

Ethical hacking and Penetration Testing

Information gathering. Open source intelligence (OSINT)

Identifying the goals of lesson

- Understanding basic terms
- Understanding EXIF
- Practicing OSINT tools
- Practicing Maltego

Information gathering

- Active Reconnaissance – you connect to the objects of scope
- Passive Reconnaissance – you don't connect to the objects of scope

Active information gathering

- Nmap
- DNS enumeration
- SMB enumeration
- NFS enumeration and etc.

Passive information gathering

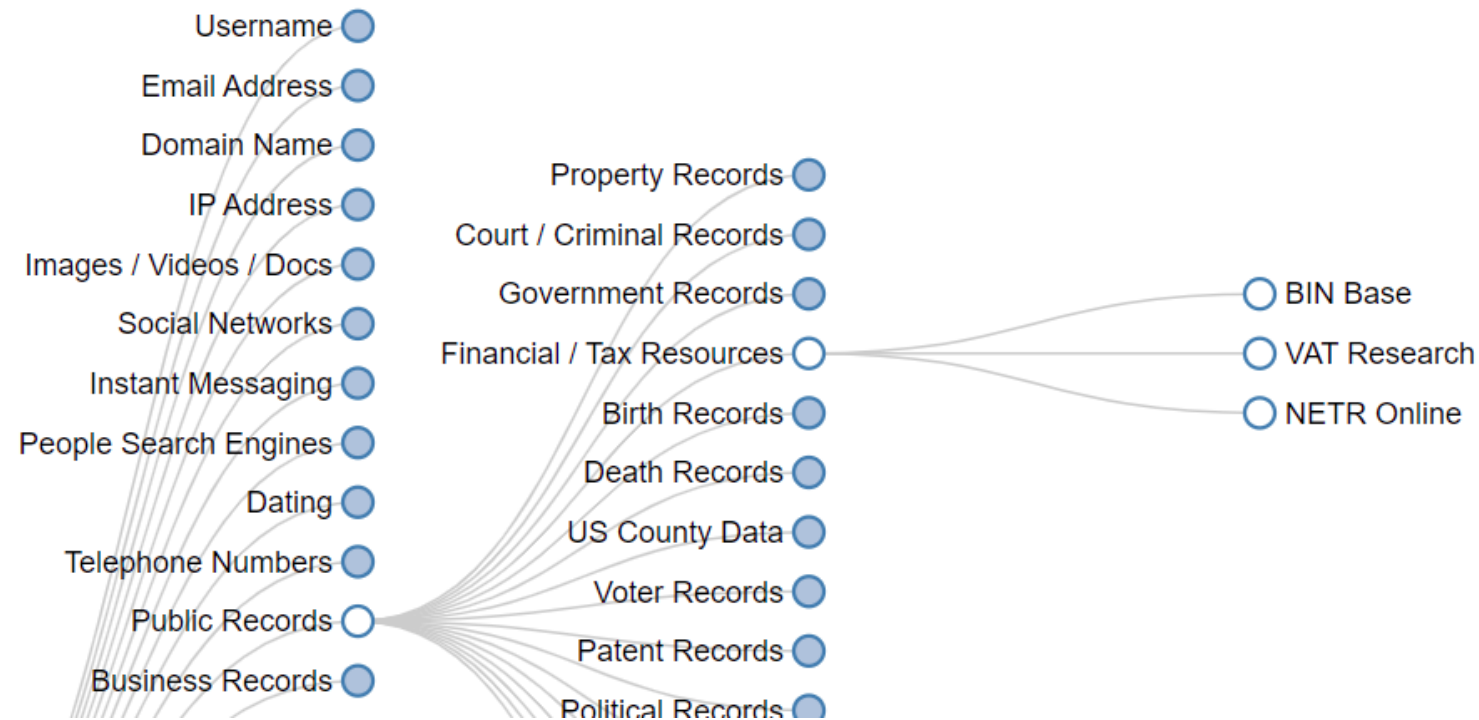
- OSINT
- Google Hacking
- Shodan.io, Censys.io
- Web.Archive.Org and etc.

What is OSINT?

- **Open-source intelligence (OSINT)** is a multi-factor (qualitative, quantitative) methodology for collecting, analyzing and making decisions about data accessible in publicly available sources to be used in an intelligence context.

OSINT Framework

- <https://osintframework.com/>



What is EXIF?

- **Exchangeable image file format (officially Exif, according to JEIDA/JEITA/CIPA specifications)** is a standard that specifies the formats for images, sound, and ancillary tags used by digital cameras (including smartphones), scanners and other systems handling image and sound files recorded by digital cameras.

ExifTool

- **ExifTool** is a customizable set of Perl modules plus a full-featured command-line application for reading and writing meta information
- <https://en.wikipedia.org/wiki/ExifTool>
- <https://github.com/exiftool/exiftool>



sebastienpage
Oceanside Pier >

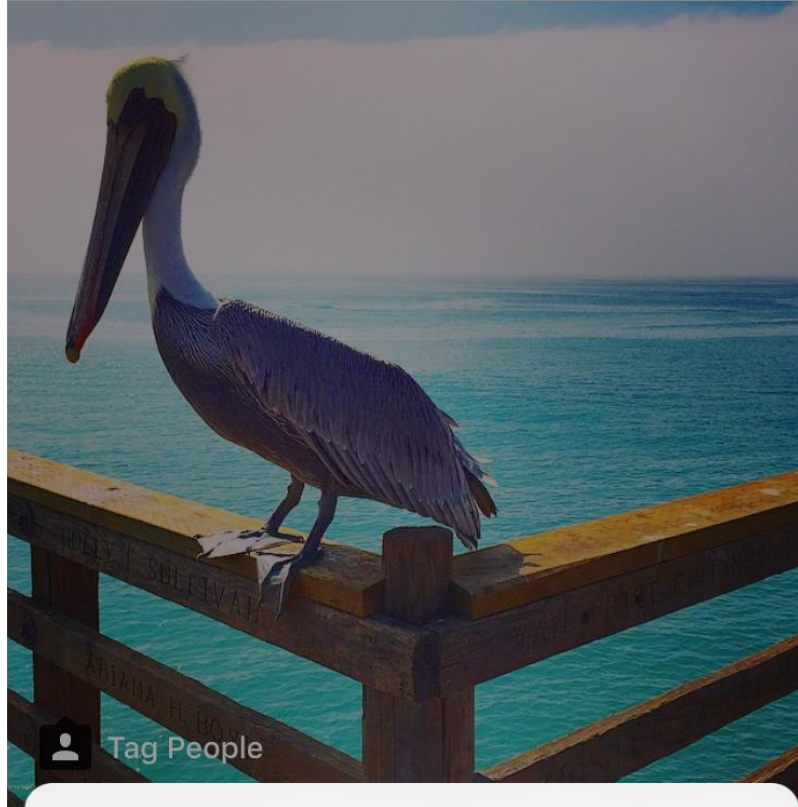


Tag People

The pelican brief



sebastienpage
Oceanside Pier >



Tag People


Remove Location

Change Location

Cancel

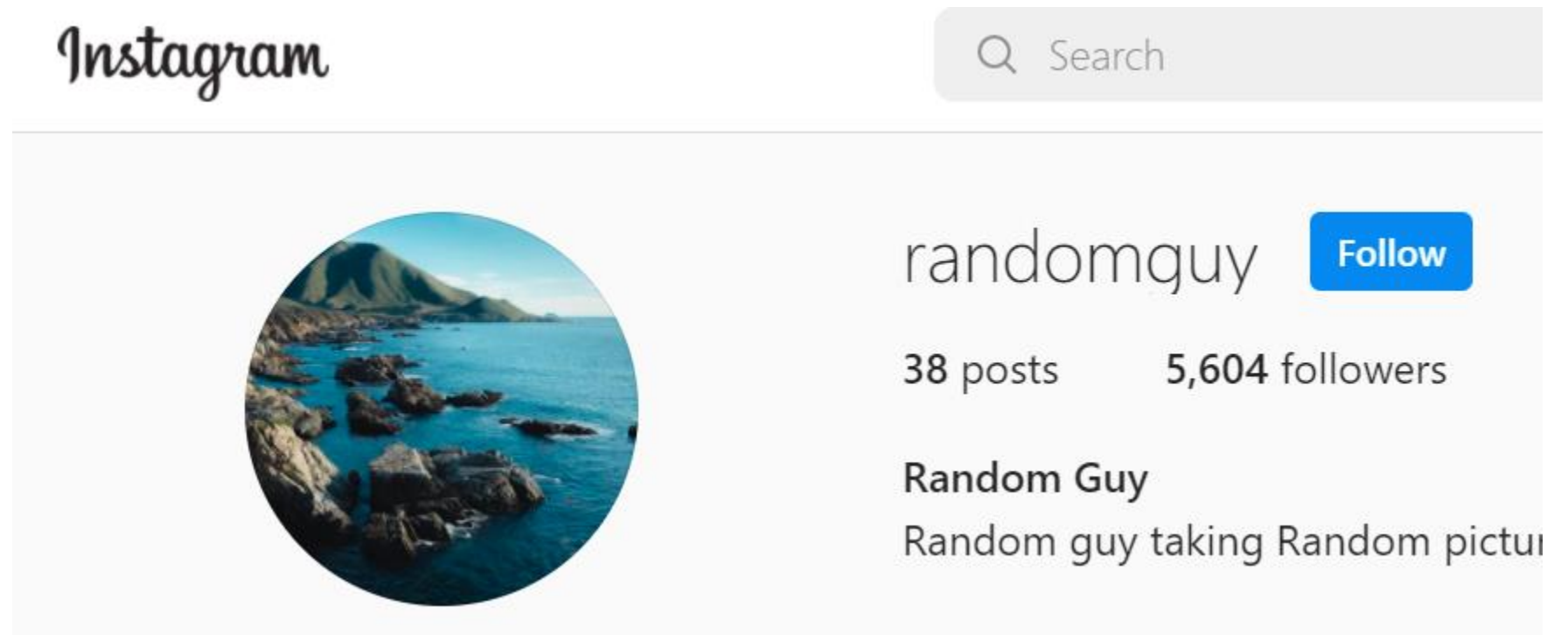
Search Instagram posts in same location

- <https://help.instagram.com/717817284984139>

1. Tap  at the bottom to go to Search & Explore.
2. Tap **Search** in the search bar at the top.
3. Type the location name, then tap the search button in the bottom right of your keyboard.
4. Tap **Places** below the search bar to see a list of the locations that match your search.
5. Select the place that you want to see photos for.

Download Instagram profile picture

- <https://izoomyou.app/>
- Example:



IZOOMYOU

randomguy Download Instagram Profile Picture

PROFILE DP

STORIES

PHOTO

VIDEO

CAROUSEL


Download



Telegram bots

- @getfb_bot
- @get_kontakt_bot
- @LeakCheckBot
- @findmekz_bot
- @get_kolesa_bot

Hunter.IO, finding company emails

 [Product](#) [Pricing](#) [Resources](#) [Company](#) [Sign in](#) [Sign up](#)

[Find email addresses](#)

Most common pattern: {first}.{last}@astanait.edu.kz 126 email addresses

[c sten.wolff@astanait.edu.kz](#) 2 sources [^](#)

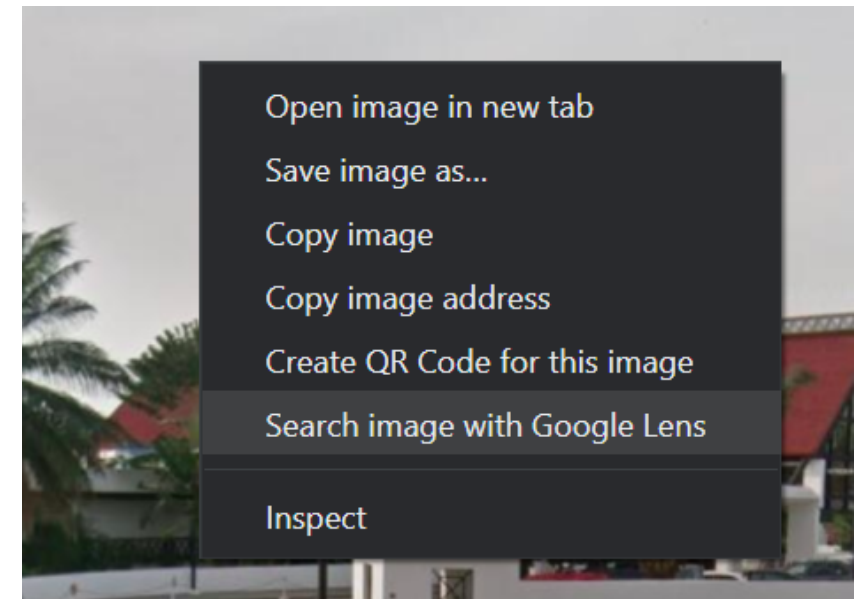
<http://astanait.edu.kz/rectorate> Aug 16, 2021

<http://astanait.edu.kz/kk/rectorate-3> Mar 30, 2021

[r an.maslov@astanait.edu.kz](#) 2 sources [^](#)

Google lens, search what you see

- <https://lens.google/>
- In Google Chrome, right click on the image



Emailrep.io, find sites, where email registered

[DOCS](#)[API KEY](#)[CONTACT](#)[LOGIN](#)

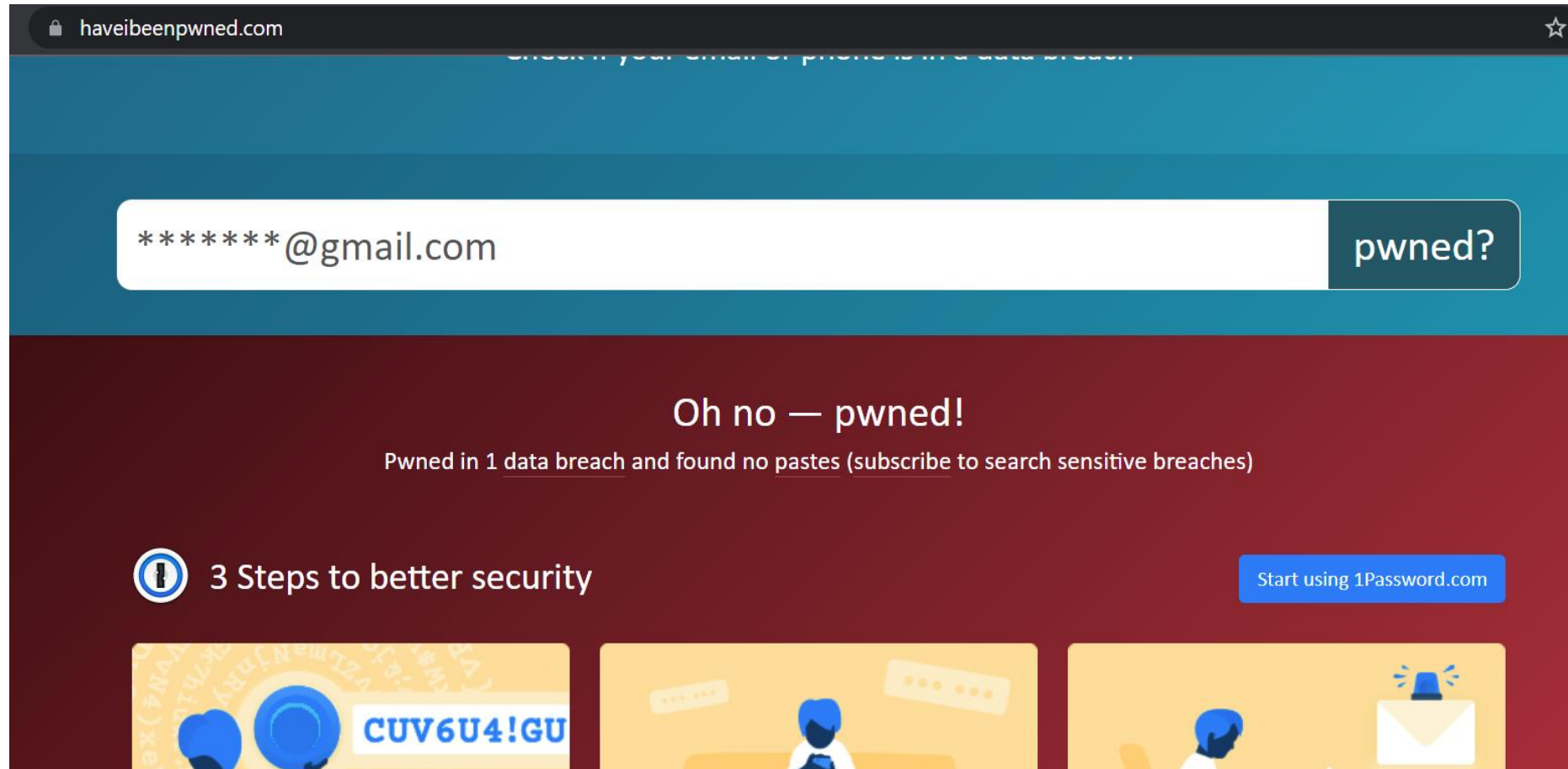
Simple Email Reputation

[SEARCH](#)

MEDIUM REPUTATION

Not suspicious. This email address has been seen in 2 reputable sources on the internet, including Twitter. It has been seen in data breaches or credential leaks as recent as 06/29/2020, but not recently. We've observed no malicious or suspicious activity from this address.

Haveibeenpwned.com, check password leak



Leakcheck.io, check password leak

The screenshot shows the Leakcheck.io website with a search results modal open. The modal has a dark background and a light blue information box at the top. Below this, there's a 'Show 10 entries' dropdown and a table with two columns: '@ Source' and '@ Last breach'. The table contains one entry: 'Wattpad.com' and '2020-05'. At the bottom of the modal, there's a pagination bar showing 'Showing 1 to 1 of 1 entries' and buttons for 'Previous', '1', and 'Next'. A 'Close' button is located at the bottom right of the modal.

leakcheck.io

LEAKCHECK

Home

Terms of Service

Search results

1 entries found from 1 known sources
Only sources are displayed. Register to see detailed information.
To remove your data, submit a request to removal@leakcheck.net

Show 10 entries

@ Source	@ Last breach
Wattpad.com	2020-05

Showing 1 to 1 of 1 entries

Previous 1 Next

Close

Dehashed.com, check password leak

- <https://dehashed.com/>

Searchcode.com



[Home](#) [About](#) [API](#) [searchcode server](#)

astana

search

2,587 results for 'astana' (476 ms)

apply filters

Source

- ☐ Github (1,394)
- ☐ Bitbucket (930)
- ☐ GitLab (91)
- ☐ Google Code (63)
- ☐ CodePlex (43)
- ☐ Fedora Project (41)
- ☐ Tizen (11)
- ☐ ... (0)

questions-words.txt <https://bitbucket.org/tmill/word2vecf> | text | 19,559 lines

```
516 Abuja Nigeria Asmara Eritrea
517 Abuja Nigeria Astana Kazakhstan
518 Abuja Nigeria Athens Greece
554 Accra Ghana Asmara Eritrea
555 Accra Ghana Astana Kazakhstan
556 Accra Ghana Athens Greece
592 Algiers Algeria Asmara Eritrea
593 Algiers Algeria Astana Kazakhstan
594 Algiers Algeria Athens Greece
630 Amman Jordan Asmara Eritrea
631 Amman Jordan Astana Kazakhstan
632 Amman Jordan Athens Greece
668 Ankara Turkey Asmara Eritrea
669 Ankara Turkey Astana Kazakhstan
670 Ankara Turkey Athens Greece
```

slimservice-strings.txt <https://github.com/Excito/squeezecenter.git> | text | 1,450 lines

Torrent download detector

- <https://iknowwhatyoudownload.com/>

Torrent downloads and distributions for IP 37.99.45.92

Static IP Likes porn Asia Kazakhstan Almaty 2Day Telecom LLP

[Check your IP address 37.99.45.96](#)

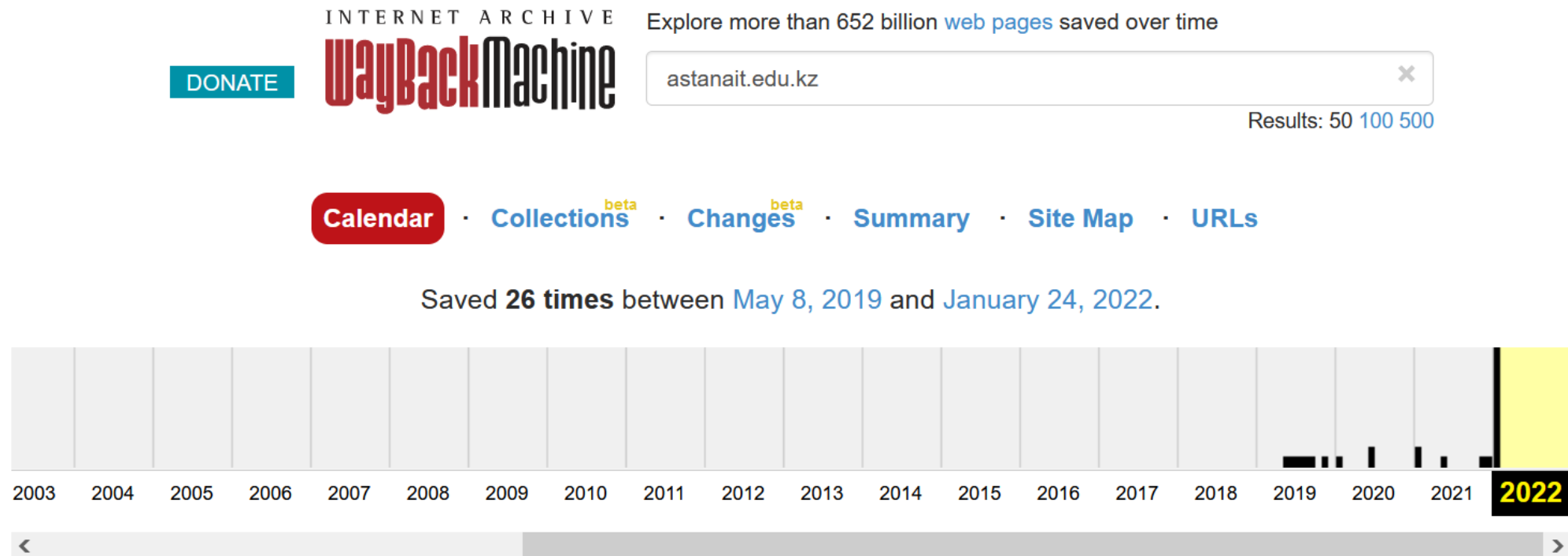
Computers connected to a network are assigned a unique number known as IP Address. IP addresses consist of four numbers in the range 0-255 separated by periods (i.e. 135.77.129.134). A computer may have either a permanent (static) IP address, or one that is dynamically assigned/leased to it.

Use internet connection of other people (Wi Fi, their computers, tablets and smartphones) to know what they download in torrent network, [spy on them via special generated link](#) or see other similar IPs: [37.99.45.87](#) [37.99.45.88](#) [37.99.45.89](#) [37.99.45.90](#) [37.99.45.91](#) **37.99.45.92** [37.99.45.93](#) [37.99.45.94](#) [37.99.45.95](#) [37.99.45.96](#)

FIRST SEEN (UTC)	LAST SEEN (UTC)	CATEGORY	TITLE	SIZE
Feb 2, 2022, 6:56:06 AM	Feb 2, 2022, 3:55:49 PM	Games	Serious.Sam.Siberian.Mayhem.GOG.Rip-InsaneRamZes	28.51GB
Feb 2, 2022, 6:53:00 AM	Feb 2, 2022, 3:52:42 PM	Movies	Harry Potter and the Sorcerer's Stone	23.31GB

Web archive

- <https://web.archive.org>



Other tools

- <https://www.shodan.io/>
- <https://spyse.com/>
- <https://search.censys.io/>
- <https://viewdns.info/>

Useful queries

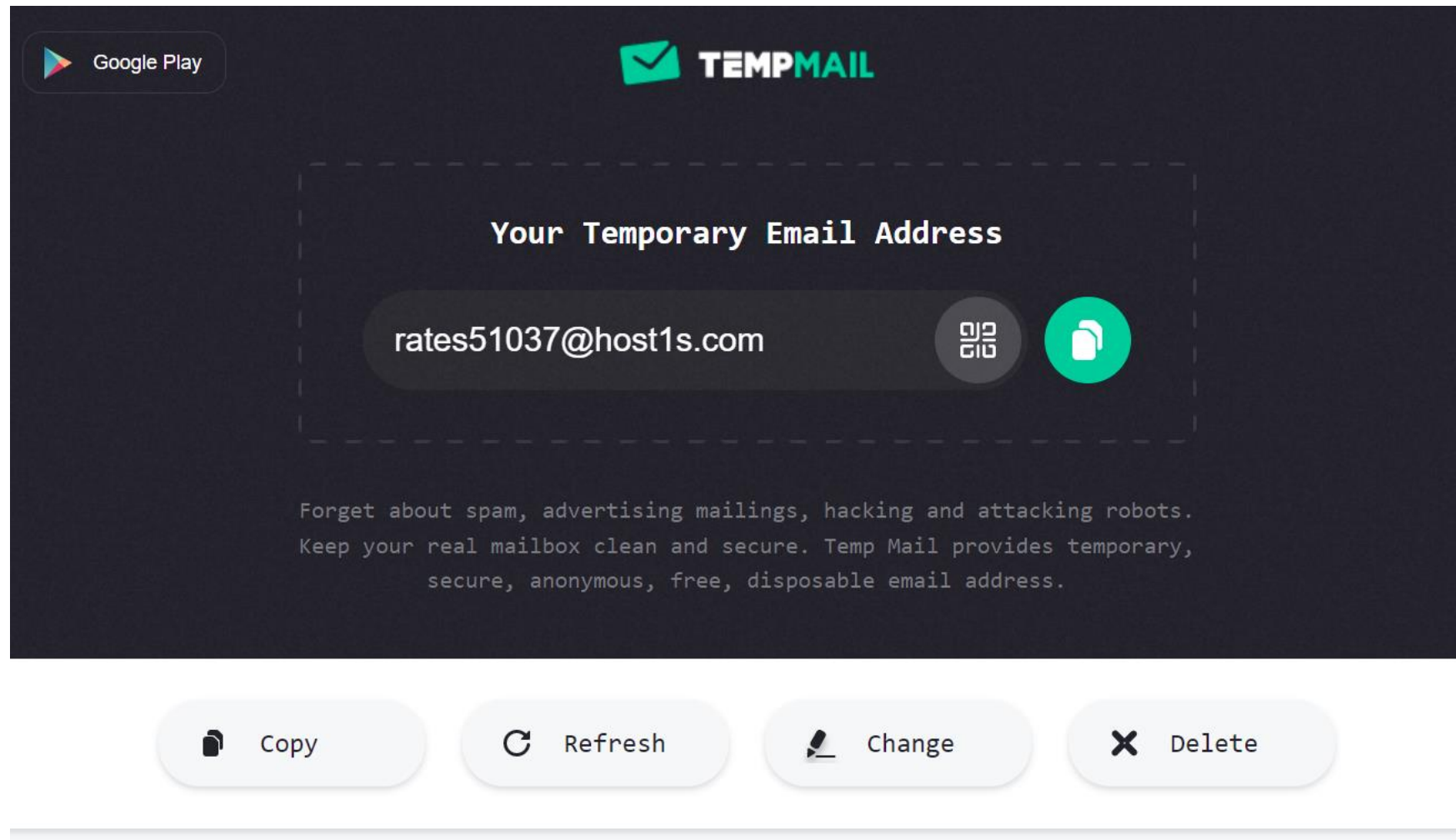
- <https://www.osintme.com/index.php/2021/01/16/ultimate-osint-with-shodan-100-great-shodan-queries/>
- <https://www.exploit-db.com/google-hacking-database>

Other OSINT resources

- <https://medium.com/week-in-osint>
- <https://twitter.com/OsintStash>
- <https://sector035.nl/>

How to hide phone number and email?

Temp-mail.org



Getfreesmsnumber.com

Numbers: +447488854991 is Online !

Update SMS

Change number

Sender: [Cashmo](#)

the ra - From GetFreeSMSNumber.COM

— 4 minutes ago

Sender: [Cashmo](#)

Welcome to Cashmo! Get started on your casino journey today, with up to
50 FREE SPINS in Rainbow Slots, at: <http://cashmo.uk/93326> Slide over

— 4 minutes ago

Other SMS receive services

- <http://freeonlinephone.org>
- <http://sms-receive.net>
- <http://smsreceivefree.com>
- <http://receive-a-sms.com>
- <http://receivefreesms.com>
- <http://freephonenum.com>
- <http://receive-smss.com>
- <http://receivetxt.com> and etc.

Maltego

- **Maltego** is software used for open-source intelligence and forensics. Maltego focuses on providing a library of transforms for discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining.
- <https://en.wikipedia.org/wiki/Maltego>
- <https://www.maltego.com/>
- Practice: <https://www.youtube.com/watch?v=D2rutsb-ft0>

Any questions?

Homework for the next lesson

- Find the exact name (in latin) of this flower:

<https://murat.one/wp-content/uploads/2022/02/flower.jpg>

- Find the exact point, where this photo was taken:

<https://murat.one/wp-content/uploads/2022/02/test.jpg>

- Find all information related to the phrase “@manfromkz” using Maltego

Feedback: did we achieved the goals of our lesson?

- Discussion 5-10 minutes

Useful links

- https://en.wikipedia.org/wiki/Open-source_intelligence
- <https://en.wikipedia.org/wiki/Exif>
- <https://en.wikipedia.org/wiki/ExifTool>
- <https://github.com/exiftool/exiftool>
- <https://medium.com/week-in-osint>
- <https://twitter.com/OsintStash>
- <https://sector035.nl/>
- <https://2gis.kz>