Open-Source Intelligence
HockeyTea1360

SEARCH LIGHT-IMINT
A TRY HACK ME WRITE UP

INTRODUCTION

Welcome to searchlight- IMINT room! This section of the tasks gives you a brief overview of what to expect and which tools you will most likely encounter and use to solve the various tasks.

The objective of this room is to enhance the user's analytical mindset and extract key data points from images & videos by visually exploring the target. Using different tools such as google, google dorks, maps, image reversing tools such as Yandex and intro to ffmepg.

The tasks in this room consist of 8 tasks which start easy and then progress getting harder each time you move on to the next download the images in each task to answer the questions.

As noted in the introduction to the room make sure you pay attention to the flag format

The flag format is : sl{flag) once reading this we notice a little further down the page that is asks us to put ready so the answer is

#1FLAG: sl{ready}

There are 5 elements of IMINT that everyone one should consider when looking at an image, according to Geoint expert Benjamin strick there are:

- Context
- Foreground
- Background
- Map markings
- Trial and error

Task 2 - Your first challenge

The first thing we do as humans when we are presented with an image is we use our eyes. So, when we are presented with this challenge, and we download the image (see below) Question we are posed with is: What is the name of the street the image was taken?

Well, this is simple, just by looking we can see the answer

#2FLAG: sl{carnaby street}

Task 3 - Just Google it

This is our second challenge where we are introduced to something called Google Dorking the art of using google search queries to have google return specific types of data that we have requested.

Once we have downloaded the image (see below) the first two questions that we are posed with is:

Which city is the tube station located in?

Which tube station do these stairs lead to?

Well, we know from the image that we can see underground and make out the name of the station. By looking at the picture we can make out the name Piccadilly Circus which if we place into google maps, we can see is located in London. Which answers our first two questions.

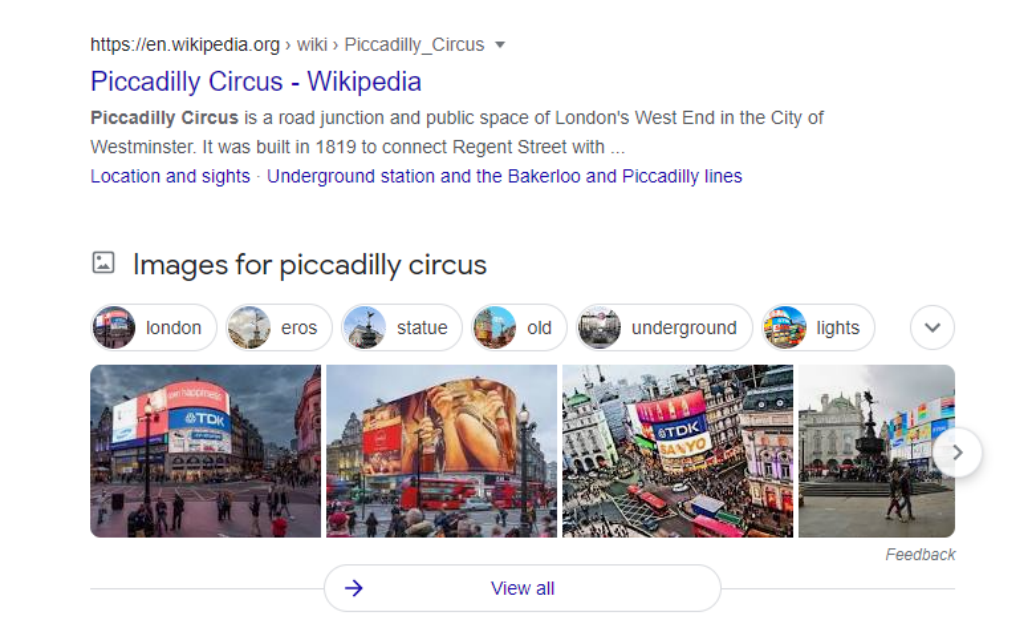
#3FLAG: sl{london} **#4FLAG: sl{piccadilly circus}**

Now the next two questions ask us the following:

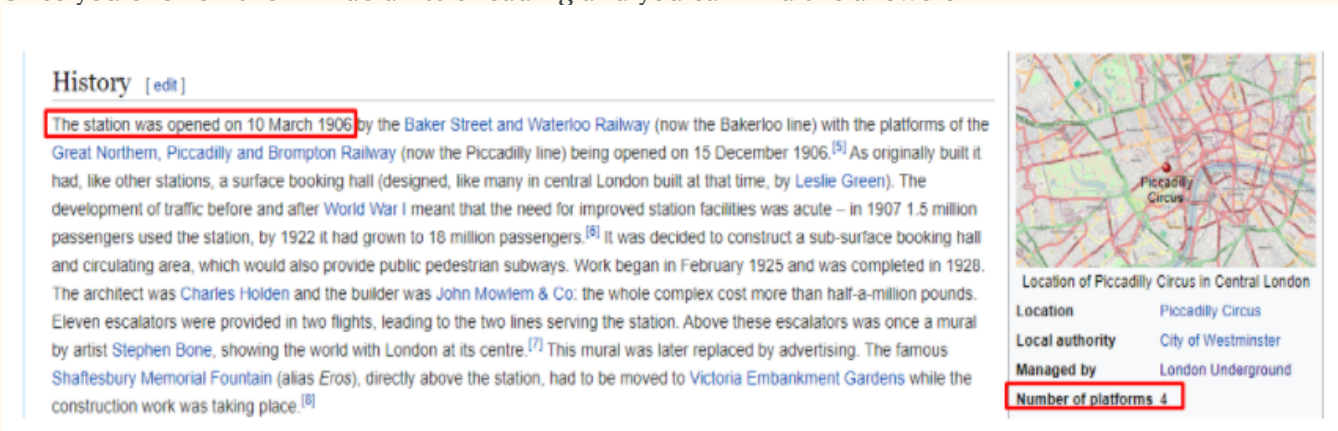
Which year did the station open?

How many platforms are there in the station?

From here it's best to navigate back to google and search for piccadilly circus and the first result we get up is from wiki



Once you click on the link do a little reading and you can find the answers



#5FLAG: sl{1906} **#6FLAG: sl{4}**

Task 4 - Keep at it!

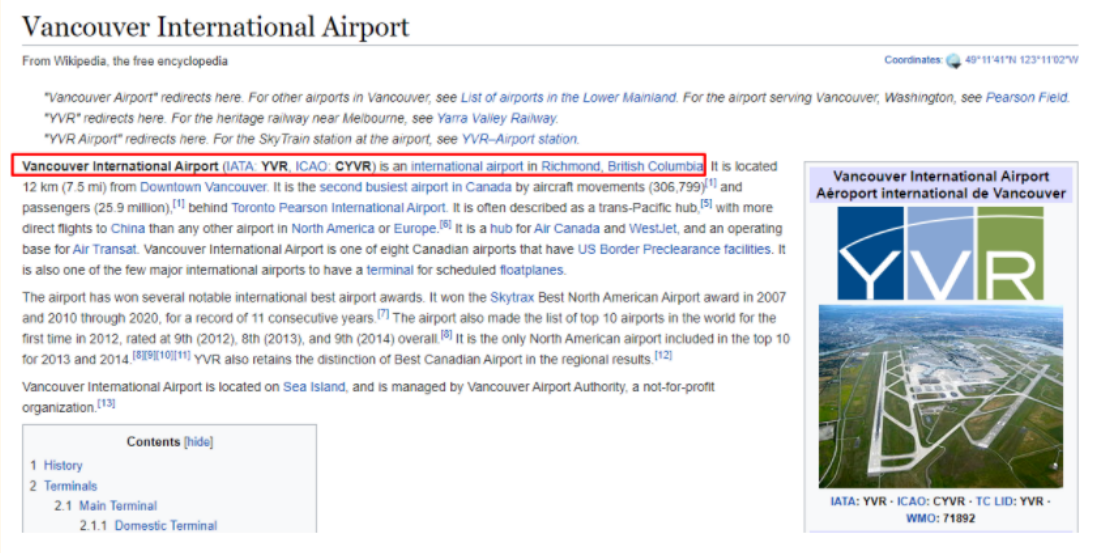
As we have now discovered the tasks are now getting harder for this one, we need to look at the picture and see if anything in the image can be used in google or another search engine to see if we can narrow down the location and to answer the following questions:

Which building is this photo taken in?

Which country is this building located in?

Which city is this building located in?

Looking at the picture the first thing that sticks out that can be of some interest is the banner that says YVR connects, so once placing this in a search query we get back the first result as Wikipedia once we click on that we get the following information which allows us to answer are three questions.



Vancouver International Airport

From Wikipedia, the free encyclopedia

Coordinates: 49°11'41"N 123°11'02"W

"Vancouver Airport" redirects here. For other airports in Vancouver, see List of airports in the Lower Mainland. For the airport serving Vancouver, Washington, see Pearson Field.
"YVR" redirects here. For the heritage railway near Melbourne, see Yarra Valley Railway.
"YVR Airport" redirects here. For the SkyTrain station at the airport, see YVR–Airport station.

Vancouver International Airport (IATA: **YVR**, ICAO: **CYVR**) is an international airport in Richmond, British Columbia. It is located 12 km (7.5 mi) from Downtown Vancouver. It is the second busiest airport in Canada by aircraft movements (306,799)[1] and passengers (25.9 million),[1] behind Toronto Pearson International Airport. It is often described as a trans-Pacific hub,[5] with more direct flights to China than any other airport in North America or Europe.[6] It is a hub for Air Canada and WestJet, and an operating base for Air Transat. Vancouver International Airport is one of eight Canadian airports that have US Border Preclearance facilities. It is also one of the few major international airports to have a terminal for scheduled floatplanes.

The airport has won several notable international best airport awards. It won the Skytrax Best North American Airport award in 2007 and 2010 through 2020, for a record of 11 consecutive years.[7] The airport also made the list of top 10 airports in the world for the first time in 2012, rated at 9th (2012), 8th (2013), and 9th (2014) overall.[8] It is the only North American airport included in the top 10 for 2013 and 2014.[8][9][10][11] YVR also retains the distinction of Best Canadian Airport in the regional results.[12]

Vancouver International Airport is located on Sea Island, and is managed by Vancouver Airport Authority, a not-for-profit organization.[13]

Contents [hide]
1 History
2 Terminals
2.1 Main Terminal
2.1.1 Domestic Terminal

Vancouver International Airport
Aéroport international de Vancouver

YVR

IATA: YVR · ICAO: CYVR · TC LID: YVR · WMO: 71892

#7FLAG: sl{vancouver international airport} #8FLAG: sl{canada} #9FLAG: sl{richmond}

Task 5 - Coffee and a light lunch

Task 5 and 5 questions to solve this is where Google Dorking is a major player in this task - we will be using the google the image below does not give us much to go off bar we know that it's in Scotland and it's a one way system and the shop across the road is The Edinburgh Woolen Mill as seen in the picture below The questions we need to answer are:

Which city is the coffee shop located in?

Which street is the coffee shop located in?

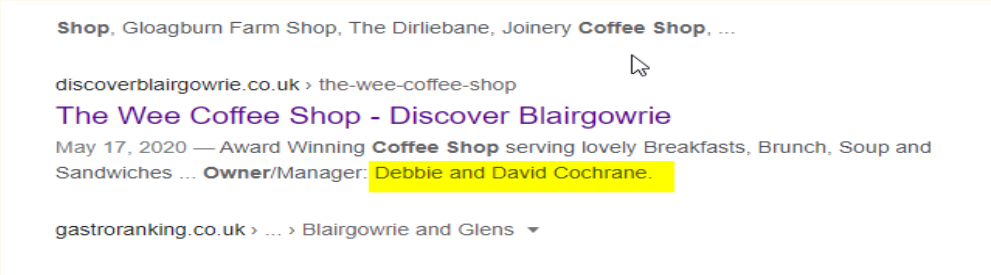
What is their email address?

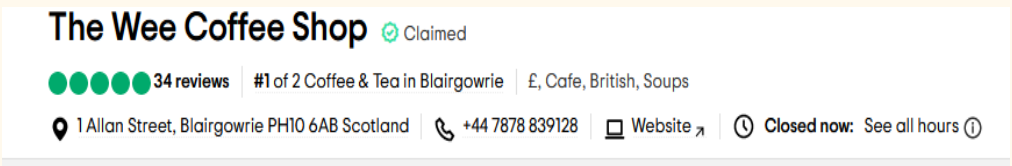
What is the surname of the owners?

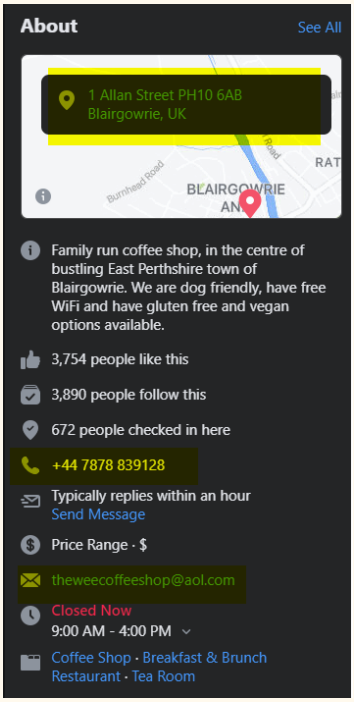
Using the search query, we get a lot of results back from google maps so narrow it down to Scotland and we then have a more limited selection form here I went through each one until I found the Mill I was looking for. After searching I found out it was 1 Allen Street, Blairgowrie

From I went on to on to street view and then into 360 and spinning the camera round it shows you the "Wee Coffee Shop" in Blairgowrie. #

So now to find out the email address etc. Well since I have the name and address of the coffee shop, finding the phone number and email address wasn't hard. This shop had a Facebook page with all the details. , you can also find it on trip advisor. For finding the surname I scrolled through Facebook posts / google who owns the shop







#10FLAG: sl{blairgowrie}

#11FLAG: sl{allan street}

#12FLAG: sl{+447878 839128}

#13FLAG: sl{theweecoffeeshop@aol.com}

#14FLAG: sl{cochrane}

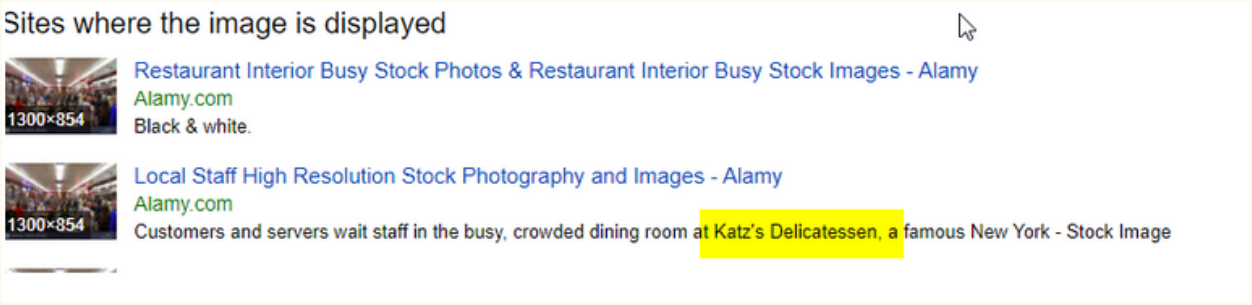
Task 6 - Reverse your thinking

This challenge we have a hint that we need to use a reverse image search so heading to google or Yandex image search. The questions we need to answer are:

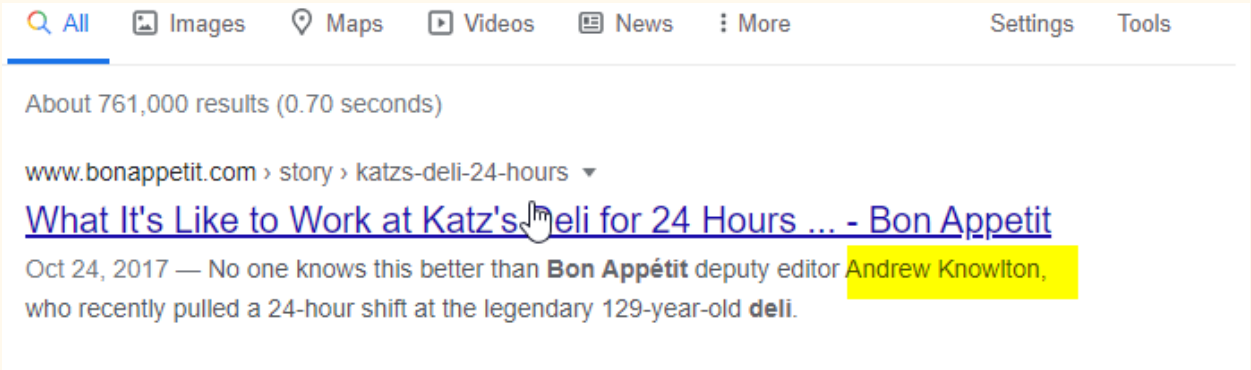
Which restaurant was this picture taken at?

What is the name of the Bon Appétit editor that worked 24 hours at this restaurant?

The reverse image search comes back instantly and gives the following results



Now we know the restaurant we can google what's it like to work in katz for 24 hrs and it returns the following you can also just include katz +bon appetit



#15FLAG: sl{Katz' delicatessen} **#16FLAG: sl{andrew knowlton}**

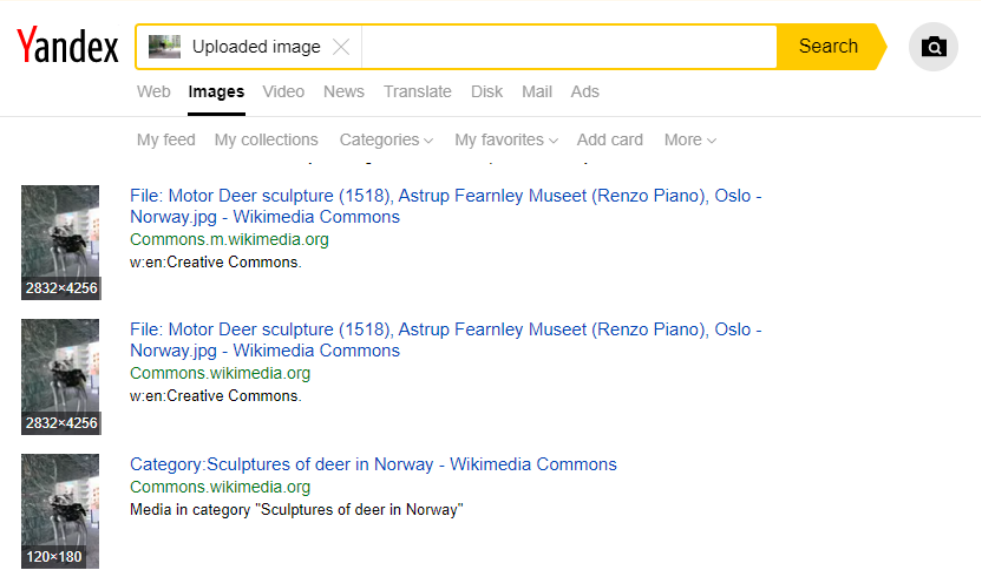
Task 7 - Locate this sculpture

With this challenge I went to google image reverse search and then Yandex and found that Yandex did come back with the best results. Questions we need to answer:

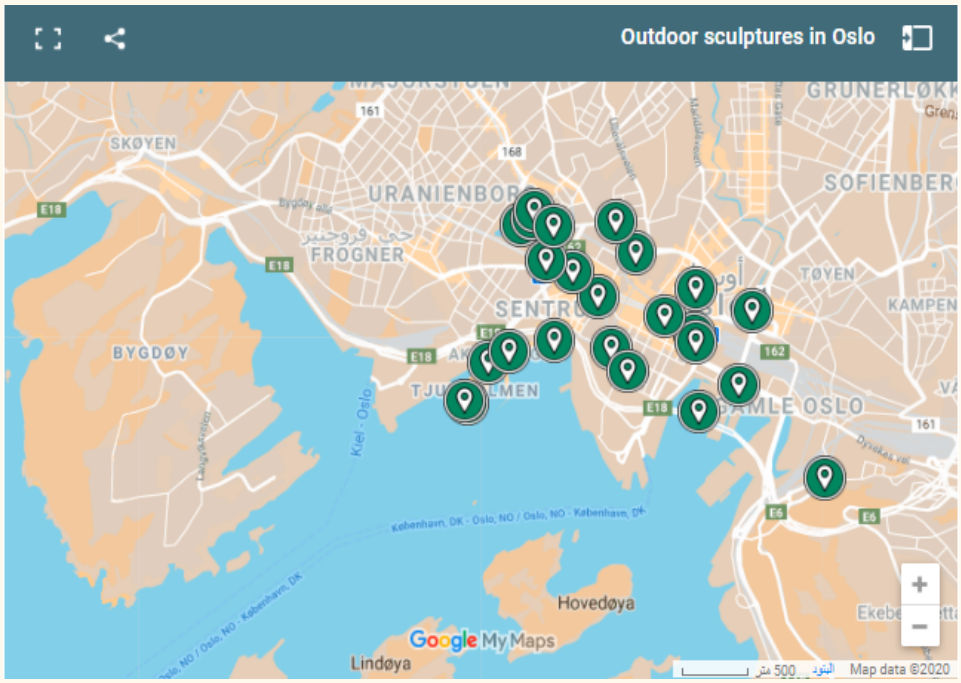
What is the name of this statue?

Who took this image?

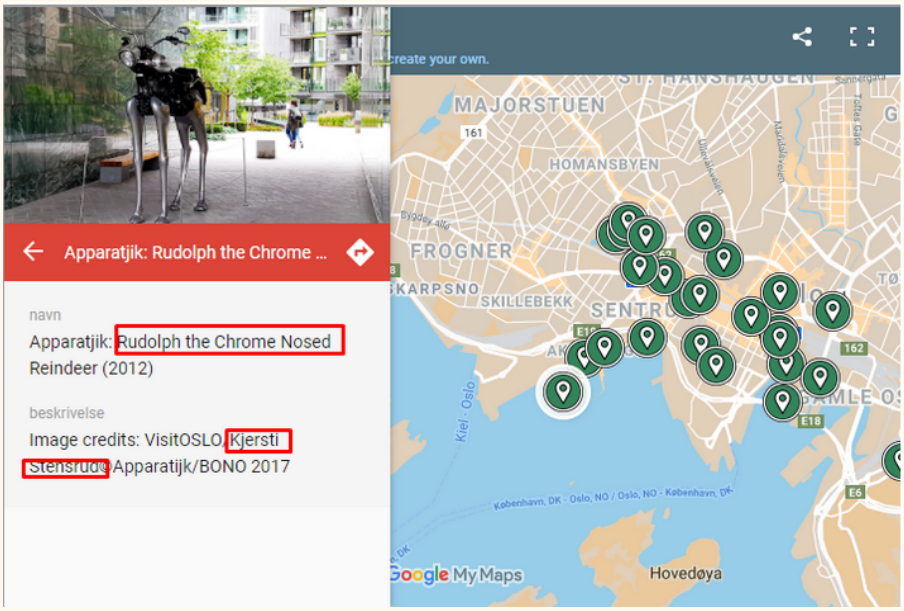
The research results will show below if you use Yandex



After using a google search query we can find that motor Deer sculpture is in Oslo. The hint also tells us “If you know the location of the statue you may want to visitoslo”



Once doing so we can just look through the map on the website and find the correct one



#17FLAG: sl{rudolph the chrome nosed reindeer} #18FLAG:sl{kjersti stensr}

Task 8 - ...and justice for all

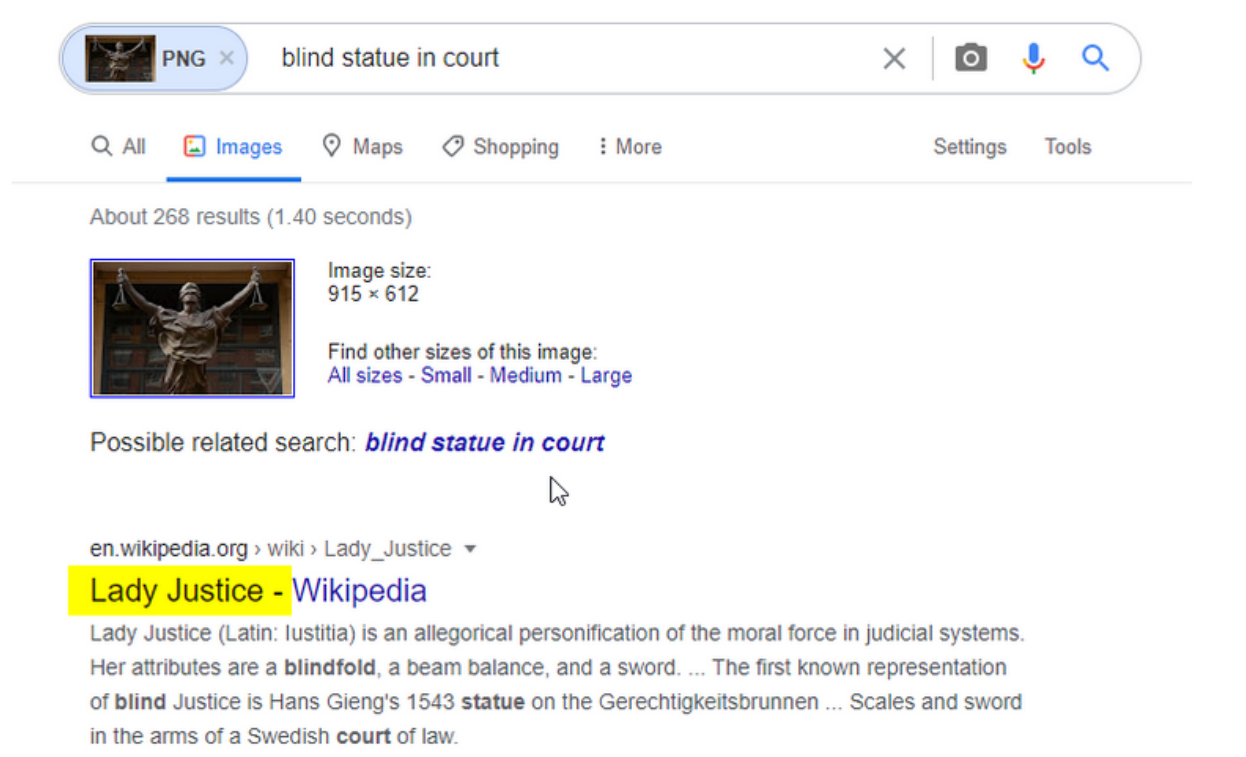
Once I downloaded the files, I looked at what questions I needed to answer and then went to an image search.

Questions we need to answer:
What is the name of the character that the statue depicts?

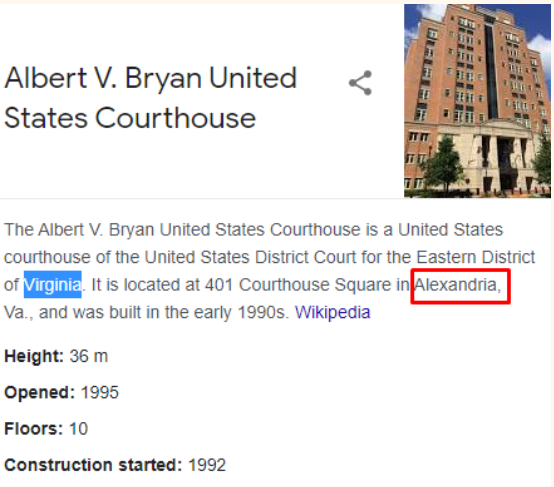
Where is this statue located?

What is the name of the building opposite from this statue?

Using google image search I found the following results:



From here I then googled the name of the landmark, and the location came up on google maps click on the link and you get the following results.



In order to find the opposite building head to google maps head to street view pan the camera round and there we have The hotel -The Westin Alexandria Old town.

#19FLAG: slsl{lady justice} **#20FLAG: sl{alexandria, virginia}**

#21FLAG: sl{the westin alexandria old town}

Task 9 - The view from my hotel room

The final task and this was a challenge to extract information from a video clip and have to examine the frame and work out where the location might be. Lucky that I have seen some of the buildings previously from films. I managed to locate the country straight off but we will work to the knowledge that I did not.

Questions we need to answer – what is the name of the hotel that my friend is staying at?

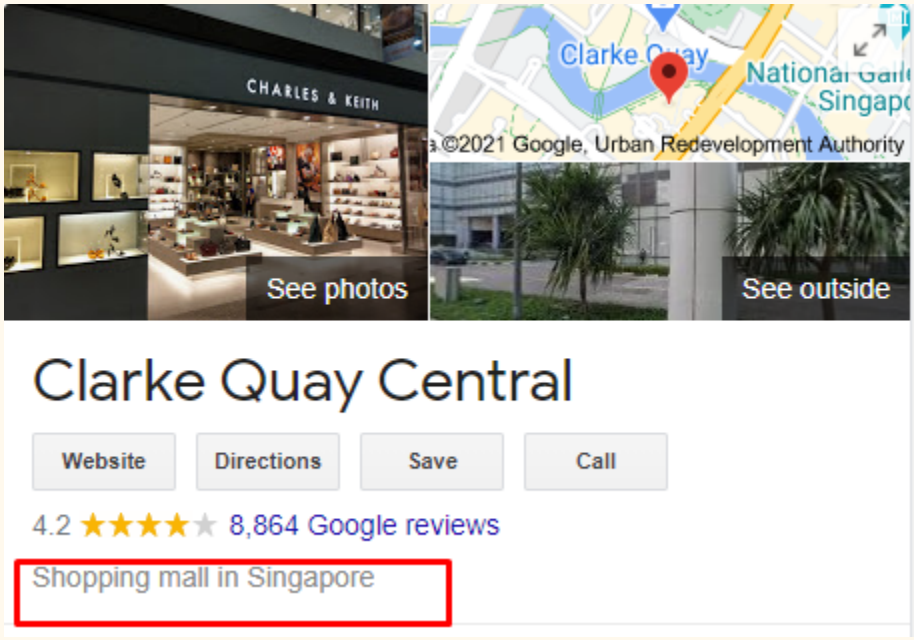
From here we will be using a tool called Ffmpeg follow the https://nixintel.info/osint-tools/using-ffmpeg-to-grab-stills-and-audio-for-osint/ for setting up this tool.

```
[redacted]\THM_Searchlight>ffmpeg -i task9.mp4 img%06d.png -hide_banner
Input #0, mov,mp4,m4a,3gp,3g2,mj2, from 'task9.mp4':
  Metadata:
    major_brand     : isom
    minor_version   : 512
    compatible_brands: isomiso2avc1mp41
    encoder         : Lavf58.29.100
  Duration: 00:00:47.57, start: 0.000000, bitrate: 5160 kb/s
    Stream #0:0(und): Video: h264 (High) (avc1 / 0x31637661), yuv420p(tv, bt709), 1920x1080 [SAR 1:1 DAR 16:9], 4858 kb/s, 29.97 fps, 29.97 tbr, 30k tbn, 59.94 tbc (def
ault)
    Metadata:
      handler_name    : VideoHandler
    Stream #0:1(und): Audio: aac (LC) (mp4a / 0x6134706D), 48000 Hz, stereo, fltp, 295 kb/s (default)
    Metadata:
      handler_name    : SoundHandler
Stream mapping:
  Stream #0:0 -> #0:0 (h264 (native) -> png (native))
Press [q] to stop, [?] for help
Output #0, image2, to 'img%06d.png':
  Metadata:
    major_brand     : isom
    minor_version   : 512
    compatible_brands: isomiso2avc1mp41
    encoder         : Lavf58.45.100
    Stream #0:0(und): Video: png, rgb24, 1920x1080 [SAR 1:1 DAR 16:9], q=2-31, 200 kb/s, 29.97 fps, 29.97 tbn, 29.97 tbc (default)
    Metadata:
      handler_name    : VideoHandler
      encoder         : Lavc58.91.100 png
frame=  563 fps=8.4 q=-0.0 size=N/A time=00:00:18.65 bitrate=N/A speed=0.28x
```

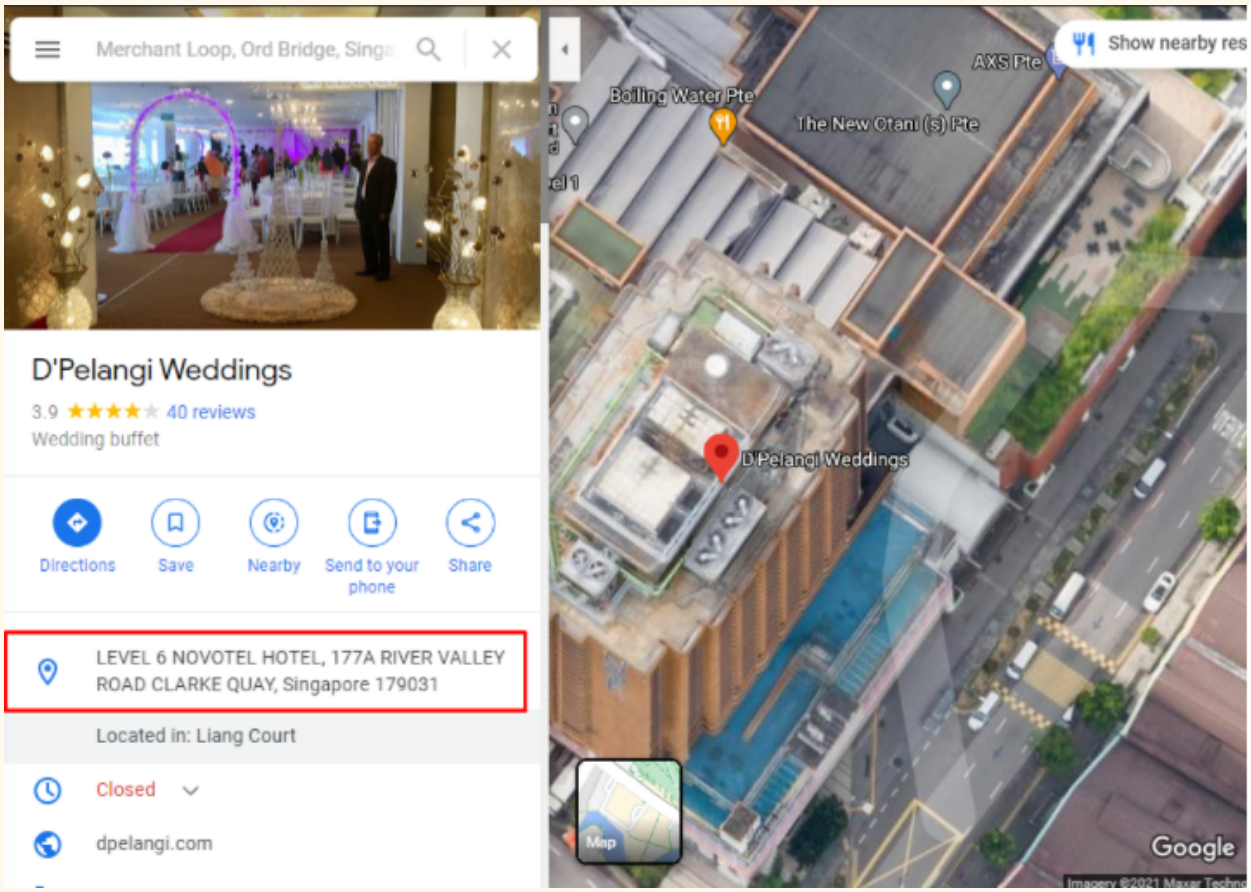
Run the following code above and remember that there will be a lot of frames extracted in the folder. From here we can look through the frames so see where we can try to pinpoint the location of the friend (this is a step which you can also just watch the video multiple times and white down the names etc but I would recommend using the tools provided.)

The first picture we come across is the Clarke query central building so if we do a google search query we can see it's a shopping mall in Singapore.

From here if we jump on to google maps, we can also see what is around.



Head to street view and explore this we can also see from the other pictures in the video that there are multiple shops and river ports we can use to pinpoint the exact location have a look around and we can see that, if we click on D'Pelangi weddings, that we can find out hotel, which is called Novotel Singapore Clarke quay.



#22FLAG: sl{novotel singapore clarke quay}

Conclusion

This was a good room, and it shows that anyone can use image searches and tools to find out information. Sometimes we just need to slow down, have a think and think analytically and it will become easier to extract more information related to the target you are gathering intelligence on.