



Introduction to OSINT
WORKED SOLUTIONS

CONTENTS:

Click to go to a solution:

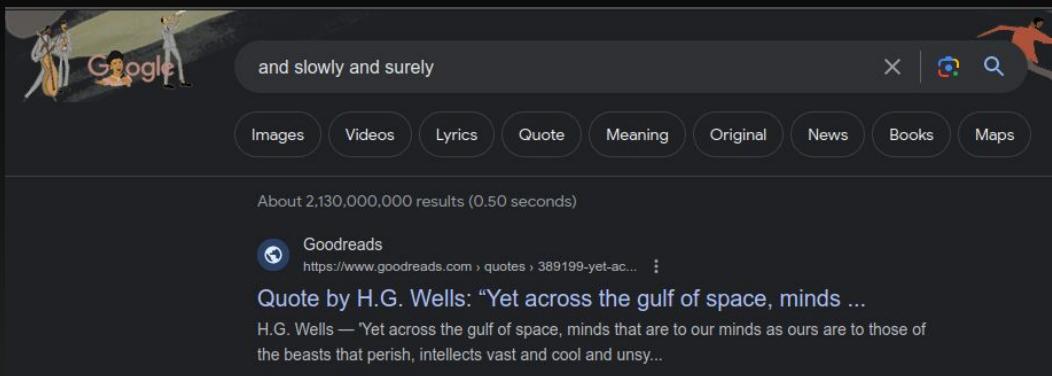
Non-Image-Related	EXIF	Non-EXIF
Task 1	Task 1	Task 1
Task 2	Task 2	Task 2
Task 3	Task 3	Task 2a
	Task 4	Task 3
		Task 4
		Task 5



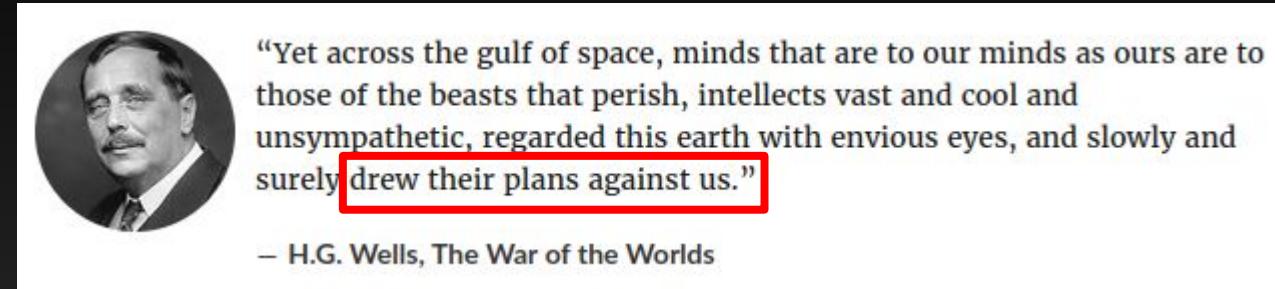
Non-Image-Related Questions



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



A screenshot of a Google search results page. The search query is "and slowly and surely". The results include a snippet from H.G. Wells' quote: "Yet across the gulf of space, minds that are to our minds as ours are to those of the beasts that perish, intellects vast and cool and unsympathetic, regarded this earth with envious eyes, and slowly and surely drew their plans against us." Below the snippet is the attribution: "— H.G. Wells, The War of the Worlds". There are also links to Goodreads and the original quote on quotes.com.



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?

The Guardian
John McAfee: antivirus entrepreneur found dead in ...
Wed 23 Jun 2021 18.39 EDT First published on Wed 23 Jun 2021 15.54 EDT. The antivirus software entrepreneur John McAfee has been found dead in his cell in ...

Wikipedia
John McAfee
John McAfee : Born: John David McAfee, (1945-09-18)18 September 1945, Cinderford, Gloucestershire, England ; Died: 23 June 2021(2021-06-23) (aged 75). Sant Esteve ...
Early life · Ventures · Politics · Legal issues

Daily Mail
Spanish court rules John McAfee's death was suicide
29 Sept 2023 — John McAfee, 75, was found hanging in his jail cell in Spain on June 23, 2021 after a court ruled him to be extradited to the US; His death ...

DW
John McAfee found dead in Barcelona prison
John McAfee found dead in Barcelona prison. 06/23/2021 June 23, 2021. Antivirus software creator John McAfee, 75, has been found dead in his Barcelona ...

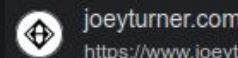
Search 'John McAfee 23rd June 2021'
Multiple news articles talking about what happened

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:



OSINT Writeup: @quiztime 18th October - Joey Turner

2 Nov 2021 — ... the encouragement of the people running our wednesday offshoot of DMU Hackers, 'CTF club', that day came one Wednesday afternoon in a local pub!

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

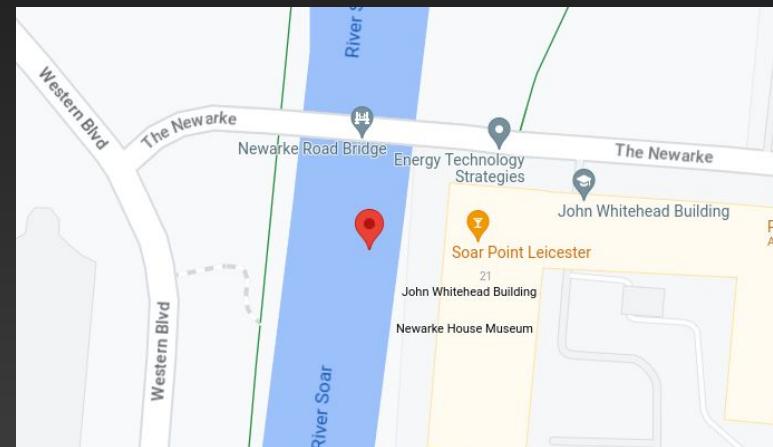
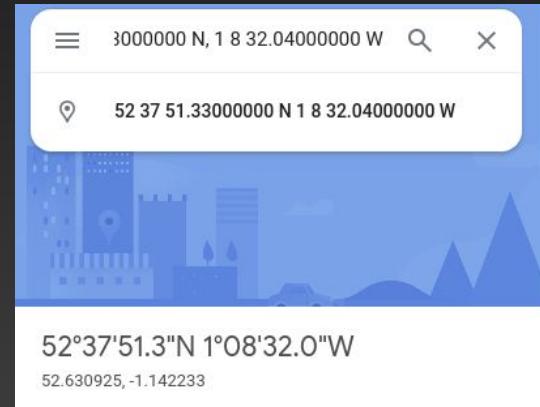


3. Which place was this photo taken?



```
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

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

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



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/>

Convert HEICs to JPEGs

Convert HEIC photos to JPEGs without harming their quality

+ Choose heic/jpg photos or drop them here Maximum 5 photos


exif-image-4.jpg 1.0 MB



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:

o2 June 20 2022

Images News Setlist Tickets Seating plan Videos Events Tour Maps

About 13,900,000 results (0.37 seconds)

The O2 <https://www.theo2.co.uk/Events> Queen + Adam Lambert Rescheduled to June 2022. Buy tickets · Premium seats. Date, 5 June - 21 June 2022. Venue, The O2 arena. Availability. On sale now · AXS Official Ticket Source ...

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

Facebook
<https://www.facebook.com/abc-snooker-club>

ABC Snooker Club | Letchworth

ABC Snooker Club, Letchworth. 331 likes · 1 talking about this · 35 were here. One of the last traditional remaining snooker clubs in the area.

★★★★★ Rating: 5 · 6 votes

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



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



Answer: The Three Magnets, Letchworth



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

J D Wetherspoon
<https://www.jdwetherspoon.com/pubs/hertfordshire/the-three-magnets>

The Three Magnets | Pubs In Letchworth

The Three Magnets is a Wetherspoon pub in Letchworth, Hertfordshire. Our pub offers a range of real ales, craft beers and freshly ground Lavazza coffee.



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 menu with a bit of scrolling (but this is a dead end)

Menu View
View our menu

Westons Rosie's Pig ⚡ 16
4.2% ABV, 2.4 units £3.73

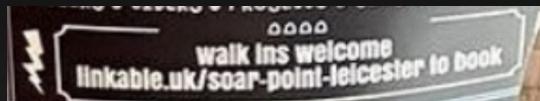
Answer: £3.73



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



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

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

It's always for Bingo Club on a Thursday!



Answer: Thursday



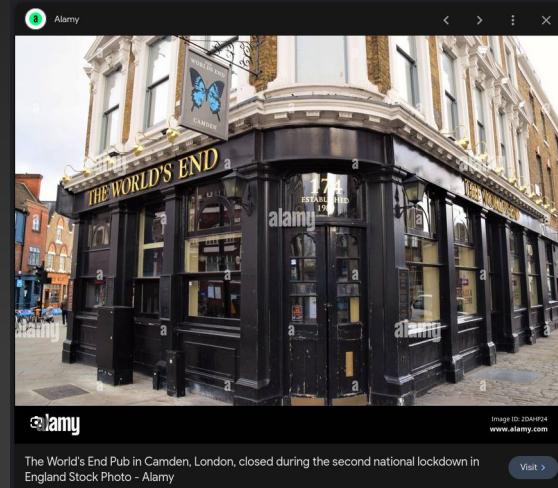
4. Where is this pub located?

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.

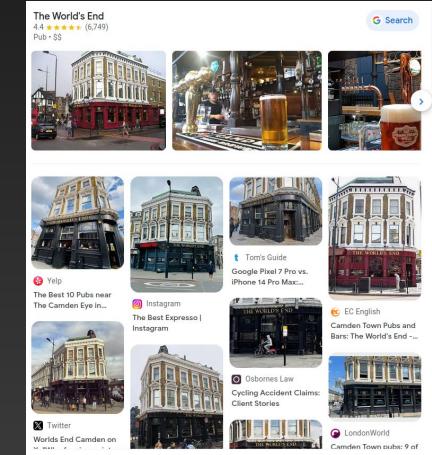
You have to search with either:
'the worlds end - film' (due to the Pegg/Frost/Wright film
of the same name)

Or

'The worlds end pub'



Or of course, you could reverse image search it!



Answer: Camden, London



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

← Post

ScreenTime 🌐 @screentime

Grogu Statue has replaced Master Yoda at former Lucasfilm Singapore

Two photographs of the Grogu statue. The left photo shows the statue from a side-on perspective, highlighting its profile and the texture of its robe. The right photo is a front-facing view, showing its face and hands clasped together. Both images are taken outdoors, with the statue resting on a circular stone base surrounded by rocks and greenery.

A vertical list of social media posts. From top to bottom: 1. A Twitter post from ScreenTime (@screentime) stating "Grogu Statue has replaced Master Yoda at former Lucasfilm Singapore" with a link. 2. An Instagram post from "A Grogu statue has replaced the Old Yoda Statue at Lucasfilm "Sandcrawler" Studio in Singapore. This comes as a surprise as Disney had..." 3. A Yahoo news article titled "Grogu Statue Has Replaced Master Yoda At Former Lucasfilm Singapore Sandcrawler Building". 4. Another Yahoo news article with the same title. 5. A Twitter post from Star Wars Universe (@TheStarWarsUniv) with a link. 6. A Geek Culture post titled "Grogu Statue Has Replaced Master Yoda At Former Lucasfilm Singapore Sandcrawler Building | Geek Culture".

Answer: Lucasfilm Offices, Singapore

