Методы анонимизации в Сети: как искать, но не быть найденным

ДОКЛАДЧИК: @dukera

Методы анонимизации

Приватность — люди знают, кто вы, но не знают, что вы делаете.

Анонимность — люди знают, что вы делаете, но не знают, кто вы.

Ваш IP-адрес

Узнать свой IP-адрес:
https://resolve.rs/
https://www.dnsleaktest.com/ (также можно проверить свой IP на наличие утечек DNS)

Resolve.rs

DNS (Domain Name System) is a key part of the internet: it maps human-readable **domain names** (like `wikipedia.org`) to the corresponding numeric **IP address** (like `208.80.154.224`). The servers that do this mapping are called **resolvers**.

Open DNS Resolvers
You do not have to use your ISP's DNS resolver. Here are some alternatives that may better suit your needs.
List of alternative resolvers

Your Nameservers
IP address: [redacted]
Reverse DNS: not found
ASN: PJSC Moscow city telephone network (25513)
How this works

Your IP Address
[redacted]
Reverse DNS: [redacted]
ASN: PJSC Moscow city telephone network (25513)
More...

Your Location
IP Geolocation uses your IP address to guess your approximate location.
Your location: Moscow, Russia: 55.7483, 37.6171
More...

DNS Lookups
Lookup a hostname across all the open resolvers
More...

Reverse DNS Lookup
Given an IP address, find the corresponding hostname
More...

Tools
Random tools I made that needed a good home.
Details...

API
Most of the pages have a corresponding JSON and/or text endpoint that you can call.
Details...

• Contact • Validate HTML

Test complete

Query round	Progress...	Servers found
1	.....	2

IP	Hostname	ISP	Country
[redacted]	None	Moscow City Telephone Network	Moscow, Russian Federation
[redacted]	None	Moscow City Telephone Network	Moscow, Russian Federation

What do the results of this test mean?

- The servers identified above receive a request to resolve a domain name (e.g. www.eff.org) to an IP address everytime you enter a website address in your browser.
- The owners of the servers above have the ability to associate your personal IP address with the names of all the sites you connect to and store this data indefinitely. This does not mean that they do log or store it indefinitely **but they may and you need to trust whatever their policy says**.
- If you are connected to a VPN service and ANY of the servers listed above are not provided by the VPN service then you have a DNS leak and are choosing to trust the owners of the above servers with your private data.

Dnsleaktest.com is proudly brought to you by IVPN, an open-source, audited, no BS, no logs, VPN provider run by privacy advocates.

Ваш IP-адрес

Узнать свой IP-адрес или местоположение любого IP-адреса:
https://resolve.rs/ip/geolocation.html
Показывает торренты, которые были скачаны с указанного IP-адреса:
https://iknowwhatyoudownload.com

IP Address Geolocation

Geolocating an IP address is not an exact science. It depends on data collected (or volunteered by the community), and needs constant updates.

Results for [redacted]

ASN: PJSC Moscow city telephone network (25513)

Provider	Results
AbstractAPI	▼RU: Moscow, Moscow, Russia: 55.7483, 37.6171


```
{
  "ip_address": [redacted],
  "city": "Moscow",
  "city_geoname_id": 524901,
  "region": "Moscow",
  "region_iso_code": "MOW",
  "region_geoname_id": 524894,
  "postal_code": "129226",
  "country": "Russia",
  "country_code": "RU",
  "country_geoname_id": 2017370,
  "country_is_eu": false,
  "continent": "Europe",
  "continent_code": "EU",
  "continent_geoname_id": 6255148,
  "longitude": 37.6171,
  "latitude": 55.7483,
  "security": {
    "is_vpn": false
  },
  "timezone": {
    "name": "Europe/Moscow",
    "abbreviation": "MSK",
    "gmt_offset": 3,
    "current_time": "15:03:58",
    "is_dst": false
  },
  "flag": {
    "emoji": "RU",
    "unicode": "U+1F1F7 U+1F1FA",
    "png": "https://static.abstractapi.com/country-flags/RU_flag.png",
    "svg": "https://static.abstractapi.com/country-flags/RU_flag.svg"
  },
  "currency": {
    "currency_name": "Ruble",
    "currency_code": "RUB"
  },
  "connection": {
    "autonomous_system_number": 25513,
```


About Us [redacted] Find IP

Torrent downloads and distributions for IP [redacted]

Static IP | Europe | Russia | Moscow | PJSC Moscow city telephone network

[redacted] is your IP address.

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. 155.135.109.48). A computer may have either a permanent (static) IP address, or one that is dynamically assigned/leased to it.

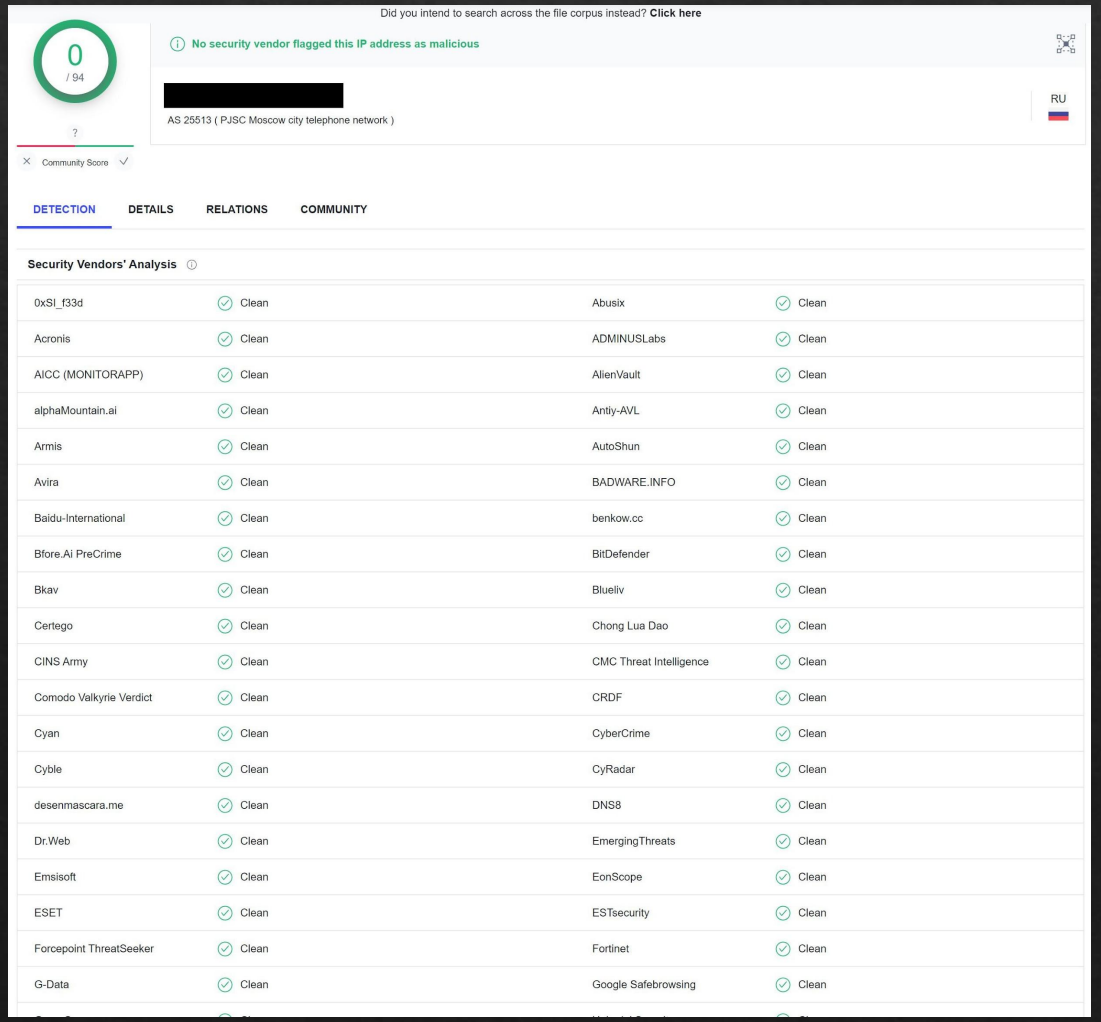
Use internet connection of other people (Wi Fi, their computers, tablets and smartphones) to know what they download in torrent network, spy on them via special generated link or see other similar IPs: [redacted]

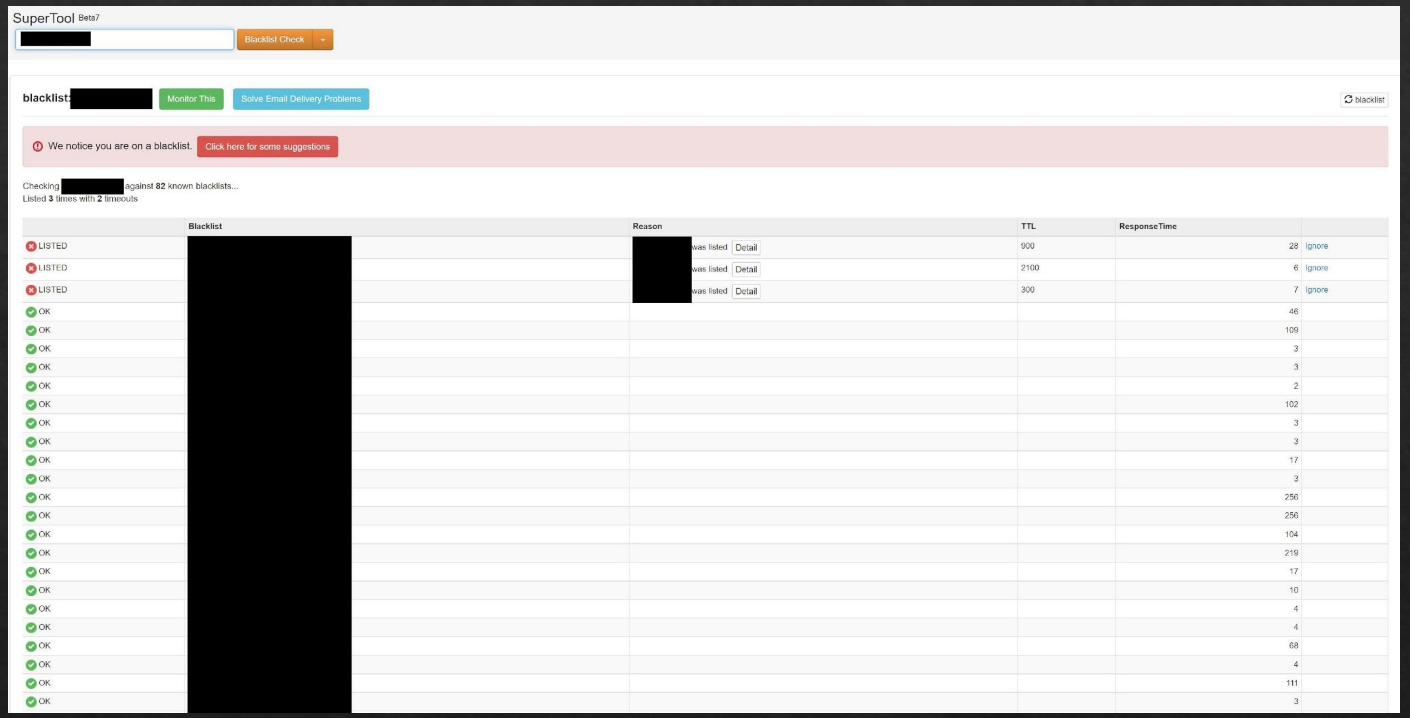
FIRST SEEN (UTC)	LAST SEEN (UTC)	CATEGORY	TITLE	SIZE
11 окт. 2022 г., 12:11:55	14 окт. 2022 г., 13:53:40	Movies	Westworld	21.81GB
10 окт. 2022 г., 19:04:41	10 окт. 2022 г., 19:04:41	Movies	Ozark	37.69GB
10 окт. 2022 г., 18:55:09	10 окт. 2022 г., 18:55:09	Movies	Westworld	29.81GB

Follow Us

Ваш IP-адрес

Узнайте, является ли IP-адрес «подозрительным»:
https://mxtoolbox.com/blacklists.aspx
https://www.virustotal.com/gui/home/search





Ваш IP-адрес

Регистрационная информация IP:
https://whois.domaintools.com/
Узнать, подключены ли вы через Tor
https://check.torproject.org

IP Information for [redacted]

– Quick Stats

IP Location	Russian Federation Moskva Moscow Local Telephone Network (oao Mgts)
ASN	[redacted]
Resolve Host	[redacted]
Whois Server	whois.ripe.net
IP Address	[redacted]

```
% Abuse contact for [redacted]

inetnum:
netname:
descr:
country:
admin-c:
tech-c:
status:
mnt-by:
created:
last-modified:
source:

role:
address:
address:
address:
e-mail:
admin-c:
admin-c:
admin-c:
tech-c:
tech-c:
tech-c:
abuse-mailbox:
nic-hdl:
mnt-by:
created:
last-modified:
source:

route:
descr:
descr:
origin:
mnt-by:
created:
last-modified:
source:
```

Sorry. You are not using Tor.

Your IP address appears to be: [redacted]

If you are attempting to use a Tor client, please refer to the Tor website and specifically the frequently asked questions.

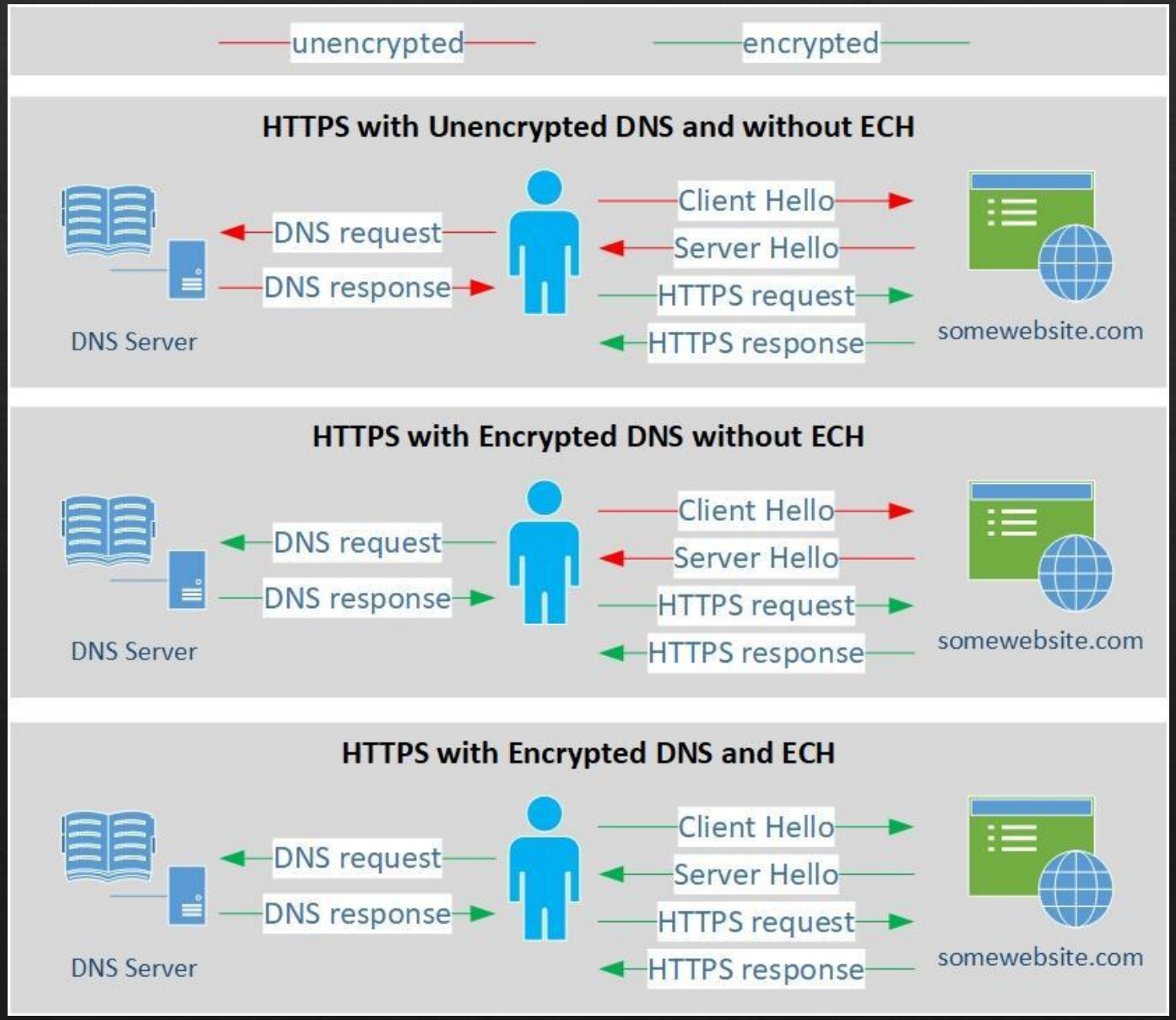
Donate to Support Tor

Tor Q&A Site | Volunteer | Run a Relay | Stay Anonymous

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn More »

JavaScript is enabled.

Ваши запросы DNS и IP



Tor Hidden DNS Service или ODoH (Oblivious DNS over HTTPS) однако эти методы предоставляются только Cloudflare:

https://blog.cloudflare.com/welcome-hidden-resolver/

https://blog.cloudflare.com/oblivious-dns/

Если есть опыт в Linux, то можно рассмотреть DoHoT (DNS через HTTPS через Tor):

https://github.com/alecmuffett/dohot

Метаданные

Данные, которые собирает о нас Google:

DuckDuckGo Privacy Browser

Data Linked to You

The following data may be collected and linked to your identity:

DuckDuckGo does not collect or share any personal information.

Google Chrome

Data Linked to You

The following data may be collected and linked to your identity:

Analytics

- Location
  - Coarse Location
- User Content
  - Audio Data
  - Customer Support
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
- Diagnostics
  - Crash Data
  - Performance Data
  - Other Diagnostic Data
- Other Data
  - Other Data Types

Product Personalisation

- Location
  - Coarse Location
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction

App Functionality

- Financial Info
  - Payment Info
- Location
  - Coarse Location
- User Content
  - Audio Data
  - Customer Support
  - Other User Content
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
- Diagnostics
  - Crash Data
  - Performance Data
  - Other Diagnostic Data
- Other Data
  - Other Data Types

Google

Data Linked to You

The following data may be collected and linked to your identity:

Third-Party Advertising

- Location
  - Coarse Location
- Search History
  - Search History
- Browsing History
  - Browsing History
- Usage Data
  - Advertising Data

Developer's Advertising or Marketing

- Location
  - Coarse Location
- Contact Info
  - Physical Address
  - Email Address
  - Name
- Search History
  - Search History
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
  - Advertising Data

Analytics

- Location
  - Precise Location
  - Coarse Location
- Contact Info
  - Physical Address
  - Email Address
- Contacts
  - Contacts
- User Content
  - Audio Data
  - Customer Support
  - Other User Content
- Search History
  - Search History
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
  - Advertising Data
  - Other Usage Data
- Diagnostics
  - Crash Data
  - Performance Data
  - Other Diagnostic Data
- Other Data
  - Other Data Types

Product Personalisation

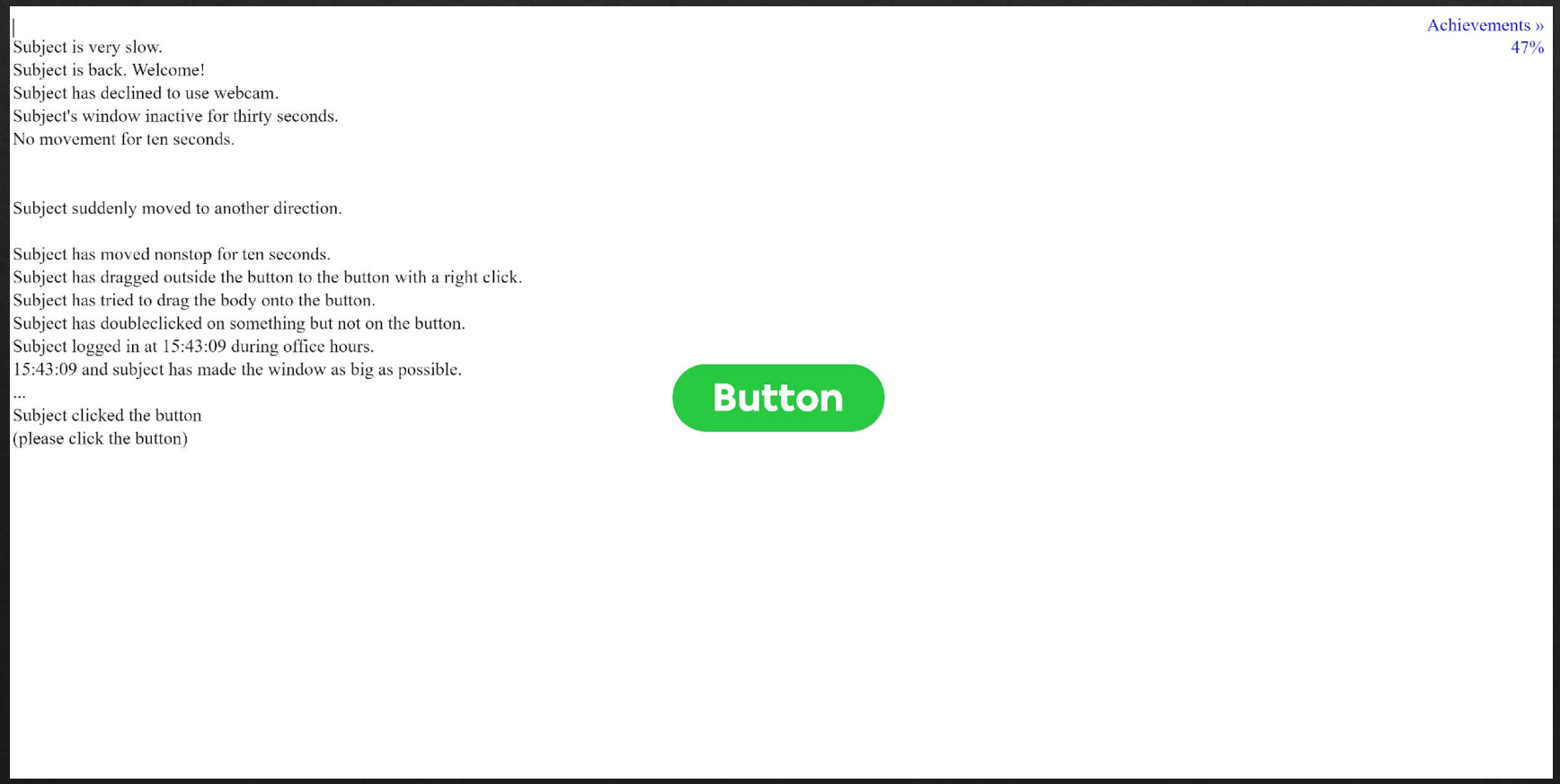
- Location
  - Precise Location
  - Coarse Location
- Contact Info
  - Physical Address
  - Email Address
- User Content
  - Photos or Videos
  - Other User Content
- Search History
  - Search History
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
  - Advertising Data

App Functionality

- Financial Info
  - Payment Info
- Location
  - Precise Location
  - Coarse Location
- Contact Info
  - Physical Address
  - Email Address
  - Name
  - Phone Number
- Contacts
  - Contacts
- User Content
  - Photos or Videos
  - Audio Data
  - Customer Support
  - Other User Content
- Search History
  - Search History
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
  - Advertising Data
- Diagnostics
  - Crash Data
  - Performance Data
  - Other Diagnostic Data
- Other Data
  - Other Data Types

Метаданные

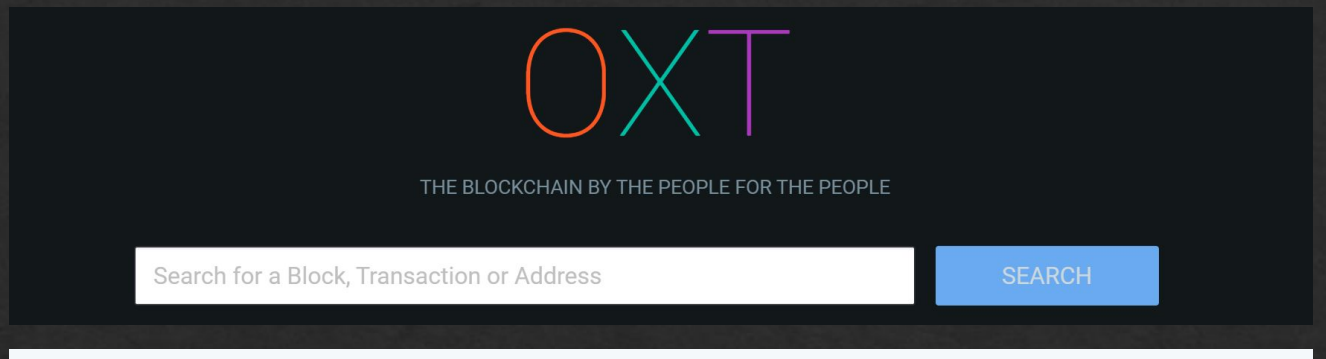
Компания, которая продает правоохранительным органам продукты для анализа активности в соц. сетях:
https://mediasonar.com/
Вот пример, с помощью которого вы сами можете увидеть в реальном времени отслеживание ваших действий. Требуется включенный JavaScript:
https://clickclickclick.click

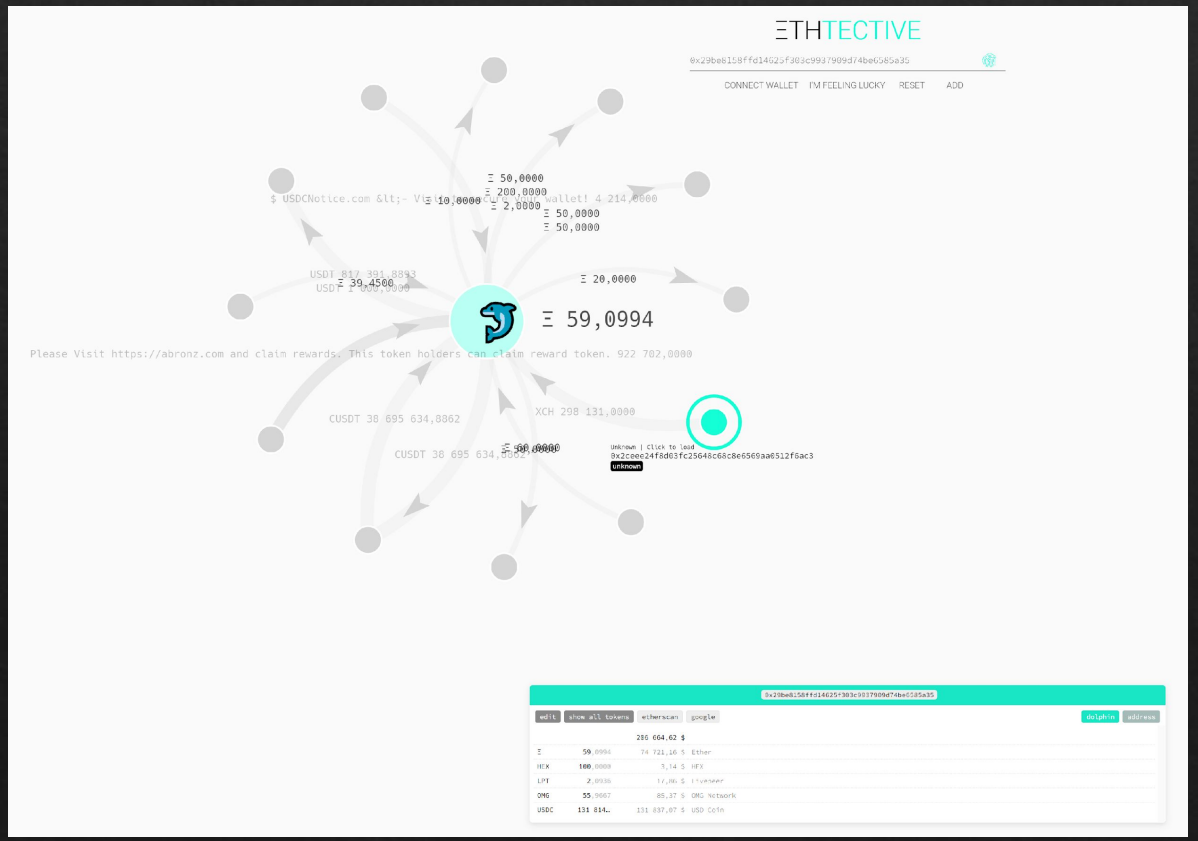


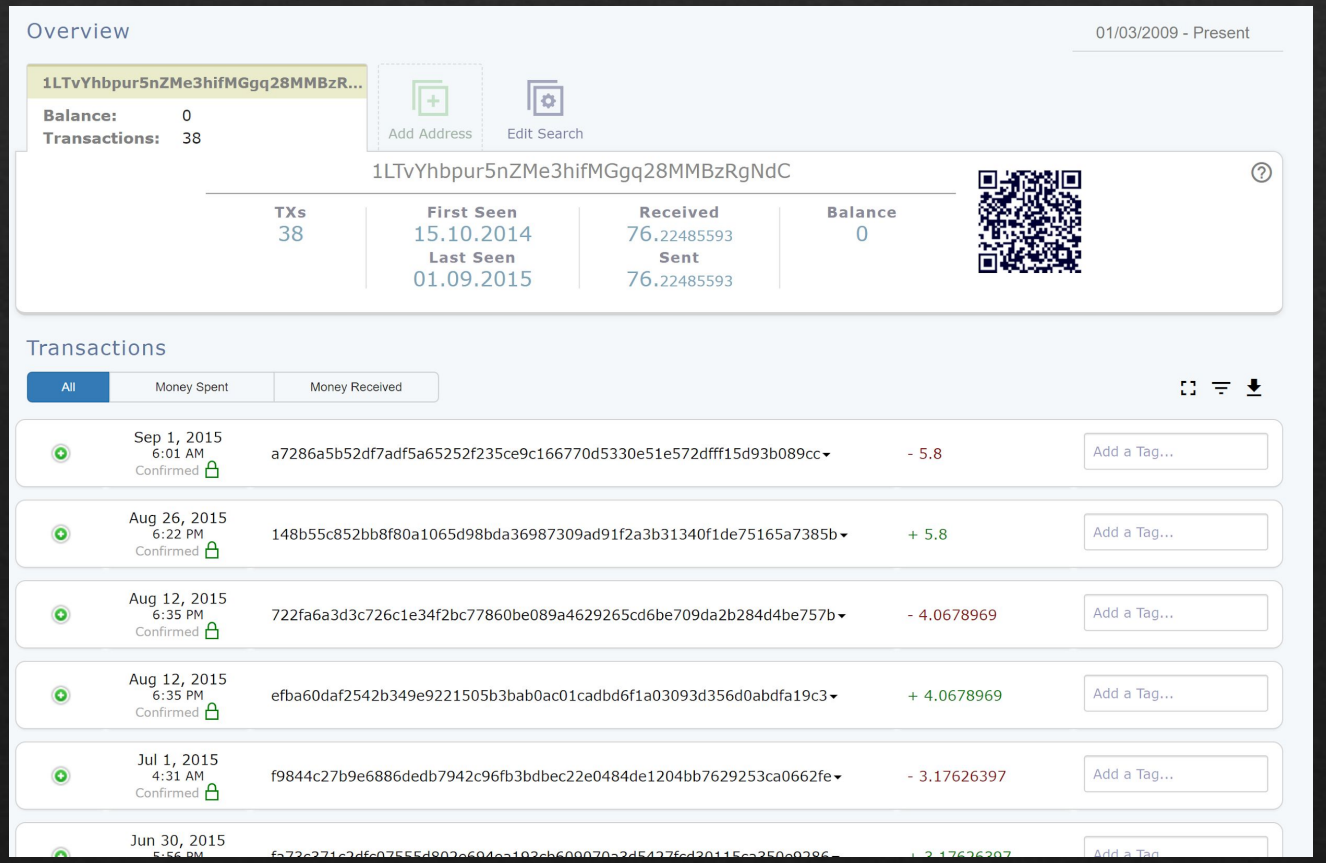
Криптовалютные транзакции

Moscow OSINT meetup №3
Методы анонимизации в Сети:
как искать, но не быть
найденным
@dukera

Сервисы которые позволяют отслеживать операции с криптовалютами:
https://ethtective.com/
https://blockpath.com/
https://oxt.me/







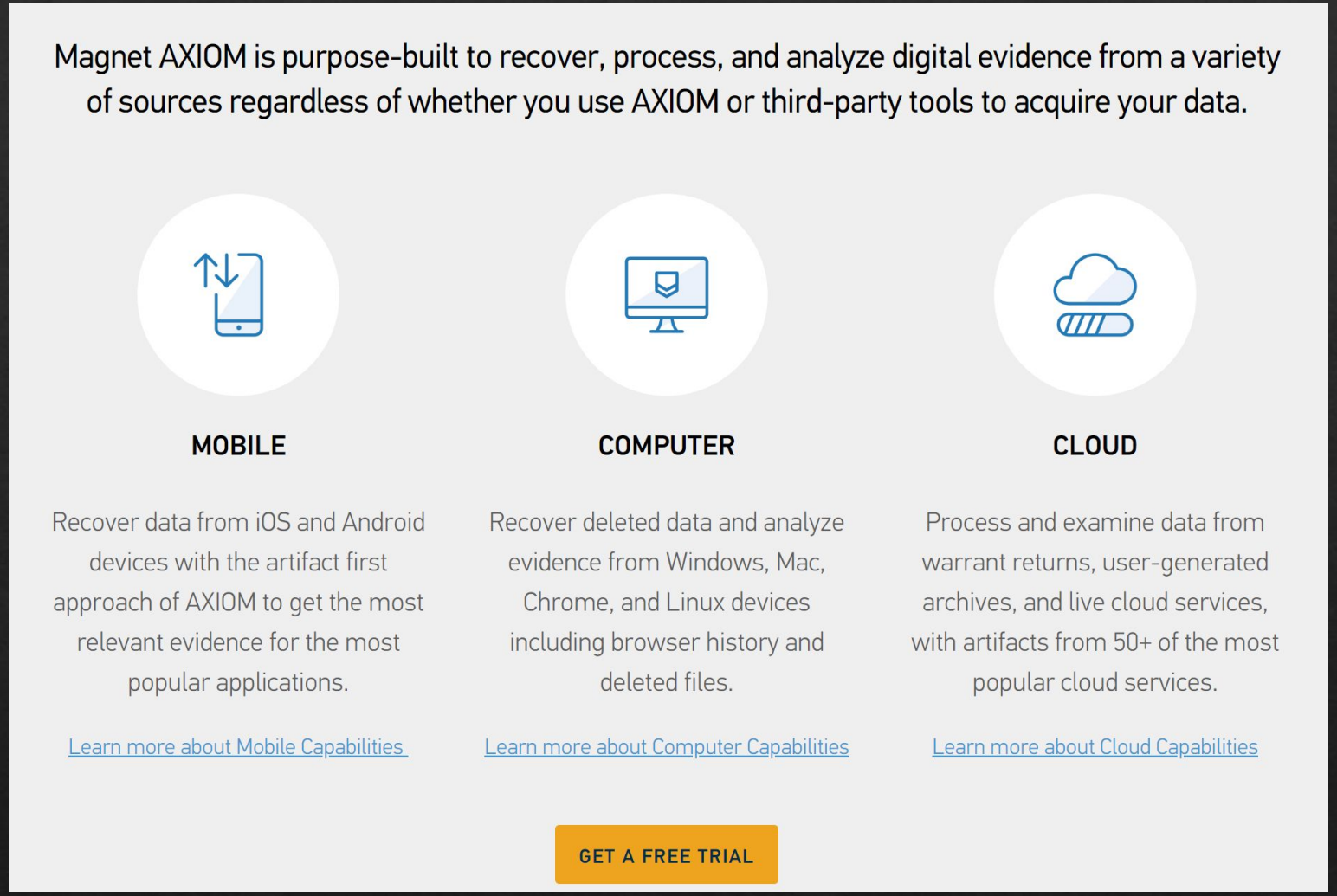
Облачные сервисы

Проекты, которые могут помочь злоумышленнику проанализировать ваши облачные данные:

https://www.magnetforensics.com/products/magnet-axiom/

https://cellebrite.com/en/ufed-cloud/

Единственный способ обезопасить себя – шифровать данные самостоятельно



Отпечатки вашего браузера

Отпечатки вашего браузера и устройства — это набор свойств/возможностей вашей системы/браузера.

Больше подробной информации и публикаций:

https://amiunique.org/links

https://brave.com/brave-fingerprinting-and-privacy-budgets/

Устойчивость к сбору отпечатков сама по себе может быть использована для отпечатков пальцев:

https://palant.info/2020/12/10/how-anti-fingerprinting-extensions-tend-to-make-fingerprinting-easier/

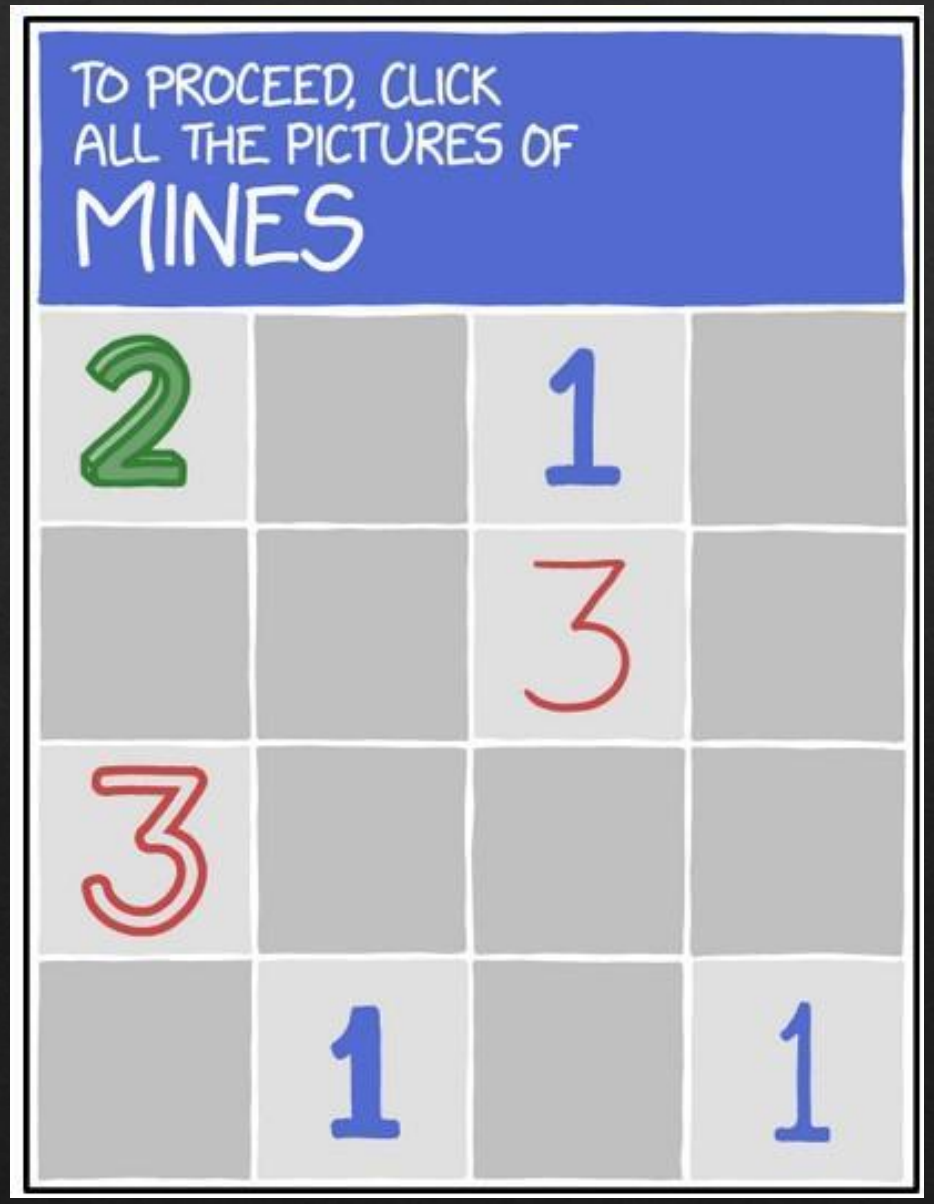
CAPTCHA

Современные капчи используют следующие методы проверки, что позволяет собирать отпечаток пользователя:

- проверяют ваш браузер, файлы cookie и историю посещенных страниц с помощью отпечатков браузера
- отслеживают движения вашего курсора (скорость, точность)
- отслеживание поведения до, во время и после тестов

Расширение Buster для браузеров, которое может за вас решить reCaptcha:

https://github.com/dessant/buster



Отпечатки браузера и устройства

Службы, которые вы можете использовать для проверки отпечатков:

https://abrahamjuliot.github.io/creepjs/

https://amiunique.org

https://browserleaks.com/

https://www.deviceinfo.me/

Attribute	Similarity ratio All time	Value
User agent	0.77%	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36
Accept	44.12%	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Content encoding	95.27%	gzip, deflate, br
Content language	<0.01%	ru-RU,ru;q=0.9,en-GB;q=0.8,en;q=0.7,en-US;q=0.6
Upgrade Insecure Requests	90.38%	1
Referer	52.26%	https://amiunique.org/
headers.sec-ch-ua.name	0.92%	"Chromium";v="106", "Google Chrome";v="106", "Not;A=Brand";v="99"
headers.sec-ch-ua-mobile.name	24.89%	?0
headers.sec-ch-ua-platform.name	17.85%	"Windows"

551.70ms

Worker 9556831d

lang/timezone:

ru-RU (1 доллар США)
ru

Europe/Moscow (-180)

gpu: confidence: high

Google Inc. (AMD)
ANGLE (AMD, Radeon Pro 580 Direct3D11 vs_5_0 ps_5_0, D3D11)

userAgent: ua reduction

Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/106.0.0.0 Safari/537.36

device:

Windows (Win32)
Windows 10 (64-bit)
cores: 4, ram: 8

userAgentData:

Google Chrome 106 (106.0.5249.119)
Windows 10 (2004|20H2|21H1) [10.0.0] x86_64

ServiceWorkerGlobalScope

WebGL 6cd98ae2 103.50ms

images: 8f22af98
pixels: 73a293e1
params (78): 926bfffb
exts (47): cea46de1
gpu: confidence: high

Google Inc. (AMD)
ANGLE (AMD, Radeon Pro 580 Direct3D11 vs_5_0 ps_5_0, D3D11)

Screen c8d3811c 0.10ms

...screen: 2560 x 1440
....avail: 2560 x 1400
touch: false
depth: 24|24
viewport:

1292
1278
1261

1406
1230
1230

browser
landscape
landscape-primary
2

Другие меры предосторожности

Финансовые операции:

Платформа может потребовать выполнить финансовую транзакцию на небольшую сумму

Очевидно, это еще один метод проверки личности и деанонимизации

Войти через какую-либо платформу:

«Зачем самим проводить проверку пользователей, если мы можем просто попросить других разобраться с этим?»

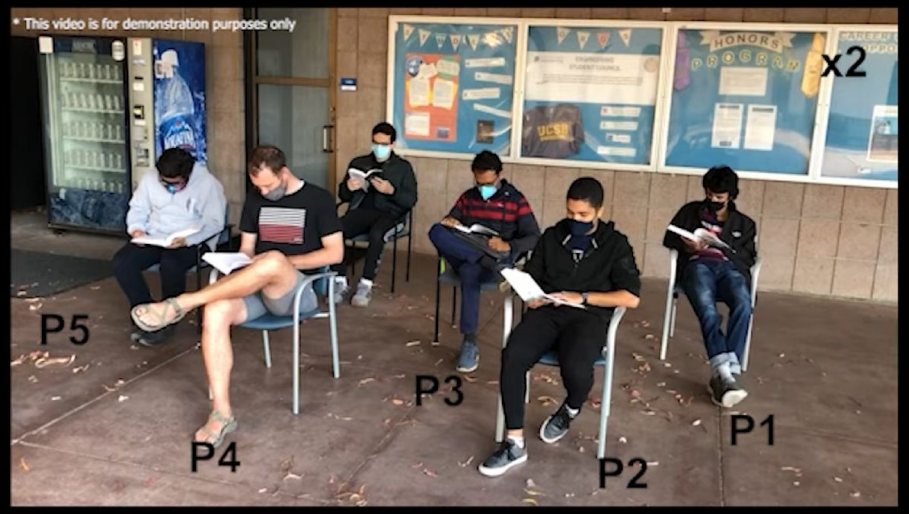
Сайт может предлагать авторизацию через Google, Facebook, VK и тд. Для сервиса это более удобный способ собирать о вас информацию

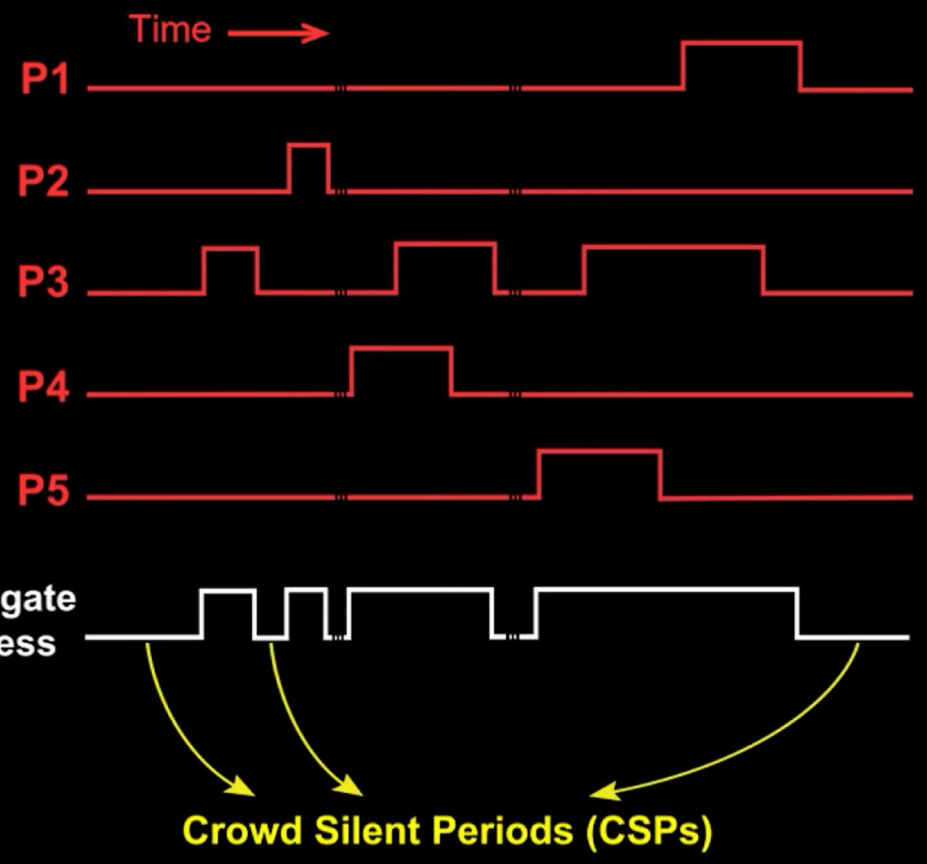
Устройства Wi-Fi и Bluetooth

Отслеживание движений основываясь на радиопомехах:
http://rfpose.csail.mit.edu/
https://www.youtube.com/watch?v=HgDdaMy8KNE

Устройства Wi-Fi и Bluetooth

Способ подсчета людей в помещении с помощью Wi-Fi:
https://www.news.ucsb.edu/2021/020392/dont-fidget-wifi-will-count-you





Crowd Fidgeting Period: A time period where at least one person is fidgeting

Crowd Silent Period: A time period where no one is fidgeting

Лицо, голос, биометрия

Социальные сети могут использовать расширенное распознавание лиц.
Например, вы в любой момент можете оказаться на чей-то фотографии, а после публикации, социальная сеть распознает на ней ваше лицо с привязкой к геолокации и времени

Распознавание походки и внешности

Платформы Google и Facebook уже знают кто вы по следующим причинам:

1. Потому что у вас есть или был профиль с ними, и вы идентифицировали себя

2. Даже если вы никогда не создавали профиль на этих платформах, он все равно у вас может быть

3. Потому что другие люди отметили вас или идентифицировали вас на своих фотографиях

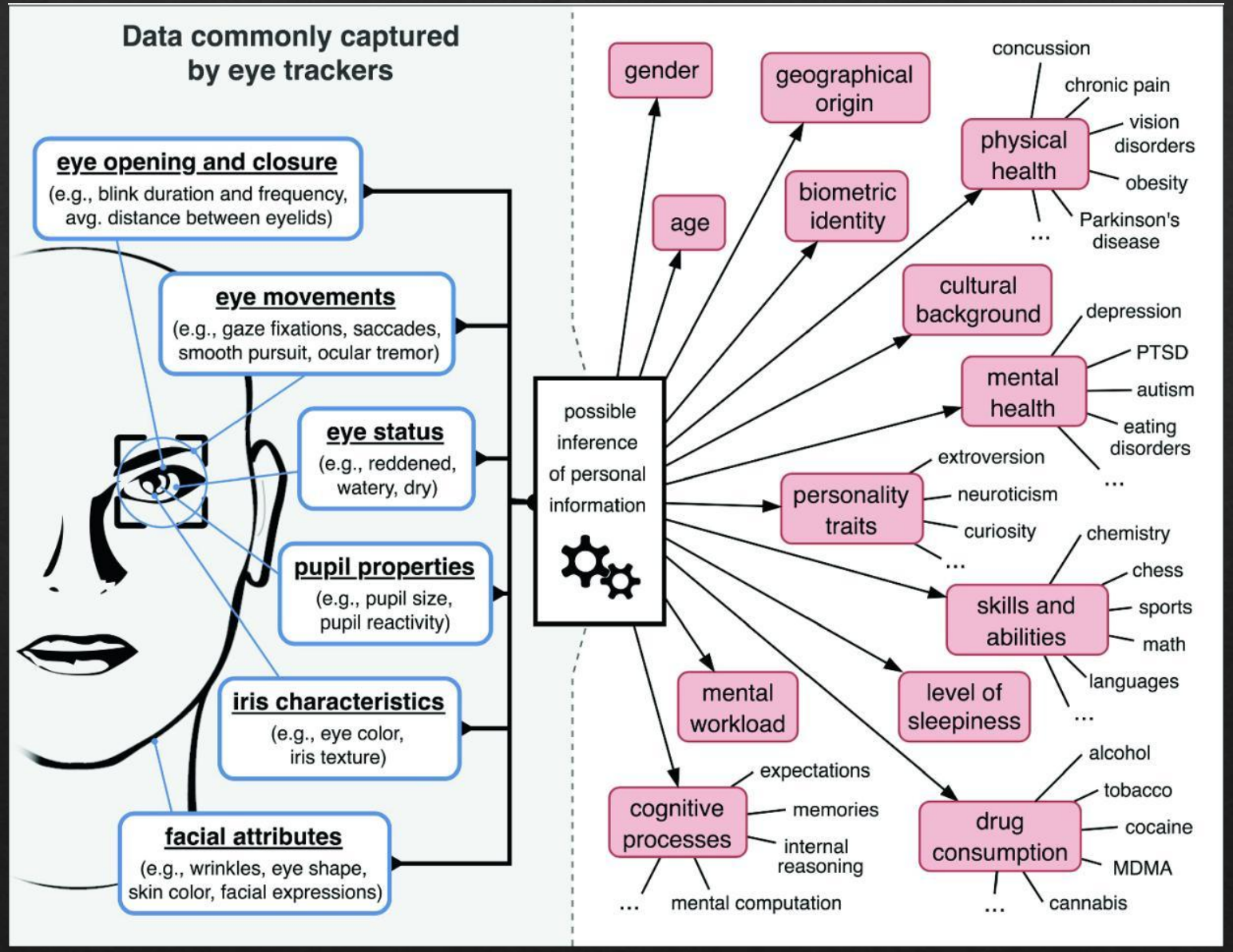
4. Потому что другие люди поместили ваше изображение в свой список контактов, которым они затем поделились с ними

Распознавание походки и внешности

Лучший способ обмануть систему – носить свободную одежду, которая скроет движения ваших мышц.

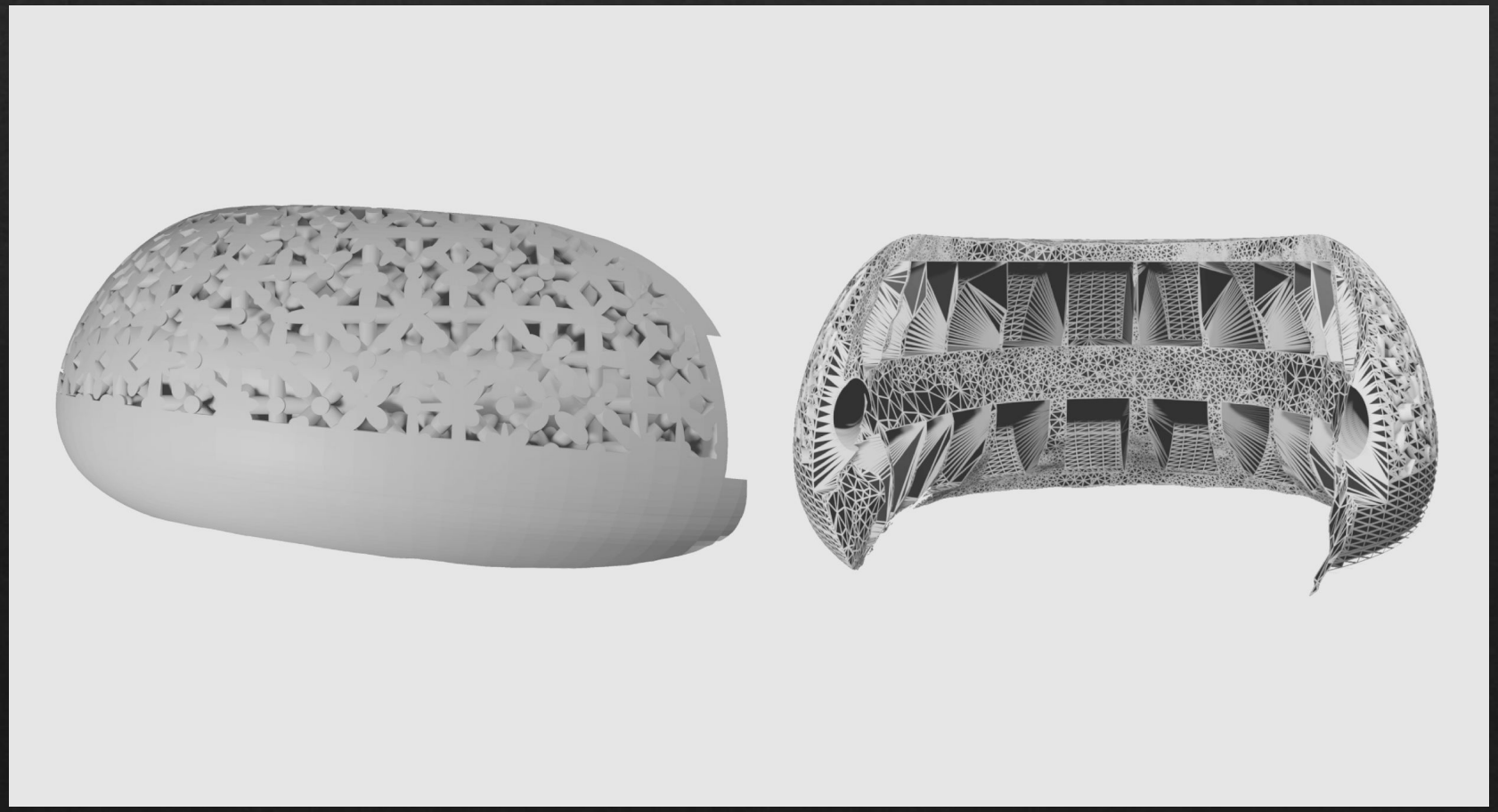
Способы, которыми можно частично или полностью исключить распознавание лиц:

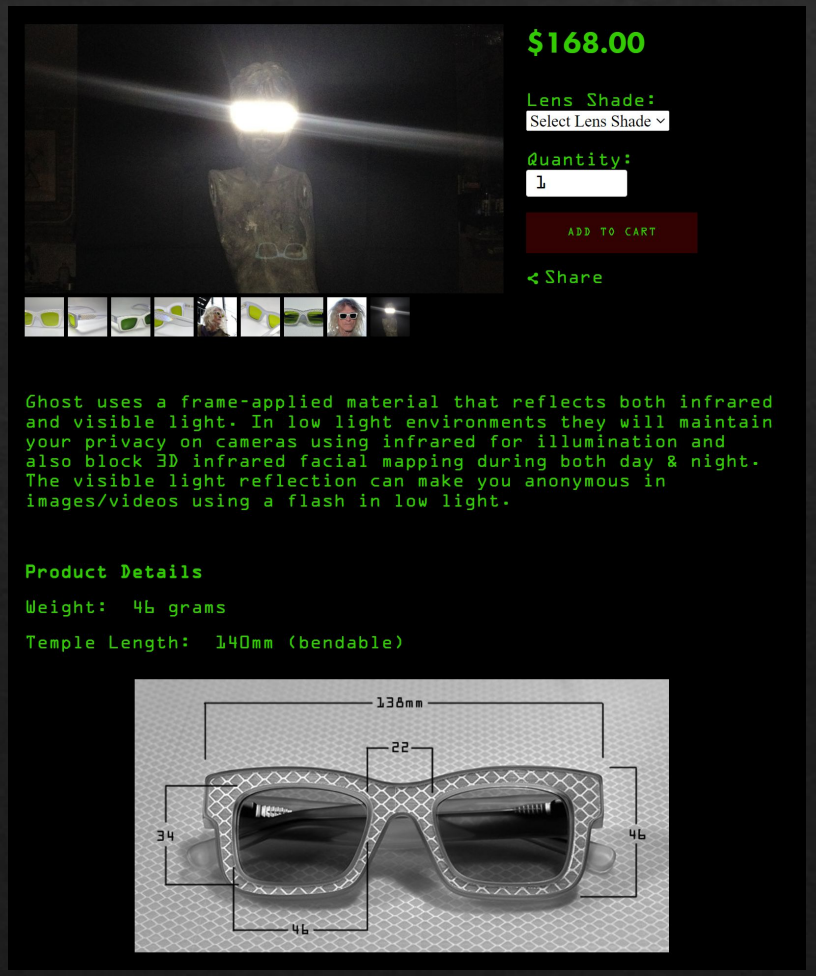
- Носить маску
- Носить головной убор
- Носить солнцезащитные очки



Распознавание походки и внешности

Специальные очки «Reflectacles»:
https://www.reflectacles.com/
Если у вас есть 3D-принтер, вы можете попробовать изменить собственную походку:
https://gitlab.com/FG-01/fg-01





IMEI, IMSI и номер телефона

IMEI и IMSI можно отследить благодаря следующим обстоятельствам:

1. Мобильные операторы хранят в связке IMEI и IMSI

2. В журналах антенн также будет храниться IMSI и IMEI. Они регистрируют комбинации IMEI/IMSI, которые подключены к набору антенн а также мощность сигнала

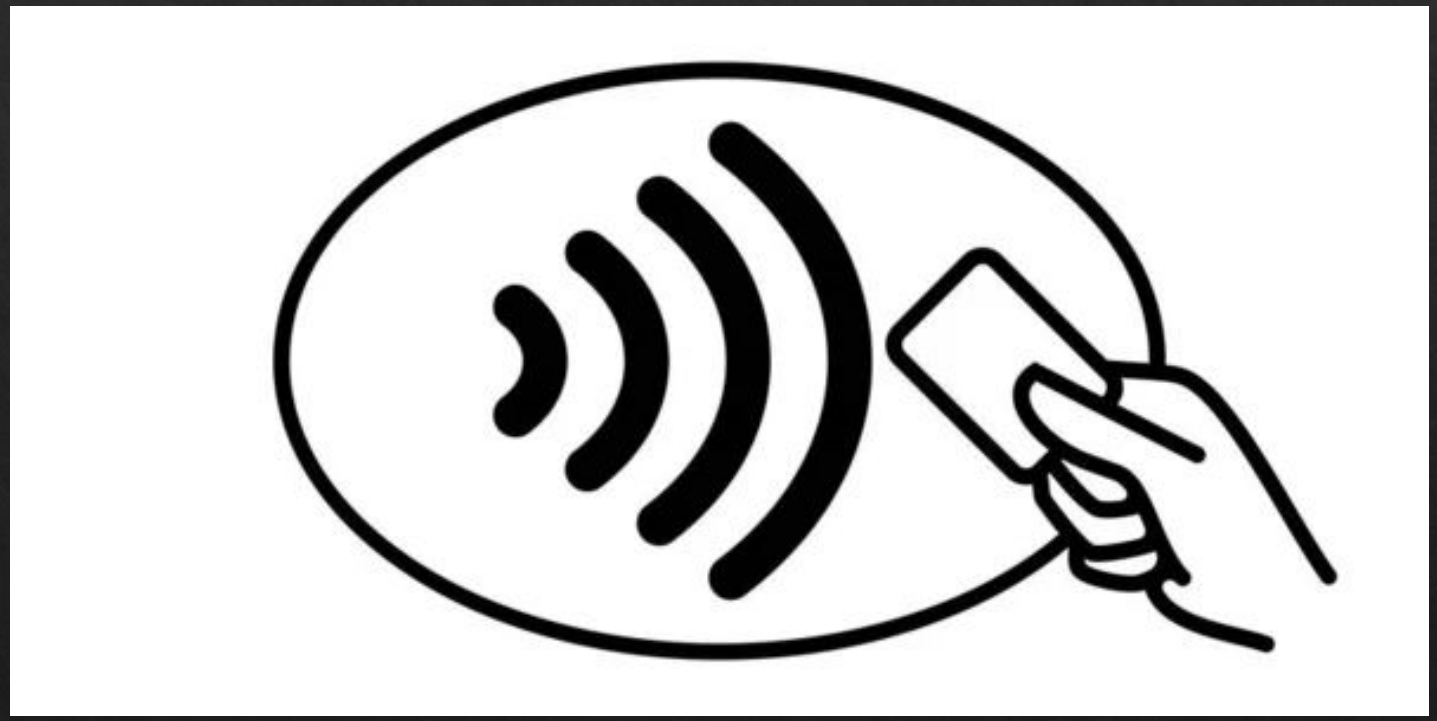
3. Таким образом можно отследить продажу/покупку нового телефона если ваш основной телефон находился при вас

4. Также могут использоваться специальные устройства вроде Stingray или Nyxcell. Эти устройства выдают себя за базовую станцию и заставляют определенный IMSI подключаться к ней для доступа к сотовой сети

Устройства с поддержкой RFID

Примеры устройств с поддержкой RFID:

- банковские карты с поддержкой бесконтактного платежа
- NFC в телефоне
- карты лояльности магазинов
- транспортные платежные карты
- карты доступа
- ключи от машины (не все)
- ключи от домофона
- RFID метки на предметах/одежде



Устройства с поддержкой RFID

Антенны способны считывать метки RFID на расстоянии до 15 метров

Существуют изделия, способные защитить RFID метки от электромагнитных волн

Создание анонимной личности

Создание новых личностей

Что для этого нужно?
1. Понимать, от чего требуется скрыться
2. Находиться в безопасном месте без камер видеонаблюдения и смартфона
3. Иметь анонимный номер телефона

Должна быть продумана полная легенда вашего персонажа:

- Возраст
- Пол
- Этническая принадлежность
- Место рождения и дата рождения
- Место жительства
- Страна происхождения
- Посещенные страны
- Хобби и интересы
- История семьи
- Состав семьи, если есть
- Семейный статус, если есть
- Языки
- Опыт работы
- Состояние здоровья
- Вероисповедание
- Черты характера
- Цели

Создание новых личностей

Социальные сети могут искать подозрительные вещи в ваших данных, например:

- IP-адрес из страны, отличной от страны вашего профиля
- возраст в профиле не соответствует возрасту на фото
- национальность в профиле не соответствует национальности на фото
- язык не соответствует языку страны
- неизвестный в чьих-либо контактах (имеется в виду, что никто другой вас не знает)
- блокировка настроек конфиденциальности после регистрации
- имя, которое не соответствует этнической принадлежности/языку/стране

Создание новых личностей

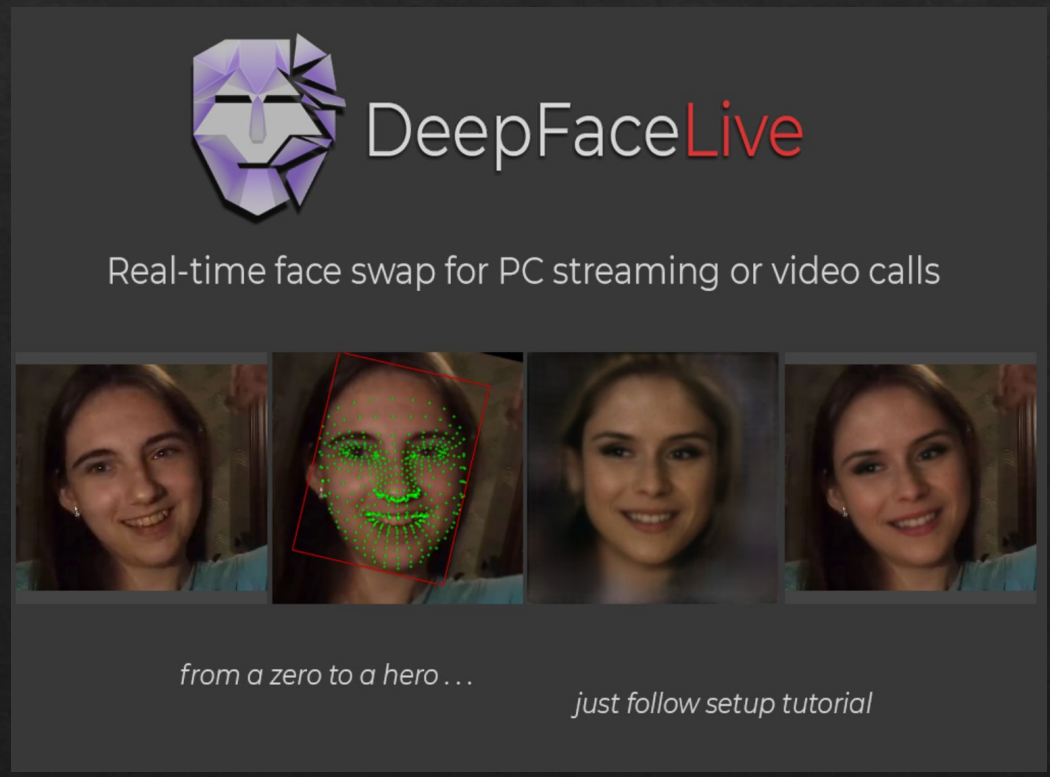
Некоторые платформы/приложения требуют, чтобы вы сфотографировали себя вживую.

Методом обхода может быть использование дипфейка faceswap:

https://github.com/deepfakes/faceswap

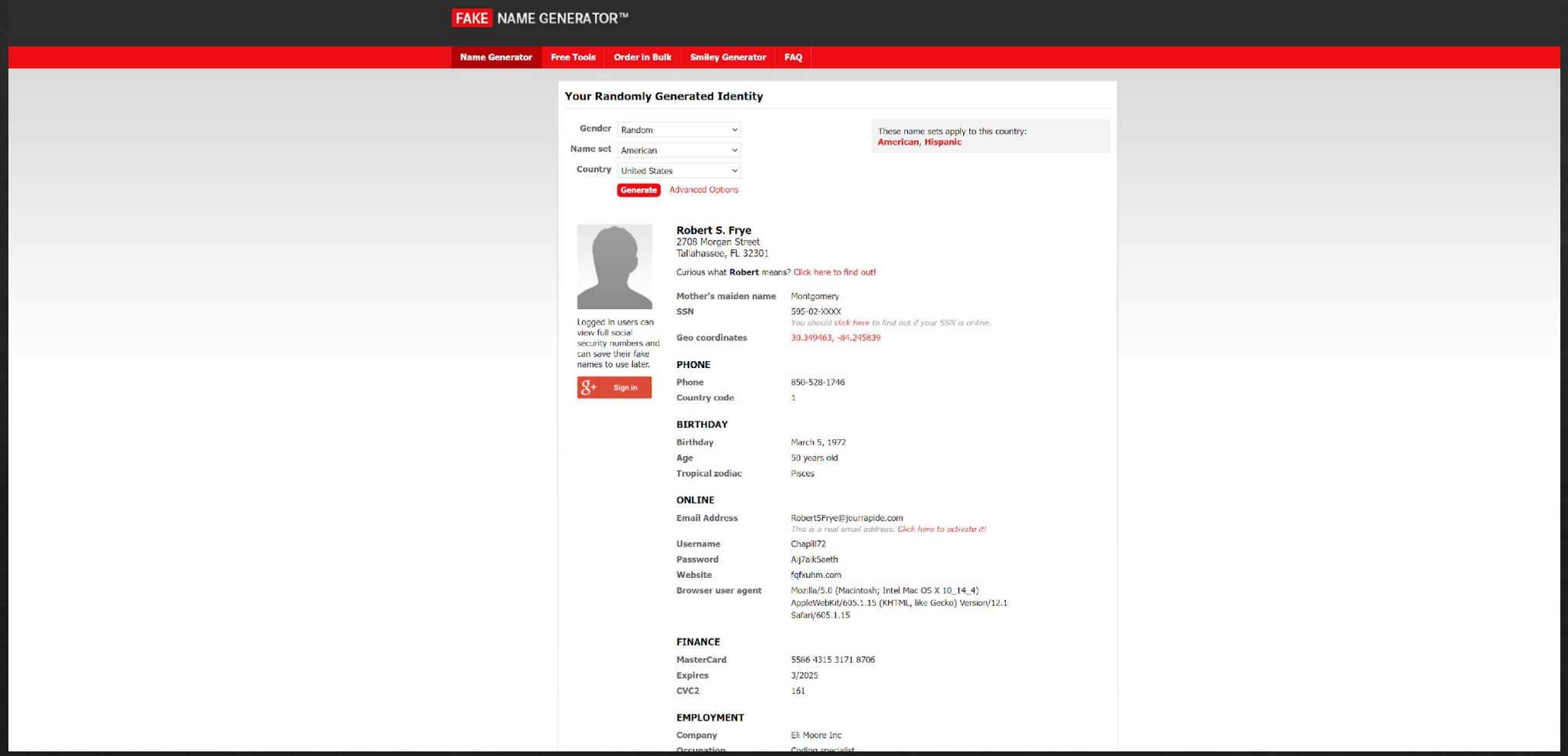
В некоторых случаях требуется «замена лица» прямо в камере, а не на фото:

https://github.com/iperov/DeepFaceLive



Создание новых личностей

Инструменты, которые могут помочь в создании личностей:
https://www.fakenamegenerator.com/
https://thispersondoesnotexist.com/



Создание новых личностей

Инструменты, которые могут помочь в создании личностей:
https://generated.photos/face-generator
Также с помощью проекта StyleGan можно самому создавать изображение:
https://github.com/NVlabs/stylegan2
Бонусом можно сделать изображение подвижным:
https://www.myheritage.com/deep-nostalgia

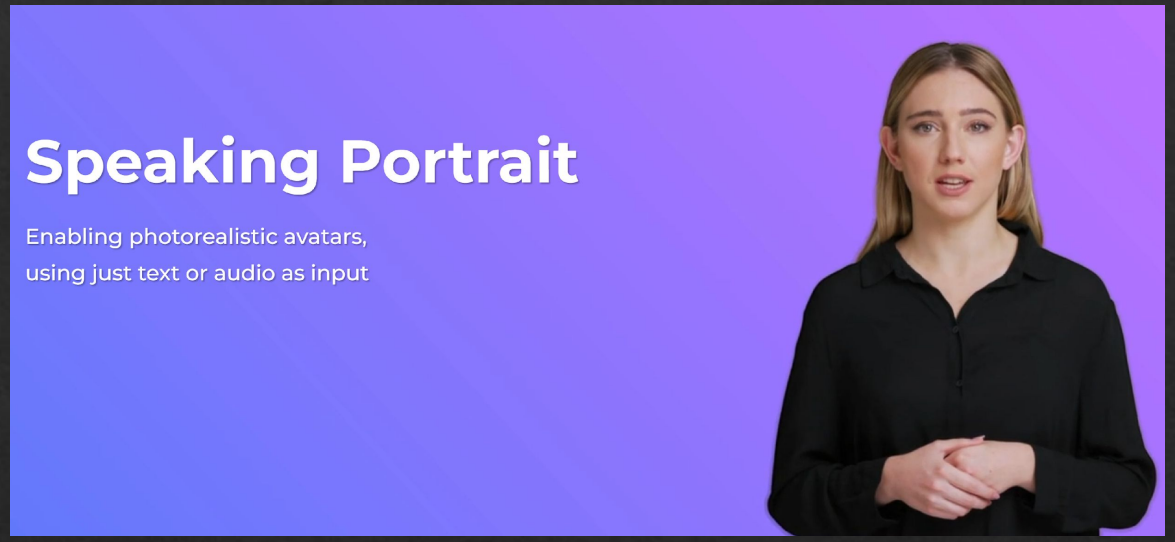
Создание новых личностей

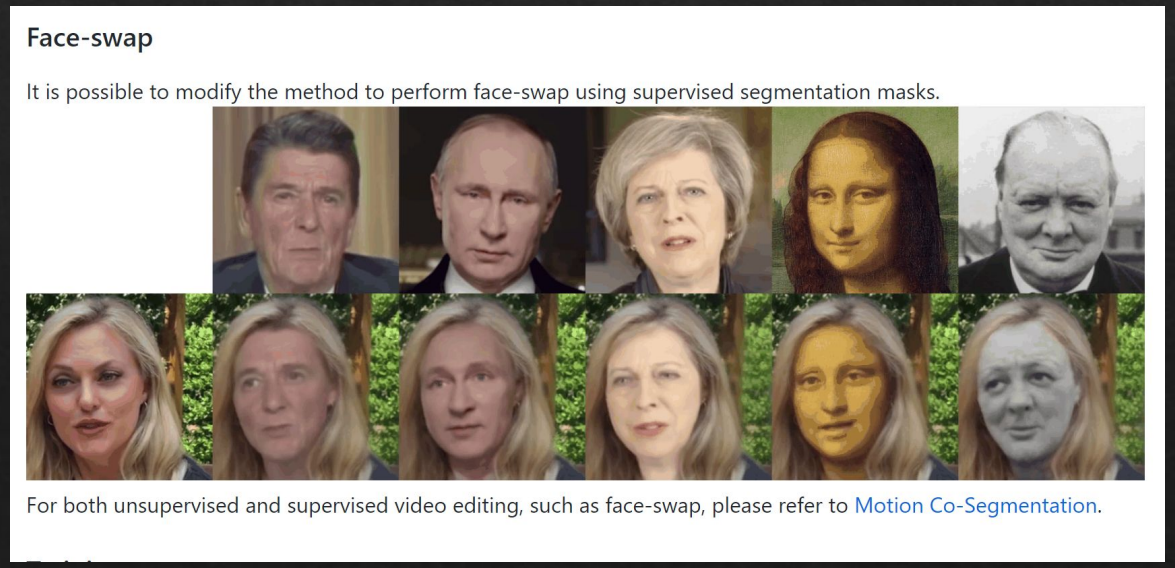
Такого эффекта можно добиться самостоятельно:

https://github.com/AliaksandrSiarohin/first-order-model

Также доступен такой сервис:

https://www.d-id.com/talkingheads/



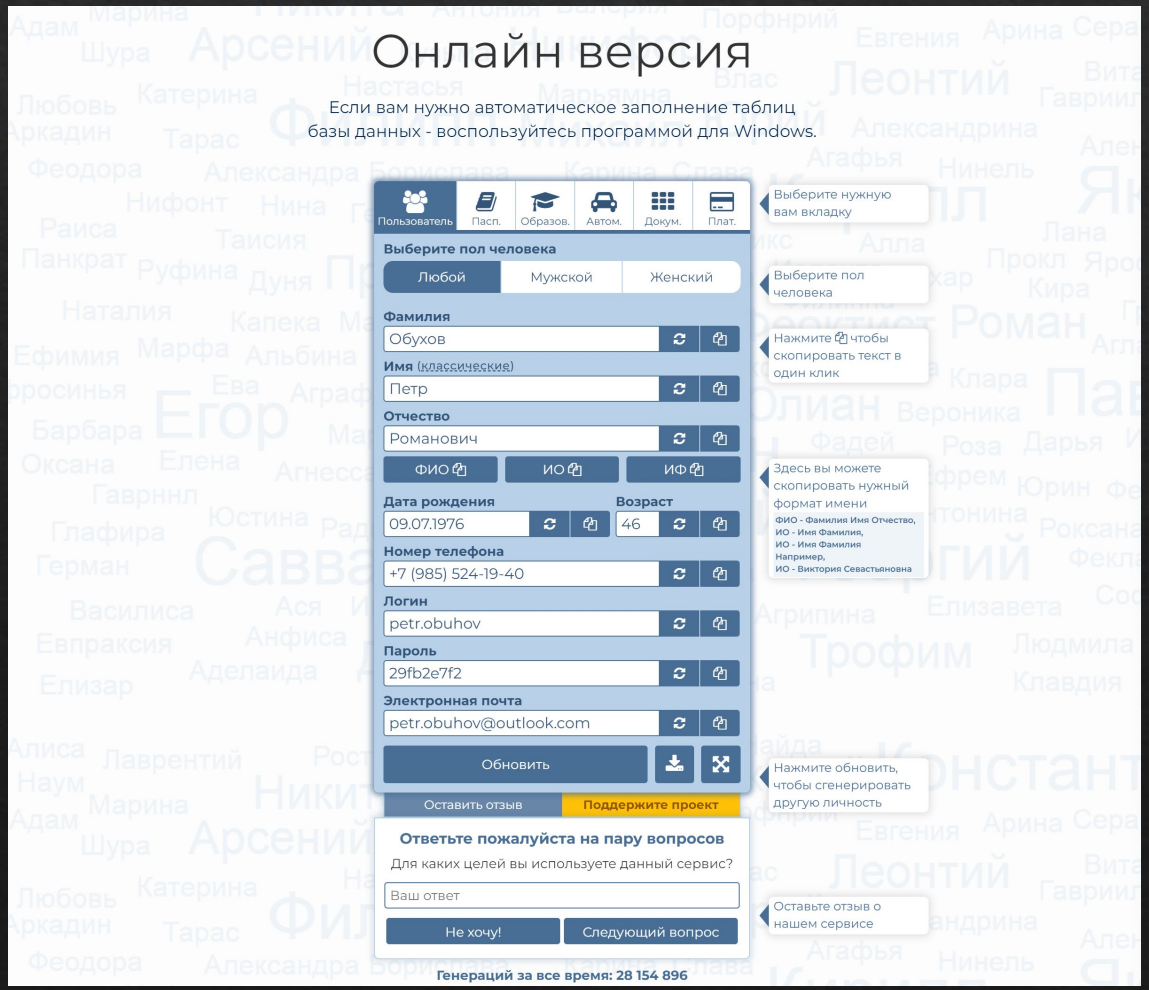


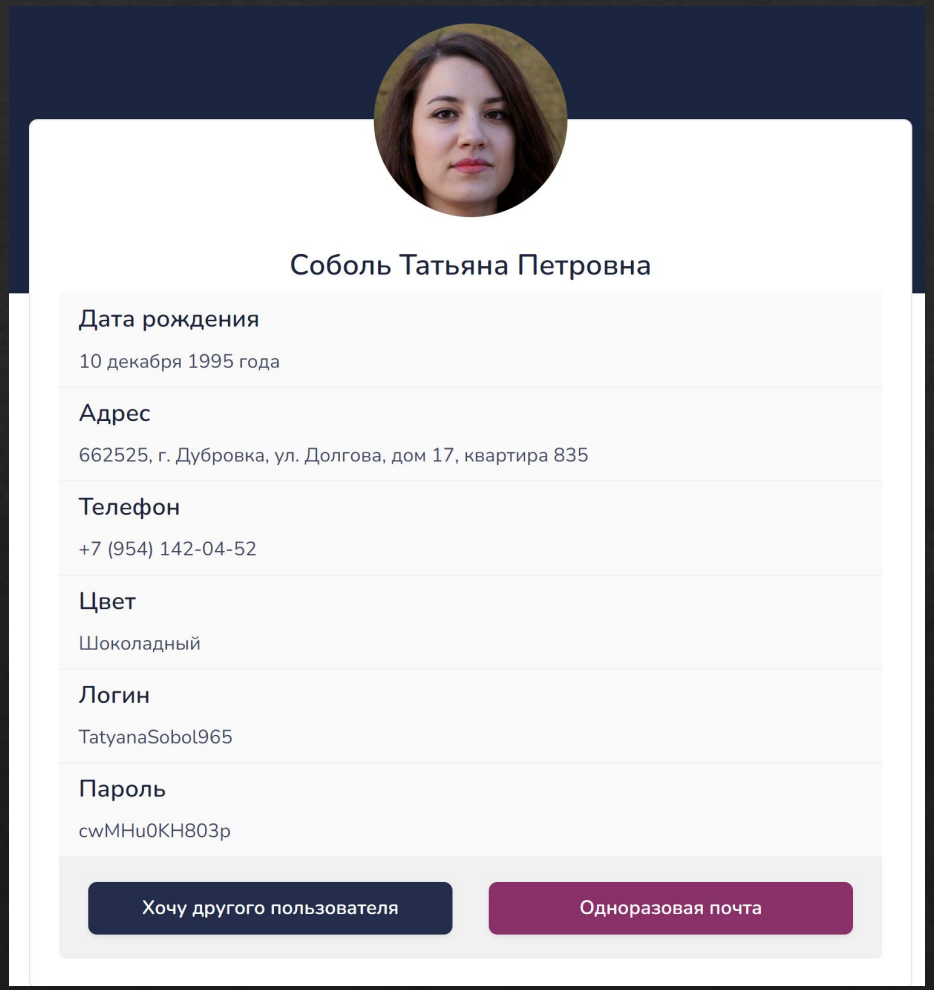
Необходимо:

- учитывать предысторию личностей
- использовать разные номера телефонов для каждой личности.
- адаптировать свою речь к личности
- снизить вероятность снятия отпечатков браузера

Дополнительные инструменты

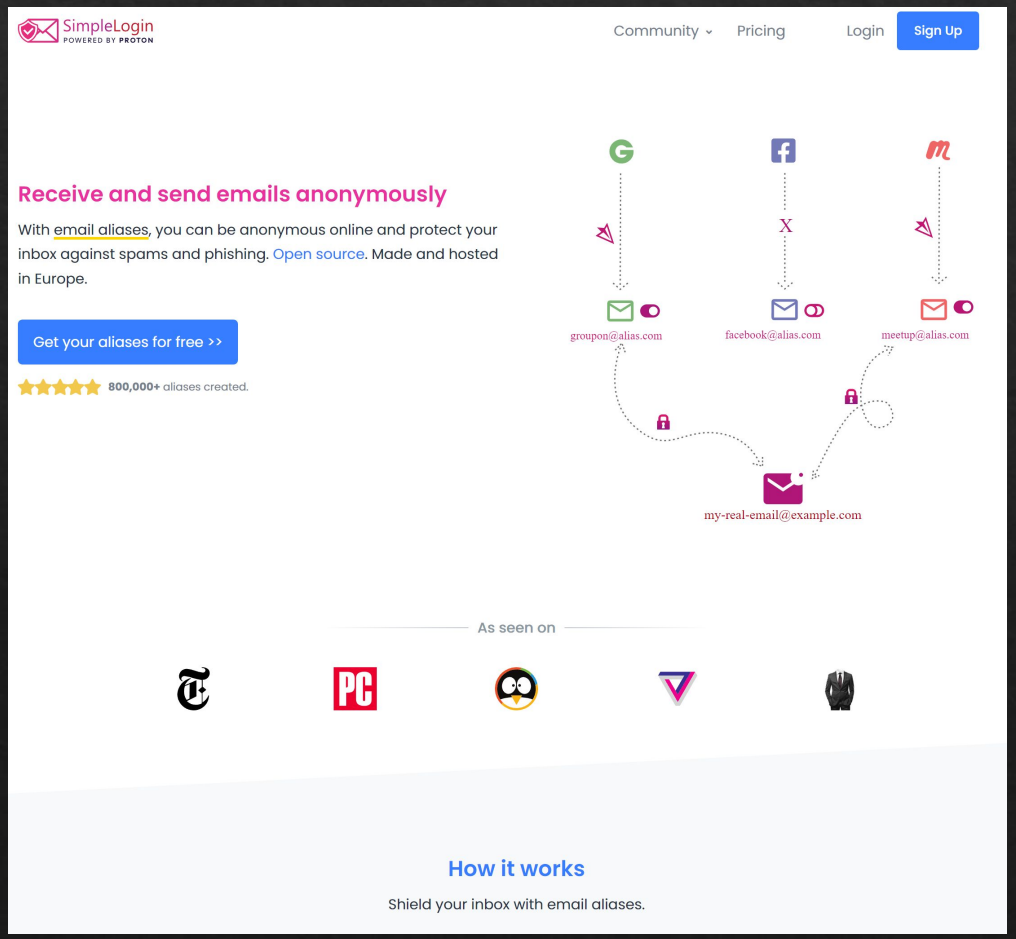
Сервисы для создания личностей:
https://randomdatatools.ru/
https://randus.org/

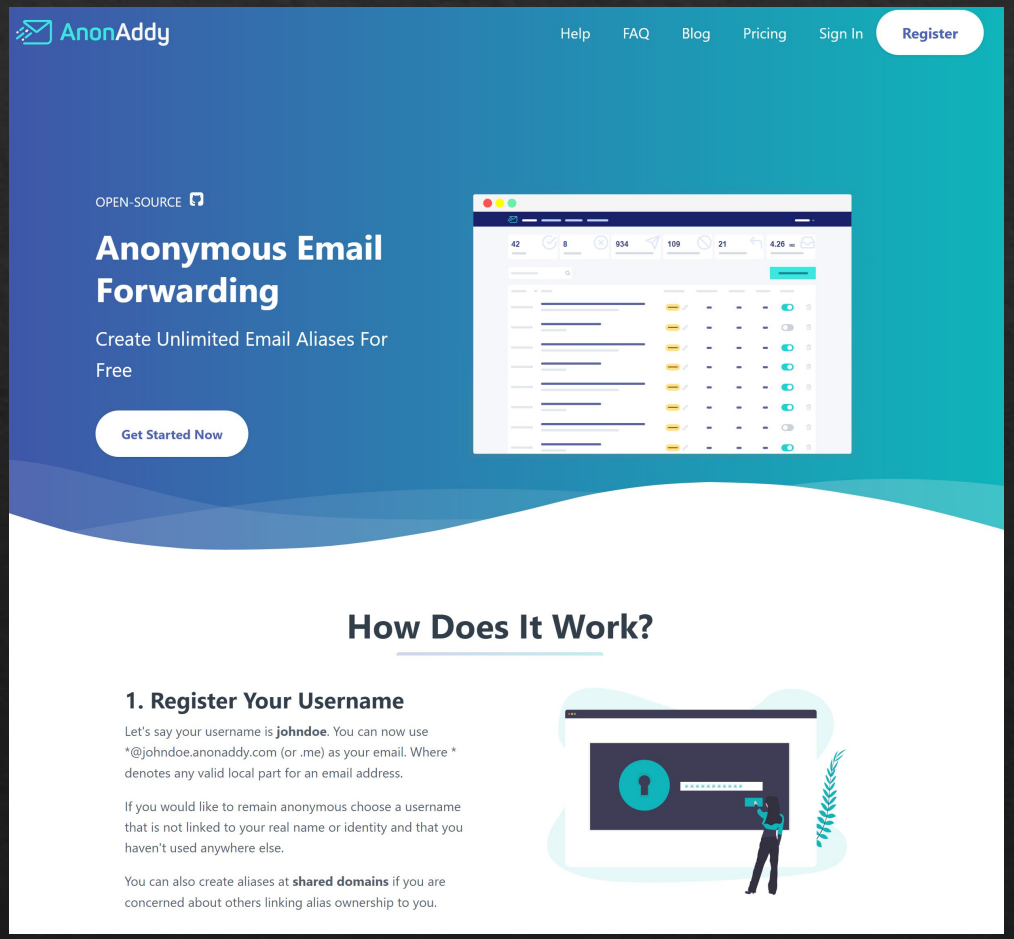




Дополнительные инструменты

Защитить реальный адрес вашей электронной почты можно с помощью следующих сервисов:
https://simplelogin.io/
https://anonaddy.com/





Дополнительные инструменты

Сервисы для поиска геолокации человека:

https://github.com/Alb-310/Geogramint

https://github.com/thewhiteh4t/seeker

https://github.com/Bafomet666/Bigbro

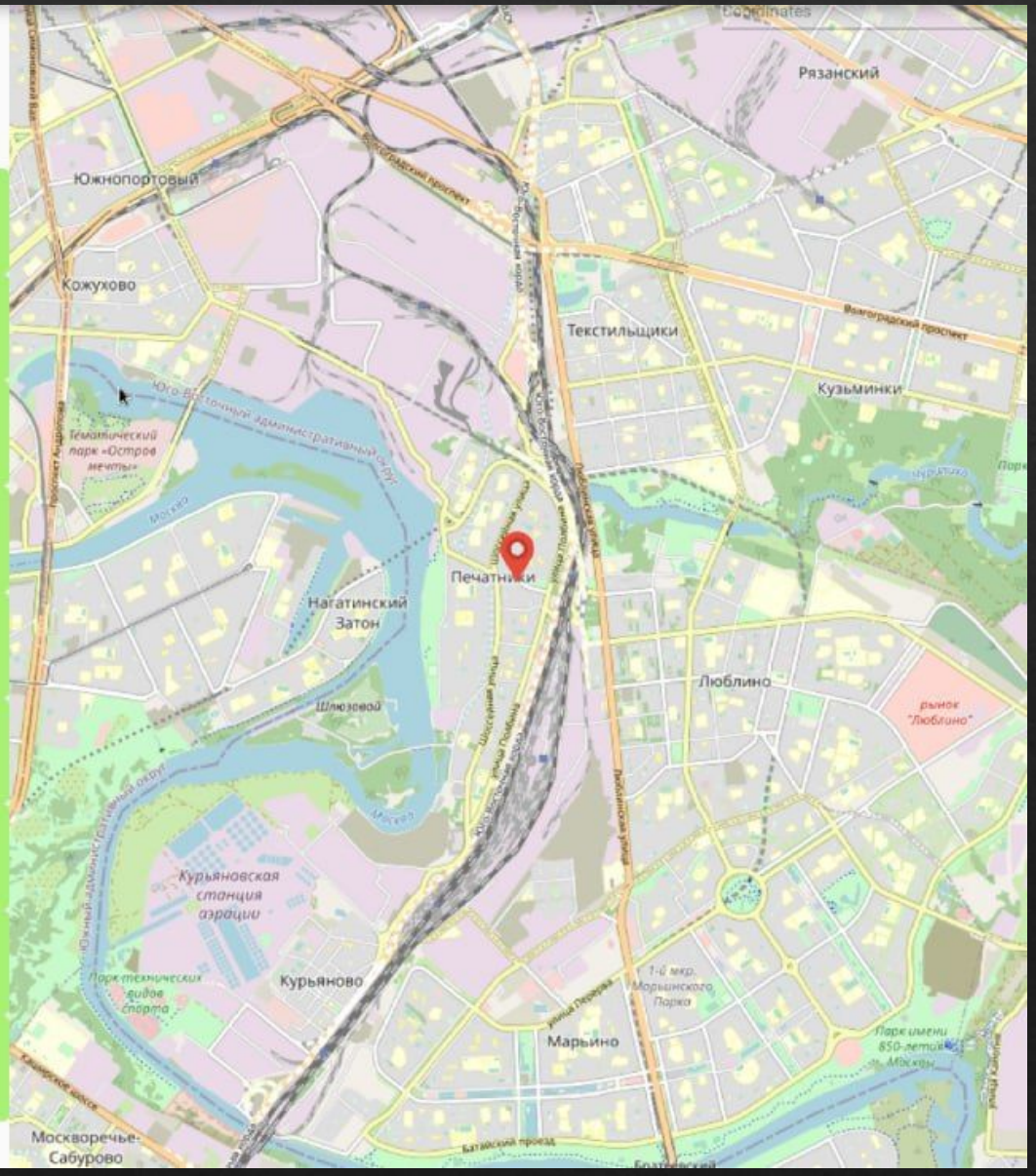
Geogramint

```
└─$ pip3 install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: telethon in /home/aldenteman/.local/lib/python3
.10/site-packages (from -r requirements.txt (line 1)) (1.25.4)
Requirement already satisfied: trio in /home/aldenteman/.local/lib/python3.10/
site-packages (from -r requirements.txt (line 2)) (0.22.0)
Requirement already satisfied: kivy in /home/aldenteman/.local/lib/python3.10/
site-packages (from -r requirements.txt (line 3)) (2.1.0)
Requirement already satisfied: kivymd in /home/aldenteman/.local/lib/python3.1
0/site-packages (from -r requirements.txt (line 4)) (1.1.1)
Requirement already satisfied: kivy-garden in /home/aldenteman/.local/lib/pyth
on3.10/site-packages (from -r requirements.txt (line 5)) (0.1.5)
Requirement already satisfied: mapview in /home/aldenteman/.local/lib/python3.
10/site-packages (from -r requirements.txt (line 6)) (1.0.6)
Requirement already satisfied: rsa in /home/aldenteman/.local/lib/python3.10/s
ite-packages (from telethon->-r requirements.txt (line 1)) (4.9)
Requirement already satisfied: pyaes in /home/aldenteman/.local/lib/python3.10
/site-packages (from telethon->-r requirements.txt (line 1)) (1.6.1)
Requirement already satisfied: sniffio in /usr/lib/python3/dist-packages (from
 trio->-r requirements.txt (line 2)) (1.2.0)
Requirement already satisfied: attrs>=19.2.0 in /home/aldenteman/.local/lib/py
thon3.10/site-packages (from trio->-r requirements.txt (line 2)) (22.1.0)
Requirement already satisfied: async-generator>=1.9 in /home/aldenteman/.local
/lib/python3.10/site-packages (from trio->-r requirements.txt (line 2)) (1.10)
Requirement already satisfied: outcome in /home/aldenteman/.local/lib/python3.
10/site-packages (from trio->-r requirements.txt (line 2)) (1.2.0)
Requirement already satisfied: idna in /home/aldenteman/.local/lib/python3.10/
site-packages (from trio->-r requirements.txt (line 2)) (3.4)
Requirement already satisfied: exceptiongroup>=1.0.0rc9 in /home/aldenteman/.l
ocal/lib/python3.10/site-packages (from trio->-r requirements.txt (line 2)) (1
.0.0rc9)
Requirement already satisfied: sortedcontainers in /usr/lib/python3/dist-packa
ges (from trio->-r requirements.txt (line 2)) (2.4.0)
Requirement already satisfied: docutils in /home/aldenteman/.local/lib/python3
.10/site-packages (from kivy->-r requirements.txt (line 3)) (0.19)
Requirement already satisfied: pygments in /usr/lib/python3/dist-packages (fro
m kivy->-r requirements.txt (line 3)) (2.12.0)
Requirement already satisfied: pillow in /usr/lib/python3/dist-packages (from
kivymd->-r requirements.txt (line 4)) (9.2.0)
Requirement already satisfied: requests in /home/aldenteman/.local/lib/python3
.10/site-packages (from kivy-garden->-r requirements.txt (line 5)) (2.28.1)
Requirement already satisfied: kivy-garden.mapview in /home/aldenteman/.local/
lib/python3.10/site-packages (from mapview->-r requirements.txt (line 6)) (1.0
.6)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in /usr/lib/python3/dist-
```

```
└─$ git clone https://github.com/Alb-310/Geogramint.git
Cloning into 'Geogramint'...
remote: Enumerating objects: 72, done.
remote: Counting objects: 100% (72/72), done.
remote: Compressing objects: 100% (59/59), done.
remote: Total 72 (delta 19), reused 54 (delta 8), pack-reused 0
Receiving objects: 100% (72/72), 2.68 MiB | 109.00 KiB/s, done.
Resolving deltas: 100% (19/19), done.
```

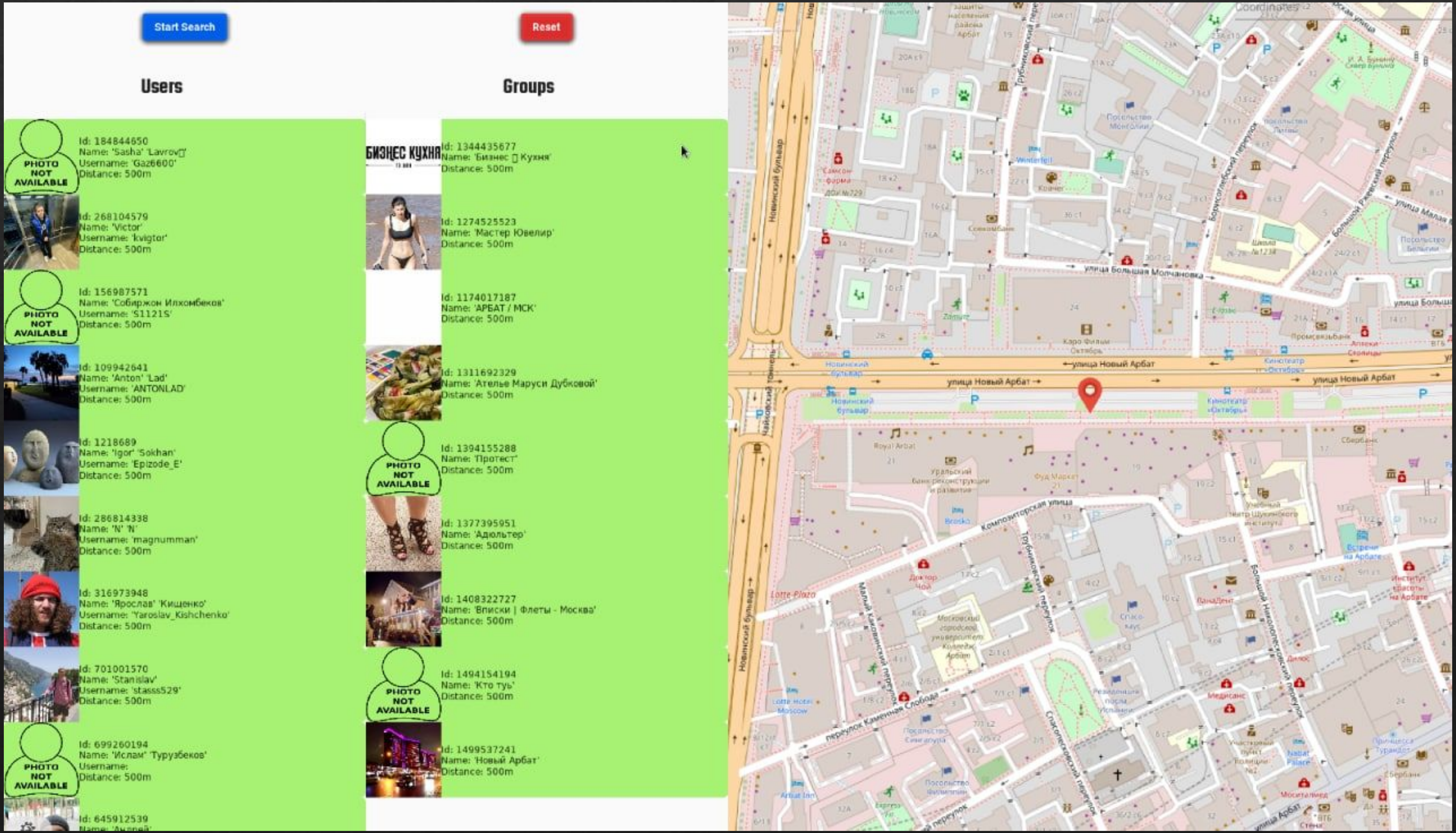
Geogramint


Start Search
Reset
Users
Groups
PHOTO NOT AVAILABLE
Id: 5322067334
Name: 'joxongir.'
Username:
Distance: 500m
Id: 5181439632
Name: 'Chebyrek'
Username:
Distance: 500m
Id: 5117953273
Name: 'Sebuhi' 'Memmedov'
Username:
Distance: 500m
Id: 5080820503
Name: 'E'
Username:
Distance: 500m
Id: 5499790479
Name: 'Luis Miguel' 'Mellet'
Username:
Distance: 500m
Id: 5598021892
Name: '~Hello~'
Username:
Distance: 500m
Id: 445247872
Name: 'I' 'M'
Username: 'Misha7708'
Distance: 500m
Id: 403605249
Name:
Username: 'Hel_91'
Distance: 500m
Id: 385255168
Name: 'Спорт'
Username:
Distance: 500m
Id: 5740514847
Id: 1186996611
Name: 'КЛУБ ЛЮБИТЕЛЕЙ ПРОФЕССИОНАЛЬНОГО МАССАЖА'
Distance: 500m
Id: 1335044942
Name: UYDA QOLING
Distance: 500m
Id: 1215851895
Name: 'Все кому не спится))'
Distance: 500m
Id: 1351045883
Name: 'Люблино'
Distance: 500m
Id: 1184187600
Name: 'Магазин строймаркет'
Distance: 500m
Id: 1226839893
Name: 'ЮВАО'
Distance: 500m
Id: 1237215533
Name: 'Dental'
Distance: 500m
Id: 1525823238
Name: 'Секс Знакомства Люблино'
Distance: 500m
Id: 1175963576
Name: 'Tt'
Distance: 500m


Рязанский
Южнопортовый
Кожухово
Текстильщики
Кузьминки
Печатники
Нагатинский Затон
Люблино
Курьяновская станция аэрации
Курьяново
Марьино
Москворечье-Сабурово

Geogramint

Moscow OSINT meetup №3
Методы анонимизации в Сети:
как искать, но не быть
найденным
@dukera



seeker

```
└─$ git clone https://github.com/thewhiteh4t/seeker.git
Cloning into 'seeker'...
remote: Enumerating objects: 1340, done.
remote: Total 1340 (delta 0), reused 0 (delta 0), pack-reused 1340
Receiving objects: 100% (1340/1340), 3.88 MiB | 50.00 KiB/s, done.
Resolving deltas: 100% (654/654), done.
```

```
ngrok

Visit http://localhost:4040/ to inspect, replay, and modify your requests

Session Status                online
Account                       [redacted] (Plan: Free)
Version                       3.1.0
Region                        Europe (eu)
Latency                       56ms
Web Interface                 http://127.0.0.1:4040
Forwarding                    https://5b7b-79-139-185-167.eu.ngrok.io -> http://localhost:8080

Connections                   ttl     opn     rt1     rt5     p50     p90
                              0       0       0.00    0.00    0.00    0.00
```

```
└─$ ./install.sh
[!] Installing Dependencies...

Python3 - Installed
Pip - Installed
PHP - Installed
Requests - Installed
Packaging - Installed
```

seeker

```
└─$ python3 seeker.py


                  __
  ______  ____  ____ |  | __ ____ _______
 /  ___/ _/ __ \_/ __ \|  |/ /  _ \\_  __ \
 \___ \ \  ___/\  ___/|    <\  ___/ |  | \/
/____  > \___  >\___  >__|_ \ \___  >|__|
     \/      \/     \/     \/     \/

[>] Created By    : thewhiteh4t
 |---> Twitter    : https://twitter.com/thewhiteh4t
 |---> Community  : https://twc1rcle.com/
[>] Version       : 1.2.8

[!] Select a Template :

[0] NearYou
[1] Google Drive
[2] WhatsApp
[3] WhatsApp Redirect
[4] Telegram
[5] Zoom
[6] Google ReCaptcha
[>] 1

[+] Loading Google Drive Template...
[+] Enter GDrive File URL : https://docs.google.com/document/d/1UHMJ8yXxPF9Fwmz4EnNF4nc-SF0fErur/edit?usp=sharing&ouid
=100380009475813962864&rtpof=true&sd=true

[+] Port : 8080

[+] Starting PHP Server...[ ✔ ]

[+] Waiting for Client...[ctrl+c to exit]
```

seeker

```
[+] Starting PHP Server...[ ✔ ]

[+] Waiting for Client...[ctrl+c to exit]

[!] Device Information :

[+] OS          : Android 12
[+] Platform    : Linux aarch64
[+] CPU Cores   : 8
[+] RAM         : 8
[+] GPU Vendor  : ARM
[+] GPU         : Mali-G77
[+] Resolution  : 412x915
[+] Browser     : Chrome/106.0.0.0
[+] Public IP   : [redacted]

[!] IP Information :

[+] Continent : Europe
[+] Country   : Russia
[+] Region    : Moscow
[+] City      : Moscow
[+] Org       : PJSC Moscow city telephone network
[+] ISP       : PJSC Moscow city telephone network

[!] Location Information :

[+] Latitude  : [redacted] deg
[+] Longitude : [redacted] deg
[+] Accuracy  : 15.213000297546387 m
[+] Altitude  : 184 m
[+] Direction : Not Available
[+] Speed     : Not Available

[+] Google Maps : https://www.google.com/maps/place/[redacted]
[+] Data Saved : /home/[redacted]/seeker/db/results.csv

[+] Waiting for Client...[ctrl+c to exit]
```

```
Visit http://localhost:4040/ to inspect, replay, and modify your requests

Session Status                online
Account                       [redacted] (Plan: Free)
Version                       3.1.0
Region                        Europe (eu)
Latency                       53ms
Web Interface                 http://127.0.0.1:4040
Forwarding                    https://5b7b-79-139-185-167.eu.ngrok.io -> http://localhost:8080

Connections                   ttl     opn     rt1     rt5     p50     p90
                              1       0       0.01    0.00    0.00    0.00
```

Bigbro

```
Выберите версию для запуска

( 1 ) Termux

( 2 ) Desktop

( 3 ) Идти нахуй из инструмента

( 4 ) Получить полную версию

└─> Bafomёd production ──> Введите номер опции:
```

```
Тайна это безопасность, а безопасность это победа

 _______  __                  _______
|       \ |  \                |       \
| $$$$$$$\ \$$  _______      | $$$$$$$\  ______   ______
| $$__/ $$|  \ /       \     | $$__/ $$ /      \ /      \
| $$    $$| $$|  $$$$$$$\    | $$    $$|  $$$$$$\|  $$$$$$\
| $$$$$$$\| $$| $$  | $$     | $$$$$$$\| $$   \$$| $$  | $$
| $$__/ $$| $$| $$__| $$     | $$__/ $$| $$      | $$__/ $$
| $$    $$| $$ \$$    $$     | $$    $$| $$       \$$    $$
 \$$$$$$$  \$$ _\$$$$$$$      \$$$$$$$  \$$        \$$$$$$
               |  \__| $$
                \$$    $$
                 \$$$$$$

Новая архетиктура x0com, big brother 13.0

Скачать полную версию framework: https://t.me/osint_san_framework

[ 1 ]  Nearyou          [ 11 ]  Блогер рядом       [ 21 ]  Друг вокруг       [ 31 ]  Свободный
[ 2 ]  Погода           [ 12 ]  Курсы Skillbox     [ 22 ]  Биржа bitcoin     [ 32 ]  Свободный
[ 3 ]  Hostel           [ 13 ]  Лучшее свидание    [ 23 ]  Каршеринг авто    [ 33 ]  Свободный
[ 4 ]  Авиабилеты       [ 14 ]  Ближ фотограф      [ 24 ]  Portugal друзья   [ 34 ]  Свободный
[ 5 ]  YouTube          [ 15 ]  Premium ngrok      [ 25 ]  Свободный         [ 35 ]  Свободный
[ 6 ]  Почта РФ         [ 16 ]  Знакомства, секс   [ 26 ]  Свободный         [ 36 ]  Свободный
[ 7 ]  Telegram         [ 17 ]  Флирт в регионе    [ 27 ]  Свободный         [ 37 ]  Свободный
[ 8 ]  Проститундер     [ 18 ]  Туризм, отдых      [ 28 ]  Свободный         [ 38 ]  Свободный
[ 9 ]  Fast Jobs        [ 19 ]  Ближайший ресторан [ 29 ]  Свободный         [ 39 ]  Свободный
[ 10 ] Bitcoin          [ 20 ]  Игра " Тайга "     [ 30 ]  Свободный         [ 40 ]  Свободный

[ 0 ]  Покинуть

------------------------------------------------------------

└─> Bafomёd production ──> Введите номер сайта: 12
t=2022-10-21T14:21:10-0400 lvl=warn msg="can't bind default web address, trying alternatives" obj=web addr=127.0.0.1:4
040
------------------------------------------------------------------------------

Функция ловли долбаебов переходящих по ссылкам запущена, выбранный сайт активирован.

https://1648-79-139-185-167.ngrok.io -> https://localhost:8767

Отправте ссылку жертве ...
```

Bigbro

abe4-79-139-185-167.eu.ngrok.io/#team

...ngrok.io запрашивает разрешение на:

доступ к данным о вашем местоположении

Разрешить Блокировать

```
----------------------------------------------------------

└──> Bafomёd production ──> Введите номер сайта: 12
t=2022-10-21T14:34:57-0400 lvl=warn msg="can't bind default web address, trying alternatives" obj=web addr=127.0.0.1:4
040
 ----------------------------------------------------------------------------

Функция ловли долбаебов переходящих по ссылкам запущена, выбранный сайт активирован.

https://8606-79-139-185-167.ngrok.io -> https://localhost:8767

Отправте ссылку жертве ...

                Жертва попалась

IP address жертвы    :   [redacted]
Операционная система :   Windows
Версия системы       :   10
Количество ядер      :   4
Название браузера    :   Chrome
Версия Браузера      :   106.0.0.0
Архитектура ЦП       :   amd64
Разрешение экрана    :   2560x1440
Временная зона       :   Москва, стандартное время
Язык системы         :   ru-RU

Отлично, теперь ждем когда цель нажмет на любую кнопку на сайте


Координаты цели: Широта - [redacted] Долгота - [redacted]

https://www.google.com/maps/place/[redacted]

Сайты с геолокацией открыты
```

OSINT CTF

M. Mainz, биолог

Имя и фамилия

Возраст

Место жительства (страна, город)

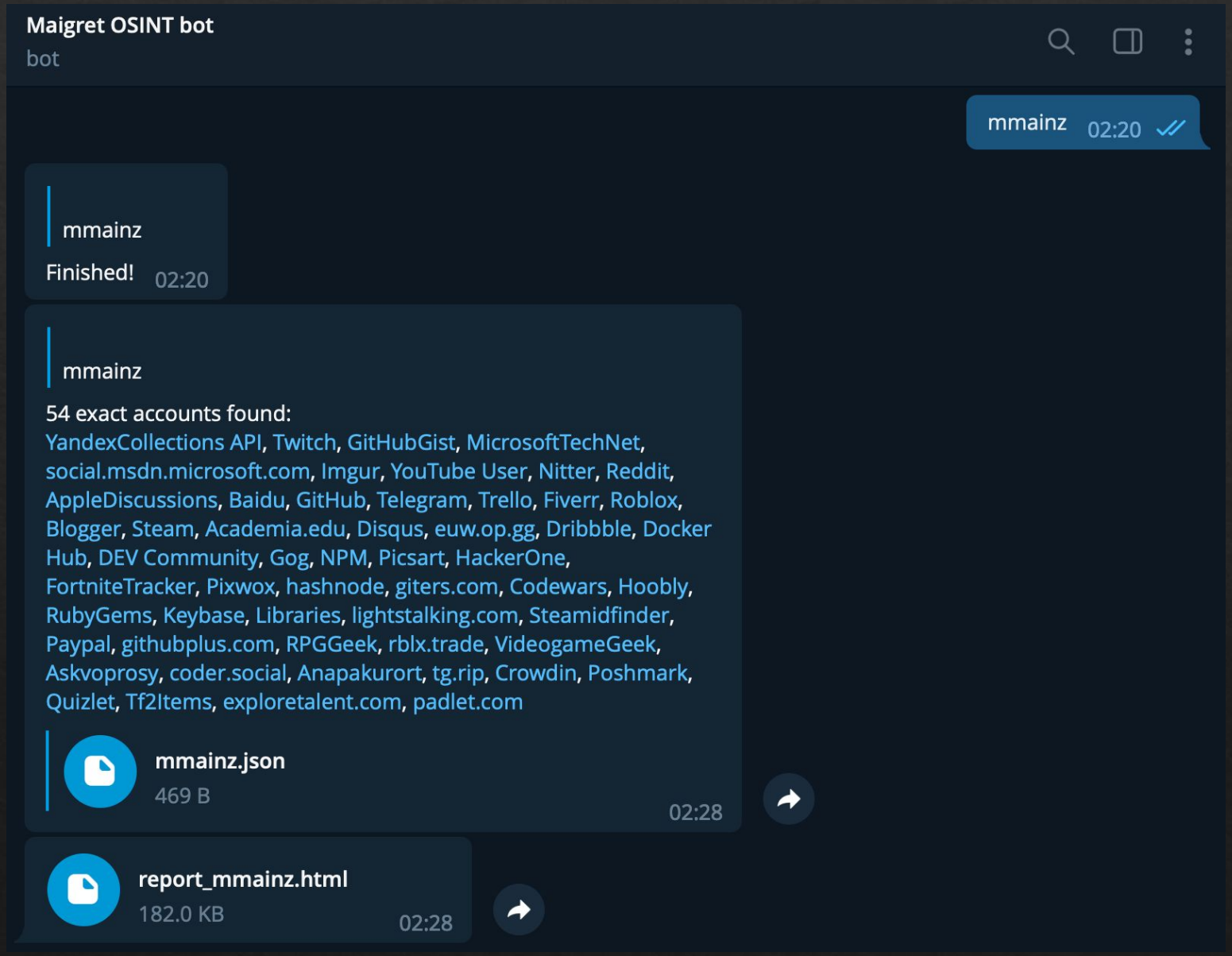
Место работы и должность

Цвет глаз

Номер телефона

Недавние путешествия

Разбор OSINT CTF



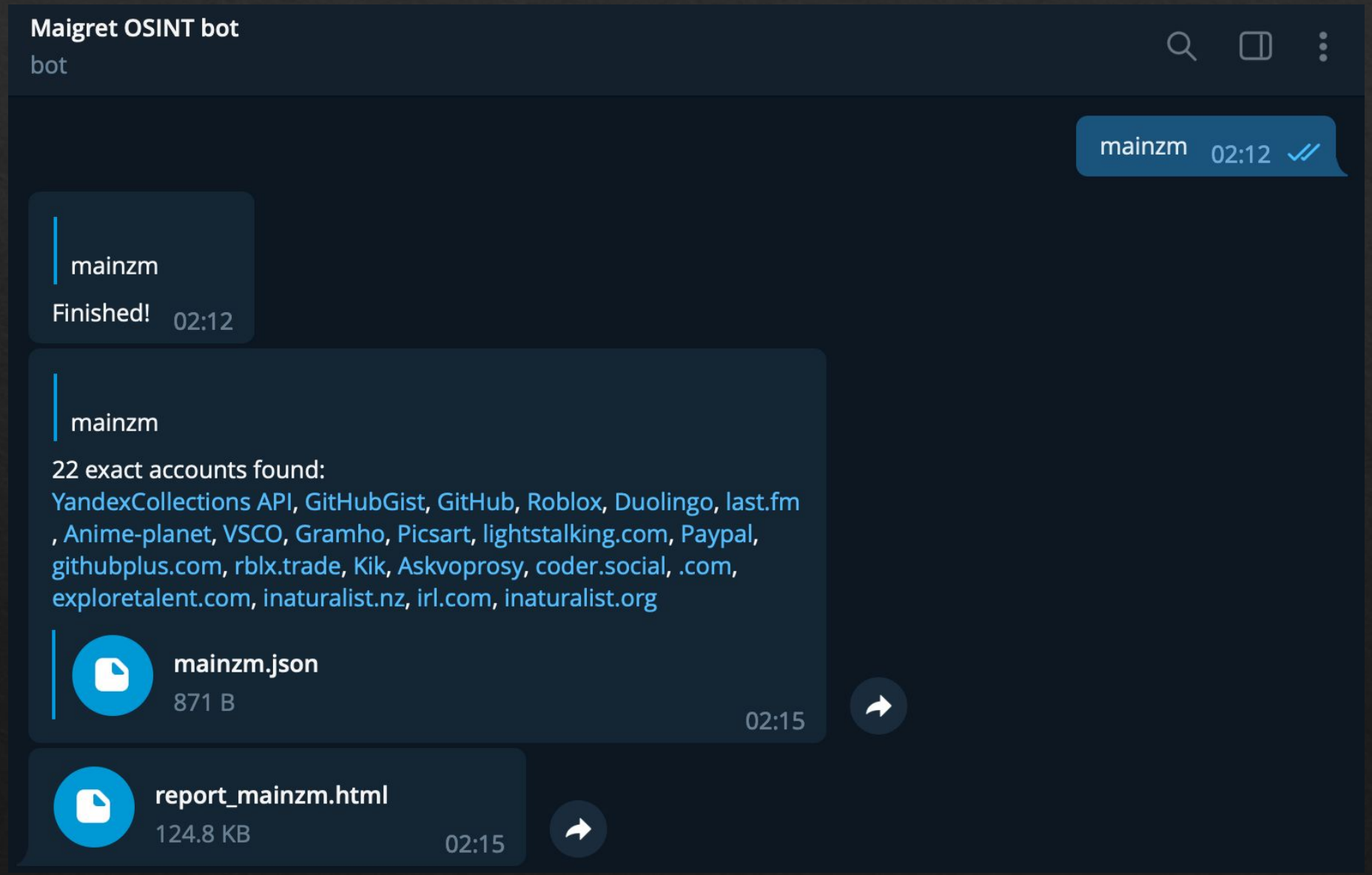
Можно предположить, что “M.” это первая буква имени, а “Mainz” это фамилия.

Для начала возьмем несколько самых очевидных возможных никнеймов:

mmainz
mainzm
mainz
m.mainz
mainz.m

Воспользуемся инструментом maigret (https://github.com/soxoj/maigret) для определения на каких сайтах зарегистрирован каждый никнейм.

Разбор OSINT CTF



Разбор OSINT CTF

Moscow OSINT meetup №3
Методы анонимизации в Сети:
как искать, но не быть
найденным
@dukera

Maigret OSINT bot
bot

mainz 02:29

mainz

Finished! 02:29

mainz

223 exact accounts found:
YandexCollections API, GitHubGist, Twitch, Naver, My.Mail.ru@mail.ru, YouTube User, Reddit, WordPress, Imgur, MicrosoftTechNet, Nitter, social.msdn.microsoft.com, AppleDiscussions, Baidu, GitHub, SoundCloud, Slack, CNET, linktr.ee, Behance, Pinterest, Pornhub, Roblox, Zhihu, Blogger, Rutracker, Mozilla Support, opensea.io, Issuu, Freelancer.com, Championat, Disqus, giphy.com, MyAnimeList, Redtube, Discogs, Eksisozluk, note, Ameba, 123rf, Ultimate-Guitar, Pikabu, sports.ru, Kaskus, Myspace, Dribbble, drive2, Plurk, Windy, Pastebin, Ccm, Lichess, profile.hatena.ne.jp, Pathofexile, BodyBuilding, Wykop, Codecademy, ArchiveOfOurOwn, Docker Hub, MixCloud, Warrior Forum, last.fm, 999.md, Thechive, BitBucket, amp.flipboard.com, Itch.io, AdultFriendFinder, jeuxvideo, Flipboard, ImgInn, Sporcle, Gog, banki.ru, Gitee, Newgrounds, Boarc
https://mainz.itch.io/
Anime-planet, IFTTT, Pokemon Showdown

mainz.json
869 B
02:36 👍

mainz

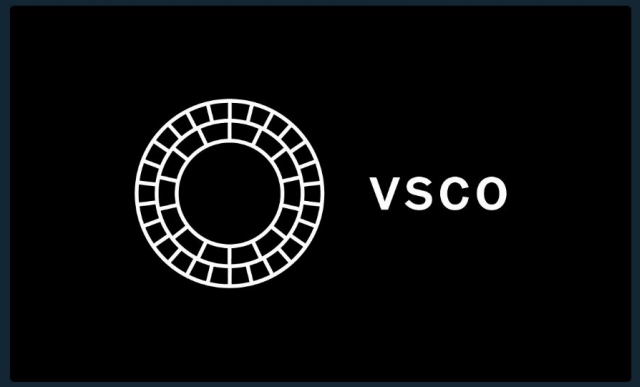
, VSCO, kwork, Typeracer, About.me, Gramho, Computerbase, Picsart, FortniteTracker, Freesound, ProductHunt, 3ddd, Proza.ru, TheSimsResource, Pixwox, Smule, Pbase, interpals, Giantbomb, Picarto, InfosecInstitute, Armorgames, DigitalPoint, Folkd, Launchpad, Ariva, forums.digitalpoint.com, Dumpor, Etxt, geocaching, DonationsAlerts, couchsurfing, igromania, Kinja, Shikimori, Star Citizen, E621, YouNow, imgsrc.ru, Hoobly, ProtonMail

Maigret OSINT bot
bot

mainz

, VSCO, kwork, Typeracer, About.me, Gramho, Computerbase, Picsart, FortniteTracker, Freesound, ProductHunt, 3ddd, Proza.ru, TheSimsResource, Pixwox, Smule, Pbase, interpals, Giantbomb, Picarto, InfosecInstitute, Armorgames, DigitalPoint, Folkd, Launchpad, Ariva, forums.digitalpoint.com, Dumpor, Etxt, geocaching, DonationsAlerts, couchsurfing, igromania, Kinja, Shikimori, Star Citizen, E621, YouNow, imgsrc.ru, Hoobly, ProtonMail, Coroflot, Weblancer, Jetpunk, Datpiff, TruckersMP.com, Tripster, Mpgh, MeetMe, ICQ, Tellonym.me, Bookcrossing, 7Cups, Periscope, Djagi, Libraries, 4gameforum, Sprashivai, Dating.Ru, WOW Circle, Tripline, Steamidfinder, lightstalking.com, monitoringminecraft.ru, free-otvet.ru, 21buttons, F3.cool, Niketalk, elibrary.tips, Cmet4uk, Paypal, RPGGeek, Chpoking, SportsTracker, githubplus.com, Root-me, www.kinokopilka.pro, jAlbum.net, ProfilesTigweb

VSCO®
Page Not Found
Launching soon

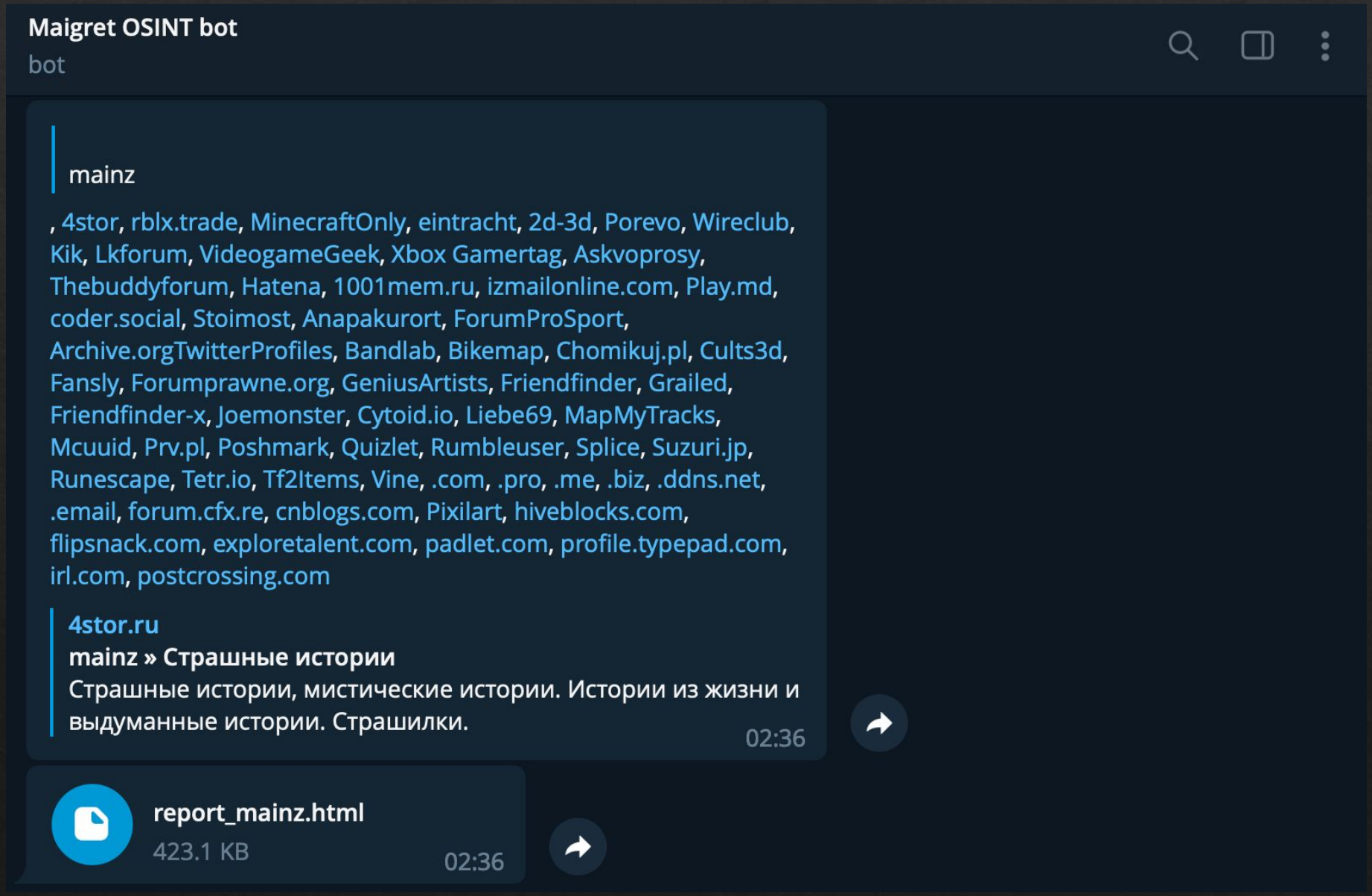


02:36

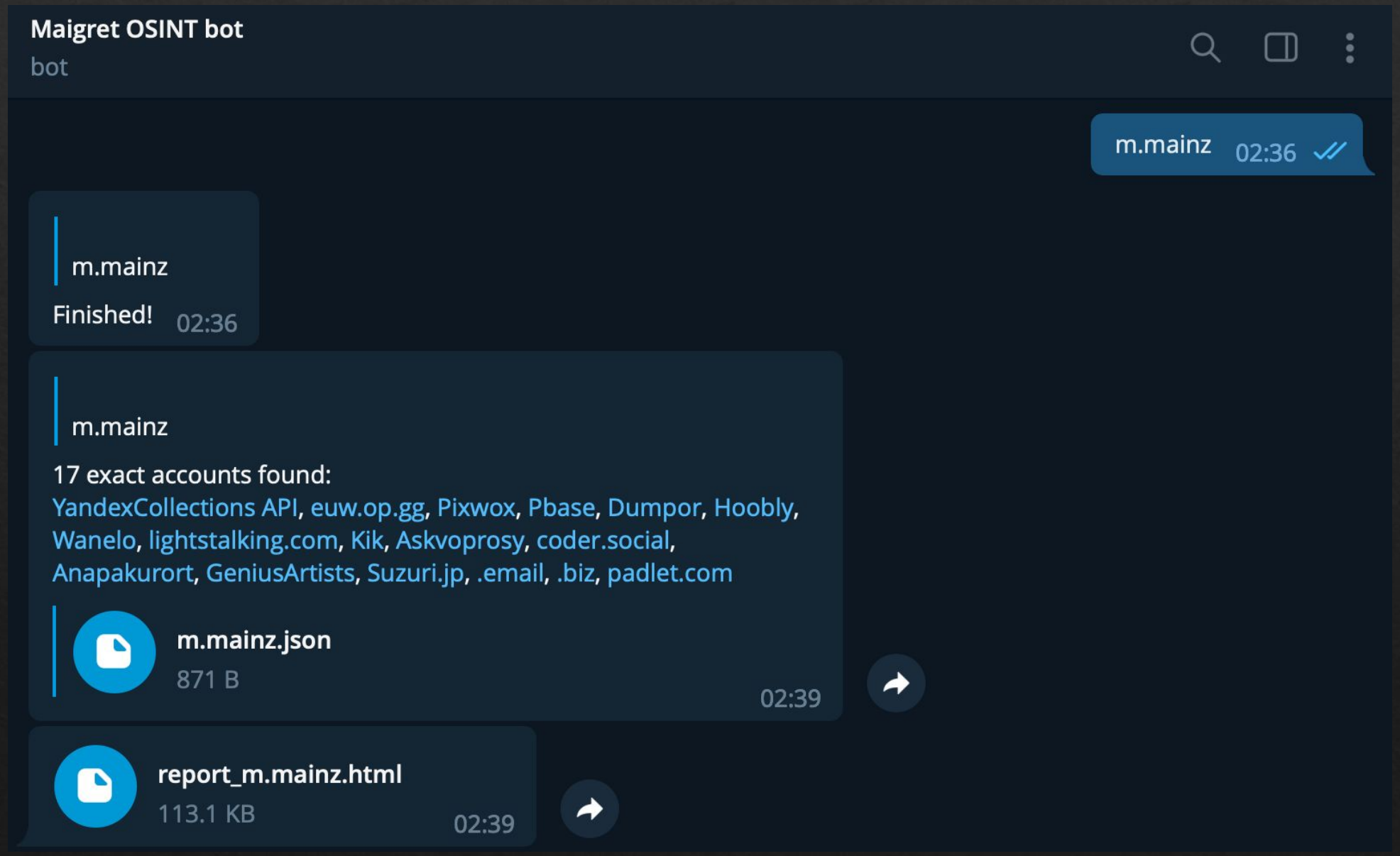
mainz

, 4stor, rblx.trade, MinecraftOnly, eintracht, 2d-3d, Porevo, Wireclub,

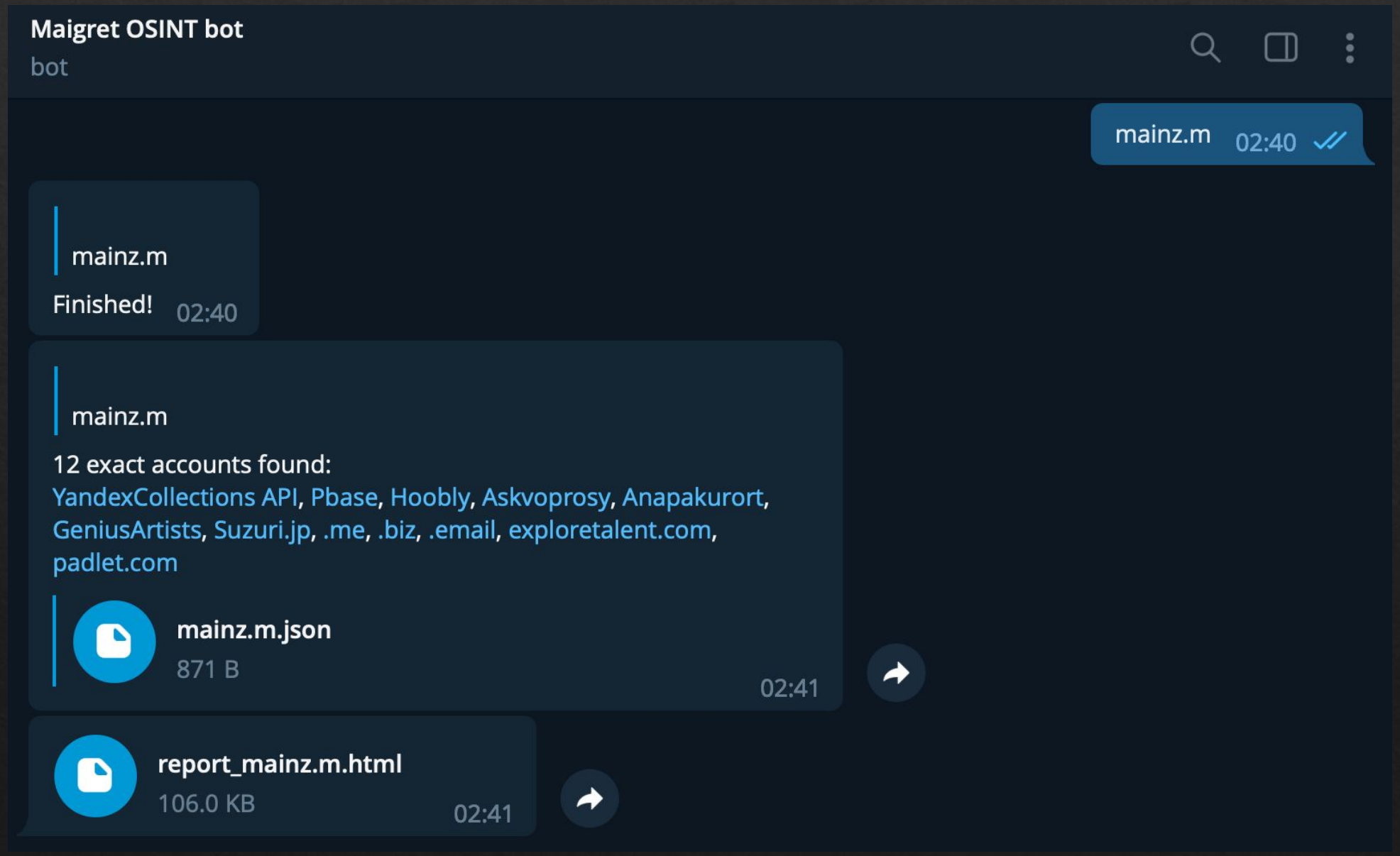
Разбор OSINT CTF



Разбор OSINT CTF

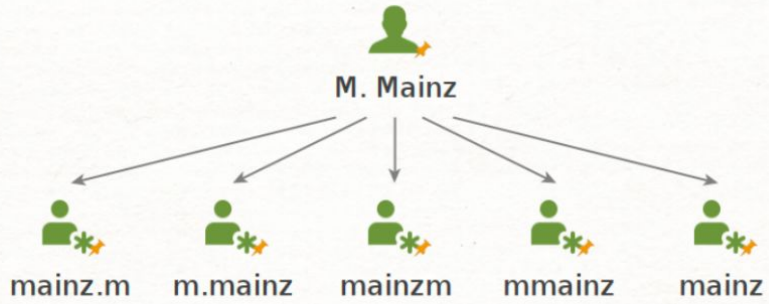


Разбор OSINT CTF



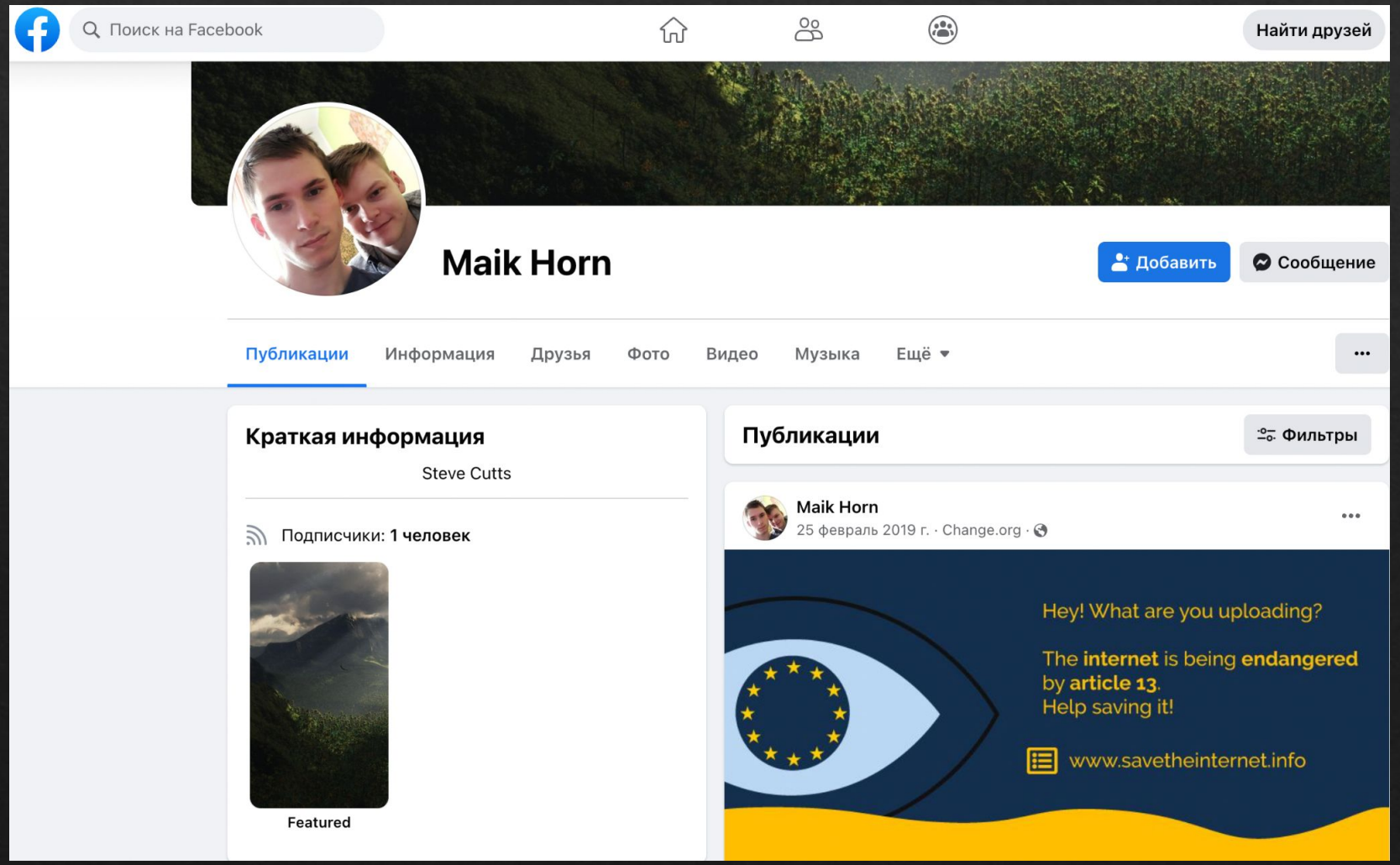
Разбор OSINT CTF

Будем систематизировать полученные данные в программе maltego. Перебрав все псевдонимы, вариант mainzm дал наиболее реалистичные результаты, его и будем рассматривать.



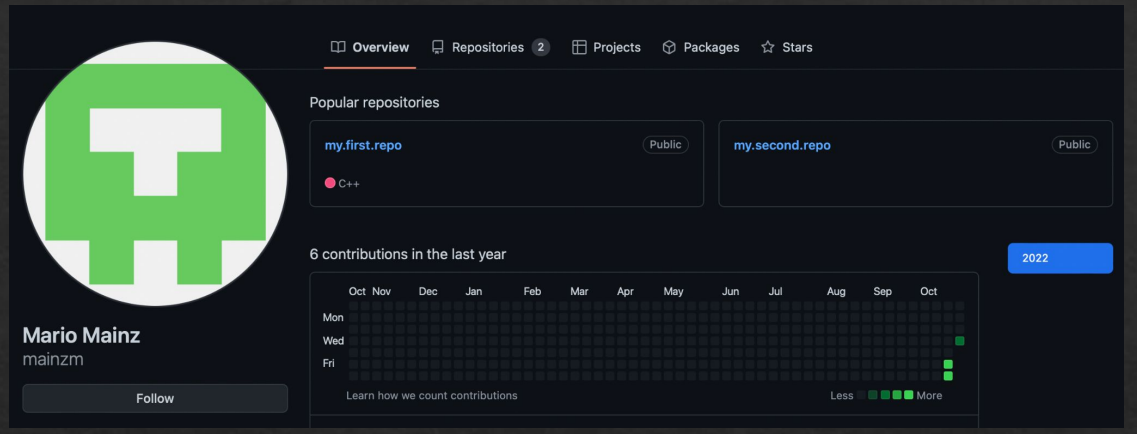
Разбор OSINT CTF

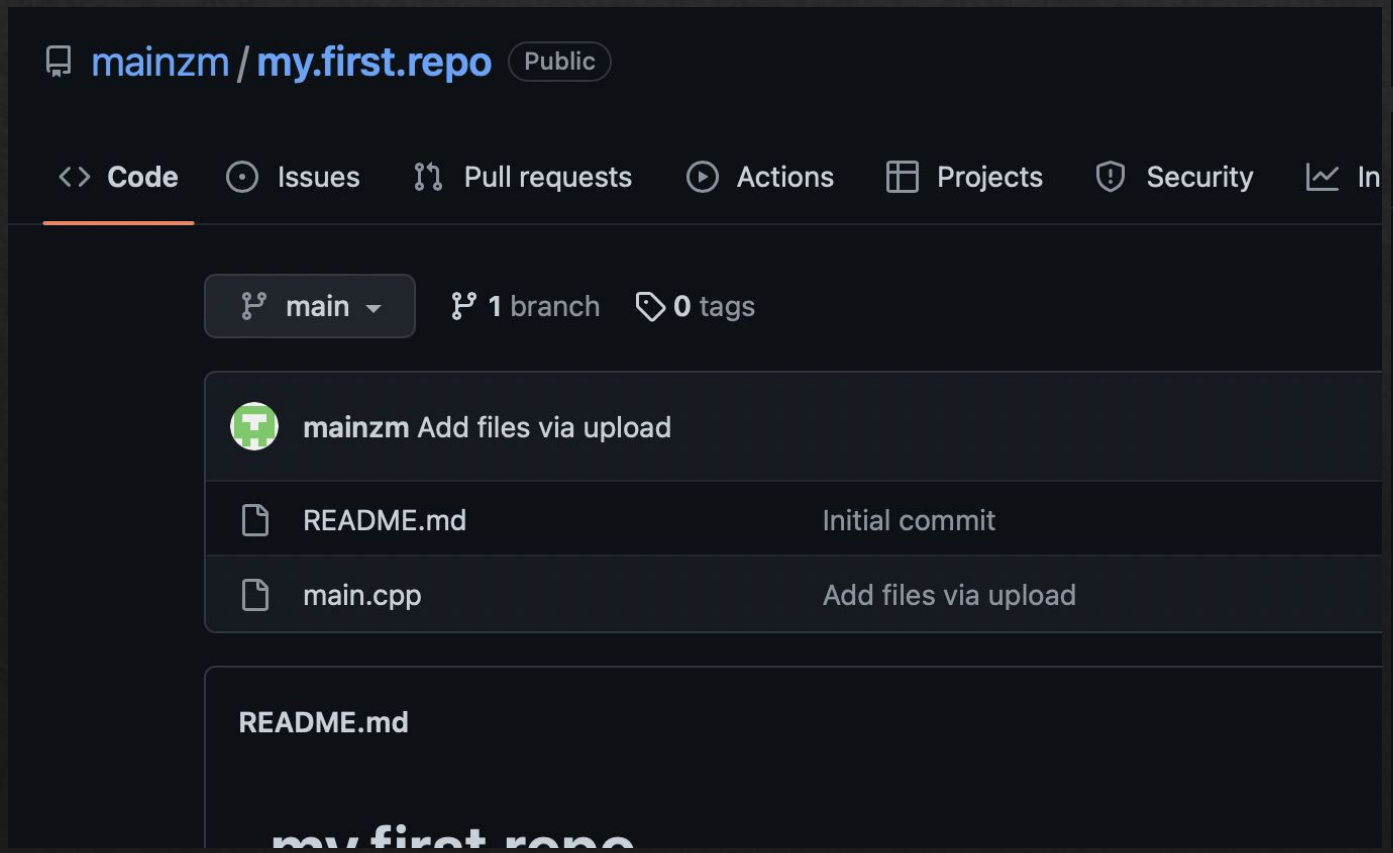
Если перейти по ссылке на Facebook (https://www.facebook.com/mainzm) то увидим человека с именем Maik Horn. На M. Mainz не очень похоже.

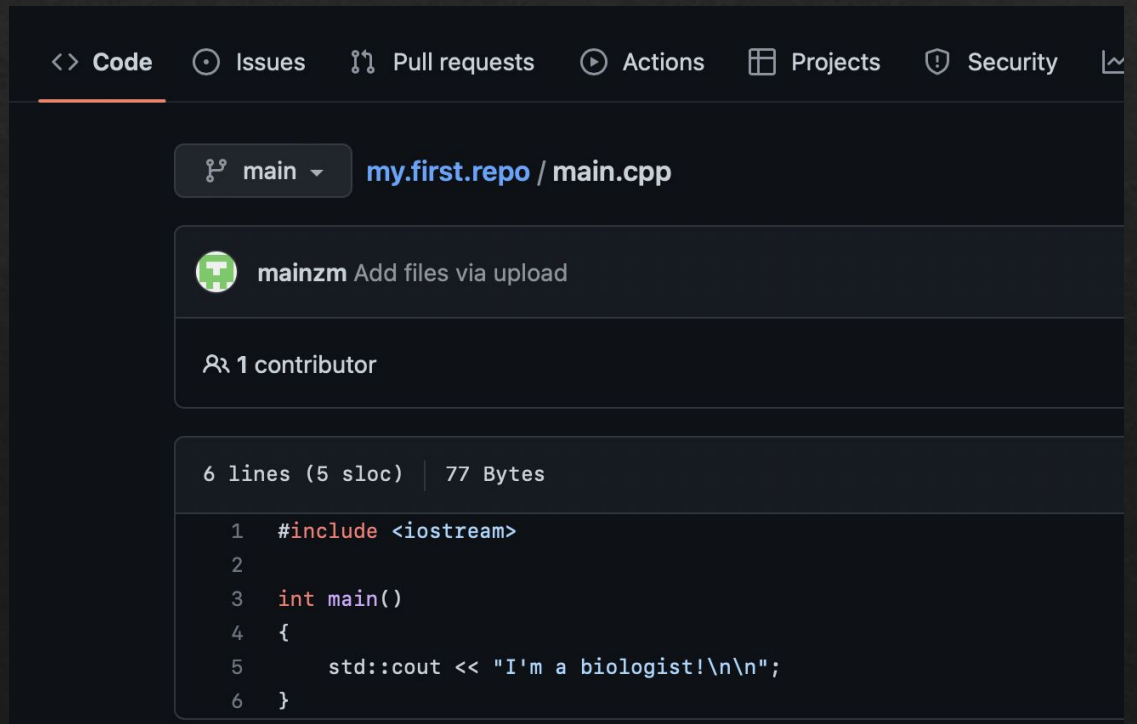


Разбор OSINT CTF

Проверим Github. Имя и фамилия владельца Mario Mainz. В репозитории my.first.repo есть файл main.cpp с программой. В программе нас ждет приятная подсказка, которая говорит о правильности выбранного пути.

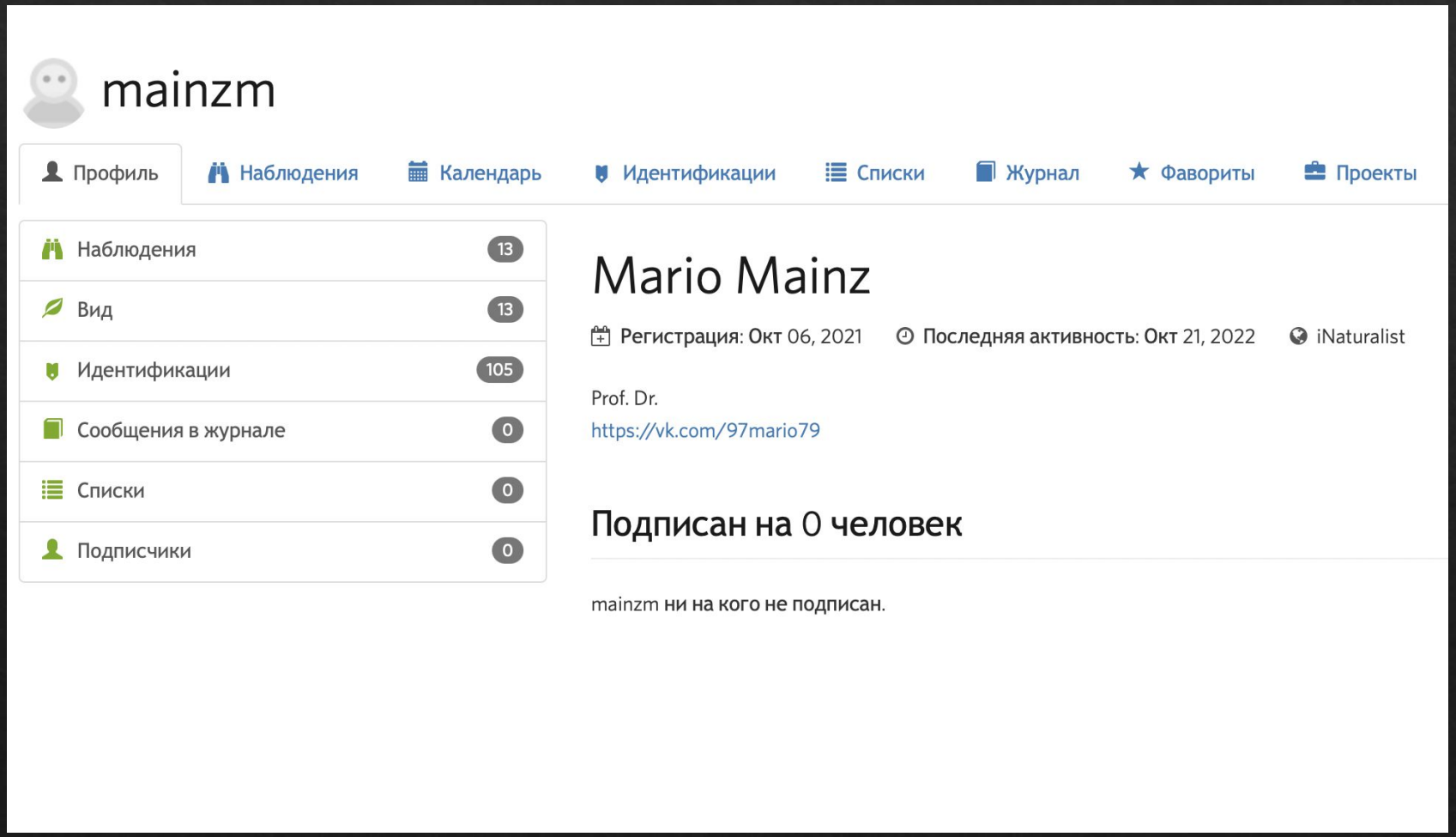






Разбор OSINT CTF

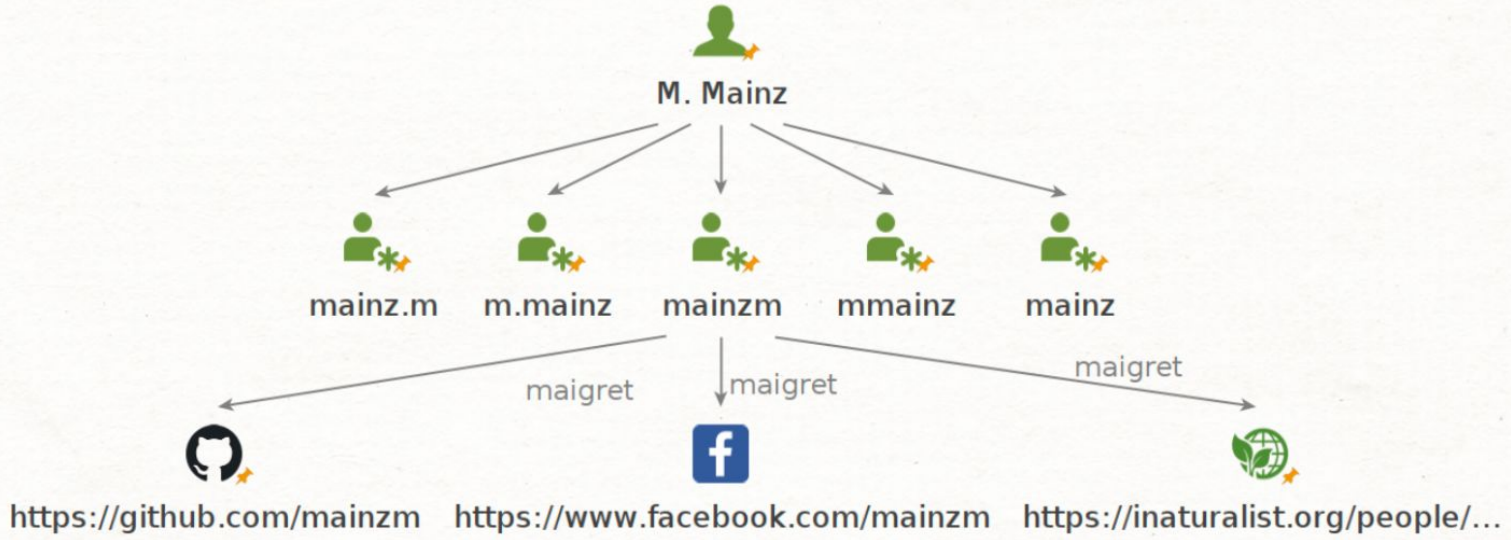
Заметим, что mainzm - единственный никнейм, который имеет профиль на сайте iNaturalist. Это социальная сеть для учёных-биологов и всех заинтересованных, созданная для картографирования и описания наблюдений за биоразнообразием Земли.



Видим Mario Mainz, а также должность и ученую степень нашего незнакомца - профессор, доктор.

В профиле прикреплена ссылка на страницу ВКонтакте.

Разбор OSINT CTF



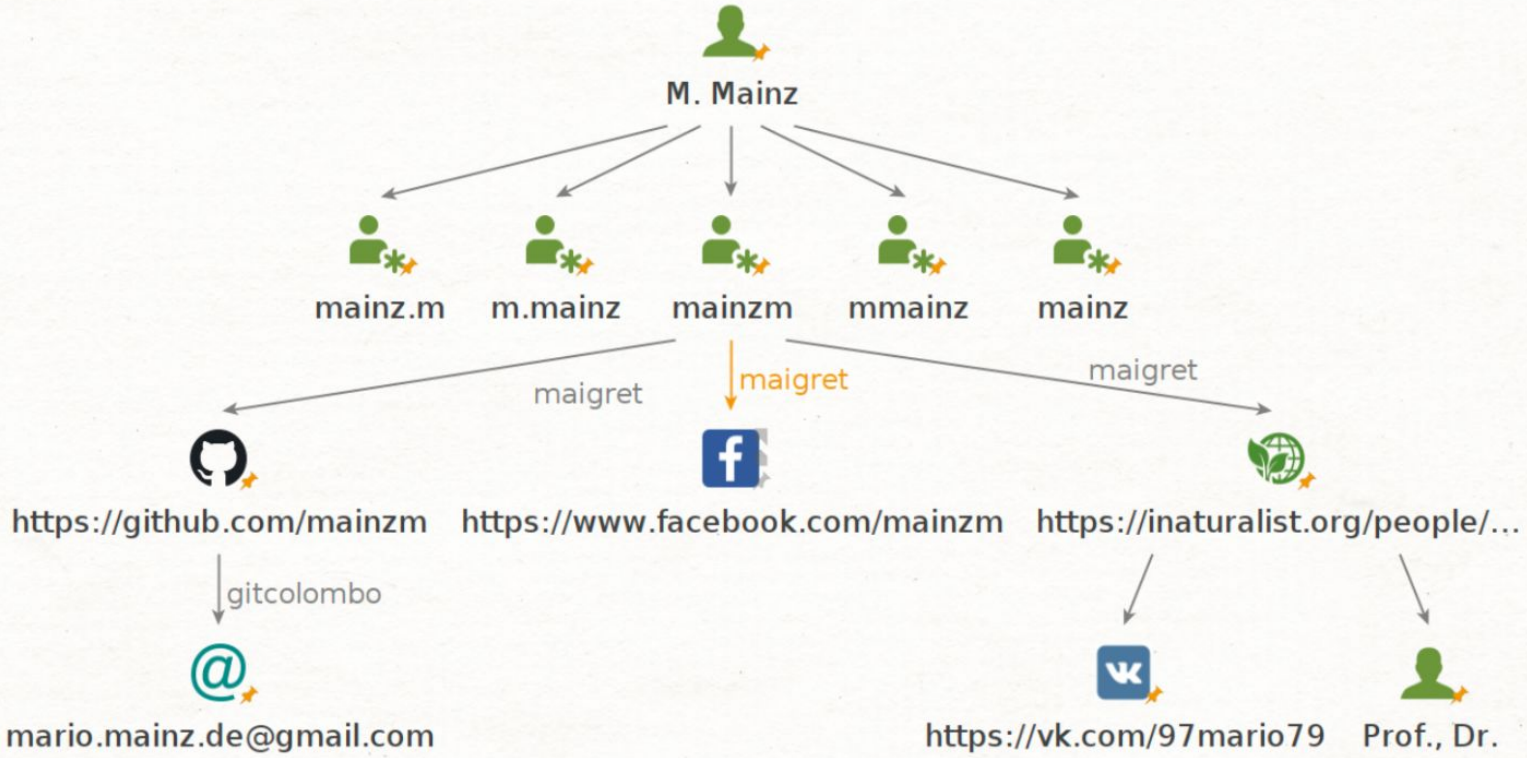
Разбор OSINT CTF

Воспользуемся gitcolombo (https://github.com/soxoj/gitcolombo) и проанализируем репозиторий. Таким образом, получим почту: mario.mainz.de@gmail.com

kali@kali: ~ | kali@kali: ~/gitcolombo

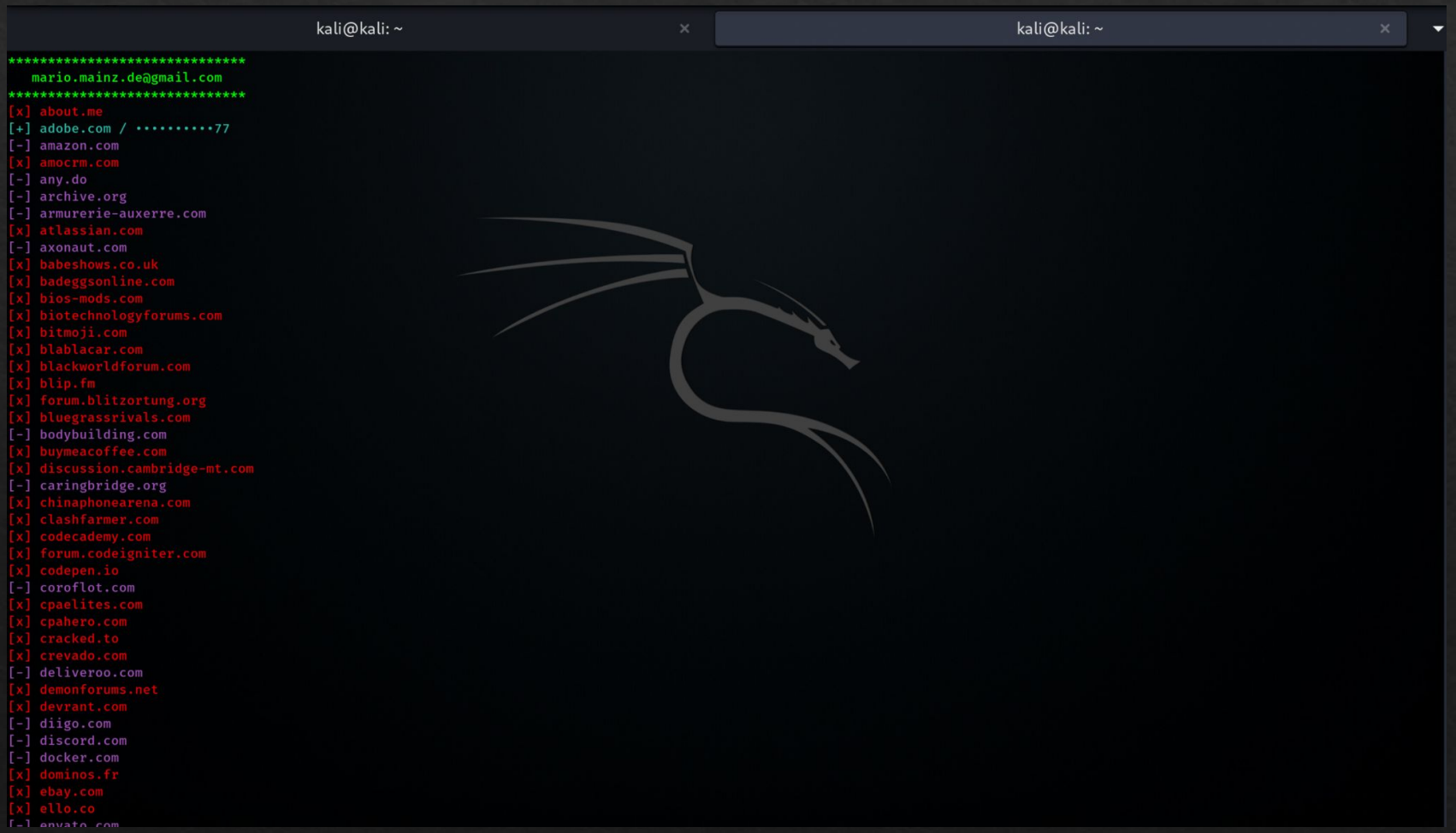
```
┌──(kali㉿kali)-[~/gitcolombo]
└─$ ./gitcolombo.py -u https://github.com/mainzm/my.first.repo
Cloning into 'my.first.repo'...
remote: Enumerating objects: 6, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 6 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (6/6), done.
----------------------------------------
INFO: Resolving GitHub usernames, please wait...
Analyze of the git repo(s) "my.first.repo"
Verbose persons info:
---------------
Name:                   Mario Mainz
Email:                  mario.mainz.de@gmail.com
Appears as author:      1 times
Verified account:
                        https://github.com/mainzm
Also appears with:
                        GitHub noreply@github.com
---------------
Name:                   Mario Mainz
Email:                  116330840+mainzm@users.noreply.github.com
Appears as author:      1 times
Verified account:
                        https://github.com/mainzm
Also appears with:
                        GitHub noreply@github.com
---------------
Name:                   GitHub
Email:                  noreply@github.com
Appears as committer:   2 times
Also appears with:
                        Mario Mainz mario.mainz.de@gmail.com
                        Mario Mainz 116330840+mainzm@users.noreply.github.com

Matching info:
---------------
Mario Mainz is the owner of emails:
                        116330840+mainzm@users.noreply.github.com
                        mario.mainz.de@gmail.com

Statistics info:
---------------
Total persons: 3
```

Разбор OSINT CTF



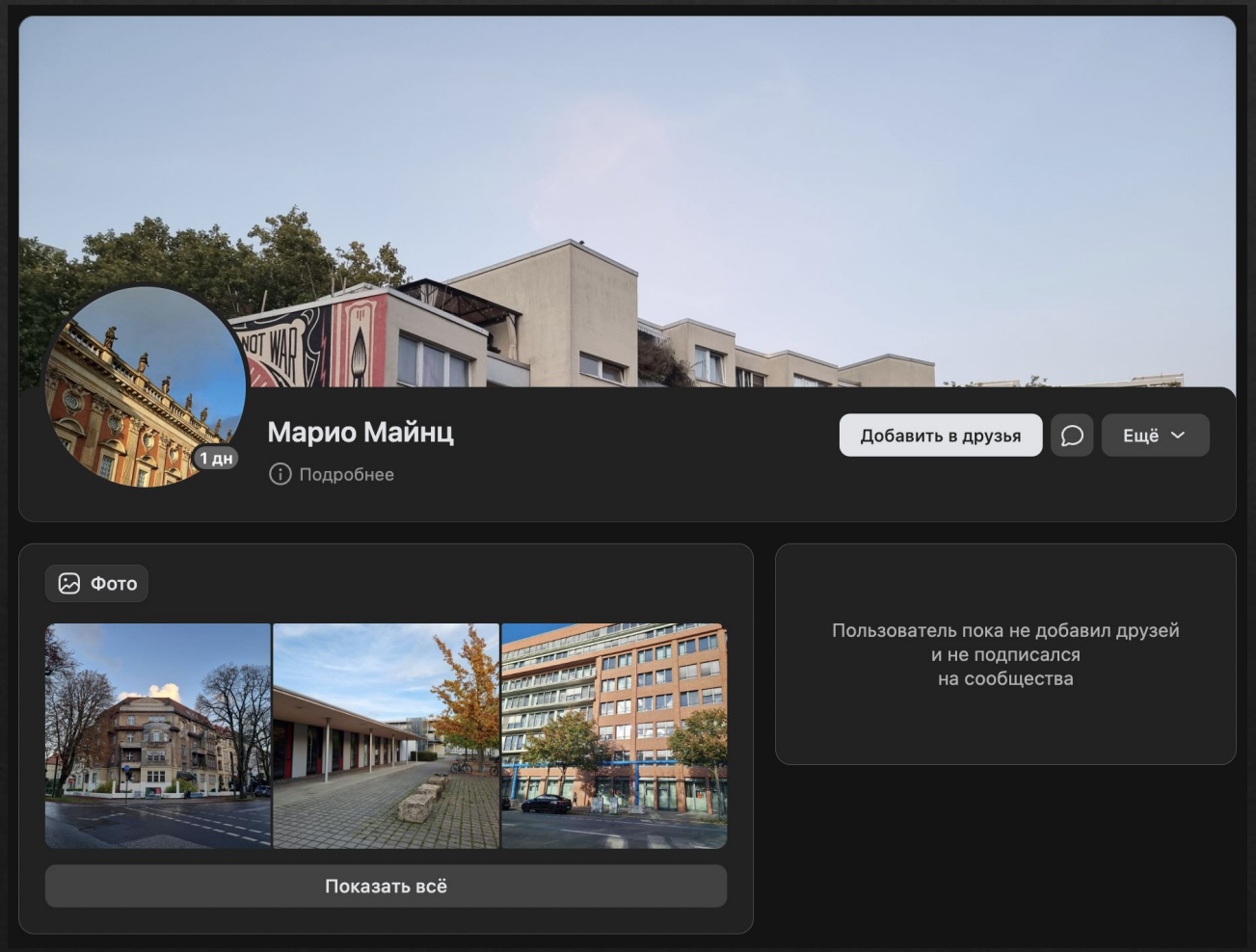
Разбор OSINT CTF

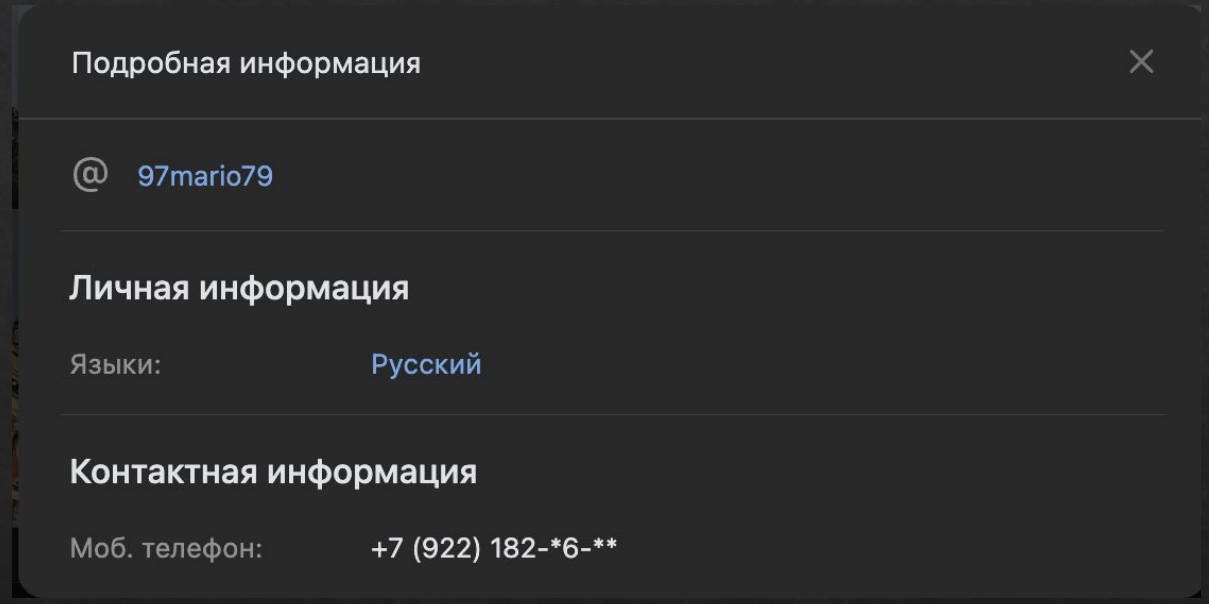
Воспользуемся инструментом holehe (https://github.com/megadose/holehe), чтобы узнать, где полученный нами email адрес зарегистрирован. С сайта adobe.com получаем две последние цифры номера телефона.



Разбор OSINT CTF

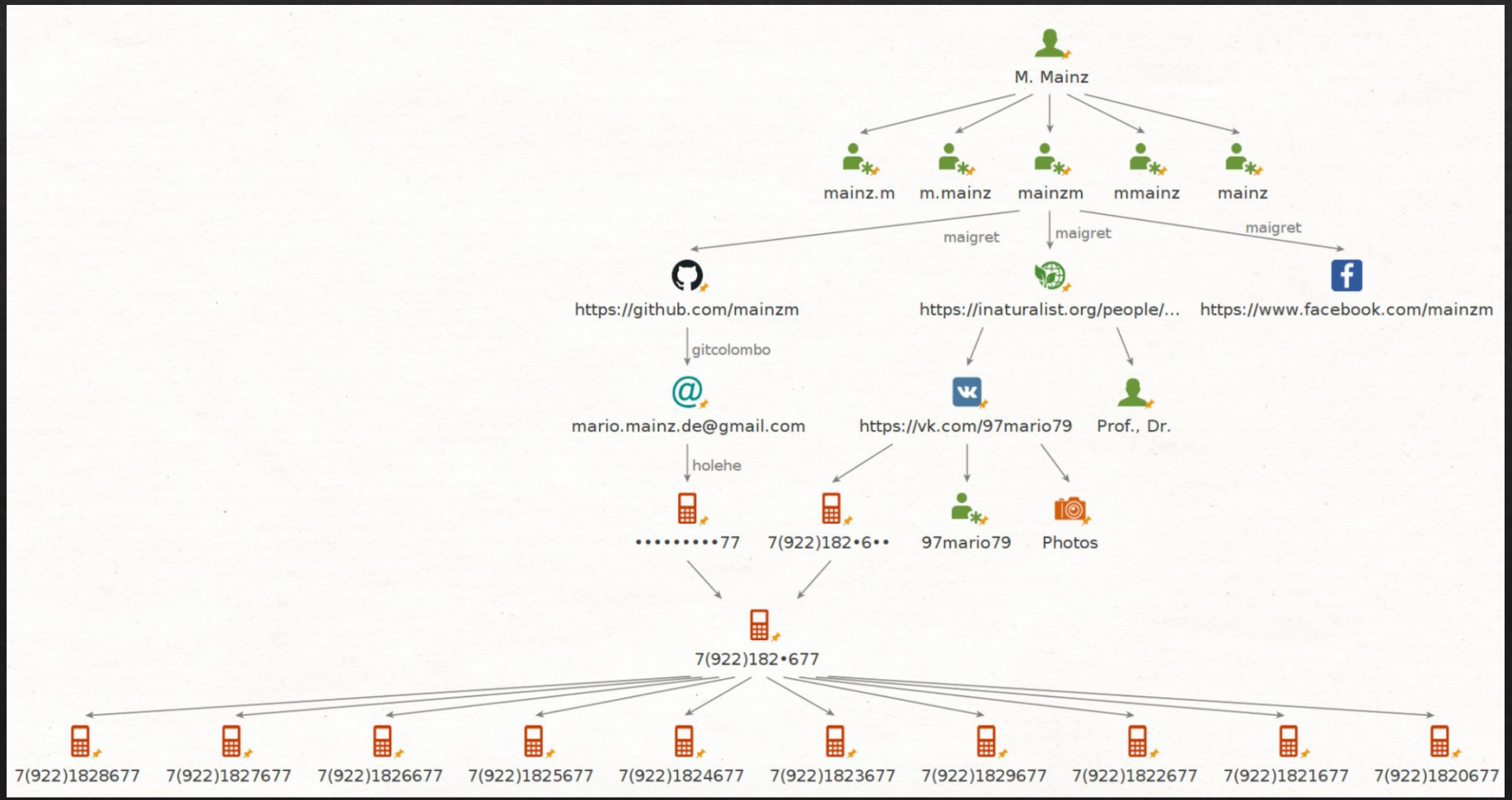
Перейдем по адресу страницы ВК и посмотрим профиль. В профиле есть часть мобильного телефона и различные фотографии. Также можно проверить псевдоним 97mario79. Имеют ли значения числа 97 и 79?





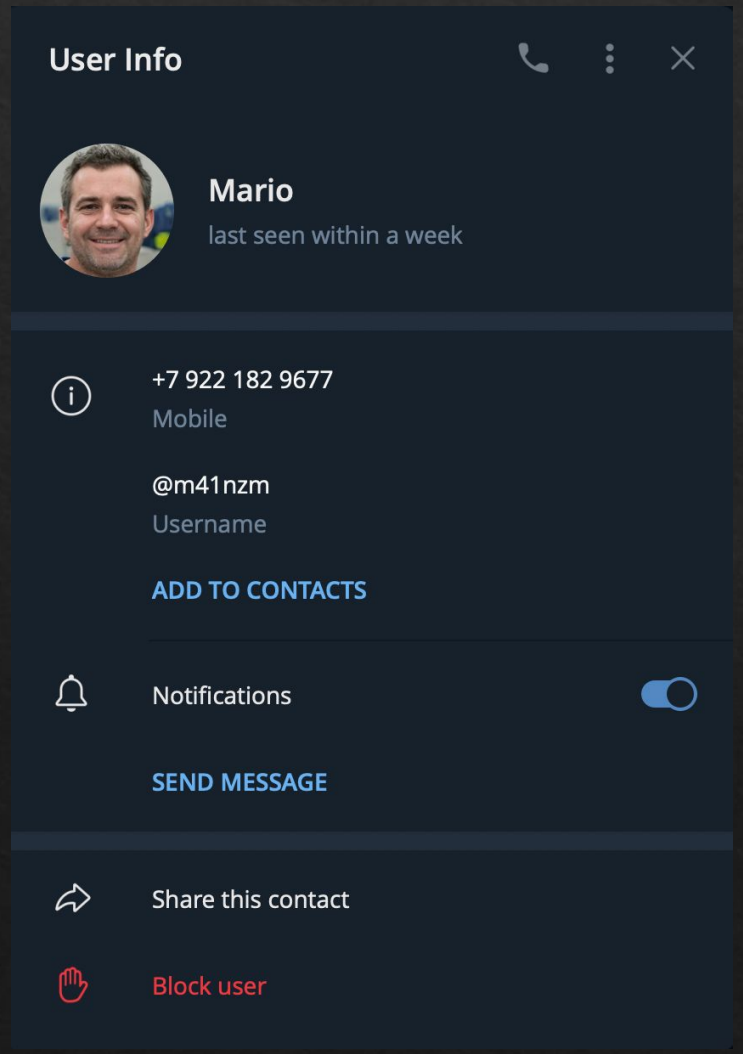
Разбор OSINT CTF

Совмещая отрывки номеров телефона, получаем +7922182•677. Теперь необходимо перебрать 10 вариантов номеров телефонов. Попробуем их искать в Telegram, подставляя каждый в ссылку https://t.me/+number вместо number



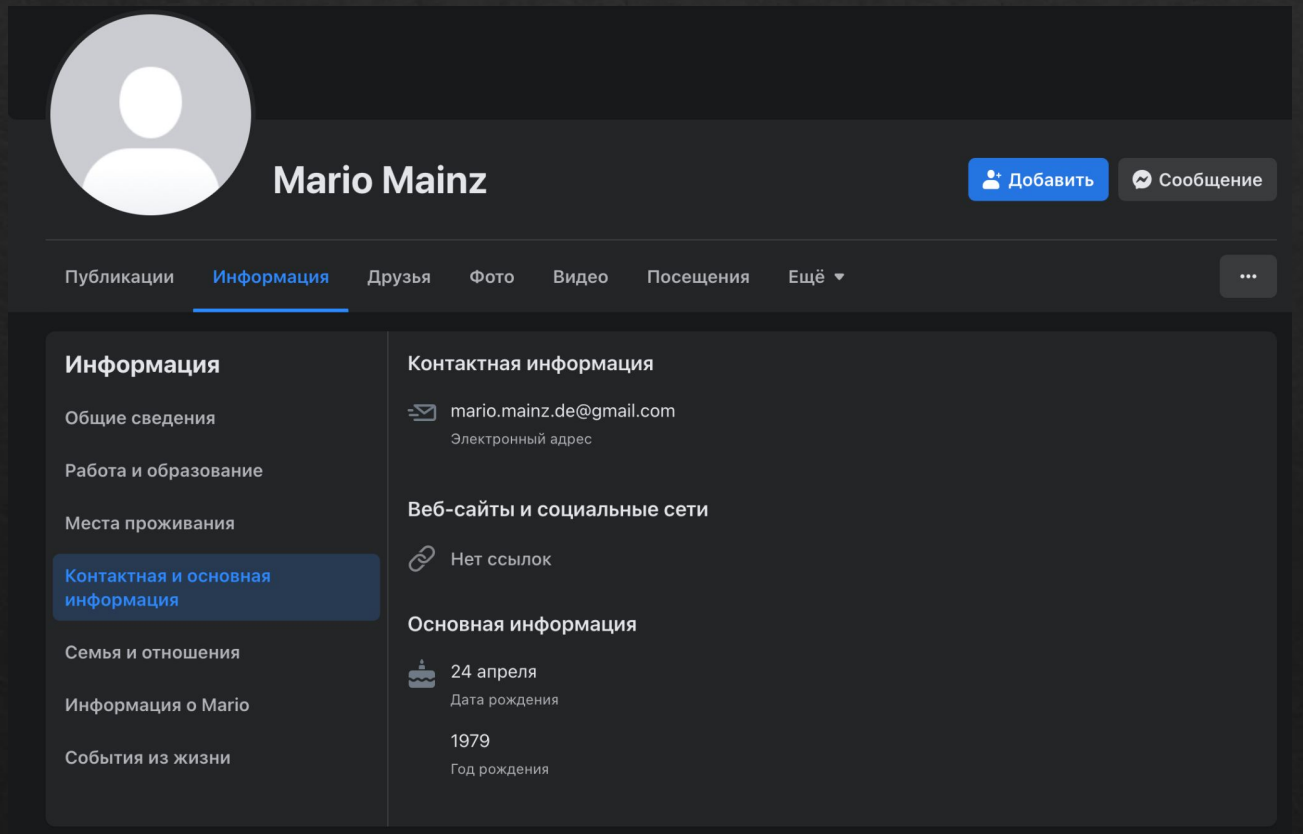
Разбор OSINT CTF

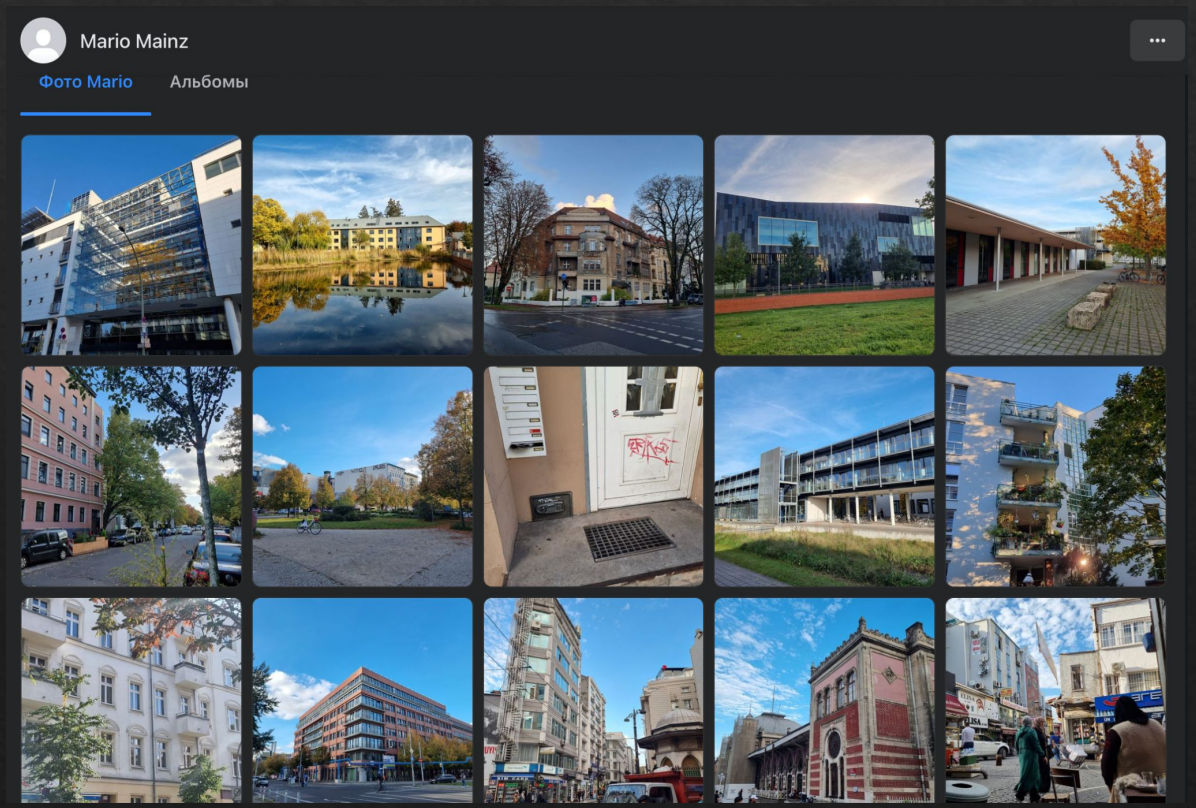
Перебрав все номера, находим Telegram-аккаунт с именем Mario, фотографией и псевдонимом @m41nzm. Как видим, псевдоним указывает на фамилию Mainz. Цвет глаз - зеленый.



Разбор OSINT CTF

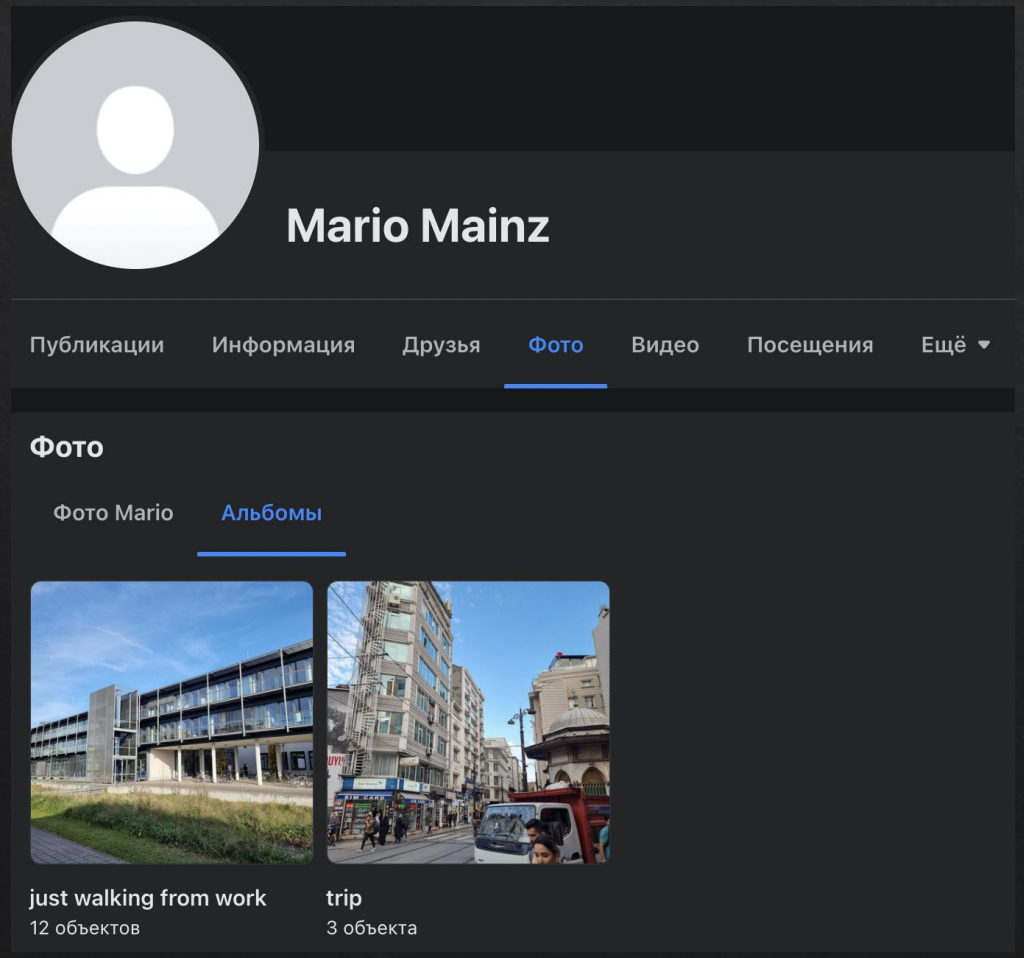
Мы нашли о Марио Майнце все кроме возраста, места жительства, места работы и недавних путешествий. Попробуем найти Марио на Facebook вручную. После просмотра каждой страницы натыкаемся на страницу (https://www.facebook.com/profile.php?id=100086947483845) с фото, которые видели в профиле ВК. День рождения нашли, а год рождения 1979, что можно связать с псевдонимом 97mario79.

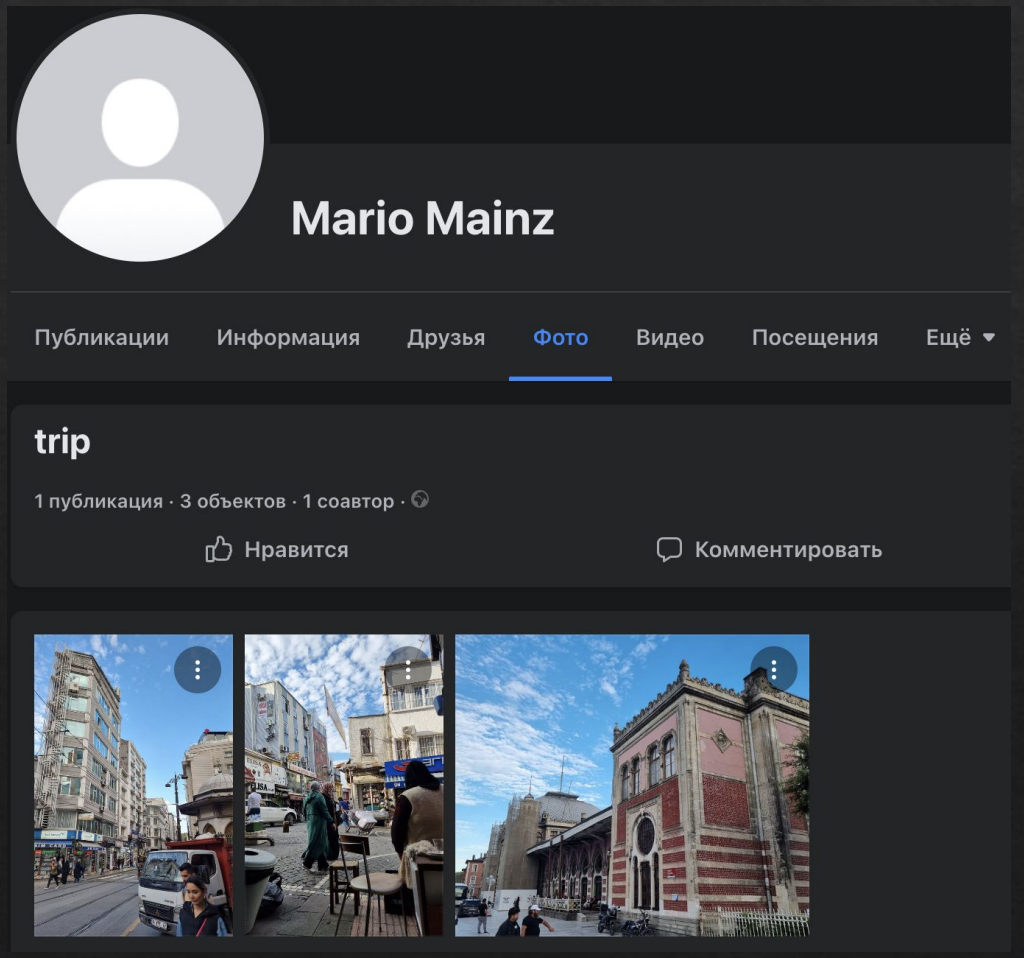




Разбор OSINT CTF

Обратим внимание на альбом “trip” на Facebook. С помощью методов GEOINT, о которых я рассказывал на прошлом докладе (https://www.youtube.com/watch?v=94NaqKYSVXU), мы можем вычислить, что недавняя поездка была совершена в Турцию.





Разбор OSINT CTF

А альбом “just walking from work”, а также фотографии из ВК указывают на то, что Марио живет в Потсдаме, Германия и работает профессором в Университете Потсдама.

Фото из ВК

Фото из Google

Разбор OSINT CTF

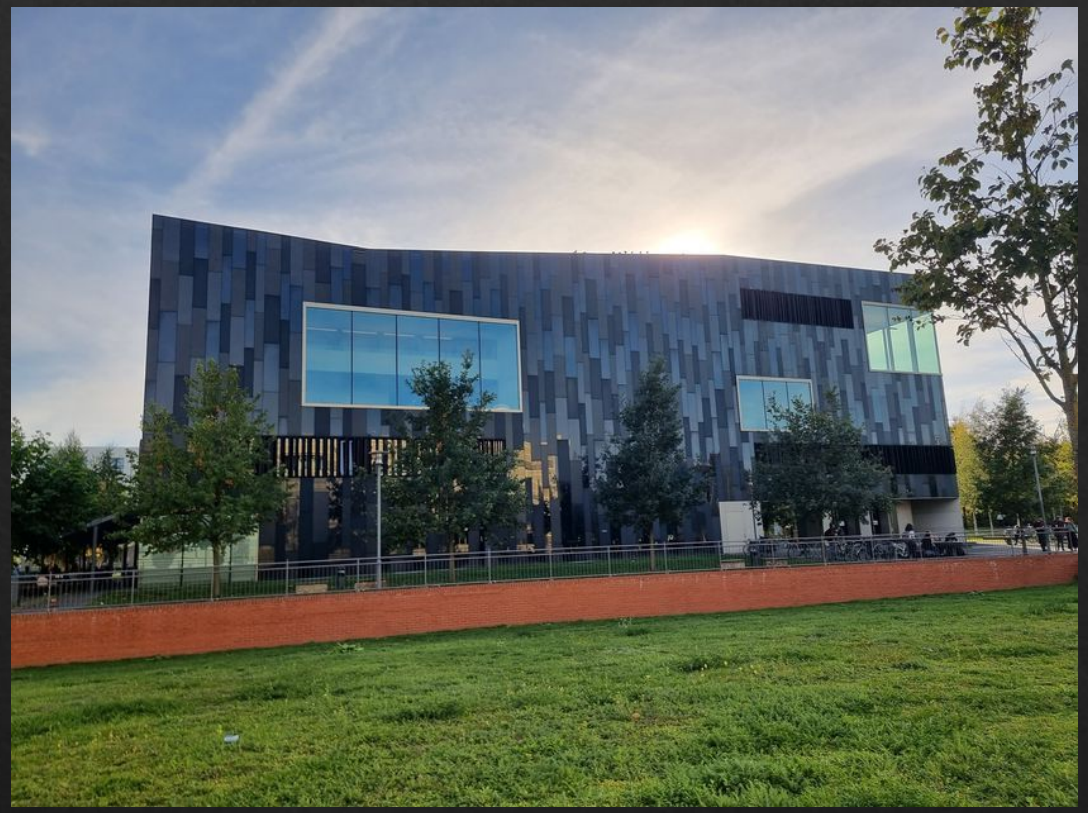
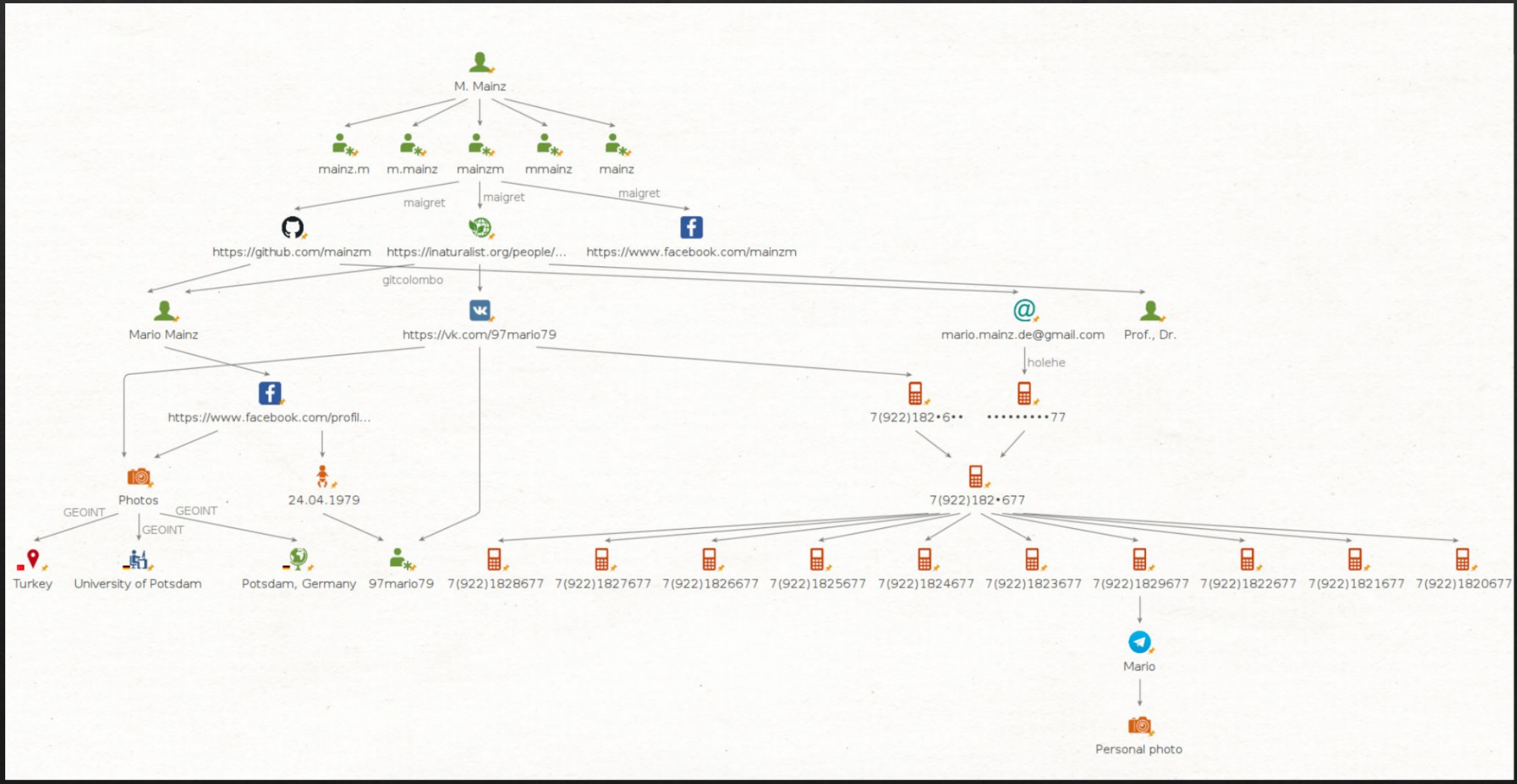


Фото из Facebook

Фото из Google

Разбор OSINT CTF



Разбор OSINT CTF

Имя и фамилия: Mario Mainz

Возраст: 43 года

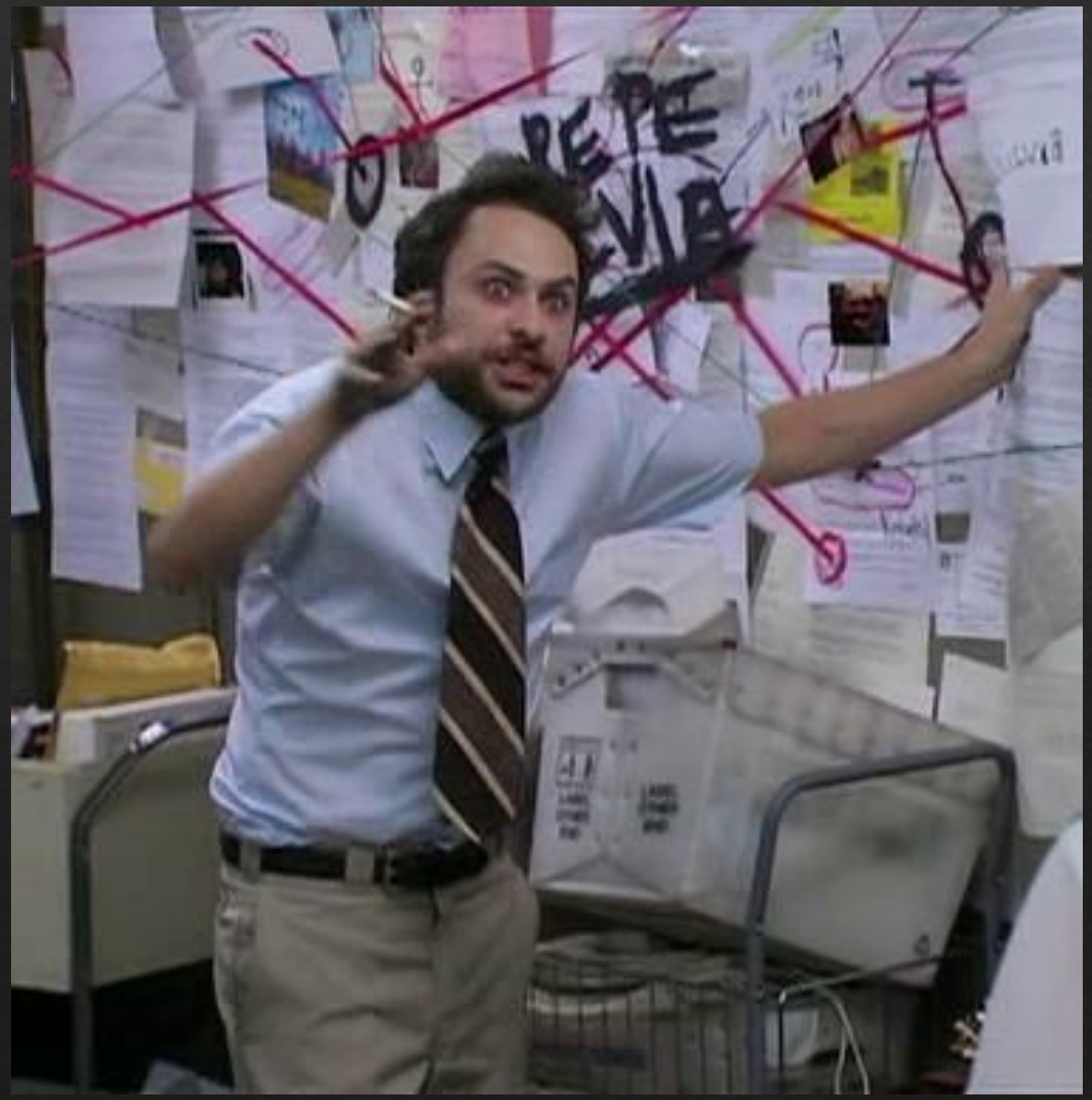
Место жительства (страна, город): Германия, Потсдам

Место работы и должность: Университет Потсдама, профессор

Цвет глаз: зеленый

Номер телефона: +79221829677

Недавние путешествия: Турция



https://t.me/osint_mindset

https://t.me/infosec_dukera

Спасибо. Вопросы?