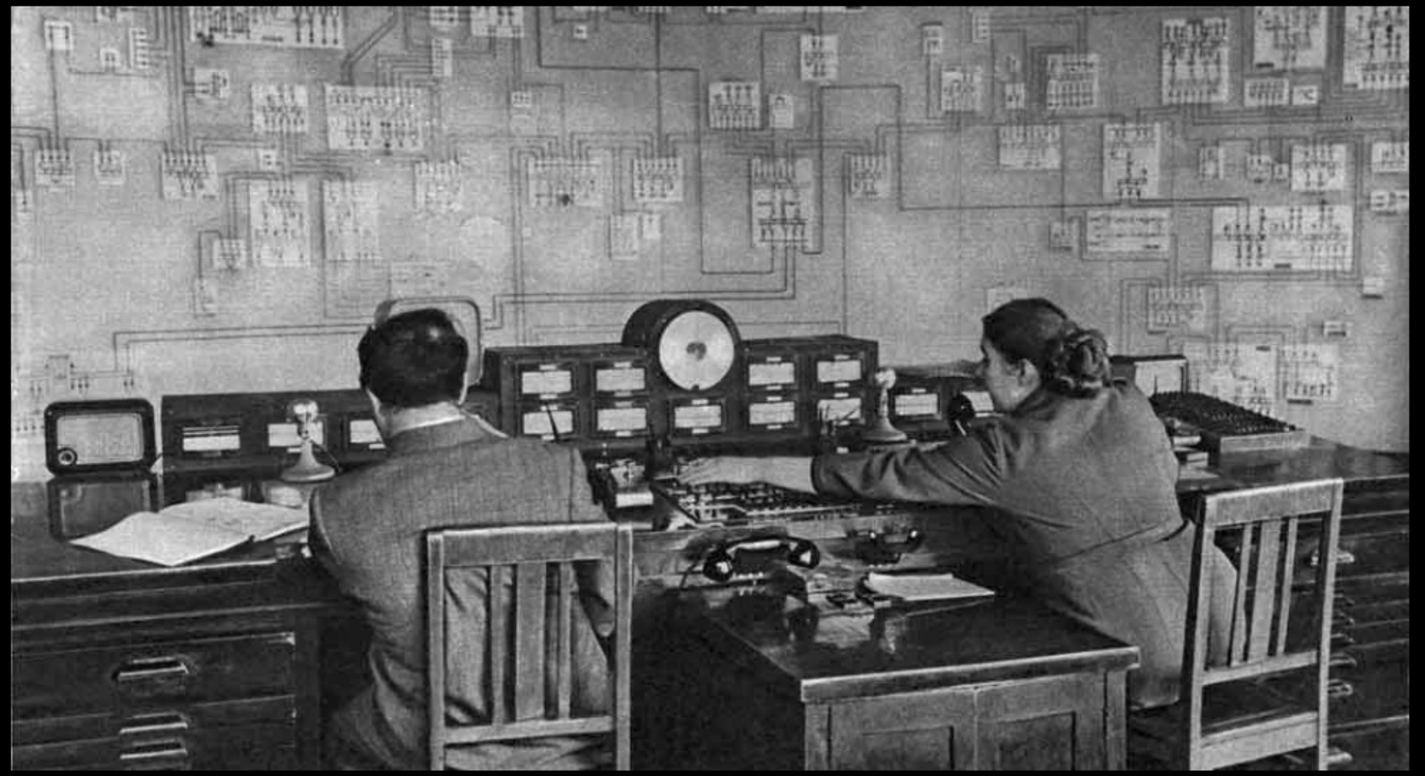
# OSINT в расследовании киберинцидентов v 0.0.2

Куплено
благодаря
Skladchik.com

ДОКЛАДЧИК: **@soxoj**

# Open-source intelligence
# Разведка на основе открытых источников

90 процентов разведданных приходит из открытых источников [1]



**Пример:** ЦРУ составило схему электроснабжения советской ядерной программы по фотографии из журнала “Огонёк” [2]

[1] https://vpk-news.ru/articles/7324

[2] https://vakhnenko.livejournal.com/235426.html

# РАССЛЕДОВАНИЕ КИБЕРИНЦИДЕНТОВ



- Внешний нарушитель
  - DoS
  - Фишинг
  - Малварь
- Внутренний нарушитель
  - Утечки данных
  - Атаки изнутри

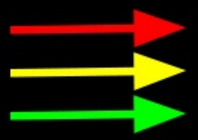
Основная цель -- **определение субъекта-нарушителя**

**Примеры:** Конкурентная разведка на PHDays [1], CTF HackIt-2017 [2]

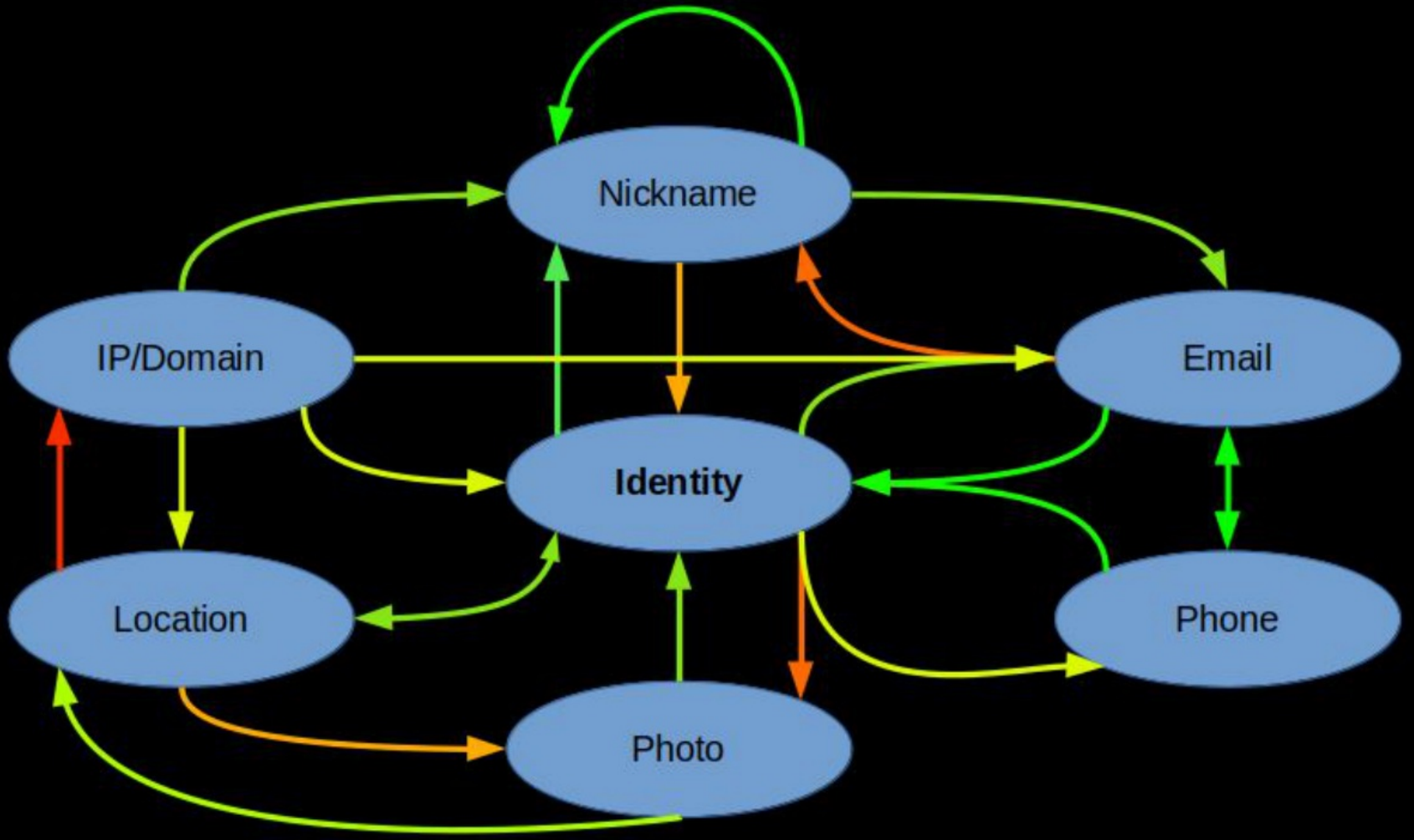
[1] https://habr.com/ru/company/pt/blog/413203/
[2] https://habr.com/ru/post/338078/

# СХЕМА ПОИСКА НАРУШИТЕЛЯ





Градации точности и эффективности, от низких до высоких



# БАЗОВЫЕ ПРИНЦИПЫ ПОИСКА



Мало сделать запрос в Google, надо уметь им пользоваться.

- Составить план
- Уточнять запросы
- Отсекать лишнее
- Обновлять цель
- Понимать, где и что искать

*Fravia - реверс-инженер и искатель* [1]

[1] https://t.me/netstalking_overground/78

# IP-АДРЕСА



**Получение**

- Изначально известные данные
- Определение по домену
  - Обход CDN: Cloudfail, etc.
- Поиск по местоположению (Wi-Fi -- BSSID)
  - 3wifi.stascorp.com [1]
- Социальная инженерия
  - IP logging

**Использование**

- Домен -> Whois [2] GDPR :(
- Местоположение: GeoIP
- Статистика и логи
  - iknowwhatyoudownload.com
- Блэклисты и спам-базы
- Комментарии на сайтах и форумах
- Запущенные сервисы и другое
  - Shodan, Censys, Zoomeye, Fofa, etc.

**Пример:** нигерийский скам


[1] http://telegra.ph/Instrukciya-po-opredeleniyu-IP-diapazonov-po-koordinatam-03-18

[2] https://medium.com/threat-intel/cybercrime-investigation-insights-bachosens-e1d6312f6b3a

# ПОЧТОВЫЕ ЯЩИКИ



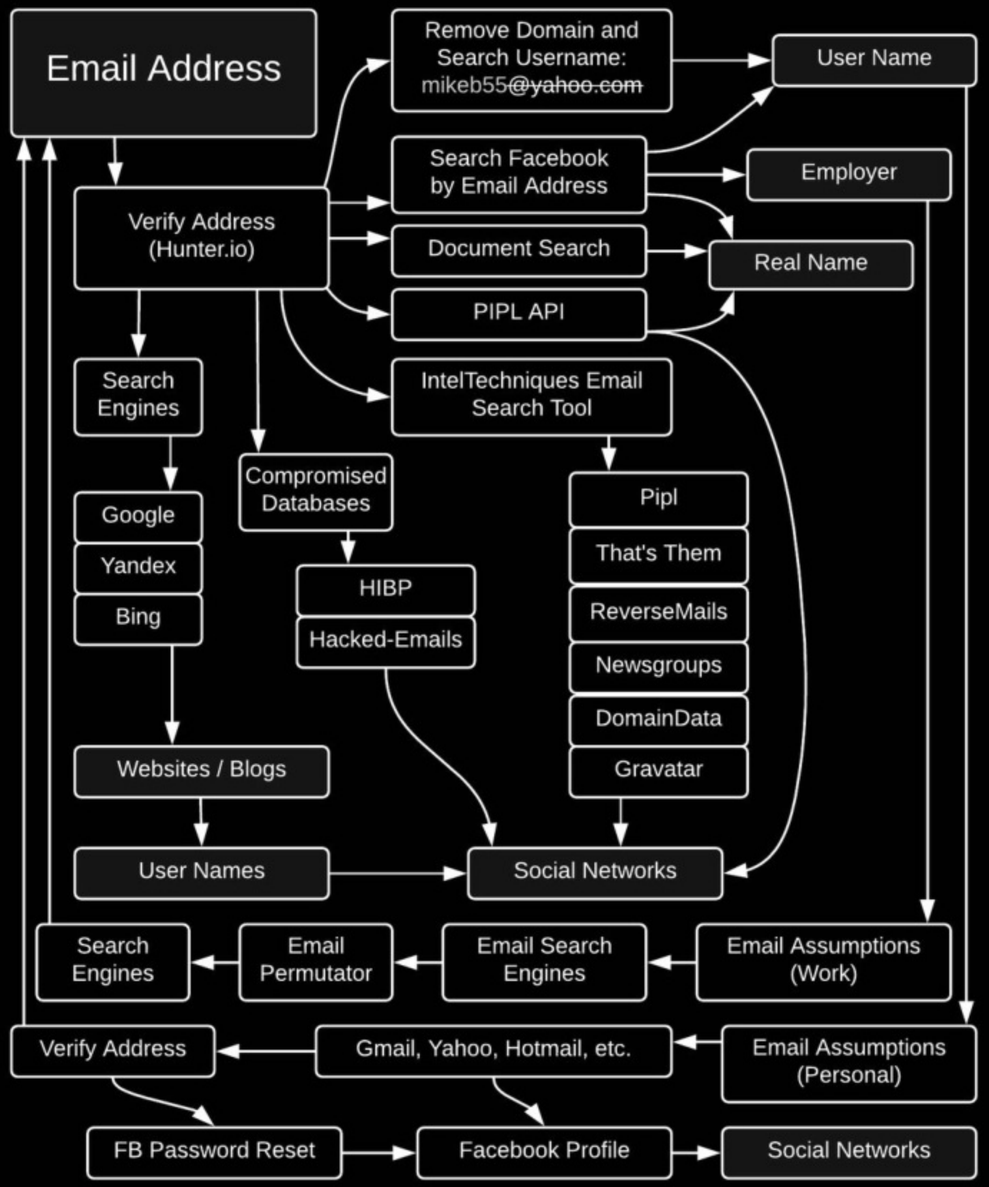
## Получение

- Контакты :)
- Whois
- Восстановление доступа к аккаунтам [1]
- Сервисы
  - hunter.io, snov.io
  - haveibeenpwned.com

## Использование

- Аккаунты соцсетей, форумов, etc.
  - Резервные ящики, телефоны

**Пример:** кейс с обманом скаммера




[1] https://telegra.ph/Kak-ya-po-niknejmu-v-Instagram-nashyol-imya-familiyu-datu-rozhdeniya-propisku-i-nomer-telefona-ego-vladelca-11-13

# НИКНЕЙМЫ



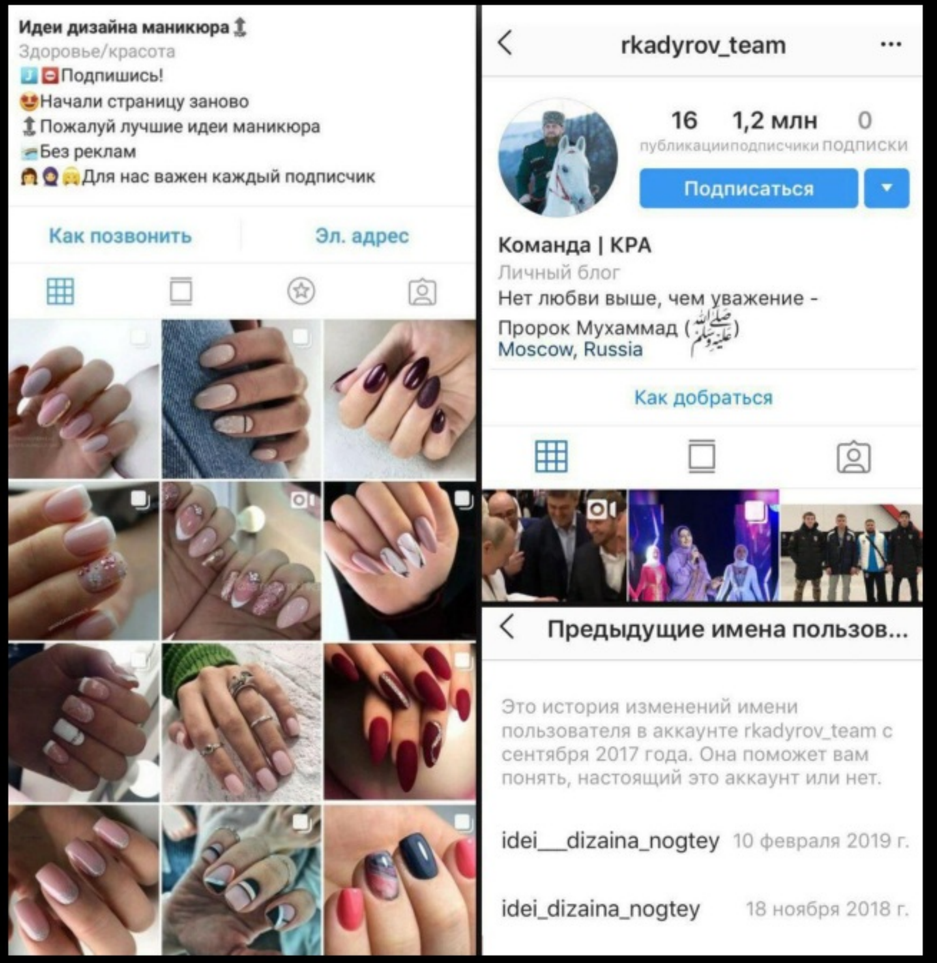
## Получение

- Личные данные
- Метаданные
- История изменений
  - В самих сервисах: Steam, etc. [1]
  - Архивные копии

## Использование

- Аккаунты
  - Ищем ники по никам [2]
  - namechk.com, checkusernames.com, usersherlock.com
- Упоминания
  - socialmention.com
- Авторство
  - search.buzz.im

## **Пример:** переименование аккаунта




[1] https://t.me/buzzfeed_news/1458

[2] https://pikabu.ru/story/mamkinyi_khakeryi_na_strazhe_nezalezhnosti_6629474

# МЕСТОПОЛОЖЕНИЕ



## Получение

- Аккаунты и социальные связи [1]
- Фотографии
- Wikimapia
- Примерное по IP
- Социальная инженерия
  - HTML5 geolocation

## Использование

- Поиск по геометкам в соцсетях
  - VK: photo-map.ru
  - Twitter: onemilliontweetmap.com
  - Youtube: youtube.github.io (self-hosted)
  - Facebook, Flickr, Instagram
- Картографические сервисы
- Региональная специфика

**Пример:** отслеживание связей террористов, похитителей и скаммеров


[1] https://medium.com/@benjamindbrown/tracing-syrian-cell-kidnappers-scammers-finances-through-blockchain-e9c52fb6127d

# ФИО

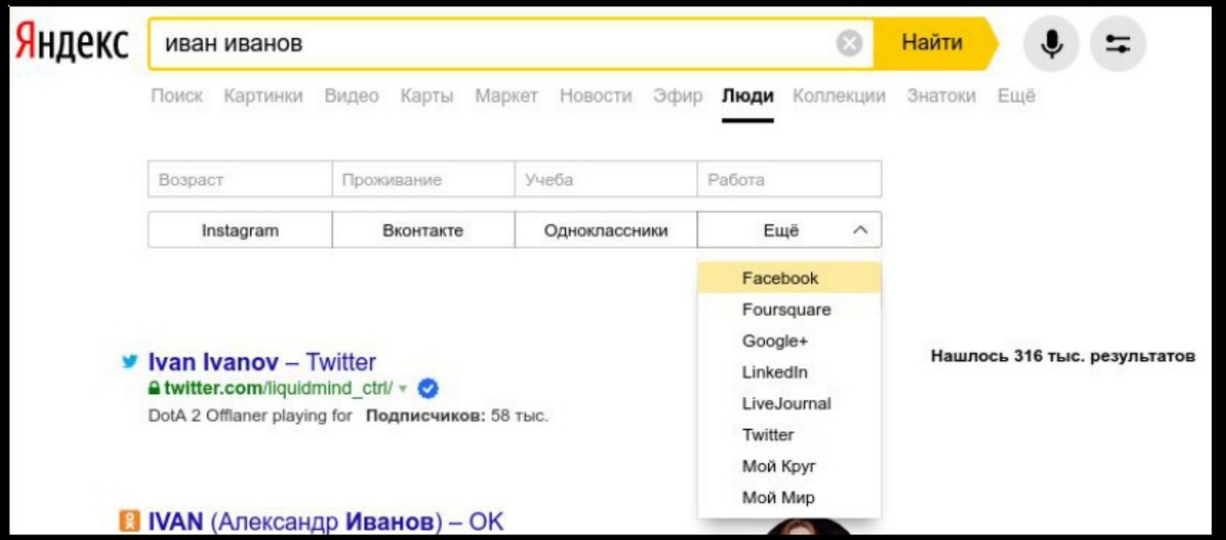


## Получение

- Поиск людей
  - Соцсети
  - PeakYou, people.yandex.ru, etc. [1]
- Государственные идентификаторы [2]
  - Учёба: заведение, группа, etc.
  - Транспорт: номер, VIN, etc.
  - Налоги: ИНН, СНИЛС, etc.
  - Бизнес
  - Паспорт

## Использование

- Соцсети
  - Другие аккаунты, ящики, телефоны
  - Связи [3]
    - VK: vk.barkov.net, 220vk.com
    - Facebook: graph.tips, stalkscan.com
- Государственные идентификаторы [2]




[1] https://cumshoat.blogspot.com/2019/04/osint.html
[2] https://vas3k.ru/blog/389/
[3] https://telegra.ph/Delo-Bogatova-Kto-takoj-Ajrat-Bashirov-05-02

# ТЕЛЕФОННЫЙ НОМЕР



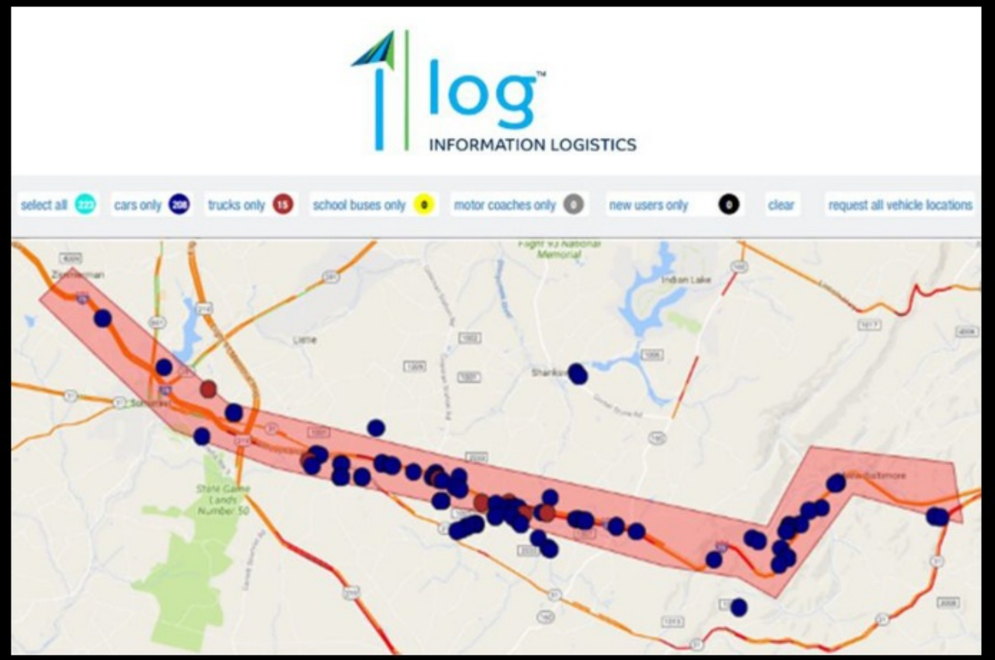
## Получение

- Контакты :)
- Whois
- Восстановление доступа к аккаунтам [1]

## Использование

- Уточнение имени
  - Мессенджеры [2]
  - Интернет-банки [2]
  - Базы [3, 4]
    - nomer.cc, phonenumber.to
    - GetContact @get_kontakt_bot
- Аккаунты соцсетей, форумов, etc.
  - Прямое получение: Facebook
  - Восстановление доступа

**Пример:** LocationSmart [5]




[1] http://web.archive.org/web/20170323165517/http://amdn.news/rassliedovaniie-kto-stoit-za-spinoi-putina-usami-pieskova-surkovskoi-propaghandoi-minoborony-roissi-i-mud-roissi
[2] https://telegra.ph/Pyatiminutnyj-kejs-po-OSINT-3-03-12
[3] https://ftpn.ru/search-phone/
[4] https://t.me/imonfire_official/41
[5] https://www.androidauthority.com/locationsmart-tracking-demo-867138/

# ФОТО

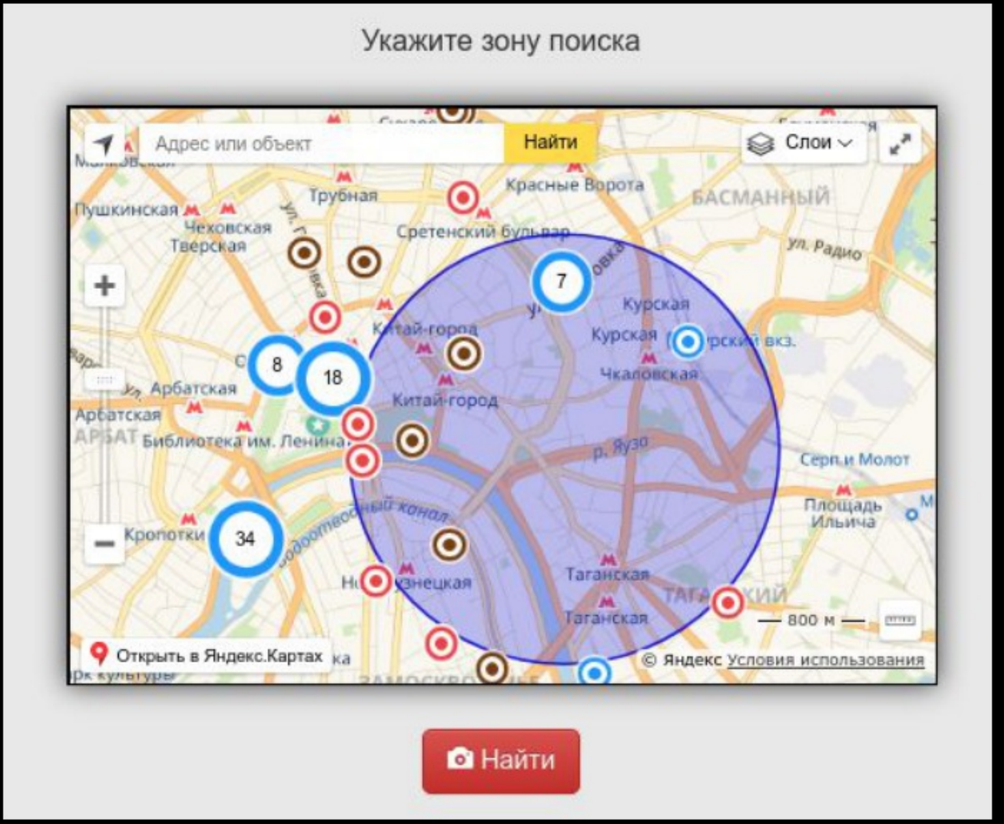


## Получение

- Аккаунты
- Поиск по местоположению
  - Flickr, Instagram, VK, etc. [1]

## Использование

- Поиск по изображениям
  - Google, Yandex, VK, etc. [1]
- Поиск по лицам
  - VK: FindMeVK, FindClone, etc. [1]
  - people.yandex.ru
  - Собственный сервис за полчаса [2]
- Метаданные: EXIF
- Контент




[1] https://cumshoat.blogspot.com/2019/04/osint.html

[2] https://imonfire.xyz/read/post/delaem-svojj-findface-1550974741

# МЕТАДАННЫЕ



## Получение

- Облачные хранилища
  - Владельцы
- Файлы
  - Автор и редактор
  - Debug info
- Git

## Использование

- Никнеймы и ФИО
- Местоположение
- Дата и время -> Местоположение

*“Говорят, здоровый смех продлевает жизнь. Если это в действительности так, то, анализируя полученные образцы стилеров, вирусные аналитики явно выиграли пару-тройку дополнительных лет, ибо смотреть без смеха на подобный чудесный код попросту невозможно”* [1]

[1] https://xakep.ru/2018/05/22/hunting-for-raccoon/

# ПРОФИЛЬ ПОЛЬЗОВАТЕЛЯ

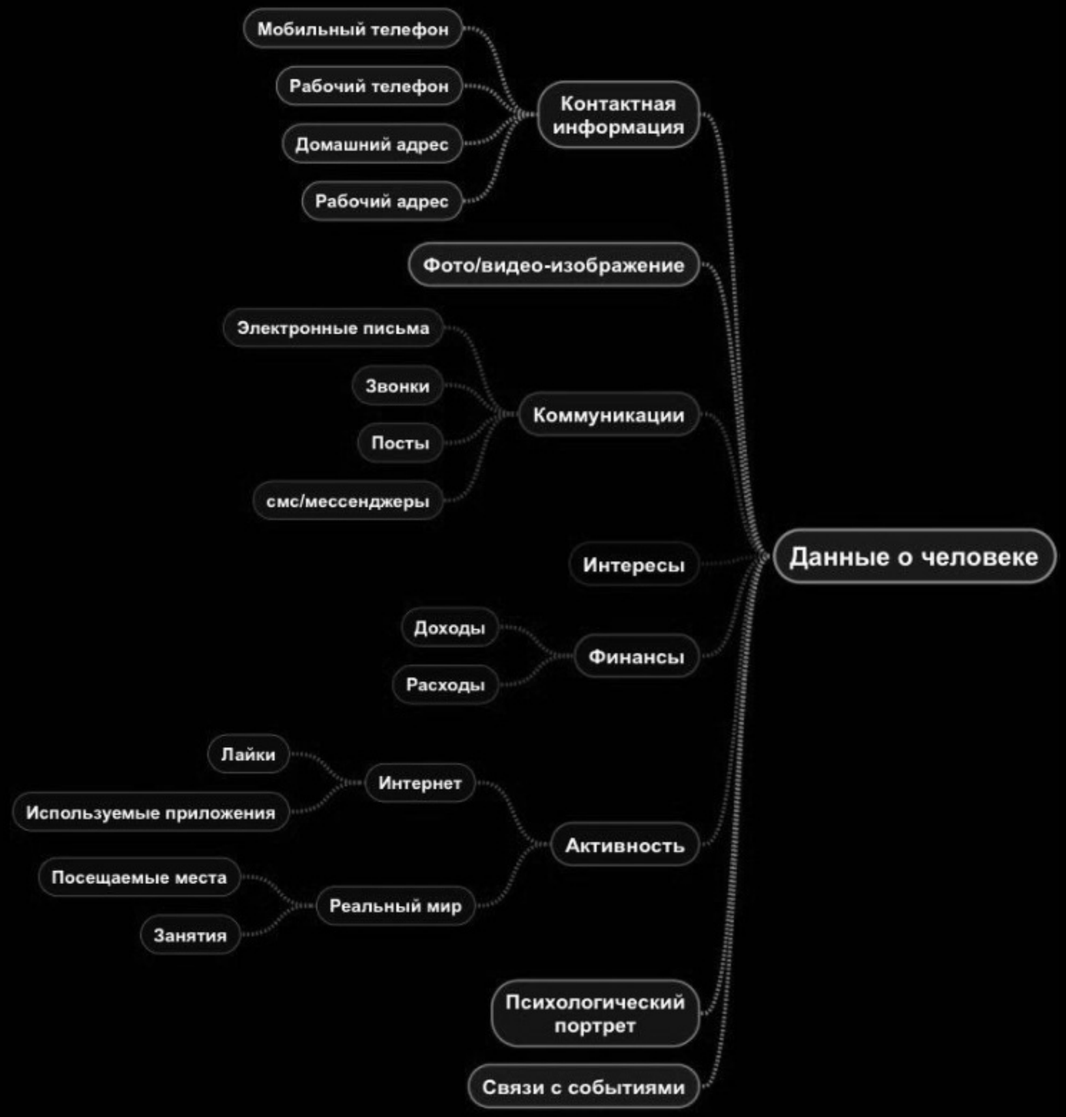


## Получение

- Аккаунты: базовая информация, посты
- Сопоставление
  - Стилометрия [1]
  - Голос [2]
  - Статус онлайна [3]

## Использование

- Психологический портрет и интересы
  - Продажа
  - Реклама
  - Влияние на общественное мнение (Cambridge Analytica)
  - Разбор внутренних инцидентов




[1] https://xakep.ru/2013/01/10/59921/
[2] https://habr.com/ru/post/144491/
[3] https://www.securitylab.ru/analytics/490726.php

# CTRL + S



- Парсеры и агрегаторы
  - Instagram, VK, Авито, etc.
- Хранение копий и ссылок
  - web.archive.org, archive.is [1]
  - Hunchly
- Системы версионирования
- Мониторинг

**Пример:** отслеживание миграций мошенников

[1] https://habr.com/ru/company/echelon/blog/321754/

# УТЕЧКИ БАЗ ДАННЫХ



- Любые пользовательские данные -- товар
  - Не люди, а **лиды**
- Агрегация самых разных данных
  - Все мыслимые схемы пробива
- Поиск и индексация общедоступных БД давно поставлены на поток [1]

[1] https://t.me/dataleak

# ИНСТРУМЕНТЫ И АВТОМАТИЗАЦИЯ



## Подборки

- https://osintframework.com/
- https://github.com/OldBonhart/Osint-Resources
- https://github.com/netstalking-core/netstalking-osint
- https://github.com/Ph055a/OSINT-Collection

## Агрегаторы

- RISKIQ
- Lampyre.io
- Maltego
- SpiderFoot
- theHarvester
- Dataspoit


СПАСИБО. ВОПРОСЫ?