

OPEN-SOURCE INTELLIGENCE

*A primer on how to utilise public data in lieu of
privileged information*

Yoga Smara (a.k.a. Einzwell)

[me\[at\]einzwell\[dot\]dev](mailto:me[at]einzwell[dot]dev)

OSINT?

Collection, analysis, and dissemination of publicly available information for intelligence purposes

Data source:

- social media (SOCMINT)
- geospatial data (GEOINT)
- public records
- others

(more on this later)

WHY IMPORTANT?

- Every minute, users generate*:
 - 500 hours of YouTube video
 - 1.7 million Facebook posts
 - 66 thousands Instagram posts
 - 347 thousands Twitter posts
- Organisations are becoming more transparent and publishing data online

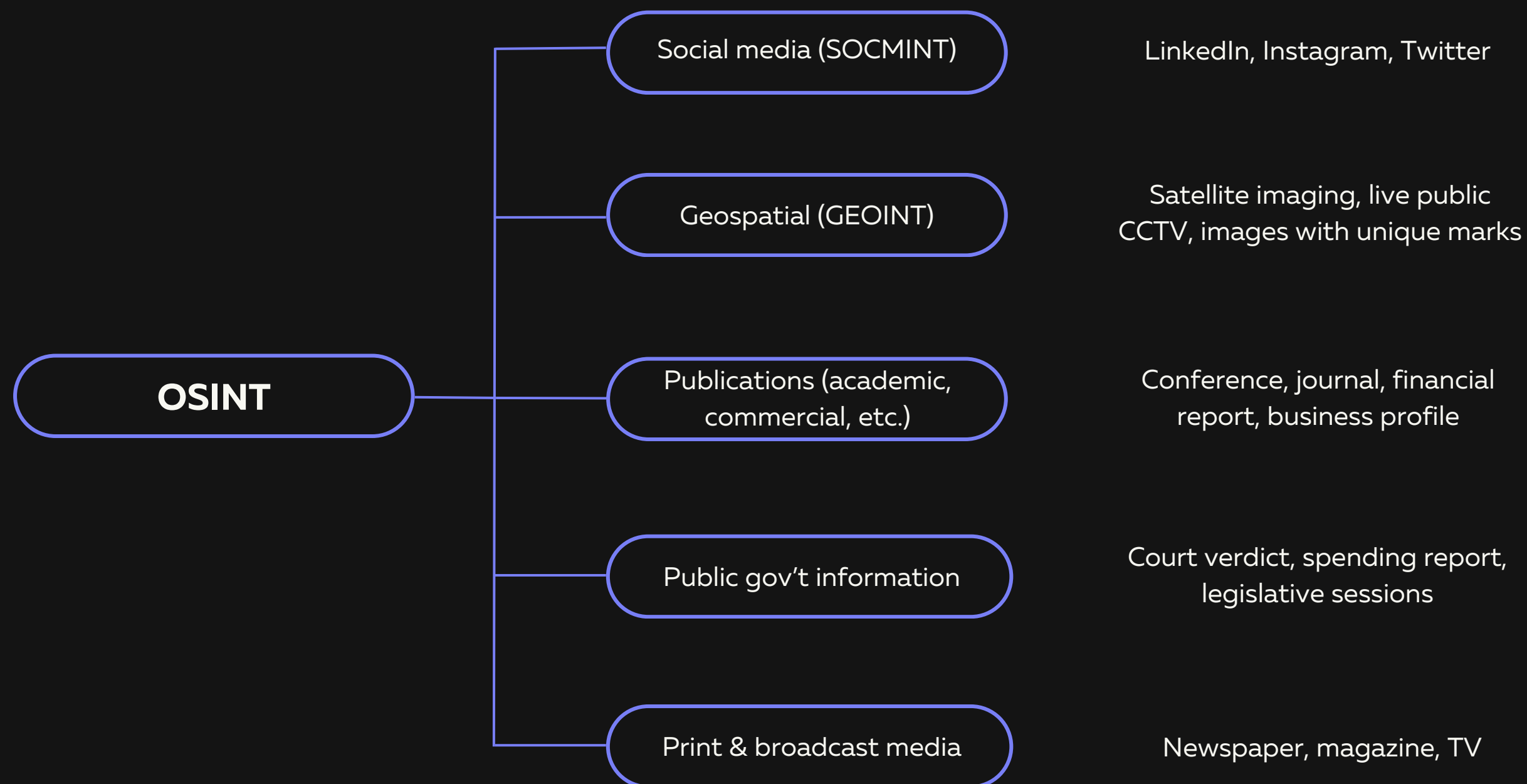
Useful for:

- Intelligence & security
- Investigative journalism
- Academic research
- Legal proceedings
- Business research



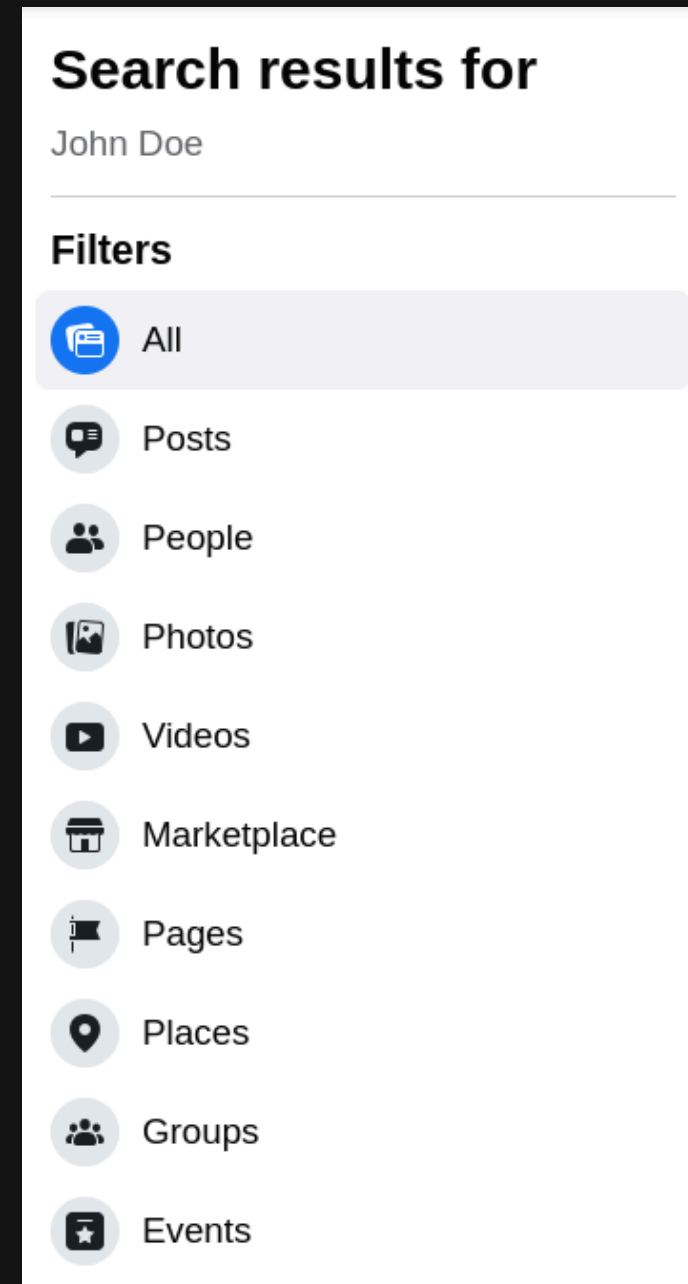
*according to "Data Never Sleeps 10.0" by DOMO

CLASSIFICATIONS



SOCIAL MEDIA: FACEBOOK

- Intimate/biographical information of one's life (place & date of birth, education, personal relationships, hobby, etc.)
- Use the search filter whenever possible
- More specific searching requires complex manipulation of URL parameters
 - Involves JSON formatting with Base64 encoding
 - Read more: blog.nem.ec/2020/06/07/new-facebook-graph-search
- Use online tool: inteltechniques.com/tools/Facebook.html



SOCIAL MEDIA: TWITTER

- Daily activities & interests
- Twitter Advanced search: <https://twitter.com/search-advanced>
- Search operator:
 - **"A phrase" (double quotes)**: tweet containing that specific phrase/keyword
 - **x AND y**: tweet containing keywords "x" AND "y"
 - **x OR y**: tweet containing keywords "x" OR "y"
 - **-keyword**: tweet NOT containing said keyword
 - **from:x** : tweet from account with username "x"
 - **to:y** : tweet directed to account with username "y"
 - **since:2020-12-25** : tweet after 25 December 2020
 - **until:2021-07-01** : tweet before 1 July 2021
 - Read more: developer.twitter.com/en/docs/twitter-api/v1/rules-and-filtering/search-operators

× 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"

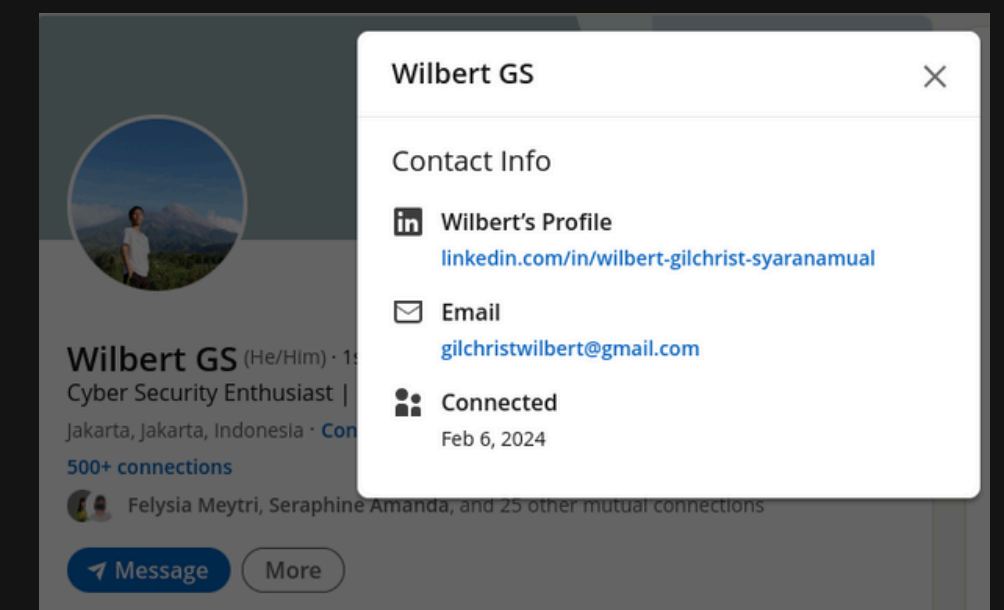
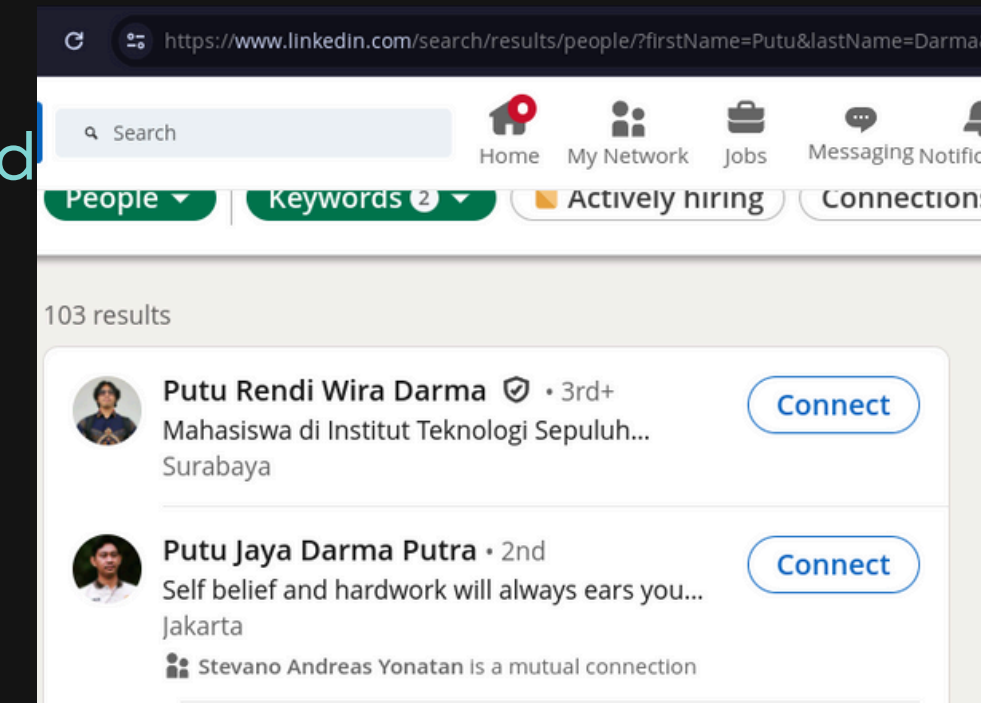
Any of these words
Example: cats dogs · contains either "cats" or "dogs" (or both)

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



SOCIAL MEDIA: LINKEDIN

- Professional work history, education, achievement, affiliations, and others.
- Knowing target's full name will greatly aid search efforts.
- Targeted searching with **URL parameter**:
 - **First & last name**: [https://www.linkedin.com/search/results/people/?firstName=\[Nama depan\]&lastName=\[Nama belakang\]](https://www.linkedin.com/search/results/people/?firstName=[Nama depan]&lastName=[Nama belakang])
 - **Company**: [https://www.linkedin.com/search/results/people/?company=\[perusahaan\]](https://www.linkedin.com/search/results/people/?company=[perusahaan])
 - **Job title**: [https://www.linkedin.com/search/results/people/?title=\[title\]](https://www.linkedin.com/search/results/people/?title=[title])
 - **School**: [https://www.linkedin.com/search/results/people/?school=\[sekolah\]](https://www.linkedin.com/search/results/people/?school=[sekolah])
- **Places of interest**:
 - Contact Info
 - Recent Activity



EMAIL & USERNAME

Look up username with **sherlock**

```
~/Downloads/Git/sherlock
python3 sherlock hackerman1337
[*] Checking username hackerman1337 on:
[+] 9GAG: https://www.9gag.com/u/hackerman1337
[+] AllMyLinks: https://allmylinks.com/hackerm
[+] Archive.org: https://archive.org/details/@
[+] AskFM: https://ask.fm/hackerman1337
```

github.com/sherlock-project/sherlock

Look up email with **holehe**

```
~/Downloads/Git
holehe test@gmail.com --only-used --no-clear
Twitter : @palenath
Github : https://github.com/megadose/holehe
For BTC Donations : 1FHDM49QfZX6pJmhjLE5tB2K6CaTLMZpXZ
99%|

*****
test@gmail.com
*****
[+] any.do
[+] archive.org
[+] blip.fm
```

github.com/megadose/holehe

PUBLIC RECORDS

Public informations such as court records and company legal entity data can help with OSINT investigation.

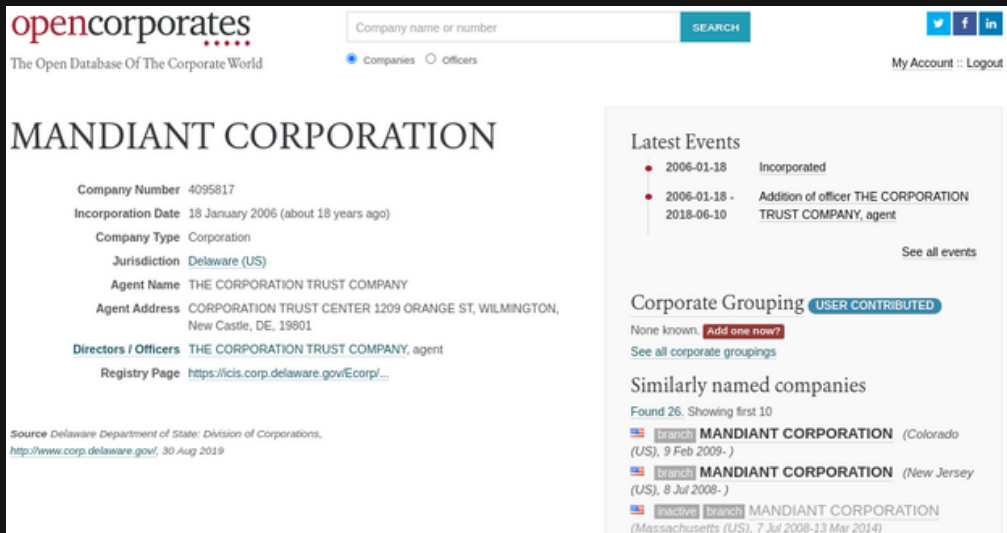
Data source:

- **Company registry**
 - Basic business information such as its proper name, HQ location, director's name
 - Financial records gives insight about the company's performance
- **Court records**
 - Information may vary (depending on the nature of the case)
 - Useful for investigations involving legal cases
- **Property records**
 - Trace the ownership of a property to an individual or organisation
 - Determine target's asset value
- **Other public database** (e.g., vehicle, education, website WHOIS)

Note:

- Data is not always available online
- Think outside the box
- Gather info from multiple sources

WHERE TO SEARCH THEM?



opencorporates
The Open Database Of The Corporate World

Company name or number SEARCH

Companies officers My Account :: Logout

MANDIANT CORPORATION

Company Number 4095817
Incorporation Date 18 January 2006 (about 18 years ago)
Company Type Corporation
Jurisdiction Delaware (US)
Agent Name THE CORPORATION TRUST COMPANY
Agent Address CORPORATION TRUST CENTER 1209 ORANGE ST, WILMINGTON, New Castle, DE, 19801.
Directors / Officers THE CORPORATION TRUST COMPANY, agent
Registry Page [https://icis.corp.delaware.gov/Ecorp/...](https://icis.corp.delaware.gov/Ecorp/)

Latest Events

- 2006-01-18 Incorporated
- 2006-01-18 - 2018-06-10 Addition of officer THE CORPORATION TRUST COMPANY, agent

See all events

Corporate Grouping **USER CONTRIBUTED**

None known [Add one now?](#)
See all corporate groupings

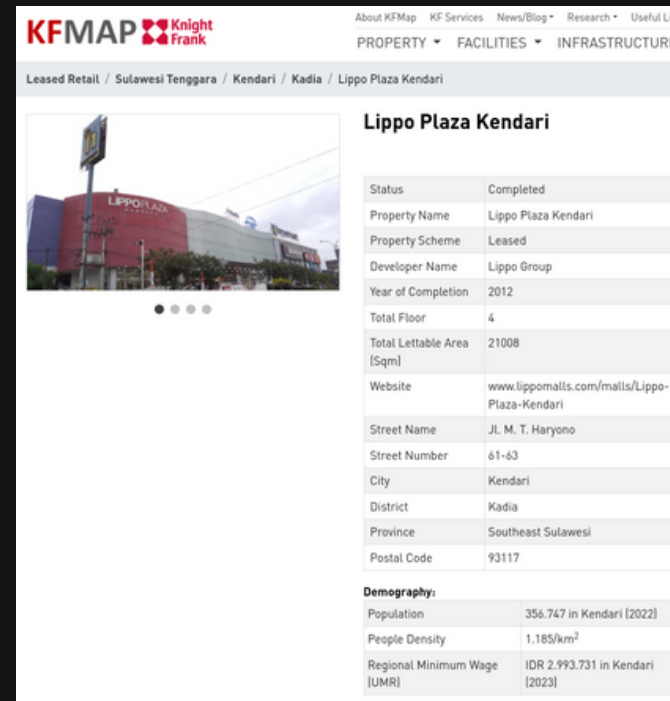
Similarly named companies

Found 26, Showing first 10

- [branch](#) **MANDIANT CORPORATION** (Colorado (US), 9 Feb 2009-)
- [branch](#) **MANDIANT CORPORATION** (New Jersey (US), 8 Jul 2008-)
- [inactive branch](#) **MANDIANT CORPORATION** (Massachusetts (US), 7 Jul 2008-13 Mar 2014)

Source Delaware Department of State, Division of Corporations, <http://www.corp.delaware.gov/>, 30 Aug 2019

OpenCorporates



KFM MAP Knight Frank

About KFM Map KFM Services News/Blog Research Useful Link

PROPERTY FACILITIES INFRASTRUCTURE

Leased Retail / Sulawesi Tenggara / Kendari / Kadia / Lippo Plaza Kendari

Lippo Plaza Kendari

Status Completed

Property Name Lippo Plaza Kendari

Property Scheme Leased

Developer Name Lippo Group

Year of Completion 2012

Total Floor 4

Total Lettable Area (Sqm) 21008

Website www.lippomalls.com/malls/Lippo-Plaza-Kendari

Street Name Jl. M. T. Haryono

Street Number 61-63

City Kendari

District Kadia

Province Southeast Sulawesi

Postal Code 93117

Demography:

Population 356,747 in Kendari (2022)

People Density 1,185/km²

Regional Minimum Wage (UMR) IDR 2,993,731 in Kendari (2023)

KFMap 



Pencarian

CARI RESET

Panduan

☐ Putusan 38

Amar

☐ Lain-lain 33

☐ Tidak dapat diterima 3

Ditemukan 38 data

Urut Berdasarkan - A-Z

Penelusuran terkait : [Pt. mamuang](#); [Pt. paninkorp](#) [Pt bkl](#) [Pt. kitadin](#) [Pt djuandasawit](#) [Pt. realimas](#); [Pt. kavindo](#); [Pt. pritho](#); [Pt. parisal](#);

Pengadilan » PN JAKARTA SELATAN » Perdata

Register : 08-11-2021 — Putus : 30-03-2022 — Upload : 14-09-2022

Putusan PN JAKARTA SELATAN Nomor 1016/Pdt.G/2021/PN JKT.SEL

Tanggal 30 Maret 2022 — Pengugat: OTTO LAMHOT TAMBUNAN, ST

Tergugat:


1.CV PERO INDONESIA

2.[PT TOKOPEDIA](#)

220 — 90

Pengugat: OTTO LAMHOT TAMBUNAN, ST

Tergugat: 1.CV PERO INDONESIA 2.[PT TOKOPEDIA](#)

Direktori Putusan MA




PDDikti 



judyrecords

search anything Search

740 million+
United States Court Cases

[home](#) [terms](#) [info](#) [API](#)

JudyRecord 



NOW WITH OVER 37,000 FREE PUBLIC RECORD LOOKUPS!

BLACK BOOK *ONLINE*.INFO

THE FREE PUBLIC RECORDS SEARCH SITE

FIND FREE PUBLIC RECORD LOOKUPS:

EXAMPLE: DALLAS, TX JAIL

MORE EXAMPLES: LOS ANGELES, CA OR MARICOPA COUNTY COURTS OR FLORIDA CRIMINAL OR TEXAS ARRESTS NOT JOHN SMITH

[SEARCH FOR LOOKUPS](#)

Black Book Online

...and much more

GOOGLE DORKING

Use various search operators to optimise search results.

COMMON OPERATORS:

- " " → has said keyword
- **OR** → has one of the two keywords
- ***** (**wildcard**) → match any word
 - Used with " "
- **AND** → has both keywords
- **-** → exclude keyword
- **()** → groups search operations
- **cache:** → cache of recent pages
- **filetype:/ext:** → files of a certain type
- **site:** → page of a specific website
- **before:** → page created before a certain date
- **after:** → page created after a certain date
- **intitle:** → page with a specific word in the title
- **inurl:** → page with a specific word in its URL
- **intext:** → page with specific words in their content
- **allintitle:/allinurl:/allintext:** → several keywords at once

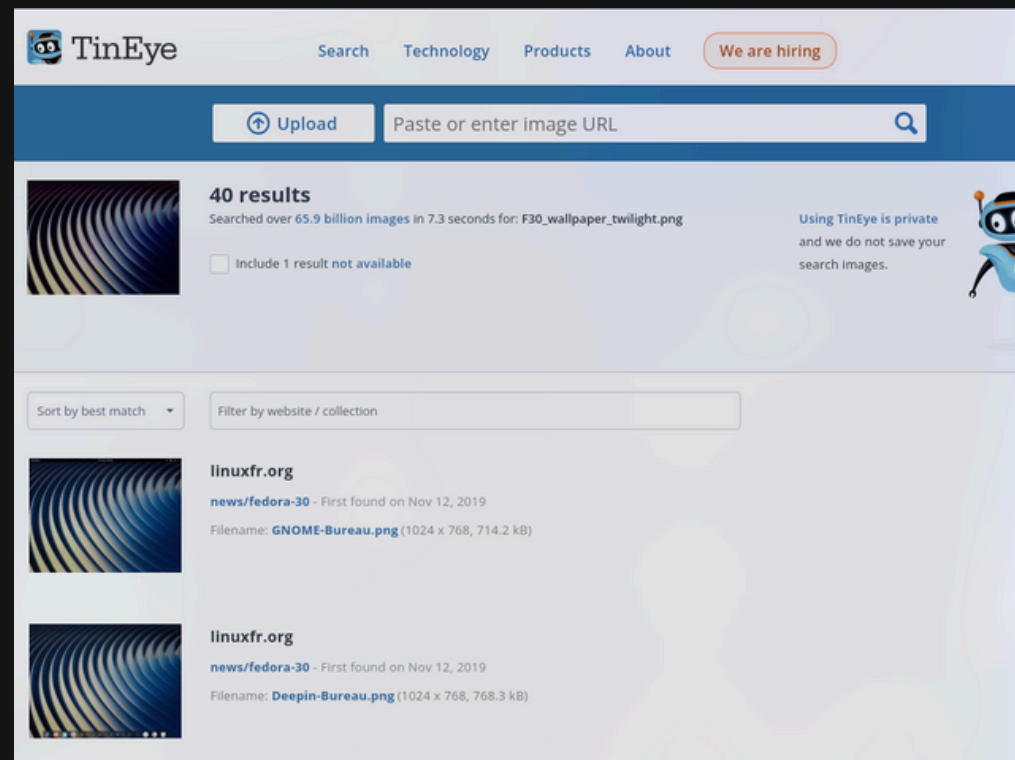
GEOSPATIAL INTELLIGENCE

GEOINT can help geolocate (identify geographical location) and chronolocate (identify time) in image analysis to aid in OSINT investigations.

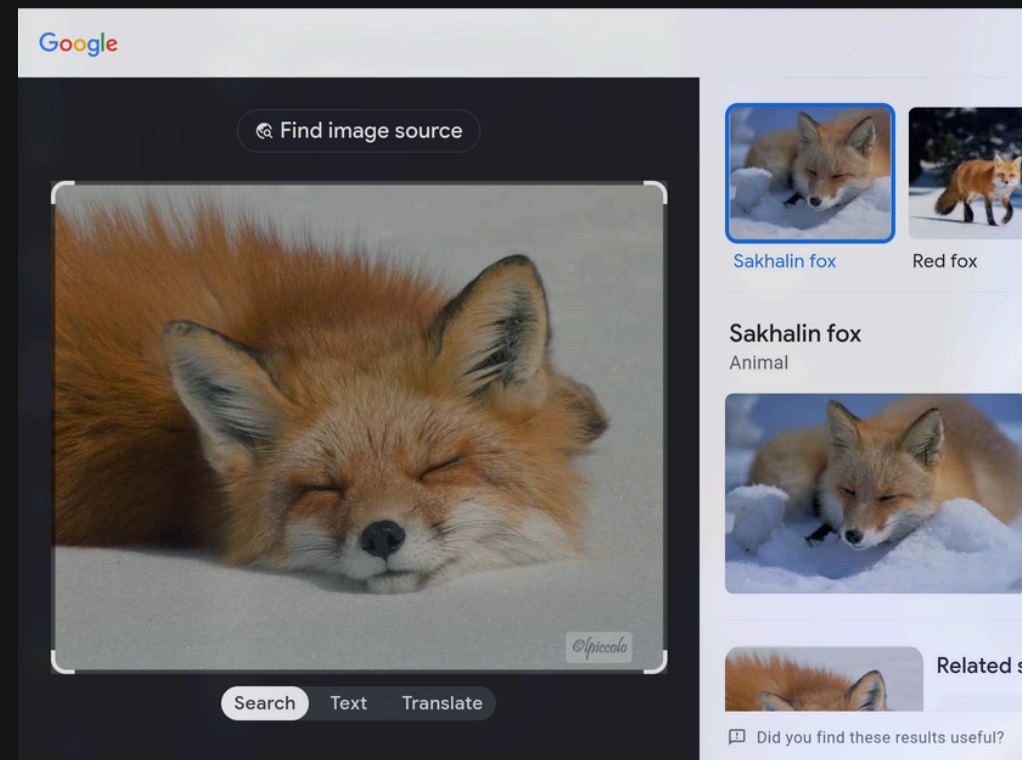


Can you identify where this is taken from?

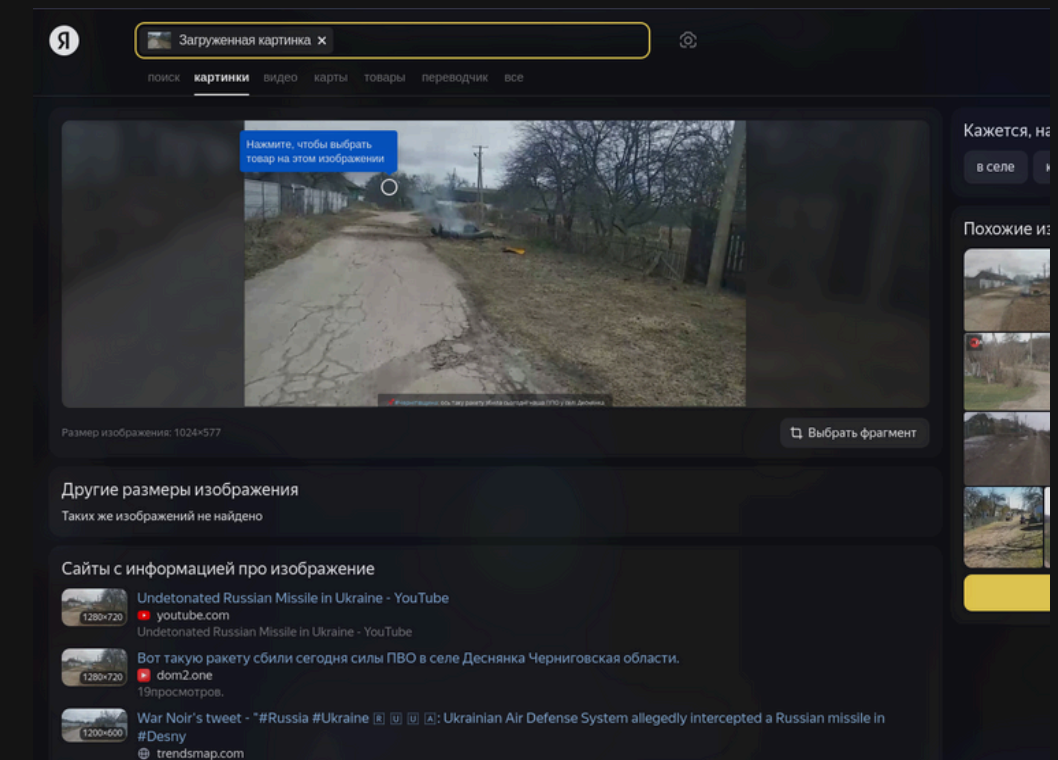
REVERSE IMAGE SEARCH



Tineye (tineye.com)



Google (images.google.com)



Yandex (yandex.ru/images)

CASE STUDY - BELLINGCAT

Finding the Facebook Account of a Paris Suicide Bomber

- November 13, 2015: 6 terrorist attacks in Paris; one near *Stade de France* during a Germany-France football match.
- There are 3 perpetrators; one of them is Bilal Hadfi
- Bellingcat came accross the account "bilal.hadfi.1" on Facebook, which has connection to another account "Billy du Hood."
- "bilal.hadfi.1" has no public photos. However, "Billy du Hood" does have several public photos.
- Identified Bilal Hadfi from a Dutch article.
- There are similarities between the photo in the article and the one uploaded by "Billy du Hood" on Facebook.
 - There is a kind of birthmark between the eyebrows.
 - Both persons wear clothes with the same motif.



BE CAREFUL!

- Identify the use of inflammatory hyperboles in content
- Always use more than one source to prevent bias
- Beware of fake accounts.
 - Usually use a profile photo generated by AI
 - Do a reverse image search to be sure (e.g., TinEye, Google Reverse Image Search, Yandex)
- Be wary of the sources themselves
- If unsure, turn to fact-checking sites (e.g. Snopes)
- Maintain skepticism; don't get carried away by your own bias