PSP0201 Week 4 Writeup

Group Name: ikun no 1

Members

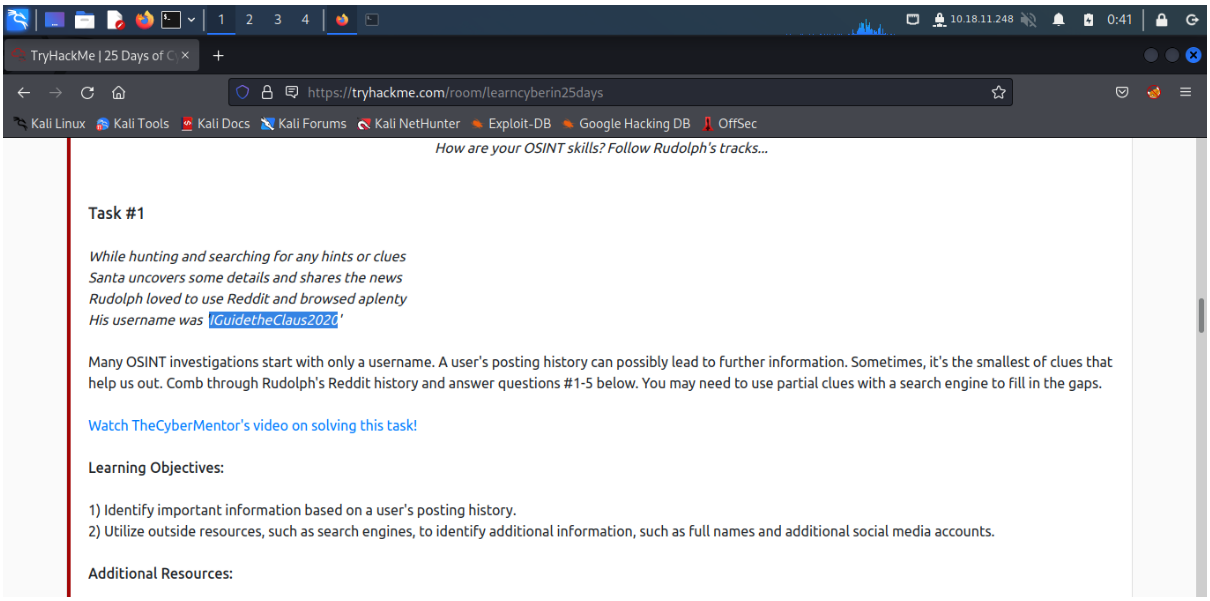
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

Day 14: OSINT Where's Rudolph?

Tool used: Kali-Linux, twitter, reddit

Solution/walkthrough:

Question 1



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'

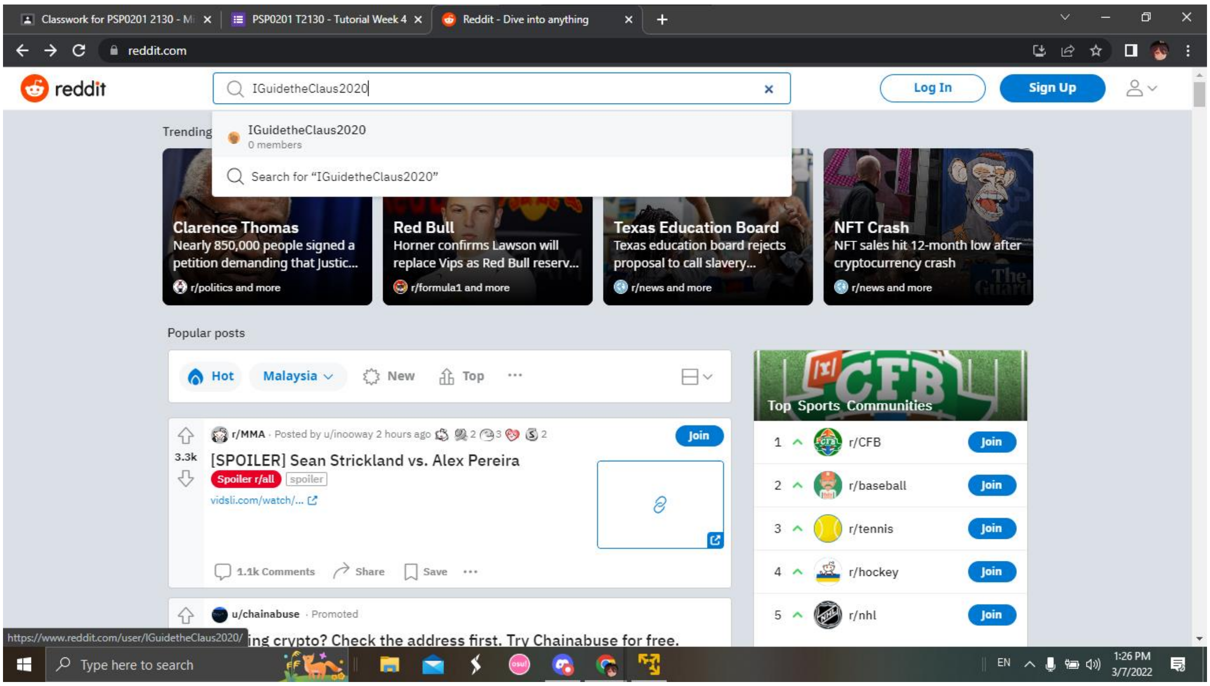
Many OSINT investigations start with only a username. A user's posting history can possibly lead to further information. Sometimes, it's the smallest of clues that help us out. Comb through Rudolph's Reddit history and answer questions #1-5 below. You may need to use partial clues with a search engine to fill in the gaps.

Watch TheCyberMentor's video on solving this task!

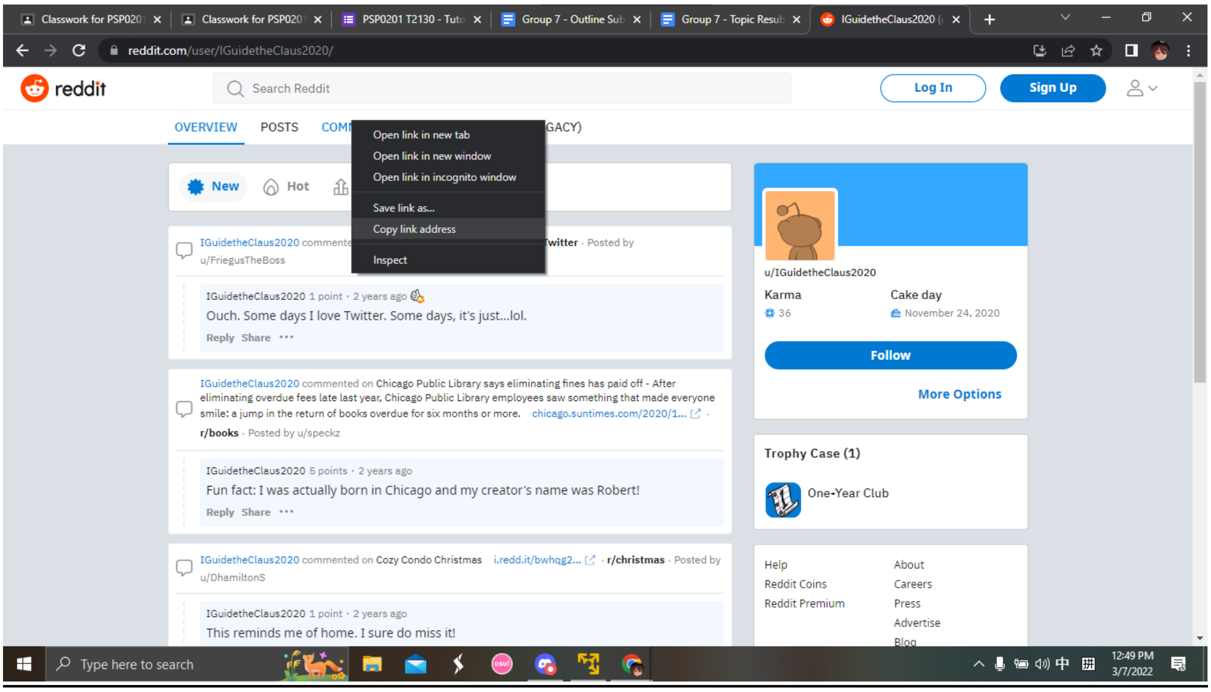
Learning Objectives:

1) Identify important information based on a user's posting history.
2) Utilize outside resources, such as search engines, to identify additional information, such as full names and additional social media accounts.

Additional Resources:


Classwork for PSP0201 2130 - M
PSP0201 T2130 - Tutorial Week 4
Reddit - Dive into anything
reddit.com
reddit
IGuidetheClaus2020
Log In
Sign Up
Trending
IGuidetheClaus2020
0 members
Search for "IGuidetheClaus2020"
Clarence Thomas
Nearly 850,000 people signed a petition demanding that Justic...
r/politics and more
Red Bull
Horner confirms Lawson will replace Vips as Red Bull reserv...
r/formula1 and more
Texas Education Board
Texas education board rejects proposal to call slavery...
r/news and more
NFT Crash
NFT sales hit 12-month low after cryptocurrency crash
r/news and more
Popular posts
Hot
Malaysia
New
Top
r/MMA · Posted by u/inooway 2 hours ago
3.3k
[SPOILER] Sean Strickland vs. Alex Pereira
Spoiler r/all
spoiler
vidsli.com/watch/...
Join
1.1k Comments
Share
Save
u/chainabuse · Promoted
ing crypto? Check the address first. Try Chainabuse for free.
Top Sports Communities
1 r/CFB Join
2 r/baseball Join
3 r/tennis Join
4 r/hockey Join
5 r/nhl Join
https://www.reddit.com/user/IGuidetheClaus2020/
Type here to search
EN
1:26 PM
3/7/2022

Copy the username and paste it in reddit.



IGuidetheClaus2020 commente... 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 ···

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/2020/1... · r/books · Posted by u/speckz

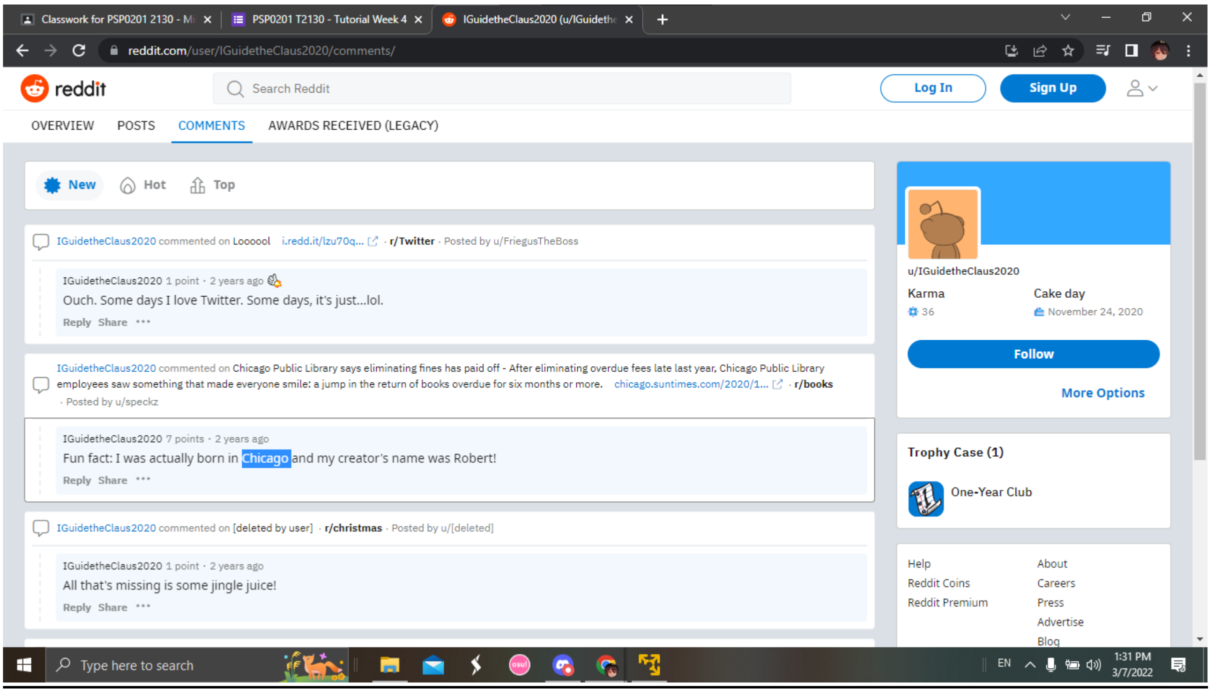
IGuidetheClaus2020 5 points · 2 years ago
Fun fact: I was actually born in Chicago and my creator's name was Robert!
Reply Share ···

IGuidetheClaus2020 commented on Cozy Condo Christmas i.redd.it/bwhqg2... · r/christmas · Posted by u/DhamiltonS

IGuidetheClaus2020 1 point · 2 years ago
This reminds me of home. I sure do miss it!

Then right click the comment and copy the link address.

Question 2



IGuidetheClaus2020 commented on Loooool i.redd.it/lzu70q... · 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 ···

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/2020/1... · r/books · Posted by u/speckz

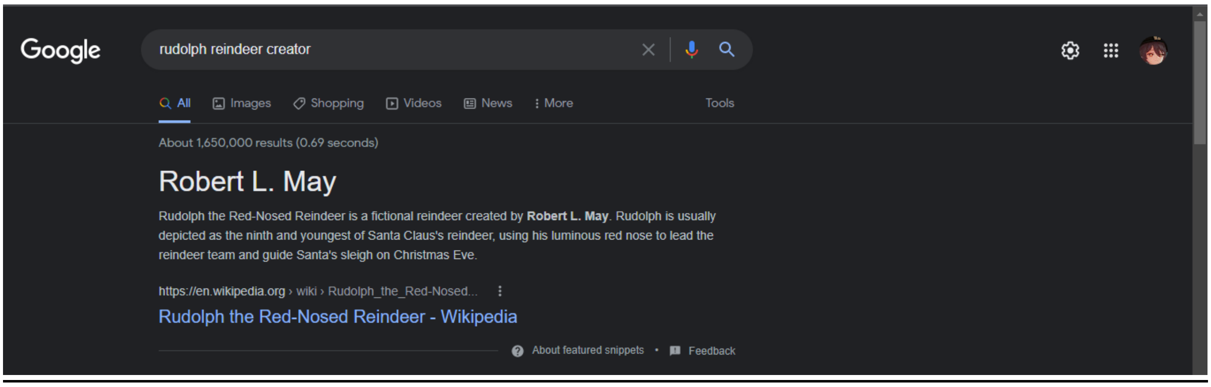
IGuidetheClaus2020 7 points · 2 years ago
Fun fact: I was actually born in Chicago and my creator's name was Robert!
Reply Share ···

IGuidetheClaus2020 commented on [deleted by user] · r/christmas · Posted by u/[deleted]

IGuidetheClaus2020 1 point · 2 years ago
All that's missing is some jingle juice!
Reply Share ···

Find the answer in reddit.

Question 3



About 1,650,000 results (0.69 seconds)

Robert L. May

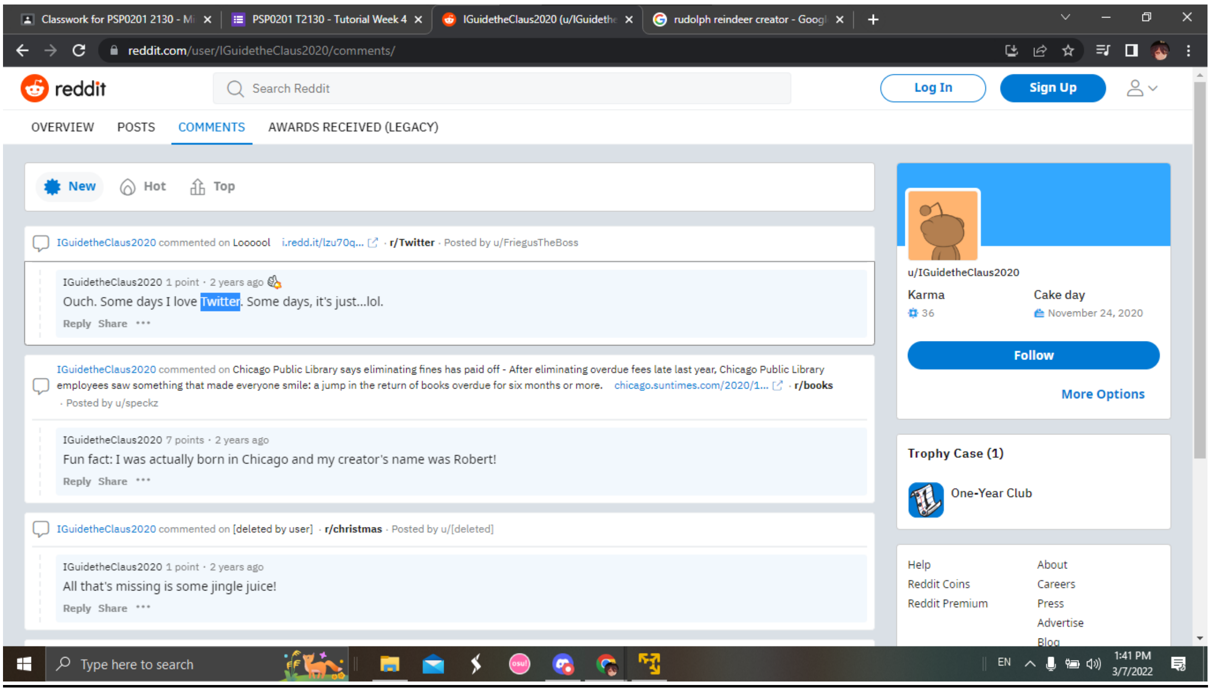
Rudolph the Red-Nosed Reindeer is a fictional reindeer created by **Robert L. May**. Rudolph is usually depicted as the ninth and youngest of Santa Claus's reindeer, using his luminous red nose to lead the reindeer team and guide Santa's sleigh on Christmas Eve.

https://en.wikipedia.org › wiki › Rudolph_the_Red-Nosed...

Rudolph the Red-Nosed Reindeer - Wikipedia

Find the hint in reddit and google search Rudolph reindeer creator. The answer shown.

Question 4



Classwork for PSP0201 2130 - M
PSP0201 T2130 - Tutorial Week 4
IGuidetheClaus2020 (u/IGuidethe
rudolph reindeer creator - Googl
reddit.com/user/IGuidetheClaus2020/comments/
reddit
Search Reddit
Log In
Sign Up
OVERVIEW
POSTS
COMMENTS
AWARDS RECEIVED (LEGACY)
New
Hot
Top

IGuidetheClaus2020 commented on Loooool i.redd.it/lzu70q... · 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 •••

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/2020/1... · r/books · Posted by u/speckz

IGuidetheClaus2020 7 points · 2 years ago

Fun fact: I was actually born in Chicago and my creator's name was Robert!

Reply Share •••

IGuidetheClaus2020 commented on [deleted by user] · r/christmas · Posted by u/[deleted]

IGuidetheClaus2020 1 point · 2 years ago

All that's missing is some jingle juice!

Reply Share •••

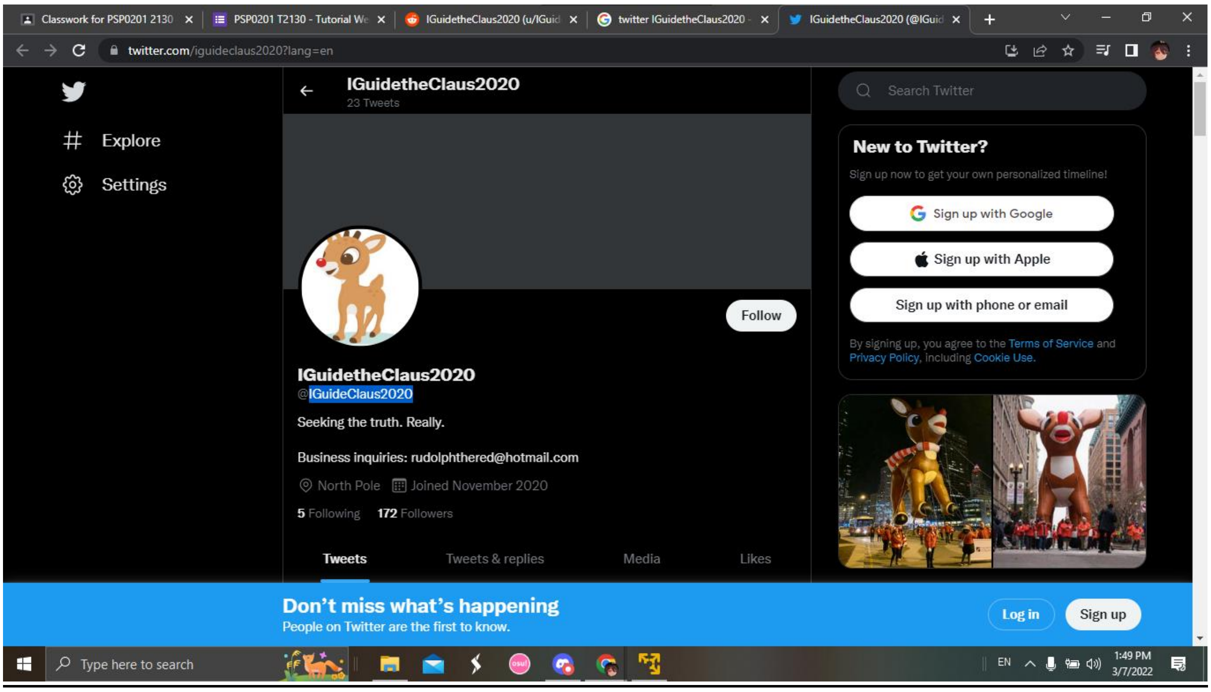
u/IGuidetheClaus2020

Karma: 36

Cake day: November 24, 2020

Find the answer in reddit.

Question 5


Classwork for PSP0201 2130
PSP0201 T2130 - Tutorial We
IGuidetheClaus2020 (u/IGuid
twitter IGuidetheClaus2020 -
IGuidetheClaus2020 (@IGuid
twitter.com/iguideclaus2020?lang=en
Explore
Settings
Search Twitter
Follow
Tweets
Tweets & replies
Media
Likes
Sign up with Google
Sign up with Apple
Sign up with phone or email
Log in
Sign up
Type here to search
EN
1:49 PM
3/7/2022

IGuidetheClaus2020
23 Tweets

IGuidetheClaus2020
@IGuideClaus2020

Seeking the truth. Really.

Business inquiries: rudolphthered@hotmail.com

North Pole Joined November 2020

5 Following 172 Followers

New to Twitter?

Sign up now to get your own personalized timeline!

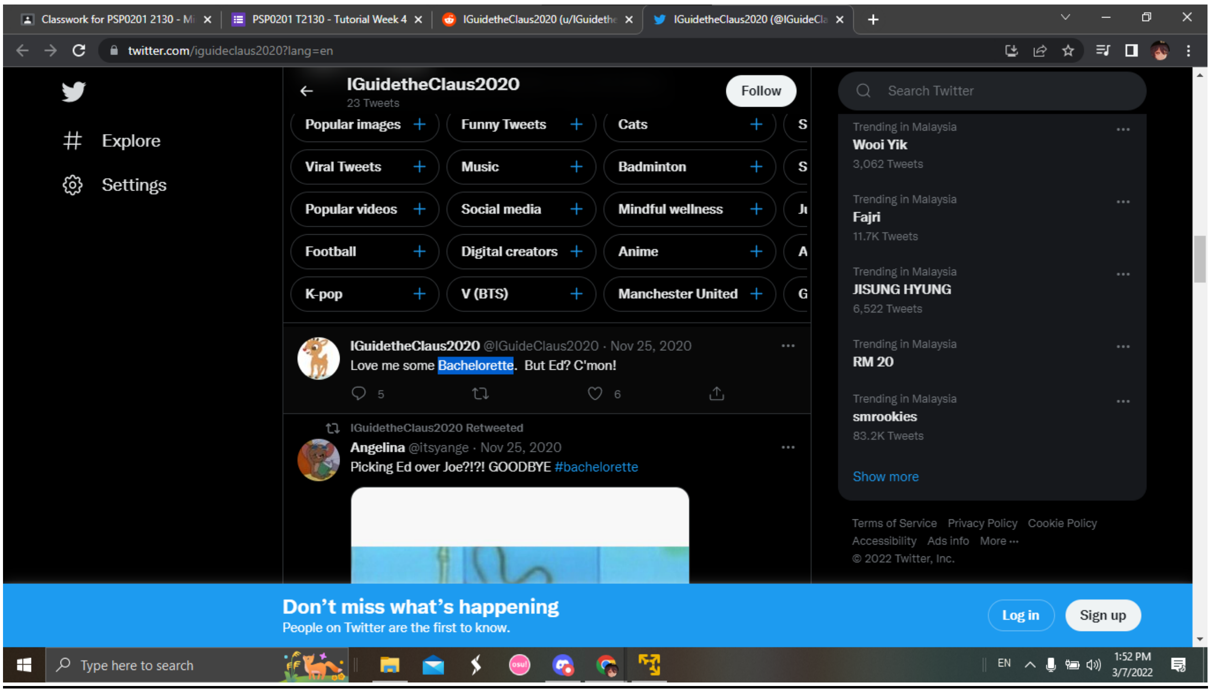
By signing up, you agree to the Terms of Service and Privacy Policy, including Cookie Use.

Don't miss what's happening

People on Twitter are the first to know.

Google search IGuidetheClaus2020 in twitter and the answer shown.

Question 6



IGuidetheClaus2020
23 Tweets

IGuidetheClaus2020 @IGuideClaus2020 · Nov 25, 2020
Love me some Bachelorette. But Ed? C'mon!
5 6

IGuidetheClaus2020 Retweeted
Angelina @itsyange · Nov 25, 2020
Picking Ed over Joe?!?! GOODBYE #bachelorette

Trending in Malaysia
Wooi Yik
3,062 Tweets

Trending in Malaysia
Fajri
11.7K Tweets

Trending in Malaysia
JISUNG HYUNG
6,522 Tweets

Trending in Malaysia
RM 20

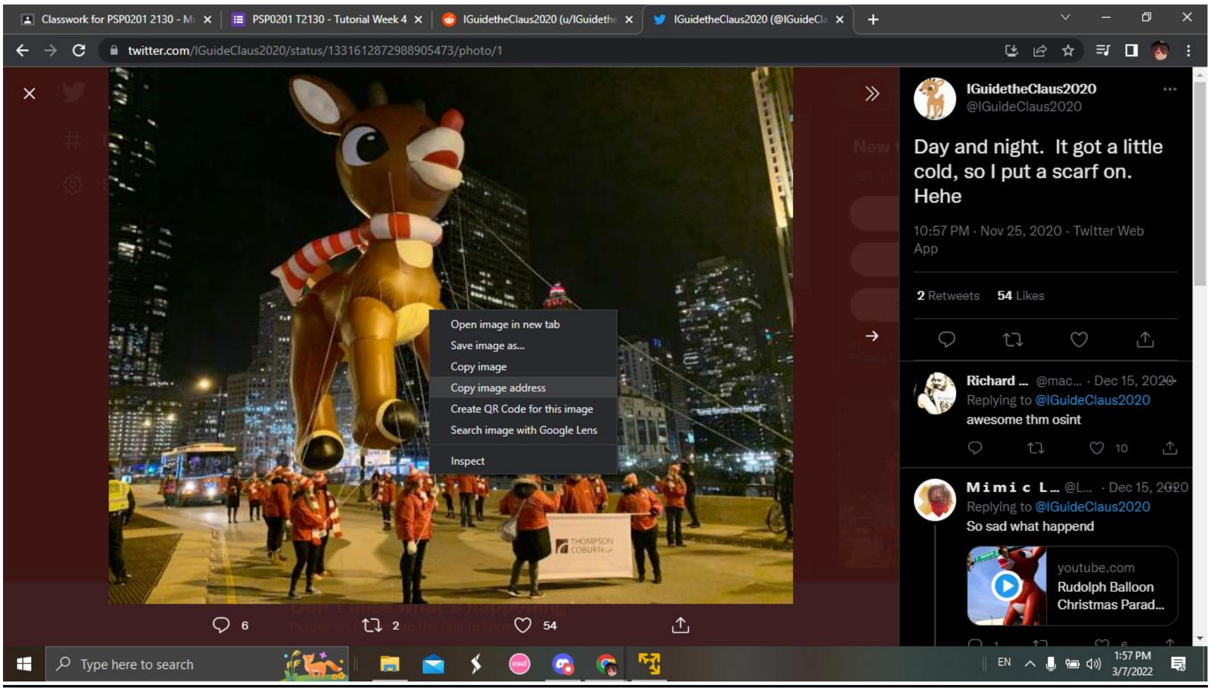
Trending in Malaysia
smrookies
83.2K Tweets

Don't miss what's happening

People on Twitter are the first to know.

Find the answer in Twitter.

Question 7


Classwork for PSP0201 2130 - M
PSP0201 T2130 - Tutorial Week 4
IGuidetheClaus2020 (u/IGuidethe
IGuidetheClaus2020 (@IGuideCla
twitter.com/IGuideClaus2020/status/1331612872988905473/photo/1
Open image in new tab
Save image as...
Copy image
Copy image address
Create QR Code for this image
Search image with Google Lens
Inspect
6
2
54
Type here to search
1:57 PM
3/7/2022

IGuidetheClaus2020
@IGuideClaus2020

Day and night. It got a little cold, so I put a scarf on. Hehe

10:57 PM · Nov 25, 2020 · Twitter Web App

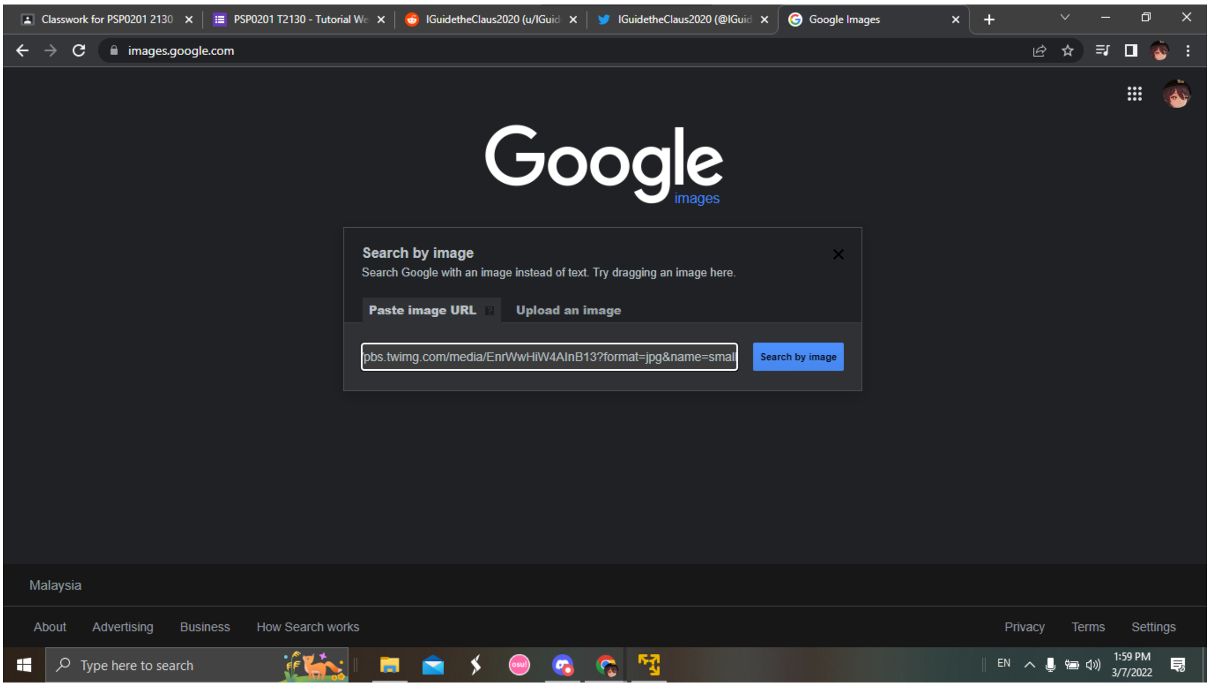
2 Retweets 54 Likes

Richard ... @mac... · Dec 15, 2020
Replying to @IGuideClaus2020
awesome thm osint

Mimic L... @L... · Dec 15, 2020
Replying to @IGuideClaus2020
So sad what happend

youtube.com
Rudolph Balloon Christmas Parad...

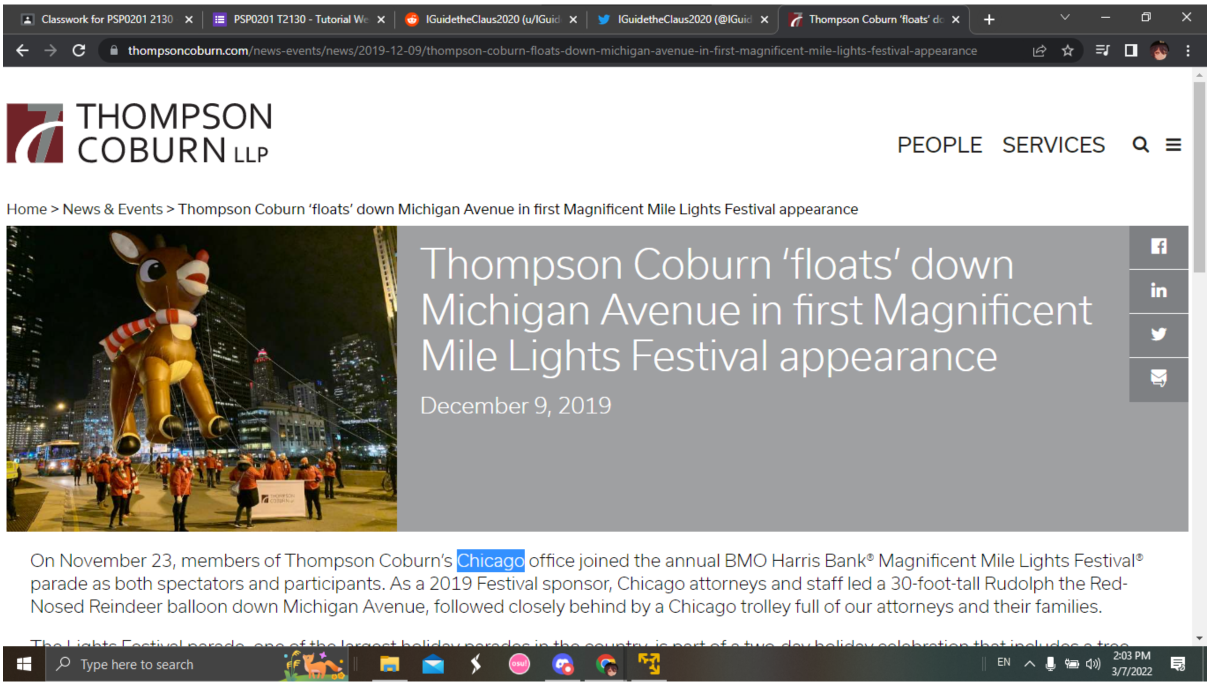
Copy the image address of the post.



Search by image
Search Google with an image instead of text. Try dragging an image here.

pbs.twimg.com/media/EnrWwHiW4AInB13?format=jpg&name=small

Use google image reverse and paste the URL in it.


Classwork for PSP0201 2130
PSP0201 T2130 - Tutorial We
IGuidetheClaus2020 (u/IGuid
IGuidetheClaus2020 (@IGuid
Thompson Coburn 'floats' d
thompsoncoburn.com/news-events/news/2019-12-09/thompson-coburn-floats-down-michigan-avenue-in-first-magnificent-mile-lights-festival-appearance
THOMPSON COBURN LLP
PEOPLE
SERVICES
Type here to search
EN
2:03 PM
3/7/2022

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

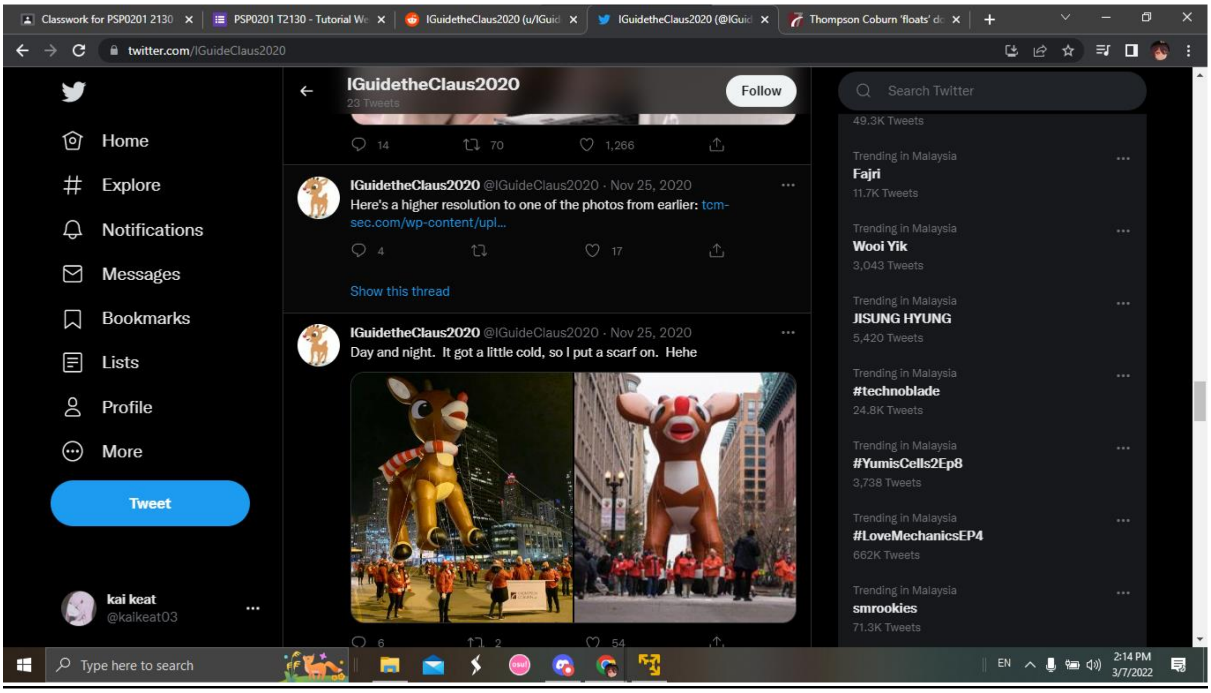
December 9, 2019

On November 23, members of Thompson Coburn's Chicago office joined the annual BMO Harris Bank® Magnificent Mile Lights Festival® parade as both spectators and participants. As a 2019 Festival sponsor, Chicago attorneys and staff led a 30-foot-tall Rudolph the Red-Nosed Reindeer balloon down Michigan Avenue, followed closely behind by a Chicago trolley full of our attorneys and their families.

The Lights Festival parade, one of the largest holiday parades in the country, is part of a two-day holiday celebration that includes a tree

Press in the correct link and the answer shown.

Question 8



14 70 1,266

IGuidetheClaus2020 @IGuideClaus2020 · Nov 25, 2020
Here's a higher resolution to one of the photos from earlier: tcm-sec.com/wp-content/upl...

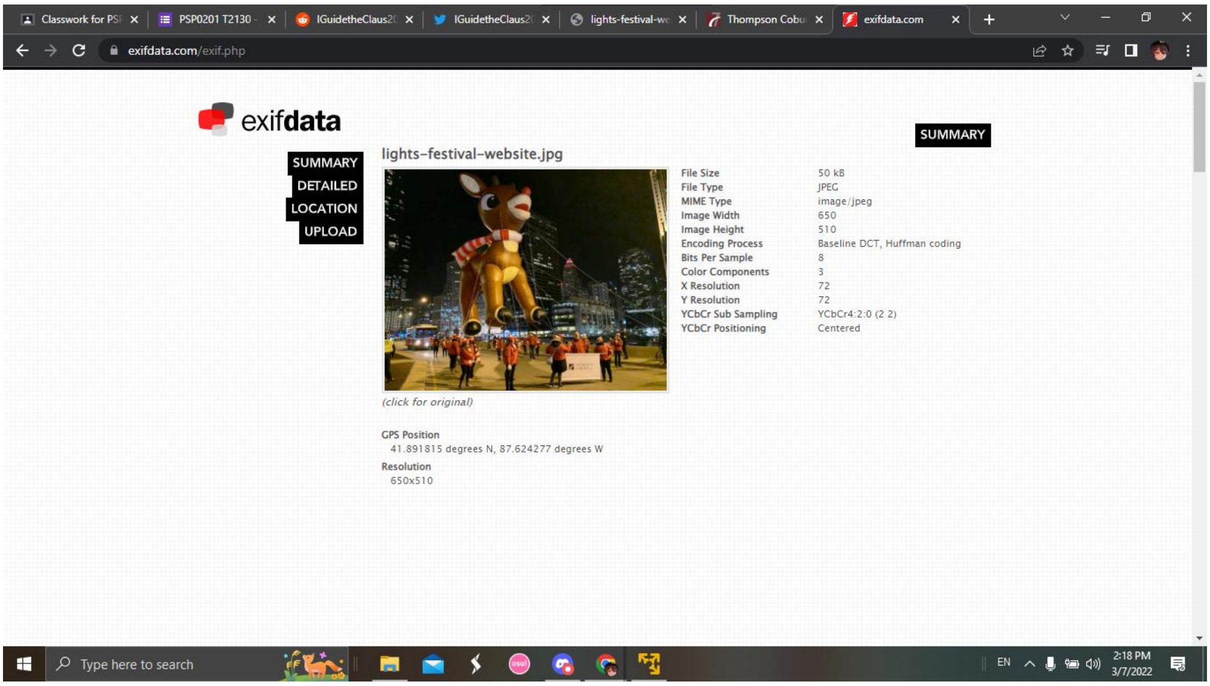
4 17

Show this thread

IGuidetheClaus2020 @IGuideClaus2020 · Nov 25, 2020
Day and night. It got a little cold, so I put a scarf on. Hehe

6 2 54

Click on the link to view and download the high resolution photo.



SUMMARY

lights-festival-website.jpg

File Size	50 kB
File Type	JPEG
MIME Type	image/jpeg
Image Width	650
Image Height	510
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
X Resolution	72
Y Resolution	72
YCbCr Sub Sampling	YCbCr4:2:0 (2 2)
YCbCr Positioning	Centered

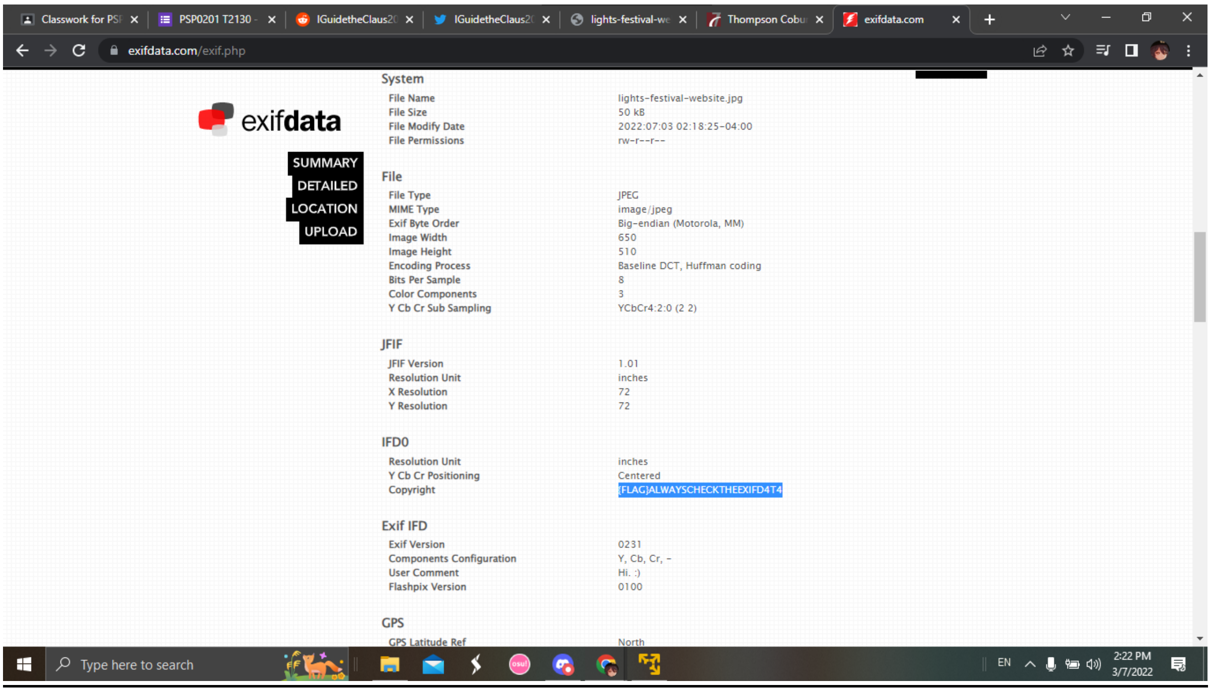
(click for original)

GPS Position
41.891815 degrees N, 87.624277 degrees W

Resolution
650x510

After that, paste the image in the exif data website. The specific location shown.

Question 9



System

File Name	lights-festival-website.jpg
File Size	50 kB
File Modify Date	2022:07:03 02:18:25-04:00
File Permissions	rw-r--r--

File

File Type	JPEG
MIME Type	image/jpeg
Exif Byte Order	Big-endian (Motorola, MM)
Image Width	650
Image Height	510
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)

JFIF

JFIF Version	1.01
Resolution Unit	inches
X Resolution	72
Y Resolution	72

IFD0

Resolution Unit	inches
Y Cb Cr Positioning	Centered
Copyright	{FLAG}ALWAYSCHECKTHEEXIFD4T4

Exif IFD

Exif Version	0231
Components Configuration	Y, Cb, Cr, -
User Comment	Hi. :)
Flashpix Version	0100

GPS

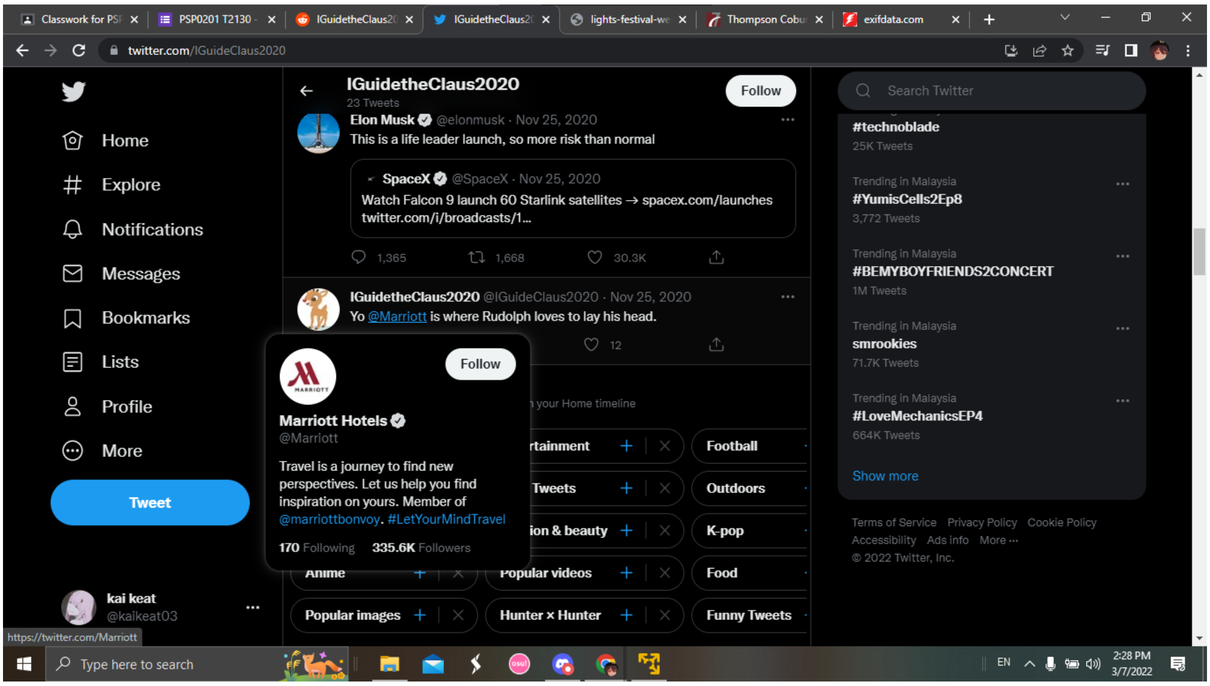
GPS Latitude Ref	North

Scroll down and the flag shown.

Question 10

The http://scylla.sh/ website is down.

Question 11



IGuidetheClaus2020
23 Tweets

Elon Musk @elonmusk · Nov 25, 2020
This is a life leader launch, so more risk than normal

SpaceX @SpaceX · Nov 25, 2020
Watch Falcon 9 launch 60 Starlink satellites → spacex.com/launches twitter.com/i/broadcasts/1...

1,365 1,668 30.3K

IGuidetheClaus2020 @IGuideClaus2020 · Nov 25, 2020
Yo @Marriott is where Rudolph loves to lay his head.

12

Marriott Hotels
@Marriott
Travel is a journey to find new perspectives. Let us help you find inspiration on yours. Member of @marriottbonvoy. #LetYourMindTravel
170 Following 335.6K Followers

your Home timeline

	rtainment	Football
	Tweets	Outdoors
	ion & beauty	K-pop
Anime	Popular videos	Food
Popular images	Hunter × Hunter	Funny Tweets

#technoblade
25K Tweets

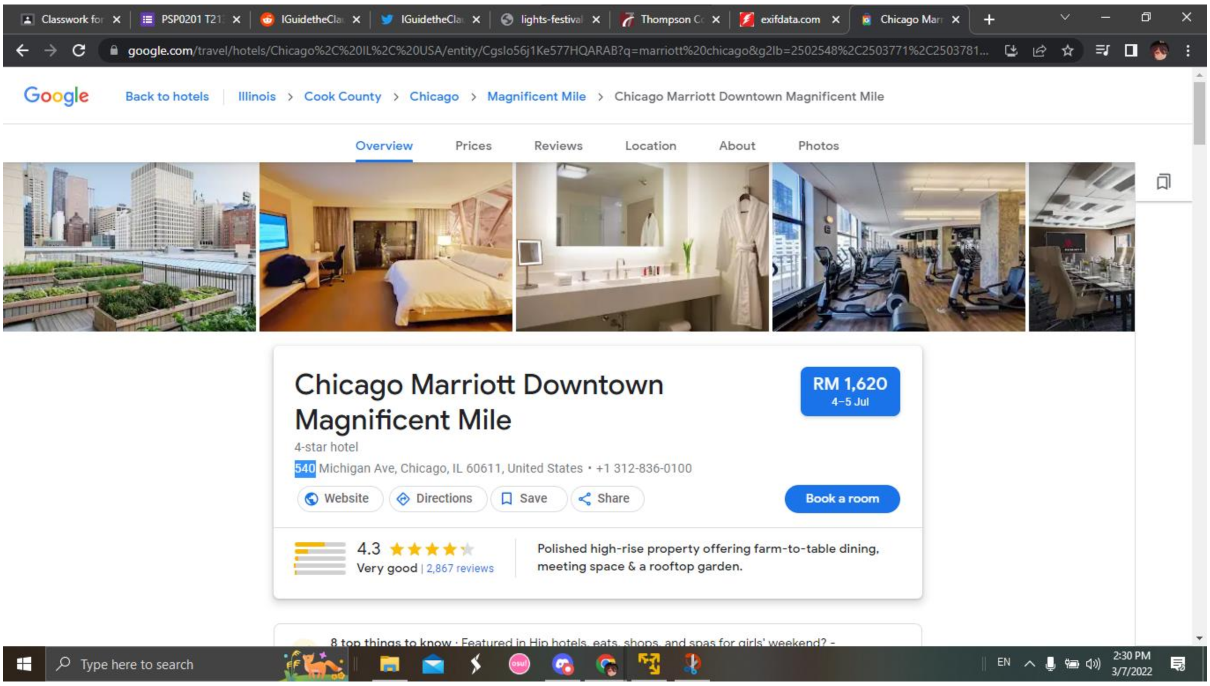
Trending in Malaysia
#YumisCells2Ep8
3,772 Tweets

Trending in Malaysia
#BEMYBOYFRIENDS2CONCERT
1M Tweets

Trending in Malaysia
smrookies
71.7K Tweets

Trending in Malaysia
#LoveMechanicsEP4
664K Tweets

Look for the clue in twitter to find which hotel and the location. The answer is Marriott Hotels in Chicago.


Classwork for
PSP0201 T21
IGuidetheCla
IGuidetheCla
lights-festival
Thompson C
exifdata.com
Chicago Marr
google.com/travel/hotels/Chicago%2C%20IL%2C%20USA/entity/CgsIo56j1Ke577HQARAB?q=marriott%20chicago&g2lb=2502548%2C2503771%2C2503781...
Google
Back to hotels
Illinois › Cook County › Chicago › Magnificent Mile › Chicago Marriott Downtown Magnificent Mile
Overview
Prices
Reviews
Location
About
Photos
Website
Directions
Save
Share
Book a room
Type here to search
EN
2:30 PM
3/7/2022

Chicago Marriott Downtown Magnificent Mile
4-star hotel
540 Michigan Ave, Chicago, IL 60611, United States • +1 312-836-0100

RM 1,620
4–5 Jul

4.3 ★★★★
Very good | 2,867 reviews

Polished high-rise property offering farm-to-table dining, meeting space & a rooftop garden.

8 top things to know · Featured in Hip hotels, eats, shops, and spas for girls' weekend? -

Then, google search the place and the street number is 540.