



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

ДОКЛАДЧИК: @dukera

Методы анонимизации

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



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)

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



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...](#)

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>

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



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	<div>▼ RU: Moscow, Moscow, Russia: 55.7483, 37.6171</div> <pre>{ "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, "autonomous_system_name": "PJSC Moscow city telephone network (25513)" } }</pre>

About Us

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>

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



0 / 94

Community Score

Did you intend to search across the file corpus instead? [Click here](#)

No security vendor flagged this IP address as malicious

AS 25513 (PJSC Moscow city telephone network)

RU

DETECTION

DETAILS

RELATIONS

COMMUNITY

Security Vendors' Analysis

0xSI_f33d	Clean	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AICC (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
Armis	Clean	AutoShun	Clean
Avira	Clean	BADWARE.INFO	Clean
Baidu-International	Clean	benkow.cc	Clean
Bfore.AI PreCrime	Clean	BitDefender	Clean
Bkav	Clean	Blueliv	Clean
Certego	Clean	Chong Lua Dao	Clean
CINS Army	Clean	CMC Threat Intelligence	Clean
Comodo Valkyrie Verdict	Clean	CRDF	Clean
Cyan	Clean	CyberCrime	Clean
Cyble	Clean	CyRadar	Clean
desenmascara.me	Clean	DNS8	Clean
Dr.Web	Clean	EmergingThreats	Clean
Emsisoft	Clean	EonScope	Clean
ESET	Clean	ESTsecurity	Clean
Forcepoint ThreatSeeker	Clean	Fortinet	Clean
G-Data	Clean	Google Safebrowsing	Clean

SuperTool Beta7

Blacklist Check

blacklist

Monitor This

Solve Email Delivery Problems

blacklist

We notice you are on a blacklist. [Click here for some suggestions](#)

Checking [redacted] against 82 known blacklists...

Listed 3 times with 2 timeouts

	Blacklist	Reason	TTL	Response Time	
LISTED		was listed Detail	900		28 ignore
LISTED		was listed Detail	2100		6 ignore
LISTED		was listed Detail	300		7 ignore
OK					46
OK					109
OK					3
OK					3
OK					2
OK					102
OK					3
OK					3
OK					17
OK					3
OK					256
OK					256
OK					104
OK					219
OK					17
OK					10
OK					4
OK					4
OK					68
OK					4
OK					111
OK					3

Ваш IP-адрес

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

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



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:

[REDACTED]

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:

[REDACTED]

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

[REDACTED]



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.

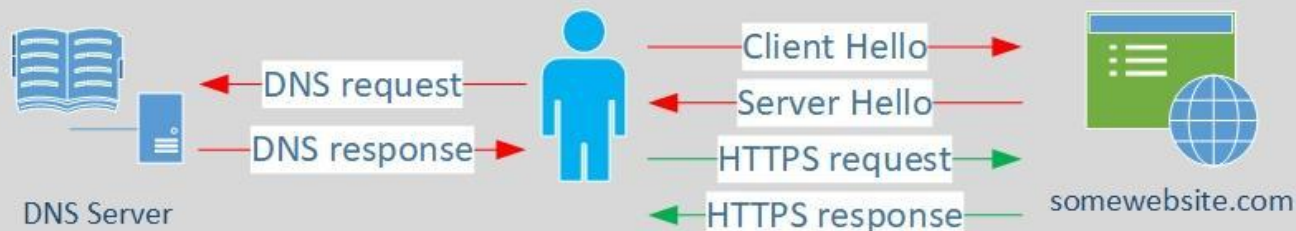
Ваши запросы DNS и IP

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

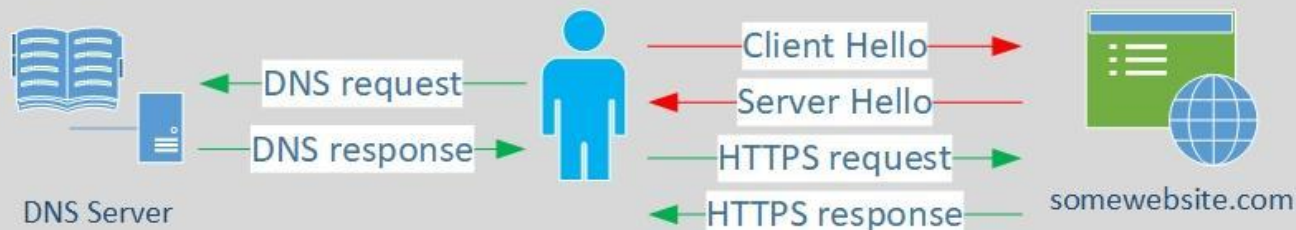


unencrypted encrypted

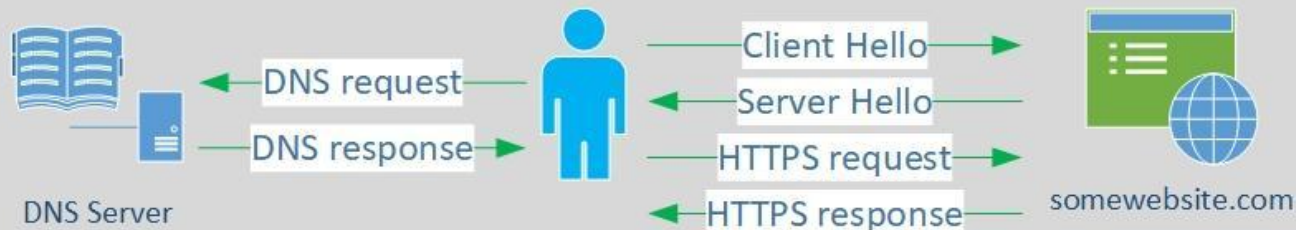
HTTPS with Unencrypted DNS and without ECH



HTTPS with Encrypted DNS without ECH



HTTPS with Encrypted DNS and ECH



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/alectmuffett/dohot>

Метаданные

Данные, которые собирает о нас Google:

Moscow OSINT meetup №3
Методы анонимизации в Сети:
КАК ИСКАТЬ, НО НЕ БЫТЬ
НАЙДЕННЫМ
@dukera



 DuckDuckGo Privacy Browser	 Google Chrome	 Google
<div> Data Linked to You The following data may be collected and linked to your identity:</div> <div>DuckDuckGo does not collect or share any personal information.</div>	<div> Data Linked to You The following data may be collected and linked to your identity:</div> <div><div>Analytics<ul style="list-style-type: none"> Location<ul style="list-style-type: none">Coarse Location User Content<ul style="list-style-type: none">Audio DataCustomer Support Browsing History<ul style="list-style-type: none">Browsing History Identifiers<ul style="list-style-type: none">User IDDevice ID Usage Data<ul style="list-style-type: none">Product Interaction Diagnostics<ul style="list-style-type: none">Crash DataPerformance DataOther Diagnostic Data Other Data<ul style="list-style-type: none">Other Data Types</div><div>Product Personalisation<ul style="list-style-type: none"> Location<ul style="list-style-type: none">Coarse Location Browsing History<ul style="list-style-type: none">Browsing History Identifiers<ul style="list-style-type: none">User IDDevice ID Usage Data<ul style="list-style-type: none">Product Interaction</div><div>App Functionality<ul style="list-style-type: none"> Financial Info<ul style="list-style-type: none">Payment Info Location<ul style="list-style-type: none">Coarse Location User Content<ul style="list-style-type: none">Audio DataCustomer SupportOther User Content Browsing History<ul style="list-style-type: none">Browsing History Identifiers<ul style="list-style-type: none">User IDDevice ID Usage Data<ul style="list-style-type: none">Product Interaction Diagnostics<ul style="list-style-type: none">Crash DataPerformance DataOther Diagnostic Data Other Data<ul style="list-style-type: none">Other Data Types</div></div>	<div> Data Linked to You The following data may be collected and linked to your identity:</div> <div><div>Third-Party Advertising<ul style="list-style-type: none"> Location<ul style="list-style-type: none">Coarse Location Search History<ul style="list-style-type: none">Search History Browsing History<ul style="list-style-type: none">Browsing History Usage Data<ul style="list-style-type: none">Advertising Data</div><div>Developer's Advertising or Marketing<ul style="list-style-type: none"> Location<ul style="list-style-type: none">Coarse Location Contact Info<ul style="list-style-type: none">Physical AddressEmail AddressName Search History<ul style="list-style-type: none">Search History Browsing History<ul style="list-style-type: none">Browsing History Identifiers<ul style="list-style-type: none">User IDDevice ID Usage Data<ul style="list-style-type: none">Product InteractionAdvertising Data</div><div>Analytics<ul style="list-style-type: none"> Location<ul style="list-style-type: none">Precise LocationCoarse Location Contact Info<ul style="list-style-type: none">Physical AddressEmail Address Contacts<ul style="list-style-type: none">Contacts User Content<ul style="list-style-type: none">Audio DataCustomer SupportOther User Content Search History<ul style="list-style-type: none">Search History Browsing History<ul style="list-style-type: none">Browsing History Identifiers<ul style="list-style-type: none">User IDDevice ID Usage Data<ul style="list-style-type: none">Product InteractionAdvertising Data Diagnostics<ul style="list-style-type: none">Crash DataPerformance DataOther Diagnostic Data Other Data<ul style="list-style-type: none">Other Data Types</div><div>Product Personalisation<ul style="list-style-type: none"> Location<ul style="list-style-type: none">Precise LocationCoarse Location Contact Info<ul style="list-style-type: none">Physical AddressEmail Address User Content<ul style="list-style-type: none">Photos or VideosOther User Content Search History<ul style="list-style-type: none">Search History Browsing History<ul style="list-style-type: none">Browsing History Identifiers<ul style="list-style-type: none">User IDDevice ID Usage Data<ul style="list-style-type: none">Product InteractionAdvertising Data</div><div>App Functionality<ul style="list-style-type: none"> Financial Info<ul style="list-style-type: none">Payment Info Location<ul style="list-style-type: none">Precise LocationCoarse Location Contact Info<ul style="list-style-type: none">Physical AddressEmail AddressNamePhone Number Contacts<ul style="list-style-type: none">Contacts User Content<ul style="list-style-type: none">Photos or VideosAudio DataCustomer SupportOther User Content Search History<ul style="list-style-type: none">Search History Browsing History<ul style="list-style-type: none">Browsing History Identifiers<ul style="list-style-type: none">User IDDevice ID Usage Data<ul style="list-style-type: none">Product InteractionAdvertising Data Diagnostics<ul style="list-style-type: none">Crash DataPerformance DataOther Diagnostic Data Other Data<ul style="list-style-type: none">Other Data Types</div></div>

Метаданные

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



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>

Subject is very slow.
Subject is back. Welcome!
Subject has declined to use webcam.
Subject's window inactive for thirty seconds.
No movement for ten seconds.

Subject suddenly moved to another direction.

Subject has moved nonstop for ten seconds.
Subject has dragged outside the button to the button with a right click.
Subject has tried to drag the body onto the button.
Subject has doubleclicked on something but not on the button.
Subject logged in at 15:43:09 during office hours.
15:43:09 and subject has made the window as big as possible.
...
Subject clicked the button
(please click the button)

Button

Achievements »
47%

Криптовалютные транзакции

Сервисы которые позволяют отслеживать операции с криптовалютами:

<https://ethtective.com/>

<https://blockpath.com/>

<https://oxt.me/>

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

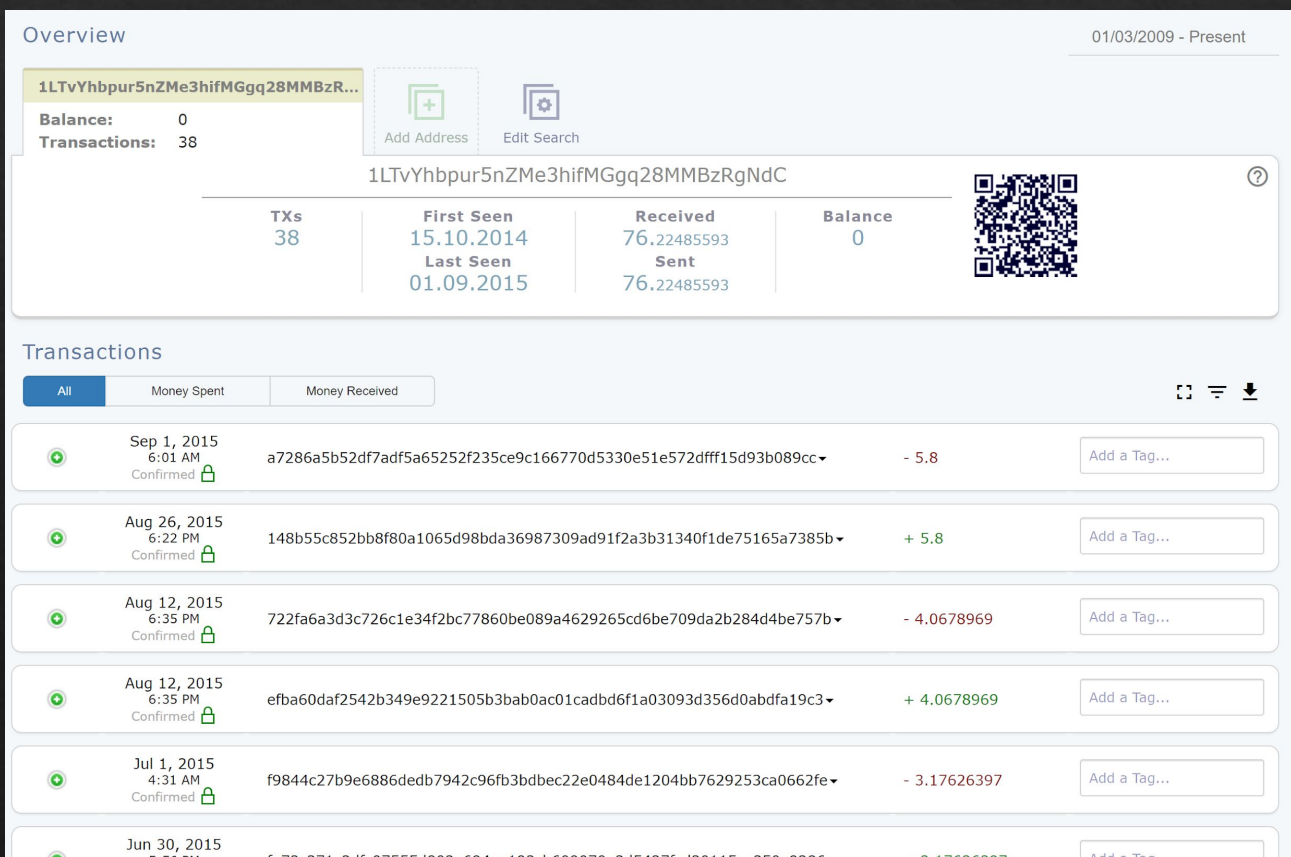
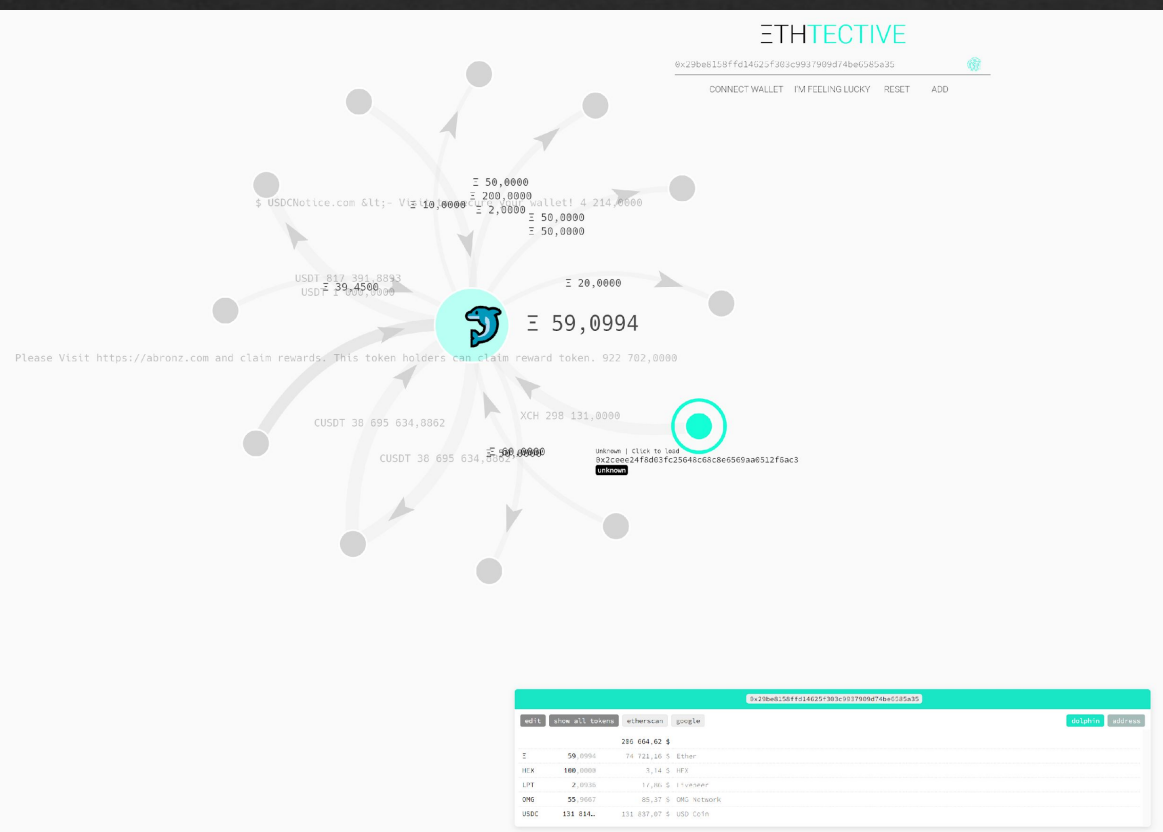


OXT

THE BLOCKCHAIN BY THE PEOPLE FOR THE PEOPLE

Search for a Block, Transaction or Address

SEARCH



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

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



Magnet AXIOM is purpose-built to recover, process, and analyze digital evidence from a variety of sources regardless of whether you use AXIOM or third-party tools to acquire your data.



MOBILE

Recover data from iOS and Android devices with the artifact first approach of AXIOM to get the most relevant evidence for the most popular applications.

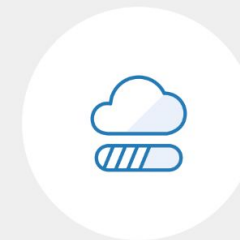
[Learn more about Mobile Capabilities](#)



COMPUTER

Recover deleted data and analyze evidence from Windows, Mac, Chrome, and Linux devices including browser history and deleted files.

[Learn more about Computer Capabilities](#)



CLOUD

Process and examine data from warrant returns, user-generated archives, and live cloud services, with artifacts from 50+ of the most popular cloud services.

[Learn more about Cloud Capabilities](#)

GET A FREE TRIAL

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/>

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



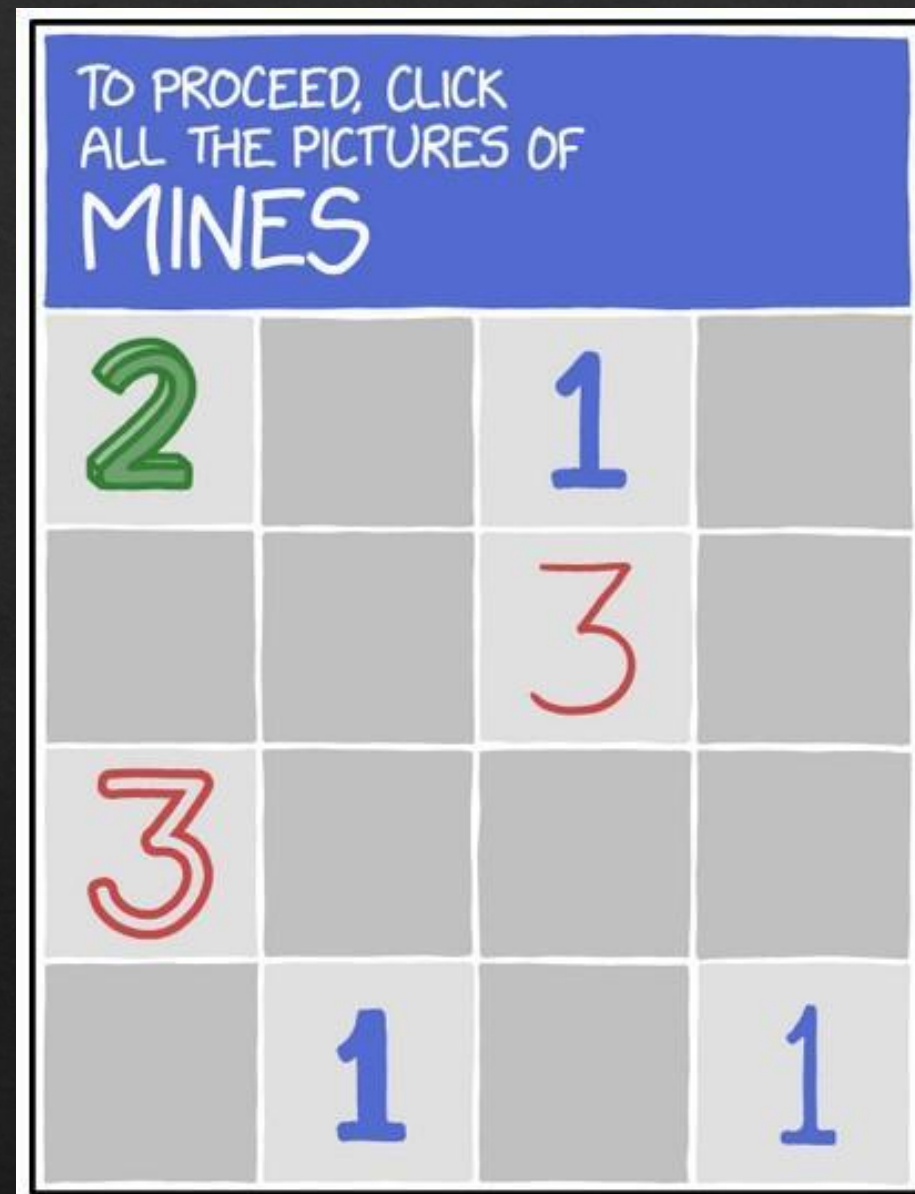
CAPTCHA

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/>

Similarity ratio ⓘ		
Attribute	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"

Moscow OSINT meetup №3
Методы анонимизации в Сети:
КАК ИСКАТЬ, НО НЕ БЫТЬ
НАЙДЕННЫМ
@dukera



Worker 9556831d

lang/timezone:

ru-RU (1 доллар США)
ru
Europe/Moscow (-180)

551.70ms
ua reduction

userAgent:

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

confidence: high

gpu:

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

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): 926bffffb
exts (47): cea46de1

confidence: high

gpu:

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

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



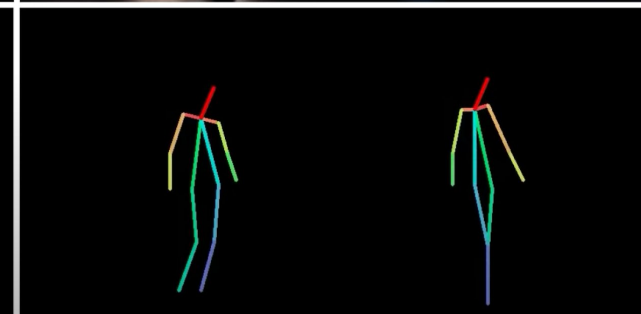
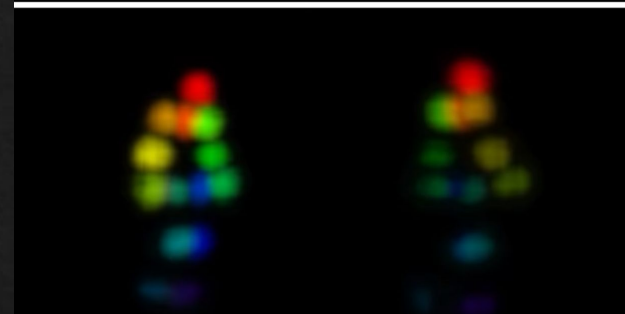
Отслеживание движений основываясь на радиопомехах:

<http://rfpose.csail.mit.edu/>

<https://www.youtube.com/watch?v=HgDdaMy8KNE>



It also works in poor
lighting conditions



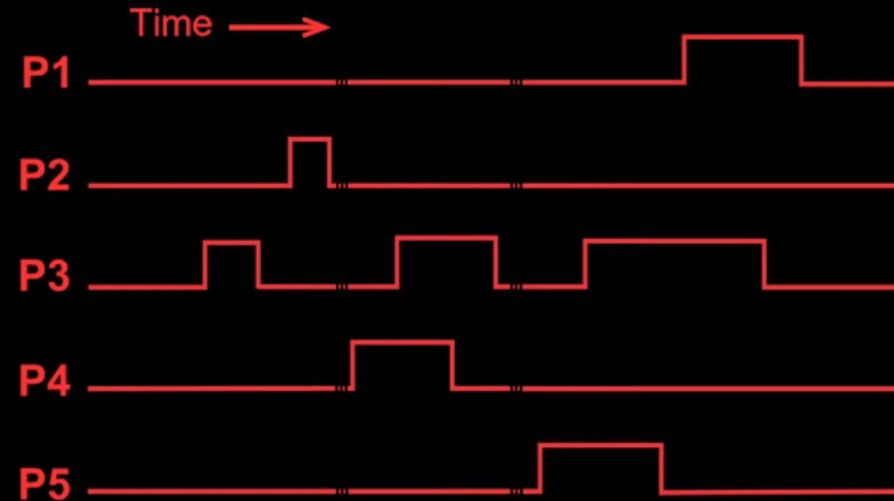
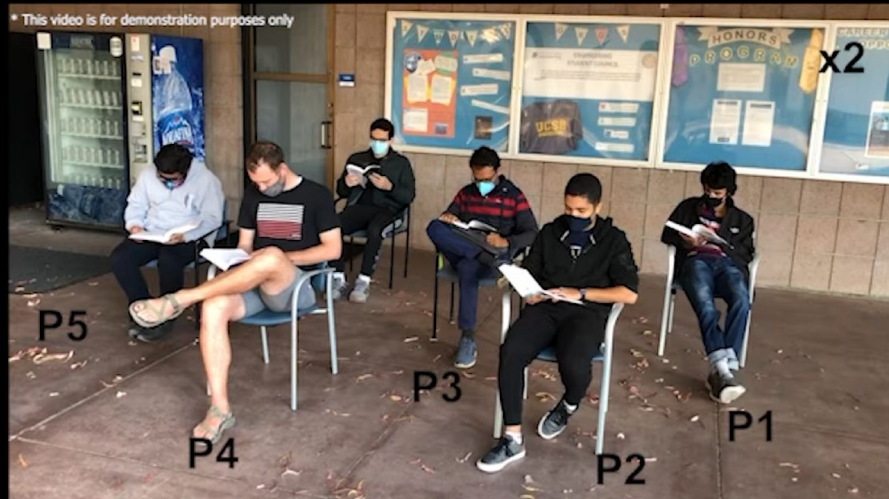
Устройства Wi-Fi и Bluetooth

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



Способ подсчета людей в помещении с помощью Wi-Fi:

<https://www.news.ucsb.edu/2021/020392/dont-fidget-wifi-will-count-you>



Aggregate
Process



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

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

Crowd Silent Periods (CSPs)

Лицо, голос, биометрия

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



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

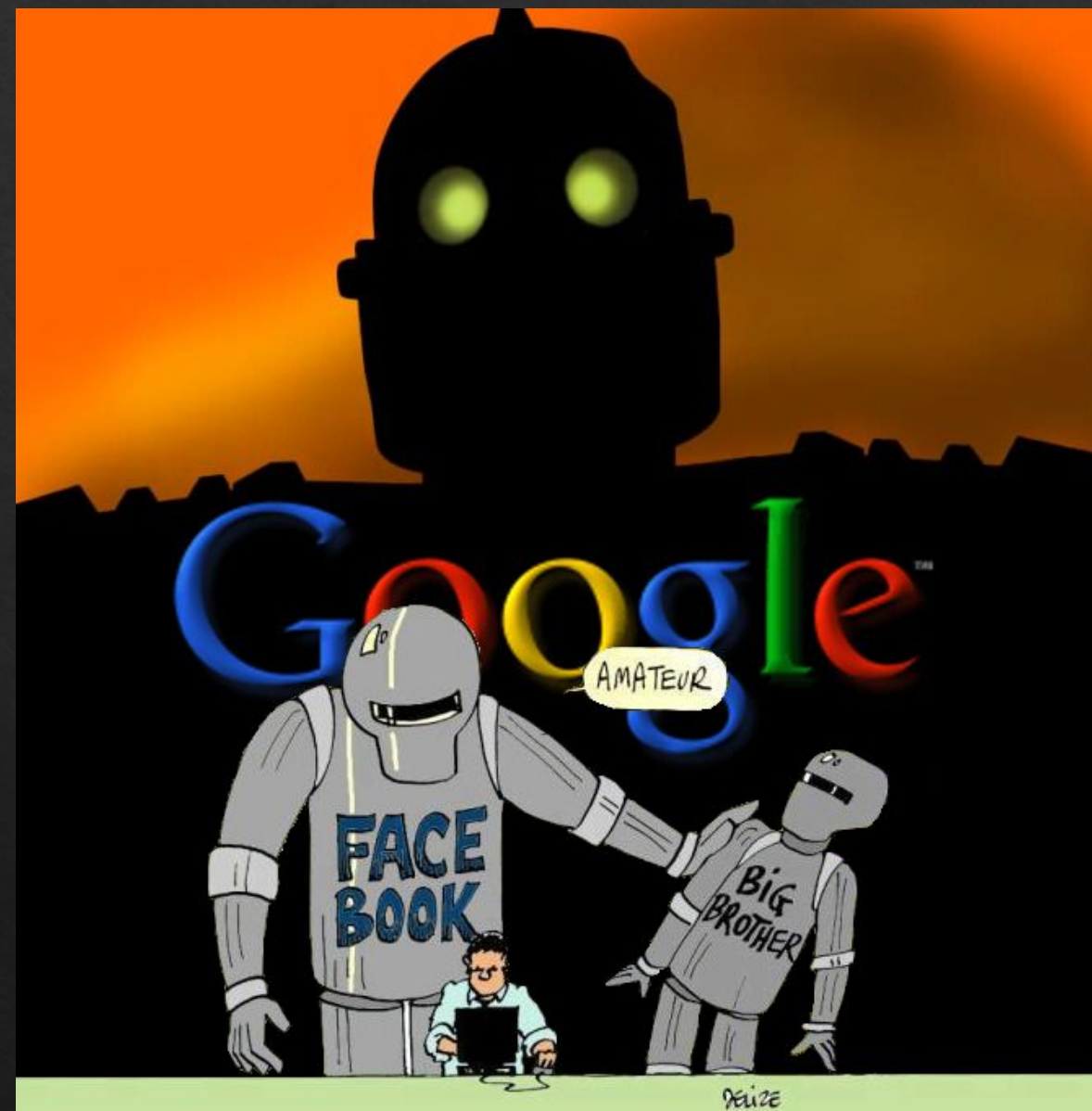


Распознавание походки и внешности

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

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

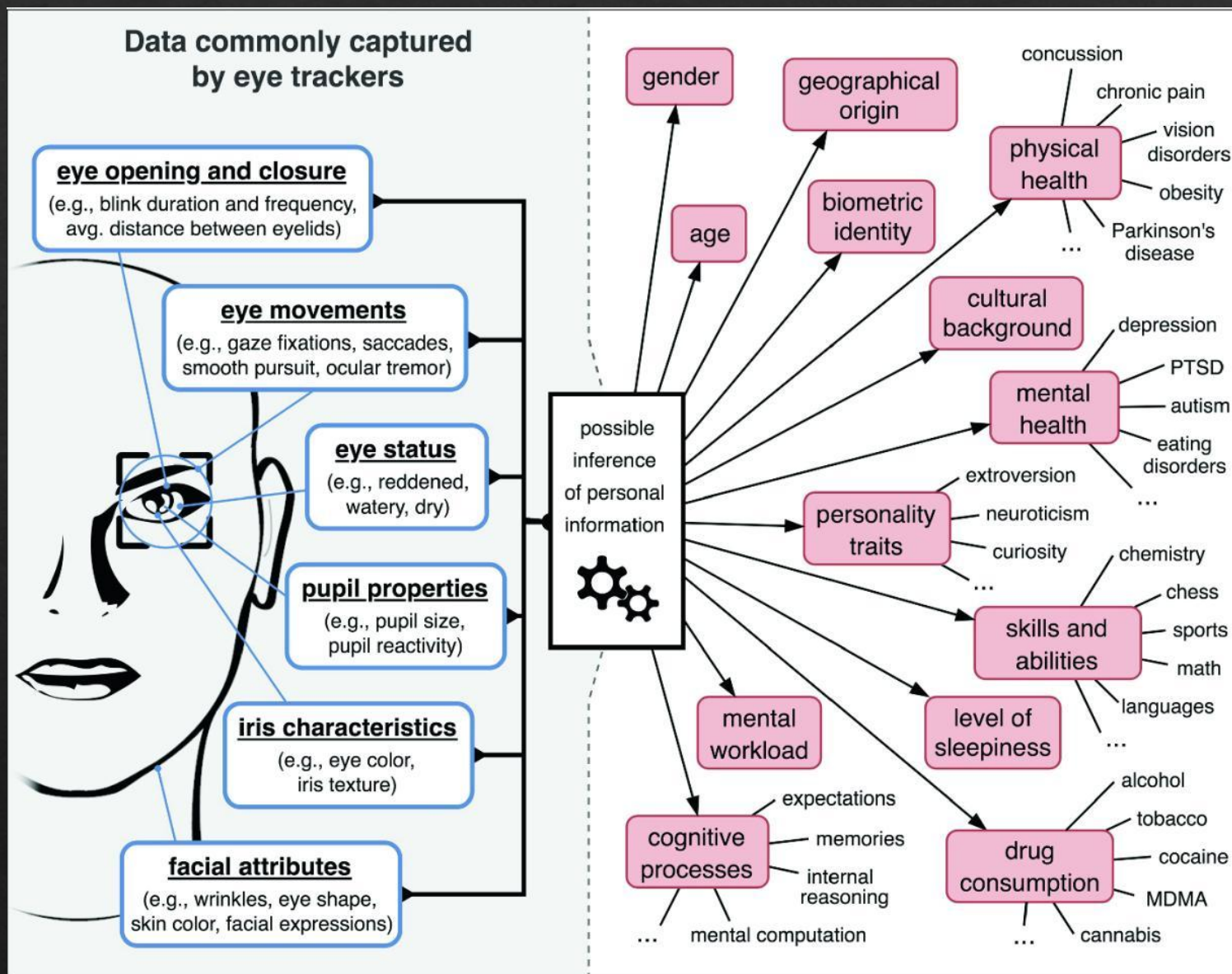


Распознавание походки и внешности

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

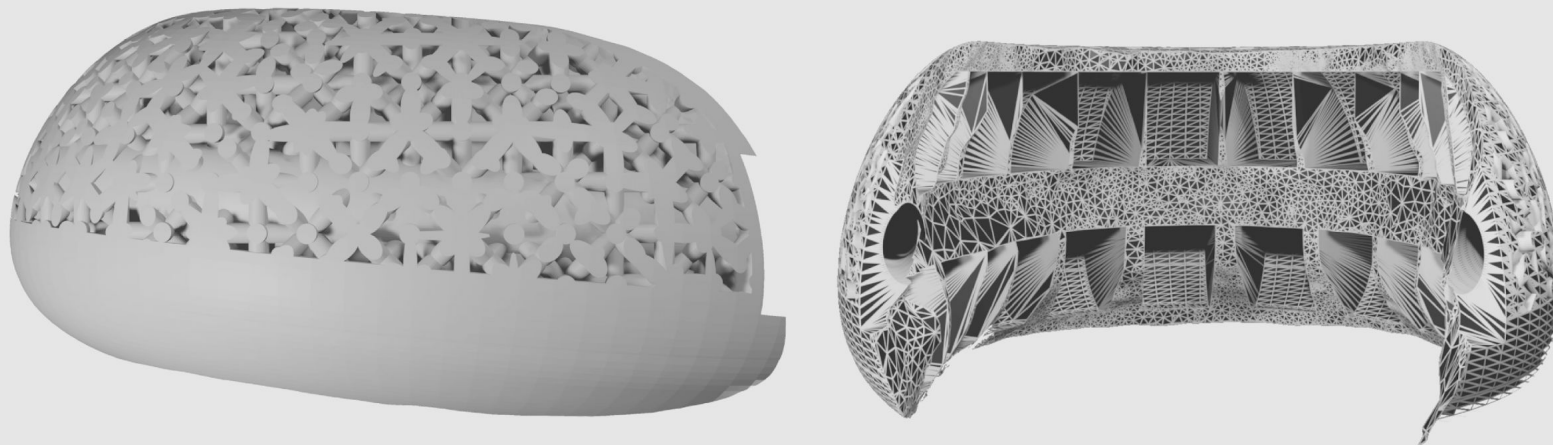
Специальные очки «Reflectacles»:

<https://www.reflectacles.com/>

Если у вас есть 3D-принтер, вы можете попробовать изменить собственную походку:

<https://gitlab.com/FG-01/fg-01>

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



\$168.00

Lens Shade:
Select Lens Shade ▾

Quantity:
1

ADD TO CART

< Share

Ghost uses a frame-applied material that reflects both infrared and visible light. In low light environments they will maintain your privacy on cameras using infrared for illumination and also block 3D infrared facial mapping during both day & night. The visible light reflection can make you anonymous in images/videos using a flash in low light.

Product Details

Weight: 46 grams

Temple Length: 140mm (bendable)

IMEI, IMSI и номер телефона

IMEI и IMSI можно отследить благодаря следующим обстоятельствам:

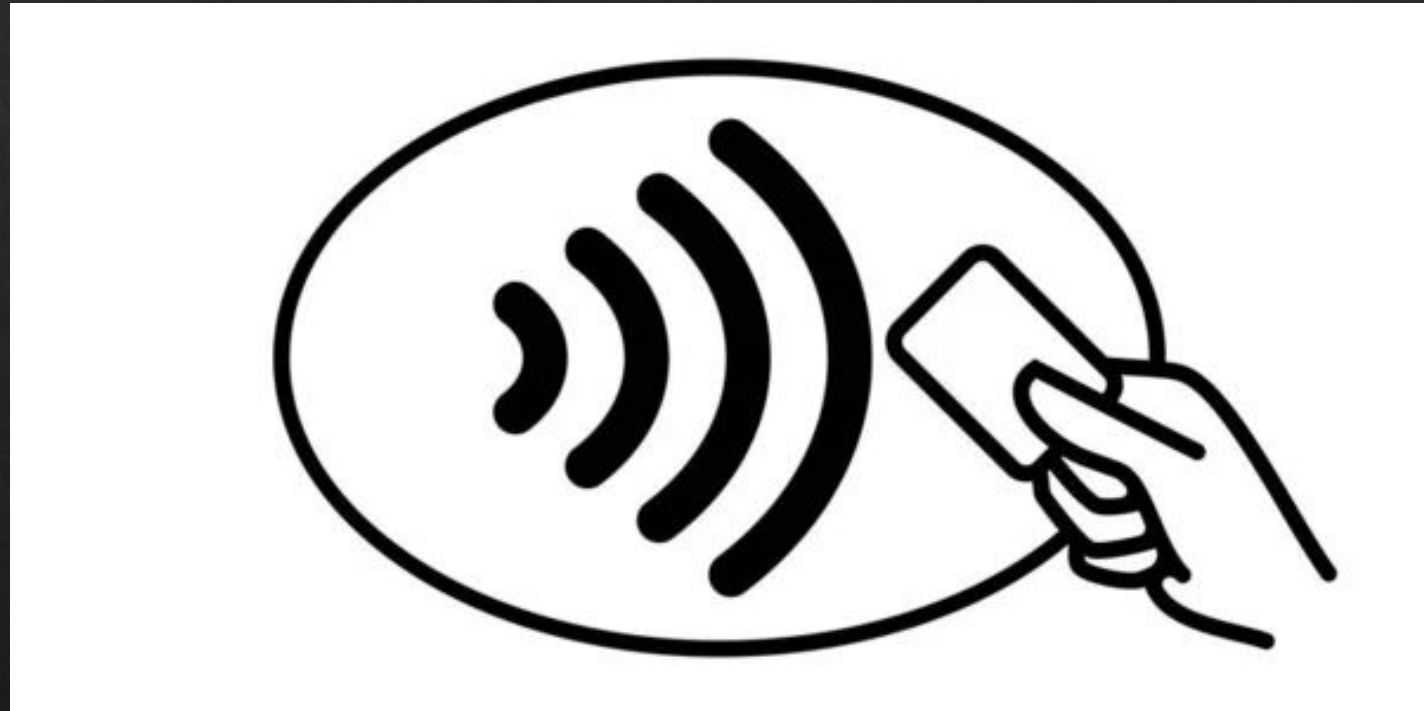
1. Мобильные операторы хранят в связке IMEI и IMSI
2. В журналах антенн также будет храниться IMSI и IMEI. Они регистрируют комбинации IMEI/IMSI, которые подключены к набору антенн а также мощность сигнала
3. Таким образом можно отследить продажу/покупку нового телефона если ваш основной телефон находился при вас
4. Также могут использоваться специальные устройства вроде Stingray или Nuxcell. 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

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



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

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



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

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



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

Методом обхода может быть использование дипфейка faceswap:

<https://github.com/deepfakes/faceswap>

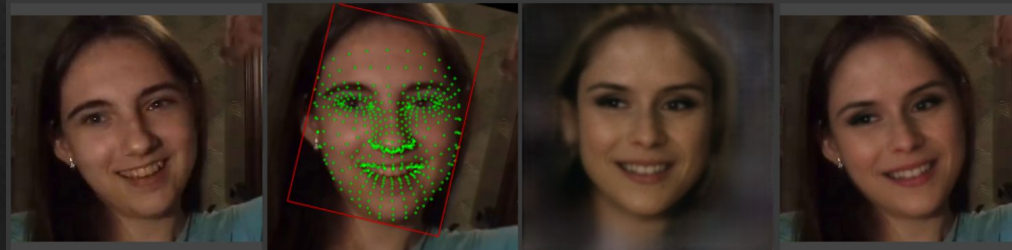
В некоторых случаях требуется «замена лица» прямо в камере, а не на фото:

<https://github.com/iperov/DeepFaceLive>



DeepFaceLive

Real-time face swap for PC streaming or video calls



from a zero to a hero...

just follow setup tutorial

Создание новых личностей

Инструменты, которые могут помочь в создании личностей:

<https://www.fakenamegenerator.com/>

<https://thispersondoesnotexist.com/>

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



FAKE NAME GENERATOR™

Name Generator

Free Tools

Order in Bulk

Smiley Generator

FAQ

Your Randomly Generated Identity

Gender: Random
Name set: American
Country: United States

Generate

Advanced Options

These name sets apply to this country:
American, Hispanic



Robert S. Frye
2708 Morgan Street
Tallahassee, FL 32301

Curious what **Robert** means? [Click here to find out!](#)

Mother's maiden name: Montgomery

SSN: 595-02-XXXX
You should [click here](#) to find out if your SSN is online.

Geo coordinates: 30.349463, -84.245839

PHONE

Phone: 850-528-1746
Country code: 1

BIRTHDAY

Birthday: March 5, 1972
Age: 50 years old
Tropical zodiac: Pisces

ONLINE

Email Address: RobertSFrye@jourrapide.com
This is a real email address. [Click here to activate it!](#)
Username: Chaplin72
Password: Aj7aIk5eeth
Website: fgfxuhm.com
Browser user agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_4) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1 Safari/605.1.15

FINANCE

MasterCard: 5586 4315 3171 8706
Expires: 3/2025
CVC2: 161

EMPLOYMENT

Company: Eli Moore Inc
Occupation: Codex specialist

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



Sign in

Создание новых личностей

Инструменты, которые могут помочь в создании личностей:

<https://generated.photos/face-generator>

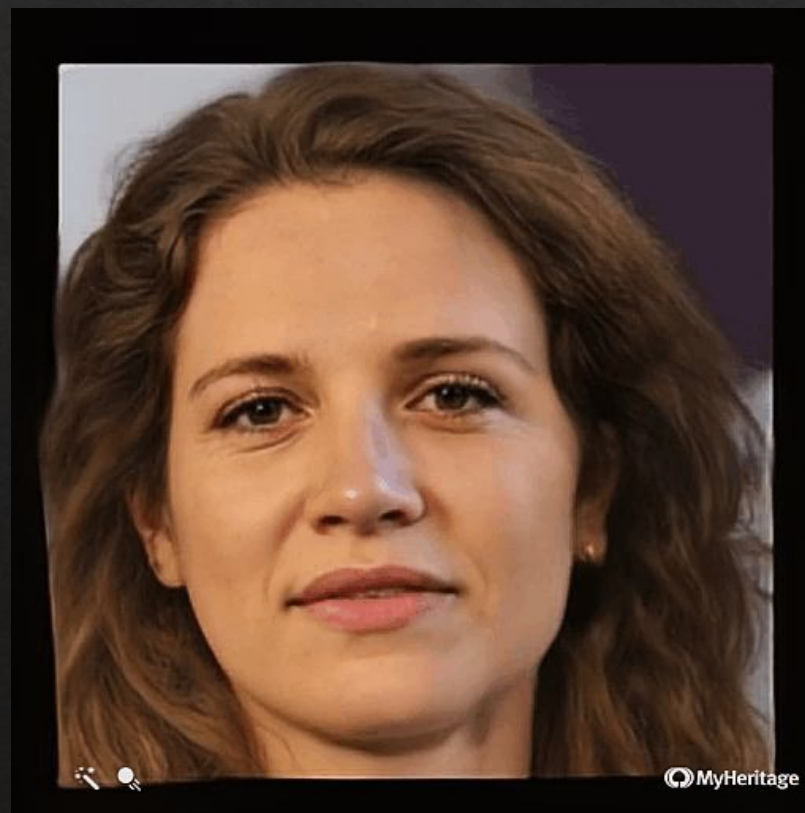
Также с помощью проекта StyleGan можно самому создавать изображение:

<https://github.com/NVlabs/stylegan2>

Бонусом можно сделать изображение подвижным:

<https://www.myheritage.com/deep-nostalgia>

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



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

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



Speaking Portrait

Enabling photorealistic avatars,
using just text or audio as input



Face-swap

It is possible to modify the method to perform face-swap using supervised segmentation masks.



For both unsupervised and supervised video editing, such as face-swap, please refer to [Motion Co-Segmentation](#).

Дополнительные инструменты

Сервисы для создания личностей:

<https://randomdatatools.ru/>

<https://randus.org/>

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



Онлайн версия

Если вам нужно автоматическое заполнение таблиц
базы данных - воспользуйтесь программой для Windows.

Пользователь Пасп. Образов. Автом. Докум. Плат.

Выберите пол человека

Любой Мужской Женский

Фамилия
Обухов

Имя (классическая)
Петр

Отчество
Романович

ФИО ИО ИФ

Дата рождения 09.07.1976 Возраст 46

Номер телефона
+7 (985) 524-19-40

Логин
petr.obuhov

Пароль
29fb2e7f2

Электронная почта
petr.obuhov@outlook.com

Обновить

Оставить отзыв Поддержать проект

Ответьте пожалуйста на пару вопросов
Для каких целей вы используете данный сервис?

Ваш ответ

Не хочу! Следующий вопрос

Генераций за все время: 28 154 896

Выберите нужную
вам вкладку

Выберите пол
человека

Нажмите чтобы
скопировать текст в
один клик

Здесь вы можете
скопировать нужный
формат имени
ФИО - Фамилия Имя Отчество,
ИО - Имя Фамилия,
ИФ - Имя Фамилия
Например,
ИО - Виктория Севастьяновна

Нажмите обновить,
чтобы сгенерировать
другую личность

Оставьте отзыв о
нашем сервисе



Соболь Татьяна Петровна

Дата рождения

10 декабря 1995 года

Адрес

662525, г. Дубровка, ул. Долгова, дом 17, квартира 835

Телефон

+7 (954) 142-04-52

Цвет

Шоколадный

Логин

TatyanaSobol965

Пароль

cwMНu0KN803p

Хочу другого пользователя

Одноразовая почта

Дополнительные инструменты

Защитить реальный адрес вашей электронной почты можно с помощью следующих сервисов:

<https://simplelogin.io/>

<https://anonaddy.com/>

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



SimpleLogin
POWERED BY PROTON

Community ▾ Pricing Login Sign Up

Receive and send emails anonymously

With **email aliases**, you can be anonymous online and protect your inbox against spams and phishing. **Open source**. Made and hosted in Europe.

Get your aliases for free >>

★★★★★ 800,000+ aliases created.

As seen on

et PC penguin V

How it works

Shield your inbox with email aliases.

AnonAddy

Help FAQ Blog Pricing Sign In Register

OPEN-SOURCE

Anonymous Email Forwarding

Create Unlimited Email Aliases For Free

Get Started Now

How Does It Work?

1. Register Your Username

Let's say your username is **john.doe**. You can now use ***@john.doe.anonaddy.com** (or **.me**) as your email. Where ***** denotes any valid local part for an email address.

If you would like to remain anonymous choose a username that is not linked to your real name or identity and that you haven't used anywhere else.

You can also create aliases at **shared domains** if you are concerned about others linking alias ownership to you.

Дополнительные инструменты

Сервисы для поиска геолокации человека:

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

<https://github.com/thewhiteh4t/seeker>

<https://github.com/Bafomet666/Bigbro>

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



Geogramint

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



```
└─$ 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/python3.10/site-packages (from -r requirements.txt (line 4)) (1.1.1)
Requirement already satisfied: kivy-garden in /home/aldenteman/.local/lib/python3.10/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/site-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/python3.10/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/.local/lib/python3.10/site-packages (from trio->-r requirements.txt (line 2)) (1.0.0rc9)
Requirement already satisfied: sortedcontainers in /usr/lib/python3/dist-packages (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 (from 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

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



Start Search

Reset

Users

Groups

PHOTO NOT AVAILABLE

Id: 5322067334
Name: 'Joxongir.'
Username:
Distance: 500m

PHOTO NOT AVAILABLE

Id: 5181439632
Name: 'Chebyrek'
Username:
Distance: 500m

PHOTO NOT AVAILABLE

Id: 5117953273
Name: 'Sebuh' 'Memmedov'
Username:
Distance: 500m

PHOTO NOT AVAILABLE

Id: 5080820503
Name: 'E'
Username:
Distance: 500m

PHOTO NOT AVAILABLE

Id: 5499790479
Name: 'Luis Migue' 'Mellet'
Username:
Distance: 500m

PHOTO NOT AVAILABLE

Id: 5598021892
Name: 'j' 'Hello-'
Username:
Distance: 500m

PHOTO NOT AVAILABLE

Id: 445247872
Name: 'I' 'M'
Username: 'Misha7708'
Distance: 500m

PHOTO NOT AVAILABLE

Id: 403605249
Name: 'H'
Username: 'Hel_91'
Distance: 500m

PHOTO NOT AVAILABLE

Id: 385255168
Name: 'Cnop'
Username:
Distance: 500m

PHOTO NOT AVAILABLE

Id: 5740514847
Name: 'Rozana' 'Elerina'

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: 'ЮБАО'
Distance: 500m

Id: 1237215533
Name: 'Dental'
Distance: 500m

Id: 1525823238
Name: 'Секс Знакомства Люблино'
Distance: 500m

Id: 1175963576
Name: 'Tr'
Distance: 500m

Geogramint

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



Start Search

Reset

Users

Groups

PHOTO NOT AVAILABLE

Id: 184844650
Name: 'Sasha' Lavrov
Username: 'Gaz6600'
Distance: 500m

PHOTO NOT AVAILABLE

Id: 268104579
Name: 'Victor'
Username: 'kvigor'
Distance: 500m

PHOTO NOT AVAILABLE

Id: 156987571
Name: 'Собиржон Илхомбеков'
Username: 'S11215'
Distance: 500m

PHOTO NOT AVAILABLE

Id: 109942641
Name: 'Anton' 'Lad'
Username: 'ANTONLAD'
Distance: 500m

PHOTO NOT AVAILABLE

Id: 1218689
Name: 'Igor' 'Sokhan'
Username: 'Epizode_E'
Distance: 500m

PHOTO NOT AVAILABLE

Id: 286814338
Name: 'N' 'N'
Username: 'magnumman'
Distance: 500m

PHOTO NOT AVAILABLE

Id: 316973948
Name: 'Ярослав' 'Кищенко'
Username: 'Yaroslav_Kishchenko'
Distance: 500m

PHOTO NOT AVAILABLE

Id: 701001570
Name: 'Stanislav'
Username: 'stass529'
Distance: 500m

PHOTO NOT AVAILABLE

Id: 699260194
Name: 'Ислам' 'Турузбеков'
Username: ''
Distance: 500m

PHOTO NOT AVAILABLE

Id: 645912539
Name: 'Андрей'

Бизнес Кухня

Id: 1344435677
Name: 'Бизнес Кухня'
Distance: 500m

Id: 1274525523
Name: 'Мастер Ювелир'
Distance: 500m

Id: 1174017187
Name: 'ARBAT / МСК'
Distance: 500m

Id: 1311692329
Name: 'Ангель Маруси Дубковой'
Distance: 500m

PHOTO NOT AVAILABLE

Id: 1394155288
Name: 'Протест'
Distance: 500m

Id: 1377395951
Name: 'Адальтер'
Distance: 500m

Id: 1408322727
Name: 'Вписки | Флеты - Москва'
Distance: 500m

PHOTO NOT AVAILABLE

Id: 1494154194
Name: 'Кто туз'
Distance: 500m

Id: 1499537241
Name: 'Новый Арбат'
Distance: 500m

seeker

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



```
└─$ 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	██████████ (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													
	<table><thead><tr><th>t1</th><th>opn</th><th>rt1</th><th>rt5</th><th>p50</th><th>p90</th></tr></thead><tbody><tr><td>0</td><td>0</td><td>0.00</td><td>0.00</td><td>0.00</td><td>0.00</td></tr></tbody></table>	t1	opn	rt1	rt5	p50	p90	0	0	0.00	0.00	0.00	0.00
t1	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

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



```
└─$ python3 seeker.py
```



```
[>] Created By   : thewhite4t  
|---> Twitter   : https://twitter.com/thewhite4t  
|---> 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&rtfpof=true&sd=true
```

```
[+] Port : 8080
```

```
[+] Starting PHP Server...[ ✓ ]
```

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


seeker

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



```
[+] 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	
	t1l opn rt1 rt5 p50 p90
	1 0 0.01 0.00 0.00 0.00

Bigbro

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



Выберите версию для запуска

- (1) Termux
- (2) Desktop
- (3) Идти нахуй из инструмента
- (4) Получить полную версию

└─> Bafomëd production ─> Введите номер опции:

Тайна это безопасность, а безопасность это победа

```

  _____
 | $$$$$$ \ $$ |
 | $$__ / $$ | \ |
 | $$   $$ | $$ | $$$$$$ \
 | $$$ / $$ | $$ | $$_
 | $$   $$ | $$ \ $$$$
 \ $$$$$$ \ $$ \ $$$$$$
   | \_ | $$
   \ $$  $$
   \ $$$$

  _____
 | $$$$$$ \
 | $$__ / $$ | \ |
 | $$   $$ | $$ | $$$$$$ \
 | $$$ / $$ | $$ | $$_
 | $$   $$ | $$ \ $$$$
 \ $$$$$$ \ $$ \ $$$$$$
   | \_ | $$
   \ $$  $$
   \ $$$$

```

Новая архитектура 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]	Близ 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

└─> Bafomëd 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=127.0.0.1:4040

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

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



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

...ngrok.io запрашивает разрешение на:

📍 доступ к данным о вашем местоположении

Разрешить

Блокировать

```
-----  
└─> Bafomöd 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=127.0.0.1:4040  
-----
```

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      : ██████████  
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 - ██████████ Долгота - ██████████

https://www.google.com/maps/place/██████████

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

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



Maigret OSINT bot

bot



mmainz 02:20 ✓✓

mmainz

Finished! 02:20

mmainz

54 exact accounts found:

YandexCollections API, Twitch, GitHubGist, MicrosoftTechNet, social.msdn.microsoft.com, Imgur, YouTube User, Nitter, Reddit, AppleDiscussions, Baidu, GitHub, Telegram, Trello, Fiverr, Roblox, Blogger, Steam, Academia.edu, Disqus, euw.op.gg, Dribbble, Docker Hub, DEV Community, Gog, NPM, Picsart, HackerOne, FortniteTracker, Pixwox, hashnode, giters.com, Codewars, Hoobly, RubyGems, Keybase, Libraries, lightstalking.com, Steamidfinder, Paypal, githubplus.com, RPGGeek, rblx.trade, VideogameGeek, Askvoprosy, coder.social, Anapakurort, tg.rip, Crowdin, Poshmark, Quizlet, Tf2Items, exploretalent.com, padlet.com



mmainz.json

469 B

02:28



report_mmainz.html

182.0 KB

02:28



Можно предположить, что “М.” 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

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



Maigret OSINT bot
bot



mainzm 02:12 ✓✓

mainzm
Finished! 02:12

mainzm
22 exact accounts found:
YandexCollections API, GitHubGist, GitHub, Roblox, Duolingo, last.fm
, Anime-planet, VSCO, Gramho, Picsart, lightstalking.com, Paypal,
githubplus.com, rblx.trade, Kik, Askvoprosy, coder.social, .com,
exploretalent.com, inaturalist.nz, irl.com, inaturalist.org

 mainzm.json
871 B

02:15



 report_mainzm.html
124.8 KB

02:15



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, Thehive, BitBucket, amp.flipboard.com, [Itch.io](https://mainz.itch.io/),
AdultFriendFinder, jeuxvideo, Flipboard, Imglnn, <https://mainz.itch.io/>,
Sporcle, Gog, banki.ru, Gitee, Newgrounds, Boarc
Anime-planet, IFTTT, Pokemon Showdown

 mainz.json
869 B

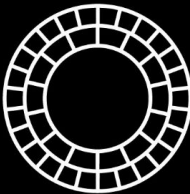
02:36

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

VSCO®
Page Not Found
Launching soon



02:36

mainz

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

Разбор OSINT CTF

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



Maigret OSINT bot

bot



mainz

, 4stor, rblx.trade, MinecraftOnly, eintracht, 2d-3d, Porevo, Wireclub, Kik, Lkforum, VideogameGeek, Xbox Gamertag, Askvoprosy, Thebuddyforum, Hatena, 1001mem.ru, izmailonline.com, Play.md, coder.social, Stoimost, Anapakurort, ForumProSport, Archive.orgTwitterProfiles, Bandlab, Bikemap, Chomikuj.pl, Cults3d, Fansly, Forumprawne.org, GeniusArtists, Friendfinder, Gailed, Friendfinder-x, Joemonster, Cytoid.io, Liebe69, MapMyTracks, Mcuuid, Prv.pl, Poshmark, Quizlet, Rumbleuser, Splice, Suzuri.jp, Runescape, Tetr.io, Tf2Items, Vine, .com, .pro, .me, .biz, .ddns.net, .email, forum.cfx.re, cnblogs.com, Pixilart, hiveblocks.com, flipsnack.com, exploretalent.com, padlet.com, profile.typepad.com, irl.com, postcrossing.com

4stor.ru

mainz » Страшные истории

Страшные истории, мистические истории. Истории из жизни и выдуманные истории. Страшилки.

02:36



report_mainz.html

423.1 KB

02:36



Разбор OSINT CTF

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



Maigret OSINT bot

bot



m.mainz 02:36 ✓✓

m.mainz

Finished! 02:36

m.mainz

17 exact accounts found:

YandexCollections API, euw.op.gg, Pixwox, Pbase, Dumpor, Hoobly,
Wanelo, lightstalking.com, Kik, Askvoprosy, coder.social,
Anapakurort, GeniusArtists, Suzuri.jp, .email, .biz, padlet.com



m.mainz.json

871 B

02:39



report_m.mainz.html

113.1 KB

02:39



Разбор OSINT CTF

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



Maigret OSINT bot

bot



mainz.m 02:40 ✓✓

mainz.m

Finished! 02:40

mainz.m

12 exact accounts found:

YandexCollections API, Pbase, Hoobly, Askvoprosy, Anapakurort,
GeniusArtists, Suzuri.jp, .me, .biz, .email, exploretalent.com,
padlet.com



mainz.m.json

871 B

02:41



report_mainz.m.html

106.0 KB

02:41

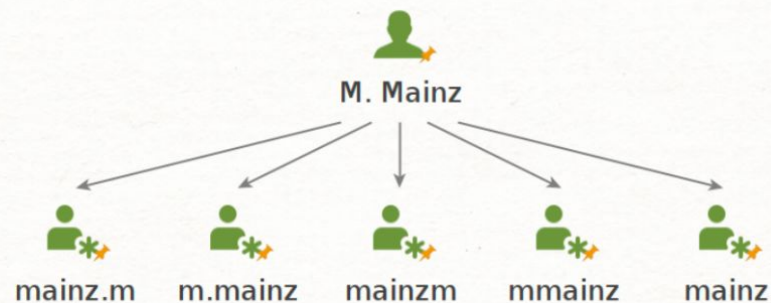


Разбор OSINT CTF

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



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



Разбор OSINT CTF

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



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

The screenshot shows the Facebook profile of Maik Horn. The profile picture is a circular photo of two young men. The cover photo is a landscape image of a forest. The name 'Maik Horn' is displayed prominently. Below the name are buttons for 'Добавить' (Add) and 'Сообщение' (Message). The navigation bar includes 'Публикации' (Posts), 'Информация' (Info), 'Друзья' (Friends), 'Фото' (Photos), 'Видео' (Videos), 'Музыка' (Music), and 'Ещё' (More). The 'Публикации' section is active, showing a post from Maik Horn dated 25 February 2019, featuring a graphic with the European Union flag and the text 'Hey! What are you uploading? The internet is being endangered by article 13. Help saving it! www.savetheinternet.info'. The left sidebar shows 'Краткая информация' (Quick Info) with 'Steve Cutts' and 'Подписчики: 1 человек' (Followers: 1 person).

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.

Moscow OSINT meetup №3
Методы анонимизации в Сети:
КАК ИСКАТЬ, НО НЕ БЫТЬ
НАЙДЕННЫМ
@dukera



mainzm / my.first.repo Public

<> Code Issues Pull requests Actions Projects Security In

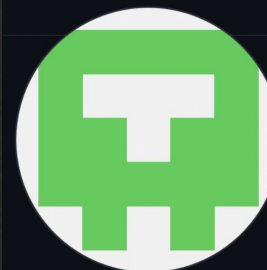
main 1 branch 0 tags

mainzm Add files via upload

README.md	Initial commit
main.cpp	Add files via upload

README.md

my.first.repo



Mario Mainz
mainzm

Follow

Overview Repositories 2 Projects Packages Stars

Popular repositories

my.first.repo

Public

my.second.repo

Public

6 contributions in the last year



<> Code Issues Pull requests Actions Projects Security In

main my.first.repo / main.cpp

mainzm Add files via upload

1 contributor

6 lines (5 sloc) 77 Bytes


```
1 #include <iostream>
2
3 int main()
4 {
5     std::cout << "I'm a biologist!\n\n";
6 }
```


Разбор OSINT CTF

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



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.

 mainzm

Профиль

Наблюдения

Календарь

Идентификации

Списки

Журнал

Фавориты

Проекты

Наблюдения

13

Вид

13

Идентификации

105

Сообщения в журнале

0

Списки

0

Подписчики

0

Mario Mainz

Регистрация: Окт 06, 2021 Последняя активность: Окт 21, 2022 iNaturalist

Prof. Dr.
<https://vk.com/97mario79>

Подписан на 0 человек

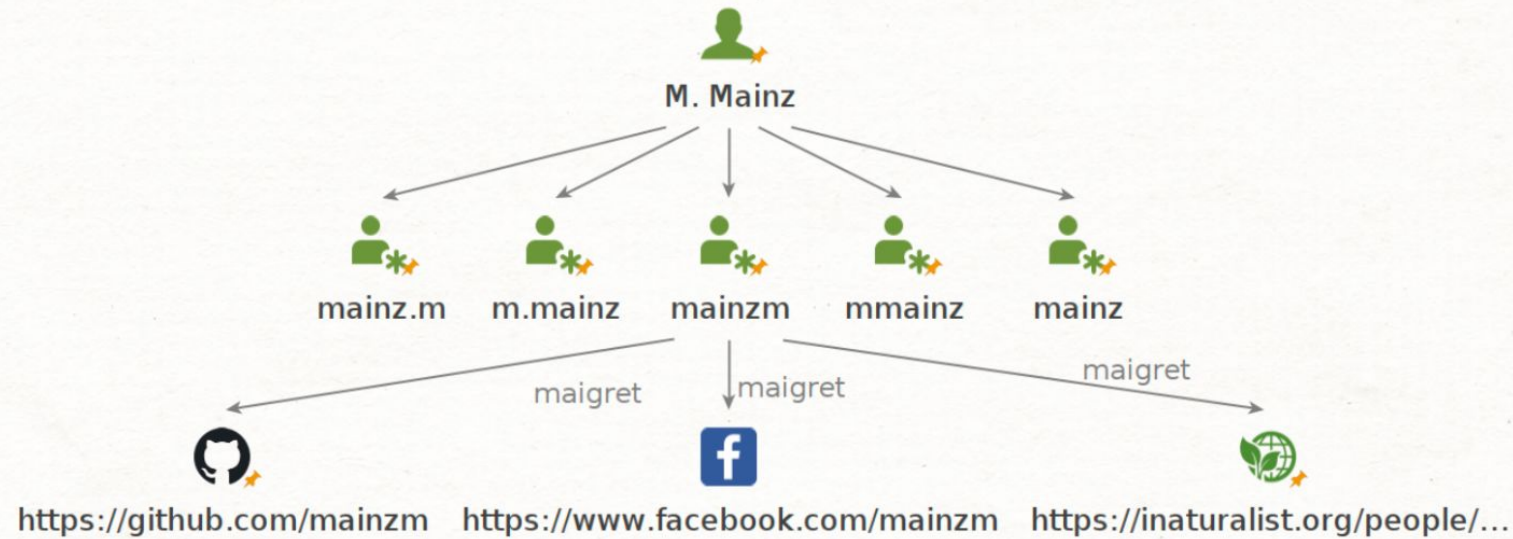
mainzm ни на кого не подписан.

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

В профиле прикреплена ссылка на страницу ВКонтакте.

Разбор OSINT CTF

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



Разбор OSINT CTF

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



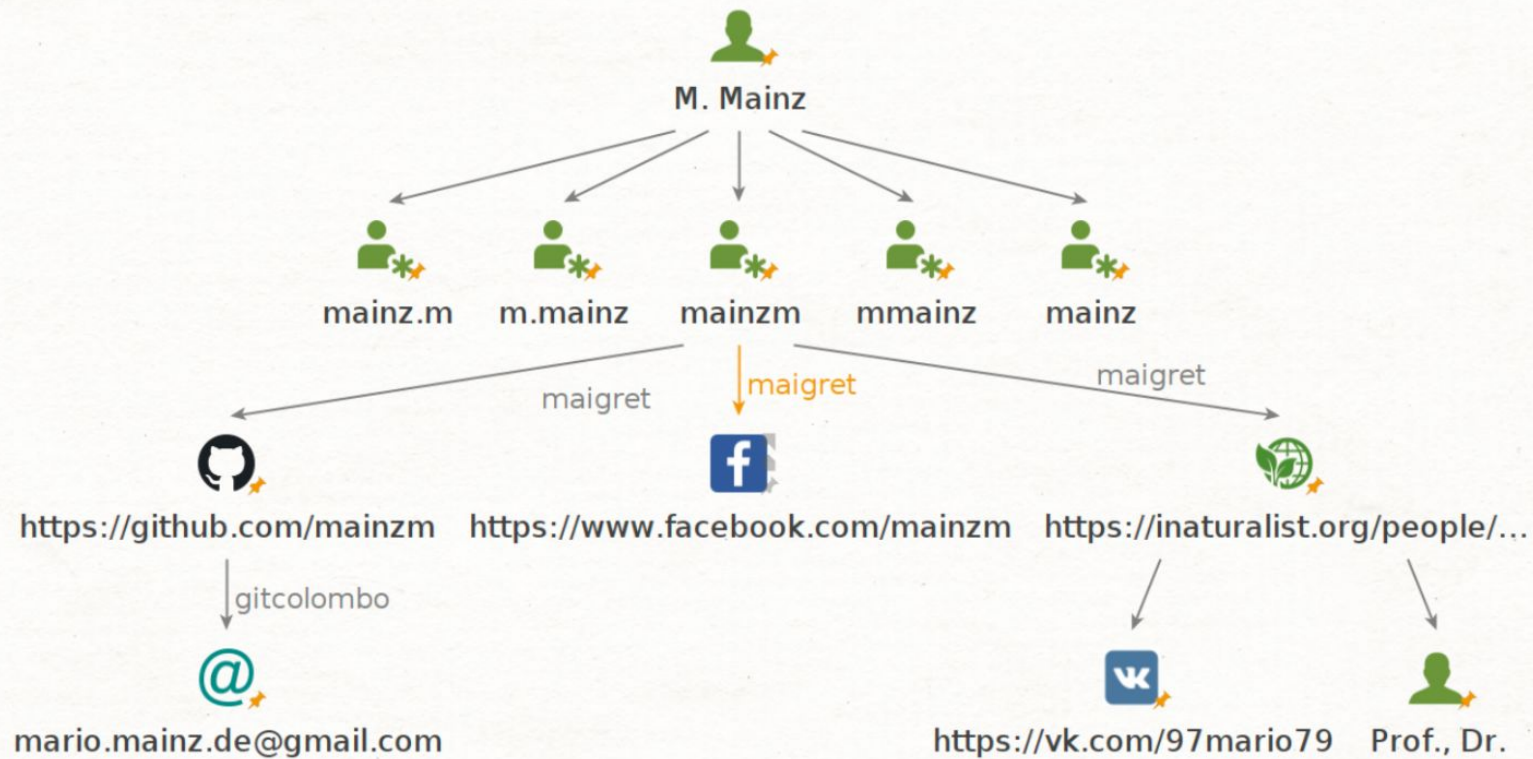
Воспользуемся gitcolombo (<https://github.com/soxoj/gitcolombo>) и проанализируем репозиторий.
Таким образом, получим почту: mario.mainz.de@gmail.com

```
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:
Also appears with: https://github.com/mainzm
GitHub noreply@github.com
-----
Name: Mario Mainz
Email: 116330840+mainzm@users.noreply.github.com
Appears as author: 1 times
Verified account:
Also appears with: https://github.com/mainzm
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

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



Разбор OSINT CTF

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



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.


```
kali@kali: ~
*****
mario.mainz.de@gmail.com
*****
[x] about.me
[+] adobe.com / .....77
[-] amazon.com
[x] amocrm.com
[-] any.do
[-] archive.org
[-] armurerie-auxerre.com
[x] atlassian.com
[-] axonaut.com
[x] babeshows.co.uk
[x] badeggsonline.com
[x] bios-mods.com
[x] biotechnologyforums.com
[x] bitmoji.com
[x] blablacar.com
[x] blackworldforum.com
[x] blip.fm
[x] forum.blitzortung.org
[x] bluegrassrivals.com
[-] bodybuilding.com
[x] buymeacoffee.com
[x] discussion.cambridge-mt.com
[-] caringbridge.org
[x] chinaphonearena.com
[x] clashfarmer.com
[x] codecademy.com
[x] forum.codeigniter.com
[x] codepen.io
[-] coroflot.com
[x] cpaelites.com
[x] cpahero.com
[x] cracked.to
[x] crevado.com
[-] deliveroo.com
[x] demonforums.net
[x] devrant.com
[-] diigo.com
[-] discord.com
[-] docker.com
[x] dominos.fr
[x] ebay.com
[x] ello.co
[-] envato.com
```

Разбор OSINT CTF

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




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?



Марио Майнц
1 дн
Добавить в друзья
Ещё ▾

Фото



Показать всё

Пользователь пока не добавил друзей
и не подписался
на сообщества

Подробная информация

@ 97mario79

Личная информация

Языки: Русский

Контактная информация

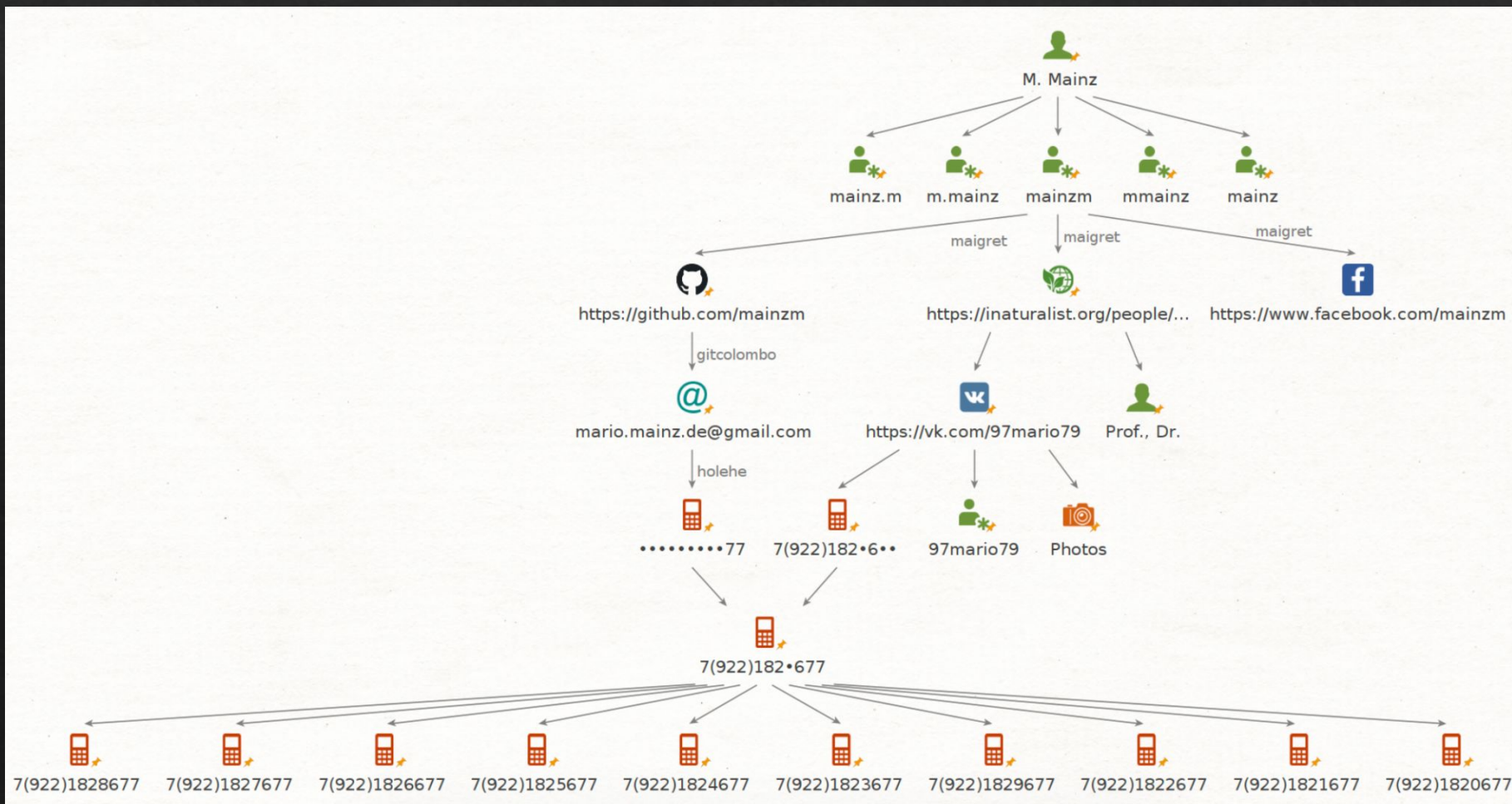
Моб. телефон: +7 (922) 182-*6-**

Разбор OSINT CTF

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



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

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



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

User Info



Mario

last seen within a week



+7 922 182 9677

Mobile

@m41nzm

Username

[ADD TO CONTACTS](#)



Notifications



[SEND MESSAGE](#)



Share this contact



[Block user](#)



Разбор OSINT CTF

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



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.



Mario Mainz

Добавить

Сообщение

Публикации **Информация** Друзья Фото Видео Посещения Ещё ▾

Информация

Общие сведения

Работа и образование

Места проживания

Контактная и основная информация

Семья и отношения

Информация о Mario

События из жизни

Контактная информация

✉ mario.mainz.de@gmail.com
Электронный адрес

Веб-сайты и социальные сети

🔗 Нет ссылок

Основная информация

🎂 24 апреля
Дата рождения

1979
Год рождения



Mario Mainz

Фото Mario

Альбомы

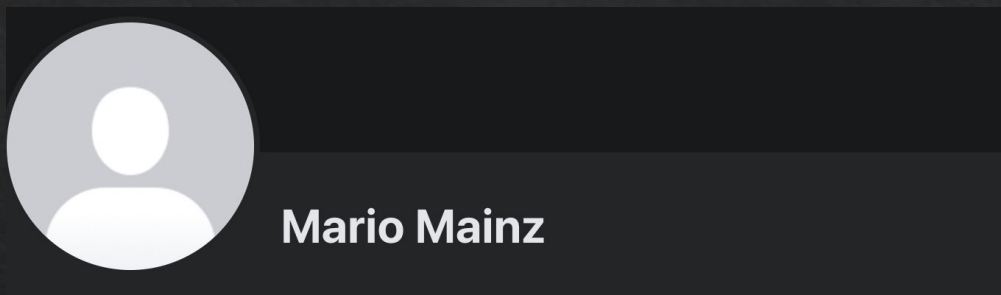


Разбор OSINT CTF

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



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.



Публикации Информация Друзья **Фото** Видео Посещения Ещё ▾

Фото

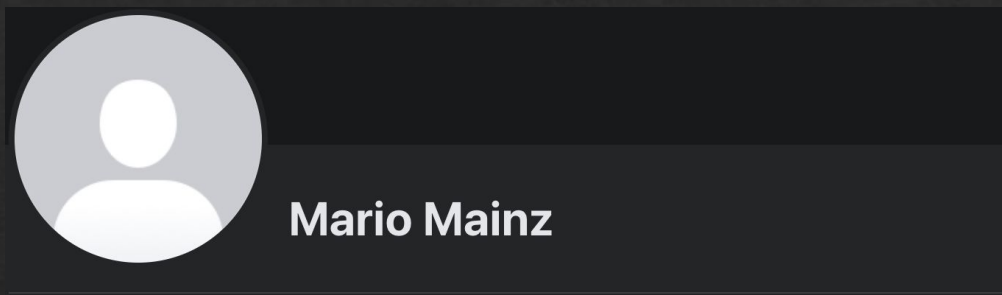
Фото Mario **Альбомы**



just walking from work
12 объектов



trip
3 объекта



Публикации Информация Друзья **Фото** Видео Посещения Ещё ▾

trip

1 публикация · 3 объектов · 1 соавтор · 🌐

👍 Нравится

💬 Комментировать



Разбор OSINT CTF

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



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

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



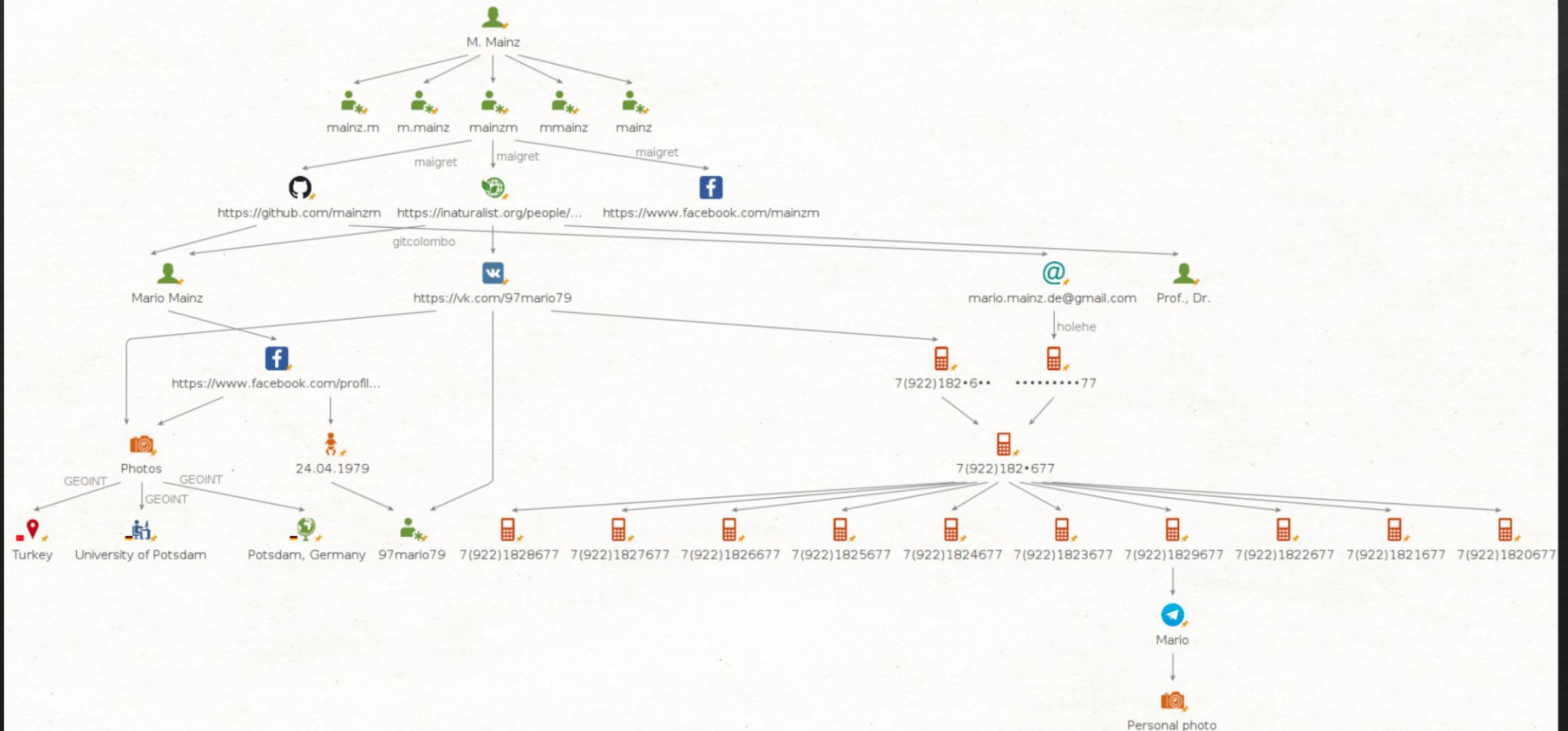
Фото из Facebook



Фото из Google

Разбор OSINT CTF

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



Разбор OSINT CTF

Имя и фамилия: Mario Mainz

Возраст: 43 года

Место жительства (страна, город): Германия,
Потсдам

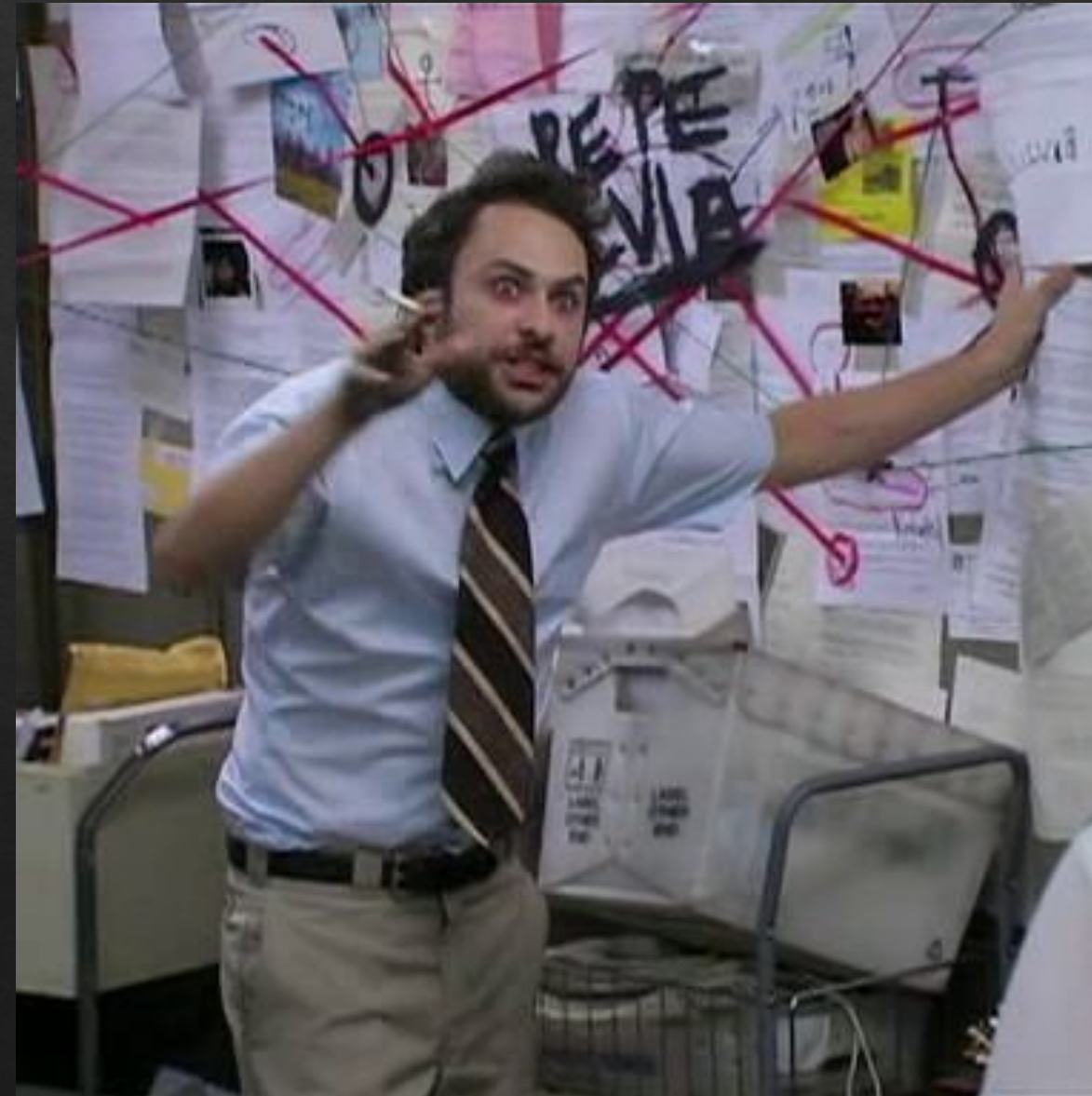
Место работы и должность: Университет Потсдама,
профессор

Цвет глаз: зеленый

Номер телефона: +79221829677

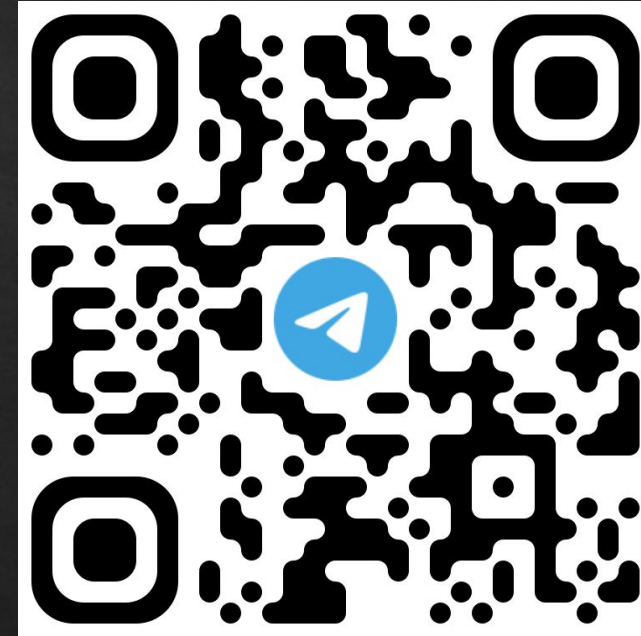
Недавние путешествия: Турция

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





https://t.me/osint_mindset



https://t.me/infosec_dukera

The End

Спасибо. Вопросы?