

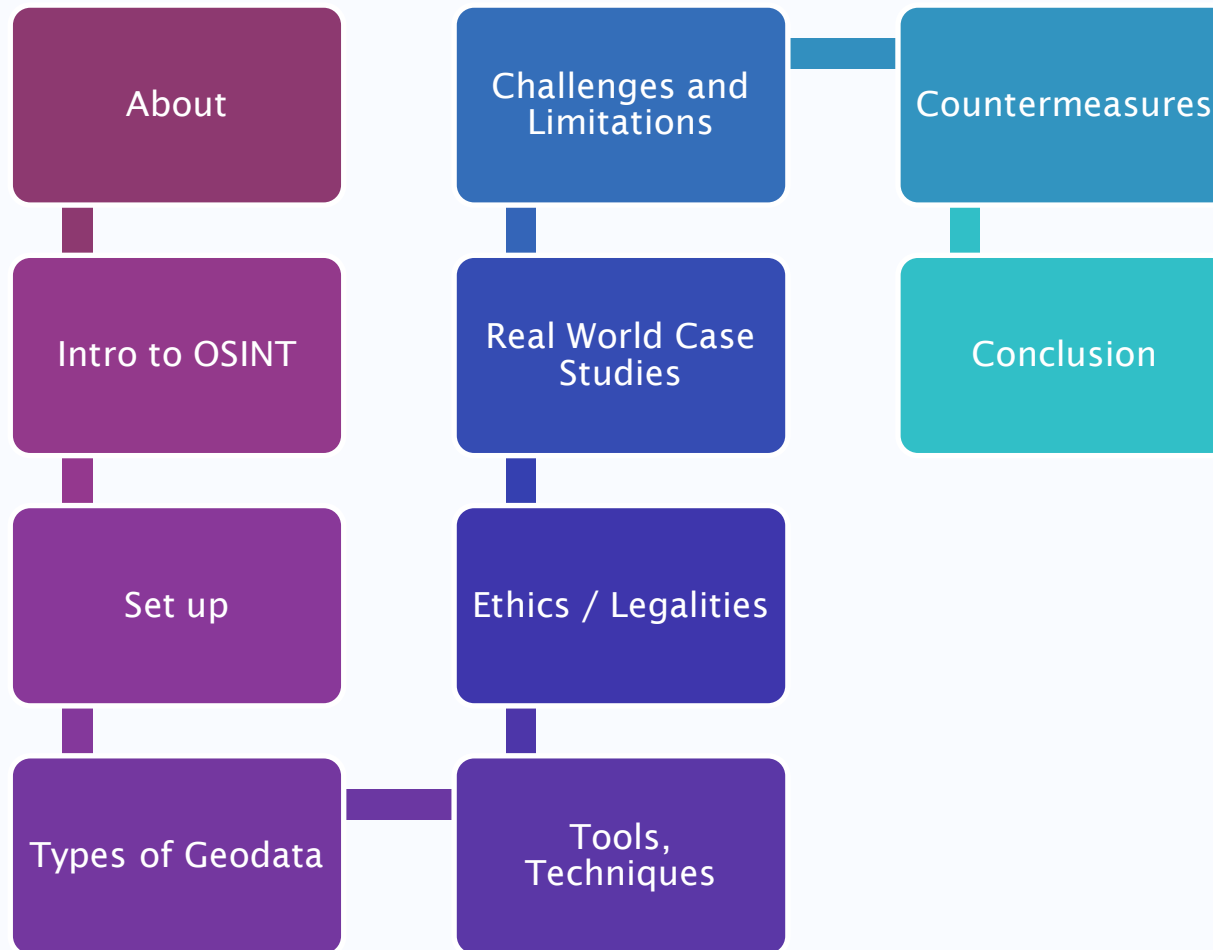
UNIVERSITY OF
Southampton

OSINT for GeoData

Professor Sarah Morris

2024 V.2

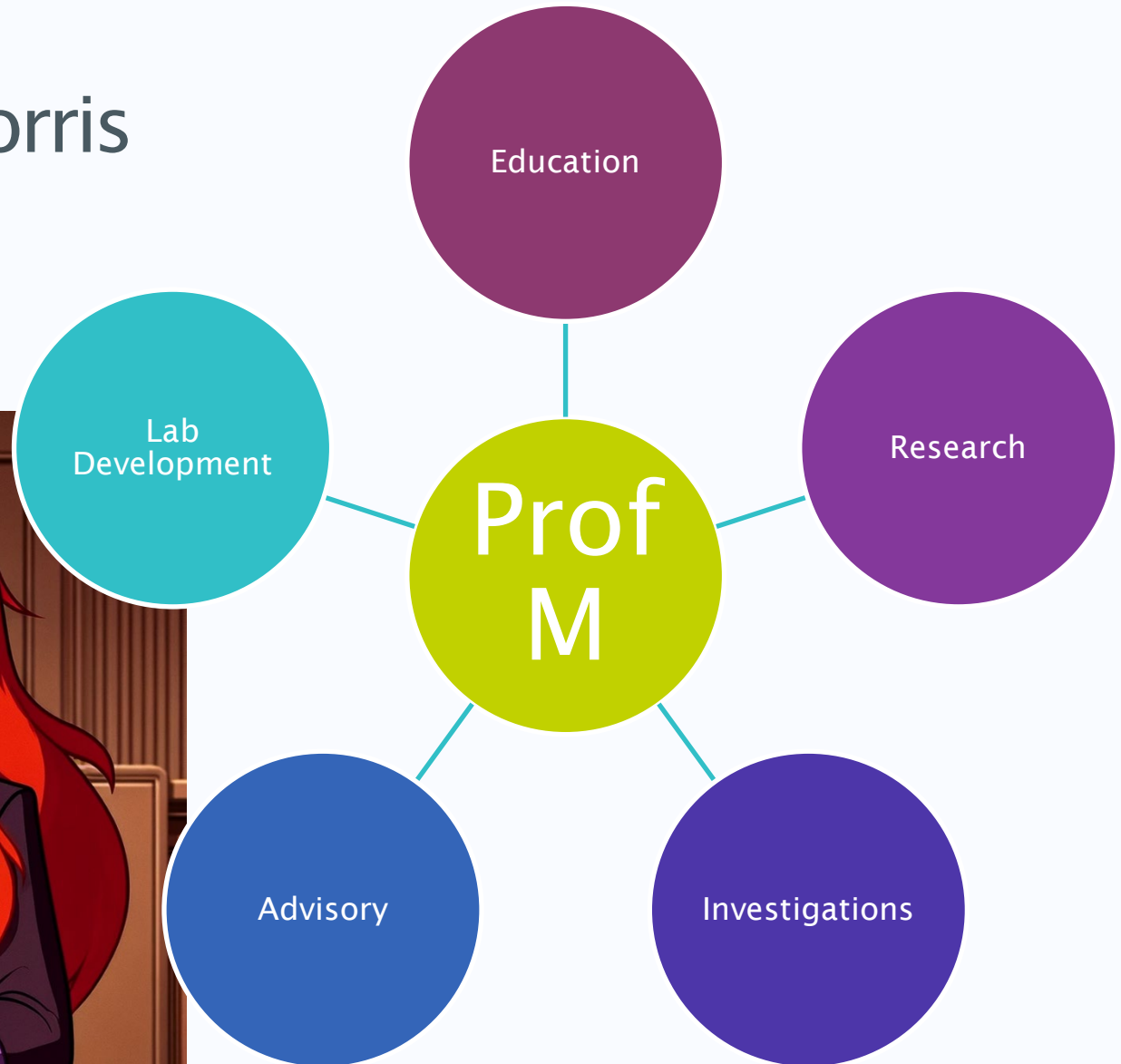
Things I plan* to cover



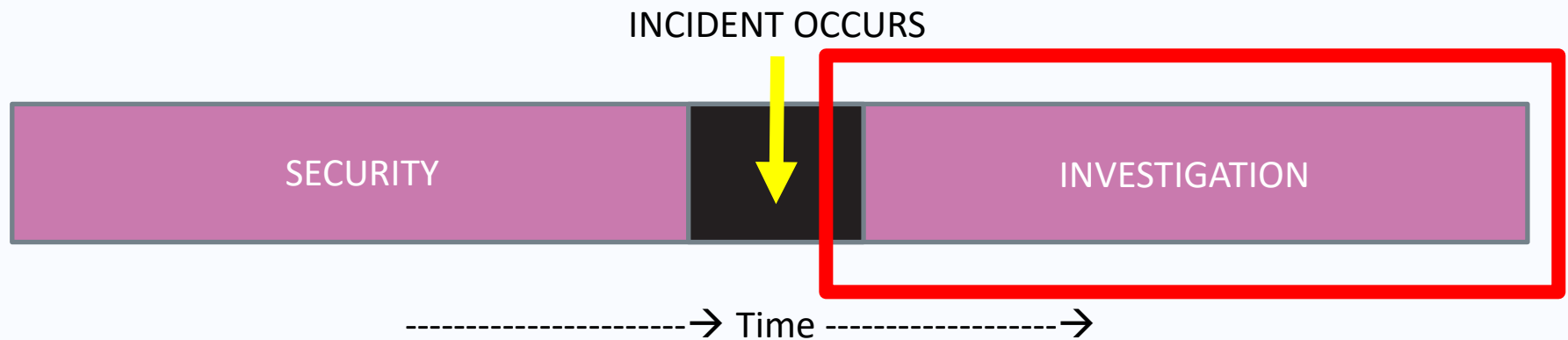
* According to the slides

About me

Prof. Sarah Morris



What is Digital Investigation?



OSINT for Geodata

What is OSINT?

- **Intelligence** produced from **publicly** available information
- **Collected, exploited, and disseminated** in a **timely** manner
- To an **appropriate** audience
- For the purpose of addressing a **specific** intelligence requirement.

Why?

Locate
something

Monitor
Environment

Track
Movement
and Patterns

Verify
Information

Identifying
Networks

Timelining

Cross
Referencing
data

Initial
intelligence

Incident
Response

Map to
Landscape

Trace Covert
/Anon
Activity

Applications

Law Enforcement

Investigative
Reporting

Military/Intelligence

Humanitarian Aid

Environmental
Monitoring

Corporate Security

Public Health

Urban Planning

Incident Response

Social Justice
Advocacy

BBC Home News Sport Weather iPlayer

NEWS

Home | InDepth | Israel-Gaza war | US election | Cost of Living | War in Ukraine


Business

Technology

Fitness app Strava lights up staff at military bases

🕒 29 January 2018

🔗



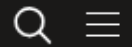
STRAVA

The movements of soldiers within Bagram air base - the largest US military facility in Afghanistan

<https://www.bbc.co.uk/news/technology-42853072>

Salisbury Poisoning Suspects

bellingcat



BellingChat Episode 3 - Hunting the The Salisbury Poisonings Suspects

June 16, 2020
Novichok Russia

The new BBC series [The Salisbury Poisonings](#) tells the story of the impact of the Skripal assassination attempt on the people of Salisbury, but what do we know about the two suspects identified by UK authorities? Bellingcat's Christo Grozev explains the work he did to reveal the true identities of the Skripal suspects, how he identified their commanders, and how that connected to other Russian spy operations, from assassination to coup attempts, across Europe.

<https://www.bellingcat.com/resources/podcasts/2020/06/16/bellingchat-episode-3-hunting-the-the-salisbury-poisonings-suspects/>



← → ↻ missingpersonshackathon.com.au ☆ 🌐 📄 📱 📧 📞

NATIONAL MISSING PERSONS HACKATHON 2024

HOW IT WORKS
2024 EVENT
2020 EVENT
2019 EVENT
CONTACT & FAQS

REGISTRATION OPENS
5 JULY 2024

WEBSITE POWERED BY
 **CYGENUS**

**EVENT START
13 SEP 2024**

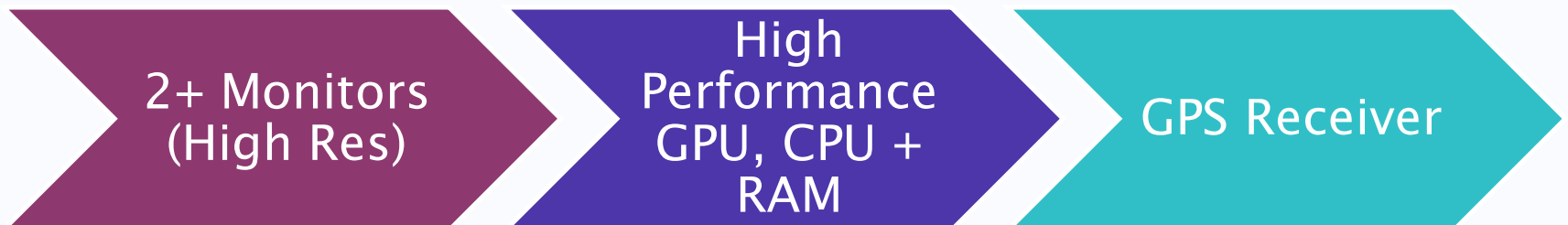
00:02:05:55:25
0 weeks, 2 days, 5 hours, 55 minutes, 25 seconds left

THE NATIONAL MISSING PERSONS HACKATHON HAS RETURNED FOR 2024

Join other ethical hackers and investigators to gather open source intelligence and find new leads on real missing person cases.

Setting up your OSINT Station

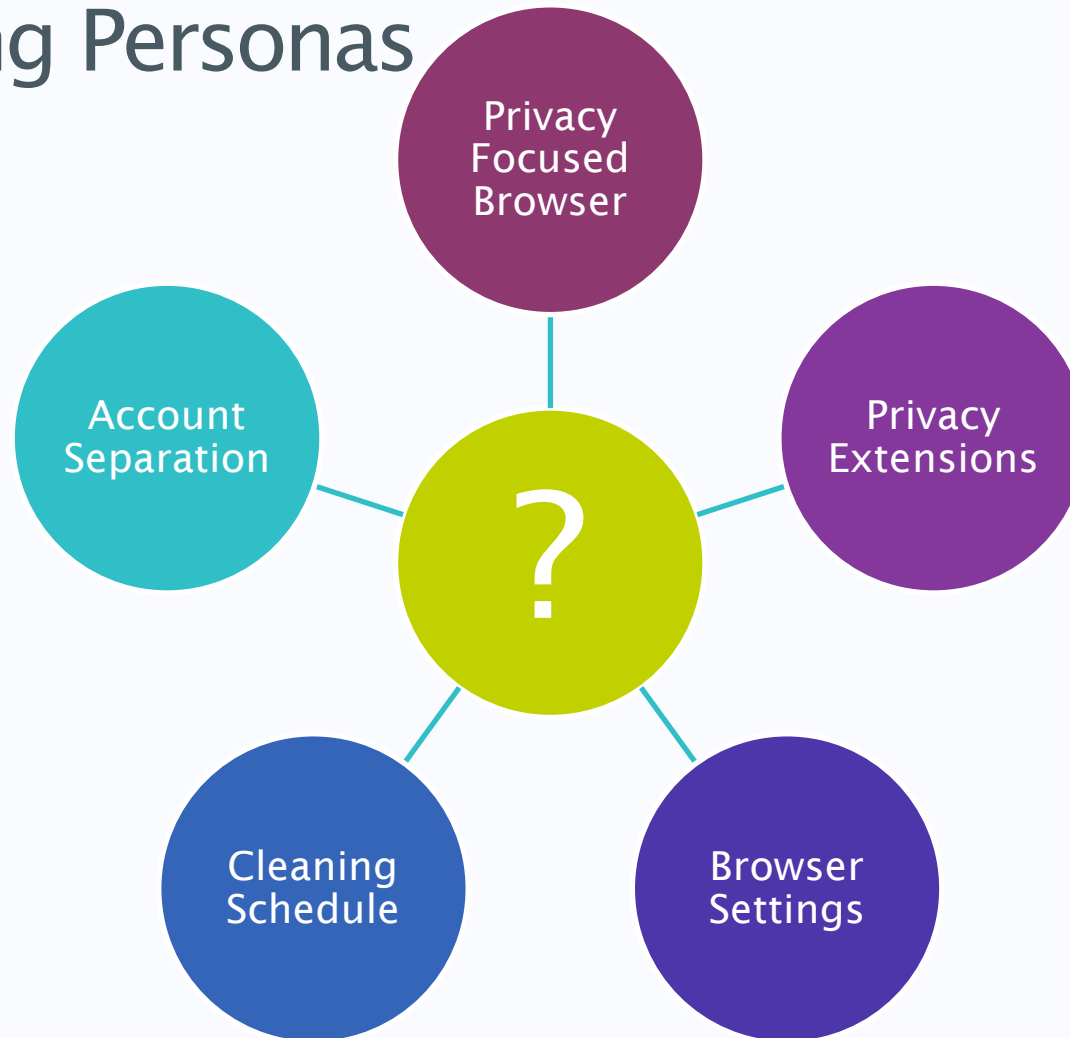
Hardware Considerations



Software



Managing Personas



Anonymous?



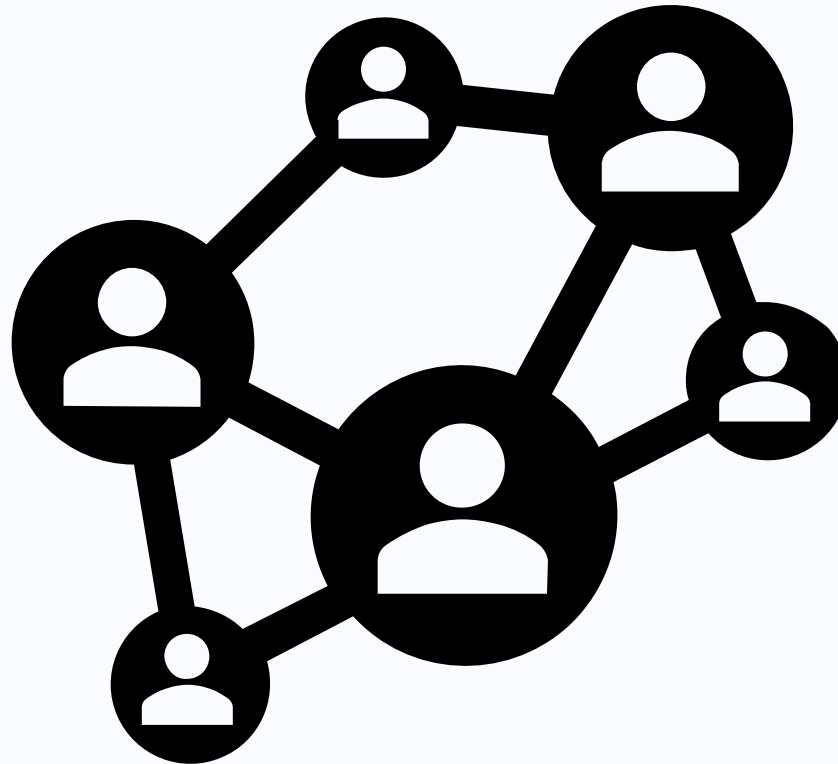
Good Practice

- Clean System
- Clean Accounts
- Regular sanitisation
- Clean link (VPN / separate from normal network)
- Test Sources
- Take Notes!!! (Repeatable, safety!)

Good Practice - Safety

- Notes!
 - Accidents happen
 - Things appear
 - Welfare policy
 - Containment/notification policy
 - Lab protection policy

When it goes wrong



Types of Geodata

Raw Geo Data for Digital Investigations

Mobile & Network

GPS Data

Cell Tower
Triangulation

Wi-Fi Access Points

IP Geolocation

Public Transport

Mobile Payment

Device & Sensor

Vehicle Telematics

Drone Logs

Smartwatch/Health
Trackers /
Wearables

Bluetooth / wireless
data

IoT Device Location

Handheld Device

Media & Social

Geotagging

Location / Check in
Data

IP / Connection
Data

Aerial & Satellite

Satellite Imagery

Drone GPS

Travel

Airline

Public Transport

Vehicle Tracking
Systems

Phone Connection
Data

Smart Wearable
Data

Processed / Prepared

Records

Open
Mapping
Platforms

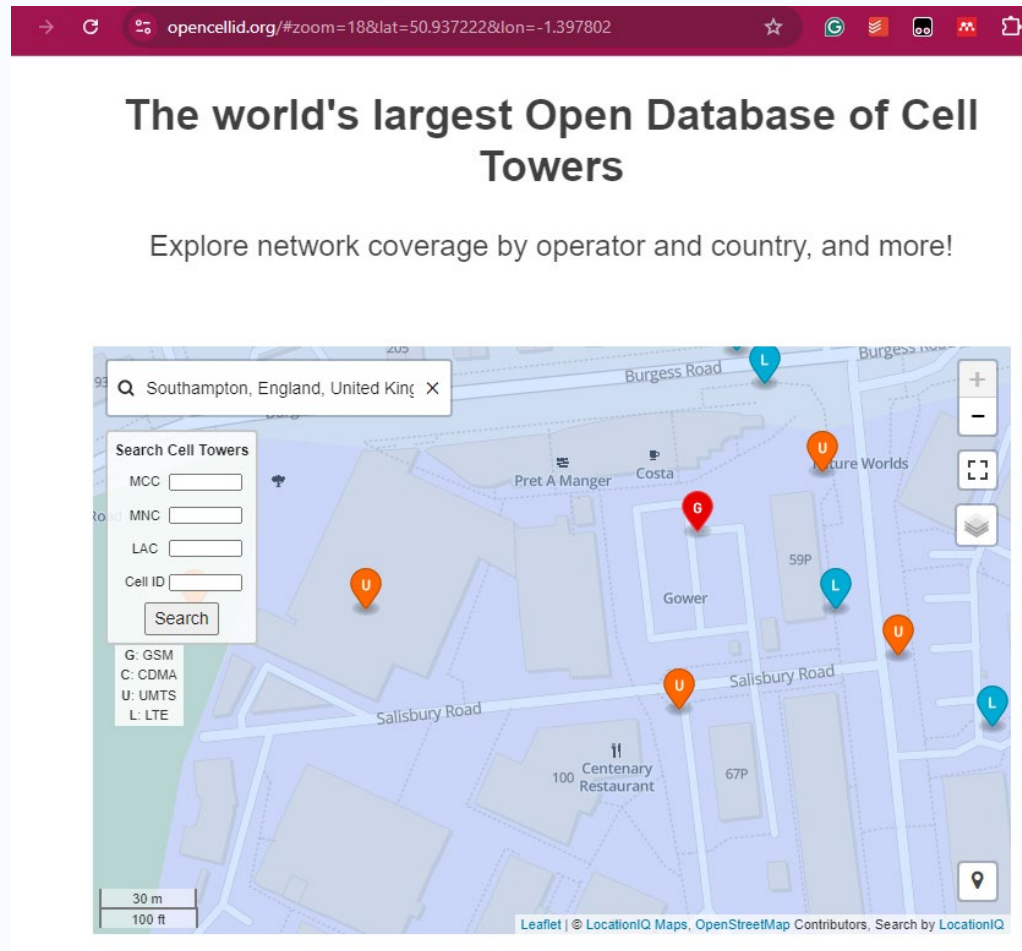
Crowdsourcing

Data Breach
/ Leaks

OSINT Techniques for Geodata Collection

Online Services

Opencellid.org



<https://www.opencellid.org/#zoom=18&lat=50.937222&lon=-1.397802>

Opencellid.org

Search Cell Towers

MCC

MNC

LAC

Cell ID

Search

<p>MMC</p> <p>Mobile Country Code</p> <p>UK 234 USA 310</p>	<p>MNC</p> <p>Mobile Network Code</p> <p>Vodafone UK 15 02 Germany 03</p>
<p>LAC</p> <p>Location Area Code</p> <p>Cluster of Cell Towers</p>	<p>Cell ID</p> <p>Cell Identifier</p> <p>Unique Tower ID</p>

GPS Data

ExifTool by Phil Harvey
Read, Write and Edit Meta Information!

Also available --> [Utility to fix Nikon NEF images corrupted by Nikon software](#)

Note: IP's that aggressively download multiple copies of the distribution files or access web pages too quickly will be blocked.

Installing	Tag Names	Resources	History	Forum	FAQ
------------	-----------	-----------	---------	-------	-----

[Download Version 12.96 \(7.1 MB\) - Sept. 1, 2024](#)

ExifTool is a platform-independent [Perl library](#) plus a [command-line application](#) for reading, writing and editing meta information in a [wide variety of files](#). ExifTool supports many different metadata formats including [EXIF](#), [GPS](#), [IPTC](#), [XMP](#), [JFIF](#), [GeoTIFF](#), [ICC Profile](#), [Photoshop IRB](#), [FlashPix](#), [ACF](#) and [ID3](#), [Lyrics3](#), as well as the maker notes of many digital cameras by [Canon](#), [Casio](#), [DJI](#), [FLIR](#), [FujiFilm](#), [GE](#), [GoPro](#), [HP](#), [JVC/Victor](#), [Kodak](#), [Leaf](#), [Minolta/Konica-Minolta](#), [Motorola](#), [Nikon](#), [Nintendo](#), [Olympus/Epson](#), [Panasonic/Leica](#), [Pentax/Asahi](#), [Phase One](#), [Reconyx](#), [Ricoh](#), [Samsung](#), [Sanyo](#), [Sigma/Foveon](#) and [Sony](#).

ExifTool is also available as a **Windows executable** and a **MacOS package**: (Note that these versions contain the executable only, and do not include the HTML documentation or other files of the full distribution above.)

Windows

32-bit: [exiftool-12.96_32.zip](#) (10.8 MB)
64-bit: [exiftool-12.96_64.zip](#) (10.6 MB)

The Windows executable archives include Perl. Just download and un-zip the appropriate archive then double-click on "exiftool(-k).exe" to read the application documentation, drag-and-drop files and folders to view meta information, or rename to "exiftool.exe" for command-line use. Note that if you move the .exe to another folder, you **must also move the "exiftool_files" folder** to the same location.

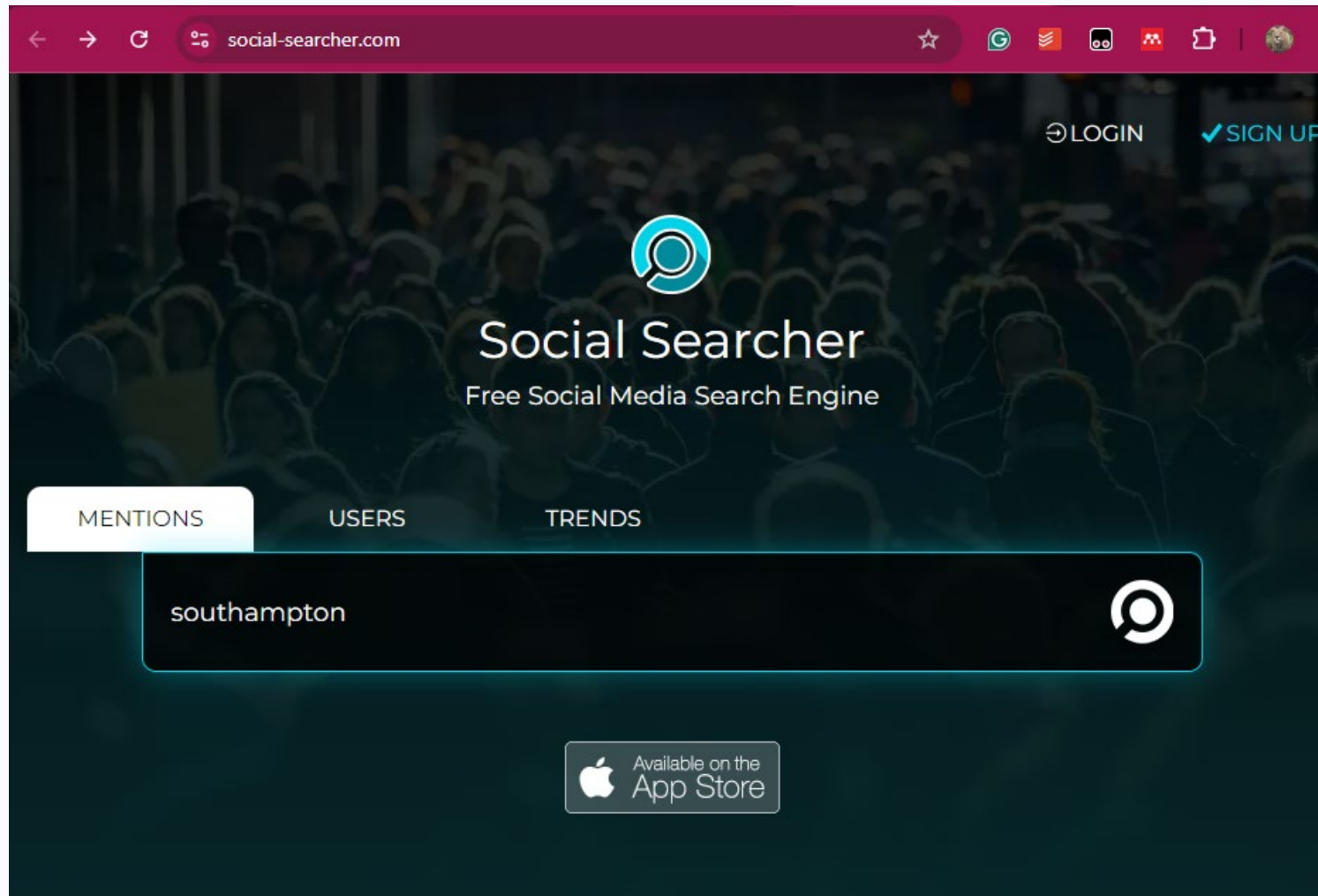
(The Windows packages are based on work by Oliver Betz, and use his launcher. [Oliver also provides self-installing versions of these executables](#). See [this forum post](#) if you have any problems/comments with these versions.)

MacOS Package: [ExifTool-12.96.pkg](#) (5.1 MB)

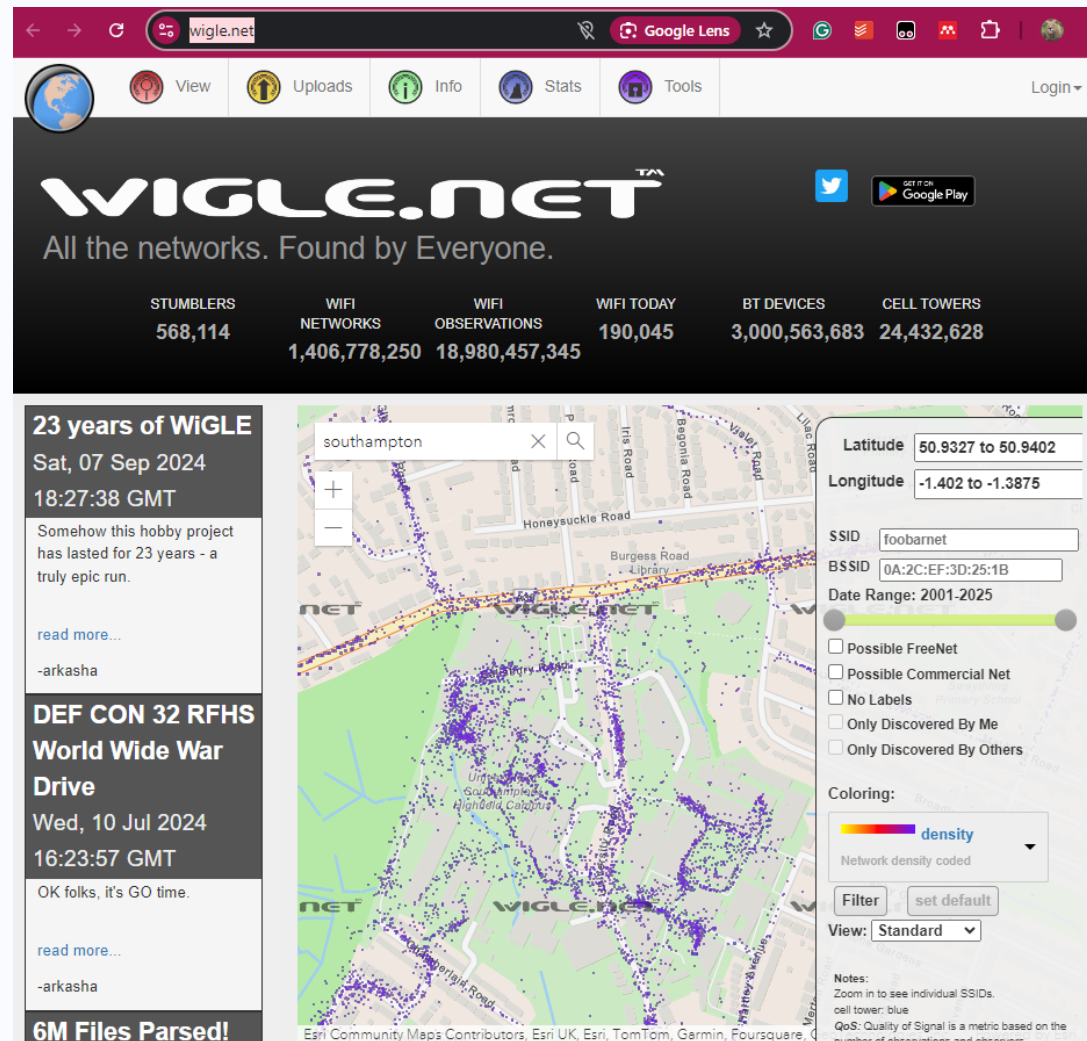
[Features](#)
[User Comments](#)
[Supported File Types](#)
[System Requirement](#)
[Running ExifTool](#)
[Example Output](#)
[Tag Names Explainer](#)
[Tag Groups](#)
[Writing Information](#)
[Writer Limitations](#)
[Known Problems](#)
[Security Issues](#)
[Date/Time Shift](#)
[Renaming Files](#)
[Performance](#)
[ExifTool Library](#)
[Additional Resources](#)
[New Discoveries](#)
[Acknowledgements](#)
[License](#)
[Donate](#)
[Background](#)
[Contact Me](#)

<https://exiftool.org/>

Social Searcher



Wigle.net



<https://wigle.net/>

IP Info

The screenshot shows the IPinfo.io website. At the top is a dark red browser bar with navigation icons and the URL 'ipinfo.io'. Below this is a light green banner with the text 'Explore our IP Address Database Downloads for instant access to our IP address insights' and a green 'Learn more' button. The main header features the IPinfo logo on the left and a navigation menu with links for 'Products', 'Solutions', 'Why IPinfo?', 'Pricing', 'Resources', and 'Docs', followed by a hamburger menu icon. The main content area has a large heading 'The Trusted Source For IP Address Data' and a subtext 'Accurate IP address data that keeps pace with secure, specific, and forward-looking use cases.' Below this are two buttons: 'Sign up for free' (blue) and 'Contact sales' (light blue). At the bottom is a dark blue search bar containing the IP address '82.30.50.19' and a magnifying glass icon.

ipinfo.io

Explore our IP Address Database Downloads for instant access to our IP address insights

[Learn more](#)

IPinfo Products Solutions Why IPinfo? Pricing Resources Docs

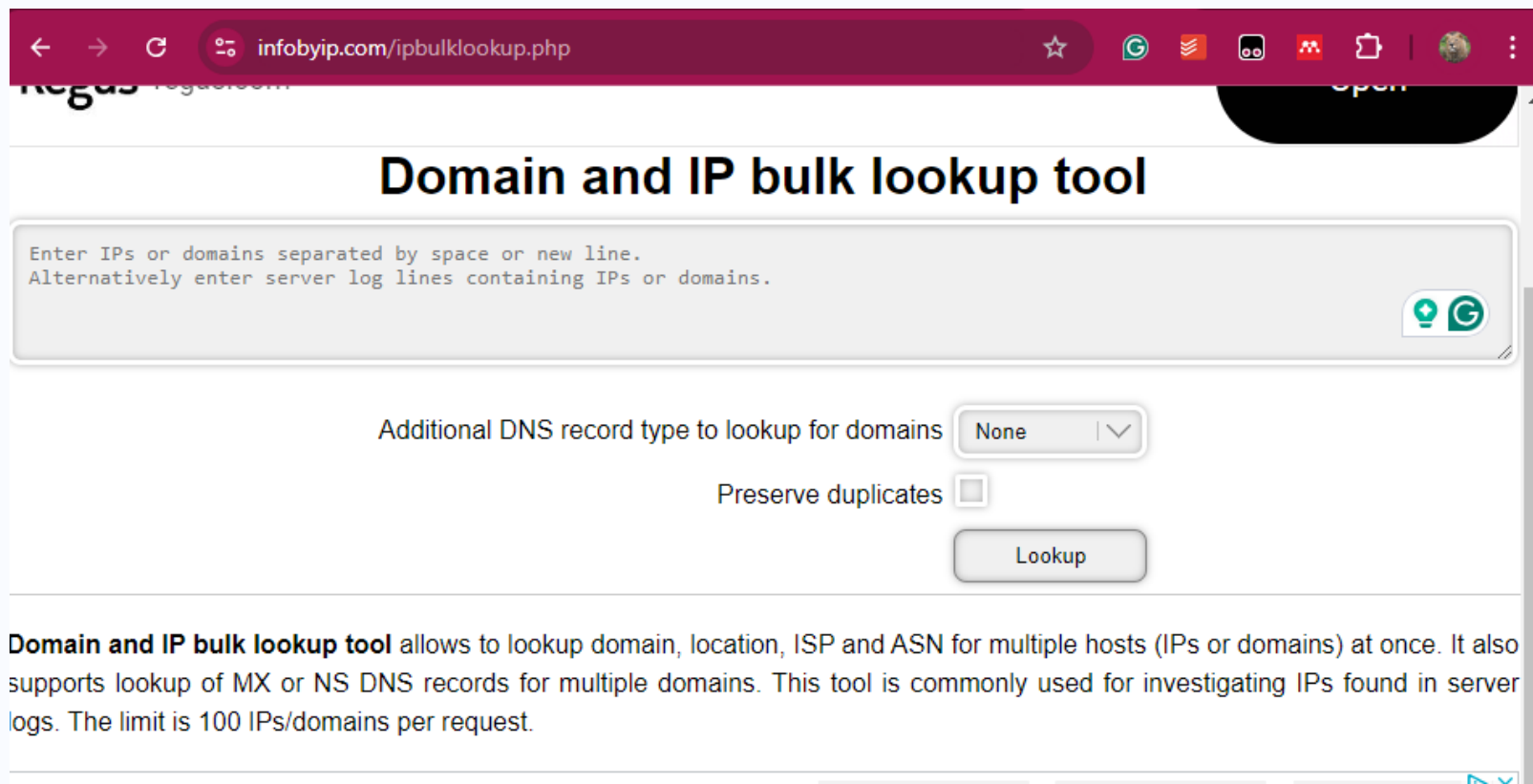
The Trusted Source For IP Address Data

Accurate IP address data that keeps pace with secure, specific, and forward-looking use cases.

[Sign up for free](#) [Contact sales](#)

82.30.50.19

IP Bulk Lookup



The screenshot shows a web browser window with the address bar displaying `infobyip.com/ipbulklookup.php`. The page title is "Domain and IP bulk lookup tool". Below the title is a large text input field with placeholder text: "Enter IPs or domains separated by space or new line. Alternatively enter server log lines containing IPs or domains." To the right of the input field is a small icon of a lightbulb and a green circle. Below the input field are two options: "Additional DNS record type to lookup for domains" with a dropdown menu set to "None", and "Preserve duplicates" with an unchecked checkbox. A "Lookup" button is positioned below these options. At the bottom of the page, there is a paragraph of text describing the tool's functionality and a limit of 100 IPs/domains per request.

Domain and IP bulk lookup tool

Enter IPs or domains separated by space or new line.
Alternatively enter server log lines containing IPs or domains.

Additional DNS record type to lookup for domains None

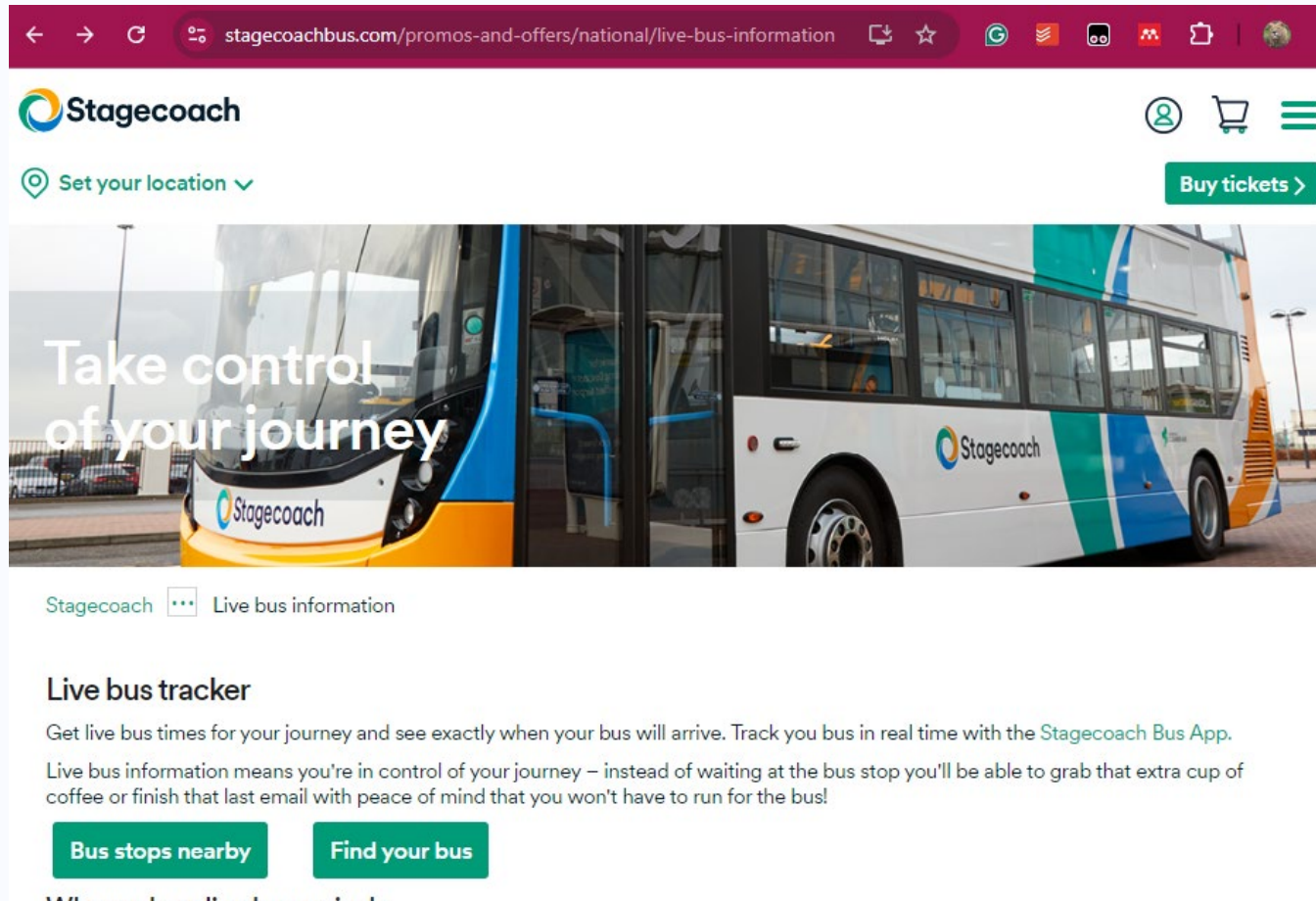
Preserve duplicates ☐

Lookup

Domain and IP bulk lookup tool allows to lookup domain, location, ISP and ASN for multiple hosts (IPs or domains) at once. It also supports lookup of MX or NS DNS records for multiple domains. This tool is commonly used for investigating IPs found in server logs. The limit is 100 IPs/domains per request.

<https://www.infobyip.com/ipbulklookup.php>

Individual Travel Apps



The screenshot shows the Stagecoach website's 'Live bus information' page. The browser address bar displays 'stagecoachbus.com/promos-and-offers/national/live-bus-information'. The Stagecoach logo is in the top left, and navigation icons (user profile, shopping cart, menu) are in the top right. A 'Set your location' dropdown and a 'Buy tickets >' button are also visible. The main banner features a Stagecoach bus with the text 'Take control of your journey'. Below the banner, a breadcrumb trail reads 'Stagecoach > Live bus information'. The section is titled 'Live bus tracker' and includes a paragraph about the Stagecoach Bus App. Two green buttons, 'Bus stops nearby' and 'Find your bus', are present. The text 'Where have live bus arrivals' is partially visible at the bottom.

stagecoachbus.com/promos-and-offers/national/live-bus-information

Stagecoach

Set your location ▾

Buy tickets >

Take control of your journey

Stagecoach

Stagecoach > Live bus information

Live bus tracker

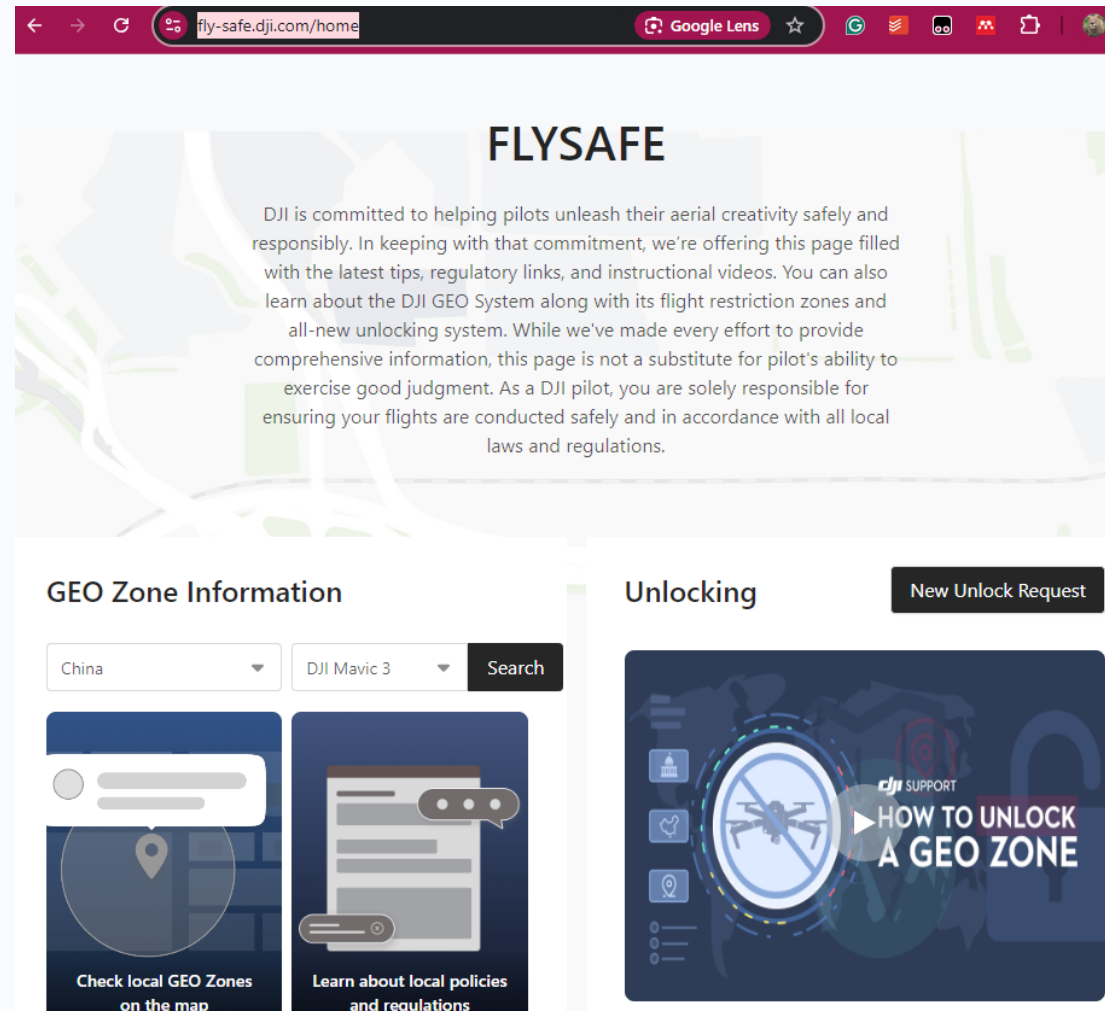
Get live bus times for your journey and see exactly when your bus will arrive. Track your bus in real time with the [Stagecoach Bus App](#).

Live bus information means you're in control of your journey – instead of waiting at the bus stop you'll be able to grab that extra cup of coffee or finish that last email with peace of mind that you won't have to run for the bus!

Bus stops nearby Find your bus

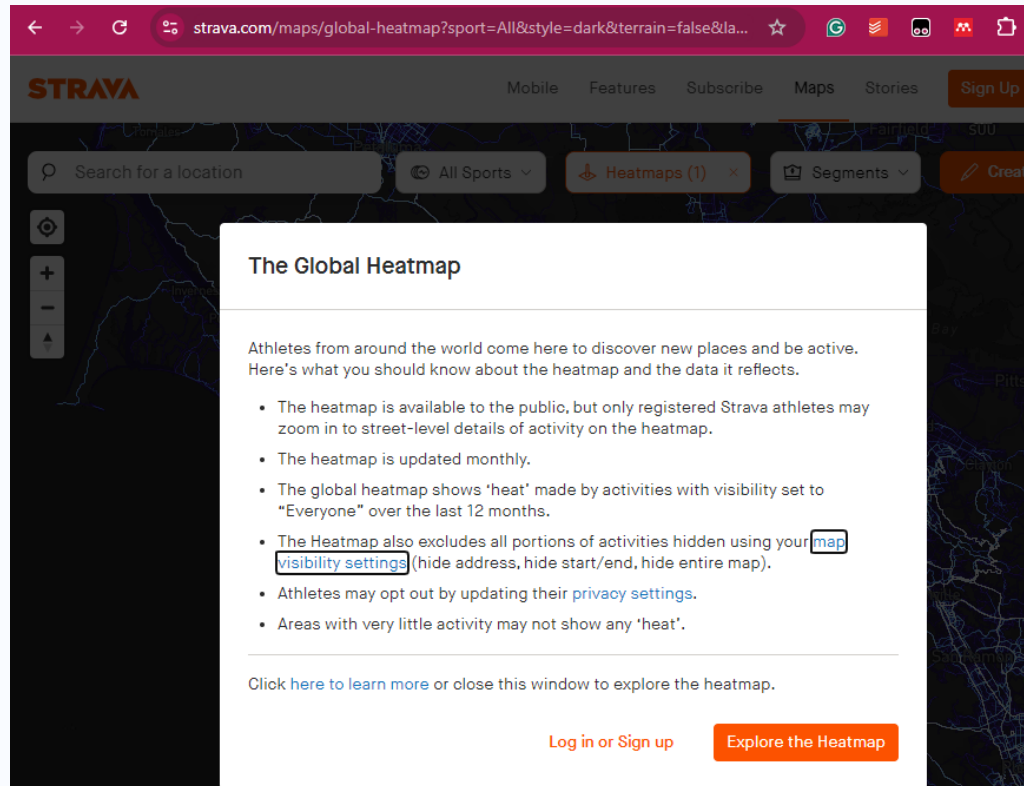
Where have live bus arrivals

DJI Flysafe



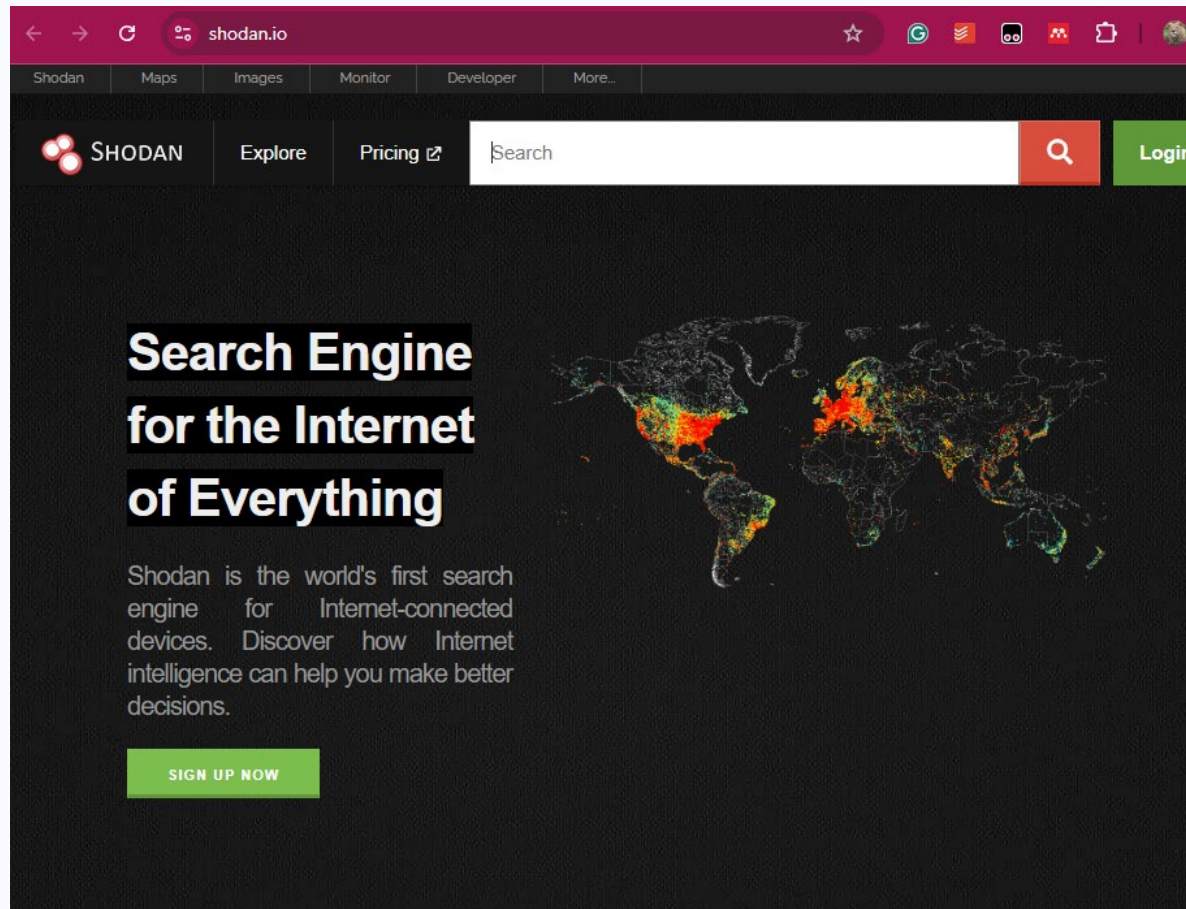
<https://fly-safe.dji.com/home>

Strava Wearable Heatmap



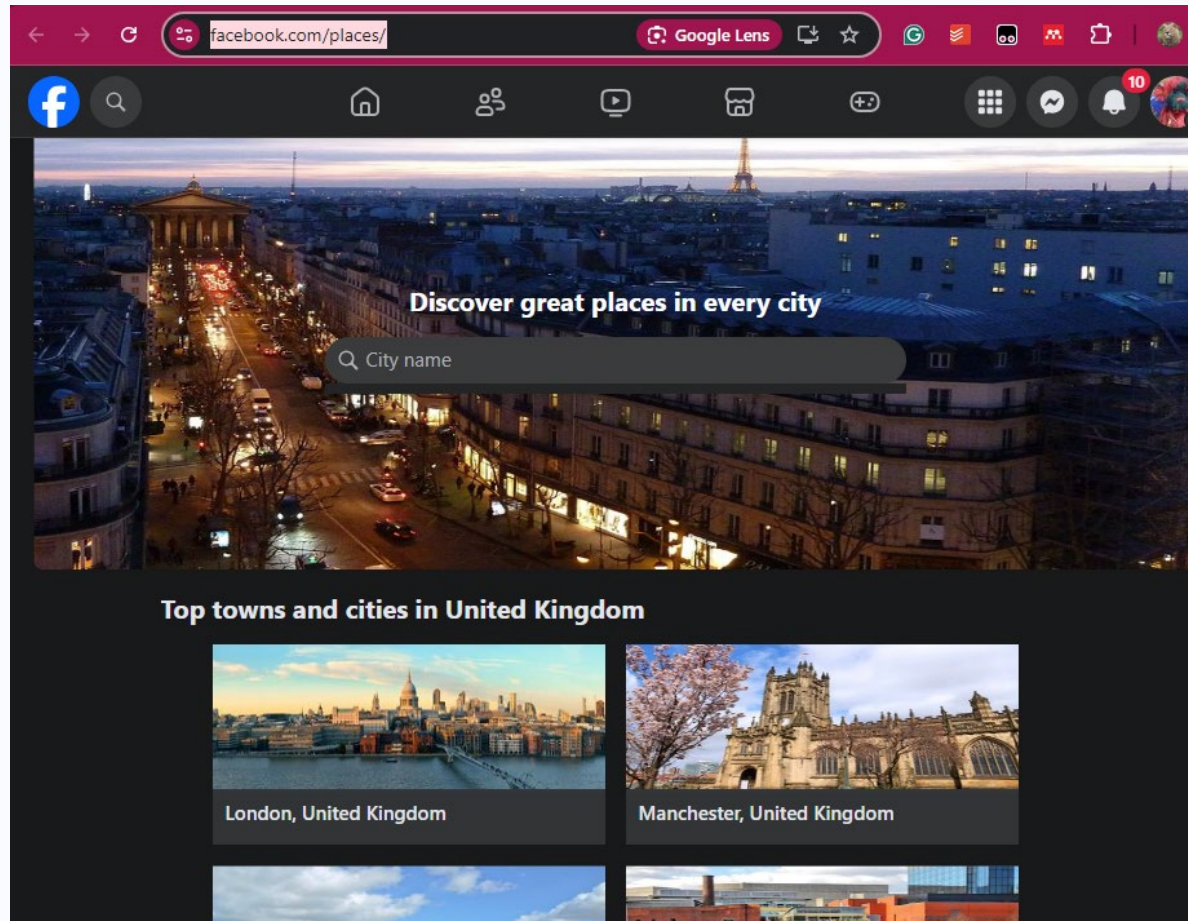
<https://www.strava.com/maps/global-heatmap>

Shodan



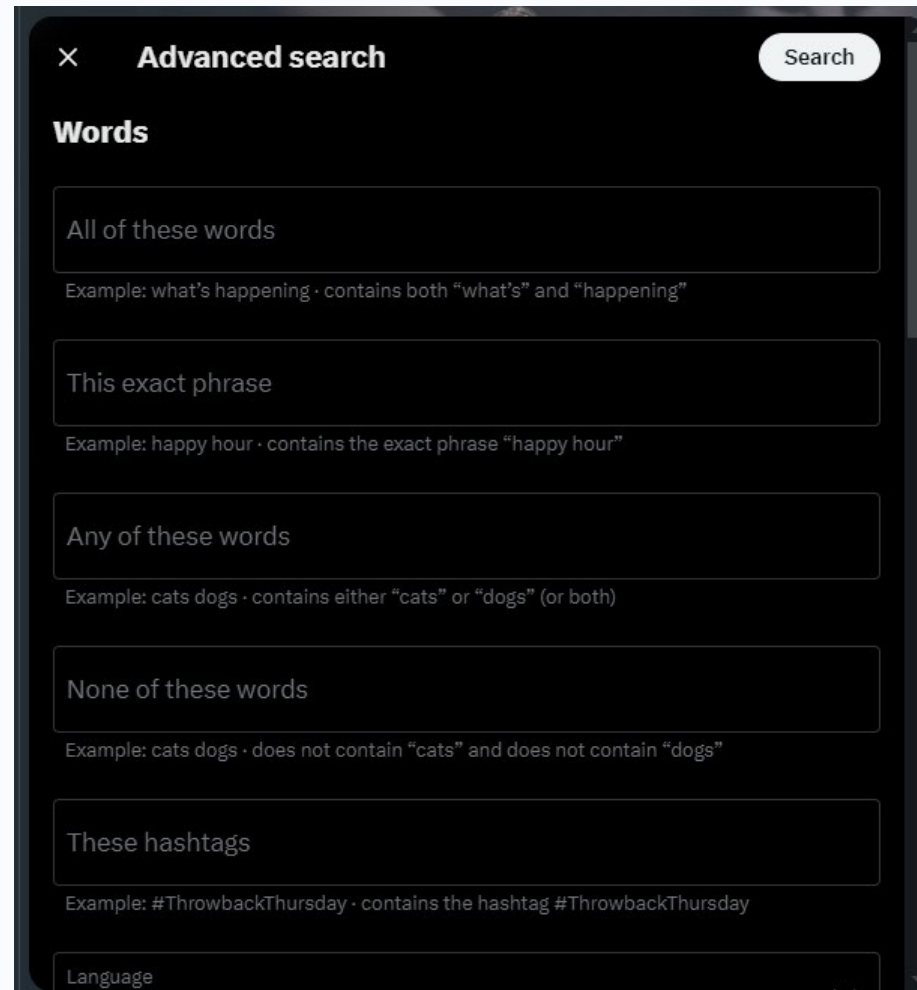
<https://www.shodan.io/>

Social Media Places



<https://www.facebook.com/places/>

X Advanced Search



The screenshot shows the 'Advanced search' modal on the X platform. It features a dark theme with a white 'Search' button in the top right corner. The modal is titled 'Advanced search' with a close button (X) on the left. Below the title, the section 'Words' is highlighted. There are five search criteria options, each with a text input field and an example: 1. 'All of these words' with example 'what's happening · contains both "what's" and "happening"'. 2. 'This exact phrase' with example 'happy hour · contains the exact phrase "happy hour"'. 3. 'Any of these words' with example 'cats dogs · contains either "cats" or "dogs" (or both)'. 4. 'None of these words' with example 'cats dogs · does not contain "cats" and does not contain "dogs"'. 5. 'These hashtags' with example '#ThrowbackThursday · contains the hashtag #ThrowbackThursday'. At the bottom, there is a 'Language' filter option.

× **Advanced search** Search

Words

All of these words
Example: what's happening · contains both "what's" and "happening"

This exact phrase
Example: happy hour · contains the exact phrase "happy hour"

Any of these words
Example: cats dogs · contains either "cats" or "dogs" (or both)

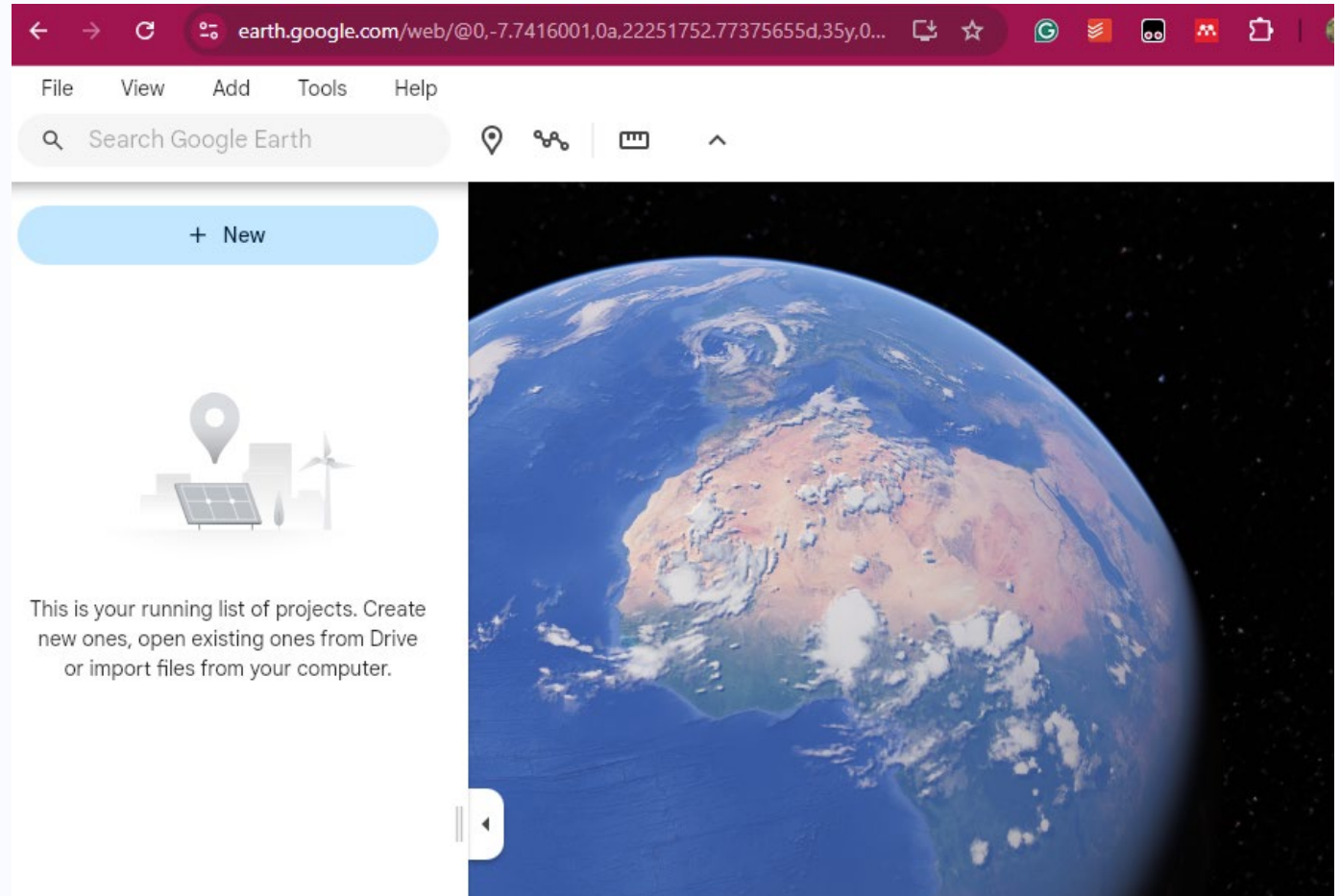
None of these words
Example: cats dogs · does not contain "cats" and does not contain "dogs"

These hashtags
Example: #ThrowbackThursday · contains the hashtag #ThrowbackThursday

Language

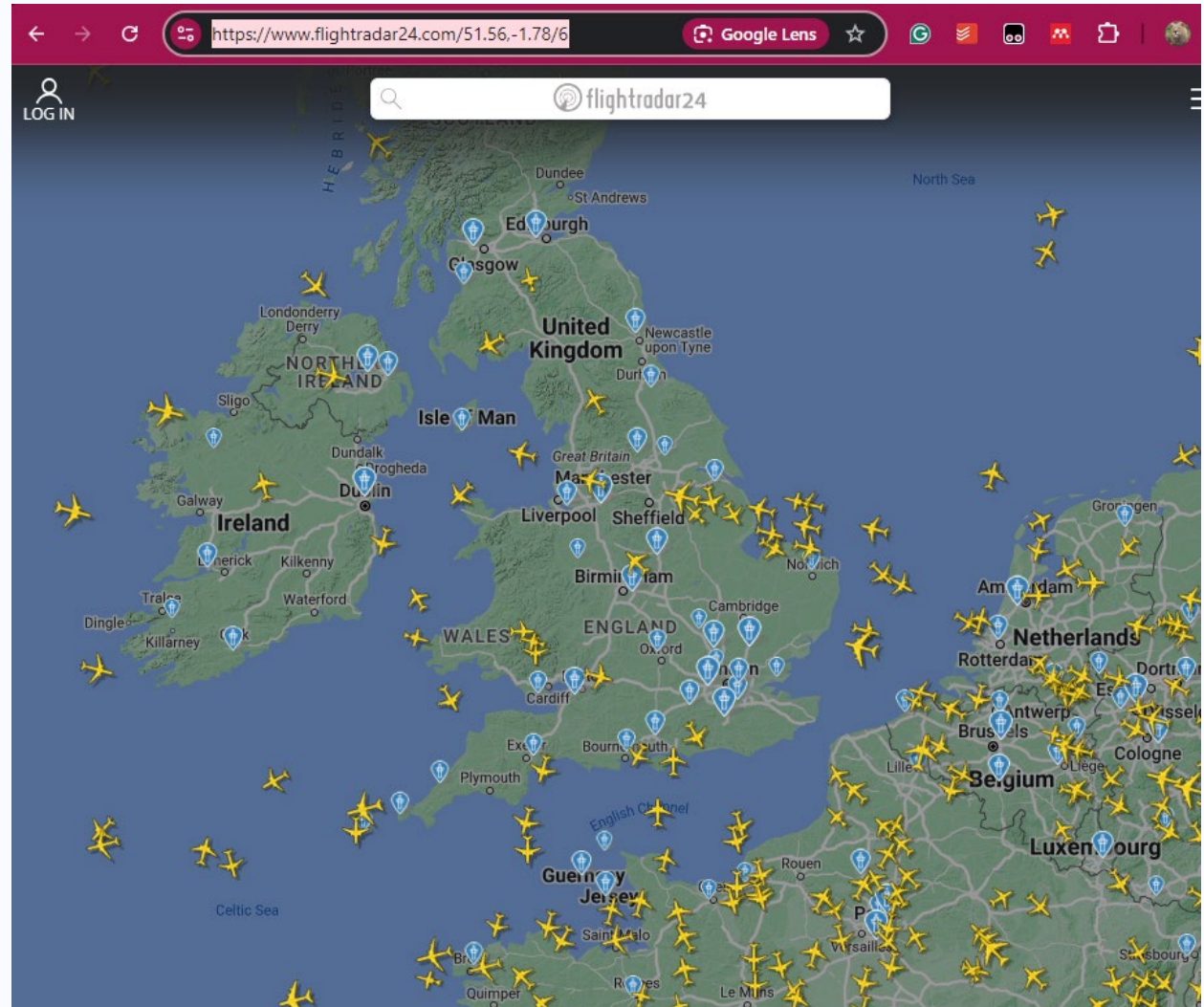
<https://x.com/search-advanced>

Google Earth



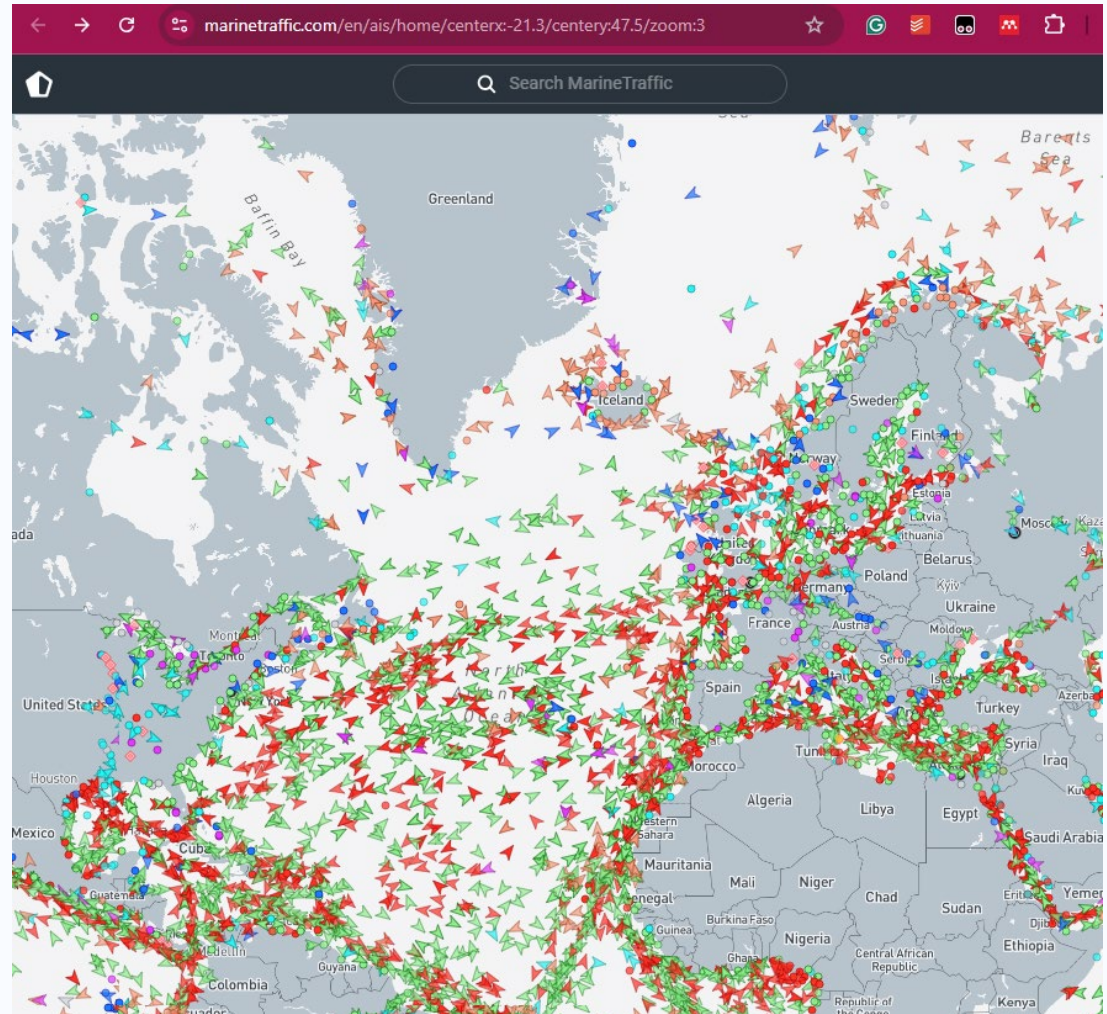
<https://earth.google.com>

Flight Radar



<https://www.flightradar24.com/>

Marine Traffic



<https://www.marinetraffic.com>

General

Search Engines

- Search Terms
 - site:[url] [term]
 - Filetype:[type]
 - Related:[url]
 - Cache:[url]
- <https://datasetsearch.research.google.com/>
- <https://www.google.co.uk/maps/preview>

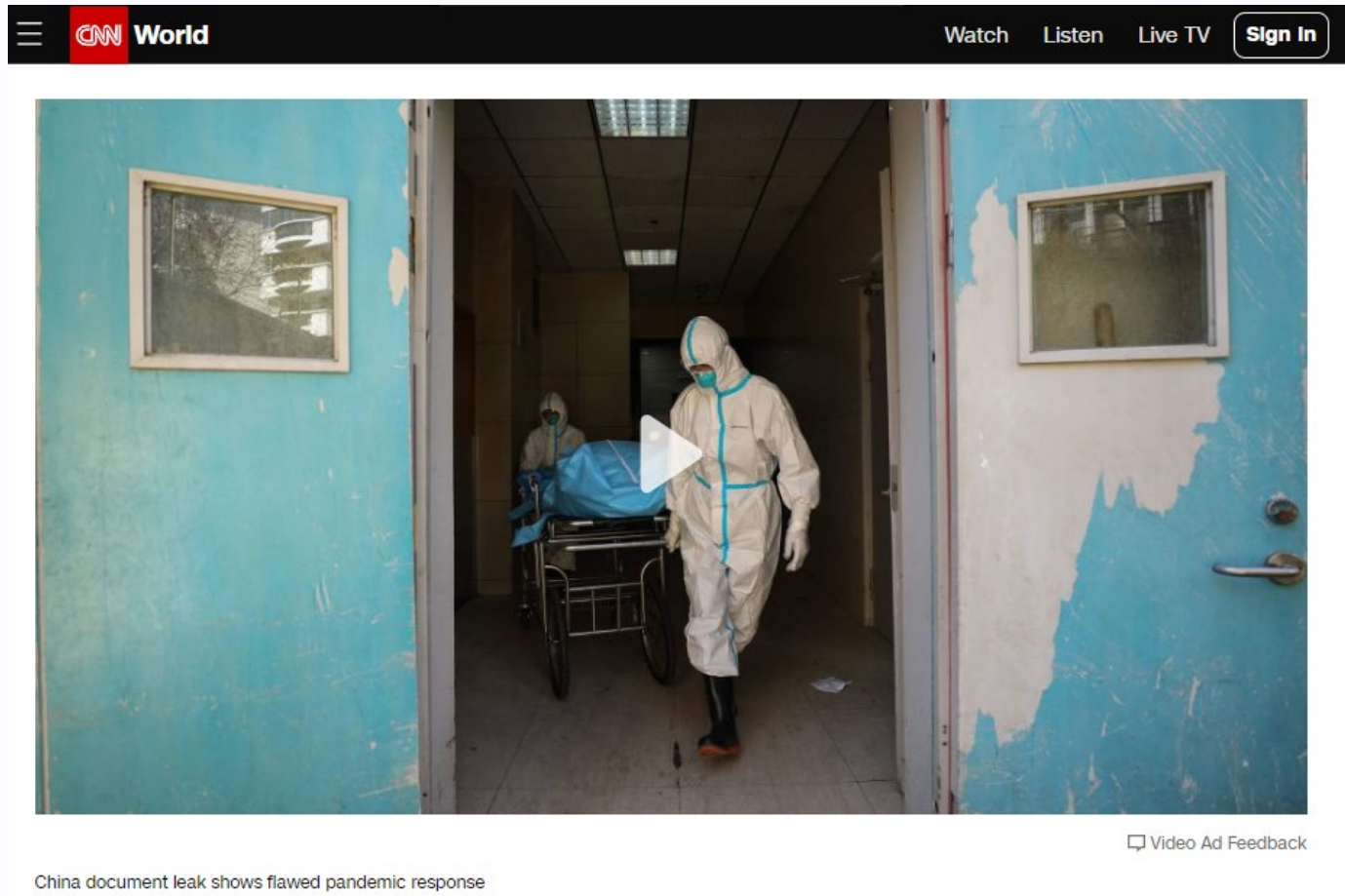
Social Media and News Sites

- Useful for current trends
- Need validating / corroborating
- May contain items with geodata (e.g. videos, photos, docs)

Metadata / Hidden / Deleted Data!!

- Under documents / images / videos there is much data
- We can geolocate based on many factors including
 - Hidden Data
 - Metadata
 - Techniques / Software used

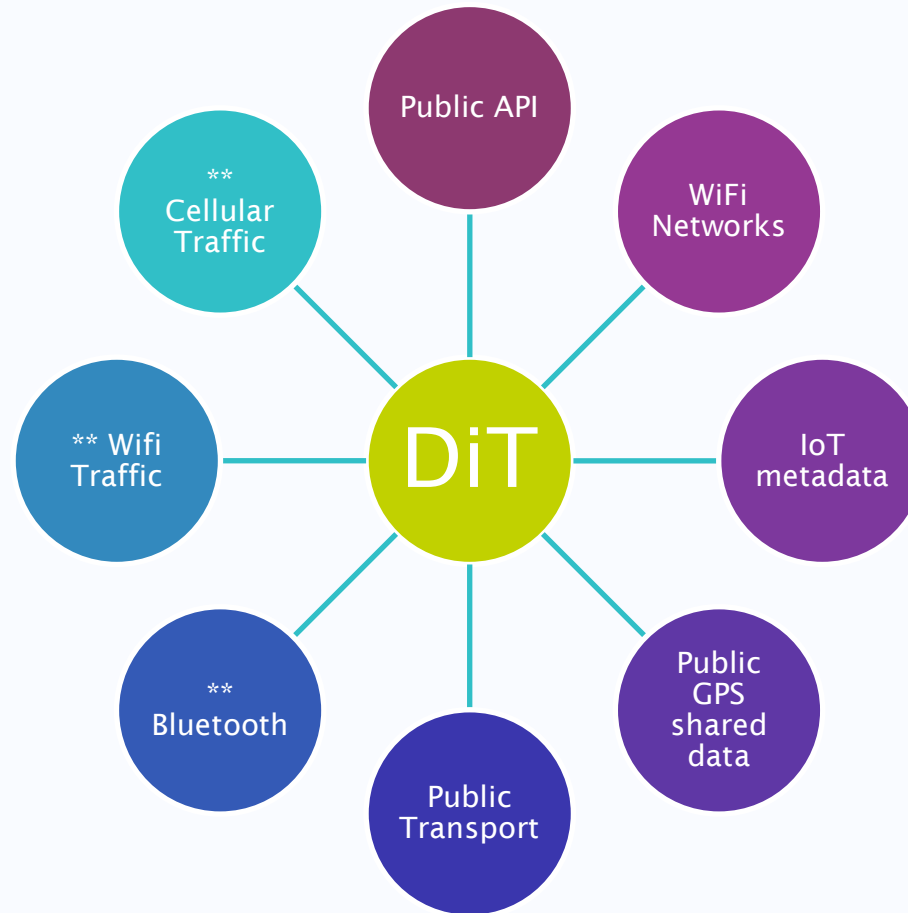
Metadata / Hidden / Deleted Data!!



<https://edition.cnn.com/2020/11/30/asia/wuhan-china-covid-intl/index.html>

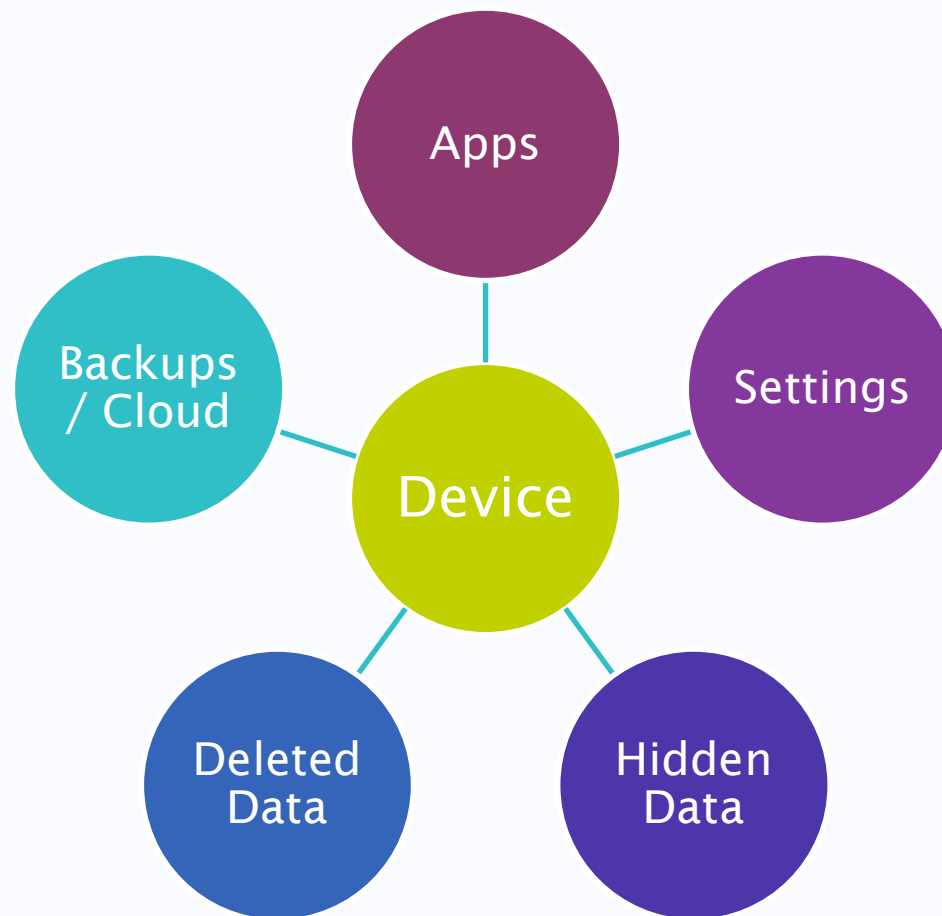
Data in Transit & On Device

Data in Transit



** Generally requires permission

Data on Device



** Generally not available via OSINT unless publicly shared / breach

Ethics and Legalities

Ethics / Legalities

Privacy
Violations

Data Misuse

Accidental De-
Anon.

Stalking /
Surveillance

Unintended
Consequences!!

Violating ToS

Data Accuracy
issues

Discrimination
/ Bias

Legal Issues

Lab Issues

Challenges and Limitations

Challenges

Data
Availability

Accuracy

Reliability

Fragmentation

Geolocation
Restrictions

Legal
Boundaries

Language
Barriers

Rapid Data
Change

Large Data

Limitations

Limited Data
in Free Layer

Dependence
on Sharing

Attribution
Issues

Geographic
Bias

Platform
Limitations

Data
Interpretation
Challenges

Metadata
Removal

Security Risks

Countermeasures

Limiting
Metadata
Exposure

Control Social
Media Sharing
(Privacy)

Anon. Online
Activity

Restrict Data
Access

API Control,
inconsistency

IoT Security

Deepfake /
Misinformation

Conclusion

Conclusion

- Experiment / Test Sources before use
- Corroborate data where possible
- Set your system up wisely
- Take notes of Activity!

YOUR QUESTIONS

Professor Sarah Morris
s.morris@soton.ac.uk