Ethical Student Hackers

OSINT



The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.

- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.

- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

- Relevant UK Law: https://www.legislation.gov.uk/ukpga/1990/18/contents



Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at https://shefesh.com/downloads/SESH%20Code%20of%20Conduct.pdf

EGM Time!

We’re looking for:

Treasurer

- Manage finances
- Apply for funding
- Handle reimbursements

General Member

- Run sessions
- Help out
- Have fun!

https://forms.gle/SR4s8BnqGikVfaMm7



OSINT - What is it?

Open **S**ource **Int**elligence - collection and analysis of data gathered from open sources (overt sources and publicly available information) to produce actionable intelligence

Malicious use:

- Cyber criminals
- Marketing
- Stalking

Protection use:

- Data protection
- Cybersecurity defense
- Finding missing people



Note: <u>Intelligence ≠ Information</u>

Information only becomes Intelligence when we look at it in a critical manner, analysed and given meaning

FAMOUS FAILURES (KIND OF)

Venmo public by default transactions.

Until 2021 all venmo payments were public by default.

This lead to many people accidentally sharing valuable information about themselves. For better or worse.

In 2018 a US congressman paid accused sex offender seemingly for prostitution.

Lime Scooters details are public and easy to access

Lime publishes the location, battery level and status of every available vehicle in a public feed that requires no authentication

Can reconstruct routes for particular scooters by watching this data



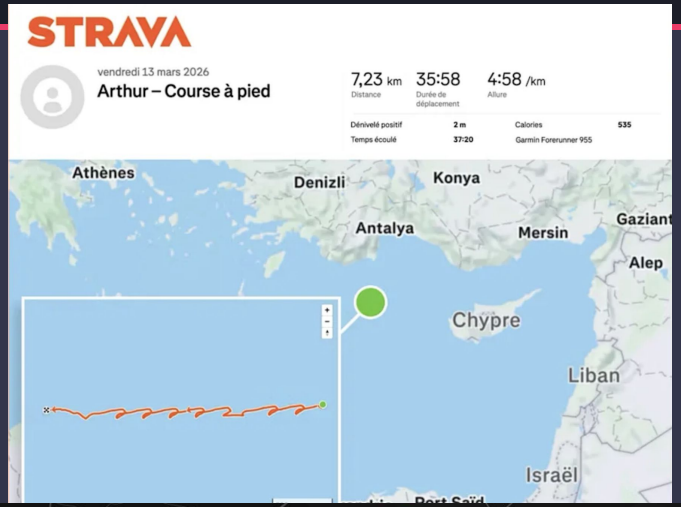
FAMOUS FAILURES

Strava heatmap failure

By default, strava runs ‘activities’ are publicly shown, paired with GPS data it can reveal sensitive locations

- French warship was revealed on its way to the Middle East because of one sailor’s strava run
- Location of secret military bases in Afghanistan revealed
- Locations of world leaders (Macron, Putin, Biden, etc) revealed by security team logging their runs

Even the most common of daily tasks can be used against you!





FAMOUS FAILURES (NOW WITH AI)

Hallucinated Nuclear Components on a Chinese ship

In September 2026, an AI-generated intelligence report nearly contributed to a US special operations raid on a Chinese merchant vessel travelling to Iran.

The AI had synthesised open source satellite imagery with classified signals intelligence, identifying the cargo as nuclear components for Iran's nuclear program.

AI is used by intelligence agencies to process information at speed and scale, but has a tendency to reinforce biases and validate incorrect information; very similar to how commercially available LLMs can spiral into "delusion" in order to validate user beliefs.





WHY?

OSINT allows us to monitor everything in real time completely **legally** and **ethically**.

In everyday life the information we empower ourselves with can give us the slight edge in such a media driven world. As well as verifying the authenticity of sources and info given by others.

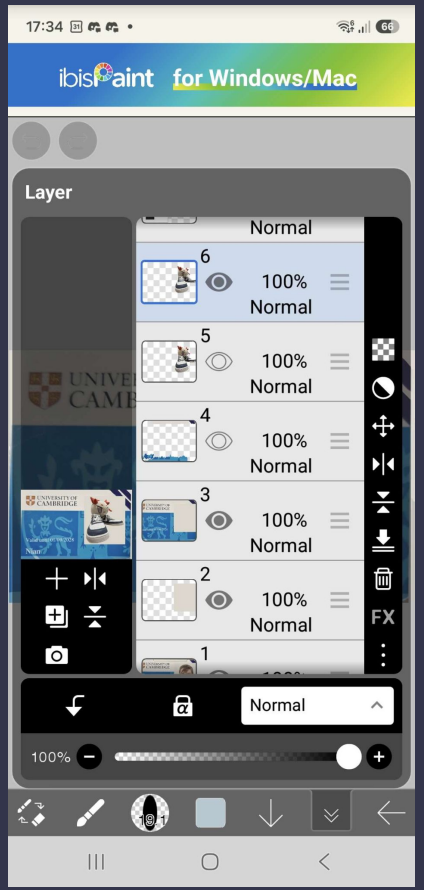
It equips us decision makers to make better, more informed decisions by monitoring and analyzing public opinions and sentiments.

As ethical hackers we can use OSINT to investigate potential security threats or vulnerabilities to prepare an attack.

It can also enhance traditional intelligence gathering which can prepare us for a social engineering attack and help us make better decisions later on in the attack.



Keycards


17:34
ibisPaint for Windows/Mac
Layer
Normal
6
100%
Normal
5
100%
Normal
4
100%
Normal
3
100%
Normal
2
100%
Normal
1
FX
Normal
100%


UNIVERSITY OF CAMBRIDGE
Valid until 01/09/2028
Nian

USEFUL WEBSITES/TECHNIQUES

https://archive.org/web/ - A wayback machine that allows us to view previous versions of websites

https://www.192.com/ - A UK based directory of People, businesses, electoral data and property info

Social media + search engines - Information about everyone + everything. Advanced search and filtering options can be particularly useful

Public records - Whois databases, financial records, government documents

Google Advanced Search - we'll cover this in a minute



PRACTICAL

DAVID BECKHAM.

1. What primary school did he attend
2. Where did he meet his partner?
3. Where was he on the 27th of March 2023?
4. What date + time did he purchase his website?



Clue

He didn't purchase the website himself - his agent at SFX sports did

ANSWERS

1. Chase Lane Primary School
2. Littlewood FA Charity Shield 1997
3. Mandarin Oriental - Geneva, Switzerland
4. 23rd of May 2002 at 10:47:24



You have to laugh at this move by the Green Party.

Back in 2015, andy4leader.co.uk was Andy Burnham's campaign website when he was fighting Jeremy Corbyn for the Labour leadership.

Fast forward to 2026, and the Greens have snapped up the old domain.

Now, instead of taking you to Burnham's leadership campaign, it takes you to a Green Party sign up page.

Imagine having your old leadership campaign website turned into a recruitment tool for your political rivals.

That is top tier political trolling.

> **Andy Burnham** @andyburnham · Aug 6, 2015
> Proud to launch A Radical Labour Vision for the 21st Century - my election manifesto - this morning. Read it here: andy4leader.co.uk/manifesto

Andy Burnham
@andyburnham

Proud to launch A Radical Labour Vision for the 21st Century - my election manifesto - this morning. Read it here:



From join.greenparty.org.uk

8:05 AM · Aug 6, 2015

Shodan

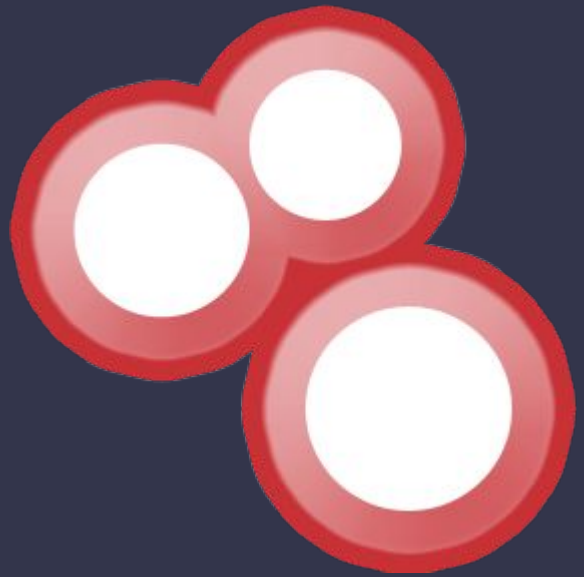
the world's first search engine for Internet-connected devices

Works by randomly finding IPs and testing a random port

Used by defenders to understand what's publically available

Shodan interacts with only services running on the devices

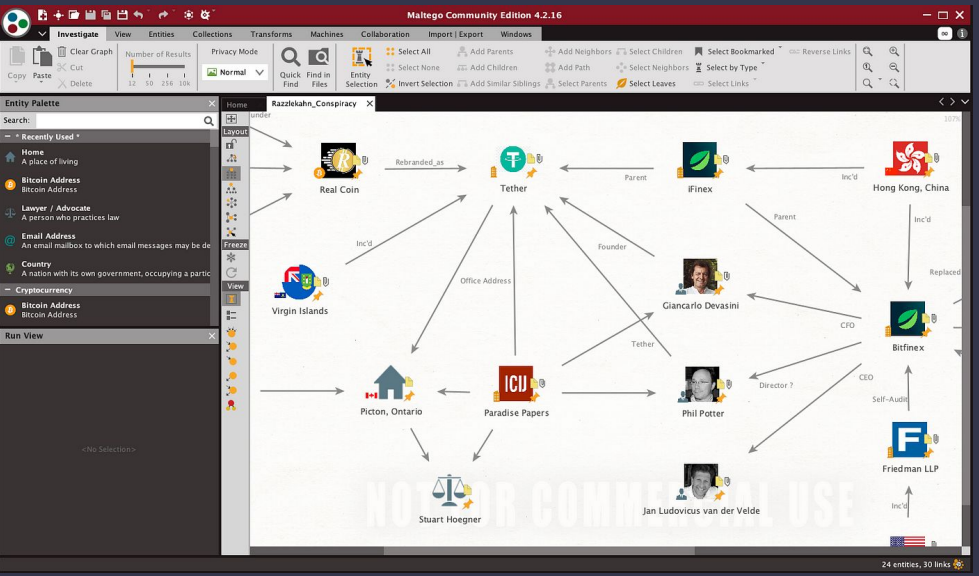
Helps identify vulnerable services



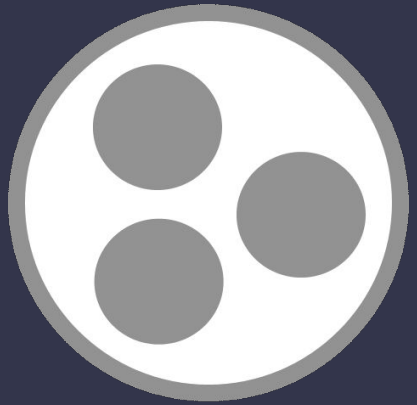
```
Copyright: Original Siemens Equipment
PLC name: S7_Turbine
Module type: CPU 313C
Unknown (129): Boot Loader           A
Module: 6ES7 313-5BG04-0AB0  v.0.3
Basic Firmware: v.3.3.8
Module name: CPU 313C
Serial number of module: S Q-D9U083642013
Plant identification:
Basic Hardware: 6ES7 313-5BG04-0AB0  v.0.3
```



Maltego

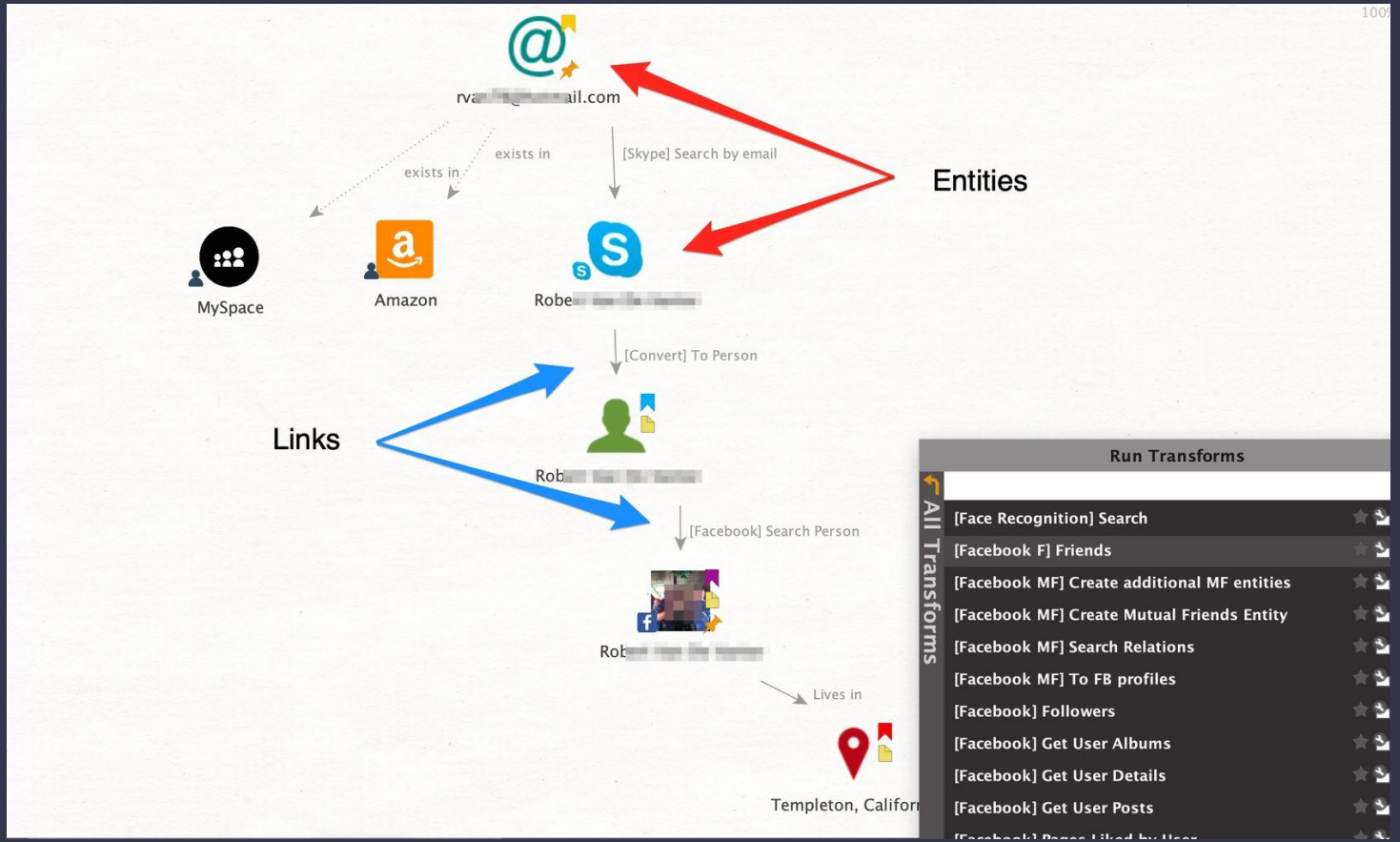


- Gathers data on an entities and **graphically represents relationships**
- Run functions on entities
- Create your own manually
- On kali



Example Functions

- Facebook search , Facebook friends
- whois lookup
- DNS lookup


rva[redacted]ail.com
exists in
exists in
[Skype] Search by email
Entities
MySpace
Amazon
Robe[redacted]
[Convert] To Person
Links
Rob[redacted]
[Facebook] Search Person
Rob[redacted]
Lives in
Templeton, Califor
Run Transforms
All Transforms
[Face Recognition] Search
[Facebook F] Friends
[Facebook MF] Create additional MF entities
[Facebook MF] Create Mutual Friends Entity
[Facebook MF] Search Relations
[Facebook MF] To FB profiles
[Facebook] Followers
[Facebook] Get User Albums
[Facebook] Get User Details
[Facebook] Get User Posts

Google Advanced Search

Taking advantage of advanced search features on google to find vulnerables indexed websites.

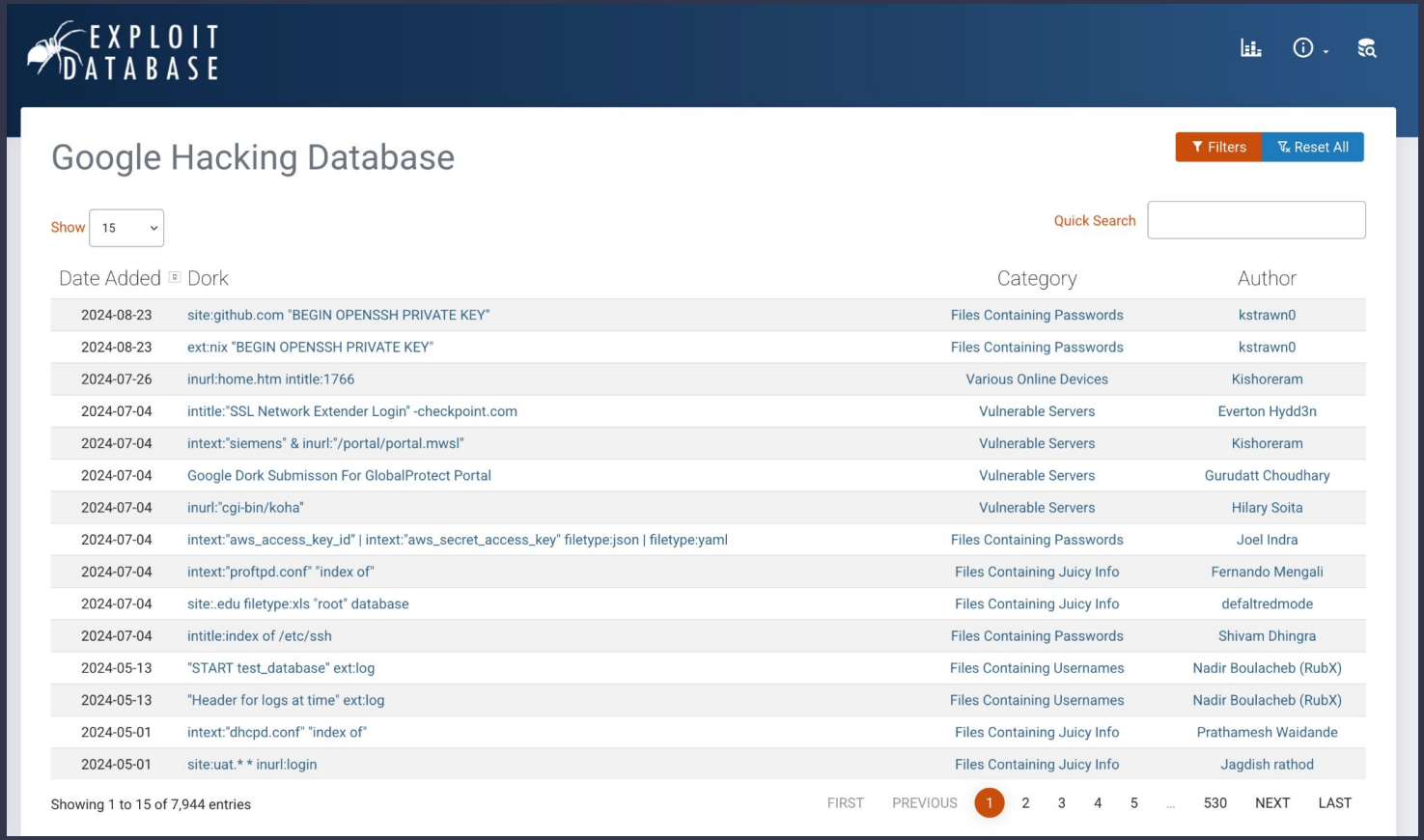
Examples:

Intitle:’login’ - pages with login in their title

Ext:.env - environment files (usually contain secret keys!)

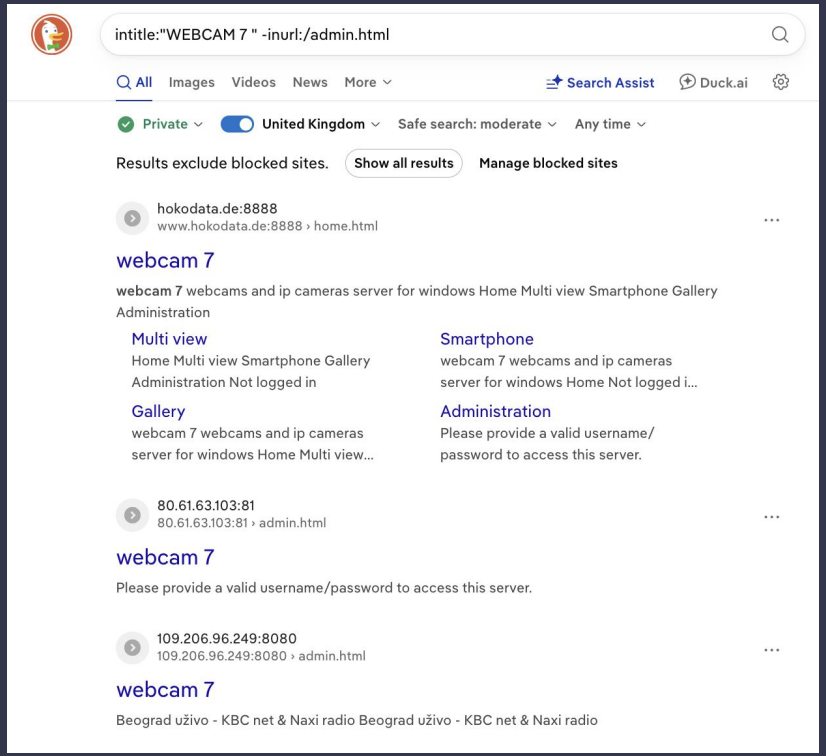


ExploitDB: Google Hacking





2020-05-18 intitle:"WEBCAM 7 " -inurl:/admin.html





DON'T BREAK THE LAW

Cheat Sheet

( )	Group a set of words/operators separately (gun | pistol) ammo
-	Exclude results including this word chicago baseball -cubs
$	Search for a certain price “apple watch” $299
cache:	Most recent cached version of a domain cache:boston.gov
filetype:	Only search for specific filetype, ext: works the same filetype:pdf “confidential” or ext:pdf “confidential”
related:	Search for sites related to a domain related:sony.com
intitle:	Find pages with a term in the page title intitle:sabotage
inurl:	Find pages with a term in the url inurl:private
around(x)	Find pages with terms in X words proximity of each other microsoft (7) surface
info:	Sometimes shows related pages, cache date etc. info:chicago.gov

Search operator	What it does	Example
" "	Search for results that mention a word or phrase.	"steve jobs"
OR	Search for results related to X or Y.	jobs OR gates
|	Same as OR:	jobs | gates
AND	Search for results related to X and Y.	jobs AND gates
-	Search for results that don't mention a word or phrase.	jobs -apple
filetype:	Search for particular types of files (e.g., PDF).	apple filetype:pdf
ext:	Same as filetype:	apple ext:pdf
site:	Search for results from a particular website.	site:apple.com
related:	Search for sites related to a given domain.	related:apple.com
before:	Search for results from before a particular date.	apple before:2007-06-29
after:	Search for results from after a particular date.	apple after:2007-06-29

Practical

Have a play around with Google advanced search / Exploit DB

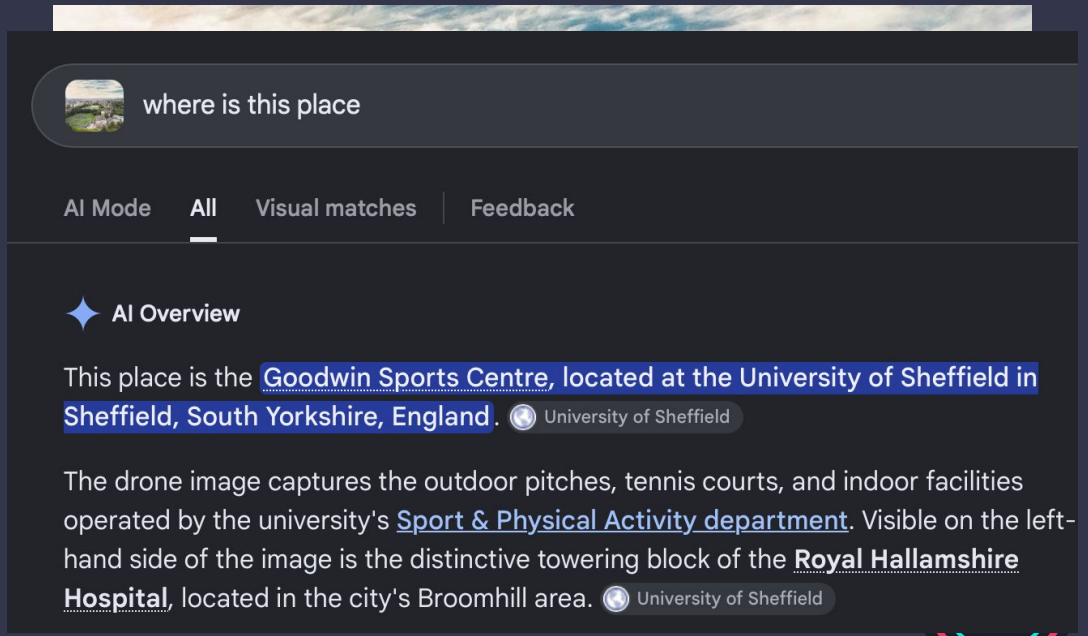
- Find out what information is out there about you
  - “<your name>” University of Sheffield

- Find some webcams / site secrets
  - Be careful what you click on
  - Do not start trying to guess passwords/credentials
    - This is what makes it illegal



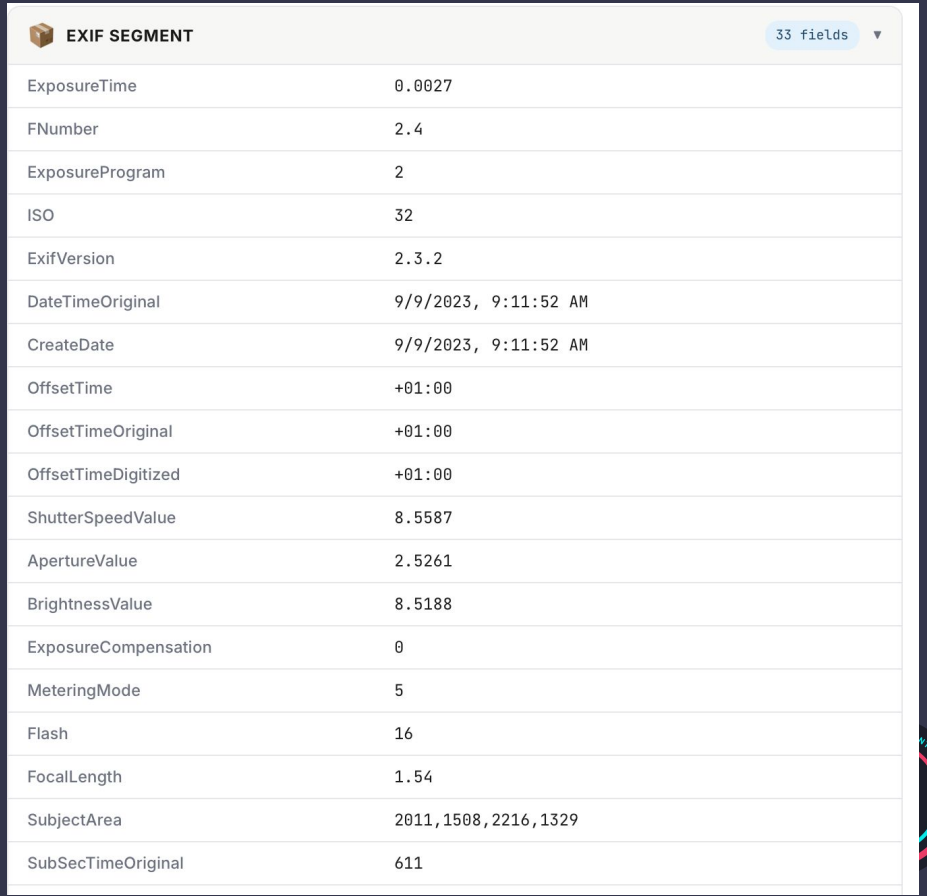
Images - Location

- Reverse image search to find the image
  - https://images.google.com/
  - https://tineye.com/
- Find similar images
  - Google lens
- Look for clues in the image
  - Signs
  - Buildings
  - Terrain
- Location **Metadata**



Images - Metadata

- What is metadata
- Types of data
  - How
  - Where
  - When
- Tools
  - Properties in photo viewer
  - Special tools (exiftool etc.)
  - Online tools



EXIF SEGMENT — 33 fields

ExposureTime	0.0027
FNumber	2.4
ExposureProgram	2
ISO	32
ExifVersion	2.3.2
DateTimeOriginal	9/9/2023, 9:11:52 AM
CreateDate	9/9/2023, 9:11:52 AM
OffsetTime	+01:00
OffsetTimeOriginal	+01:00
OffsetTimeDigitized	+01:00
ShutterSpeedValue	8.5587
ApertureValue	2.5261
BrightnessValue	8.5188
ExposureCompensation	0
MeteringMode	5
Flash	16
FocalLength	1.54
SubjectArea	2011,1508,2216,1329
SubSecTimeOriginal	611

Practical

https://shefesh.com/rp/picture_challenge_1.jpg - Where was this taken?

https://shefesh.com/rp/picture_challenge_2.jpg - Where was this taken?

https://shefesh.com/rp/picture_challenge_3.jpeg - What software was used to edit this?

https://shefesh.com/rp/picture_challenge_4.jpeg - When was this taken?

https://shefesh.com/rp/passport.png - What is the redacted information?

https://shefesh.com/rp/medical_form.pdf - What is the redacted information?

Finished Early? Try out these OSINT challenges: https://gralhix.com/list-of-osint-exercises/



Geoguessr

BIG GAME OF GEOGUESSR!!! (Kinda)



GO TO: https://openguessr.com/multiplayer/join



Useful resource

https://www.osintdojo.com/resources/

https://gralhix.com/list-of-osint-exercises/



Upcoming Sessions

What's up next?

www.shefesh.com/sessions

Any Questions?



www.shefesh.com

Thanks for coming!

