CRYPTOPARTY TIRANA 2023

RECLAIMING OUR ONLINE PRIVACY!

NOV 04 2023 | 10:00 AM

ORGANIZED WITH PASSION FOR INTERNET FREEDOM BY

IDM Institute for Democracy and Mediation
Instituti për Demokraci dhe Ndërmjetësim

open labs

Table of contents

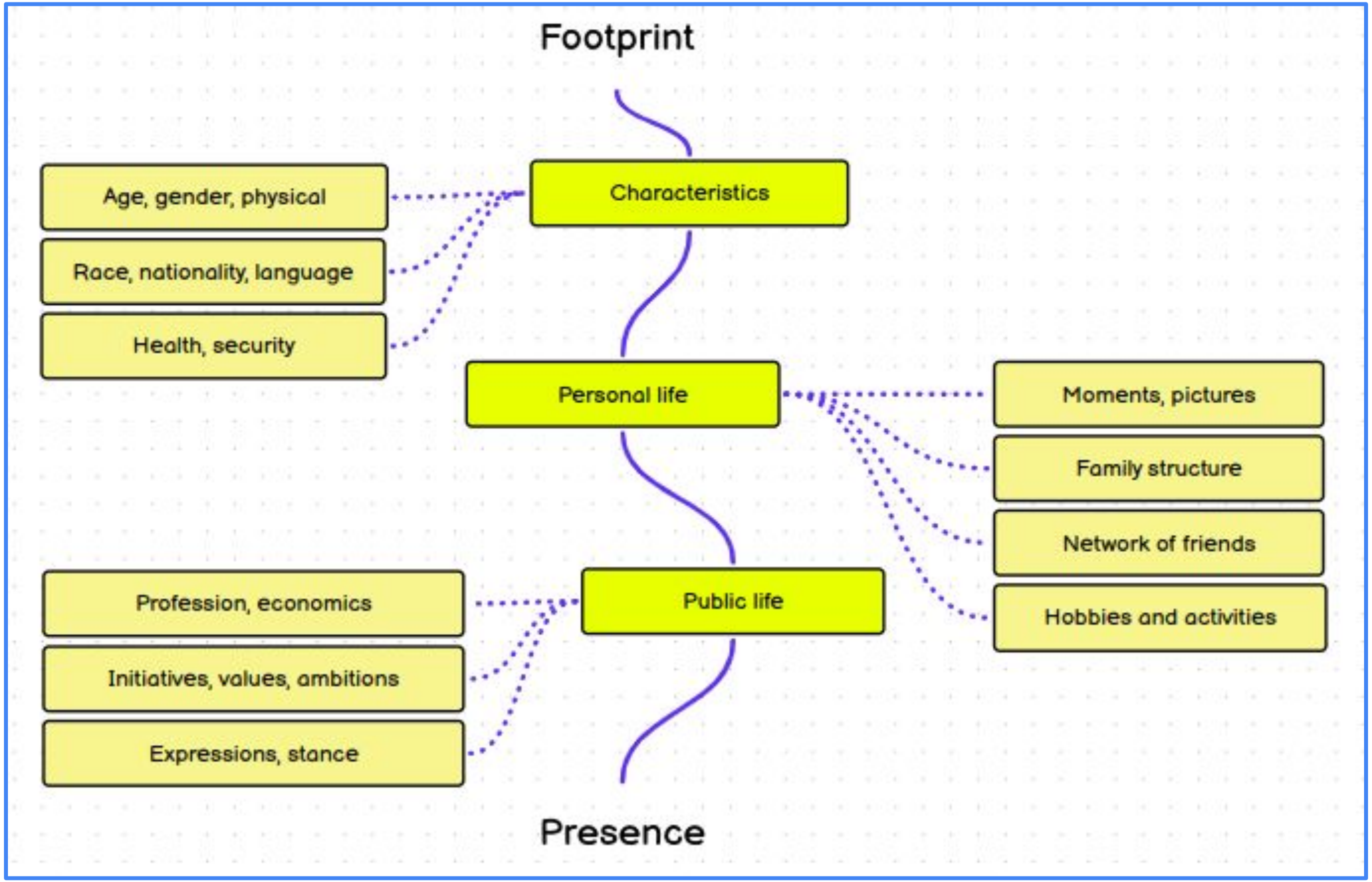
- Digital Footprints?
- Case studies

○ *Leaks*?	HIBP, Telegram	*Scale*
○ *Artifacts?*	Docs, Images, Videos	*Verification*
○ *Public opinion*?	Social media, Sentiment	*Research*
○ *Geosint*?	OpenStreetMap, Satellites	*Story*

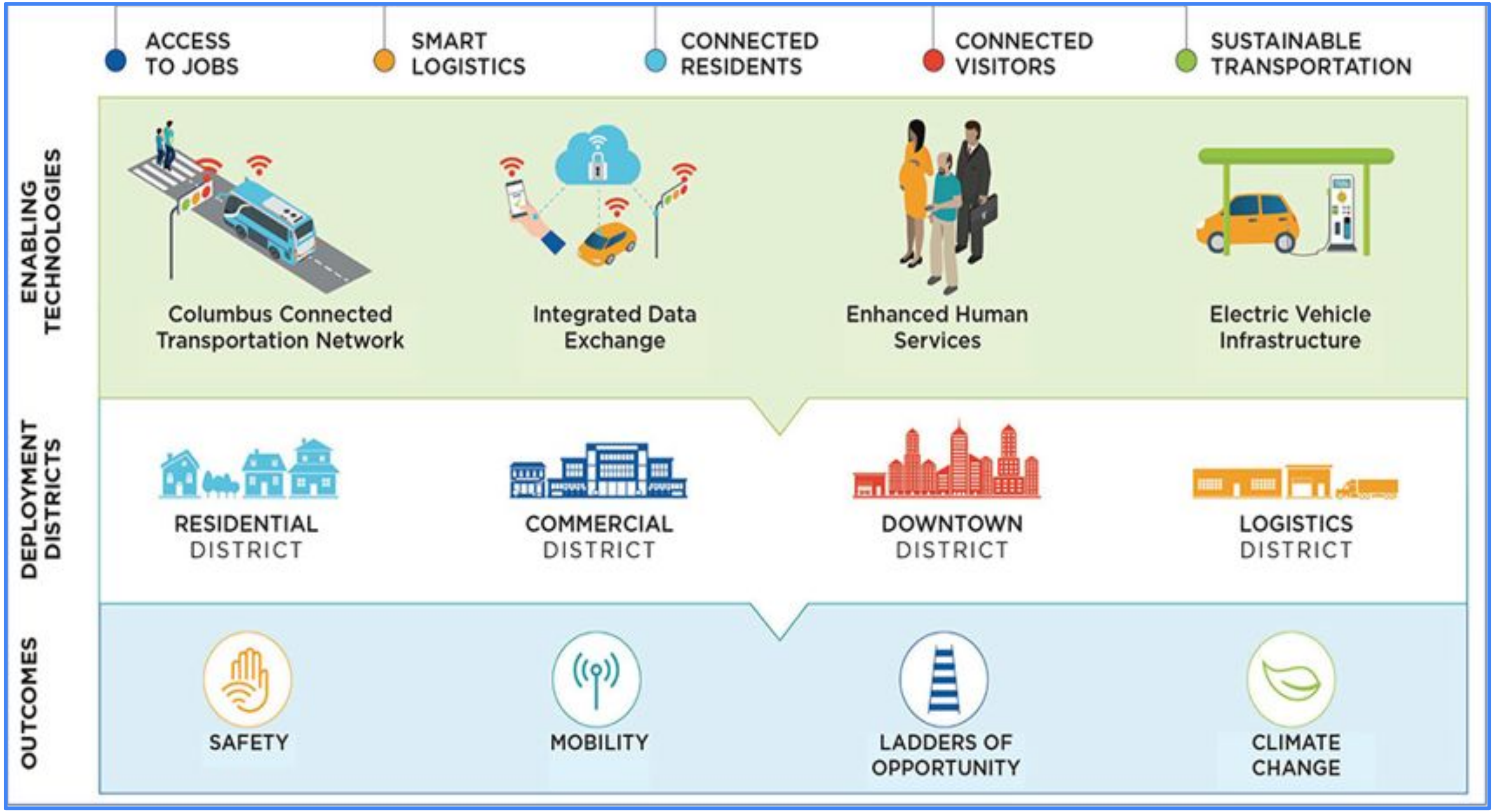
- Next steps?
- Discussion

The role of the digital footprint?

*An **illustration** of the footprint that a person can have in each sphere.*

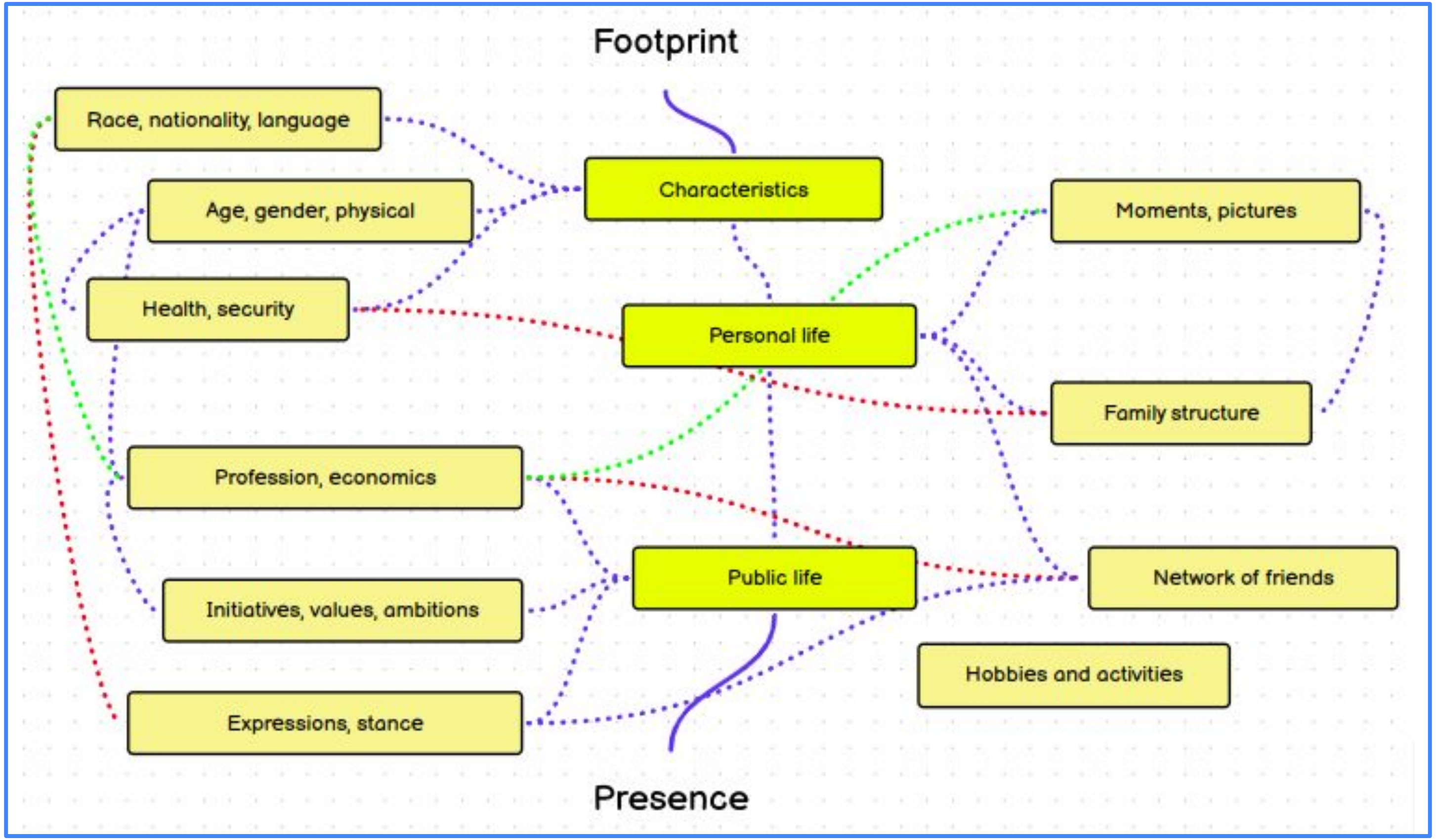


*With digitalization life has a **quicker pace**, so components are more connected.*

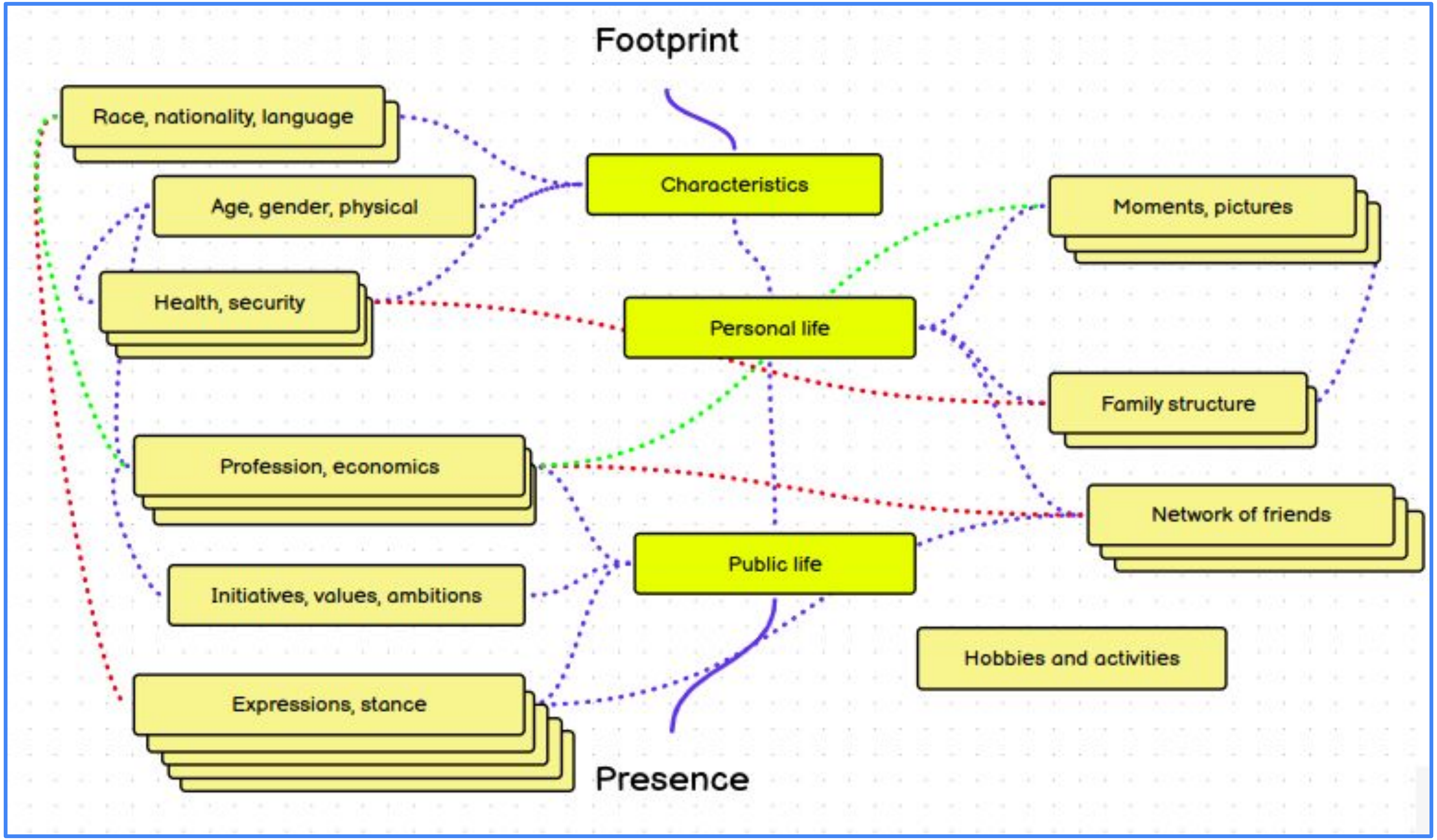


The Digital Footprint

A more realistic illustration of the connection of info that is going on.

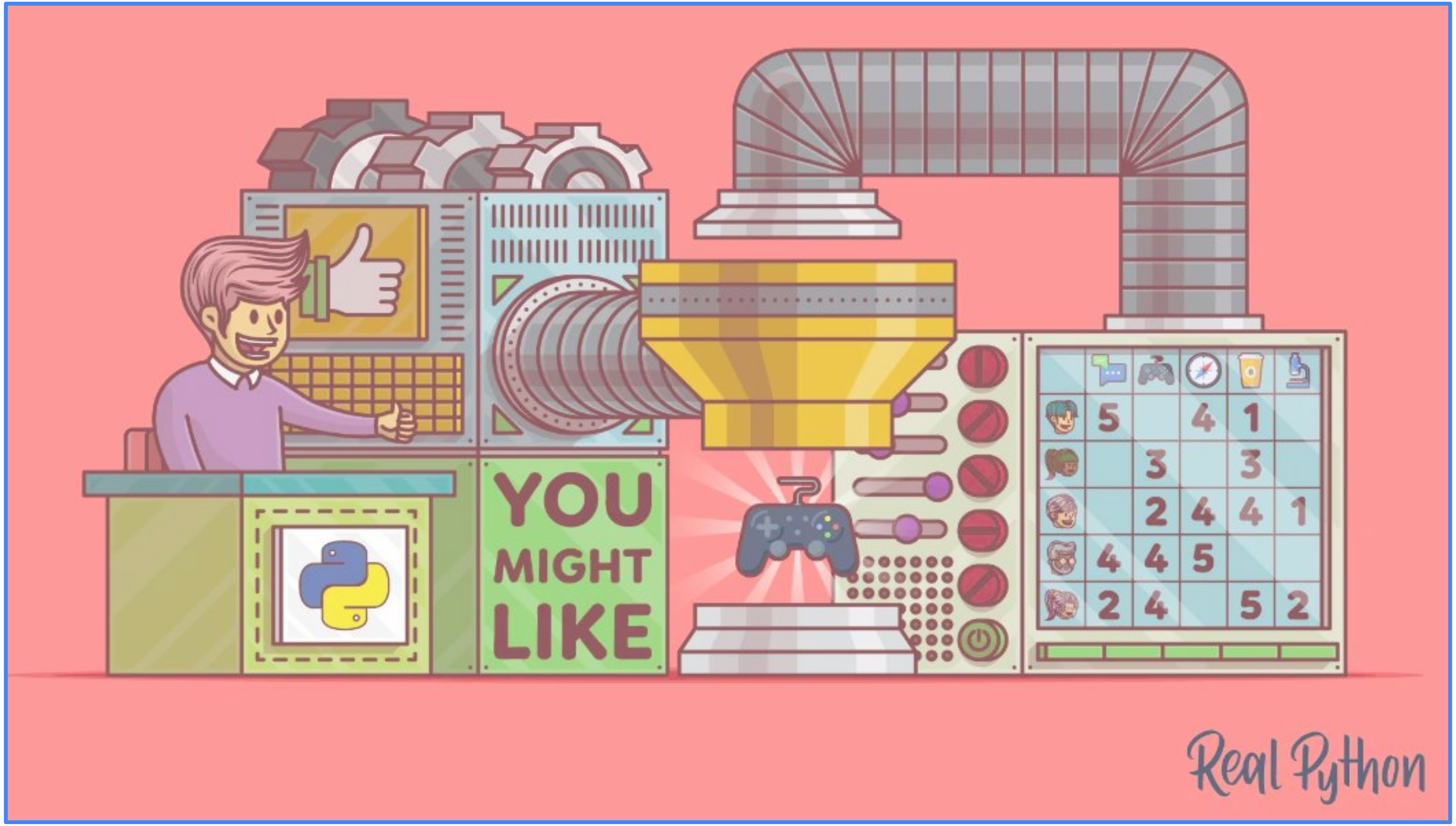


*With info that doesn’t get deleted, the **management** of footprint is difficult.*



An industry of processing

And now we have some entities that only profit with these profiles.



	5		4	1	
		3		3	
		2	4	4	1
	4	4	5		
	2	4		5	2

Result?

- A lot of data, and a lot of metadata
- A lot of analysis can be done quicker
- Advanced analysis is at the door
- Very good dashboards for story-making (…)

- Communities that open-data
- Open-Source initiatives that share knowledge
- **Tools** that can help with digital investigation ⇒ **OSINT**

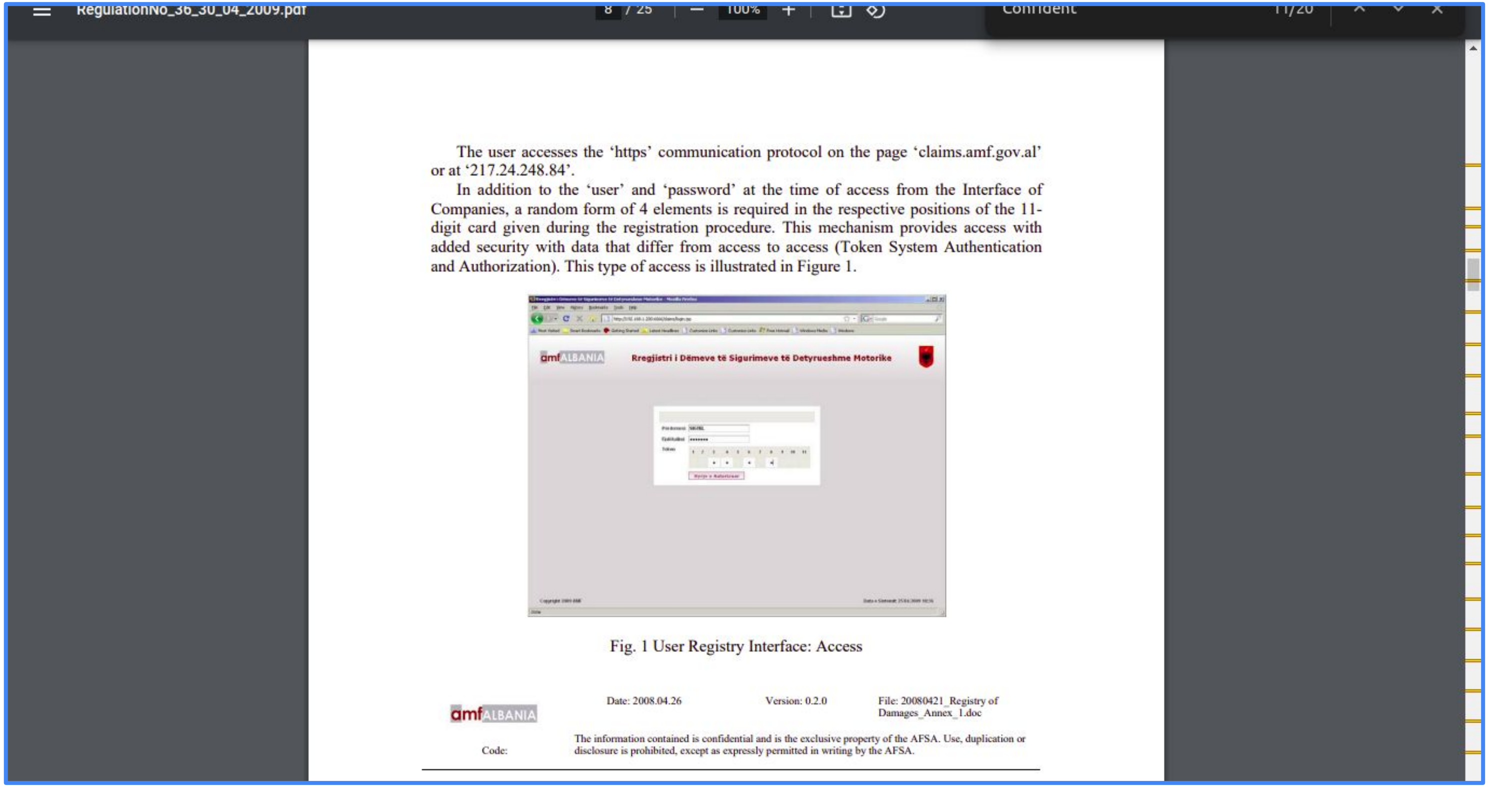
Which tools can be useful?

Searching (Dorks)

Advanced searching in normal engines can bring about sensitive information.

https://www.google.com/advanced_search

https://twitter.com/search-advanced?lang=en



RegulationNo_36_30_04_2009.pdf
8 / 25
100%
Confident
11/20
amf ALBANIA
Regjistri i Dëmeve të Sigurimeve të Detyrueshme Motorike

The user accesses the 'https' communication protocol on the page 'claims.amf.gov.al' or at '217.24.248.84'.

In addition to the 'user' and 'password' at the time of access from the Interface of Companies, a random form of 4 elements is required in the respective positions of the 11-digit card given during the registration procedure. This mechanism provides access with added security with data that differ from access to access (Token System Authentication and Authorization). This type of access is illustrated in Figure 1.

Fig. 1 User Registry Interface: Access

amfALBANIA

Date: 2008.04.26

Version: 0.2.0

File: 20080421_Registry of Damages_Annex_1.doc

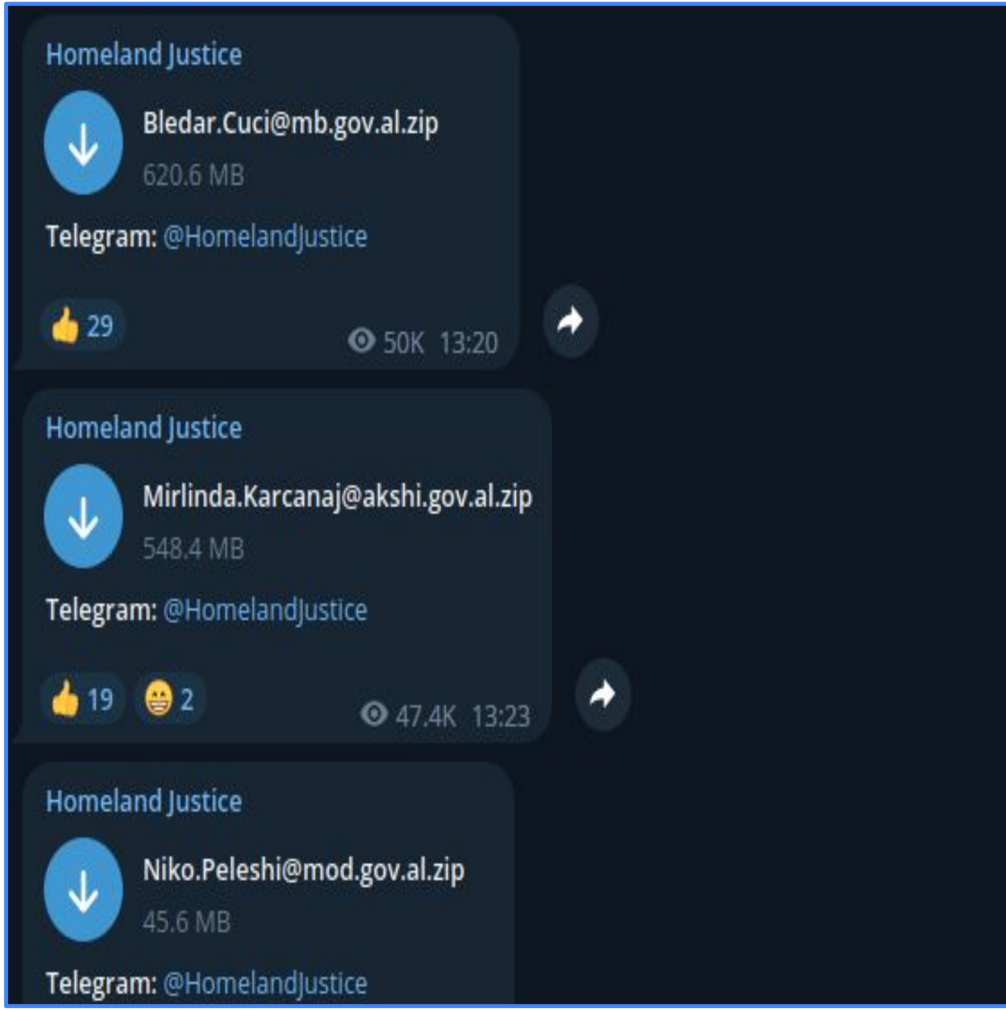
Code:

The information contained is confidential and is the exclusive property of the AFSA. Use, duplication or disclosure is prohibited, except as expressly permitted in writing by the AFSA.

Leaks

Some of the information leaked is in Deep Web. There are other cases when you can find the information in generic channels.

Like in Telegram…



Homeland Justice

Bledar.Cuci@mb.gov.al.zip
620.6 MB

Telegram: @HomelandJustice

👍 29 · 50K 13:20

Homeland Justice

Mirlinda.Karcanaj@akshi.gov.al.zip
548.4 MB

Telegram: @HomelandJustice

👍 19 😬 2 · 47.4K 13:23

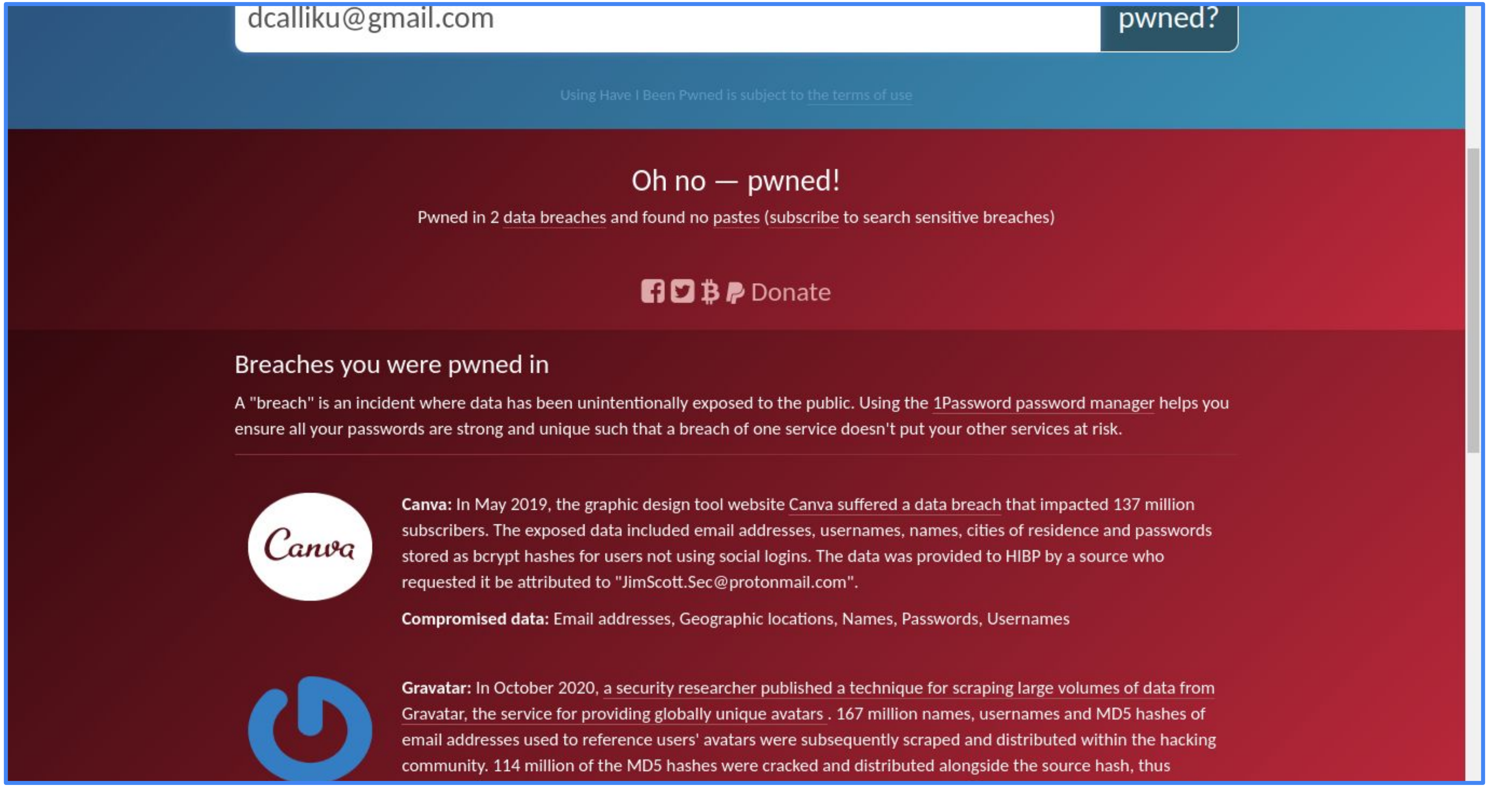
Homeland Justice

Niko.Peleshi@mod.gov.al.zip
45.6 MB

Telegram: @HomelandJustice

HaveIBeenPwned

There have been multiple leaks, and many of them from very well-known searches. HIBP provides the opportunity to check your email. *https://haveibeenpwned.com/*



Oh no — pwned!

Pwned in 2 data breaches and found no pastes (subscribe to search sensitive breaches)

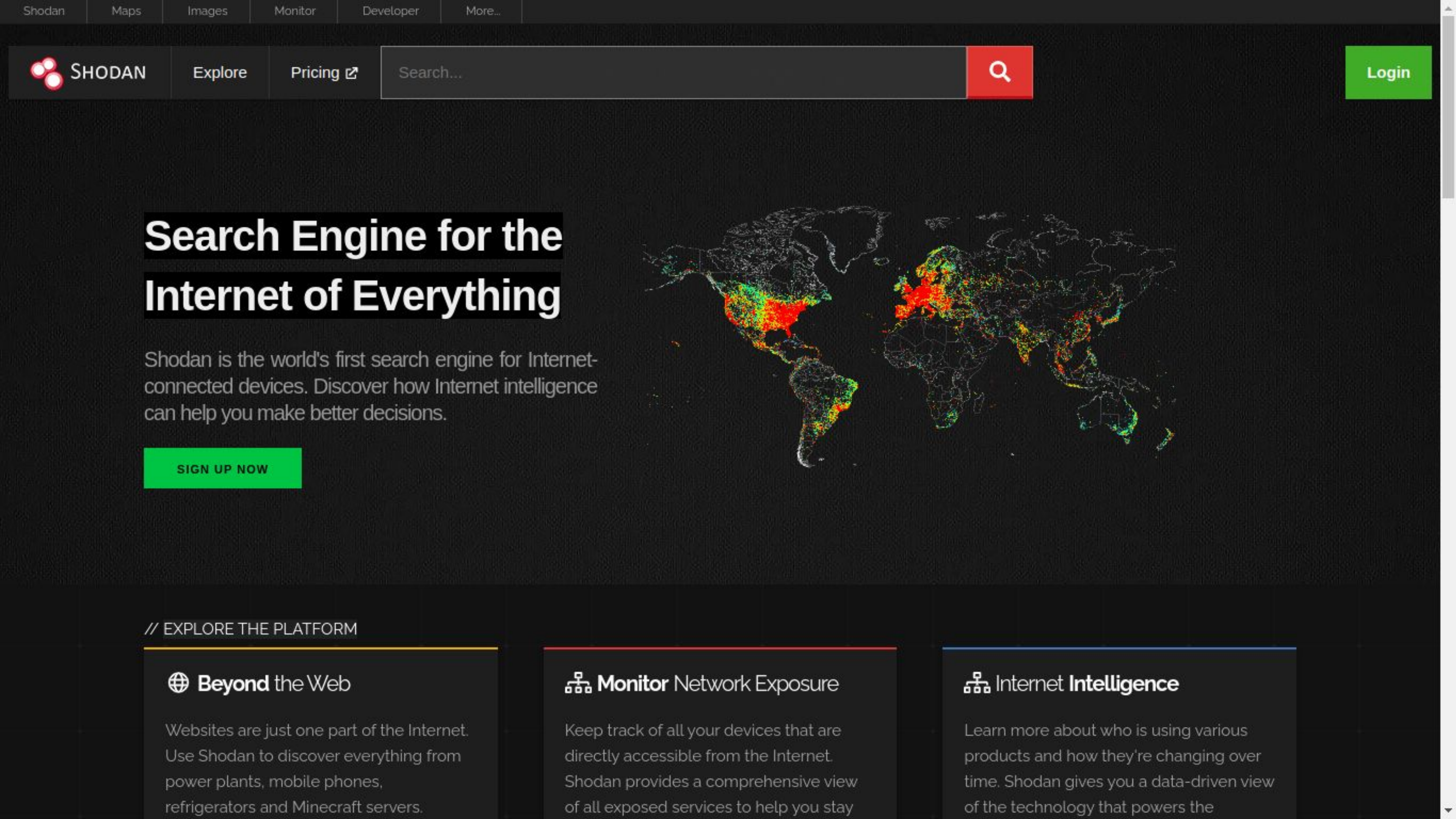
Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Canva: In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Compromised data: Email addresses, Geographic locations, Names, Passwords, Usernames

Gravatar: In October 2020, a security researcher published a technique for scraping large volumes of data from Gravatar, the service for providing globally unique avatars . 167 million names, usernames and MD5 hashes of email addresses used to reference users' avatars were subsequently scraped and distributed within the hacking community. 114 million of the MD5 hashes were cracked and distributed alongside the source hash, thus



Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

// EXPLORE THE PLATFORM

Beyond the Web

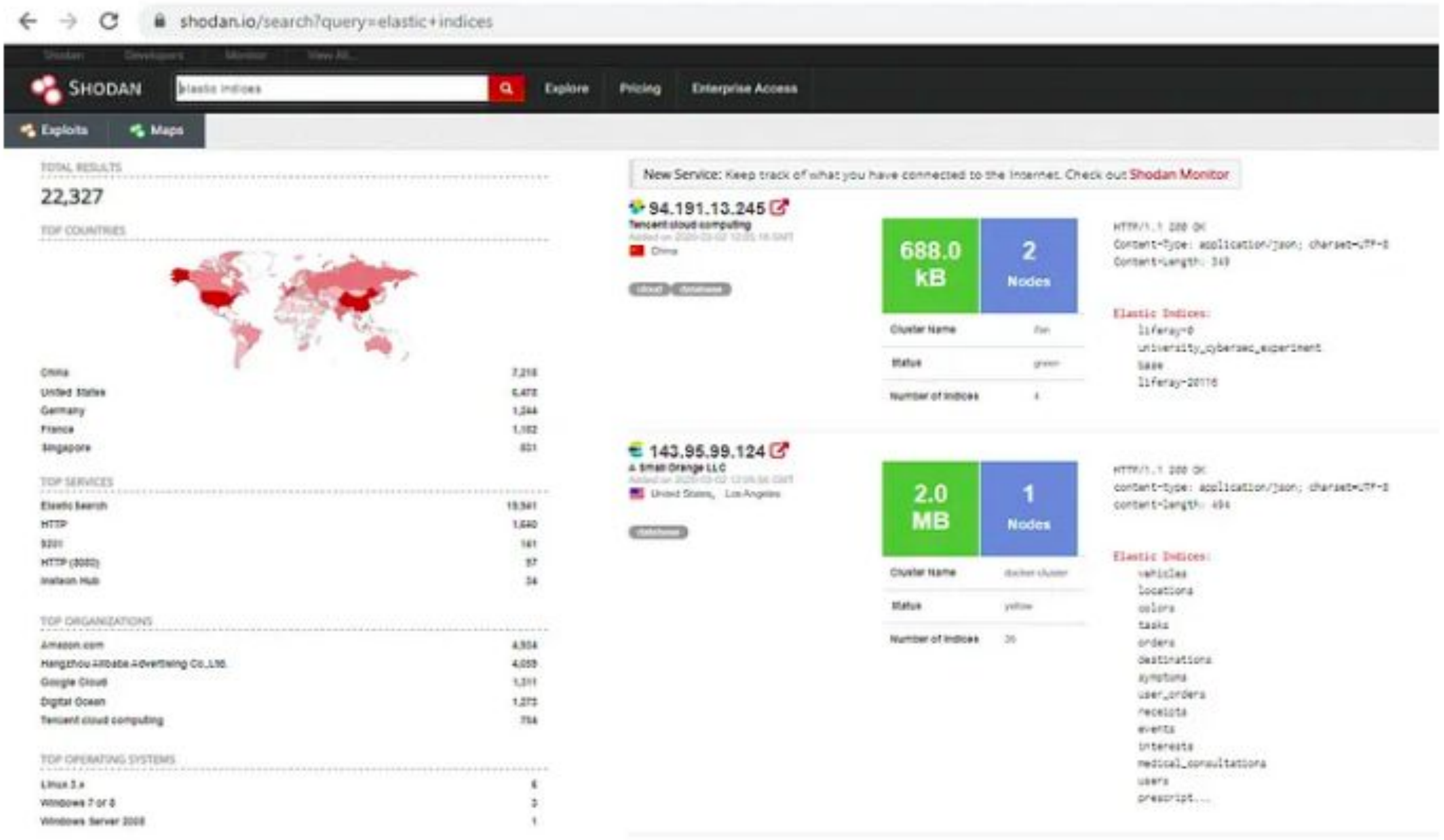
Websites are just one part of the Internet. Use Shodan to discover everything from power plants, mobile phones, refrigerators and Minecraft servers.

Monitor Network Exposure

Keep track of all your devices that are directly accessible from the Internet. Shodan provides a comprehensive view of all exposed services to help you stay

Internet Intelligence

Learn more about who is using various products and how they're changing over time. Shodan gives you a data-driven view of the technology that powers the



TOTAL RESULTS

22,327

TOP COUNTRIES

China	7,218
United States	6,478
Germany	1,244
France	1,102
Singapore	831

TOP SERVICES

Elastic Search	19,341
HTTP	1,640
9201	161
HTTP (8080)	57
Instacon Hub	34

TOP ORGANIZATIONS

Amazon.com	4,934
Hangzhou Alibaba Advertising Co.,Ltd.	4,033
Google Cloud	1,311
Digital Ocean	1,273
Tencent cloud computing	754

TOP OPERATING SYSTEMS

Linux 3.x	6
Windows 7 or 8	3
Windows Server 2008	1

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

94.191.13.245
Tencent cloud computing
Added on 2020-03-02 12:05:16 GMT
China

cloud database

688.0 kB | 2 Nodes

Cluster Name	[illegible]
Status	green
Number of indices	4

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Content-Length: 349

Elastic Indices:
    liferay-0
    university_cybersec_experiment
    base
    liferay-20116
```

143.95.99.124
A Small Orange LLC
Added on 2020-03-02 12:05:56 GMT
United States, Los Angeles

database

2.0 MB | 1 Nodes

Cluster Name	docker-cluster
Status	yellow
Number of indices	26

```
HTTP/1.1 200 OK
content-type: application/json; charset=UTF-8
content-length: 494

Elastic Indices:
    vehicles
    locations
    colors
    tasks
    orders
    destinations
    symptoms
    user_orders
    receipts
    events
    interests
    medical_consultations
    users
    prescript...
```

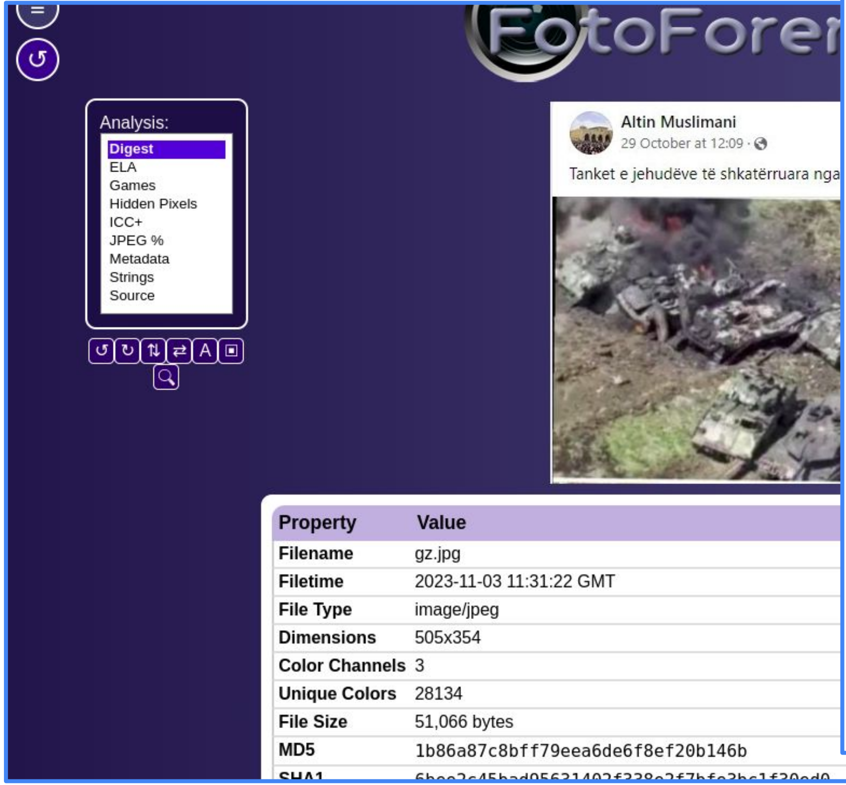
Sample Query elastic search

Verification

Image Verification

Find information regarding the origin, date, location through checking metadata of the picture. For the origin, you can ask the author themselves.

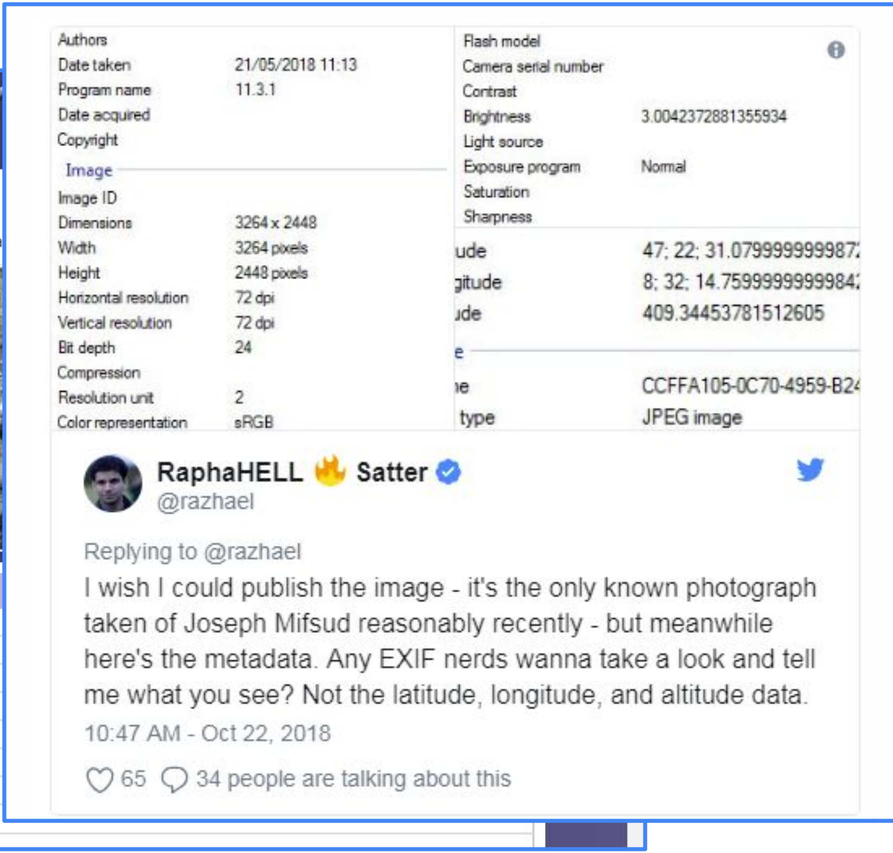
https://fotoforensics.com/



Altin Muslimani
29 October at 12:09 ·

Tanket e jehudëve të shkatërruara nga

Property	Value
Filename	gz.jpg
Filetime	2023-11-03 11:31:22 GMT
File Type	image/jpeg
Dimensions	505x354
Color Channels	3
Unique Colors	28134
File Size	51,066 bytes
MD5	1b86a87c8bff79eea6de6f8ef20b146b
SHA1	6bea2c45bad95631402f338e2f7bfe3bc1f30ed0



Authors	
Date taken	21/05/2018 11:13
Program name	11.3.1
Date acquired	
Copyright	
Image	
Image ID	
Dimensions	3264 x 2448
Width	3264 pixels
Height	2448 pixels
Horizontal resolution	72 dpi
Vertical resolution	72 dpi
Bit depth	24
Compression	
Resolution unit	2
Color representation	sRGB

Flash model	
Camera serial number	
Contrast	
Brightness	3.0042372881355934
Light source	
Exposure program	Normal
Saturation	
Sharpness	
ude	47; 22; 31.0799999999987
gitude	8; 32; 14.7599999999984
ude	409.34453781512605
e	
ne	CCFFA105-0C70-4959-B24
type	JPEG image

RaphaHELL 🔥 Satter
@razhael

Replying to @razhael

I wish I could publish the image - it's the only known photograph taken of Joseph Mifsud reasonably recently - but meanwhile here's the metadata. Any EXIF nerds wanna take a look and tell me what you see? Not the latitude, longitude, and altitude data.

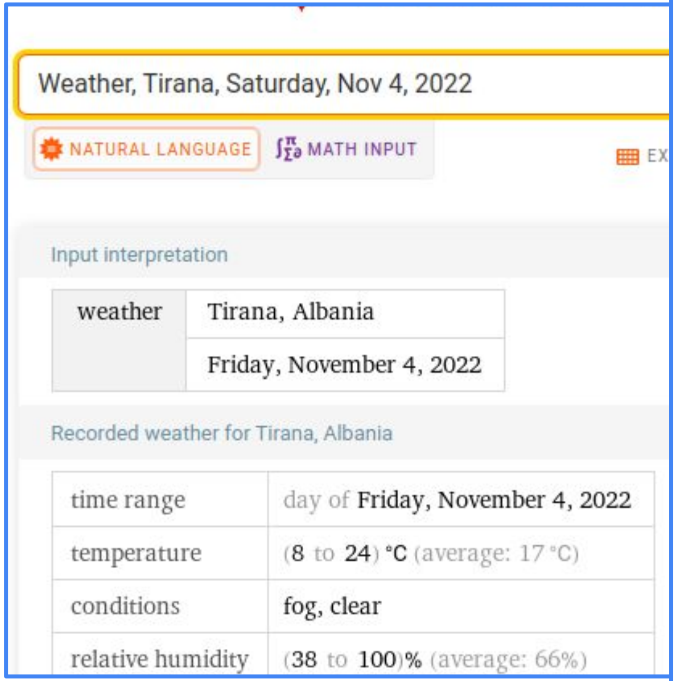
10:47 AM - Oct 22, 2018

♡ 65 💬 34 people are talking about this

Video verification

Find the earliest date uploaded, check thumbnail, check whether it has been shared from other sources, check the author and their upload time.

https://www.wolframalpha.com/input?i=Weather%2C+Tirana%2C+Saturday%2C+Nov+4%2C+2022



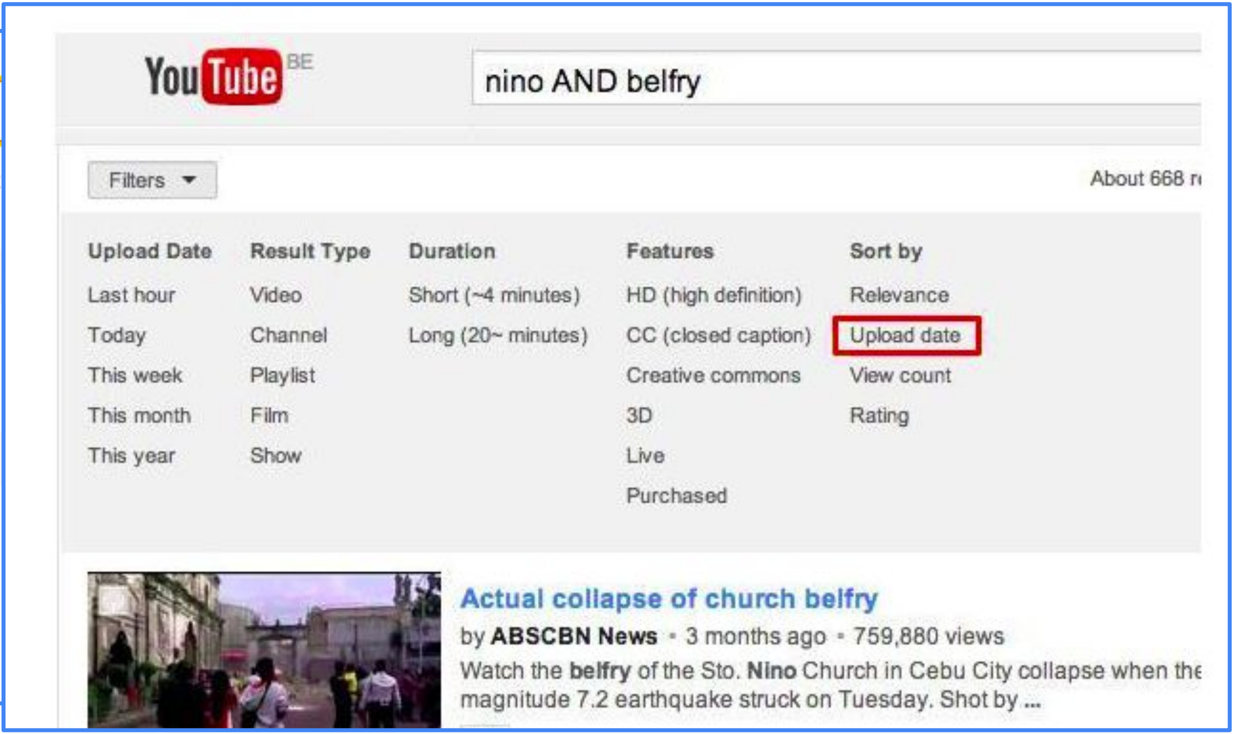
Weather, Tirana, Saturday, Nov 4, 2022

Input interpretation

weather	Tirana, Albania
	Friday, November 4, 2022

Recorded weather for Tirana, Albania

time range	day of Friday, November 4, 2022
temperature	(8 to 24) °C (average: 17 °C)
conditions	fog, clear
relative humidity	(38 to 100)% (average: 66%)



nino AND belfry

Upload Date	Result Type	Duration	Features	Sort by
Last hour	Video	Short (~4 minutes)	HD (high definition)	Relevance
Today	Channel	Long (20~ minutes)	CC (closed caption)	Upload date
This week	Playlist		Creative commons	View count
This month	Film		3D	Rating
This year	Show		Live	
			Purchased	

Actual collapse of church belfry

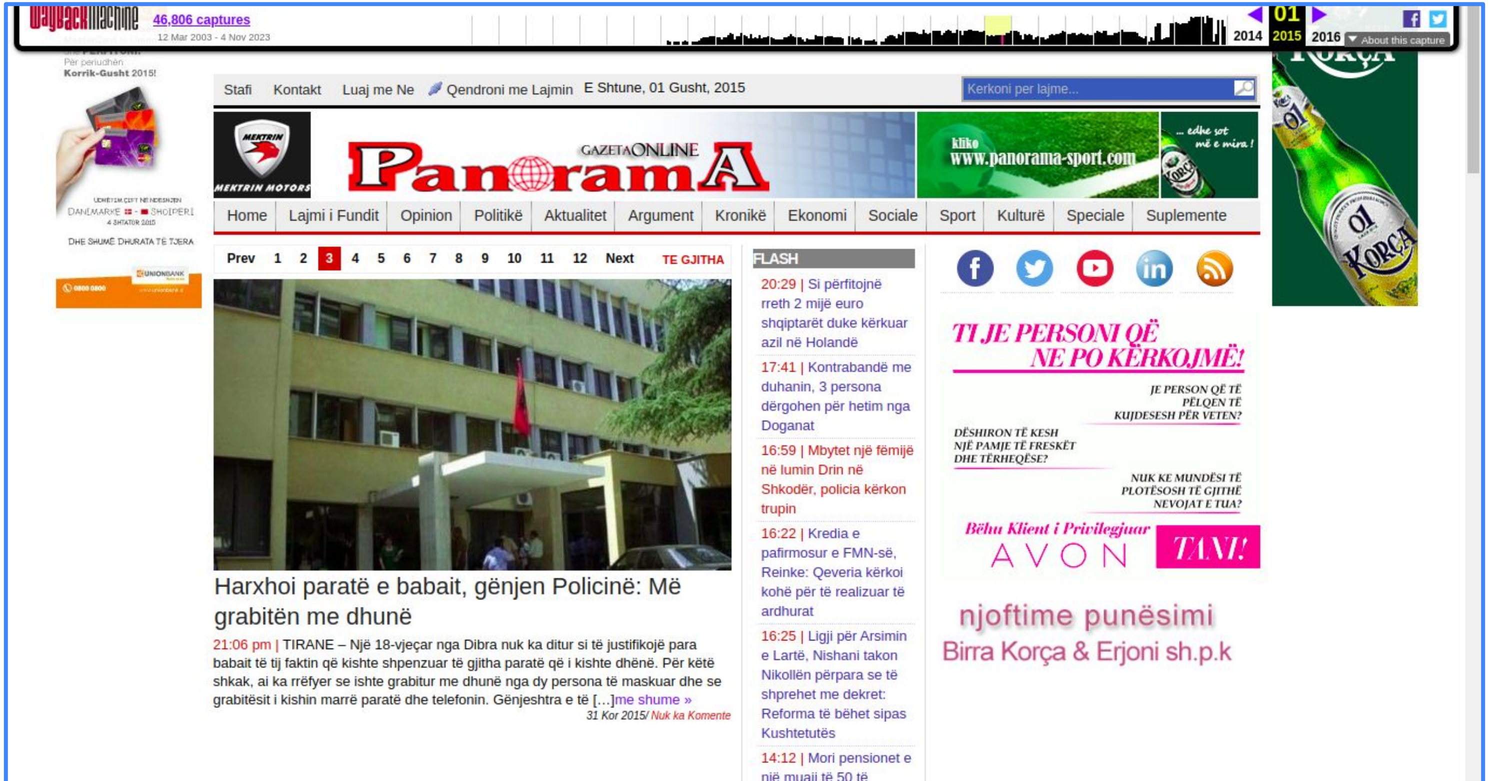
by **ABSCBN News** · 3 months ago · 759,880 views

Watch the **belfry** of the Sto. **Nino** Church in Cebu City collapse when the magnitude 7.2 earthquake struck on Tuesday. Shot by ...

Wayback Machine

Find how content has changed in a website. Can be useful for fact-checking and checking how the relevant news was set in relation to other news.

https://web.archive.org/web/20150801031955/http://www.panorama.com.al/



46,806 captures
12 Mar 2003 - 4 Nov 2023

2014 01 2015 2016
About this capture

Për periudhën Korrik-Gusht 2015!

DANIMARKË - SHQIPËRI
4 SHTATOR 2015

DHE SHUMË DHURATA TË TJERA

UNIONBANK

Stafi Kontakt Luaj me Ne Qendroni me Lajmin E Shtune, 01 Gusht, 2015

Kerkoni per lajme...

GAZETA ONLINE PanoramA

kliko www.panorama-sport.com

... edhe sot më e mira!

Home | Lajmi i Fundit | Opinion | Politikë | Aktualitet | Argument | Kronikë | Ekonomi | Sociale | Sport | Kulturë | Speciale | Suplemente

Prev 1 2 3 4 5 6 7 8 9 10 11 12 Next TE GJITHA

Harxhoi paratë e babait, gënjen Policinë: Më grabitën me dhunë

21:06 pm | TIRANE – Një 18-vjeçar nga Dibra nuk ka ditur si të justifikojë para babait të tij faktin që kishte shpenzuar të gjitha paratë që i kishte dhënë. Për këtë shkak, ai ka rrëfyer se ishte grabitur me dhunë nga dy persona të maskuar dhe se grabitësit i kishin marrë paratë dhe telefonin. Gënjeshtra e të […]me shume »

31 Kor 2015/ Nuk ka Komente

FLASH

20:29 | Si përfitojnë rreth 2 mijë euro shqiptarët duke kërkuar azil në Holandë

17:41 | Kontrabandë me duhanin, 3 persona dërgohen për hetim nga Doganat

16:59 | Mbytet një fëmijë në lumin Drin në Shkodër, policia kërkon trupin

16:22 | Kredia e pafirmosur e FMN-së, Reinke: Qeveria kërkoi kohë për të realizuar të ardhurat

16:25 | Ligji për Arsimin e Lartë, Nishani takon Nikollën përpara se të shprehet me dekret: Reforma të bëhet sipas Kushtetutës

14:12 | Mori pensionet e një muaji të 50 të

TI JE PERSONI QË NE PO KËRKOJMË!

JE PERSON QË TË PËLQEN TË KUJDESESH PËR VETEN?

DËSHIRON TË KESH NJË PAMJE TË FRESKËT DHE TËRHEQËSE?

NUK KE MUNDËSI TË PLOTËSOSH TË GJITHË NEVOJAT E TUA?

Bëhu Klient i Privilegjuar AVON TANI!

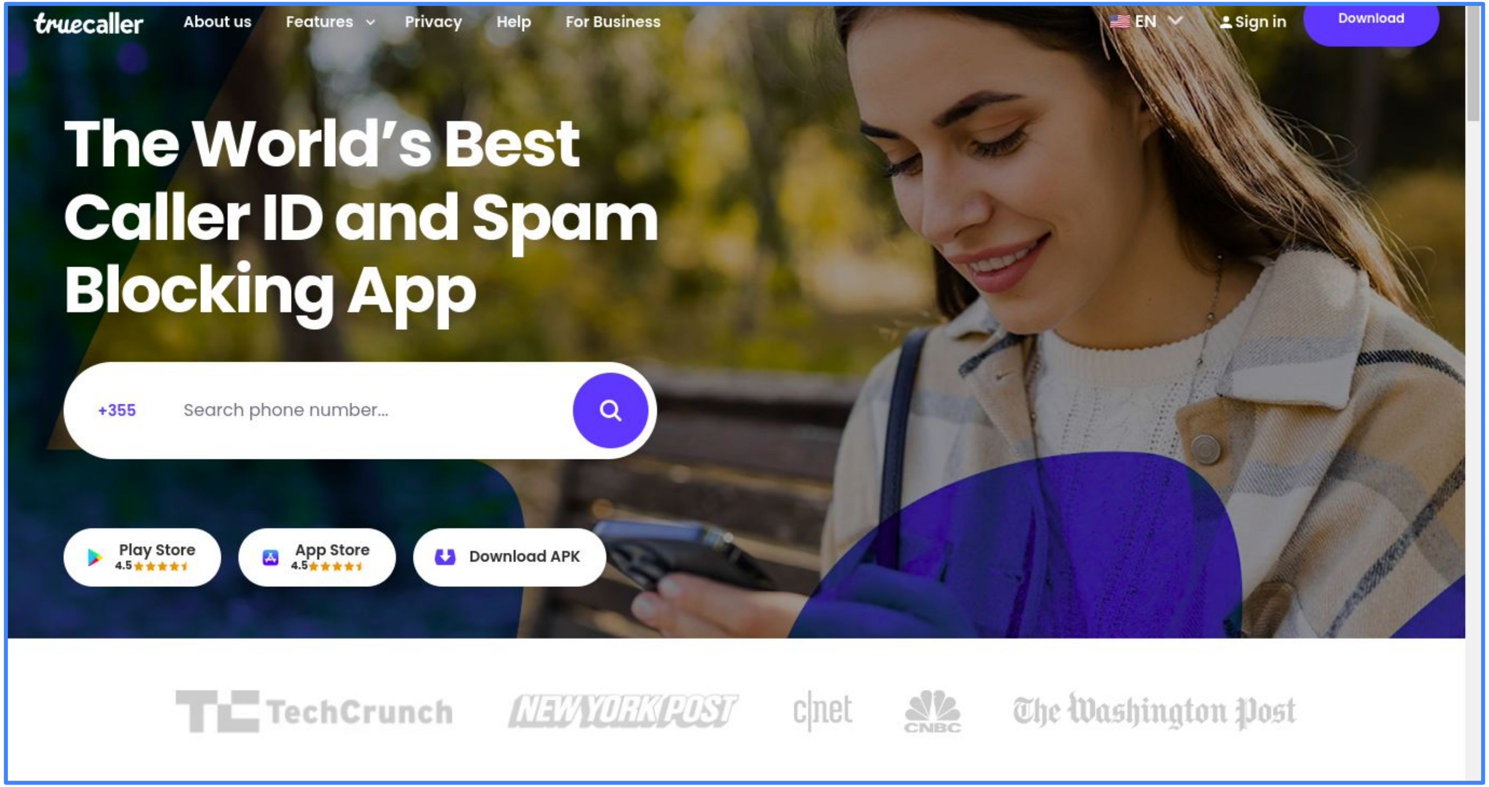
njoftime punësimi
Birra Korça & Erjoni sh.p.k

Social / profile analysis

Your phone

TrueCaller, a database of phone numbers, given voluntarily (...).

https://www.truecaller.com/

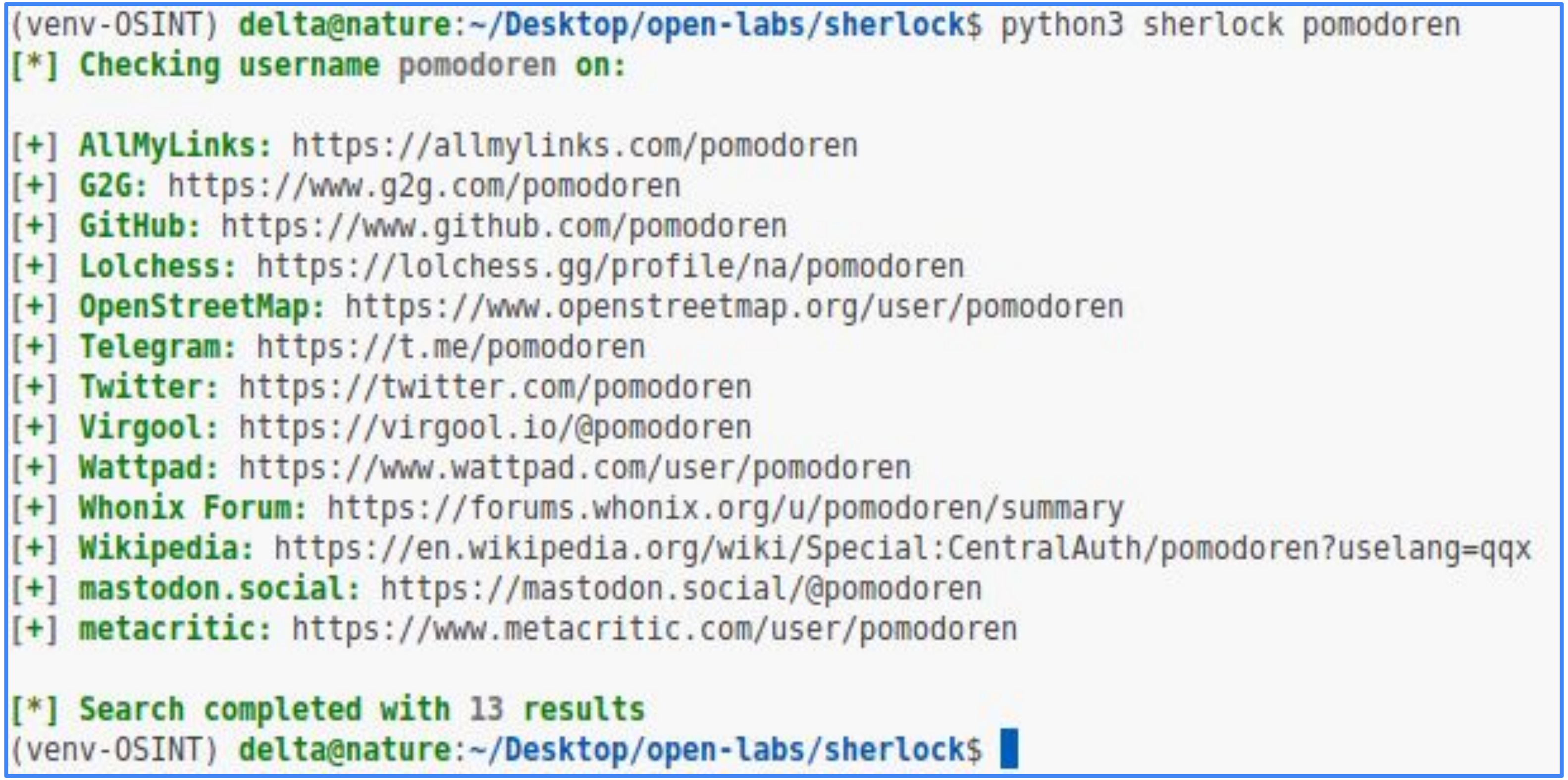


The World's Best Caller ID and Spam Blocking App

Social profiles

Filter all the related social/professional profiles based on usernames.

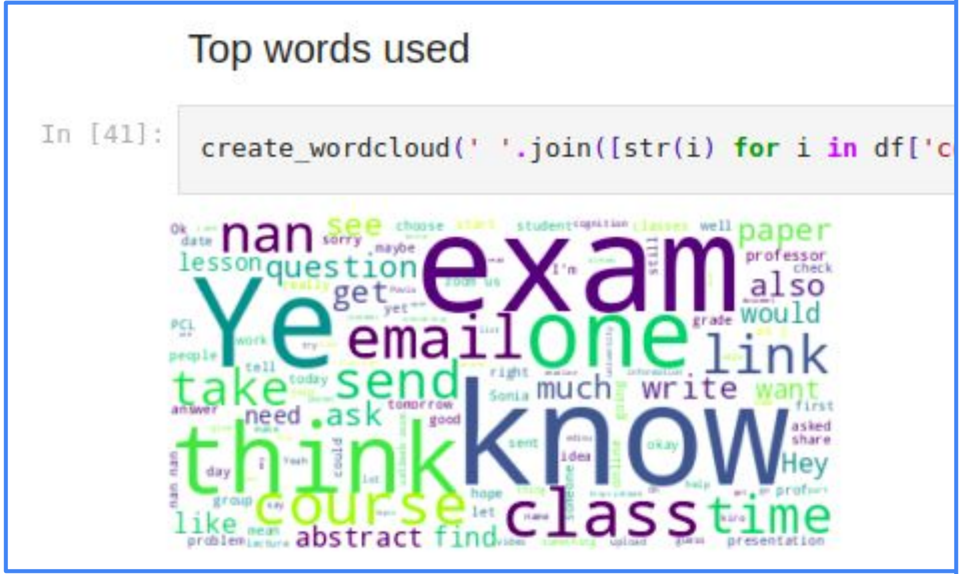
https://github.com/sherlock-project/sherlock



```
(venv-OSINT) delta@nature:~/Desktop/open-labs/sherlock$ python3 sherlock pomodoren
[*] Checking username pomodoren on:

[+] AllMyLinks: https://allmylinks.com/pomodoren
[+] G2G: https://www.g2g.com/pomodoren
[+] GitHub: https://www.github.com/pomodoren
[+] Lolchess: https://lolchess.gg/profile/na/pomodoren
[+] OpenStreetMap: https://www.openstreetmap.org/user/pomodoren
[+] Telegram: https://t.me/pomodoren
[+] Twitter: https://twitter.com/pomodoren
[+] Virgool: https://virgool.io/@pomodoren
[+] Wattpad: https://www.wattpad.com/user/pomodoren
[+] Whonix Forum: https://forums.whonix.org/u/pomodoren/summary
[+] Wikipedia: https://en.wikipedia.org/wiki/Special:CentralAuth/pomodoren?uselang=qqx
[+] mastodon.social: https://mastodon.social/@pomodoren
[+] metacritic: https://www.metacritic.com/user/pomodoren

[*] Search completed with 13 results
(venv-OSINT) delta@nature:~/Desktop/open-labs/sherlock$
```

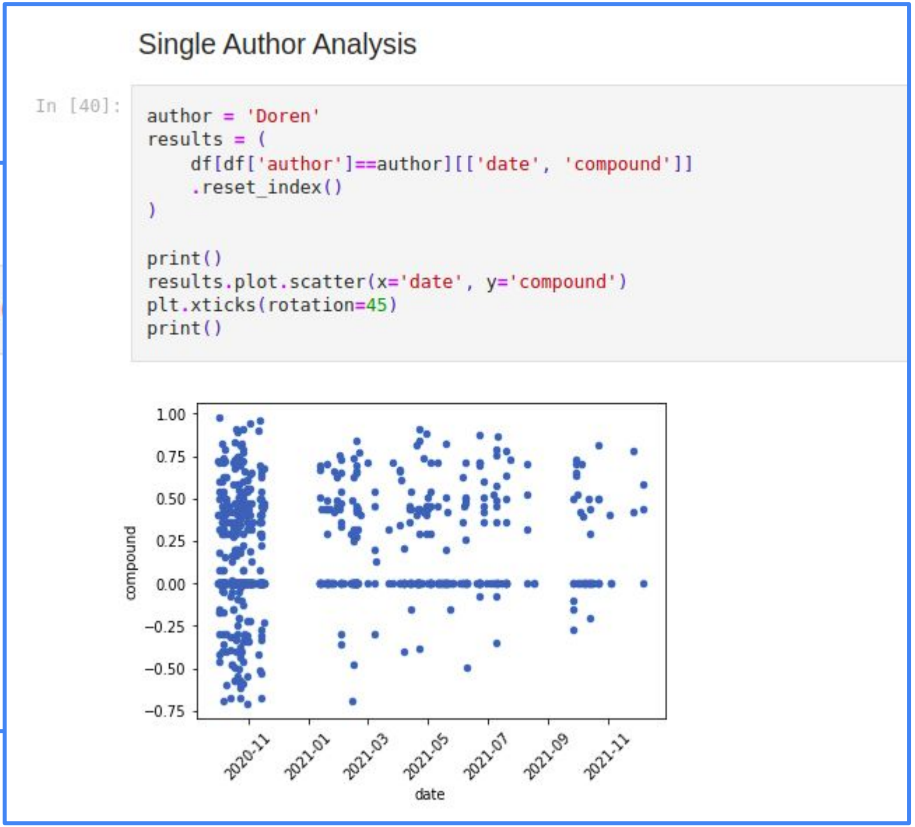
Analyze the chat

Get and analyze the data from your chat.
Local, will share.



Top words used

```
In [41]: create_wordcloud(' '.join([str(i) for i in df['c
```



Single Author Analysis

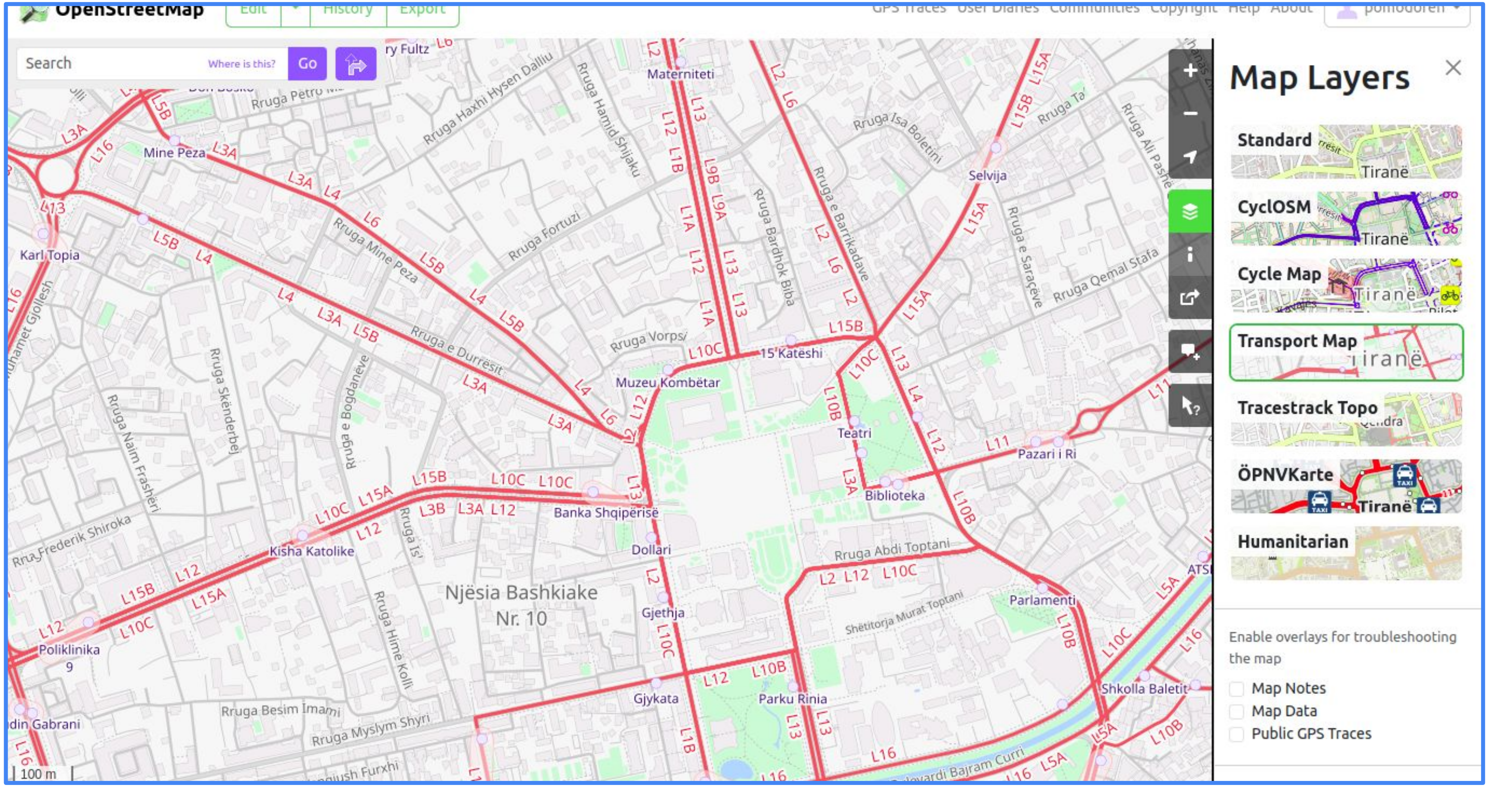
```
In [40]: author = 'Doren'
         results = (
             df[df['author']==author][['date', 'compound']]
             .reset_index()
         )

         print()
         results.plot.scatter(x='date', y='compound')
         plt.xticks(rotation=45)
         print()
```

Geospatial

OpenStreetMap

Has extensive information about the city’s infrastructure, buildings, landuse, natural properties, and more. It can be useful to understand scale.

https://www.openstreetmap.org/#map=16/41.3293/19.8154&layers=T



Map Layers

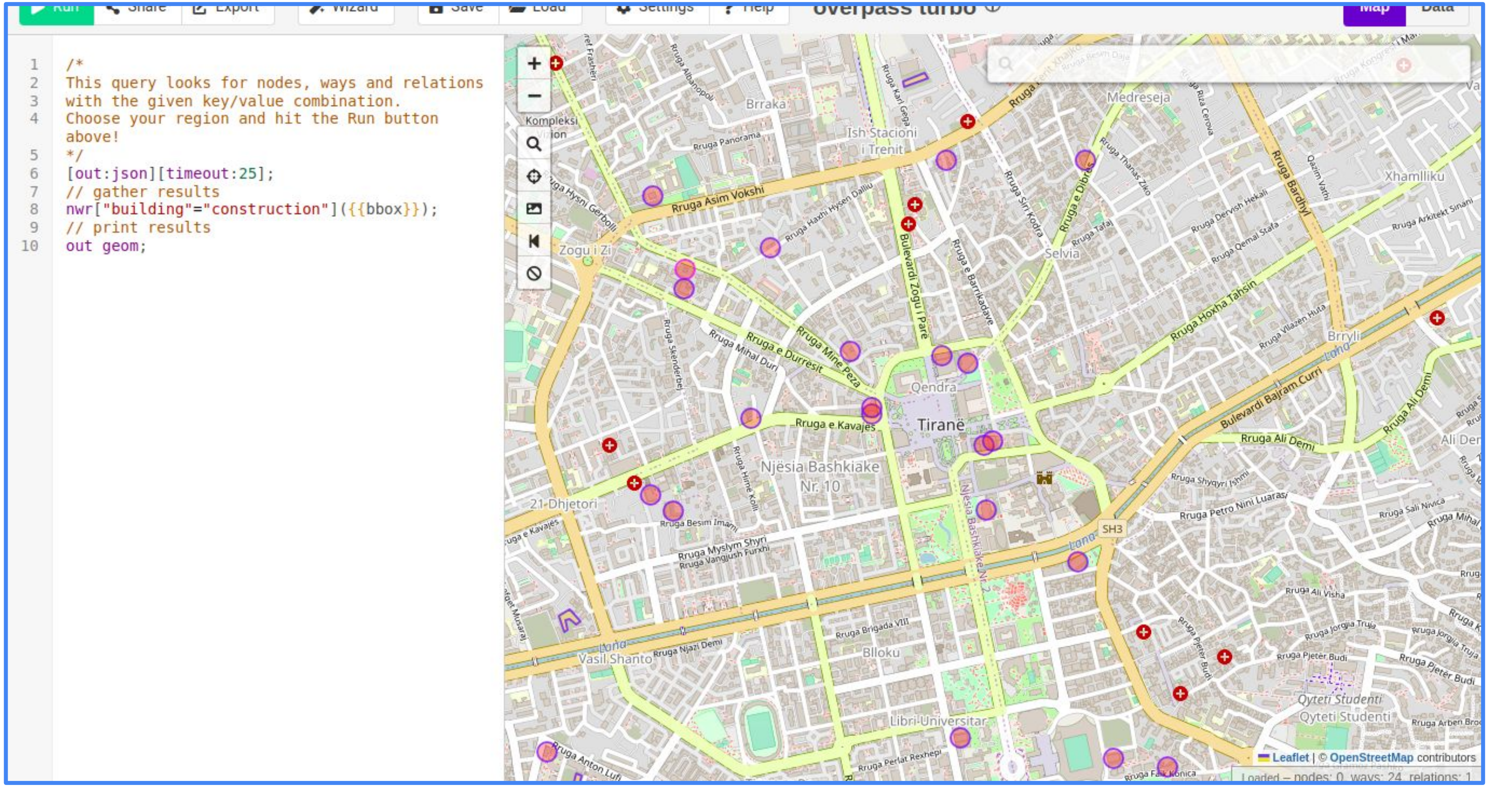
- Standard
- CyclOSM
- Cycle Map
- Transport Map
- Tracestrack Topo
- ÖPNVKarte
- Humanitarian

Enable overlays for troubleshooting the map

□ Map Notes
□ Map Data
□ Public GPS Traces

Overpass-Turbo

Advanced searching for all the properties of the OpenStreetMap.
Below you can see all the active building sites in the center of Tirana.
https://overpass-turbo.eu/?template=key-value&key=building&value=construction



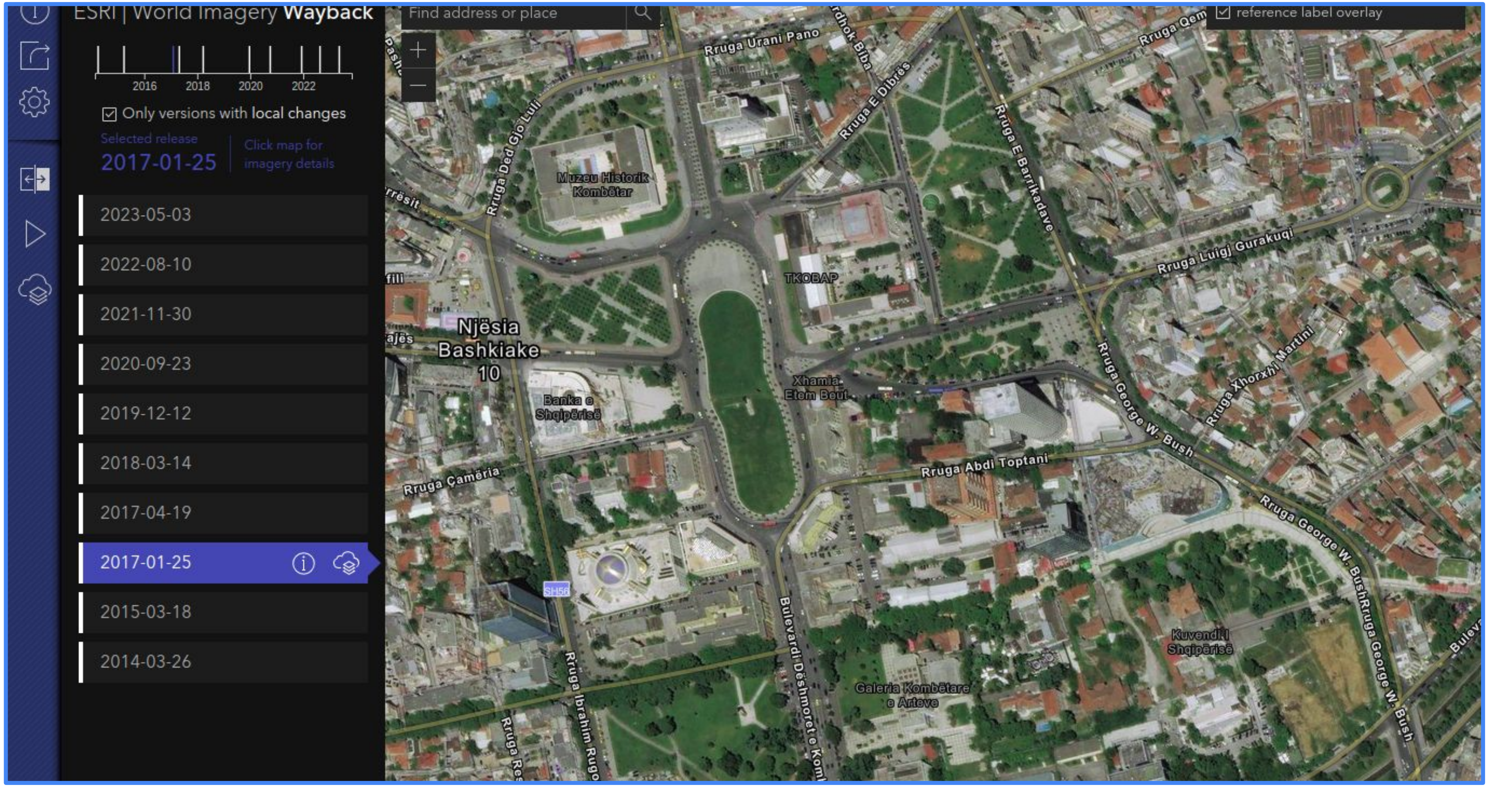
```
/*
This query looks for nodes, ways and relations
with the given key/value combination.
Choose your region and hit the Run button
above!
*/
[out:json][timeout:25];
// gather results
nwr["building"="construction"]({{bbox}});
// print results
out geom;
```

Loaded – nodes: 0, ways: 24, relations: 1

Geospatial Wayback Machines

They allow different tools for comparing the satellite data in time. It can be helpful in case of searching some specific information change you can't get from OSM.

https://livingatlas.arcgis.com/wayback/#active=9486&mapCenter=19.820%2C41.328%2C17



ESRI | World Imagery **Wayback**

Find address or place

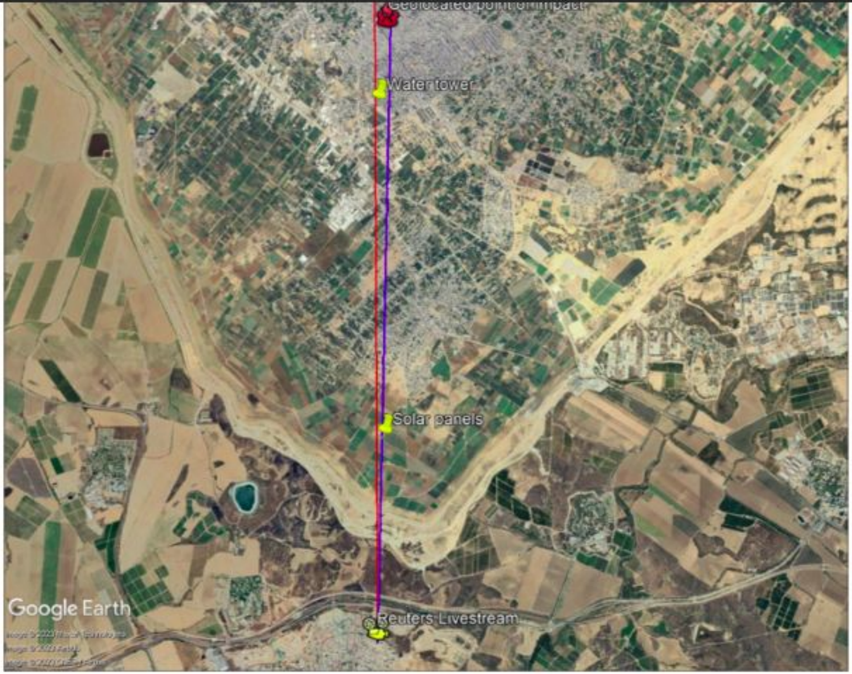
☑ reference label overlay

☑ Only versions with local changes

Selected release
2017-01-25

Click map for imagery details

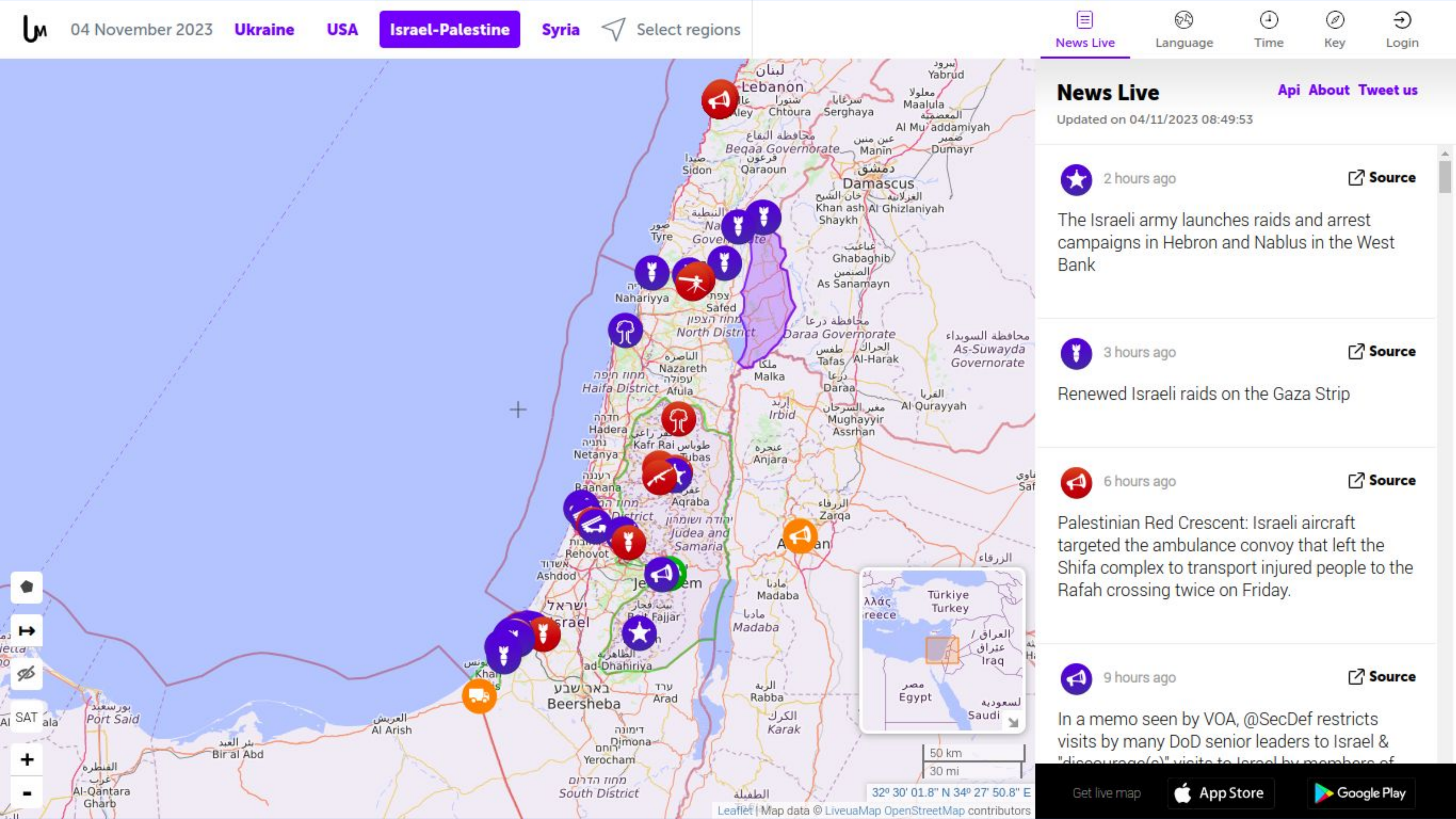
- 2023-05-03
- 2022-08-10
- 2021-11-30
- 2020-09-23
- 2019-12-12
- 2018-03-14
- 2017-04-19
- 2017-01-25
- 2015-03-18
- 2014-03-26



Top: Reuters Livestream (Source: Reuters) Bottom: Image showing alignment used for identification of point of impact (Source: Google/Maxar Technologies/Airbus/CNES)

At least 40 people were reportedly killed in the strike.

The IDF confirmed an airstrike was carried out on Jabalia, stating, "The strike damaged Hamas's command and control in the area, as well as its ability to directly military activity against IDF soldiers operating throughout the Gaza Strip."



News Live

Api About Tweet us

Updated on 04/11/2023 08:49:53

2 hours ago Source

The Israeli army launches raids and arrest campaigns in Hebron and Nablus in the West Bank

3 hours ago Source

Renewed Israeli raids on the Gaza Strip

6 hours ago Source

Palestinian Red Crescent: Israeli aircraft targeted the ambulance convoy that left the Shifa complex to transport injured people to the Rafah crossing twice on Friday.

9 hours ago Source

In a memo seen by VOA, @SecDef restricts visits by many DoD senior leaders to Israel & "discourage(s)" visits to Israel by members of

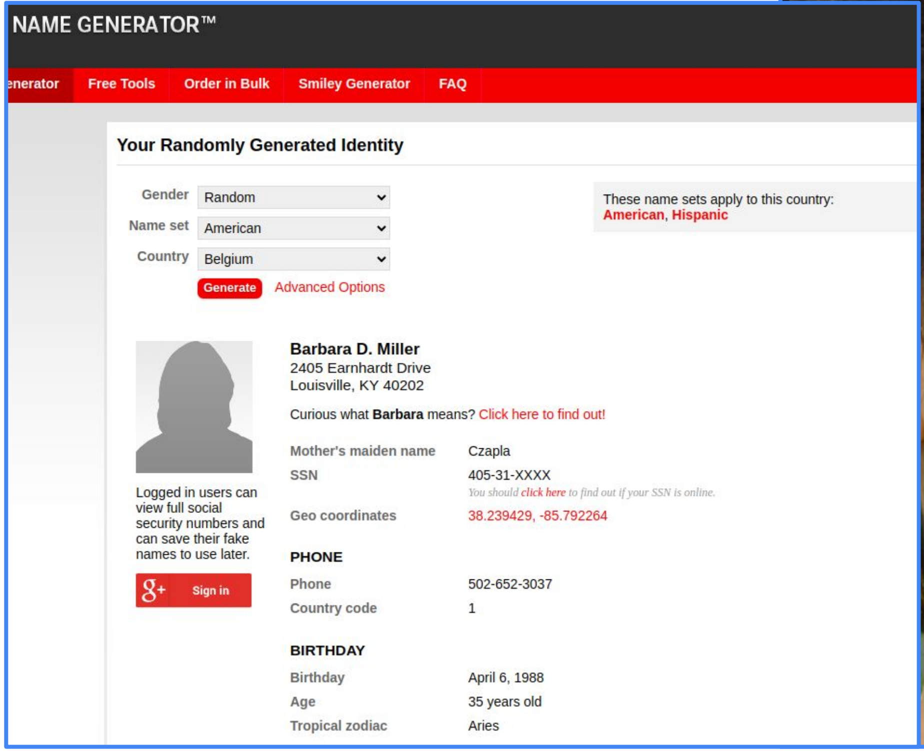
Artificial Generation

This Person Does Not Exist

How to create a persona …

https://thispersondoesnotexist.com/

https://www.fakenamegenerator.com/ge



NAME GENERATOR™

Your Randomly Generated Identity

Gender	Random
Name set	American
Country	Belgium

Generate Advanced Options

These name sets apply to this country: American, Hispanic

Logged in users can view full social security numbers and can save their fake names to use later.

Sign in

Barbara D. Miller
2405 Earnhardt Drive
Louisville, KY 40202

Curious what **Barbara** means? Click here to find out!

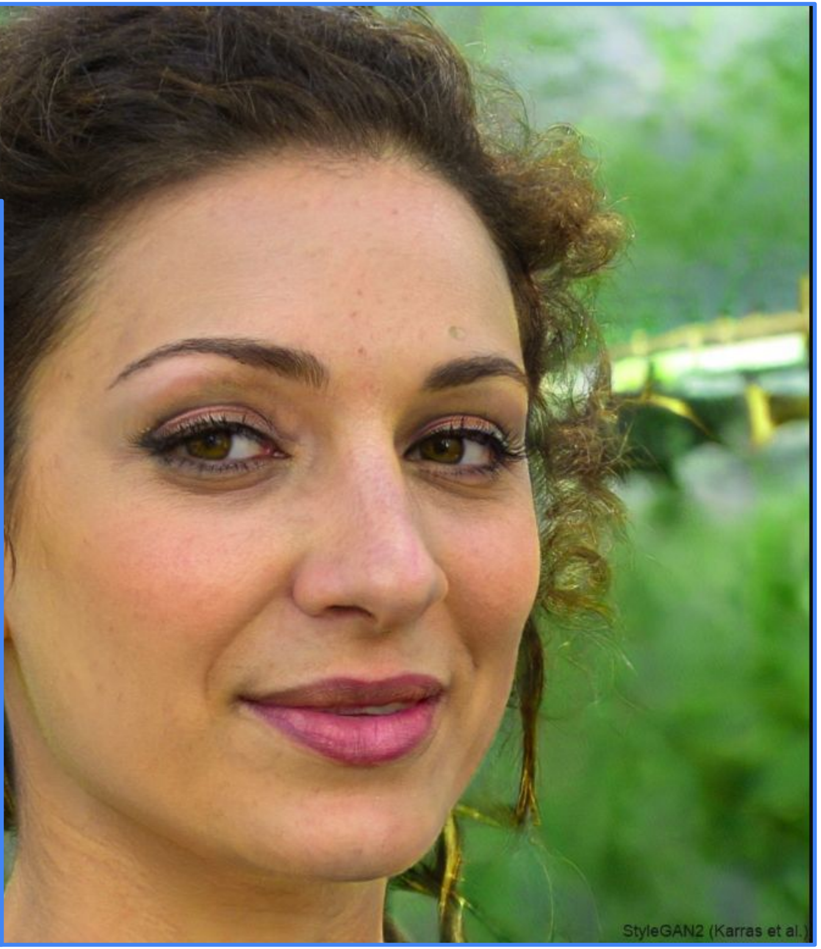
Mother's maiden name	Czapla
SSN	405-31-XXXX You should click here to find out if your SSN is online.
Geo coordinates	38.239429, -85.792264

PHONE

Phone	502-652-3037
Country code	1

BIRTHDAY

Birthday	April 6, 1988
Age	35 years old
Tropical zodiac	Aries



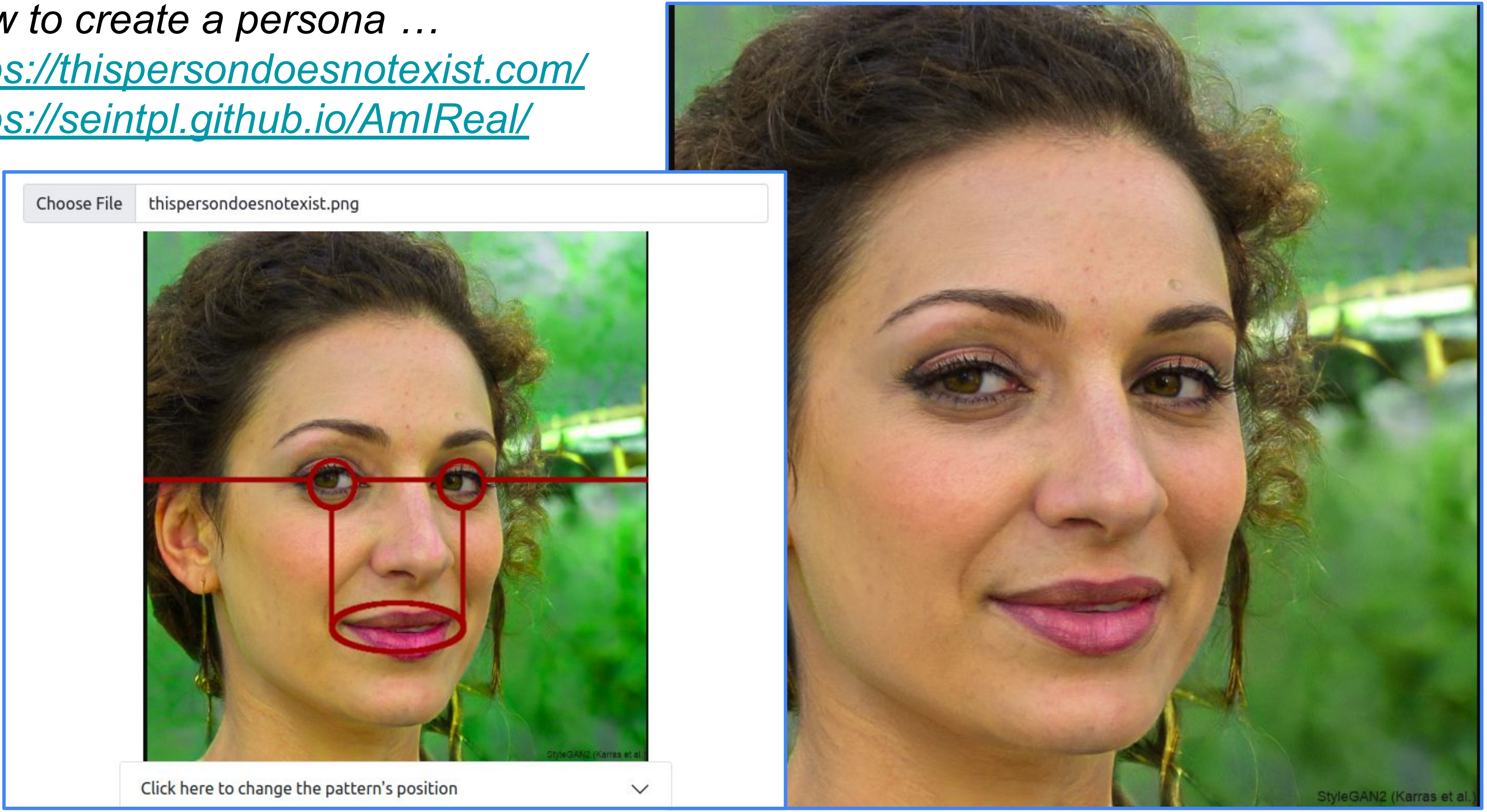
StyleGAN2 (Karras et al.)

This Person Does Not Exist

How to create a persona …

[*https://thispersondoesnotexist.com/*](https://thispersondoesnotexist.com/)

[*https://seintpl.github.io/AmIReal/*](https://seintpl.github.io/AmIReal/)



Choose File thispersondoesnotexist.png

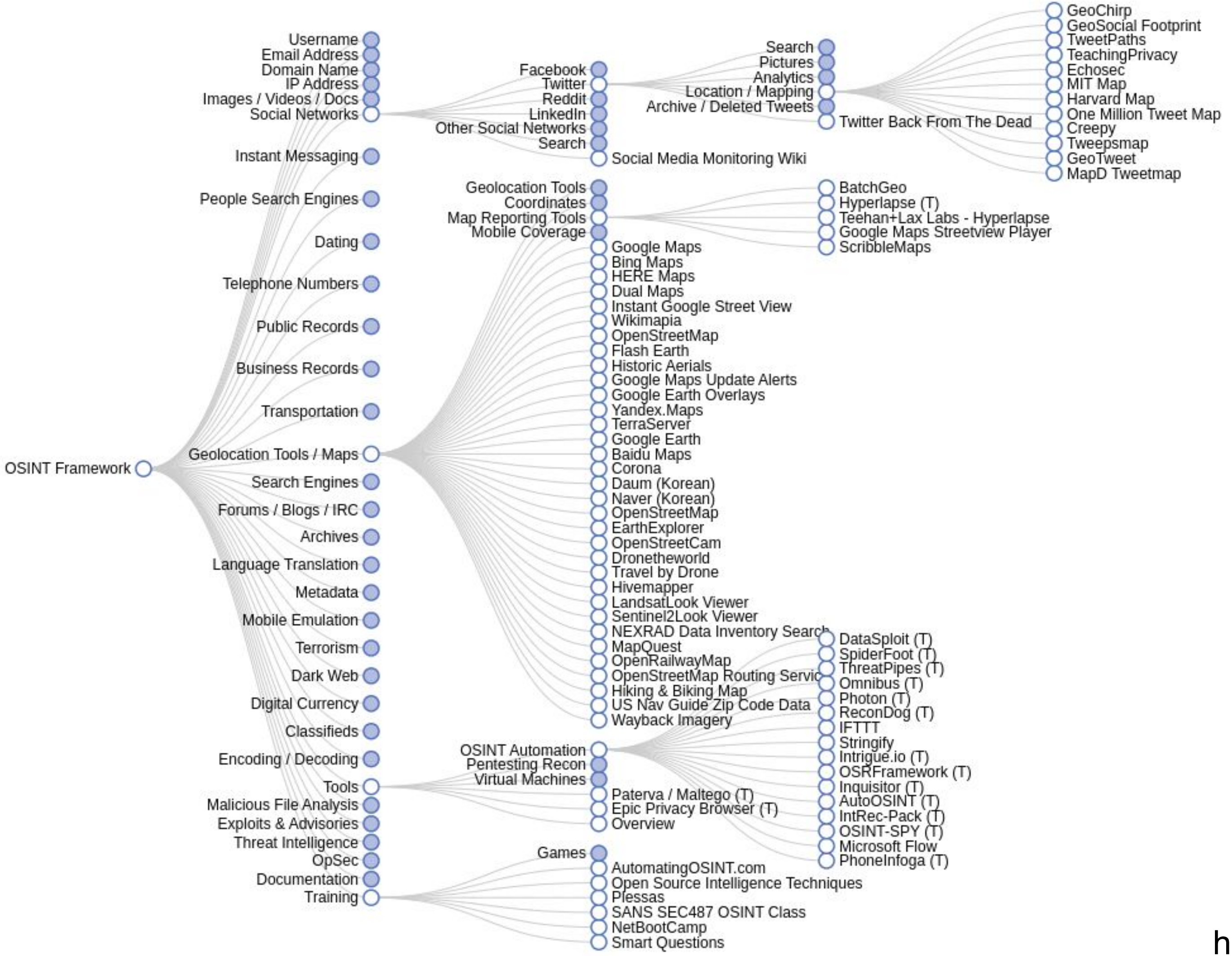
StyleGAN2 (Karras et al.)
Click here to change the pattern's position
StyleGAN2 (Karras et al.)

Next steps?

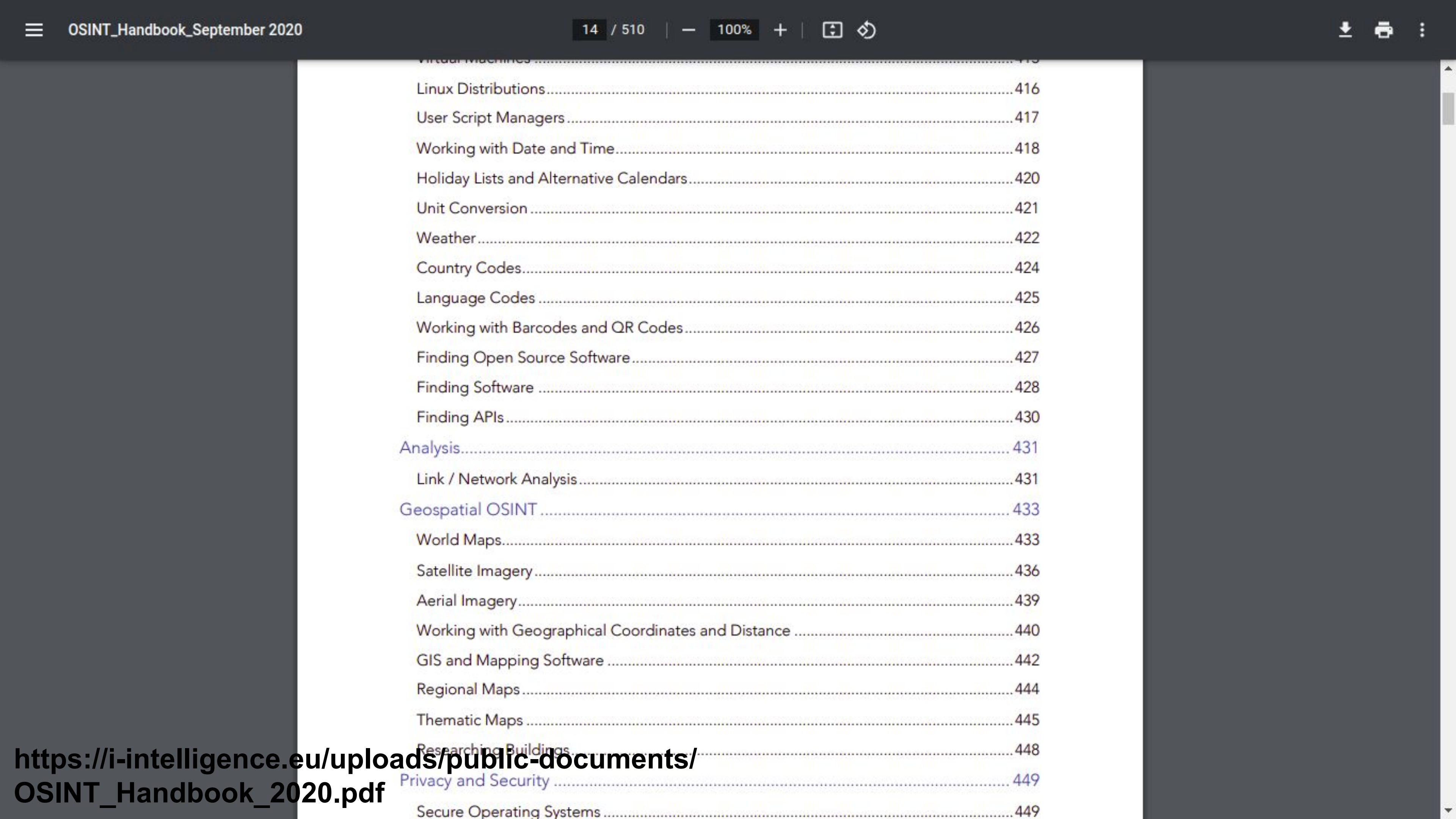
Appendix

References

- https://github.com/cipher387/Dorks-collections-list
- https://benjaminstrick.com/twitter-analysis-identifying-a-pro-bjp-influence-operation-in-india/
- https://gbhackers.com/latest-google-dorks-list/
- https://forensic-architecture.org/
- https://exposingtheinvisible.org/en/news/summer-series-investigation-2023/#w4
- https://www.bellingcat.com/news/americas/2018/10/26/joseph-mifsud-rush-exif/



https://osintframework.com/



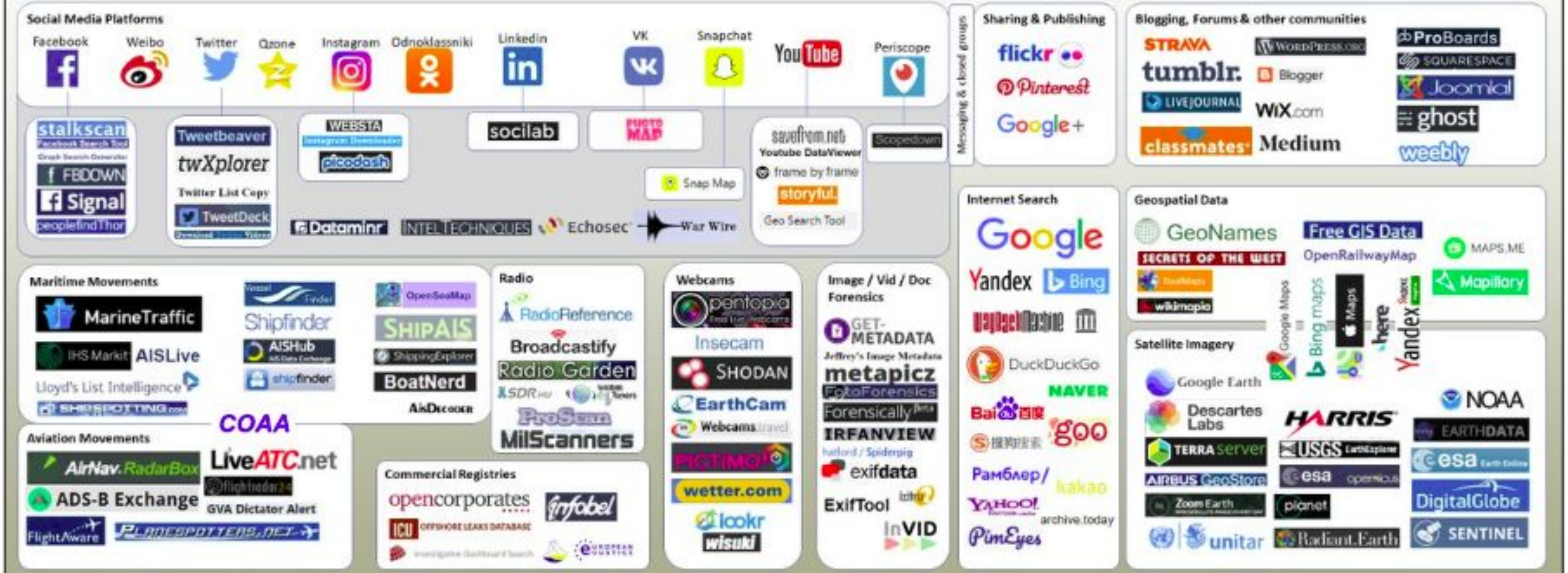
Virtual Machines 415
Linux Distributions 416
User Script Managers 417
Working with Date and Time 418
Holiday Lists and Alternative Calendars 420
Unit Conversion 421
Weather 422
Country Codes 424
Language Codes 425
Working with Barcodes and QR Codes 426
Finding Open Source Software 427
Finding Software 428
Finding APIs 430
Analysis 431
Link / Network Analysis 431
Geospatial OSINT 433
World Maps 433
Satellite Imagery 436
Aerial Imagery 439
Working with Geographical Coordinates and Distance 440
GIS and Mapping Software 442
Regional Maps 444
Thematic Maps 445
Researching Buildings 448
Privacy and Security 449
Secure Operating Systems 449

https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf

OSINT Landscape v.1 February 2018

Open Source Intelligence (/OSINV – Open Source Investigation)

COVERT SHORES www.hisutton.com bellingcat



Social Media Platforms

Facebook, Weibo, Twitter, Qzone, Instagram, Odnoklassniki, Linkedin, VK, Snapchat, YouTube, Periscope

stalkscan Facebook Search Tool, Graph Search Generator, FBDOWN, Signal, peoplefindThor

Tweetbeaver, twXplorer, Twitter List Copy, TweetDeck

WEBSTA, Instagram Downloader, picodash

socilab

PHOTO MAP

Snap Map

savefrom.net, Youtube DataViewer, frame by frame, storyful, Geo Search Tool

Scopedown

Dataminr, INTELTECHNIQUES, Echosec, War Wire

Messaging & closed groups

Sharing & Publishing

flickr, Pinterest, Google+

Blogging, Forums & other communities

STRAVA, WordPress.org, ProBoards, SQUARESPACE, tumblr., Blogger, Joomla!, LIVEJOURNAL, WIX.com, ghost, classmates, Medium, weebly

Internet Search

Google, Yandex, Bing, WayBackMachine, DuckDuckGo, NAVER, Baidu 百度, goo, 搜狗搜索, Рамблер/, kakao, YAHOO!, archive.today, PimEyes

Geospatial Data

GeoNames, Free GIS Data, SECRETS OF THE WEST, OpenRailwayMap, MAPS.ME, Mapillary, wikimapia, Google Maps, Bing maps, Maps, here, Yandex

Satellite Imagery

Google Earth, Descartes Labs, HARRIS, NOAA, TERRA server, USGS EarthExplorer, EARTHDATA, AIRBUS GeoStore, esa copernicus, esa, Zoom Earth, planet, DigitalGlobe, unitar, Radiant.Earth, SENTINEL

Maritime Movements

MarineTraffic, VesselFinder, OpenSeaMap, Shipfinder, SHIPAIS, IHS Markit, AISLive, AISHub, ShippingExplorer, Lloyd's List Intelligence, shipfinder, BoatNerd, SHIPSPOTTING.com, AirDecoder

COAA

Aviation Movements

AirNav RadarBox, LiveATC.net, flightradar24, ADS-B Exchange, GVA Dictator Alert, FlightAware, PLANESPOTTERS.NET

Radio

RadioReference, Broadcastify, Radio Garden, SDR, ProScan, MilScanners

Webcams

pentopia, Insecam, SHODAN, EarthCam, Webcams.travel, PICTIMO, wetter.com, lookr, wisuki

Image / Vid / Doc Forensics

GET-METADATA, Jeffrey's Image Metadata, metapicz, FotoForensics, Forensically, IRFANVIEW, hatlord / Spiderpig, exifdata, ExifTool, InVID

Commercial Registries

opencorporates, infobel, ICIJ OFFSHORE LEAKS DATABASE, Investigative Dashboard Search, european e-justice

This landscape shows data sources (mostly platforms, tools or apps) that provide publicly available data which may be of use in OSINT. Some tools may charge for data access. It is intended to be extensive, but not exhaustive, and may be updated periodically.

Authors:

H I Sutton, (@CovertShores) Covert Shores and Jane's contributor.

Allaume Leroy, (@Yaolt) Bellingcat & BBC.

Tony Roper, (@Tool_M1127), planesandstuff, Jane's contributor