Mobile Forensics Day 2019

Ваш шпион: что может рассказать о вас ваше мобильное устройство

Владимир Каталов

ООО «Элкомсофт»

Облако это…

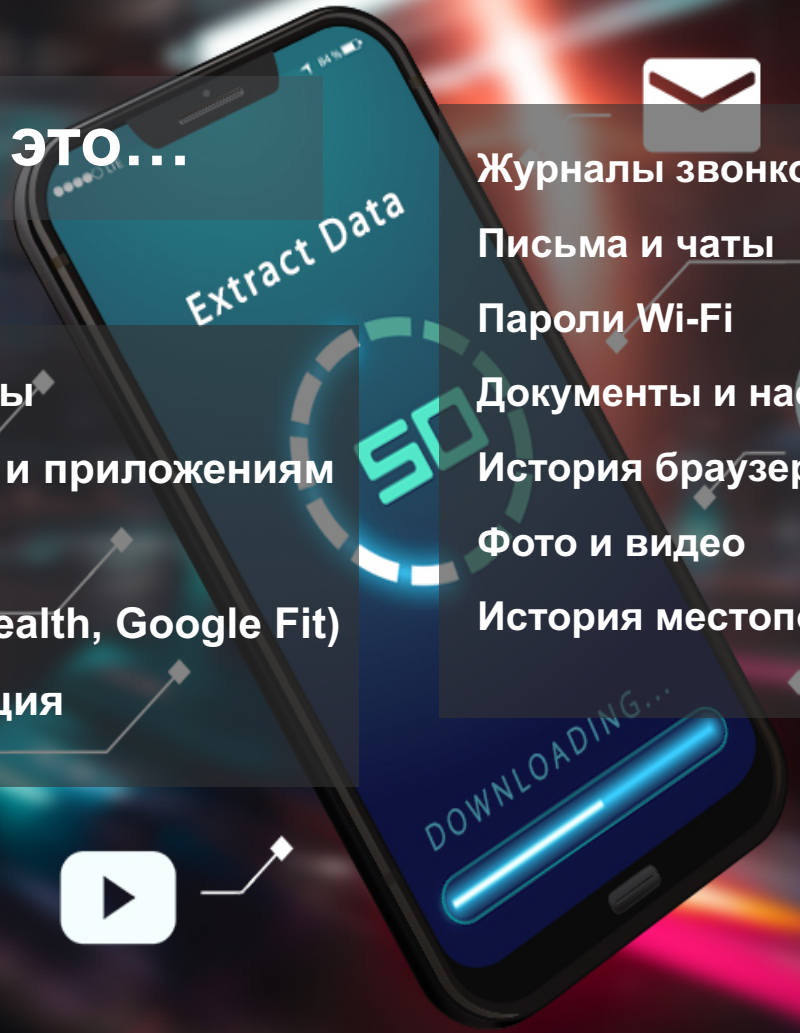
Ваши пароли и токены

Пароли к веб-сайтам и приложениям

SMS и iMessage

«Здоровье» (Apple Health, Google Fit)

Платёжная информация



Журналы звонков

Письма и чаты

Пароли Wi-Fi

Документы и настройки

История браузера и поисковые запросы

Фото и видео

История местоположения и маршруты

Apple и Google

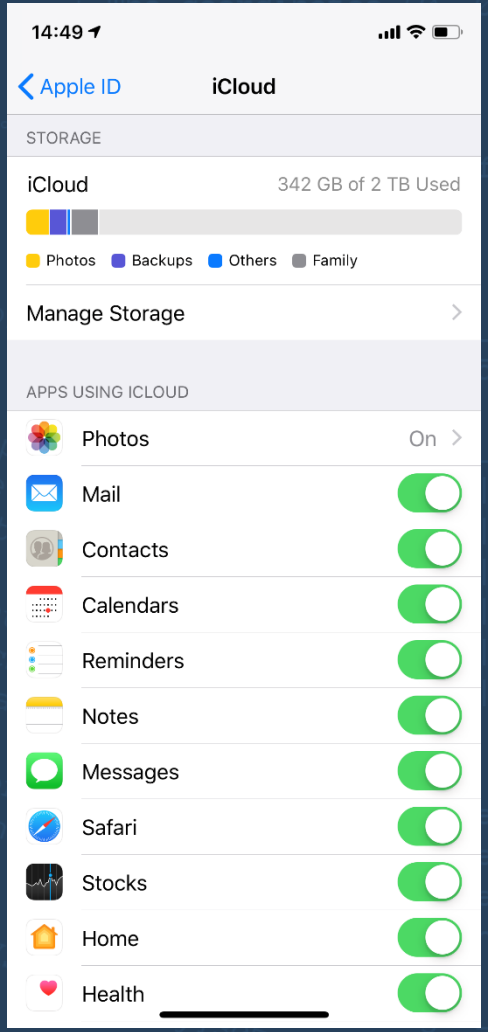
Обе компании собирают ваши данные

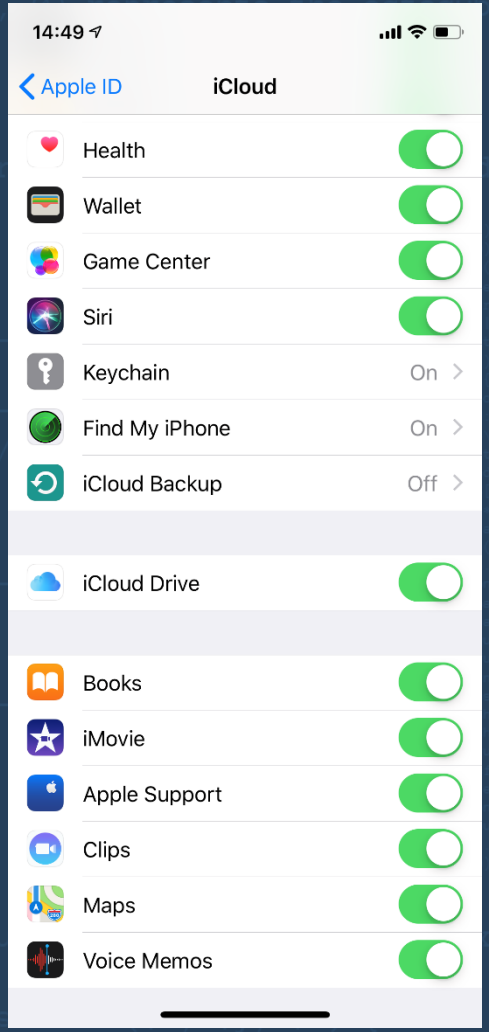
- И у Apple, и у Google есть собственные облачные сервисы
  - Apple iCloud, Google Drive
- Обе компании обрабатывают и хранят гигантские объёмы данных
- Подходы к хранению и обработке кардинально отличаются
- Обе компании сотрудничают с правоохранительными органами, но…
- **По запросу выдаются совершенно разные типы данных**

Что есть в iCloud

Настройки iOS

- На скриншотах показаны основные настройки
- Не все данные есть в настройках (так, журналы звонков, подписи к отправленным письмам, чёрные списки, словари автокоррекции не показаны, но синхронизируются)
- Некоторые данные требуют синхронизации «связки ключей» (Здоровье, Сообщения)
- iCloud Drive – собирательная категория (часть данных доступна только создавшим их приложениям, например, резервные копии WhatsApp и Viber)





Что есть в iCloud

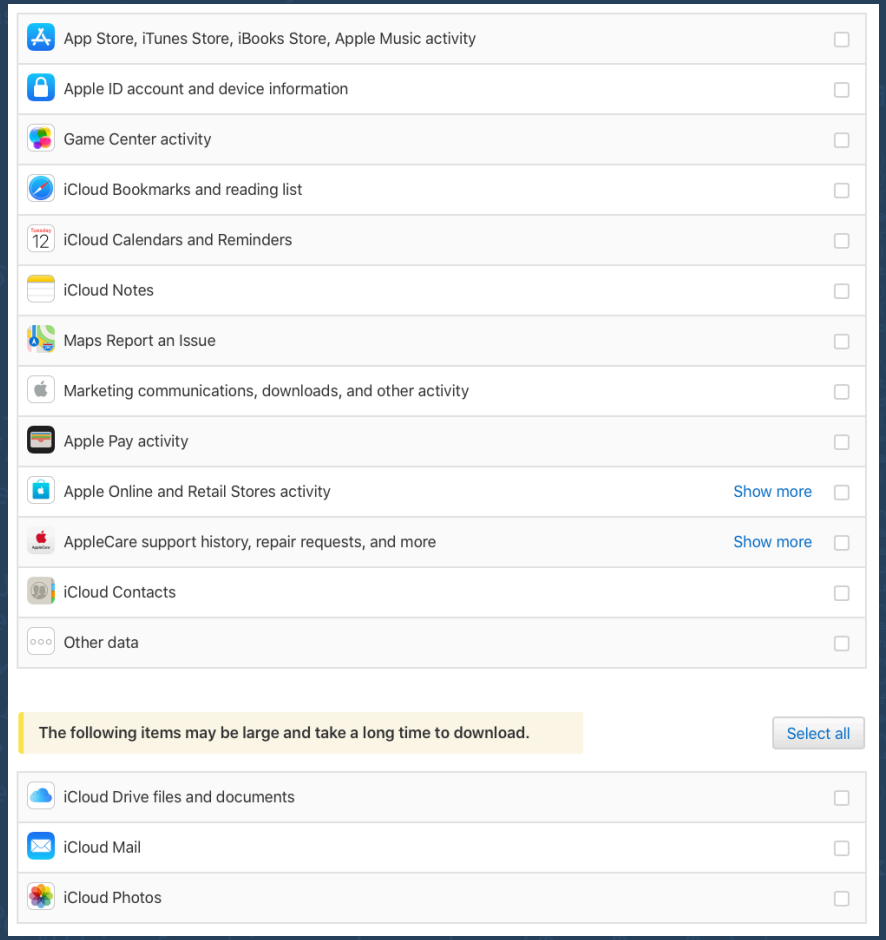
Доступ через icloud.com

- Через сайт icloud.com доступны лишь основные категории
- Владелец учётной записи уведомляется по email
- Работает через браузер (токен сохраняется в виде cookie)

Что есть в iCloud

Портал privacy.apple.com

- Портал доступен для пользователей из ЕС и США (а также некоторых других стран)
- Данные выдаются в течение 7 дней
- Множество форматов данных (txt, csv, xml, json)
- Некоторые данные для внутреннего использования Apple доступны только здесь
- Наибольший интерес представляет категория *Other data*



Безопасность iCloud

Запросы от правоохранительных органов

iii. Email Content and Other iCloud Content. My Photo Stream, iCloud Photo Library, iCloud Drive, Contacts, Calendars, Bookmarks, Safari Browsing History, Maps Search History, Messages, iOS Device Backups

iCloud stores content for the services that the subscriber has elected to maintain in the account while the subscriber's account remains active. Apple does not retain deleted content once it is cleared from Apple's servers. iCloud content may include email, stored photos, documents, contacts, calendars, bookmarks, Safari browsing history, Maps Search History, Messages and iOS device backups. iOS device backups may include photos and videos in the Camera Roll, device settings, app data, iMessage, Business Chat, SMS, and MMS messages and voicemail. All iCloud content data stored by Apple is encrypted at the location of the server. When third-party vendors are used to store data, Apple never gives them the keys. Apple retains the encryption keys in its U.S. data centers. iCloud content, as it exists in the subscriber's account, may be provided in response to a search warrant issued upon a showing of probable cause.

III. Information Available from Apple

A. Device Registration
B. Customer Service Records
C. iTunes
D. Apple Retail Store Transactions
E. Apple Online Store Purchases
F. Gift Cards
G. iCloud
H. Find My iPhone
I. Extracting Data from Passcode Locked iOS Devices
J. Other Available Device Information
K. Requests for Apple Retail Store CCTV Data
L. Game Center
M. iOS Device Activation
N. Sign-on Logs
O. My Apple ID and iForgot Logs
P. FaceTime
Q. iMessage

Что собирает Google

Google Account содержит:

- Информация о пользователе
- Список устройств
- Резервные копии Android (Android 9: зашифрованы)
- **Многолетняя история местоположения**
- Контакты, заметки, календари
- Почти Gmail
- Журналы звонков, текстовые сообщения SMS
- Фото и медиа-файлы
- Чаты Hangouts
- История поиска в Google и YouTube
- Данные Chrome
  - История, закладки, вкладки, переходы
  - **Пароли к учётным записям** и данные автозаполнения
- Статистика использования устройств

Безопасность данных в Google

Дополнительная безопасность?

- По умолчанию, логин, пароль и 2FA достаточны для доступа к основной части данных
  - Даже пароли
  - Даже данные «Здоровья» (Google Fit)
- Данные доступны любому, кто сможет войти в учётную запись
- Google Takeout возвращает практически все данные
- В разнообразных форматах (txt, csv, xml, json)
- Резервные копии в Android зашифрованы начиная с Android 9
  - ~10% устройств на сентябрь 2019

Безопасность данных в Google

Можно ли защитить данные?

- С недавних пор на синхронизированные данные Chrome (и только на них) стало возможным установить пароль
- В этом случае логины и пароли, история поисковых запросов, закладки и открытые вкладки будут зашифрованы паролем
- Включение пароля потребует ввести тот же пароль на каждом устройстве, где пользователь использует Chrome
- Включение пароля не приводит к моментальному удалению синхронизированных данных Chrome
  - Мы отслеживали изменения в течение нескольких дней после включения кодовой фразы, но синхронизация и извлечение данных **Elcomsoft Cloud Explorer** продолжали работать и без пароля
- Как создать кодовую фразу: https://support.google.com/chrome/answer/165139?hl=ru
- Подавляющее большинство пользователей об этой возможности не знает

iCloud и резервные копии

- Резервные копии устройств (до 2)
- Данные приложений (если разрешено разработчиком); некоторые приложения используют собственные резервные копии
- Фото (если не включена iCloud Photo Library)
- SMS/iMessage (если не включены «Сообщения в iCloud»)
- Пароли (связка ключей): восстановление только на то же устройство
- Некоторые приложения используют собственные резервные копии в iCloud Drive
- Синхронизированные данные: от заметок и календарей до здоровья

Доступ к резервным копиям

- Логин и пароль
- Прохождение 2FA
- Часть данных зашифрована аппаратным ключом, не может быть расшифрована при скачивании

Резервные копии Android

Ограничения и содержимое

Большая часть данных синхронизируется, а не сохраняется в резервной копии

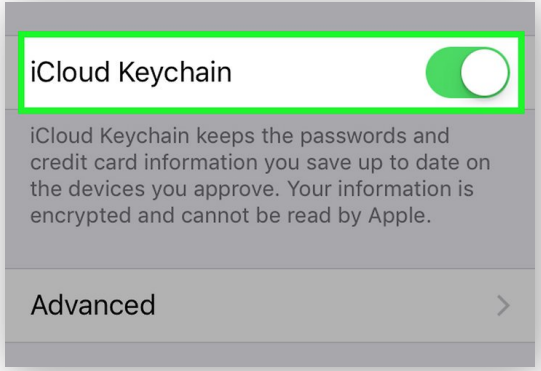
- Android 6.0: появление резервного копирования
- Android 8.0: сохраняются SMS
- Android 9.0: шифрование кодом блокировки
- Настройки
- Часть данных приложений (ограничение на объём)
- SMS (Android 8.0 и выше)
- Журнал звонков

- Создаются автоматически, даже если пользователь их не включал
- Удаляются из Google Drive через 60 дней

iCloud: пароли

Связка ключей iCloud Keychain

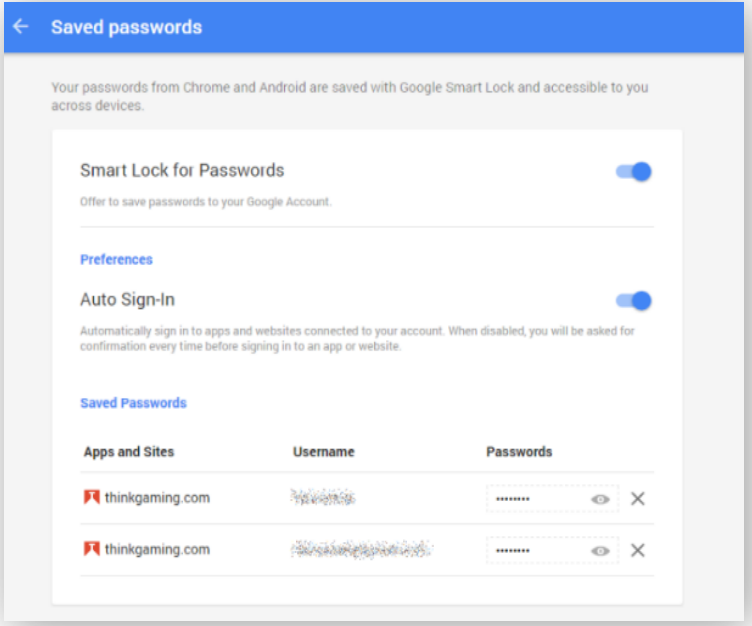
- Пароли, карты и токены синхронизируются в iCloud
- Apple не предоставляет API для доступа к данным
- Компания Apple не имеет доступа к паролям (они зашифрованы)
- Для доступа требуется код блокировки одного из устройств, участвующих в синхронизации



Google: пароли

Пароли в Chrome

- Синхронизация через Google Drive
- Доступна для Android, Chrome для iOS, Windows, macOS
- По умолчанию дополнительной защиты нет
    - Может быть установлен дополнительный пароль
- Доступны по логину, паролю и 2FA
- Моментальное извлечение из компьютеров Windows и Mac (если Chrome установлен, а пользователь вошёл в учётную запись)



iCloud: SMS и iMessage

Облачные сообщения

- Синхронизация сообщений появилась в iOS 11.4
- Сообщения зашифрованы
  - AES256, требуется код блокировки
- Apple ID, пароль и 2FA
- Код блокировки или системный пароль одного из участвующих в синхронизации устройств

Google: SMS

SMS в резервных копиях

- Сообщения в Android не синхронизируются
- SMS сохраняются в резервных копиях
  - Android 8 и новее (Pixel: Android 7.1+)
  - MMS не сохраняются
- Для извлечения достаточно зайти в Google Account
  - Android 9 и новее: резервные копии зашифрованы кодом блокировки устройства

Местоположение

Ваш смартфон – идеальное устройство для слежки

- Активное и пассивное определение местоположение
- Высокая или приблизительная точность
- Постоянно активно (если не выключено в явном виде)
- Выключение не всегда помогает https://www.bbc.com/news/technology-45183041 https://www.macrumors.com/2018/08/13/google-location-history-disabled-still-stores-data/

Местоположение

Кто отслеживает местоположение?

- Google (iOS, Android, компьютеры – Chrome, все сервисы Google)
- Apple (iOS, macOS)
- Facebook (на всех платформах)
- Огромное количество сторонних приложений, в том числе использующих рекламные SDK; в большинстве приложений таких SDK более одного; каждый SDK отправляет данные по нескольким адресам
- *Даже если вы отключите определение местоположения*

Местоположение

Зачем Google, Apple и FB ваши координаты?

- **Разумеется, для вашей пользы:**
  - Google/Apple Maps, навигация
  - FB: локальные события и группы
  - Релевантный поиск
  - Find My Phone / Find My Device
  - Удобство: можно узнать заполненность заведения заранее в любое время, в том числе в реальном времени
  - Навигация внутри помещений

Местоположение

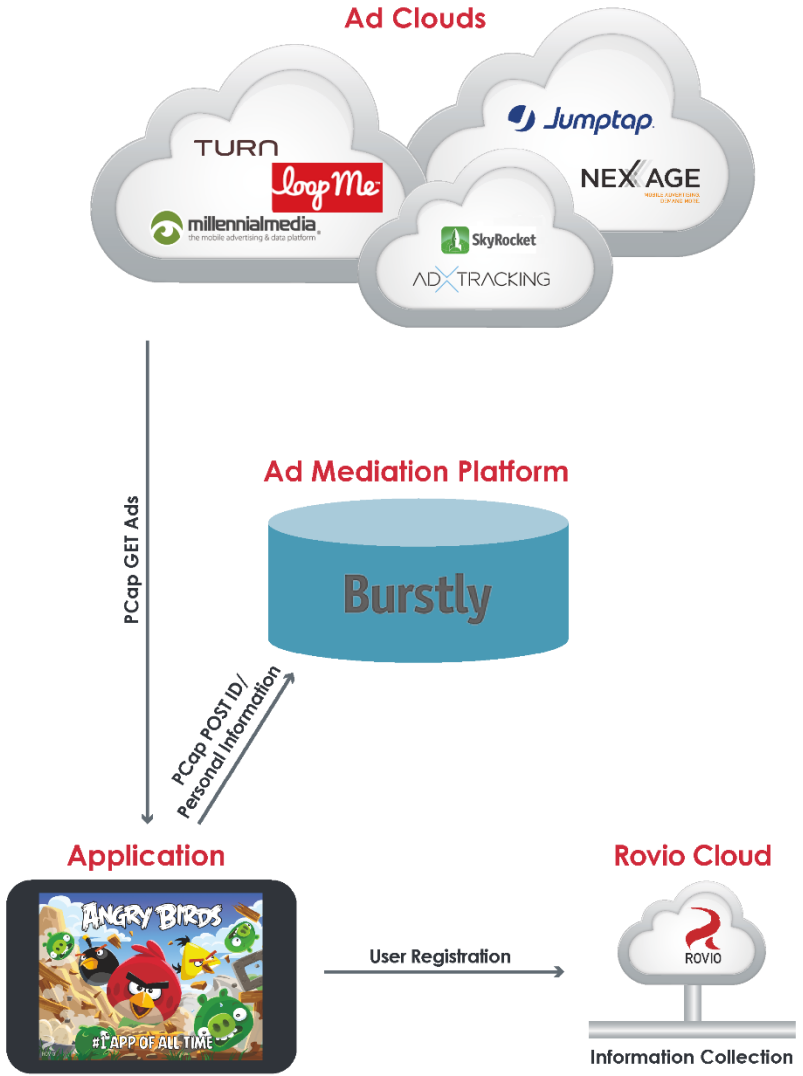
Зачем Google, Apple и FB ваши координаты на самом деле?

- **Продажа рекламы**
  - Основной источник дохода Google
  - Реклама, привязанная к местоположению
  - Facebook: гигантская рекламная сеть
- **Продать ваши данные**
  - Apple и Google не продают данные
  - Продажа данных – основной бизнес Facebook

Местоположение

Сторонние приложения

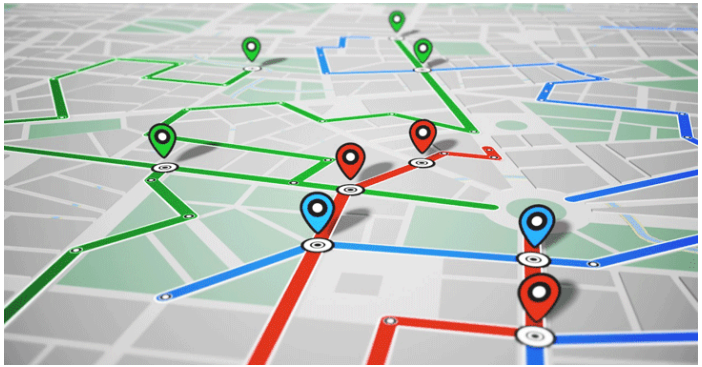
- **Сторонние приложения собирают все данные, к которым могут получить доступ**
- Разумеется, для вашей пользы:
  - Вы можете играть в эту игру совершенно бесплатно!
- Продать ваши данные:
  - Многочисленные брокеры и посредники
  - Данные собираются любыми способами
  - Например, сканированием сетей Wi-Fi и определением местоположения по BSSID
  - IP адрес для приблизительного определения местоположения



Местоположение

Где хранятся данные?

- На самих устройствах (iOS, Android, Windows, macOS X и т.п.)
- Apple iCloud (резервные копии и синхронизированные данные)
- Google Account
- Сторонние облачные сервисы
  - Социальные сети
  - Фитнес-приложения
  - Мессенжеры
  - Сайты и приложения знакомств
  - Приложения такси
  - Планирование поездок



Местоположение

Как хранит данные Apple

- Данные хранятся:
  - Записи в базах данных
  - В файлах PLIST
  - В записях JSON
  - Смешанные структуры PLIST/JSON в БД
  - Журналы
- Где:
  - Системные базы данных
  - Песочницы встроенных и сторонних приложений
  - Временные данные и кэш
  - iCloud

Местоположение

Что собирает Apple

- Зависит от источника и места хранения
- Доступны всегда:
  - **Широта**
  - **Долгота**
  - **Время** (как правило, в формате UNIX Epoch)
  - Иногда время отсутствует
  - Иногда отсутствуют и координаты
- Могут быть доступны:
  - **Высота над уровнем моря**
  - **Точность**
  - **Уверенность** (насколько система уверена в заданной точности)
  - **Рамки возможных широты и долготы**
  - **Скорость**
  - **Направление**
  - **Дата, когда устройство покинуло точку**
  - **Адрес** – строка или список

Местоположение

Wallet

- Пути:
- /HomeDomain/Library/Passes/Cards
- /HomeDomain/Library/Passes/BadUbiquitousPasses
- Папки .pkpass
- В файлах pass.json


```
{
  "description": "SOURCE to DESTINATION",
  "formatVersion": 1,
  "organizationName": "The Airlines",
  "relevantDate": "2013-02-20T20:40:00+01:00",
  "boardingPass": {
    "transitType": "PKTransitTypeAir"
  },
  "locations": [
    {
      "latitude": 12.11334800,
      "longitude": 13.56972200,
      "relevantText": "AirportName1"
    },
    {
      "latitude": 80.45861100,
      "longitude": 80.10611100,
      "relevantText": "AirportName2"
    }
  ]
}
```

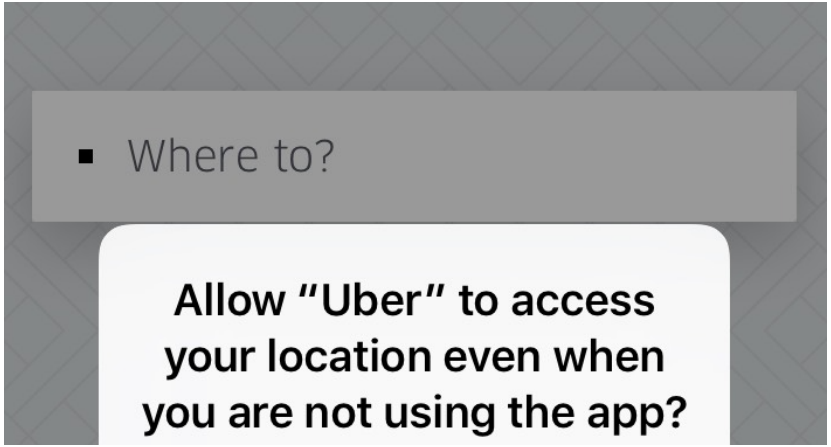
Местоположение

Сторонние приложения

- Многочисленные приложения собирают данные
  - В том числе в фоновом режиме
- Могут не попадать в резервные копии
- Хранятся на устройстве:

  /private/var/mobile/Containers/Data/Application/<UUID>/Library/Caches/

  <UUID>: уникальный идентификатор приложения




```
{
   "jsonConformingObject":{
      "meta":{
         "location":{
            "course":-1,
            "city":"test",
            "speed":-1,
            "longitude":3.4,
            "gps_time_ms":1506351484216,
            "latitude":1.2,
            "horizontal_accuracy":65,
            "vertical_accuracy":10,
            "altitude":0.1
         }
      }
   }
}
```

Местоположение

Часть данных доступно только при физическом анализе

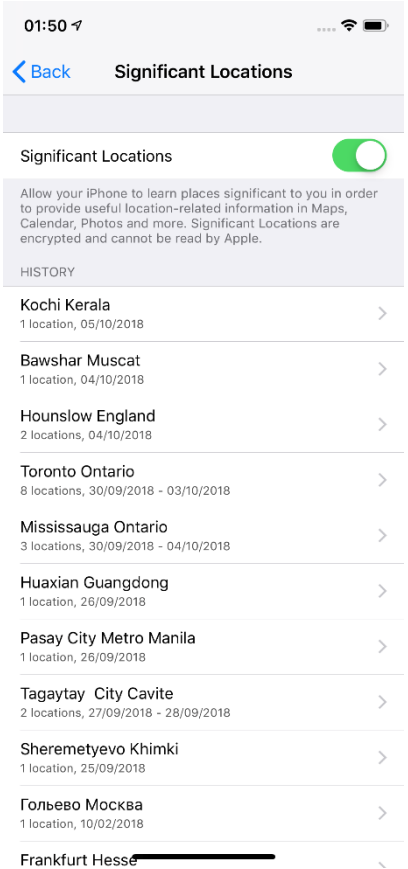
- Образ файловой системы
- Кэш местоположения (3G/LTE, Wi-Fi)
- Частые/значительные точки
- Кэш анализа медиа-файлов
- Кэш сторонних приложений
- Apple Pay

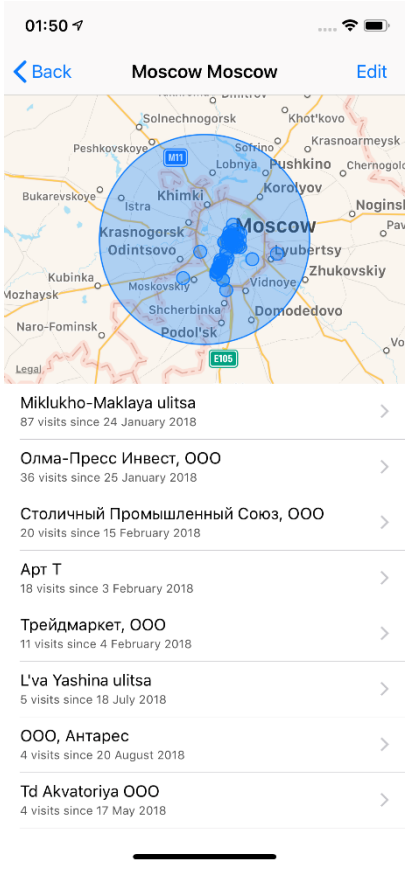
Местоположение

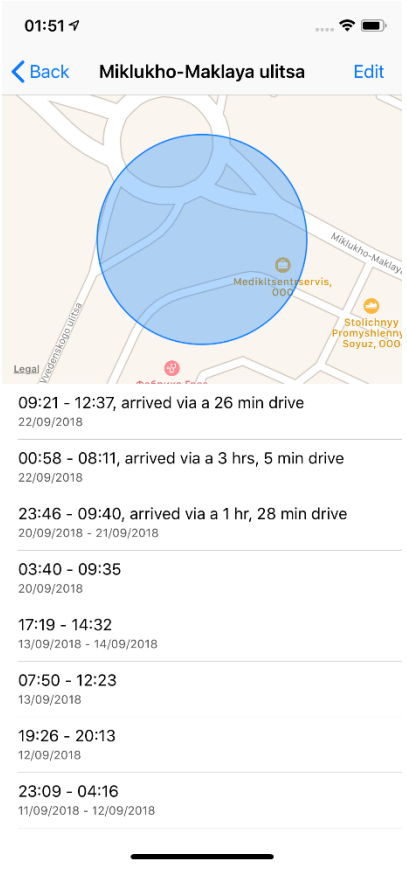
Кэш местоположения (физический анализ)

- Базы данных:
  - /private/var/root/Library/Caches/locationd/cache_encryptedA.db
  - /private/var/root/Library/Caches/locationd/cache_encryptedB.db
  - /private/var/mobile/Library/Caches/com.apple.routined/cache_encryptedA.db
  - /private/var/mobile/Library/Caches/com.apple.routined/cache_encryptedB.db
- Таблицы:
  - Latitude, Longitude, Altitude, Timestamp, HorizontalAccuracy, VerticalAccuracy, Speed, Course, Confidence
  - MinimumLatitude, MinimumLongitude, MaximumLatitude, MaximumLongitude

Significant locations







Местоположение

Данные в iCloud

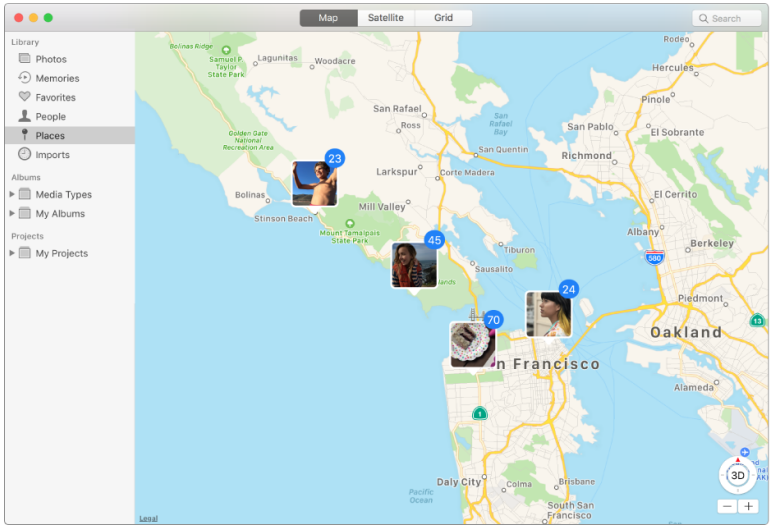
- Синхронизированные данные приложений:
  - Apple Maps
  - Health
  - Calendar
  - Wallet
- Прямая синхронизация:
  - Significant Locations: только прямая синхронизация минуя iCloud
- Подключения Wi-Fi
  - Определение по BSSID
  - Часто только время подключения и отключения
  - В журналах содержится время и дата

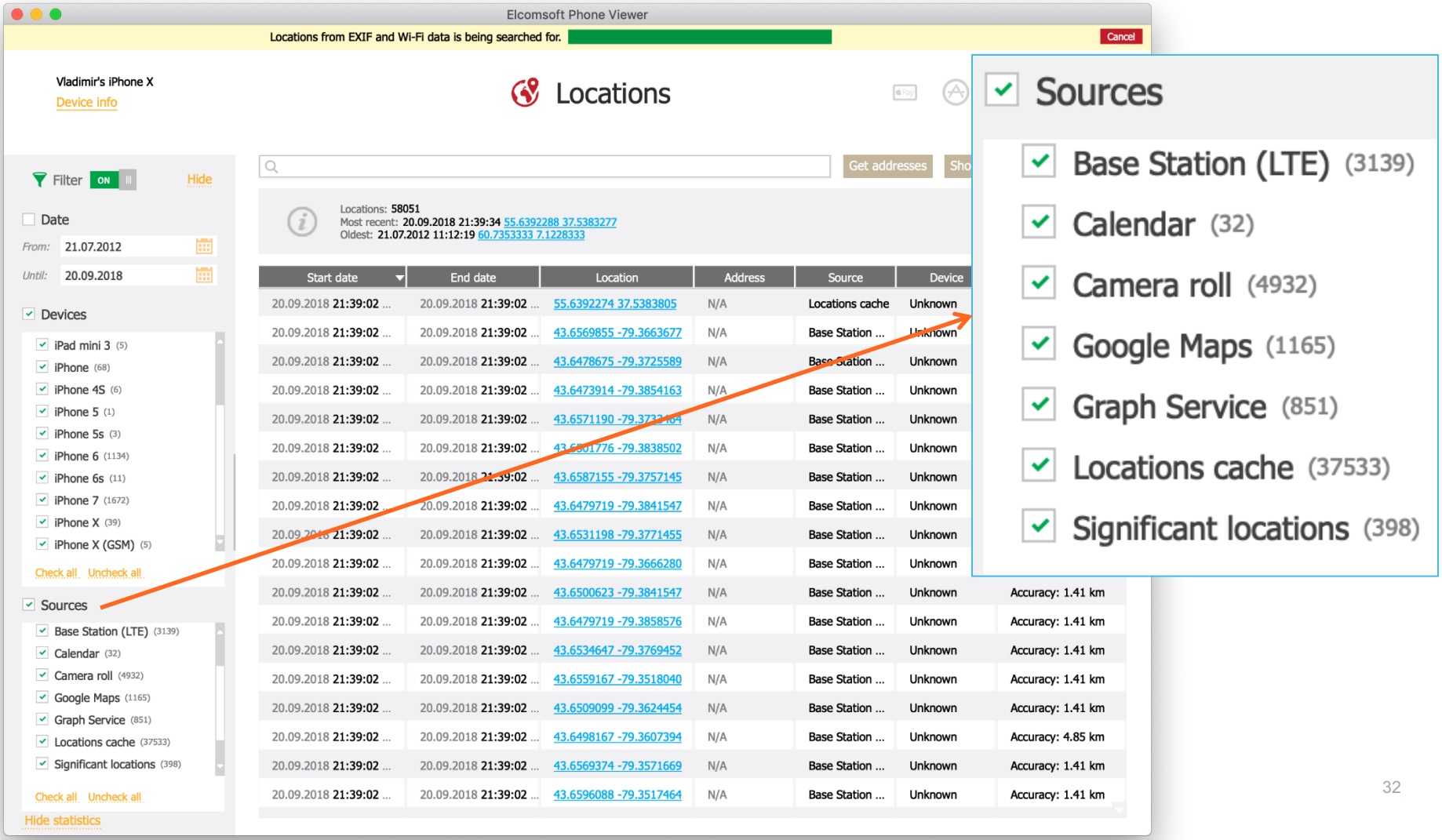
Местоположение

Кэш анализа медиа-файлов

- **photoanalysisd** – процесс, анализирующий медиа-файлы для назначения тегов, определения лиц, каталогизации
- **photosgraph** точки из EXIF на карте

/private/var/mobile/Media/PhotoData/Caches/GraphService/PhotosGraph/photosgraph.graphdb

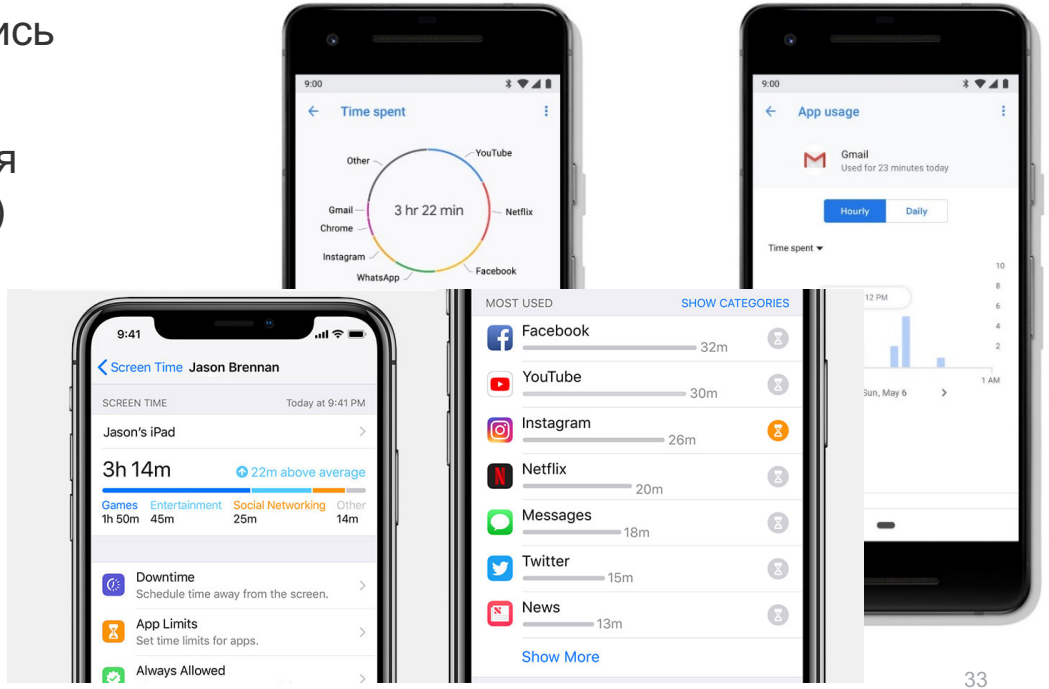



Elcomsoft Phone Viewer
Locations from EXIF and Wi-Fi data is being searched for.
Cancel
Vladimir's iPhone X
Device info
Locations
Filter ON
Hide
Date
From: 21.07.2012
Until: 20.09.2018
Devices
iPad mini 3 (5)
iPhone (68)
iPhone 4S (6)
iPhone 5 (1)
iPhone 5s (3)
iPhone 6 (1134)
iPhone 6s (11)
iPhone 7 (1672)
iPhone X (39)
iPhone X (GSM) (5)
Check all Uncheck all
Sources
Base Station (LTE) (3139)
Calendar (32)
Camera roll (4932)
Google Maps (1165)
Graph Service (851)
Locations cache (37533)
Significant locations (398)
Check all Uncheck all
Hide statistics
Get addresses
Locations: 58051
Most recent: 20.09.2018 21:39:34 55.6392288 37.5383277
Oldest: 21.07.2012 11:12:19 60.7353333 7.1228333
Start date
End date
Location
Address
Source
Device
20.09.2018 21:39:02 ... 20.09.2018 21:39:02 ... 55.6392274 37.5383805 N/A Locations cache Unknown
20.09.2018 21:39:02 ... 20.09.2018 21:39:02 ... 43.6569855 -79.3663677 N/A Base Station ... Unknown
20.09.2018 21:39:02 ... 20.09.2018 21:39:02 ... 43.6478675 -79.3725589 N/A Base Station ... Unknown
20.09.2018 21:39:02 ... 20.09.2018 21:39:02 ... 43.6473914 -79.3854163 N/A Base Station ... Unknown
20.09.2018 21:39:02 ... 20.09.2018 21:39:02 ... 43.6571190 -79.3731464 N/A Base Station ... Unknown
20.09.2018 21:39:02 ... 20.09.2018 21:39:02 ... 43.6601776 -79.3838502 N/A Base Station ... Unknown
20.09.2018 21:39:02 ... 20.09.2018 21:39:02 ... 43.6587155 -79.3757145 N/A Base Station ... Unknown
20.09.2018 21:39:02 ... 20.09.2018 21:39:02 ... 43.6479719 -79.3841547 N/A Base Station ... Unknown
20.09.2018 21:39:02 ... 20.09.2018 21:39:02 ... 43.6531198 -79.3771455 N/A Base Station ... Unknown
20.09.2018 21:39:02 ... 20.09.2018 21:39:02 ... 43.6479719 -79.3666280 N/A Base Station ... Unknown
20.09.2018 21:39:02 ... 20.09.2018 21:39:02 ... 43.6500623 -79.3841547 N/A Base Station ... Unknown Accuracy: 1.41 km
20.09.2018 21:39:02 ... 20.09.2018 21:39:02 ... 43.6479719 -79.3858576 N/A Base Station ... Unknown Accuracy: 1.41 km
20.09.2018 21:39:02 ... 20.09.2018 21:39:02 ... 43.6534647 -79.3769452 N/A Base Station ... Unknown Accuracy: 1.41 km
20.09.2018 21:39:02 ... 20.09.2018 21:39:02 ... 43.6559167 -79.3518040 N/A Base Station ... Unknown Accuracy: 1.41 km
20.09.2018 21:39:02 ... 20.09.2018 21:39:02 ... 43.6509099 -79.3624454 N/A Base Station ... Unknown Accuracy: 1.41 km
20.09.2018 21:39:02 ... 20.09.2018 21:39:02 ... 43.6498167 -79.3607394 N/A Base Station ... Unknown Accuracy: 4.85 km
20.09.2018 21:39:02 ... 20.09.2018 21:39:02 ... 43.6569374 -79.3571669 N/A Base Station ... Unknown Accuracy: 1.41 km
20.09.2018 21:39:02 ... 20.09.2018 21:39:02 ... 43.6596088 -79.3517464 N/A Base Station ... Unknown Accuracy: 1.41 km
Sources
Base Station (LTE) (3139)
Calendar (32)
Camera roll (4932)
Google Maps (1165)
Graph Service (851)
Locations cache (37533)
Significant locations (398)

Использование телефона

Ваш сматрфон знает больше о вашей жизни

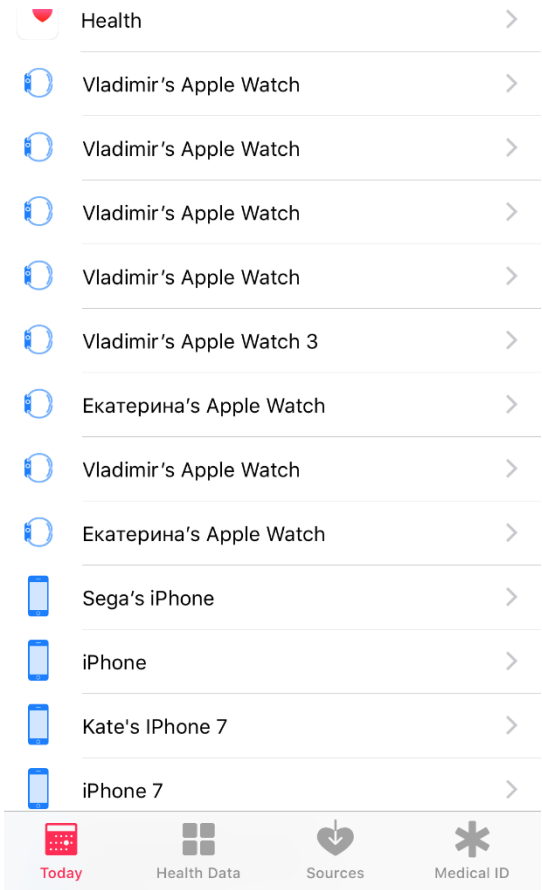
- У Apple и Google недавно появились средства учёта и статистики
- Детальные данные использования приложений (плюс по категориям)
- Часовая, дневная и недельная статистика



Apple Health

Источники данных «Здоровье»

- Приложение «Здоровье» собирает данные как с самого iPhone, так и из многочисленных сторонних приложений
- Используются датчики часов Apple Watch и данные установленных на часах приложений
  - Данные поступают автоматически
  - Пульс пользователя в момент совершения преступления – важная косвенная улика



Часы и «Здоровье»

Облачный анализ

- Apple Watch – одно из основных устройств, поставляющих информацию системе Apple «Здоровье»
- Большинство пользователей устанавливает одно или несколько сторонних приложений (Pedometer++, Runkeeper, Strava и т.п.)
- Подсчёт шагов пользователя и измерение пульса даже в отсутствие iPhone
- Во время пробежек и физических упражнений пульс измеряется постоянно; включается автономный датчик GPS, отслеживаются и сохраняются координаты

Анализ Apple Watch

Облачный анализ

- Данные «Здоровья» в облаке надёжно зашифрованы (iOS 12, 13)
  - Не предоставляются Apple по запросу от правоохранительных органов
  - Мы единственные, кто способен извлечь и расшифровать эти данные
- **Для извлечения данных «Здоровья» необходимы:**
  - Elcomsoft Phone Breaker (Forensic Edition)
  - Логин и пароль от учётной записи Apple ID пользователя
  - Одноразовый код двухфакторной аутентификации (можно получить на SIM-карту в виде SMS)
  - Код блокировки iPhone или пароль от компьютера Mac пользователя

Экранное время

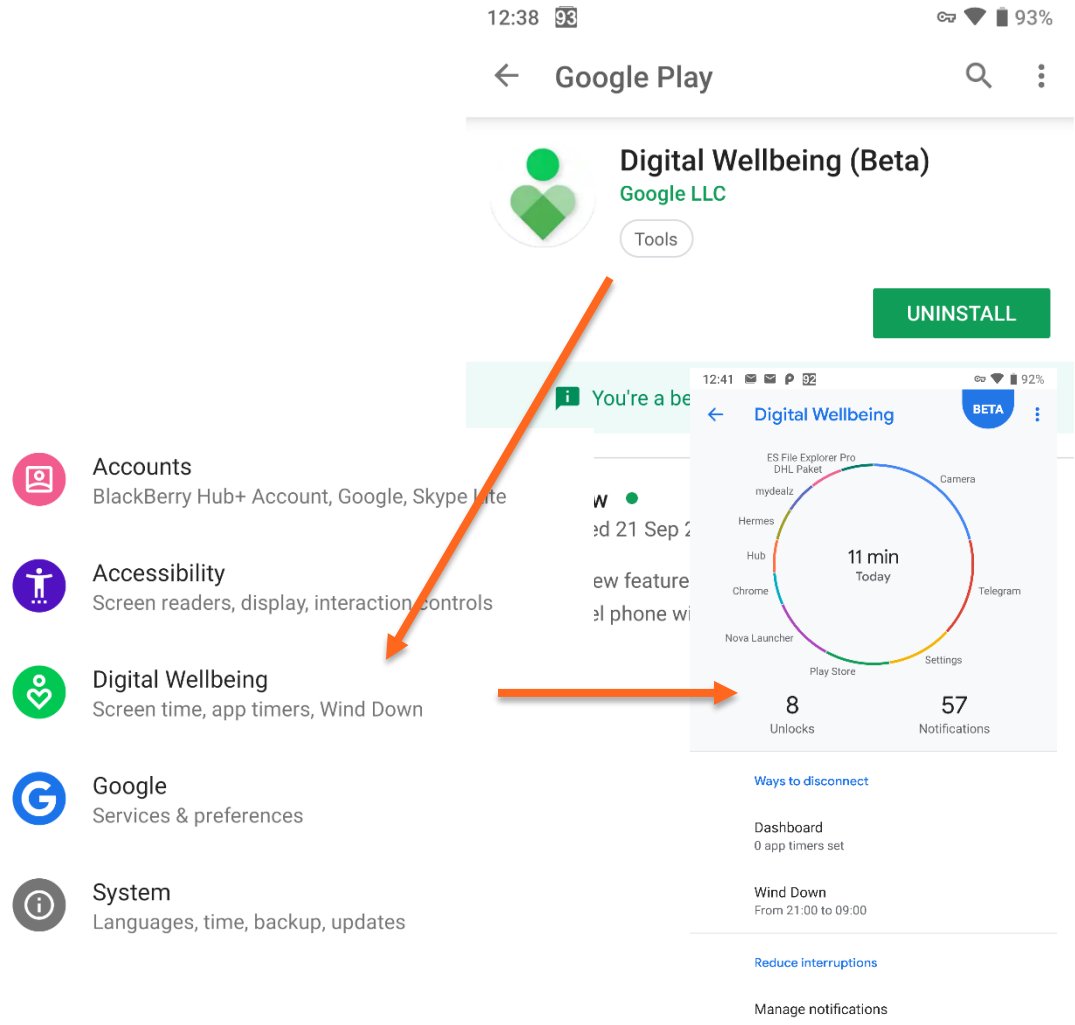
Статистика использования

- Отчёты по дням и неделям
- Категоризация приложений
- Отслеживание каждого приложения и целых категорий
- Учёт количества включений и разблокирований устройства
- **Синхронизируется с облако со всех устройств в рамках учётной записи**

Google

Digital Wellbeing

- Доступно в некоторых смартфонах с Android Pie
- До сих пор бета
- Нужна установка из Google Play
- Доступ через настройки устройства
- Ежедневные отчёты
  - Количество разблокировок
  - Уведомления
  - Статистика использования по приложениям



Google

Family Link

- **Отдельная подсистема контроля «детского времени»**
- Только для детских учётных записей
  - Автоматические ограничения (например, становится недоступным приложение YouTube)
  - Ограничения: общие и по конкретным приложениям
  - Нет категоризации
  - Родитель должен вручную настроить устройство
  - Дальнейший контроль через облако

Экранное время и ограничения

Реализации Apple и Google

- **Apple Screen Time**
  - Статистика по использованию приложений и категорий
  - Ежедневные и недельные сводки
  - Синхронизация через iCloud
    - Статистика и ограничения
  - Ограничение по времени суток
  - Статистика по уведомлениям
  - Код-пароль ограничений Экранного времени

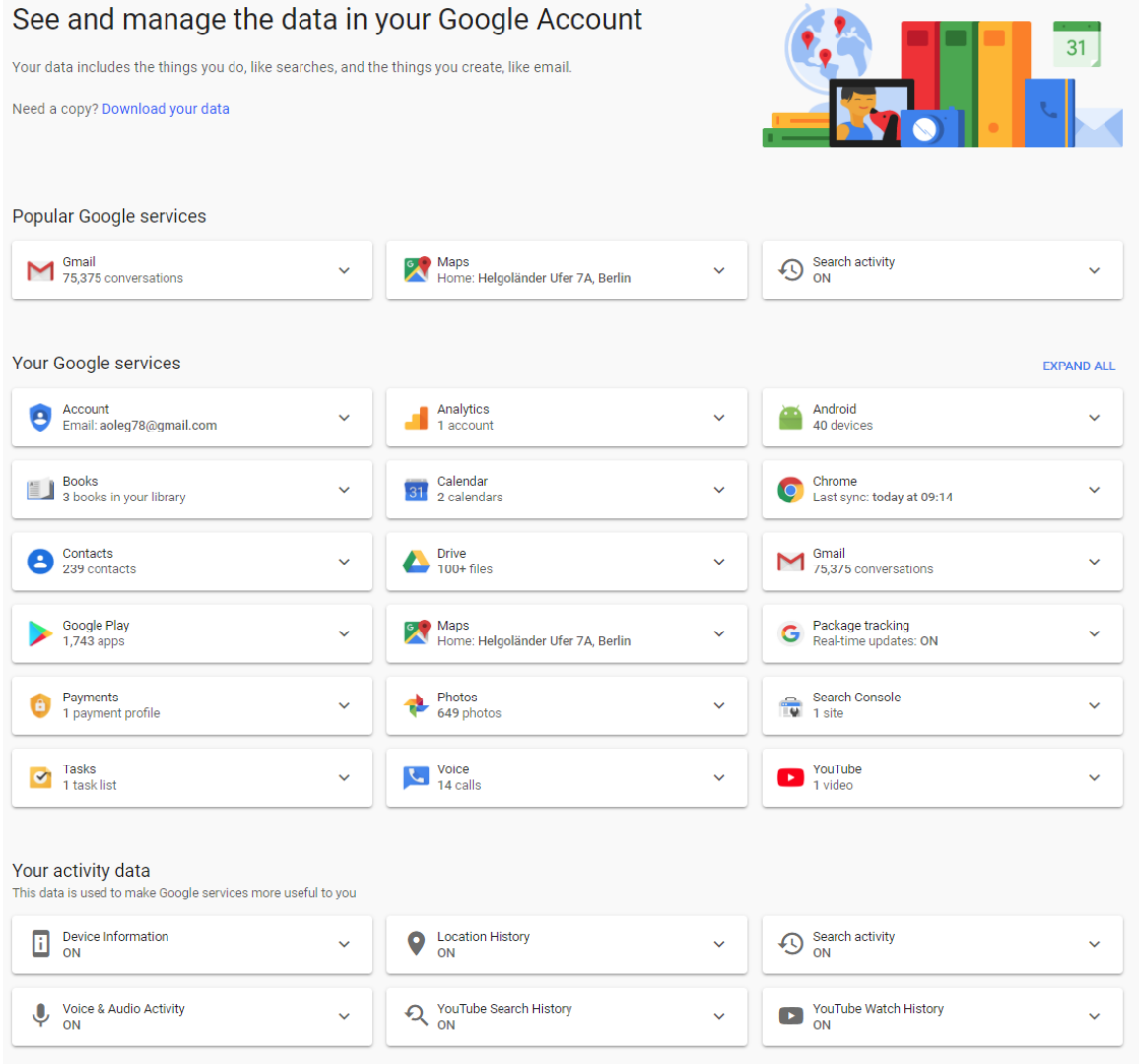
- **Google Digital Wellbeing**
  - Только статистика приложений
  - Ежедневные сводки
  - Синхронизации нет
    - Только при использовании Family Link (только для детей)
  - Статистика по уведомлениям
  - Нет кода или пароля ограничений

Google Dashboard

- Apple синхронизирует Экранное время
- Google – нет
- Google знает меньше?

Это не так!

- **Google Dashboard** содержит подробнейшую информацию об использовании устройств (больше, чем Screen Time и Digital Wellbeing вместе взятые)



Ближайшее будущее

iCloud

Всё больше данных для синхронизации

- Умный дом (HomePod, датчики, термостаты и освещение)
- Экранное время
- Данные, ранее доступные в резервных копиях, будут переноситься в синхронизируемые контейнеры
  - Это уже происходит
  - iOS 13: журнал звонков и история Safari исключены из облачных резервных копий, доступны только в виде синхронизированных записей

Приватность данных

Google Android

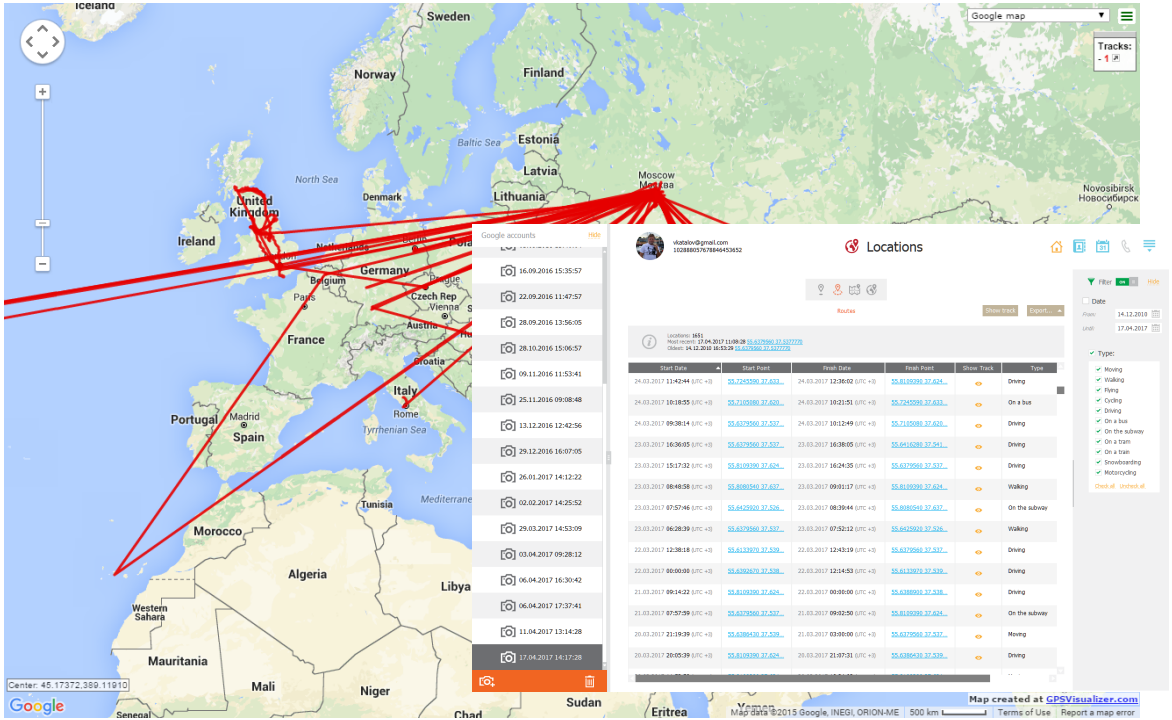
- Многие приложения отслеживает локацию; для этого не нужен доступ к разрешению «Местоположение»
- Любое приложение Android может получить BSSID текущей точки доступа Wi-Fi
- Модно определить локацию (приблизительно) и по IP
- Любое приложение может сканировать список сетей Wi-Fi
  - Единственная точка BSSID позволяет определить местоположение с точностью порядка 20 метров
  - Триангуляция нескольких BSSID ещё точнее
  - Для этого создано множество сервисов, как платных, так и полностью открытых
  - openwlanmap.org

- **Android собирает больше данных, чем iOS**
- **Google собирает больше данных, чем Apple**

Приватность данных

История местоположения Google Location History

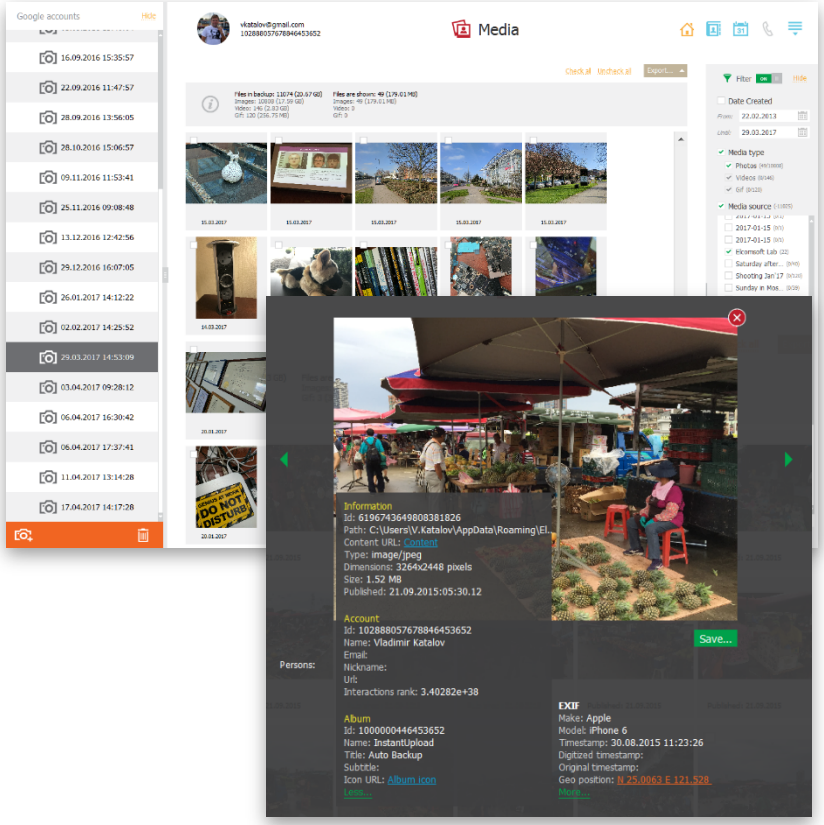
- Подробные и точные данные
- Собираются долгие годы
- Из всех устройств с одним Google Account
- Android, iOS, Windows, Mac
- Сервисы Google в любом браузере
- Координаты, время и дата

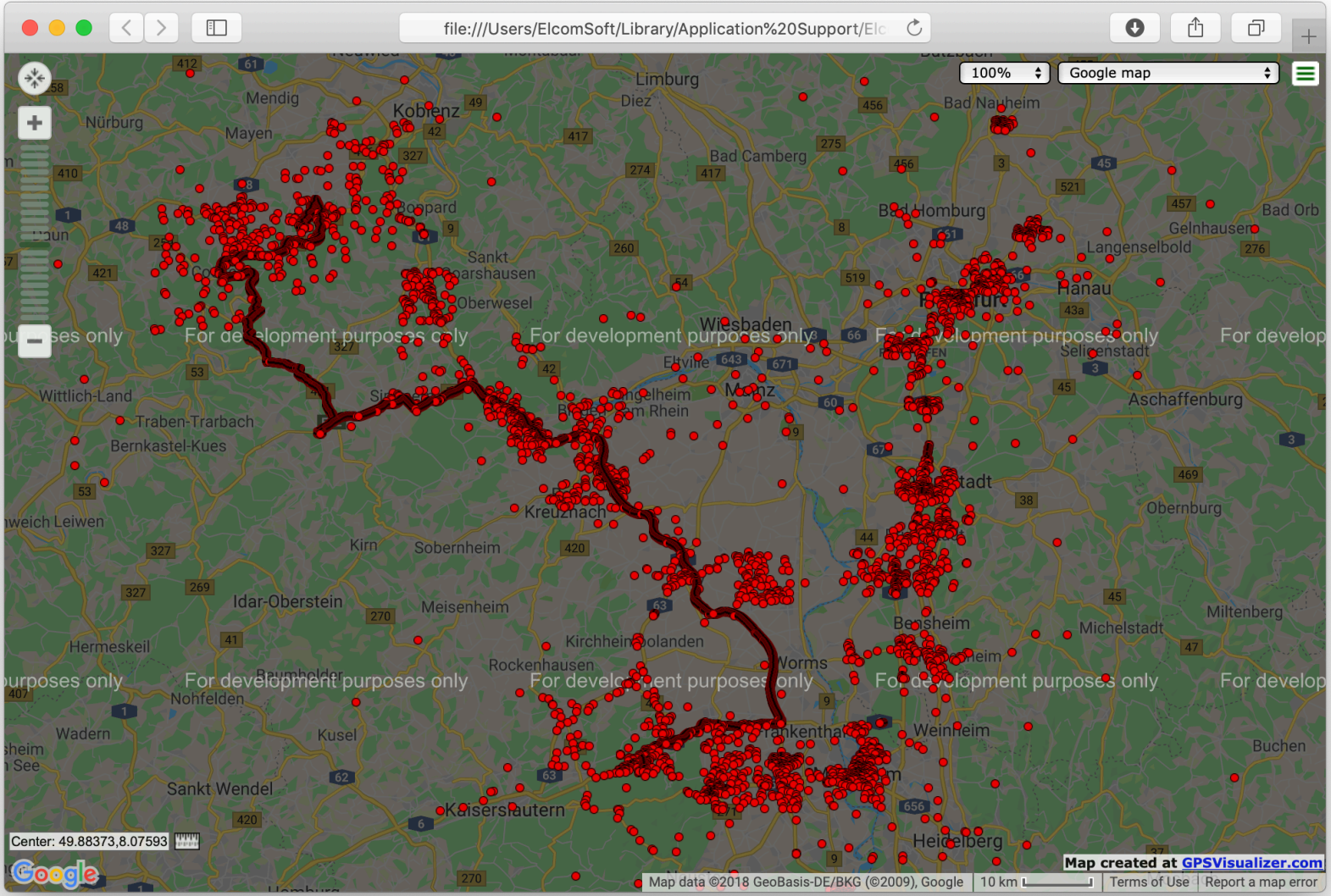


Приватность данных

Фотографии

- Фотографии попадают в Google Photos по умолчанию
- Это бесплатно: сжатые фотографии не учитываются в квоте (для моделей Pixel – не учитываются и несжатые фото)
- Данные доступны в EXIF




file:///Users/ElcomSoft/Library/Application%20Support/Elc
100%
Google map
For development purposes only
Center: 49.88373,8.07593
Map created at GPSVisualizer.com
Map data ©2018 GeoBasis-DE/BKG (©2009), Google
10 km
Terms of Use
Report a map error

Приватность данных

Откуда можно извлечь данные

- Устройство: локальные резервные копии
- Учётная запись: облачные резервные копии
- Устройство: физический доступ
- Данные с устройства, синхронизированные на компьютер пользователя (например, пароли браузера, закладки, история посещений)
- Учётная запись: синхронизированные данные
- Учётная запись: службы Apple Find My Phone, Apple Find Friends. Google Find My Device
- Сторонние сервисы и облака: зависит от владельца сервиса

Apple и закон

Обработка запросов от правоохранительных органов

- Для выдачи информации по запросу не нужны логин и пароль, достаточно Apple ID, серийного номера устройства, IMEI, email
- Если логин и пароль недоступны, запрос может быть единственным способом получить данные

- Бюрократия: сложность и длительность оформления
  - Обработка до двух месяцев
- Apple выдаёт данные в зашифрованном двоичном файле
  - Ключ шифрования прилагается, инструмент для расшифровки – нет
  - Сторонние сервисы и инструменты стоят дополнительных денег
- Apple не выдаёт пароли, сообщения и данные «Здоровья»
  - Используется дополнительное шифрование

Извлечение из облака

Инструменты облачного анализа

- Пароли, сообщения, данные Здоровья и Экранного времени в облаке надёжно зашифрованы (iOS 12, 13)
  - Не предоставляются Apple по запросу от правоохранительных органов
- **Для извлечения данных необходимы:**
  - Соответствующий продукт (например, Elcomsoft Phone Breaker)
  - Логин и пароль от учётной записи Apple ID пользователя
  - Одноразовый код двухфакторной аутентификации (можно получить на SIM-карту в виде SMS)
  - Код блокировки iPhone или пароль от компьютера Mac пользователя

Ваш шпион: что может рассказать о вас ваше мобильное устройство

Владимир Каталов

ООО «Элкомсофт»