

OSINT

Johan van den Broek
Erasmus Brussels University for Applied
Sciences & Arts

© Johan van den Broek, 2025.

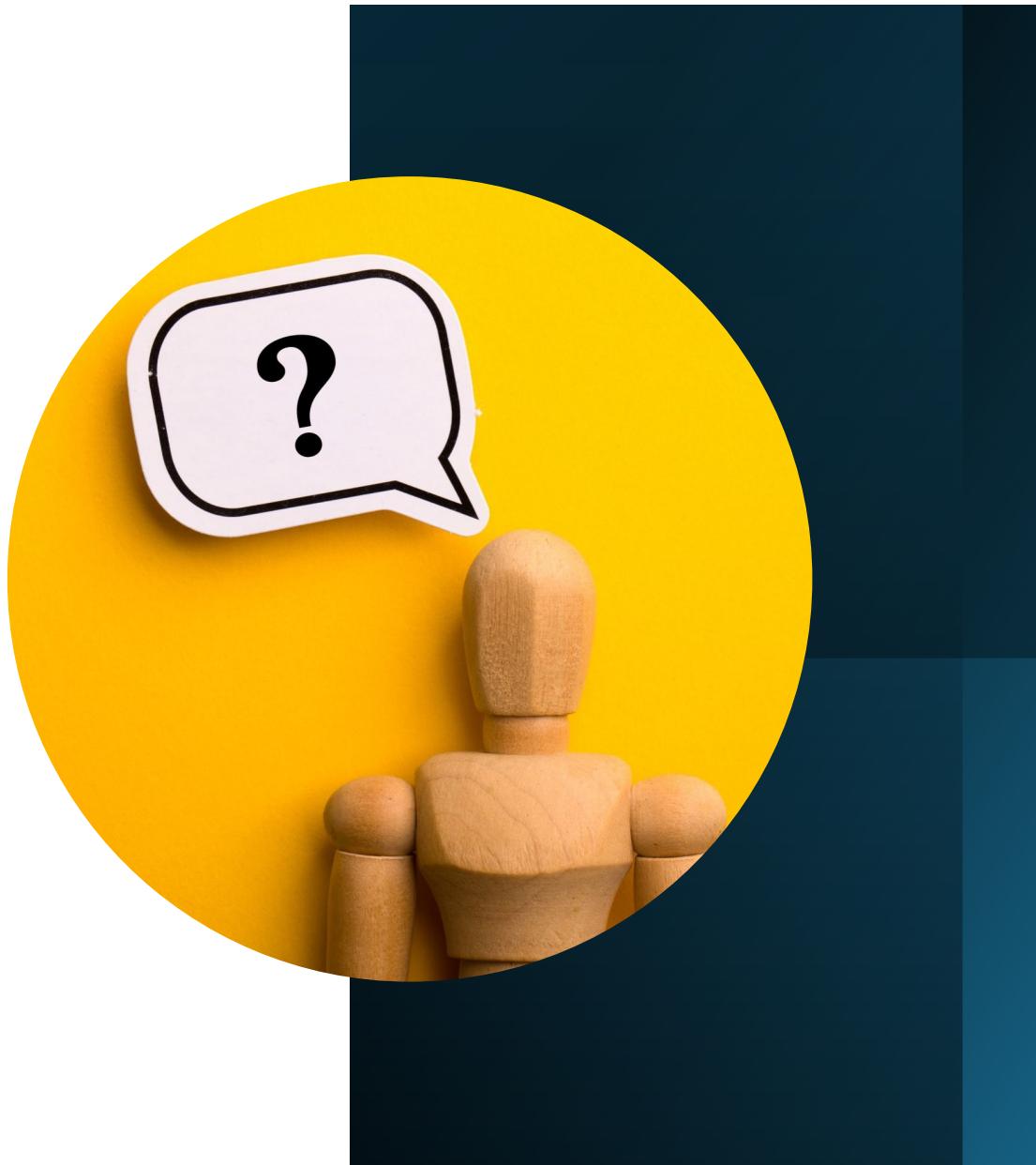
This material may be shared, copied, and reused for educational purposes, provided proper attribution is given to the author.



OSINT workshop files!

<https://github.com/Johanvdb-ehb/BIP-OSINT-Workshop>

What is OSINT?



What is OSINT?

- Open Source Intelligence =
Collecting and analyzing publicly available information to produce actionable insights.
- It's not just "Googling". It's systematic, targeted, and analytical.



What is OSINT?

- Sources may include:
 - Websites, news, public databases
 - Social media platforms
 - Domain/IP information
 - Government records
 - Metadata, images, leaked data

Why is OSINT important?

In cybersecurity / ethical hacking

- Reconnaissance phase of penetration testing
- Identifying vulnerabilities before touching the target
- Mapping infrastructure & technologies
- Understanding people and processes

Real-World Examples



MH17 Airliner Shootdown (2014)



Tracking Russian troop movements via TikTok videos

Case 1: MH17 Airliner Shootdown (2014)

- Malaysia Airlines Flight MH17 was shot down over Eastern Ukraine, killing 298 people.
- Official story (at first): Confusion, blame-shifting, denials.



[NEWSLETTERS](#) [SIGN IN](#) [NPR SHOP](#)

[NEWS](#) [CULTURE](#) [MUSIC](#) [PODCASTS & SHOWS](#) [SEARCH](#)

WORLD

Malaysian Airlines shootdown probe finds 'strong indications' Putin approved missiles

FEBRUARY 8, 2023 · 11:05 AM ET

By The Associated Press



People walk among the debris at the crash site of Malaysia Airlines flight MH17 near the village of Grabovo, Ukraine, on July 17, 2014. All 298 people on board were killed.

Dmitry Lovetsky/AP

Case 1: MH17 Airliner Shootdown (2014)



<https://www.youtube.com/watch?v=RyxliW9m2mM>

Case 1: MH17 Airliner Shootdown (2014)

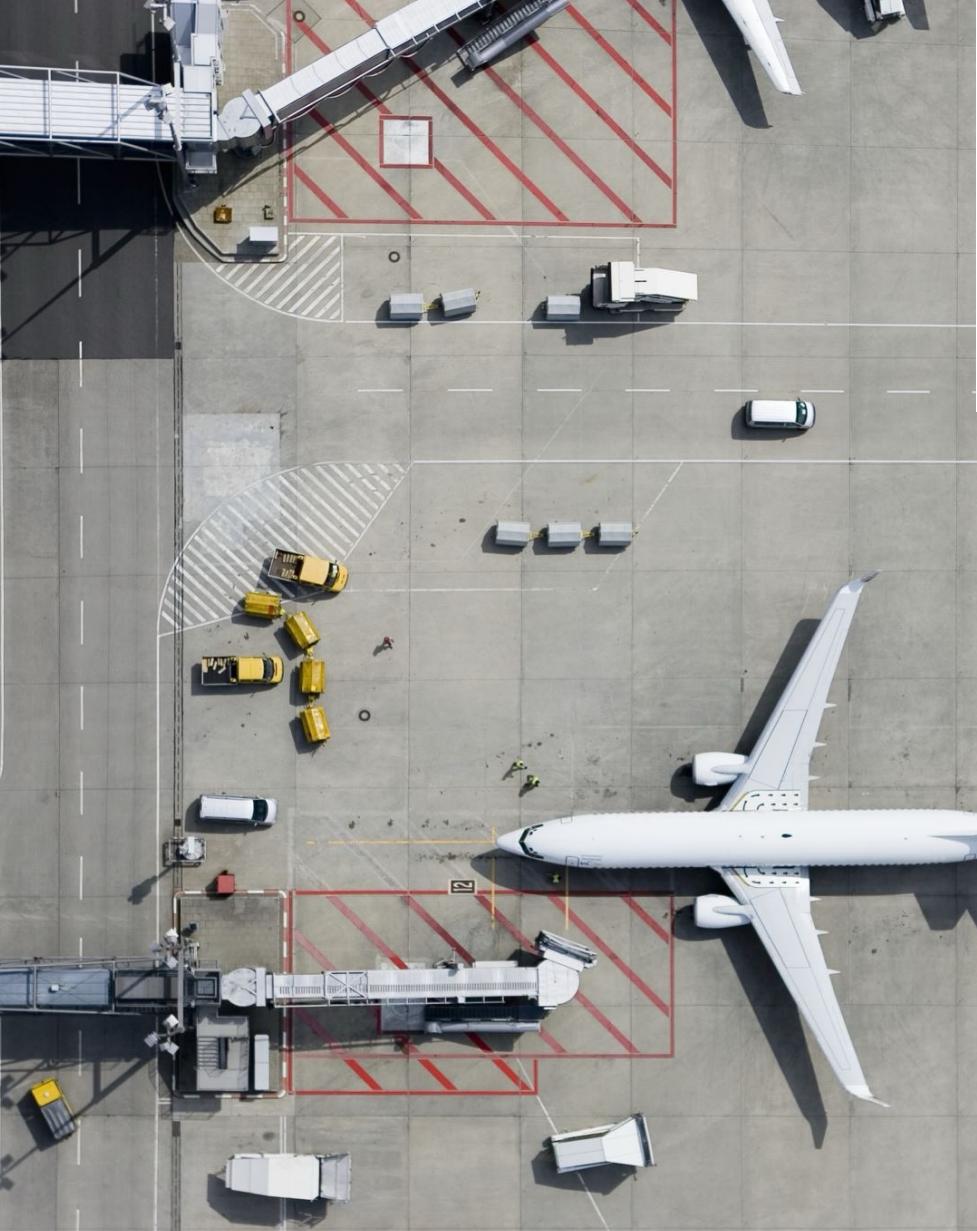
- What Bellingcat (<https://www.bellingcat.com>) did:
- Collect public photos & videos
 - Social media posts from locals
 - Buk missile launcher seen in multiple locations
- Identify unique markings
 - Numbers, paint, dents → match across images



Case 1: MH17 Airliner Shootdown (2014)

- Match background: buildings, trees, road signs
- Use Google Earth / satellite imagery





Case 1: MH17 Airliner Shootdown (2014)

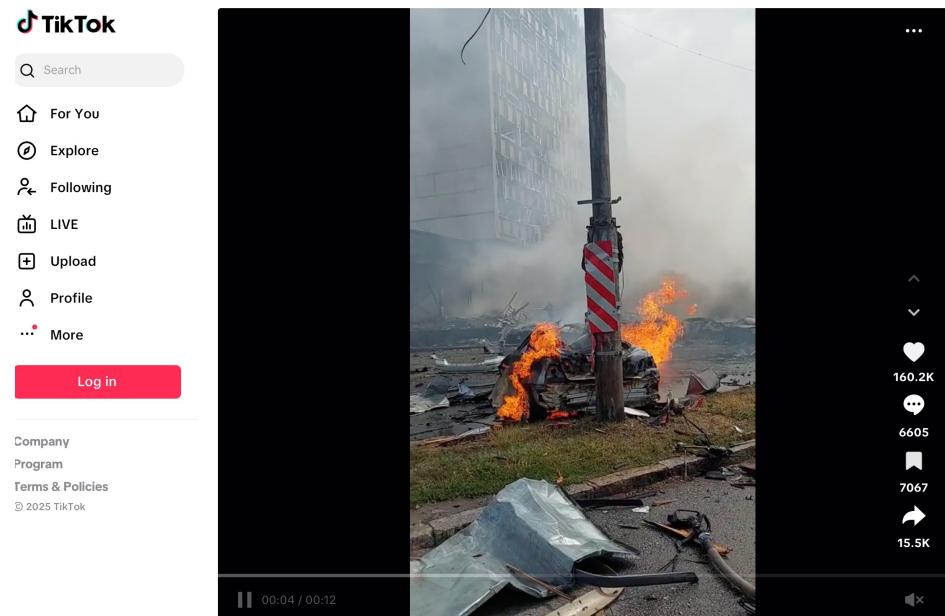
- They proved
 - The Buk came from Russian 53rd Brigade
 - It crossed the border into Ukraine
 - It was near the launch site hours before impact
 - Later seen missing one missile
- Result:
 - Their findings were confirmed by official international investigators and used in court.
- OSINT can solve real-world global crimes with public data only.

Who is Bellingcat?

- Bellingcat is an independent investigative journalism collective founded in 2014.
- They became famous for using OSINT techniques like public data, social media and satellite imagery to uncover the truth in major global events.
- They showed the world that you don't need to be a government or spy agency to do intelligence work. A laptop, internet, and smart analysis can be enough.
- <https://www.bellingcat.com>

Tracking Russian troop movements via TikTok videos

- TikTok's short, highly visual clips created a huge, fast stream of on-the-ground footage during the Ukraine crisis. The clips were often filmed by locals, conscripts, or soldiers themselves. Investigators estimated a large portion of frontline visual evidence came from TikTok.
- TikTok strips EXIF/location metadata from videos, so investigators rely on visual clues, user captions, comments, language, and other posts by the same account to infer origin/time.
- <https://www.bellingcat.com/resources/how-tos/2022/11/02/how-to-investigate-tiktok-using-tiktok-ukraine-research/>



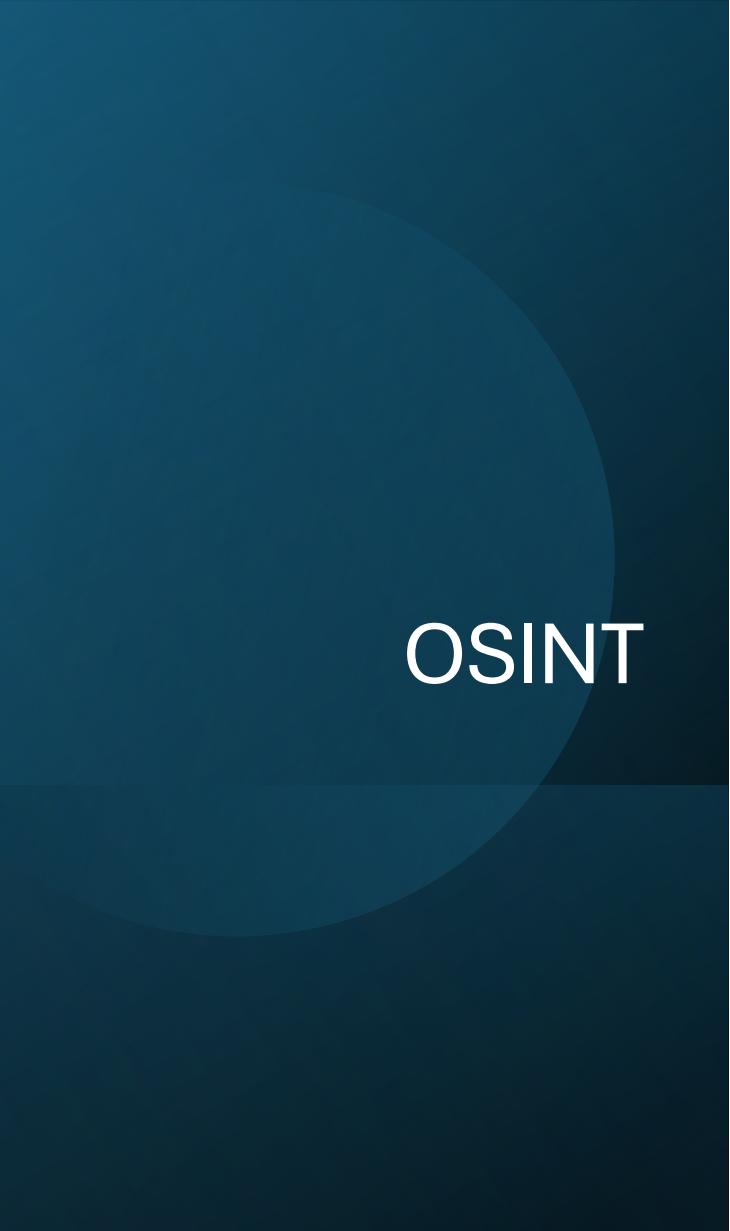
OSINT PRINCIPLES & MINDSET

OSINT is not just searching. It's a PROCESS.



Intelligence Cycle

- Define the question / objective
 - “What exactly do I need to know?”
- Plan & choose sources
 - Where can I find reliable information?
- Collect data
 - Tools, searches, scraping, social media, docs, images,...
- Verify & analyze
 - Check credibility, cross-check, extract insights.
- Produce output
 - Write report / profile / timeline / map.
- Review & repeat
 - Often cyclic. New info = new questions.



OSINT

- OSINT is NOT just finding data.
- It's turning data into intelligence into action.

Data	Raw info	“Johan’s email is...”
Intelligence	Analysis + context + relevance	“This email connects Johan to company/organisation X and explains his role.”

- To produce intelligence, not just collect data.

OSINT goal

Mindset shift for ethical hackers

- **Traditional hacking starts with technical exploitation.**
- **Modern hacking starts with information exploitation.**
- OSINT allows you to:
 - Map infrastructure BEFORE touching it
 - Discover vulnerabilities without scanning
 - Understand the human layer (employees, passwords, behaviors)
 - Reduce noise and stay stealthy
- **“The fewer packets you send, the better the hacker you are.”**

Documentation & Reproducibility

- Why?
 - Keep evidence trail
 - Allow others to verify
 - If you present findings, you must show HOW you got them
- Good habit: record URLs, dates, queries, screenshots!

Legal & Ethical Boundaries

- OSINT is based on public information, but:
 - Legal does not always mean ethical
 - Information can still be sensitive or personal
 - Some sites forbid scraping or automated access
 - Don't expose private individuals unnecessarily

Legal & Ethical Boundaries

- Ask yourself:
 - Should I access this?
 - Should I store/share it?
 - Could this harm someone?
- Golden rule:
 - OSINT = Open Source, but always Responsible.

Exercise: Ethical Dilemma

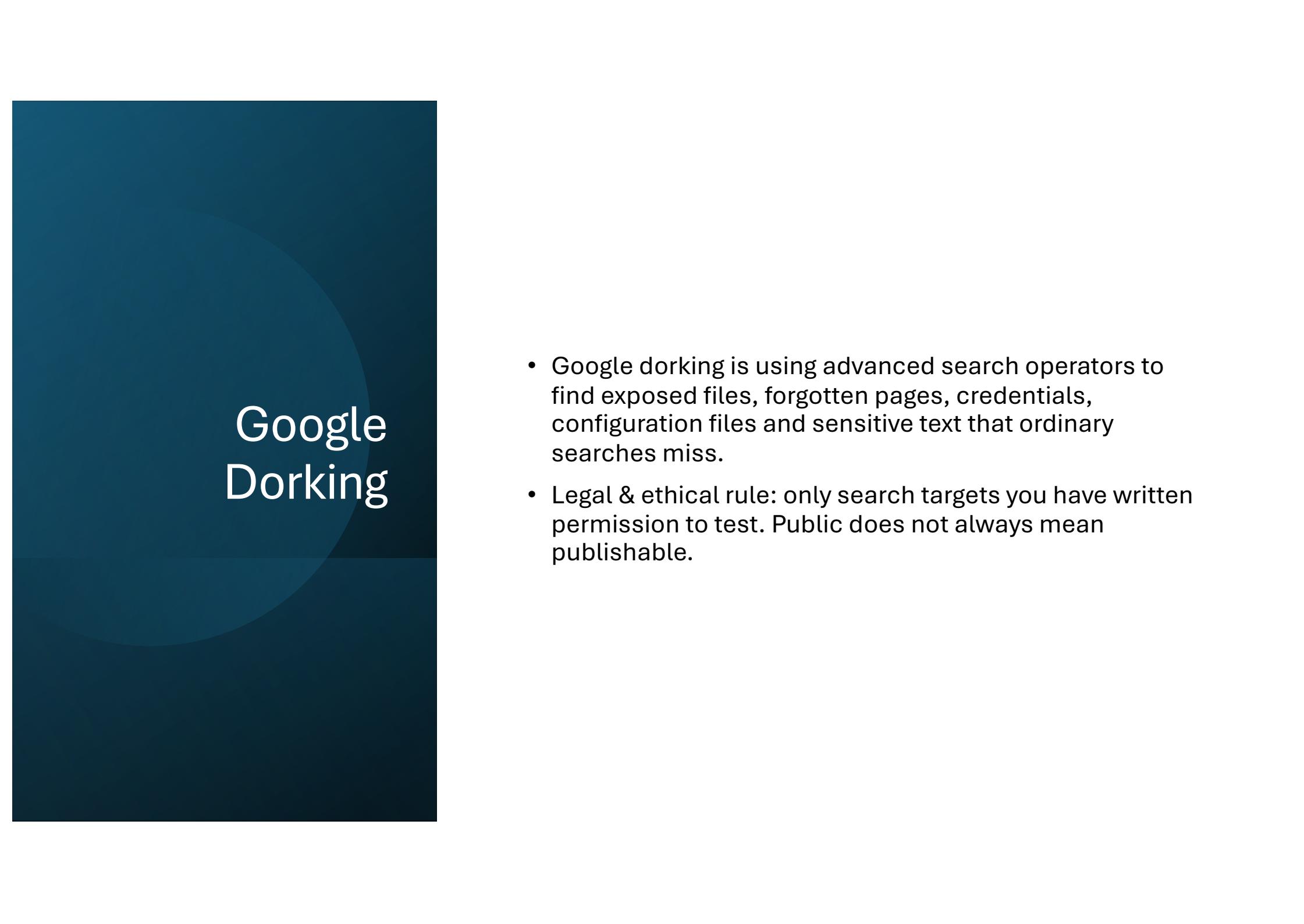
- While researching a client during a reconnaissance task you find a publicly available PDF (on the client's website) that contains an employee's personal phone number. The PDF is clearly internal (labelled "internal" in the filename) but accessible without login.
- Include it in the report? Redact it? Contact client first?



Exercise

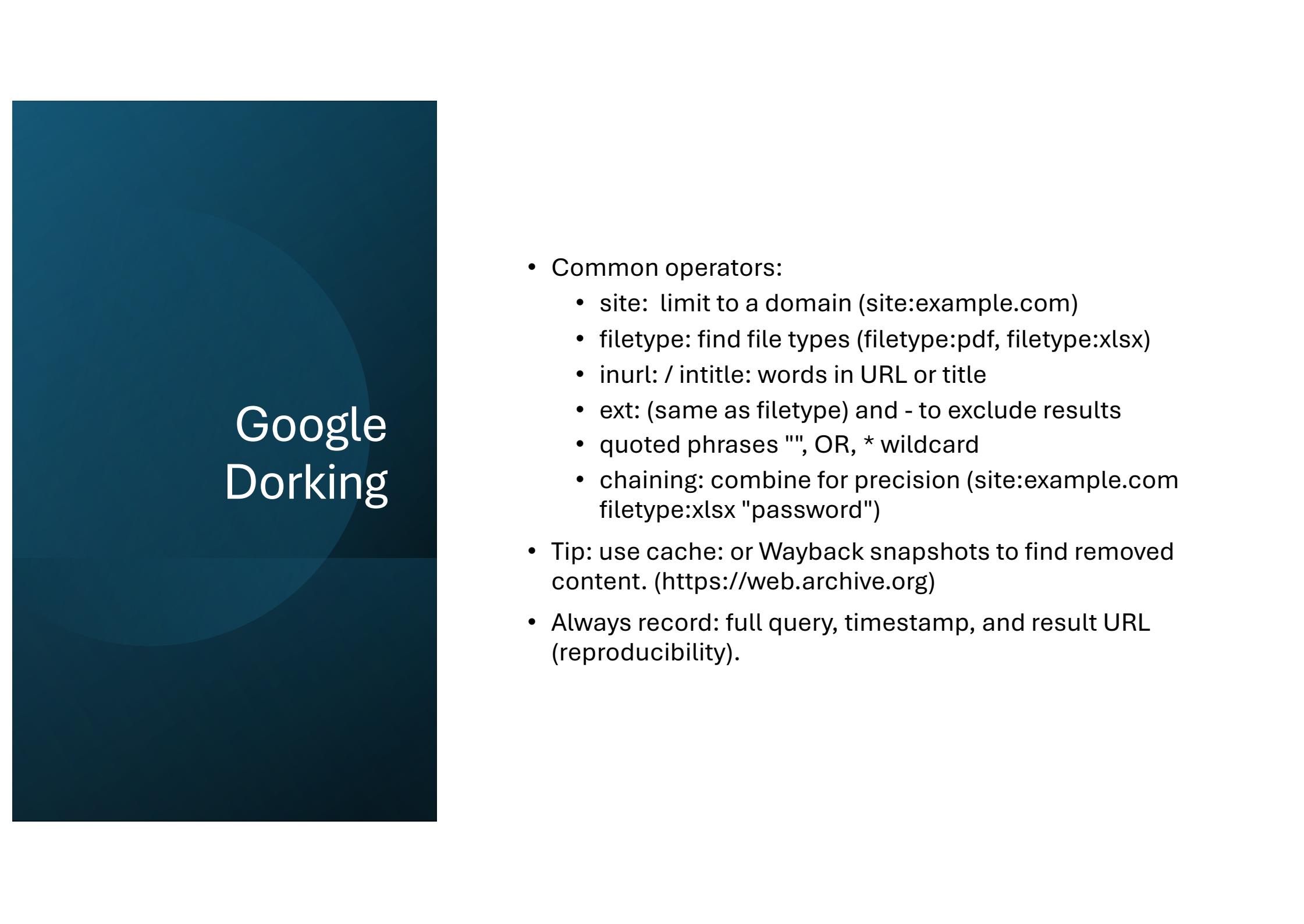
- We are doing a penetration test for ehb.be.
- Can we identify staff members who may be vulnerable to phishing?

Google dorking/hacking



Google Dorking

- Google dorking is using advanced search operators to find exposed files, forgotten pages, credentials, configuration files and sensitive text that ordinary searches miss.
- Legal & ethical rule: only search targets you have written permission to test. Public does not always mean publishable.



Google Dorking

- Common operators:
 - site: limit to a domain (site:example.com)
 - filetype: find file types (filetype:pdf, filetype:xlsx)
 - inurl: / intitle: words in URL or title
 - ext: (same as filetype) and - to exclude results
 - quoted phrases "", OR, * wildcard
 - chaining: combine for precision (site:example.com filetype:xlsx "password")
- Tip: use cache: or Wayback snapshots to find removed content. (<https://web.archive.org>)
- Always record: full query, timestamp, and result URL (reproducibility).

Google Hacking

Advanced operators use the following syntax:

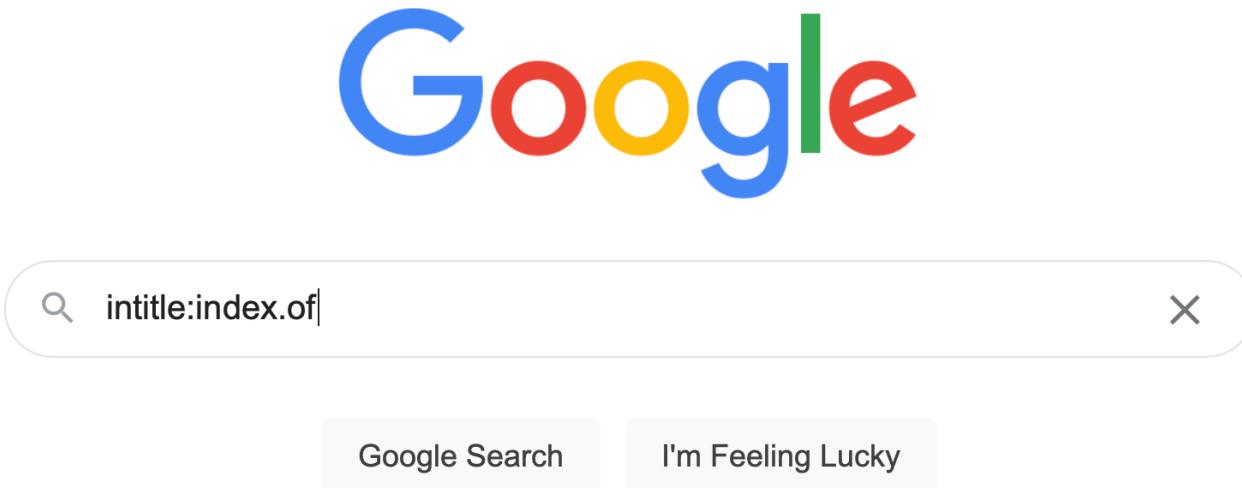
Operator	Purpose	Mixes with other Operators?	Can be used alone?
intitle	Search page title	yes	yes
allintitle	Search page title	yes	yes
inurl	Search URL	yes	yes
allinurl	Search URL	no	yes
filetype	Search specific files	yes	no
allintext	Search text of page only	yes	yes
site	Search specific site	yes	yes
link	Search for links to pages	no	yes
inanchor	Search links anchor text	yes	yes
numrange	Search numbers within a desired range.	yes	yes
daterange	Search in date range	yes	no

Google Hacking

Special Search Characters

Character	Purpose
+	forced inclusion of something common
-	exclude a search term
“ ”	use quotes around search phrases
.	a single wildcard
*	any word
	Boolean ‘OR’
(“master card” mastercard)	Parenthesis group queries

Examples of Google Hacking



- The `intitle:` operator is used to search for specific terms in the title of a webpage.
- For example, `intitle:"index of"` could reveal web servers with directory listing enabled.

Directory listings

intitle:index.of "parent directory"



All

Images

Videos

News

Shopping

More

Tools

About 6.300.000 results (0,24 seconds)

Directory listings

- A basic query that returns a large number of false-positive results:
 - **intitle:index.of**
- These queries return some more interesting stuff:
 - **intitle:index.of "parent directory"**
 - **intitle:index.of name size**

Index of /internet

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 plugins/	2010-02-26 14:04	-	
 servers/	2010-02-26 14:04	-	

Apache/2.4.58 (Ubuntu) Server at tronche.com Port 443

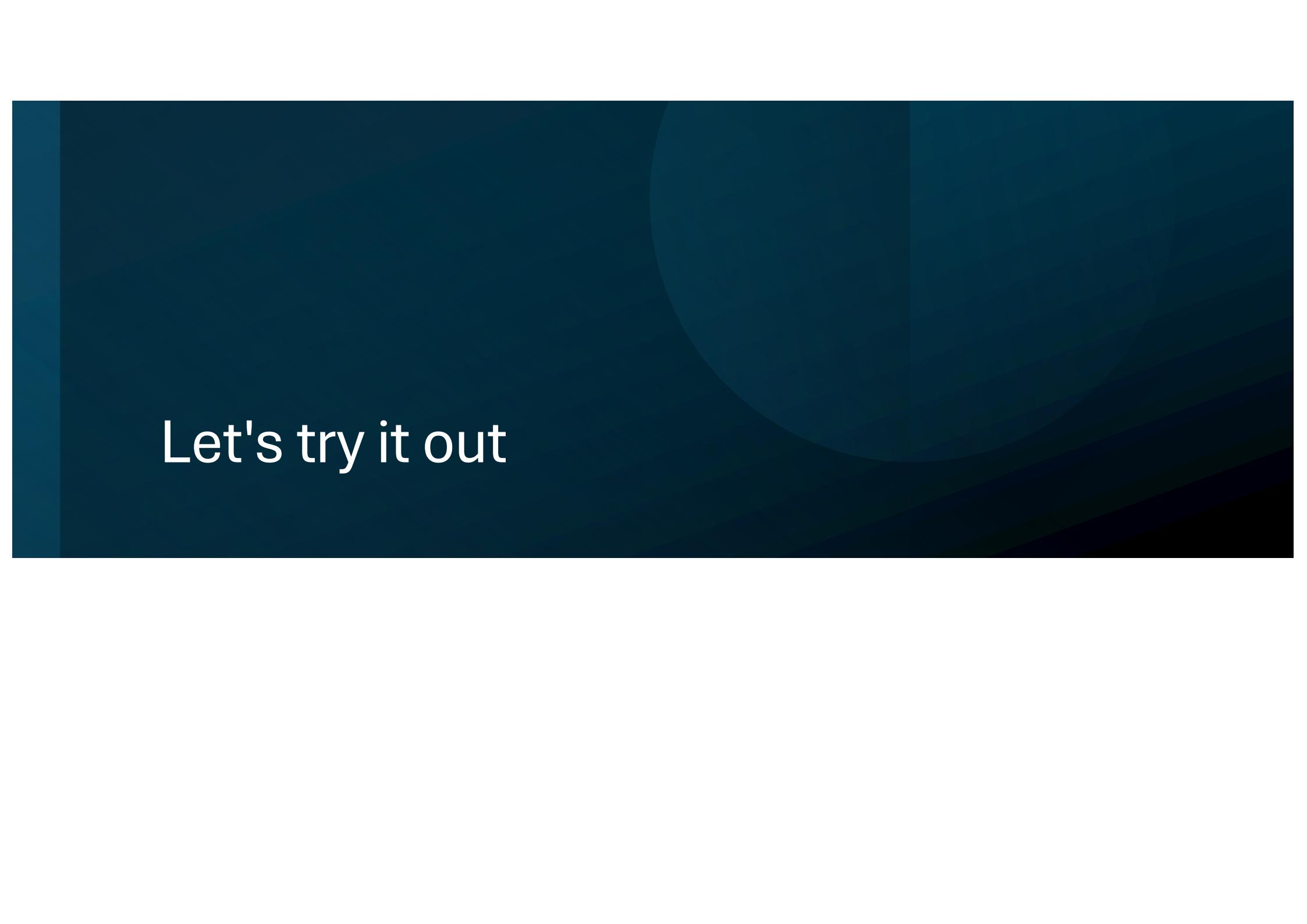
Web Server Detection

- A Security Tester can use this information to determine the version of the web server, or to search Google for vulnerable targets. In addition, this indicates whether the web server is well maintained or not. Query:
 - intitle:index.of server.at
- This query focuses on the term “index of” in the title and “server at” appearing at the bottom of the directory listing.



Discover open vulnerabilities on a network

- You can discover open vulnerabilities on a network. For example, the following provides any page holding the results of a vulnerability scan using Nessus:
 - intitle:"Nessus Scan Report" "This file was generated by Nessus"

The background features a solid dark blue color with a subtle, large circular gradient overlay. This gradient is centered in the upper half of the slide, transitioning from a lighter shade of blue at the top to a darker shade towards the bottom. There are also faint, darker diagonal stripes on the right side.

Let's try it out

Assignment

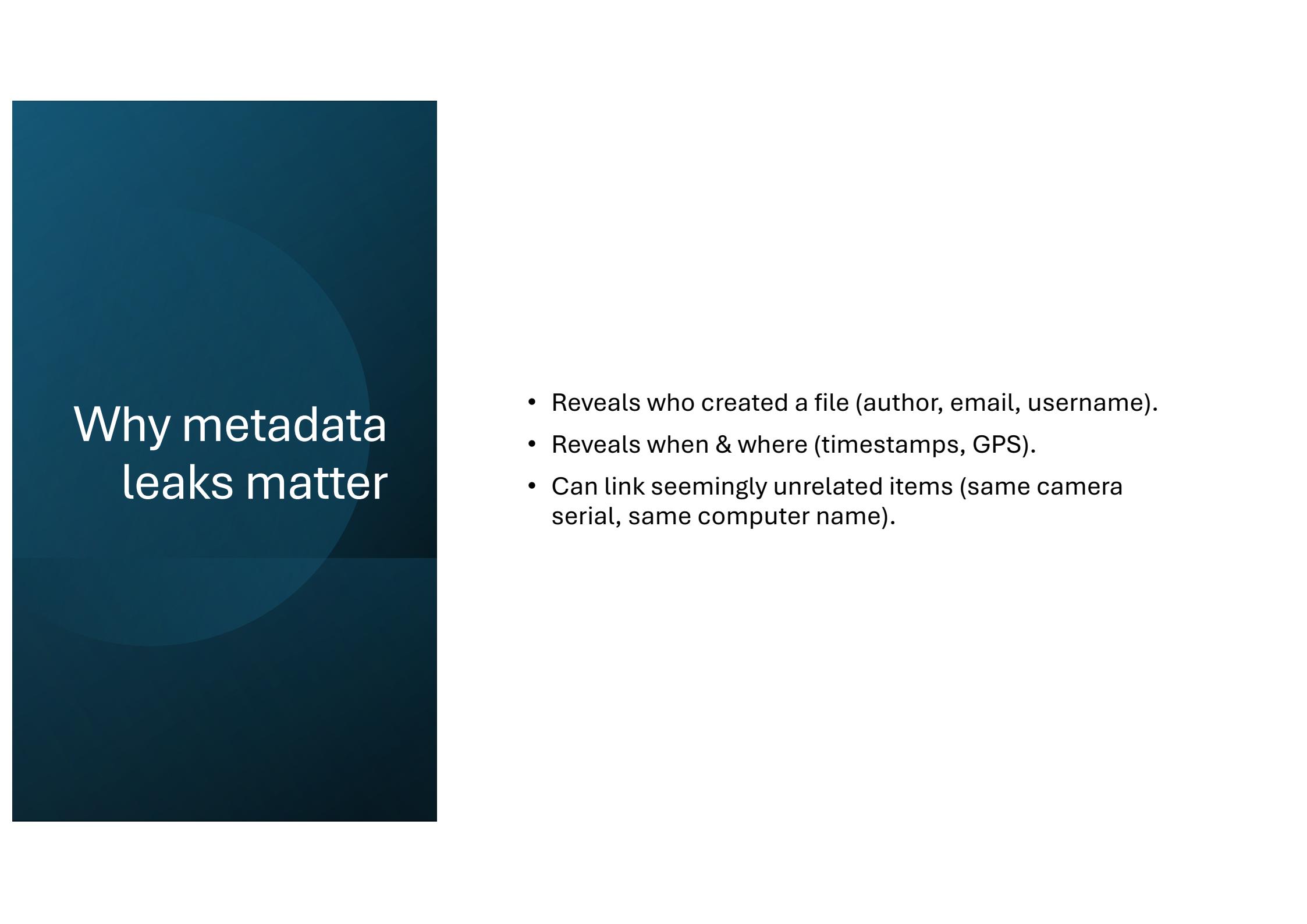
- Let's use Google to search for
 1. Find directory listings (exposed folders / “index of” pages).
 2. Discover public web servers (default pages, server banners).
 3. Locate email lists (email.xls/csv) containing possible Personally Identifiable Information (PII).
 4. Find FTP servers / exposed file shares.
- Check out
 - <https://www.exploit-db.com/google-hacking-database>
- **Dorking is passive. You are only using search engines. Don't attempt to access admin interfaces, authenticate, or exploit anything.**

Metadata & geolocation

Leaking sensitive information

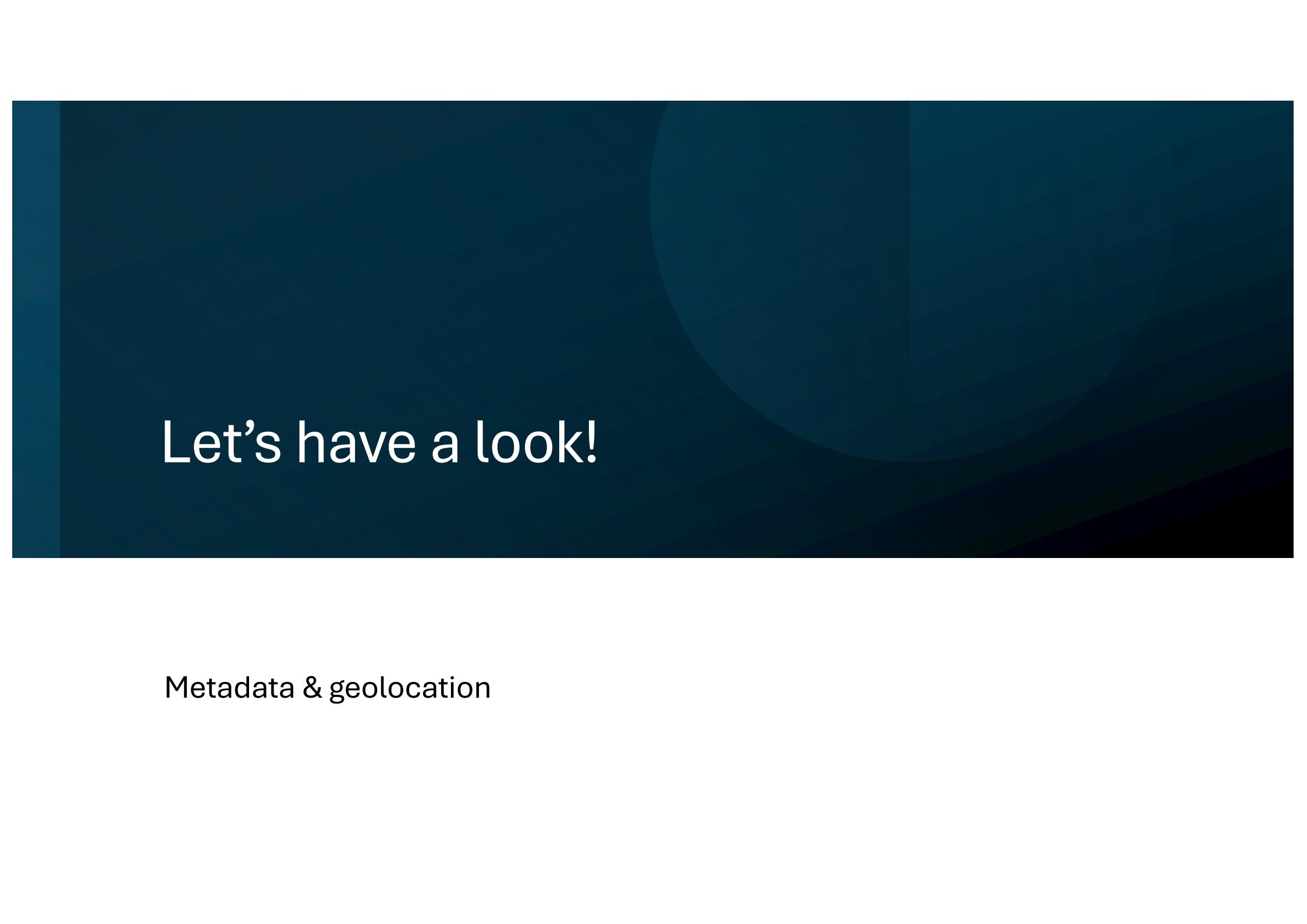
Leaking of sensitive information

- Metadata = information about a file.
- Examples:
 - Photo EXIF: camera model, timestamp, GPS coordinates, ...
 - Office docs (DOCX/PPTX): author name, computer username, editing history, hidden comments.
 - PDFs: title, author, creation/modification timestamps.
 - Images inside docs can carry their own EXIF too.



Why metadata leaks matter

- Reveals who created a file (author, email, username).
- Reveals when & where (timestamps, GPS).
- Can link seemingly unrelated items (same camera serial, same computer name).



Let's have a look!

Metadata & geolocation

Find hidden metadata

- Use a real public image:
 - <https://github.com/ianare/exif-samples/blob/master/jpg/gps/DSCN0010.jpg>
- In Kali terminal

```
wget -O DSCN0010.jpg https://raw.githubusercontent.com/ianare/exif-samples/master/jpg/gps/DSCN0010.jpg
```

```
exiftool DSCN0010.jpg
```

```
exiftool -c "%.6f" DSCN0010.jpg # convert to decimal
```

Google Maps

The screenshot shows a Google Maps interface. At the top left is a search bar containing the coordinates "43°28'02.8"N 11°53'06.5"E". Below the search bar is a blurred image of a city skyline. The main map area shows a location in Arezzo, Italy, with a red pin marking the exact coordinates. The map includes labels for "Passeggio del Prato", "Via Ricasoli", "Via dell'Orto", "Viale Bruno Buozzi", "Palazzo della Fraternità dei Laici", and "Forte". Various icons for "Restaurants", "Hotels", "Things to do", "Transit", and "Park" are visible along the top edge. On the left side of the map, there is a sidebar with options like "Directions", "Save", "Nearby", "Send to phone", and "Share". Below the sidebar, there are buttons for "Add a missing place", "Add your business", "Add a label", and "Layers".

Practical mitigation

- Command to strip EXIF with exiftool:

```
exiftool -all= -overwrite_original DSCN0010.jpg
```

Where is this Starbucks?



<https://img.enjoy-osaka-kyoto-kobe.com/wp-content/uploads/2025/09/26165119/starbucks-coffee-01-1024x678.webp>

Google Image

Google



Add to your search



AI Mode

All

Exact matches

Products

Visual matches

About this image

Feedback



Adobe

二寧坂」の写真素材 | 1,229件の
無料イラスト画像 | Adobe Stock

[See exact matches](#)

Related searches

Ninenzaka



Sannenzaka



Kiyomizu-dera



W Wikipedia
Kyoto – Wikipedia



Wikimedia.org



Video Frame Extraction + Reverse Image Search

- Take any video
- Pause at a moment with background features
- Use screenshot
- Upload frame to Google Images or Yandex Images.

Exercise

- “15 Stunning City Street — Free Stock Footage” youtube
 - <https://youtu.be/MZmWJGzcTX8?si=PAkhHR40GAvscWz9>

```
yt-dlp -f best -o "class_video.mp4" https://www.youtube.com/watch?v=MZmWJGzcTX8
# Extract single frame at 00:00:12.500 (12.5 seconds)
ffmpeg -ss 00:00:12.500 -i video.mp4 -frames:v 1 frame_12_5s.jpg
```

InVID

- InVID = In Video Veritas
- It's a browser plugin and web-based tool that provides a set of forensic utilities to analyze online videos and images.
- It helps users:
 - Detect manipulation
 - Trace source/origin
 - Extract frames from videos
 - Perform reverse image searches
 - Check metadata
 - Analyze image integrity

“Shark on the highway”



FACT-CHECKS

WHO WE ARE

WHAT WE DO

HOW WE FACT-CHECK

GET INVOLVED

A composite image. On the left, a screenshot of a Facebook post shows a photo of a shark in water next to a barrier, with social sharing icons (Facebook, Twitter, WhatsApp, Email, Share) and the caption "Shark swimming on flooded highway? No, image photoshopped". The date "Published on 21 February 2020" is below. On the right, a large red banner with the word "FAKE" in white, bold letters is overlaid across the image, suggesting it is a fake news item.

“Believe it or not, this is a shark on the freeway in Houston, Texas. #HurricaneHarvey,” reads the text of what seems to be a [screenshot of a Twitter post](#), shared on Facebook in South Africa in October 2019.

It [shows](#) a small shark swimming in water flowing alongside some kind of barrier. A rear-view mirror on the right [suggests the image](#) may have been snapped from a car.

[Hurricane Harvey](#) was a storm that hit the coast of Texas in late August 2017, carrying with it massive rainfall and causing severe flooding across the US state.



Africa Check

How?

- Open InVID plugin, right click on image
 - https://en.wikipedia.org/wiki/Hurricane_Shark
- Run quick checks:
 - Reverse image search with at least Google and Bing
 - Metadata tab: any EXIF/IPTC left?
 - Forensic filters (ELA / clone) for obvious anomalies (optional but fun).
- Real or manipulated?

InVid Forensics

- ELA / Compression: shows if parts were edited later.
- Noise Analysis: checks if all areas come from the same source.
- Clone Detection: finds copy-paste areas.
- Magnifier / Deep Learning : look for strange edges, lighting, or AI signs.

- Each filter answers a different question. Combine results to make a smart conclusion.

Shodan

the search engine for the Internet of Things

Safety & ethical rules

- **Discovery only:** documenting banners and ports is allowed; do not attempt to log in, exploit, or run active scans.
- **No changes:** never interact with device management interfaces.
- **Responsible disclosure:** if you find highly sensitive exposures do not publish them. Notify the owner privately via appropriate channels.

Shodan

- **Indexes internet-connected devices** (servers, routers, webcams, IoT, databases).
- **Collects service banners** (open ports, protocol, software/version, TLS certs).
- **Outputs:** IP, ports, banners, geolocation, hostnames, ...
- **Common uses:** asset discovery, attack-surface mapping, vulnerability reconnaissance, monitoring.

- **Ethical reminder:** Discovery only, never exploit or attempt unauthorized access.

TOTAL RESULTS

228,676

TOP COUNTRIES



United States	33,372
Iran, Islamic Republic of	27,258
Malaysia	15,268
Korea, Republic of	15,171
China	14,585

[More...](#)

TOP PORTS

[View Report](#)[Browse Images](#)[View on Map](#)**New Service:** Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)**2.179.139.118**

Data Office of qom for adsl users

Iran, Islamic Republic of, Qom

220 D-Link FTP version 1.0 ready at Fri Jan 7 04:46:26 2000
530 User anonymous cannot log in.
Login failed.

2022-10-02T15:56:41.971843

46.100.76.38

Telecommunication Company of Azarbayejan Gharbi

Iran, Islamic Republic of, Kandovān

SNMP:
Uptime: 11415400
Description: DSL-2600U
Service: 14
Versions:
1
Objectid: 1.3.6.1.4.1.1.2.3.4.5
Name: D-Link

2022-10-02T15:56:26.727232

46.59.28.245

h-46-59-28-245.A980.priv.bahn

HTTP/1.1 200 OK

2022-10-02T15:56:00.923875

Shodan

D-link devices
(popular WiFi router and IoT manufacturer)

Shodan

Find devices in a particular city

 SHODAN Explore Downloads Pricing ↗ apache city:"brussels" 

TOTAL RESULTS
39,798

TOP PORTS

80	19,706
443	15,477
8080	709
5006	469
5005	403

[More...](#)

TOP ORGANIZATIONS

Google LLC	21,238
Proximus NV	1,954
Combell NV	896

 View Report  View on Map

New Service: Keep track of what you have connected to the Internet. Check out [Shodan M](#)

Superpan | Nuevo tablero de FINSA ↗

35.233.20.70
70.20.233.35.bc.googleusercontent.com
superpan.finsa.com
Google LLC
Belgium, Brussels

 cloud

 **SSL Certificate**
Issued By:
|- Common Name:
R3
|- Organization:
Let's Encrypt
Issued To:
|- Common Name:
superpan.finsa.com

HTTP/1.1 200 OK
Date: Sun, 02 Oct 2022 16:38:23 G
Server: Apache
X-Powered-By: PHP/7.2.13
Link: <https://superpan.finsa.com>
X-Frame-Options: SAMEORIGIN
X-Mod-Pagespeed: 1.13.35.2-0
Vary: Accept-Encoding
Ca...

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

Apache HTTP Server Test Page powered by CentOS ↗

34.76.117.10
HTTP/1.1 403 Forbidden

Results

- IP address & reverse DNS (top)
- Open ports list (left column)
- Service banners (HTTP headers, SSH banner, product/version)
- Location & ISP / Org (where the IP is registered)
- Port history / last update (when Shodan last saw the host)
- HTTP page preview and screenshots (if available)

TOTAL RESULTS
4

TOP COUNTRIES

Country	Count
Belgium	2
Netherlands	2

TOP PORTS

Port	Count
443	3
179	1

TOP ORGANIZATIONS

Organization	Count
Erasmushogeschool Brussel	2
Microsoft Corp	1
Microsoft Corporation	1

193.191.183.6
smtp.ehb.be
Erasmushogeschool Brussel
Belgium, Antwerpen

193.191.131.111
cds.ehb.be
desdenius.ehb.be
Erasmushogeschool Brussel
Belgium, Jette

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

View Report | View on Map | Advanced Search

HTTP/1.1 303 See Other
Date: Tue, 14 Oct 2025 22:36:54 GMT
Server: Apache
Set-Cookie: PHPSESSID=ak3bzjel3idquntfikpt6ellg2; path=/; SameSite=Lax
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Set-Cookie: SimpleSAML=9tjtoolloz7dbb...
2025-10-14T22:36:54.205400

HTTP/1.1 302 Found
Date: Sat, 11 Oct 2025 19:05:59 GMT
Server: Apache/2.4.23 (Ubuntu)
Strict-Transport-Security: max-age=63072000; includeSubdomains;
Cache-Control: max-age=9, private, must-revalidate
Set-Cookie: 14321862712f18bb34adef48631d0fdc=o4h4cjtl1h50lroaeb06r3pnd; path=/
Location: ...
2025-10-11T19:05:59.156940

Results

Apache » Http Server » 2.4.52																							
Vulnerabilities (37)		Metasploit Modules																					
Version names																							
<ul style="list-style-type: none">Apache Software Foundation Apache HTTP Server 2.4.52cpe:2.3:a:apache:http_server:2.4.52:**:**:**:**cpe:/a:apache:http_server:2.4.52																							
Product information																							
<ul style="list-style-type: none">https://httpd.apache.org/download.cgi Change Log																							
Vulnerabilities by types/categories																							
Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation	CVE											
2022	2	0	0	0	0	0	0	0	0	0	0	CVE-2022-22964											
2023	0	0	0	0	0	0	0	0	0	0	0	CVE-2023-21974											
2024	0	1	0	0	0	0	0	0	4	0	0	CVE-2024-21974											
2025	0	0	0	0	0	0	0	0	2	0	0	CVE-2025-21974											

The screenshot shows the Shodan search interface with the query "product:MongoDB country:LT". The results page displays 80 total results. Key sections include:

- TOTAL RESULTS:** 80
- TOP CITIES:**
 - Vilnius: 66
 - Šiauliai: 11
 - Kaunas: 1
 - Panėvėžys: 1
 - Telsiai: 1
- TOP PORTS:**
 - 27017: 76
 - 3000: 1
 - 5432: 1
 - 5555: 1
 - 30111: 1
- TOP ORGANIZATIONS:**
 - UAB Interneto vizija: 33
- Product Spotlight:** We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)
- Results List:** Three examples are shown in detail:
 - 185.80.130.105**: mail.tg-holding.com, UAB ESNET, Lithuania, Vilnius. Database. MongoDB Server Information. Authentication partially enabled. Partial JSON output:

```
{  "storageEngines": [    "devnull",    "wiredTiger"  ],  "buildEnvironment": {    "distarch": "x86_64",    "cc": "/opt/mongodbtoolchain/v4/bin/gcc: gcc (GCC) 11.3.0",    "cppdefines": "SAFEINT_USE_I..."  }}
```

Timestamp: 2025-10-19T15:10:40.571533
 - 31.97.206.203**: srv1022348.hstgr.cloud, Hostinger Operations, UAB, Lithuania, Vilnius. Database. MongoDB Server Information. Authentication partially enabled. Partial JSON output:

```
{  "storageEngines": [    "devnull",    "wiredTiger"  ],  "buildEnvironment": {    "distarch": "x86_64",    "cc": "external:/mongo_toolchain_v4/v4/bin/gcc: gcc (GCC) 11.3.0\nCopyright (C) 2021 Free Software..."}}
```

Timestamp: 2025-10-19T08:49:11.887286
 - 217.147.15.189**: Elisteka UAB, Lithuania, Vilnius. MongoDB Server Information.

product:MongoDB country:LT

Exposed databases

The screenshot shows the Shodan search interface with the query "port:3389 country:DE". The results page displays 169,734 total results. Key sections include:

- TOP CITIES:** Frankfurt am Main (65,025), Falkenstein (21,351), Berlin (20,647), Düsseldorf (19,445), Nürnberg (13,608).
- TOP ORGANIZATIONS:** Contabo GmbH (33,840), Hetzner Online GmbH (26,258), IONOS SE (19,327), Deutsche Telekom AG (8,626), OVH GmbH (4,660).
- TOP PRODUCTS:** Remote Desktop Protocol (159,473).
- Product Spotlight:** We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#).
- Results List:** Three examples are shown:
 - 43.157.79.102**: Issued by Asia Pacific Network Information Center, Pty. Ltd. (Germany, Frankfurt am Main) via eqi-os self-signed SSL Certificate. Details: Remote Desktop Protocol, OS: Windows 8.1/Windows Server 2012 R2, Build: 6.3.9608, Target Name: 10_0_16_4, NetBIOS Domain Name: 10_0_16_4, NetBIOS Computer Name: 10_0_16_4, DNS Dom... (2025-10-19T16:02:09.822559)
 - 4.182.232.192**: Issued by Microsoft Corporation (Germany, Frankfurt am Main) via cloud self-signed SSL Certificate. Details: Remote Desktop Protocol, OS: Windows 11, Build: 10.0.26100, Target Name: GERPC001, NetBIOS Domain Name: GERPC001, NetBIOS Computer Name: GERPC001, DNS Domain Name: GERPC001, FQDN: G... (2025-10-19T16:00:15.080103)
 - 5.231.226.39**: play2go.cloud - Cheap and reliable hosting (Germany, Frankfurt am Main) via SSL Certificate. Details: Remote Desktop Protocol, OS: Windows 10, Build: 10.0.26100, Target Name: GERPC001, NetBIOS Domain Name: GERPC001, NetBIOS Computer Name: GERPC001, DNS Domain Name: GERPC001, FQDN: G... (2025-10-19T15:59:50.613137)

port:3389 country:DE

High-risk remote access (RDP)

Assignment

- Use Shodan to discover publicly exposed webcams/cameras.
- **This is discovery only which means no logins, no control attempts, no downloading or sharing images.**



Maltego

Maltego?

- Maltego is a powerful data mining and information gathering tool used for open-source intelligence (OSINT) gathering and footprinting.
- It provides a graphical interface that enables users to visualize and explore relationships and connections between various entities, such as people, organizations, websites, email addresses, domains, and more.
- Maltego allows analysts, investigators, and security professionals to conduct investigations and gather intelligence by aggregating and analyzing data from multiple sources.

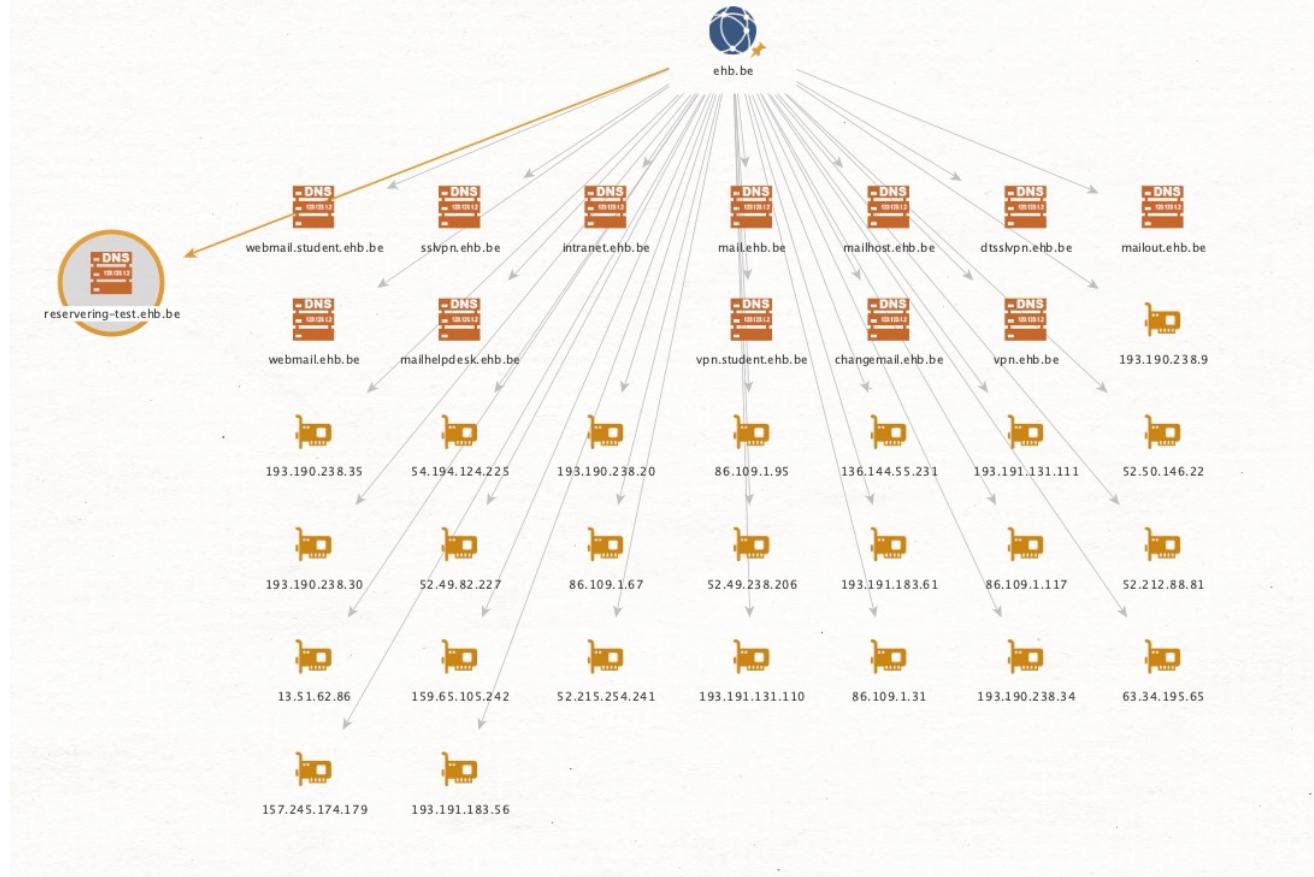
Maltego CE / Basic plan

- CE is free but limits transforms / results (rate limiting and fewer commercial transforms).
- Many useful transforms (Shodan, Censys, FullContact, WhoisXML API) need API keys (you can often times use them for free but you do need to register on their platforms)
- CE is intended for learning and non-commercial OSINT.

Demo

- New Graph: from the left palette drag a Domain entity onto the canvas.
- Double-click it, set value to ehb.be (or kaunokolegija.lt)
- Right-click the Domain node → Run Transform → choose:
 - To DNS Name / DNS from Domain
 - To IP Address (resolve A records)
 - Expand a discovered subdomain, right-click → To IP Address, then on IP

Result



Explanation

- ehb.be
 - This is the starting point — the official domain of the institution.
- Middle layer: Subdomains (DNS names)
 - Examples we found:
 - webmail.student.ehb.be
 - sslvpn.ehb.be
 - intranet.ehb.be
 - mail.ehb.be
 - changemail.ehb.be
 - vpn.ehb.be

Explanation

- Why subdomains matter:
 - Each subdomain = a specific service (mail, VPN, intranet, test environment...)
 - This reveals what technology the organization uses internally.
 - “test” / “intranet” / “vpn” often = high-value targets for attackers.

Explanation: Bottom layer: IP Addresses (Servers)

- Each subdomain resolves to one or more IP addresses.
- Example IPs:
 - 193.190.238.35
 - 52.215.24.241
 - 136.144.55.231
 - 157.245.174.179
 - 13.51.62.86
 - ...many more

Explanation

- Why IPs matter:
 - This tells us where the service is hosted (on-premise, cloud, VPN, data center).
- IPs can be looked up in Shodan to see:
 - open ports
 - software versions
 - vulnerabilities
 - Multiple subdomains pointing to same IP = same server hosting many services.

Key Observations

- They have multiple mail systems (mail.ehb.be, mailhost.ehb.be, mailstudent.ehb.be)
 - email infrastructure is complex, so maybe potential misconfigurations.
- There are VPN endpoints (vpn.ehb.be, sslvpn.ehb.be, vpn.student.ehb.be)
 - crucial entry points, they must be secured and up to date.
- Intranet and helpdesk visible from public DNS
 - internal tools may be exposed to the internet (risky if not protected).

Key Observations

- reservering-test.ehb.be
 - "test" subdomain is a red flag.
 - Test environments often:
 - have weak security
 - use default credentials
 - are forgotten/unpatched

Why this graph is powerful in OSINT / Ethical Hacking

- It shows the attack surface:
 - All exposed services
 - What runs where
 - Which parts might be forgotten or weak
- From here, an analyst can:
 - Prioritize high-risk systems
 - Check Shodan for vulnerabilities
 - Connect infrastructure to people (next step!)

Next?

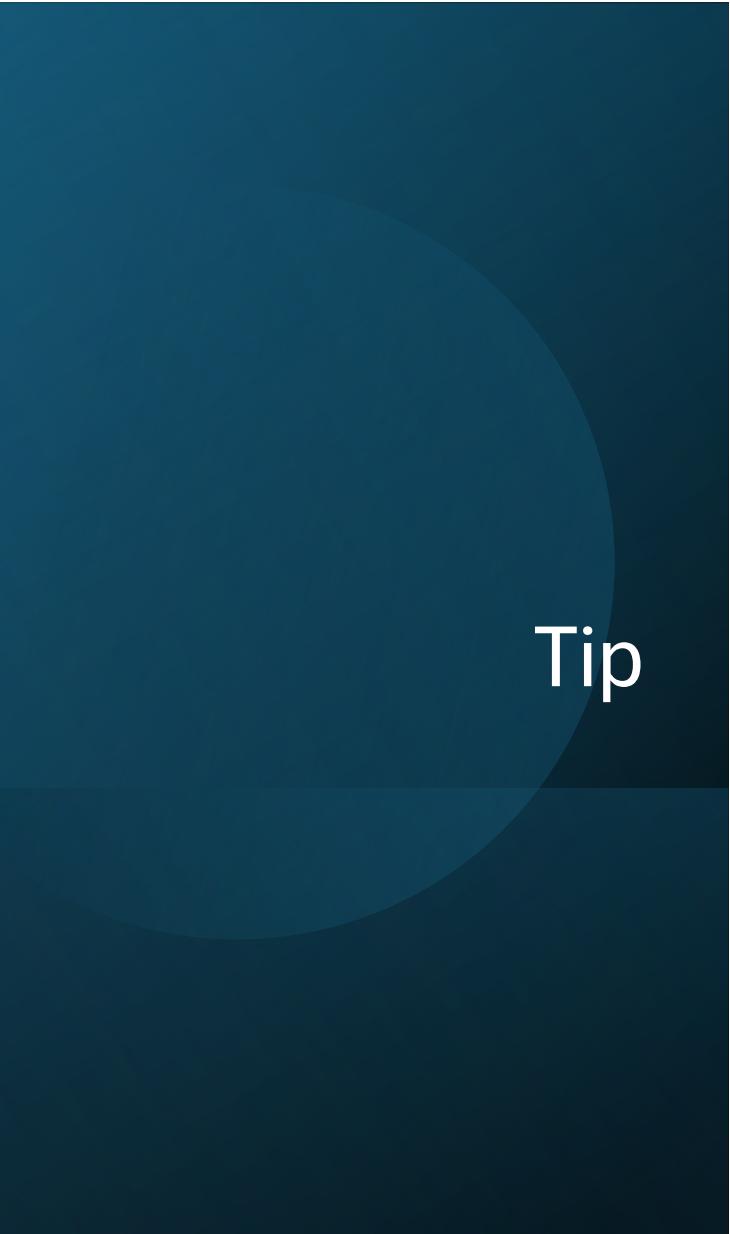
- From here, an analyst can:
 - Prioritize high-risk systems
 - Check Shodan for vulnerabilities
 - Connect infrastructure to people (next step!)

Maltego assignment

Map your online presence

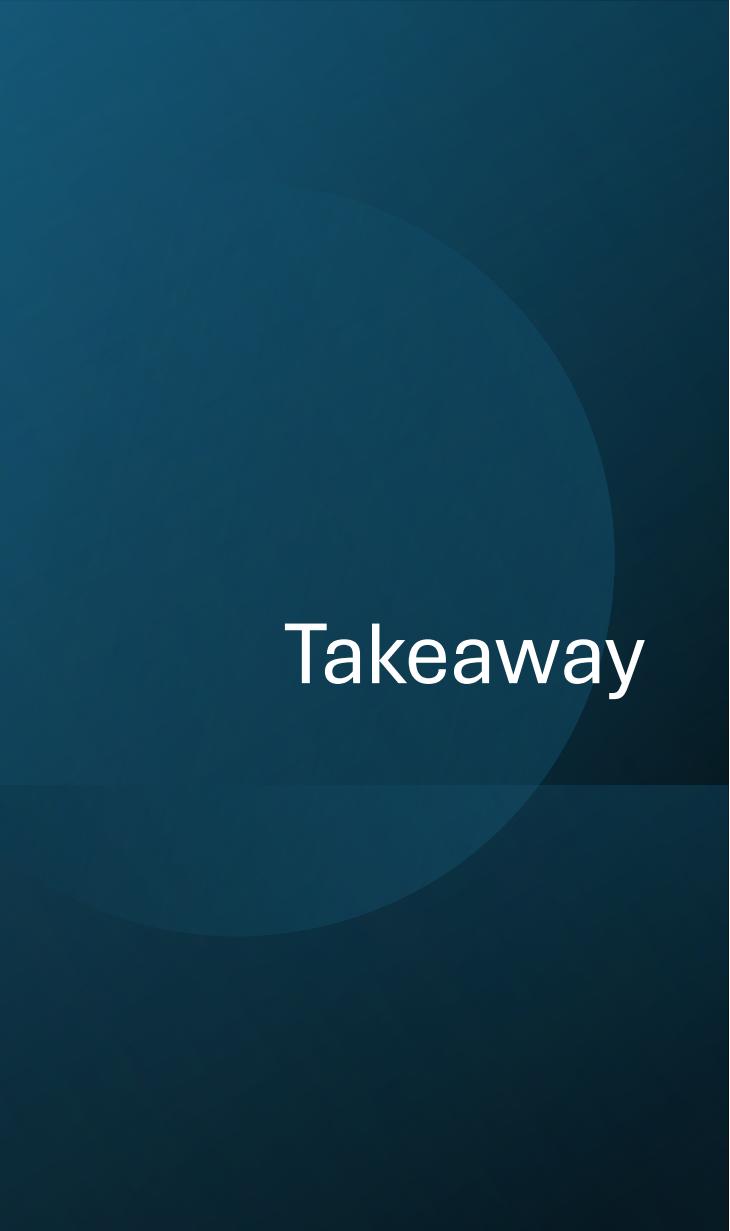
Map your online presence

- Build a Maltego graph of your public footprint and identify one privacy risk
- Use Maltego to collect and visualise publicly available links, social profiles, domains, and leaked references about yourself then triage and recommend 3 quick privacy fixes.



Tip

- For example:
 - To Person → (if starting from email)
 - To Email addresses (find associated emails)
 - To Domain / To DNS Name (from personal website or email domain)
 - To Website → To URL → To Links (discover linked pages)
 - Search Engines
 - To Social Profiles / To Twitter Account / To LinkedIn Profile (where available)
 - To WHOIS (from domain)
 - HaveIBeenPwned transform
 - In Maltego, find a profile/website node → To URL → click the page → copy image URL of avatar. Open a browser and upload that image to Google Images.



Takeaway

- OSINT = Skill + Mindset + Responsibility
- Tools change, mindset stays.
- Information is power, context is intelligence.
- Everything you do leaves a trace, so act with integrity.