
OMU
HACKERS

Announcements

- This is the LAST free session - please buy your memberships!
- Come see us to claim your Firebug card
- CTF club
- Halloween next week

CyberFirst

cyberfirst@dmu.ac.uk or sarah.hd@dmu.ac.uk

wing wednesdays

wing wednesdays

CTF Club

wing wednesdays

wing wednesdays

WHAT IS CTF CLUB????

- Meet up every wednesday from 2pm
- Starts next week - 25/10/23
- Soar Point
- Collaboratively do THM boxes / CTFs / OSINT challenges
- No experience needed!

2pm Wednesday 25th October
@ Soar Point

TryHackMe Premium

- If you're interested in buying THM Premium, please use our referral code - will save you $5
- It's pretty worth it, use your student email (.ac.uk) and it's discounted by 20% to £10 a month

https://tryhackme.com/signup?referrer=612e9d2c35ba4b005a24feee

Halloween Next Week

- Spooky session
- **FANCY DRESS IS MANDATORY**
  (unless you *really* don't want to…)

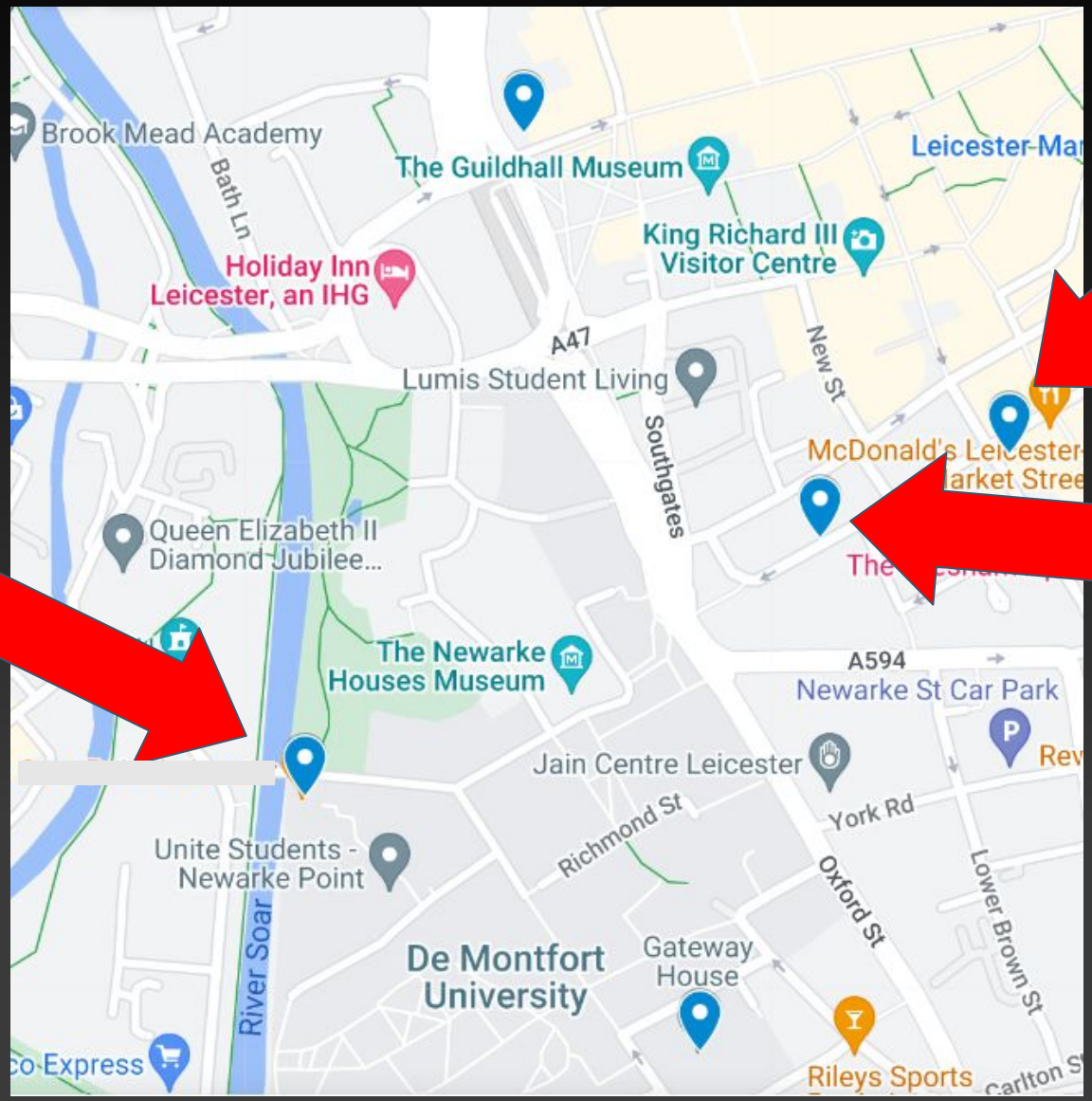
- Prepare to be scared!

25th October - NEXT WEEK

OMU HACKERS

Social

THE SOAR POINT



FIREBUG
BAR . VENUE . FOOD

oddbar

DMU HACKERS


hackers.dmu
@dmuhackers
DMU
HACKERS
Introduction to OSINT

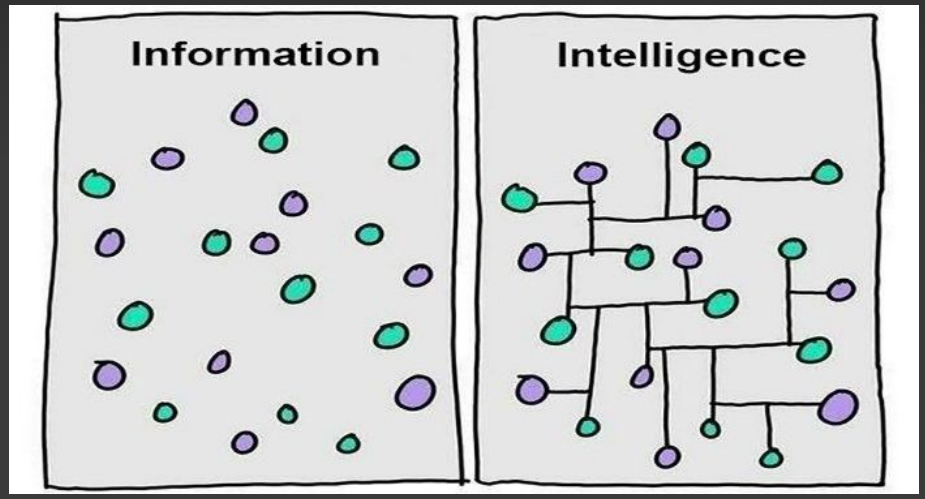
Don't do creepy shit

OSINT

Open Source INTelligence

What is OSINT?

- The collection and analysis of openly available data
- Information vs Intelligence - ?
- Information is raw, unprocessed data
- Intelligence is processed information!



What is it used for?

- Corporate security
- Background checks on new hires
- Police investigation/counter terrorism
- Threat Hunting/Research
- Pentesting
- Vetting
- To socially engineer people…

Some Areas of OSINT

Google Dork

Command-Line Tools

Domain & IP Investigation

News + Media

Image Analysis

Dark Web

Geolocation

Social Media Investigation

Reverse Image Search

OMU HACKERS

Google Dorking (aka 'Google Hacking')

- Basically being clever with how you Google 🤓🤓🤓
- Also useful for assignments/job/placement searching
- Use symbols and keywords for *precise* searching

Use Case	Operator	Example Usage
Searching Within a Specific Website	site:	site:dmuhackers.com orlin
Finding Specific File Types	filetype:	filetype:pdf developed vetting uk
Discard pages which mention a certain word	-	Cyber jobs -trainee
Search for an exact result	""	Cyber Security "placement"
Searching for Specific Text on a Web Page	intext:	intext:geolocation

Google Dorking (aka 'Google Hacking')

- More specifically for pentesters/bug bounty chasers, there's a whole list of searches you can use:

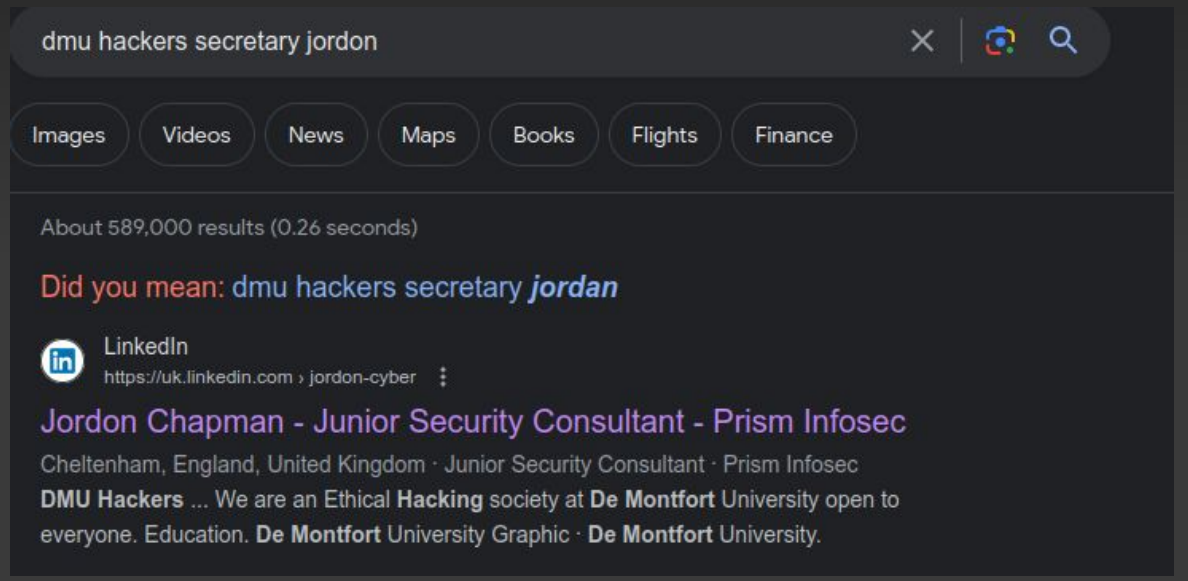
https://www.exploit-db.com/google-hacking-database

```
site:linkedin.com intitle:"@gmail"
intitle:"index of" "postman_collection.json"
intitle:"index of" intext: "login.php"
inurl:"/login.php" intitle:"admin"
intitle:"Index of" inurl:/backup/ "wp-config"
intitle:"index of" "username.txt"
```

Social Media Investigations

- A lot of people overshare ***way*** too much online - this works in our favour!
- Especially if profiles are public!!
- If you have a name, a great avenue to go down

'DMU Hackers secretary Jordon'



Social Media Investigations

- A great tool for finding the services a given username has signed up to: https://whatsmyname.app

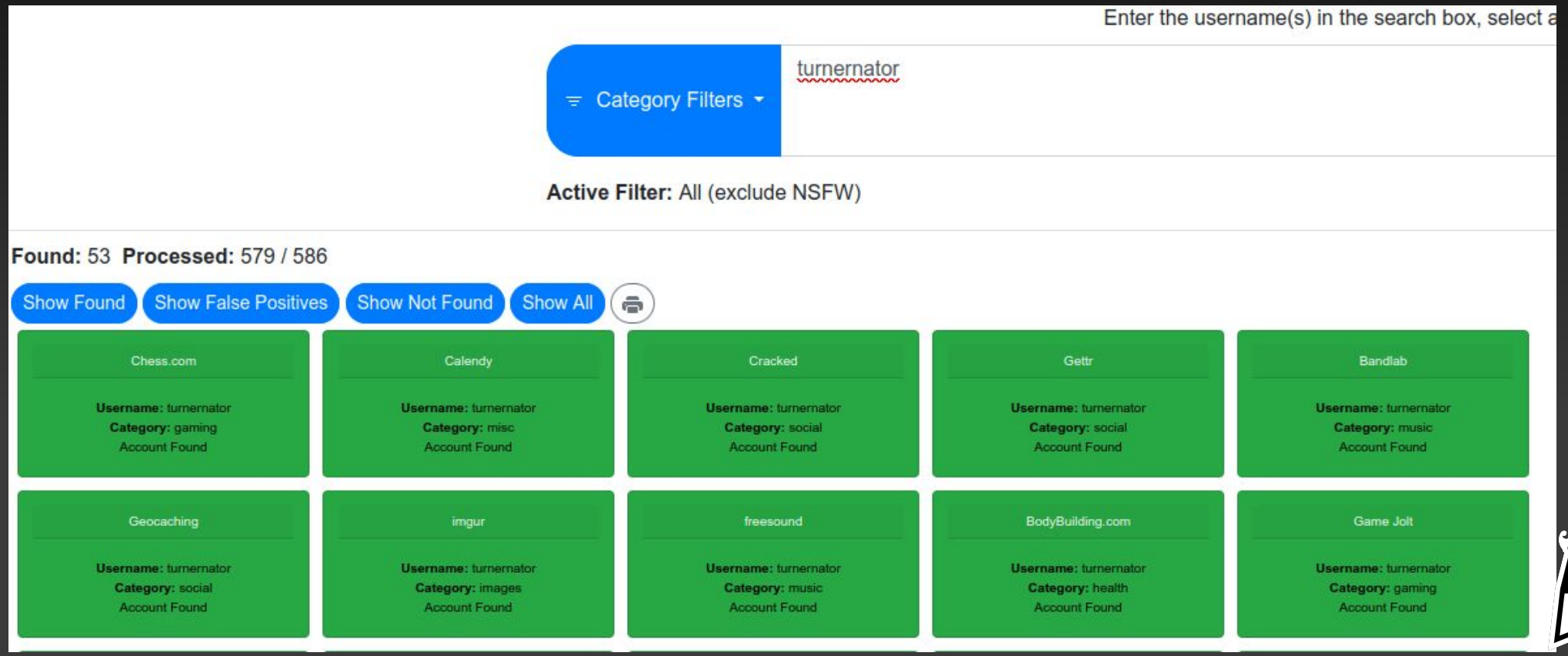
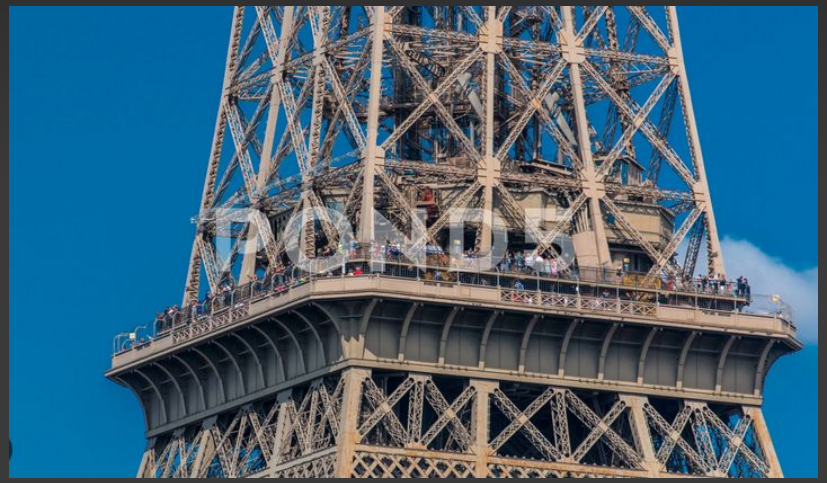


Image Analysis

- Reverse image searching - great for landmarks, photos that might have been taken by others
- Yandex >>>>>>>>>>>>>>>> Google Images, but always worth trying one if you don't get results from the other
- Google Lens - AI Powered



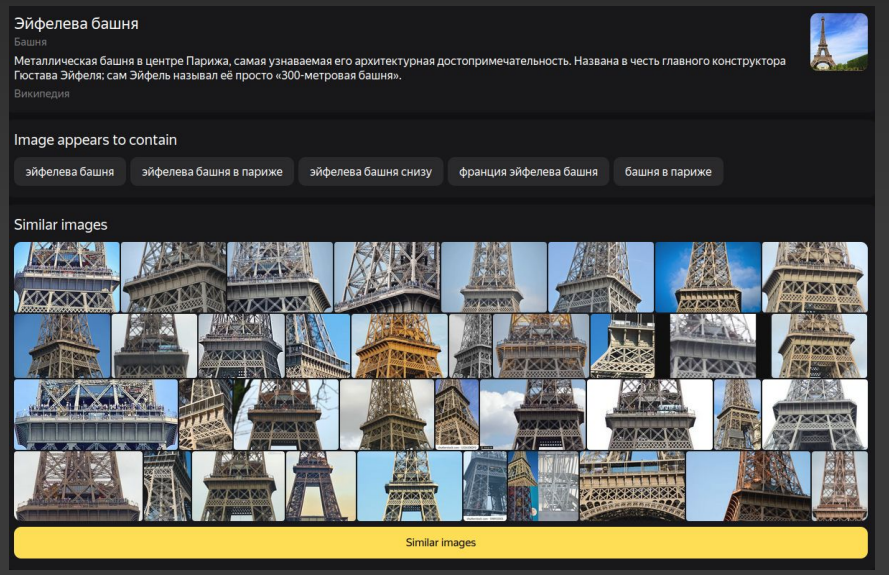
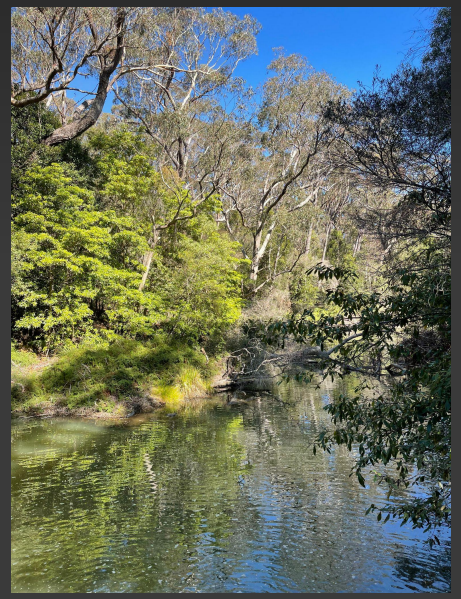


Image Analysis

- EXIF - Image metadata
- Most social media sites 'strip' this now, but a good shout especially for CTFs or websites
- Image coordinates, type of camera, all sorts!

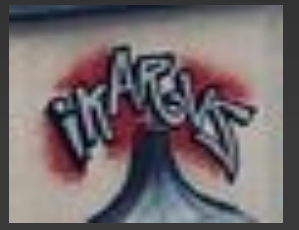


```
Shutter Speed                   : 1/672
Create Date                     : 2023:09:10 13:57:29.493+10:00
Date/Time Original              : 2023:09:10 13:57:29.493+10:00
Modify Date                     : 2023:09:10 13:57:29+10:00
GPS Altitude                    : 655.4 m Above Sea Level
GPS Latitude                    : 34 deg 38' 51.42" S
GPS Longitude                   : 150 deg 28' 59.85" E
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                    : 34 deg 38' 51.42" S, 150 deg 28' 59.85" E
Hyperfocal Distance             : 2.76 m
Light Value                     : 12.4
Lens ID                         : iPhone 12 Pro Max back triple camera 5.1mm f/1.6
```

Geolocation

- Working out where in the world a photo was taken
- Google Earth/Maps/Street View, Land Registry, Snapchat/Instagram, Yandex - possibilities are endless
- Some things to think about:

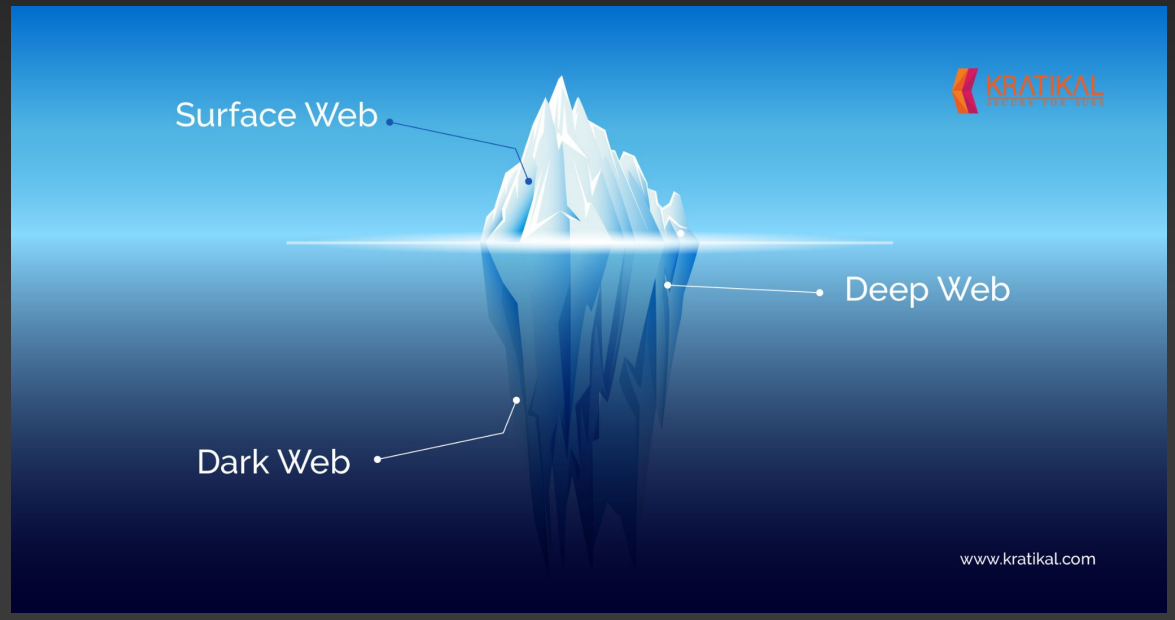
- Signs/Shop Names - can you google them? Can you reverse image search?
- What side of the road are people driving on?
- Anything that looks particularly unique?
- Any kind of blurry text - search all possibilities, ie ikarvs, ikarus
- Where did the image come from? Is this in itself a clue???
- **Never assume - confirm suspicions with proper evidence/another viewpoint**



https://www.osintcurio.us/2021/04/06/ten-minute-tip-image-geolocation-part-2/
https://medium.com/quiztime/how-to-tell-the-geolocation-of-places-based-on-old-sources-using-osint-a-case-study-e44e0faed388

Dark Web

- Most obvious use for this is cybercrime investigations
- In corporate world - dark web monitoring - checking for breaches

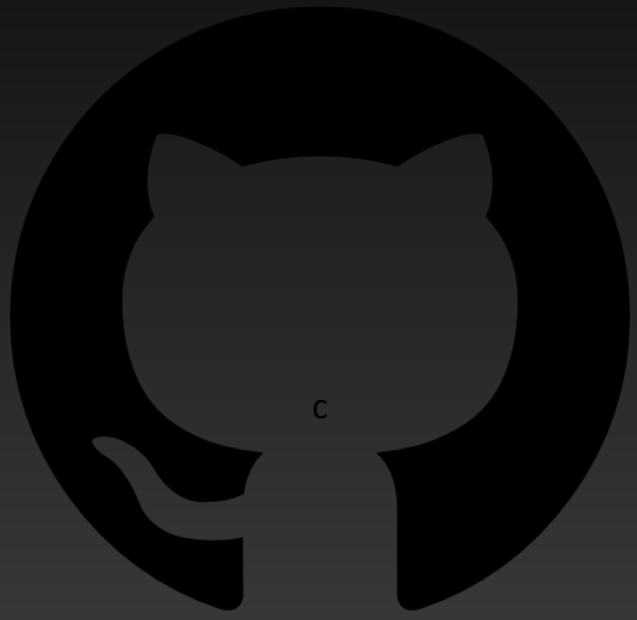


OSINT Tools

- A HUGE AMOUNT of tools on GitHub - have a play with some!
- Some of the more well-known ones:
- TheHarvester - finds emails, subdomains and more from a given domain
- Maltego - link analysis
- VirusTotal - file/URL checking
- Spiderfoot - similar to TheHarvester but on a larger scale

```
theharvester -d microsoft.com -l 500 -b google -h myresults.html
theharvester -d microsoft.com -b pgp
theharvester -d microsoft -l 200 -b linkedin
theharvester -d apple.com -b googleCSE -l 500 -s 300
```

Today's Task...



Can be found on the DMU Hackers GitHub under weekly_sessions\2023-2024\week_03\Tasks

OSINT Challenges:

https://github.com/DMUHackers/weekly_sessions/tree/master/2023-2024/week_03/tasks

Week 3: Introduction to OSINT

NON-IMAGE-RELATED:

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

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

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

EXIF:

1. What phone was this photo taken on?

2. What city was this photo taken in?

3. Which place was this photo taken?

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

NON-EXIF:

1. What is this an image of?

2. This image was taken outside a pub. Which pub was it? (The name as well as the chain)

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

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

4. Where is this pub located?

5. Where is this statue located?

EXTENSION CHALLENGE: Joey took this photo on a plane which originated from Dubai. Find the flight number as well as the name of the airport where the plane is about to land.

Answers and/or solutions are located inside the tasks folder

Resources

- exiftool
- whatsmyname.app username OSINT tool
- List of 'juicy' google search terms
- TryHackMe referral link
- OSINT Cheatsheet

- Geolocation - Example 1
- Geolocation - Example 2


PUB TIME
DRIVETRIBE