

Beginner OSINT Training for CTFs

UWA training

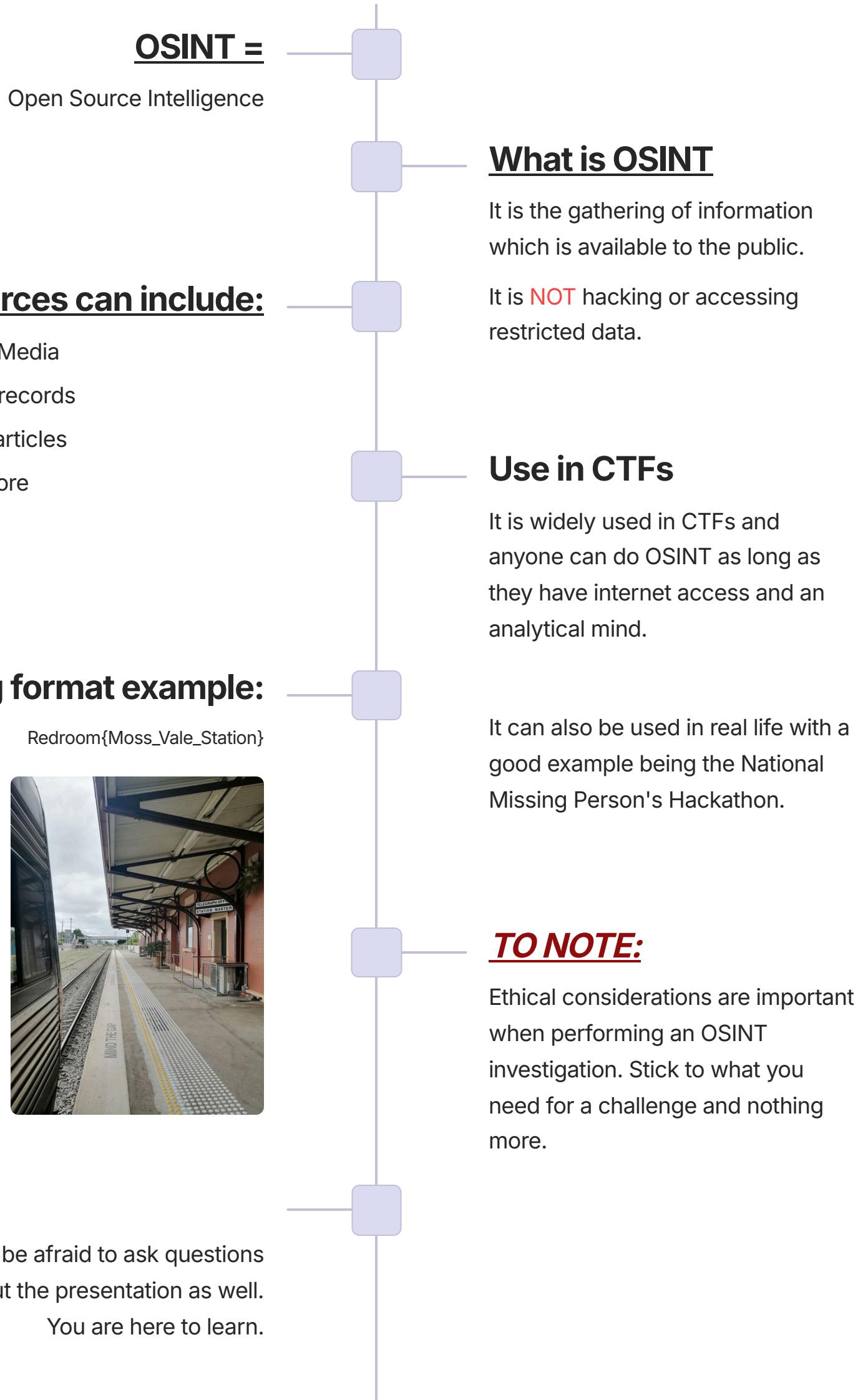
April 23rd 2025.

Training by - Lindsay Coudert

What will we be covering today?

- OSINT in general
- Some demos and walkthroughs
- Try some yourself

What is OSINT



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. For example, an OSINT challenge can include the someone's github username.

Reverse Image lookups

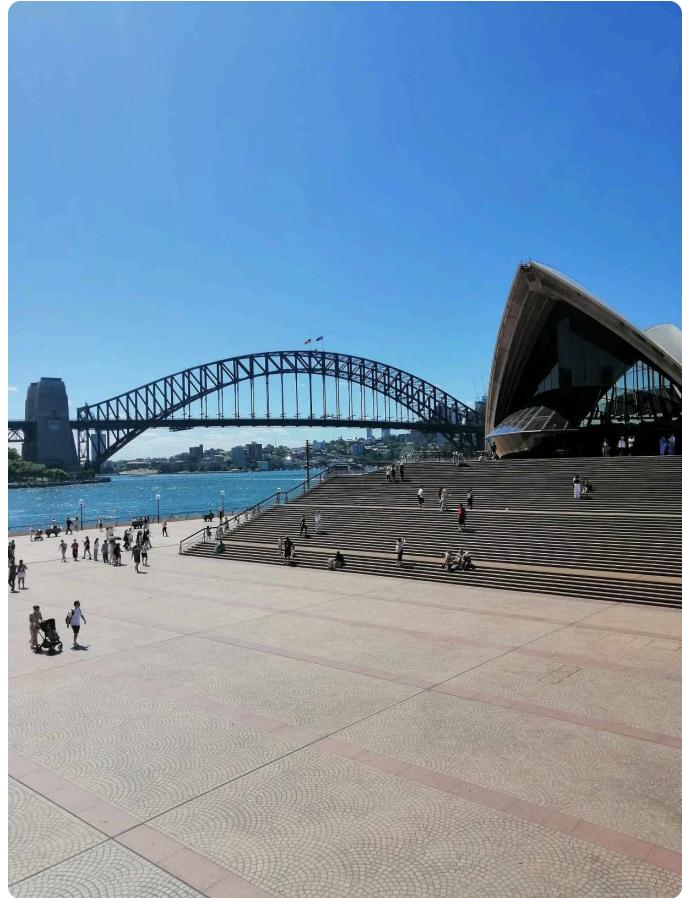
Another very popular CTF challenge is reverse image lookups, this is usually used when the flag is looking for a specific location whether it's the name or the coordinates of said location.

Map co-ordinates.

Common CTF challenge examples

▼ Find the location of a given image:

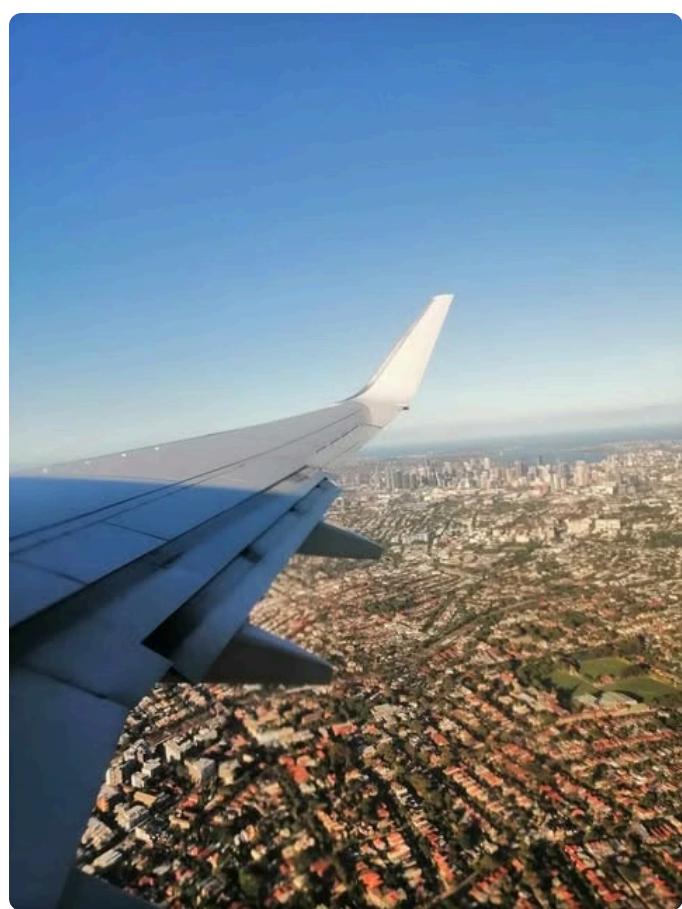
One of the common CTF challenges are finding locations of a given image:



▼ Another Cool challenge we have come across:

- Email that we encountered and this is what gets put into Epieos: CipherBre4ker@gmail.com
- To find the birthday we simply go back through the calendar to find the date.
- To find the cat's name and the accounts favourite colour we simply use their reddit account.

This isn't the actual photo from the challenge I took this one myself.



▼ Tools to help solve and Commands:



On-time Performance, delay statistics and flight information

Flightera.net – On-time Performance, delay statistics and flight information



exiftool Plen.jpg

exiftool -DateTimeOriginal Plen.jpg

Give this one a go:

Find the co-ordinates of this Train Station

Moss Vale



▼ Answer:

Answer: -34.5479° S, 150.3715° E

And this one:



Yes I actually do know this horse personally:



▼ Answer:

Answer Etymology - Baggot Handicap

Extra Tools:

Shodan

// USAGE
More than 4 million users
Data on thousands of ports
Globally-distributed network of crawlers

// SERVICES
Search the Internet
Go beyond the web. Search the entire internet for connected devices.

Monitor Networks
Know what you have exposed to the Internet and get notified when that changes.

Build Products
Leverage the Shodan API to give your products unprecedented insights about the Internet.

 Shodan

Shodan

Search engine of Internet-connected devices. Create a free account to get started.

 inteltechniques.com

IntelTechniques Search Tool

Search Engines Facebook Twitter Instagram LinkedIn Communities Email Addresses Usernames Names Addresses Telephone Numbers Maps Documents Pastes Images Videos Domains IP Addresses Business & Government Vehicles Virtual Currencies...

 osintframework.com

OSINT Framework

(T) – Indicates a link to a tool that must be installed and run locally (D) – Google Dork, for more information: Google Hacking (R) – Requires registration (M) – Indicates a URL that contains the search term and the URL itself must be edited manually

Try some Geoguessing:



geohunt.vercel.app

GeoHunt



Try some on your own at home:

Below is a website that you can go to and practice some exercises they range from easy to hard so feel free to try out at your own pace:



Sofia Santos | OSINT Analysis & Exercises



List of OSINT Exercises – Challenge Yourself!

Looking to expand your OSINT skills or put your existing ones to the test? Give it a go on my list of free OSINT challenges! What are the OSINT Exercises? These OSINT exercises...

▼ Real Case Scenarios:



www.missingpersonshackathon.com.au



Home | NMP Hackathon

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



www.tracelabs.org



Trace Labs | Crowdsourced OSINT to Find Missing People

Trace Labs is a nonprofit organization whose mission is to accelerate the family reunification of missing persons while training members in the tradecraft of open...

Questions???

Hope you learned something

