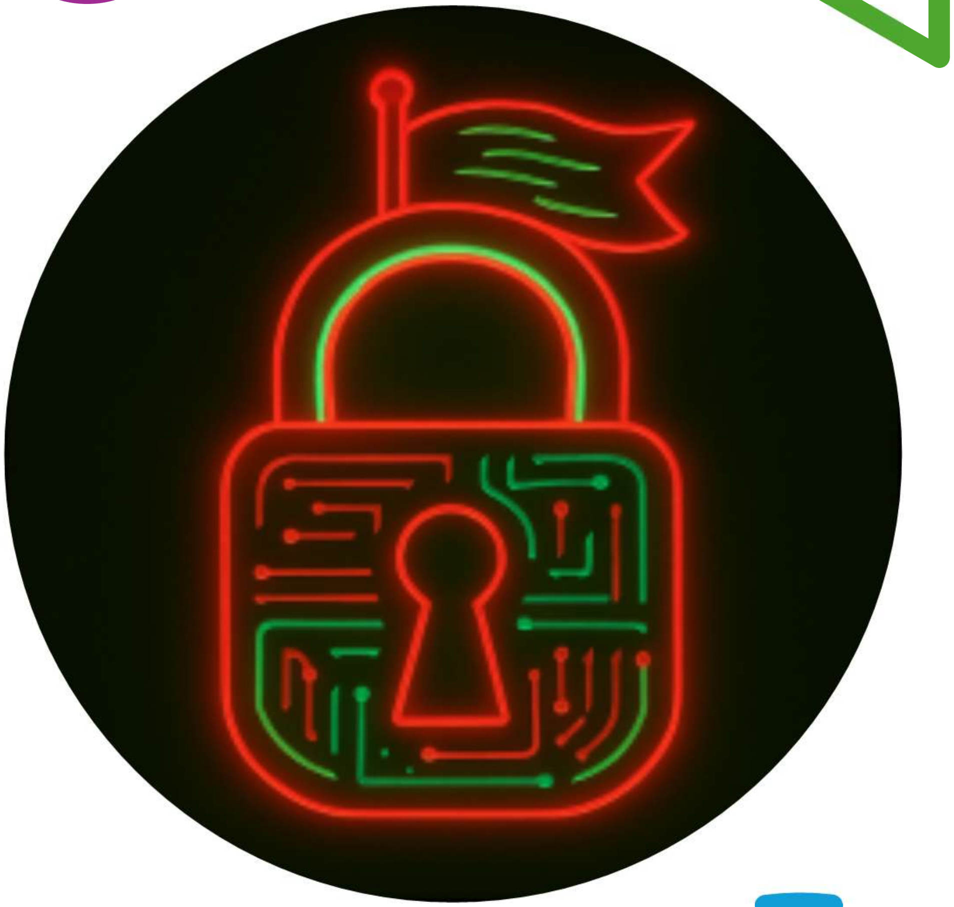
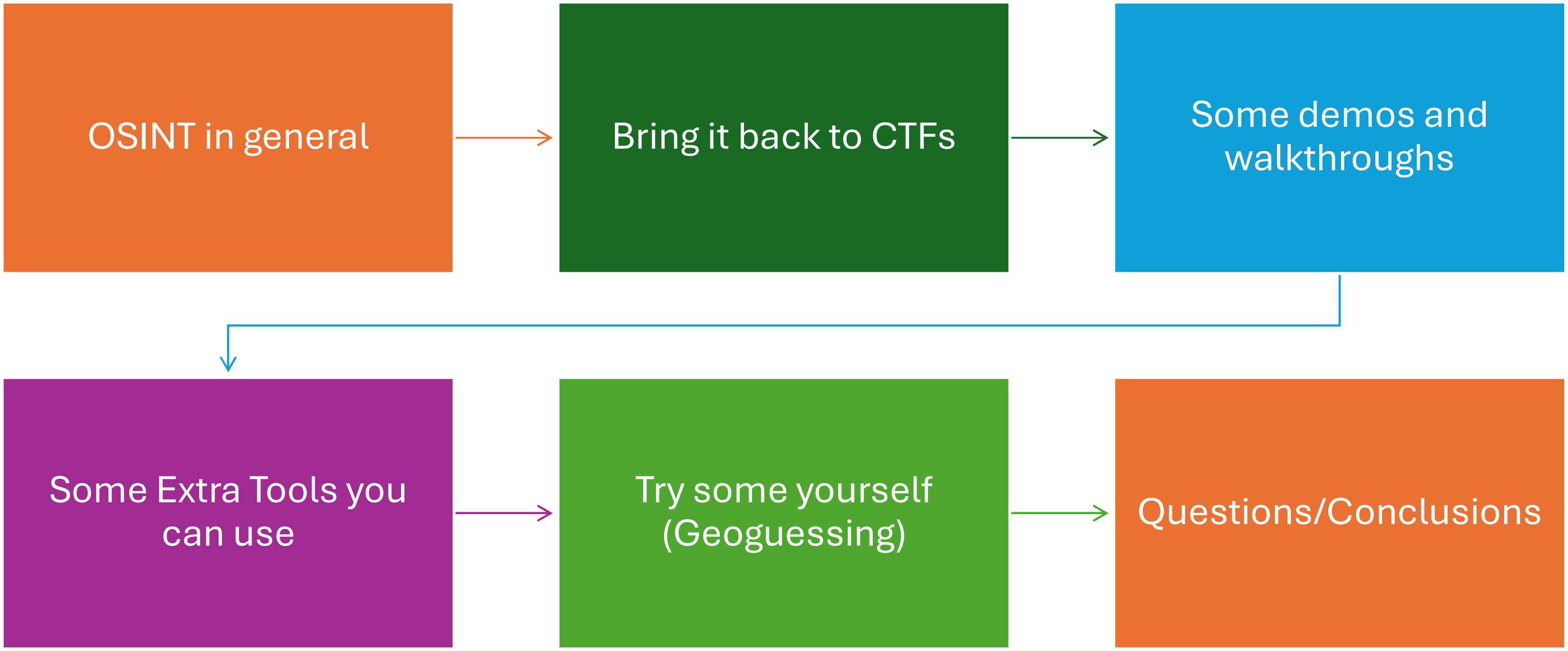


RedRoom CTF Workshop – OSINT (Open-Source Intelligence)

Training By – Lindsay (Y14)

27th November 2025

What will we be covering today?



OSINT in general

Bring it back to CTFs

Some demos and walkthroughs

Some Extra Tools you can use

Try some yourself (Geoguessing)

Questions/Conclusions

What is OSINT

Stands for Open-Source Intelligence

It is the gathering of information which is available to the public.

It is NOT hacking or accessing restricted data.

Sources Include: Social Media, Public records, News Articles and More

TO NOTE: Ethical considerations are important when performing an OSINT investigation. Stick to what you need for a challenge and nothing more.

Quick Disclaimer

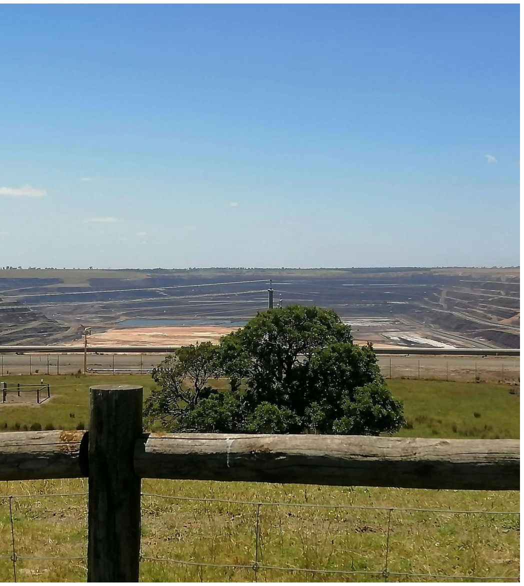
It is very easy to go into stalking territory which is why a lot of CTFs use mainly image reverse lookup

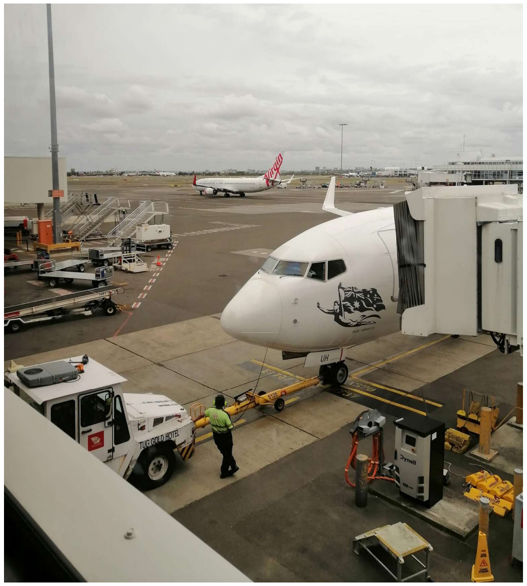
RedRoom does NOT condone illegal or malicious activities

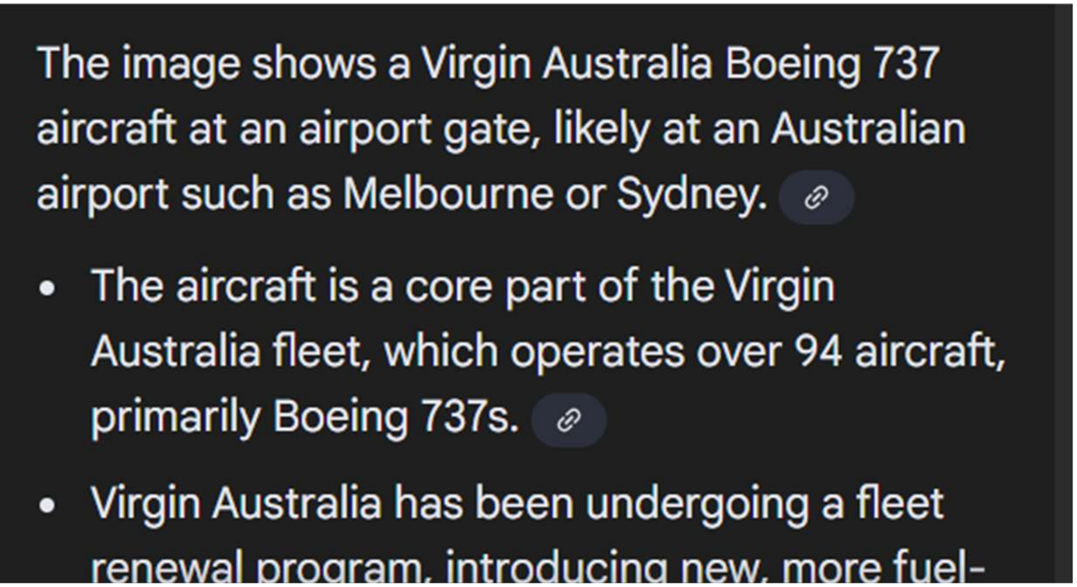
It is three years in prison if you are caught stalking however it can go up to 8 years

If you choose to use any of these tools for any malicious purposes do not say I (or any of members of RedRoom) have told you how to do any of this

If a CTF does use social media and give you links to profiles (insta, Steam etc ...) those are consented profiles by the challenger creator DO NOT do anything you are not supposed to do





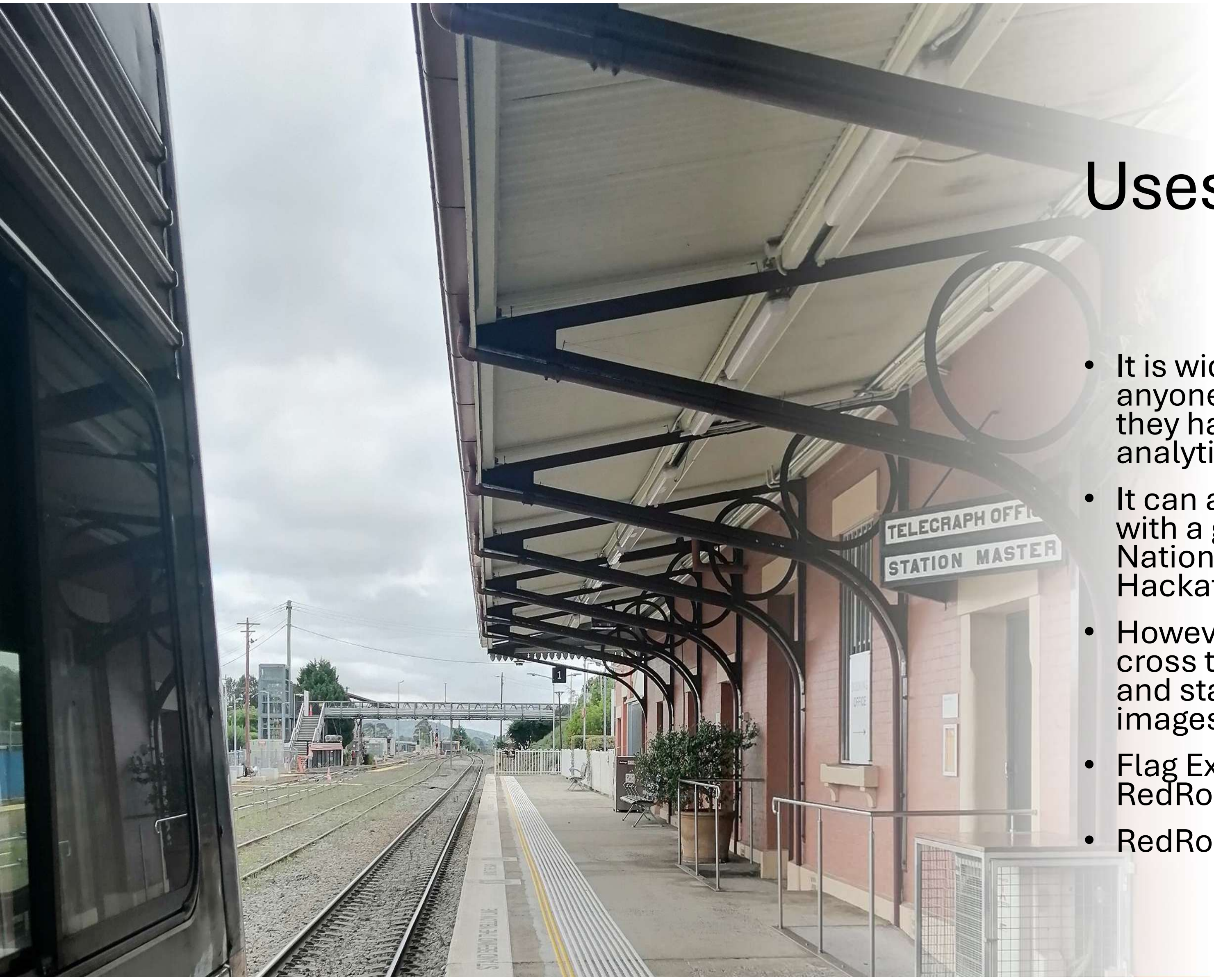


The image shows a Virgin Australia Boeing 737 aircraft at an airport gate, likely at an Australian airport such as Melbourne or Sydney.

- The aircraft is a core part of the Virgin Australia fleet, which operates over 94 aircraft, primarily Boeing 737s.
- Virgin Australia has been undergoing a fleet renewal program, introducing new, more fuel-

The OSINT Process:

- Define your objective
- Collect data
- Verify and validate sources
- Pivot and go deeper
- Document Findings
- Find your flag



Uses in CTF:

- It is widely used in CTFs and anyone can do OSINT as long as they have internet access and an analytical mind.
- It can also be used in real life with a good example being the National Missing Person's Hackathon.
- However, because it so easy to cross the line between innocent and stalking CTFs tend to stick to images
- Flag Example RedRoom{Moss_Vale_Station}
- RedRoom{-34.5479_150.3718}

Common OSINT Methods for CTFs

OSINT is widely used in CTFs. Beginner challenges often include things such as using social media profiling, finding the location that an image was taken, reverse image lookups.

Social Media

Social media is a valuable resource for OSINT. Profiles can reveal names, locations, interests, and more. This information can be used to solve challenges.

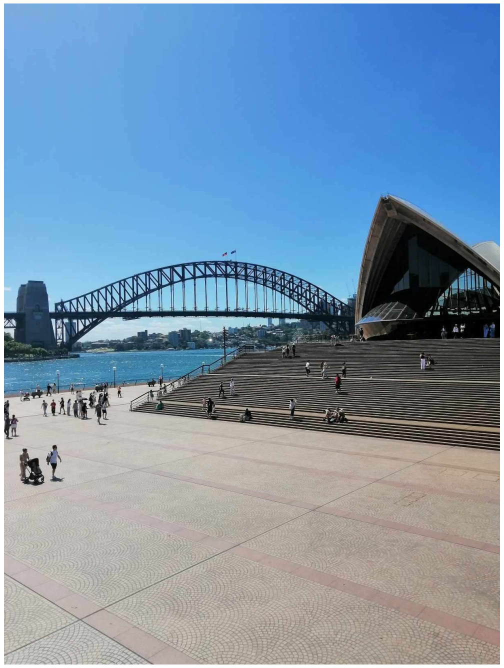
Reverse Image lookups

The most popular type of CTF challenge is reverse image lookups, this is usually used when the flag is looking for a specific location whether it is:

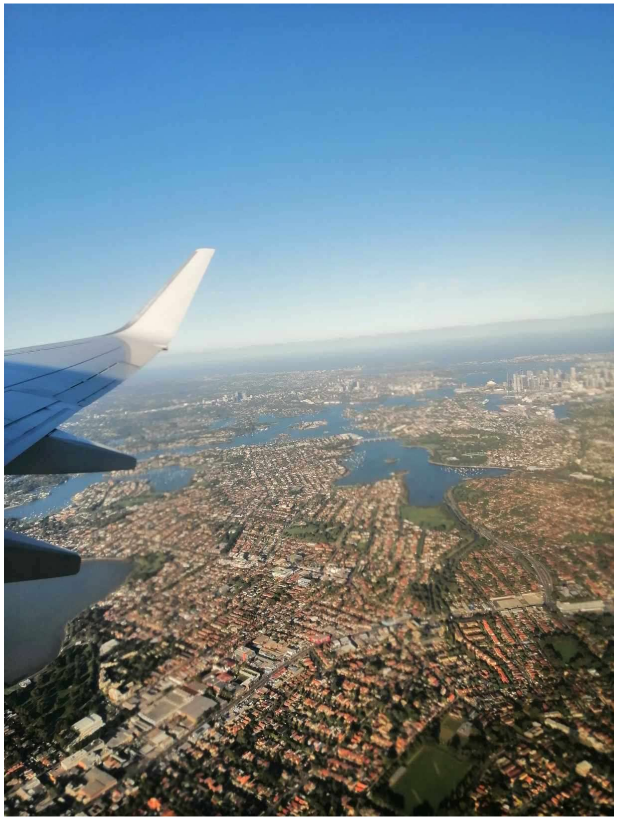
- **Map co-ordinates**
- **Name of Location**
- **Name of a Painting**

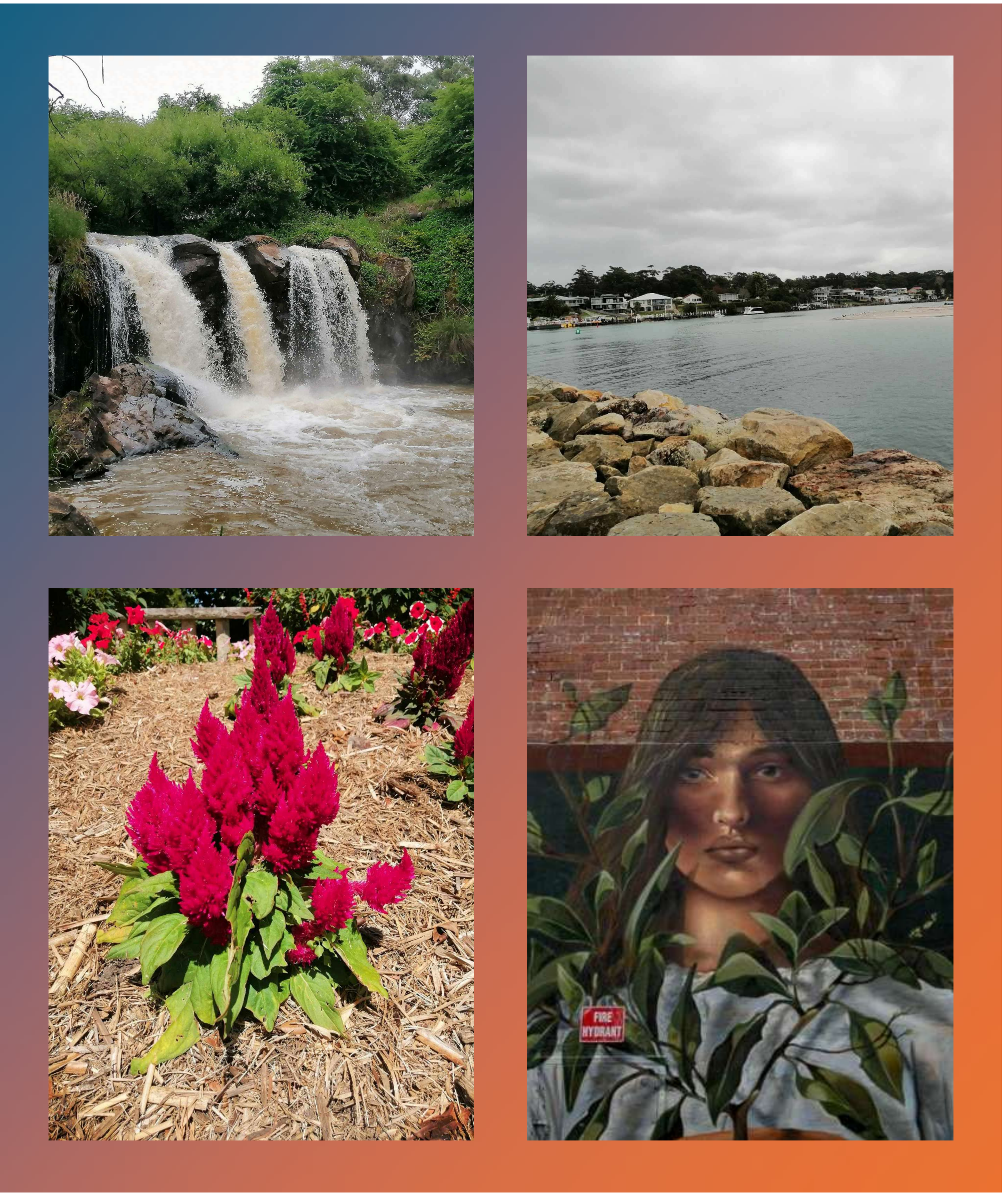
Examples

- Find what is in an image (i.e.) building



- Challenges can also be a bit more difficult with having to do a bit more digging (i.e. Find this flight number)





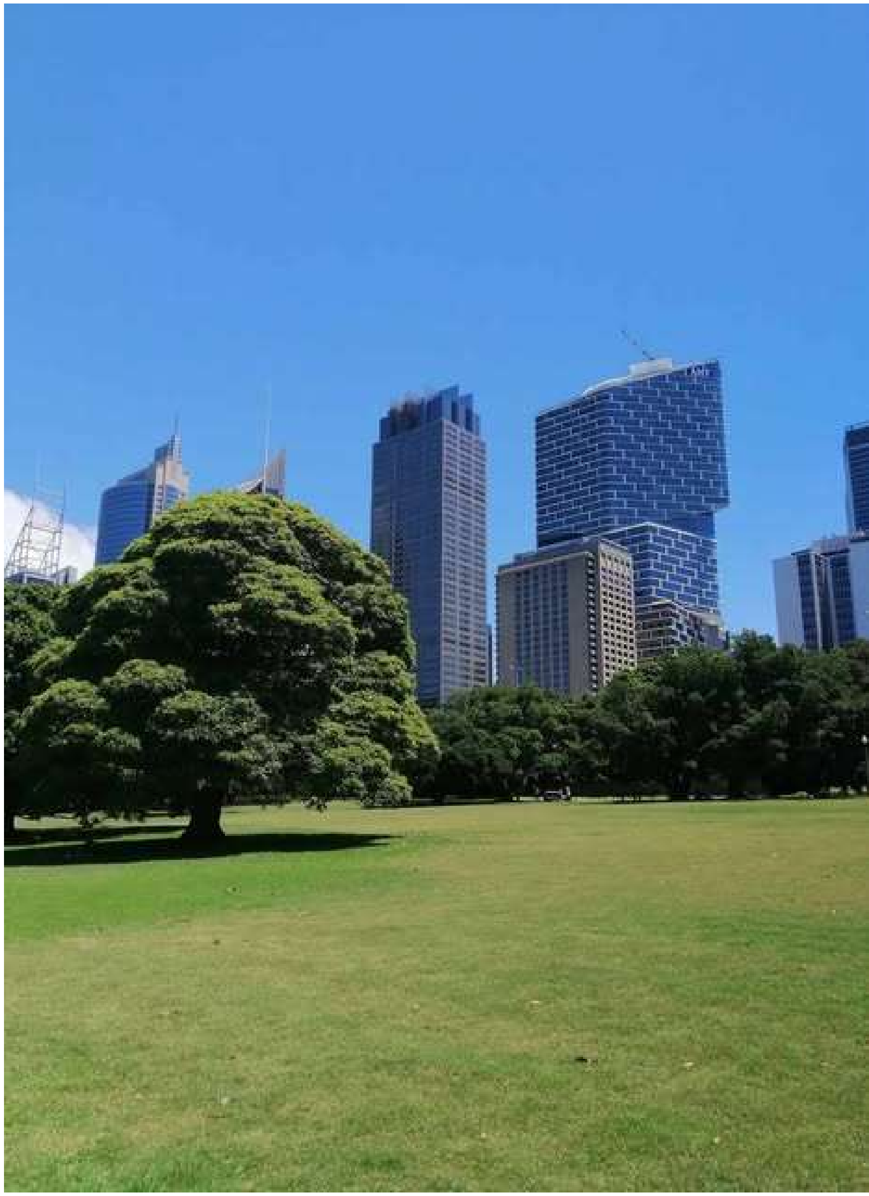
Other types of challenges

- Sceneries
- Bodies of water/coastlines
- Plants (whether as their own challenge or can be used to identify scenery)
- Street arts/murals
- You will also sometimes see challenges obstructed by shapes to make it a little harder to identify

Give this one a go: (very simple)

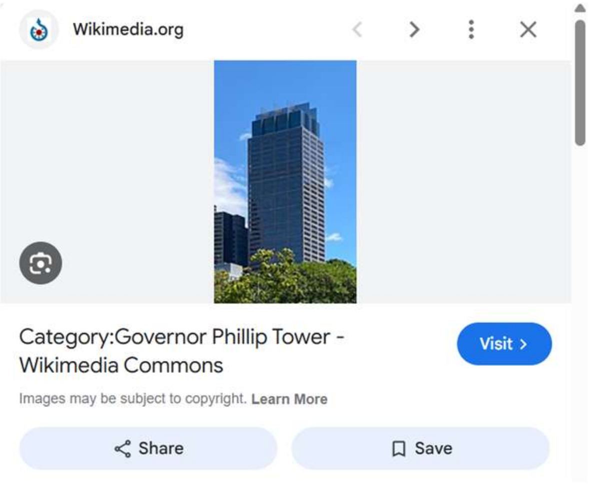
Which City was this photo taken in

Bonus point if you can get the garden it was taken from



Answer

- Step 1: Find the name of any building in the photo
- Step 2: Find the city that building is in
- Step 3: Find the garden!


Wikimedia.org

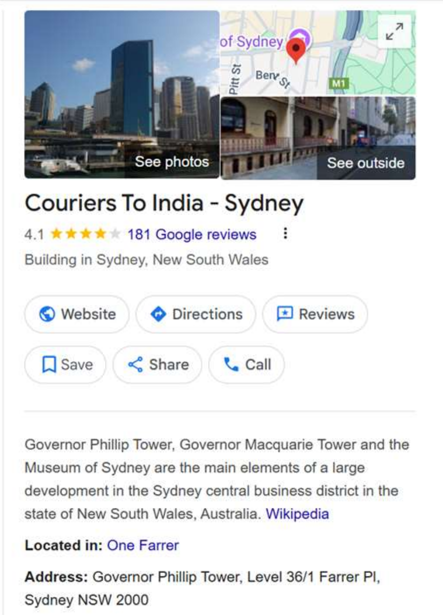
Category:Governor Phillip Tower - Wikimedia Commons

Visit ›

Images may be subject to copyright. **Learn More**

Share

Save



Couriers To India - Sydney

4.1 ★★★★☆ 181 Google reviews

Building in Sydney, New South Wales

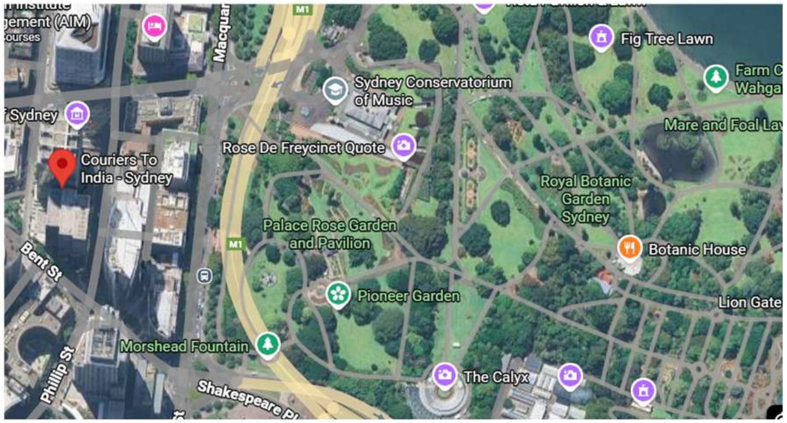
Website Directions Reviews

Save Share Call

Governor Phillip Tower, Governor Macquarie Tower and the Museum of Sydney are the main elements of a large development in the Sydney central business district in the state of New South Wales, Australia. Wikipedia

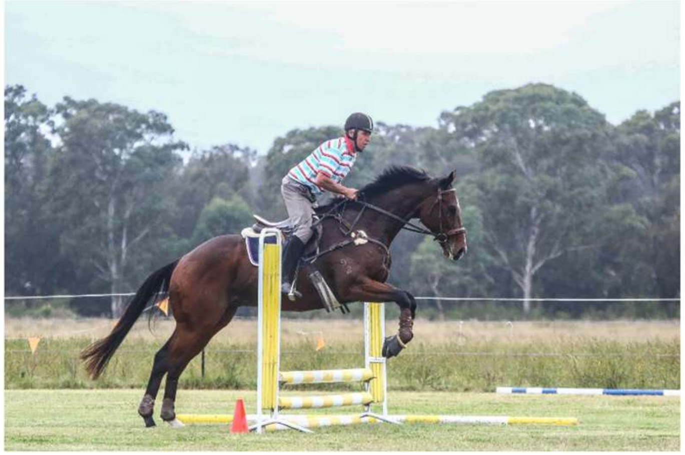
Located in: One Farrer

Address: Governor Phillip Tower, Level 36/1 Farrer Pl, Sydney NSW 2000

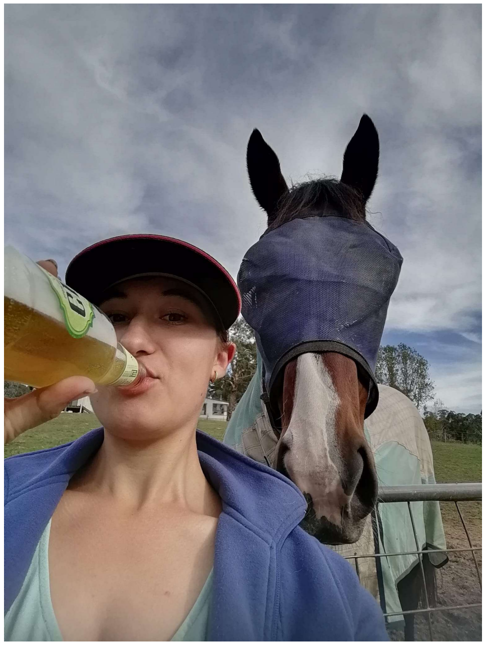


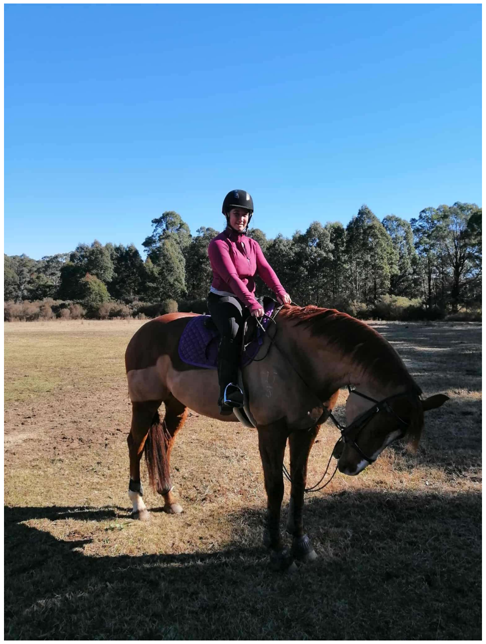
And this one:

- What is the name of this horse (Bonus points if you can find his age (hint – Bagot handicap 2019)



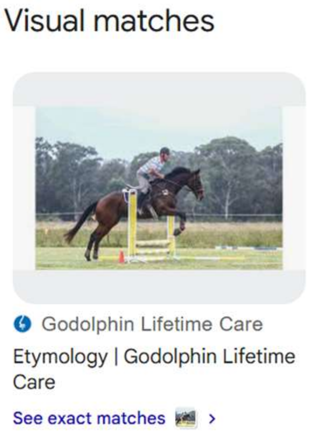
- Yes I do know this horse personally and one of his half brothers they are both retired





Answer

- Step 1: Put the image in Google Images
- Step 2: Click on the Godolphin Link!
- Step 3: Google the horse and find his age

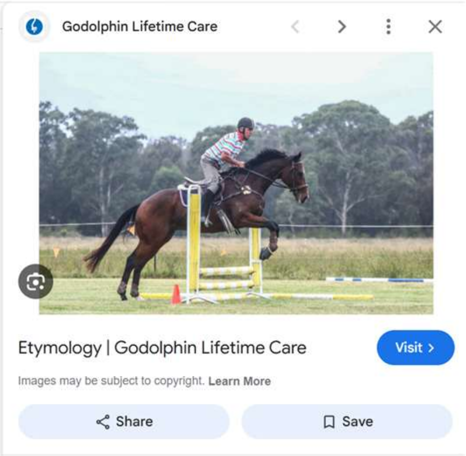


Visual matches

Godolphin Lifetime Care

Etymology | Godolphin Lifetime Care

See exact matches ›



Godolphin Lifetime Care

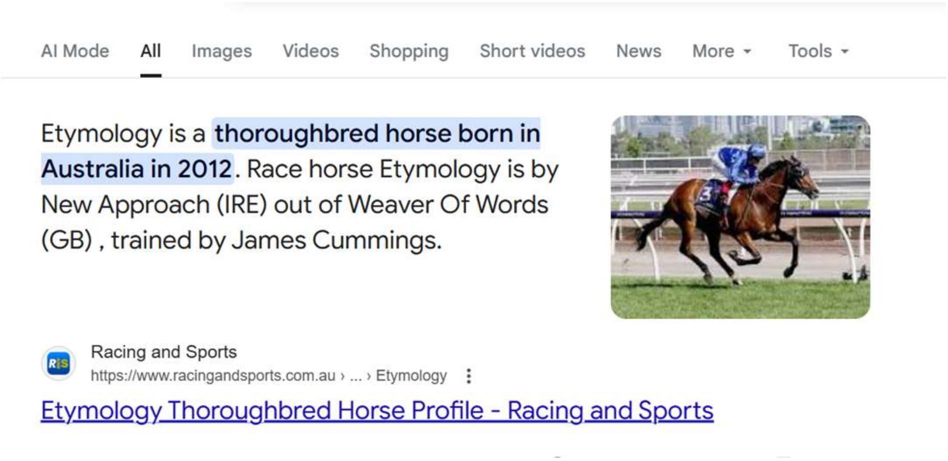
Etymology | Godolphin Lifetime Care

Visit ›

Images may be subject to copyright. **Learn More**

Share

Save



AI Mode | **All** | Images | Videos | Shopping | Short videos | News | More ▾ | Tools ▾

Etymology is a **thoroughbred horse born in Australia in 2012**. Race horse Etymology is by New Approach (IRE) out of Weaver Of Words (GB) , trained by James Cummings.

Racing and Sports
https://www.racingandsports.com.au › ... › Etymology ⋮

Etymology Thoroughbred Horse Profile - Racing and Sports

Extra Tools:

- https://www.shodan.io/
- https://inteltechniques.com/tools/index.html
- https://osintframework.com/
- https://epieos.com/
- Google - Maps, Images
- TinEye
- Flightera
- Exiftool – can be useful for data extraction such as date and time and sometimes even location. There are online tools as well:
  - https://www.metadata2go.com/delete-metadata*

Geoguessing and CTFs how does it help?

- https://geohunt.vercel.app/
- https://www.mapcrunch.com/

- Can help hone skills to find what country you're in, road signs and anything else that Google Images may struggle to identify
- Good for team building as well

Try some at home

- Hack the Box
- TryHackMe
- https://gralhix.com/list-of-osint-exercises/
- Real Case scenarios:
- https://www.tracelabs.org/

Questions??

And if you want the slide deck you can get it at wecommitorganisedcrime.org/workshop.pdf

And for making you sit through this a photo of Huey