Компьютерно-техническая экспертиза

Извлечение данных из мобильных устройств, резервных копий и облачных хранилищ

Экспертиза в мобильных устройствах

Сравнение методов извлечения информации: физический доступ, логический доступ и доступ к облачным хранилищам.

Используемые подходы, типичные проблемы

О компании

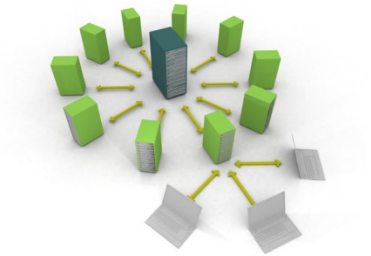
- Образована 1990 году
- Форма собственности - общество с ограниченной ответственностью
- Головной офис в Москве
- Около 20 разработчиков
- Выделенная исследовательская команда из 6 специалистов
- Разработки и исследования безопасности проводятся только внутри компании
- Microsoft Certified Partner
- Intel Software Partner (Premier Elite)
- Партнёр AMD и NVIDIA
- Более 400,000 пользователей в 100+ странах

Microsoft Partner
Gold Application Development
Gold Intelligent Systems

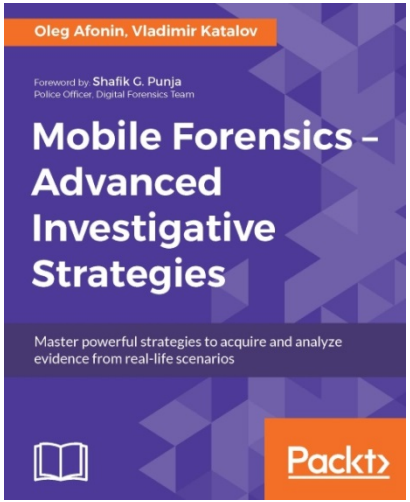
intel Software Partner

Доступ к зашифрованным данным

- **Поддержка сотен форматов данных и приложений**
  - Офисные документы, архивы, базы данных
  - Интернет-браузеры, программы мгновенного обмена сообщениями, почтовые программы
  - Системные пароли (Windows, UNIX, macOS)
  - Менеджеры паролей
  - Резервные копии
- **Восстановление паролей к сотням форматов данных**
  - Ускорение на GPU (в ~50-200 раз быстрее, чем CPU)
  - Thunder tables (мгновенная расшифровка 40-битного шифрования)
- **Исключительная скорость благодаря собственным разработкам**
  - Ускорение на видеокартах (в ~50-200 раз)
  - Мгновенная расшифровка Word/Excel/PDF (40-битное шифрование)
  - Сброс пароля там, где это возможно (нет необходимости восстанавливать
- **Распределённые вычисления**
  - Работа в локальной или глобальной сети
  - Линейное масштабирование
  - Использование незадействованных ресурсов, планировка
  - Управление очередью задач
- **Работа с популярными криптоконтейнерами**
  - BitLocker, FileVault 2, PGP, TrueCrypt, VeraCrypt, McAfee, LUKS
  - Автоматический детект используемого шифрования
  - Нахождение ключа шифрования в памяти или hibernation-файле
  - Монтирование или расшифровка с использованием пароля, ключа шифрования или ключа восстановления

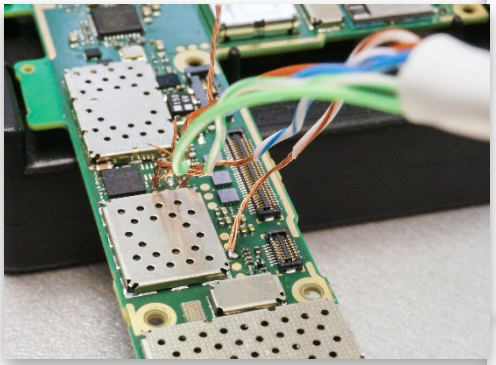


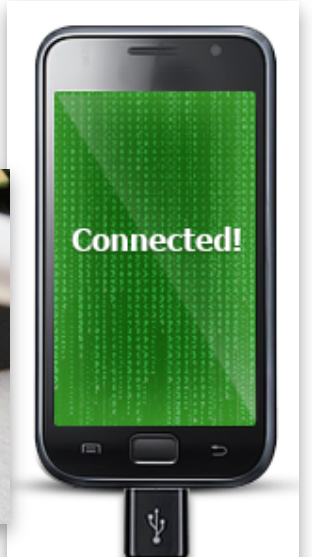
Timeline



- **2002**: Выигран процесс “Соединённые Штаты против ElcomSoft” (https://www.cnet.com/news/elcomsoft-verdict-not-guilty/)
- **2007**: Обнаружена «ход для спецслужб» в Quicken (http://www.theregister.co.uk/2007/06/23/quicken_password_backdoor/)
- **2007**: Патент на аппаратное ускорение с помощью видеокарт (https://www.elcomsoft.com/news/135.html)
- **2008**: Расшифровка 40-битного шифрования в PDF & Word (http://www.prweb.com/releases/thunder/tables/prweb1324054.htm)
- **2010**: Взлом шифрования iOS (http://www.pcworld.com/article/202629/article.html)
- **2011**: Восстановление паролей BlackBerry (https://blog.elcomsoft.com/2011/09/recovering-blackberry-device-passwords/)
- **2013**: Извлечение резервных копий из iCloud (https://www.elcomsoft.com/news/556.html)
- **2014**: Расшифровка резервных копий BlackBerry 10 (https://blog.elcomsoft.com/2014/05/phone-password-breaker-3/#bb10)
- **2014**: Доступ в iCloud без Apple ID и пароля: (https://www.elcomsoft.com/news/584.html)
- **2015**: Извлечение данных Google (http://www.prnewswire.com/news-releases/elcomsoft-cloud-explorer-forensic-acquisition-of-google-accounts-563228681.html)
- **2016**: Удалённые фотографии остаются в iCloud (https://blog.elcomsoft.com/2016/08/icloud-photo-library-all-your-photos-are-belong-to-us/)
- **2016**: Моментальный доступ к истории звонков и синхронизированным данным (https://blog.elcomsoft.com/2016/11/iphone-user-your-calls-go-to-icloud/)
- **2017**: Извлечение паролей и номеров кредитных карт из Apple iCloud, облачные вычисления на Amazon EC2, доступ к данным Microsoft Account (звонки, переписка, интернет-активность, Skype), расшифровка данных WhatsApp, работа с облачными резервнами копиями Android, […]

Способы получения информации





- **Физический доступ**
  - Android, некоторые Windows-устройства
- **Логический доступ (резервные копии)**
  - Android*, Apple iOS
- **Беспроводное (облачное) извлечение**
  - Google, Apple iOS, Windows-устройства
- *Иногда работают другие способы, но они небезопасны и ненадёжны*

Физическое извлечение (iOS)

- До iPhone 4 включительно: почти полный доступ даже, если не удастся взломать пароль
- iPhone 4S/5/5S/5C/6/6S/7: не можем взломать пароль, но если он известен, возможно извлечение (после установки jailbreak) – существенно *больше*, чем логическим извлечением:
  - Уже загруженная на устройство почта
  - История передвижений за последние 45 дней
  - История подключений к сотовым и беспроводным сетям
  - Журналы активности устройства (включение-выключение, разблокирование, подключение гарнитуры, установка и запуск приложений
  - Данные приложений (социальные сети, переписка в программах обмена сообщениями: Telegram, Signal и т.д.)

Почему предпочтителен удаленный доступ?

- Помогает разбираться с **заблокированными** и **зашифрованными** устройствами
- Практически не зависит от модели устройства и версии системного ПО
- Последняя надежда, когда все другие методы исключены
- Облачные резервные копии включены по умолчанию в устройствах Apple; если нет, обычно включена как минимум синхронизация
- Google собирает информацию со **всех** устройств, с которых был произведен вход в учетную запись
- Учетная запись в облаке может содержать больше данных, чем само физическое устройство

Облачные экосистемы

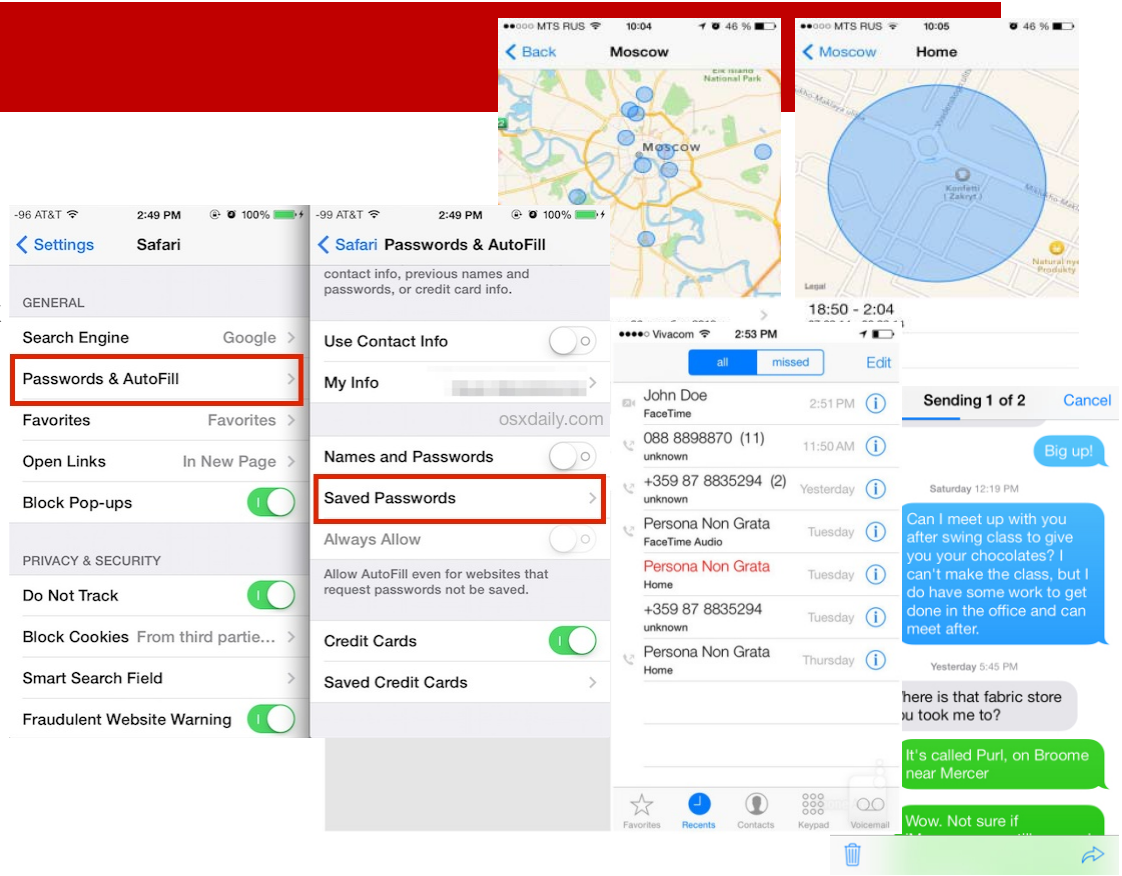
- **Apple iOS**
  - В облаке хранятся полные резервные копии
  - Много данных попадает в облако в рамках синхронизации
  - Облачное хранилище: iCloud Drive
- **Google/Android *(и/или)***
  - Резервные копии практически бесполезны
  - Основной механизм – синхронизация
  - Облачное хранилище: Google Drive
- **Windows Phone, Windows 10 Mobile**
  - Ограниченное количество данных в резервных копиях
  - Часть информации с устройств синхронизируются
  - Собираются данные и с настольных систем
  - Облачное хранилище: Microsoft OneDrive

Облако Apple (iCloud)

- Впервые появилось в октябре 2011 в iOS 5
- 5 GB бесплатно, далее платно вплоть до 2 ТБ
- Помимо резервных копий в облаке хранятся документы, заметки, календари, данные геолокации и многое другое
- Синхронизация данных между устройствами
- Фото и видео (iCloud Photo Library)
- *Пароли и номера кредитных карт*

Облако Apple это…

- Контакты
- Журнал звонков и СМС
- Переписка в социальных сетях и программах обмена сообщениями
- Календари и события
- *Почта*
- Интернет-активность (посещения, поиск)
- Документы, настройки и базы данных
- Фото и видео
- Данные приложений
- Уведомления
- …и многое другое



Получение данных из Apple iCloud

У вас есть:

- Apple ID и пароль

или

- Маркер аутентификации (authentication token)

Прблемы:

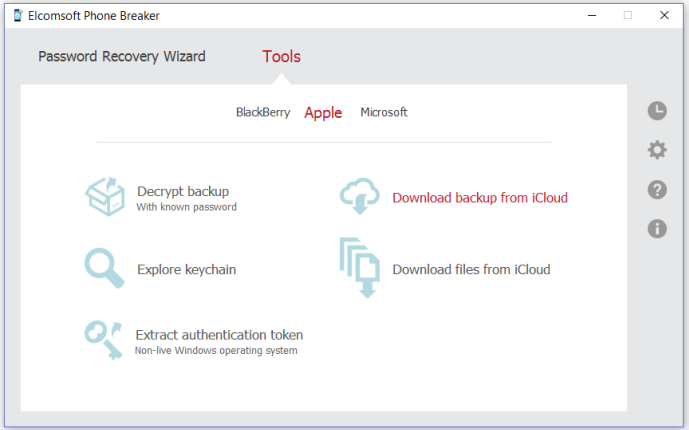
- Может использоваться двухфакторная аутентификация (2FA), но - используя токен, её можно обойти
- Если вход осуществляется по паролю, владелец устройства может получить уведомление
- Пароли и данные кредитных карт дополнительно защищены
- Извлечение всех данных – долгий процесс, но есть возможность выборочного доступа (только к нужным категориям)

Доступ к данным – это нетривиальная задача

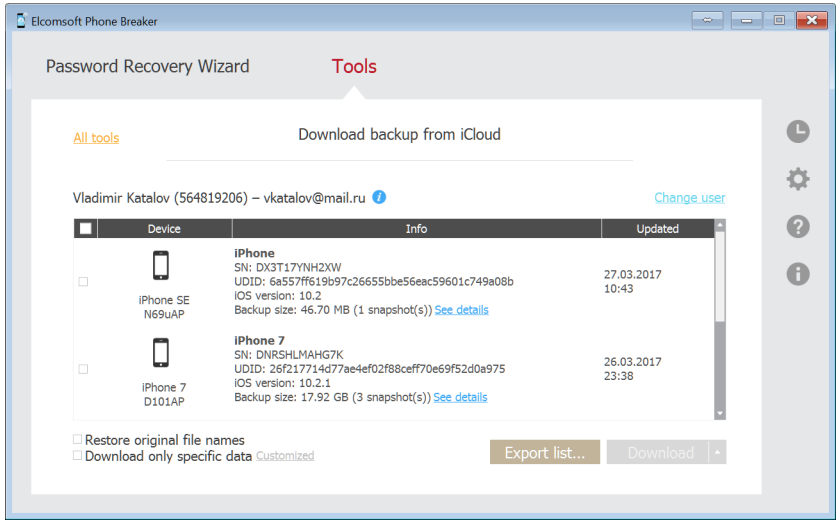
- Данные зашифрованы и находятся в хранилищах сторонних поставщиков услуг (Amazon, Microsoft, Google)
- Apple имеет ключ шифрования к этим данным
- Некоторые данные (пароли, данные о здоровье, данные кредитных карт) дополнительно зашифрованы, используя специальные ключи, привязанные к конкретному устройству

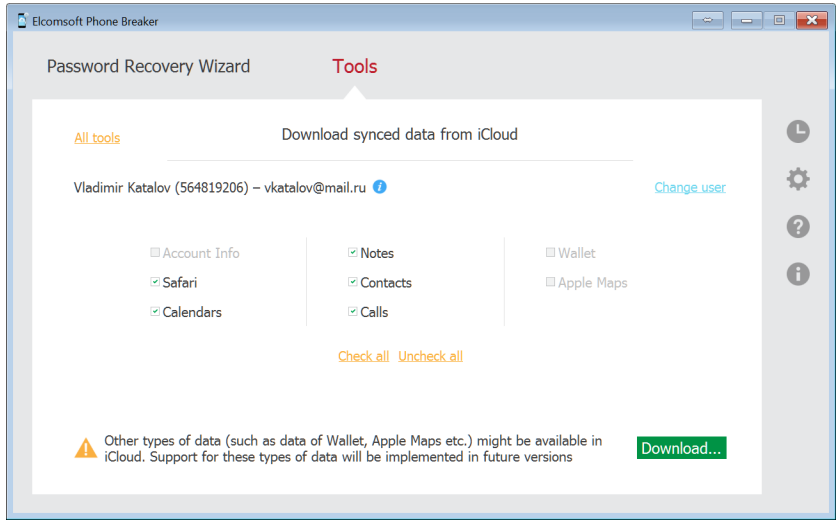
Доступ к Apple iCloud

- Возможен выборочный доступ к данным:
  - сообщения
  - журнал звонков
  - адресная книга,
  - заметки
  - календари
  - фото/видео
  - документы
  - данные приложений
  - интернет-активность (история посещений и поиска)
- *По фото можно восстановить данные геолокации*
- *Часто можно получить доступ к облачной «связке ключей», с данными других учётных записей, социальных сетей, мессенджеров и т.д.*

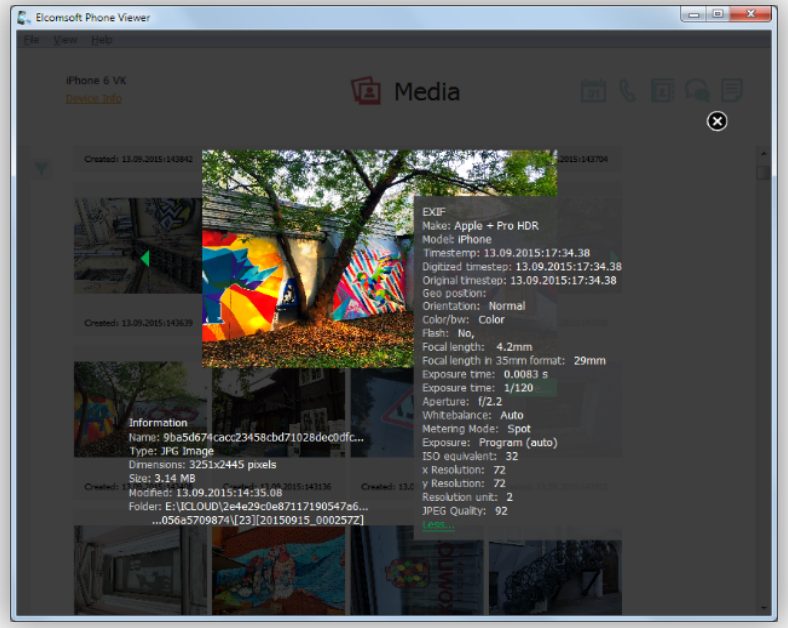


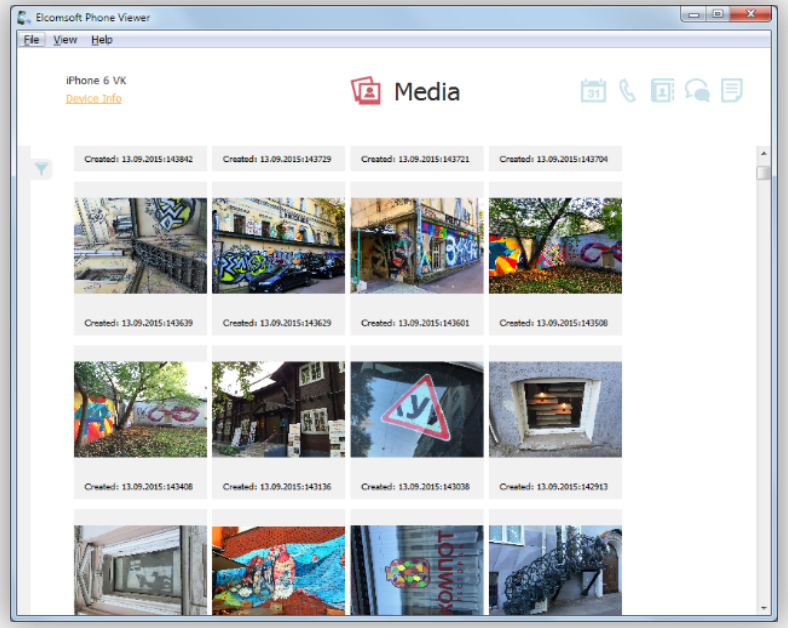
Доступ к Apple iCloud





iCloud Photo Library: *только в облаке*



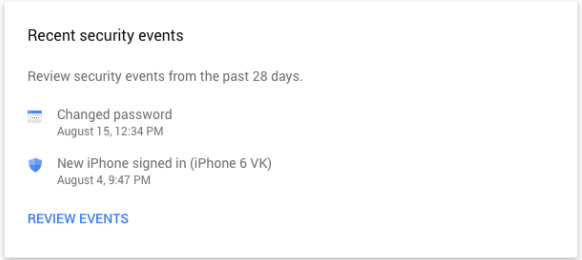


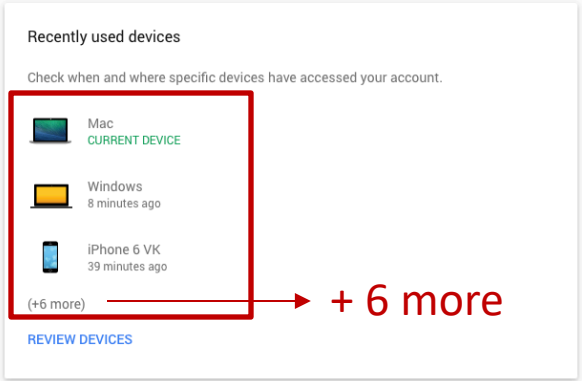
Android vs. Google

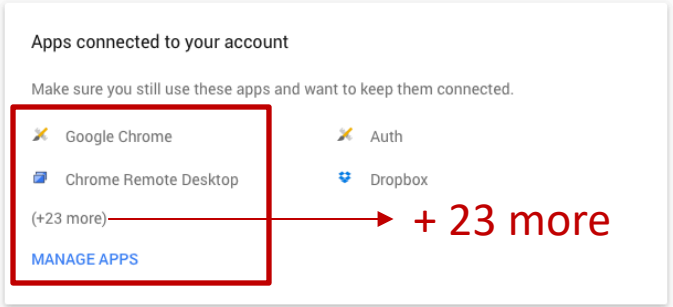
- Рынок Android-устройств сильно фрагментирован (*десятки тысяч*)
- Нет и не может быть универсального решения для извлечения данных из Android-устройств
- Google – это не только Android
- Google собирает данные из других источников, если пользователь зарегистрировался
  - Chrome browser (интернет-активность)
  - Google Maps (карты)
  - Gmail (почта)
  - Google search (поиск)
- **Включая конкурирующие платформы** (iOS, Windows Phone/Mobile, PC/Mac, другие)

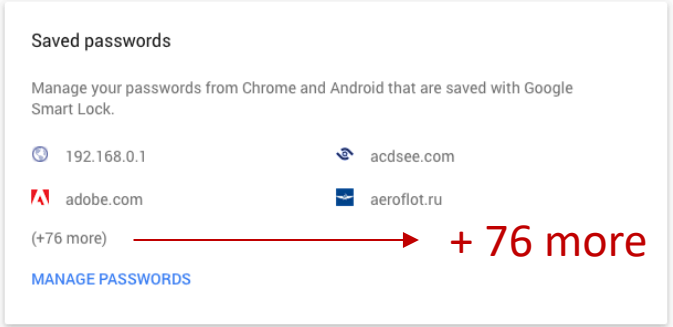
Google собирает данные из множества источников

- Множество устройств
  - Mac
  - Windows
  - iPhone
  - iPad
  - …и Android
- Приложения
  - Dropbox
  - Auth
  - Chrome
  - Remote desktop
  - Many more









Google Account: что внутри

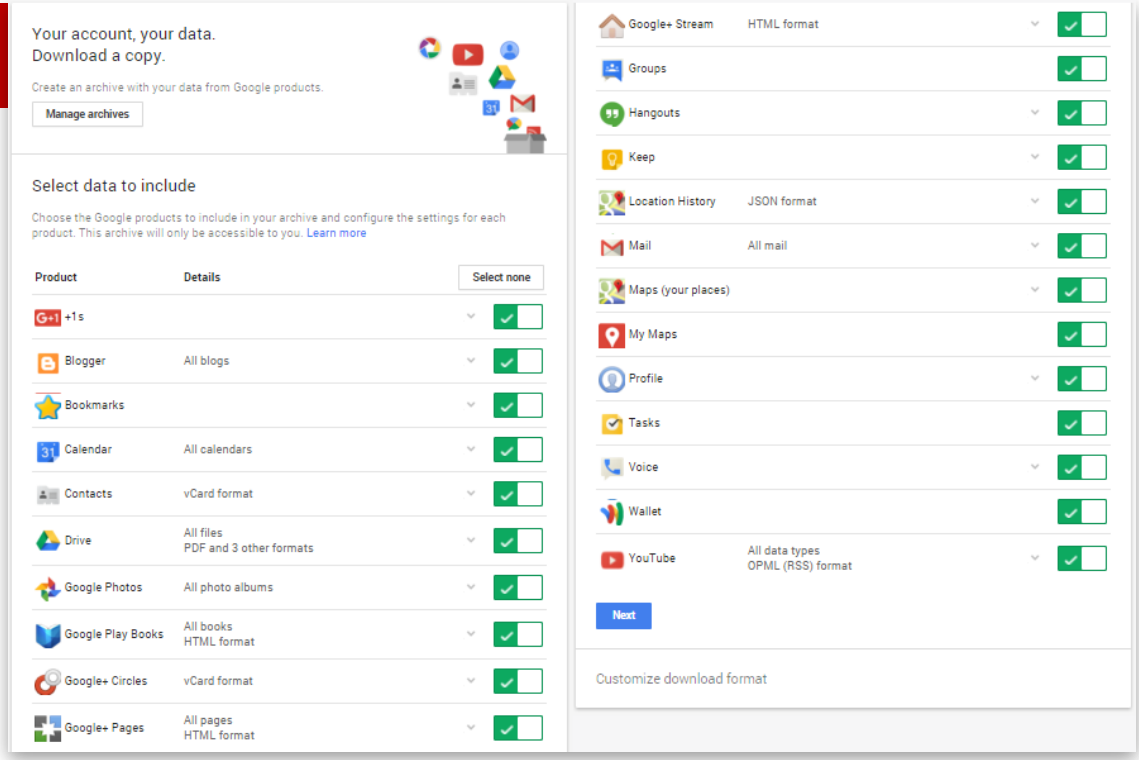
- Данные пользователя (возраст, интересы и т.д.)
- Все привязанные устройства
- Активности приложений, доступ к сервисам
- Контакты, календари, задачи, заметки
- Почта
- Альбомы (фото/видео)
- Чаты Hangouts
- Данные о здоровье/активностях (Google Fit)
- Передвижения, места
- Chrome
  - История
  - Сохраненные пароли и данные для автозаполнения
  - Закладки
  - История поиска
  - Множество статистической информации

Топ приложений для смартфонов (Google: 3 из 5)

- Facebook
- **YouTube**
- Facebook Messenger
- **Google Search**
- **Google Play**

Google Takeout

- Оставляет много следов
- Не вся информация экспортируется
- Ограниченная гибкость
- Множество странных и неудобных форматов
- Безумно медленно
- При доступе с «необычного» IP доступ может блокироваться



Google

New sign-in from Chrome on Windows

Hi Vladimir,
Your Google Account vkatalov@gmail.com was just used to sign in from Chrome on Windows.

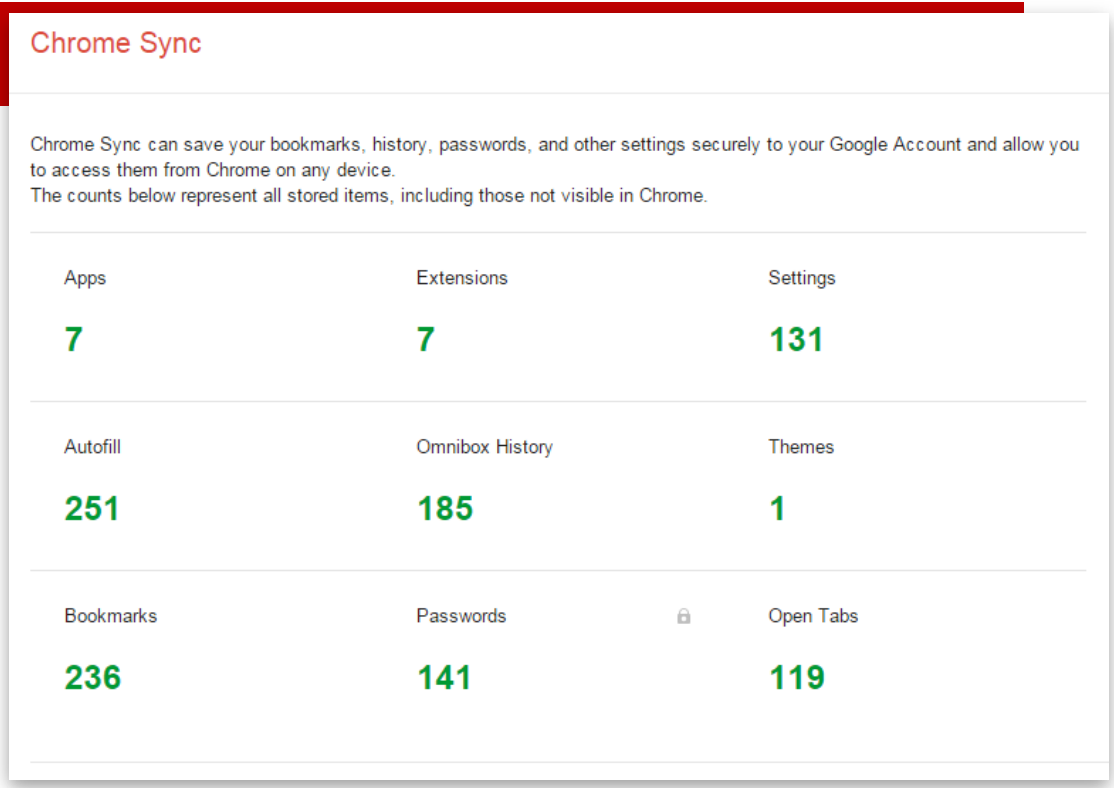
Vladimir Katalov
vkatalov@gmail.com

Windows
Wednesday, March 29, 2017 2:53 PM (Moscow Time)
Russia*
Chrome

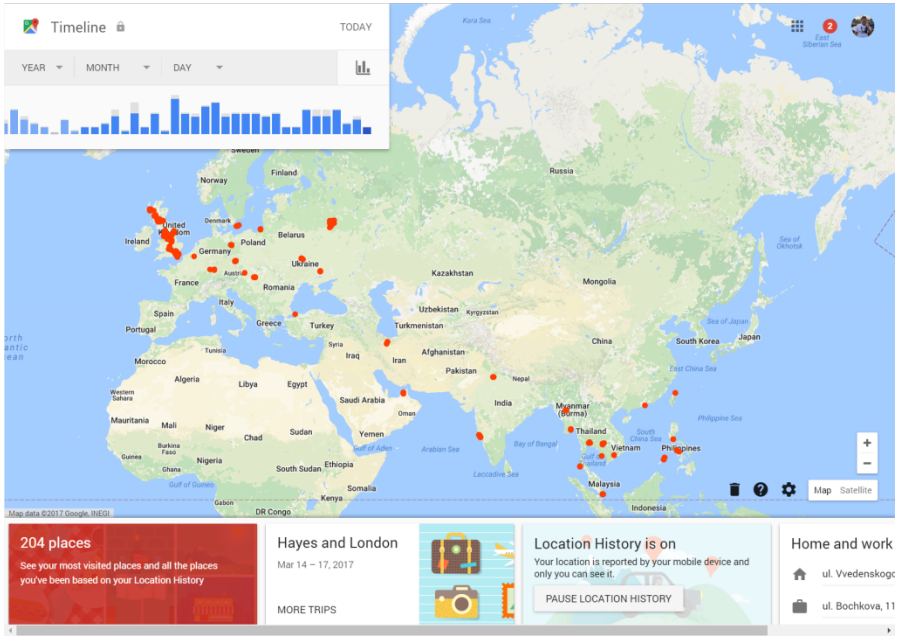
Don't recognize this activity?
Review your recently used devices now.

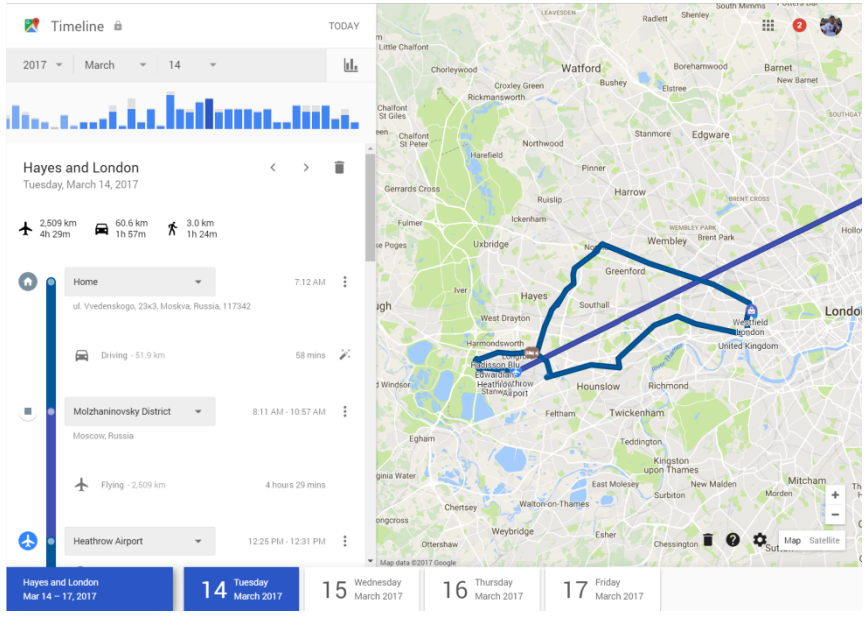
Chrome

- **Все устройства**
- Закладки
- История сёрфинга
- Открытые вкладки
- Формы
- Пароли
- Переходы страниц

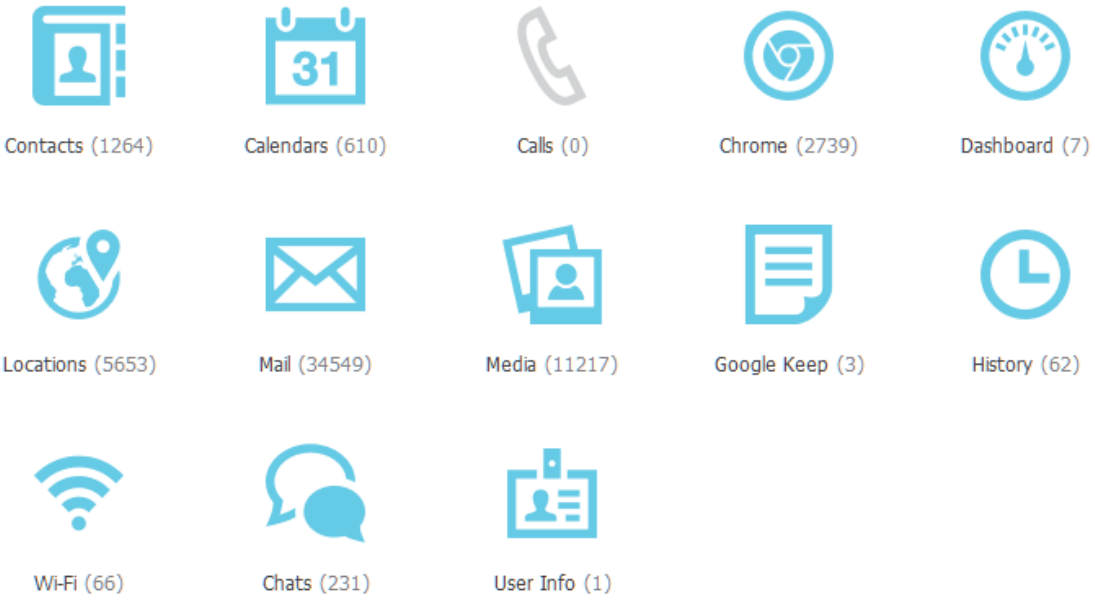


Google Timeline





Что можно получить через Elcomsoft Cloud Explorer



Google Dashboard – то, что недоступно через Google Takeout

Учётная запись
- email
- number of Google API clients (sites and apps)
- account time: personal, work, both
- Activities in last 28 days
    - browsers and OSs that had access
    - locations
    - new apps and sites

YouTube
- number of videos and playlists loaded
- user name
- sex
- last video rating (+video name and date)
- activities for last 28 days
    - number of views, by day
    - total views
    - searches
    - likes and dislikes

История поиска
- last Web search
- last image search
- last news search
- last video search
- last maps search
- last books search
- activities for last 28 days
    - top 10 searches
    - percentage of searches by category (web, image etc.)
    - activity (by day)

Синхронизация Google
- number of bookmarks
- last sync date
- number of passwords
- number of Chrome extensions

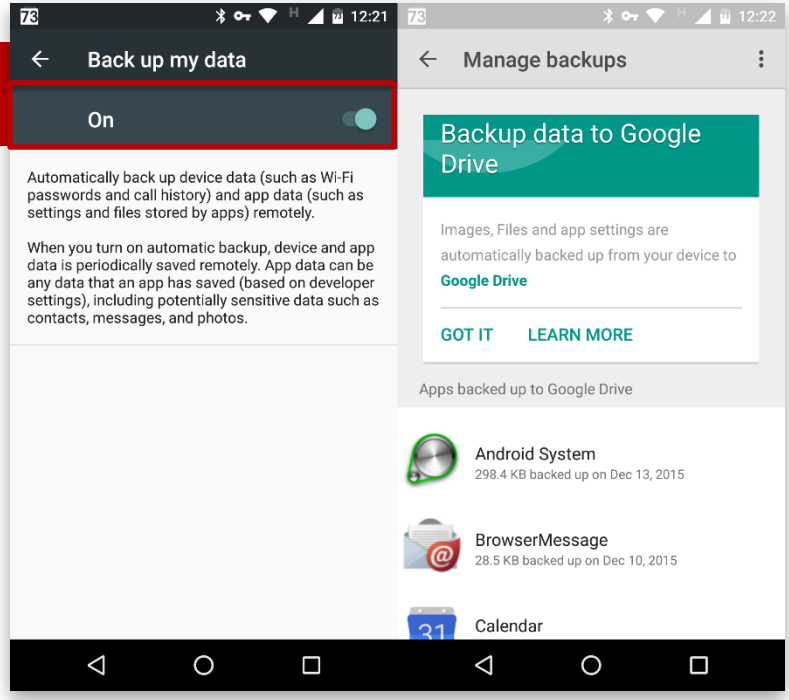
Данные профиля
- Google+ name
- profile URL
- number of phone numbers
- number of "+1"

Почта
- number of mail threads
- last thread subject
- number of messages in inbox
- last incoming message subject
- number of sent mails
- last sent mail subject

Андроид
- make, model
- first auth date/time
- last activity date/time
- apps that backup their data (name, date, size)

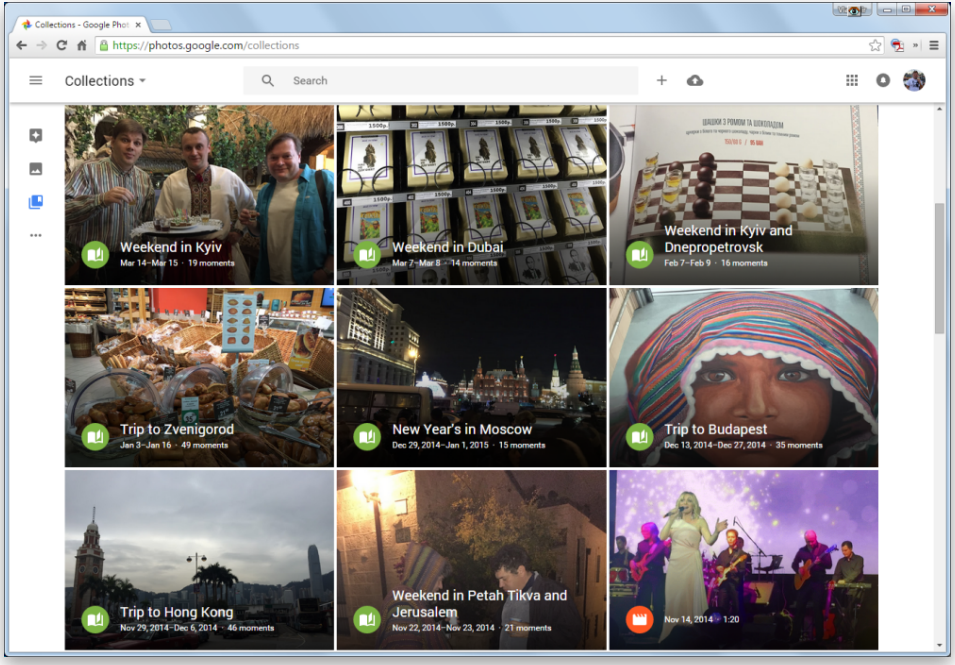
Резервные копии Android

- Настройки календарей
- Беспроводные сети & пароли
- Обои домашнего экрана
- Настройки почты
- Установленные приложения
- Настройки языка
- Дата и время
- Настройки сторонних программ и их данные (очень ограниченно)
- *Журнал звонков*
- *SMS*



Google Photos

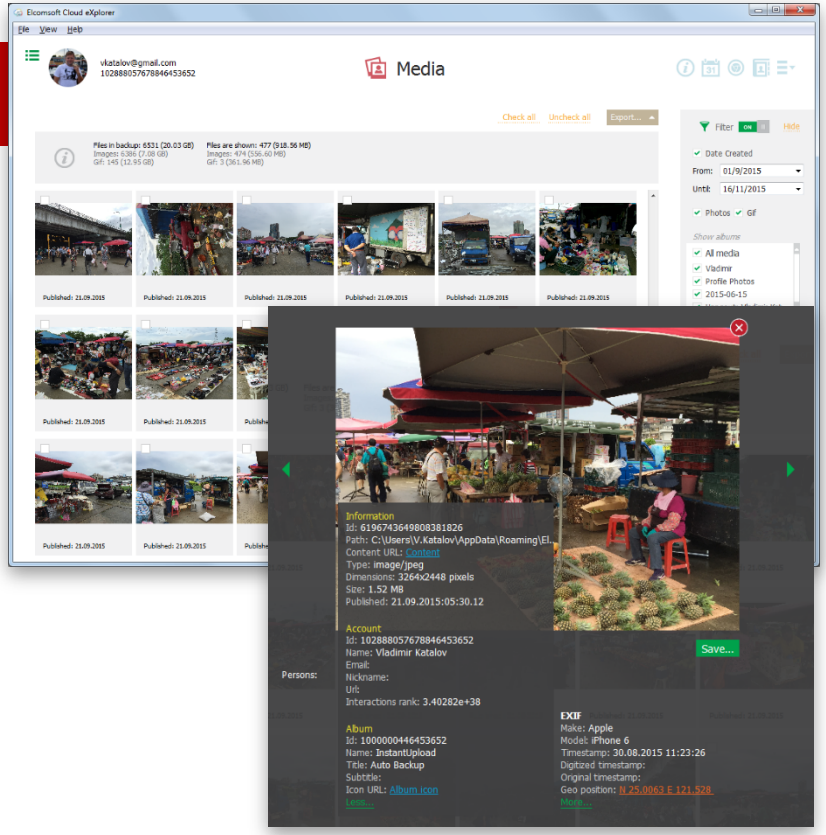
- Альбомы/события
- Комментарии
- EXIF (дата, параметры)
- Геолокации
- Отмеченные люди



Экспертиза в мобильных устройствах

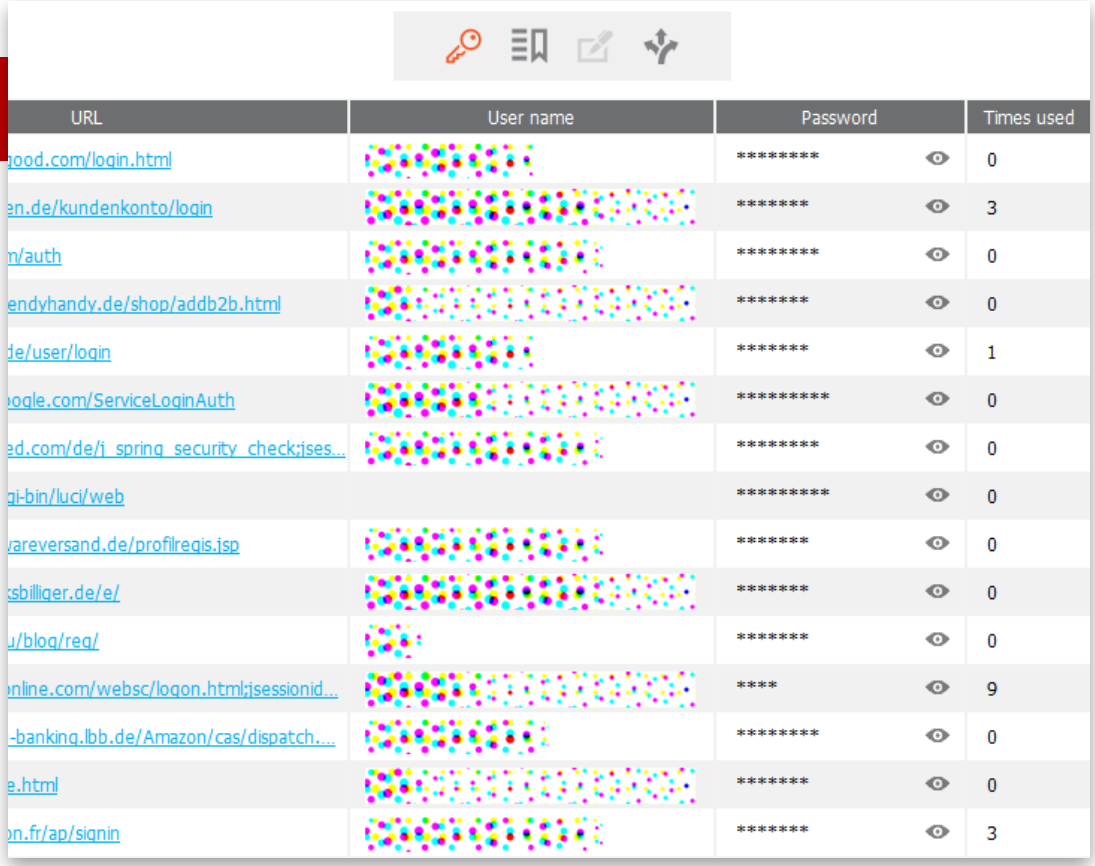
Медиа

- Фото со всех устройств пользователя могут быть выгружены в Google Photos
- И могут быть загружены через Elcomsoft Cloud Explorer или вручную через Google Drive
- Google Photos - **это не то же самое, что и** Google Drive!
- Дополнительная информация (т.е. метки лиц, данные о местоположении, данные об адресе)
- Elcomsoft Cloud Explorer использует Google Photos для получения полного доступа к метаданным изображений



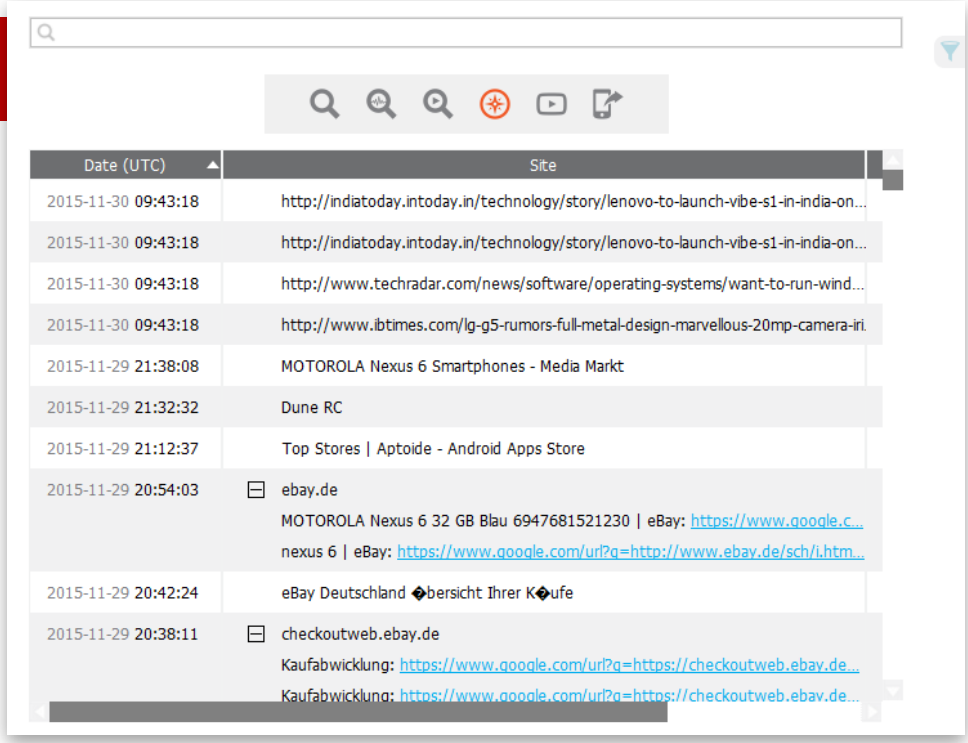
Пароли

- Данные из Google Chrome
- Пароли синхронизованы между устройствами
- Не только Android
- **Screenshot**: мы маскировали реальные имена пользователей и пароли :)
- Также: закладки, переходы страниц



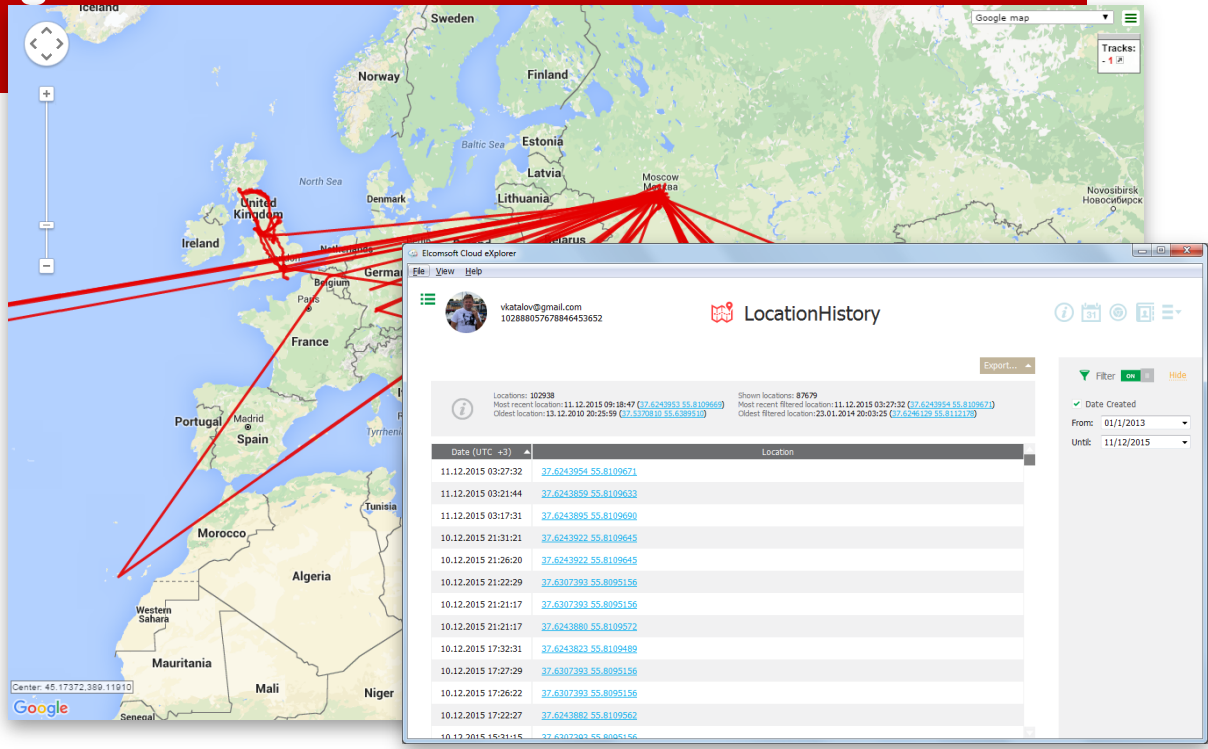
История поиска

- Можно просматривать в виде дерева
- Удобная группировка по доменным адресам
- Заголовок страницы и URL (там, где это возможно)

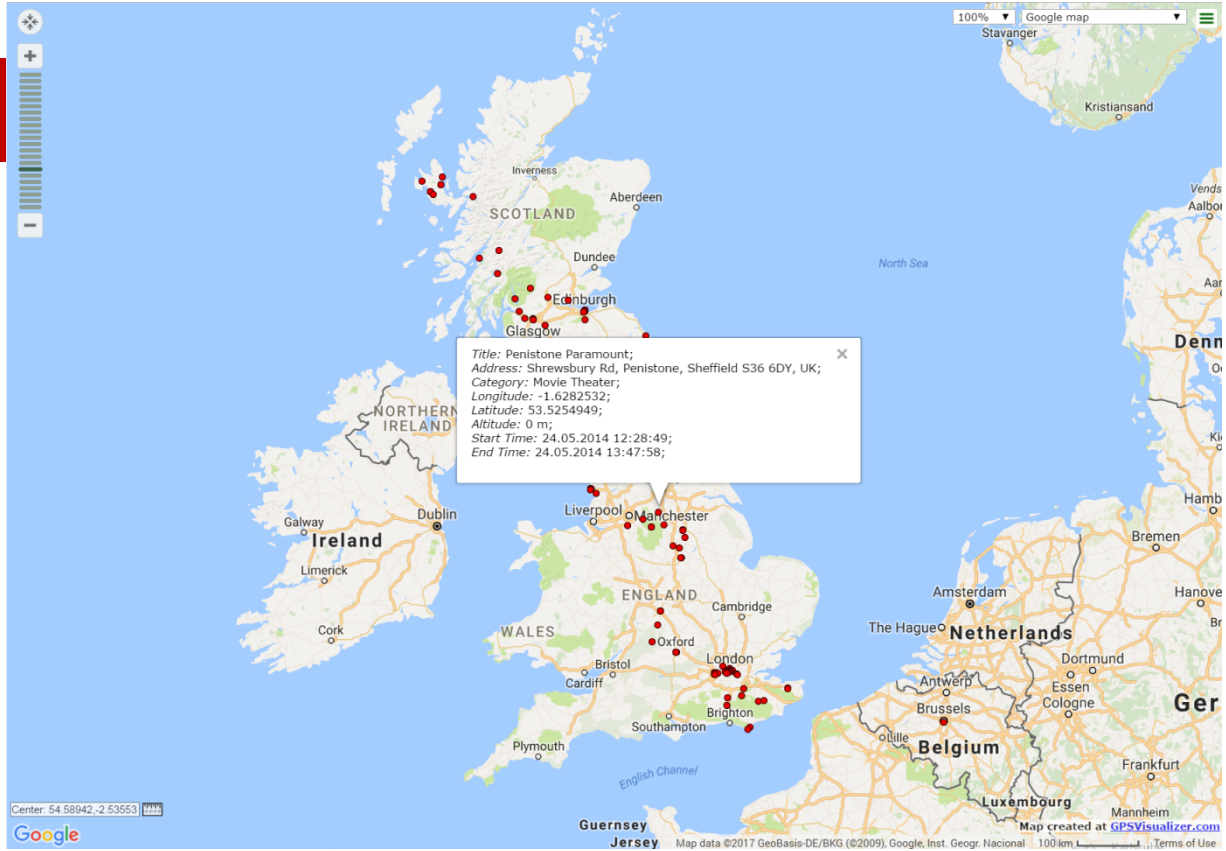


Местоположения: Google Timeline vs. Elcomsoft Cloud Explorer

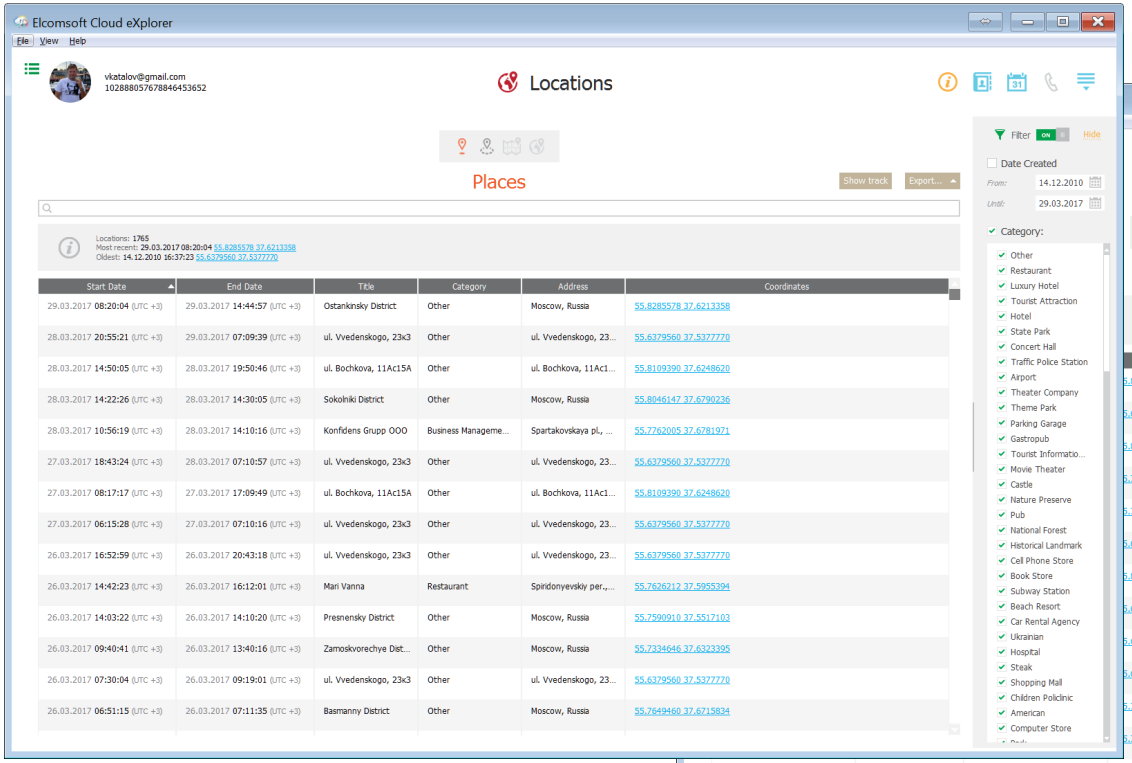
- Можно выбирать диапазон дат
- Настраиваемый масштаб
- Места и маршруты
- Просмотр в виде списка и в виде карты

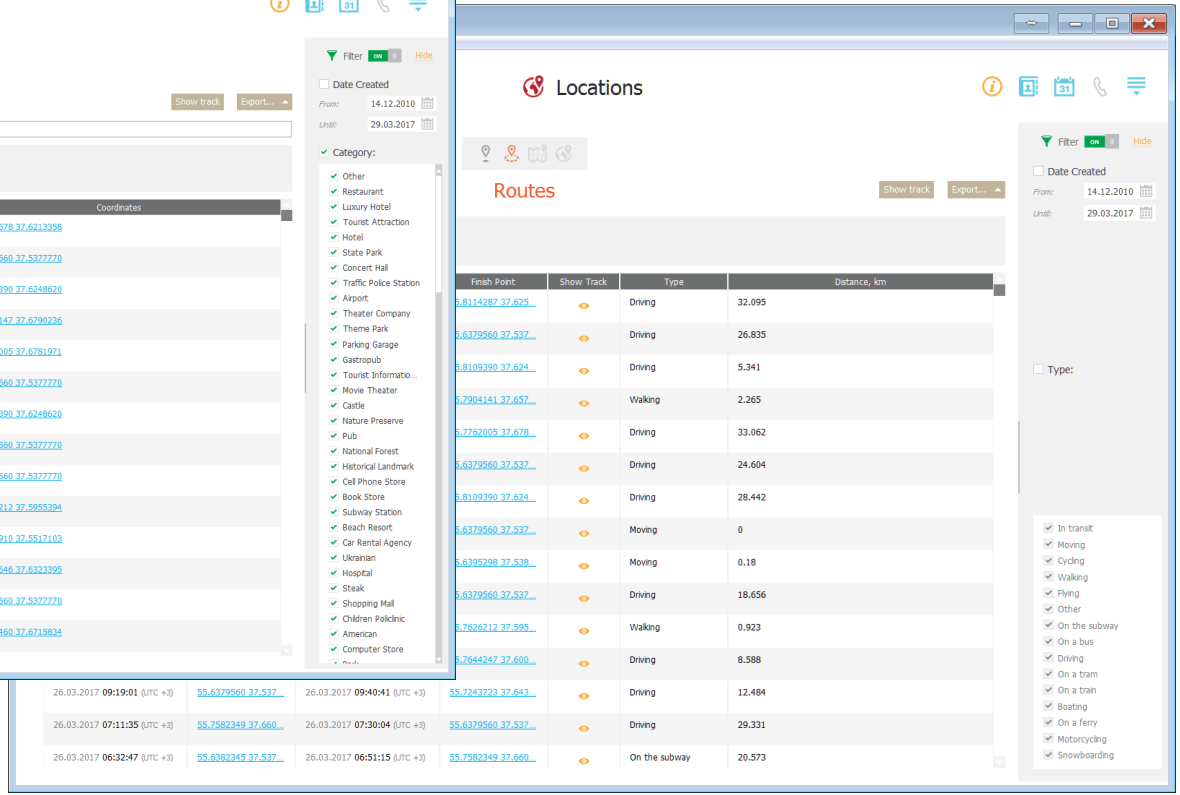


Местоположения



Экспертиза в мобильных устройствах





Учетные записи Microsoft

- Windows 8/10 (Mobile) и более поздние версии имеют развитую систему облачных резервных копий, концептуально схожую с iOS
  - Журнал звонков
  - SMS
- Синхронизируемые данные (+Desktop):
  - Контакты
  - Заметки
  - Пароли
  - История посещений
  - История поиска
  - Переписка и звонки Skype
  - Данные о здоровье (HealthVault)
  - Голосовое управление/поиск (Cortana)

Спасибо!