


NO  
FF  
ONE  
2023

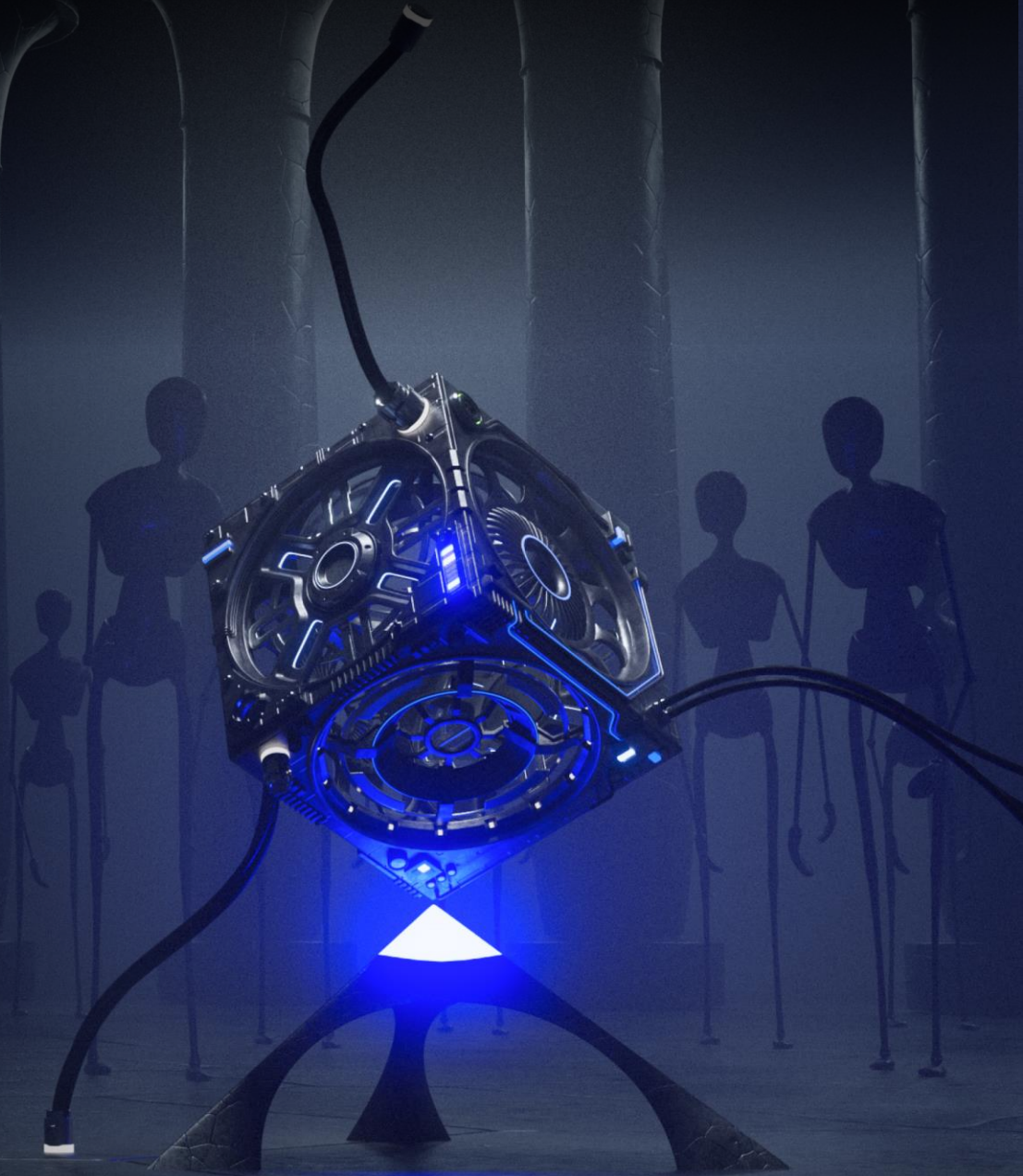


# bOSINTus

Speaker: Alexander Goncharov

Penetration Tester, Innostage

 @Adkkkkkkkk



# whoami



- PHDays, OffZone, Codeby, KazHackStan  
OSINT mindset
- OSINT specialist
- CTF enjoyer
- sOSINTer



# Agenda

## > Preparations

## > OSINT

- Basic
- Features
- Cases

## > GEOINT

- Basic
- Features
- Cases

## > Kid's level

## > Useful links

## > Practice Time



# OSINT

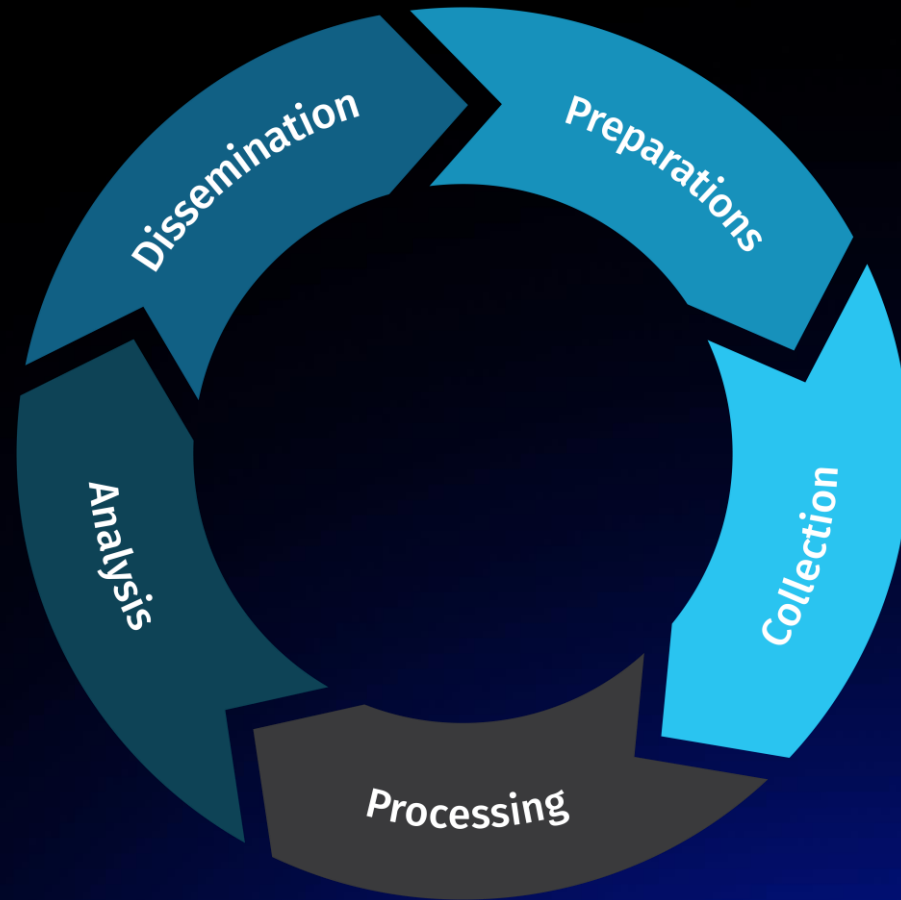
**OSINT** is a category of challenges in CTF events that involve gathering information from publicly available sources on the internet to solve specific tasks.

How many years have you been in OSINT?

- 4 year
- It must be a very cool feeling to look for people, companies, places, links every day



# Are you sure it's CTF?

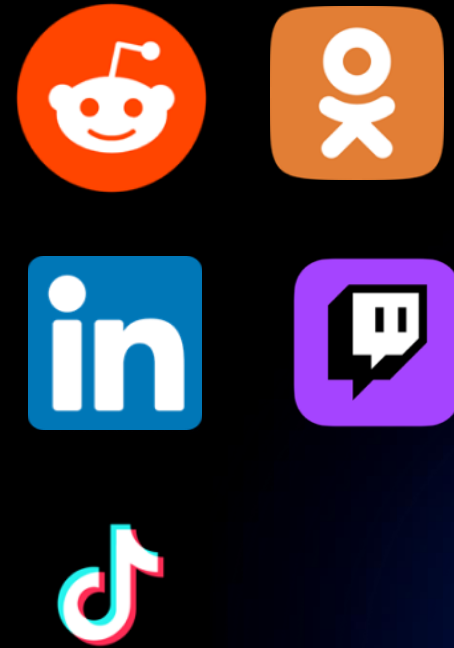


# The Many-Faced



# Social Links

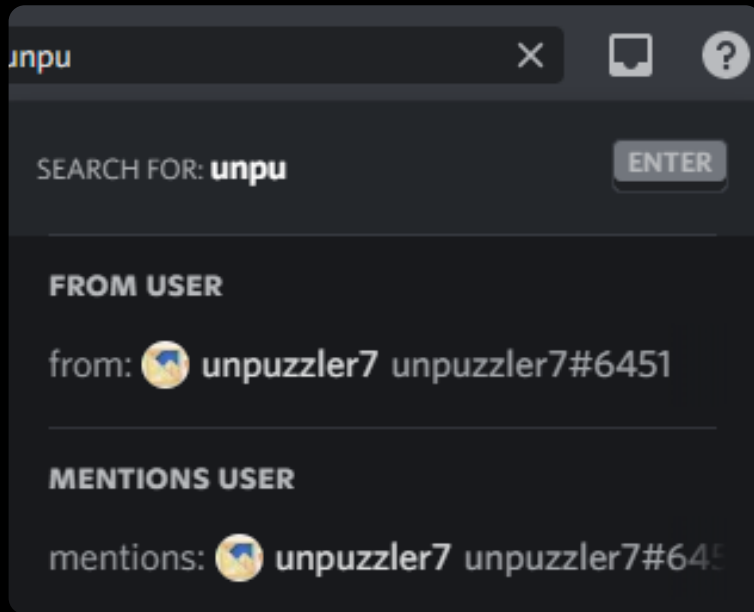
Must have



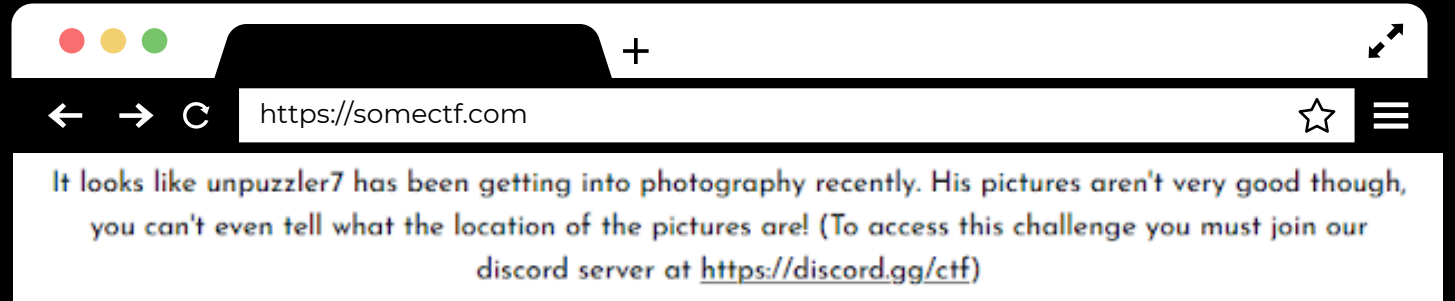
Optional



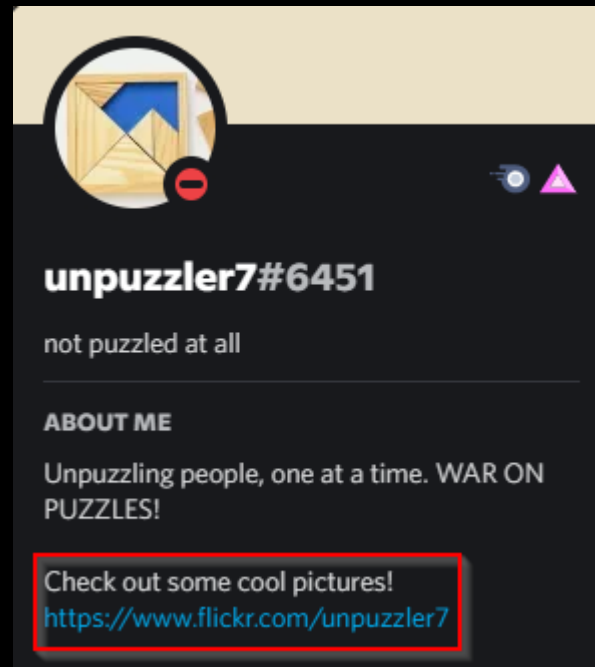
# I'm fast as f\*ck boi



Discord search interface showing results for 'unpu'. The search bar contains 'unpu' and an 'ENTER' button. Below the search bar, there are two sections: 'FROM USER' and 'MENTIONS USER'. Both sections list 'unpuzzler7 unpuzzler7#6451' with a user profile icon.



Web browser screenshot showing the URL 'https://somectf.com'. The page content reads: 'It looks like unpuzzler7 has been getting into photography recently. His pictures aren't very good though, you can't even tell what the location of the pictures are! (To access this challenge you must join our discord server at <https://discord.gg/ctf>)'



Discord user profile for 'unpuzzler7#6451'. The profile picture shows a puzzle box with a blue arrow. The bio reads: 'not puzzled at all'. The 'ABOUT ME' section contains the text: 'Unpuzzling people, one at a time. WAR ON PUZZLES!'. A red box highlights a message: 'Check out some cool pictures! <https://www.flickr.com/unpuzzler7>'.



# Discord OSINT



- Tools for searching groups, messages
- Tools for searching bots
- Tools for searching for users and information about them
- Discord OSINT attack surface
- Discord Dorks



A screenshot of a web browser displaying the GitHub repository page for 'wddadk/Discord-OSINT'. The browser's address bar shows the URL 'https://github.com/wddadk/Discord-OSINT'. The repository page includes a header with the repository name 'Discord-OSINT' and 'Private' status, along with 'Unwatch 1', 'Fork 0', and 'Star 0' buttons. Below the header, there are navigation options for 'main', '1 branch', and '0 tags', and buttons for 'Go to file', 'Add file', and 'Code'. The main content area shows a commit history table with columns for user, file name, and time. The commit 'wddadk Update README.md' is highlighted. Below the commit history, the 'README.md' file is open, showing the title 'Discord OSINT' and a description: 'OSINT Discord resources that may be useful for searching or pivoting on Discord.' A 'Table of Contents' section lists four items: 'Tools for searching groups, messages', 'Tools for searching bots', 'Tools for searching for users and information about them', and 'Discord OSINT attack surface'. The right sidebar contains 'About' information, 'Releases', and 'Packages' sections.

# Nickname search

## 1. Maigret

Collect a dossier on a person by username from thousands of sites

## 2. Sherlock

Hunt down social media accounts by username across social networks (EU based)



## 3. Snoop

Инструмент разведки на основе открытых данных (RU based)

## 4. Social-analyzer

API, CLI, and Web App for analyzing and finding a person's profile in 1000 social media \ websites



# Email search

## 1. Mailcat

Find existing email addresses by nickname using API/SMTP checking methods without user notification.

## 2. socialscan

Python library for accurately querying username and email usage on online platforms

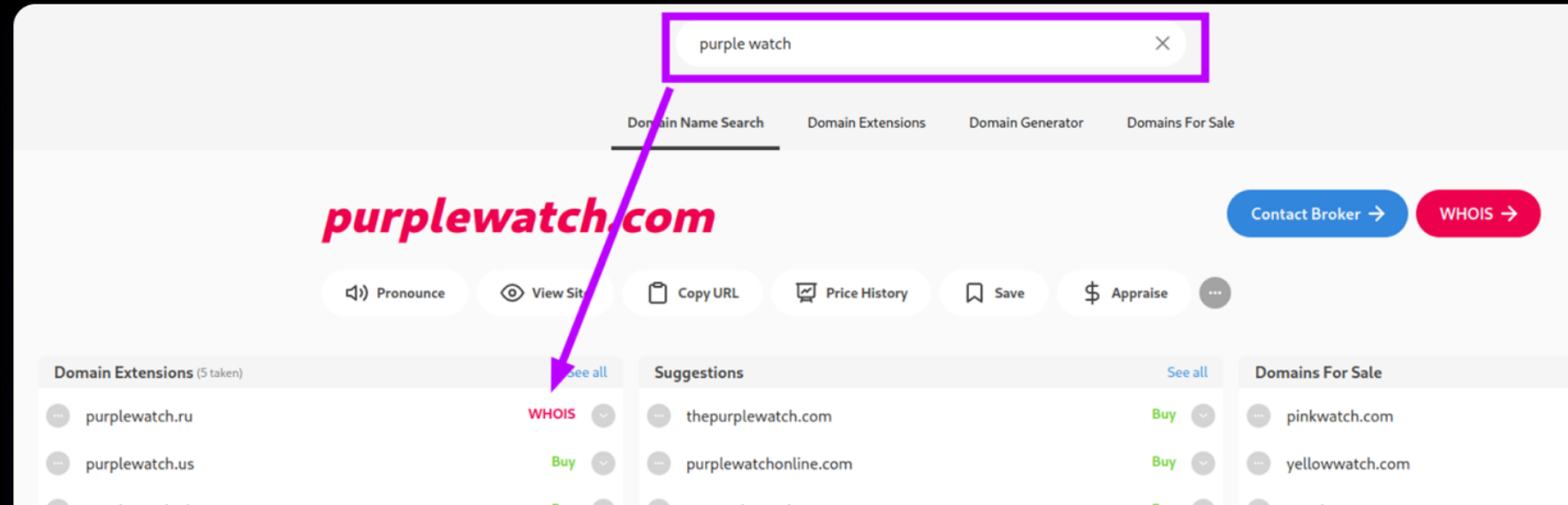
```
iojw@io-comp:socialscan$ socialscan username-2 email74@gmail.com
-----
                        username-2
-----
GitLab
Lastfm
Pastebin
GitHub
Reddit
Snapchat
Tumblr
Instagram: Usernames can only use letters, numbers, underscores and periods.
Twitter: Your username can only contain letters, numbers and '_'
-----
                        email74@gmail.com
-----
GitHub
Lastfm
Pastebin
Pinterest
Instagram
Spotify
Tumblr
Twitter
```

# Case #1



**Purple Watch has published a press release on its website,  
find it!**

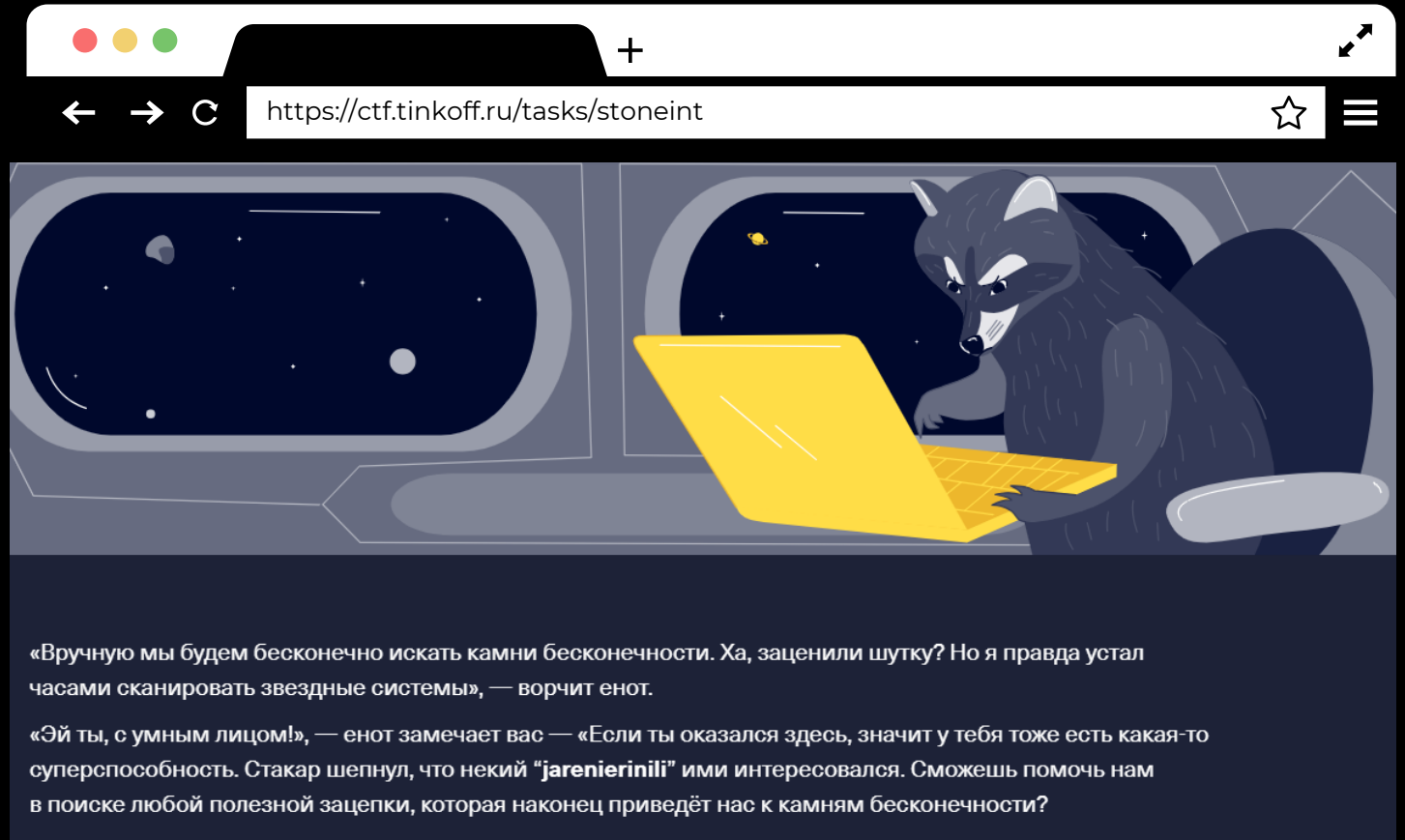
# Case #1



- Instant Domain Checker
- Domain Generator
- Domains For Sale
- Search All Domain Extensions

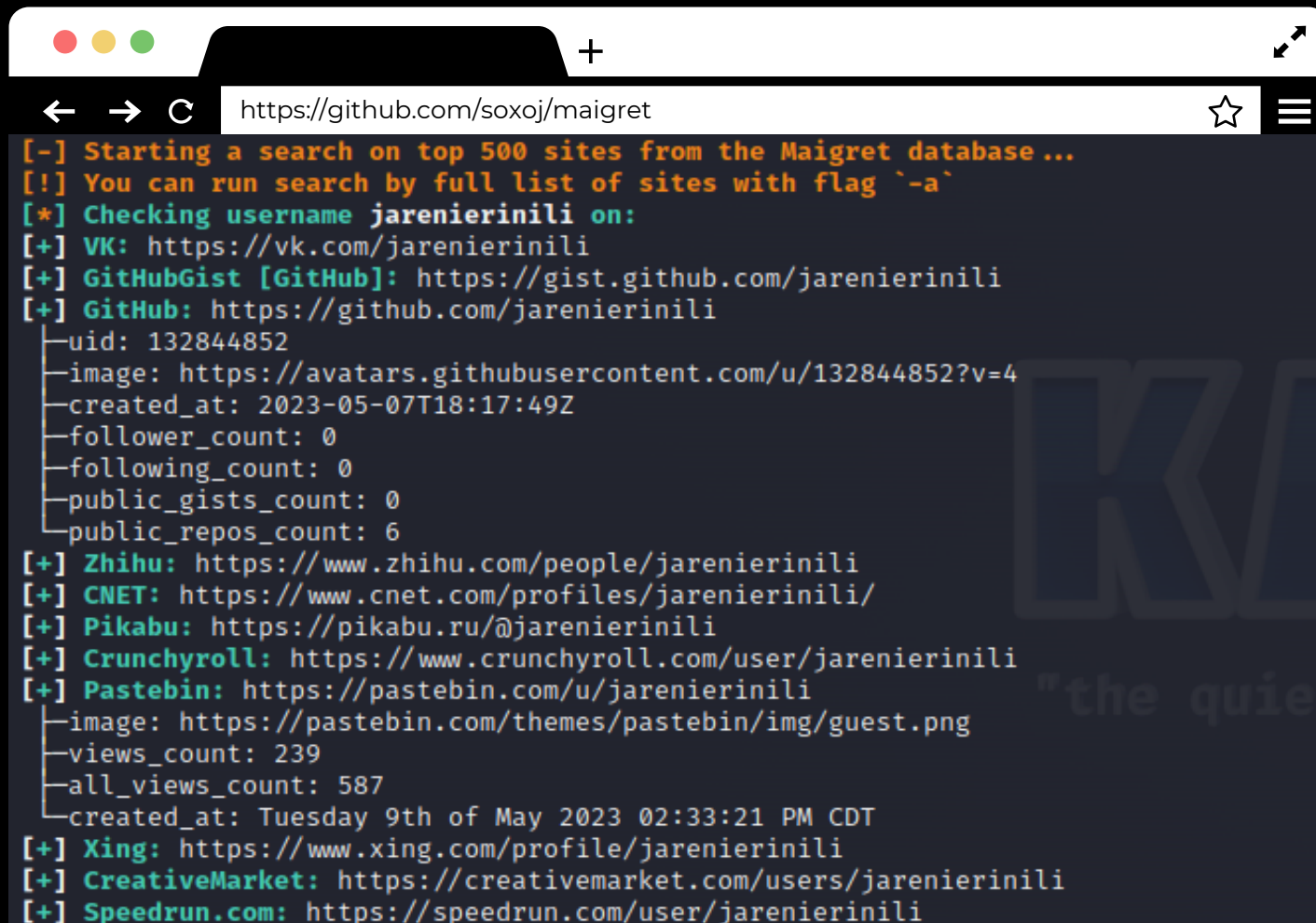
# Case #2

- Some «Jarenierinili»
- Can you help us with any leads?



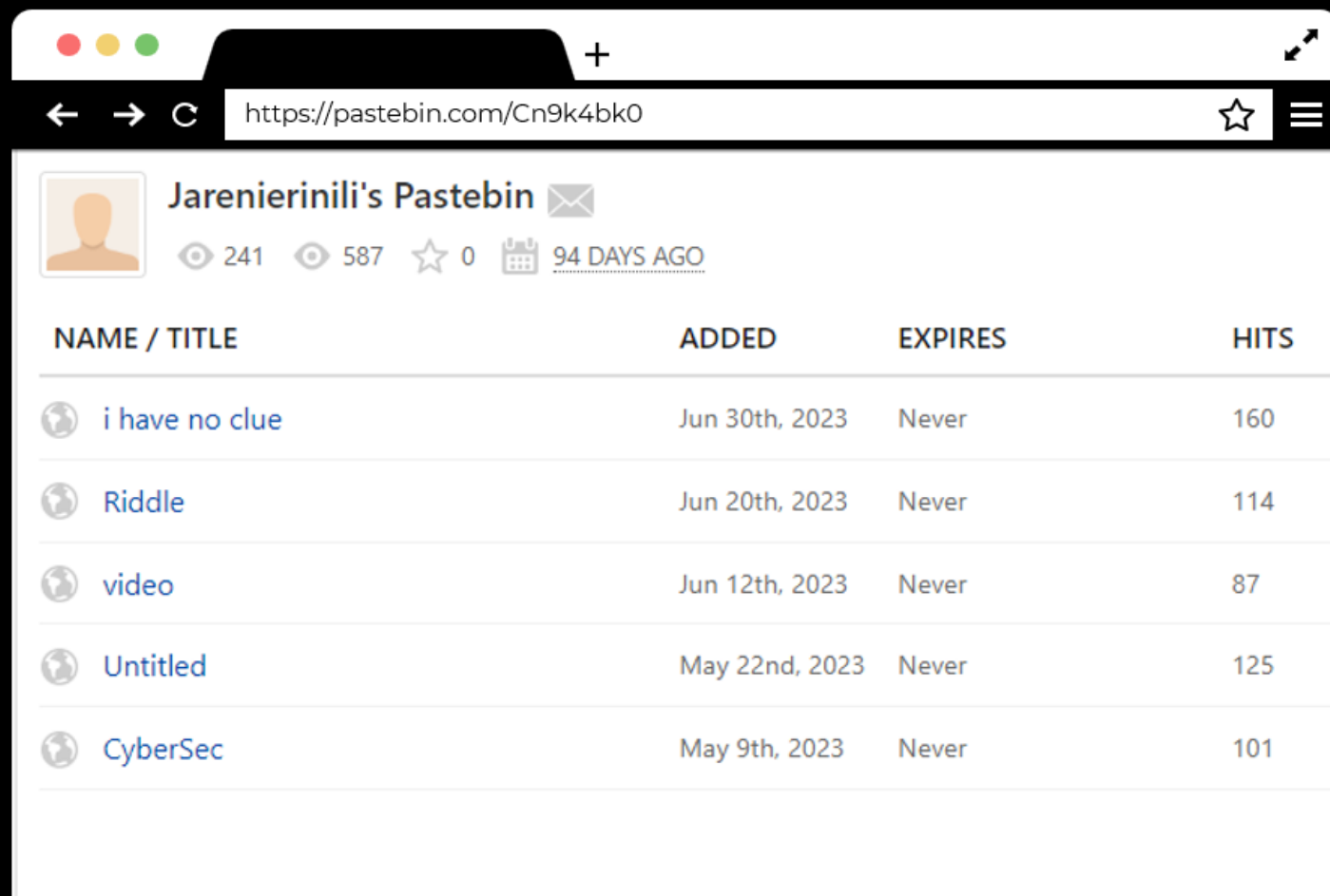
# Case #2 – Username search

- VK
- GitHub
- Zhihu
- Pikabu
- Crunchyroll
- Pastebin
- Xing
- CreativeMarket
- Speedrun.com



```
[-] Starting a search on top 500 sites from the Maigret database ...
[!] You can run search by full list of sites with flag `-a`
[*] Checking username jarenierinili on:
[+] VK: https://vk.com/jarenierinili
[+] GitHubGist [GitHub]: https://gist.github.com/jarenierinili
[+] GitHub: https://github.com/jarenierinili
  |uid: 132844852
  |image: https://avatars.githubusercontent.com/u/132844852?v=4
  |created_at: 2023-05-07T18:17:49Z
  |follower_count: 0
  |following_count: 0
  |public_gists_count: 0
  |public_repos_count: 6
[+] Zhihu: https://www.zhihu.com/people/jarenierinili
[+] CNET: https://www.cnet.com/profiles/jarenierinili/
[+] Pikabu: https://pikabu.ru/@jarenierinili
[+] Crunchyroll: https://www.crunchyroll.com/user/jarenierinili
[+] Pastebin: https://pastebin.com/u/jarenierinili
  |image: https://pastebin.com/themes/pastebin/img/guest.png
  |views_count: 239
  |all_views_count: 587
  |created_at: Tuesday 9th of May 2023 02:33:21 PM CDT
[+] Xing: https://www.xing.com/profile/jarenierinili
[+] CreativeMarket: https://creativemarket.com/users/jarenierinili
[+] Speedrun.com: https://speedrun.com/user/jarenierinili
```

# Case #2 – Honeytrap #1

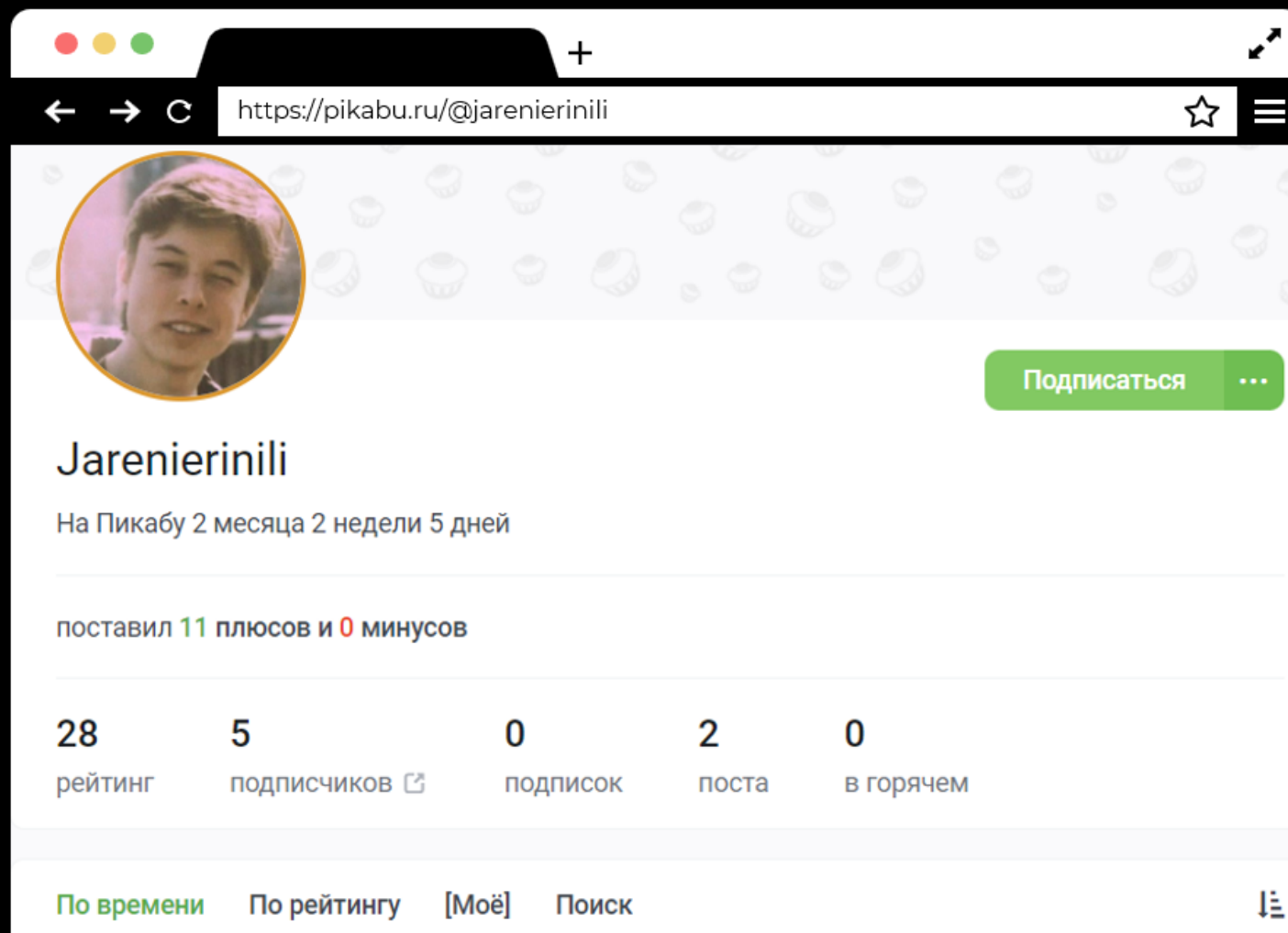


The screenshot shows a web browser window with the address bar displaying `https://pastebin.com/Cn9k4bk0`. The page content includes a user profile for 'Jarenierinili's Pastebin' with a profile picture, 241 views, 587 hits, 0 stars, and a post date of 94 days ago. Below the profile is a table listing pasted items.

NAME / TITLE	ADDED	EXPIRES	HITS
<a href="#">i have no clue</a>	Jun 30th, 2023	Never	160
<a href="#">Riddle</a>	Jun 20th, 2023	Never	114
<a href="#">video</a>	Jun 12th, 2023	Never	87
<a href="#">Untitled</a>	May 22nd, 2023	Never	125
<a href="#">CyberSec</a>	May 9th, 2023	Never	101



# Case #2 – Honeypot #2



The screenshot shows a web browser window with the address bar containing `https://pikabu.ru/@jarenierinili`. The page displays the profile of a user named "Jarenierinili". The profile includes a circular profile picture of a young man, a green "Подписаться" (Subscribe) button, and a menu icon. Below the name, it states "На Пикабу 2 месяца 2 недели 5 дней" (On Pikabu 2 months 2 weeks 5 days). The user has "поставил 11 плюсов и 0 минусов" (set 11 pluses and 0 minuses). A statistics row shows: 28 рейтинг (rating), 5 подписчиков (followers), 0 подписок (subscriptions), 2 поста (posts), and 0 в горячем (in hot). At the bottom, there are sorting options: "По времени" (selected), "По рейтингу", "[Моё]", and "Поиск".

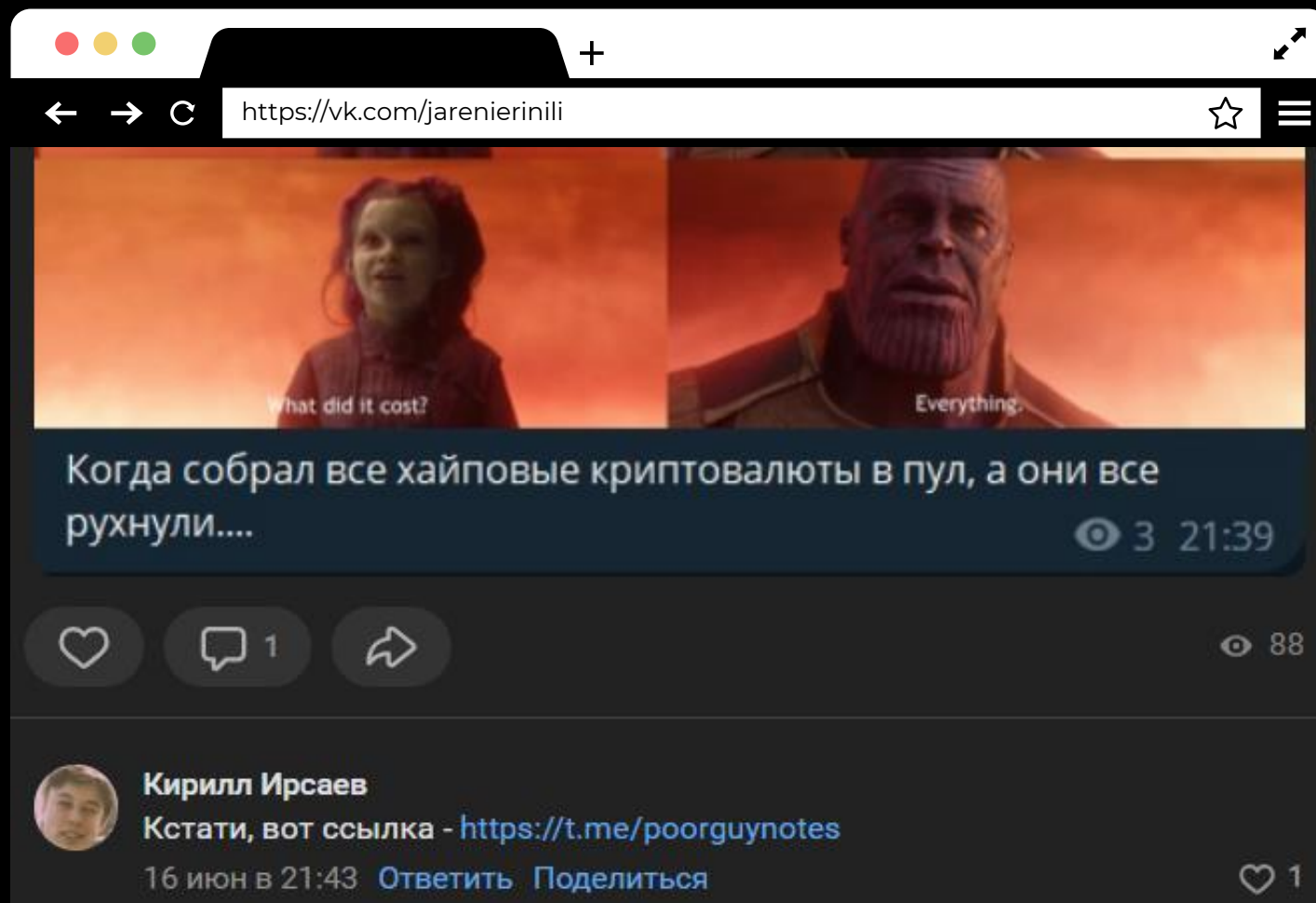
Метрика	Значение
Рейтинг	28
Подписчиков	5
Подписок	0
Постов	2
В горячем	0

# Case #2

- Personal account/blog

## Interest:

- Movies
- Cryptocurrencies
- IT

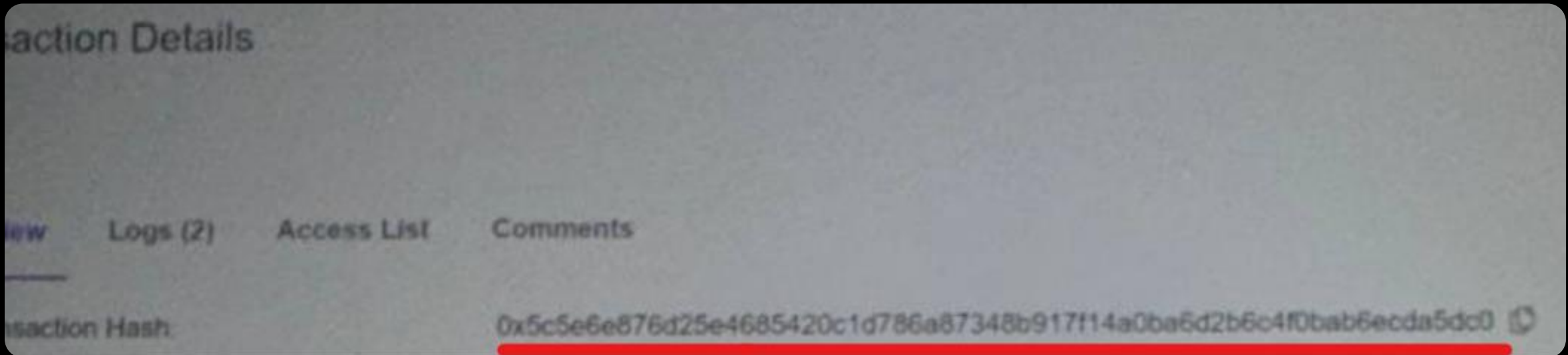


## Case #2

- TG blog is filled with a variety of content
- Significant part about cryptocurrencies
- An unremarkable photo of a Red Bull?



# Case #2 – Transaction analysis



- An unremarkable photo of a Red Bull?

# Case #2 – Transaction analysis



- And that's where we start to unravel the tangle.

Transaction Details

Overview Logs (2) Access List Comments

Transaction Hash: 0x5c5e6e876d25e4685420c1d786a87348b917f14a0ba6d2b6c4f0bab6ecda5dc0

Status: Success

Block: 44727087 1484714 Block Confirmations

Timestamp: 37 days 12 hrs ago (Jul-05-2023 09:50:45 PM +UTC)

Sponsored:

From: 0x0b3202b6c03876a470106be1f02f719225e7334a








To: 0x79458ff3d6e9e382d10f414cfba943eef5f18943

Value: 104.340042852891345289 MATIC (\$70.98)

Transaction Fee: 0.002700405862938 MATIC (\$0.00)

# Case #2 – Transaction analysis

- After several hours of analyzing addresses, we find a wallet with "ERC-721 Token"

Transactions	Internal Txns	ERC-20 Token Txns	ERC-721 Token Txns	Analytics	Comments
📄 Latest 7 ERC-721 Token Transfer Events					
Txn Hash	Age	From	To		
 <a href="#">0x42159613f009d7b1e1...</a>	37 days 10 hrs ago	<a href="#">0x45f8fb39143c6657049...</a>	<a href="#">0x609762d9f6a50f33655...</a>	IN	
 <a href="#">0xe62614dc802292606f...</a>	37 days 10 hrs ago	<a href="#">0x45f8fb39143c6657049...</a>	<a href="#">0x609762d9f6a50f33655...</a>	IN	
 <a href="#">0x627ab9632d8ff759653...</a>	37 days 10 hrs ago	<a href="#">0x45f8fb39143c6657049...</a>	<a href="#">0x609762d9f6a50f33655...</a>	IN	
 <a href="#">0x82548c8aaa0d1d91fd...</a>	37 days 10 hrs ago	<a href="#">0x45f8fb39143c6657049...</a>	<a href="#">0x609762d9f6a50f33655...</a>	IN	
 <a href="#">0x4d7e7006e4d328c556...</a>	37 days 10 hrs ago	<a href="#">0x45f8fb39143c6657049...</a>	<a href="#">0x609762d9f6a50f33655...</a>	IN	
 <a href="#">0xc4d4c7c47b8b084991...</a>	37 days 10 hrs ago	<a href="#">0x45f8fb39143c6657049...</a>	<a href="#">0x609762d9f6a50f33655...</a>	IN	
 <a href="#">0xd0c7f9f9a3d7fab5137...</a>	37 days 10 hrs ago	<a href="#">0x45f8fb39143c6657049...</a>	<a href="#">0x609762d9f6a50f33655...</a>	IN	

# Case #2 – AI help



What is an ERC-721 token and what is it typically used for?



An ERC-721 token is a type of Ethereum-based cryptocurrency token standard that defines a non-fungible token (NFT). Unlike traditional cryptocurrencies like Bitcoin or Ethereum, where each token is identical and interchangeable, NFTs are unique and indivisible. Each ERC-721 token represents a distinct digital asset or item, making them ideal for representing ownership of digital or physical assets that are one-of-a-kind or limited in supply.



ChatGPT



# Case #2 – Victory



Rarible Singles

## The Infinity Gauntlet

Creator  
Name

Current owner  
0x60976...dd...

0 Share Refresh ...

Price  
Not for sale

There are no bids yet. Be the first!

Place a bid

<https://rarible.com/user/0x609762d9f6a50f336554f24ffe98a7c47393dde8/owned>



# Case #3

About



No description, website, or topics provided.

From the owner

"The Wyatt P. Memorial water tower was established as a tribute to a man that has contributed a great deal to the Genesee County community. Well known for his high energy, love for adventure and passion for boats. He was a phenomenal athlete at Carman-Ainsworth High School and was a role model of service to many students and staff members. Though now you may not know where he is, we forever remember him when we view the engineering marvel that is the Wyatt P. Memorial water tower. byuctf{h0w\_d1d\_1\_st34l\_4\_w4t3r\_t0w3r}



3 Photos



blackhat\_abhinav

Follow



10 posts

61 followers

99 following

Abhinav

Discord - noob\_abhinav#4962

Searching myself in the foggy world.

Αμπινάβ Κουμάρ

Secret:- <https://goo.gl/maps/gHbUHjqFyNcB7aqi9>

[abhinav.abhinavkumar65.repl.co](https://repl.co/abhinav.abhinavkumar65)

ctf{5f4d-cc3b5aa765d6-1d8327deb882-cf99} >

ГЛАВНАЯ

ВИДЕО

ТРАНСЛЯЦИИ

ПЛЕЙ

Описание

ctf{5f4d-cc3b5aa765d6-1d8327deb882-cf99}

Дополнительно

Страна: Россия

# Twitter Tips

from:

@NASA

to:

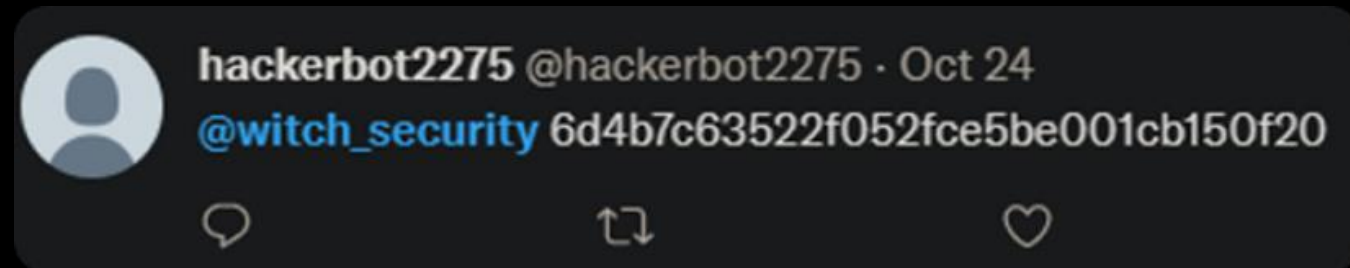
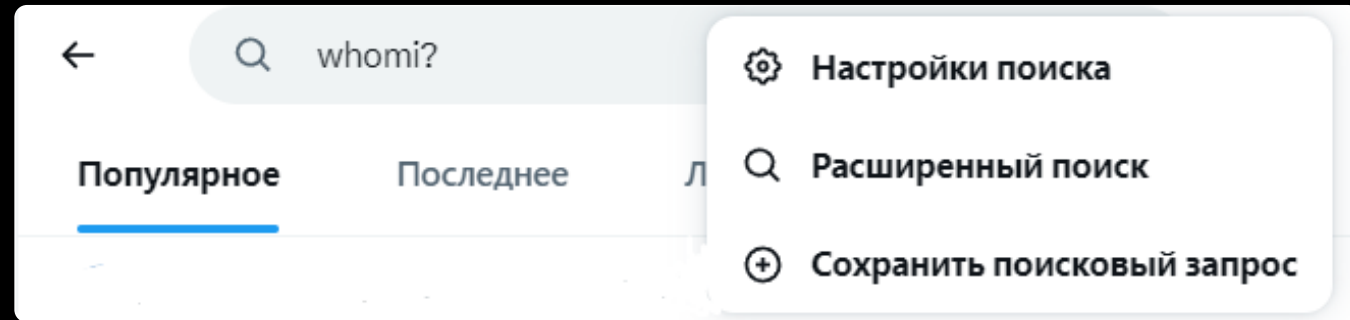
Codeby OR CyberSec

since:2022-02-24

Codeby-CyberSec

until:2022-02-24


lang:fr



# Twitter Tips – Image description

Abhinav KUMAR  
@Abhinav78082932

A nice place



ALT

**Image description**

[n00bz{gr0tt4\\_1sl4nd\\_1s4\\_n1c3\\_pl4c3\\_t0\\_v1st}](#)

Dismiss

Like

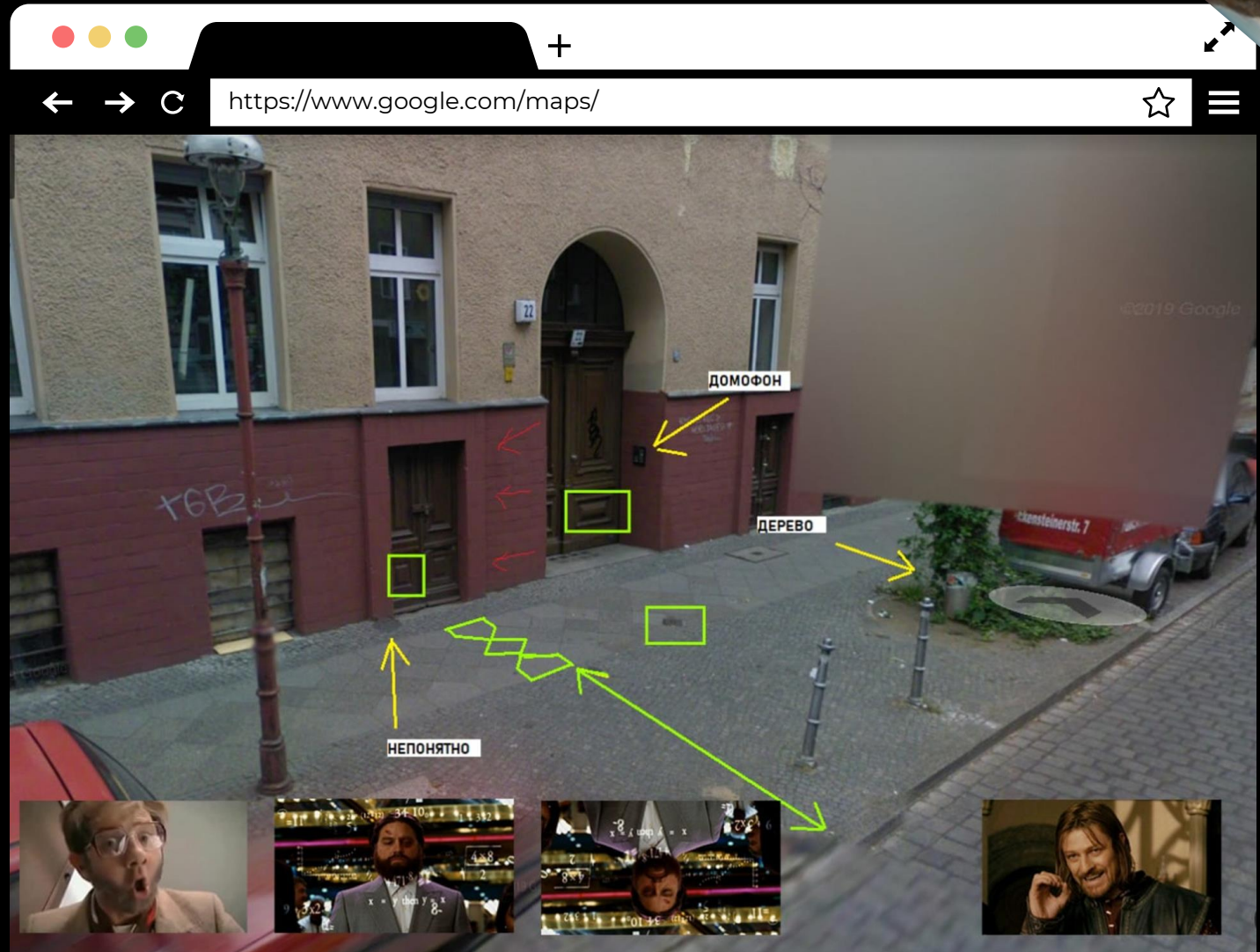
Bookmark

Share

Reply

# GEOINT

**GEOINT** stands for Geospatial Intelligence, which is a field of intelligence analysis that involves the collection, analysis, and visualization of geospatial data



# GEOINT - Reverse Image Search

Google Lens



Yandex Images

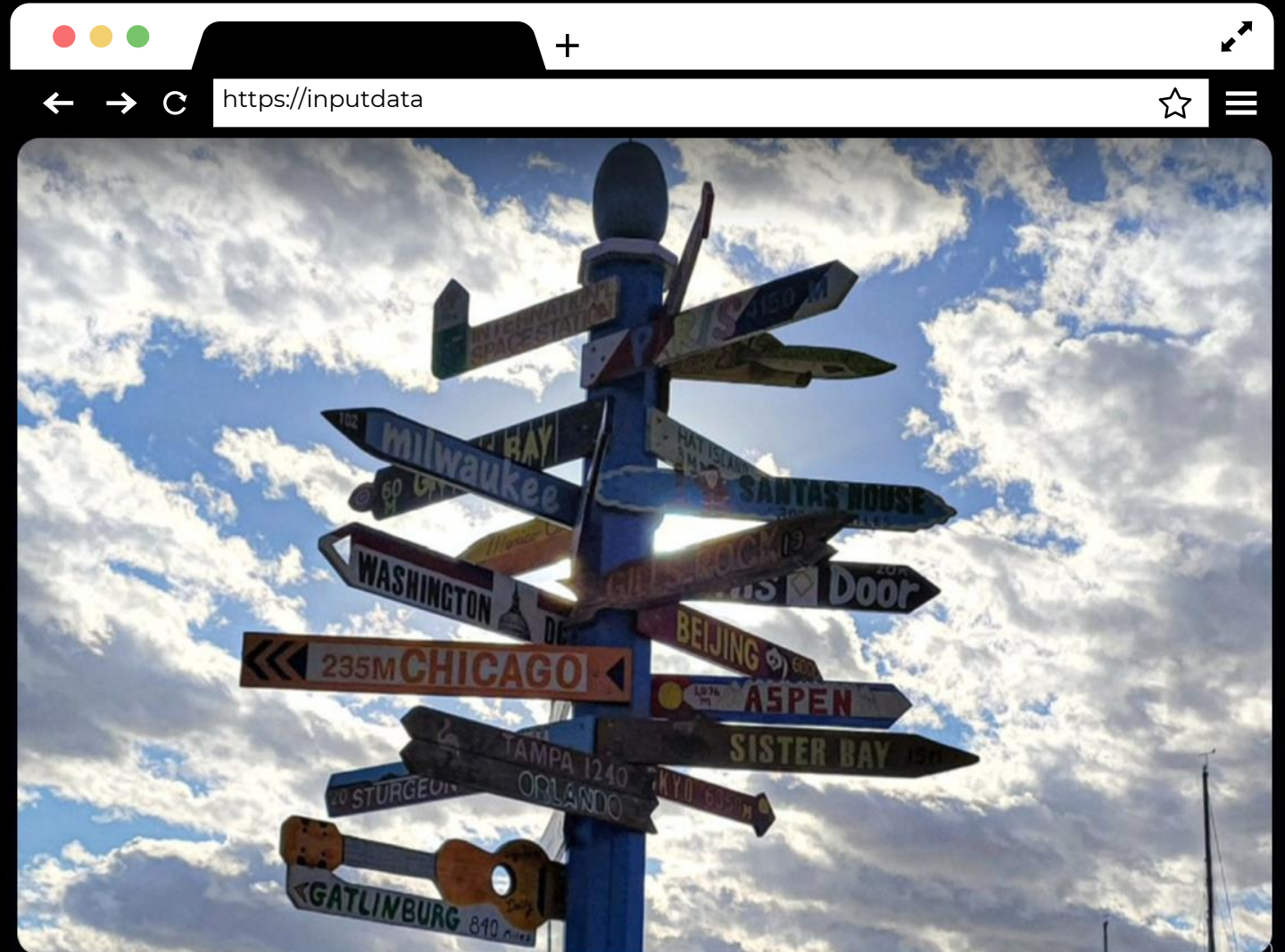


Bing



# Case #4

- Some signpost?
- We can take a look at the inscriptions? – Yes, but it's too hard, let's take the shortcut



# Case #4

← → ↻ yandex.ru/images/ ☆ ☰

Кажется, на изображении

указатель путешествий столб с указателями городов указатель направления traveler crossroads


Похожие изображения


Больше похожих


# Case #4


Browser address bar: <https://lens.google/>


### Visual matches


- 


istockphoto.com  
Multidirectional Sign For Globetrotters Stoc...
- 


cardboarddogcoac...  
Individual Transition, Discernment...
- 

istockphoto.com  
Road Signs Stock Photo - Download Image No...
- 

123rf.com  
Distance Marker And Sign Post To Major...
- 

dreamstime.com  
Direction To Different Places of the World...
- 

tripadvisor.com  
Fun sign at the Marina - Picture of Egg Harbor...
- 

shutterstock.com  
World Landmarks Signpost Containing...
- 

dreamstime.com  
Key west signpost stock photo. Image of...



# Case #5



## Visual matches



 [cbre.co.nz](https://www.cbre.co.nz)  
Office For Rent, 51  
Shortland Street,...

 [tripadvisor.com](https://www.tripadvisor.com)  
big screen with city  
buildings all around -...

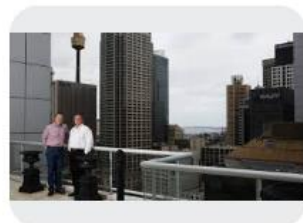
 [tripadvisor.com](https://www.tripadvisor.com)  
King Hilton Deluxe  
Room on the 33rd Flo...



 [interest.co.nz](https://www.interest.co.nz)  
Plenty of bidders at  
Auckland apartment...



 [tripadvisor.com.ph](https://www.tripadvisor.com.ph)  
CAPRI BY FRASER,  
BRISBANE - UPDATED...

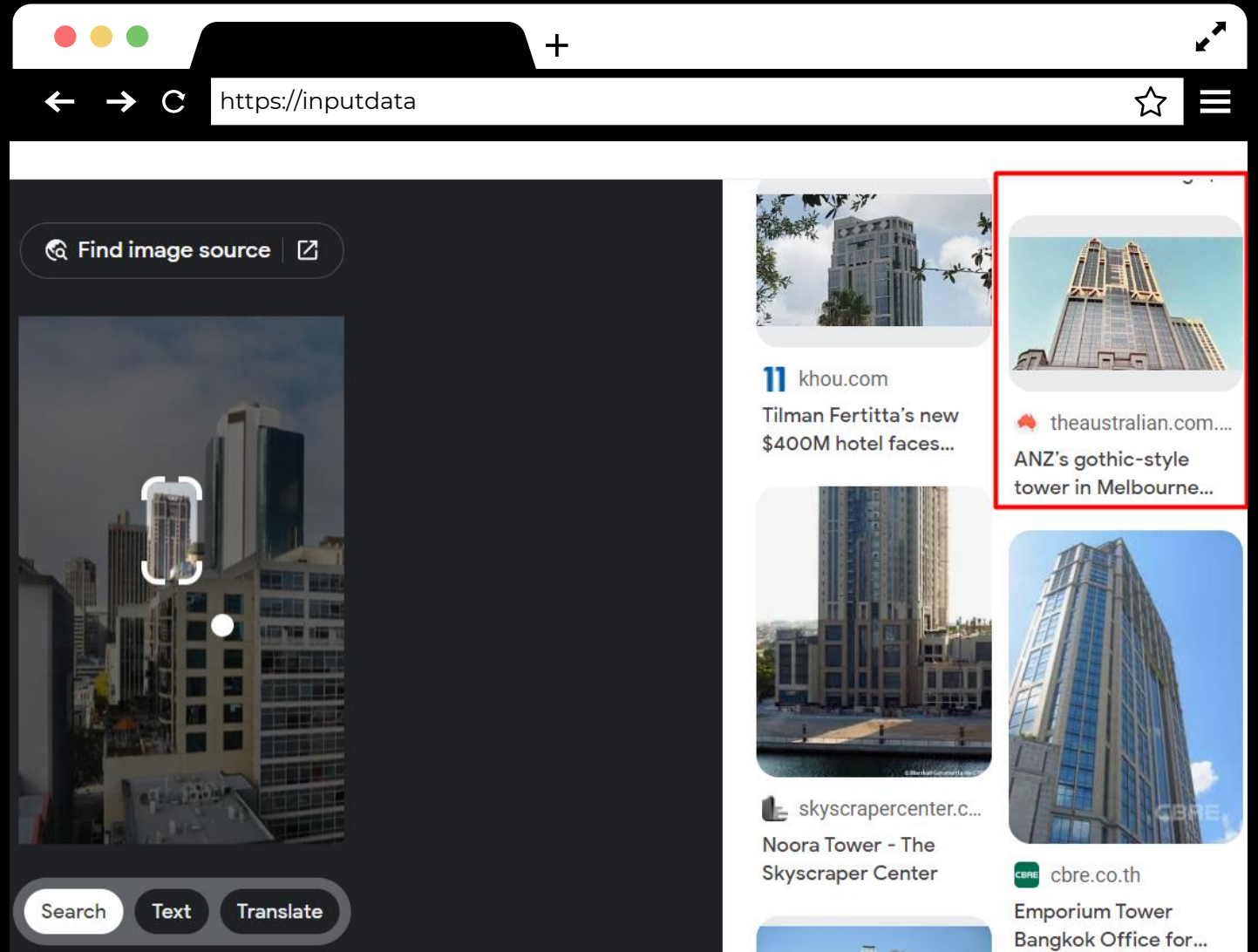


 [dailytelegraph.com...](https://www.dailytelegraph.com...)



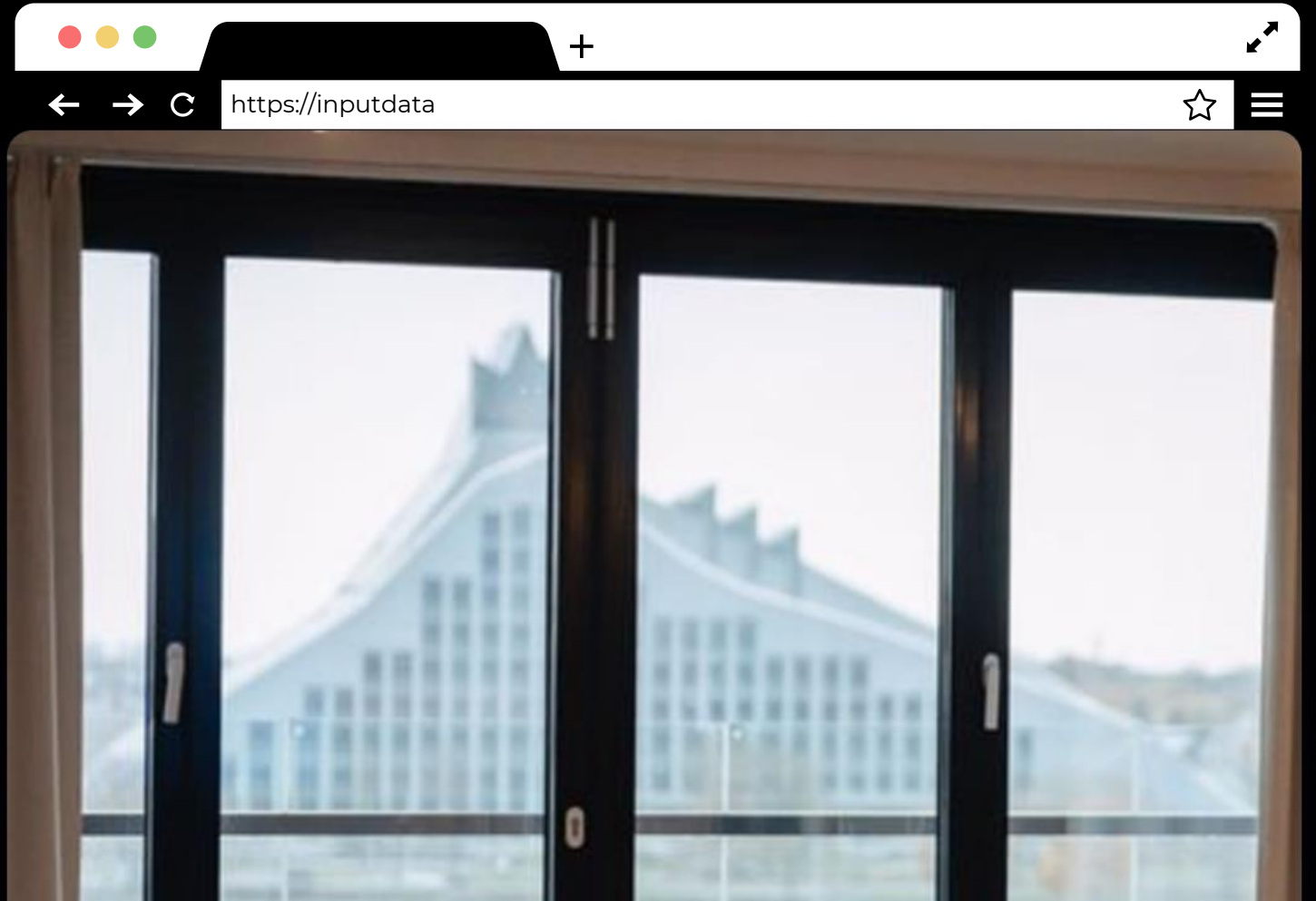
# Case #5

- By reducing the search area we increase the accuracy of the data output



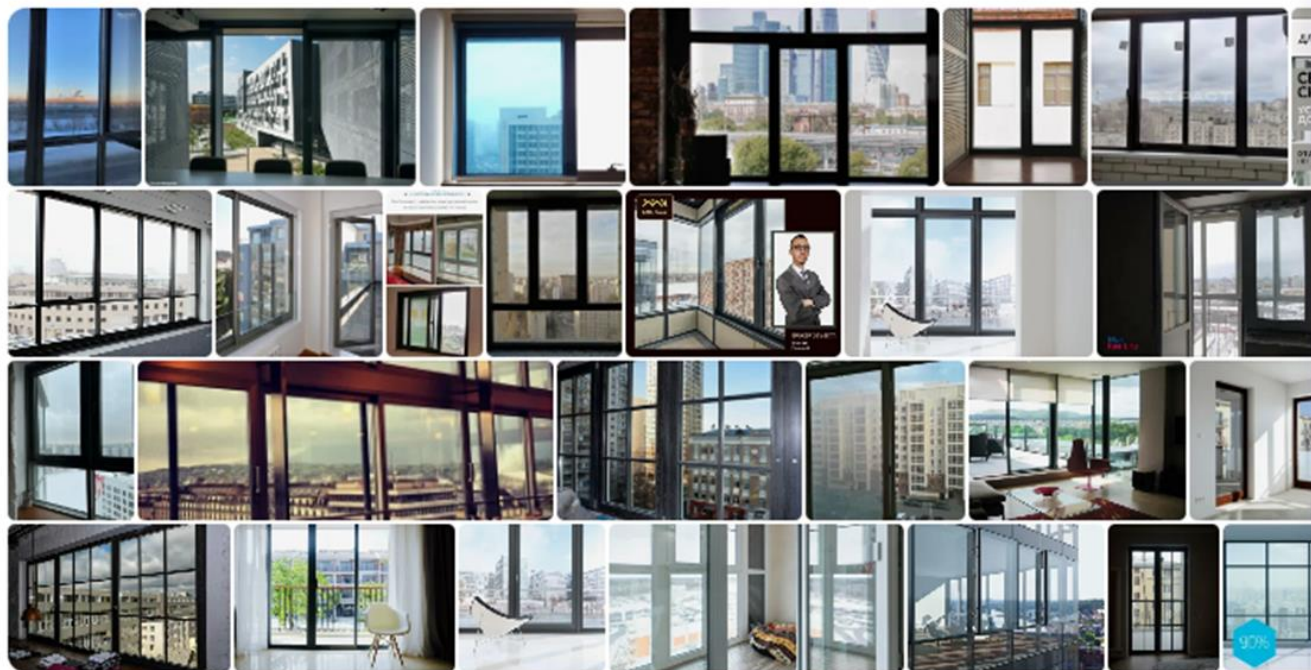
# Case #6

- Some building
- Google it?
- Metadata?















# Case #6 - :(

## Похожие изображения



Больше похожих

## Visual matches

 <p>thelocal.de Nearly 1,800 people turn up for single flat...</p>	 <p>pellaatlowes.com Pella Lifestyle Series Patio Doors   Pella At...</p>	 <p>brickvastgoed.nl De Plaetse, 5708 ZJ Helmond - Aanbod  ...</p>	 <p>gites.fr Absolute Waterfront - Tropical Aurora Top...</p>
 <p>futureglazewindow... Be bold with Bi-fold!   Futureglaze Windows...</p>	 <p>veka.de VEKA   Experience VEKA SPECTRAL</p>	 <p>wfmmedia.com Sudhakar Profile Systems: Delivering...</p>	 <p>vesternet.com Shelly Porta Finestra 2 - Vesternet</p>
 <p>alamy.com Mediterranean sea maritime scenic view...</p>	 <p>smartsystems.co.uk Alitherm Heritage</p>	 <p>pella.com Black Windows &amp; Patio Door Make Bold Desig...</p>	 <p>midlandaluminium</p>

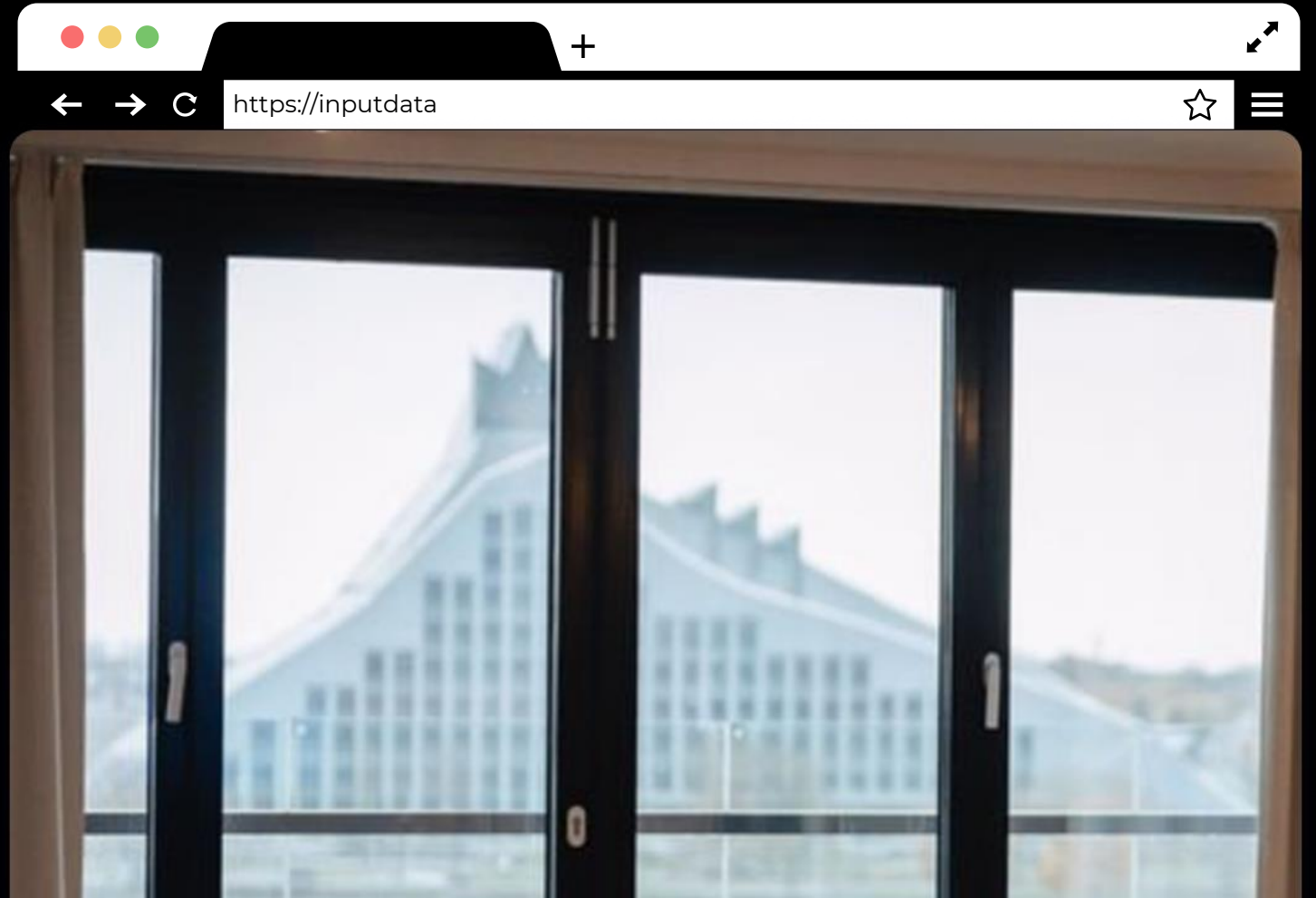
Did you find these results useful?

Yes No

# Case #6

## What to do???

- Google it?
- Metadata?
- Pray?



# Case #6 – cleanup.pictures



Caption

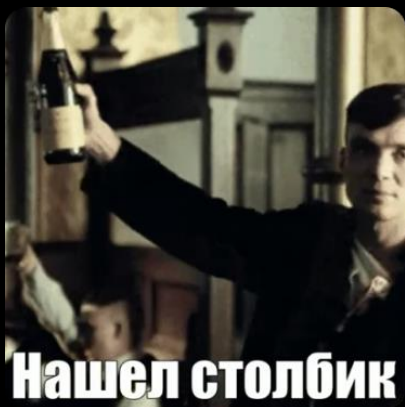
# Case #6 - Victory

The image shows a browser window with the URL `https://lens.google/`. Below the address bar, the heading "Visual matches" is displayed. Eight search results are shown in a grid, each featuring a thumbnail image of the National Library of Latvia and a text description below it.

Source	Thumbnail Description	Title
librarybuildings.eu	Daytime view of the library building across a river.	National Library of Latvia - LIBER...
alamy.com	Daytime view of the library building across a river.	National Library of Latvia in Riga, the...
aia.org	Nighttime view of the library building reflected in water.	National Library of Latvia - AIA
bnn-news.com	Daytime view of the library building across a river.	Latvia's National Library adopts new prices for...
arrivalguides.com	Aerial view of the library building and surrounding area.	Castle of Light —
fromplacetoplace.tr...	View of the library building in winter with snow on the ground.	Winter walk along the
archdaily.com	View of the library building from a distance.	The Architect as
form-five.com	View of the library building from a distance.	Latvia's Castle of Light I

# Case #7

- Pillar?



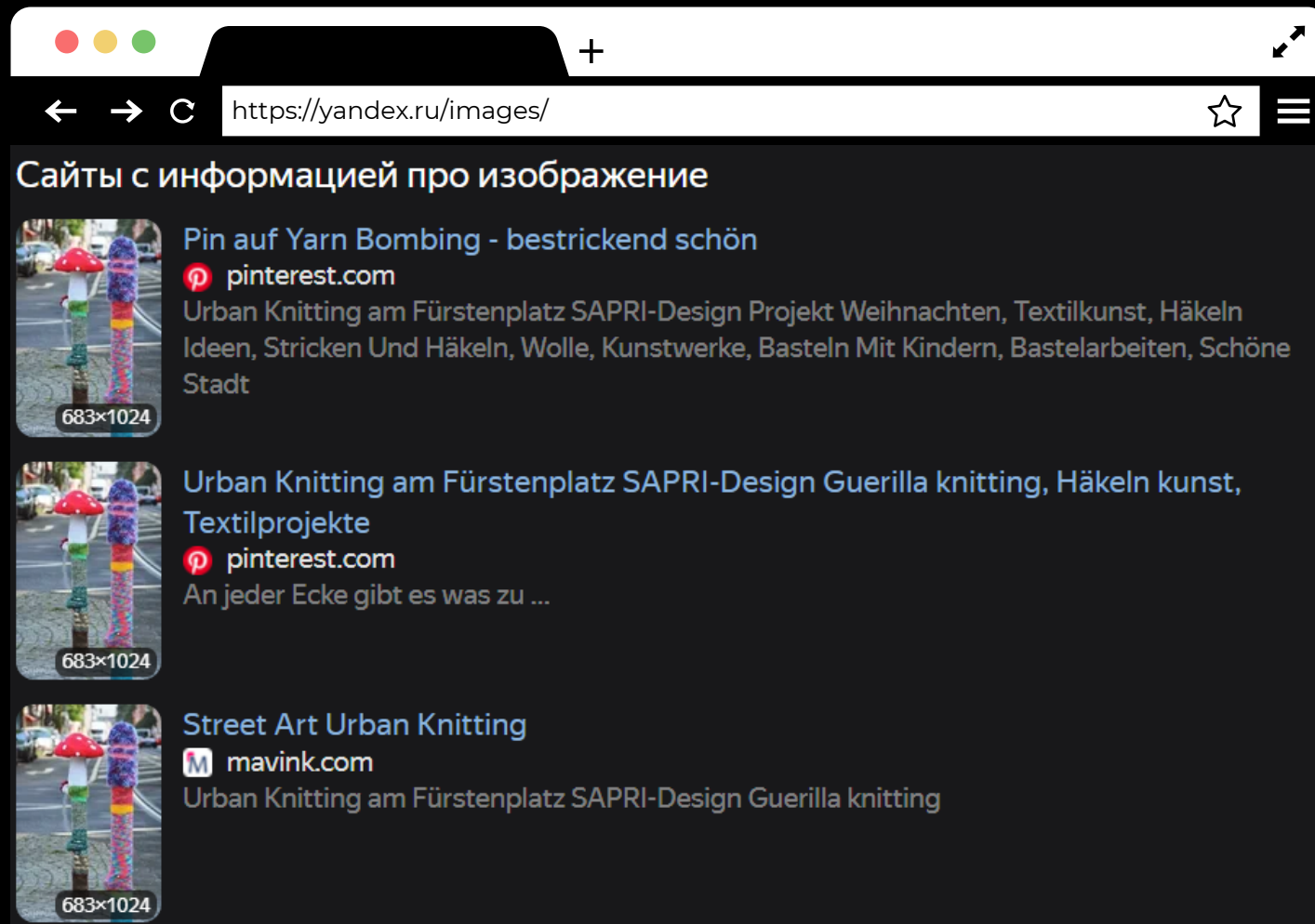
**Нашел столбик**





# Case #7

- Okay, it's probably Germany.



# Case #7 - Leaves

- Fine, it's Germany.

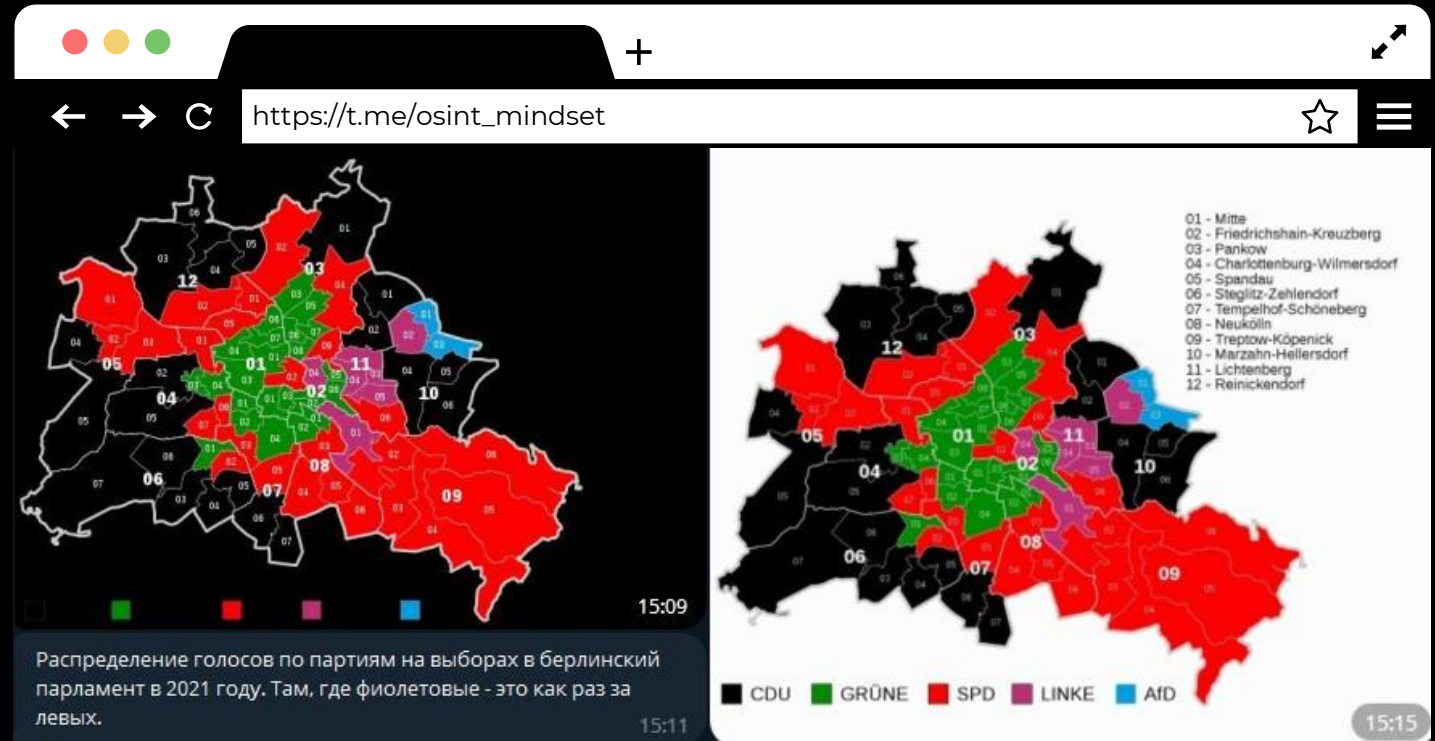
The screenshot shows a Telegram post from the user 'osint\_mindset'. On the left is a photograph of a street post covered in leaves, with several red circles highlighting specific leaf shapes. On the right is a reference chart titled 'HEIMISCHE BAUMBLÄTTER' (Native Tree Leaves) with a grid of 40 leaf silhouettes labeled with German tree names. A red box highlights the silhouettes for 'Hainbuche' and 'Traubeneiche'. To the right of the chart is another reference image titled 'British Tree Leaves' with various leaf photos. At the bottom of the post, there is Russian text: 'Листья больше похожи на немецкие (на второй фотке британские)' and a timestamp 'изменено 20:47'.

# Case #7 - Processing photos



# Case #7 – Thoughts

- Germany
- District with a high percentage of Turkish residents;
- District with the support of the Left Party.





# IP/Domain research



**1.**

Identification of the owner

**2.**

Analysis of archived DNS records

**3.**

Analysing whois / archived whois information

**4.**

Searching for subdomains

**5.**

Google dorks xd

# Website research at CTF



**1.**

Robots.txt

**2.**

Source code analysis

**3.**

Searching for domain links

**4.**

Searching for subdomains

**5.**

WebArchive

# IP/Domain research



**[github.com/jivoi/awesome-osint](https://github.com/jivoi/awesome-osint)**

1. Appropriate for more basic analysis
2. Contains a large number of different tools
3. Suitable for all OSINT specialists

**[github.com/wddadk/Offensive-OSINT-Tools](https://github.com/wddadk/Offensive-OSINT-Tools)**

1. Appropriate for more detailed IP/Domain analysis
2. Suitable for Offensive OSINT spec



# OSINT for countries

**Often CTF tasks are related to the host country and you don't know anything about it.**

- Australia
- UK
- China
- Hungary
- Canada
- Japan
- Korea
- Netherlands

*\* Other countries will be added later*



Caption

# OSINT CTF Tips



**1.**

Pay attention to the country in which the CTF is held. OSINT tasks may be indirectly related to the country

**2.**

Don't give up after two hours spent on google maps.

**3.**

As cliché as it sounds, but pay attention to details. The devil is in the details.

**4.**

Try Harder © whoamins

**5.**

Play CTF and read WriteUp :)

**6.**

Use google dorks xd

# Kid's level

## 1. Web archive

If you have a website/personal account, it is a good idea to check the WebArchive link

## 2. Metadata



## 3. Google Dorks



# Useful links



# Practice Time



## Resources for practicing OSINT

- [geoguessr.com](https://geoguessr.com)
- [twitter.com/quiztime](https://twitter.com/quiztime)
- OSINT: форум расследований
- [t.me/geoint](https://t.me/geoint)
- [t.me/GEOINT](https://t.me/GEOINT)
- [ctftime.org/event/list/upcoming](https://ctftime.org/event/list/upcoming) :)
- [codeby.games](https://codeby.games)

# Practice Time



## TryHackMe Rooms

- googledorking
- searchlightosint
- shodan
- geolocatingimages
- somesint
- Sakura
- redteamrecon

Questions?



**NO  
FF  
ONE  
2023**

 @adkkkkkkkkk