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

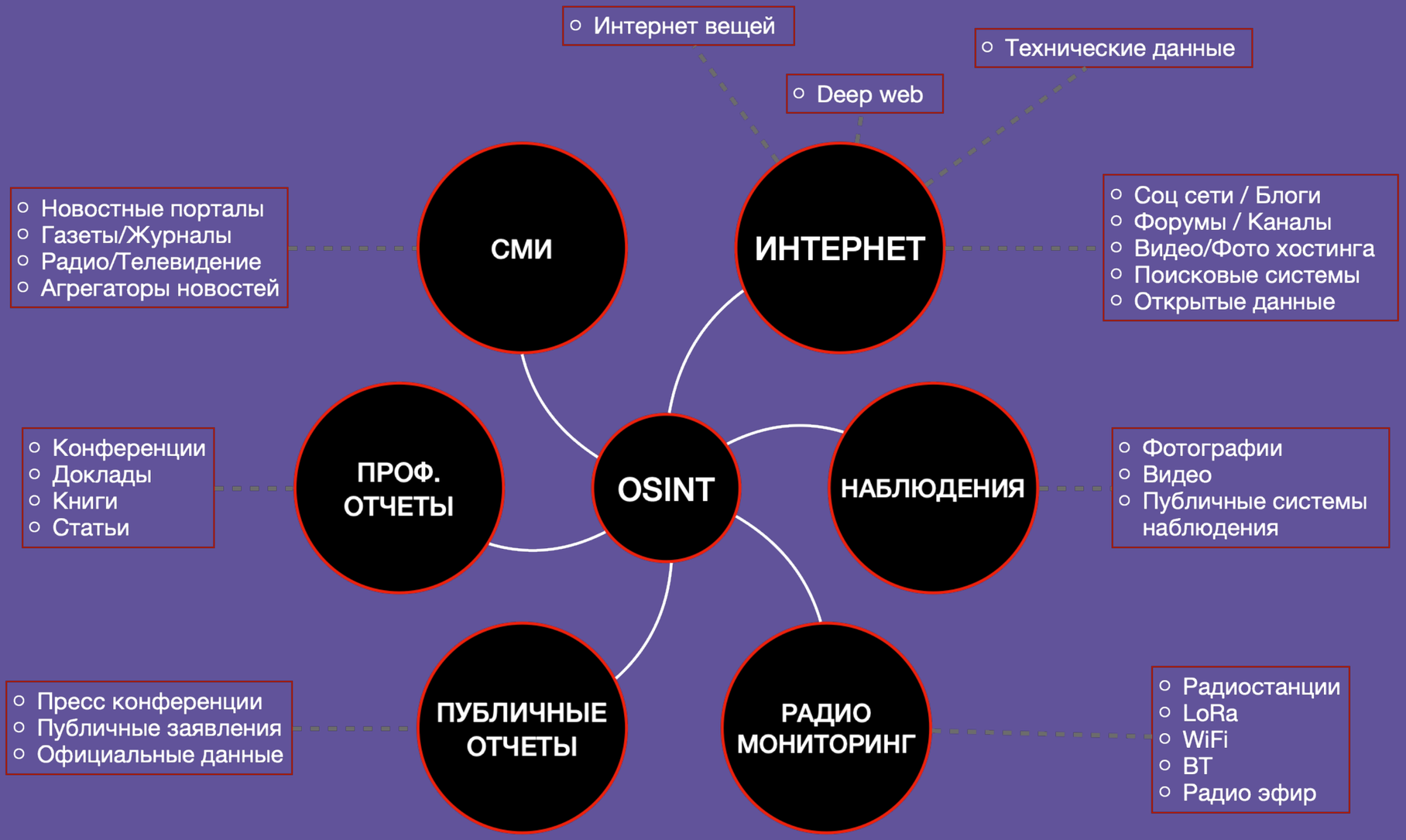
Дать каждому подразделению основы недостающих навыков друг друга

03

Дороговизна специализированных аппаратных и программных решений

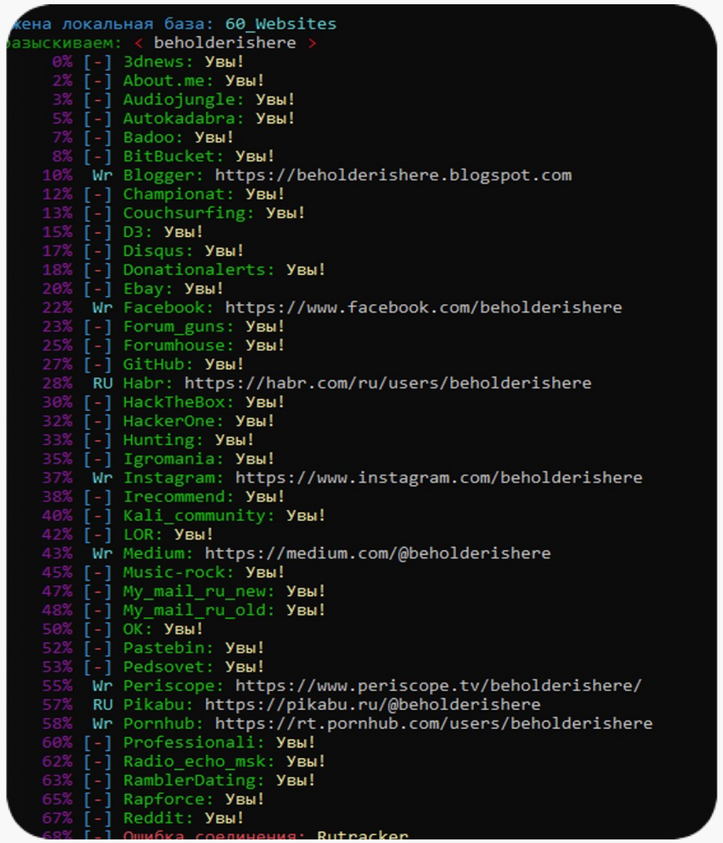
Использовать бесплатные, условно- бесплатные или open-source решения

# OSINT – методология разведки по открытым источникам информации


Интернет вещей
Технические данные
Deep web
СМИ
ИНТЕРНЕТ
Новостные порталы
Газеты/Журналы
Радио/Телевидение
Агрегаторы новостей
Соц сети / Блоги
Форумы / Каналы
Видео/Фото хостинга
Поисковые системы
Открытые данные
ПРОФ. ОТЧЕТЫ
OSINT
НАБЛЮДЕНИЯ
Конференции
Доклады
Книги
Статьи
Фотографии
Видео
Публичные системы наблюдения
ПУБЛИЧНЫЕ ОТЧЕТЫ
РАДИО МОНИТОРИНГ
Пресс конференции
Публичные заявления
Официальные данные
Радиостанции
LoRa
WiFi
BT
Радио эфир

# Что знает о нас СЕТЬ?

# SNOOP



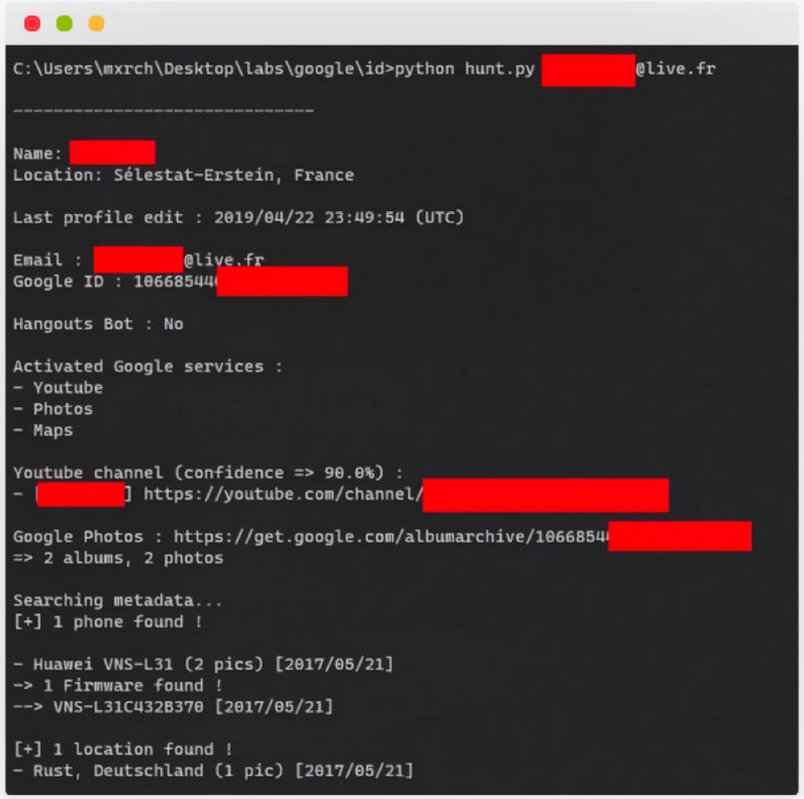

## Функционал:

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

[ github.com/snooppr/snoop ]

# GHunt



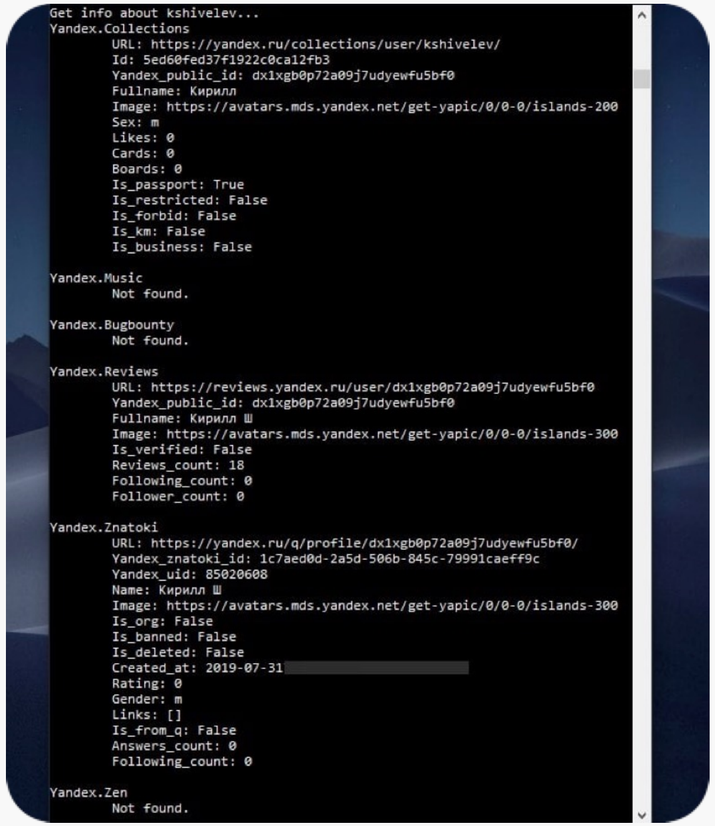

## Функционал:

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

[ github.com/mxrch/GHunt ]

# YaSeeker



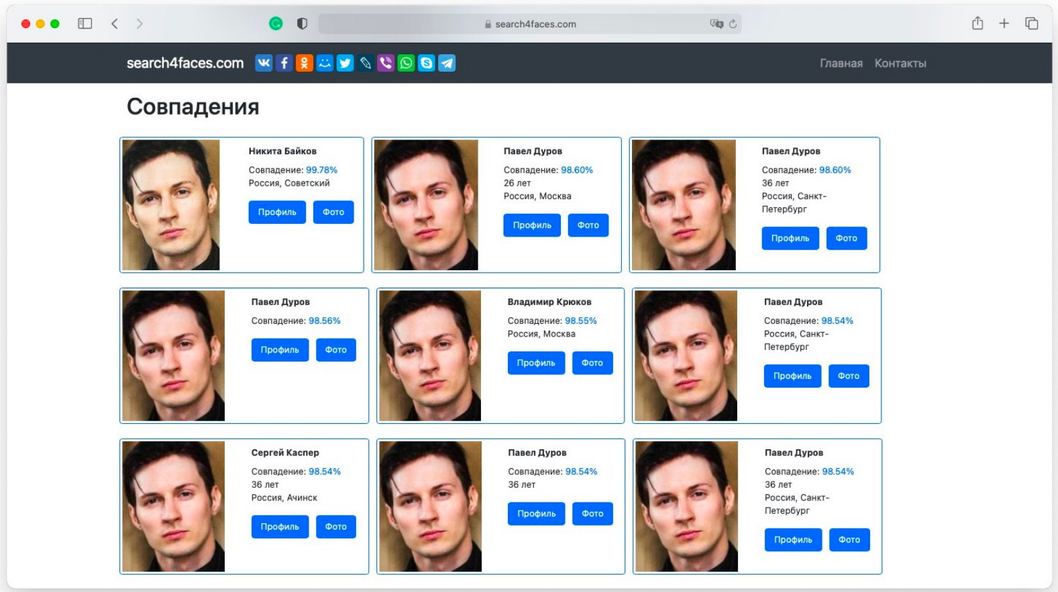

## Функционал:

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)

[ github.com/HowToFind-bot/YaSeeker ]

# Search4face




## Функционал:

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

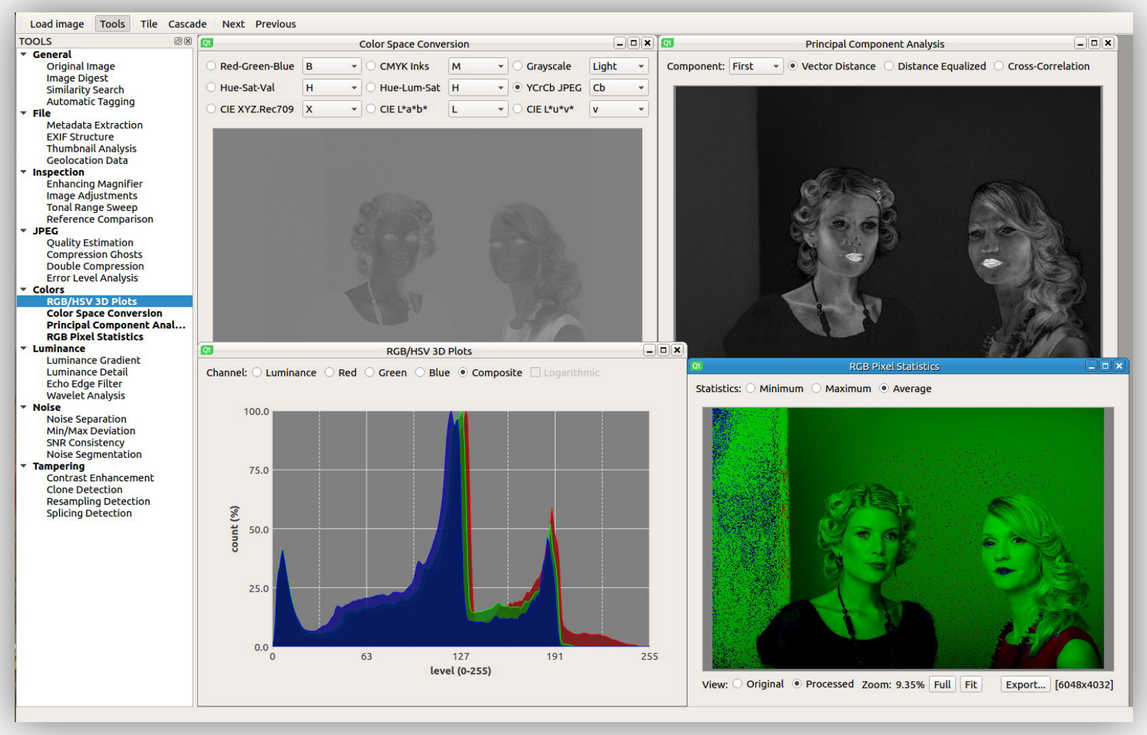
[ search4faces.com ]

# 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.

github.com/GuidoBartoli/sherloq

# Image Verification Assistant

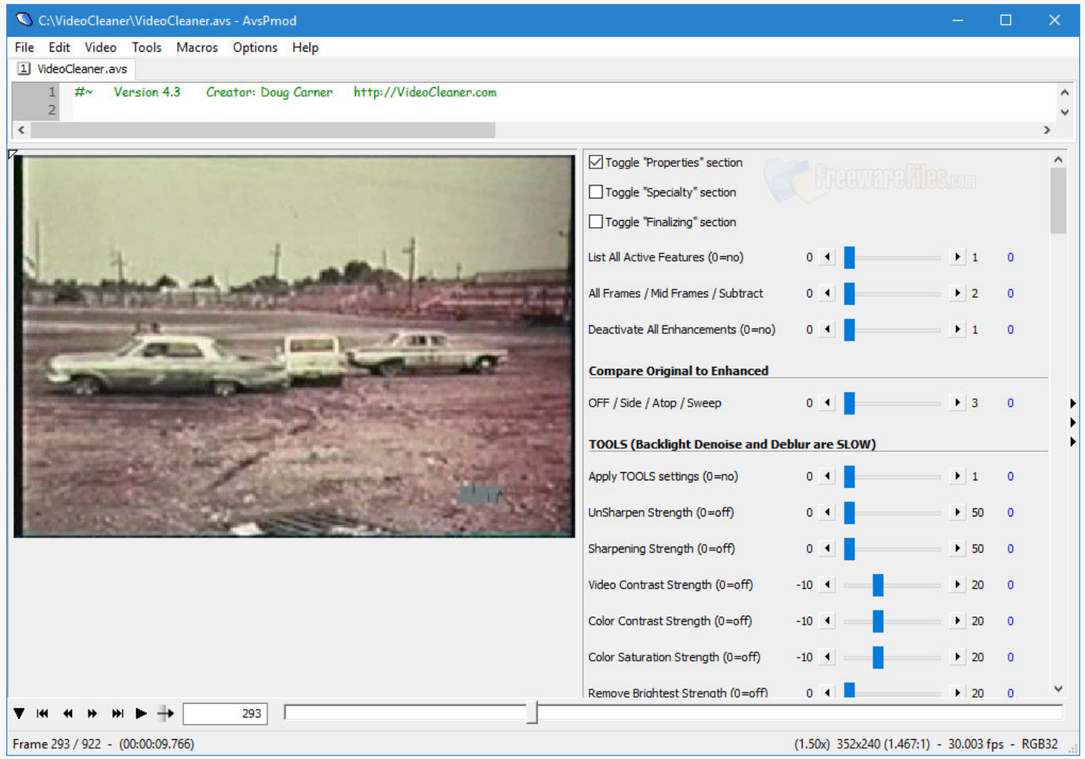

## Функционал:

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.

[ mever.iti.gr/forensics ]

# Как улучшить «картинку» полученную из системы видеонаблюдения?

# Video Cleaner



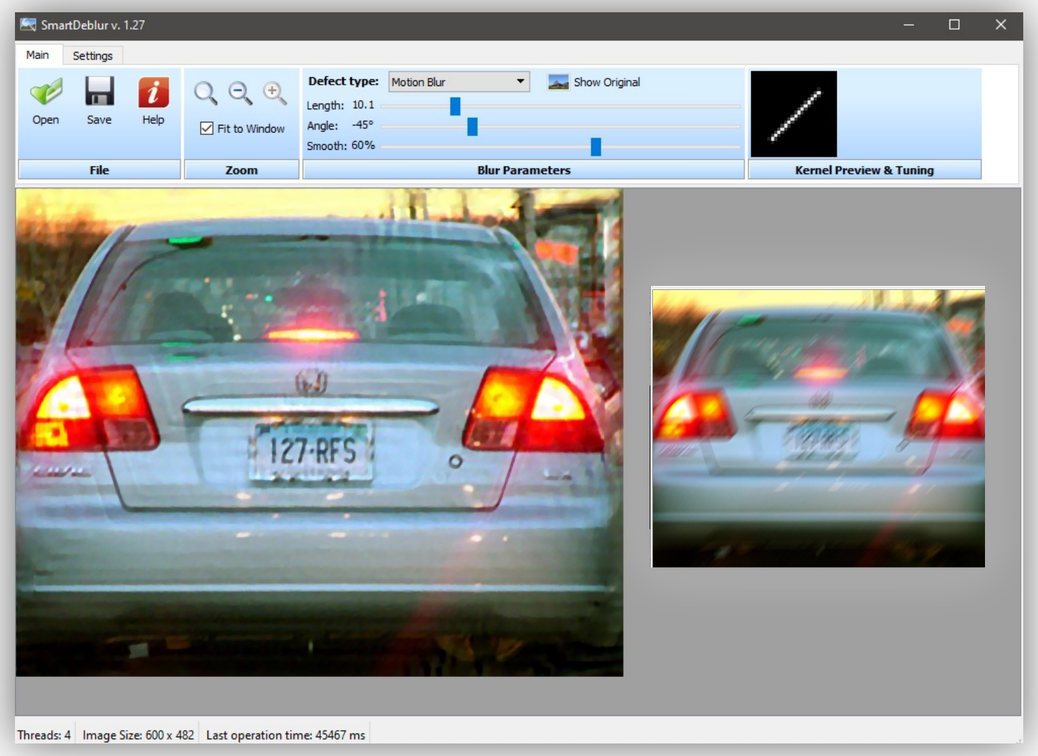

## Функционал:

- 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.

videocleaner.com

# SmartDeblur




## Функционал:

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

## Особенности:

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

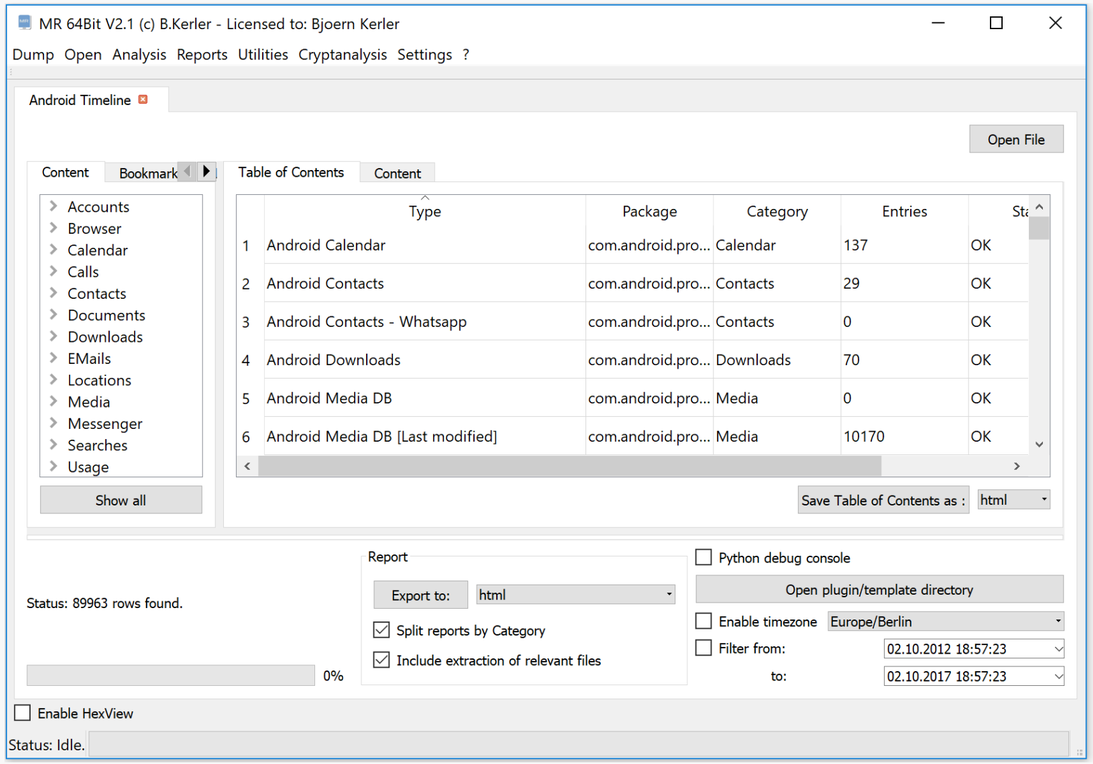
Работает под Windows и MacOS

github.com/Y-Vladimir/SmartDeblur

# Как извлечь данные из смартфона?

# Mobile Revelator

Mobile Forensic




## Функционал:

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

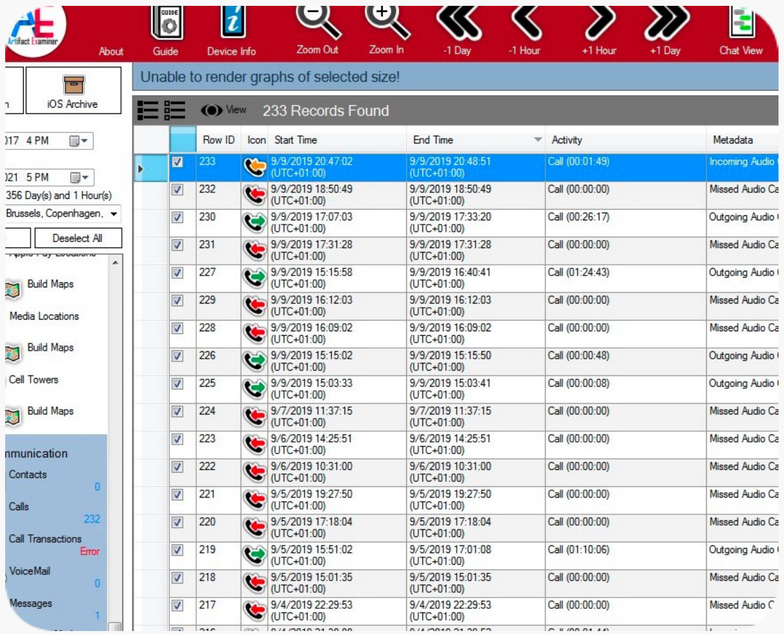
… и еще много что

Работает под Windows

github.com/bkerler/MR

# ArtEx - Artifact Examiner

Mobile Forensic




## Функционал:

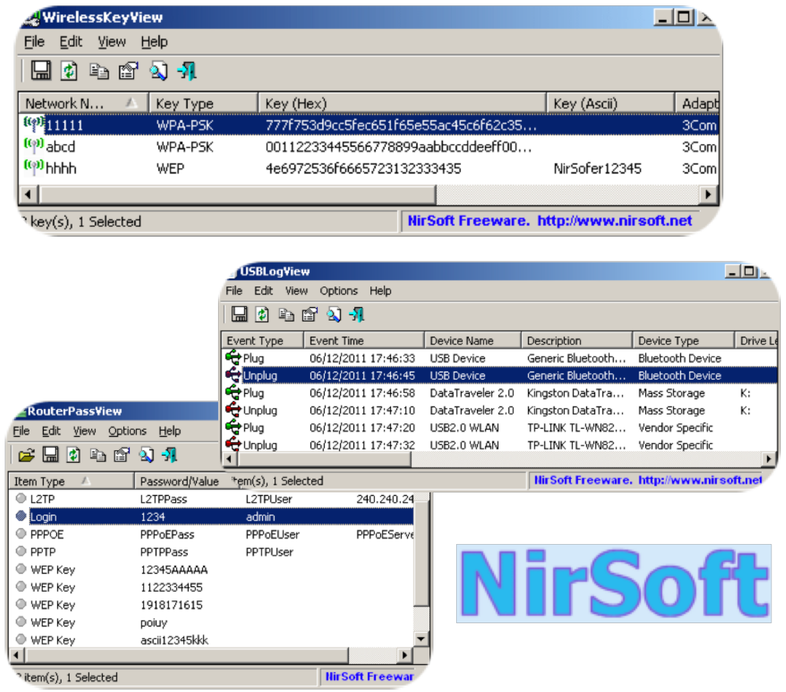
- артефакты: уровень заряда, активность, используемое приложение, события, звонки, сообщения и др.
- построение различных таймлайнов от работы аккумулятора до действий пользователя.
- поддержка извлечений на основе BFU
- местоположение сотовых вышек с поддержкой OpenCellID и CSV • просмотрщик каталогов,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

[ doubleblak.com/software.php?id=1 ]

# Как и какие данные можно вытащить из windows?

# NirSoft Utilites

Более 200 утилит извлечения данных из windows




## 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

nirsoft.net/computer_forensic_software.html

# И еще немного про прикладные задачи...

# Как сделать черный вход в систему win/mac?

# Kon-Boot

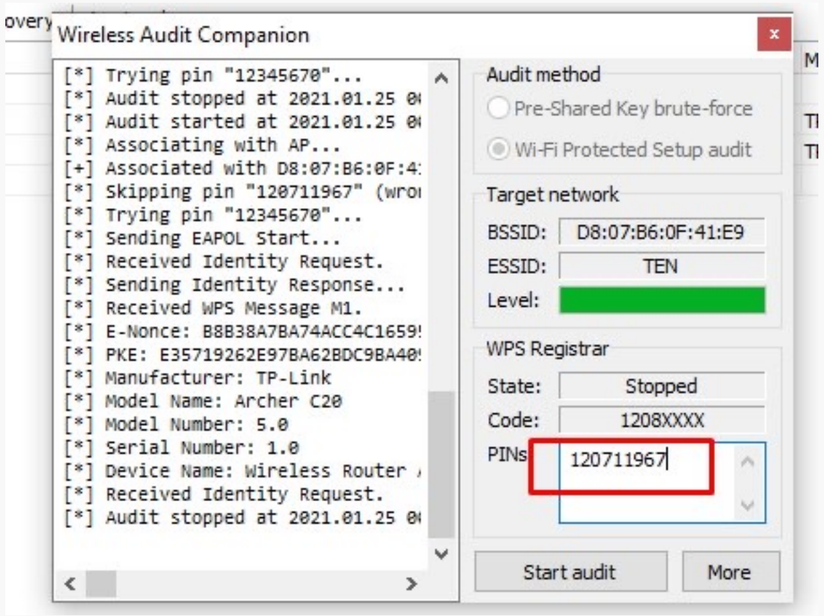

Это инструмент, который позволяет получить доступ к целевому компьютеру, не зная пароля пользователя. В отличие от других решений Kon-Boot не сбрасывает и не изменяет пароль пользователя, и все изменения возвращаются в предыдущее состояние после перезагрузки системы.

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

kon-boot.com

# Как проверить собственную беспроводную сеть на уязвимости?

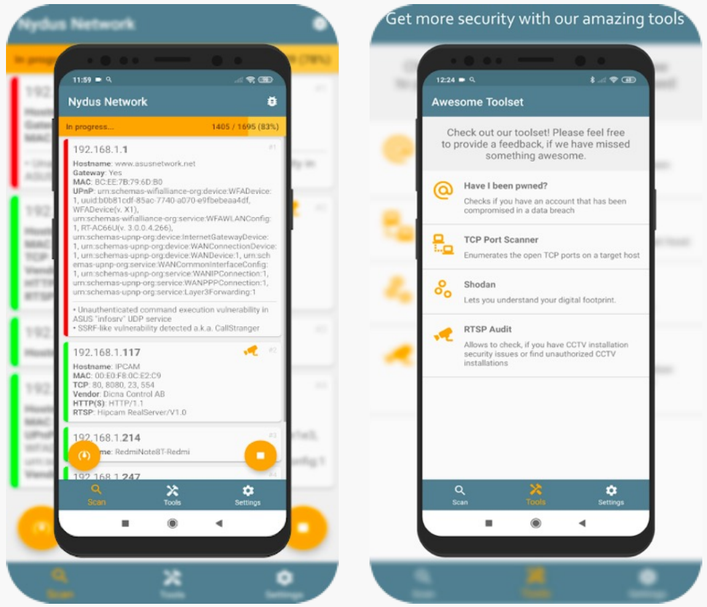
# RouterScan




- находит и определят 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.

stascorp.com/load/1-1-0-56

# IoPT: Network Security Scanner



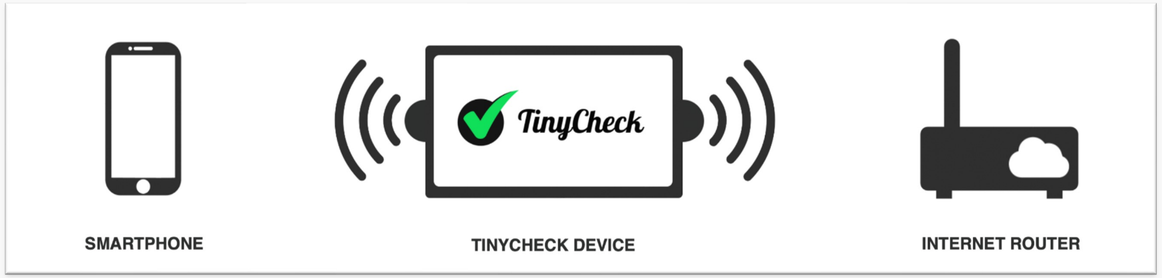




- Аудит безопасности - определение сервисов в сети и выполнение аудита безопасности.
- Обнаружение хостов - определение хостов в сети.
- Сканирование портов - перечислить открытые TCP-порты на целевом хосте.
- Интеграция HiBP - убедитесь, что ваши личные данные не были скомпрометированы в результате 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»

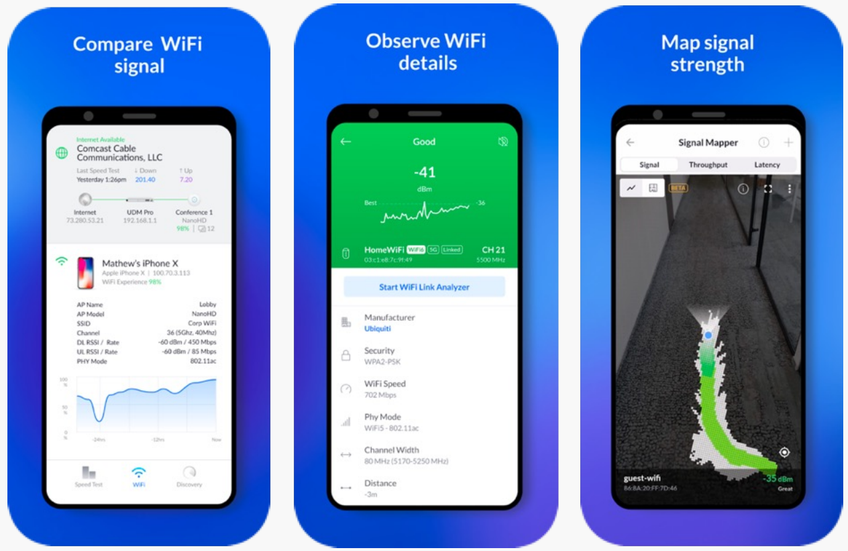
## Особенности:

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

github.com/KasperskyLab/TinyCheck

# Как найти «wifi закладку»

# WiFiman



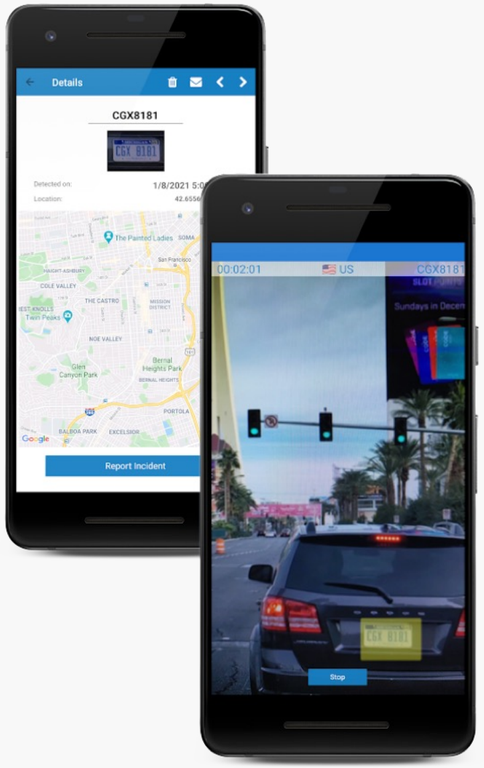

WiFiman идеально подходит для анализа Wi-Fi сетей, устройств Bluetooth LE, обнаружение новых устройств в сети и измерения скорости. Эти возможности доступны в удобном и элегантном интерфейсе пользователя, разработанным Ubiquiti Networks. WiFiman не содержит рекламы и является бесплатным.

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

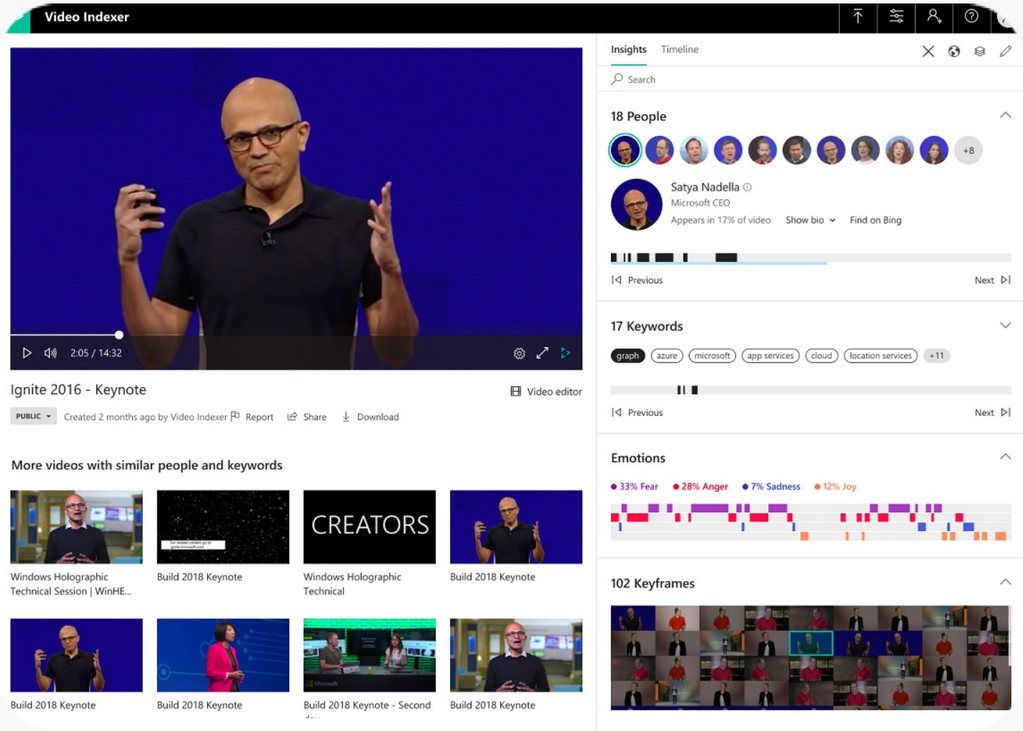



Функционал:
Поддерживает черные/белые списки.
Фиксирование номеров при движение с привязкой к местоположению.
Push уведомления
Отправка уведомлений на почту или в облако.
Поддержка подключения внешних сетевых видеокамер
Возможность сканирования номеров из видеофайлов

Может быть полезно при отслеживание 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




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