Open Source Intelligence

A Quickstart Guide



Lukas M
Lukas@physsec.org

What is OSINT?

- Open Source
- Intelligence

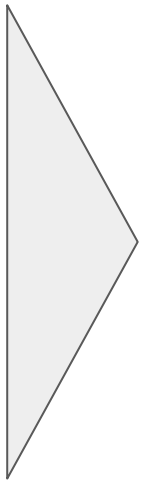
Can be any information found online, as long as you do not interact or ‘touch’ anything to find it

(No breaking into emails or other accounts)

Commonly used resources

Sources of Information

- Facebook
- Linkedin
- Twitter
- Instagram
- Yelp
- Google Maps
- Tiktok



What OSINT experts gain from these sites

- Name
- Age
- Location (Also frequented places)
- Known associates
- Car information
- Family
- Where you work
- What you invest your time in

Tools

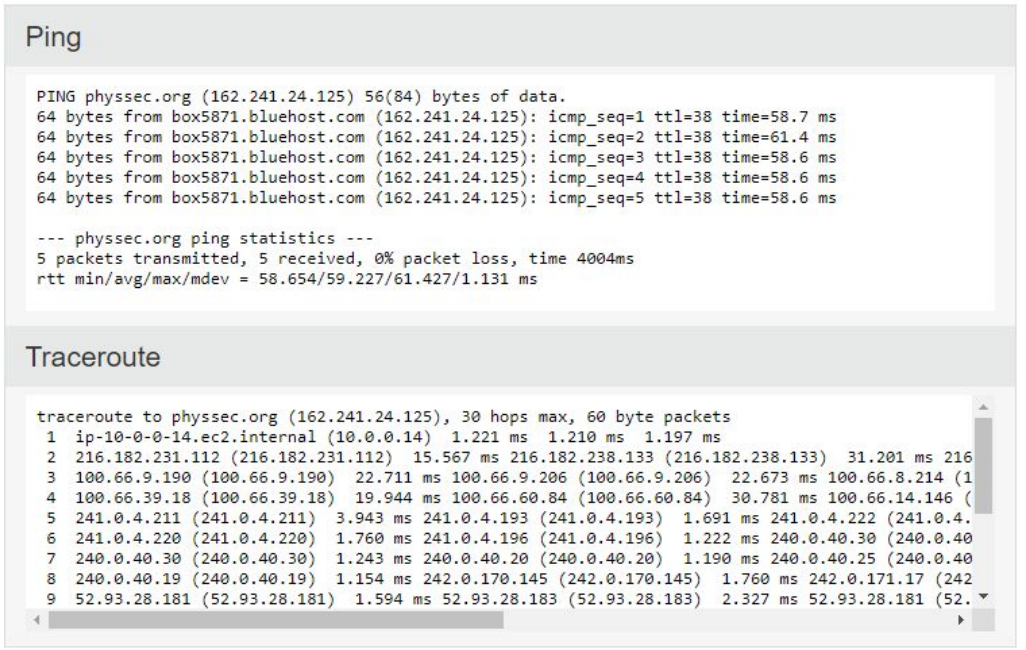
Maltego

https://www.maltego.com/



whois

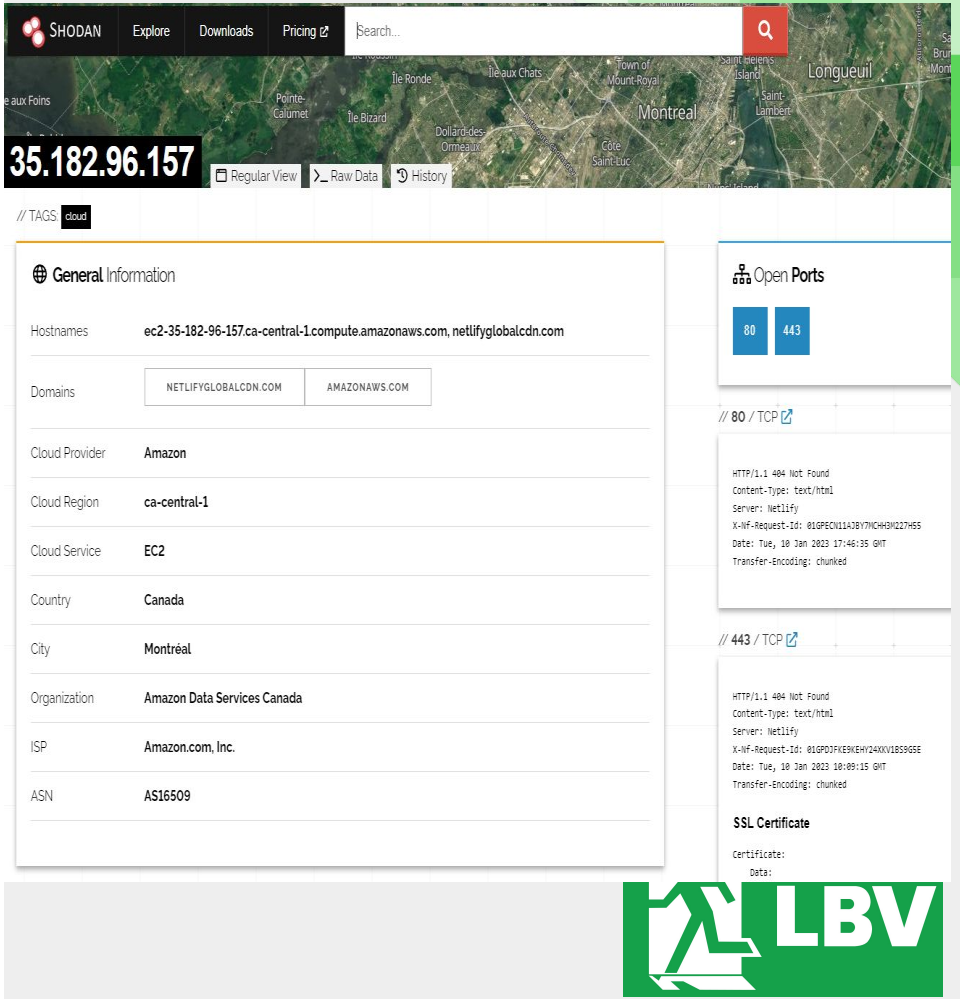
who.is


Ping
PING physsec.org (162.241.24.125) 56(84) bytes of data.
64 bytes from box5871.bluehost.com (162.241.24.125): icmp_seq=1 ttl=38 time=58.7 ms
64 bytes from box5871.bluehost.com (162.241.24.125): icmp_seq=2 ttl=38 time=61.4 ms
64 bytes from box5871.bluehost.com (162.241.24.125): icmp_seq=3 ttl=38 time=58.6 ms
64 bytes from box5871.bluehost.com (162.241.24.125): icmp_seq=4 ttl=38 time=58.6 ms
64 bytes from box5871.bluehost.com (162.241.24.125): icmp_seq=5 ttl=38 time=58.6 ms
--- physsec.org ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 58.654/59.227/61.427/1.131 ms
Traceroute
traceroute to physsec.org (162.241.24.125), 30 hops max, 60 byte packets
1 ip-10-0-0-14.ec2.internal (10.0.0.14) 1.221 ms 1.210 ms 1.197 ms
2 216.182.231.112 (216.182.231.112) 15.567 ms 216.182.238.133 (216.182.238.133) 31.201 ms 216
3 100.66.9.190 (100.66.9.190) 22.711 ms 100.66.9.206 (100.66.9.206) 22.673 ms 100.66.8.214 (1
4 100.66.39.18 (100.66.39.18) 19.944 ms 100.66.60.84 (100.66.60.84) 30.781 ms 100.66.14.146 (
5 241.0.4.211 (241.0.4.211) 3.943 ms 241.0.4.193 (241.0.4.193) 1.691 ms 241.0.4.222 (241.0.4.
6 241.0.4.220 (241.0.4.220) 1.760 ms 241.0.4.196 (241.0.4.196) 1.222 ms 240.0.40.30 (240.0.40
7 240.0.40.30 (240.0.40.30) 1.243 ms 240.0.40.20 (240.0.40.20) 1.190 ms 240.0.40.25 (240.0.40
8 240.0.40.19 (240.0.40.19) 1.154 ms 242.0.170.145 (242.0.170.145) 1.760 ms 242.0.171.17 (242
9 52.93.28.181 (52.93.28.181) 1.594 ms 52.93.28.183 (52.93.28.183) 2.327 ms 52.93.28.181 (52.


LBV

Shodan

https://www.shodan.io/dashboard



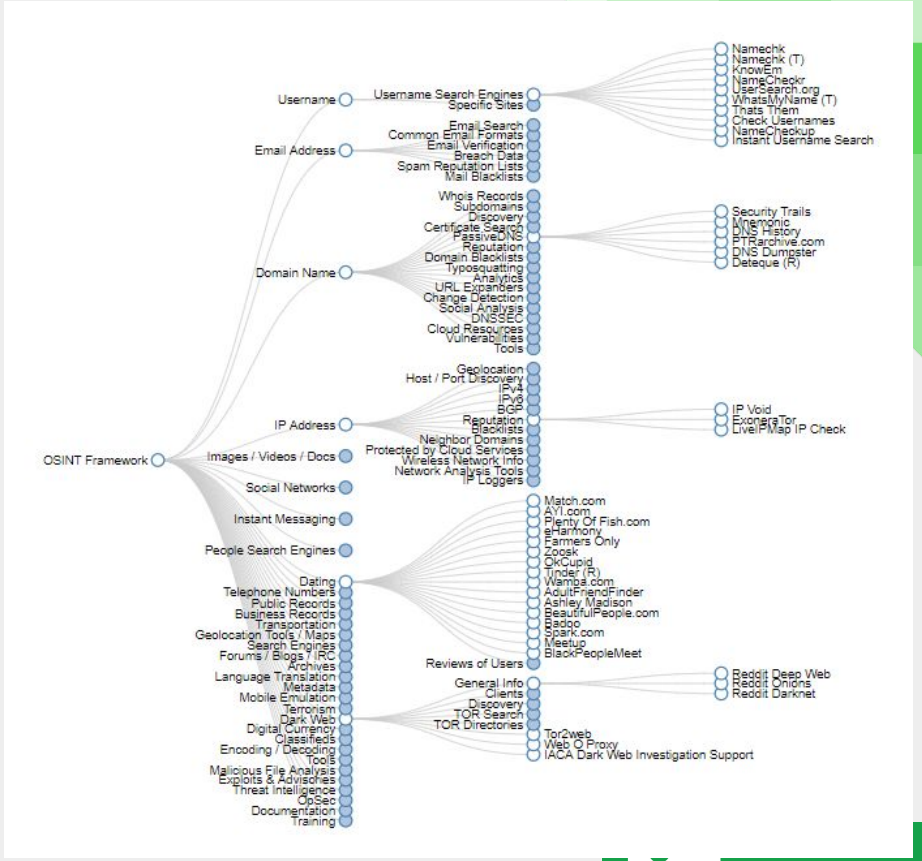
Demo time!

shodan.io and who.is



Example of an OSINT Framework

https://osintframework.com/



Transition to Locations

OSINT Online

Often floorplans are available with a simple Google search:

```
location keywords filetype:pdf
location keywords “basement plan” site:example.com filetype:pdf
location keywords “drawn by” filetype:pdf (approved by, reviewed by)
```

Other good keywords to find floorplans:

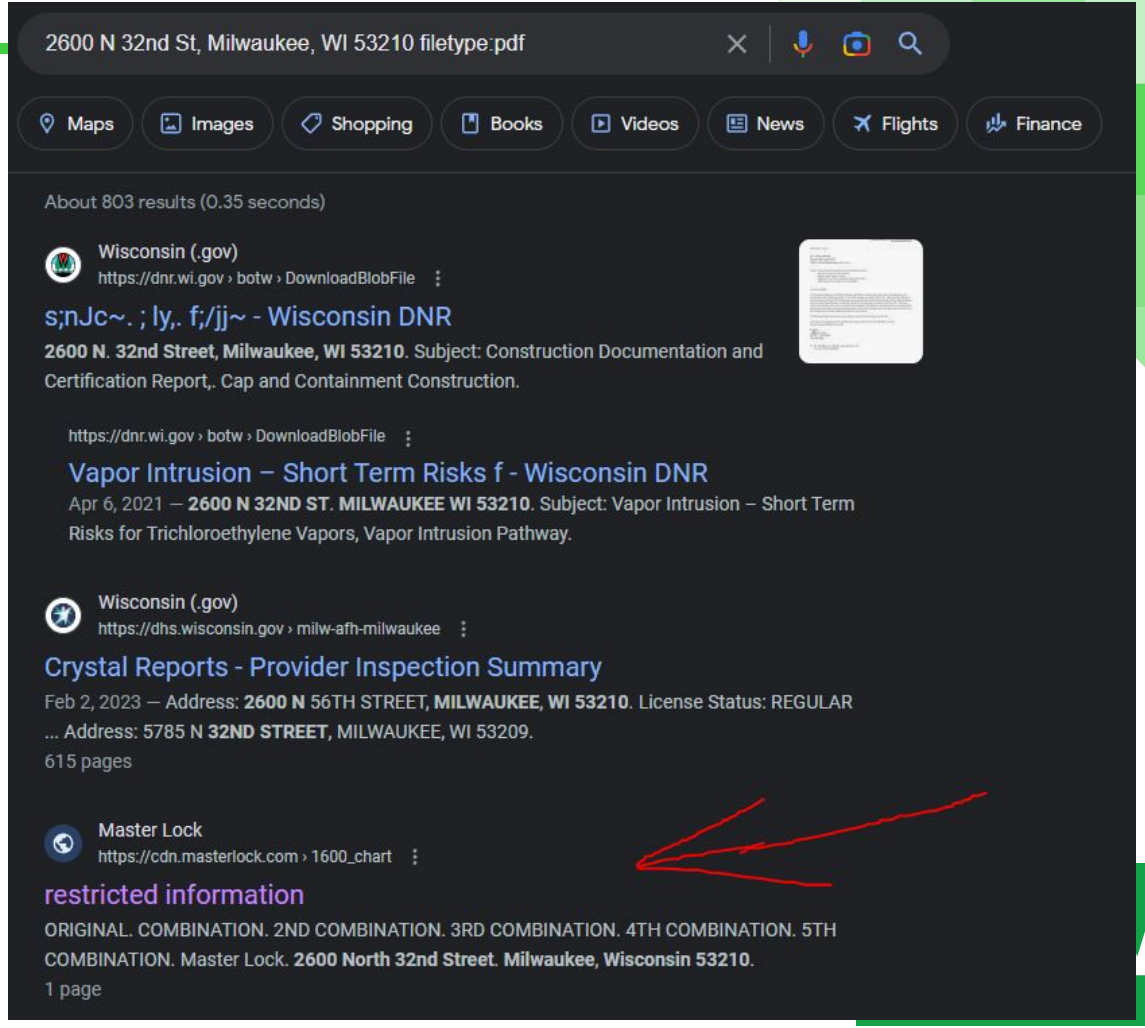
```
bsmt elevator elev unassigned unexcavated “pipe space” mech
rev wshrm dn wc rm “outline of” mezz pump lobby storage
tunnel “open to below” drwg shaft
```

Public building? Look for the public tenders website!



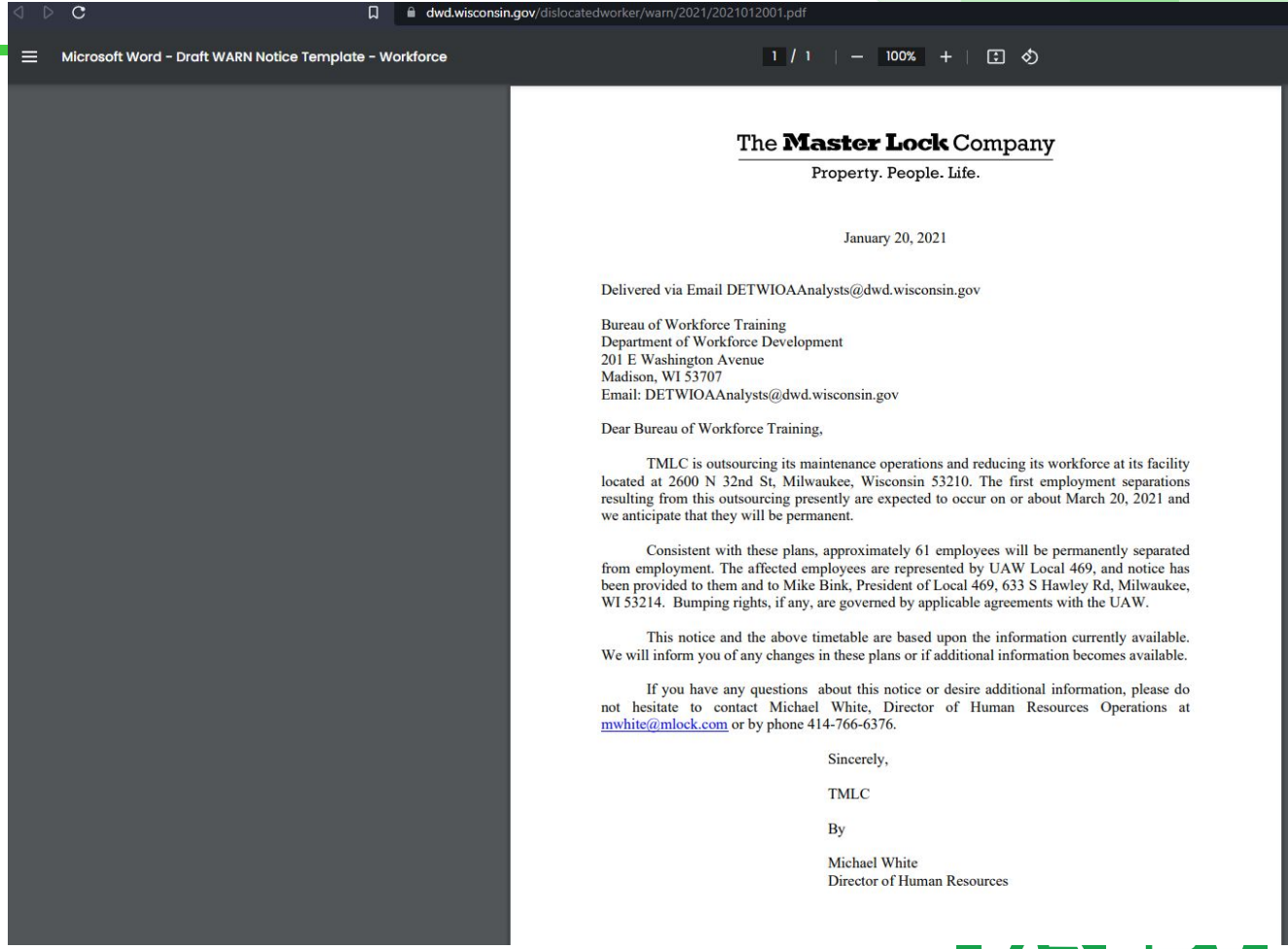
An example…

An internal document from master lock that is clearly labelled ‘restricted information’



An example Part 2

A template found its way online regarding how masterlock intends to permanently separate AKA fire people through a corporate notice



An example Part 3

This shows how Master lock was in contact with a separate party involving DNR, (department of natural resources), and the contact linking the two. Social engineering can now come into play by creating a relation between you and either DNR, or the site contact or program director

If you have questions regarding this letter, please contact the assigned DNR Project Manager or DNR Site contact:

BINYOTI AMUNGWAFOR
(414) 708-5874
binyoti.amungwafor@wisconsin.gov

Sincerely,

Christine Haag
Program Director
Remediation & Redevelopment Program

State of Wisconsin
DEPARTMENT OF NATURAL RESOURCES
101 S. Webster Street
Box 7921
Madison WI 53707-7921

Tony Evers, Governor
Preston D. Cole, Secretary
Telephone 608-266-2621
Toll Free 1-888-936-7463
TTY Access via relay - 711

WISCONSIN DEPT. OF NATURAL RESOURCES

April 6, 2021

ANNETTE JAKUBIAK
MASTER LOCK COMPANY LLC
2600 N 32ND ST
MILWAUKEE WI 53210

Subject: Vapor Intrusion – Short Term Risks for Trichloroethylene Vapors, Vapor Intrusion Pathway Assessment, and Immediate and Interim Actions
MASTER LOCK CO - WASTEWATER PUMP
2600 N 32ND ST, MILWAUKEE, WI
BRRTS# 02-41-553429 FID# 241038820

Dear Sir or Madam:

This letter is being sent to all Responsible Parties (RPs) that currently have an active contamination response site on the Department of Natural Resources (DNR's) Bureau for Remediation and Redevelopment Tracking System (BRRTS). It reiterates and enhances information about vapor intrusion risk that has been previously provided to you by DNR, either in a letter sent by DNR in 2011 regarding assessment of the vapor pathway or in your responsible party letter if your case was opened after 2011. Recent studies indicate that vaporized trichloroethylene (TCE) in indoor air is more toxic than previously understood and the risk posed by TCE vapors requires an immediate response when women of child-bearing years are present.

The purpose of this letter is to communicate three points related to vapor intrusion:

1. **TCE poses short-term risks to human health that justify accelerated assessment, investigation and mitigation of the vapor intrusion pathway.**
2. Assessment of the vapor intrusion pathway is part of the investigation process and should be assessed as early as possible and routinely re-assessed throughout the life of a project.
3. Immediate and interim actions may be necessary early in the site investigation process to protect human health from contaminated vapors.

We encourage you to discuss this information with your environmental consultant. The DNR believes the health risks of TCE vapors are serious enough that it should be one of *the first things* evaluated as part of a site investigation, especially at sites where contamination may impact sensitive populations. RPs should be diligent about screening for TCE in vapors as early in the site investigation process as possible, to determine if immediate actions are warranted to reduce harmful exposure.

LBV

Commercial Properties

Almost all commercial rental space plans can be OSINT'd!

- Very few companies own their offices nowadays.
- Office buildings are owned by property management companies (Brookfield, Oxford, Menkes, etc)
- They are always trying to find tenants for the building
- They post floorplans for units they're trying to rent
- Highrises are stacked and largely uniform floor-to-floor
- They often do not remove old listings, if you have the link



AI-Based Geolocation

GeoSpy AI

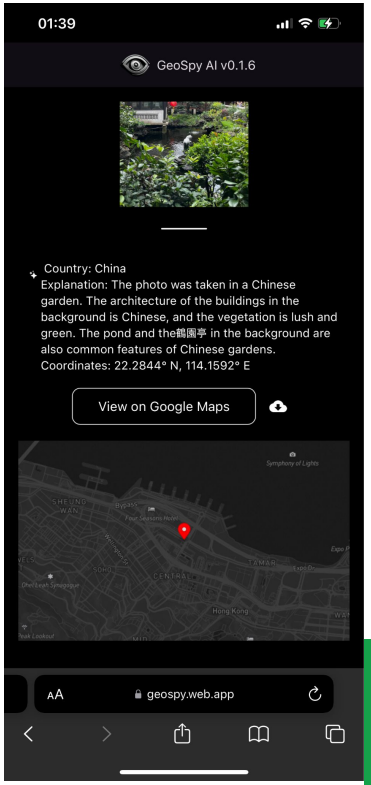

GeoSpy AI v0.1.6
Let's start a search
Welcome to GeoSpy Public Demo. Photo location prediction using AI. Take a picture or select an existing one.
Press or drag here to upload / take a photo

Take it with a grain of salt

This photo WAS taken in mainland China

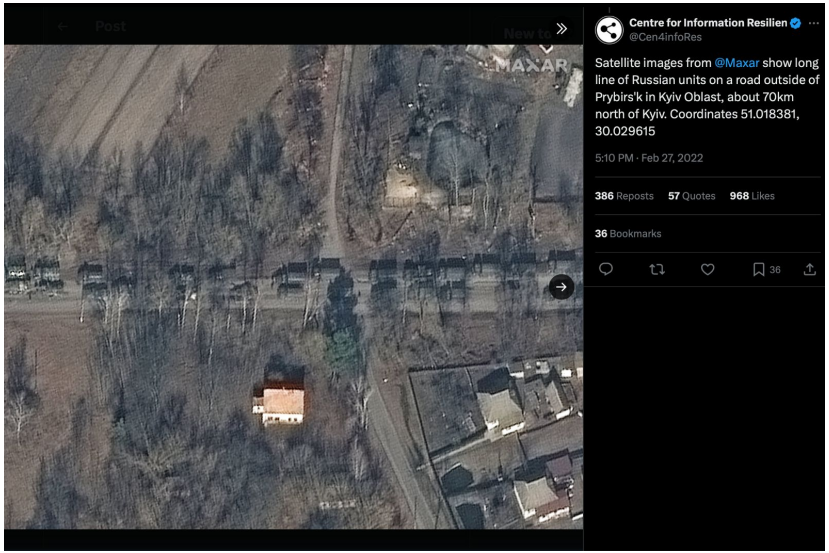
Not in Hong Kong

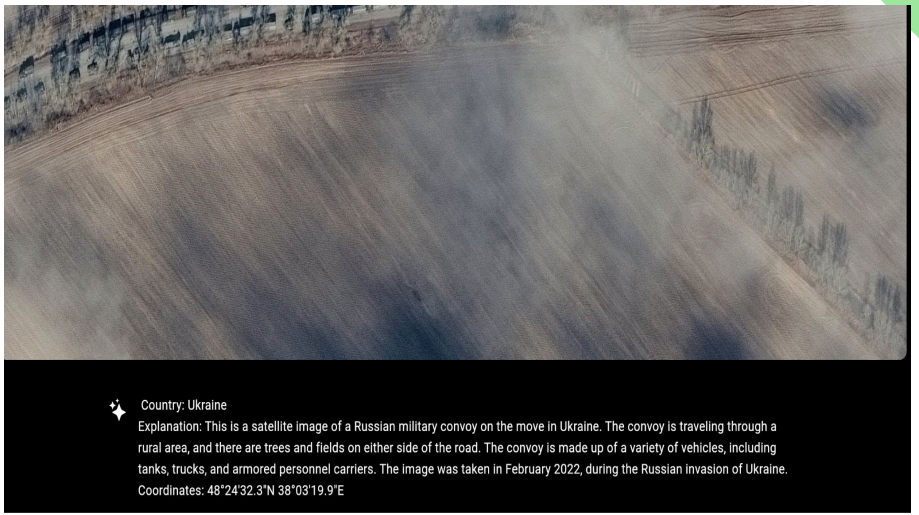




LBV

It does work! Just have to verify





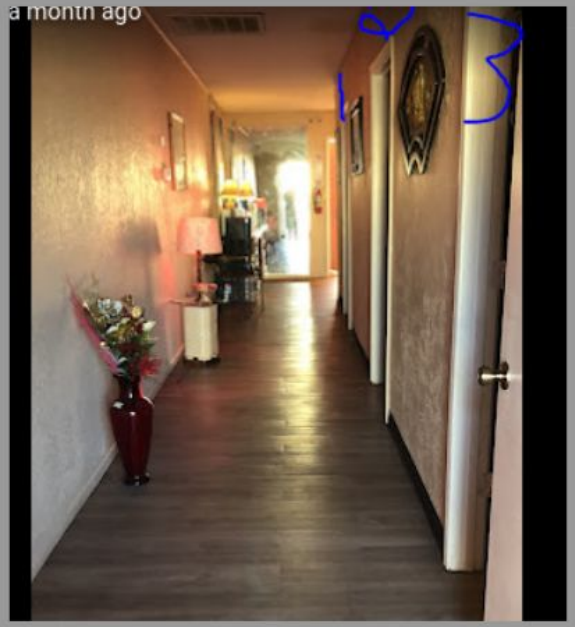
LBV

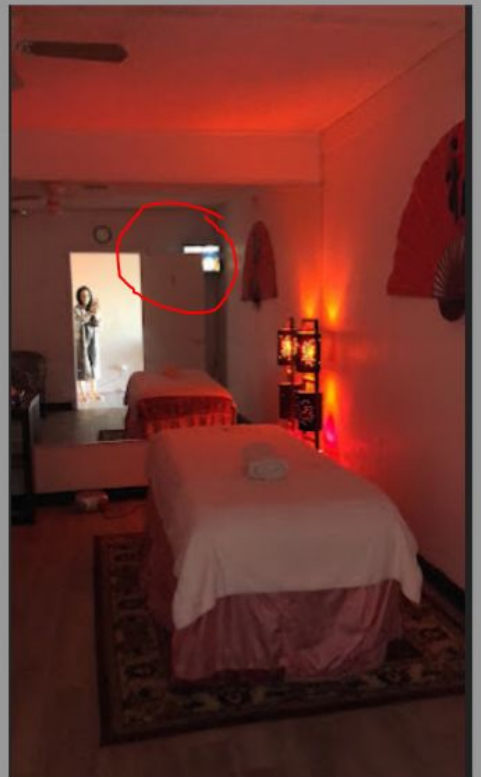
Applied OSINT Vignette

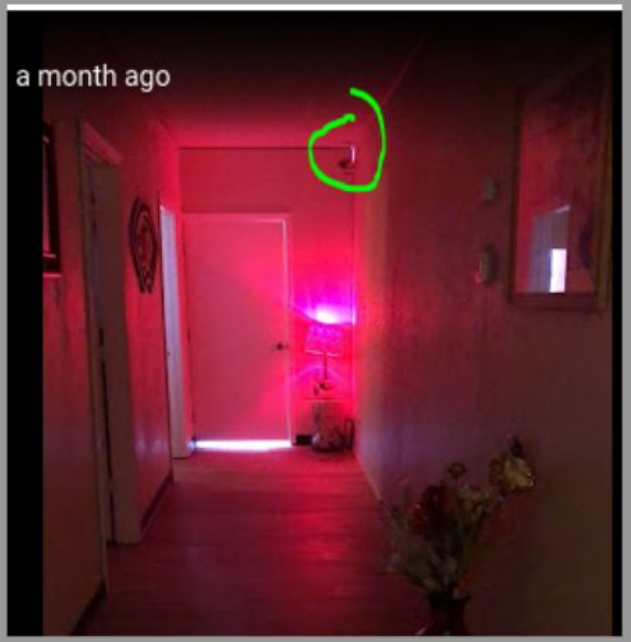


Inside location

Location





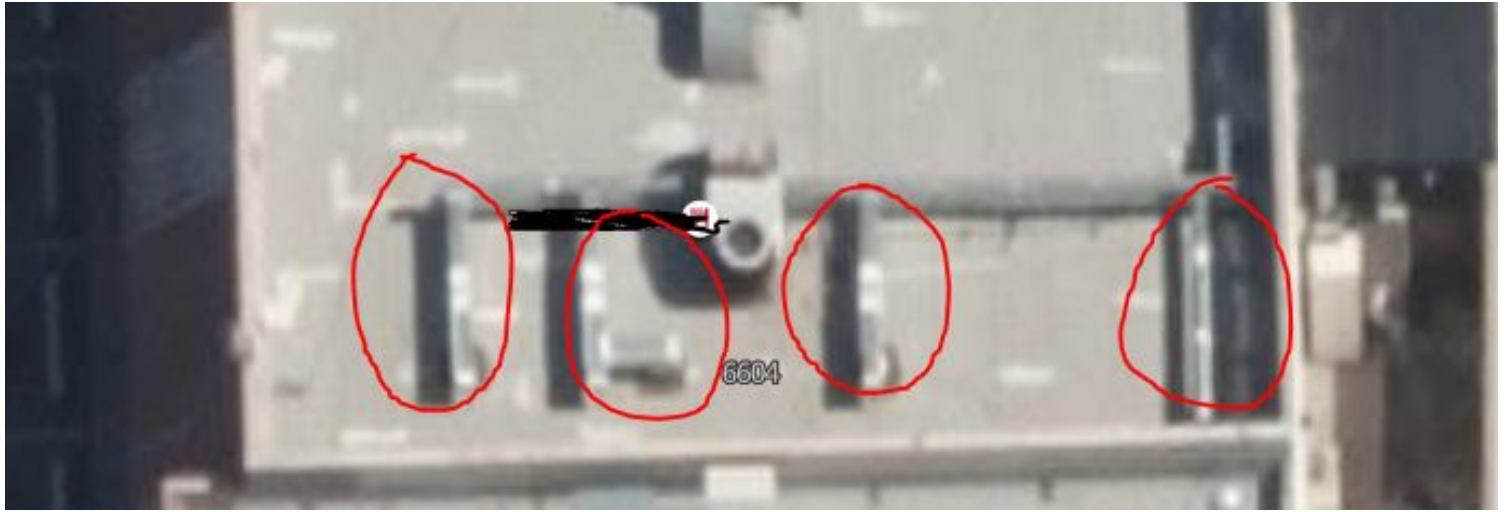


Outside Location





Outside continued



Questions?

Lukas McCullough
lukas@physsec.org

Resources used:

Osintframework.com

Who.is

Shodan.io

maltego.com

