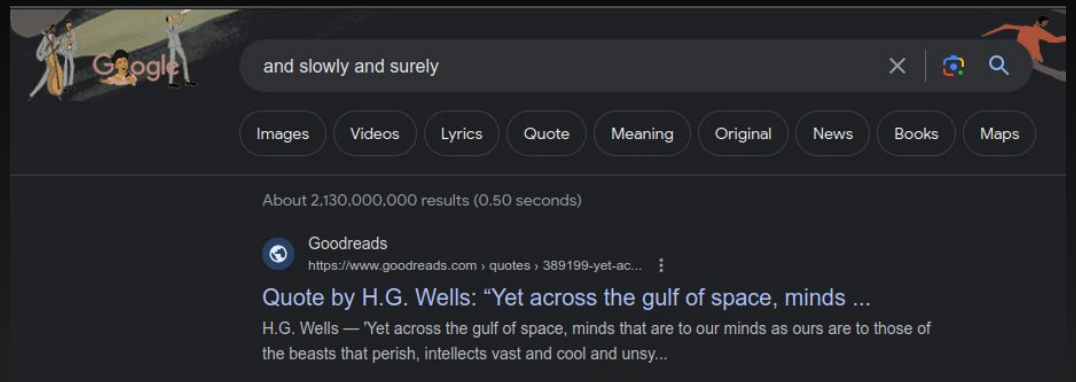
Introduction to OSINT
WORKED SOLUTIONS

CONTENTS:

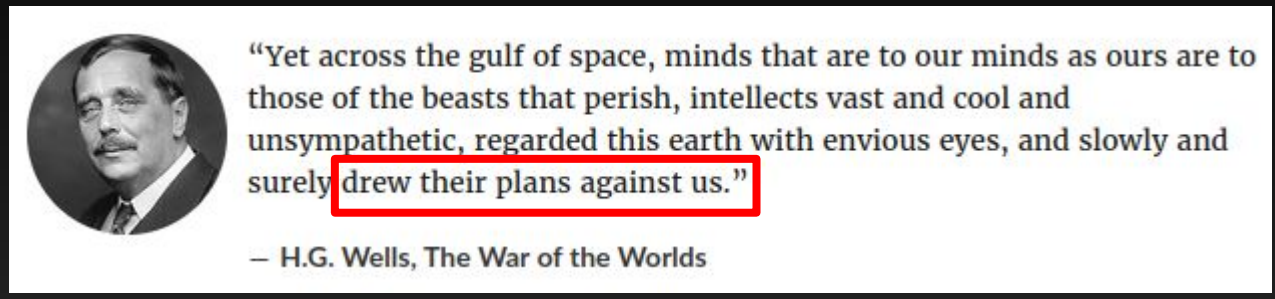
Click to go to a solution:

Non-Image-Related Questions

1. Finish the sentence: And slowly, and surely, _____



Search what you've been given already
First result on Google - brings up a book - click this

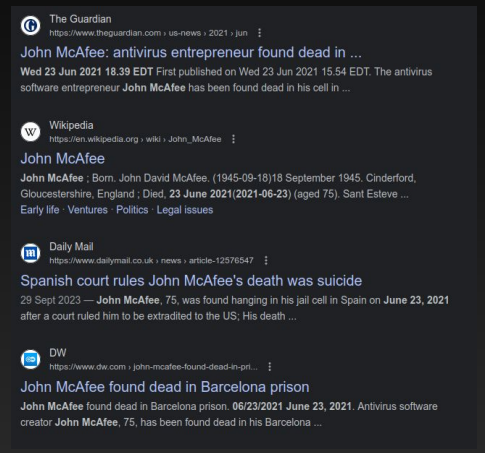


The quote is here on the page

Answer: (They)* drew their plans against us.

*With or without the 'They', which is added in the 1978 album by Jeff Wayne.

2. Where was John McAfee on 23rd June 2021?

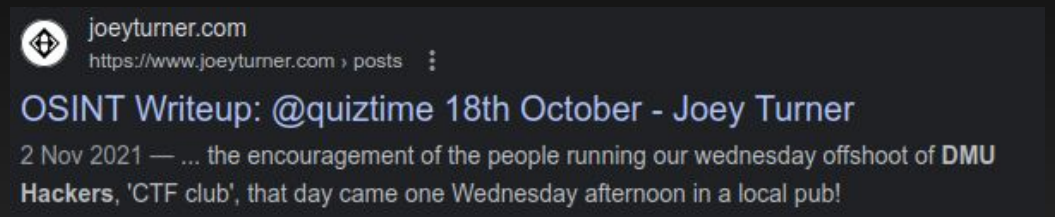


Search 'John Mcafee 23rd June 2021'
Multiple news articles talking about what happened

Answer: Found dead in his prison cell

3. Where did Joey buy the domain for his website from?

There are quite a few solutions to this question (as often happens in OSINT), but this is just one way of doing it:



Searching 'Joey DMU Hackers' and scrolling down a bit brings up an article from his website

We now know his domain is joeyturner.com

```
turnernator@gandalf:~$ whois joeyturner.com
   Domain Name: JOEYTURNER.COM
   Registry Domain ID: 2583457652_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.namecheap.com
   Registrar URL: http://www.namecheap.com
   Updated Date: 2022-12-09T06:57:00Z
   Creation Date: 2021-01-08T18:18:14Z
```

Doing a whois lookup shows very clearly who the registrar is - if you weren't aware what a registrar was, then a search of 'Namecheap' confirms this

NB: This didn't have to be command-line based, there are plenty of tools on the web which let you do whois lookups, ie whois.com

Answer: Namecheap

EXIF

You are able to complete these questions by mainly looking at EXIF data

A quick note: EXIF data is viewable both by command-line tools and on websites with a friendlier UI, it's easier to do it the website way but these examples will show both methods. However, use whatever is available and/or works for you!

1. What phone was this photo taken on?

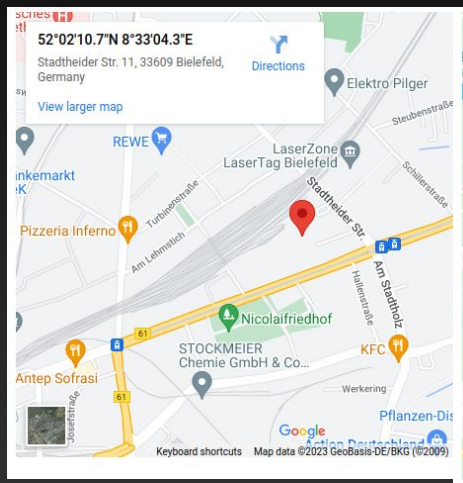
exiftool exif-image-1.jpg

```
Circle Of Confusion             : 0.006 mm
Field Of View                   : 69.4 deg
Focal Length                    : 5.1 mm (35 mm equivalent: 26.0 mm)
GPS Position                    : 51 deg 56' 56.75" N, 0 deg 29' 45.23" W
Hyperfocal Distance             : 2.76 m
Light Value                     : 13.5
Lens ID                         : iPhone 12 Pro Max back triple camera 5.1mm f/1
```

Answer: iPhone 12 Pro Max

2. What city was this photo taken in?

Using a website such as jimpl.com to show location of an image:



Answer: Bielefeld, Germany

OMU HACKERS

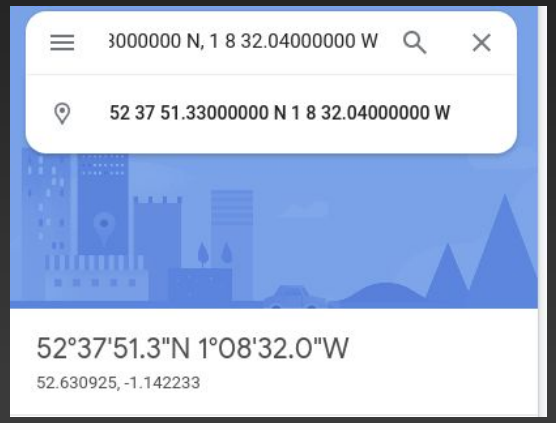
3. Which place was this photo taken?

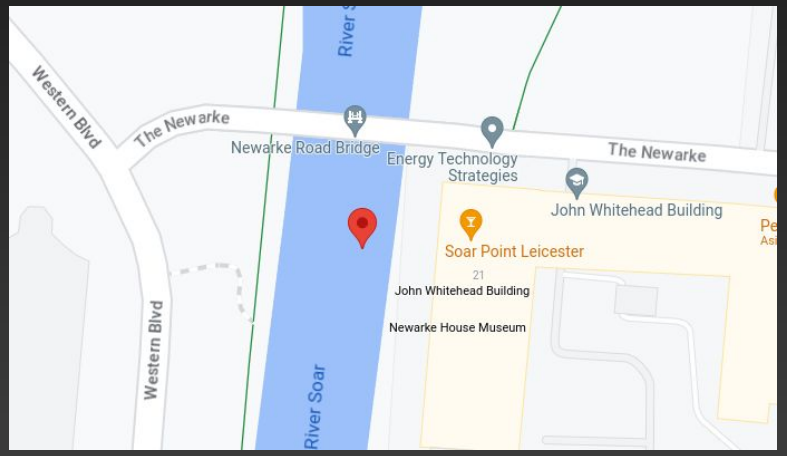
This just makes it easier to paste into Google Maps: [read more about it here]

```
exiftool exif-image-3.jpg -c "%d %d %.8f"

Field Of View                   : 69.4 deg
Focal Length                    : 5.1 mm (35 mm equivalent: 26.0 mm)
GPS Position                    : 52 37 51.33000000 N, 1 8 32.04000000 W
Hyperfocal Distance             : 2.76 m
```

Copy and paste the co-ordinates into Google Maps:





Using a bit of common sense (because why would somebody be sat in the River Soar with a laptop and some Ketchup?!), it's reasonable to conclude this was taken in the Soar Point pub!

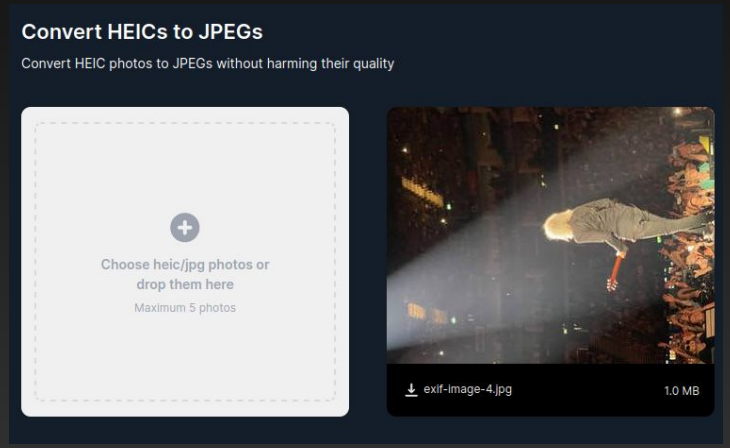
Answer: Soar Point, Leicester

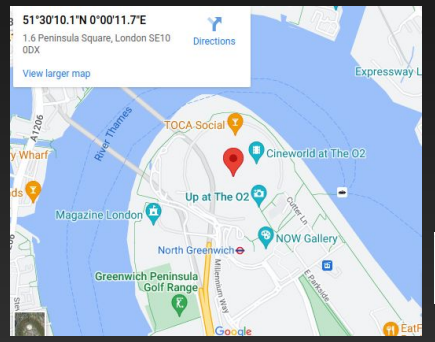
4. Who was playing this gig and where was it?

If you knew this is Brian May and therefore Queen, then gg

Won't be able to view this within GitHub as it's a HEIC file (Apple live photo format) - can either exiftool it or convert to jpg first and then upload to a website as previously

https://heictojpg.com/

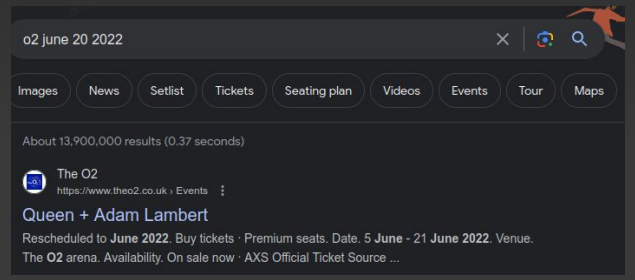




We know this was taken at the O2 Arena on June 20th, 2022

Created	June 20, 2022 20:31

A quick search for O2 June 20 2022 brings us the band name:



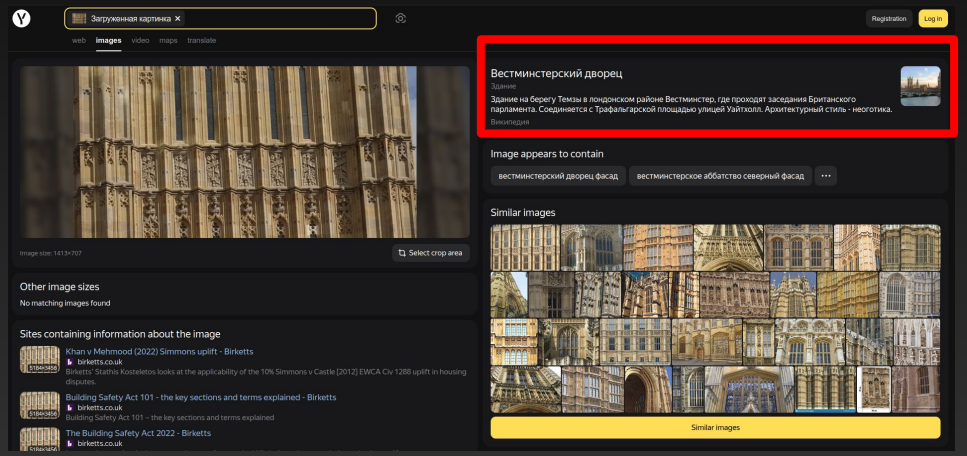
Answer: Queen + Adam Lambert at the O2 Arena, London

NON-EXIF

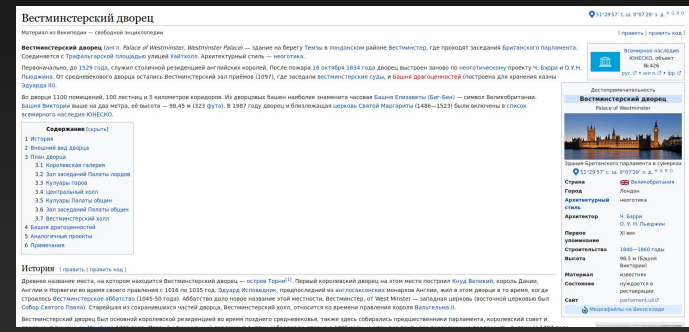
EXIF data won't help you here!!!

1. What is this an image of?

Reverse image search it - best to use Yandex although Google works too in this instance



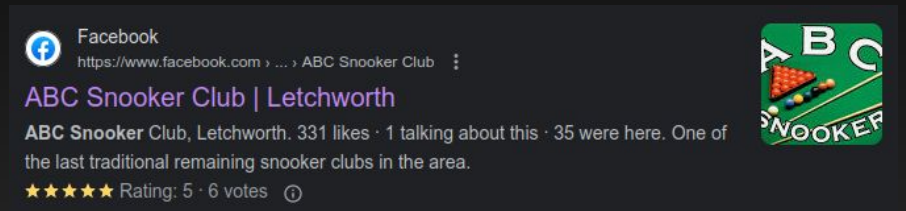
Don't need to even translate it to see what it is



Answer: Palace of Westminster/Big Ben

2. This image was taken outside a pub. Which pub was it?

Search for 'ABC Snooker' and scrolling through some results, shows a Facebook page with the same logo



Searching 'ABC Snooker' Letchworth on Google Maps, you are able to confirm it's the same location

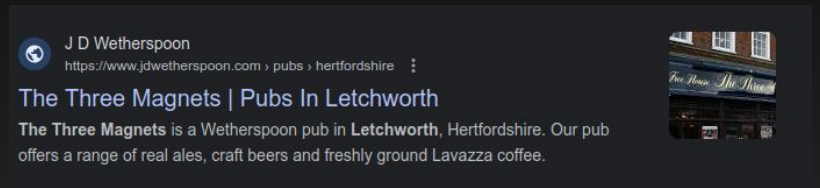
Turning to face the direction closer to where the picture was taken from, you can see there's a pub there

Answer: The Three Magnets, Letchworth

OMU HACKERS

2a. How much is a pint of Rosie's Pig Cider in this pub? (as of 19/10/2023)

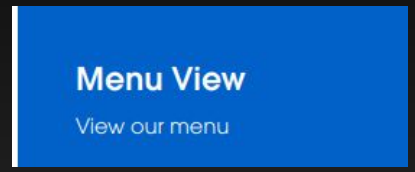
From the previous question, you can search for the pub online and find that it's a Wetherspoon pub

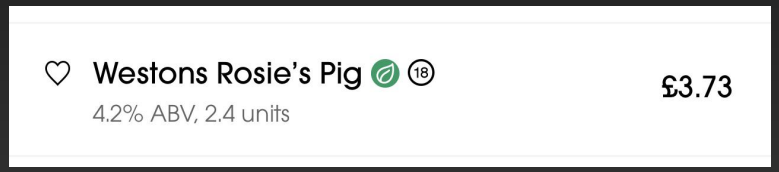


There is actually a Wetherspoon app which can be used for table ordering, however we'll be using it for price check.

Select the pub and then find Rosie's Pig cider

You'll find an option to view their manu with a bit of scrolling (but this is a dead end)

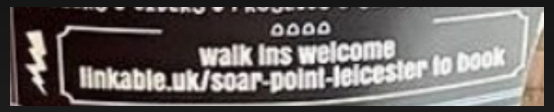




Answer: £3.73

3. On what day of the week could you win Jack Black?

If you look closely, you can see it's the Soar Point pub



If you look through their Instagram account @soarpoint, you can see numerous postings of cardboard cutouts with a re-ocurring theme:

It's always for Bingo Club on a Thursday!

This is confirmed by finding the Jack Black post on 8th May, where it explicitly talks about winning him during Bingo Club on Thursday

Answer: Thursday

OMU HACKERS

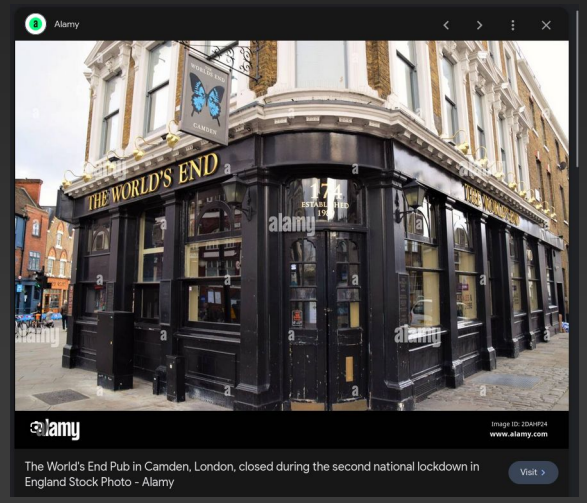
4. Where is this pub located?

There are a lot of pubs called 'The World's End', but if you search and then go by images, you should be able to spot the one matching the picture quite quickly.

You have to search with either:
'the worlds end - film' (due to the Pegg/Frost/Wright film of the same name

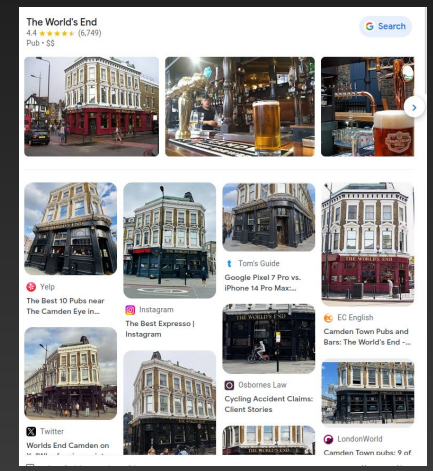
Or

'The worlds end pub'



Answer: Camden, London

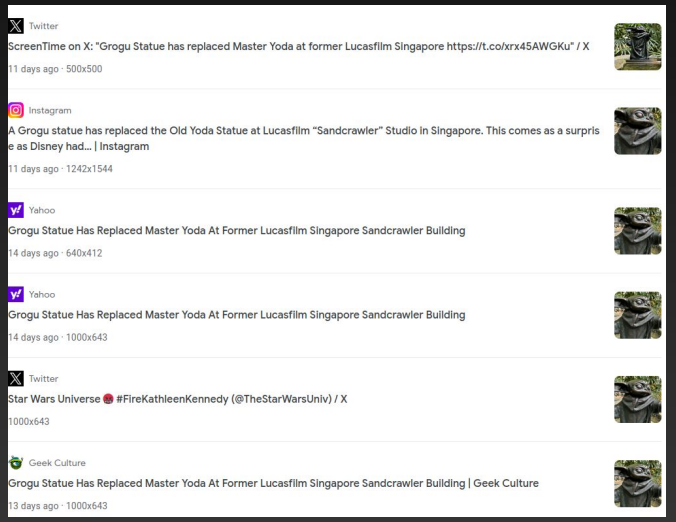
Or of course, you could reverse image search it!



OMU HACKERS

5. Where is this statue located?

Searching 'Grogu statue' or 'Baby Yoda' statue doesn't return a lot, however a reverse image search gives numerous tweets/news articles



Answer: Lucasfilm Offices, Singapore