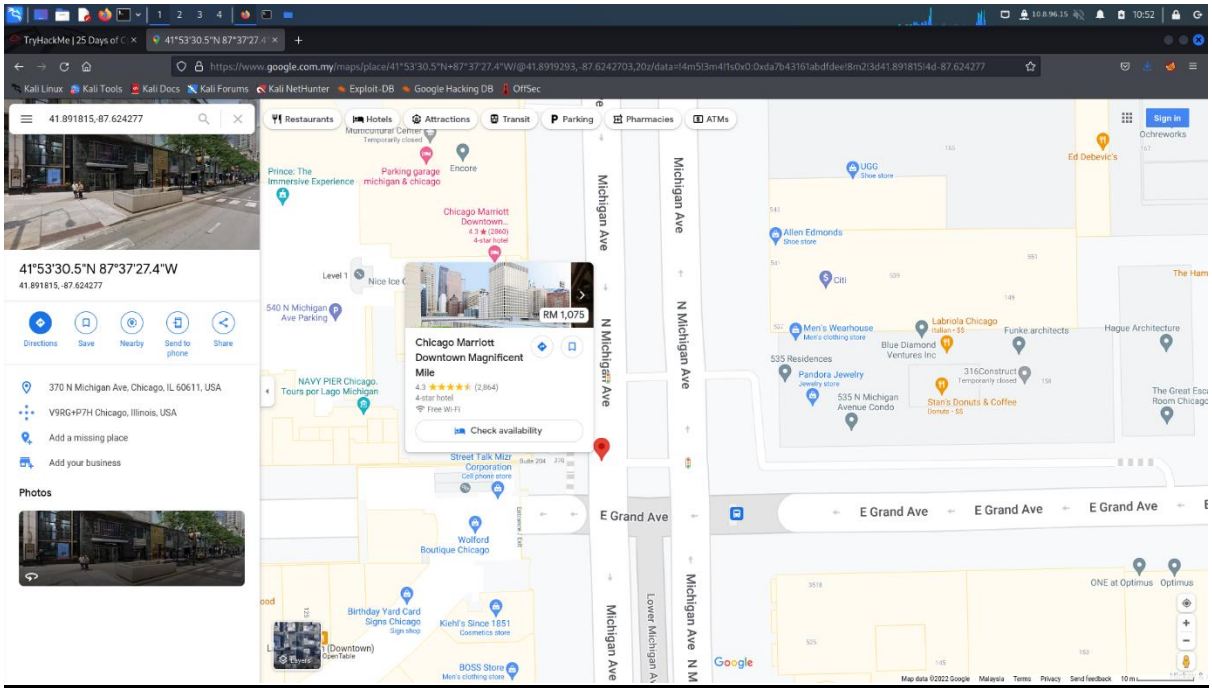


We searched for other alternatives, but we could not find any, so we resort to our last option which is obtaining the password from other people's walkthrough. Here, we finally retrieve the password 'spygame'.

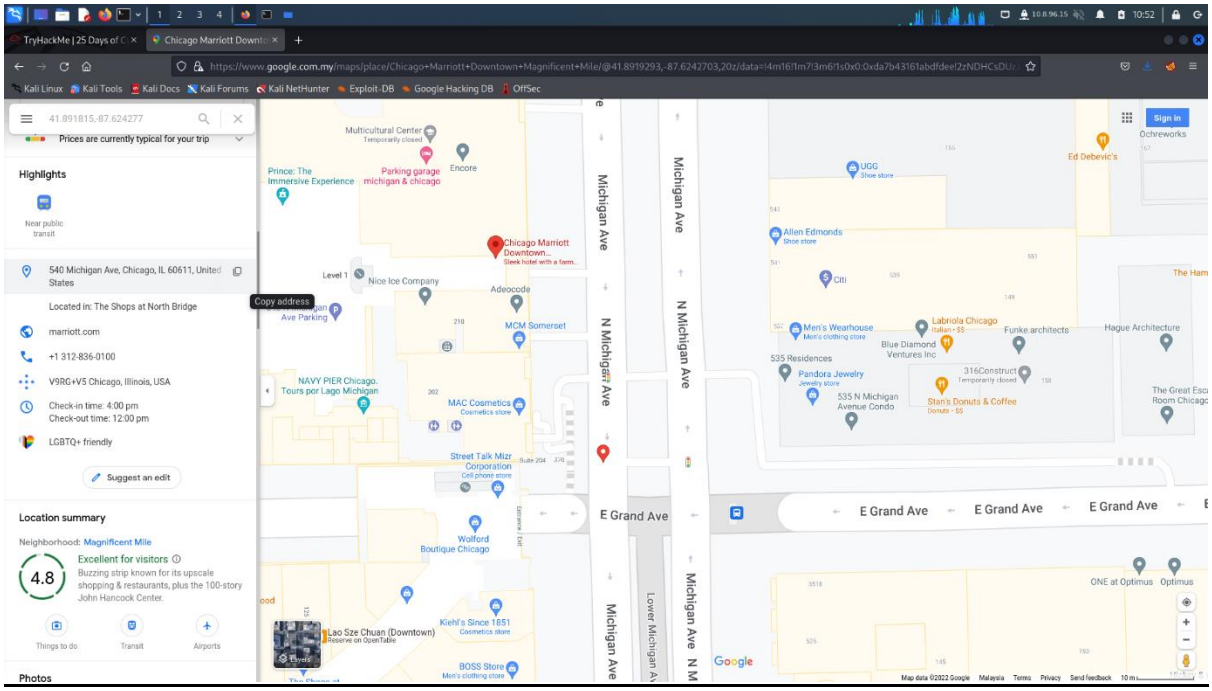


Question 11

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.