A Case Study in geOSINT

Wagner recruiting in Serbia?

Allegedly, Wagner mercenaries are recruiting Serbians for Russia's war against Ukraine.

Research question:
Using this photo, what information can be gathered about the people responsible for this graffiti?

https://www.bbc.com/news/world-europe-64329371

How to Approach the Research

Process:

1. Break down the question.
2. Identify key components and phrases.
3. Use what's known to discover what isn't.

https://www.bbc.com/news/world-europe-64329371

Potential Questions and What's Known

Questions:

- Where in Belgrade was this painted?
- Exactly who painted it?
- Why?
- When did they paint it?
- What does it look like now?
- How could we observe future activity remotely?

Knowns:

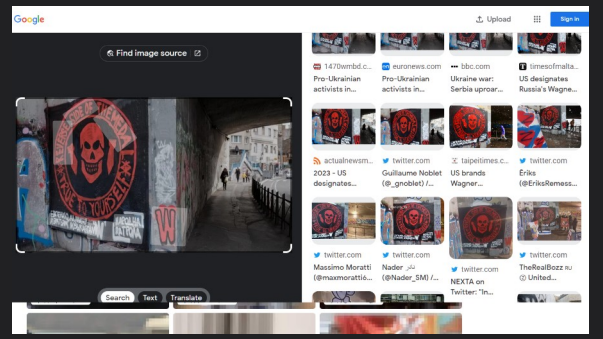
- "Reverse Side of the Medal"
  "True to Yourself"
- Skull in red against black
- "Narodna Patrola"
- "Евгению, админу и братьям музыкантам "W"
- Belgrade, Serbia

https://www.bbc.com/news/world-europe-64329371

GeoLocation: Reverse Image Search

Goal: Find the original photo:

- Exifdata – if we're lucky
- Post or article may contain details about the location or the event that could be useful
- Photo could be photoshopped



Results:

- @Nader_SM reposted from **@alleyesonwagner**
- Blurred face in group photo
  - Article - "It's **Damnjan Knezevic**". But is it?
- Closeup of Wagner logo on jacket
- Telegram Group: **t.me/orly_rs**

Every return presents an opportunity to pivot. This flow is not the only way to go.

GeoLocation: Dorks & Phrase Lists

- (Wagner OR "Narodna Patrola") AND graffiti AND Belgrade
- Spelling variation:
  - "Narodne Patrole"

Returned:

- Twitter account: @ivanastradner
  - 1st close connection to those involved?
  - **Orly-Narodna Patrola – Cyber Front Z**

Phrases for later exploration:

- "wagner group" musicians
- Евгению, админу и братьям музыкантам
- Eugene, admin and brother musicians wagner group
- Orly-Narodna Patrola – Cyber Front Z
- January 15?

OSINT isn't linear.
Lists of search phrases help you keep track of leads and ideas.

Geolocation: Image Prep & Mapping

What geographical features do you see?

What geographical features do you see?

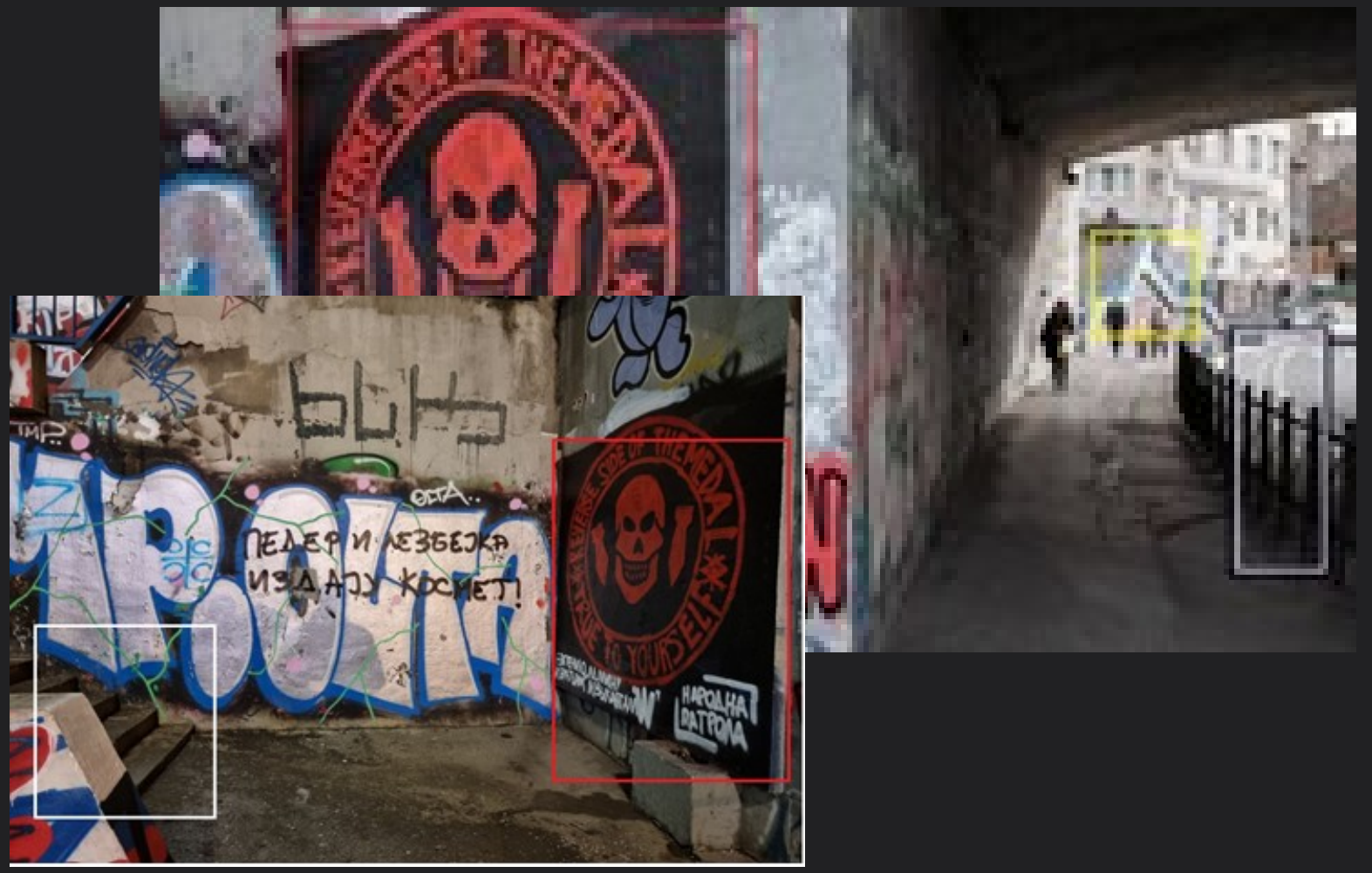
- Yellow: The steepled stairway edged in blue, with a tan building and a white one next to each other behind it.

- Grey: Steel fence with yellow trimmings.

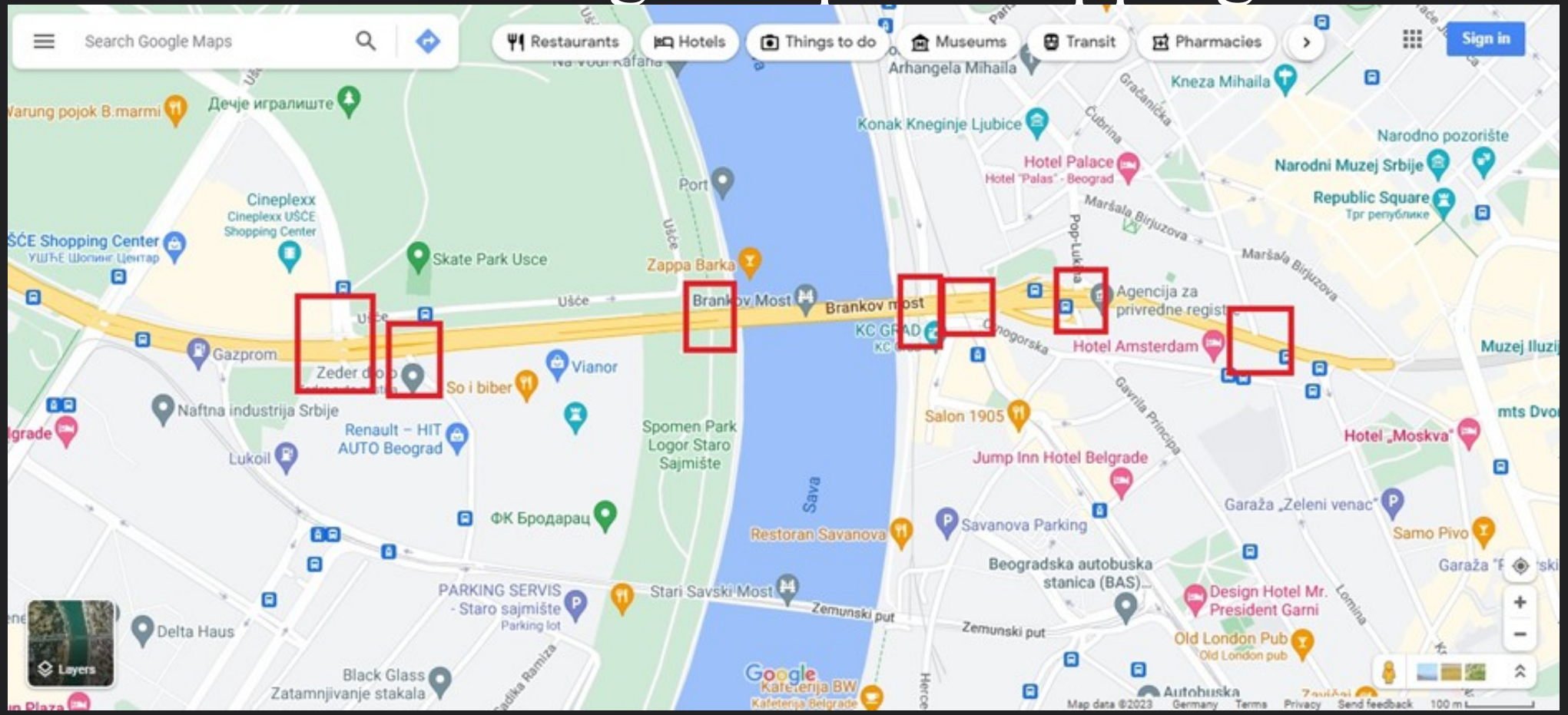
- Red: The wall and edge where the graffiti was painted.

- White: The staircase leading down to the wall, (seen in another photo)

Also, the curved road...



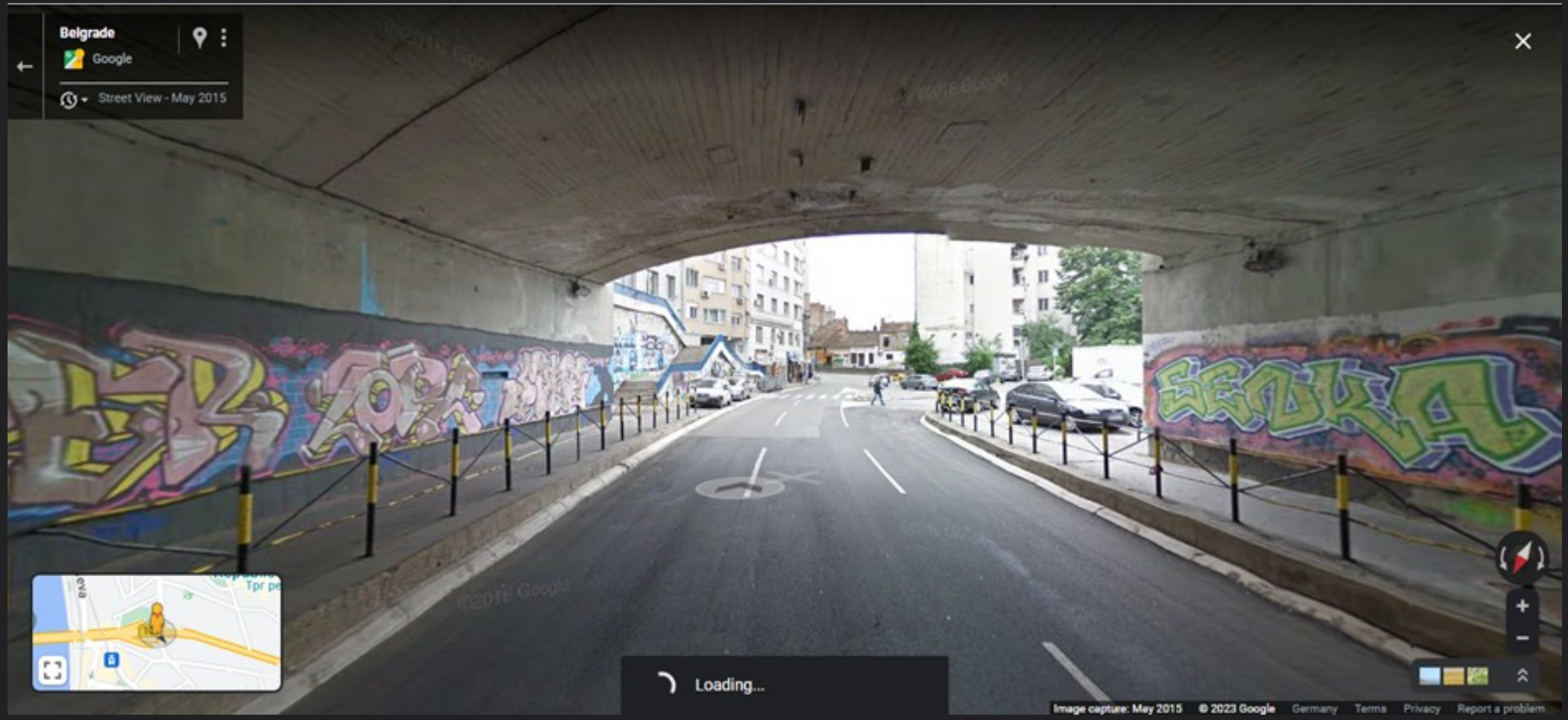
GeoLocation: Image Prep & Mapping



https://www.google.com/maps/@44.8148344,20.4468746,17z

Brankov Most: Seven candidates. Two good possibilities.

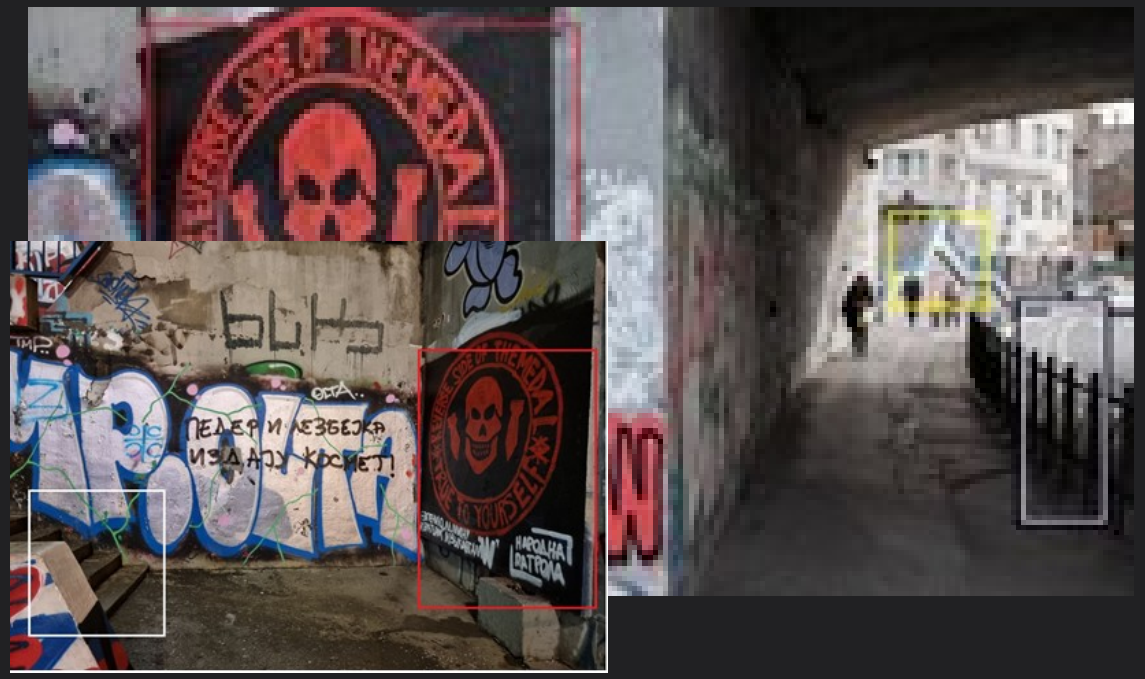
GeoLocation: Image Prep & Mapping



Always look behind you..

GeoCoordinates: 44.8152368, 20.4526931

GeoCoordinates: 44.8152368, 20.4526931



Location identified: but what about the unblurred man in the group photo?

Wait, which photo?

https://pbs.twimg.com/media/Fmqr-zzXkAIt3zw?format=jpg&name=large

This one.
Found in reverse search. Slide 4.

What do we have?

- Uncorroborated name: Damnjan Knezevic
- Photoshopped version of the group photo
- Closeup web pix of Knezevic on web

KEYWORD LIST

- **"Narodna Patrola" - Social Media search!**
- January 14

- Question: Do they have any accounts, and did they post anything around that date?

Results: @narodna_patrola

https://mobile.twitter.com/narodna_patrola/status/1614295995067539456/photo/1

http://srpskidnevnik.com/magazin/damnjan-u-rusiji-su-mi-otkrili-cim-zavrse-u-ukrajini-pomoci-ce-i-srbiji-video/

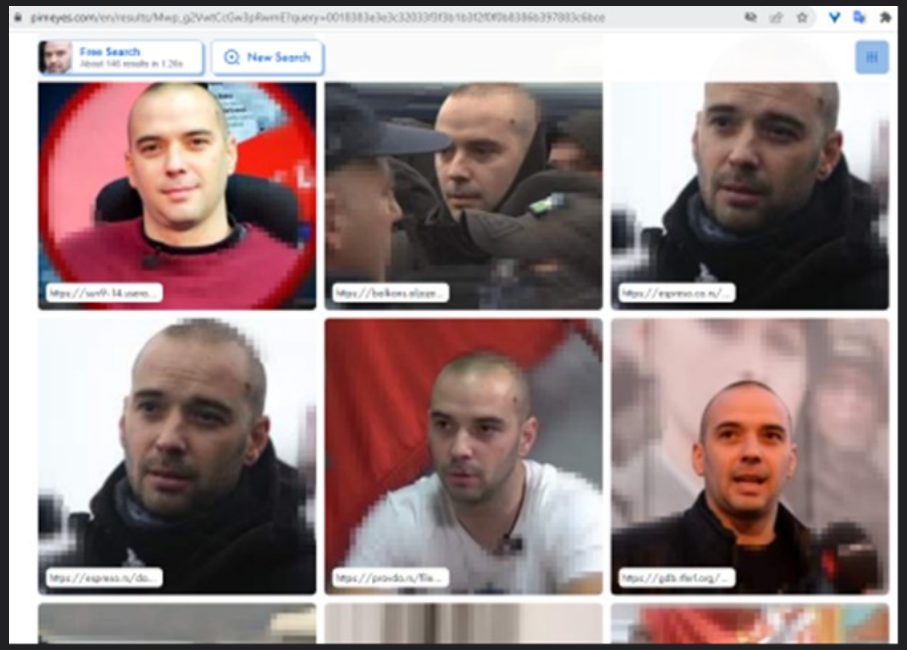
It looks like the same person, at a glance.
How could we gain more confidence?

AI: Facial Recognition

PimEyes, returned 145 results, nearly all of Knezevic.

Facecheck.id provided a 88% confidence rating, which is good for this kind of tool.

Assessment: it is likely the person in the group photo is Knezevic.



https://pimeyes.com/en/results/Mwp_g2VwtCcGw3pRwmE?query=0018383e3e3c32033f3f3b1b3f2f0f0b8386b397883c6bce

Online facial recognition tools return links to media where they have found a face with similar characteristics.

It is **not** confirmation, and not reliable. It's notoriously bad at discerning non-white faces. But it does help build an argument.

Next Steps: Follow-up

Monitoring this location might provide insight to the players and their activities.

- This location is contested between political groups:
  - Previous image: commemorating journalist, Daria Dugina.
  - Cover-up: "Mahno society" (anti-fascism group) claims credit

These groups also freely post their activities on social media.

https://t.me/mahnosociety/21

Note: the stairs observed in the Google Maps image.

Next Steps: Followup

Given Knezevic's recent trip to the PMC Wagner Center in St. Petersburg, and the announcement of the opening of the Orly – RSCC* in Belgrade, it is probable that Narodna Patrola political actions will continue.

While it does not appear the new organization has a Belgrade office yet, monitoring known members' social media feeds might lead to the location once it does.

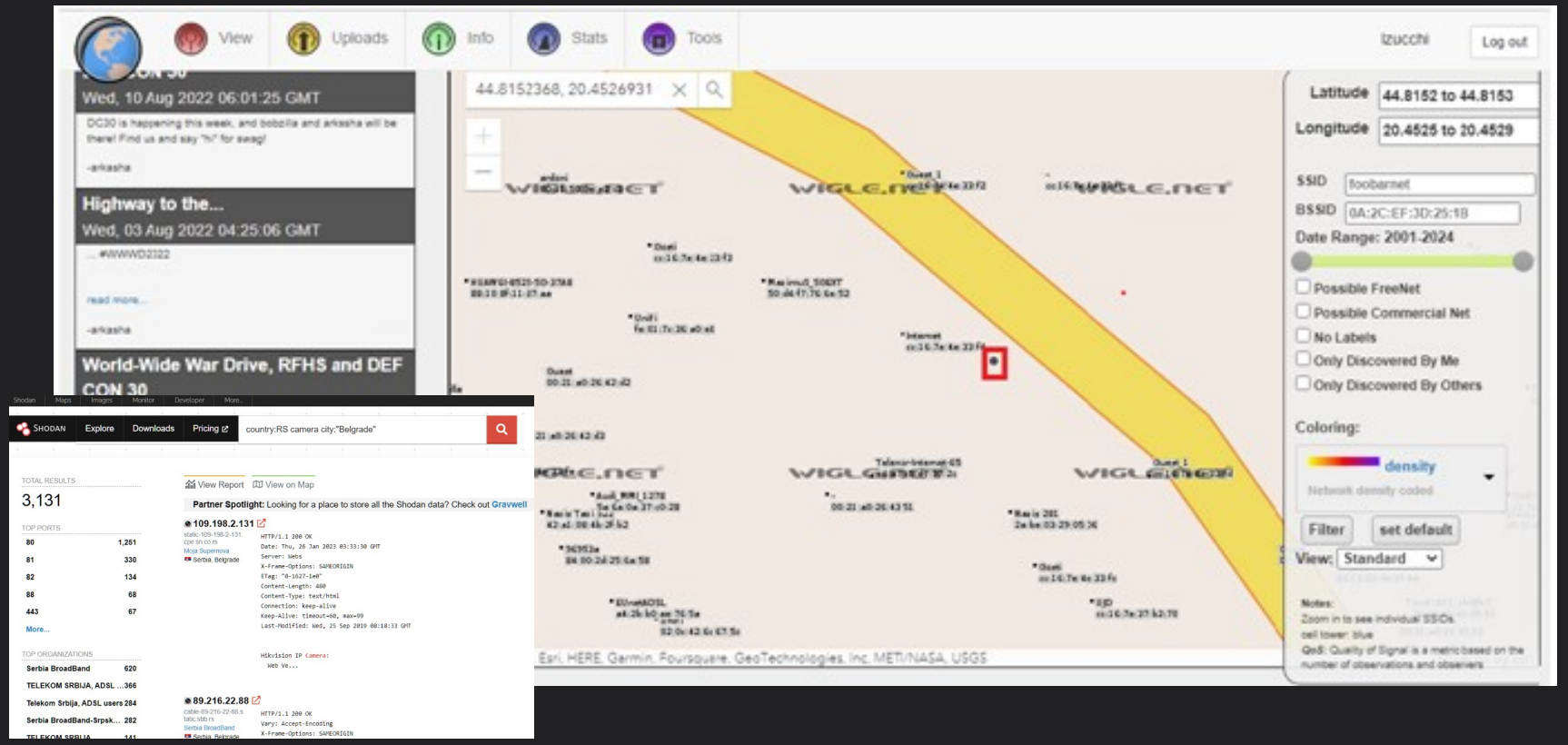
In the meantime, it might be useful to monitor open signals in the vicinity of Russia House.

*PMC Wagner Center – Russian-Serbian Cultural and Informational Centre of Friendship and Cooperation ANO Orly

https://t.me/mahnosociety/21

Shodan/Wigle.net

A search through wigle.net and Shodan.io confirmed that there are no freely accessible cameras in the area of the graffiti.



Shodan is a search engine for IoT devices with IP addresses. Some may be cameras with publicly available screenshots or livefeeds. With a subscription, one can see their location on a map.

WiGLE.net is a search engine for wifi routers and more that can be used to try to gain unauthorized access to wifi networks and to potentially access the devices connected to them. **Accessing them in this way is illegal. Identifying the networks is not.**

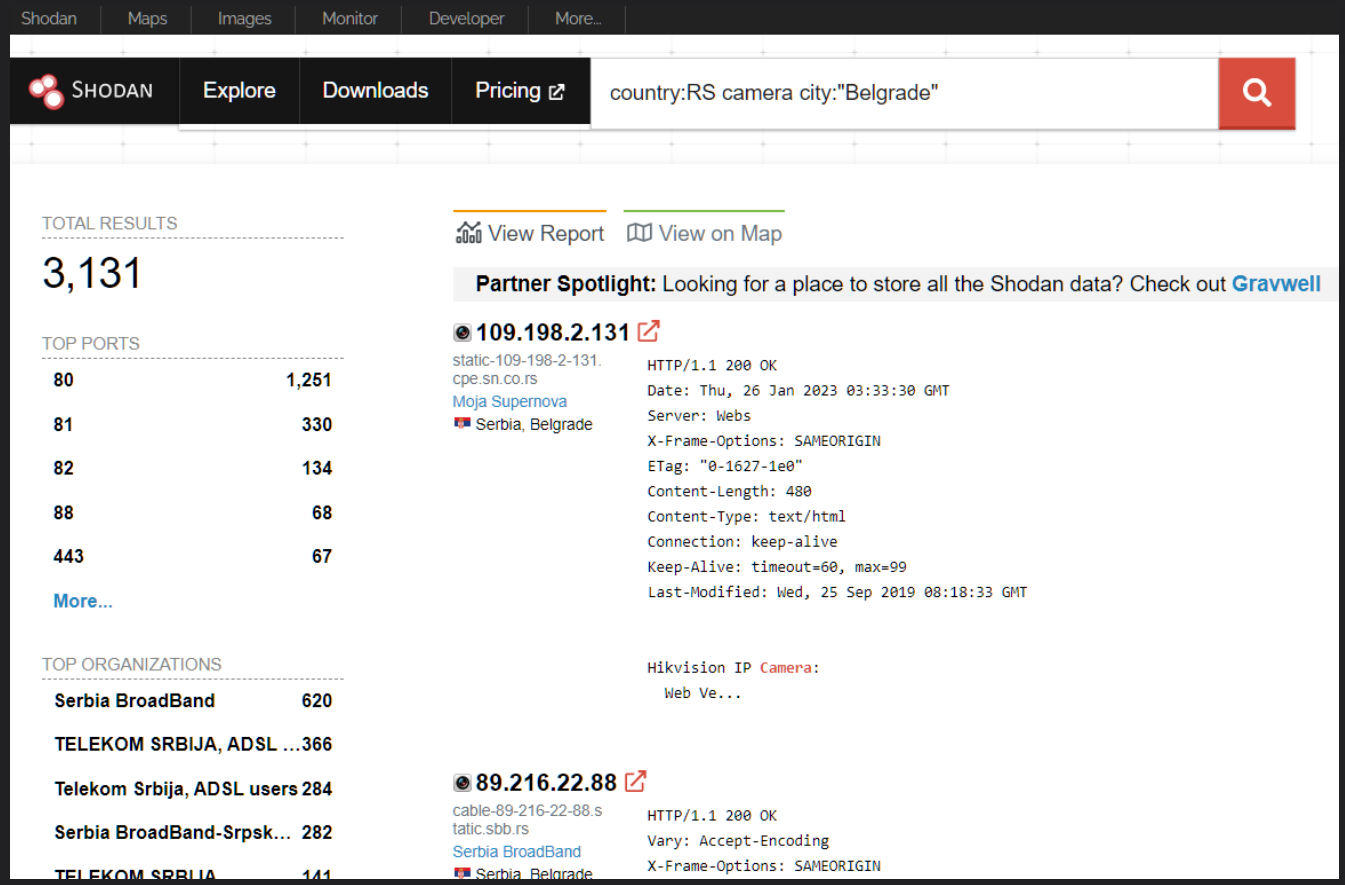
Shodan/Wigle.net

Without a subscription:

1. Copy the IP address
2. Enter it into **ip2location.com.**
3. Compare to location.

Known cameras in Belgrade:

- Belgrade Traffic Camera Network
- Belgrade Street Camera Network
- Security cameras:
- Republic Square
- Belgrade Fortress
- and others..



webcam country:RS city:Belgrade has_screenshot:TRUE

Shodan

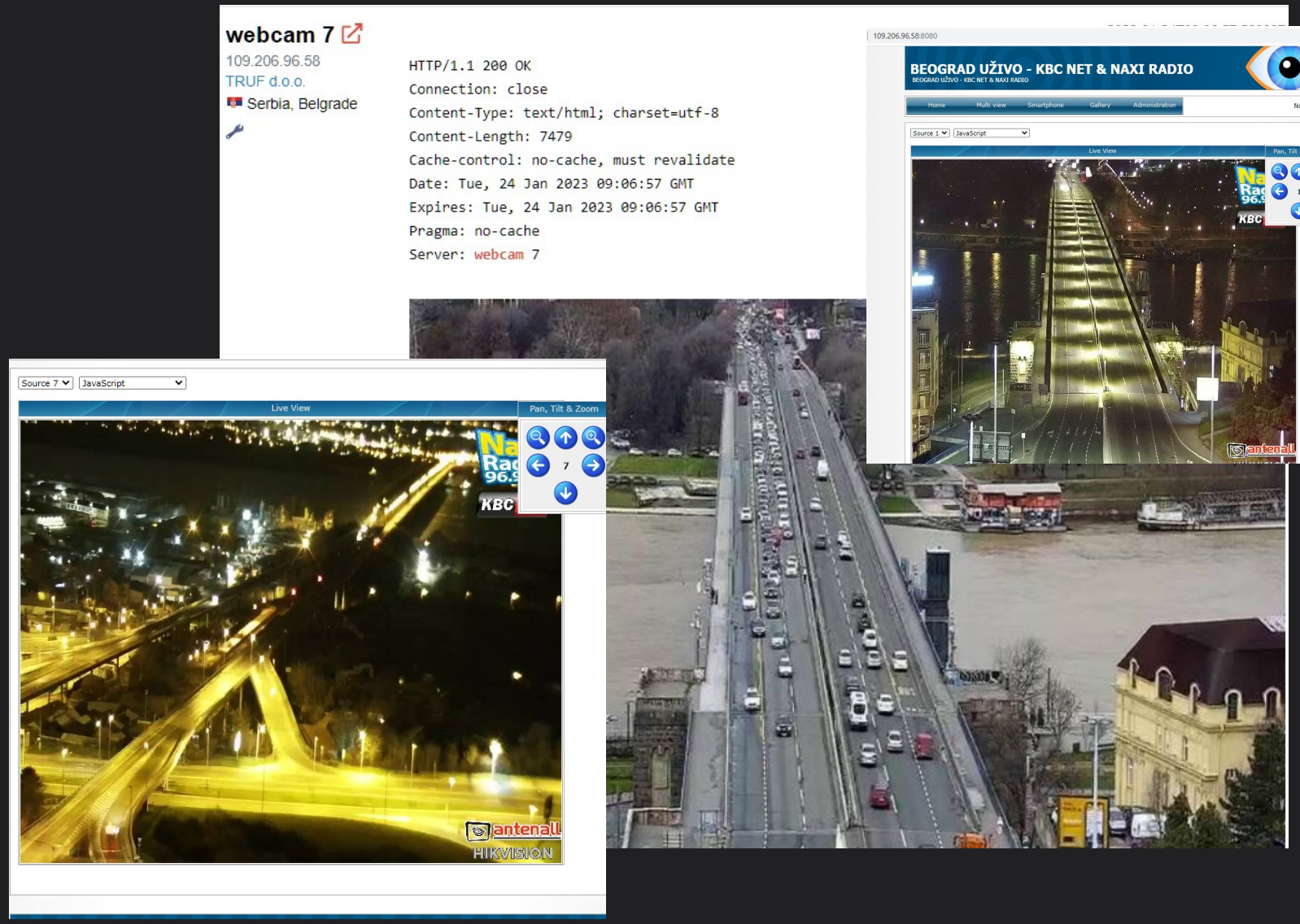
Without a subscription:

1. Copy the IP address
2. Enter it into **iplocation.net/ip-lookup or similar**
3. Compare to location.

Example:
http://109.206.96.58:8080/

IP address location is not necessarily exact.

44.8165, 20.4479 - the middle of the river.



Gains:

ACCOUNTS:
Orly RS Telegram Group: https://t.me/orly_rs

Narodna Patrola Facebook: https://www.facebook.com/narodna.patrola.96/
Narodna Patrola Telegram: https://t.me/s/narodnapatrola
Narodna Patrola Tiktok: https://www.tiktok.com/@narodna__patrola?lang=en
Narodna Patrol Twitter: https://twitter.com/narodna_patrola

Mahno Society Telegram: https://t.me/mahnosociety

Cyber Front Z Telegram: https://t.me/s/cyber_frontZ

Russian House (in Serbia): https://t.me/ruserbia

Useful subreddit: r/FreedomofRussia
Useful Twitter accounts: @ivanastradner, @alleyesonwagner

Key success factors

<u>Preparation makes pivoting easier</u>

- Do create lists and keep track of them.
  - It's easier to tweak a dork you've already made.

- Save things that pique your curiosity, even if you don't have time to follow up now.
  - They may be useful later – repeating work is a pain.

- "Why" and "How" lead to more research questions and future work.
  - Why this location? Why now?
  - How is this being coordinated?

OSINT is an art.
Organization gets you out of the rabbit hole.
You're *going* to go down it – pack crumbs.
And a torch.

https://servantsofgrace.b-cdn.net/wp-content/uploads/2017/03/quotescover-JPG-51-e1489852200923.jpg.webp

Summary of Steps for Geolocation (Prep)

Geolocation is often start of an investigation.

Background preparation can provide new leads, context, and meaning to the interpretation of the image.

Even if fast attribution is possible, background research and note-taking saves time later and results in a stronger intelligence product.

Box Key Elements
Highlight significant features of the image you want to use for verification. It will help you remember, and aid in making your case.

Enter keyword(s) in Google Maps
Search each potential site. Remember to turn around, pan, zoom, and check historical imagery.

Compare to reference image
Use the boxed features to make a point by point comparison to what you find. Finding additional images may help.

Screenshot what you find and box it.
Box the matched features in the same colors as the reference image. Add geocoordinates.

Copy the 2 images to Notebook.
Add the URL directly to the site/location. Describe why it's the same. Put them side by side in a table.

Basic Steps

1. Identify key terms
2. Construct dorks
3. Search (Reverse Image, Google, etc.)
    1. Yandex has an excellent reverse search.
    2. Baidu does, too: https://image.baidu.com/
4. Box elements in reference image & add to report
5. Google Maps and compare
6. Box results & add to report

Want to monitor the area?:

1. Shodan .io– do use their custom "dorks"
2. WiGLE.net
3. Whatismyipaddress.com/ip-lookup or Tools.keycdn.com/geo
4. Find geocoordinates in Google Maps

Basic Steps

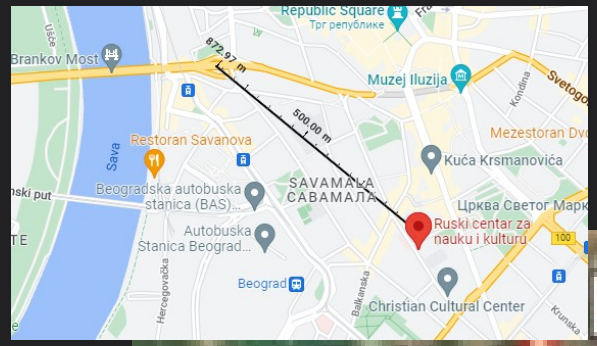
Ruski centar za nauku I kulturu

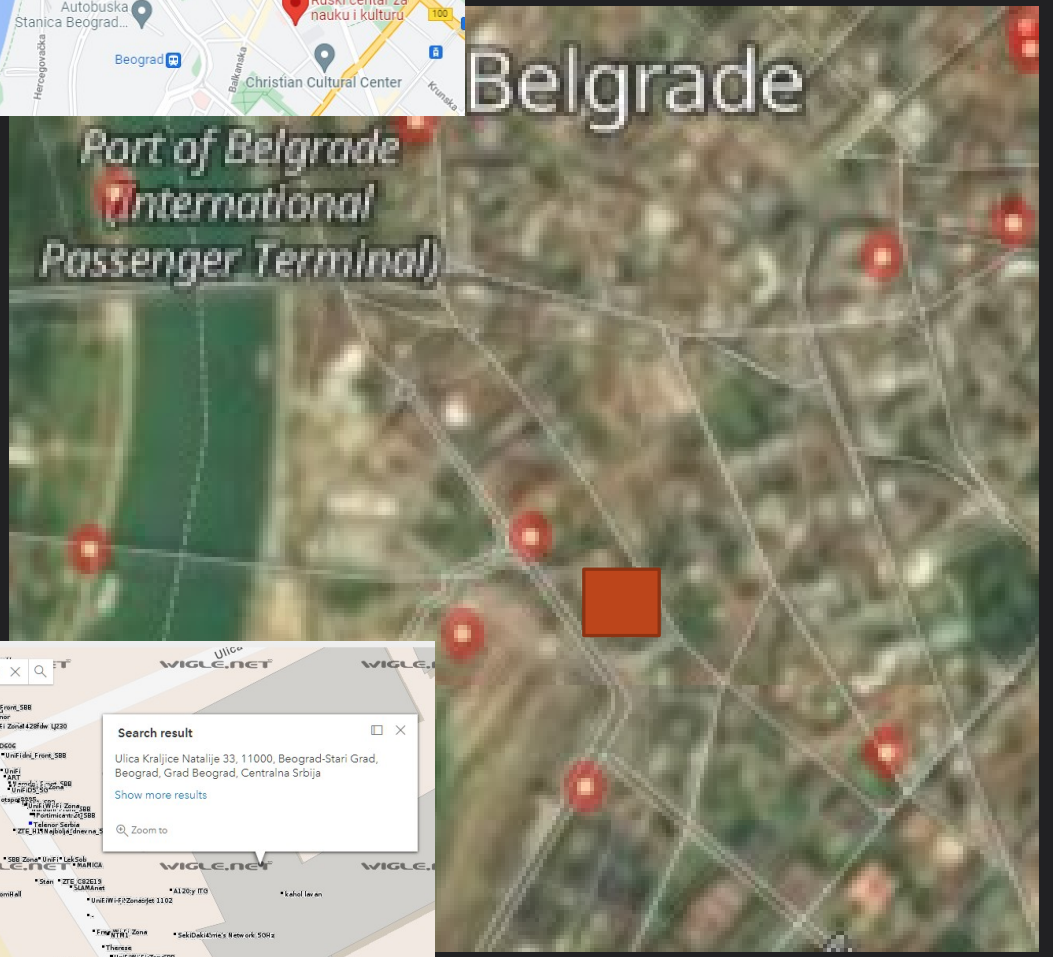
Kraljice Natalije 33, Beograd, Serbia

https://ruskidom.rs/

Potential location for the future Orly-RSCC?

No cameras, but exposed IPs and more.





TOOL	Purpose	URL
Google	Search	https://www.google.com (changes - .rs, etc)
Dorking	Improve Google results	https://www.stationx.net/google-dorks-cheat-sheet/
Reverse Image Search	Where else does the image live?	Rightclick on the camera in Google search bar. Or the image.
Twitter	Social Media	https://twitter.com/search-advanced?vertical=trends
Telegram	Social Media	Channel dependent
Google Maps	Location, images, history	https://maps.google.com
PimEyes	Shows where images are published – used for facial recognition	https://pimeyes.com/
Facecheck.id	Facial recognition	https://facecheck.id/
Shodan.io	IoT – find cameras on the 'net	https://shodan.io
wigle.net	Find wifi	https://wigle.net
WhatsMyIPAddress	IP to geocoordinates conversion	https://whatsmyipaddress
ToolsKeyCDN/Geo	IP to geocoordinates conversion	https://tools.keycdn.com/geo

Questions?