

КОД ИБ: ВЛАДИВОСТОК

ОСНОВЫ КОРПОРАТИВНОЙ РАЗВЕДКИ

или простые решения прикладных задач
корпоративной службы безопасности

Борощук Дмитрий

Исследователь-криминалист

BeholderIsHere Consulting





Борощук Дмитрий

Более 18 лет на рынке информационной и технической безопасности.

- ✓ Опыт разработки систем защиты и получения информации.
- ✓ Руководил техническими подразделениями международных охранных холдингов Group 4 Securicor и Wackenhut service
- ✓ Основная специализация: моделирование угроз и техническая криминалистика

Типовые проблемы работы СБ:

01

Отсутствие
технических
компетенций у
сотрудников СБ

Сотрудники не обладают
глубоким навыком работы со
специализированным
инструментарием

02

Несогласованность
концепций
взаимодействия служб
ИБ и Безопасности

У «технарей» нет навыков
«безопасников» у которых, в свою
очередь, нет навыков «технарей»

03

Дороговизна
специализированных
аппаратных и программных
решений

Руководство не хочет тратить
большие деньги на
технологические решения для
расследований

Решения проблем:

01

Отсутствие технических компетенций у сотрудников СБ

Дать простой и надежный инструмент для решения определенной задачи

02

Несогласованность концепций взаимодействия служб ИБ и Безопасности

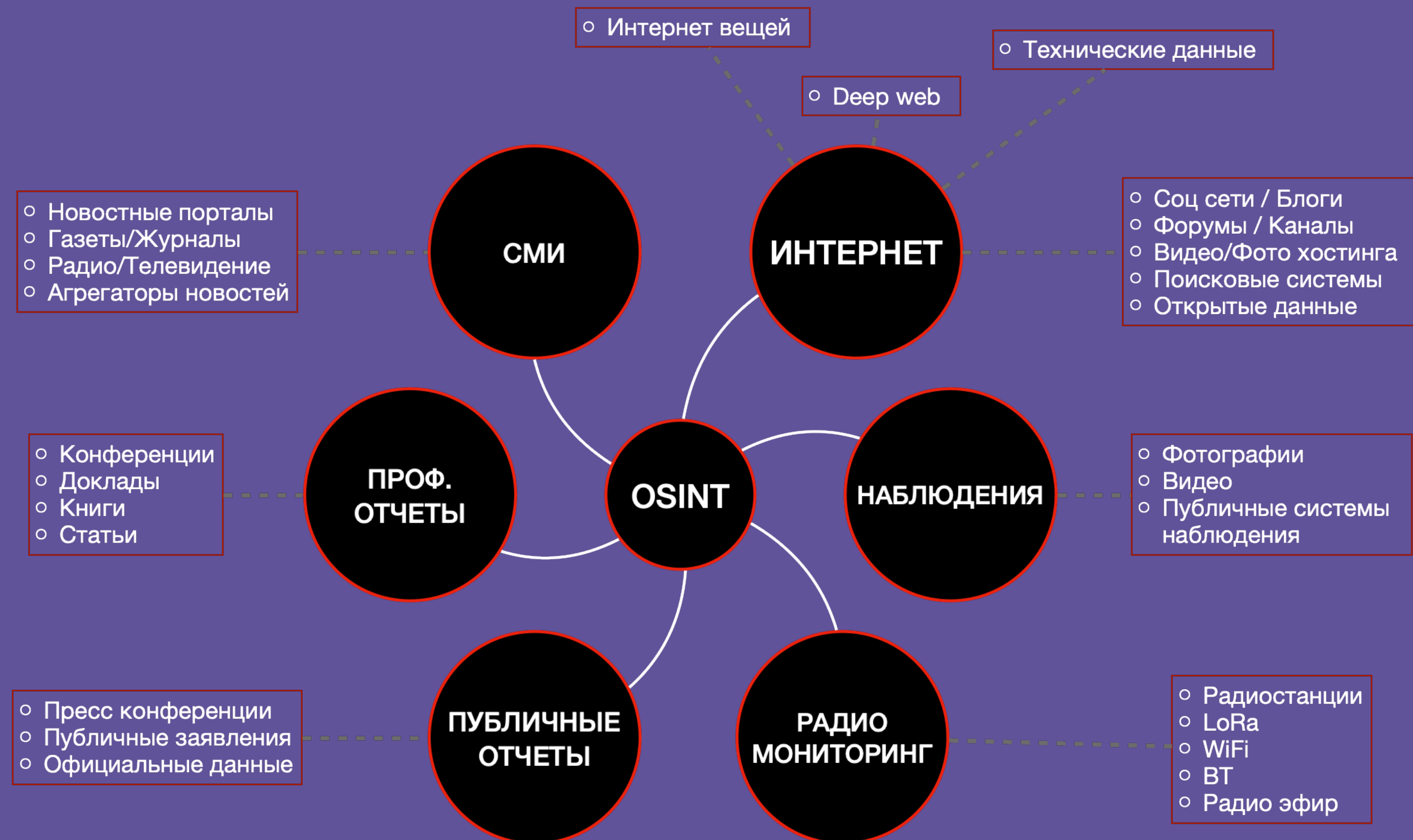
Дать каждому подразделению основы недостающих навыков друг друга

03

Дороговизна специализированных аппаратных и программных решений

Использовать бесплатные, условно-бесплатные или open-source решения

OSINT – методология
разведки по открытым
источникам информации





Что знает о нас СЕТЬ?



SNOOP

```
Имена локальная база: 60 Websites
Ищем: < 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: Putlocker
```

Функционал:

Программа анализирует различные сайты, форумы и социальные сети 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 более 2500 сайтов и сервисов



GHunt

```
C:\Users\mxrch\Desktop\labs\google\id>python hunt.py [REDACTED]@live.fr
-----
Name: [REDACTED]
Location: Sélestat-Erstein, France
Last profile edit : 2019/04/22 23:49:54 (UTC)
Email : [REDACTED]@live.fr
Google ID : 10668544[REDACTED]
Hangouts Bot : No
Activated Google services :
- Youtube
- Photos
- Maps
Youtube channel (confidence => 90.0%) :
- [REDACTED] https://youtube.com/channel/[REDACTED]
Google Photos : https://get.google.com/albumarchive/10668544[REDACTED]
=> 2 albums, 2 photos
Searching metadata...
[+] 1 phone found !
- Huawei VNS-L31 (2 pics) [2017/05/21]
-> 1 Firmware found !
--> VNS-L31C432B370 [2017/05/21]
[+] 1 location found !
- Rust, Deutschland (1 pic) [2017/05/21]
```

Функционал:

Извлекаемые данные:

- Имя владельца
- Последний раз профиль редактировался
- Google ID
- Если это аккаунт Hangouts
- Активированные сервисы Google (Youtube, Фото, Карты, News360, Hangouts и т. Д.)
- Возможный канал Youtube
- Возможные другие имена пользователя
- Публичные фотографии
- Модели телефонов
- Прошивки телефонов
- Установленное ПО
- Обзоры Google Maps
- Возможное физическое местонахождение



YaSeeker

```
Get info about kshivelev...
Yandex.Collections
  URL: https://yandex.ru/collections/user/kshivelev/
  Id: 5ed60fed37f1922c0ca12fb3
  Yandex_public_id: dx1xgb0p72a09j7udyewfu5bf0
  Fullname: Кирилл
  Image: https://avatars.mds.yandex.net/get-yapic/0/0-0/islands-200
  Sex: m
  Likes: 0
  Cards: 0
  Boards: 0
  Is_passport: True
  Is_restricted: False
  Is_forbid: False
  Is_km: False
  Is_business: False

Yandex.Music
  Not found.

Yandex.Bugbounty
  Not found.

Yandex.Reviews
  URL: https://reviews.yandex.ru/user/dx1xgb0p72a09j7udyewfu5bf0
  Yandex_public_id: dx1xgb0p72a09j7udyewfu5bf0
  Fullname: Кирилл Ш
  Image: https://avatars.mds.yandex.net/get-yapic/0/0-0/islands-300
  Is_verified: False
  Reviews_count: 18
  Following_count: 0
  Follower_count: 0

Yandex.Znatoki
  URL: https://yandex.ru/q/profile/dx1xgb0p72a09j7udyewfu5bf0/
  Yandex_znatoki_id: 1c7aed0d-2a5d-506b-845c-79991caeff9c
  Yandex_uid: 85020608
  Name: Кирилл Ш
  Image: https://avatars.mds.yandex.net/get-yapic/0/0-0/islands-300
  Is_org: False
  Is_banned: False
  Is_deleted: False
  Created_at: 2019-07-31
  Rating: 0
  Gender: m
  Links: []
  Is_from_q: False
  Answers_count: 0
  Following_count: 0

Yandex.Zen
  Not found.
```

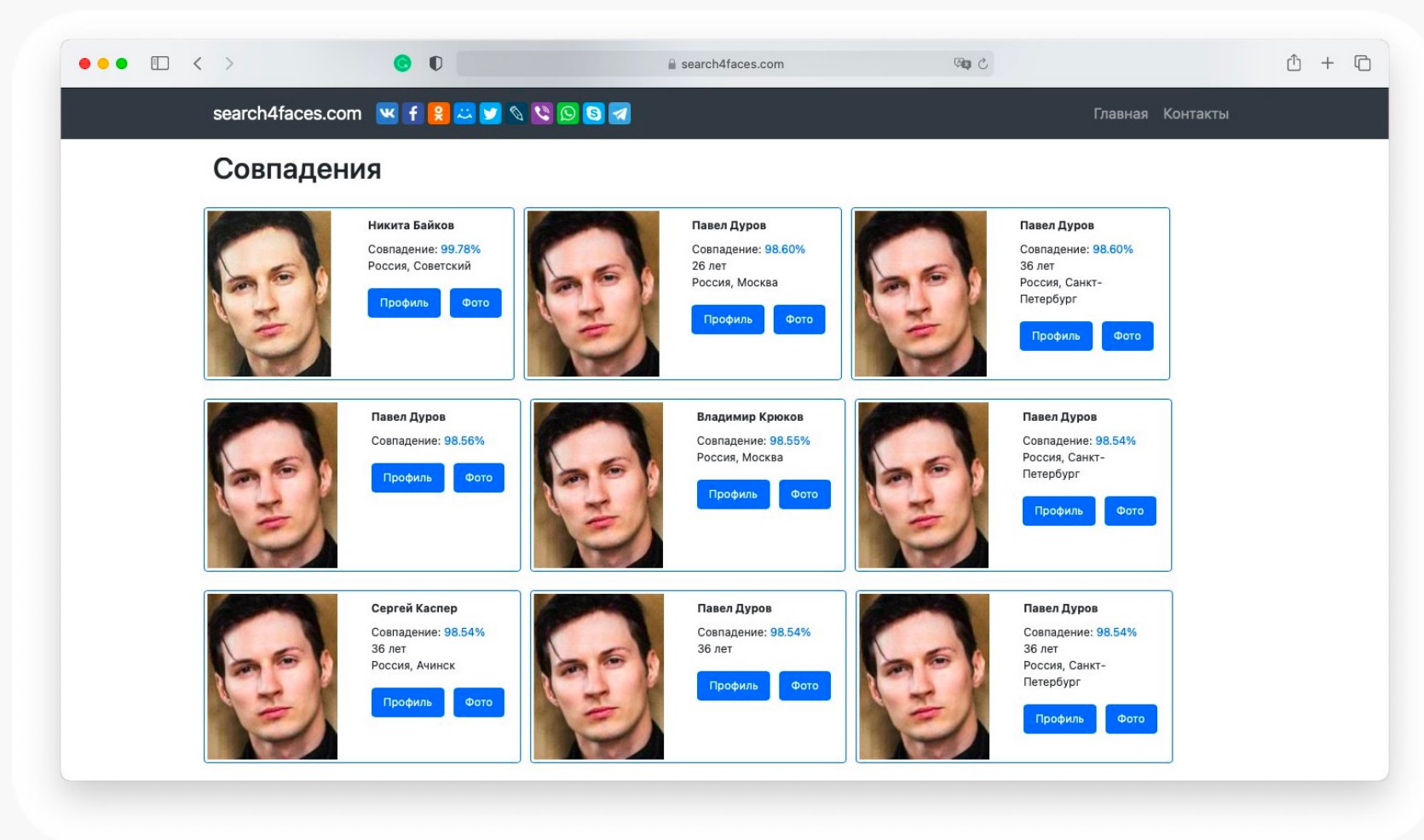
Функционал:

Извлекаемые данные:

- Имя владельца
- Фото
- Yandex ID публичный
- Yandex UID
- Активированные сервисы Yandex (Music, Collections, Bugbounty, Reviews, Q (Znatoki), O (Classified), Zen, Market, Messenger.)
- Привязанные социальные аккаунты.
- Возможные другие имена пользователя
- Публичные фотографии
- Активности (комментарии, подписки, подписчики)



Search4face



Функционал:

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

ФОРЕНЗИКА –

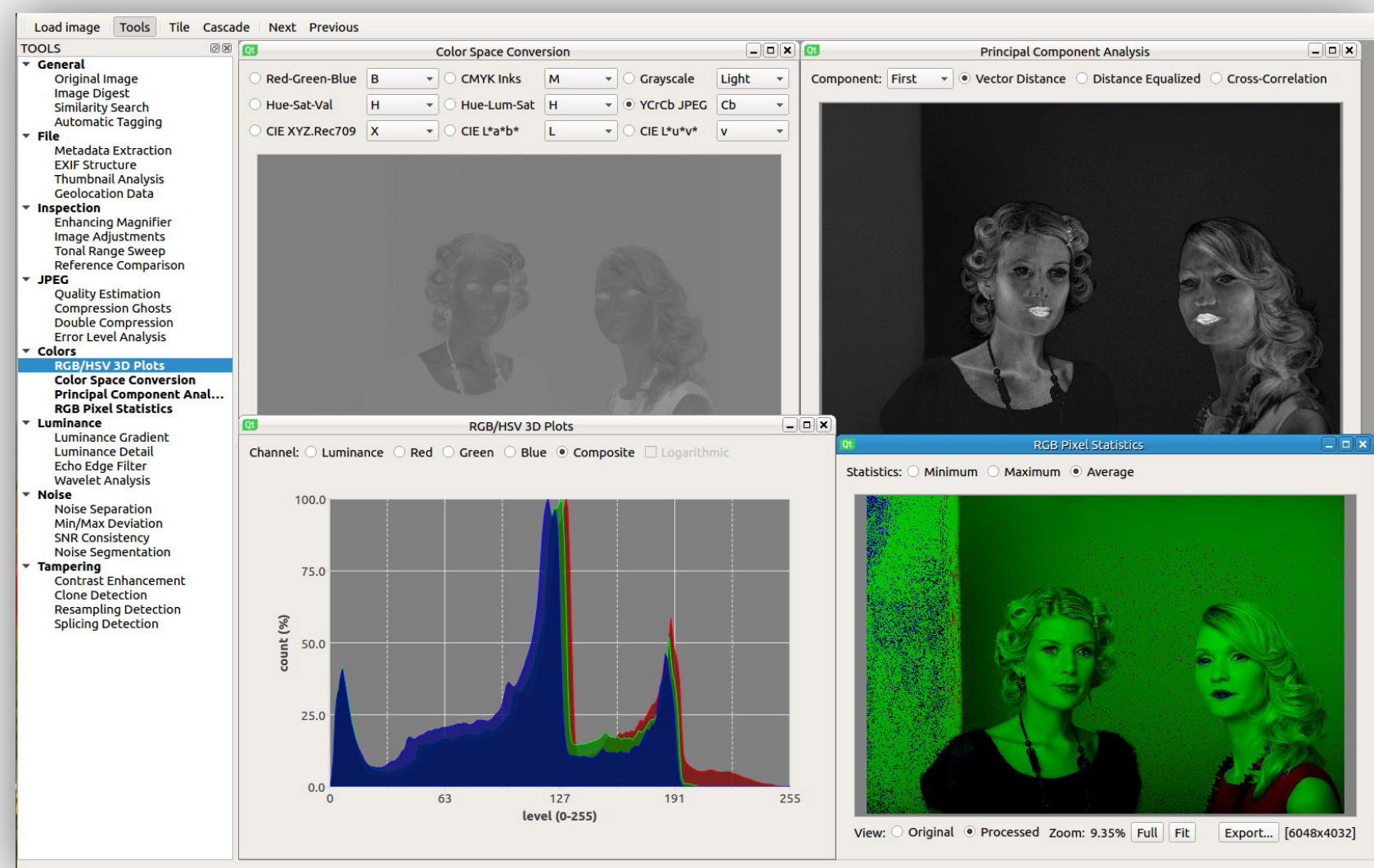
поиск следов «инцидентов» на любых носителях и предметах, содержащих информацию



Как выявить факт подделки
цифровых изображений?



Sherloq



Функционал:

- Извлечение метаданных
- Извлечение геолокации
- Анализ уровней
- Анализ освещения
- Структурный анализ изображения
- Выявление графических аномалий
- Извлечение и анализ хешей

... и еще много чего.



Image Verification Assistant

Metadata summary more metadata fields

Significant Data		JPEG	JFIF		
description	value	description	value	description	value
Exif IFD0		Compression Type	Baseline	Version	1.1
Date/Time	Not found	Data Precision	8 bits	Resolution Units	none
Gain Control	Not found	Image Height	600 pixels	X Resolution	1 dot
Image Description	Not found	Image Width	290 pixels	Y Resolution	1 dot
Image Height	Not found	Number of Components	3	Thumbnail Width Pixels	0
Image Width	Not found	Component 1 Y component: Quantization table 0, Sampling factors 2 horiz/2 vert	Component 2 Cb component: Quantization table 1, Sampling factors 1 horiz/1 vert	Thumbnail Height Pixels	0
Make	Not found				
Model	Not found				
Software	Not found	Component 3 Cr component: Quantization table 1, Sampling factors 1 horiz/1 vert			
Exif SubIFD					
Aperture Value	Not found				
Artist	Not found				
Body Serial Number	Not found				

send this image to [Google reverse image search](#)

Map 0 Map 1 Map 2 Map 3 Map 4

Функционал:

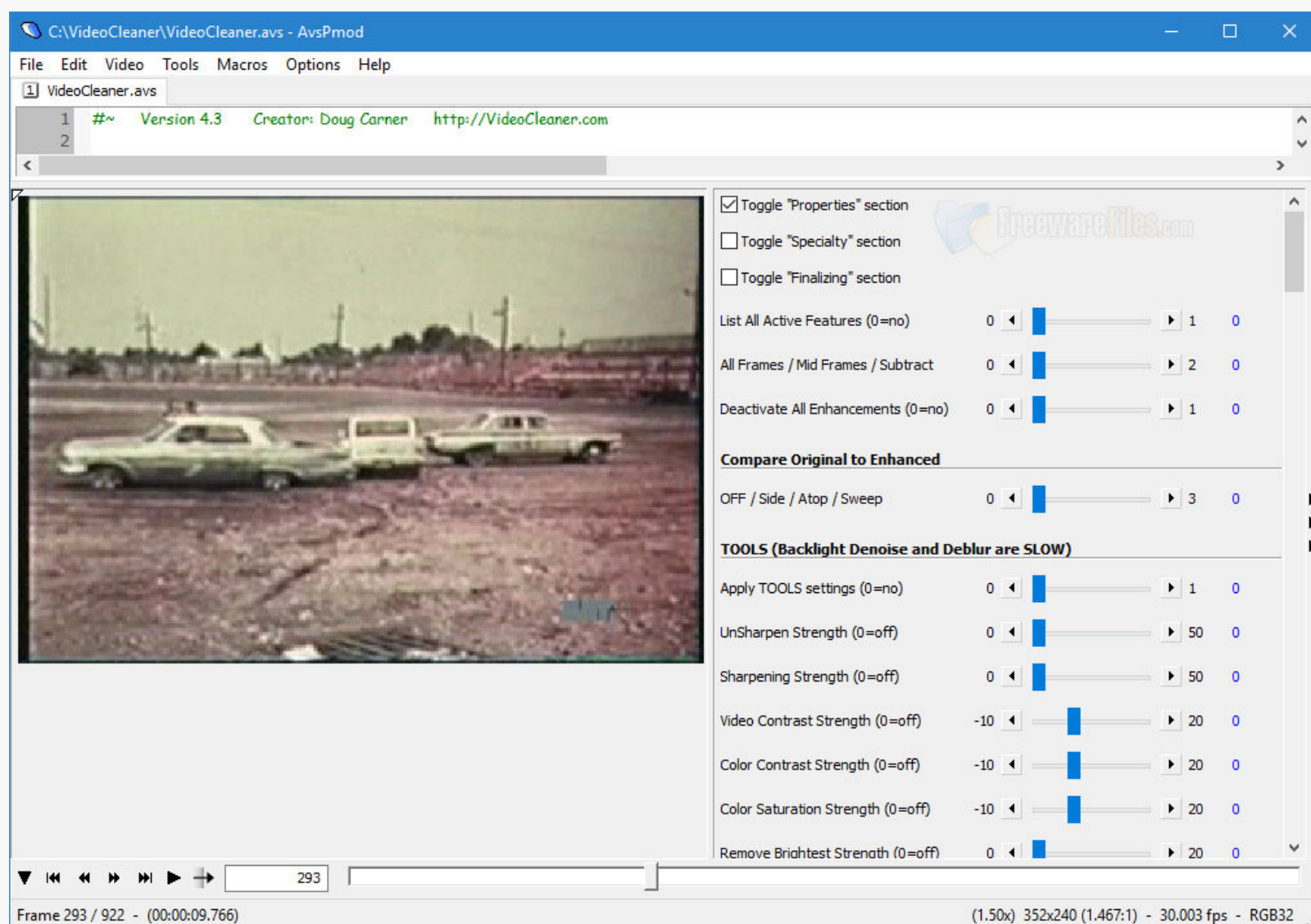
Бесплатный онлайн-инструмент для анализа достоверности изображений в медиа. Внутри алгоритмы обнаружения подделки изображений, анализ метаданных, геолокации GPS, извлечение миниатюр EXIF и интеграция с обратным поиском изображений Google.



Как улучшить «картинку»
полученную из системы
видеонаблюдения?



Video Cleaner



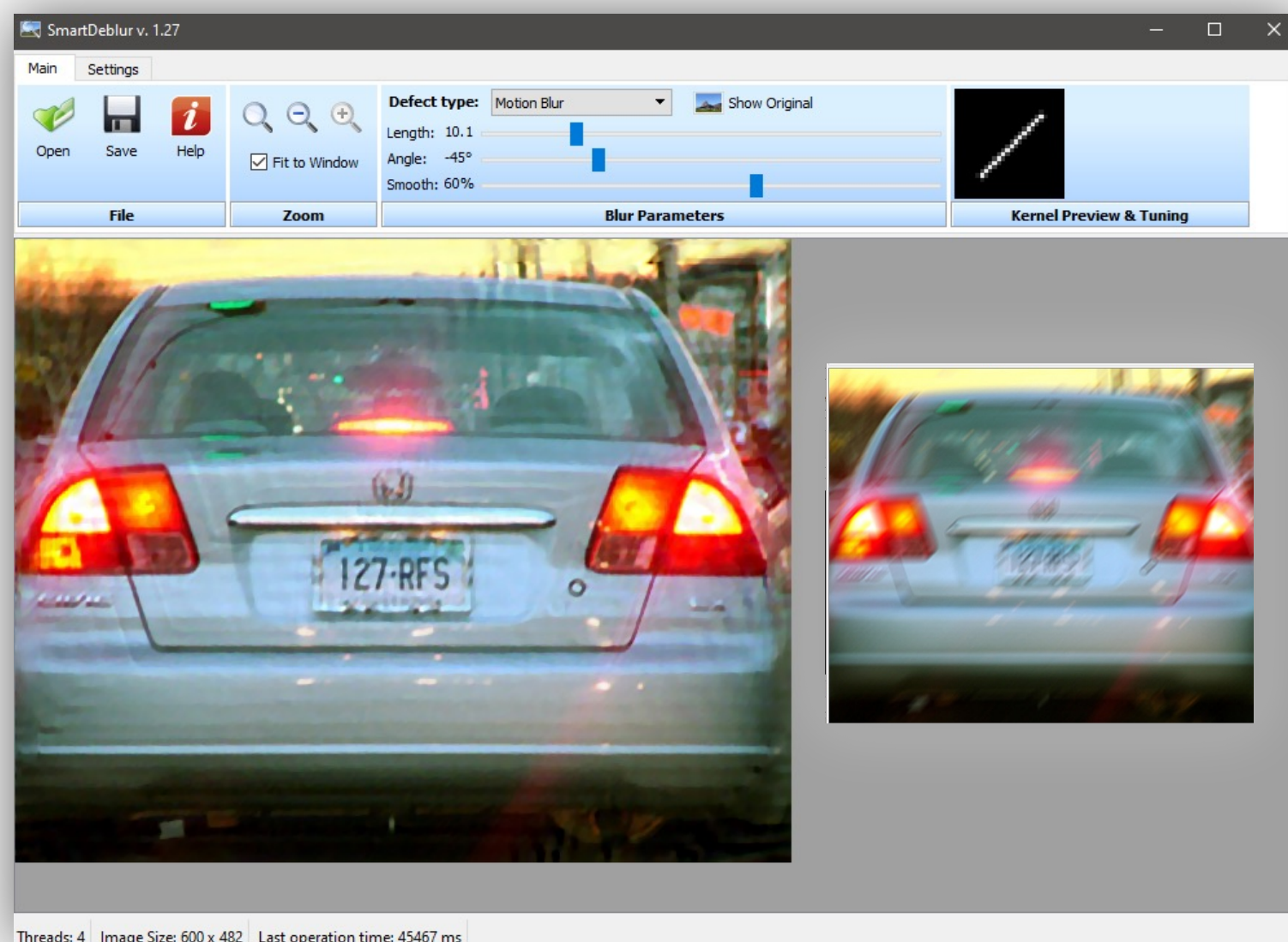
Функционал:

- Освещение затемненных сцен
- Улучшение четкости лиц
- Восстановление видимости автомобильных номеров
- Изменение перспективы просмотра
- Восстановление изображения от искажений оптики
- Стабилизация движений камеры

... и еще много чего.



SmartDeblur



Функционал:

- Исправление размытия вне фокуса.
- Исправление размытия от движения.
- Исправление размытия по Гауссу.

Особенности:

- Быстрая работа с большим разрешением исходного видео
- Просмотр изменений в реальном времени
- Простой интерфейс

Работает под Windows и MacOS

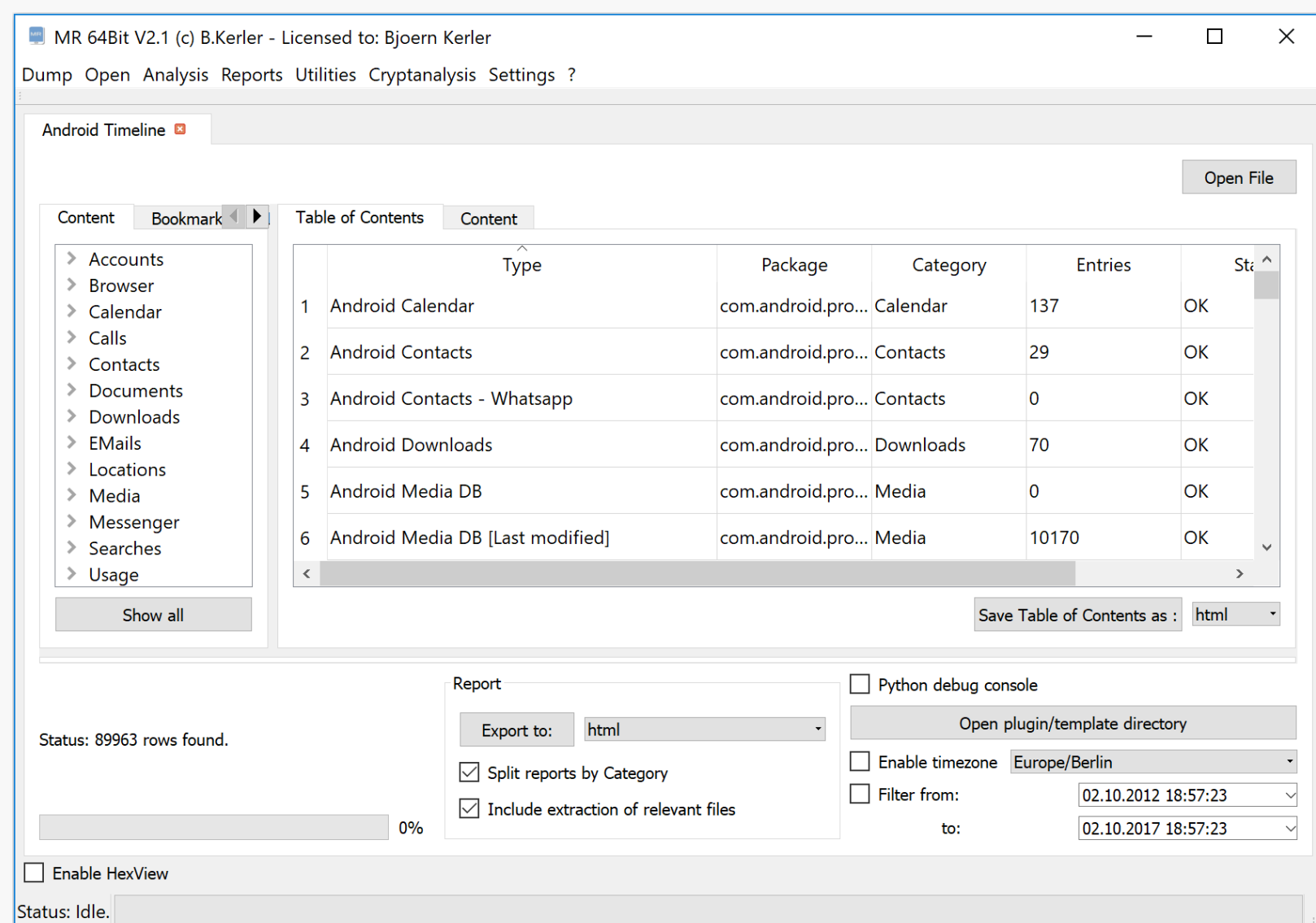


Как извлечь данные из
смартфона?



Mobile Forensic

Mobile Revelator



Функционал:

Позволяет извлекать и восстанавливать

- Аккаунты
- Историю браузера
- Календарь
- Журнал звонков
- Контакты
- Документы
- Содержимое электронной почты
- Медиа файлы
- SMS
- Историю поиска

... и еще много что

Работает под Windows

github.com/bkerler/MR



ArtEx - Artifact Examiner

Mobile Forensic

Unable to render graphs of selected size!

View 233 Records Found

Row ID	Icon	Start Time	End Time	Activity	Metadata
233		9/9/2019 20:47:02 (UTC+01:00)	9/9/2019 20:48:51 (UTC+01:00)	Call (00:01:49)	Incoming Audio
232		9/9/2019 18:50:49 (UTC+01:00)	9/9/2019 18:50:49 (UTC+01:00)	Call (00:00:00)	Missed Audio Ca
230		9/9/2019 17:07:03 (UTC+01:00)	9/9/2019 17:33:20 (UTC+01:00)	Call (00:26:17)	Outgoing Audio
231		9/9/2019 17:31:28 (UTC+01:00)	9/9/2019 17:31:28 (UTC+01:00)	Call (00:00:00)	Missed Audio Ca
227		9/9/2019 15:15:58 (UTC+01:00)	9/9/2019 16:40:41 (UTC+01:00)	Call (01:24:43)	Outgoing Audio
229		9/9/2019 16:12:03 (UTC+01:00)	9/9/2019 16:12:03 (UTC+01:00)	Call (00:00:00)	Missed Audio Ca
228		9/9/2019 16:09:02 (UTC+01:00)	9/9/2019 16:09:02 (UTC+01:00)	Call (00:00:00)	Missed Audio Ca
226		9/9/2019 15:15:02 (UTC+01:00)	9/9/2019 15:15:50 (UTC+01:00)	Call (00:00:48)	Outgoing Audio
225		9/9/2019 15:03:33 (UTC+01:00)	9/9/2019 15:03:41 (UTC+01:00)	Call (00:00:08)	Outgoing Audio
224		9/7/2019 11:37:15 (UTC+01:00)	9/7/2019 11:37:15 (UTC+01:00)	Call (00:00:00)	Missed Audio Ca
223		9/6/2019 14:25:51 (UTC+01:00)	9/6/2019 14:25:51 (UTC+01:00)	Call (00:00:00)	Missed Audio Ca
222		9/6/2019 10:31:00 (UTC+01:00)	9/6/2019 10:31:00 (UTC+01:00)	Call (00:00:00)	Missed Audio Ca
221		9/5/2019 19:27:50 (UTC+01:00)	9/5/2019 19:27:50 (UTC+01:00)	Call (00:00:00)	Missed Audio Ca
220		9/5/2019 17:18:04 (UTC+01:00)	9/5/2019 17:18:04 (UTC+01:00)	Call (00:00:00)	Missed Audio Ca
219		9/5/2019 15:51:02 (UTC+01:00)	9/5/2019 17:01:08 (UTC+01:00)	Call (01:10:06)	Outgoing Audio
218		9/5/2019 15:01:35 (UTC+01:00)	9/5/2019 15:01:35 (UTC+01:00)	Call (00:00:00)	Missed Audio Ca
217		9/4/2019 22:29:53 (UTC+01:00)	9/4/2019 22:29:53 (UTC+01:00)	Call (00:00:00)	Missed Audio C

Функционал:

- артефакты: уровень заряда, активность, используемое приложение, события, звонки, сообщения и др.
- построение различных таймлайнов от работы аккумулятора до действий пользователя.
- поддержка извлечений на основе BFU
- местоположение сотовых вышек с поддержкой OpenCellID и CSV
- просмотрщик каталогов, включающий LOG, IMAGE, PLIST, SQL и Hex
- Мгновенный просмотр изображения/видео/URL
- история местоположений с визуализацией на карте
- парсеры мессенджеров
- распознавание лиц на фото
- анализ транзакций Apple Pay

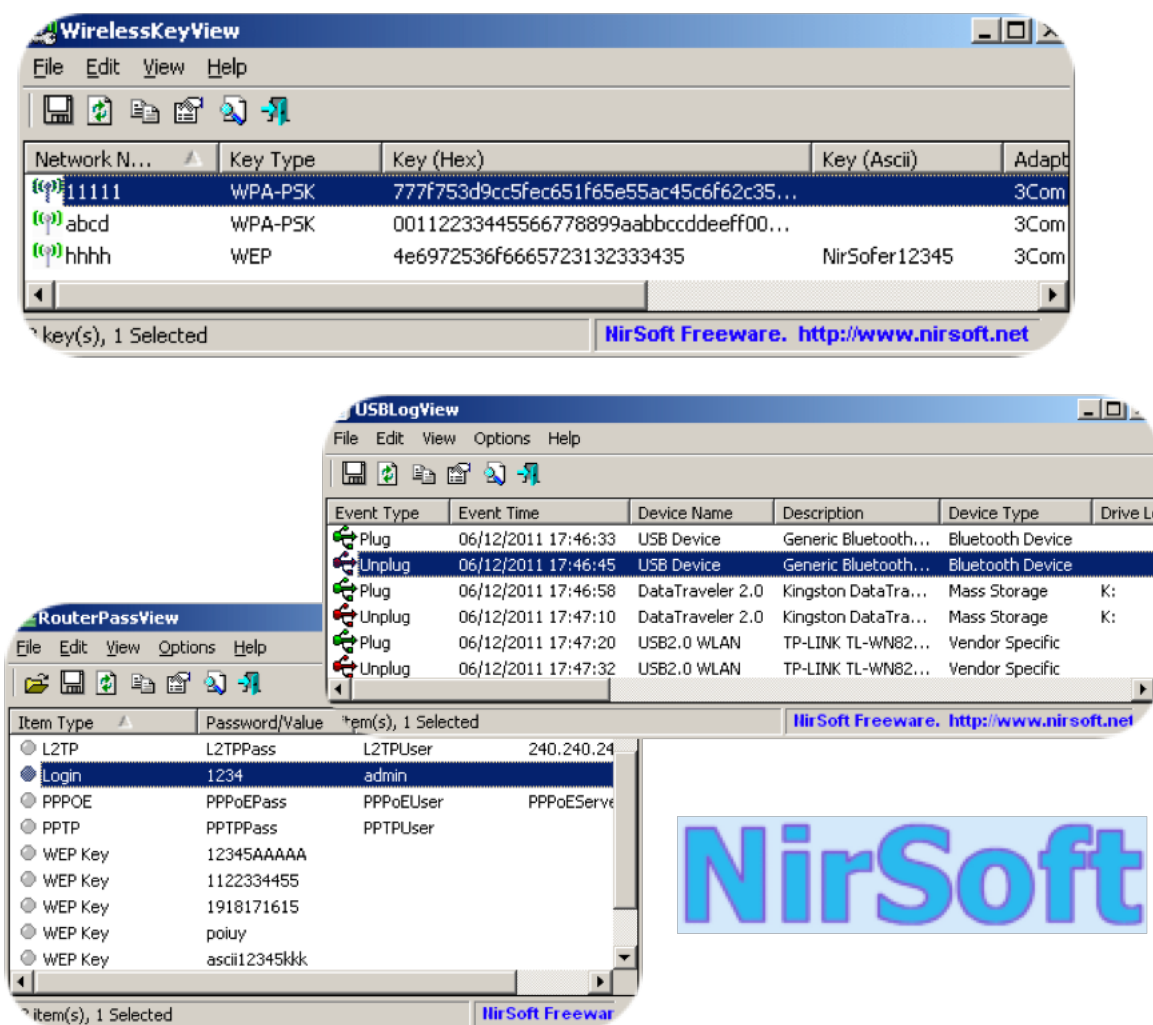


Как и какие данные можно
вытащить из windows?



NirSoft Utilites

Более 200 утилит извлечения данных из windows



NirSoft

Собираем данные из windows

- История/кеш/куки/пароли браузеров
- Логи событий системы
- Пароли от Wifi
- Историю поиска
- История обращения к файлам
- Историю подключенных устройств

...и многое многое другое

**И еще немного про
прикладные задачи...**



Как сделать черный вход в
систему win/mac?



Kon-Boot



Это инструмент, который позволяет получить доступ к целевому компьютеру, не зная пароля пользователя. В отличие от других решений Kon-Boot не сбрасывает и не изменяет пароль пользователя, и все изменения возвращаются в предыдущее состояние после перезагрузки системы.

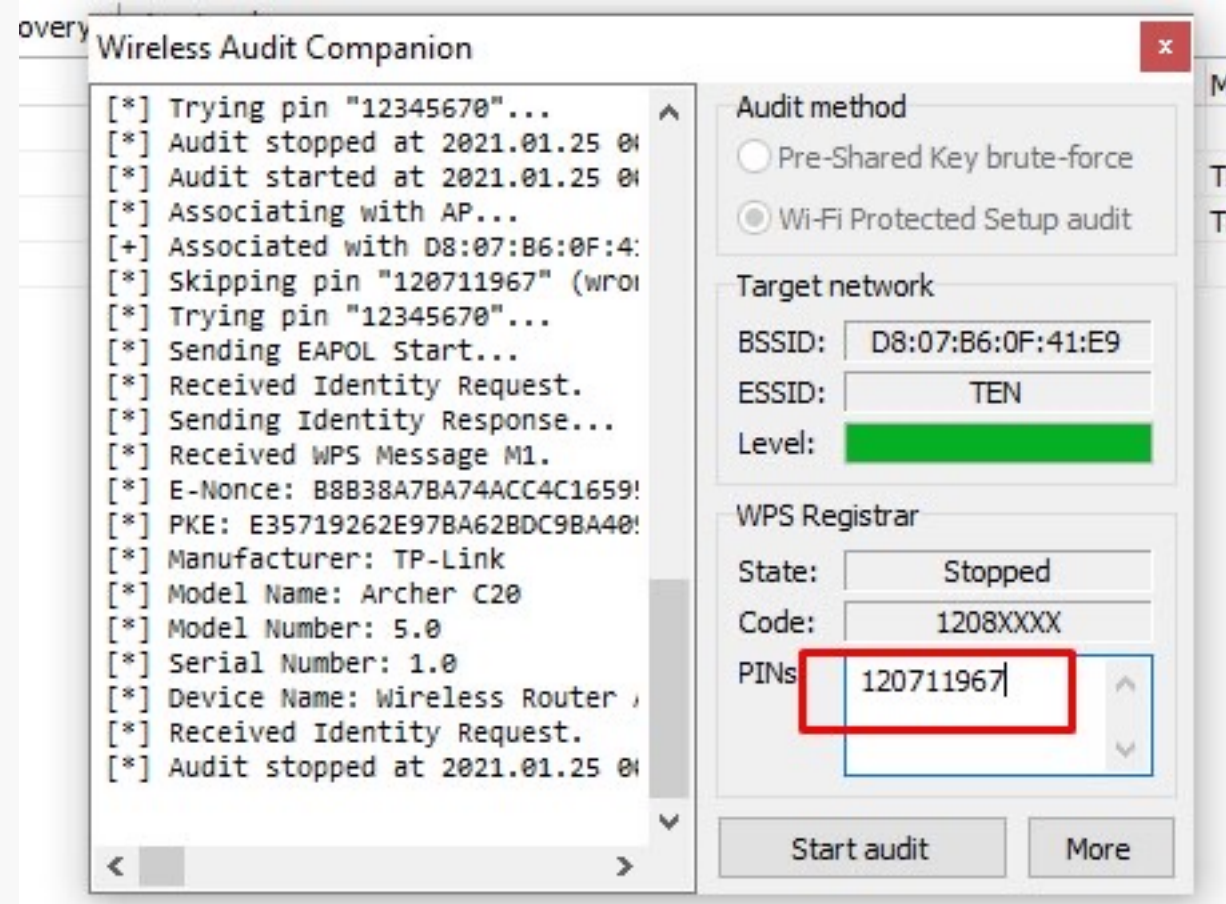
В настоящее время это единственным во всем мире решение, которое может обойти сетевую учетную запись Windows 10!



Как проверить собственную
беспроводную сеть на
уязвимости?



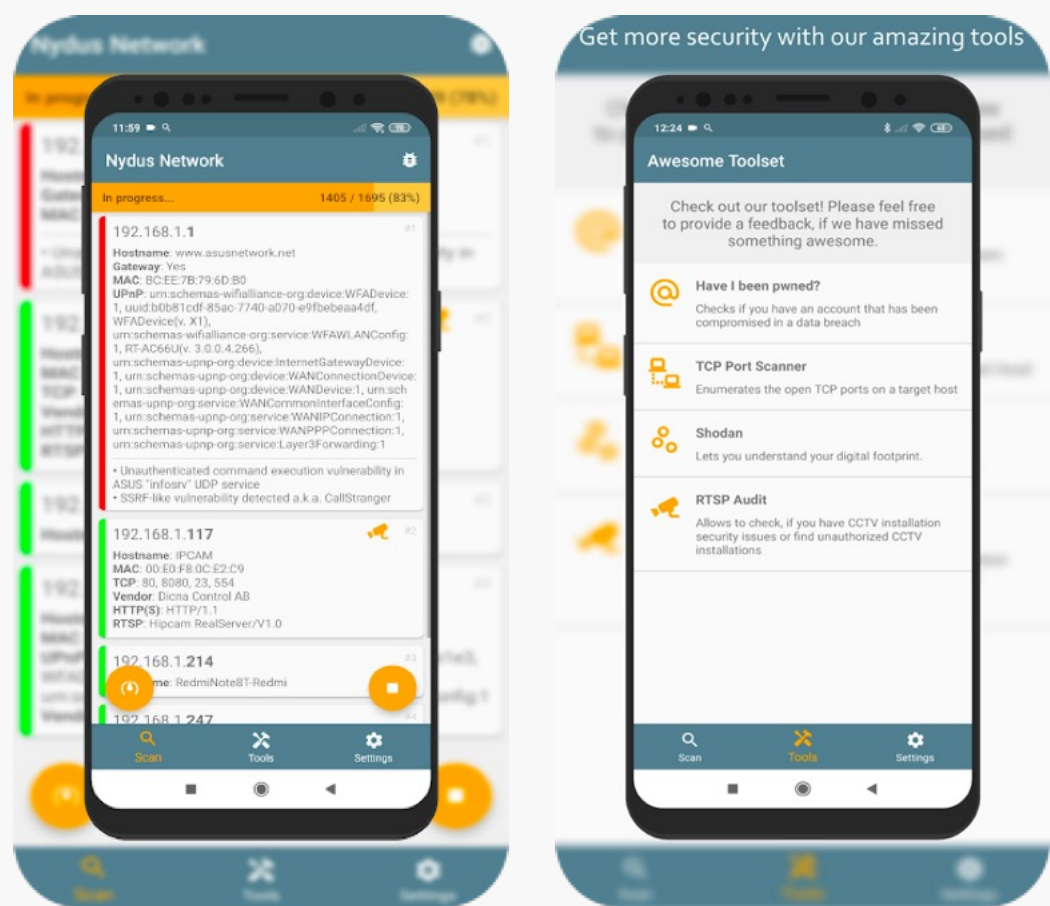
RouterScan



- находит и определяет различные устройства из большого числа известных роутеров/маршрутизаторов:
- вытаскивает из них полезную информацию, в частности характеристики беспроводной сети: способ защиты точки доступа (шифрование)
- имя точки доступа (SSID) и ключ точки доступа (парольная фраза).
- получает информацию о WAN соединении (удобно при сканировании локальной сети) и выводит марку и модель роутера.



IoPT: Network Security Scanner



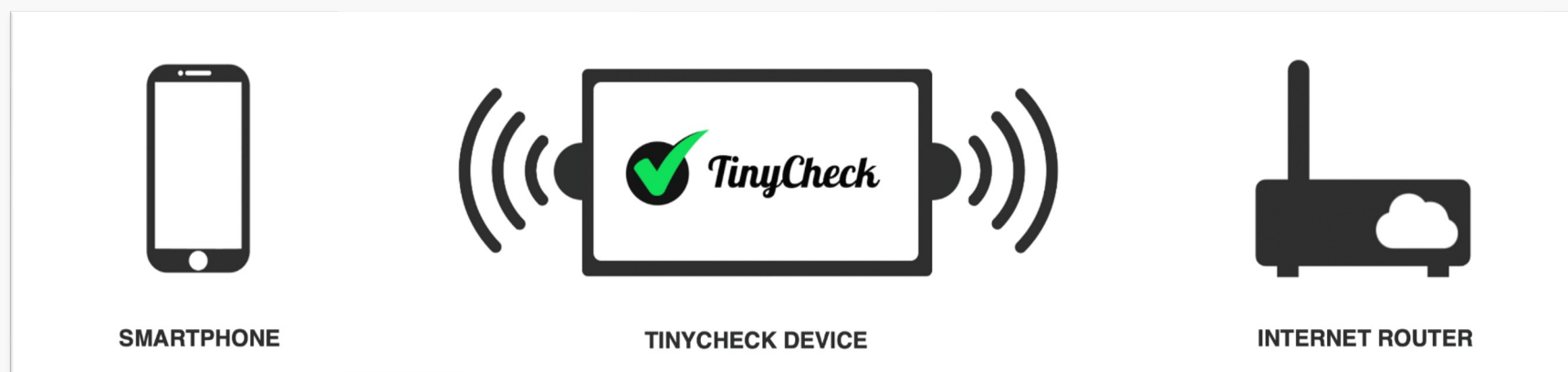
- Аудит безопасности - определение сервисов в сети и выполнение аудита безопасности.
- Обнаружение хостов - определение хостов в сети.
- Сканирование портов - перечислить открытые TCP-порты на целевом хосте.
- Интеграция HiBP - убедитесь, что ваши личные данные не были скомпрометированы в результате утечки данных.
- Интеграция Shodan - убедитесь, что вы знаете все «вещи» в сети, напрямую подключенной к Интернету.
- Аудит RTSP - Выполните аудит безопасности для источника RTSP (например, установки системы видеонаблюдения). Проверьте свою сеть на предмет несанкционированных установок видеонаблюдения.



Как выявить факт негласного
наблюдения за вами через
смартфон?



TinyCheck



Функционал:

- Ищет на мобильных устройствах «шпионское» ПО распознавая их наличие «по паттернам поведения»

Особенности:

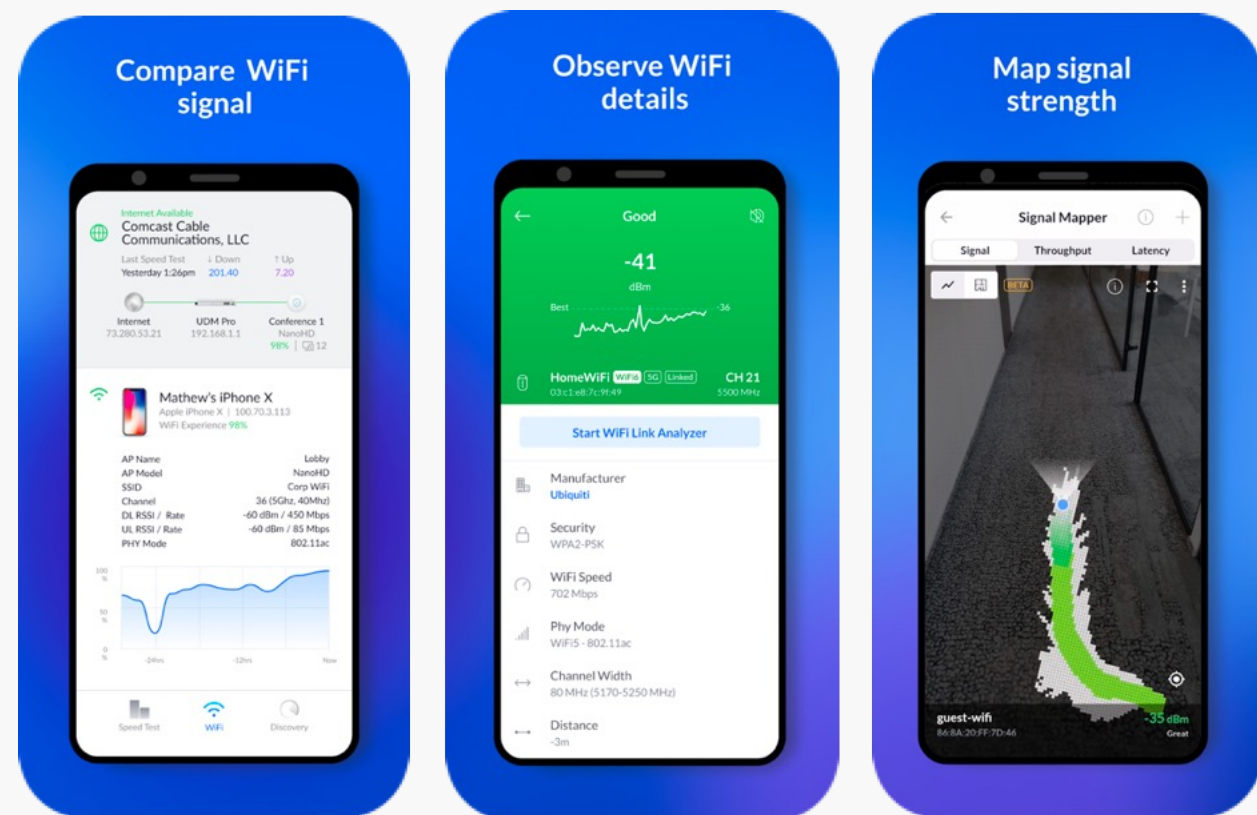
- Простота использования
- Не требует глубокого понимания сетевых протоколов
- Использует в качестве аппаратной основы RPi
- Может работать в автоматическом режиме и ручном режиме.



Как найти «wifi закладку»



WiFiman



WiFiman идеально подходит для анализа Wi-Fi сетей, устройств Bluetooth LE, обнаружение новых устройств в сети и измерения скорости. Эти возможности доступны в удобном и элегантном интерфейсе пользователя, разработанным Ubiquiti Networks. WiFiman не содержит рекламы и является бесплатным.

WiFiman поможет вам найти свободный канал для вашей Wi-Fi точки доступа. WiFiman отображает список каналов Wi-Fi и устройств Bluetooth LE которые используются неподалеку и предоставляет их детальную информацию о них.

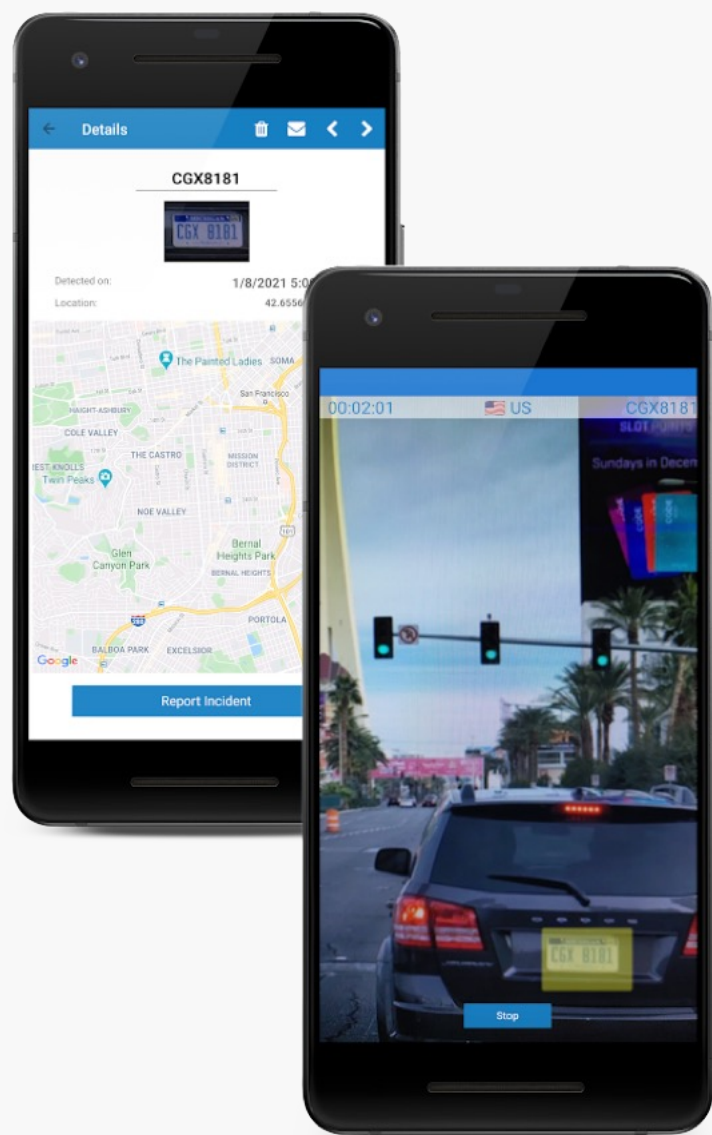
С помощью приложения вы с легкостью сможете обнаружить и анализировать устройства подключенные к вашей сети. WiFiman анализирует всю подсеть и отображает все доступные устройства и сервисы, используя протоколы Bonjour, SNMP, NetBIOS и UBNT



Как найти нужный
автомобиль на видео или
запомнить все авто номера
вокруг вас



MOBILE LPR



Функционал:

Поддерживает черные/белые списки.

Фиксирование номеров при движении с привязкой к местоположению.

Push уведомления

Отправка уведомлений на почту или в облако.

Поддержка подключения внешних сетевых видеокамер

Возможность сканирования номеров из видеофайлов

Может быть полезно при отслеживании определенных автомобилей в потоке, например при поиске угнанных машин. Осуществлять контр-наблюдение, контролируя все машины в потоке по ходу движения.



Как найти человека и то, что
он говорил на видео



Azure Video Analyzer for Media

The screenshot displays the Azure Video Indexer interface. On the left, a video player shows a man speaking. The main panel on the right is titled 'Insights' and contains several sections:

- 18 People:** A list of detected faces, with Satya Nadella (Microsoft CEO) highlighted. It notes he appears in 17% of the video.
- 17 Keywords:** A list of detected terms including 'graph', 'azure', 'microsoft', 'app services', 'cloud', and 'location services'.
- Emotions:** A bar chart showing emotion percentages: 33% Fear, 28% Anger, 7% Sadness, and 12% Joy.
- 102 Keyframes:** A grid of small video frames representing key moments in the video.

At the bottom left, there are recommendations for 'More videos with similar people and keywords', including 'Windows Holographic Technical Session | WinHE...' and 'Build 2018 Keynote'.

Сервис позволяющий проиндексировать видео или аудио данные на предмет поиска упоминаний ключевых слов (имя, название компании и тп) или появление в кадре определенного лица и разложить это на тайм лайне.

Поддерживаемые языки: английский, испанский, арабский, французский, итальянский, хинди, японский, португальский, упрощенный китайский, корейский и русский.

Вопросы?

**BEHOLDER
IS
HERE**

исследования
и консалтинг



Telegram

@BeholderIsHere

t.me/Forensictools