

/февраль  
2022

BEHOLDER  
IS  
HERE

CONSULTING

# 10 **ЛУЧШИХ** БЕСПЛАТНЫХ OSINT ИНСТРУМЕНТОВ

по версии **t.me/forensictools**



..то, что мы **используем** в работе сами и нам это нравится!

# 10. SOCIAL OSINT ПОИСК ЧЕЛОВЕКА В СОЦИАЛЬНЫХ СЕТЯХ И СЕРВИСАХ

BEHOLDER  
IS  
HERE

CONSULTING

## SNOOP

[ [github.com/snooppr/snoop](https://github.com/snooppr/snoop) ]

Инструмент для анализа различных сайты, форумов и социальных сетей на предмет наличия искомого имени пользователя, т.е. позволяет определить на каких сайтах присутствует пользователь с указанным ником. Проект разработан на материалах исследовательской работы в области скрапинга публичных данных. На данный момент поисковая база содержит 2400 сайтов!

И субъективно, одно из лучших решений для OSINTа в русскоязычном сегменте интернета.

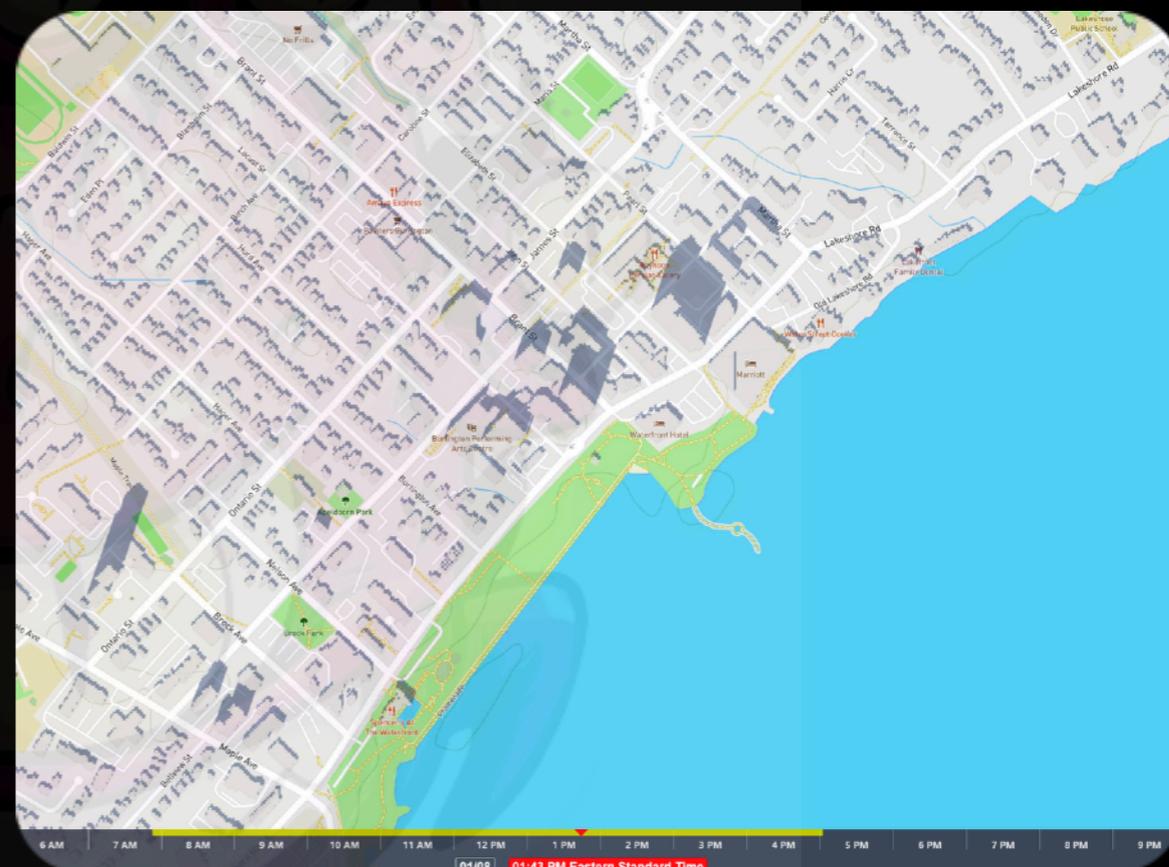
```
ужена локальная база: 60_Websites
языскиваем: < beholderishere >
0% [-] 3dnews: Увы!
2% [-] About.me: Увы!
3% [-] Audiojungle: Увы!
5% [-] Autokadabra: Увы!
7% [-] Badoo: Увы!
8% [-] BitBucket: Увы!
10% Wr Blogger: https://beholderishere.blogspot.com
12% [-] Championat: Увы!
13% [-] Couchsurfing: Увы!
15% [-] D3: Увы!
17% [-] Disqus: Увы!
18% [-] Donationalerts: Увы!
20% [-] Ebay: Увы!
22% Wr Facebook: https://www.facebook.com/beholderishere
23% [-] Forum_guns: Увы!
25% [-] Forumhouse: Увы!
27% [-] GitHub: Увы!
28% RU Habr: https://habr.com/ru/users/beholderishere
30% [-] HackTheBox: Увы!
32% [-] HackerOne: Увы!
33% [-] Hunting: Увы!
35% [-] Igromania: Увы!
37% Wr Instagram: https://www.instagram.com/beholderishere
38% [-] Irecommend: Увы!
40% [-] Kali_community: Увы!
42% [-] LOR: Увы!
43% Wr Medium: https://medium.com/@beholderishere
45% [-] Music-rock: Увы!
47% [-] My_mail_ru_new: Увы!
48% [-] My_mail_ru_old: Увы!
50% [-] OK: Увы!
52% [-] Pastebin: Увы!
53% [-] Pedsovet: Увы!
55% Wr Periscope: https://www.periscope.tv/beholderishere/
57% RU Pikabu: https://pikabu.ru/@beholderishere
58% Wr Pornhub: https://rt.pornhub.com/users/beholderishere
60% [-] Professionali: Увы!
62% [-] Radio_echo_msk: Увы!
63% [-] RamblerDating: Увы!
65% [-] Rapforce: Увы!
67% [-] Reddit: Увы!
68% [-] Ошибка соединения: Rutracker
```

### Shademap

[ [shademap.app](https://shademap.app) ]

Карта движения теней, которая учитывает все здания и городской рельеф, показывая расположение тени как в реальном времени, так и на любые выбранные дату и время. В наличии очень интуитивный интерфейс и режим 3D- карты.

Очень наглядное решения, хоть и не такое информативное как [suncalc](#) и [mooncalc](#).



# 8. DATA analyze

## СТРУКТУРИРОВАНИЕ ДАННЫХ

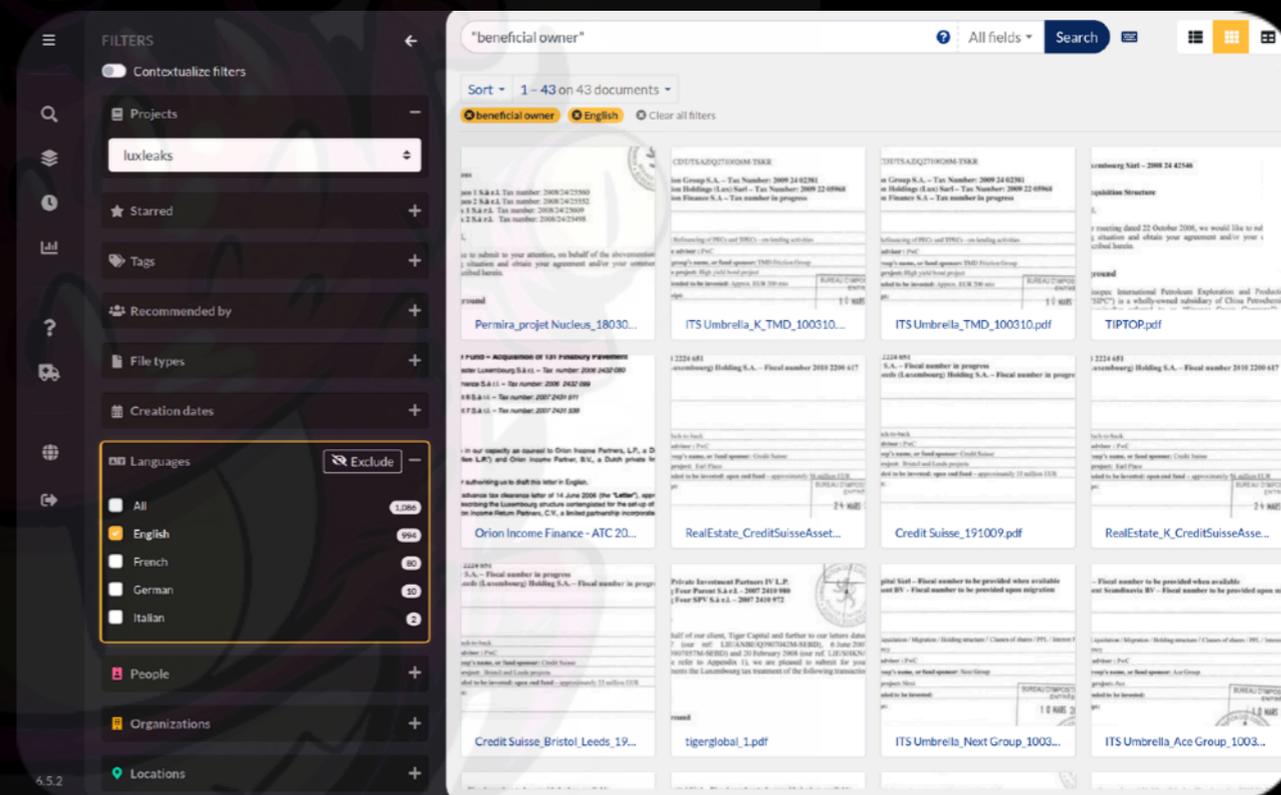
### Datashare

[ [datashare.icij.org](https://datashare.icij.org) ]

Инструмент для агрегации, хранения и анализа данных. Особенно хорош для командной работы.

#### Возможности:

- индексировать и сохранять ваши документы в базе данных, ставить теги на документы
- искать PDF-файлы, изображения, тексты, электронные таблицы, слайды и любые файлы одновременно, а также осуществлять поиск по содержимому
- фильтровать документы по различным параметрам, операторам и регулярным выражениям
- производить автоматическое обнаружение людей, организаций и местоположений
- умеет алгоритмы обработки естественного языка, пакетный поиск
- устанавливать плагины и расширения
- использовать приложение в качестве сервера для обмена документами между несколькими пользователями



# 7. SOCIAL OSINT ВОССТАНАВЛИВАЕМ СОЦИАЛЬНЫЙ ГРАФ

## SOCIAL MAPPER

[ [github.com/Greenwolf/social\\_mapper](https://github.com/Greenwolf/social_mapper) ]

Инструмент с открытым исходным кодом, который использует распознавание лиц для масштабной корреляции профилей социальных сетей на разных сайтах. Он использует автоматизированный подход к поиску популярных социальных сетей по именам и фотографиям целей, чтобы точно обнаружить цель, выводя результаты в отчет.

Social Mapper имеет множество применений - например, автоматизированный сбор большого количества профилей в социальных сетях для использования в целевых фишинговых кампаниях. Распознавание лиц помогает этому процессу, удаляя ложные срабатывания в результатах поиска, чтобы быстрее просматривать эти данные.

The screenshot shows the Social Mapper interface with a grid of social media profiles for Jacob Wilkin. The grid has columns for Photo, Name, LinkedIn, Facebook, Twitter, and Instagram. Below the grid, an Excel spreadsheet is visible, showing the results of the search. The spreadsheet has columns for Name, Email, and Facebook profile URLs.

| Photo | Name         | LinkedIn   | Facebook  | Twitter | Instagram |
|-------|--------------|------------|-----------|---------|-----------|
|       | Jacob Wilkin | GooglePlus | YKontakte | Weibo   | Douban    |

| A        | B          | C                  | D                         | E   |   |
|----------|------------|--------------------|---------------------------|---|---|
| Jacob    | Wilkin     | Jacob Wilkin       | jwilkin@trustwave.com     | https://www.facebook.com/jacobwilkin123?ref=br_rs       | https://scontent-waw1-1.xx.fbcdn.net/v/t1.0-1/p320x320/     |
| Lawrence | Munro      | Lawrence Munro     | lmunro@trustwave.com      | https://www.facebook.com/lawrence.munro?ref=br_rs       | https://scontent-waw1-1.xx.fbcdn.net/v/t1.0-1/c0.0.320.320/ |
| Hans     | Boshoff    | Hans Boshoff       | hboshoff@trustwave.com    | https://www.facebook.com/johannes.boshoff.167?ref=br_rs | https://scontent-waw1-1.xx.fbcdn.net/v/t1.0-1/p320x320/     |
| Michael  | Gianarakis | Michael Gianarakis | mgianarakis@trustwave.com | https://www.facebook.com/mgianarakis?ref=br_rs          | https://scontent-waw1-1.xx.fbcdn.net/v/t1.0-1/p320x320/     |

## GEOWIFI

[ [github.com/GONZOosint/geowifi](https://github.com/GONZOosint/geowifi) ]

Скрипт позволяющий определить фактическое местоположение беспроводных точек доступа по BSSID и SSID основываясь на открытых данных из таких сервисов как Wigle, Apple, OpenWifi и через API Mylnikov.

```
GEO WIFI by GONZO

----- MAC DATA -----
[-] BSSID: A0:F3:90
[-] Vendor: TP-LINK TECHNOLOGIES CO.,LTD.
[-] MAC type: MA-L

----- LOCATION DATA -----
[📍] Wigle results: not_found
[📍] Apple results: not_found
[📍] OpenWiFi results: 6 23499, 3 07328
[📍] Milnikov results: not_found
[📄] Json output saved: results/1644237496_900801.json
[🗺] Map output saved: results/1644237496_927158.html
```

# SOCIAL OSINT

## 5. ИЩЕМ ГЕОЛОКАЦИЮ ПОСТОВ В СОЦ СЕТЯХ

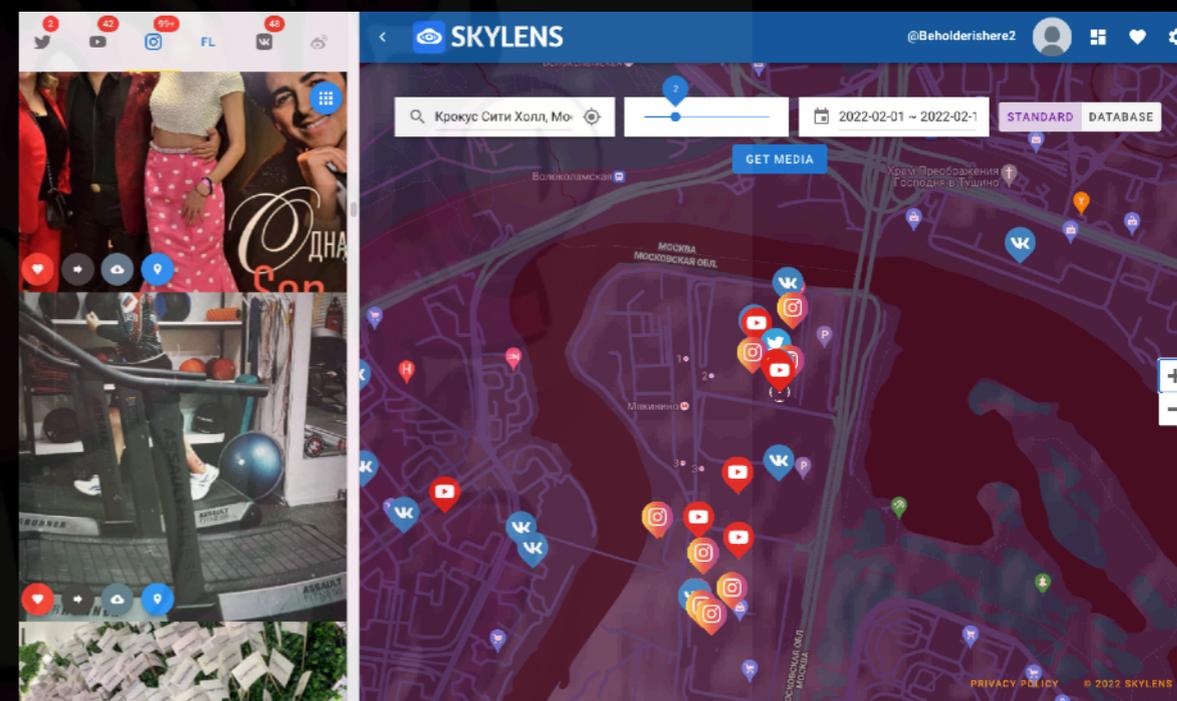
BEHOLDER  
IS  
HERE

CONSULTING

### SKYLENS

[ [app.skylens.io](http://app.skylens.io) ]

Веб-сервис позволяющий просматривать все посты созданные в Twitter, Youtube, Instagram, Flickr, VK и Weibo в определенный момент времени, в определенном радиусе на карте и хештегу.



# 4. DATA verification ПРОВЕРКА ВИДЕО НА ПОДЛИННОСТЬ

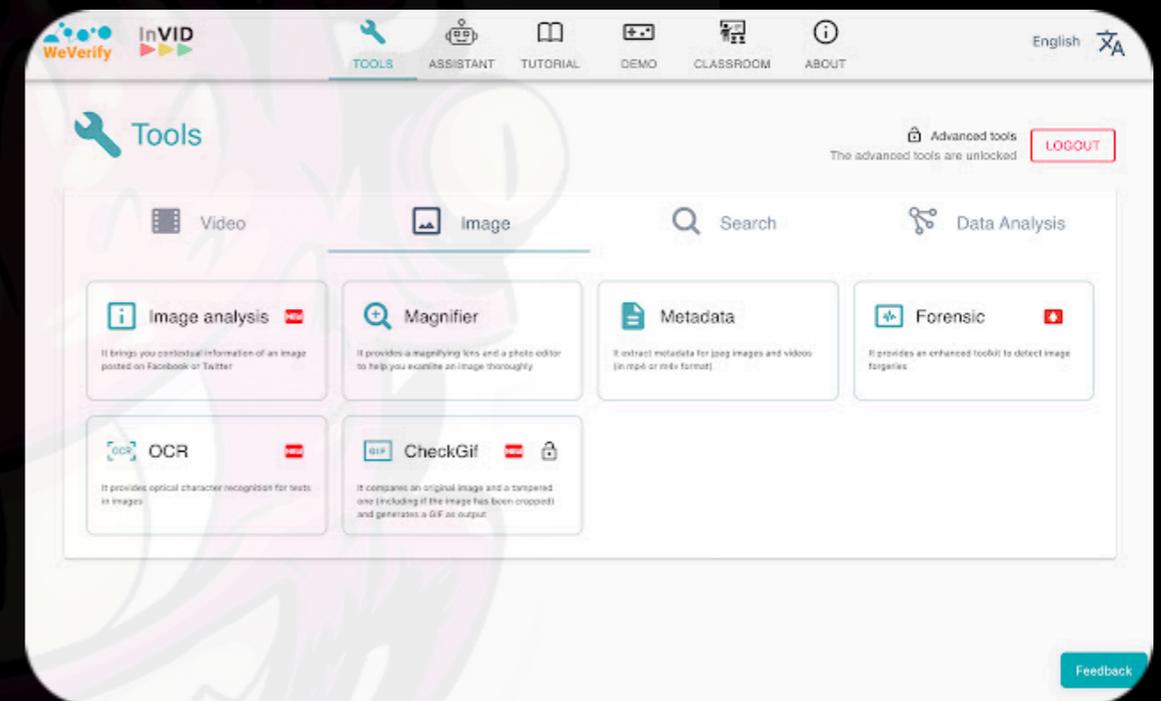
BEHOLDER  
IS  
HERE

CONSULTING

## InVID-WeVerify

[ [invid-project.eu/tools-and-services/invid-verification-plugin](https://invid-project.eu/tools-and-services/invid-verification-plugin) ]

Расширение для Chrome и Firefox для проверки изображений и видео. С помощью расширения можно получать контекстную информацию о видео Facebook и YouTube, выполнять обратный поиск изображений в поисковых системах Google, Baidu или Яндекса, посмотреть метаданные, поискать по ключевым кадрам, узнать, кто первый загрузил видео или изображение в сеть, чтобы установить авторство.



# SOCIAL OSINT

## 3. ПОИСК ЛЮДЕЙ ПО ФОТО В СОЦИАЛЬНЫХ СЕТЯХ

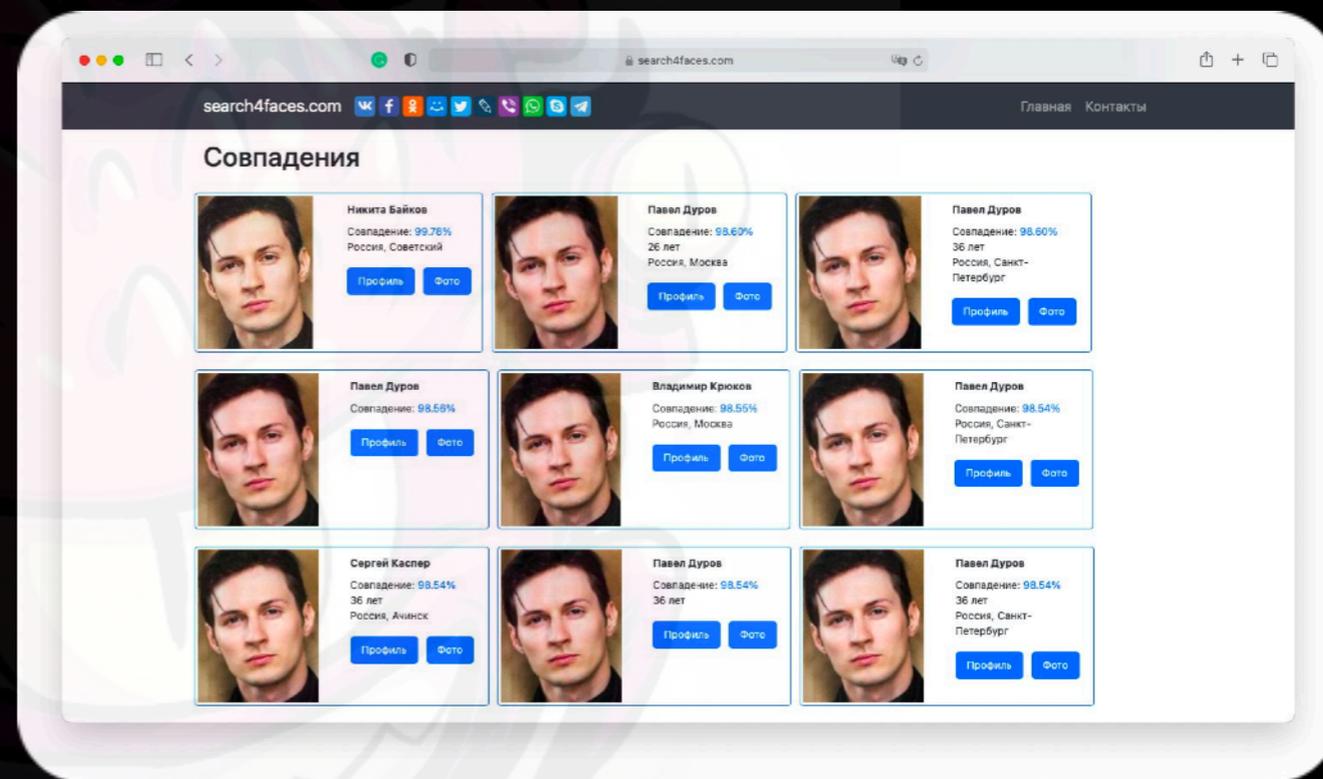
BEHOLDER  
IS  
HERE

CONSULTING

### Search4face

[ [search4faces.com](https://search4faces.com) ]

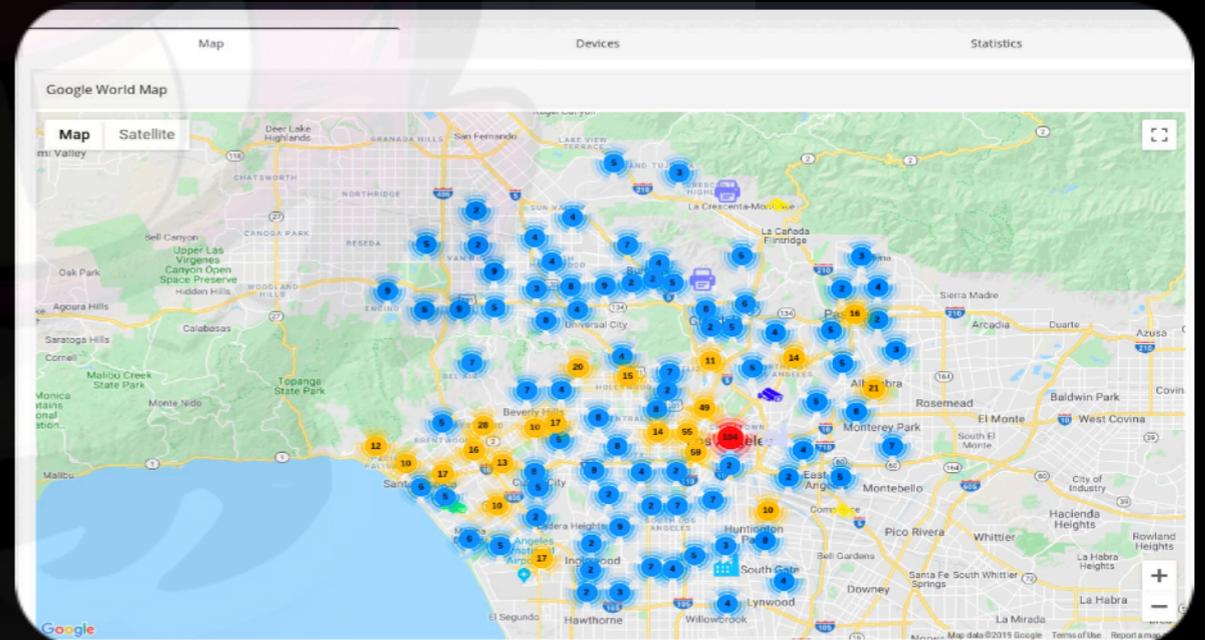
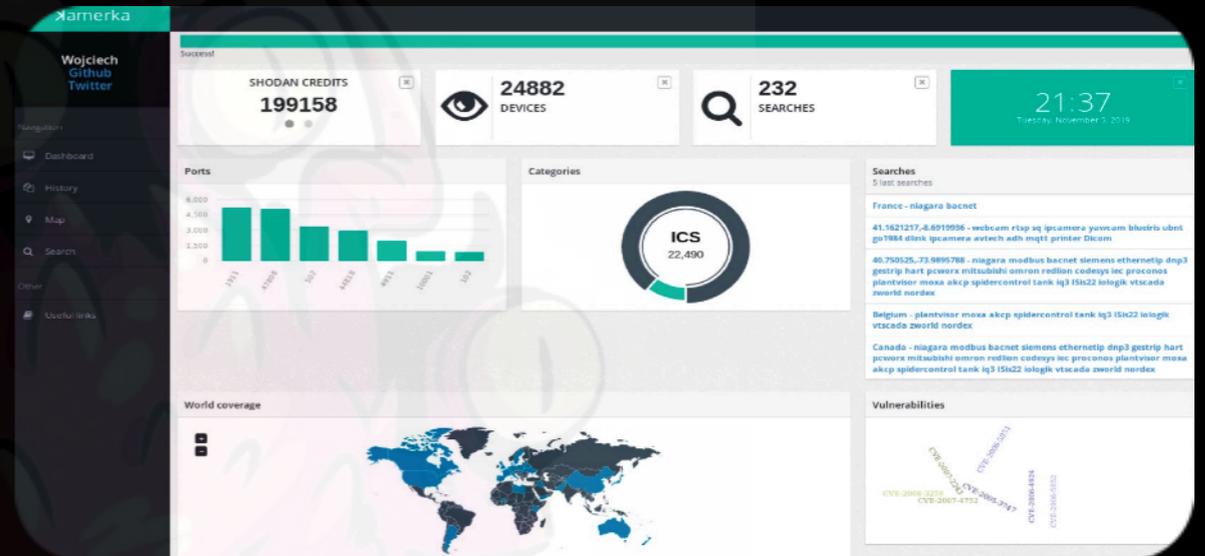
Поисковый сервис поиска по фото (вернее по аватарке) в социальных сетях. Может искать в VK, Одноклассники, Инстаграм, Тикток, Клубхауз.



### Kamerka-GUI

[ <https://github.com/woj-ciech/Kamerka-GUI> ]

Поисковый инструмент построенный на движке Shodan для поиска устройств интернета вещей и контрольных панелей промышленных устройств смотрящих в интернет. Отличный инструмент дополняющий возможности Shodan и делающий работу с ним удобней и информативней.



## WAYBACK MACHINE

[ [web.archive.org](http://web.archive.org) ]

Самый большой интернет архив. Поиск удаленных из сети страниц, данных и файлов



## 1. Технический аудит

# T.ME/FORENSICTOOLS

### 1.1. Аудит информационной безопасности

- Аудит сетевой инфраструктуры
- Аудит внедренных политик безопасности и их актуальность
- Тестирование на проникновение в информационную инфраструктуру
- Аудит актуальности мер защиты относительно модели угроз ИБ

### 1.2. Аудит технических систем безопасности (видеонаблюдение, скуд, опс)

- Проверка проектной и рабочей документации и ее актуальность
- Проверка технического состояния установленных систем безопасности
- Проверка целесообразности размещения элементов ТСБ для эффективного решения задач безопасности относительно модели угроз
- Проверка конфигураций программной платформы системы безопасности
- Проверка конфигураций аппаратных элементов системы безопасности.

## 2. Ситуационный аудит

- Проведение исследований на проникновение в защищенный периметр компании для тестирования эффективности противодействия к определенным моделям угроз и противодействию им.

## 3. Моделирование угроз

- Ситуационные симуляции для изучения поведения сотрудников компании при определенных моделях угроз информационной безопасности (фишинговый рассылки, имитация хакерских атак, имитация утечек информации)
- Ситуационные симуляции для изучения поведения сотрудников СБ при определенных моделях угроз (физическое проникновение, рейдерский захват, террористическая угроза)

## 4. Определение модели угроз и нарушителей

Описание существующих угроз безопасности, их актуальности, возможности реализации и последствий.

- Выявление критичных объектов информационной инфраструктуры.
- Определение перечня угроз для каждого критического объекта.
- Определение способов реализации угроз.
- Определение модели нарушителя.
- Оценка материального ущерба и других последствий возможной реализации угроз.

## 5. Форензика

- Криминалистический анализ информационных систем на наличие определенных данных.
- Криминалистический анализ компьютеров, смартфонов, планшетов, телефонов, дронов направленный на извлечение данных различных сервисов.
- Восстановление данных с носителей, смартфонов, компьютеров.
- Проведение расследований случаев промышленного шпионажа.
- Поиск технических каналов утечки информации.

